



# **Diver Platform 7.2 Installation Guide for Windows**

# Diver Platform 7.2 Installation Guide for Windows

Revision: Doc-DPIW-7.2-122023-10

December, 2023

Diver Platform and Diver Solution software and documentation © 2015 Dimensional Insight, Inc.

60 Burlington Mall Road, Burlington, Massachusetts 01803

[www.dimins.com](http://www.dimins.com)

## U.S. Export Administration Act: Restrictions on Exporting Software

The Software includes cryptographic software that may be subject to export controls under the U.S. Export Administration Act. The Software may not be exported to any country or to any foreign entity or "foreign person" to the extent prohibited under applicable U.S. government regulations. By downloading or using the Software, you are acknowledging and agreeing to the foregoing limitations on your right to export or re-export the Software, and are also representing and warranting that you are neither on any of the U.S. government's lists of export precluded parties nor otherwise ineligible to receive software containing cryptography that is subject to export controls under the U.S. Export Administration Act.

Administrators must be aware that allowing users outside the United States to access data via certain DI-Clients qualifies as exporting encryption software (either the client executable or the Java applet sent to the browser). Export or re-export of encrypted software must be in accordance with the Export Administration Regulations. Diversion of encryption software contrary to U.S. law is prohibited.

## More Information

More information about trademarks, product warranty, and third-party license notices is available in your DI software Help system. Near the bottom of the Help **home** page, select the **Resources** link, and then on the **Support** page, select **Disclaimers, Trademarks, Warranty, and Third-Party Licenses**.

# Contents

<b>Diver Platform 7.2 Overview</b> .....	<b>1</b>
About This Installation Guide .....	1
About Roles and Environments .....	2
About Diver Platform Server 7.2 .....	3
About Diver Platform Developer 7.2 .....	5
Software Requirements .....	6
Building the DI Directory Structure .....	9
About Diver Platform and Solution 7.2 Licenses .....	11
Diver Platform Licenses .....	11
Diver Solution Licenses .....	12
What Is Named User Licensing? .....	12
About License Types .....	12
Perpetual Licenses .....	12
Trial Licenses .....	12
<b>Installing Diver Platform Server</b> .....	<b>14</b>
Downloading the Server Installation Package .....	14
Extracting the Server Installation Package .....	17
Requesting a License .....	18
Installing a License File .....	22
Installing DiveLine .....	24
DiveLine Files .....	35
Testing the DiveLine Installation .....	36
Installing DivePort .....	38
URI Encoding .....	49

Configuring Apache Tomcat .....	49
Verifying the DivePort Installation .....	52
Installing NetDiver .....	56
NetDiver Customizations .....	60
Verifying the NetDiver Installation .....	60
Setting the Executable Path Variables .....	64
<b>Installing Diver Platform Developer .....</b>	<b>68</b>
Downloading and Extracting the Developer Installation Package .....	68
Installing ProDiver .....	70
ProDiver Installation Silent Option .....	73
Verifying the ProDiver Installation .....	74
Installing Workbench .....	79
Verifying the Workbench Installation .....	82
<b>Updating the DI Software .....</b>	<b>86</b>
<b>Renewing a License .....</b>	<b>88</b>
<b>Uninstalling the DI Software .....</b>	<b>93</b>
<b>Appendix A: Bridge .....</b>	<b>95</b>
Design .....	95
How it Works .....	96
Requirements .....	97
Bridge Configuration .....	97
Authentication .....	98
Installing Bridge .....	98
Configuration Options .....	105
Adding Login Options .....	105

Edit Dialogs .....	107
Configuring Destinations .....	108
Configuring Users .....	115
Configuring Other Settings .....	115
Custom Graphics .....	120
User Access .....	121
<b>Appendix B: Help Desk .....</b>	<b>123</b>
Installing Help Desk .....	123
Verifying the Help Desk Installation .....	126
<b>Appendix C: DiveLine Authentication Options .....</b>	<b>129</b>
Own Authentication .....	129
Configuring Own Authentication .....	129
System Authentication .....	131
Configuring System Authentication .....	132
Web Server Authentication .....	133
Configuring the Web Server .....	134
Configuring IIS Windows 10 / Server 2016 / Server 2019 .....	134
Configuring IIS Windows 8 / Server 2012 .....	142
Configuring IIS Windows 7 / Server 2008 .....	146
Domain Issues .....	155
Configuring Web Server Authentication .....	156
Configuring DivePort for Web Server Authentication .....	158
LDAP Authentication .....	161
Obtaining Information .....	162
Exporting the LDAP Database Listing .....	162

Configuring LDAP Authentication .....	163
Configuring LDAPS .....	165
Implementing SSO on Linux .....	167
OIDC Authentication .....	167
Configuring OIDC Authentication .....	167
Running DiveLine in Clustered Mode .....	170
<b>Appendix D: AntiVirus Exclusions List .....</b>	<b>173</b>
Client Machines .....	173
Application Server .....	173
Solution Directory .....	173
Projects Directory .....	174
Web Server .....	174
Webapps Directory .....	174
Webdata Directory .....	174
<b>Appendix E: Troubleshooting .....</b>	<b>175</b>
Licenses .....	175
DiveLine .....	175
DivePort .....	177
Spectre .....	179
ProDiver .....	179

# Diver Platform 7.2 Overview

## About This Installation Guide

This guide contains installation, configuration, and verification procedures to install the Diver Platform Server 7.2 and the Diver Platform Developer 7.2 packages for Windows. The server package contains DiveLine and web clients DivePort, NetDiver, Bridge, and DIAL; the developer package contains the desktop clients Workbench, ProDiver, and Help Desk. All Dimensional Insight products in these packages are listed as follows:

**IMPORTANT:** The developer package examples are specific to Windows 10, unless stated otherwise. Please keep in mind that steps may differ depending on your configuration.

- **Diver Platform**—The Dimensional Insight software suite that contains Diver 7.2 software, including Workbench and Spectre. User categories are: Developer, ProDiver, DivePort, and DiveTab.
- **Diver Solution**—The Dimensional Insight software suite that contains Diver 7.2 software, including Workbench. User types are tiered: Developer, Advanced, General, and Casual.
- **DiveLine**—The server component of the Diver Platform and Diver Solution. DiveLine authenticates users and controls access to data through Diver clients such as Workbench, ProDiver, DivePort, and DiveTab.
- **Spectre**—The data analysis software in the Diver Platform. Spectre processes data from a database or file to build a column-oriented database (cBase) that caches efficiently on both the server and client device. Spectre is integrated with DiveLine.
- **Workbench**—An integrated development environment to develop, test, and manage projects associated with a Diver application.
- **ProDiver**—The desktop analytics client of the Diver Platform and Diver Solution.
- **NetDiver**—The zero-footprint web-based analytics client that provides ad hoc reporting.
- **DivePort**—The client used to build and display portals that present your Diver data and any other content you need to share over the web.
- **Help Desk**—A desktop component that provides access to user maintenance for the DI client-server applications on the DiveLine server.

## Diver Platform 7.2

- **DiveTab**—The client that provides mobile users access to unstructured content and structured data. It uses guided data navigation and one-touch access on an iPad, PC, or phone. DiveTab is distributed separately.
- **Bridge**—A web application based on DivePort technology that you can use to navigate your DI applications from one central place. For more information, see [Appendix A: Bridge on page 95](#).

**NOTE:** You need to be an administrative user to install the software.

The steps to download and install licenses and components for Diver Platform 7.2 and Diver Solution 7.2 packages are virtually the same. Although the examples in this guide specify Diver Platform 7.2, the procedures can also be used to install Diver Solution 7.2.

If you run into any issues during the installation, contact DI Customer Support for assistance:

- North America: 920-436-8299 or [support@dimins.com](mailto:support@dimins.com)
- United States: <https://www.dimins.com/how-to-contact-dimensional-insight/>
- China: +86 20-8129-6052
- Germany: +49 711 490 04-218
- Netherlands: +31 (0) 88-514 88 00
- Outside of the United States: <https://www.dimins.com/international/>

## About Roles and Environments

DI suggests that there are four basic roles to consider in a customer installation and deployment. The roles are:

1. **Development**—People responsible for the creation of cBases, cPlans, Dive files, classic models, DivePlans and markers, and pages for DivePort or DiveTab
2. **Test**—People responsible for change control and data validation when rolling out a new application, or upgrading software
3. **Production**—People responsible for delivering data to users through any of the DI clients
4. **Build**—People responsible for the part of the extract, transform, and load (ETL) process involving the creation of up-to-date cBase and model files on a regular, usually nightly, schedule

Roles are independent of machines or engines and more than one role can be performed in the same environment. For example, if the people responsible for content development are also responsible for testing and validation, you can



combine the Development and Test roles in the same environment. However, Test and Development environments should be isolated from the Production environment to prevent untested content from reaching users.

DI supports and recommends the use of virtual machines to manage resources. A best practice is to host virtual machines on hardware dedicated to DI applications.

DI recommends that the Production, Development, and Test environments reside on separate machines, either physical or virtual, and host one DiveLine service for each role.

**NOTE:** DI recommends running Bridge on a separate DiveLine, with port number 3330. Bridge serves as a gateway to all other applications.

## About Diver Platform Server 7.2

The Diver Platform Server 7.2 package includes a license utility as well as the following setup files:

- *Bridge-Setup.exe*
- *DiveLine-Setup.exe*
- *DivePort-Setup.exe*
- *NetDiver-Setup.exe*

The *di-license-admin.exe* file is also part of the Server package.

DI recommends that you isolate installation environments by role. Each role, such as Development, Test, and Production, should have its own server environment to ensure optimal data processing. You can install multiple server environments on computers with VM capabilities. In some cases, several roles can share a single server environment by assigning different DiveLine port numbers to each role.

The following table shows common mid-range deployment environments and the DiveLines that they typically connect to on a physical or virtual machine. Each installed DiveLine requires its own port number and license. You must perform a complete Diver Platform Server installation for each DiveLine.

Environment	Port Number
Production	2130
Test	2131

## Diver Platform 7.2

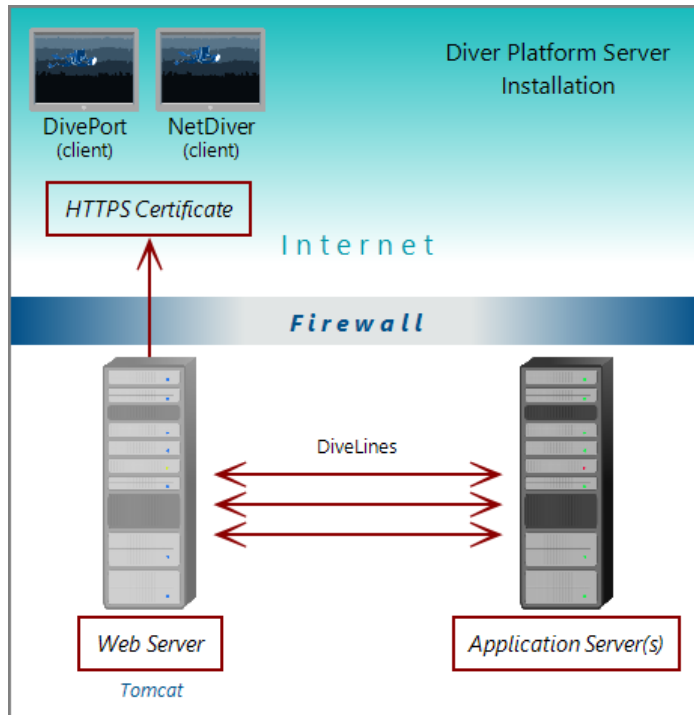
Environment	Port Number
Development	2132
Build	2135
Bridge	3330

The following table shows common low-range deployment environments and the DiveLines that they typically connect to on a physical or virtual machine.

Environment	Port Number
Production	2130
Development/Test	2132

**NOTE:** DI recommends running Bridge on a separate DiveLine, but it is not required. For more information, see [Appendix A: Bridge on page 95](#).

The following illustration provides an overview of the DI server infrastructure that is installed with the Diver Platform Server package. It highlights the primary clients and how the DiveLine servers are installed on a virtual server machine.



**NOTE:** When using Unicode for one component, make sure all components are Unicode. For example, you must have a Unicode DiveLine server to serve Unicode encoded content to a Unicode client.

## About Diver Platform Developer 7.2

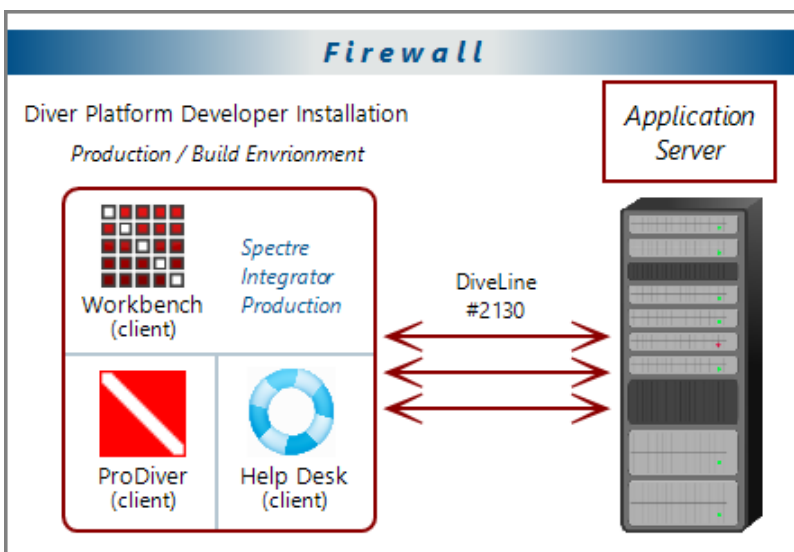
The Diver Platform Developer 7.2 package includes the following executable files:

- **di-broadcast.exe**—A DiveLine client that delivers data to selected users through email. Deliveries can be scheduled on an episodic or periodic basis, or triggered by a specific event.
- **di-config.exe**—A DiveLine subcomponent that allows an administrator to configure DiveLine options by using a Windows user interface. Included to ease transition from version 6.x to 7.2. In 7.2, DI-Config functionality is part of the Workbench Server Settings.
- **di-scheduler.exe**—A DiveLine subcomponent that allows administrators to schedule jobs by using a Windows user interface. Included to ease transition from version 6.x to 7.2. DI-Scheduler functionality is integrated into Workbench.
- **HelpDesk-Setup.exe**—Installation software for the desktop component of the Diver Platform. Help Desk provides access to user maintenance for client-server applications on DiveLine. It requires a separate license.

- **ProDiver-Setup.exe**—Installation software for the desktop analytics client of the Diver Platform. ProDiver is the client in a client–server architecture, which means it requires a connection to a DiveLine server to access data.
- **Workbench-Setup.exe**—Installation software for the integrated visual development environment to develop, test, and manage projects associated with Diver Platform software.

The Diver Platform Developer package contains the Workbench and ProDiver clients that are required to build a DI data infrastructure. You install the developer software on computers independent of any other computers or machines that contain the server software. The developer software typically resides on computers intended for the system administrator or DI content developers.

The following illustration shows some of the components of Workbench and ProDiver that are installed with the DI Platform Developer package. You can see that all of the client applications in this package are installed on user computers connected to the application server behind the company firewall.



## Software Requirements

Before you install and operate Diver Platform 7.2 software, ensure that the following application server, web server, and desktop client requirements are met. In general, DI recommends that you use the latest versions.

**TIP:** Check the DI website periodically for new **Security Notices**.

**NOTE:** A 64-bit operating system is required for servers.

Application and Web Server	Support Notes
Microsoft Windows Server 2019 or later	Minimum version for 7.2. Fully supported. For more information about memory limits of specific versions, please refer to Microsoft's guidelines.
Linux	Fully supported in the following configurations: Red Hat Enterprise Linux, CentOS, Debian, Ubuntu, SuSE. Latest version is recommended. 64-bit is required. The Mono component is required to run Diver Solution and Diver Platform on Linux systems. DI recommends that you download the latest release from <a href="http://www.mono-project.com/download/">http://www.mono-project.com/download/</a> .

Desktop Operating System	Support Notes
Microsoft Windows 11	Fully supported.
Microsoft Windows 10	Fully supported. Recommended version.
Microsoft Windows 8.1	Not supported. Browser compatibility may impact 7.2.
Microsoft Windows 8	Not supported. Browser compatibility may impact 7.2.
Microsoft Windows 7	Browser compatibility issues might impact web clients. <b>IMPORTANT:</b> Windows 7 does not support TLS 1.2 in its default configuration, which DiveLine 7.1 requires to communicate with Workbench. For more information, see Technical Notice 9 on DI's customer website.

**NOTE:** Controls for HTTP cookies and JavaScript must be enabled for each client computer's web browser.

Web Browser	Support Notes
Internet Explorer 9 or later	Unsupported for 7.2.
Google Chrome, Microsoft Edge, Mozilla Firefox, Safari	Fully supported. Latest version recommended.

**NOTE:** The following third-party software comes bundled with the DI installers for Windows.

Java	Support Notes
OpenJDK 17	Latest version is required.
Java 10	Minimum version required. Some features might not function.

**IMPORTANT:** Due to Java licensing changes, updates for Oracle's Java Runtime Environment are no longer available for business, commercial, or production use without a commercial license. DI recommends using OpenJDK.

Apache Tomcat	Support Notes
Tomcat 9.0	Minimum version is required for use of 7.2 web clients. Latest version is recommended.
Tomcat 7.0	Tomcat 7.0 reached it's end-of-life as of March 2021, and no longer receives updates. DI recommends updating to Tomcat 9.0.

Microsoft	Support Notes
.NET Framework 4.7.2 or later	The .NET Framework helps you create mobile, desktop, and web applications that run on Windows PCs, devices, and servers.

**NOTE:** When installing to a VM, DI recommends that you use a fixed Media Access Control (MAC) address. This prevents licenses issues if the VM is relocated. See the VMware Knowledge Base at <http://kb.vmware.com>.

## Building the DI Directory Structure

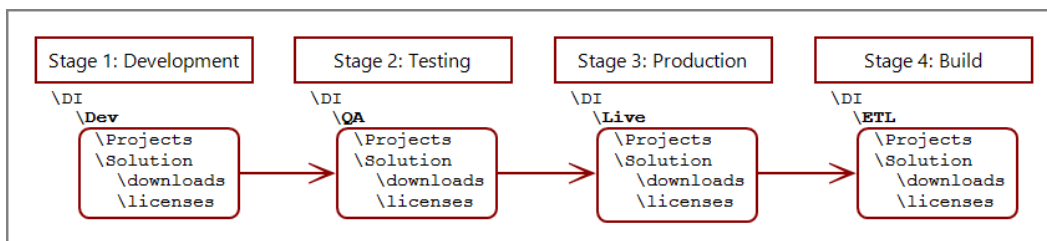
Prior to downloading and installing DI Platform server and developer software for 7.2, DI recommends that you create the following directory structure on your machine:

```

\DI
  \Projects
  \Solution
    \downloads
    \licenses

```

If yours is a large site where content is developed, tested, released, and extracted in four separate phases, but the content is stored on a single server, consider using a four-stage release process with a slightly different DI directory structure.



**NOTE:** This reflects the environments used on a single server so the `DI` directory has subdirectories for each environment.

You can install server and developer software on a single machine or different machines using the same directory structure. You can install Java and Apache Tomcat third-party software using *DivePort-Setup.exe*.

The following table provides a brief description of the default directories and subdirectories that the installer uses in a typical DI directory structure.

Directory	Subdirectory	Description
DI	\Projects	Default location for Workbench projects. This folder is created manually.
DI	\Solution	Default location for folders and files created by DI product installations. This folder is created manually.
DI\Solution	\downloads	Default location for DI software downloads. This folder is created manually.
DI\Solution	\licenses	Folder for licenses and key files. This folder is created manually.
DI\Solution	\diveline	Subdirectory with program files required by the DiveLine service. Each installed DiveLine instance can have its own <code>\diveline</code> folder.
DI\Solution	\dl-dataroot	Top level directory for the DiveLine server for configuration information, cache, and log files. Each installed DiveLine instance can have its own <code>\dl-dataroot</code> folder.
DI\Solution	\executables	Default location for many DI executable files.



Directory	Subdirectory	Description
DI\Solution	\webapps	Program, configuration, and setup files for DivePort and NetDiver.
DI\Solution	\webdata	Data and customization files for DivePort and NetDiver.

## About Diver Platform and Solution 7.2 Licenses

Diver Platform 7.2 is the paid upgrade path for customers who want to use the Spectre engine, DiveTab, or Measure Factory. Diver Solution 7.2 is the free, standard software upgrade path for Diver Solution 7.0 customers on a maintenance plan. Users licenses differ depending on whether you use Diver Platform or Diver Solution.

**NOTE:** Some features, such as Input Tables, Measure Factory, and Help Desk, are licensed separately from your Diver Platform or Diver Solution license. Contact your Dimensional Insight sales representative for more information.

### Diver Platform Licenses

User categories are defined for Diver Platform licensing. To use different client programs, a user can belong to multiple license categories. Each named user is in zero or more user categories.

Each category has a limited number of users, based on the number of licenses. If more users are assigned to the category than the license allows, excess users are denied access. Users that do not authenticate successfully are denied access and told to contact an administrator.

The user license types for Platform 7.2 are:

- **Developer**—Grants access to Workbench and all Diver clients
- **ProDiver**—Grants access to ProDiver, Broadcast, and DIAL
- **DivePort**—Grants access to DivePort and NetDiver
- **DiveTab**—Grants access to DiveTab for the iPad and PC
- **Help Desk**—Grants access to Help Desk and DI-Config to manage user account changes without consuming a Developer license
- **ODBC**—Grants access to DI-ODBC driver

## Diver Solution Licenses

Diver Solution 7.2 maintains the tiered user licensing scheme that is used in Diver Solution 6.4, with the addition of a new tier called Developer. Different tiers give users access to different client programs. Each named user is in one tier only. If you assign more users to a tier than the license allows, the administrator sees a warning, and the last user assigned is disabled.

The tiered user types for Solution 7.2 are:

- **Developer**—Grants access to Workbench and all Diver clients
- **Advanced**—Grants access to ProDiver, DivePort, NetDiver, DI-Config, DI-Broadcast, DI-Scheduler, and DIAL
- **General**—Grants access to DivePort, NetDiver, and DI-Config
- **Casual**—Grants access to DivePort

## What Is Named User Licensing?

Diver Platform and Diver Solution use *named user licensing*. In this type of licensing scheme, each user has their own unique logon information and can be logged on from only one computer at a time.

## About License Types

Whether you use Diver Platform or Diver Solution, your product licenses fall into one of two categories:

### Perpetual Licenses

You use a perpetual license for software that you purchased on a maintenance contract. This type of license allows you to have a certain number of users and virtual environments based on the conditions in your maintenance contract and provides for routine software updates.

Perpetual licenses become outdated on the same day that your maintenance contract ends. When you renew your maintenance contract, you receive a new license so that you can continue to receive software updates.

If you choose not to renew your maintenance contract, you can continue to run the software using the outdated license. However, you cannot upgrade the software or move it to a new machine.

### Trial Licenses

You use a trial license for software that you are trying for a short period of time.

Trial licenses have an expiration date. Once the expiration date passes, you can no longer run the software that the trial license enables.

**NOTE:** A license's expiration or maintenance date is always on the first of the month. For example, a license with a maintenance date of 11/2021 becomes outdated on November 1st, 2021.

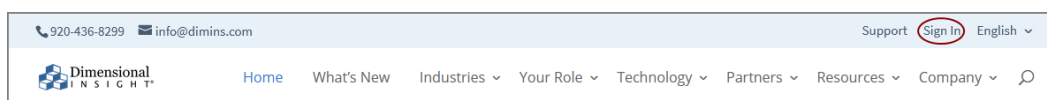
# Installing Diver Platform Server

These installation procedures use most of the installer defaults. Be sure to alter the defaults as required when you repeat these steps to create separate environments, for example, Test versus Production. See [Building the DI Directory Structure on page 9](#) and [About Roles and Environments on page 2](#).

## Downloading the Server Installation Package

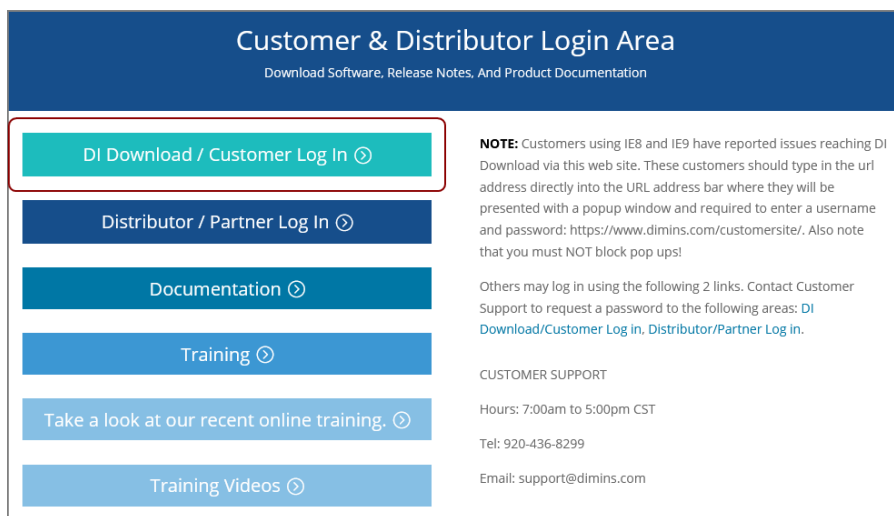
You can download purchased software from the Dimensional Insight website.

1. Using a web browser, go to the Dimensional Insight website:  
<http://www.dimins.com>.
2. On the home page, click **Sign In**.



The **Customer & Distributor Login Area** page opens.

3. Click **DI Download / Customer Log In**.



A dialog box prompting for your sign-in information opens.

4. Enter your **Username** and **Password**, and click **OK**.  
The **Dimensional Insight Customers** home page opens.
5. Click **DI-DOWNLOAD**.

The software and documents download page opens.

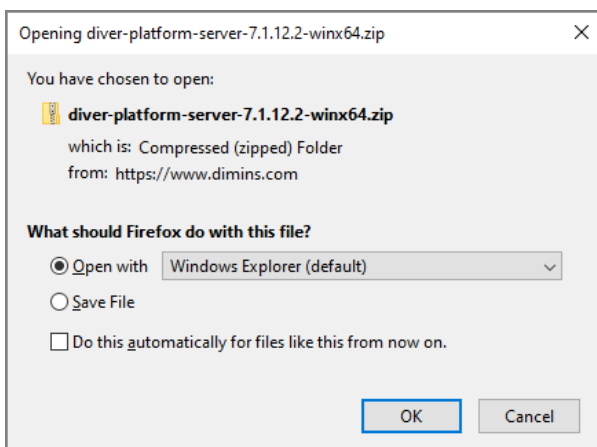
Available for Download	Current Point Release	Previous Point Releases	Release Notes	Manual
- Info 6.4	<a href="#">6.4.1 (1166KB)</a>	<a href="#">Previous Point Releases</a>	Not Available	Not Available
- Licensing 7.1	Update not available	None Available	Not Available	Not Available
- Licensing 7.0	<a href="#">7.0.29 (23102KB)</a>	<a href="#">Previous Point Releases</a>	Not Available	Not Available
- Licensing 6.4	<a href="#">6.4.25 (2817KB)</a>	<a href="#">Previous Point Releases</a>	Not Available	Not Available

6. Locate the latest version of the 7.2 software that you purchased, and click the blue version number.

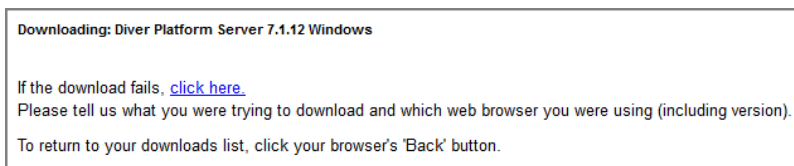
## Diver Platform 7.2

Diver Platform Server 7.2 linux64	7.2.10 (679575KB)	<a href="#">Previous Point Releases</a>	<a href="#">Release Notes (30KB)</a>	Not Available
Diver Platform Server 7.2 linux64 limited	7.2.10 (679572KB)	<a href="#">Previous Point Releases</a>	<a href="#">Release Notes (30KB)</a>	Not Available
Diver Platform Server 7.2 Windows Unicode limited	7.2.10 (1831346KB)	<a href="#">Previous Point Releases</a>	<a href="#">Release Notes (30KB)</a>	Not Available
Diver Platform Server 7.2 Windows	7.2.10 (1875872KB)	<a href="#">Previous Point Releases</a>	<a href="#">Release Notes (30KB)</a>	Not Available
Diver Platform Server 7.2 Windows limited	7.2.10 (1875875KB)	<a href="#">Previous Point Releases</a>	<a href="#">Release Notes (30KB)</a>	Not Available
Diver Platform Server 7.1 linux64_uc limited	7.1.33 (642238KB)	<a href="#">Previous Point Releases</a>	<a href="#">Release Notes (546KB)</a>	Not Available
Diver Platform Server 7.1 linux64	7.1.33 (664389KB)	<a href="#">Previous Point Releases</a>	<a href="#">Release Notes (546KB)</a>	Not Available

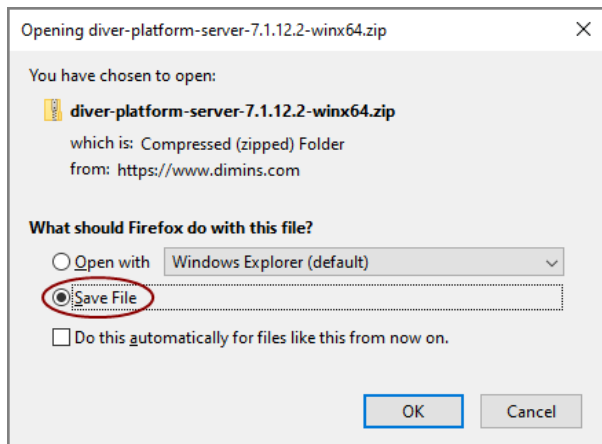
The **Opening** download verification dialog box opens.



The **Downloading** page opens in the browser. If the **Opening** dialog box does not open automatically, follow the instructions on the page:



7. Select **Save File**, and click **OK**.



The Diver Platform Server software package *zip* file downloads to the `Downloads` directory on the local computer.

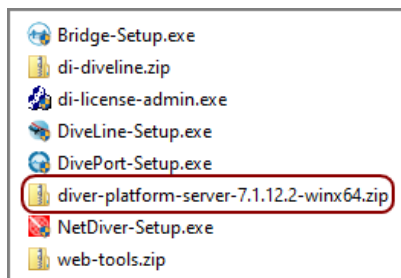
**NOTE:** Most browsers enable you to configure the download location for files downloaded from the Internet. For example, if you are using the Firefox browser in Windows, you can choose **Settings** > **General** and configure the download location in the **Files and Applications** section.

## Extracting the Server Installation Package

After you download the Diver Platform Server 7.2 software package, extract the files:

1. Move the server package from your `Downloads` directory to the `DI\Solution\downloads` directory.
2. Right-click the package and select **Extract All**, or use a third-party tool, to unzip the file.

The following executable files are extracted to the directory:



## Requesting a License

Before you install the DI server software, you must request and install a DI license. You must do this for every physical or virtual environment in your deployment.

Complete the following process using the same machine that you plan to install the licenses on later. Keep in mind that your machine must have Internet access to submit a license request.

To request a license to install the Diver Platform Server 7.2 and Diver Platform Developer 7.2 packages:

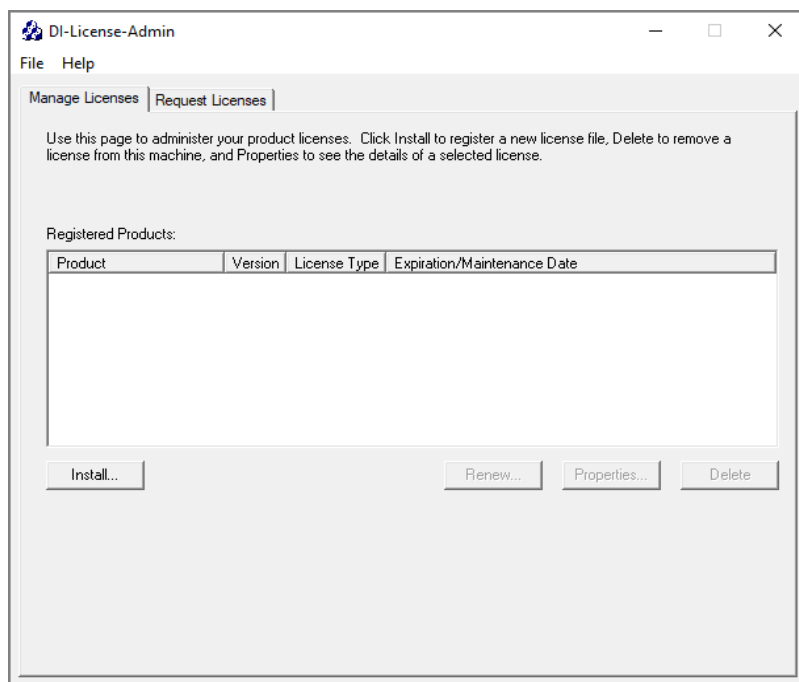
1. Navigate to the `DI\Solution\downloads` directory.
2. Double-click the **di-license-admin.exe** file.

The **User Account Control** dialog box opens, asking you to confirm making changes to your device.

**NOTE:** Depending on your Windows version and user account settings, you might see the **Open File - Security Warning** dialog box instead. Confirm that you want to open and run the executable.

3. Click **Yes**.

The DI-License-Admin utility starts.

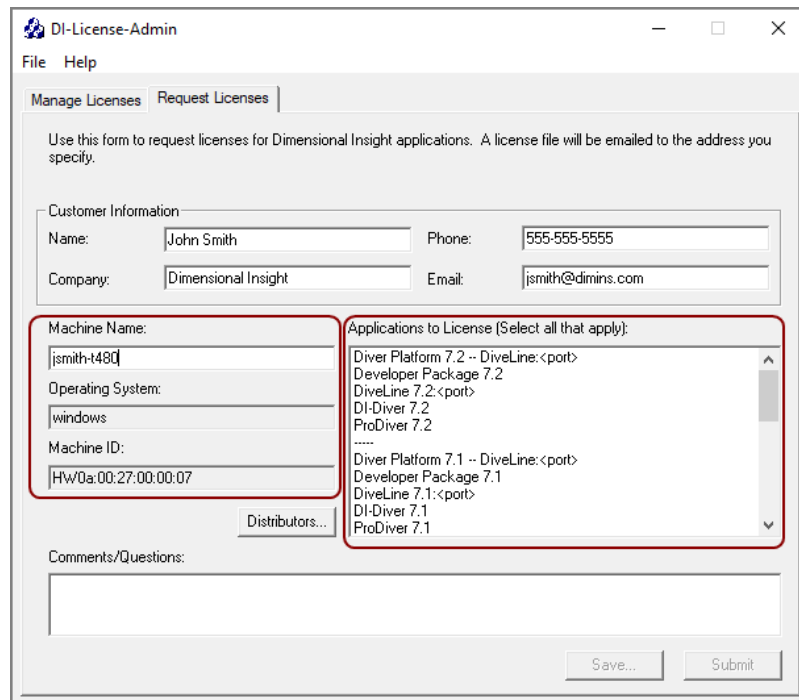


4. Click the **Request Licenses** tab.

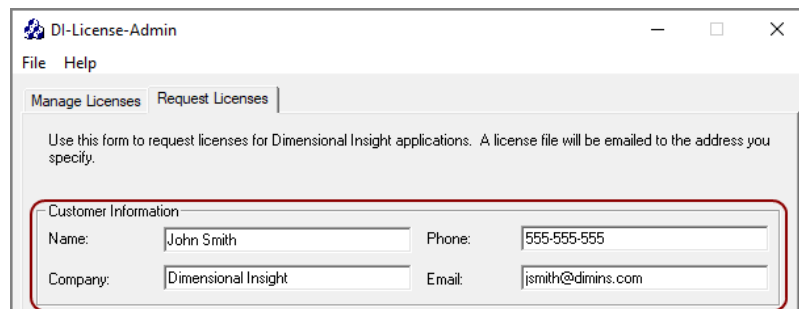


On the left, the **Machine Name**, **Operating System**, and **Machine ID** boxes are populated with your machine's information.

On the right side of the dialog box, the **Applications to License** box is populated with the licenses you can request.



