CygNet Bridge Installation Guide

Release Dates:

CygNet Bridge v4.6 compatible with CygNet v9.7, April 3, 2023

CygNet Bridge v4.5 compatible with CygNet v9.6, March 2, 2022

CygNet Bridge v4.4 compatible with CygNet v9.5, July 2, 2021

This document provides important information to help you get started, prepare your system, install, upgrade, and configure **CygNet Bridge** application and its companion applications:

- **CygNet Mobile**
- **CygNet Dispatch**
- **CygNet Bridge API**

This document provides the *same* content as is available in the main CygNet Help.

Contents

CHAPTER 1: About CygNet Bridge

This chapter introduces CygNet Bridge and provides an overview of the application, licensing information, and how to access other user assistance. Also includes the system requirements to run CygNet Bridge.

In this chapter:

CygNet Bridge

CygNet Bridge is a set of services provided to run outside of a CygNet network so that CygNet production data can be made available to consumers who require access to CygNet data, but are external to a CygNet installation. The following optional CygNet products utilize CygNet Bridge for this purpose:

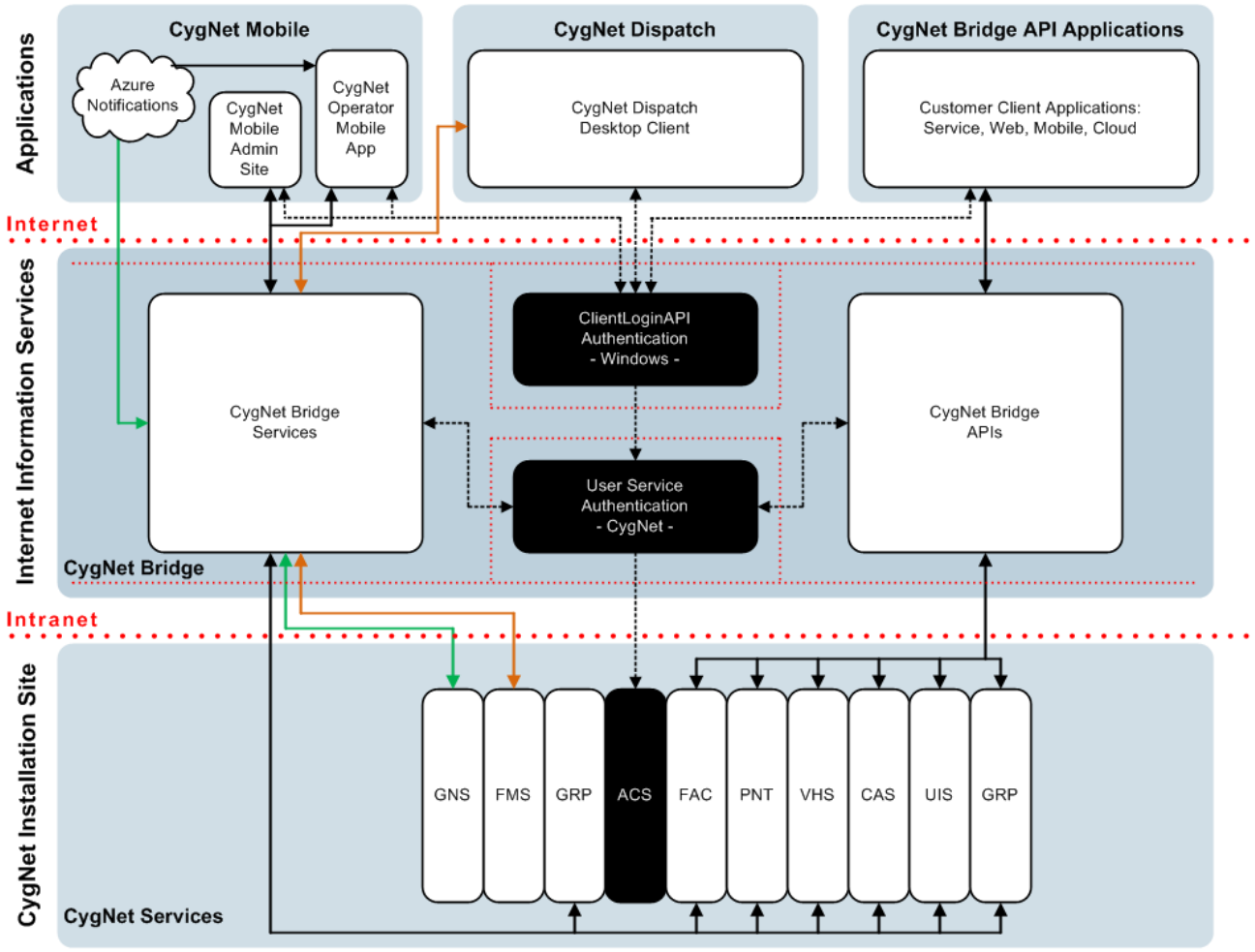
- CygNet Mobile
- CygNet Dispatch (operates in conjunction with CygNet Measurement)
- CygNet Bridge API
- CygNet OPC UA Server

These CygNet products require connection via an instance of CygNet Bridge to securely connect to a CygNet installation for CygNet data access.

> **Note:** CygNet Bridge v4.6 is required for interoperability with CygNet v9.7. Refer to the **CygNet Release Documents** for additional version compatibility information.

Architecture

The following diagram shows how CygNet Mobile, CygNet Dispatch, and CygNet Bridge API communicate with CygNet services via Bridge services.



CygNet Bridge Architecture

CygNet Bridge License

CygNet Bridge is licensed in conjunction with its companion products: CygNet Mobile, CygNet Dispatch, CygNet Bridge API and/or CygNet OPC UA Server, each of which must be licensed separately from existing CygNet SCADA or CygNet Measurement components. Trial or full licenses are available.

For more information about obtaining and licensing CygNet Bridge and associated products, contact your Account Manager.

Install CygNet Bridge

For software version requirements, and for specific considerations appropriate for all components you plan to install, verify and comply with requirements listed in the CygNet system requirements. See the **CygNet System Requirements** document for more information.

Once all system requirements are met, for CygNet Bridge and any companion products you plan to install, install CygNet Bridge using the CygNet Bridge Setup installer.

Installing CygNet Bridge concludes with the addition of your selected CygNet components:

1. Prepare your system for CygNet Bridge, and select component features

   See Preparing your System for CygNet Bridge for more information.

2. Install CygNet Bridge using the CygNet Bridge Installer (CygNet Bridge Setup.exe)

   See Installing CygNet Bridge for more information.

After your CygNet Bridge installation is complete, perform any additional tasks required for the companion feature (s) selected for your installation.

Access CygNet Bridge User Assistance

Other portions of the CygNet Help relate to **CygNet Bridge** usage and preparation of your system for the components utilizing it. The following sections may prove helpful:

- CygNet Mobile
- CygNet Dispatch
- CygNet Bridge API
- CygNet OPC UA Server
- Security Reference for CygNet Bridge Applications

About this Installation Guide

The CygNet Bridge Installation Guide introduces the CygNet Bridge Setup installer (CygNet Bridge Setup.exe) and describes how to install the CygNet Bridge software to operate with your selected companion features. Refer to the CygNet Help for more information and usage guidance.

In this document, installation tasks are described in the order in which they should be considered or performed.

After you finish the installation, if you plan to use CygNet Mobile, you will need to configure CygNet Mobile as described in the CygNet Mobile Help.

The CygNet Bridge Installation Guide includes the following sections:

- Chapter 1: About CygNet Bridge — This chapter introduces CygNet Bridge and provides an overview of the application, licensing information, and how to access other user assistance. Also includes the system requirements to run CygNet Bridge.
- Chapter 2: Installing CygNet Bridge — This chapter describes how to prepare your machine and CygNet software for CygNet Bridge, how to install and update CygNet Bridge, and some tips for troubleshooting potential issues.
- Chapter 3: Installing CygNet Mobile — This chapter introduces CygNet Mobile, how to prepare your system for CygNet Mobile, how to install CygNet Mobile, how to install and configure the CygNet Mobile notification plugin, and some tips for troubleshooting potential issues.
- Chapter 4: Installing CygNet Dispatch — This chapter introduces CygNet Dispatch, how to prepare your system for CygNet Dispatch, how to install and update CygNet Dispatch.
- Chapter 5: Installing CygNet Bridge API — This chapter introduces CygNet Bridge API, how to prepare your system for CygNet Bridge API, how to configure and manage two-factor authentication mode, accessing and updating CygNet Bridge API, build the the CygNet Bridge API sample web application, and some tips for troubleshooting potential issues.
- Chapter 6: Other Information — This chapter includes other relevant information including a security reference for CygNet Bridge applications, a CygNet Bridge glossary, and copyright information.

Related Documents

For information about the supporting software (such as Microsoft IIS) required for the CygNet Bridge software installation, refer to documentation available from the specific software provider.

For information about the CygNet Mobile Application Suite and CygNet Bridge SCADA, refer to the following resources:

- CygNet Mobile Help — If you are using CygNet Mobile, after the CygNet Bridge software is installed and you have completed the optional steps for Mobile, go to **http://localhost/Help** with your web browser[1]
- CygNet Help — An online Help file is available for the CygNet product
- CygNet Mobile Application Suite — An online Help file is available for the CygNet Mobile Application Suite.

[1]If you are not logged into the web server or have installed with https, replace *localhost* with your web host name when specifying this pathname.

Plan the Installation

CygNet Bridge is a set of services intended to run outside the production network. The CygNet Bridge software product makes CygNet production data available to external consumers, allowing them to view and work with CygNet data.

CygNet Bridge works in conjunction your CygNet system and with the additional companion features you select to install. Available CygNet companion products include:

- CygNet Mobile
- CygNet Dispatch
- CygNet Bridge API

Installing CygNet Bridge with CygNet Mobile

- Use this document for installation guidance only if **CygNet Mobile** is the sole companion feature you will be selecting when you install CygNet Bridge.
- This document describes how to install CygNet Mobile using the CygNet Bridge Setup installer (CygNet Bridge Setup.exe) for installations selecting to install only CygNet Mobile as a companion feature with CygNet Bridge.

Installing CygNet Bridge with Multiple Companion Features

- Refer to the CygNet Bridge chapter in the online CygNet Help for installation guidance if you will be selecting multiple companion features (any combination of **CygNet Mobile**, **CygNet Dispatch**, and **CygNet Bridge API**) when you install CygNet Bridge.
- CygNet Bridge installations selecting additional features require additional preparations and configuration with your existing CygNet system. The CygNet Help describes how to prepare for and install CygNet Bridge using the CygNet Bridge Setup installer (CygNet Bridge Setup.exe) for installations selecting to install multiple CygNet companion features with CygNet Bridge.

CygNet Bridge System Requirements

Your system must satisfy minimum requirements to run the CygNet Bridge setup. Be sure to consider your CygNet BridgeSCADA setup when determining installation requirements.

The following table describes the system requirements for a installation. Your specific system setup may have additional requirements that are not covered here.

Description	Requirement
Operating System	Windows Server 2019 Windows Server 2016 Windows Server 2012 R2 Windows Server 2012
C++ Support	Microsoft Visual C++ Redistributable for Visual Studio 2015-2019 (x64) - v14.28.29325 or later
.NET Framework	Microsoft .NET Framework 4.7.2 Developer Pack or later with ASP.NET 4.7.2 or later
Script Engine	ASP.NET
Web Server — Internet Information Services (IIS)	IIS 10 on Windows Server 2019 IIS 10 on Windows Server 2016 IIS 8.5 on Windows Server 2012 R2 IIS 8.0 on Windows Server 2012 The specific IIS version requirement is determined by your operating system. For details, see Installing IIS for CygNet Bridge.
CygNet Software — Group Service (GRP) for CygNet Bridge settings	A new or existing CygNet Group (GRP) service to store CygNet Bridge settings. It should be distinct from the GRP service chosen for hierarchy storage. For details, see To Configure CygNet Group Services for CygNet Mobile.
CygNet Software — Group Service (GRP) for hierarchies	One or more CygNet SCADA Group Service(s) to use as a hierarchy service.
SSL Certificate	By default, the CygNet Bridge software uses HTTPS as the communication protocol. We strongly recommend using HTTPS (secure) host-client communications, as HTTPS traffic is encrypted from end-to-end to help ensure secure data transmission between the web server and the mobile application. Note that self-signed certificates are not supported. To provide HTTPS, you must install an SSL certificate either before or after installing the CygNet Bridge software. For details, see Activating HTTPS.

Description	Requirement
CygNet Bridge License	To use CygNet Bridge, two types of licenses are available: • Trial — try out the CygNet Bridge application. These licenses have an expiration date and will not allow you to start the software after the expiration date has passed. • Full — run CygNet Bridge for a specified number of configured facilities. These licenses have no expiration date. The number of configured facilities varies by installation, and is based on your site needs. For details, contact your CygNet or Weatherford representative.
The following system requirements are optional and only necessary for users of **CygNet Mobile**.	
Mobile Operating Systems	Apple iOS 8 or later Android 5.0 (Lollipop) or later
CygNet Software — Polling application	CygNet SCADA v8.5.1 or later
CygNet Software — Plugin	CygNet Mobile Notification Plugin The CygNet Mobile Notification Plugin is provided with the CygNet Mobile Application Suite. To use the plugin, the CygNet Notification Plugin Manager, which is included in CygNet 8.5.1 or later versions, is also required. For installation instructions, see the following topics: • Installing the CygNet Mobile Notification Plugin • Configuring the CygNet Mobile Notification Plugin

CHAPTER 2: Installing CygNet Bridge

This chapter describes how to prepare your machine and CygNet software for CygNet Bridge, how to install and update CygNet Bridge, and some tips for troubleshooting potential issues.

In this chapter:

Preparing Your System for CygNet Bridge

CygNet Bridge works with your existing CygNet system in conjunction with the additional CygNet Bridge companion products you select to install, so your system must first be prepared to support interoperation of these features.

Preparation Overview

Preparing your system is necessary prior to adding CygNet Bridge and its companion components to your CygNet installation. Preview the following topics for more information before beginning.

- Prepare your system for CygNet Bridge:
  - Enable .NET Framework
  - Install IIS
  - Activate HTTPS
- Prepare your system for intended companion features:
  - Prepare your system for CygNet Mobile
  - Prepare your system for CygNet Dispatch
  - Prepare your system for CygNet Bridge API

Prepare Your CygNet System

To prepare your CygNet system, prior to installing CygNet Bridge or associated products, complete the following preparatory tasks:

- Comply with CygNet system requirements
- Prepare CygNet Software

Comply with CygNet System Requirements

Before installing CygNet Bridge, ensure that all components supporting the applications you will be installing are available and in compliance with CygNet system requirements. Follow the steps described to prepare your server and system to interoperate with all required elements.

See the **CygNet System Requirements** document for more information.

To Comply with CygNet System Requirements for CygNet Bridge

- **Components** — For all components you plan to install, verify and comply with requirements listed in the CygNet system requirements. The following list is an overview only, and is not a substitute for specific components and versions listed in the systems requirements document.
  - **Operating System** — Verify the operating system, which must be one of the following. Follow Microsoft instructions for this process.
    - Microsoft Windows Server 2019
    - Microsoft Windows Server 2016

        - Microsoft Windows Server 2012 R2
        - Microsoft Windows Server 2012.
    - **Visual C++ Redistributable Packages (x64)** — Verify or install the required Microsoft Visual C++ Redistributable Packages (x64) appropriate for your operating system.
    - **ASP.NET Framework** — Verify or install .NET Framework 4.6.2 or later on your system. See Installing .NET Framework for CygNet Bridge for more information.
        - The .NET framework (HTTP and TCP) is included with most supported operating systems.
    - **Internet Information Services (IIS) Web Software** — Verify or install IIS Web Software on your system with Administrative privileges; your operating system version determines which version is installed, and you must have administrative rights to do so. Follow Microsoft instructions for this process. See Installing IIS for CygNet Bridge for more information.
    - **IIS Web Server Secure Sockets Layer (SSL)** — Although HTTP or HTTPS could be used, installing the HTTPS secure certificate communication version (**https://***) is strongly recommended. HTTPS traffic is encrypted from end to end, helping to ensure that data transmitted between the web server and your CygNet installation is more secure; HTTP is not secure and is not safe for production environments. Verify or install IIS Web Server SSL protocol to use HTTPS. See Installing HTTPS for CygNet Bridge for more information.
    - **Windows Authentication** — Verify that Windows Authentication is enabled in your operating system.
        1. In the Control Panel, click **Programs and Features**
        2. In the left pane, select **Turn Windows Features on or off**
        3. Expand Internet Information Services > World Wide Web Services > Security. Click the check box to select **Windows Authentication** and then click **OK**.