5. Complete the **Customer Information** section.



6. Specify details about the server-side licenses that you want to request:
  - a. In the **Applications to License** box, select the license that enables the server-side software that you purchased. For example, if you purchased Diver Platform Server 7.2 for Windows, select **Diver Platform 7.2 BI – DiveLine <port>**.

The **Define Port-locked Information** dialog box opens.

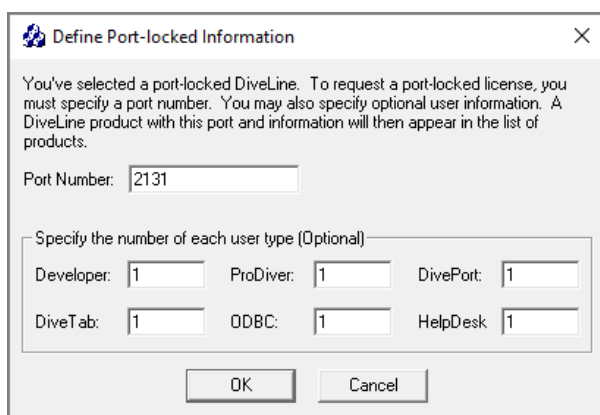
- b. Enter the port number that you want to use.

You must specify a unique port number for every virtual environment in your deployment.

**TIP:** The default port number is 2130, however you can use any number that you want.

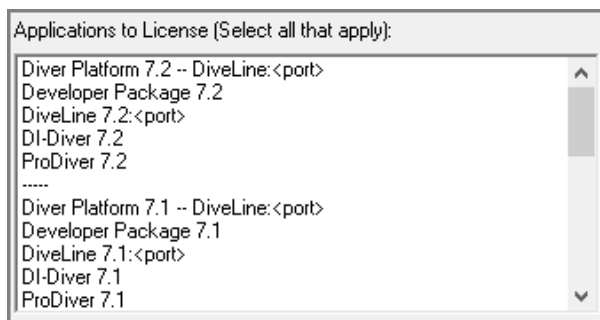
- c. If you know the number of users of each type that you purchased access for, complete the remaining fields.

Otherwise, Dimensional Insight Customer Support can find this information when they create your license.



- d. Click **OK**.

The options that you specified display as a new entry in the **Applications to License** box.



- e. Repeat Steps **a** through **d** to request a server-side license for each virtual environment on your machine.

**NOTE:** If you plan to install Bridge, Dimensional Insight recommends that you request an additional server-side license. When implementing Bridge, you typically install an extra DiveLine that only Bridge connects to.

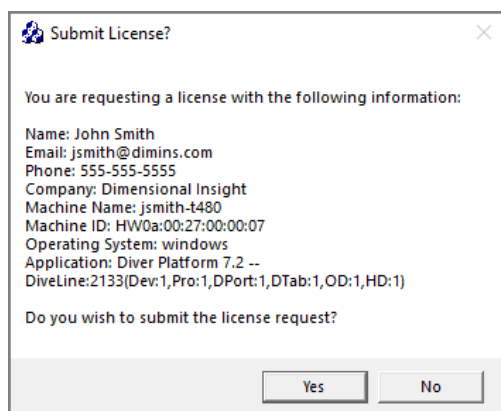
7. In the **Applications to License** box, select the remaining licenses for the products that you purchased.

For example, if you purchased Diver Platform, select **Developer Package 7.2**.

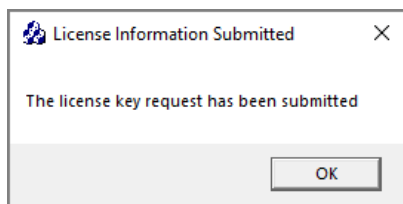
8. In the **Comments/Questions** box, specify any additional purchases, such as Input Tables, Measure Factory, or Help Desk, and include any comments or questions that you have. Dimensional Insight recommends that you also provide your machine's media access control (MAC) address.

**NOTE:** If installed on a virtual machine and that machine is relocated, a new license is required. This can be avoided by ensuring the virtual machine is installed with a fixed MAC address. For more information, see <http://kb.vmware.com>.

9. Click **Submit** to open the **Submit License?** dialog box showing your selections.



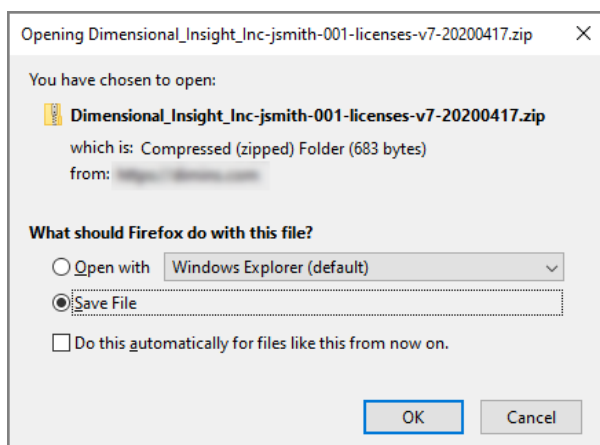
10. Click **Yes** to submit the license request.
11. Click **OK** to acknowledge the submission.



12. Click **Save** to store the license request file to the `DI\Solution\licenses` directory.

**NOTE:** In the event that the installation does not have internet access, locate the saved request file (for example, `di_request_jsmith-001.request`) and forward to a machine with email access. Send the request file to [support@dimins.com](mailto:support@dimins.com).

13. After DI Customer Support sends you the requested license, save it to the `DI\Solution\licenses` directory.



**NOTE:** Some email programs might include this file as inline text. Make sure that the license file is an attachment.

14. Right-click the package and select **Extract All**, or use a third-party tool, to unzip the file.

The following example shows a Diver Platform Server 7.2 license file:

```
c3931_jsmith-001_platform72_p2131_m202107.license
```

## Installing a License File

After receiving a DI license file (and before attempting to install the software), you must extract the attached file from the support email to `DI\Solution\licenses`, and then install the license file.

**TIP:** After installing a new license, restart DiveLine and Tomcat, and close and reopen the software to update the license information.

1. Navigate to the `DI\Solution\downloads` directory.
2. Double-click the **di-license-admin.exe** file.

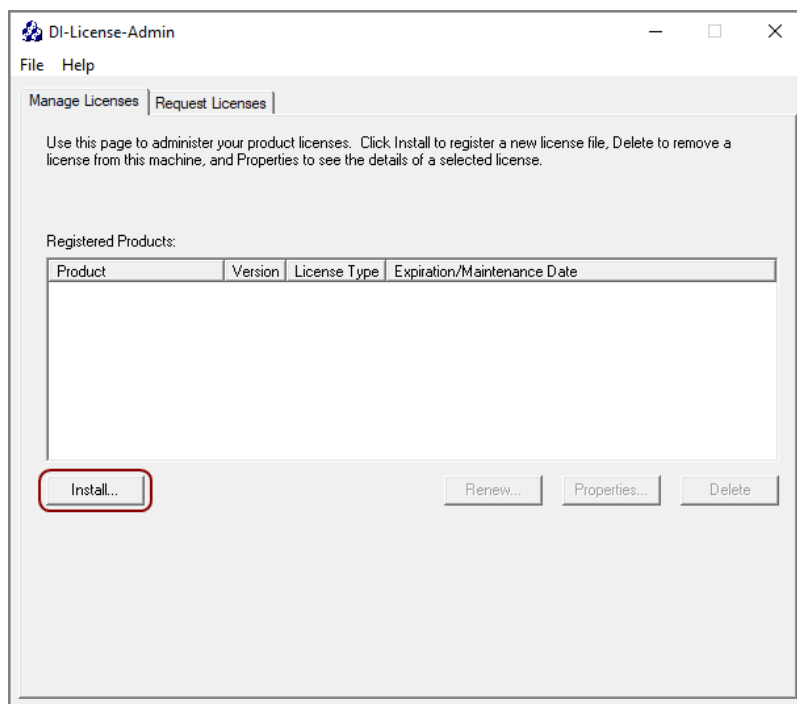
The **User Account Control** dialog box opens, asking you to confirm making changes to your device.

**NOTE:** Depending on your Windows version and user account settings, you might see the **Open File - Security Warning** dialog box instead. Confirm that you want to open and run the executable.

3. Click **Yes**.

The DI-License-Admin utility starts.

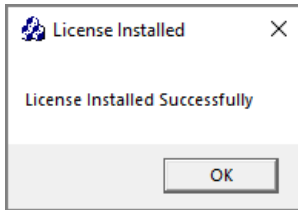
4. On the **Manage Licenses** tab, click **Install**.



5. From the **Open License File** dialog box, navigate to the `DI\Solution\licenses` directory.
6. Select the license file that you want to install, and click **Open**.

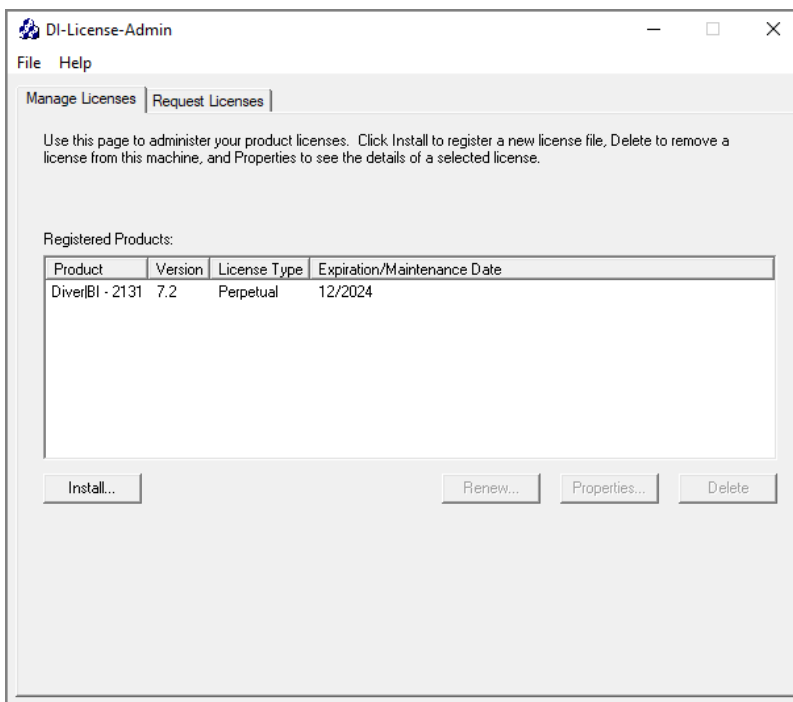
**NOTE:** If you are replacing an existing license with a more restrictive license, the **Restrictive License Info** dialog opens, asking if you still want to install the file. Note the conditions of the new license, and click **Yes**.

The license program displays a confirmation message.



7. Click **OK**.

The license displays in the list of **Registered Products**.



**NOTE:** Open the DI-License-Admin utility to the **Manage Licenses** tab to view all registered products and their license types.

## Installing DiveLine

DiveLine is the Diver server component that authenticates users and provides centralized access to cBase and model data. DiveLine shares processing with various DI clients, such as Workbench, DivePort, ProDiver, NetDiver, and DiveTab. DiveLine accepts connections from clients and communicates with them by means of a proprietary protocol. DiveLine runs in the background as a

service and requires a Windows user account that you or the installation wizard creates.

Note that with Diver Server 7.2, DI is building 64-bit encrypted DiveLines only.

**NOTE:** You need to be an administrative user to install the software.

To install DiveLine, complete the following steps:

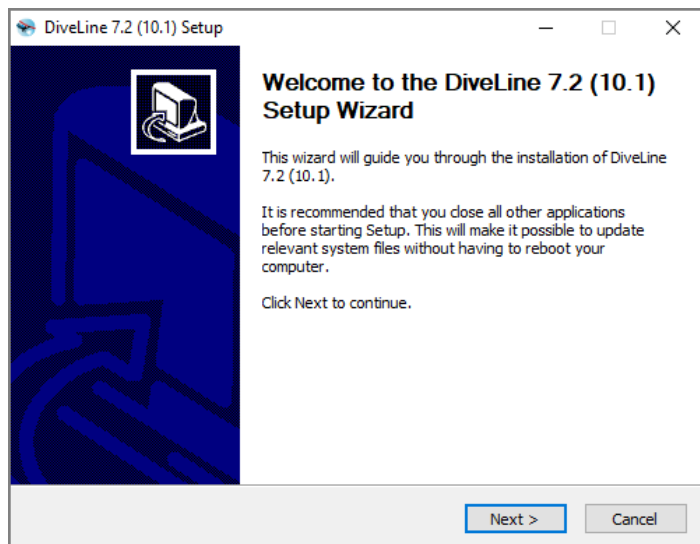
1. Navigate to the `DI\Solution\downloads` directory.
2. Double-click the **DiveLine-Setup.exe** file.

The **User Account Control** dialog box opens, asking you to confirm making changes to your device.

**NOTE:** Depending on your Windows version and user account settings, you might see the **Open File - Security Warning** dialog box instead. Confirm that you want to open and run the executable.

3. Click **Yes**.

The **DiveLine 7.2 <version number> Setup Wizard** dialog box opens.



4. Review the setup instructions, and click **Next**.

**CAUTION:** If NET 4.7.2 is not installed, the **Verify Microsoft .NET 4.7.2 Install** page displays.

- a. Click the **Install .NET 4.7.2** button.

The **Microsoft .NET Framework** window opens.

- b. Select the check box to accept the licensing terms.

- c. Click **Install**.

When the installation completes, the **Installation is Complete** page opens.

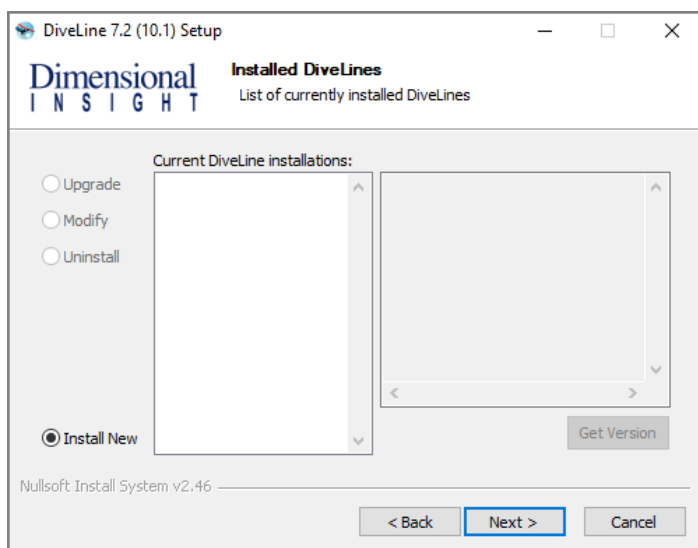
- d. Click **Finish**.

- e. Click **Restart Now**, to restart your machine.

**IMPORTANT:** Choosing to restart later may cause applications depending on .NET to stop working.

After restarting your machine, return to [Step 1](#) to start the DiveLine installation process again.

The **Installed DiveLines** page displays.

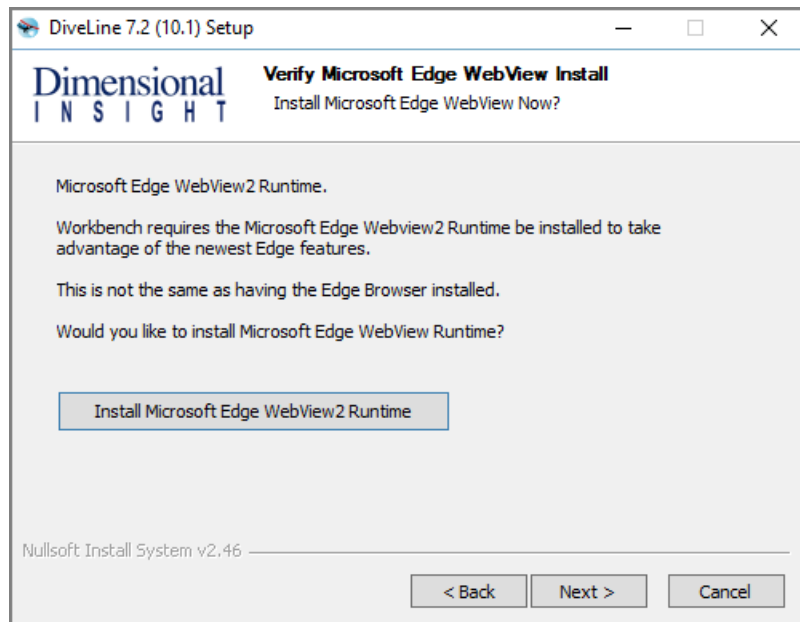


- 5. Select the **Install New** option. This page lists any existing DiveLine installations, which you can choose to **Upgrade**, **Modify**, or **Uninstall**.
- 6. Click **Next**.

If Microsoft Edge WebView2 Runtime is not installed, the **Verify Microsoft Edge WebView Install** page displays.

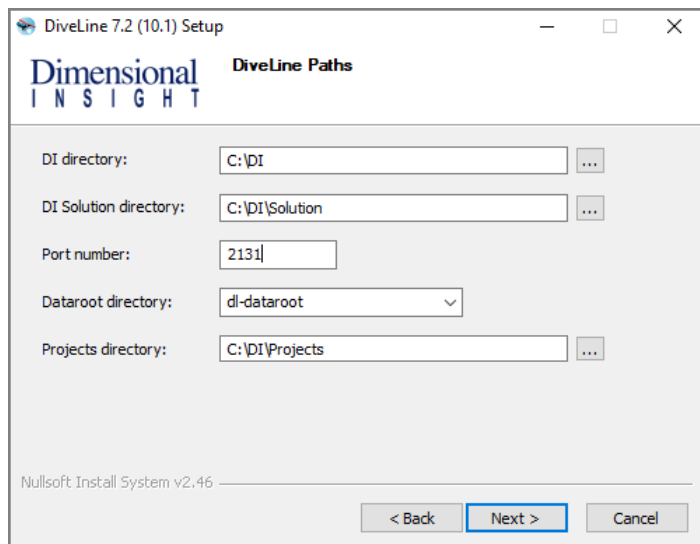
- a. Click the **Install Microsoft Edge WebView2 Runtime** button to start the installation process.





b. Click **Next** when the installation process finishes.

The **DiveLine Paths** page displays.



7. Accept the default values or select new ones for the following options:

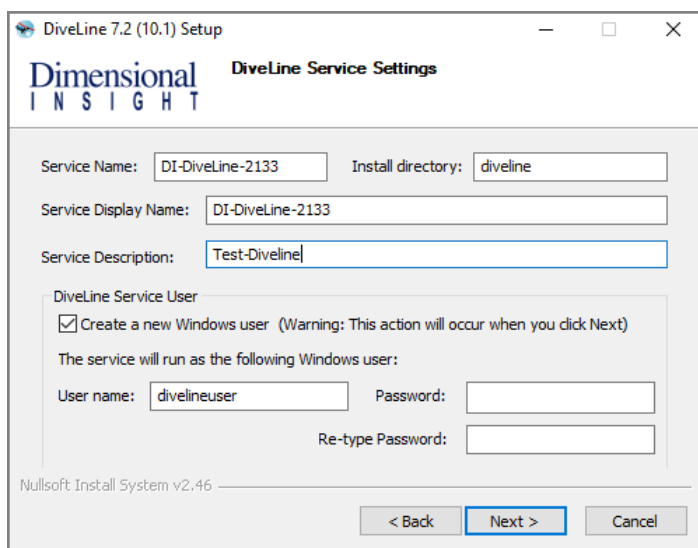
- **DI directory**—The default path is `C:\DI`.
- **DI Solution directory**—The default path is `C:\DI\Solution`.
- **Port number**—The default port number is **2130**, but it must match the port number used in the license request. Assign unique port

numbers for different environments. For example, **2131** for a Test environment.

- **Dataroot directory**—The default directory is `dl-dataroot`. If you previously installed DiveLine or have another instance, you can choose that Dataroot directory. However, sharing dataroots between environments such as test and production is not recommended.
- **DI Projects directory**—The default directory is `C:\DI\Projects`.

8. Click **Next**.

The **DiveLine Service Settings** page displays.



9. The DiveLine Service Settings dialog box is populated with default values (which you can change).

- **Service Name**—The default is **DI-DiveLine**. If you specify a port number other than the default, 2130, the port number is appended to the end of the name. For example, **DI-DiveLine-2131**.
- **Install directory**—The default is **diveline**. You can change this to give it a meaningful label. For example, specifying a particular DiveLine if more than one is in use.
- **Service Display Name**—The default is **DI-DiveLine**. If you specify a port number other than the default, 2130, the port number is appended to the end of the name. For example, **DI-DiveLine-2131**.
- **Service Description**—Add a service description; recommended when more than one diveline resides on a machine. The description

should indicate the purpose of the DiveLine. For example, **Test DiveLine**.

- **DiveLine Service User**—Specifies which user on the machine owns the DiveLine service. Clear the **Create a new Windows user** check box if you have already identified a Windows user for the DiveLine service. The Windows user must have administrator rights.

**NOTE:** A non-blank password for the Windows user is required.

- **User name**—The default is **divelineuser**. If you are not creating a new Windows user, enter the existing user name and password. If you are creating a new user, choose a user name and enter and retype a password for the account.

This is the user that runs the service in the background. You can either create a new Windows user, **divelineuser**, on your machine to act as the DiveLine Service user, or use an existing user by clearing the **Create a new Windows user** check box and entering an existing Windows user name and password.

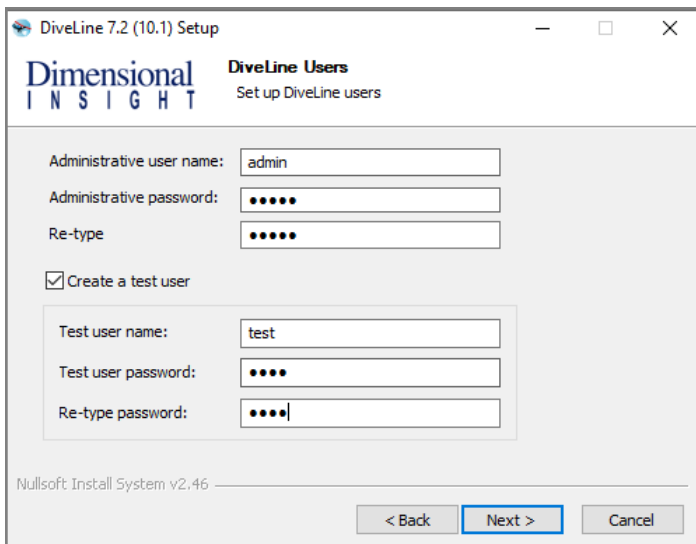
**NOTE:** As of 7.1(9), you can run the DiveLine service as special users **LocalService** or **NetworkService** (or the equivalent **NTAuthority\LocalService** or **NTAuthority\NetworkService**). No password is required for these users.

**CAUTION:** When installing DiveLine as the Local Service user, be aware that changes to the Windows share permissions property can remove Local Service user access to files and folders, resulting in "permission denied" errors in Workbench and ProDiver.

10. Click **Next**.

The **DiveLine Users** page displays. You must specify an Administrative user name and password and, optionally, create a test user. Be sure to re-type the password. The administrative user is needed in order to access and make configuration changes to the DiveLine server. A test account is useful for verifying access by a non-administrative user.

**NOTE:** If you used a preexisting Dataroot directory (see [Step 7](#)), this **DiveLine Users** dialog box is skipped.

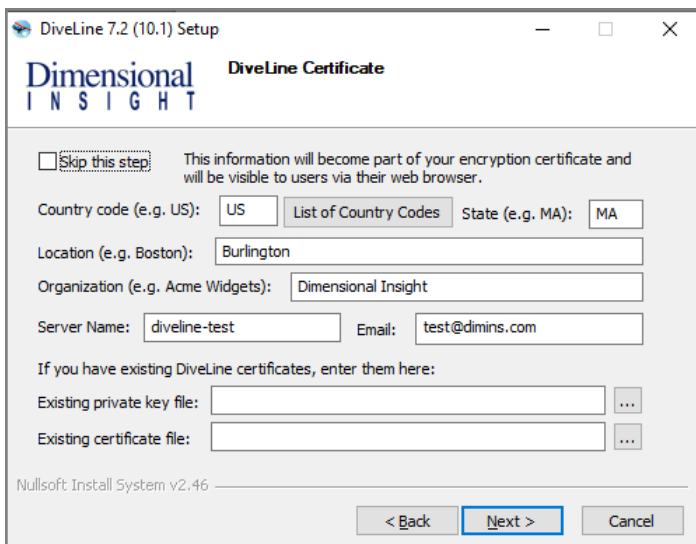


Creating an administrative user enables you to log in to DiveLine. No specified user results in an inaccessible DiveLine.

A test user gives you a non-administrative user to test with. To create a test user, select the **Create a test user** check box, and enter a Test user name, a Test user password, and re-type the password.

11. Click **Next**.

The **DiveLine Certificate** page displays.



12. Do one of the following:

- If you do not want to create or use an encryption certificate, select **Skip this step**. This is not recommended.

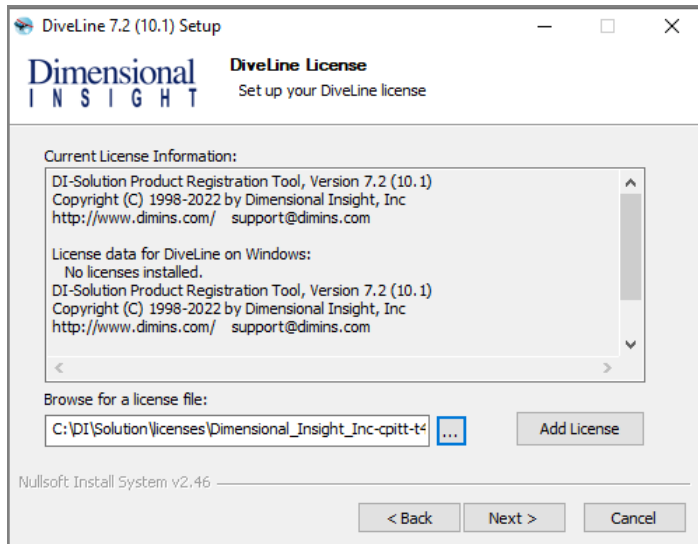
**NOTE:** If you select this option, users see a message similar to **This site is insecure** when using DiveLine to access data. If you have existing DiveLine certificates, click the ellipsis buttons to locate and select their private key files and certificate key files.

- If you do not already have an encryption certificate, fill in the following fields to create one:
  - **Country code**—Enter your two character country code. Click **List of Country Codes** to display a complete list of country codes.
  - **State**—Enter your state abbreviation.
  - **Location**—Enter a city name or other identifier.
  - **Organization**—Enter the name of your company or organizational name.
  - **Server Name**—Enter the name of the server (the machine name).
  - **Email**—Enter an email address.
- If you already have an encryption certificate (for example, from a previous installation), select your private key and certificate files. These files are located in the `DI\Solution\<DiveLine directory>\install-files` directory, and are the *privatekey.txt* and *certificate.pem* files.

13. Click **Next**.

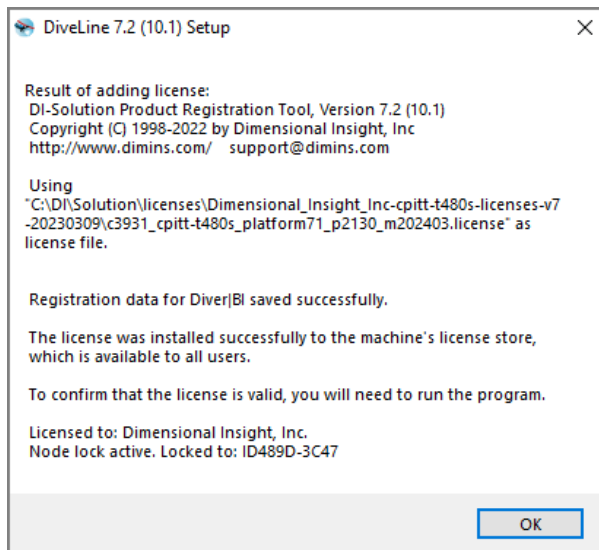
The **DiveLine License** page displays. Browse for and open the license file.

## Diver Platform 7.2



14. Click **Add License**.

The **Result of adding license** window opens.

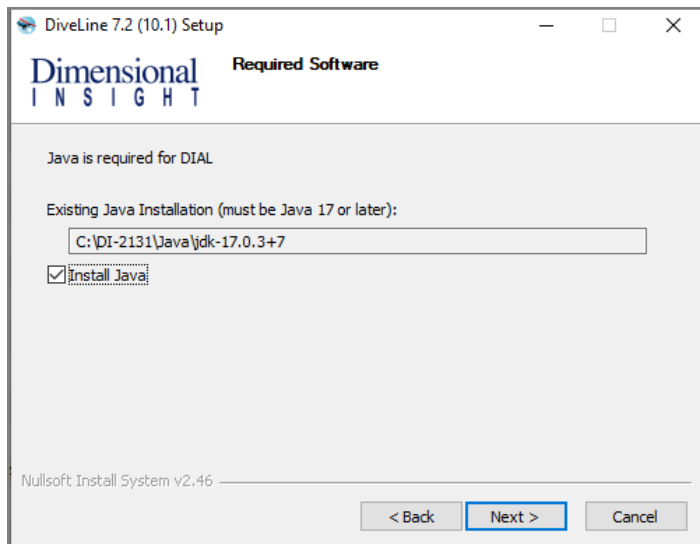


15. Click **OK**.

The window closes.

16. Click **Next**.

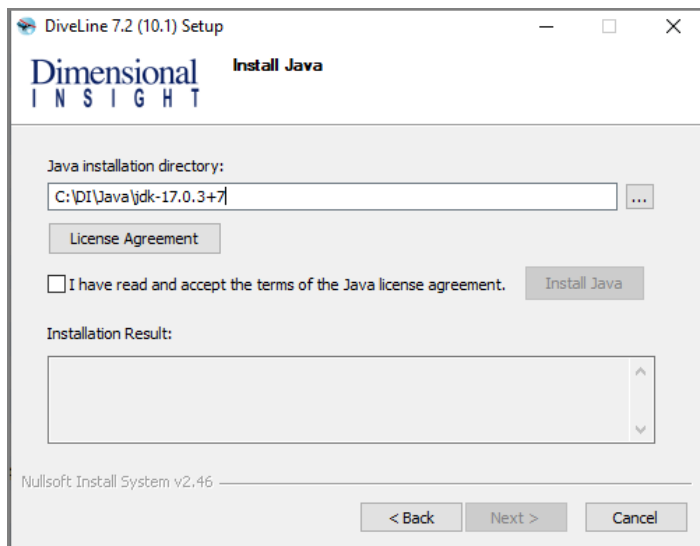
The **Required Software** page displays for installing Java 17 or later (if not already installed). This is required to run DIAL (Dimensional Insight Access Language) and DivePort.



**NOTE:** If Java already exists on your machine, it appears in the Existing Java Installation box with the **Install Java** check box cleared. Click **Next**, and proceed to [Step 21](#).

17. Click **Next**.

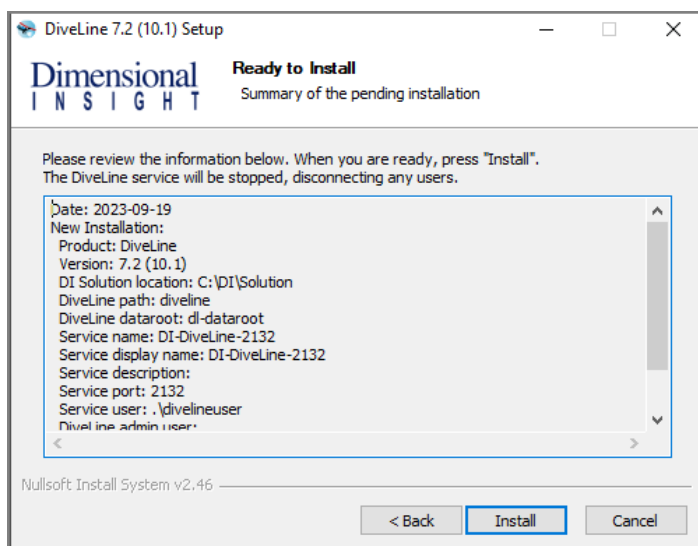
The **Install Java** page displays.



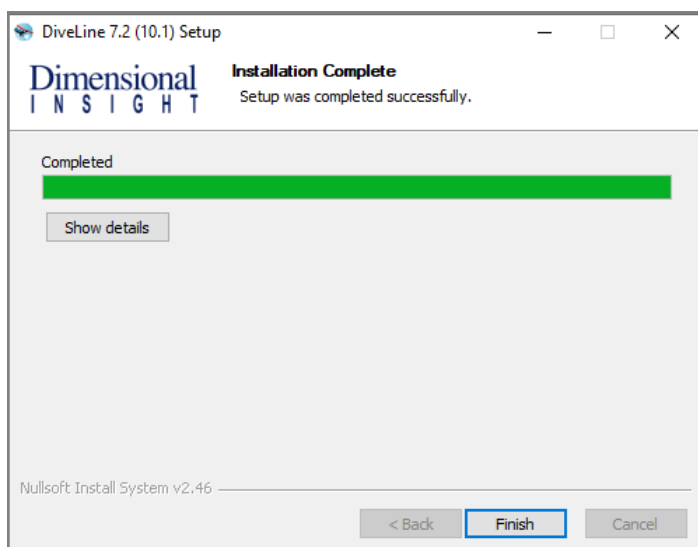
18. Do the following:

- Accept or change the Java installation directory.
- Click **License Agreement** to open the terms of the license.
- Select the license agreement check box to accept the license terms.

- Click **Install Java**, and click **OK** in the pop-up window to confirm the installation. This might take several minutes.
19. After you see the **Successfully installed Java** message in the Installation Result text box, click **Next**.
  20. When the **Ready to Install** dialog box opens giving a summary of the pending DiveLine installation, click **Install**.



21. When you see the **Installation Complete** confirmation message, click **Finish**.



22. Restart your machine.



## DiveLine Files

The DiveLine installation wizard adds the following files to the

`C:\DI\Solution\executables` directory:

- **dial.jar**—The Dimensional Insight Access Language component that enables you to remotely analyze and report the content of models and cBases.
- **di-broadcast.exe**—The DiveLine client that provides scheduled or event-driven delivery of Diver markers using email.
- **dicfg.exe**—The DiveLine subcomponent that allows an administrator to configure DiveLine options using a command line tool.
- **di-config.exe**—The DiveLine client that allows an administrator to configure DiveLine options using a Windows user interface. It is included to ease the transition from 6.x.
- **dictl.exe**—The command line tool for DI-Controller; used to disconnect users accessing a particular model or cBase. It is included to ease the transition from 6.x.
- **disch.exe**—The command line tool for DI-Scheduler. It is included to ease the transition from 6.x.
- **di-scheduler.exe**—The DiveLine subcomponent that allows an administrator to create, automate, and monitor events related to DI products using a Windows user interface. It is included to ease the transition from 6.x.
- **di-updater.exe**—The subcomponent that creates a package for managing downloads to DiveLine.
- **diver.exe**—The desktop version of the Diver application. It does not work with cBases.
- **exportinfo.exe**—The subcomponent that provides machine identification information for licensing a machine that is not connected to the Internet.
- **prodiver.exe**—The desktop analytics client of the Diver Platform.
- **register.exe**—The command line tool for license maintenance.

In addition to the above listed executables, the DiveLine installer adds the following Diver 7.2 executables to the `C:\DI\Solution\\bin` directory:

- **builder.exe**—The Diver component that transforms data by summarizing and preprocessing it in order to create classic models.

- **dial.jar**—The Dimensional Insight Access Language component that enables you to remotely analyze and report the content of models and cBases.
- **di-diveline.exe**—The main component of the DiveLine application server software that servers data to client applications.
- **di-listener.exe**—The component of the application server that manages incoming client connections.
- **di-logger.exe**—The component of the application server that collects a list of activities performed by the server.
- **di-scheduler-engine.exe**—The component of the application server that handles the scheduling of jobs.
- **di-service.exe**—The component of the application server that manages services.
- **integ.exe**—The Diver Solution extract, transform, and load scripting tool.
- **spectre.exe**—The data analysis software that is used to build and query cBases. It powers the DiveLine server software for efficient queries from DI clients against those cBases.

## Testing the DiveLine Installation

To verify the successful implementation of DiveLine, you must connect to the correct DiveLine port on the server using a DiveLine client, such as *prodiver.exe*.

**NOTE:** This test uses a copy of the ProDiver application placed on the server by the DiveLine installer.

Complete the following steps:

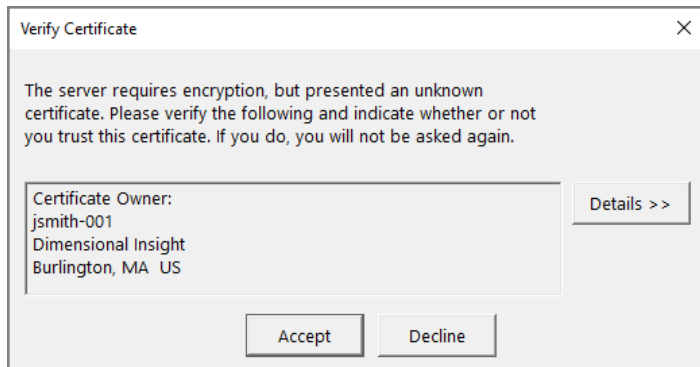
1. Navigate to the `DI\Solution\executables` directory.
2. Double-click the **prodiver.exe** file.

ProDiver and the **DI-DiveLine Hostname** dialog box opens.

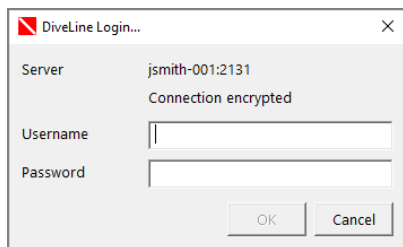


3. Enter the server name. For example, **jsmith-001:2131**.
4. Click **OK**.

- If this is the first time you are opening a client after the server install in which you created a self-signed certificate, the client opens the **Verify Certificate** dialog box asking you to verify and accept the certificate presented to the server.

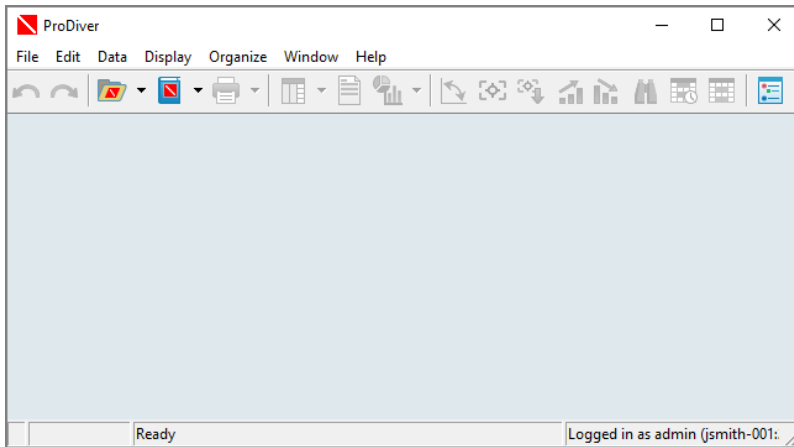


- If you want to view information about the certificate, click **Details**.
- Click **Accept** to trust the certificate.
- On the **DiveLine Login** dialog box, enter the DiveLine **Username** and **Password**.

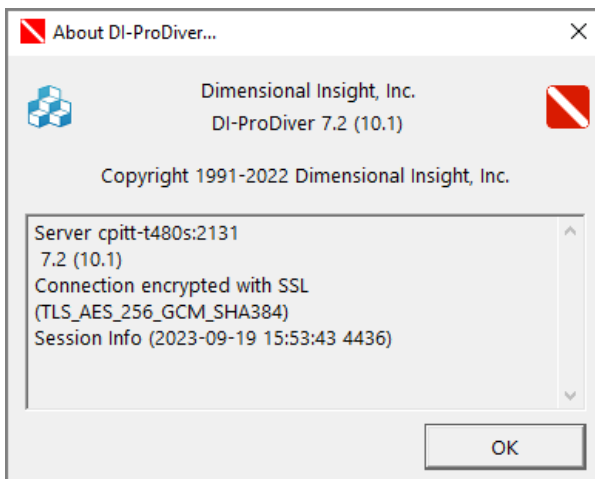


- Click **OK** to open the **ProDiver** home page.

## Diver Platform 7.2



10. To verify the installed version of ProDiver, click **Help > About ProDiver**.



11. Click **File > Exit**.

## Installing DivePort

DivePort is a client component that resides on a web application server, typically Apache Tomcat. DivePort uses portlet web technology (both page and portlet instances) to create and customize presentations and dashboards using data compiled from multiple sources, including ProDiver markers and Spectre Dive files. You access DivePort using an Internet web browser.

**NOTE:** You need to be an administrative user to install the software.

To install DivePort:

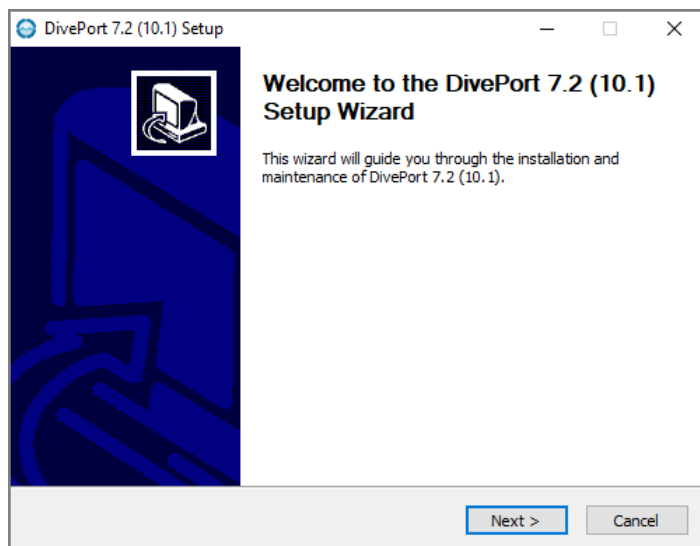
1. Navigate to the `DI\Solution\downloads` directory.
2. Double-click the **DivePort-Setup.exe** file.

The **User Account Control** dialog box opens, asking you to confirm making changes to your device.

**NOTE:** Depending on your Windows version and user account settings, you might see the **Open File - Security Warning** dialog box instead. Confirm that you want to open and run the executable.

3. Click **Yes**.

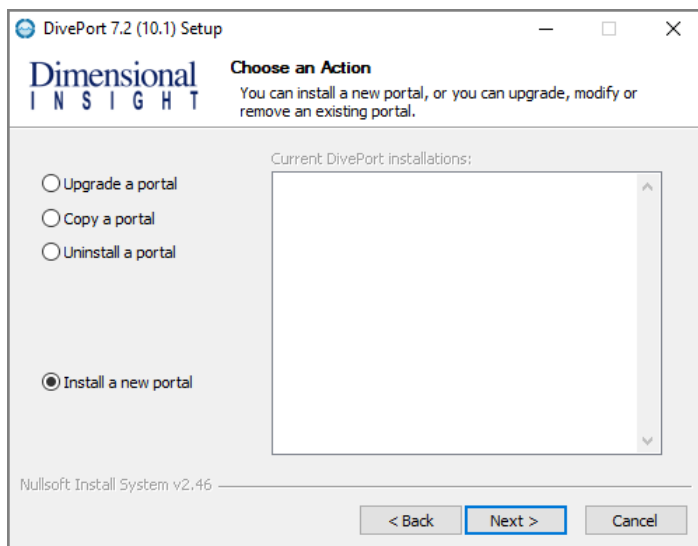
The **DivePort <version number> Setup Wizard** dialog box takes a moment to open.



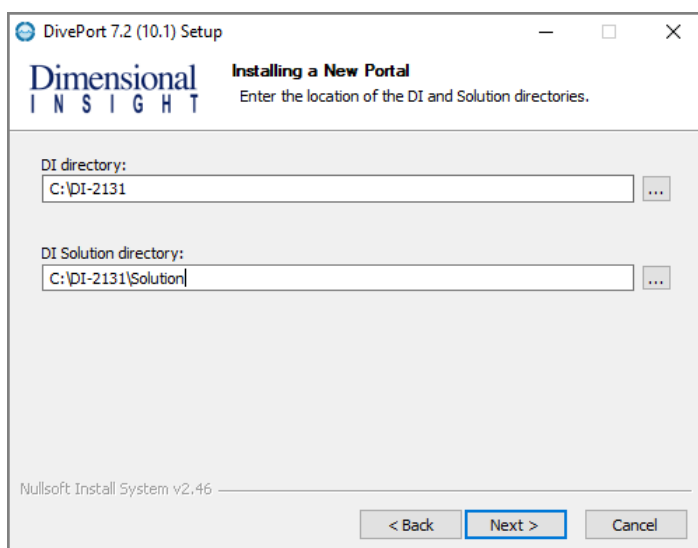
4. Click **Next** to continue.

The **Choose an Action** page opens.

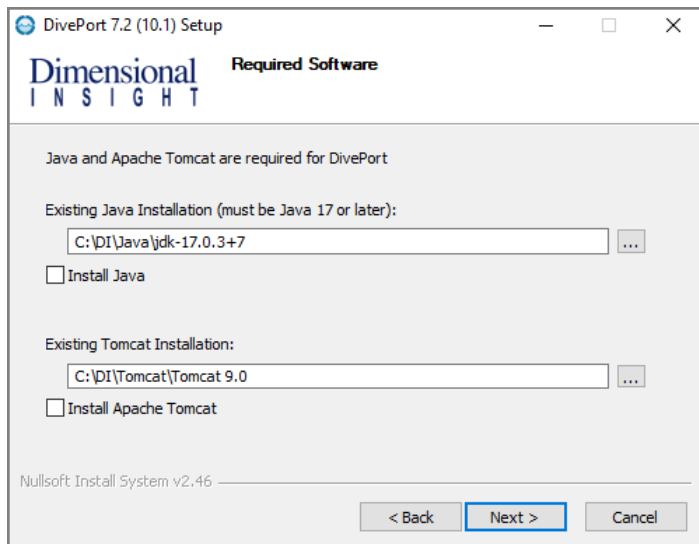
## Diver Platform 7.2



5. Click **Install a New Portal**, then click **Next** to continue.  
The **Installing a New Portal** page opens.



6. Verify the default locations for the `DI` and `DI Solution` directories.
7. Click **Next** to continue.  
The **Required Software** page opens.



This dialog prompts you to install Java (version 17 or later) and Tomcat.

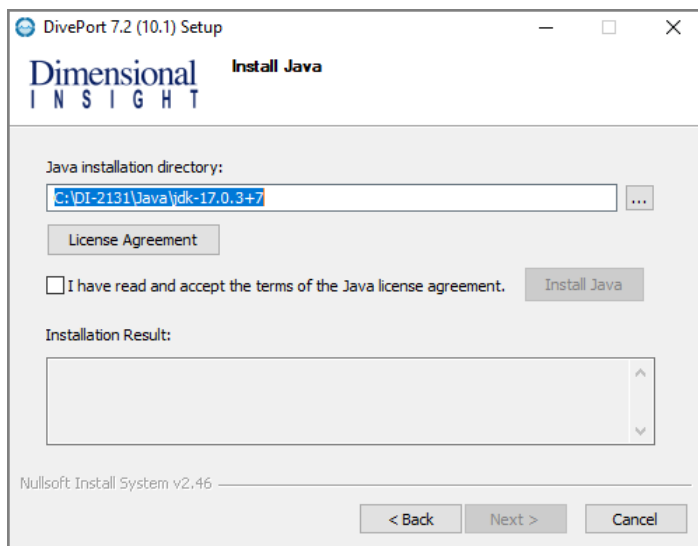
8. Select the check boxes for the software you must install or update.

**TIP:** If a path appears in the **Existing Installation** box, the software is already installed.

- If you installed Java, verify the existing path, and skip to [Step 10](#).
- If you installed Java and Tomcat, verify the existing paths, and skip to [Step 12](#).
- If Tomcat already has HTTPS installed, skip to [Step 18](#).

9. Click **Next**.

The **Install Java** page opens.



10. Perform the following actions:

- Accept or change the Java installation directory.
- Click **License Agreement** to open the terms of the license.
- Select the license agreement check box to accept the license terms.
- Click **Install Java**, and click **OK** in the pop-up window to confirm the installation. This might take several minutes.

After the installation finishes, the wizard displays the message **Successfully installed Java** in the **Installation Result** box.

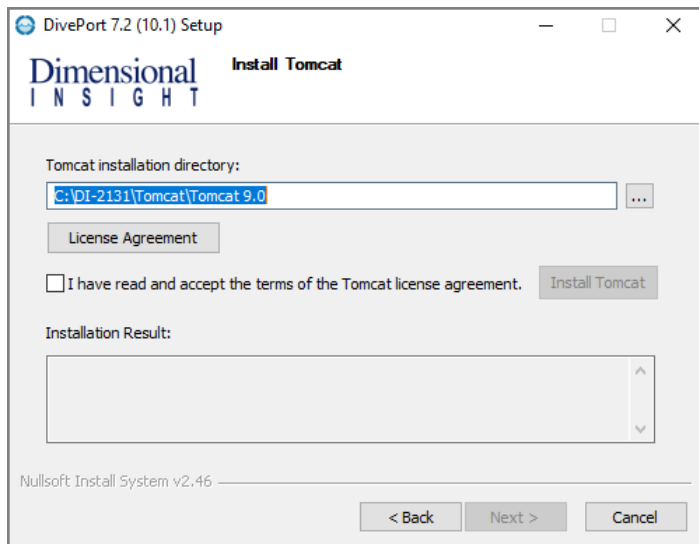
11. Click **Next**.

The **Install Tomcat** page opens. If you already installed Tomcat, skip to [Step 12](#). If Tomcat already has HTTPS installed, skip to [Step 18](#).

If you have Tomcat 7 installed, you are prompted to automatically switch use from Tomcat 7 to Tomcat 9. This switches your existing and future DI web applications to Tomcat 9 and leaves Tomcat 7 files available for viewing. If you decided to not switch automatically, Tomcat 9 is still installed and you must manually resolve any conflicts between Tomcat 7 and Tomcat 9.

**CAUTION:** Tomcat 9 does not work with version 6.4 installers.





12. Perform the following actions:

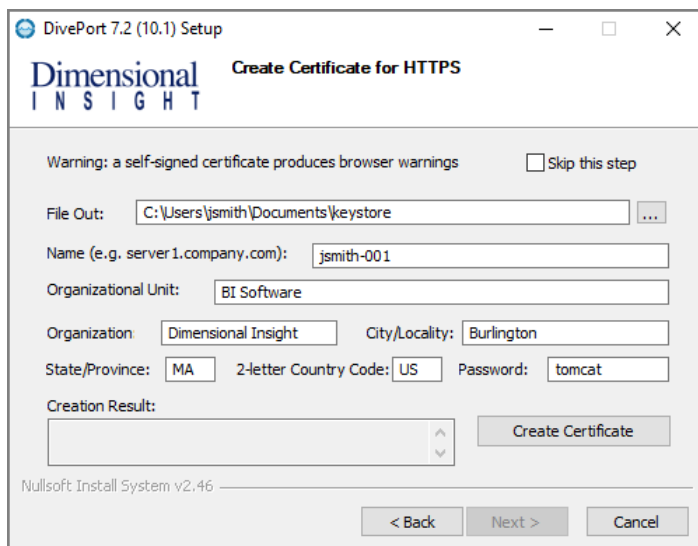
- Accept or change the Tomcat installation directory
- Click **License Agreement** to open the terms of the license
- Select the license agreement check box to accept the license terms
- Click **Install Tomcat**

After the installation finishes, the wizard displays the message **Successfully installed Tomcat** in the **Installation Result** box.

13. Click **Next**.

The **Create Certificate for HTTPS** page opens.

Because DivePort resides outside of the company firewall, it requires an HTTPS certificate to communicate with the Tomcat protocol which resides inside the firewall.



This step enables you to create a self-signed certificate. You can create a self-signed certificate to get your DivePort working as soon as possible. You can later create a Certificate Service Request that you can forward to a certification authority, such as GoDaddy. You can then work with this vendor to install a fully validated HTTPS certificate. The vendor (certificate authority) from whom you purchase the certificate should provide you with or point you to directions for installing the certificate.

**NOTE:** If you want to skip this step and subsequently create a Certificate Service Request (CSR) document using the wizard, select **Skip this step** and proceed to [Step 14](#).

To complete the self-signed certificate, enter the following information:

- **File Out**—The path to the directory where you want to store the certificate. The default path is  
`C:\Users\\Documents\keystore.`
- **Name**—The server name that the DivePort connects to. If you are performing a local installation, enter the name of that machine. Otherwise, this value is typically the domain name of your site. For example, a local installation is **jsmith-001**, while a domain name is **<server>.<company>.com**.
- **Organizational Unit**—A name that describes your type of business. For example, **BI Software**.
- **Organization**—The name of your company. For example, **Dimensional Insight**.

- **City/Locality, State/Province, and 2-Letter Country Code**—The location where your company is licensed to do business with local or state government.
  - **Password**—The certificate password, which defaults to **tomcat**. Be sure to remember the password, if you create a CSR.
14. Click **Create Certificate** to generate the certificate and display the message **Successfully created Certificate** in the **Creation Result** box.
- NOTE:** A self-signed certificate generates browser warnings requiring you to verify the authenticity of the certificate.

15. Click **Next**.

The **Certificate Signing Request for HTTPS** page opens.

The wizard populates the dialog box with information needed by a Certificate Authority to authorize the signed certificate (for example, keystore location and *tomcat\_cert\_request.csr* location).

The screenshot shows a window titled "DivePort 7.2 (10.1) Setup" with the "Dimensional INSIGHT" logo. The main heading is "Certificate Signing Request for HTTPS". Below the heading, there is a checkbox labeled "Skip this step" which is currently unchecked. The text reads: "Submit this Certificate Signing Request (.csr) file to a Certificate Authority to obtain a signed certificate".

There are three input fields:

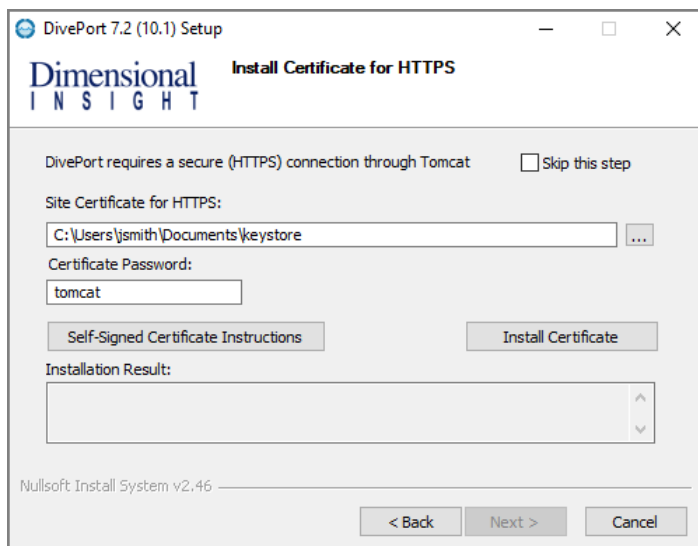
- Key File:** C:\Users\jsmith\Documents\keystore
- File Out:** C:\Users\jsmith\Documents\tomcat\_cert\_request.csr
- Password:** tomcat

Each of the first two fields has a browse button (three dots) to its right. Below these fields is a "Create Request" button. Underneath is a "Request Result:" label followed by an empty text area with a vertical scrollbar. At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel". The footer text reads "Nullsoft Install System v2.46".

If you generated a self-signed certificate in the previous step, you can select **Skip this step** to continue with the installation of the self-signed certificate. Proceed to [Step 16](#).

16. Optionally, click **Create Request** to create a certificate request. Upon completion, the wizard displays the message **Successfully created Request** in the **Request Result** box.
17. Click **Next**.

The **Install Certificate for HTTPS** page opens.



18. Click **Install Certificate** to install the self-signed certificate created in [Step 12](#).

Upon completion, the wizard displays the **Successfully installed certificate** message in the **Installation Result** box.

The following events happen when you install the self-signed certificate:

- The wizard copies the certificate keystore from  
 C:\Users\
 C:\DI\Tomcat\Tomcat 9.0\conf (when installed).
- The wizard updates the *server.xml* file located in the **conf** directory with the following line of XML code:

```
<Connector port="443"
protocol="org.apache.coyote.http11.Http11Protocol"
SSLEnabled="true" maxThreads="150" scheme="https"
secure="true" clientAuth="false" sslProtocol="TLS"
keystoreFile="C:\DI\Tomcat\Tomcat 9.0\conf\keystore"
keystorePass="tomcat" />
```

The HTTPS-enabled self-signed certificate enables your DivePort to communicate with the server over the **Transport Layer Security (TLS)** communication.

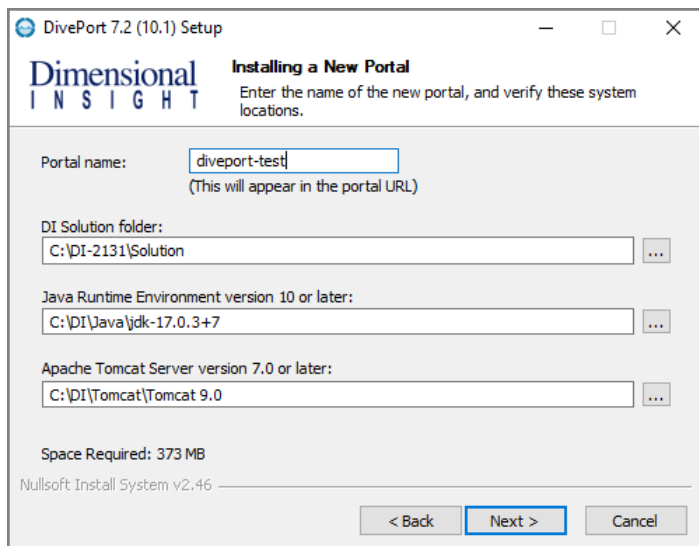
**TLS** is a security protocol for establishing an encrypted link between a server and a client, typically a Web Server and a browser, or a mail client and another mail client.

19. Click **Next**.

The **Installing a New Portal** page opens, with the following field defaults:

- **Portal name**—The default name is **diveport**. You can change it to suit your needs.
- **Path to DI Solution folder**—The default folder is `C:\DI\Solution`.
- **Path to Java**—The default path is `C:\DI\Java\jdk-11.0.1`.
- **Path to Tomcat**—The default path is `C:\DI\Tomcat\Tomcat 9.0`.

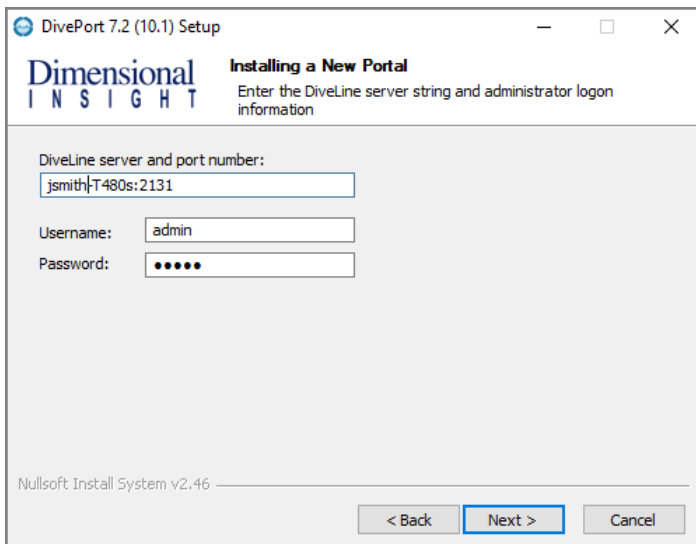
A best practice is to change the default Portal name to something other than **diveport** (for example, **diveport-test**) to keep the software distinct from the project or application implementation. One installation of the software can support multiple instances or portals. Verify the other default fields.



## 20. Click **Next**.

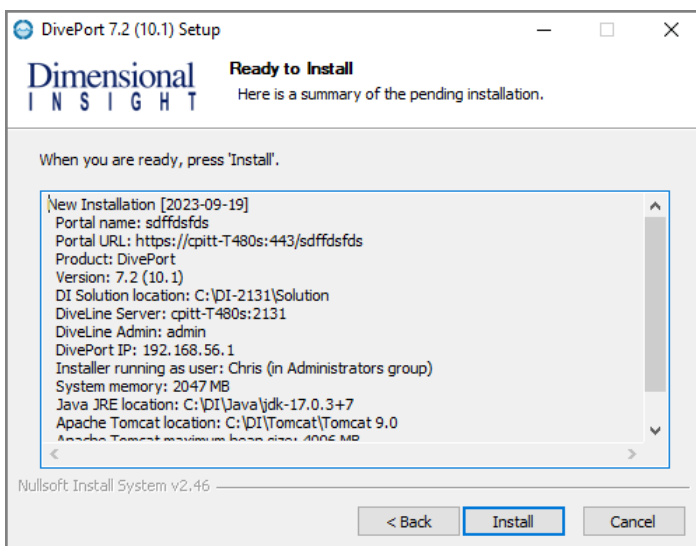
The second **Installing a New Portal** page opens, with the default name of the DiveLine service and port number (for example, **jsmith-001:2131**). Verify that the port number matches the DiveLine service. This dialog also prompts you to enter the administrator Username and Password previously defined for the DiveLine administrator.

## Diver Platform 7.2



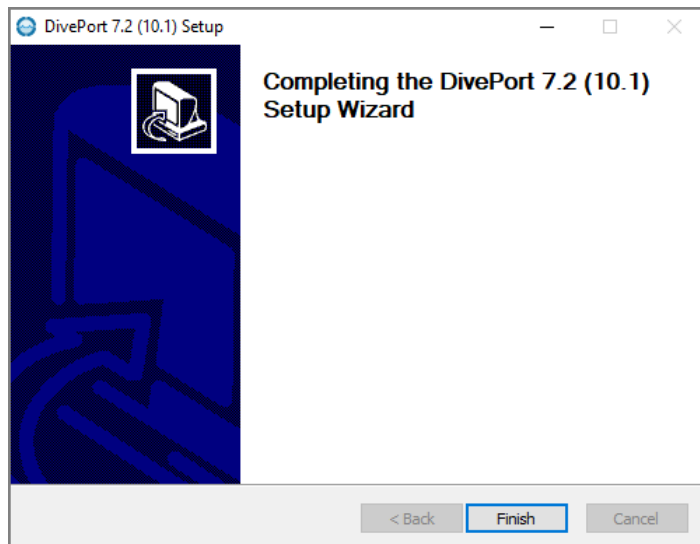
21. Click **Next**.

The **Ready to Install** page opens, with a summary of the DivePort installation information.



**NOTE:** Take note of the **Portal URL**. This is used to access DivePort from a web browser.

22. Click **Install**.
23. When you see the **Completing the DivePort <version number> Setup Wizard** dialog box, click **Finish**.



24. Restart your machine.

## URI Encoding

The default URI encoding for Tomcat is ISO-8859-1. For earlier versions of DivePort, the *server.xml* file installation instructions included setting the `URIEncoding` variable to UTF-8. This setting is not performed by the Windows installer for version 7.2.

ISO-8859-1 and UTF-8 overlap for the ASCII character set. When DivePort software generates URLs, non-ASCII characters are encoded so that the URL only contains ASCII characters. For these generated strings, either ISO-8859-1 or UTF-8 encoding is acceptable.

It is possible that a user might want to enter a URL directly, which could contain non-ASCII characters. If those characters are high-bit ISO-8859-1 characters, either the default or a `URIEncoding="UTF-8"` is not accurate. If a user intends to enter URLs that contain non-ASCII characters, they should set the `URIEncoding` on their Tomcat connector according to the encoding they intend to use. This is done by stopping Tomcat, editing the *server.xml* file, and restarting the service. See [Step 17](#) about the connector section in [Installing DivePort on page 38](#).

## Configuring Apache Tomcat

After installing Tomcat as part of the DivePort install wizard, you need to verify the size of the **Maximum memory pool** and select the **Use default** box under the **Java** tab of the **Tomcat<version #> Properties** dialog box.

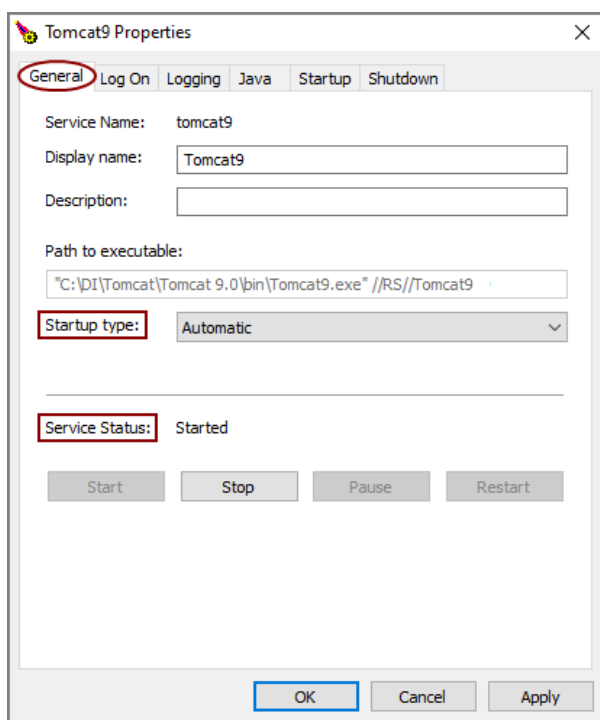
The maximum memory pool is the memory that can be allocated to the JVM. It is also known as the "Tomcat Heap".

The initial Tomcat Heap for a standard DI installation should be 4GB (4096MB). If a customer needs to exceed 10GB, they should contact DI Technical Support to help them diagnose their environment and suggest possible tuning options.

Complete the following steps:

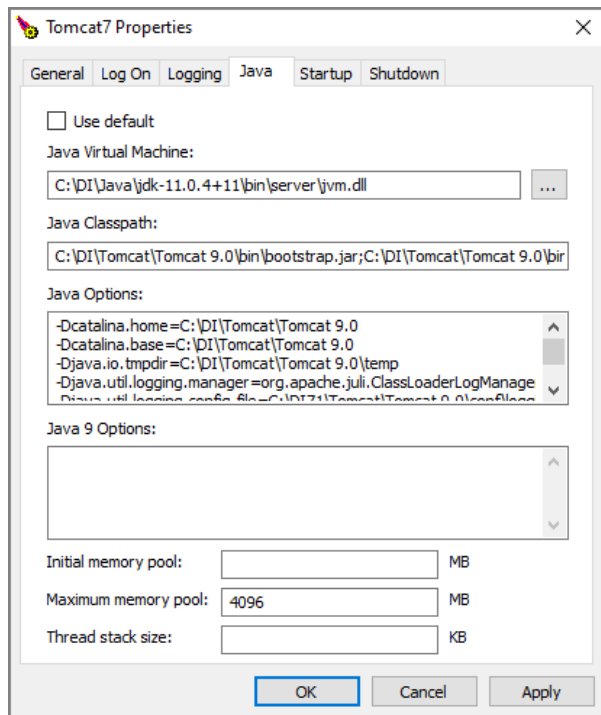
1. Open **Windows Explorer** and navigate to the Tomcat `bin` directory at `C:\DI\Tomcat\Tomcat 9.0\bin`.
2. In the `bin` directory, double-click the **tomcat9w.exe** file.

The **Tomcat9 Properties** dialog box opens.



3. On the **General** tab, verify that the **Startup type** is set to **Automatic** and that the **Service Status** is **Started**.
4. On the **Java** tab, verify that the **Maximum memory pool** is set to **4096 MB**.



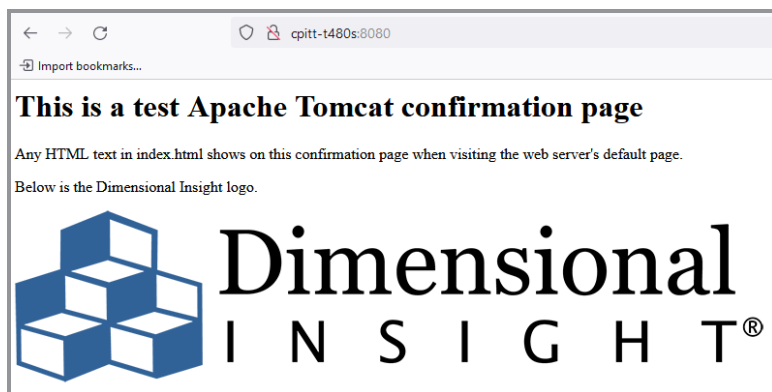


5. To implement any changes, click **Stop** then **Start** in the **Service Status** section on the **General** tab.
6. Click **Apply**.
7. To verify that the Tomcat service is working on your machine, open a browser and type **http://<DiveLine server>:8080** in the **URL** box. 8080 is the default port number for the Tomcat webserver.

For example, `http://jsmith-001:8080`.

A blank **Apache Tomcat** confirmation page appears in your browser window.

To edit the contents of the confirmation page, open **Windows Explorer** and navigate to the Tomcat **ROOT** directory at `C:\DI\Tomcat\Tomcat 9.0\webapps`. Edit the `index.html` file to control what is displayed on the confirmation page.



## Verifying the DivePort Installation

To verify a successful implementation of DivePort, complete the following steps:

1. Open a browser and enter the URL for the DivePort portal, using a format similar to the following:

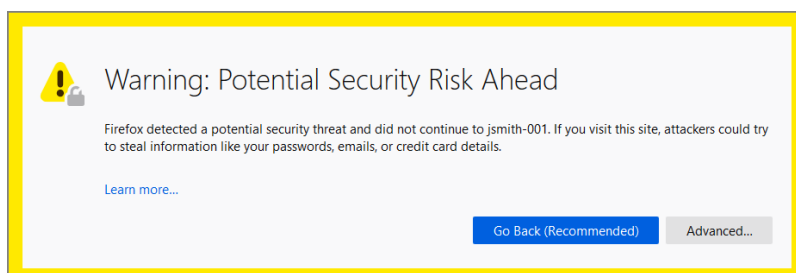
```
https://<servername>/<portal name>
```

For example, **https://jsmith-001/diveport-test**, where **jsmith-001** is the server name, and **diveport-test** is the name of the DivePort portal. The URL must use a secure version of an HTTP, or HTTPS. This URL can also be found in [Step 20](#) of [Installing DivePort](#).

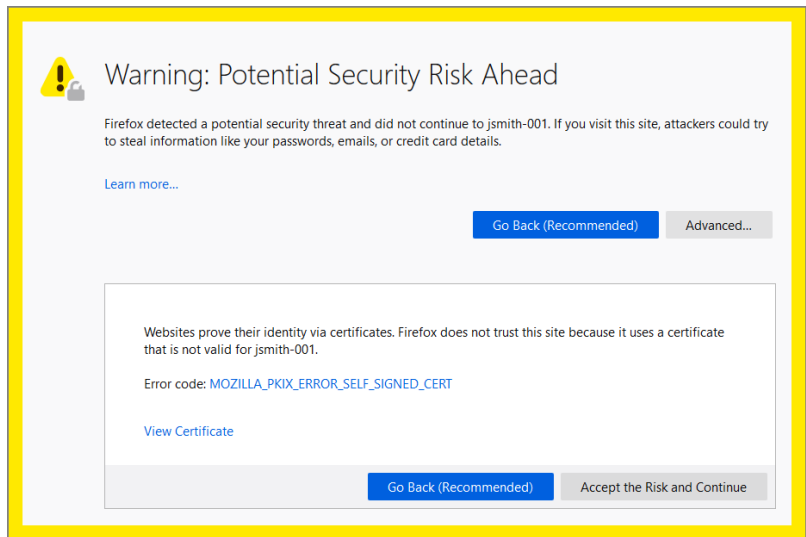
Proceed to [Step 5](#) if you installed a signed HTTPS certificate during the initial install.

**NOTE:** DivePort resides outside of the company firewall and requires an HTTPS certificate to communicate with the Tomcat protocol.

2. The first time you log on to DivePort after an installation using a self-signed certificate, you see the **Your connection is not secure** warning page.



3. Click **Advanced** to view the error message: The certificate is not trusted because it is self-signed.

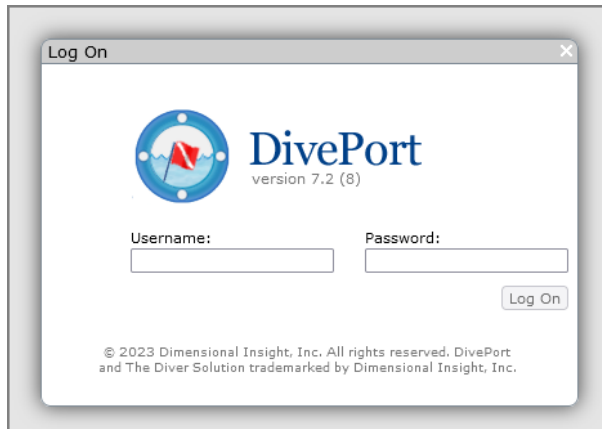


4. If you created a self-signed certificate using the DivePort installation wizard, click **Accept the Risk and Continue**.