Once CygNet system requirements are complete for CygNet Bridge, prepare your system for each CygNet product you are installing.

To Comply with CygNet System Requirements for CygNet Bridge Companion Features

- Prepare Your System for CygNet Mobile
- Prepare Your System for CygNet Dispatch
- Prepare Your System for CygNet Bridge API

After all system requirements are complete for CygNet software and each CygNet Bridge companion product you intend to install, proceed to preparing your CygNet software installation for CygNet Bridge.

Prepare Your CygNet Software Installation

To Configure CygNet Software for CygNet Bridge and Companion Products

1. Verify or upgrade your CygNet software to be v8.5.1 or above. It is highly recommended to use the latest version of CygNet Software as your baseline to access additional product functionality.

2. In the Address Resolution Service (ARS), install the CygNet license provided by your Account Manager if you need to update licensing for additional products.

   - Trial license — Runs CygNet Bridge and selected companion products as a trial until a specified date; will not start after the expiration date

   - Full license — Runs CygNet Bridge and selected companion products for a specified level of service based on your site needs; has no expiration date

3. In the Access Control Service (ACS), configure the ACS security settings needed for access to CygNet Bridge and each of your selected companion products.

   See **Configuring Applications** and **Events and Assigning Permissions to Events** in the **Security** section of the CygNet Help for more information about this process.

   a. On the **Permissions** page, right-click to access the context menu and then select **New App** to access the New Application dialog box.

   b. Enter the following values to add ACS security events for each desired Bridge feature, for the service and permission levels needed (examples shown; replace with levels appropriate for your usage):

      - CygNet Mobile
        - Application: **FAC**, Description: **Facility Service**, Event: **ACCESS**, Event Description: **Bridge Access**, Security ID: **IIS APPPOOL\CygNet Bridge**, Level: **1**, ID Type: **CG**
        - Application: **GRP**, Description: **Group Service**, Event: **ACCESS**, Event Description: **Bridge Hierarchy**, Security ID: **IIS APPPOOL\CygNet Bridge**, Level: **1**, ID Type: **CG**
        - Application: **GRP**, Description: **Group Service**, Event: **ACCESS**, Event Description: **Bridge**, Security ID: **IIS APPPOOL\CygNet Bridge**, Level: **3**, ID Type: **CG**
        - Application: **MOBILE**, Description: **Mobile Security**, Event: **ACCESS**, Event Description: **Mobile Access**, Security ID: *[Enter all desired User IDs for Level 2]*, Level: **2**, ID Type: **US**
      - CygNet Bridge API
        - Application: **BRDGAPI**, Description: **Bridge API Security**, Event: **ACCESS**, Event Description: **Bridge API Access**, Security ID: *[Enter all desired User IDs for Level 1]*, Level: **1**, ID Type: **US**
        - Similar service application access for all services providing required data, e.g. **VHS** for History API calls, **PNT** for points, etc.
      - CygNet Dispatch
        - Application: **FMS**, Description: **Flow Measurement Service**, Event: **JOB**, Event Description: **Dispatch Job**, Security ID: *[Enter all desired User IDs for Level 5]*, Level: **5**, ID Type: **US**

See Security Reference for CygNet Bridge Applications (CygNet Dispatch: FMS/JOB, CygNet Mobile: MOBILE/ACCESS, or CygNet Bridge: BRDGAPI/ACCESS) for more information about user authorization levels for these CygNet products.

Preparing Your System: Enabling .NET Framework

Microsoft .NET Framework software is required to run CygNet Bridge. The way .NET Framework is enabled is determined by the operating system running on your host computer. For most operating systems, .NET Framework is included with your operating system as an easily accessible option, and can be upgraded if necessary to be in accordance with the CygNet system requirements. See the **CygNet System Requirements** document for more information.

Refer to Microsoft .NET Framework online documentation for information beyond the scope of this document.

After Enabling .NET Framework

After enabling .NET Framework, proceed to installing IIS.

Preparing Your System: Installing IIS for CygNet Bridge

Microsoft Internet Information Services (IIS) web software is required to run CygNet Bridge. The version of IIS needed is determined by the operating system running on your host computer.

Required IIS settings for CygNet Bridge are described below for each of the following IIS versions.

- IIS 10 (on Windows Server 2019)
- IIS 10 (on Windows Server 2016)
- IIS 8.5 (on Windows Server 2012 R2)
- IIS 8 (on Windows Server 2012)

Refer to Microsoft IIS online documentation for information beyond the scope of this document.

Install IIS

Prior to installing CygNet Bridge or associated products, and after installing .NET Framework if applicable, complete the following tasks to install the correct version of IIS, as appropriate to your operating system, on the server where you will be installing CygNet Bridge. For all IIS versions, install with Administrative rights.

Install IIS 8 for CygNet Bridge

If you are using Windows Server 2012, complete the following procedure to install IIS 8.

To Install IIS 8 for CygNet Bridge

1. Log in to the machine where you will be installing CygNet Bridge, using Administrative privileges.
2. Open Server Manager. Click **Start** > **Administrative Tools** > **Server Manager** to open it.
3. In Server Manager, select **Dashboard** > **Add roles and features**.
4. In the **Add Roles and Features Wizard** on the **Before you begin** page, click **Next**.
5. On the **Select installation type** page, select **Role-based or feature-based installation**, and then click **Next**.

6. On the **Select destination server** page, select **Select a server from the server pool**, select your server name from the **Server Pool** list, and then click **Next**.
7. In the **Select server roles** window, expand **Web Server (IIS)**, select **Web Server**, and make the following selections:
    a. Select **Web Server**, and make the following selections:
        i. For **Common HTTP**, select the following options:
            - Default Document
            - Directory Browsing
            - HTTP Errors
            - Static Content
        ii. For **Health and Diagnostics**, select the following options:
            - HTTP Logging
        iii. For **Performance**, select the following options:
            - Static Content Compression
        iv. For **Security**, select the following options:
            - Request Filtering
            - Windows Authentication
        v. For **Application Development**, select the following options:
            - .NET Extensibility 4.5
            - Application Initialization
            - ASP.NET 4.5
            - ISAPI Extensions
            - ISAPI Filters
    b. Select **Management Tools**, and make the following selections:
        i. **IIS Management Console**
    c. Click **Next**.
8. In the **Selected features** window, select and expand **.NET Framework 4.5 Features** and do the following:
    a. Select **.NET Framework 4.5**
    b. Select **ASP .NET 4.5**
    c. For **WCF Services**, select the following options:
        - HTTP Activation
        - TCP Port Sharing
    d. Click **Next**.

9. On the **Confirm installation selections** page, click **Install**.
10. On the **Installation progress** page, confirm your installation completed successfully, and then click **Close**.

Install IIS 8.5 for CygNet Bridge

If you are using Windows Server 2012 R2, complete the following procedure to install IIS 8.5.

To Install IIS 8.5 for CygNet Bridge

1. Log in to the machine where you will be installing CygNet Bridge, using Administrative privileges.
2. Open Server Manager. Click **Start** > **Server Manager** to open it.
3. In Server Manager, select **Dashboard** > **Add roles and features**.
4. In the **Add Roles and Features Wizard** on the **Before you begin** page, click **Next**.
5. On the **Installation type** page, select **Role-based or feature-based installation**, then click **Next**.
6. On the **Server Selection** page, select **Select a server from the server pool**, select your server name from the **Server Pool** list, and click **Next**.
7. On the **Server roles** page, select **Web Server (IIS)**.
8. In the **Add Roles and Features** wizard, click **Add Features** if you want to install the IIS Management Console.

   > **Note:** Do not select **Include management tools (if applicable)** unless you want to install the Management Console.

9. On the **Server Roles** page, click **Next**.
10. On the **Features** page, verify .NET Framework installation. Select and expand **.NET Framework 4.5 Features** and do the following:
    a. Select **ASP.NET 4.5**.
    b. Select and expand **WCF Services**, and select the following options:
       - HTTP Activation — When the **HTTP Activation** dialog appears, click **Add Features** to confirm the following features will be installed.
         - ASP.NET 4.5
         - ISAPI Extensions
         - ISAPI Filters
         - .NET Extensibility 4.5

           along with
         - Configuration APIs
         - Process Model

    c. Select and expand **Message Queuing**, and select the following options:
       - Message Queuing Services
    d. Click **Next**.

11. On the **Web Server Role (IIS)** page, click **Next**.
12. On the **Role Services** page, expand **Web Server**, and make the following selections:
    a. For **Common HTTP Features**, select the following options:
        - Default Document
        - Directory Browsing
        - HTTP Errors
        - Static Content
    b. For **Health and Diagnostics**, select the following options:
        - HTTP Logging
    c. For **Performance**, select the following options:
        - Static Content Compression
    d. For **Security**, select the following options:
        - Request Filtering
        - Windows Authentication
    e. For **Application Development**, select the following options:
        - .NET Extensibility 4.5
        - Application Initialization
        - ASP.NET 4.5
        - ISAPI Extensions
        - ISAPI Filters
    f. For **Management Tools**, select the following options:
        - .IIS Management Console
    g. Click **Next** to dismiss the **Roles Services** window.
13. On the **Confirmation** page, verify that the correct role services and features are selected. Your installation can be initiated in one of the following ways.
    - To make the settings take effect immediately, select **Restart the destination server automatically if required** to restart the destination server after installation.
    - To save the settings to use for unattended installations with Windows PowerShell, save the configuration information to an XML-based file for later use. Select **Export configuration settings**, type the file path in the **Save As** dialog box, enter a file name, and then click **Save**.
    - When you are ready to start the IIS installation process, click **Install**.
14. On the **Results** page, confirm your installation completed successfully, and then click **Close**.

Install IIS 10 for CygNet Bridge

If you are using Windows Server 2016 or Windows Server 2019, complete the following procedure to install IIS 10.

Note: There may be small variations in labels or options presented, depending on the version of your Windows Server operating system.

To Install IIS 10 for CygNet Bridge

1. Log in to the machine where you will be installing CygNet Bridge, using Administrative privileges.
2. Open Server Manager. Click **Start** > **Server Manager** to open it.
3. In Server Manager, select **Dashboard** > **Add roles and features** to launch the **Add Roles and Features Wizard**.
4. If the **Before You Begin** page appears, read the information provided, and then click **Next**.
5. On the **Installation Type** page, select **Role-based or feature-based installation**, and then click **Next**.
6. On the **Server Selection** page, select **Select a server from the server pool**, select your server name from the **Server Pool** list, and then click **Next**.
7. On the **Server Roles** page, verify Web Server (IIS) installation.
   a. Select **Web Server (IIS)**.
   b. If additional features are required to install Web Server (IIS), the **Add Roles and Features Wizard** appears, listing all (and auto-selecting any remaining) features required to install Web Server (IIS).
   c. Click **Add Features** to add required Web Server (IIS) features and any related management tools.
   d. Back on the **Server roles** page, click **Next**.
8. On the **Features** page, verify .NET Framework installation.
   a. Select and expand **.NET Framework 4.7 Features** and select the following options:
      - .NET Framework 4.7
      - ASP.NET 4.7
      - WCF Services — expand and select the following options:
        - HTTP Activation
        - TCP Port Sharing
   b. If additional features are required (and not yet selected) to install HTTP Activation, the **Add Roles and Features Wizard** appears. The wizard lists all (and auto-selects any remaining) features required to install HTTP Activation.
   c. Click **Add Features** to add required HTTP Activation features and any related management tools.
   d. Back on the **Features** page, click **Next**.
9. On the **Web Server Role (IIS)** page, read the information provided, and then click **Next**.
10. On the **Role Services** page, select and expand **Web Server** to select the following role services.
    a. For **Common HTTP Features**, select the following options:
       - Default Document
       - Directory Browsing

- HTTP Errors
- Static Content

b. For **Health and Diagnostics**, select the following options:
   - HTTP Logging

c. For **Performance**, select the following options:
   - Static Content Compression

d. For **Security**, select the following options:
   - Request Filtering
   - Windows Authentication

e. For **Application Development**, select the following options:
   - .NET Extensibility 4.7
   - Application Initialization
   - ASP.NET 4.7
   - ISAPI Extensions
   - ISAPI Filters

f. For **Management Tools**, select the following options:
   - IIS Management Console

g. Click **Next**.

11. On the **Confirmation** page, verify that the correct role services and features are selected.
12. Your installation can be initiated in one of the following ways.
    - To make the settings take effect immediately, select **Restart the destination server automatically if required** to restart the destination server after installation.
    - To save the settings to use for unattended installations with Windows PowerShell, save the configuration information to an XML-based file for later use. Select **Export configuration settings**, type the file path in the **Save As** dialog box, enter a file name, and then click **Save**.
    - When you are ready to start the IIS installation process, click **Install**.
13. On the **Results** page, confirm your installation completed successfully with all selected features, and then click **Close**.

After Installing IIS

After installing IIS, proceed to activating HTTPS (strongly recommended).

Preparing Your System: Activating HTTPS

Activation of a secure (HTTPS) communications channel for the IIS Web server is strongly recommended to run CygNet Bridge. Although CygNet Bridge will operate with HTTP, the software default selection is to use HTTPS

host-client communication. Selecting to use HTTP instead is not a secure option, and is not a safe choice for production environments. When you activate and use the HTTPS protocol, HTTPS traffic is encrypted from end to end, helping to ensure that data transmitted between the web server and your CygNet installation is more secure. To provide HTTPS, you must install an SSL certificate and configure HTTPS for your system.

> **Important:** If you host multiple sites or install CygNet Bridge on an IIS Web server that also runs non-CygNet Bridge sites, additional configuration steps are required to ensure that the site port bindings do not collide with one another. Refer to Microsoft IIS online documentation for more information on these advanced configuration steps.

Activate HTTPS

Prior to installing CygNet Bridge or associated products, complete the following tasks, as appropriate to your operating system, to activate HTTPS for the server where you will be installing CygNet Bridge.

Refer to Microsoft online documentation for information beyond the scope of this document.

Import an SSL Certificate

> **Note:** CygNet Bridge does not support self-signed SSL certificates; they are not secure.

1. Log in to the machine where you will be installing CygNet Bridge, using Administrative privileges.
2. Open IIS Manager. Depending on your software version, IIS Manager might be found under **Start** > **Administrative Tools**.
3. In IIS Manager, do the following.
   a. In the **Connections** pane, click to select the name of the server where you will be hosting the CygNet Bridge software.
   b. In the **Home** pane, under **Features View**, double-click **Server Certificates**.
   c. In the **Actions** pane, click **Import** and complete the fields appearing in the resultant dialog box.

Configure HTTPS Bindings

1. Log in to the machine where you will be installing CygNet Bridge, using Administrative privileges.
2. Open IIS Manager. Depending on your software version, IIS Manager might be found under **Start** > **Administrative Tools**.
3. In IIS Manager, do the following to configure your site bindings.
   a. In the **Connections** pane, click to select the CygNet Bridge website root directory.
   b. In the **Actions** pane, click **Bindings** to access the **Site Bindings** dialog box.
   c. In the **Site Bindings** dialog box, click **Add** and then do the following.
      i. Click to access the **Type** menu, and select **https**.
         A. Provide an IP address
         B. Confirm port 443 is selected.
         C. Optionally specify a host name.

ii. Click to access the **SSL certificate** menu, and select the SSL certificate to use.

A. Click **OK**.

B. Select the default HTTP entry on port 80 and then click **Remove**.

C. When asked if you are sure that you want to remove the selected binding, click **Yes** and then **Close**.

4. In IIS Manager, do the following to configure your CygNet Bridge website to require SSL communication.
   a. In the **Connections** pane, click to select the CygNet Bridge website root directory.
   b. In the **Home** pane, under **Features View**, double-click **SSL Settings**.
      i. Check the **Require SSL** box.
      ii. Click **Apply**.
5. Test access to your secured site from outside of your firewall to verify your settings.

Installing and Updating CygNet Bridge

CygNet Bridge provides secure data access from outside of your CygNet production environment when using companion products such as CygNet Mobile, CygNet Dispatch, and CygNet Bridge API.

Install CygNet Bridge as the link between your CygNet installation and your additional enterprise applications, to serve as a secure intermediary connection. Each CygNet Bridge installation accommodates a specific access configuration.

CygNet Bridge is required to run CygNet Mobile, CygNet Dispatch, and CygNet Bridge API.

See CygNet Mobile, CygNet Dispatch, or CygNet Bridge API for general information about those components.