The exception is added to the browser automatically.

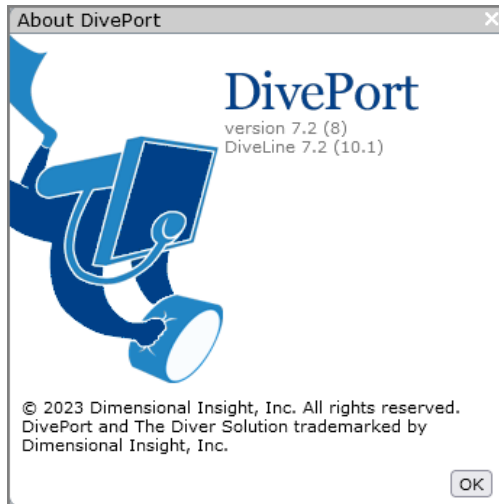
**NOTE:** You need to verify that your DivePort connection is secure when using a self-signed certificate on each machine that uses the DivePort client. In other words, include this information in your end-user training.

5. If you see the **Welcome to DivePort** page with a log on prompt, you have successfully installed DivePort.

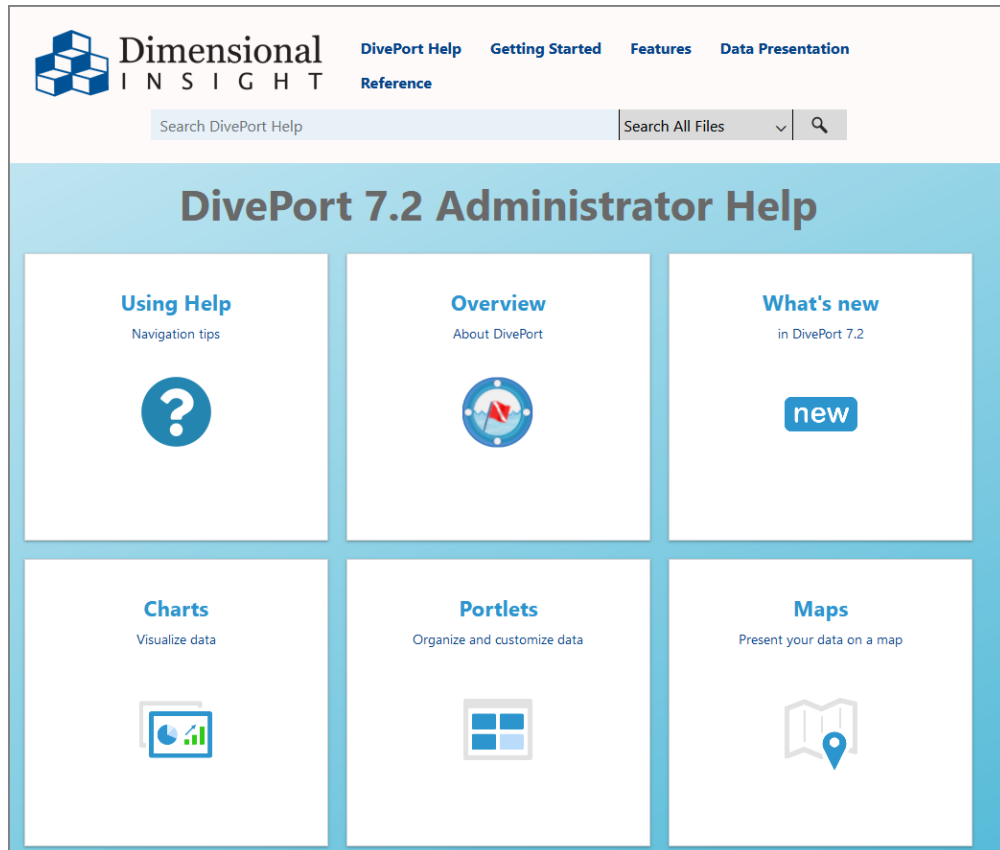


## Diver Platform 7.2

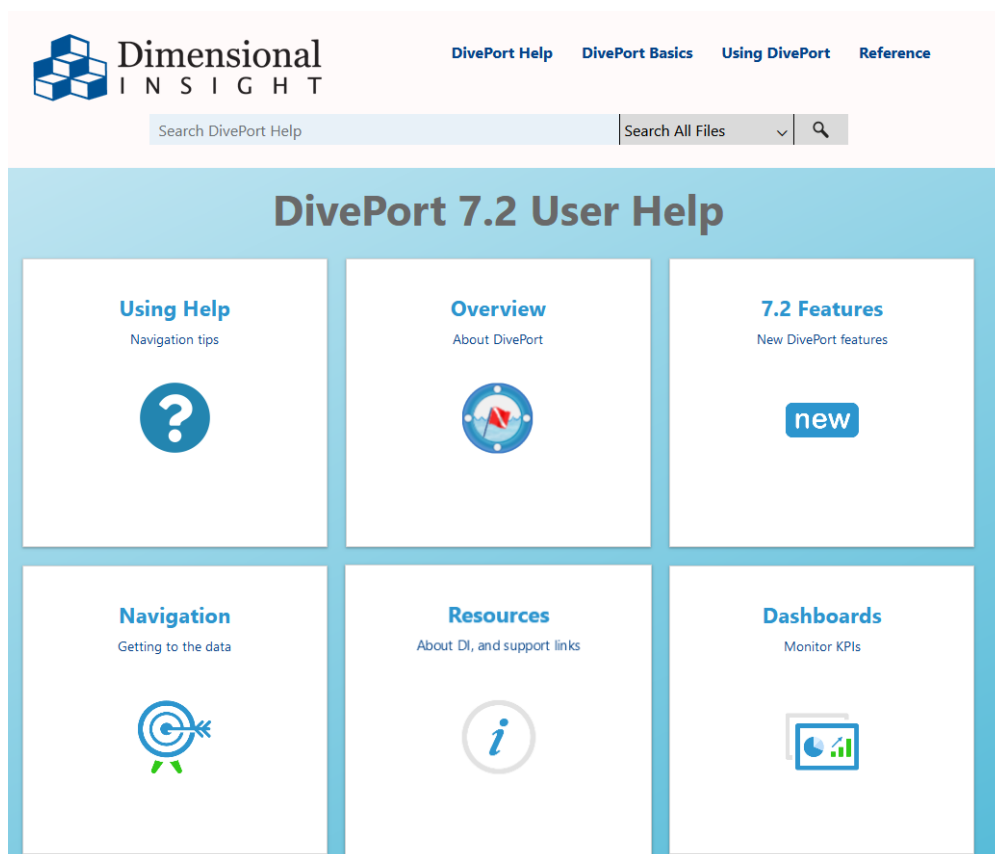
6. To log on to DivePort, enter the administrator Username and Password from the DiveLine installation, and then click **Log On**.
7. In the menu bar, click **About** to open the **About DivePort** information page with the version numbers for DivePort and DiveLine.



8. In the menu bar, click **HELP** and then **View Administrator Help** or **View User Help** to view the *DivePort Help* for the Administrator or User.  
Here is the Welcome page for the *DivePort Administrator Help*.



Here is the Welcome page for the *DivePort User Help*.



*DivePort Help opens in your default browser.*

## Installing NetDiver

NetDiver is a web-based application that resides on a web application server, such as Apache Tomcat. NetDiver enables authorized users to access and analyze their data on the web.

**NOTE:** You need to be an administrative user to install the software.

To install NetDiver, complete the following steps:

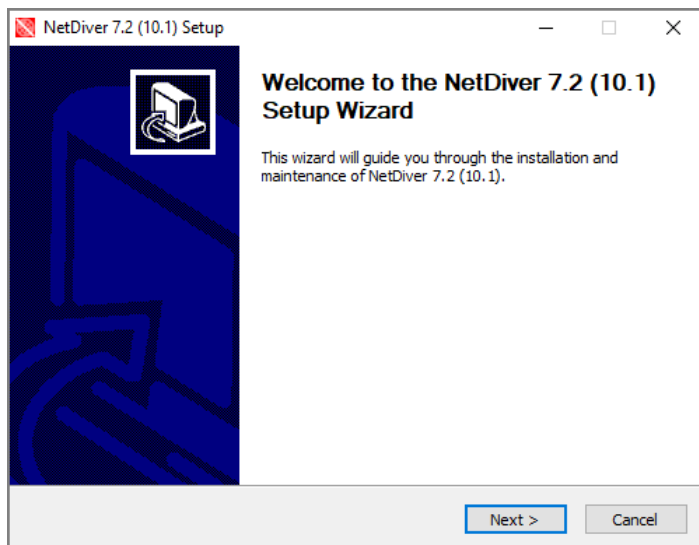
1. Navigate to the `DI\Solution\downloads` directory.
2. Double-click the **NetDiver-Setup.exe** file.

The **User Account Control** dialog box opens, asking you to confirm making changes to your device.

**NOTE::** Depending on your Windows version and user account settings, you might see the **Open File - Security Warning** dialog box instead. Confirm that you want to open and run the executable.

3. Click **Yes**.

The **NetDiver <version number> Setup Wizard** dialog box opens.



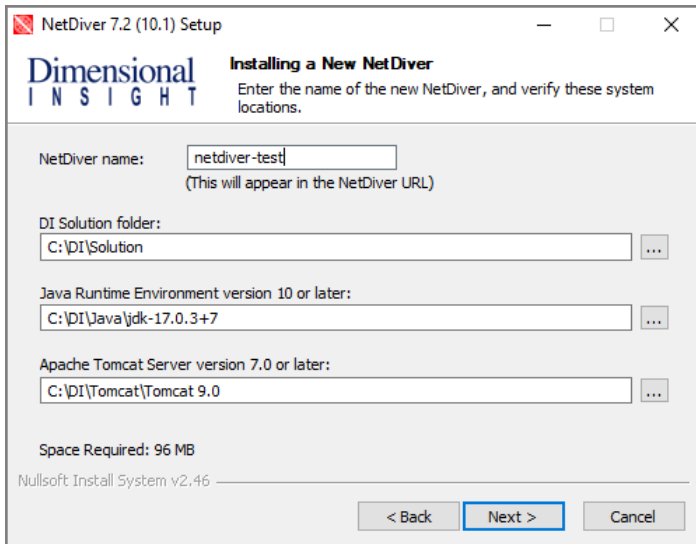
4. Click **Next**.

The **Installing a New NetDiver** page opens, with default names and locations for the following:

- NetDiver portal name, as you want it to appear in the NetDiver URL. The default is **netdiver**. Change it to suit your needs. For example, **netdiver-test**.
- DI Solution directory
- Java Runtime Environment, version 17 or later, directory
- Apache Tomcat Server, version 9 or later, directory

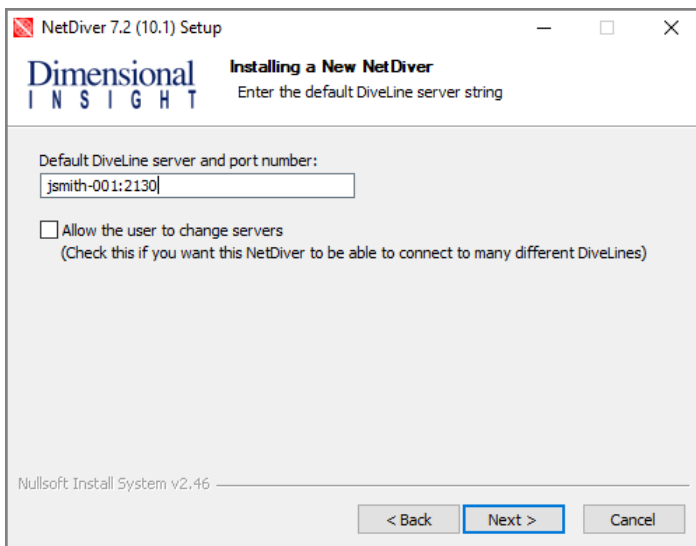
Verify the default locations and make changes if necessary.

## Diver Platform 7.2



### 5. Click **Next**.

The **Installing a New NetDiver** page displays. The name and port number defaults to the DiveLine server.

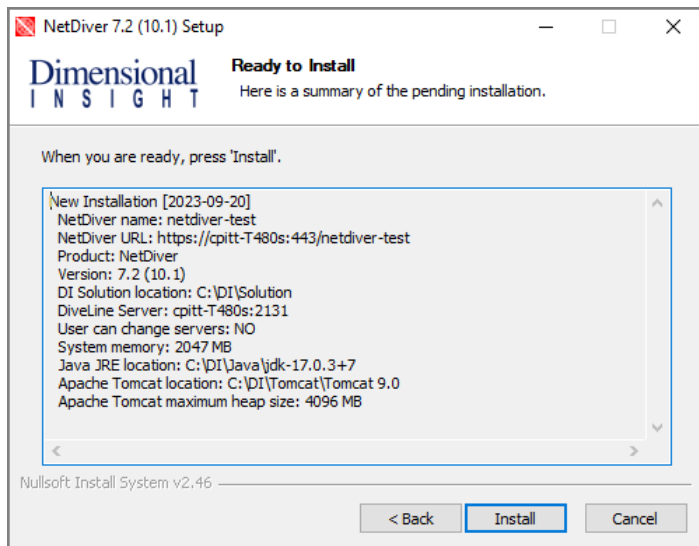


If you want NetDiver to connect to different DiveLines, select **Allow the user to change servers**.

### 6. Click **Next**.

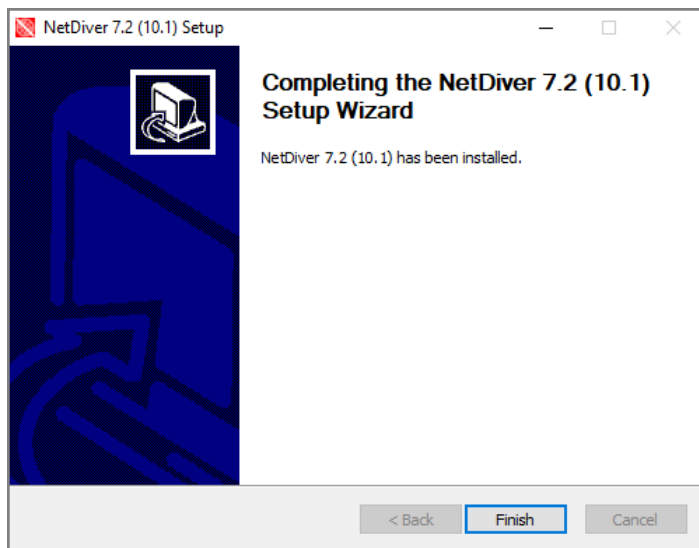
The **Ready to Install** page displays, with a summary of the NetDiver installation information.





**NOTE:** Take note of the **NetDiver URL**. This is used to access NetDiver from a web browser.

7. Click **Install**.
8. When you see the **Completing the NetDiver <version number> Setup Wizard** dialog box, click **Finish**.



**NOTE:** In the *netdiver.html* file (located in the `C:\DI\Solution\webapps\<netdiver>\dlcgi` directory), `$DL_EXTRAS` allows you pass URL parameters when using DL CGI authentication.

## NetDiver Customizations

If NetDiver is launched from DivePort, DivePort sends a **skin** parameter to NetDiver, which NetDiver uses if it is valid. If a parameter is not sent, NetDiver uses the context file parameter **netdiver.skin** if valid and present. If unavailable, NetDiver uses the skin called *default.txt*.

To change the NetDiver skin from the default:

1. Do one of the following:
  - Copy and rename an existing skin file (recommended).

NetDiver skin files are located in the

`C:\DI\Solution\webapps\<netdiver>\customization-templates\skins` directory.

- Create a new *txt* file.

**NOTE:** If launched from DivePort, use the same file name as the DivePort skin.

2. Use a text editor to specify the values of the properties for the skin.
3. Save your skin file to the  
`C:\DI\Solution\webdata\<netdiver>\customizations\skins` directory.

To change the NetDiver skin when not launching from DivePort:

1. Position the desired skin *txt* file in the  
`C:\DI\Solution\webdata\<netdiver>\customizations\skins` directory.
2. Navigate to `C:\DI\Tomcat\Tomcat 9.0\conf\Catalina\localhost` directory.
3. Open the *<netdiver>.xml* file in a text editor.
4. Add the new parameter:

```
<Parameter name="netdiver.skin" value="<netdiver skin>.txt" />
```

5. Save the *xml* file.

## Verifying the NetDiver Installation

To verify a successful implementation of NetDiver, complete the following steps:

1. Open a browser and enter the URL for the NetDiver portal, using a format similar to the following:

```
https://<servername>/<portal name>
```

For example, <https://jsmith-001/netdiver-test>.

This URL can also be found in [Step 6](#) of [Installing NetDiver on page 56](#).

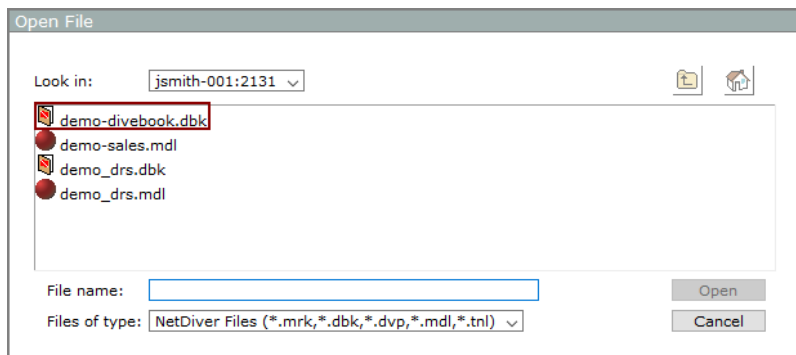
NetDiver resides outside of the company firewall and requires an HTTPS certificate to communicate with the Tomcat protocol.


**NOTE:** The first time you log in to NetDiver after an install using a self-signed certificate, you might see the **Your connection is not secure** warning page. If so, add an exception. If you see the NetDiver logon page, you have successfully installed NetDiver. You must verify that your NetDiver connection is secure when using a self-signed certificate on each machine that is used with the NetDiver client. That is, inform your new end users to verify their NetDiver connection.

- To log on to NetDiver, enter your **Username** and **Password**, and click **Log On**.



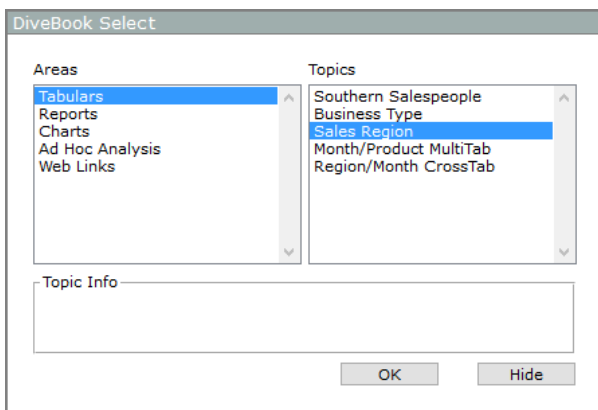
- The **Open File** dialog box appears with a list of NetDiver files.



If the dialog box does not open automatically, click the **Open File** icon, , on the top left. If no files are visible, verify that all file types are selected.

- Select a *dbk* file and click **Open**. For example, *demo-divebook.dbk*.

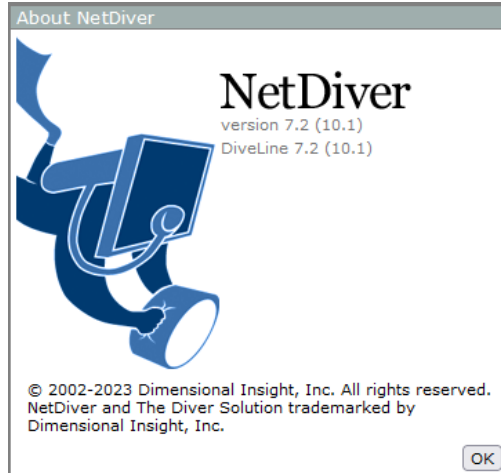
5. Select an **Area** and a **Topic** and click **OK** to open. For example, **Tabulars** and **Sales Region**.



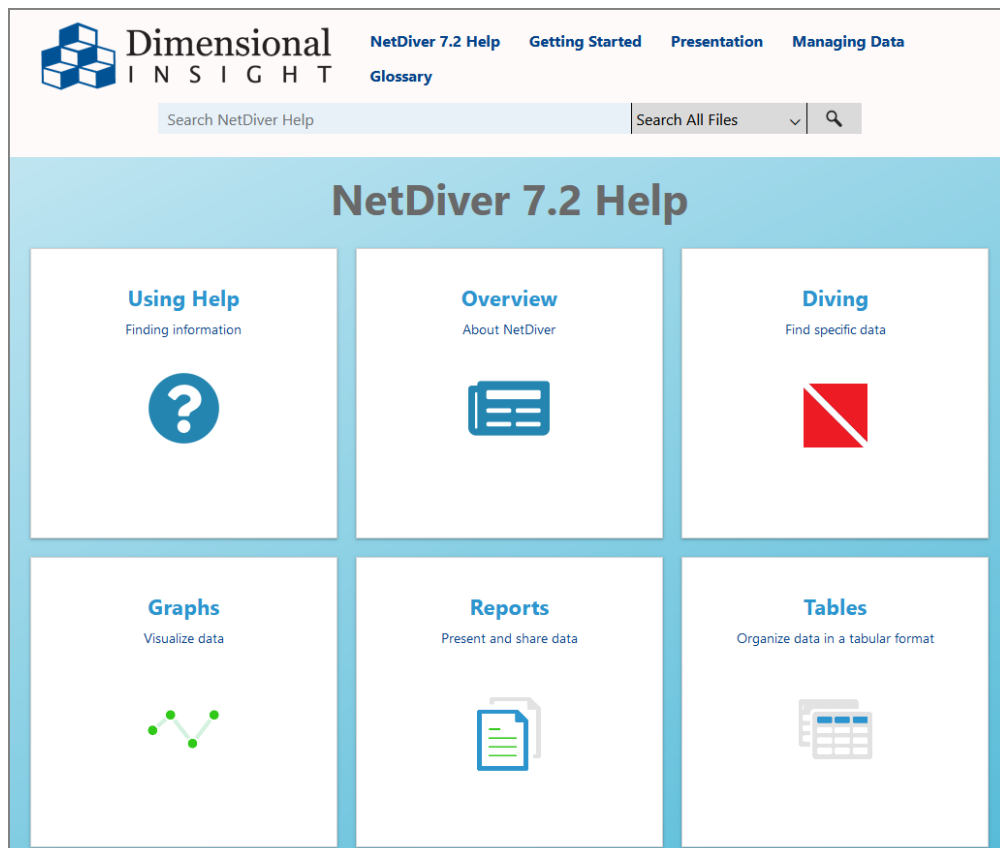
If you see a tabular similar to the following, NetDiver is functioning correctly.

Sales Region	Plan Units Total	Plan Dollars Total	Actual Units Total	Actual Dollars Total
Totals	2,092	8,630,600	2,526	9,624,200
Far West	247	1,031,100	336	1,320,700
Mid Atlantic	306	1,342,300	403	1,680,200
Mid West	222	850,200	260	779,600
Mountain West	257	1,061,300	304	1,175,200
Northeast	320	1,361,100	347	1,513,600
South	462	2,012,600	507	1,892,600
Southwest	278	972,000	369	1,262,300

6. In the menu bar, click **About** to open the **About NetDiver** information page with the version numbers for NetDiver and DiveLine.



7. In the menu bar, click **HELP** to open the help documentation in a new browser window.



## Setting the Executable Path Variables

After you have installed the Diver Platform Server components, you must add their directory paths to the **System Variables** > **PATH** on your machine.

For example:

- C:\DI\Solution\executables
- C:\DI\Solution\diveline\bin

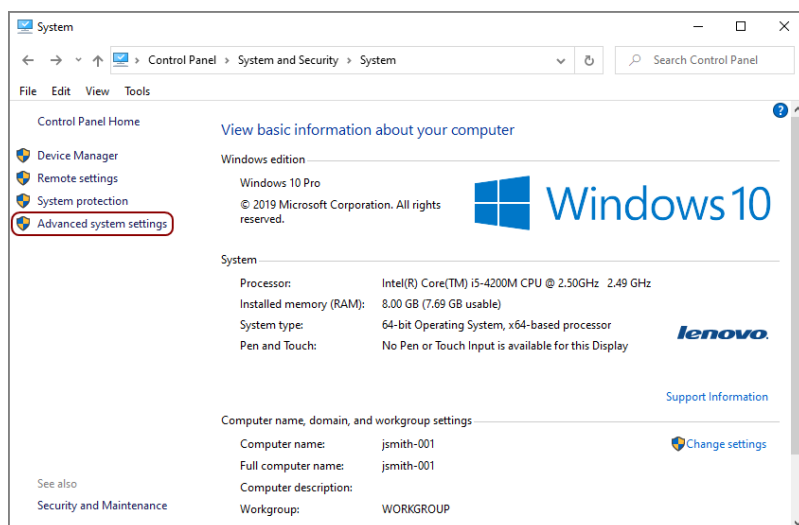
**NOTE:** This example is specific to Windows 10. If you are running a different version of Windows, the individual steps might differ.

To set the directory path variables for the executables, complete the following steps:

1. Navigate to `Control Panel\System and Security\System`.

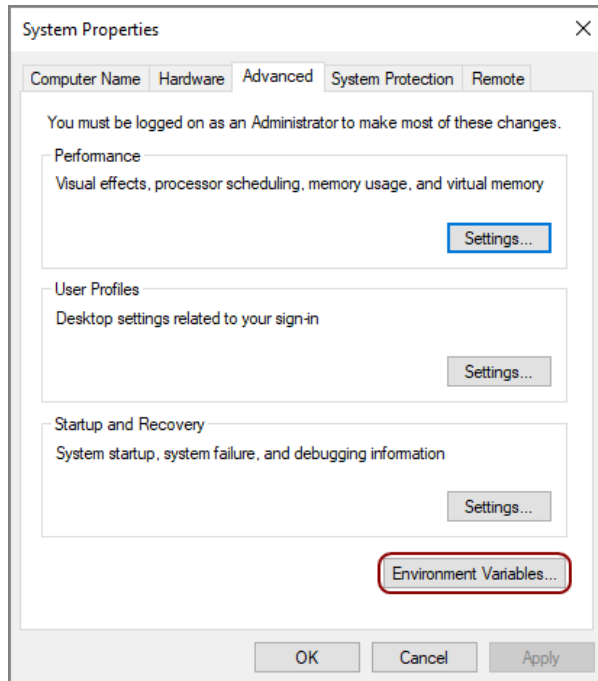
**NOTE:** There are multiple ways to navigate the Windows operating system. This method uses a path in the Windows Explorer.

The **System** window opens.

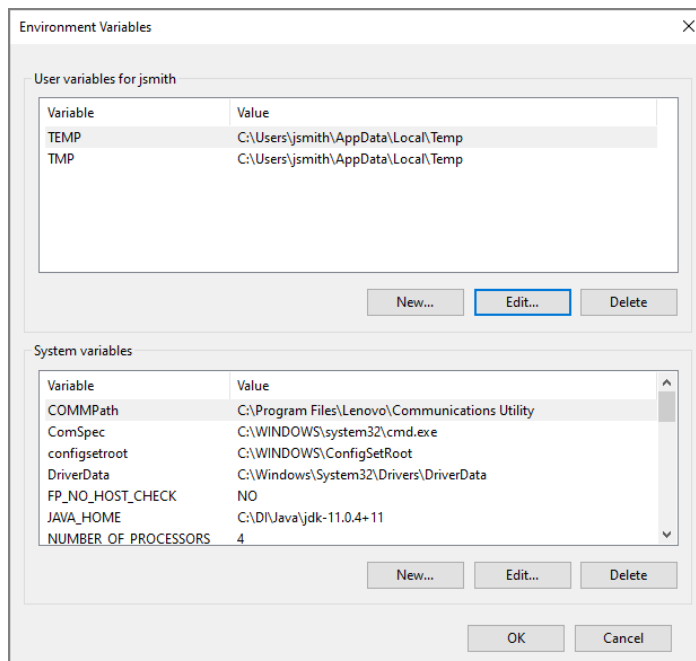


2. Click the **Advanced system settings** button.

The **System Properties** dialog box opens.

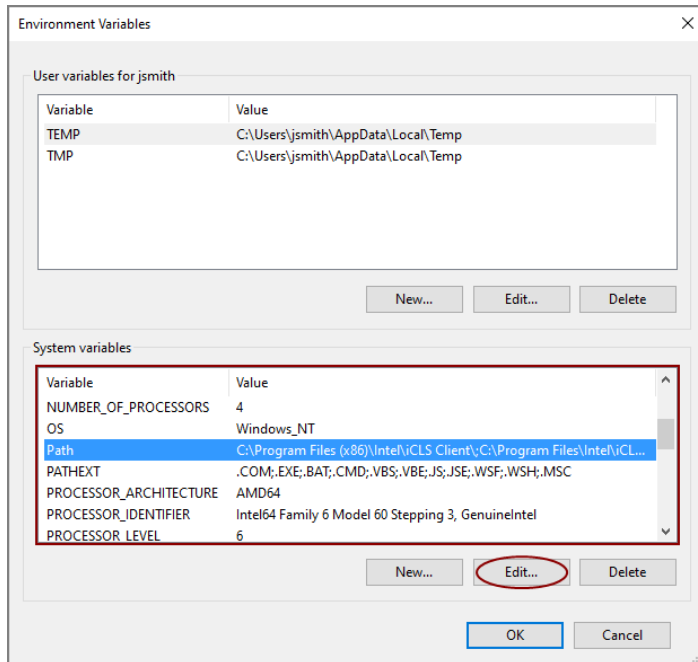


3. On the **Advanced** tab, click **Environment Variables**.  
The **Environment Variables** dialog box opens.

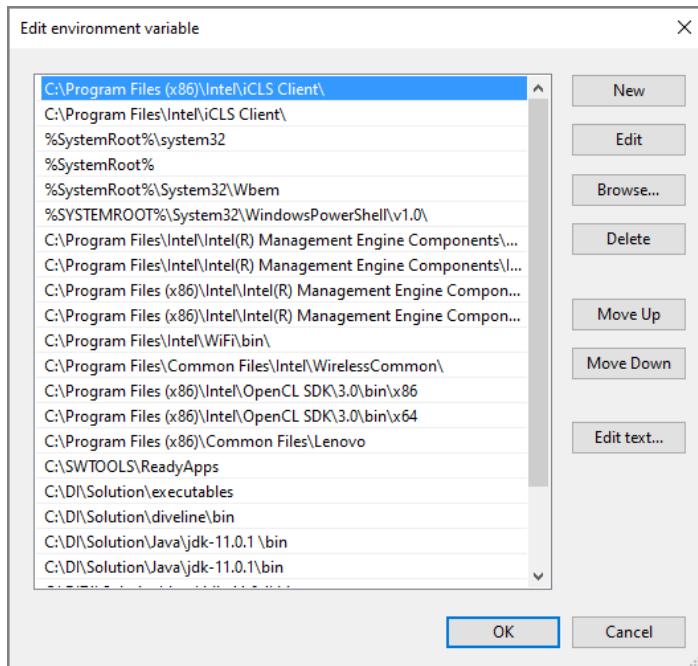


4. From the **System Variables** list, select **Path** and then click **Edit**.

## Diver Platform 7.2



The **Edit System Variable** dialog box opens.



5. Click **New**.
6. Enter the new value.
7. Repeat steps 5 and 6 for each value. These values are required:



C:\DI\Solution\executables

C:\DI\Solution\diveline\bin

**NOTE:** Depending on the Windows version, the values are in a list or string. If the values are in the string format, you must insert semi-colons as a separator.

8. Click **OK** to save changes.

The **Edit System Variable** dialog box closes.

9. Click **OK** to exit the remaining dialog boxes.

# Installing Diver Platform Developer

## Downloading and Extracting the Developer Installation Package

This topic describes how to download and extract the Diver Platform Developer 7.2 Windows software package. See [Downloading the Server Installation Package on page 14](#) for information on how to locate DI installation files.

**NOTE:** Install Diver Platform Developer on your local computer, not the server.

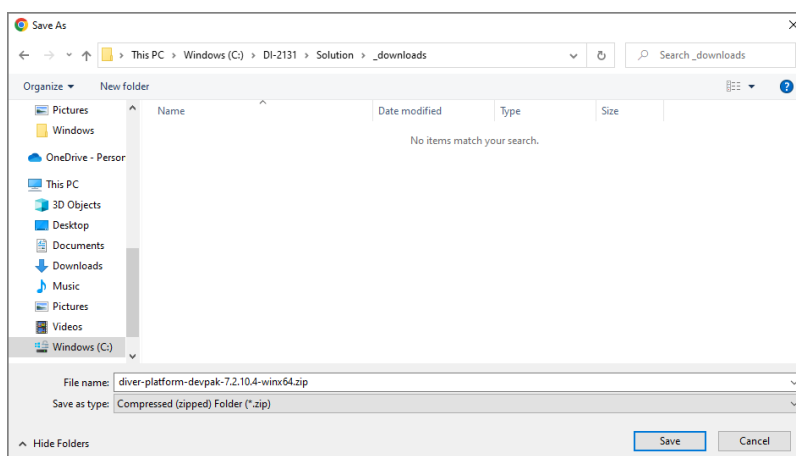
See [Building the DI Directory Structure on page 9](#) to prepare the client computers.

Complete the following steps:

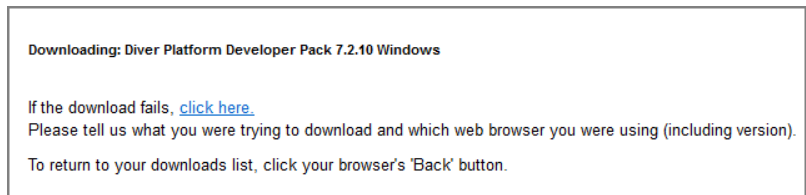
1. On the software and documents download page on DI-Download, locate the latest version of the Diver Platform Developer 7.2 Windows installation package, and click the version number.

Diver Platform Asian Language Pack 7.1 Windows Unicode	7.1.33 (323449KB)	<a href="#">Previous Point Releases</a>	Not Available	Not Available
Diver Platform Asian Language Pack 7.0 Windows Unicode	7.0.56 (132524KB)	<a href="#">Previous Point Releases</a>	Not Available	Not Available
Diver Platform Developer Pack 7.2 Windows Unicode limited	7.2.10 (432203KB)	<a href="#">Previous Point Releases</a>	Not Available	Not Available
Diver Platform Developer Pack 7.2 Windows	7.2.10 (432198KB)	<a href="#">Previous Point Releases</a>	Not Available	Not Available
Diver Platform Developer Pack 7.2 Windows limited	Update not available	None Available	Not Available	Not Available
Diver Platform Developer Pack 7.1 Windows Unicode limited	7.1.33 (418003KB)	<a href="#">Previous Point Releases</a>	<a href="#">Release Notes (1586KB)</a>	Not Available
Diver Platform Developer Pack 7.1 Windows	7.1.33 (417990KB)	<a href="#">Previous Point Releases</a>	<a href="#">Release Notes (1586KB)</a>	Not Available

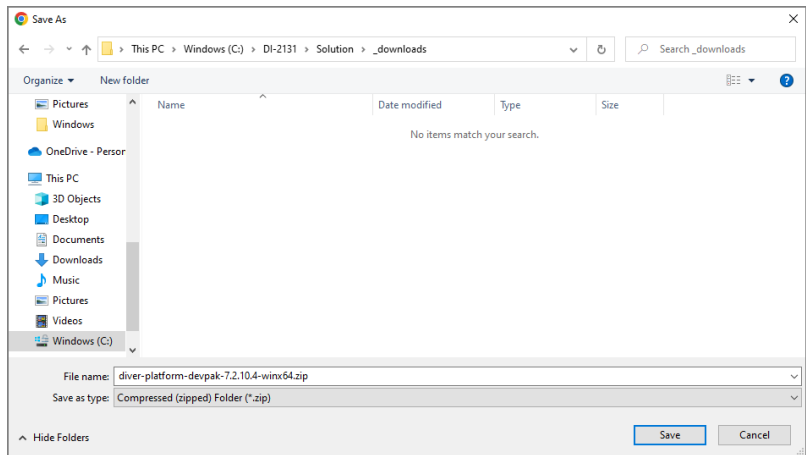
The **Opening** download verification dialog box opens.



The **Downloading** page opens in the browser. If the **Opening** dialog does not open automatically, follow the instructions on the page.



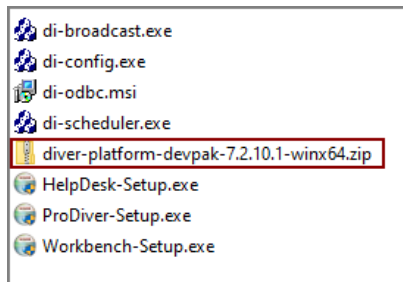
2. . Enter a file name and then click **Save**.



The Diver Platform Developer 7.2 software package is saved to the **Downloads** directory on your local computer.

3. Move the developer package to the `DI\Solution\downloads` directory.
4. Right-click the package and select **Extract All**, or use a third-party tool, to unzip the file.

The following executable files are extracted to the directory:



## Installing ProDiver

ProDiver is the desktop analytics client of the Diver Solution and Platform. With ProDiver, you can view and analyze model and cBase data with a graphical user interface. You can create markers in ProDiver and use those markers to build dashboards and presentations in DivePort.

**NOTE:** You need to be an administrative user to install the software.

The ProDiver installer places a copy of the Setup Wizard in the Program Files directory for uninstalling purposes.

To install ProDiver:

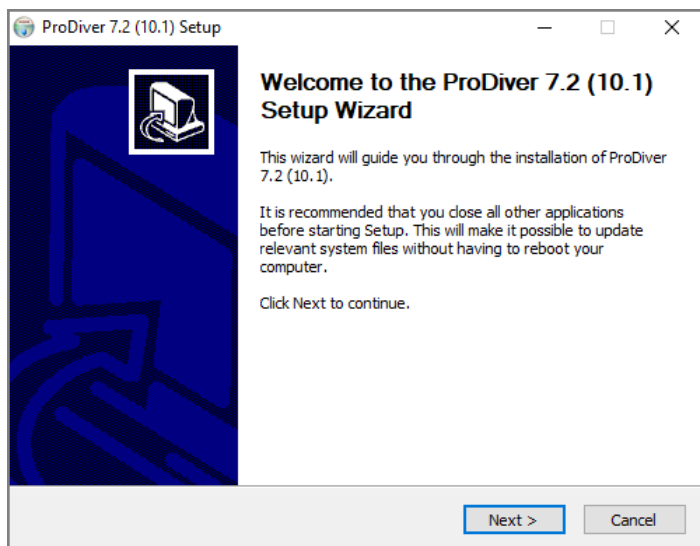
1. Navigate to the `DI\Solution\downloads` directory.
2. Double-click the **ProDiver-Setup.exe** file.

The **User Account Control** dialog box opens, asking you to confirm making changes to your device.

**NOTE:** Depending on your Windows version and user account settings, you might see the **Open File - Security Warning** dialog box instead. Confirm that you want to open and run the executable file.

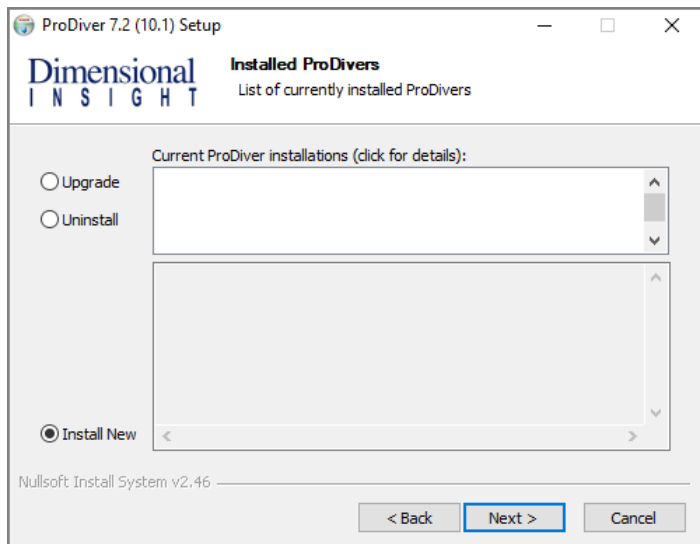
3. Click **Yes**.

The **ProDiver <version number> Setup Wizard** dialog box opens.

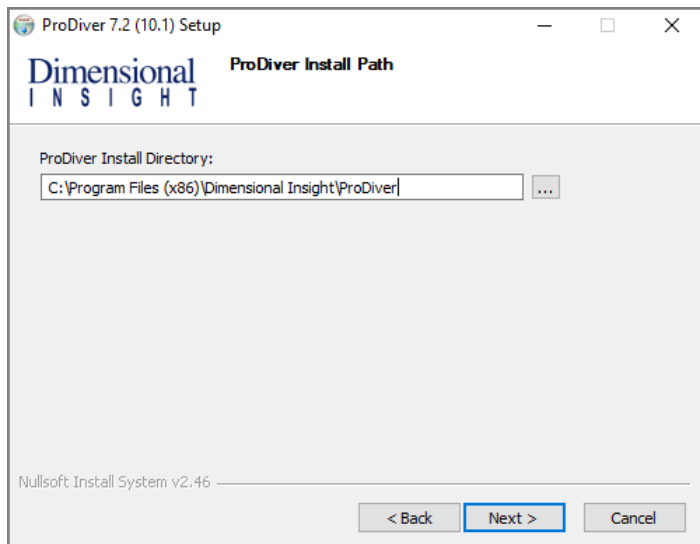


4. Review the setup instructions, and click **Next**.

The **Installed ProDivers** page displays.

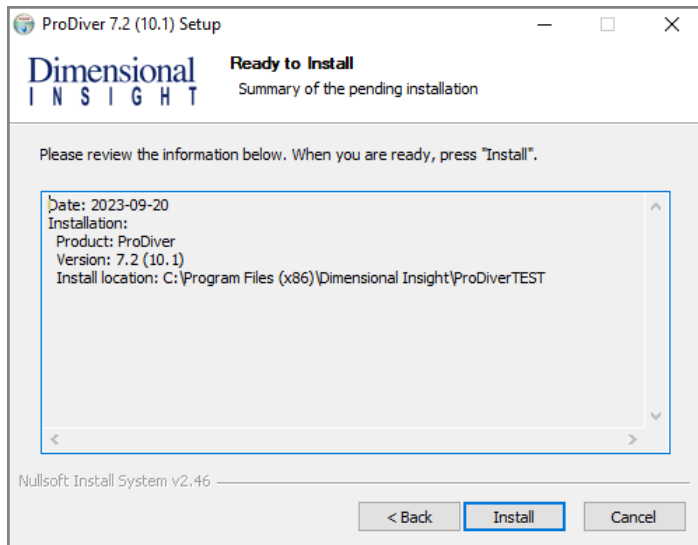


5. Select the **Install New** option.  
This page lists any existing ProDiver installations, which you can choose to **Upgrade** or **Uninstall**. If this is the first installation, **Install New** is selected by default.
6. Click **Next**.  
The **ProDiver Install Path** page displays the default installation path. For example, C:\Program Files (x86)\Dimensional Insight\ProDiver. Make changes if necessary.

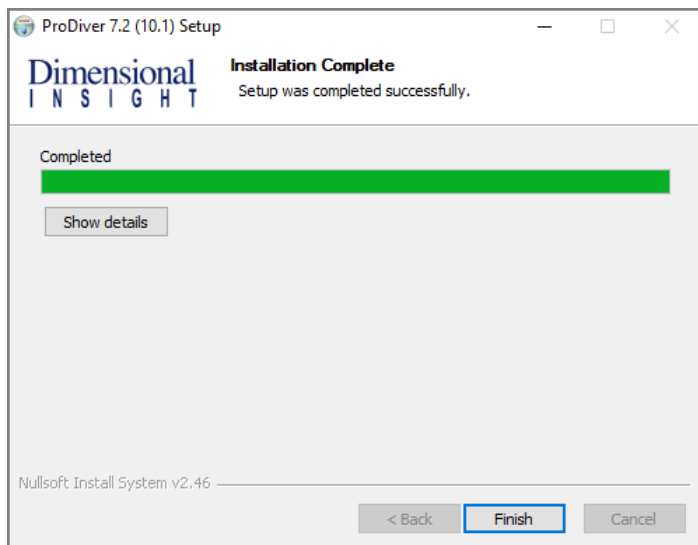


7. Click **Next**.

The **Ready to Install** page displays a summary of the pending installation.



8. Click **Install** to install the ProDiver software.  
When complete, the wizard displays the **Installation Complete** dialog box.



**NOTE:** To view a running summary of the installation process, click the **Show details** button.

9. Click **Finish** to close the installation wizard.

**NOTE:** When you run the ProDiver installer for a new installation or an upgrade, it associates *dlk* files with the ProDiver executable file for opening ProDiver from DivePort.

## ProDiver Installation Silent Option

The ProDiver installer has a "silent option" that administrators can use to run the installer remotely on multiple workstations without interaction from the user.

To run the installer in silent mode, use the `/S` option (with case sensitive, uppercase `/S`) in the command line of the end user's computer. For example:

```
ProDiver-Setup.exe /S
```

The following options can be used for more control.

Option	Description
<code>/mode=</code>	<p>Indicates the action for the installer. Values are:</p> <ul style="list-style-type: none"> <li>• <code>install</code></li> <li>• <code>upgrade</code></li> <li>• <code>uninstall</code></li> <li>• <code>list</code></li> </ul> <p>If there are no existing installations, the installer defaults to doing a new install. If there is one existing installation, the installer defaults to doing an upgrade. If there are multiple installations, there is no default mode—to perform an upgrade or uninstall, you must specify the installation. Use the <code>list</code> option to see existing installations.</p>
<code>/path=</code>	<p>Indicates the target location. The default value for the path is:</p> <pre>"C:\DI\Solution\executables\prodiver"</pre> <p>The installer writes a log file called <i>installation.log</i> to the user-specified or default path with information about the installation.</p>
<code>/installation=</code>	<p>On computers with multiple installations, indicates which installation to upgrade or uninstall. The format used is that of the GUI installer (for example "ProDiver-2019-02-26-17-41-29").</p>

**NOTE:** When output is sent to the console to display a list of errors encountered when running, you might be prompted to press **Enter** to continue. If the

message does not indicate that the installer has completed, the process might still be running in the background. If you need to perform other tasks, use a separate command window.

### Examples:

A new installation to the default path on a computer with no existing ProDiver:

```
ProDiver-Setup.exe /S
```

That installation can be upgraded using the same command line:

```
ProDiver-Setup.exe /S
```

A new installation to a non-standard path:

```
ProDiver-Setup.exe /S /path=c:\di\solution72\executables\prodiver72
```

If it is the only ProDiver on that computer, you can upgrade by using:

```
ProDiver-Setup.exe /S
```

If you want to be sure that you are doing a new installation or an upgrade, specify the mode explicitly:

```
ProDiver-Setup.exe /S /mode=install
```

```
ProDiver-Setup.exe /S /mode=upgrade
```

To see a list of installed versions:

```
ProDiver-Setup.exe /S /mode=list
```

An upgrade to a particular version:

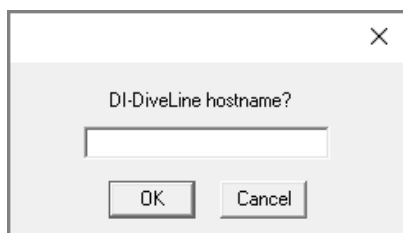
```
ProDiver-Setup.exe /S /mode=upgrade /installation=ProDiver-2019-0804-12-58-26
```

## Verifying the ProDiver Installation

To verify a successful implementation of ProDiver, complete the following steps:

1. Open the Windows **Start** menu and enter **ProDiver** in the Windows search box.
2. In the **Programs** list, click ProDiver.

The **DI-DiveLine hostname** dialog box opens.



**NOTE:** If you used ProDiver to check the DiveLine installation, this is not the initial use of ProDiver. The **DiveLine Login** dialog box opens directly.

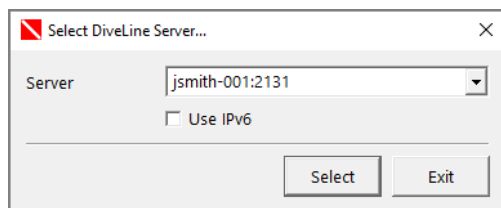


Skip to [Step 6](#). For more information about checking DiveLine, see [Testing the DiveLine Installation on page 36](#).

3. If you are using the default port number 2130, enter **<server>**. If you are using another port number, enter **<server>:<port number>**. For example, **jsmith-001:2131**.

If the connection fails, the **Select DiveLine Server** dialog box opens. If successful, skip to [Step 6](#).

4. Enter or select the name of the server and click **Select**.



**NOTE:** The default port number is 2130. If you are using another port, specify it in the **Server** box by using the format **<server name>:<port number>**.

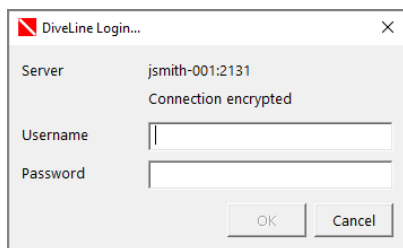
The **Verify Certificate** window opens.



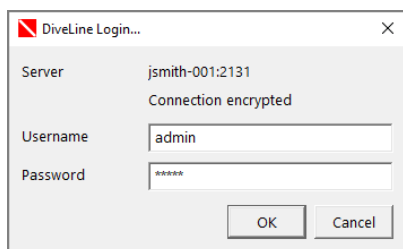
5. Review the certificate, and click **Accept**.

The **DiveLine Login** dialog box opens.


## Diver Platform 7.2



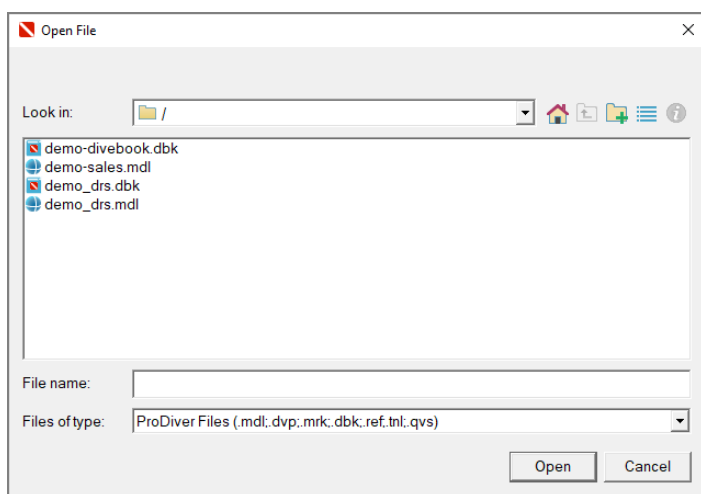
6. On the **DiveLine Login** dialog box, enter the **Username** and **Password** and click **OK**.



**TIP:** If you want to use a different server, click **Cancel**, and return to [Step 4](#).

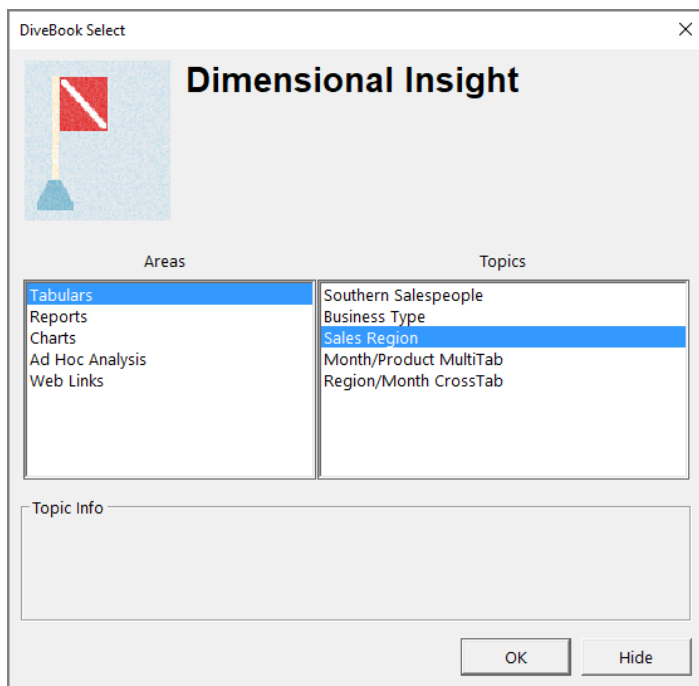
7. Select **File > Open**, or click the Open icon, . The **Open File** dialog box displays sample model and DiveBook files.

**NOTE:** Your display might contain different files.

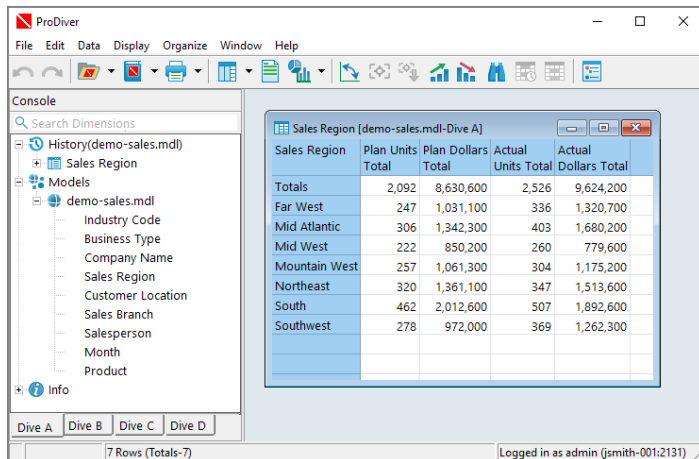


8. Select a *dbk* file, and click **Open**. For example, *demo-divebook.dbk*.

- Select an Area and a Topic, for example **Tabulars** and **Sales Region**, and click **OK**.

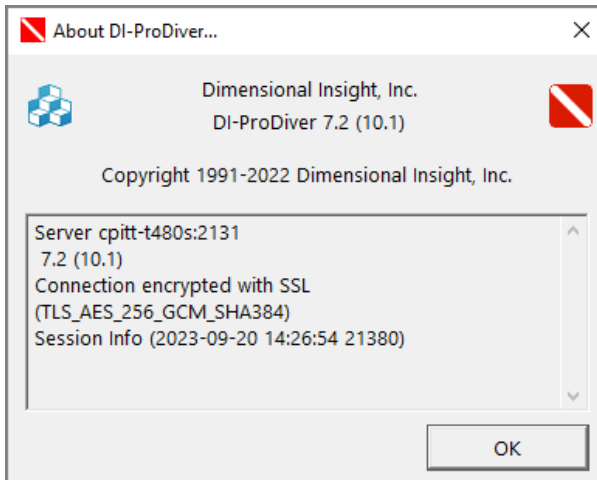


If you see a tabular display similar to the following, ProDiver is functioning correctly.

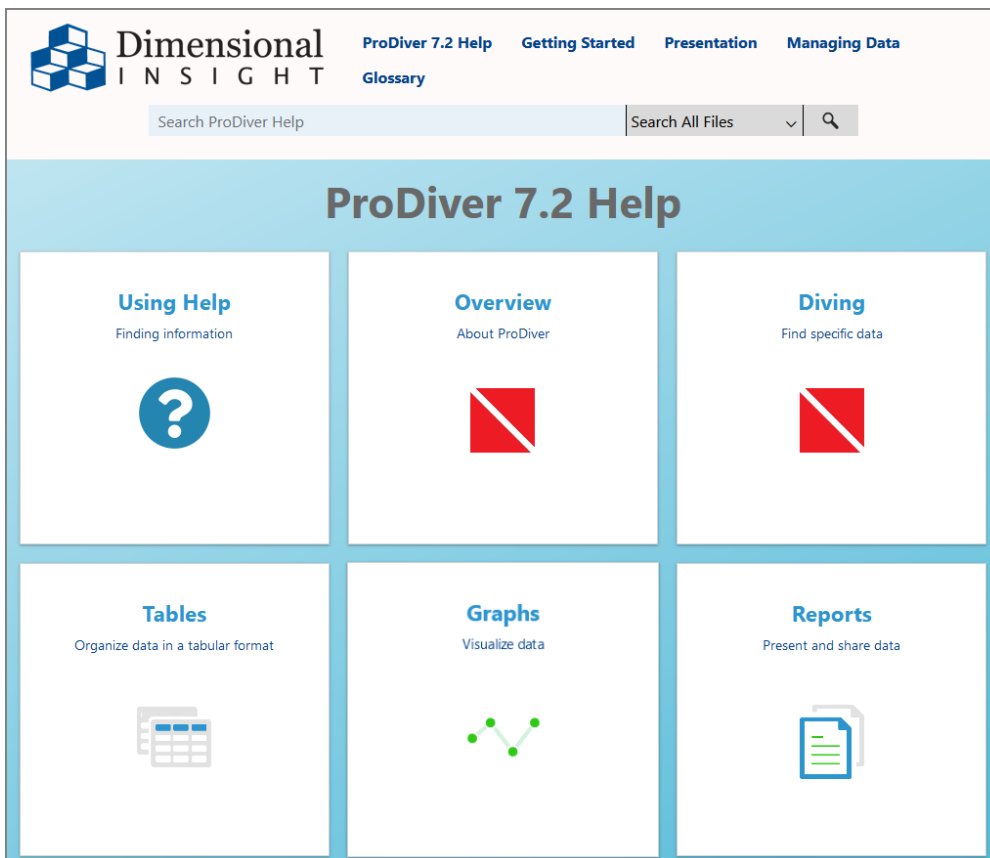


- To view the installed version of ProDiver and the DiveLine server name and version, select **Help > About ProDiver**. Confirm the versions and click **OK**.

## Diver Platform 7.2



11. To open *ProDiver Help* select **Help > View Help**. *ProDiver Help* opens in your default browser.



## Installing Workbench

Workbench is an integrated development environment (IDE), designed to simplify and speed up development of applications to model your data. With Workbench on your desktop, you can manage projects on the server, and test and visually examine your data flows and processes. In addition, Workbench provides one point of entry for all your Diver data servers, consolidating the tasks of developing, testing, and managing multiple data projects. The Workbench installation process closes all open instances of Workbench, so be sure to save any unsaved changes in Workbench before installing or updating Workbench.

**NOTE:** You need to be an administrative user to install the software.

Complete the following steps:

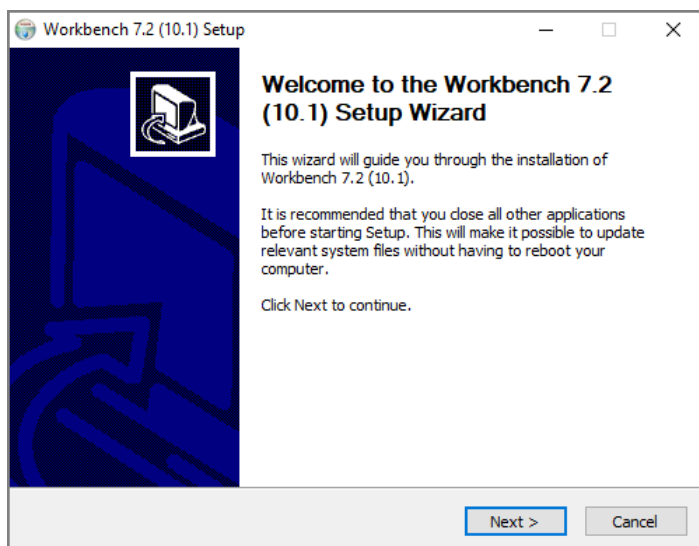
1. Navigate to the `DI\Solution\downloads` directory.
2. Double-click the **Workbench-Setup.exe** file.

The **User Account Control** dialog box opens, asking you to confirm making changes to your device.

**NOTE:** Depending on your Windows version and user account settings, you might see the **Open File - Security Warning** dialog box instead. Confirm that you want to open and run the executable file.

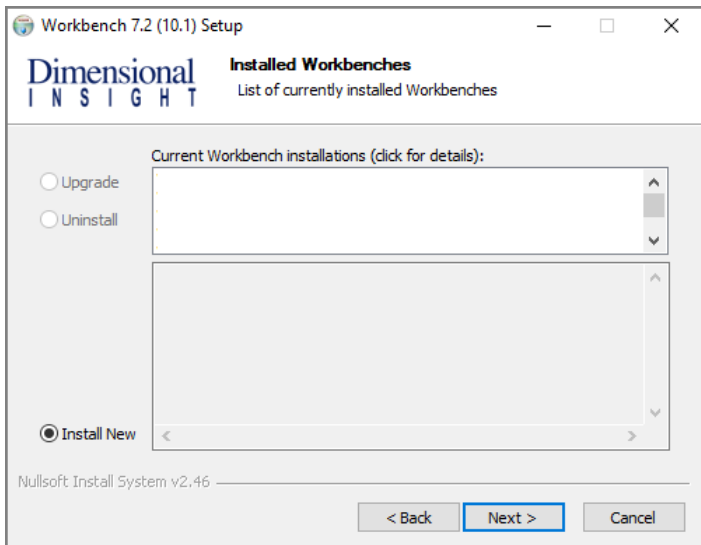
3. Click **Yes**.

The **Workbench <version number> Setup Wizard** dialog box opens.



4. Review the setup instructions and click **Next**.

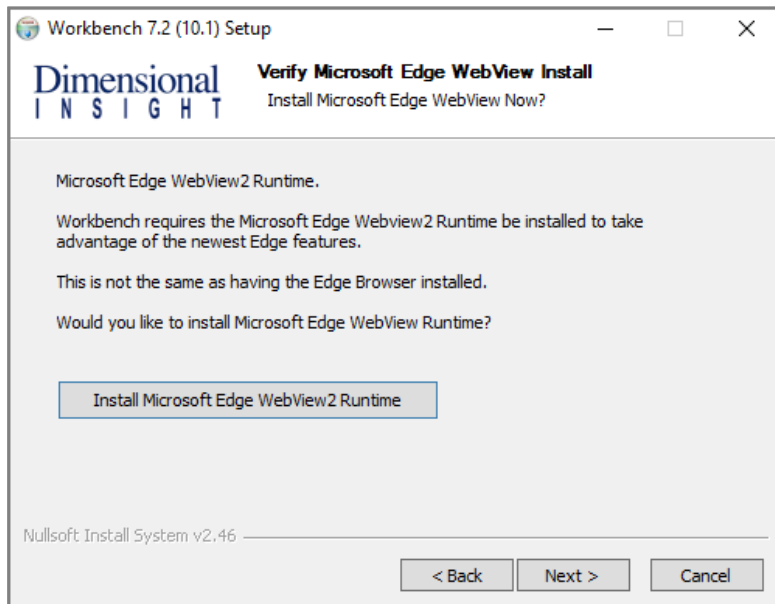
The **Installed Workbenches** page opens.



5. Select the **Install New** option. This page lists any existing Workbench installations, which you can choose to **Upgrade** or **Uninstall**. If this is the first installation, **Install New** is selected by default.
6. Click **Next**.

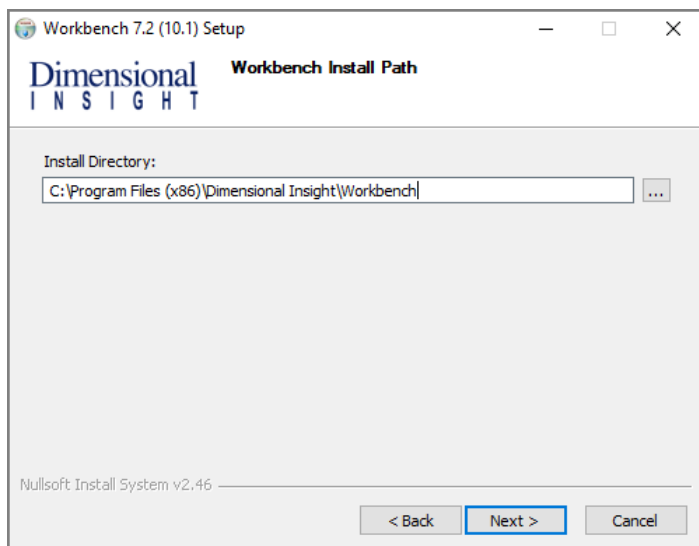
If Microsoft Edge WebView2 Runtime is not installed, the **Verify Microsoft Edge WebView Install** page displays.

- a. Click the **Install Microsoft Edge WebView2 Runtime** button to start the installation process.



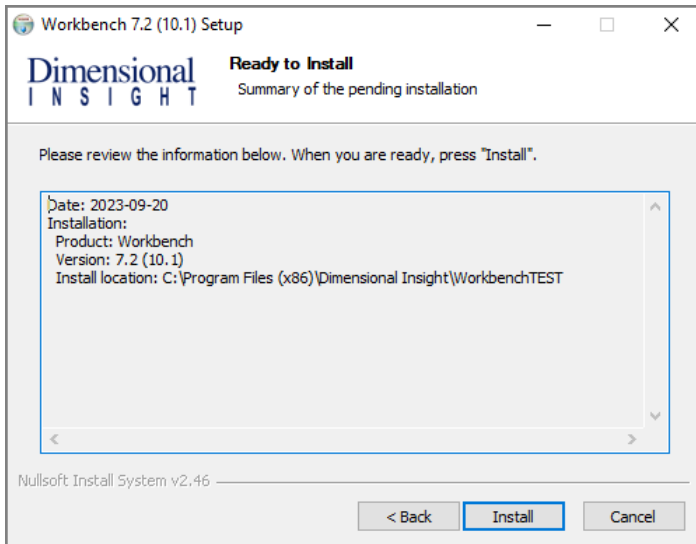
b. Click **Next** when the installation process finishes.

The **Workbench Install Path** page opens and displays the default installation path. For example, `C:\Program Files (x86)\Dimensional Insight\Workbench`. Make changes if necessary.

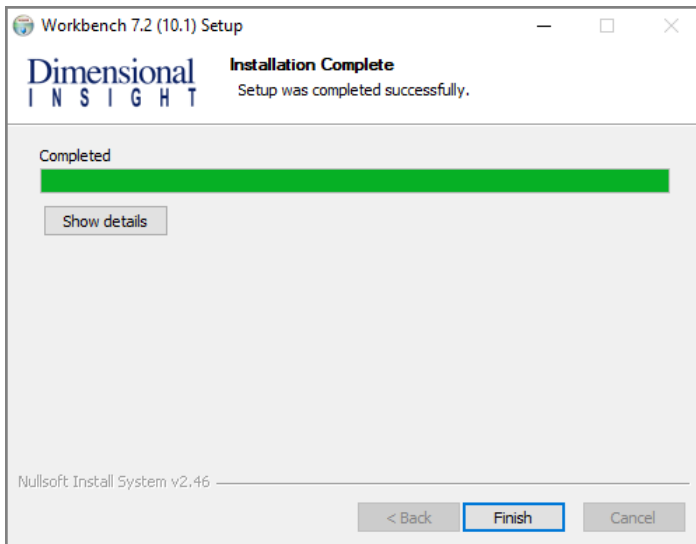


7. Click **Next**.

The **Ready to Install** page opens and displays a summary of the pending installation.



8. Click **Install** to install the Workbench software. When complete, the wizard displays the **Installation Complete** page.



**NOTE:** To view a running summary of the installation process, click the **Show details** button.

9. Click **Finish** to close the wizard.

**NOTE:** The Workbench installer enables TLS 1.2 on Windows 7 if it was not explicitly disabled by the user.

## Verifying the Workbench Installation

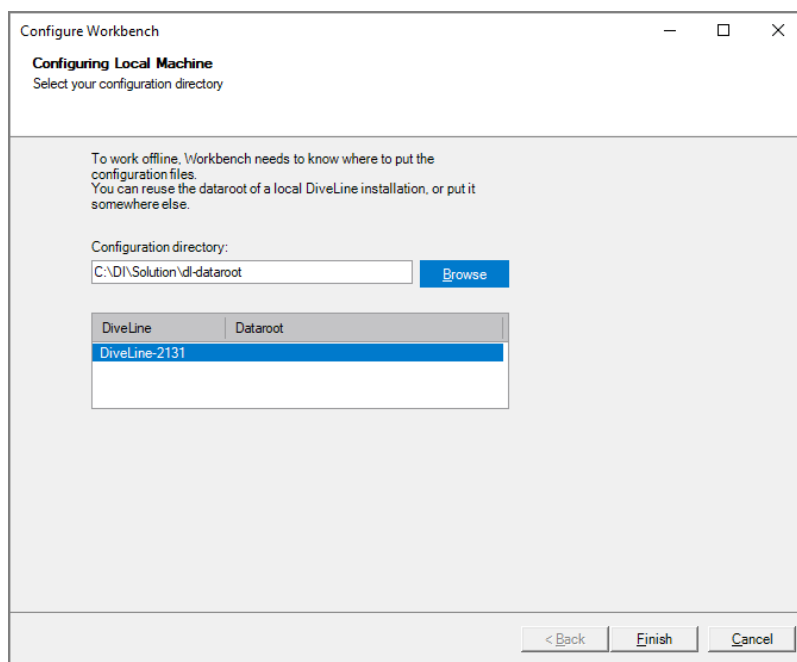
To verify a successful installation of Workbench, complete the following steps:



1. Open the Windows **Start** menu and enter **Workbench** in the Windows search box.
2. In the **Programs** list, click Workbench.

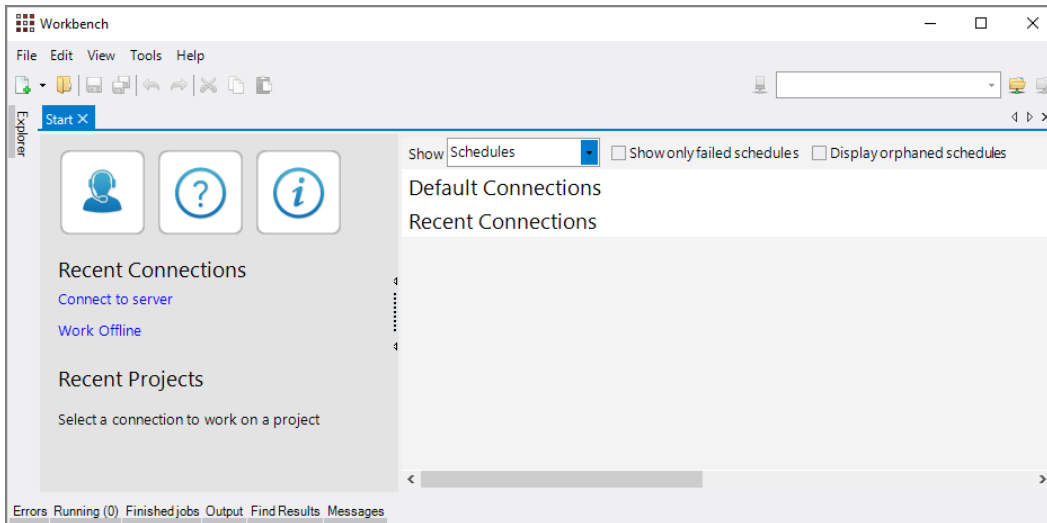
**NOTE:** When you open Workbench for the first time, it prompts you to select a directory for storing configuration files when you work offline. The default is the `C:\DI\Solution\dl-dataroot` directory for the local DiveLine installation.

- a. Click the **Browse** button to select a different Workbench configuration directory.
- b. Click **Finish**.