CygNet Bridge Log Files

CygNet Bridge log files are found in the following default storage location (if not changed during CygNet Bridge installation).

- Bridge Log files — **C:\Weatherford\CygNetBridge\Logs**

Install CygNet Bridge

Accomplish all prerequisite system preparation tasks before attempting to install CygNet Bridge. See Preparing Your System for CygNet Bridge for more information.

After you have prepared your server and system to meet all requirements, install and configure CygNet Bridge as follows, for each instance of CygNet Bridge required.

To Install CygNet Bridge

1. Ensure that all prerequisite steps are complete, including prerequisites for each CygNet Bridge companion product feature you will be installing. This ensures that your system components and CygNet SCADA installation are prepared to interoperate with CygNet Bridge. See Preparing your System for CygNet Bridge for more information.
2. Obtain the product source files from the **CygNet Software Download Website** on the Weatherford software support portal (login required).
3. Extract the source files from the .zip file.
4. Install and run CygNet Bridge Setup (**CygNet Bridge Setup.exe**).
    a. Copy the **CygNet Bridge Setup.exe** file to the staging location on the computer where you plan to install the CygNet Bridge software.
    b. Right-click the **CygNet Bridge Setup** icon and choose **Run as administrator** to launch the installation wizard.
    c. When the installation wizard appears, read the license terms and conditions, check the **I agree to the license terms and conditions** box to agree, and then click **Next** to proceed.

    > **Note:** The installer will verify that you have installed the required features or components and prompt you to correct any omissions. For some of the items, you may need to restart your system, then restart the installation process.

d. On the **System Validation** page, verify listed features, or fix/install any features as needed. When the list is in compliance, click **Next**.

e. On the **Feature Selection** page, select features and options to install. When the features are selected, click **Next**.

   i. In the **Feature Selection** section, select the features to install by clicking each check box next to the Mobile, Dispatch, and/or Bridge API options you will be installing.

   ii. In the **Supplemental Options** section, select the desired communications protocol. HTTPS is the default selection and is strongly recommended for secure communications. If you select HTTPS, type the name of your HTTPS host for CygNet Bridge into the **HTTPS host name** text box.

   > **Note:** It is strongly recommended to use the HTTPS (https://*) secure option because HTTPS traffic is encrypted from end to end, helping to ensure that data transmitted between the web server and your CygNet installation is more secure; HTTP is not secure and is not safe for production environments.

   iii. In the **Port binding** section, enter the desired port number to bind to. 80 is the default value. If you enter an alternative port selection, the system will validate your entry to ensure that the port number is valid.

f. On the **Mobile** page (if you are installing the **CygNet Mobile** feature), configure the following settings. When the **Mobile** settings are complete, click **Next**.

   - In the **Mobile Security (ACS)** section, enter your connection information.
     - In the **CygNet Domain** field, enter the domain of the CygNet system containing the ACS you want to use.
     - In the **CygNet Access Control Service** field, enter the name of the site and service *Site.Service* to be used, e.g. CYGNET.ACS.
   - In the **Mobile Settings Storage (GRP)** section, enter your connection information.
     - In the **CygNet Domain** field, enter the domain of the CygNet system containing the GRP service you want to use.
     - In the **CygNet Group Service** field, enter the name of the site and service *Site.Service* to be used, e.g. CYGNET.GRP.

     > **Note:** This Group Service is for CygNet Mobile settings, and should be distinct from any Group Service used for hierarchy storage.

g. On the **Dispatch** page (if you are installing the **CygNet Dispatch** feature), configure the following settings. When the **Dispatch** settings are complete, click **Next**.

   - In the **Dispatch (FMS)** section, enter your connection information.
     - In the **CygNet Domain** field, enter the domain of the CygNet system containing the FMS you want to use.
     - In the **CygNet Dispatch Service** field, enter the name of the site and service *Site.Service* to be used, e.g. CYGNET.FMS.

- In the **Application Blob Service (APPS)** section, enter your connection information.
  - In the **CygNet Domain** field, enter the domain of the CygNet system containing the APPS you want to use
  - In the **CygNet Application Blob Service** field, enter the name of the site and service *Site.Service* to be used, e.g. CYGNET.APPS.

h. On the **Bridge API** page (if you are installing the **CygNet Bridge API** feature), configure the following settings. When the **Bridge API** settings are complete, click **Next**.
   - In the **Bridge API Security (ACS)** section, enter your connection information.
     - In the **CygNet Domain** field, enter the domain of the CygNet system containing the ACS you want to use.
     - In the **CygNet Access Control Service** field, enter the name of the site and service *Site.Service* to be used, e.g. CYGNET.ACS.
   - In the **Allowed Domains** section, enter information specifying your accessible domains.
     - In the **Comma-separated list of CygNet domains** field, enter the domains you want to be allowed access by Bridge API.

       Example: 5432, 6543, 7654
   - In the **Relative Facility Definition File Path** section, enter your file storage information.
     - In the **Blob path of file containing Relative Facility definitions** field, enter the Blob path for the location where the definition file is stored. This file is required to use Relative Facility functionality, and could be a standard RelativeFacilityDefs.xml file stored in the BSS or, if you are using Canvas and have generated a global settings file that is stored in the BSS, it could be the GlobalSettings.gsf file containing relative facility definitions.

       Examples:

       [5432]CYGNET.BSS\Bridge\RelativeFacilityDefs.xml — relative facility definitions in .xml file format; standalone file for CygNet Bridge

       [5432]CYGNET.BSS\Canvas\GlobalSettings.gsf — relative facility definitions in .gsf file format; Canvas file shared with CygNet Bridge
   - In the **Multi-factor authentication** section, select a mode for two-factor authentication, if used, and then enter data storage information for the Group service (GRP type) to use for authentication information. See Providing Two-Factor Authentication in the CygNet Bridge API section for more information about these options.
     - In the **Two-factor mode** field, select an option from the drop-down menu. Options are **Disabled**, **Optional**, and **Required**. Default value is **Disabled**.
     - If not disabled, in the **CygNet Domain** field, enter the domain of the CygNet system containing the dedicated Group service for user authentication information.
     - If not disabled, in the **CygNet Group Service** field, enter the name of the site and service *Site.Service* of the Group service to use, e.g. CYGNET.USER2FA.

i. On the **Program Folder** page, specify an installation folder for storing your CygNet Bridge files.
   - The default location is C:\Weatherford\CygNetBridge.
   - In the **Program Folder** field, select or enter a location for the software,

- Click **Install**.

j. Once the software installation is successful, exit the installer. Note and complete any instructions provided at the end of the installation process, before proceeding to launch the software.

Start CygNet Bridge

Any time you finish installing or reinstalling CygNet Bridge, complete the following steps to initialize and launch the software.

To Start CygNet Bridge

1. Open the **Internet Information Services (IIS) Manager**.
2. In the **Connections** pane, select your host in the tree and expand the **Sites** node to view the sites present. You should see CygNet Bridge and Default Website.
3. At the bottom of the center pane, select the **Features View** page to view the status for your sites.
    a. Locate **Default Website** in the list and confirm the status.
        i. If the Default Website status is "Started" right-click **Default Website** and select **Manage Website > Stop** to stop the site and avoid a port collision.
        ii. If the Default Website status is "Stopped" leave it as is.
    b. Locate **CygNet Bridge** in the list to confirm the site is installed.
        i. Right-click **CygNet Bridge** and select **Manage Website > Start** to start the site.
4. To use HTTPS (strongly recommended), configure the HTTPS binding, if you have not already done so. See Activating HTTPS for more information.
5. If using **CygNet Mobile** or **CygNet Dispatch**, confirm the services making up CygNet Bridge are operational, as follows.
    a. In the IIS **Connections** pane, under the **CygNet Bridge** site, right-click the **Diagnostics** node and then select **Manage Application > Browse** to launch the **Web Diagnostics** application.
    b. In the **Diagnostics** application, click **Service Status** to view a list of your services and confirm all web services are active. It may take a few moments for all of the services to start.
        - If one service or more is not running, use the Diagnostics application to check its status.
        - Information is provided in the status table for services that are down, to help you troubleshoot and fix any issues found.
        - When all services are up and running, confirm service status in the table again to verify that all are active.
    c. Exit the **Diagnostics** application.

Update CygNet Bridge

CygNet Bridge 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. Obtain the product source files from the **CygNet Software Download Website** on the Weatherford software support portal (login required).
3. Extract the source files from the .zip file.
4. Copy the new **CygNet Bridge Setup.exe** file to the staging location on the computer where you previously installed CygNet Bridge.
5. Open the CygNet Bridge installer, and follow the prompts to install the software.
6. **Start** CygNet Bridge in your IIS Manager.

Troubleshooting CygNet Bridge

The following tips might be helpful in solving issues that may arise using or installing CygNet Bridge.

Installation Errors

If you need to correct, change, or add a CygNet *Site.Service* or multi-factor authentication setting entered during CygNet Bridge installation, do one of the following.

- Reinstall CygNet Bridge — Open the CygNet Bridge Setup application (**CygNet Bridge Setup.exe**) and select **Uninstall**. When the uninstall process is complete, **Close** CygNet Bridge and reinstall it with the setup application, entering the correct or changed *Site.Service* or multi-factor authentication values desired. See Installing CygNet Bridge for more information.
- Edit the configuration file — Open the configuration file and enter the correct or changed *Site.Service* or multi-factor authentication values.
  - web configuration file
  - CygNet Bridge configuration file

Connectivity Errors

If you are having trouble getting Bridge to talk to the CygNet Services, and Bridge is running on a different subnet than the CygNet Services you may experience connectivity issues.

Try using the **CygNet Domain Connection Utility** (CygConn.exe) on the server where Bridge is running to add the IP address of the server where CygNet is running as the **Preferred ARS**.

Restart Bridge.

Login Errors

If you encounter errors with your client login, check your IIS web configuration values to see what type of authentication is configured for your system.

> **Important:** Alternatives to Windows authentication, such as Basic or Digest, send your credentials unencrypted by default therefore they are NOT secure authentication methods. If you configure alternative authentication you must also activate HTTPS for your system.

It is strongly recommended that you activate HTTPS authentication to ensure a secure communications channel, for any authentication selection. HTTPS traffic is encrypted from end to end, helping to ensure that data transmitted between the web server and your CygNet installation is more secure; HTTP is not secure and is not safe for production environments. See Activating HTTPS for more information.

Check with your server administrator or refer to Microsoft online documentation for information beyond the scope of this document.

CHAPTER 3: Installing CygNet Mobile

This chapter introduces CygNet Mobile, how to prepare your system for CygNet Mobile, how to install CygNet Mobile, how to install and configure the CygNet Mobile notification plugin, and some tips for troubleshooting potential issues.

In this chapter:

CygNet Mobile

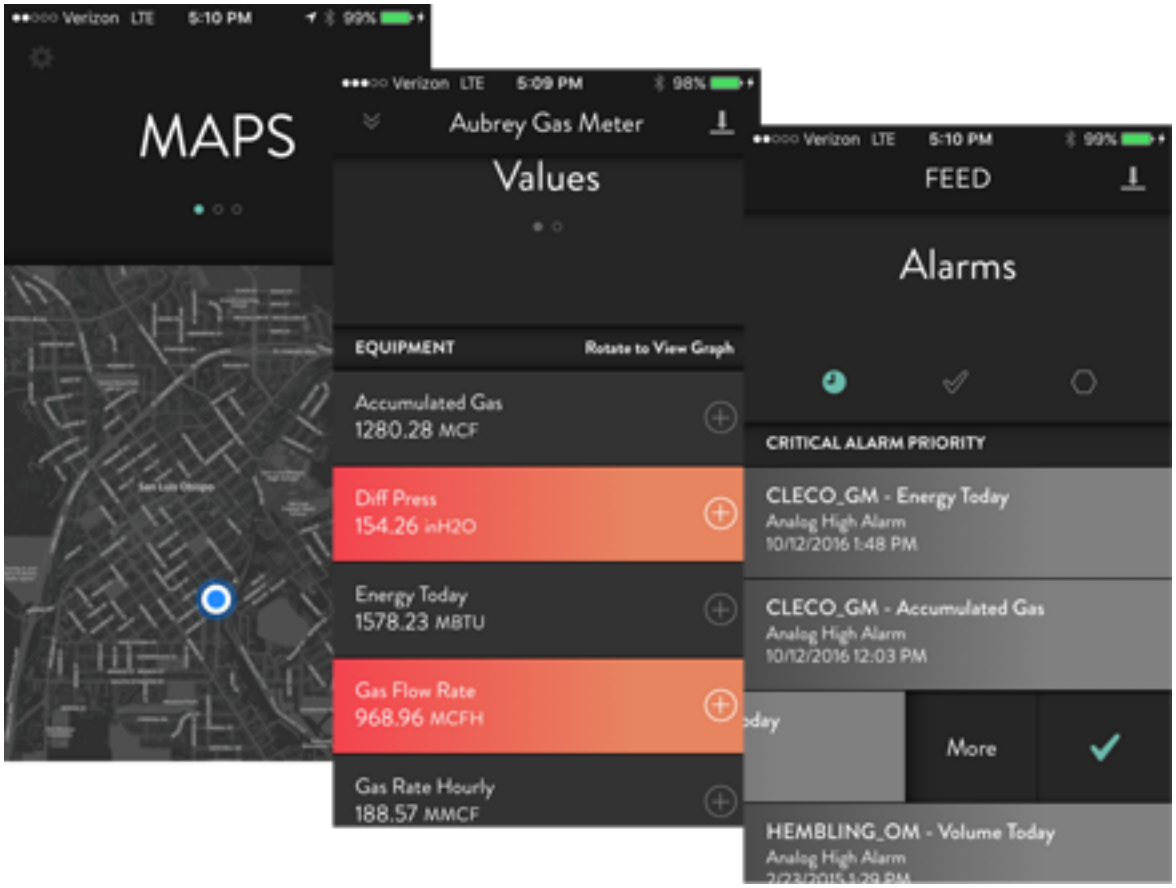
The **CygNet Mobile Application Suite** is a separately available CygNet product provided so that you can view critical CygNet SCADA data over a mobile device. You can use the **CygNet Operator** mobile application component to view a map of relevant equipment and facilities, see current data, trend historical data, and view and acknowledge both CAS alarms and GNS notifications in a single operation, on your Apple iOS or Android devices.

CygNet Mobile includes the following components.

- **CygNet Operator** mobile application — available through the Apple App Store for iOS mobile devices, or Google Play Store for Android mobile devices.
- **CygNet Mobile Notification Plugin** interface — to enable alarm and notification communication for CygNet Operator
- **Mobile Administration** site — to configure CygNet Operator features and capabilities

CygNet Mobile requires the installation of CygNet Bridge software, and must be selected as an option during the CygNet Bridge installation process. CygNet Bridge maintains secure data access, allowing you to access your required CygNet data without direct access to a CygNet system.

> **Note:** CygNet Bridge v4.6 is required for interoperability with CygNet v9.7. See CygNet Bridge for general information about that component.



Sample CygNet Operator Screens

CygNet Mobile License

CygNet Mobile is licensed in conjunction with CygNet Bridge, and must be licensed separately from existing CygNet SCADA or CygNet Measurement components.

> **Note:** When you install an updated CygNet license file, recycle CygNet Bridge in the IIS Application Pools list using the IIS Manager to refresh your web application and pick up new functionality. Refer to Microsoft IIS (Internet Information Services) documentation if you need more information about that process.

For more information about obtaining and licensing the CygNet Mobile and CygNet Bridge products, contact your Account Manager.

Install CygNet Mobile

CygNet Mobile requires the installation of CygNet Bridge software, and must be selected as an option during the CygNet Bridge installation process.

Installation also includes preparing your system, installing CygNet Bridge, installing CygNet Mobile, and installing and updating the CygNet Mobile Notification Plugin to receive and acknowledge notifications using your mobile device.

1. Prepare your system

   See Preparing Your System for CygNet Mobile for more information.

2. Install CygNet Bridge

   See Installing CygNet Bridge for more information.

3. Install CygNet Mobile

   See Installing and Updating CygNet Mobile for more information.

4. Install the CygNet Mobile Notification Plugin

   See Installing CygNet Mobile Notification Plugin for more information.

Use CygNet Mobile

Run CygNet Mobile in conjunction with CygNet Bridge and CygNet Software. See the **CygNet Release Documents** for more information about current software version requirements and considerations appropriate for your installation and usage.