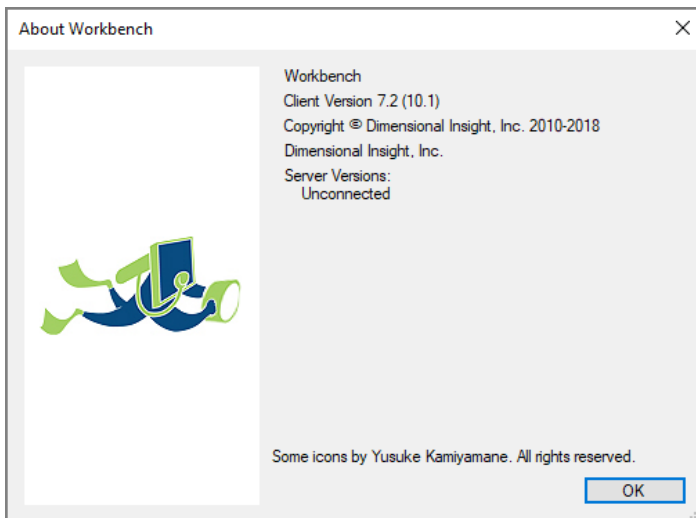


3. If successfully installed, the **Workbench** Start page opens.

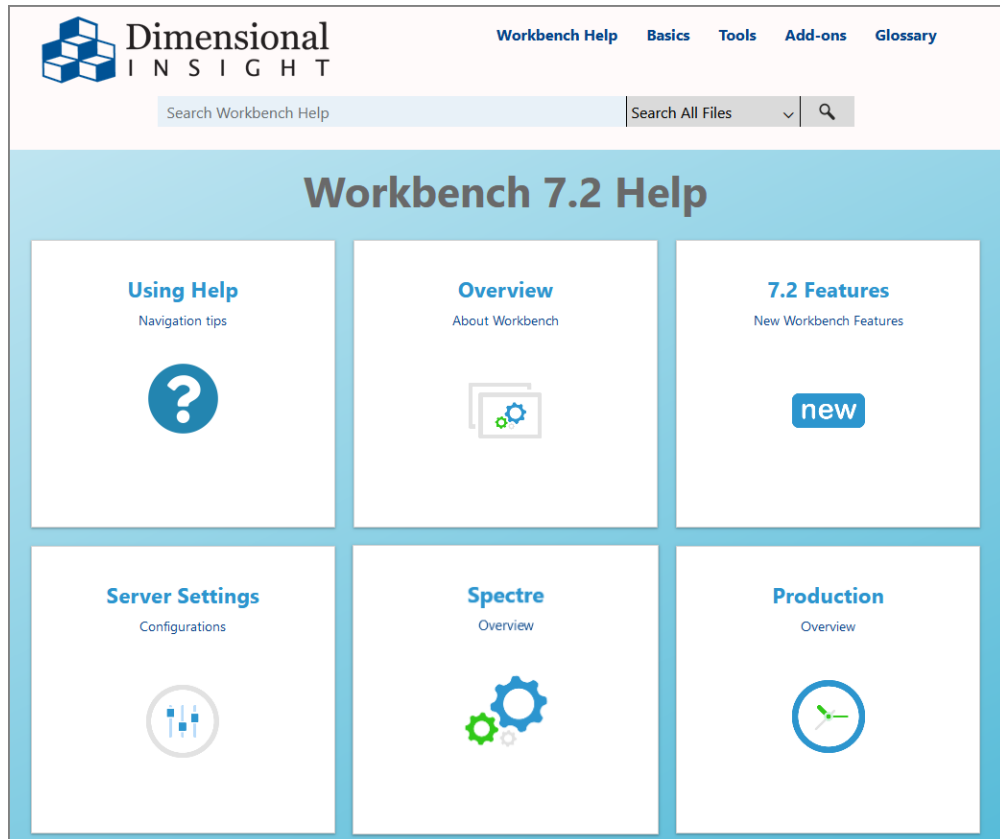
## Diver Platform 7.2



4. To view the Workbench version number, click **Help > About Workbench**. Confirm the version, and click **OK**.



5. To open *Workbench Help* in a browser window, click **Help > View Help** or click the **Question mark** icon.



The *Workbench Help* opens in your default browser. Here you can find topics that explain how to connect to a server.

# Updating the DI Software

Dimensional Insight recommends using the most recent point release of software for best results, including Tomcat and Java. The software Setup Wizard has an option for upgrading your software.

## NOTES:

- The upgrading process differs depending on which software is being updated.
- Updating the DiveLine server and its clients, DivePort and NetDiver, requires temporarily stopping Tomcat.
- Temporarily stopping Tomcat automatically disconnects users.
- When updating Bridge or DivePort 7.2, if the installer has a newer version of Tomcat 9.0 available than what is currently is installed, you have the option to allow the installer to update Tomcat to that version.
- The ProDiver installer places a copy of the Setup Wizard in the Program Files directory for uninstalling purposes.
- Use the **Copy a portal** option when installing DivePort and Bridge to upgrade from 7.0 to 7.1, and install the new required Java version and recommended Tomcat versions if necessary.
- When upgrading Tomcat from 7.0 to 9.0 using the DivePort or NetDiver installers, Tomcat 7.0 remains in the `C:\Program Files\Apache Software Foundation\Tomcat 7.0` directory with a manual start. Registry information for the DI web applications is updated to point to the new Tomcat 9.0 in use.

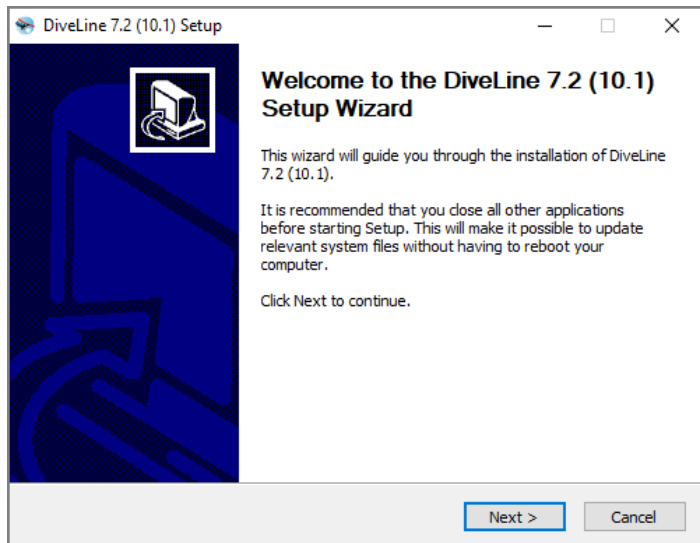
To upgrade your software:

1. Download the *zip* file for the software or software package from DI-Download at <http://www.dimins.com>.
2. Move the file from your Downloads directory to the `DI\Solution\downloads` directory.
3. Right-click the file and select **Extract All**, or use a third-party tool, to unzip the file.
4. Double-click the *exe* file. This example uses *DiveLine-Setup.exe*.  
The **User Account Control** dialog box opens, asking you to confirm making changes to your device.

**NOTE:** Depending on your Windows version and user account settings, you might see the **Open File - Security Warning** dialog box instead. Confirm that you want to open and run the executable.

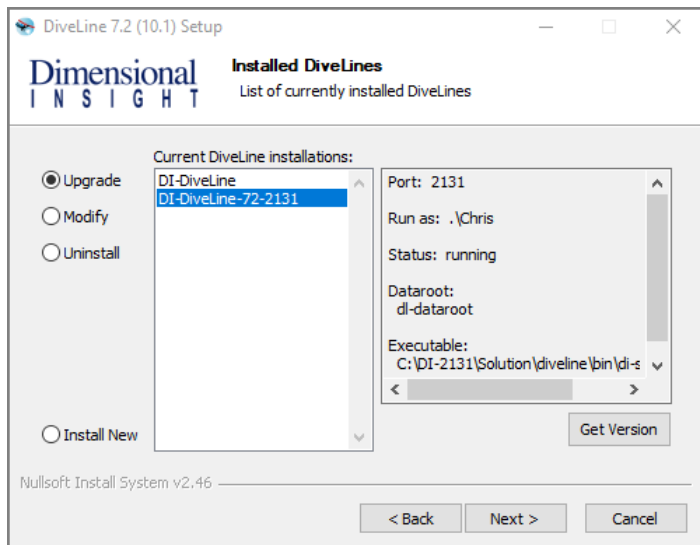
5. Click **Yes**.

The **Setup Wizard** dialog box opens.



6. Review the setup instructions, and click **Next**.

The **Installed** page displays.



**NOTE:** This page is called **Choose an Action** in some other Setup Wizards.

7. Select the installation you want to upgrade.

**TIP:** Click the **Get Version** button to discover the current installation version.

8. Click **Next**.

9. Follow the instructions to reach the **Installation Complete**, or **Completing** page.

**NOTE:** The installer checks whether the existing license is valid.

10. Click **Finish** to finish the installation.

#### **NOTES:**

- Updating DiveLine removes all *data* files from the Spectre cache, leaving the metadata in place. This speeds up the upgrading process and allows for a cache refresh operation.
- After upgrading DivePort, DI recommends checking the Web Server and Java information under **ADMIN > Portal Settings** to ensure that the versions of Tomcat and Java are supported.
  - **Web Server** displays the current version of Tomcat and alerts you if an update is due.
  - **Java** displays the current version of Java and alerts you if an update is due.
- Normally, upgrades to NetDiver do not require changes to a configured Web Server authentication scheme. However, if you are upgrading Tomcat to 7.0.73 or higher without upgrading the *dlcgi.exe* file, you may run into a bug if you are using Windows usernames. Dimensional Insight recommends upgrading *dlcgi.exe* using the one included in the latest 7.2 server package.

## Renewing a License

You can request a new license from Dimensional Insight using the DI-License-Admin utility. Keep in mind that your machine must have Internet access to submit a license renewal request.

To renew a license:

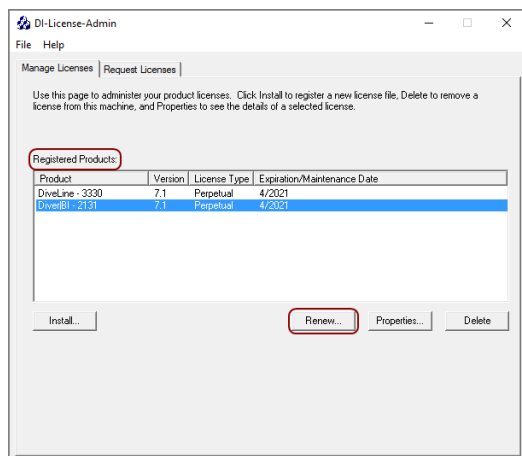
1. Navigate to the `DI\Solution\downloads` directory.
2. Double-click the **di-license-admin.exe** file.

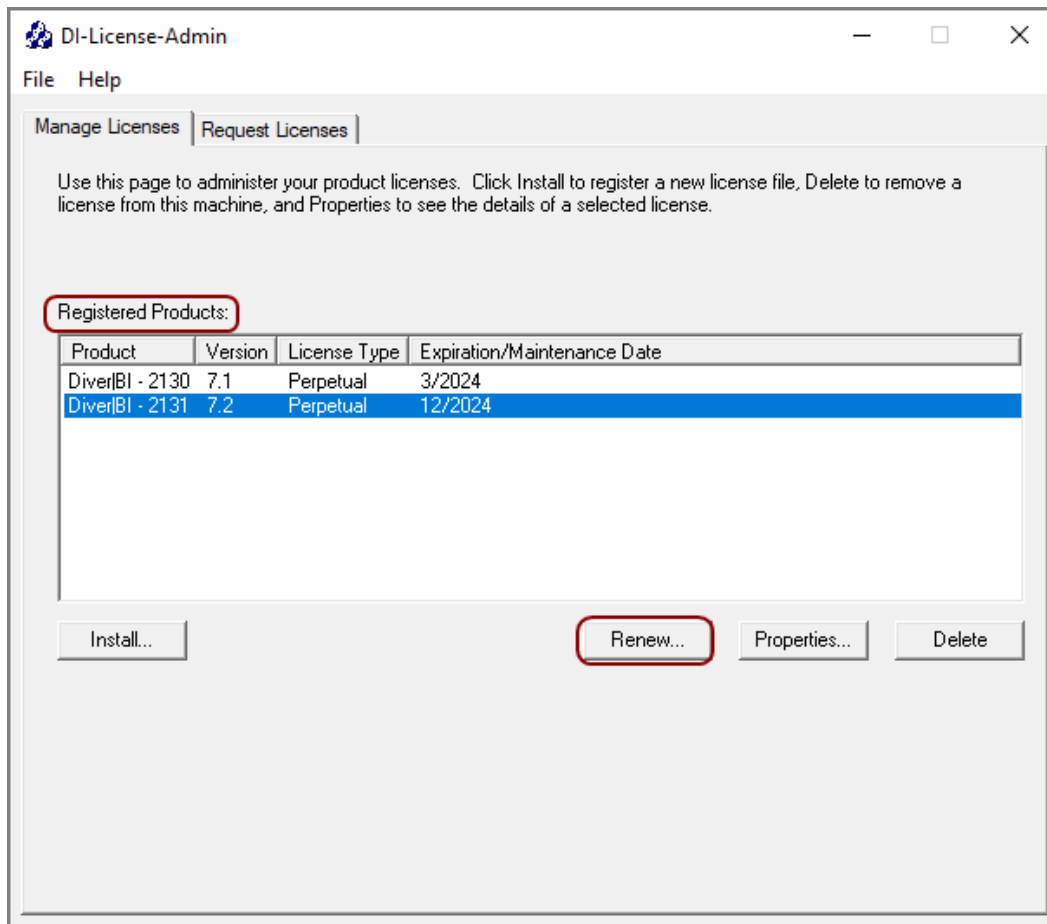
The **User Account Control** dialog box opens, asking you to confirm making changes to your device.

**NOTE:** Depending on your Windows version and user account settings, you might see the **Open File - Security Warning** dialog box instead. Confirm that you want to open and run the executable.

3. Click **Yes**.

The DI-License-Admin utility starts.





4. In the **Registered Products** list, select the license you want to renew.

5. Click **Renew**.

The **Renew License** window opens.



**Renew License**

Request a renewal of an existing license. Please check that user and machine information are correct. Any requests to change the license may be entered in the Comments field.

Application:

**Existing License Details**

License data for DiverBI  
 License Class: Enterprise  
 License Type: Perpetual  
 Licensed to: Dimensional Insight, Inc.  
 Node-locked to: Hw00:50:56:c0:00:08 IDF003:0853  
 Port number: 2131  
 User categories and limits:  
 Developer: 1  
 DivePort: 1  
 DiveTab: 1  
 HelpDesk: 1  
 ODBC: 1  
 ProDiver: 1  
 Maintenance termination date: 5/2021

**Customer Information**

Name:   
 Phone:   
 Company:   
 Email:

**Machine Information**

Machine Name:   
 Operating System:   
 Machine ID:

Enter any Comments, Questions, or Changes

**Renew License**

Request a renewal of an existing license. Please check that user and machine information are correct. Any requests to change the license may be entered in the Comments field.

Application:

**Existing License Details**

License data for DiverBI  
 License Class: Enterprise  
 License Type: Perpetual  
 Licensed to: Dimensional Insight, Inc.  
 Node-locked to: ID489D-3C47 Hw0a:00:27:00:00:07  
 Port number: 2131  
 User categories and limits:  
 Developer: 5  
 DivePort: 5  
 DiveTab: 5  
 HelpDesk: 5  
 ODBC: 5  
 ProDiver: 5  
 Maintenance termination date: 12/2024

**Customer Information**

Name:   
 Phone:   
 Company:   
 Email:

**Machine Information**

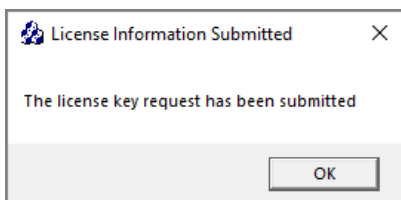
Machine Name:   
 Operating System:   
 Machine ID:

Enter any Comments, Questions, or Changes

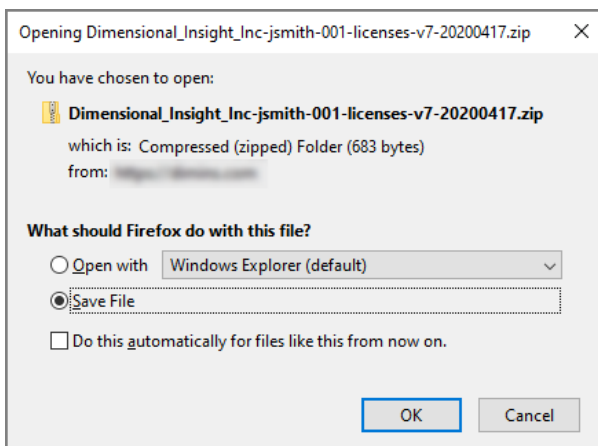
6. Verify the Customer and Machine Information on the license and make changes where necessary.
7. Review the Existing License Details.

8. In the Comments, Questions, or Changes text box, enter any changes you want to make to the license, and include any comments or questions you have.
9. Click **Submit**.

The **License Information Submitted** dialog box opens.



10. Click **OK** to acknowledge the submission.
11. After DI Customer Support sends you the requested license, save it to the `DI\Solution\licenses` directory.



**NOTE:** Some email programs might include this file as inline text. Make sure that the license file is an attachment.

12. Right-click the package and select **Extract All**, or use a third-party tool, to unzip the file.

The following example shows a Diver Platform Server 7.2 license file:

```
c3931_jsmith-001_platform72_p2131_m202107.license
```

# Uninstalling the DI Software

The software Setup Wizard has an option for uninstalling your software.

## NOTES:

- Uninstalling DI software differs depending on which software is being removed.
- Uninstalling the DiveLine server and its clients, DivePort and NetDiver, requires temporarily stopping Tomcat.
- Temporarily stopping Tomcat automatically disconnects users.
- The ProDiver installer places a copy of the Setup Wizard in the Program Files directory for uninstalling purposes.

To uninstall your software:

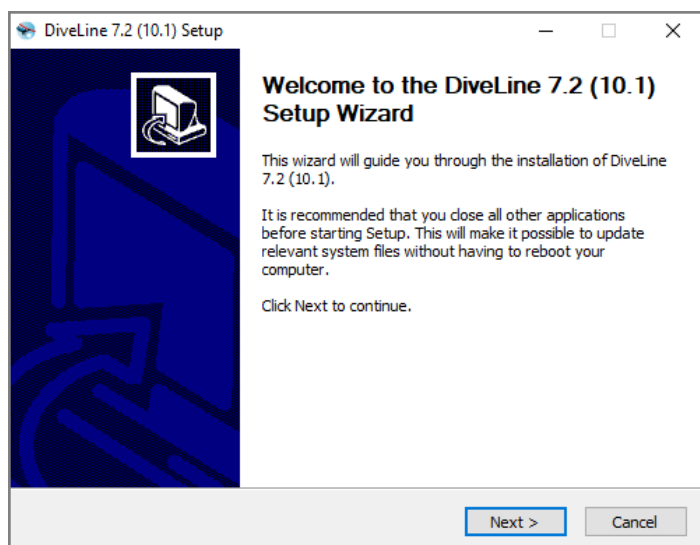
1. Double-click the *exe* file. This example uses *DiveLine-Setup.exe*.

The **User Account Control** dialog box opens, asking you to confirm making changes to your device.

**NOTE:** Depending on your Windows version and user account settings, you might see the **Open File - Security Warning** dialog box instead. Confirm that you want to open and run the executable.

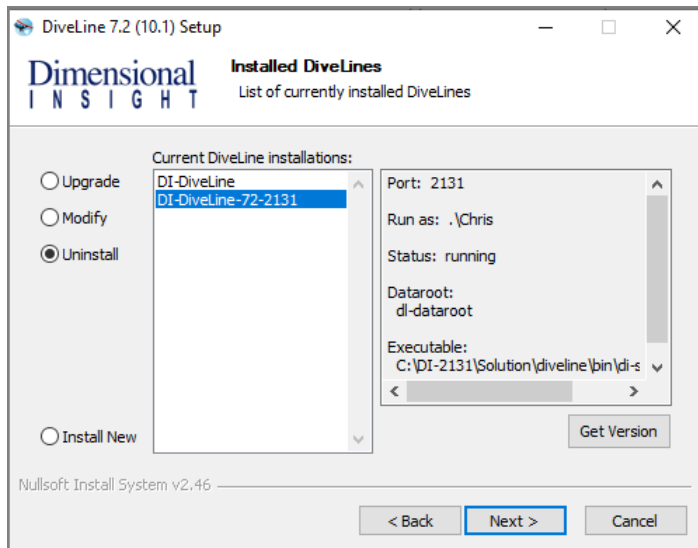
2. Click **Yes**.

The **Setup Wizard** dialog box opens.



3. Review the setup instructions, and click **Next**.

The **Installed** page displays.



**NOTE:** This page is called **Choose an Action** in some other Setup Wizards.

4. Select the **Uninstall** button.
5. Select the installation you want to uninstall.

**TIP:** Click the **Get Version** button to discover the current installation version.

6. Click **Next**.
7. Follow the instructions to reach the **Installation Complete**, or **Completing** page.

**TIP:** Bridge and DivePort include an option to remove files related to the site. Select the **Also remove site-specific files** check box to delete these files.

8. Click **Finish** to finish uninstalling the software.

You may need to restart your machine after uninstalling.

# Appendix A: Bridge

Bridge is a web application based on DivePort technology that you can use to navigate your DI applications from one central place. It gives you single-click access to your DivePort and NetDiver portals and can reach all your relevant web content without relying on browser features like bookmarks. You can also use Bridge to connect to ProDiver and DiveTab.

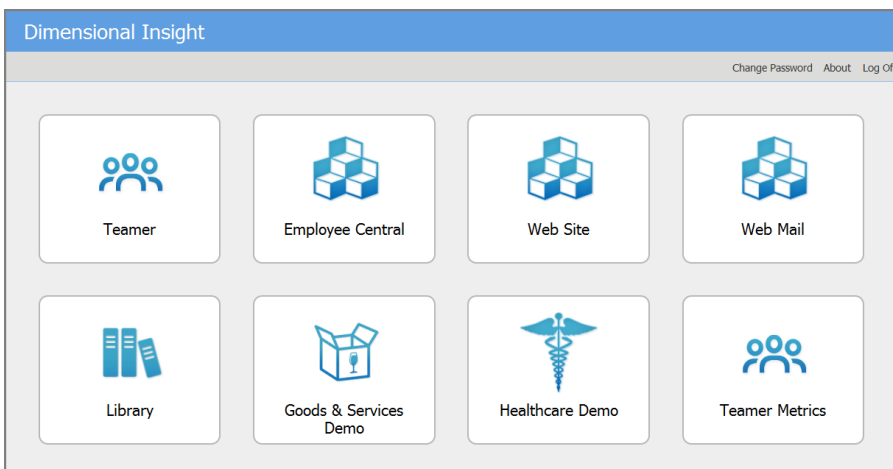
Bridge presents a single view of DivePort Applications and Portals regardless of which version is running. This allows you to build new Applications and Portals taking advantage of the latest Diver Platform functionality without first upgrading existing applications. You get seamless access to existing and future applications under one umbrella.

## Design

Bridge supports all versions of DI software. There are no cross-compatibility limitations, so you can use it to launch any functioning DI application, on one machine or multiple platforms. It can be configured to use one Authentication layer across all DI applications, supporting single sign-on. The result is a single browser window and single-click access for your end users.

Bridge must be configured to recognize the other Applications and DI Portals, and in turn, the hosting DiveLines must recognize Bridge. You can use multiple Bridges to segment your users if it suits your environment, but it is not required. The user interface can display one button for each Portal to which a user has been granted access, so the displayed buttons can vary by user. All users can be directed to a single URL to bookmark.

The interface, no matter how it is configured, is designed to be simple and consistent. Here is an example of a user interface for the Bridge component.



When installed and configured, Bridge authenticates end users when they log on. When the end user chooses a destination that is a DI application, a one time password is used to log on to the target. What a user sees in each destination is controlled by that destination’s configuration. Access is no different than what is in place without Bridge.

Furthermore, for any given destination (for example, a DivePort), Bridge does not display a destination if it goes to DivePort pages that the current user does not have access to.

## How it Works

The Bridge administrator names all the available destinations and provides an image and description for each button that is displayed for the end users. The administrator also enters the DiveLine, Application, and Portal URL information, and coordinates as needed with the administrators of the destination sites to complete configuration for single sign-on.

The tasks for Bridge are as follows:

- Use the hosting DiveLine’s user list for authentication.
- Determine what buttons to display for each user based on the settings for each destination.
- Link to other sites as configured.

### NOTES:

- The authentication methods can be different between Bridge and the various target DiveLines. The target is set up to recognize Bridge, and Bridge forwards the authentication.
- Passwords are not important—they can be the same or different. In a typical scenario, end users log on to Bridge with their Bridge password,

and can connect to any other DI application regardless of what their password is on those sites.

- New users added to sites need to be manually added to Bridge's DiveLine.

From the end-user perspective:

1. Access Bridge using the published URL in your chosen web browser.
2. Enter your Username and Password, and log on.
3. View the displayed buttons for each configured application or portal.
4. Click on a button to open that application or portal.
5. Return at any time to the Bridge tab to access another application or portal.

## Requirements

The infrastructure required for Bridge is the same as for the Diver Platform. Bridge is easy to install and deploy: it is basically another DivePort instance, so it can run on your web server with all your other DivePorts. For more information, see [Installing Bridge on the next page](#).

**NOTE:** For better control of Bridge access, particularly regarding who can modify Bridge settings, you might want to install a separate DiveLine dedicated for Bridge. A Bridge-specific DiveLine uses port number 3330. For more information, see [Installing DiveLine on page 24](#).

The basic set of users for Bridge is taken from whichever DiveLine is selected to host it. Additional users can be created using Workbench. For more information on maintaining users for DI software, please refer to **Help Desk** or the **Server Settings** section of the *Workbench Help*.

## Bridge Configuration

Bridge can be installed on an existing DiveLine, or a new DiveLine instance can be created to host Bridge specifically. When Bridge is installed, all DiveLine administrators automatically become Bridge administrators. Bridge administrators are not required to be DiveLine administrators. Only administrators have access to the **Admin** menu in Bridge. For options, see the **Server Settings** section of the *Workbench Help*.

No changes are required to DI applications on the same DiveLine as Bridge, but applications on other DiveLines require edits to the **Authorized DivePort Gateways** list under the **General** tab for Workbench **Server Settings**. This needs to be edited manually to include Bridge's IP address or DNS name. This is required for single sign-on to work, along with the DiveLine server name and

port in the Destination Settings. For more information, see [Configuring Destinations on page 108](#).

When planning your deployment, be aware that the DiveLine user list controls who has access to that Bridge instance. If user lists vary widely for your DivePorts across your organization, manual updates are required.

Once installed, an administrator can set up additional administrators and customize Bridge's look directly from the Bridge portal. For more information, see [Configuration Options on page 105](#).

## Authentication

Bridge's user list is that of the hosting DiveLine. All types of DiveLine authentication are supported (Own, LDAP, SYSTEM, or Web Server). Bridge's IP address or DNS name must be in the destination DiveLine's **gateway\_ips** list for a seamless handoff.

Bridge keeps connections open to its destination DiveLines in order to keep its lists of the users on those DiveLines up to date. It uses these user lists to decide which destinations to show to a user. If a destination has a DiveLine associated with it, it only shows that destination if the user is in the user list for that DiveLine. If the destination goes to a DivePort page ID, Bridge also makes sure that the user has access to that page and does not show a destination that the user does not have access to.

If Bridge and destination DiveLines have the same user names (irrespective of case), and the **DiveLine** and **Admin Username** are part of the Destination configuration, Bridge knows which buttons to display for the end user. One click on the button puts the user into the application.

Bridge does a case-insensitive comparison when determining whether a user is in the current list of users for a given DiveLine, to determine whether to show a destination pointing to that DiveLine to that user.

If the Destination configuration is incomplete, causing Bridge to show a destination the end user has no access to, then a secondary log on appears when the button is clicked.

**NOTE:** Bridge uses an encrypted connection when communicating with encryption-enabled 7.2 DiveLines. However, for compatibility with older DI software, it allows access to unencrypted DiveLines.

## Installing Bridge

Wherever you install Bridge, the hosting DiveLine serves as the basis for its user list. Once you have determined which DiveLine to use for Bridge, launch the



installer downloaded from DI-Download. This section guides you through the installation process of Bridge for Windows.

**NOTE:** You need to be an administrative user to install the software.

To install Bridge:

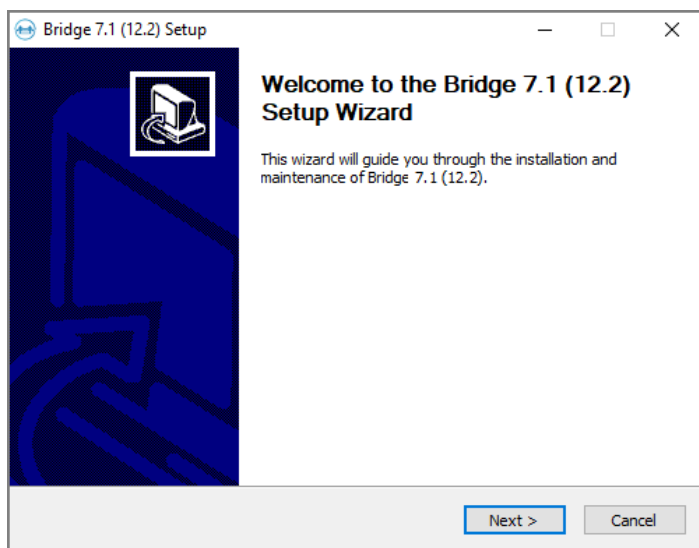
1. Navigate to the `DI\Solution\downloads` directory.
2. Double-click the **Bridge-Setup.exe** file.

The **User Account Control** dialog box opens, asking you to confirm making changes to your device.

**NOTE:** Depending on your Windows version and user account settings, you might see the **Open File - Security Warning** dialog box instead. Confirm that you want to open and run the executable.

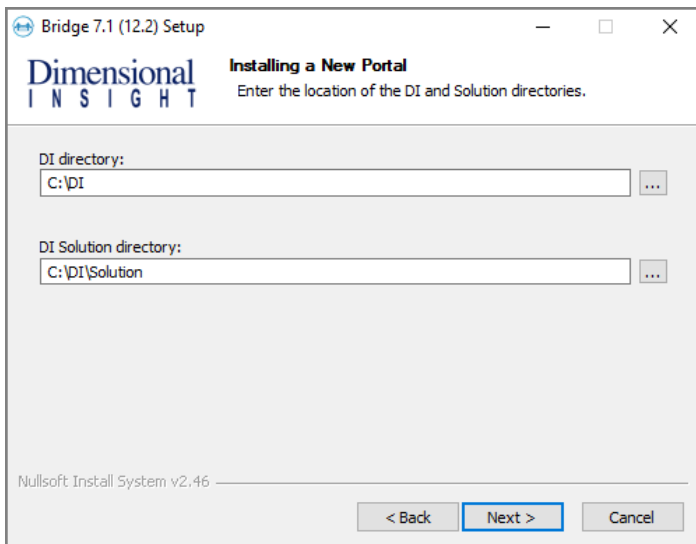
3. Click **Yes**.

The **Bridge <version number> Setup Wizard** dialog box opens.



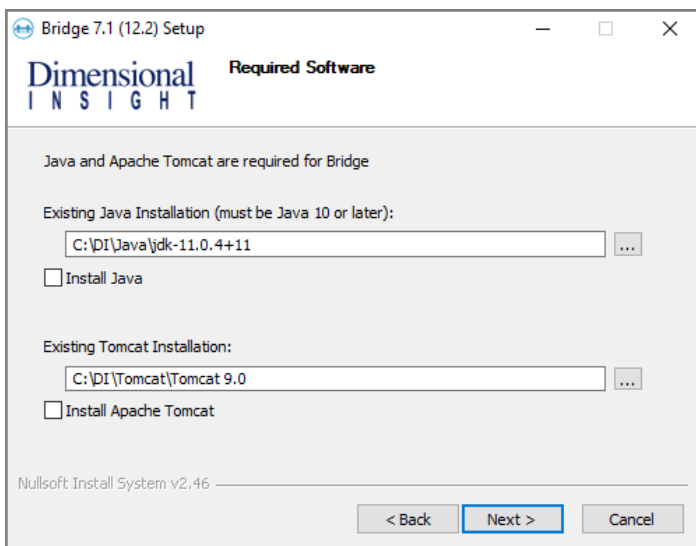
4. Click **Next**.

The **Installing a New Portal** page opens.



5. Verify the default locations for the `DI` and `DI Solution` directories.
6. Click **Next**.

The **Required Software** page opens.



7. Do one of the following:
  - If already installed, verify the existing installation paths and change if necessary.  
**NOTE:** If Tomcat already has HTTPS installed, skip to [Step 12](#).

- If not installed, select the **Install Java** or **Install Apache Tomcat** or both check boxes and follow the instructions. If following the installation guide, Java is installed in [Installing DiveLine on page 24](#), and Tomcat in [Installing DivePort on page 38](#).

8. Click **Next**.

The **Create Certificate for HTTPS** page opens.

Bridge 7.1 (12.2) Setup

**Dimensional INSIGHT** Create Certificate for HTTPS

Warning: a self-signed certificate produces browser warnings  Skip this step

File Out:  ...

Name (e.g. server1.company.com):

Organizational Unit:

Organization:  City/Locality:

State/Province:  2-letter Country Code:  Password:

Creation Result:

Nullsoft Install System v2.46

< Back Next > Cancel

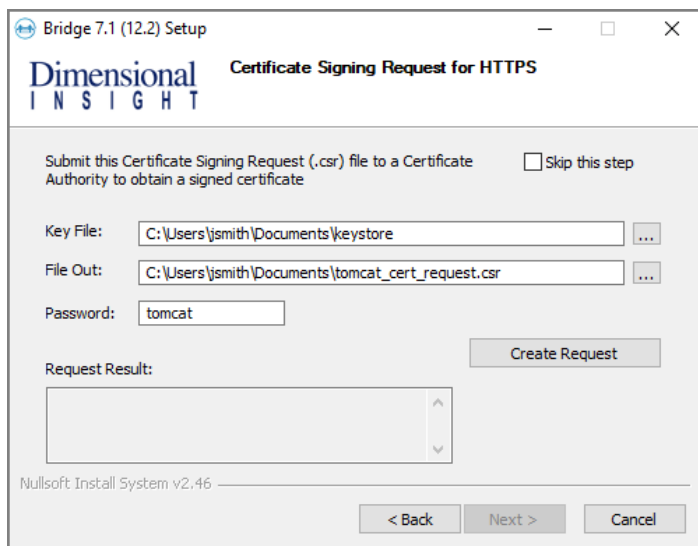
9. Do one of the following:

- Fill in the information as appropriate and click **Create Certificate**.
- Select **Skip this Step**.

**NOTE:** If you installed DiveLine, there is already a certificate available. Select **Skip this Step**.

10. Click **Next**.

The **Certificate Signing Request for HTTPS** page opens.



11. Do one of the following:

- Verify the information and click **Create Request**.
- Select the **Skip this step** check box.

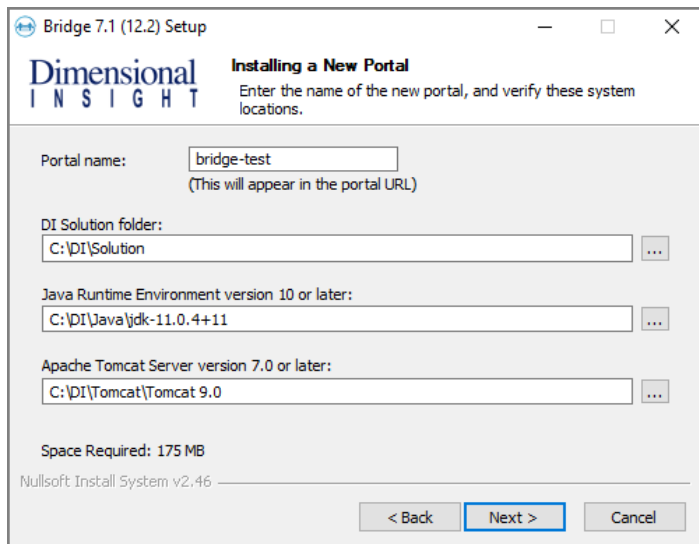
**NOTE:** If you installed DiveLine, there is already a certificate available. Select **Skip this Step**.

12. Click **Next**.

The **Installing a New Portal** page opens with the following defaults:

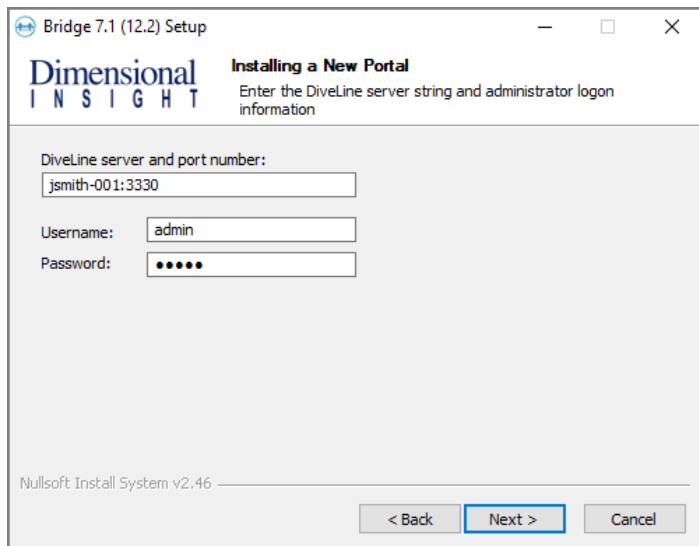
- **Portal name**—The default name is **bridge**. You can change it to suit your needs.
- **Path to DI Solution folder**—The default folder is `C:\DI\Solution`.
- **Path to Java Runtime Environment**—The default path is `C:\DI\Java\jdk-11.0.1`.
- **Path to Apache Tomcat Server**—The default path is `C:\DI\Tomcat\Tomcat 9.0`.

A best practice is to change the default Portal name to something other than **bridge** (for example, **bridge-test**) to keep the software distinct from another implementation. One installation of the software can support multiple instances or portals. Verify the other default fields.



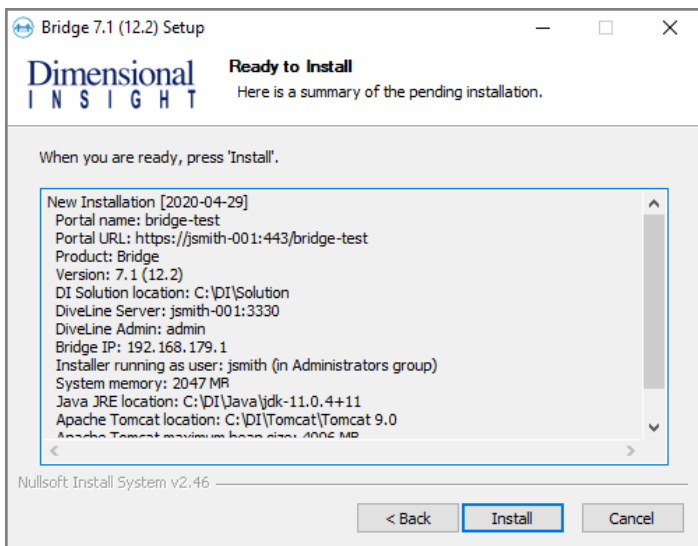
13. Click **Next**.

The second **Installing a New Portal** page opens, with the default name of the DiveLine service and port number (for example, **jsmith-001:3330**). Verify that the port number matches the DiveLine service. This page also prompts you to enter the administrator Username and Password previously defined for the DiveLine administrator.



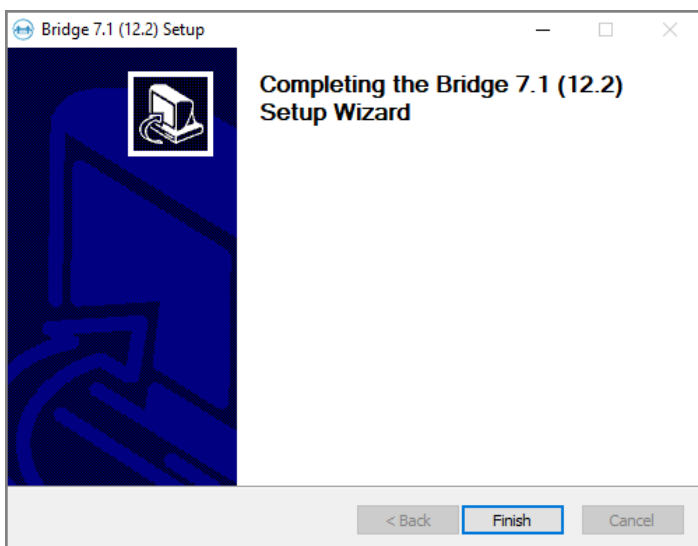
14. Click **Next**.

The **Ready to Install** page opens, with a summary of the Bridge installation information. Verify the information. Use the **Back** button if needed.



**NOTE:** Take note of the **Portal URL**. This is used to access Bridge from a web browser.

15. Click **Install**.
16. Click **Finish** to close the installation wizard.



**NOTES:**

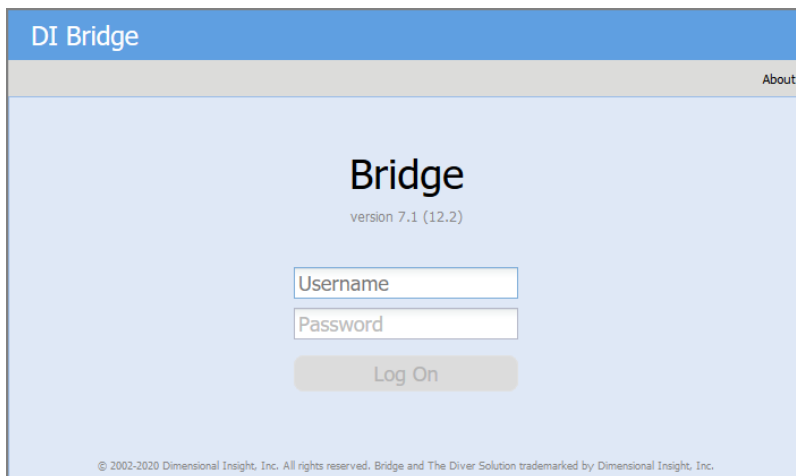
- The default web application name is **bridge**. This is easily changed when installing.
- The Bridge application has its own section in the Windows Registry.
- The Bridge software has its own section in the Windows Start menu. From the Start menu, enter "bridge" to see a link for the **<bridge> Logon Page**. Click to open in your default browser.
- When multiple instances of Bridge are installed on the same Windows machine, you might want to edit Properties to display different Program labels from the Start menu.
- Multiple Bridges can be installed on a single server, or multiple servers, and can communicate each other. When nesting Bridges, avoid creating circular loops. That is, if Bridge A points to Bridge B, Bridge B should not point back to Bridge A.

## Configuration Options

After you install Bridge, you launch it as you would a DivePort instance.

Enter the URL into your web browser. For example, **https://jsmith-001/bridge-test/#**.

A page similar to the following displays.



Use an Administrator account from the DiveLine that Bridge uses to log on.

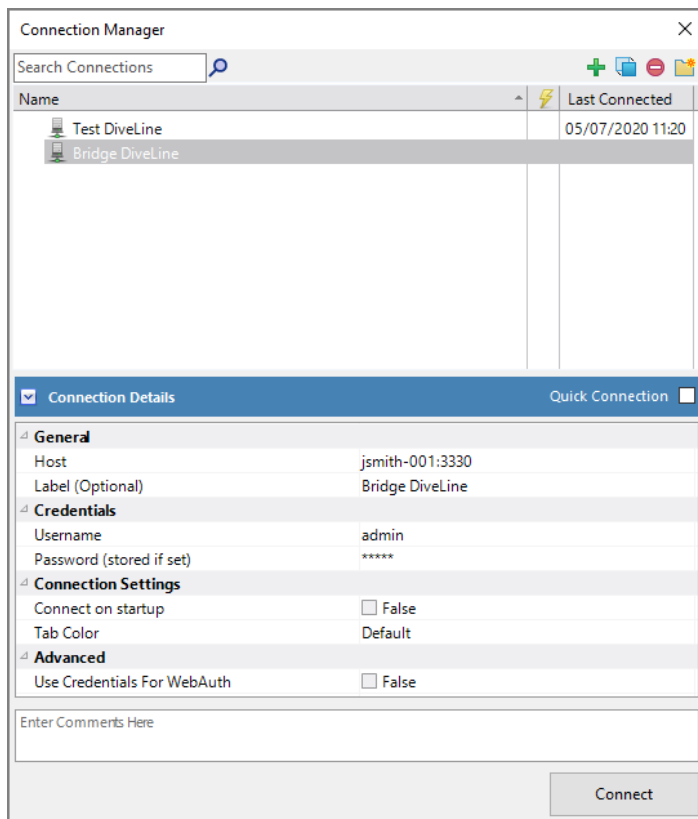
## Adding Login Options

Using Workbench, you can display messages and information to a user after login to various DI clients:

- **Welcome Message**—This message appears when the user opens Bridge.
- **Message of the Day**—This message appears after a successful log in.
- **Last Login Information**—Displays information about the user's last log in. If this option is selected, it appears as part of the Message of the Day.

To add a log in Welcome Message or a Message of the Day or both:

1. Open Workbench.
2. Navigate to the Connection Manager.
3. Open a connection to the DiveLine hosting the Bridge. For example:



4. Click **Tools > Server Settings > General > Options**.
5. Click the **Login Options** chevron to display the login settings.

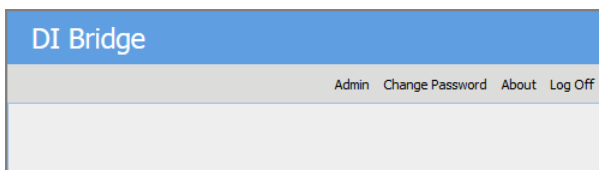


6. Optionally, enter a **Welcome Message**, or **Message of the Day**, or both, and select or clear the **Show last login information** check box.
7. Save your changes.

When Bridge is accessed by your users, they see any configured messages.

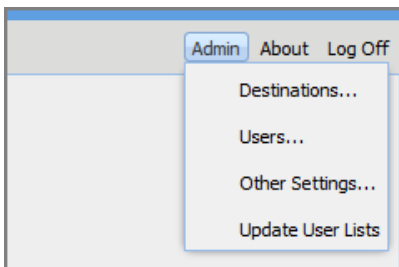
## Edit Dialogs

As in a standard DivePort portal, the edit controls are located top right below the banner. Click to display the menu or dialog.



- **Admin**—Leads to configuration dialogs.
- **Change Password**—Prompts for a new password for the current user and saves it to the corresponding DiveLine. Only available for **Own** authentication.
- **About**—Displays the version for Bridge and DiveLine.
- **Log Off**—Signs off the Bridge portal.

Use the **Admin** menu to get started.



- **Destinations**—Use to configure target portals Bridge can access.
- **Users**—Use to set additional administrators for Bridge (not DiveLine).
- **Other Settings**—Use to customize buttons and banners for Bridge.
- **Update User Lists**—Use to update Bridge's local user lists from destination DiveLines without having to wait for the next time Bridge automatically refreshes its local information. If this menu item is not used, Bridge updates its destination user information every five minutes if configured. For more information, see [Configuring Other Settings on page 115](#).

## Configuring Destinations

Use **Admin > Destinations** to access the **Destinations Settings** dialog box. This is where you define connections for Bridge.

To define a Bridge destination:

1. Click **Add** to begin.
2. Click the pull-down menu and choose a **Destination Type**.

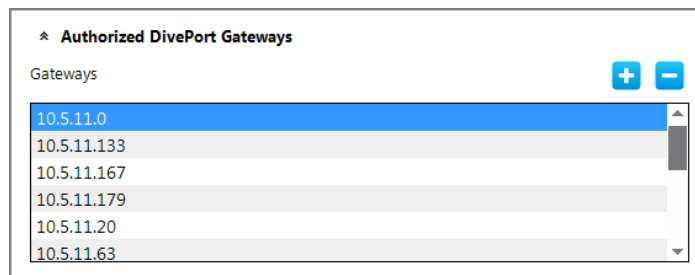
There are three Destination Types:

- **Web Application**—Destination to a web address, including a DivePort instance, possibly with a particular environment and page, or a NetDiver instance, or another website.
  - **ProDiver**—Destination to a project file, opening the file in ProDiver.
  - **DiveTab**—Destination to a DiveTab instance, opening the site with DiveTab.
3. Enter and choose attributes as needed:

**NOTE:** The attributes change based on the **Destination Type**.

- **Label**—Names the available site; appears on the button, and in the **Destinations** list dialog box.
- **Tool Tip Text**—Appears as a tooltip when hovered over.

- **Link URL**—Specifies the Uniform Resource Locator (URL) or web address for a DivePort instance, possibly with a particular environment and page, or a NetDiver or other site on the Web.  
**NOTE:** Relative paths for destination strings need to start with "/". For example: /path#page=pagename.
- **Project Name**—The name of a project ProDiver is opening. ProDiver can open a project or a specific file. This attribute is ProDiver specific. If not specified, the ProDiver application is still launched.
- **File Path**—The exact file path to a file ProDiver is opening. ProDiver can open a project or a specific file. This attribute is ProDiver specific.
- **DiveLine**—Indicates the server name and port number for the target portal (for example, jsmith-001:2131). This gives Bridge access to that DiveLine user list. The target DiveLine authorizes Bridge to authenticate users by listing the Bridge's machine in the **Authorized DivePort Gateways** list under the **General** tab for Workbench **Server Settings**.



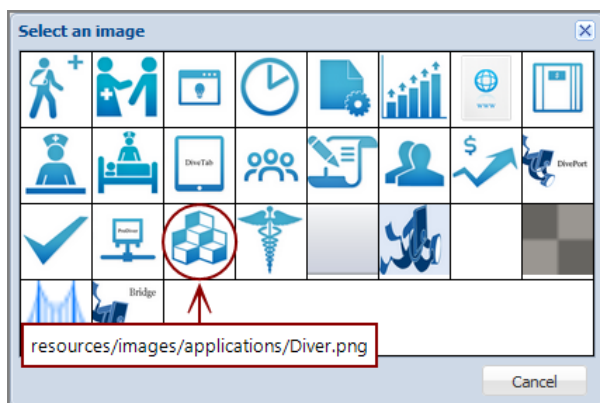
The DiveLine attribute is required for single sign-on (SSO) to DI applications from Bridge.

**TIP:** If no DiveLine is specified, a secondary logon displays. A secondary logon also displays when there is no match on the user.

- **Admin Username**—Used to control the button display for sites that use DiveLine. If a DiveLine administrator is specified for the target portal, only users in that DiveLine see the target button. If no Admin Username is specified, all visitors to Bridge see the destination as an option, even if they have no credentials. The target DiveLine must authorize Bridge to authenticate users.

**NOTE:** There is a time delay between the saving of the configuration settings and the actual application of those settings in the Bridge instance. Keep this in mind when you are trying to verify that users are seeing the appropriate buttons.

- **Image URL**—Points to a graphic file for the button. The browse button opens a dialog showing thumbnails of all images that came with Bridge or were installed in the `<bridge>/customizations/images` directory under Bridge's webdata directory. Contents of the `customizations/images` directory appear as part of the resources directory. If no image is specified, a blank box appears instead. For example:



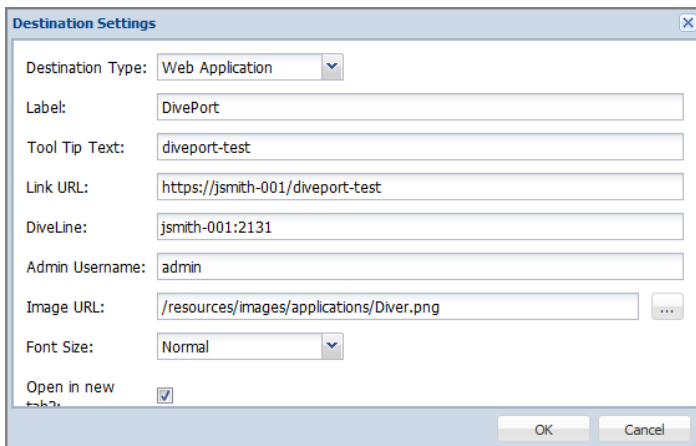
The circled icon was installed with the application.

You can also provide a full URL. For example, `https://jsmith-001:3330/bridge-test/resources/images/Diver.png`

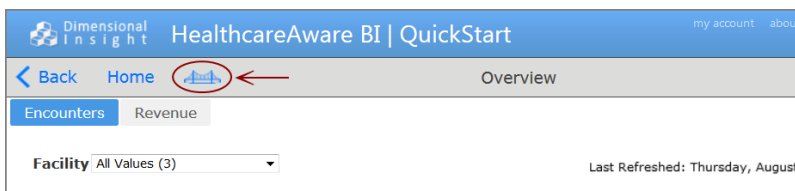
- **Font Size**—Indicates Normal (17 pixels) or Small (12 pixels) for the label text.
  - **Open in new tab**—Indicates how the target should open in the browser. When selected, the target opens in a new browser tab; when cleared, the target opens in the current tab.
4. Click **OK** to save the destination.

The dialog box closes.

Here is an example of Web Application destination to DivePort.



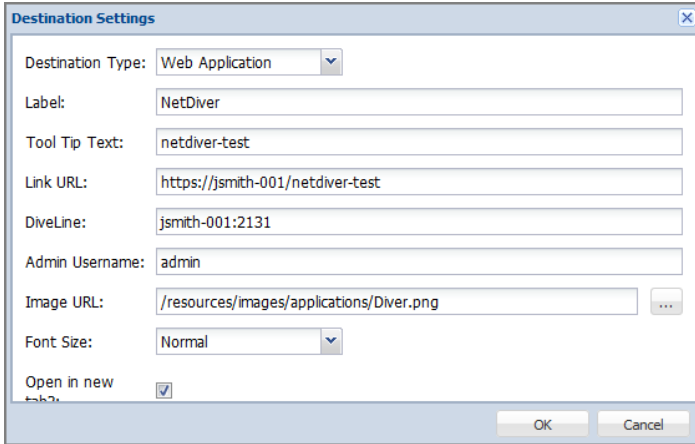
When configuring older DivePorts, take note of the fact that any DivePort or secondary Bridge opened in the same tab as the starting Bridge displays a **bridge icon** in the tool bar only if it is using the Simplified User Interface (SUI). The SUI option was first available with version 6.4. The icon is interactive, changing into a hand when selected, behaving like the **Home** and **Back** buttons.



**TIP:** Older DivePort portals, or current ones not using the SUI, should be configured to open in a new tab, so the end user can return to Bridge by selecting the starting tab, since the bridge icon will not be available.

Here is an example of Web Application destination to NetDiver.

## Diver Platform 7.2

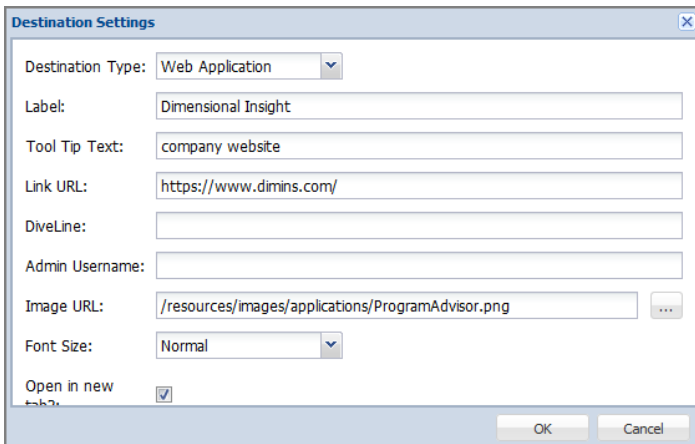


The image shows a 'Destination Settings' dialog box with the following fields and values:

- Destination Type: Web Application
- Label: NetDiver
- Tool Tip Text: netdiver-test
- Link URL: https://jsmith-001/netdiver-test
- DiveLine: jsmith-001:2131
- Admin Username: admin
- Image URL: /resources/images/applications/Diver.png
- Font Size: Normal
- Open in new tab:

Buttons: OK, Cancel

Here is an example of Web Application destination to a website.



The image shows a 'Destination Settings' dialog box with the following fields and values:

- Destination Type: Web Application
- Label: Dimensional Insight
- Tool Tip Text: company website
- Link URL: https://www.dimins.com/
- DiveLine: (empty)
- Admin Username: (empty)
- Image URL: /resources/images/applications/ProgramAdvisor.png
- Font Size: Normal
- Open in new tab:

Buttons: OK, Cancel

Here is an example of a ProDiver destination.

The screenshot shows a dialog box titled "Destination Settings" with the following fields:

- Destination Type: ProDiver (dropdown menu)
- Label: ProDiver (text input)
- Tool Tip Text: ProDiver (text input)
- Project name: (empty text input)
- File path: / (text input)
- DiveLine: jsmith-001:2131 (text input)
- Admin Username: admin (text input)
- Image URL: /resources/images/applications/Diver.png (text input with browse button)
- Font Size: Normal (dropdown menu)

Buttons: OK, Cancel

Here is an example of a DiveTab destination.

The screenshot shows a dialog box titled "Destination Settings" with the following fields:

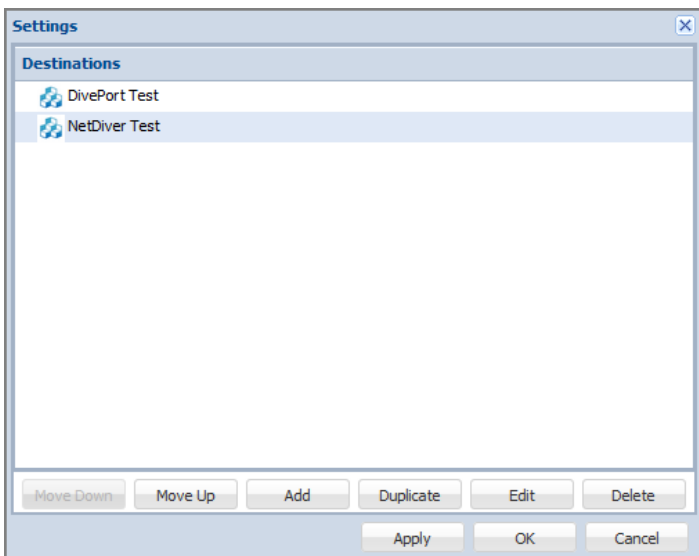
- Destination Type: DiveTab (dropdown menu)
- Label: Dive Tab (text input)
- Tool Tip Text: (empty text input)
- Link URL: https://jsmith-001:2131/divetab-test (text input)
- DiveLine: jsmith-001:2131 (text input)
- Admin Username: admin (text input)
- Image URL: /resources/images/applications/Diver.png (text input with browse button)
- Font Size: Normal (dropdown menu)

Buttons: OK, Cancel

## Reorganizing Buttons

Use **Admin > Destinations** to see the **Settings** dialog box with the currently defined buttons.

For example:



To reorder buttons:

1. Select a destination.
2. Click **Move Down** or **Move Up**.
3. Repeat as needed.
4. Click **OK** to see the new order presented in the portal.

### Making a Copy of a Destination

Use **Admin > Destinations** to make a copy of, or duplicate, an existing destination within the same Bridge. You still need to change the Link URL to be unique before committing the new destination. In the **Destination Settings** dialog box, do the following:

1. Select a destination.
2. Click **Duplicate**.
3. Change the **Link URL**. This cannot be the same as the existing destination, as the Link URL needs to be unique.
4. Make additional changes, as needed.
5. Click **OK** to see the duplicate destination listed under **Destinations**.

### Editing a Destination

To edit the settings for a destination, click **Edit** in the **Destination Settings** dialog box, or simply double-click the destination you want to edit. This opens the **Destination Settings** dialog box for that destination.



## Deleting a Destination

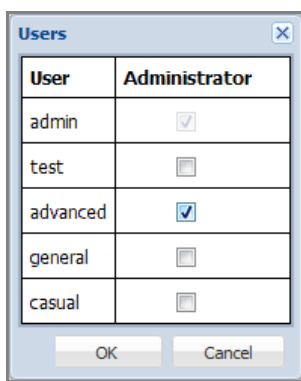
Use **Admin > Destinations** to delete an existing destination. In the **Destination Settings** dialog box, do the following:

1. Select a destination.
2. Click **Delete**.

The selected destination is removed.

## Configuring Users

Use **Admin > Users** to see all users for the Bridge instance listed in the **Users** dialog. This dialog is used to make someone an administrator for Bridge.



- **User**—This is a list of users from the DiveLine hosting Bridge.
- **Administrator**—A check mark indicates that the user can perform configuration tasks for Bridge. This includes adding and deleting sites and customizing the buttons.

Note that the administrative user used to access Bridge is listed, but the toggle box is disabled. In this example, the current user is “admin”.

### NOTES:

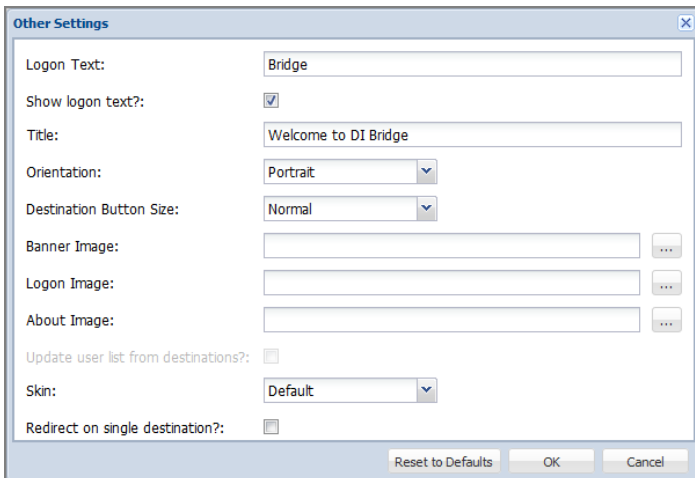
- All DiveLine administrators become Bridge administrators by default.
- Not all Bridge administrators are DiveLine administrators.

By default, the list of users is sorted alphabetically in ascending order by User. By clicking on either the User or the Administrator column, the list is sorted on that column, reversing the sort order from ascending to descending or descending to ascending. The sorting is case-insensitive.

## Configuring Other Settings

Use **Admin > Other Settings** to access the **Other Settings** dialog. This is where you can customize the general appearance of Bridge’s landing page and

subpages.



- **Logon Text**—Specifies a string for the browser tab.
- **Show logon text?**—Indicates that the Logon Text displays in the middle of the logon page.
- **Title**—Specifies the name to appear in the banner area of the landing page.
- **Orientation**—Allows you to select Portrait or Landscape for all the buttons. The image is smaller in Landscape (90 x 90 px) than in Portrait (100 x 100 px) orientation, but more text fits on each line in Landscape.
- **Destination Button Size**—For the button size, you can select Normal or Large. Images are scaled as follows:
  - Normal/Portrait: 100 x 100 pixels
  - Normal/Landscape: 90 x 90 pixels
  - Large/Portrait: 200 x 200 pixels
  - Large/Landscape: 180 x 180 pixels
- **Banner Image**—Specifies the path to the graphic file to be used for the page heading. There is no default. Whatever is used is scaled to a maximum height of 44 pixels to avoid impacting the title bar layout.
- **Logon Image**—Specifies the path to a graphic file to be used for the logon page. There is no default. As for all other images, the browse button opens a dialog showing thumbnails of all images that came with Bridge or were installed in the `<bridge>/customization-templates/images` directory under Bridge's `webdata` directory.

- **About Image**—Specifies the path to a custom graphic file to be used for the About dialog if you want to customize it. The default is `resources/images/about-art.png`, which is 282 x 241 pixels. The About Dialog's layout is set up to show version text just below the "Bridge" text in the image.
- **Update user list from destinations?**—When this option is checked, each time it updates its user information from its destinations, Bridge adds any user names that exist in any destination, but not in the Bridge's DiveLine, to its own DiveLine. No other information is added besides the user name. The option defaults to unchecked. Note that this option is disabled when the Bridge DiveLine uses **Own** authentication. This option enables **Admin > Update User Lists**.
- **Redirect on single destination?**—When this option is checked, and there is only one destination visible to a non-admin user, when the user logs on to Bridge, Bridge automatically redirects to that destination. If this is a web site, it opens in the same tab; if it is DivePort or Bridge, they do not show the Bridge icon that allows the user to return to the previous Bridge page. Administrative users do not get redirected.
- **Skin**—Lists skins included with Bridge and skins in the `webdata/bridge/customizations/skins` directory. Change the skin and click **OK** to reload the page. The new skin takes effect.

**NOTE:** Although Bridge uses some of the same skin entries as DivePort, it also uses some different skin entries, due to the differences between the user interfaces.

The **Reset to Defaults** restores the default settings, which are:

- Logon Text: **Bridge**
- **Show logon text** is selected
- Title: **Welcome to DI Bridge**
- Orientation: **Portrait**
- Destination Button Size: **Normal**
- Skin: **Default**

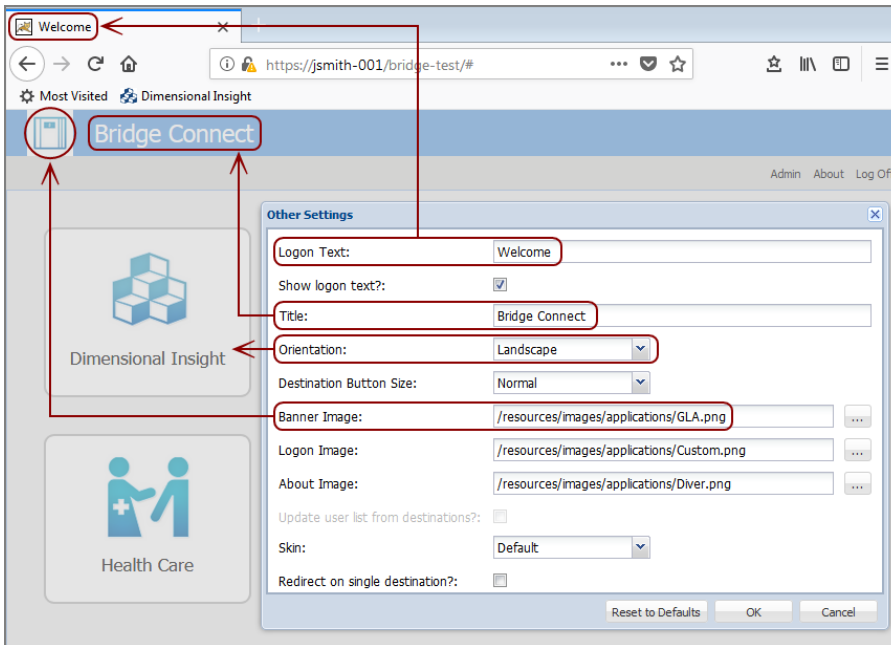
All other fields are empty.

The **Other Settings** dialog box below displays the following selects, among others: **Logon Text:** Welcome; **Title:** Bridge Connect; **Orientation:** Landscape; **Destination Button Size:** Normal; **Banner Image:**

`/resources/images/applications/GLA.png`.

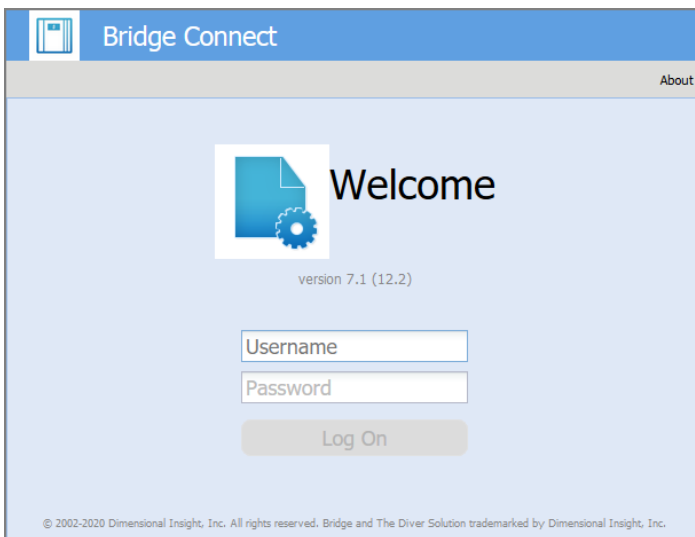
Here is an example of how these selections are applied.

## Diver Platform 7.2

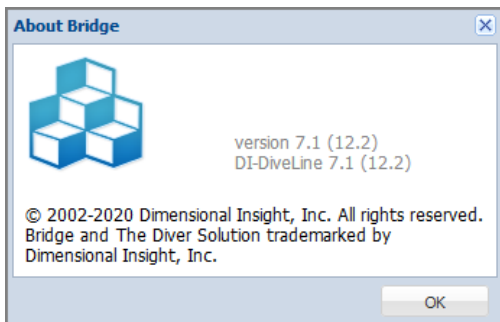


If the **Show logon text?** option is selected, the **Logon Text** appears on the log on screen. If the check box is empty, the **Logon Text** does not appear.

Here is an example of a log on screen with the **Show logon text?** check box empty, and with the **Title** and **Logon Image**.

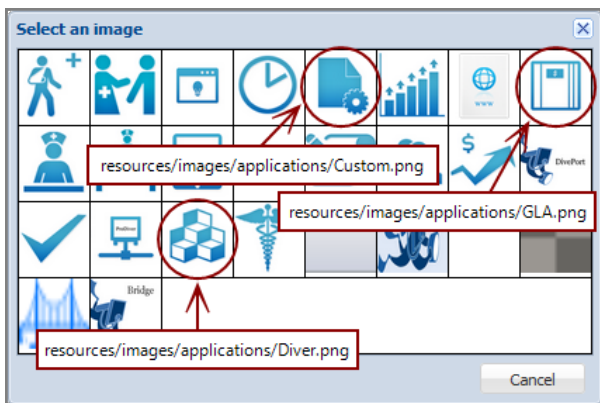


Finally, the **About Bridge** popup is displayed as follows, with **About Image**:  
`/resources/images/applications/Diver.png`.



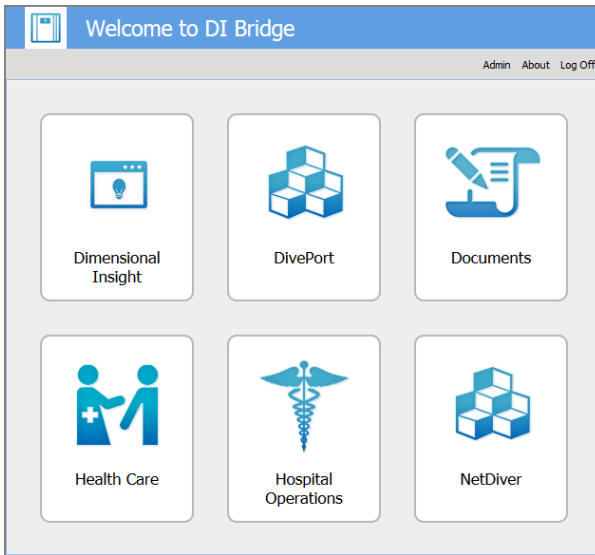
The **Select an Image** dialog below shows the image selections that were made in the above example:

- **Banner Image**—/resources/images/applications/GLA.png
- **Logon Image**—/resources/images/applications/Custom.png
- **About Image**—/resources/images/applications/Diver.png

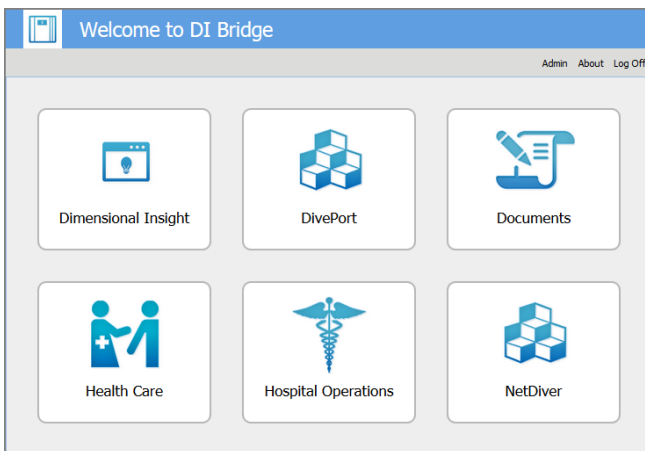


Here is an example of the same set of buttons with **Portrait** and **Landscape** orientation.

Portrait:



Landscape:



## Custom Graphics

A library of image files is delivered as part of the application. These resources are available whenever you use the browse button to configure an image file as described in [Configuration Options on page 105](#).

You can extend this resource to include your own set of files. The graphics are stored in the following directory:

```
DI/Solution/webdata/<bridge>/customizations/images/
```

The images supplied with the Bridge installation adhere to the following guidelines:

Image	Default	Size	Notes
Button	diver.png	100 x 100 px 90 x 90 px	For best results, make sure there is space around the graphic in the Image. At least 15 pixels is recommended.  The portrait orientation displays 100 x 100 px, while the landscape displays scales down to 90 x 90 px.  The application resource colors: #3ca4c6 to #1479bd, gradient; #1d83bf, solid.
Banner	none	no default	Whatever is used is scaled to a maximum height of 44 pixels. The CSS property #bridge-titlebar sets the background color of the banner as #5f9fe1.
Logon	logon-art.png	171 x 75 px	Background color: #dfe8f6 or transparent. You can use any graphic, but if the background color of the image is #dfe8f6, it blends in with the page background.
About	about-art.png	282 x 241 px	Background color: #ffffff Make sure the background color is white. Version text is shown just below the "Bridge" text in this image.

In general, the *png* format is recommended, although the Images dialog box looks for *png*, *jpg*, *gif*, and *bmp* file types.

There is some flexibility in the sizes, so run tests to see how your images display. Larger images are scaled down when needed and can result in a loss of quality.

## User Access

Once you have configured Bridge buttons for your users, you can share the URL. Things to note:

- Only Administrative users see the **Admin** button below the banner.
- Password maintenance options depend on the authentication type and server configuration.