Access CygNet Mobile User Assistance

CygNet Mobile Application Suite provides usability prompts within the feature set itself. A standalone online help file is provided for user assistance, including configuration information for your CygNet Operator installation. Refer to the CygNet Mobile Application Suite for more information. The Online Help is available via CygNet Mobile once you install CygNet Operator.

Other portions of the CygNet Help also pertain to preparation or installation of **CygNet Mobile**. The following related topics may prove helpful:

- CygNet Bridge
- Security Reference for CygNet Bridge Applications

Preparing Your System for CygNet Mobile

CygNet Mobile is designed to work with your existing CygNet system via an instance of CygNet Bridge, the intermediary application that facilitates secure data interaction. Your system must therefore be prepared to support operation of CygNet Bridge and CygNet Mobile in addition to your CygNet software installation.

Preparing your system is part of the process to add CygNet Mobile to your system.

See CygNet Bridge for general information about that component.

Prepare Your System

To prepare your system, prior to installing CygNet Bridge or CygNet Mobile, complete the following preparatory tasks:

- Comply with CygNet system requirements — See Preparing your System for CygNet Bridge for more information.
- Prepare CygNet Software

Prepare CygNet Software

Preparing for CygNet Mobile requires configuration of various CygNet software services to optimize your CygNet Operator experience. CygNet Group services store hierarchy information, control access, and additional services allow alarm state notification and acknowledgment to occur using your mobile device.

To Configure CygNet GRP Services for CygNet Mobile

Set up separate Group (GRP) services to store your CygNet Bridge settings and your CygNet Mobile hierarchies. Setting up separate Group services supports each hierarchy type and allows for greater control over security settings.

1. Set up two Group (GRP) services to support CygNet Mobile.
    - Create or select a GRP service to store your CygNet Bridge settings for CygNet Mobile. This service must be distinct from the GRP used for CygNet Mobile hierarchies. It may be an existing GRP service used for other purposes in your CygNet system, if desired.
    - Create a GRP service to store your CygNet Mobile hierarchies. Make this GRP service distinct from the GRP used for your CygNet Bridge settings.
2. Set up access control for the GRP services to support CygNet Mobile.
    - In the Access Control Service (ACS), configure Level 3 access for the Group service used for CygNet Bridge settings.

    See **Configuring Applications** and **Events and Assigning Permissions to Events** in the **Security** section of the main CygNet Help for more information about this process.

To Configure CygNet ARS and ACS Services for CygNet Mobile

Set up licensing and access control for your CygNet Mobile and CygNet Bridge components.

1. In the Address Resolution Service (ARS), install the CygNet Mobile license provided by your Account Manager.

   - Trial license — Runs CygNet Mobile as a trial until a specified date; will not start after the expiration date
   - Full license — Runs CygNet Mobile for a specified number of configured facilities based on your site needs; has no expiration date

2. In the Access Control Service (ACS), configure the ACS security settings needed for CygNet Bridge and CygNet Mobile access. Because multiple domains, facilities, and group services can be used, configure security settings in the ACS associated with each site.

   See **Configuring Applications** and **Events and Assigning Permissions to Events** in the **Security** section of the CygNet Help for more information about this process.

   a. On the **Permissions** page, right-click to access the context menu and then select **New App** to access the New Application dialog box.

   b. Enter the following values to add security events for CygNet Bridge access:
      - FAC: Configure Level 1 access for the Facility service used for CygNet Bridge: Application: *MyFACforBridge*, Event: **ACCESS**, Event Description: **Bridge Access**, Security ID: **IIS APPPOOL\CygNet Bridge**, Level: **1**, ID Type: **US**.
      - GRP: Configure Level 1 access for the Group service used for CygNet Mobile hierarchy settings: Application: *MyGRPforHeirarchySettings*, Event: **ACCESS**, Event Description: **Bridge Access**, Security ID: **IIS APPPOOL\CygNet Bridge**, Level: **1**, ID Type: **US**.
      - GRP: Configure Level 3 access for the Group service used for CygNet Bridge settings: Application: *MyGRPforBridgeSettings*, Event: **ACCESS**, Event Description: **Bridge Access**, Security ID: **IIS APPPOOL\CygNet Bridge**, Level: **3**, ID Type: **US**.

   c. Enter the following values to add security events and users for CygNet Mobile access, for each permission level needed (examples shown for levels 1 (read-only) and 5 (administrative)):
      - Application: **MOBILE**, Event: **ACCESS**, Event Description: **Mobile Access**, Security ID: *[Enter all desired User IDs for Level 1]*, Level: **1**, ID Type: **US**
      - Application: **MOBILE**, Event: **ACCESS**, Event Description: **Mobile Access**, Security ID: *[Enter all desired User IDs for Level 5]*, Level: **5**, ID Type: **US**.

Installing CygNet Mobile

CygNet Mobile accesses CygNet services via an instance of CygNet Bridge, in order to access data values over the internet. The secure CygNet Bridge connection allows CygNet Mobile to gather information and production data values from your CygNet installation.

Install **CygNet Mobile** to view and manage a variety of data. CygNet Mobile installations access CygNet data from outside of a CygNet installation by connecting to CygNet Bridge, which in turn provides a secure connection to the services hosting your CygNet data.

CygNet Mobile requires the installation of CygNet Bridge software, and must be selected as an option during the CygNet Bridge installation process.

See CygNet Bridge for general information about that component.

CygNet Mobile Log Files

CygNet Mobile log files are found in the following default storage location (if not changed during CygNet Bridge installation).

- **C:\Weatherford\CygNetBridge\Logs**

Install CygNet Mobile

Accomplish all prerequisite system preparation tasks and install CygNet Bridge before attempting to install CygNet Mobile. After you have prepared your server and system to meet all requirements, and installed and configured CygNet Bridge, install CygNet Mobile as follows.

To Install CygNet Mobile

Ensure that all prerequisite steps are complete. This ensures that your CygNet system components and settings are prepared to interoperate with CygNet Bridge and CygNet Mobile.

1. Prepare your system for CygNet Bridge. See Preparing Your System for CygNet Bridge for more information.
2. Prepare your system for CygNet Mobile. See Preparing Your System for CygNet Mobile for more information.
   a. Verify CygNet GRP services and hierarchies for CygNet Mobile.
   b. Verify ACS settings for CygNet Mobile.
3. Install CygNet Bridge, selecting **Mobile** under **Feature Selection**. See Installing CygNet Bridge for more information.
4. Install the CygNet Mobile application on your mobile device.
   a. For iOS devices, access the Apple App Store and search for the "CygNet Operator" application.
   b. For Android devices, access the Google Play Store and search for the "CygNet Operator" application.

After installing CygNet Mobile, you can use CygNet Operator to access your CygNet data over a mobile device. To enable notifications, the CygNet Mobile Notification Plugin is also required.

After Installing CygNet Mobile

Once CygNet Mobile is installed, installation of the **CygNet Mobile Notification Plugin** is required in order to receive and acknowledge notifications using CygNet Operator on your mobile device. See the following topics for more information.

- Install the CygNet Mobile Notification plugin — See Installing the CygNet Mobile Notification Plugin for more information
- Configure the CygNet Mobile Notification plugin — See Configuring the CygNet Mobile Notification Plugin for more information
- Configure the CygNet Mobile Administration site — For information about this process, refer to the **CygNet Mobile Help** provided with your CygNet Bridge source files

After installation, obtain and configure your CygNet Operator application. A dedicated CygNet Mobile Application Suite for Online Help document is included with the application to guide you in this process.

Update CygNet Mobile

CygNet Bridge contains the latest version of CygNet Mobile, 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.

See Update CygNet Bridge for more information.

CygNet Operator can be updated any time a new version of the CygNet Operator application is available. When a new version is available, search the Apple 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.

Installing the CygNet Mobile Notification Plugin

Install the **CygNet Mobile Notification Plugin** to communicate point alarm information to CygNet Operator so that you can receive and acknowledge CygNet notifications with your mobile device. This custom notification plugin is configured via the General Notification Service (GNS), using the CygNet Notification Plugin Manager feature provided with your CygNet source files. CygNet Operator users can also acknowledge Common Alarm Service (CAS) alarm records using this functionality.

Although point alarm states can be displayed in CygNet Operator without the GNS or CAS, acknowledging the notifications requires the CygNet Mobile Notification Plugin. When the GNS is notified about alarm states, notifications can then be sent to mobile devices using a push notification service, and notifications can be acknowledged using the CygNet Mobile Application Suite.

CygNet Mobile requires installation of CygNet Bridge before you can add the CygNet Mobile Notification Plugin to your system. See CygNet Bridge and Installing CygNet Bridge for more information.

CygNet Mobile Notification Plugin File Storage Locations

CygNet Bridge software source files include CygNet Mobile Notification Plugin files for the version of CygNet you are using. The default storage locations for your CygNet Mobile Notification Plugin files include the following folders on your client machine.

- Mobile Notification Plugin file — **C:\CygNet Resources\CygNet<*version*> Mobile GNS Plugin**
- Mobile Notification Plugin directory — **C:\CygNet\Services\GNS\Plugins\CygNetMobile**
- Mobile Notification Plugin file — **C:\CygNet\Services\GNS\Plugins\CygNotify.exe**
- Mobile Notification Plugin log file directory — **C:\CygNet\Services\GNS\PluginData**
- CygNet Bridge log file directory — **C:\Weatherford\CygNetBridge\Logs**

Install the CygNet Mobile Notification Plugin

Accomplish all prerequisite preparation tasks and install CygNet Bridge before attempting to install CygNet Mobile Notification Plugin. After you have met all requirements, configure the CygNet Plugin Manager and install CygNet Mobile Notification Plugin as follows.

To Install the CygNet Mobile Notification Plugin

1. Ensure that all prerequisite steps are complete.
    a. Install CygNet Bridge. See Installing CygNet Bridge for more information.
    b. In Windows Explorer, navigate to **C:\CygNet\Services\GNS\Plugins** and verify or create a directory, with a path relative to the host GNS, for the CygNet Mobile Notification Plugin called \CygNet\Services\GNS\Plugins**CygNetMobile**.
    c. Verify that all required files are present in the **Plugins** directory, as required by the notification plugin process. This includes plugin assembly files, CygNet.API .NET files, and the executable file. Use the procedure outlined in **Installing a Custom Notification Plugin**, found in the **CygNet Notification Plugin Interface** topic for more information.

2. Install the CygNet Mobile Notification Plugin.
    a. In Windows File Explorer, in the **CygNet Bridge** source directory, navigate to the **\CygNet Resources\CygNet<*version*> Mobile GNS Plugin** folder, and copy the following files.
        - CygNet.API.Coredll
        - CygNet.Notifications.dll
        - CygNetMobileGNSPlugin.dll
        - CygNetMobileGNSPlugin.dll.config
        - MobileRestClient.dll
        - MobileRestClientUtils.dll
        - MobileRestModels.dll
        - Newtonsoft.Json.dll
        - System.Net.Http.Formatting.dll
        - System.Web.Http.dll
        - Weatherford.Core.Logging.Desktop.dll
        - Weatherford.Core.Logging.dll
    b. Paste the files into the **\CygNet\Services\GNS\Plugins\CygNetMobile** directory on the CygNet server.

After Installing the CygNet Mobile Notification Plugin

Once the plugin is installed, proceed to Configuring the CygNet Mobile Notification Plugin to configure the settings required to receive and acknowledge CygNet notifications over your mobile device using CygNet Operator.

Configuring the CygNet Mobile Notification Plugin

Once the **CygNet Mobile Notification Plugin** is installed, configure the plugin to interact with your CygNet software installation and the CygNet Mobile Application Suite. After configuring the CygNet Mobile Notification Plugin, you can receive and acknowledge CygNet notifications over your mobile device using the CygNet Operator application.

Configuring CygNet Mobile Notification Plugin can occur using one of the following methods.

- Add an address to an existing Event record
- Add an address to an existing Group record
- Create a new Address record

See **Best Practice for Setting up Notification Record Types** in the **Notification** section of the CygNet Help for more information about planning your GNS records and record types.

Add an Address to an Existing Event Record

To add a primary address record to an existing Group record, use the following procedure.

To Add a Primary Address to an Existing Event Record for the CygNet Mobile Notification Plugin

1. In CygNet Explorer, open the General Notification Service (GNS) and double-click on the Event record to use. The **Properties for Entry** dialog box will appear.
   a. On the **Addresses** page, click **New** to access the **Notification Address** dialog box.
      i. In the **Type** field, use the drop-down menu to select **Reference address**.
      ii. In the **Address** field, click **...** to access the **Select GNS ID** dialog box. Select the primary address record to use (**MOBILE_PRIMARY**), and click **OK**.
      iii. Optionally in the **Description** field, type descriptive text to help you identify the record in the future.
      iv. Optionally click to select **Propagate resend rules down**, and optionally **Report Alarm Clear**. See **Configuring an Address Record** in the **Notifications** section of the CygNet Help for more information.
      v. Optionally click to select **Ignore all previous resend rules**.
      vi. Select to require acknowledgment. Select the **Acknowledgment Required** check box and continue to the next step.
      vii. Optionally select to resend notifications that are not cleared.
      viii. Optionally schedule blackouts if required. See **Configuring Blackouts** in the **Notifications** section of the CygNet Help for more information.
      ix. Click **OK** to close the **Notification Address** dialog box.
   b. In the **Properties for Entry** dialog box, click **OK** to save the new notification address for the Event record.

Add an Address to an Existing Group Record

To add a primary address record to an existing Group record, use the following procedure.

To Add a Primary Address to an Existing Group Record for the CygNet Mobile Notification Plugin

1. In CygNet Explorer, open the General Notification Service (GNS) and double-click on the Group record to use. The **Properties for Entry** dialog box will appear.
   a. On the **Addresses** page, click **New** to access the **Notification Address** dialog box.
      i. In the **Type** field, use the drop-down menu to select **Reference address**.
      ii. In the **Address** field, click **...** to access the **Select GNS ID** dialog box. Select the primary address record to use (**MOBILE_PRIMARY**), and click **OK**.
      iii. Optionally in the **Description** field, type descriptive text to help you identify the record in the future.
      iv. Optionally click to select **Propagate resend rules down**, and optionally **Report Alarm Clear**. See **Configuring an Address Record** in the **Notifications** section of the CygNet Help for more information.
      v. Optionally click to select **Ignore all previous resend rules**.
      vi. Select to require acknowledgment. Select the **Acknowledgment Required** check box and continue to the next step.
      vii. Optionally select to resend notifications that are not cleared.
      viii. Optionally schedule blackouts if required. See **Configuring Blackouts** in the **Notifications** section of the CygNet Help for more information.
      ix. Click **OK** to close the **Notification Address** dialog box.
2. In the **Properties for Entry** dialog box, click **OK** to save the new notification address for the Group record.

Create a New Address Record

To create a new address record, use the following procedure. You will be using the Notification Plugin Manager found in the General Notification Service (GNS) to aid in configuration.

To Create a New Address Record for the CygNet Mobile Notification Plugin

1. In CygNet Explorer, open the General Notification Service (**GNS**) and right-click in the white space of the pane to access the context menu. Select **View Notification Plugin Manager** to access the **Notification Plugin Manager** dialog box.
   - If the CygNet Mobile Notification Plugin is listed in the Manager, select it and then click **Edit** to access the **Edit CygNet Mobile Notification Plugin** dialog box to manage the mobile plugin settings.
   - If the CygNet Mobile Notification Plugin is not listed in the Manager, click **Add** to access the **Add New Notification Plugin** dialog box to create the mobile notification plugin settings.
2. In the **Edit...** or **Add...** dialog box, specify the following values to configure the CygNet Mobile Notification Plugin settings.

a. In the **Address type** field, type **ZM**.

b. In the **Notification name** field, type **CygNet Mobile Notification Plugin**.

c. In the **Full notification file path** field, the address is read-only to display the directory where the plugin assembly files are stored. It will be populated in part with values provided for the **Relative notification file path** value you enter in the next field, e.g. C:\CygNet\Services\GNS***Plugins\CygNetMobile\CygNetMobileGNSPlugin.dll***.

d. In the **Relative notification file path** field, define where the custom plugin assembly files are stored relative to the GNS (requires a dedicated directory for each plugin). Type in the location e.g. **Plugins\CygNetMobile\CygNetMobileGNSPlugin.dll**.

e. In the **Regular expression** field, specify acceptable addresses. Enter your primary, and optionally secondary and tertiary, record addresses. Separate multiple values with a pipe, e.g. *PrimaryAddress*|*SecondaryAddress*|*TertiaryAddress*. Default value is **.*** or all valid addresses.

f. In the **Max parallel notifications** field, type the number of push notifications to allow at the same time. Maximum value is 8; default value is 1.

g. In the **Notification time limit** field, type the number of seconds to allow for the notification delivery. Value range is 60 seconds (1 minute) - 3600 seconds (1 hour). Default value is 600 seconds (10 minutes).

h. Click **Save** to commit the settings and close the dialog.

3. Validate the settings as follows.
   a. In the **Notification Plugin Manager** dialog box, click **Validate plugins**.

   b. If errors occur, resolve the issues. See **Monitor Plugin Errors and Validation State**, in the **CygNet Notification Plugin Interface** topic for more information.

   c. When the **Plugins validated successfully** message appears, click **Close** to exit the Notification Plugin Manager.

4. Edit the CygNet Mobile Notification Plugin configuration file as follows.
   a. Open the **CygNetMobileGNSPlugin.dll.config** file using the text editor of your choice, such as Notepad++. The file is located in the **\CygNet\Services\GNS\Plugins\CygNetMobile** directory on the CygNet server.

   b. Change the URL value by locating the following line and modifying it to point to your mobile server location:

      <add key="BaseMobileRestUrl" value="*https://localhost/*" />

      Note: Use forward slashes (/) for the URL values, not backslashes.

   c. Change the GUID value (MobileNotificationGuid) as follows:
      i. Open the **Web.config** file. The file is located in the **\\localhost\Weatherford\CygNetBridge\Website\CygNetBridge** directory on the Web server.

      ii. Copy the mobile notification GUID values (MobileNotificationGuid) from the **Web.config** file into the corresponding location in the **CygNetMobileGNSPlugin.dll.config** file.

d. **Save** your changes and close the file.

5. In CygNet Explorer, in the General Notification Service (**GNS**), add your desired mobile address records.
   a. If desired, add a Tertiary Notification Address record (GNS Id = MOBILE_TERTIARY). Otherwise skip to the next step and add a Secondary Address record.
      i. In the **GNS** pane, right-click in the white space to access the context menu and click **New** to access the **New Entry** dialog box.
      ii. On the **Notifications** page, do the following.
         A. In the **Record ID** field, type **MOBILE_TERTIARY**.
         B. In the **Description** field, type **Tertiary Notification Address**.
         C. In the **Type** field, use the drop-down menu to select **Address**.
      iii. On the **Addresses** page, click **New** to access the **Notification Address** dialog box and do the following.
         A. In the **Type** field, use the drop-down menu to select **CygNet Mobile Notification Plugin**.
         B. In the **Address** field, type **Tertiary**.
         C. In the **Description** field, type **Tertiary Record**.
         D. Select to require acknowledgment. Select the **Acknowledgment Required** check box and continue to the next step. Otherwise, skip to step H.
         E. If using acknowledgment required, in the **Next GNS ID to notify** field, click **...** and select the **GNS Id** to use, and click **OK**.
         F. In the **Retries if not acknowledged** field, type **1**.
         G. In the **Minutes to wait between retries** field, type **2**.
         H. Optionally schedule blackouts if required. See **Configuring Blackouts** in the **Notifications** section of the CygNet Help for more information.
         I. Click **OK** to save the configuration settings.
      iv. Click **OK** to close the property page.
   b. If desired, add a Secondary Notification Address record (GNS Id = MOBILE_SECONDARY). Otherwise skip to the next step and add a Primary Address record.
      i. In the **GNS** pane, right-click in the white space to access the context menu and click **New** to access the **New Entry** dialog box.
      ii. On the **Notifications** page, do the following.
         A. In the **Record ID** field, type **MOBILE_SECONDARY**.
         B. In the **Description** field, type **Secondary Notification Address**.
         C. In the **Type** field, select **Address**.

iii. On the **Addresses** page, click **New** to access the **Notification Address** dialog box and do the following.

A. In the **Type** field, use the drop-down menu to select **CygNet Mobile Notification Plugin**.

B. In the **Address** field, type **Secondary**.

C. In the **Description** field, type **Secondary Record**.

D. If you are using a tertiary address, select the **Acknowledgment Required** check box and continue to the next step. Otherwise, skip to step H.

E. If using acknowledgment required, in the **Next GNS ID to notify** field, click **...** and select the **Tertiary GNS Id** (MOBILE_TERTIARY) and click **OK**.

F. If using acknowledgment required, in the **Retries if not acknowledged** field, type **1**.

G. If using acknowledgment required, in the **Minutes to wait between retries** field, type **2**.

H. Optionally schedule blackouts if required. See **Configuring Blackouts** in the **Notifications** section of the CygNet Help for more information.

I. Click **OK** to save the configuration settings.

iv. Click **OK** to close the property page.

c. Add a Primary Notification Address record (GNS Id = MOBILE_PRIMARY).

i. In the **GNS** pane, right-click in the white space to access the context menu and click **New** to access the **New Entry** dialog box.

ii. In the **Notifications** page, do the following.

A. In the **Record ID** field, type **MOBILE_PRIMARY**.

B. In the **Description** field, type **Primary Notification Address**.

C. In the **Type** field, select **Address**.

iii. In the **Addresses** page, click **New** to access the **Notification Address** dialog box and do the following.

A. In the **Type** field, use the drop-down menu to select **CygNet Mobile Notification Plugin**.

B. In the **Address** field, type **Primary**.

C. In the **Description** field, type **Primary Record**.

D. If you are using a secondary address, select the **Acknowledgment Required** check box and continue to the next step. Otherwise, skip to step H.

E. If using acknowledgment required, in the **Next GNS ID to notify** field, click **...** and select the **Secondary GNS Id** (MOBILE_SECONDARY) and click **OK**.

F. If using acknowledgment required, in the **Retries if not acknowledged** field, type **1**.

G. If using acknowledgment required, in the **Minutes to wait between retries** field, type **2**.

H. Optionally schedule blackouts if required. See **Configuring Blackouts** in the **Notifications** section of the CygNet Help for more information.

I. Click **OK** to save the configuration settings.

iv. Click **OK** to close the property page.

6. In CygNet Explorer, in the General Notification service (**GNS**), add a new notification Event record to contain the address to use for reporting alarms. See **Configuring a GNS Record** in the **Notifications** section of the CygNet Help for more information about the process.
   a. Right-click in the Database pane to access the context menu, and then click **New** to open the New Entry dialog box.
   b. On the **Notifications** page, enter **MOBILE_PRIMARY_E** as the Record ID name, and in the Details section select **Event** as the Type.
   c. On the **Messages** page, enter both Set and Clear messages as desired.
   d. On the **Addresses** page, click **New** to enter a notification Address for the new Event. Only create one address entry. Select **Reference address** as the Type, and enter **MOBILE_PRIMARY** as the Address value.
   e. Click **OK** to save the address, and then **OK** to save the new event notification entry.
7. In CygNet Explorer, open the Point service (**PNT**), to configure point properties to report to the primary mobile GNS ID (MOBILE_PRIMARY_E). Notifications from these points will be sent to the mobile service, which will notify appropriate users based on their hierarchy assignments. See **Editing Points** and **Point Configuration Manager** in the **Points** section of the main CygNet Help and more information about configuring point properties.
   a. In the **PNT** pane, double-click on the point you want to edit, or right-click on the point desired to access the context menu and then click **Properties**, to access the **Properties for Point** dialog box.
   b. Click **Edit** to access the editable fields to edit properties for the point.
   c. On the [*point type*] page (e.g. Analog, Digital), click the corresponding **Report to GNS** check box to configure each desired alarm. To specify the **GNS ID** value, type in **MOBILE_PRIMARY_E**, or click **...** to select **MOBILE_PRIMARY_E** from the GNS IDs available in your service. This is the GNS ID you previously configured to have the MOBILE_PRIMARY address value.
   d. Click **Save** to save your changes and return to the service pane.

      > **Note:** In the PNT Editor, when not in Edit mode, you can use the Previous and Next buttons to access additional points to perform more edits without returning to the service pane.

   e. Click **Refresh** to retrieve the new point information.

Troubleshooting CygNet Mobile

The following tips might be helpful in solving issues that may arise using or installing CygNet Mobile.

Installation Errors

If you install the CygNet Mobile Notification Plugin but it fails validation, you might first verify that you have met all system requirements and have installed the required versions of the Microsoft Visual C++ Redistributable Packages and all other components and updates required for your CygNet software version.

See the **CygNet System Requirements** document for more information.

Check with your server administrator or refer to Microsoft online documentation for information beyond the scope of this document.

Frequently Asked Questions About CygNet Mobile

Answers and solutions to these common installation and administration questions follow:

Why is the CygNet Mobile Notification Plugin failing to validate?

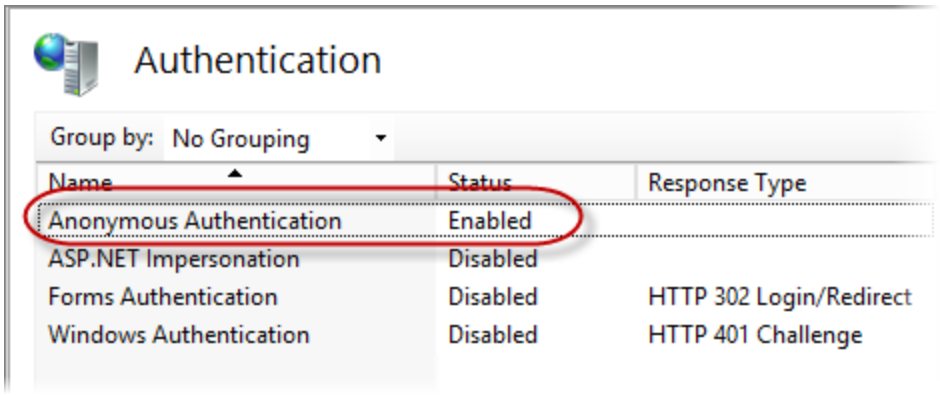
If you install the Notification Plugin but it does not validate, verify that you have installed the Microsoft Visual C++ 2017 Redistributable Package (x64) and all other system requirements.

What is HTTP Error 401.2 and how can I fix it?

If you encounter HTTP Error 401.2 error, enable Anonymous Authentication using the Internet Information Services (IIS) Manager.

To enable Anonymous Authentication

1. Open the IIS Manager.
2. In the navigation menu on the right, click on the root node.
3. In the list on the right, under **IIS**, double-click **Authentication**.



Anonymous Authentication Enabled

4. In the **Authentication** list, if **Anonymous Authentication** is not already **Enabled**, right-click on it and select **Enable**.

For more information, refer to Microsoft online documentation for IIS Anonymous Access.

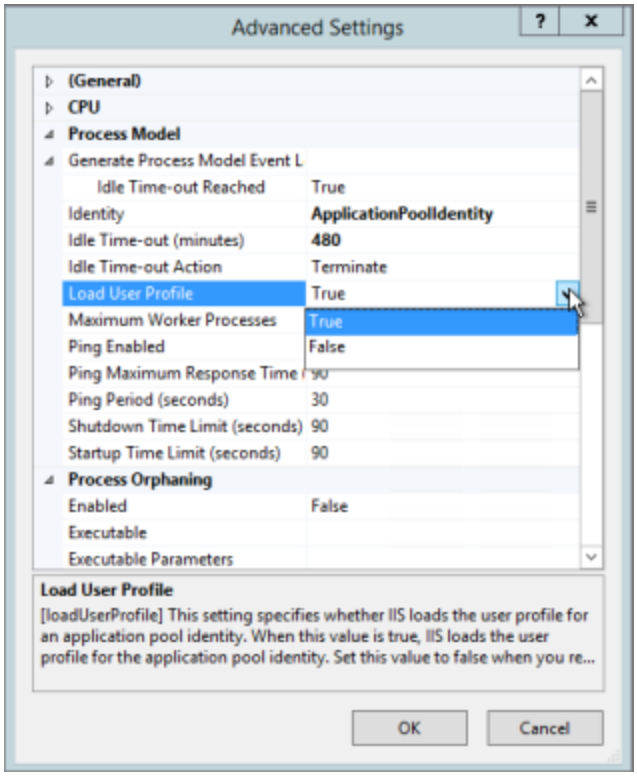
Why is the Mobile Administration site reporting licensing issues?

If you observe Mobile Administration site issues even though the software installation was successful, the IIS **Load User Profile** property for the application may not be set to **True**.

Other symptoms of this may include no default values for the Mobile Administration site, an empty or almost empty log file for the CygNet Bridge (CygNet Bridge Services) module, and an internal 500 error when you attempt to directly access the CygNet Mobile APIs.

To verify and/or change the Load User Profile property setting

1. Open the IIS Manager.
2. In the navigation menu on the left, click **Application Pools**.
3. Right-click on **CygNet Bridge** in the **Application Pools** list, and then select **Advanced Settings**.
4. In the **Advanced Settings** dialog, verify that **Load User Profile** is set to **True**.



Setting Load User Profile to True

5. If **Load User Profile** is set to **False**, right-click on it and select **True**.

CHAPTER 4: Installing CygNet Dispatch

This chapter introduces CygNet Dispatch, how to prepare your system for CygNet Dispatch, how to install and update CygNet Dispatch.

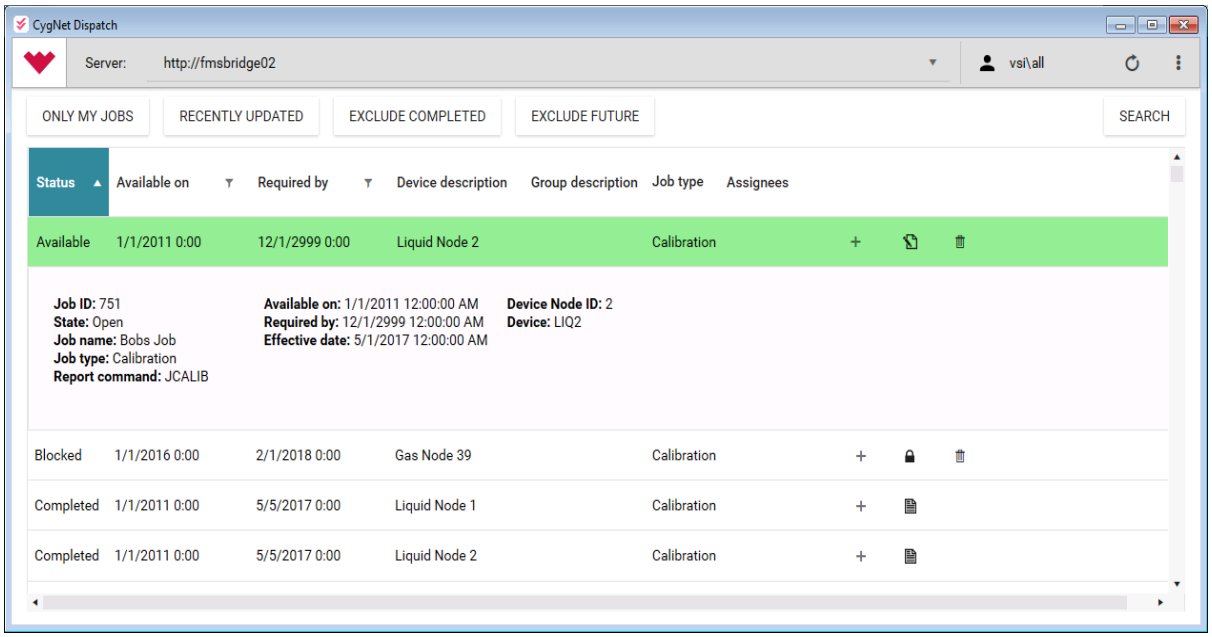
In this chapter:

CygNet Dispatch

CygNet Dispatch is a separately available CygNet product provided so that you can integrate job scheduling and tracking information from tasks performed in the field, such as calibration and inspection results, with data in your CygNet Measurement software instance.

CygNet Dispatch requires the installation of CygNet Bridge software, and must be selected as an option during the CygNet Bridge installation process. CygNet Bridge maintains secure data access, allowing you to access your required CygNet data without direct access to a CygNet system.

> **Note:** CygNet Bridge v4.6 is required for interoperability with CygNet v9.7. See CygNet Bridge for general information about that component.



CygNet Dispatch

CygNet Dispatch provides job scheduling, tracking, and reporting features to add to your measurement data tool set, so that you can incorporate results from field technician activities or "jobs" that potentially affect the gas meter data present in CygNet Measurement, specifically static pressure (SP), differential pressure (DP), and temperature values, which can result in adjustments to previously calculated volumes.

See **CygNet Measurement** in the CygNet Help for more information about CygNet Measurement functionality.

CygNet Dispatch License

CygNet Dispatch is licensed in conjunction with CygNet Bridge, and must be licensed separately from existing CygNet SCADA or CygNet Measurement components.

> **Note:** When you install an updated CygNet license file, recycle CygNet Bridge in the IIS Application Pools list using the IIS Manager to refresh your web application and pick up new functionality. Refer to Microsoft IIS (Internet Information Services) documentation if you need more information about that process.

For more information about obtaining and licensing the CygNet Dispatch and CygNet Bridge products, contact your Account Manager.

Install CygNet Dispatch

CygNet Dispatch requires the installation of CygNet Bridge software, and must be selected as an option during the CygNet Bridge installation process.

Installation includes the following steps.

1. Prepare your system

   See Preparing Your System for CygNet Dispatch for more information.

2. Install CygNet Bridge

   See Installing CygNet Bridge for more information.

3. Install CygNet Dispatch

   See Installing and Updating CygNet Dispatch for more information.

Use CygNet Dispatch

Run CygNet Dispatch in conjunction with CygNet Measurement v9.0 or greater. See the **CygNet Release Documents** for more information about current software version requirements and considerations appropriate for your installation and usage.

> **Note:** It is highly recommended to use a more recent version of CygNet Software as your baseline; v9.5 is already in limited support and has been superseded by more recent versions containing additional functionality.

CygNet Dispatch is accessible on various levels, depending on your permissions for the application and your access to CygNet Measurement. See **FMS Security** in the CygNet Help for more information about setting up permissions.

CygNet Dispatch users with valid login credentials, and basic level permissions, have access to all of the non-administrative functions available in CygNet Dispatch. This allows the field technician to view, filter, open and enter data for various job reports. For each job report selected and opened, the technician can populate the report with field data, save in-progress work, complete the work for a job or (if listed as an assignee) flag a job as blocked if necessary.

CygNet Dispatch users with valid login credentials, and higher level permissions, also have access to CygNet Dispatch administrative functions, which will appear in the administrative task menu accessible via the **...** button on the user interface. These tasks allow the administrator (such as a foreman) to also manage the users present on the assignee list, make group assignments, import or export job files to/from the server, and create new jobs manually on an ad hoc basis.

CygNet Measurement users who have appropriate security permissions can perform more functions related to measurement system data, such as setting up Nodes and group relationships in FMS Explorer to identify what will appear in CygNet Dispatch, assigning security permissions to various users, and making decisions about implementing data recalculations.

Once configured for the various user levels, you can use CygNet Dispatch to assign groups of devices to specified field technicians responsible for performing tracking and reporting tasks on a variety of scheduled jobs (for example, calibration and inspection). CygNet Dispatch job results can then be integrated with CygNet Measurement for data calculation and reporting purposes. See **Reports: Job** and **Reports: Late Job** in the CygNet Help for more information about the FMS commands to run job reports to publish the information.

> **Important:** If jobs disappear from CygNet Dispatch, it may be that the associated Node no longer exists in the system for the specified time. The actions of either deleting a Node (from a point in time) or purging a Node (and its records) from CygNet Measurement also permanently and completely removes all associated CygNet

Dispatch job information from the system. See **Deleting Nodes and Purging Records** in the CygNet Help for more information about that process in CygNet Measurement.

Access CygNet Dispatch User Assistance

CygNet Dispatch endeavors to provide usability prompts within the feature set itself, thereby not requiring an extensive dedicated Help file.

Portions of the **CygNet Measurement** section of the CygNet Help pertain to **CygNet Dispatch** and to accessing information regarding calibration and inspection job reports. Other portions of the CygNet Help also pertain to preparation and installation of **CygNet Dispatch**. The following related topics may prove helpful:

- CygNet Bridge
- Security Reference for CygNet Bridge Applications

Preparing Your System for CygNet Dispatch

Because CygNet Dispatch is designed to work with an existing CygNet Measurement system via an instance of CygNet Bridge, your system must be prepared to support operation of CygNet Bridge and CygNet Dispatch in addition to your CygNet installation. CygNet Bridge is the intermediary application that connects to both an FMS for CygNet Measurement and a CygNet Dispatch installation to facilitate secure data interaction between the two.

Preparing your system is part of the process to add CygNet Dispatch to your system.

See CygNet Bridge for general information about that component.

See **CygNet Measurement** in the CygNet Help for more information about CygNet Measurement functionality.

Prepare Your System

To prepare your system, prior to installing CygNet Bridge or CygNet Dispatch, complete the following preparatory tasks:

- Comply with CygNet system requirements — See Preparing your System for CygNet Bridge for more information.
- Prepare CygNet Software
- Prepare CygNet Measurement

Prepare CygNet Software

To Configure CygNet Software for CygNet Dispatch

1. In the Address Resolution Service (ARS), install the CygNet Dispatch license provided by your Account Manager.
    - Trial license — Runs CygNet Dispatch as a trial until a specified date; will not start after the expiration date
    - Full license — Runs CygNet Dispatch for a specified number of configured facilities based on your site needs; has no expiration date
2. In the Access Control Service (ACS), configure the ACS security settings needed for CygNet Bridge and CygNet Dispatch access.

    See **Configuring Applications** and **Events and Assigning Permissions to Events** in the **Security** section of the main CygNet Help for more information about this process.

    a. On the **Permissions** page, right-click to access the context menu and then select **New App** to access the **New Application** dialog box.

    b. Enter the following values to add security events and users for CygNet Dispatch access, for each permission level needed (examples shown for levels 2 and 5):
        - Application: **FMS**, Description: **Flow Measurement Service**, Event: **JOB**, Event Description: **Dispatch Job**, Security ID: *[Enter all desired User IDs for Level 2]*, Level: **2**, ID Type: **US**
        - Application: **FMS**, Description: **Flow Measurement Service**, Event: **JOB**, Event Description: **Dispatch Job**, Security ID: *[Enter all desired User IDs for Level 5]*, Level: **5**, ID Type: **US**.

See **FMS Security** in the CygNet Help for more information about user authorization levels for CygNet Dispatch.

Once CygNet Software is prepared, you can proceed to Preparing CygNet Measurement for CygNet Dispatch.

Prepare CygNet Measurement

To Configure CygNet Measurement for CygNet Dispatch

1. Verify or install CygNet Measurement and open **FMS Explorer**.
2. Identify the FMS Nodes you want to appear in CygNet Dispatch.
3. Assign the selected FMS Nodes to job groups, if you want them to appear in the Dispatch administrative options for group assignment.

   > **Note:** This step is solely to ensure that group assignment options appear in CygNet Dispatch, in the Group Assignment administrative option, in the drop-down list of groups. It is not required for all Dispatch job assignments. CygNet Dispatch jobs can also be assigned to Nodes using CSV files imported into CygNet Dispatch, and only Node name is required to create, modify or delete jobs in that manner.

   Set the "Category" value equal to "Job" for each group desired, so it will appear in the Dispatch client as a group job assignment option.

   > **Note:** On the FMS Explorer **Nodes** menu, click **Manage Groups** to access the Manage Groups dialog where you can insert or delete group category entries. You can also type "Job" into the Category field of the group Node properties; once typed into the Category field, it will subsequently appear as a drop-down menu option in the Group Assignment administrative menu in Dispatch. See **Managing Group Nodes** > **Managing Group Categories** in the CygNet Help for help configuring the "category" field.

4. Configure Job and Late Job Report Template files for your reports. See **Managing Report Template Files** in the CygNet Help for more information.
5. Optionally schedule any Job or Late Job reports commands in the MSS, if you want to produce them automatically. See **Scheduling FMS Command Tasks in the MSS** in the CygNet Help for more information.
6. Optionally schedule a **Precalculate Calibration Data** command in the MSS, if you want to run the process automatically. See **Scheduling FMS Command Tasks in the MSS** in the CygNet Helpor more information.

Once all preparations are complete, you can proceed to Installing CygNet Bridge and then Installing CygNet Dispatch.

Installing and Updating CygNet Dispatch

CygNet Dispatch accesses measurement data in an FMS via an instance of CygNet Bridge, in order to integrate job results with measurement data values. The secure connection via CygNet Bridge allows CygNet Dispatch to manage jobs to gather and coordinate the field information that could potentially affect production data values in your CygNet Measurement installation, and share that information with an FMS.

Install **CygNet Dispatch** directly on job and administrative computers used to manage a variety of jobs and collect field data. CygNet Dispatch installations access CygNet data from outside of a CygNet installation by connecting to CygNet Bridge, which in turn provides a secure connection to a specified FMS hosting your CygNet Measurement data.

CygNet Dispatch requires the installation of CygNet Bridge software, and must be selected as an option during the CygNet Bridge installation process.

See CygNet Bridge for general information about that component.

See **CygNet Measurement** in the CygNet Help for more information about CygNet Measurement functionality.

Dispatch File Storage Locations

The default storage locations for your CygNet Dispatch files include the following folders on your client machine (if not changed during CygNet Bridge installation).

- Dispatch files — **C:\Weatherford\CygNetDispatch**
- Dispatch Log files — **C:\ProgramData\Weatherford\CygNetDispatch\Logs**
- Report files [completed/in-progress] — **C:\Users**<*username*>**\Documents\Weatherford\CygNetDispatch\JobReports\https**<*bridgeservername*> [or...**http**<*bridgeservername*>, if not using https]

> **Note:** Job Report and Late Job Report template files are stored in CygNet Measurement, in the **C:\CygNet\Services\FMS\ReportTemplates\Samples** folder by default. See **Jobs Report**, **Late Job Reports**, and **CygNet Measurement** in the CygNet Help for more information.

Install CygNet Dispatch

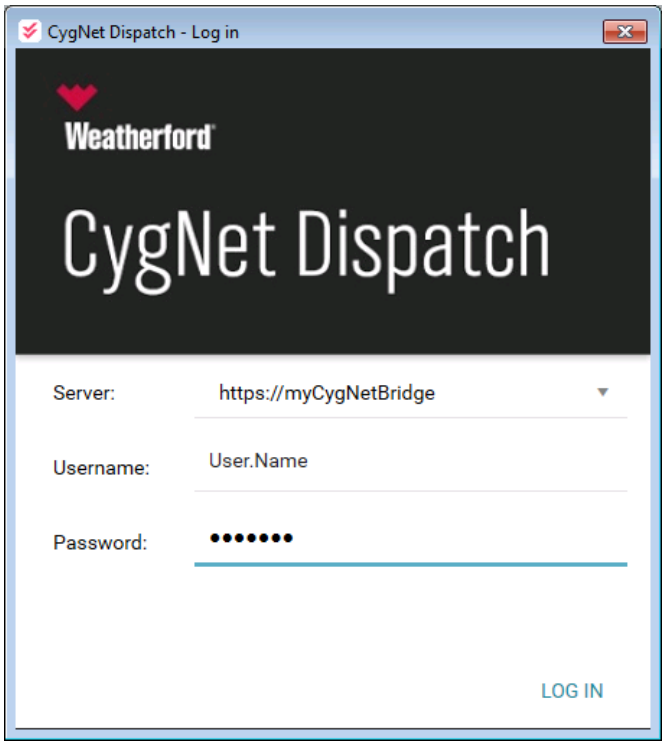
Accomplish all prerequisite system preparation tasks and install CygNet Bridge before attempting to install CygNet Dispatch. After you have prepared your server and system to meet all requirements, and installed and configured CygNet Bridge, install CygNet Dispatch as follows.

To Install CygNet Dispatch

1. Ensure that all prerequisite steps are complete. This ensures that your system components, CygNet SCADA, and CygNet Measurement settings are prepared to interoperate with CygNet Bridge and CygNet Dispatch.
   a. Step one: Prepare your system. See Preparing Your System for CygNet Dispatch for more information.
   b. Step two: Install CygNet Bridge. See Installing CygNet Bridge for more information.
2. Install CygNet Dispatch Setup and application.
   a. Copy the CygNet Dispatch Setup (**CygNetDispatchSetup.exe**) file from the **CygNet\Setup** folder of your CygNet source files to the desktop of your local machine.

b. Use the CygNet Dispatch Setup application to install CygNet Dispatch on your machine.
   i. Open the CygNet Dispatch Setup program.
   ii. Read and agree to the license terms and conditions.
   iii. Click **Install** to install the CygNet Dispatch application on your machine, and add the program icon to your desktop.

c. Launch CygNet Dispatch.
   i. Open CygNet Dispatch to access the login screen.



CygNet Dispatch Login

   ii. Enter your CygNet Bridge server url., username, and password and then log in.
   iii. To open CygNet Dispatch and display data, you must synchronize your data files with the designated server. (This is also true any time you switch servers or usernames, requiring you to log in again.) A dialog box appears after login, presenting options to synchronize now or later.
      - Click **SYNC** to proceed with synchronizing your data with the server.
      - Click **EXIT** to close the application and sync at another time.

d. Once CygNet Dispatch opens, the application provides prompts and tooltips to help guide your usage. Some basic setup is required within the application however, to proceed and use the CygNet Dispatch functionality. Click **...** in the program header to access the administrative tasks menu. The menu is the administrator's access point to configure the assignee list, make group assignments, and import or export job files.

Once CygNet Dispatch is installed, you can use it to perform job scheduling and tracking tasks, yielding field information to enhance and interact with your measurement system data.

Update CygNet Dispatch

CygNet Dispatch can be updated any time the application is synchronized with the FMS (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. Select **UPDATE** to update immediately and sync with the FMS service, or select **CANCEL** to wait until a later time to update and sync.

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. See **CygNet Host Updater Utility** in the **System Administration** section of the CygNet Help for more information.

CHAPTER 5: Installing CygNet Bridge API

This chapter introduces CygNet Bridge API, how to prepare your system for CygNet Bridge API, how to configure and manage two-factor authentication mode, accessing and updating CygNet Bridge API, build the the CygNet Bridge API sample web application, and some tips for troubleshooting potential issues.

In this chapter:

CygNet Bridge API

CygNet Bridge API is a separately available CygNet product that provides a web service to request your CygNet data over the internet, allowing you to create your own web applications to securely access your CygNet system data. CygNet Bridge API is a REST API delivering HTTP requests and responses. The API allows reading, modifying and deleting of CygNet Point records.

Accessing the CygNet Bridge API requires the installation of CygNet Bridge software, and the Bridge API feature must be selected as an option during the CygNet Bridge installation process. CygNet Bridge maintains secure data access, allowing you to access required CygNet data without direct access to a CygNet system. You can optionally require two-factor authentication to be granted access to the CygNet Bridge API.

Notes:

- CygNet Bridge v4.6 is required for interoperability with CygNet v9.7. See CygNet Bridge for general information about that component.
- CygNet Bridge and CygNet Bridge API is also used by the **CygNet OPC UA Server** to access CygNet data. Refer to the **OPC UA Server** section of the main CygNet Help for more information.

CygNet Bridge API License

CygNet Bridge API is licensed in conjunction with CygNet Bridge, which must be licensed separately from existing CygNet SCADA or CygNet Measurement software components. Licensing for CygNet Bridge API is provided according to license type; you can obtain Base licensing for API access, or obtain optional Alarm and/or Control licensing to gain access to additional features. For more information about obtaining and licensing the CygNet Bridge API and CygNet Bridge products, contact your Account Manager.

Features included in each license type are described in the following table.

License Type	CygNet Bridge API Features Included
Base	All CygNet Bridge APIs *except* those features provided with the "Alarm" or "Control" licenses. See API Information Types for a list of provided types.
Alarm	All base license features plus: • Acknowledge alarms • Clear alarms (and optionally force clear)
Control	All base license features plus: • Issue commands to a device • Initiate polling of a device data group • Retrieve data group element ID (DEID) values from a device • Send data group element ID (DEID) values to a device • Send data group transaction data to a device • Set values for a point

Note: When you install an updated CygNet license file, recycle CygNet Bridge in the IIS Application Pools list using the IIS Manager to refresh your web application and pick up new functionality. Refer to Microsoft IIS (Internet Information Services) documentation if you need more information about that process.

Access CygNet Bridge API

CygNet Bridge API requires the installation of CygNet Bridge software, and must be selected as an option during the CygNet Bridge installation process.

Accessing the CygNet Bridge API includes the following steps.

1. Prepare your system.

   See Preparing Your System for CygNet Bridge API and (optionally) Providing Two-Factor Authentication for more information.

2. Install CygNet Bridge, selecting the option to install CygNet Bridge API.

   See Installing CygNet Bridge for more information.

3. Access the CygNet Bridge API.

   See Accessing and Updating CygNet Bridge API for more information.

Use CygNet Bridge API

Use CygNet Bridge API in conjunction with CygNet Bridge and CygNet Software v8.5.1 or greater to access your CygNet data via the web. See the **CygNet Release Documents** for more information about current software version requirements and considerations appropriate for your installation and usage.

API Information Types

A variety of CygNet Bridge APIs are provided to support operations involving the following CygNet information types.

- Access
- Alarms
- Devices
- Facilities
- Measurement
- Groups
- History
- Notes
- Points
- Real-time
- Services
- Tables

> **Note:** Some API calls require specific licensing types. See Licensing above.

The CygNet Bridge APIs are accessible to authorized users of a licensed CygNet installation who are also authorized on the web server domain. Access is granted according to configured permission levels and the features you have licensed.

Authorization depends on:

- your CygNet permissions and access levels configured in the ACS.

  See CygNet Bridge API Security for more information about setting up permissions in CygNet.

- your permissions on the web server domain being used.

  See Accessing and Updating CygNet Bridge API for more information.

  > **Note:** When the authorization token expires, CygNetBridgeAPI will return the status "401 Unauthorized" and deny authorization. If that occurs, obtain a new authorization token by calling the client login API again.

Request an authorization token via the ClientLoginAPI method in your CygNet Bridge site in IIS. Prior to calling any CygNet Bridge API methods, obtain an authorization token, using the method **clientloginapi/api/login** and then pass the obtained token into all CygNet Bridge API requests in a header named **X-WFT-AuthToken**. The token is retained for 7 days before expiration.

Valid CygNet Bridge API requests must contain headers for the authorization token received and the CygNet domain ID, as follows.

- **X-WFT-AuthToken** — Required: contains the user authentication token required for the request (obtained via ClientLoginAPI method)

  > **Note:** Additional requirements apply if you have opted to use two-factor authentication. See Providing Two-Factor Authentication for more information.

- **X-WFT-CygNetDomain** — Required: contains the CygNet domain ID used for the request

CygNet Bridge API errors are logged to your **Weatherford\CygNetBridge\Logs** folder as **CygNetBridgeApi** *[logfile number]***.csv** files

CygNet Bridge API Sample Web Application

Assistance using the Bridge API is provided via a sample application. The CygNet Bridge API installation set includes the sample web application (**BridgeAPISampleApp\sample** folder in your CygNet Bridge source files) that contains examples for using the Bridge API to develop your customized web application, and for using two-factor authentication. See Building the CygNet Bridge API Sample Web Application for more information.

Access CygNet Bridge API User Assistance

CygNet Bridge API generates web-accessible user documents using an auto-generated interactive documentation library tool. On a deployed API system these documents provide up-to-date information to help developers with API usage including example requests / responses and details about each request. The built-in online help will deploy automatically when you install the new APIs.

Navigate to **localhost/CygNet/Help** to access the help documents after CygNet Bridge is installed.

> **Note:** If you have installed CygNet Bridge with HTTPS (strongly recommended), navigate to **https://**[YourWebHostName]**/CygNet/Help**.

CygNet Bridge API Help Offline

An offline version of the *CygNet Bridge API Help* is provided within the CygNet Help as a reference tool.

CygNet Help

Other portions of the CygNet Help also pertain to preparation or installation of **CygNet Bridge API**. The following related topics may prove helpful:

- CygNet Bridge
- Security Reference for CygNet Bridge Applications

Preparing Your System for CygNet Bridge API

CygNet Bridge APIs are provided with CygNet Bridge, to facilitate secure interaction with your CygNet data. Because the CygNet Bridge APIs work with an existing CygNet system via an instance of CygNet Bridge, your system must be prepared to support operation of the CygNet Bridge and CygNet Bridge API components, in addition to your existing CygNet installation.

Preparing your system is part of the process to add CygNet Bridge API to your system.

See CygNet Bridge for general information about that component.

Prepare Your System

To prepare your system, prior to installing CygNet Bridge and the CygNet Bridge API, complete the following preparatory tasks:

- Comply with CygNet system requirements — See Preparing your System for CygNet Bridge for more information.
- Prepare CygNet Software — If multi-factor authentication is used, also see Prepare for Two-Factor Authentication.

Prepare CygNet Software

Once you have complied with CygNet system requirements for all components you will be installing, and prior to installing CygNet Bridge, configure CygNet as follows.

To Configure CygNet Software for CygNet Bridge API

1. In the Address Resolution Service (ARS), install the CygNet Bridge API license provided by your Account Manager.
    - Trial license — Runs CygNet Bridge API as a trial until a specified date; will not start after the expiration date
    - Full license — Runs CygNet Bridge API for a specified number of configured facilities based on your site needs; has no expiration date
2. In the Access Control Service (ACS), configure the ACS security settings needed for CygNet Bridge and CygNet Bridge API access.

    Security is set on an application and event basis. See CygNet Bridge API (BRDGAPI) Security for more information about BRDGAPI security settings.

    See **Configuring Applications** and **Events and Assigning Permissions to Events** in the **Security** section of the CygNet Help for more information about this process.

    a. On the **Permissions** page, right-click to access the context menu and then select **New App** to access the **New Application** dialog box.

    b. Enter the following values to add security events and users for CygNet Bridge API access, for each permission level needed.

- Application: **BRDGAPI**, Description: **Bridge API Security**, Event: **ACCESS**, Event Description: **Bridge API Access**, Security ID: *[Enter all desired User IDs for Level 1 (read-only)]*, Level: **1**, ID Type: **US**
- Application: **BRDGAPI**, Description: **Bridge API Security**, Event: **ACCESS**, Event Description: **Bridge API Access**, Security ID: *[Enter all desired User IDs for Level 3 (Alarm and Control features if licensed)]*, Level: **3**, ID Type: **US**
- Application: **BRDGAPI**, Description: **Bridge API Security**, Event: **ACCESS**, Event Description: **Bridge API Access**, Security ID: *[Enter all desired User IDs for Level 5 (Administrative and 2FA resets if used)]*, Level: **5**, ID Type: **US**

3. If you will be providing two-factor authentication for CygNet Bridge API, also prepare CygNet Software as described in Preparing for Two-Factor Authentication.

Prepare for Two-Factor Authentication (Optional)

> **Important:**
>
> CygNet Bridge supports three major features, CygNet Mobile, CygNet Dispatch, and CygNet Bridge API. CygNet Bridge API is the only feature that currently supports a two-factor authentication (2FA) option. Two-factor authentication is not currently supported for operation with CygNet Dispatch, CygNet Mobile or CygNet OPC UA Server users. Because of this, system configuration requirements change depending on your planned installation.
>
> If you are planning to provide two-factor authentication for CygNet Bridge API users and also running CygNet Dispatch, CygNet Mobile, or the CygNet OPC UA Server, you must install separate instances of CygNet Bridge, on different host computers; install one instance of CygNet Bridge with the CygNet Bridge API feature selected and, on different host computers, install a separate instance of CygNet Bridge with the CygNet Dispatch, CygNet Mobile, or the CygNet OPC UA Server feature installed.

Requiring two-factor authentication to use CygNet Bridge API provides an additional layer of security to better protect access to your CygNet system. You can choose to implement this additional security option when desired, such as when allowing third-party access to your CygNet data or commands that could have access to your field devices. See Providing Two-Factor Authentication for more information about setting up this feature for CygNet Bridge API.

To Configure CygNet Software for Two-Factor Authentication of CygNet Bridge API

Once you have complied with CygNet system requirements for all components you will be installing, and prior to installing CygNet Bridge, configure CygNet as follows to prepare your system to use two-factor authentication. See **Installing and Deleting Services** in the **Services** section of the CygNet Help for more information about this process.

> **Note:** During CygNet Bridge and Bridge API installation, if 2FA is enabled, you will need to enter the new Group service information in the "Multi-factor authentication" section of the Bridge API page.

1. In the Address Resolution Service (ARS), create a new Group service (GRP type, e.g. USERDATA.GRP) specifically for storing two-factor authentication user information.
2. In the Remote Service Manager (RSM), create the new Group service (GRP type, e.g. USERDATA.GRP) specifically for storing two-factor authentication user information.
3. In the Access Control Service (ACS), add the following security settings to configure access to the Group service storing your two-factor authentication user information. See **Implementing Security** in the **Security**

section of the CygNet Help and CygNet Bridge API (BRDGAPI) Security (ACCESS event) for more information about configuring security settings.

a. On the **Permissions** page, right-click to access the context menu and then select **New App** to access the New Application dialog box, and add your required security applications.

b. Enter the following values to add security events and users for 2FA access for CygNet Bridge API, for each permission level needed.

   - Application: **GRP**, Description: [*YourUser2FAInfoGrpService*], Event: **ACCESS**, Event Description: **Bridge API Access**, Security ID: **IIS APPPOOL\CygNetBridge**, Level:**3**, ID Type: **US**
   - Application: **GRP**, Description: [*YourUser2FAInfoGrpService*], Event: **ACCESS**, Event Description: **Bridge API Access**, Security ID: *Enter all desired User IDs allowed to reset user 2FA info*, Level:**4**, ID Type: **US**
   - Application: **BRDGAPI**, Description: [*YourUser2FAInfoDescription*], Event: **ACCESS**, Event Description: **Bridge API Access**, Security ID: *Enter all desired User IDs for Level 5*, Level:**5**, ID Type: **US**

Providing Two-Factor Authentication for CygNet Bridge API

Important:

CygNet Bridge supports three major features, CygNet Mobile, CygNet Dispatch, and CygNet Bridge API. CygNet Bridge API is the only feature that currently supports a two-factor authentication (2FA) option. Two-factor authentication is not currently supported for operation with CygNet Dispatch, CygNet Mobile or CygNet OPC UA Server users. Because of this, system configuration requirements change depending on your planned installation.

If you are planning to provide two-factor authentication for CygNet Bridge API users and also running CygNet Dispatch, CygNet Mobile, or the CygNet OPC UA Server, you must install separate instances of CygNet Bridge, on different host computers; install one instance of CygNet Bridge with the CygNet Bridge API feature selected and, on different host computers, install a separate instance of CygNet Bridge with the CygNet Dispatch, CygNet Mobile, or the CygNet OPC UA Server feature installed.

Provide two-factor authentication to add an additional layer of security when using CygNet Bridge API over the web. When the option is available, providing two-factor authentication (2FA) better protects access to your CygNet data and controls. To provide two-factor authentication, you must set it up for applicable parts of your system. Currently two-factor authentication can be used with the CygNet Bridge API feature in CygNet Bridge.

Configure the Two-Factor Authentication Mode

Configure the settings governing usage of two-factor authentication during installation of CygNet Bridge API, in the **Multi-factor authentication** section of the CygNet Bridge installer. The **Two-factor mode** selection determines how, or if, two-factor authentication is available for use with CygNet Bridge API. Possible settings are as follows.

- **Disabled** — CygNet Bridge API has not enabled the use of 2FA; this is the default setting
- **Optional** — each CygNet Bridge API user can decide whether or not they want to use 2FA
- **Required** — all CygNet Bridge API users are required to use 2FA

See Installing CygNet Bridge for more information about selecting 2FA mode during the installation process.

Provide Two-Factor Authentication

Providing two-factor authentication for CygNet Bridge API adds considerations to your preparation process. If you intend on using two-factor authentication, plan your CygNet Bridge installation to include the following elements.

Element	Description
CygNet elements	
CygNet Group service (GRP service type)	You will need to set up a separate CygNet Group service specifically to store user authentication information used for 2FA. When installing CygNet Bridge with the Bridge API feature selected, you will be asked to supply the information for this separate Group service in the **Multi-factor authentication** section of the Bridge API page. See Preparing your System for CygNet Bridge API for more information.
CygNet Bridge API sample web application	(Optional) When you build the CygNet Bridge API sample web application, you will have access to samples provided to help you build calls to interact with your CygNet Bridge APIs, including an example for two-factor authentication. See Building the CygNet Bridge API Sample Web Application for more information.
Additional requirements	
Mobile phone	You will need consistent access to a mobile phone device capable of installing a two-factor authenticator app and scanning a QR code as necessary. (Examples: iOS or Android mobile devices)
Two-factor authenticator app	You will need to select and install an authenticator app that is capable of generating a time-based, one-time passcode, and is compatible with your mobile phone device. (Examples: LastPass Authenticator, Microsoft Authenticator, Google Authenticator)

Use the following procedure to provide two-factor authentication for CygNet Bridge API.

To Provide Two-Factor Authentication for CygNet Bridge API

> **Note:** Refer to the CygNet Bridge API sample web application for an example of using two-factor authentication. See Building the CygNet Bridge API Sample Web Application for more information.

1. Complete the following preparations for two-factor authentication.

    a. Verify or create a dedicated Group service (GRP service type) in your CygNet installation, to use specifically for storing user authentication information. See Preparing your System for CygNet Bridge API for more information about the process.

    > **Note:** During CygNet Bridge and Bridge API installation, when 2FA is enabled, the new Group service information will be required in the "Multi-factor authentication" section of the Bridge API page.

    b. Secure access to a mobile phone device capable of installing and running a two-factor authenticator app and scanning a QR code as necessary.

    c. Select an authenticator app capable of generating a time-based, one-time passcode, that meets your needs and is compatible with your mobile phone device. Install the authenticator app you have selected on your mobile phone device.

d. Install CygNet Bridge, with the CygNet Bridge API feature selected, the multi-factor authentication mode set to Optional or Required, and information supplied for the dedicated Group service. See Installing CygNet Bridge for more information.

e. Start your CygNet Bridge site in the IIS Manager.

Enable Two-Factor Authentication for a User Account

When the multi-factor authentication mode is set to Required, all users must enable 2FA for their user login. When the mode is set to Optional, each user can decide whether or not to enable 2FA.

> **Note:** After initial setup, your 2FA app continues to generate passcodes on a regular time interval until passcode expiration or 2FA reset.

To Enable Two-Factor Authentication for Your User Account

Using your API client, do the following to enable two-factor authentication for your user account.

1. Access the QR code and generate an authentication passcode.

   a. Create a GET **clientloginapi/api/login/tfa-qr** request to generate the CygNet Bridge API **QR code** image data.

   b. Provide your user credentials (user name, password, and domain/workstation etc. if applicable).

   c. Display the QR code image data contained in the response.

   d. Using the 2FA app on your mobile phone device, scan the QR code and process the image to produce an authentication passcode.

   > **Note:** You can still change your mind and stop the setup process at this point, if desired. The passcode will not become required until the next step (confirmation) is complete.

2. Confirm the authentication passcode.

   a. Create a GET **clientloginapi/api/login/tfa-confirm** request to confirm the authentication passcode.

   b. Provide your user credentials (user name, password, and domain/workstation etc. if applicable).

   c. Add a header named **X-WFT-AuthCode**.

   d. Enter the authentication passcode generated by your 2FA app into the value column of the **X-WFT-AuthCode** header.

   > **Note:** Once the confirmation action is complete, the **X-WFT-AuthCode** header will be required to log in successfully, until it is reset by an administrator.

3. Optionally log in at this time, to verify the process and generate an authentication token.

   a. Create a GET **clientloginapi/api/login** request to log in using the authentication passcode.

   b. Provide your user credentials (user name, password, and domain/workstation etc. if applicable).

   c. Add a header named **X-WFT-AuthCode**.

   d. Provide the authentication passcode generated by your 2FA app into the value column of the **X-WFT-AuthCode** header.

> **Note:** Because the authentication passcode is time based, you may need to regenerate the code using your 2FA app. Repeat as necessary.

e. The authentication token contained in the response is used in your CygNet Bridge API calls.

Use Two-Factor Authentication for CygNet Bridge API

Once it is set up, your CygNet Bridge API calls will have the additional protections of two-factor authentication. In Required multi-factor authentication mode, all users must use 2FA. In Optional mode, users may use 2FA if they choose.

When you access the CygNet Bridge API, do the following to use two-factor authentication.

1. Using your API client, log in to CygNet Bridge API using your authorization credentials and 2FA passcode.
   a. Create a GET **clientloginapi/api/login** request.
   b. Provide your user credentials (user name, password, and domain/workstation etc. if applicable).
   c. Add a header named **X-WFT-AuthCode**.
   d. Provide the authentication passcode generated by your 2FA app in the **X-WFT-AuthCode** header.
   > **Note:** Because the authentication passcode is time based, you may need to regenerate the code using your 2FA app. Repeat as necessary.
   e. The authentication token contained in the response is used by your CygNet Bridge API calls.
2. Create a CygNet Bridge API request including the authentication token.
   a. Create a CygNet Bridge API request.
   b. Add a header named **X-WFT-AuthToken**.
   c. Provide the authentication token generated at login in the **X-WFT-AuthToken** header. The token is retained for 7 days before expiration.

Managing Two-Factor Authentication Users for CygNet Bridge API

There will be circumstances where an administrative deactivation of two-factor authentication is required. A user's mobile device containing the authenticator app they use to access CygNet Bridge API might be lost or stolen, for example, so they will be unable to log in until two-factor authentication is deactivated for their account. User accounts can be reset by an administrator to allow a user to activate two-factor authentication for their account using a new device or 2FA app.

See CygNet Bridge API (BRDGAPI) Security (ACCESS event) for information about configuring security access for Bridge API administrative functions.

See **Group Service (GRP) Security** in the **Security** section of the CygNet Help for information about configuring security access for Bridge API administrative functions.

Reset Two-Factor Authentication User Accounts

> **Note:** An administrator must have security authorization level **4** for the [GRP]* **ACCESS** event for the Group service used to store user authentication data in order to make user data changes. [GRP]* = ACS security application name of the Group service dedicated to storing user authentication information. See Preparing your System for CygNet Bridge API for more information about configuring permissions.

An administrator with the required permissions can deactivate two-factor authentication for a user account, in one of the following ways.

- Use CygNet Bridge API as described below to call the ClientLoginApi reset deactivate two-factor authentication for a user account. This method allows you to manage user 2FA settings from outside your CygNet installation, via CygNet Bridge. The administrator must also have security authorization level **5** for the **BRDGAPIACCESS** event to make user data changes using CygNet Bridge API.
- Use CygNet Studio as described below to use the **CygNet Bridge API Two-Factor Authentication User Manager** screen provided in your Weatherford CygNetBridge source files to generate a screen that guides you through resetting the user authentication data. This method allows you to manage user 2FA settings within your CygNet installation, via CygNet Studio.
- Use CygNet Explorer as described below to navigate to the dedicated Group service created to store user authentication data, and directly remove the user authentication data desired. This method allows you to manage user 2FA settings within your CygNet installation, via CygNet Explorer.

Use CygNet Bridge API

CygNet Bridge API provides an API method, **clientloginapi/api/login/tfa-reset?username={*username*}**, that allows you to deactivate two-factor authentication for a user account via CygNet Bridge.

Use the following procedure to deactivate two-factor authentication for a user account using CygNet Bridge API.

To Reset Two-Factor Authentication for a User Account via CygNet Bridge API

> **Note:** The administrator must also have security authorization level **5** for the **BRDGAPIACCESS** event to make user data changes using CygNet Bridge API.

- Using your API client, call the ClientLoginApi reset method as follows to deactivate two-factor authentication for a user account.
    - Create a PUT **clientloginapi/api/login/tfa-reset?username={*username*}** request.
    - Specify the user to reset, as the *username* query parameter value.

- Provide your user credentials (user name, password, and domain/workstation etc.) as applicable.
- **Send** the request to reset the user authentication data.

Use CygNet Studio

CygNet provides a sample CygNet Studio screen you can use to manage two-factor authentication user accounts. When licensed for CygNet Bridge API, the sample user manager screen is located in your CygNet Bridge product source files.

The sample user manager screen contains the following fields.

Element	Description
User data service	Use the drop-down menu to select the *Site.Service* for the group service that was created specifically for storing user authentication information for your site. See Preparing your System for CygNet Bridge API for more information about the process.
Refresh [service]	Click **Refresh** to update the list of available services.
Two-factor authentication users	Lists the users of CygNet Bridge API who have set up two-factor authentication Select a user to view their setting details in the user settings box below.
Refresh [users]	Click **Refresh** to update the list of two-factor authentication users.
Reset user	Click **Reset user** to remove the selected user's authentication settings from the user data Group service. This allows the user to set up new 2FA account settings if desired.
User settings	Displays two-factor authentication setting details for the selected user, including user identity, status, and (encrypted) Pre-Shared Key (PSK) number

Use the following procedure to reset a two-factor authentication user account using CygNet Studio.

To Reset Two-Factor Authentication for a User Account via CygNet Studio

1. In the **CygNet Bridge\BridgeAPISampleScreen** folder in your CygNet Bridge source files, locate the sample **CygNet Bridge API Two-Factor Authentication User Manager.csf** file and make a copy of it.
2. Upload the copied .csf file into your Blob Storage Service (BSS).
3. In CygNet Studio, open the screen from your Blob service. Optionally make edits if desired, and **Save** any changes.
4. Using your **CygNet Bridge API Two-Factor Authentication User Manager** screen, provide information as follows to reset the desired user authentication data.
    a. From the **User data service** drop-down menu, select the *Site.Service* for the group service created to store the user authentication information for your site, to view the list of two-factor authentication users.
    b. In the **Two-factor authentication users** list box, select the user name you want to reset.
    c. Click **Refresh** to ensure you are viewing current information.
    d. In the **User settings** results box, verify that the user information shown contains the authentication details you want to reset.
    e. Click **Reset** to remove the existing two-factor authentication settings for the selected user.
    f. Click **Refresh** to view the revised data and verify that the user data was reset.

Use CygNet Explorer

Administrators with required permission levels can also directly access the CygNet Group service that was created to contain the two-factor authentication user data, and edit the data directly.

Use the following procedure to reset a two-factor authentication user account using CygNet Explorer.

To Reset Two-Factor Authentication for a User Account via CygNet Explorer

1. In CygNet Explorer, navigate to the Group service that was created to contain your two-factor authentication user data (example: **USERDATA.GRP**) and double-click to open it.
2. Navigate to the node representing the user data you want to reset, right-click to access the context menu, and click **Delete** to remove the desired settings.

Accessing and Updating CygNet Bridge API

CygNet Bridge API is an optional feature of CygNet Bridge software, available when licensed for the CygNet Bridge API product. It must be selected as an option during the CygNet Bridge installation process.

CygNet Bridge API is installed along with CygNet Bridge in your IIS CygNet Bridge site. The CygNet Bridge API produces a web service for secure CygNet data connection over the web so that you can gather CygNet information and production data values from outside of a CygNet installation, and make it available for integration with desktop, mobile, or web applications.

A sample web application is also provided with CygNet Bridge API, to help you create custom applications to access your CygNet data securely over the web. See Building the CygNet Bridge API Sample Web Application for more information.

See CygNet Bridge for general information about that component.

Access CygNet Bridge API

You must have appropriate permissions for any CygNet domain(s) you will be accessing via CygNet Bridge. After you have updated your CygNet license, prepared your system to meet all requirements, and installed and configured CygNet Bridge, you will have access and be able to use CygNet Bridge API.

To Access CygNet Bridge API

1. Ensure that all prerequisite steps are complete. This ensures that your CygNet system components and settings are prepared to interoperate with CygNet Bridge and CygNet Bridge API.
    a. Prepare your system. See Preparing Your System for CygNet Bridge API for more information.
    b. Install CygNet Bridge, selecting the **Bridge API** feature during installation, to provide connection, domain, and file storage information. See Installing CygNet Bridge for more information.

Once CygNet Bridge is installed with the Bridge API feature, you can build the sample web application containing examples to help you begin using CygNet Bridge API to create a customized web application for obtaining your CygNet data. See Building the CygNet Bridge API Sample Web Application for more information.

CygNet Bridge API Log Files

CygNet Bridge API log files are found in the following default storage location (if not changed during CygNet Bridge installation).

- **C:\Weatherford\CygNetBridge\Logs**

Update CygNet Bridge API

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.

See Update CygNet Bridge for more information.

Building the CygNet Bridge API Sample Web Application

Once you have installed CygNet Bridge along with the Bridge API feature, you may want to build the sample application to help you begin using the CygNet Bridge API to create your custom web application to securely access your CygNet data.

Build the Sample Web Application

The sample web application is included with the CygNet Bridge API feature, and provides usage examples you can use as a reference or starting point when developing your custom web application. The sample application source files are located in the **BridgeAPISampleApp\sample** folder in your CygNet Bridge product deliverable. Once built, the sample provides you with examples of the structure and capabilities of the APIs and demonstrates how to build calls to interact with CygNet Bridge APIs, including a sample using two-factor authentication (optional, but recommended).

The sample app provided is for an Angular web application. The sample application must first be compiled, before you will be able to view it in a web browser. Angular CLI is a (command line interface) tool used for compiling and building Angular web applications. Angular uses npm software as a package-manager (command line client) tool to manage JavaScript web application libraries. You can obtain current versions of these tools via web downloads, as described in the following procedure.

To Build the CygNet Bridge API Sample Web Application

Note: Your web server requires an active internet connection for you to access the sample web application.

Complete the following steps to build your sample web application.

1. Install or verify the supporting software used to deliver the sample web application. Comply with any listed prerequisites for your development environment.
    a. Install **npm** software or verify that it is already installed on your system. Refer to npm online documentation for current download and installation information, if needed.
    b. Install **Angular CLI** software or verify that it is already installed on your system. Refer to Angular CLI online documentation for current download and installation information, if needed.
2. In your CygNet Bridge source files, locate the source code for the CygNet Bridge API sample web application as follows.
    a. Open the **BridgeAPISampleApp** folder.
    b. Copy the **sample** folder and its contents to a folder on your hard drive.
3. Open a Windows command prompt pointing to the sample folder location you created for the copied files.
    a. Type the command **npm install** to download and install all of the required dependencies.
    b. Type the command **npm start** to compile the application and start a test development server on **port 4200**.
4. To test the application, open a web browser using the address **https://localhost:4200**

CygNetBridgeSampleApp on GitHub

The CygNet Bridge API sample web application provides source code that demonstrates using the API to retrieve data from your CygNet system is also available on GitHub. Refer to https://github.com/cygnet-software/CygNetBridgeSampleApp for more information.

CygNet Bridge API Help

CygNet Bridge API generates web-accessible user documents using an auto-generated interactive documentation library tool. On a deployed API system these documents provide up-to-date information to help developers with API usage including example requests / responses and details about each request. The built-in online help will deploy automatically when you install the new APIs.

Navigate to **localhost/CygNet/Help** to access the help documents after CygNet Bridge is installed.

> **Note:** If you have installed CygNet Bridge with HTTPS (strongly recommended), navigate to **https://**[YourWebHostName]**/CygNet/Help**.

CygNet Bridge API Help Offline

An offline version of the *CygNet Bridge API Help* is provided within the CygNet Help as a reference tool.

Troubleshooting CygNet Bridge API

The following tips might be helpful in solving issues that may arise using CygNet Bridge API

Authentication Errors

If you are unable to request an authentication token, examine the User web service log for potential troubleshooting information. If the supporting CygNet system is missing the required ACS event, or your user doesn't have the appropriate permissions, you will see a message such as: "User '{username}' does not have sufficient CygNet permissions." Ensure that the user has ACS permissions for the ACCESS event of the BRDGAPI application. See CygNet Bridge API Security for more information.

CHAPTER 6: Other Information

This chapter includes other relevant information including a security reference for CygNet Bridge applications, a CygNet Bridge glossary, and copyright information.

In this chapter:

Security Reference for CygNet Bridge Applications

This section describes security for CygNet applications that operate in conjunction with CygNet Bridge.

> **Note:** CygNet Mobile and CygNet Bridge API have distinct security application names. CygNet Dispatch adheres to FMS security (JOB security event).

Information provided for each software application includes:

Security Application Name	Main Security Event	Component-Level Security	Subject to Application Override
The application's security Application name.	The application's main security event. **Note:** The main security event is the event for which Admin override privileges apply. This means that if an application has more than one Event, and if the user has Level 5 (Admin) permission for the main security event, then the user has full permission for all service Events regardless of the authorization for those Events.	**Yes** indicates that security can be applied to components within the application (for example, individual records). For component-level security, the Application and, in some cases, the Event names generally are user-defined.	**Yes** indicates point records in the service are subject to security defined in the FAC or PNT.

CygNet Bridge API (BRDGAPI) Security

Security for the CygNet Bridge API application is administered by the specified Access Control Service (ACS). As with other CygNet software applications, security is set on an application and event basis. The security events are listed in the BRDGAPI Event table below.

The following tables provide details about BRDGAPI security settings.

Security Application Name	Main Security Event	Component-Level Security	Subject to Application Override
BRDGAPI	ACCESS	No	No

BRDGAPI Event

Event	Event Description	Authorization	Tasks
ACCESS	Content viewing, site management	**0** - None	None
		1 - Read	• Access read-only CygNet Bridge API • Set up two-factor authentication
		2 - Update	• Inclusive
		3 - Add	• Inclusive • Create or update notes using **Notes** API methods • Access **Alarm** and **Control** CygNet Bridge API features* *See Licensing CygNet Bridge API for more information about the API methods included in these feature groups.
		4 - Delete	• Inclusive
		5 - Admin	• Inclusive • Reset user settings for two-factor authentication

CygNet Dispatch (JOB) Security

Security for the CygNet Dispatch application is administered by the specified Access Control Service (ACS) using a Flow Measurement Service (FMS) security application event. As with other CygNet software applications, security is set on an application and event basis.

FMS security events are listed in the CygNet Measurement section. Authorization levels for the JOB security event, required for CygNet Dispatch, are also listed below for your convenience.

FMS JOB Event

Security Application	Security Event	Event Description	Authorization	Tasks
FMS	JOB	Content viewing, management	**0** - None	None

			1 - Read	• Precalculate Calibration Data
				• Build Reports:
				  ◦ Job
				  ◦ Late Job

			2 - Update	• Inclusive • Approve recal-culation • Create Jobs • Export com-pleted jobs • Schedule jobs
			3 - Add	• Inclusive
			4 - Delete	• Inclusive • Delete jobs

			5 - Admin	• Inclusive
				• Configure Extended Com-mand Options:
				  ◦ Create job schedules
				  ◦ Edit job schedules
				  ◦ Delete job schedules

CygNet Mobile (MOBILE) Security

Security for the CygNet Mobile application is administered by the specified Access Control Service (ACS). As with other CygNet software applications, security is set on an application and event basis. The security events are listed in the MOBILE Event table below.

The following tables provide details about MOBILE security settings.

Security Application Name	Main Security Event	Component-Level Security	Subject to Application Override
MOBILE	ACCESS	No	No

MOBILE Event

Event	Event Description	Authorization	Tasks
ACCESS	Content viewing, management	**0** - None	None
		1 - Read	• View CygNet Mobile administration site • Access to CygNet Operator application
		2 - Update	• Inclusive
		3 - Add	• Inclusive
		4 - Delete	• Inclusive
		5 - Admin	• Inclusive • Modify CygNet Mobile administration site

CygNet Bridge Glossary

C

CygNet Bridge

CygNet Bridge is a set of services intended to run outside the production network. The CygNet Bridge software makes CygNet production data available to external consumers, allowing them to view and work with CygNet data.

CygNet Bridge Setup

The CygNet Bridge Setup (CygNet Bridge Setup.exe) is the installer for CygNet Bridge.

CygNet Mobile

An abbreviated name for the CygNet Mobile Application Suite.

CygNet Mobile Notification Plugin

CygNet software supports a generic interface mechanism that allows the General Notification Service (GNS) to push CygNet notification messages to external recipients via a custom third-party notification plugin. The CygNet Mobile Notification Plugin is a plugin that you can use to communicate CygNet alarms and notifications to the CygNet Operator application on a mobile device.

CygNet Notification Plugin Manager

The CygNet Notification Plugin Manager is a generic interface mechanism, available in CygNet 8.5.1 or later. This interface allows the General Notification Service (GNS) to push CygNet notification messages to external recipients via a custom third-party notification plugin.

CygNet Operator

CygNet Operator is the mobile application component of the CygNet Mobile Application Suite. The CygNet Operator app is available from the Apple App Store.

H

HTTP/HTTPS

By default, the CygNet Bridge software uses HTTPS as its communication protocol. HTTPS (secure) host-client communication is strongly recommended for any enterprise applications, as HTTPS traffic is encrypted from end-to-end, helping to ensure that data transmitted between the web server and the mobile application is more secure. To provide HTTPS, you must install an SSL certificate. HTTP (non-secure) host-client communication is not considered safe for production environments. Although the CygNet Bridge software will function using HTTP communications, it is strongly recommended that you select HTTP only when your usage does not require secure data communications.

S

SSL certificate

You must install a Secure Sockets Layer (SSL) certificate to provide HTTPS (secure) host-client communications for the CygNet Bridge software. HTTPS is strongly recommended for any enterprise applications of CygNet Bridge.

Copyright Information