## Diver Platform 7.2

- If a user is required to change their password during the initial logon, either to Bridge or to a linked DivePort or NetDiver, a **Change Password** dialog box opens. If the dialog box is canceled, the user is logged out automatically. If the password is changed successfully, the user is logged on and the password on DiveLine is updated.



# Appendix B: Help Desk

Help Desk is used to perform maintenance tasks for users on a DiveLine server. All features in Help Desk are also available in Workbench. You use Help Desk to delegate the basic DiveLine user maintenance chores to individuals who do not need access to project data.

**NOTE:** Help Desk requires a separate license.

## Installing Help Desk

Help Desk allows for users without Developer licenses to edit groups and users.

**NOTE:** You need to be an administrative user to install the software.

To install Help Desk:

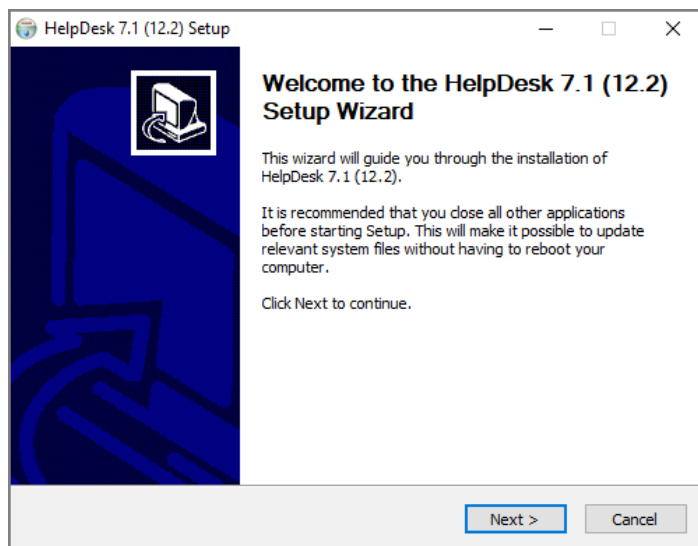
1. Navigate to the `DI\Solution\downloads` directory where you downloaded the developer package.
2. Double-click the **HelpDesk-Setup.exe** file.

The **User Account Control** dialog box opens, asking you to confirm making changes to your device.

**NOTE:** Depending on your Windows version and user account settings, you might see the **Open File - Security Warning** dialog box instead. Confirm that you want to open and run the executable.

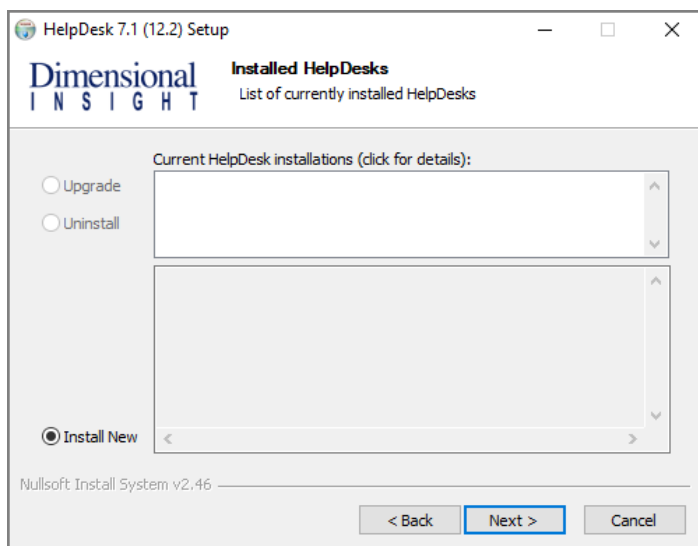
3. Click **Yes**.

The **HelpDesk <version number> Setup Wizard** dialog box opens.



4. Click **Next**.

The **Installed HelpDesks** page opens.



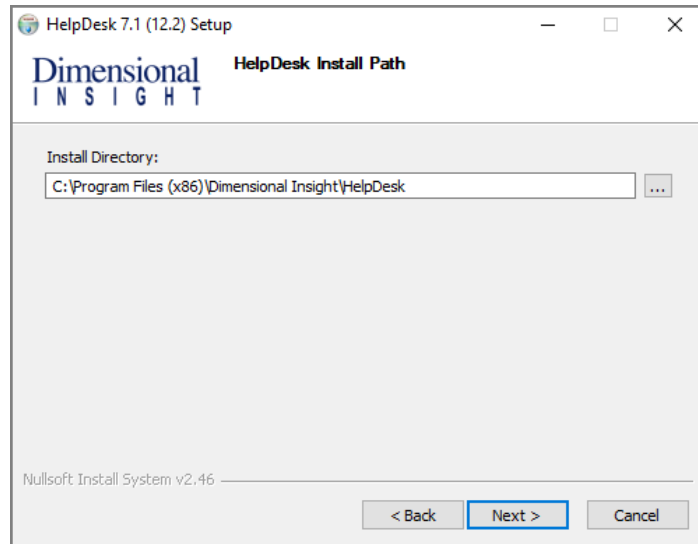
5. Select one of the following:

- Upgrade
- Uninstall
- Install New

Each option guides you through the required steps. This example uses **Install New**.

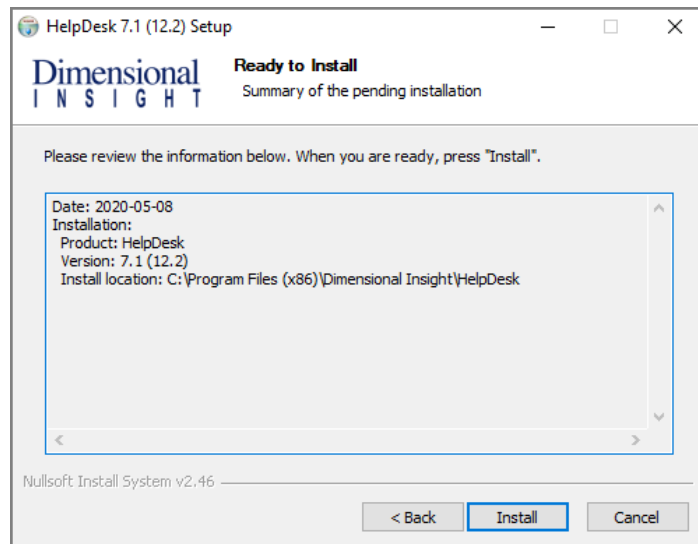
6. Click **Next**.

The **HelpDesk Install Path** page opens.



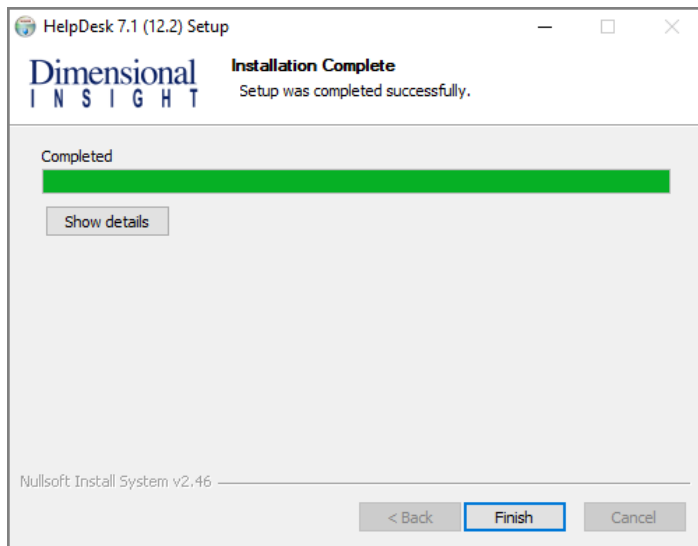
7. Verify the directory for Help Desk installation.
8. Click **Next**.

The **Ready to Install** page opens.



9. Verify the Help Desk installation information.
10. Click **Next**.

The **Installation** page opens, and displays **Installation Complete** once finished.

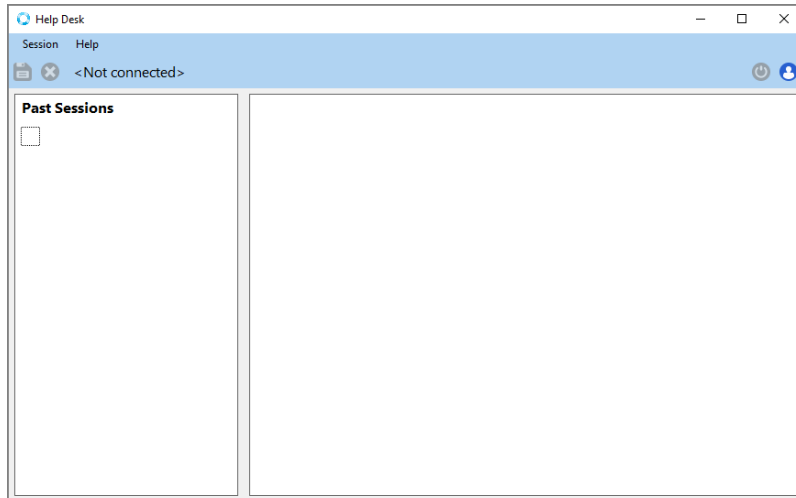


11. Click **Finish** to close the installation wizard.

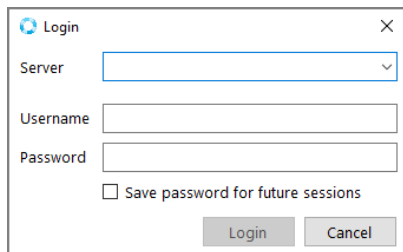
## Verifying the Help Desk Installation

To verify a successful implementation of Help Desk:

1. Open Help Desk from the Start menu.

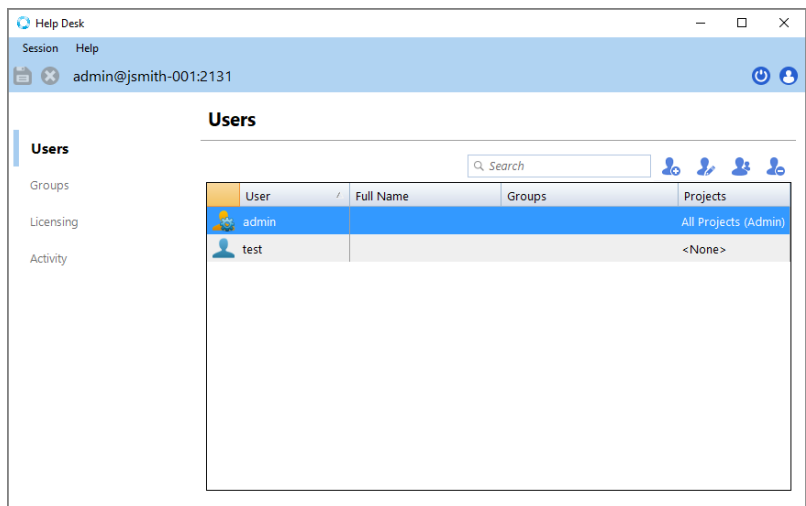


2. Select **Session > Connect**.  
The Login dialog box opens.



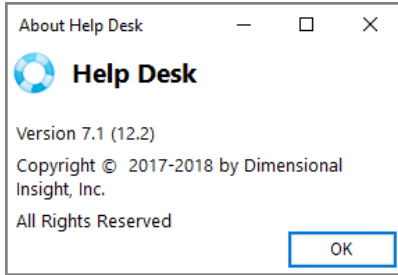
3. Do the following:
  - In the **Server** box, enter the server name. For example, *jsmith-001:2131*.
  - Enter the **Username** and **Password** for DiveLine.
  - Select **Save password for future sessions** if you want to save this information for later use.
4. Click **Login**.

A new session on Help Desk opens.

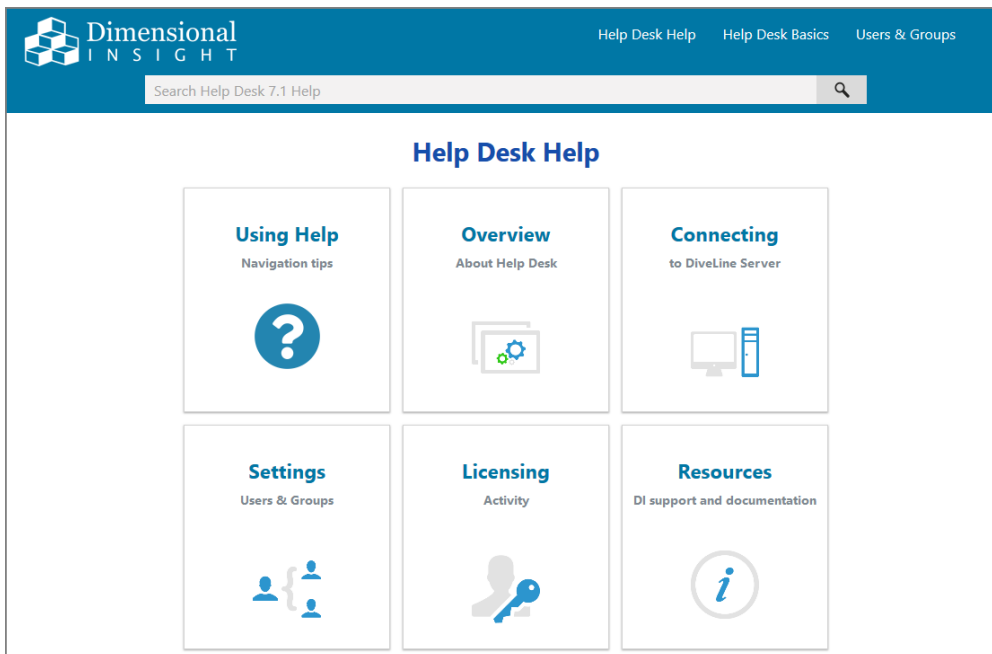


5. Click **Help > About** to view the **Help Desk** version number.

## Diver Platform 7.2



6. Click **Help** > **View Help**, to view the Help documentation in a browser window.



# Appendix C: DiveLine Authentication Options

DiveLine supports four different user authentication options. As a DiveLine administrator, choose the best type for your network environment.

- **Own**—Uses DiveLine's internal username and password list maintained using Workbench or Help Desk.
- **System**—Uses the DiveLine server's UNIX operating system user account credentials for authentication.
- **Web Server**—Uses the user information maintained by the web server to authenticate users.
- **LDAP**—Uses a Lightweight Directory Access Protocol server to request credentials and authenticate users.
- **OIDC**—Uses OpenID Connect to authenticate credentials using a third-party identity provider.

**NOTE:** All authentication types require that DiveLine users are defined in Workbench Server Settings.

## Own Authentication

Own authentication maintains user information entirely within Workbench. You can create users and passwords, and assign security and licensing levels within Workbench, and it functions independently of any other security on the system. You do not need to create operating system user accounts on the server itself because user accounts are maintained entirely within the DiveLine through Workbench. When creating users in Workbench for use with Own authentication, a password is required; blank passwords are not allowed. All user passwords are *hashed* within the application using the *scrypt* algorithm.

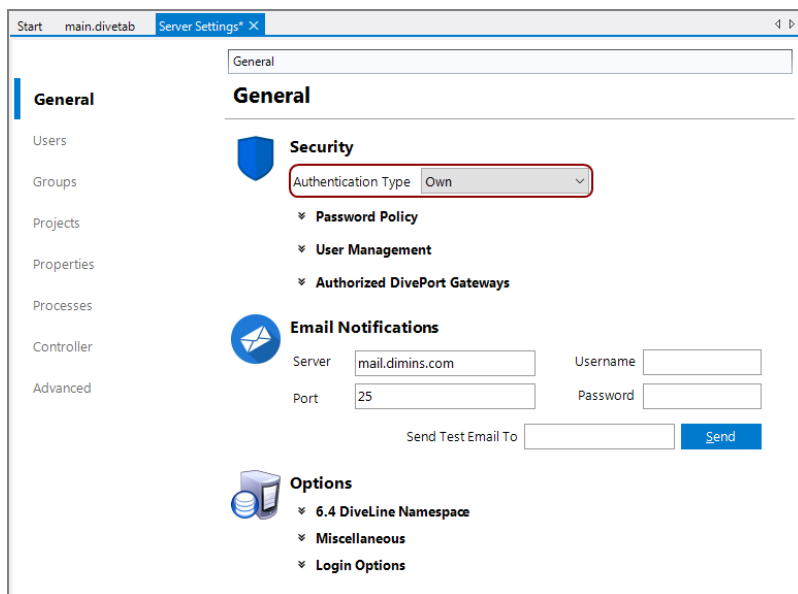
Note that most enterprise implementations of Diver Platform do not use Own Authentication because of the need to maintain separate passwords. Using LDAP, System, or Web Server authentication type supports working with an existing authentication system, such as Active Directory.

## Configuring Own Authentication

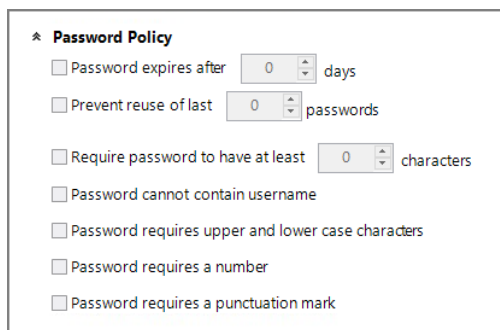
Setting Own authentication type allows you to maintain DiveLine user information entirely within Workbench. For more information, see [Own Authentication above](#).

To configure Own authentication:

1. Open **Workbench** and open a DiveLine connection.
2. Select **Tools > Server Settings > General**.
3. In the **Security** section, select **Own** from the **Authentication Type** pull-down menu.



4. Click the chevron next to **Password Policy**.  
The Password Policy options display.



The Password Policy options allow you to specify and enforce criteria for creating and maintaining strong user passwords that comply with your company's security guidelines.

**NOTE:** Password Policy options are specific to Own authentication type.

5. Specify the password options:



- **Password expires after “x” days**—Sets the number of days after which passwords expire. This allows a user to change an expired password, regardless of whether or not password changing has been allowed on the user's profile. Individual users can be exempted from mandatory password expiration by selecting the **Password never expires** check box on their user profile Security/Licensing settings. Not selecting this option results in the password not expiring.
- **Prevent re-use of last “x” passwords**—Sets the number of previously used passwords that cannot be re-used. Not selecting this option, or entering "0", disables the feature, allowing users to reuse the same password repeatedly.
- **Require passwords to have at least “x” characters**—Sets the required number of characters for a user password. Not selecting this option, or entering "0", disables the minimum requirement setting.
- **Password cannot contain username**—Prevents using part or all of the username in the password.
- **Password requires upper and lower case characters**—Requires using both upper and lower case characters as part of the user password.
- **Password requires a number**—Requires using a number as part of the password.
- **Password requires a punctuation mark**—Requires using a punctuation mark, such as an exclamation point or comma, as part of the password.

**NOTE:** The DiveLine server-level password settings interact with settings on individual user accounts. For example:

- If you select **Password expires after X days**, users can change an expired password regardless of whether the User cannot change password option is selected for their user accounts.
- If you select **Password never expires** in their user account, you exempt an individual user from mandatory password expiration.

6. **Save** the Server Settings, using **File > Save** or **Ctrl+S**.

## System Authentication

System authentication uses the DiveLine server's UNIX operating system user database for authentication. It is available only on supported UNIX platforms. This is a convenient way to handle password authentication without maintaining a separate password list. However, you do need to define your users within

Workbench, and the account user name must exactly match the user name in the server's user database.

For System authentication, you do not need to assign passwords in Workbench; any password specified in Workbench is ignored.

On UNIX, System authentication uses Pluggable Authentication Modules (PAM) if it is available. This means it is possible to use system passwords without running DiveLine as the root. It also enables the use of PAM's extensible mechanisms for authenticating to various sources. By default, DiveLine accepts passwords that work for normal, non-super user (non-su) logons on the machine. Additional customization of PAM for DiveLine can be used by modifying the PAM configuration for the *diveline.exe* file. Specify *auth* entries as desired.

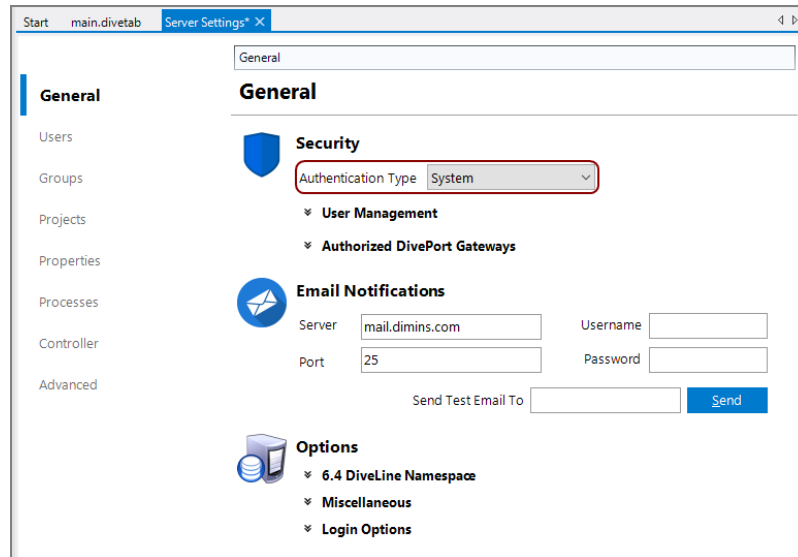
On Linux, System authentication supports PAM-based authentication and account management for authorization. Linux also supports implementing freeIPA, which allows for Host-based Access Control rules, as long as *pam\_acct\_mgmt* is called.

## Configuring System Authentication

System authentication type uses the server's user database for DiveLine authentication, and is only available for supported UNIX platforms. For more information, see [System Authentication on the previous page](#).

To configure System authentication:

1. Open **Workbench** and open a DiveLine connection.
2. Select **Tools > Server Settings > General**.
3. In the **Security** section, select **System** from the **Authentication Type** pull-down menu.



**NOTE:** There are no additional settings in Workbench for System authentication, but be sure to define users in Workbench or Help Desk.

4. **Save** the Server Settings, using **File > Save** or **Ctrl+S**.

## Web Server Authentication

Web Server authentication uses the user and password list already maintained by a Web Server. DiveLine includes a special script to communicate with the Web Server.

Web Servers respond to web requests from the local file system or execute local programs or scripts, and return the output of those programs to the browser that sent the query. DiveLine CGI (DLCGI) is such a program and is designed to allow the use of a Web Server to authenticate users and streamline maintenance of client start pages. Common Gateway Interface (CGI) programs are supported on Web Servers such as Microsoft Internet Information Server (IIS) and Apache HTTP Server. DLCGI allows users to log on and authenticate to the Web Server, and passes that logon information to DiveLine. DiveLine then takes the users configured in the Web Server, including Windows Domain users, for authentication. If multiple domains are involved, the Web Server authentication configuration needs to pass along the appropriate domain and username to DiveLine.

The result is a single sign-on with the Web Server, and the ability to maintain passwords outside of DiveLine. However, you must define your users within Workbench, and the user names in Workbench must exactly match the user names on the Web Server. Web Server authentication allows single sign-on access through ProDiver if using a Windows Domain or, if you launch ProDiver

from a DivePort using a *dllk* file. See also [Implementing SSO on Linux on page 167](#).

There are two main tasks for setting up Web Server authentication:

- [Configuring the Web Server below](#)
- [Configuring Web Server Authentication on page 156](#)

See [Configuring DivePort for Web Server Authentication on page 158](#) for additional steps for DivePort.

## Configuring the Web Server

Configure the Web Server for DiveLine CGI (DLCGI) according to system-specific instructions.

- [Configuring IIS Windows 10 / Server 2016 / Server 2019 below](#)
- [Configuring IIS Windows 8 / Server 2012 on page 142](#)
- [Configuring IIS Windows 7 / Server 2008 on page 146](#)

After the Web Server is configured, proceed to [Configuring Web Server Authentication on page 156](#).

## Configuring IIS Windows 10 / Server 2016 / Server 2019

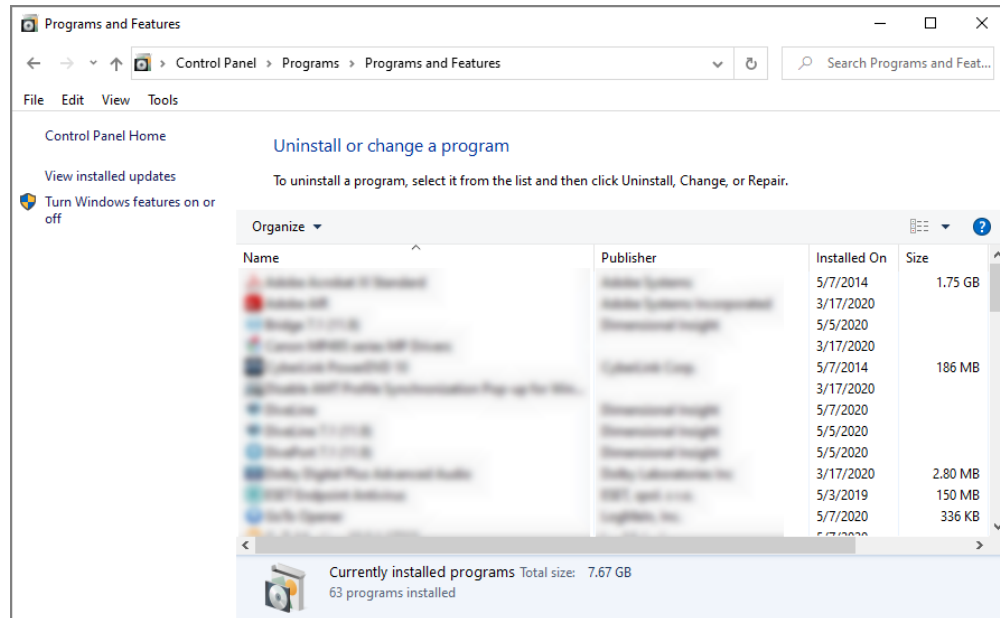
Microsoft's Internet Information Services (IIS) or Internet Information Server, is a Web Server for use with Windows NT. IIS is not turned on by default when Windows is installed and can be accessed through the Microsoft Management Console or Administrative Tools in the Control Panel. This section applies to IIS 10.0 which comes standard in Windows 10, Server 2016 and Server 2019. These steps might not be exact—refer to the latest Microsoft documentation.

To verify the IIS installation:

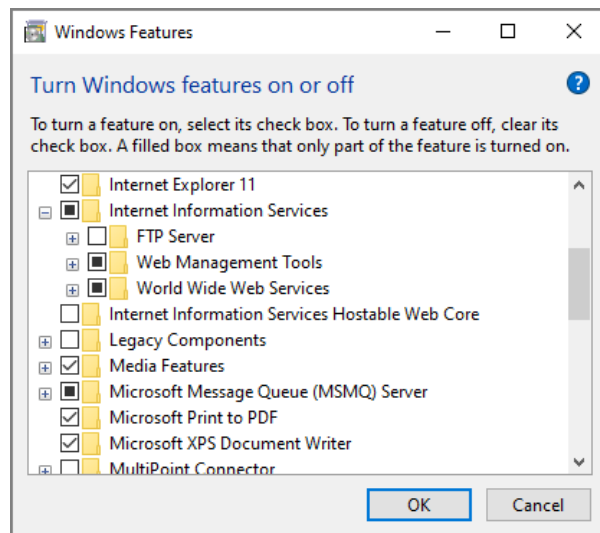
1. Navigate to `Control Panel\Programs\Programs and Features`.

**NOTE:** There are multiple ways to navigate the Windows operating system. This method uses a path in the Windows Explorer.

The **Programs and Features** window opens.



- On the left column, click **Turn Windows Features on or off.**  
The **Windows Features** window opens.



- Expand **Internet Information Services.**
- Select your options. The ones listed below are required.
  - Web Management Tools > IIS Management Console**
  - World Wide Web Services > Application Development Features**

> **CGI**

- **World Wide Web Services > Security > Windows Authentication**

5. Click **OK**.

The dialog box closes.

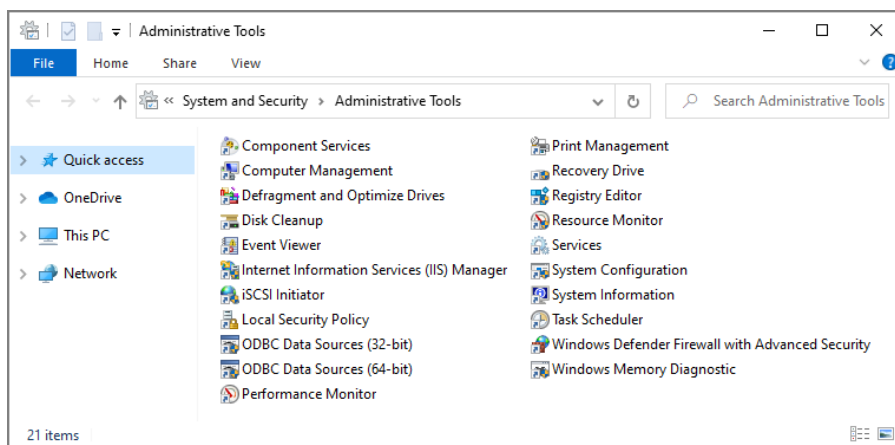
**NOTE:** You might need to restart your computer for these features to take effect.

To create a virtual directory and set the needed permissions to allow DLCGI to run:

1. Navigate to Control Panel\System and Security\Administrative Tools.

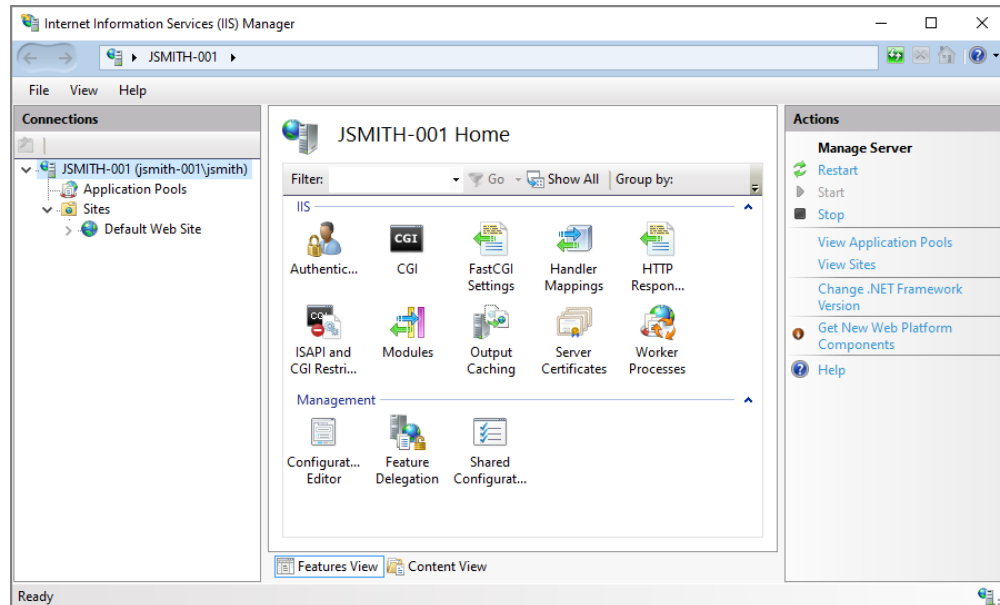
**NOTE:** There are multiple ways to navigate the Windows operating system. This method uses a path in the Windows Explorer.

The **Administrative Tools** window opens.

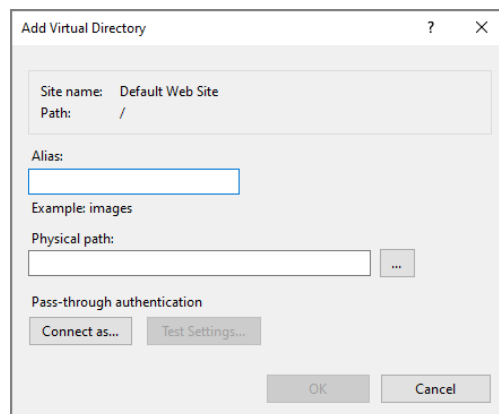


2. Click **Internet Information Services (IIS)**.

The **Internet Information Services (IIS) Manager** opens.

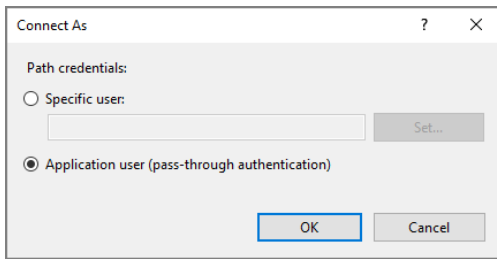


3. On the **Connections** pane on the left, expand the local computer and **Sites**.  
The **Default Web Site** displays.
4. Right-click **Default Web Site** and select **Add Virtual Directory** from the menu.  
The **Add Virtual Directory** dialog box opens.

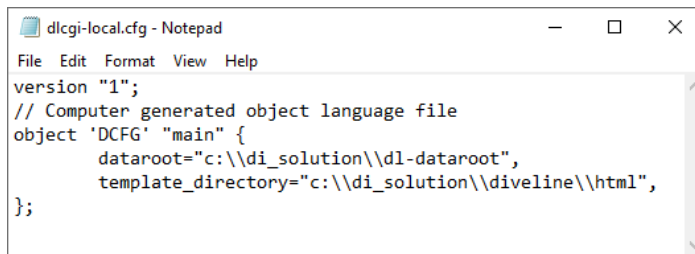


5. For the **Alias**, enter **cgi-bin** and for the **Physical Path**, browse for the path to the *dlcgi.exe* file. The default path is `C:\DI\Solution\diveline\cgi-bin`.
6. Click **Connect as**.

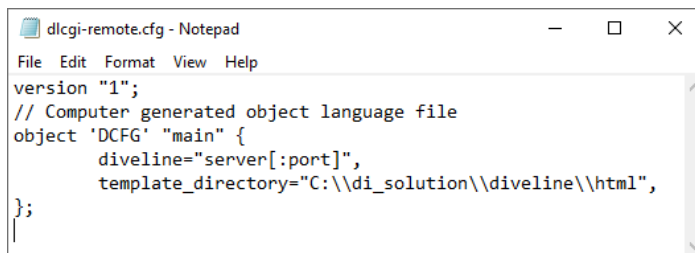
The **Connect As** dialog box opens.



7. Select the **Specific User** radio button, **Set**, fill in the credentials for the user account running DiveLine, and click **OK**.
8. Do one of the following:
  - If DiveLine and the Web Server are on the same machine, copy the `\diveline\install-files\dlcgi-local.cfg` file to the `diveline\cgi-bin` directory.



- If DiveLine and the Web Server are on different machines, copy the `\diveline\install-files\dlcgi-remote.cfg` file to the `diveline\cgi-bin` directory.

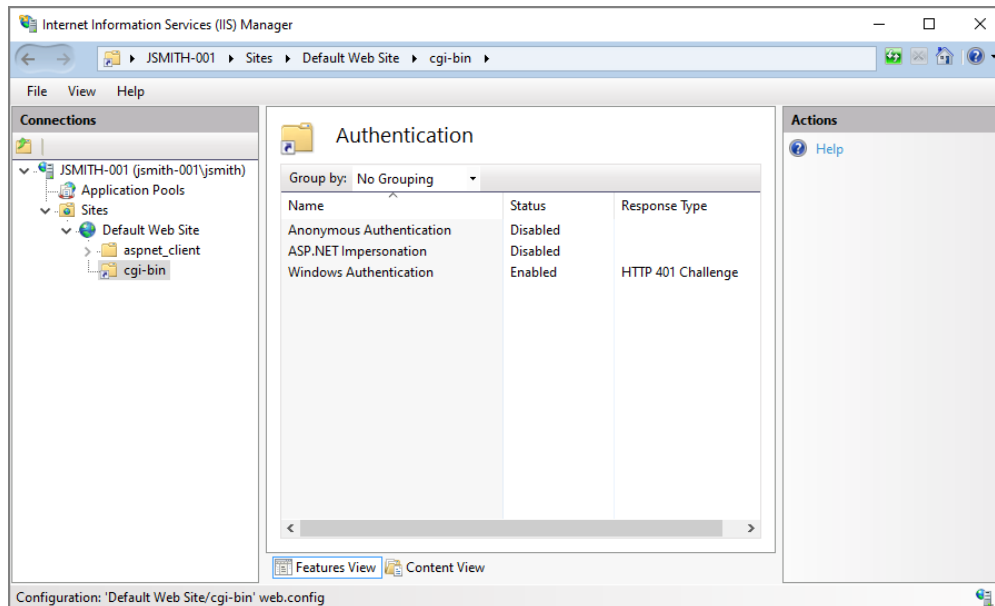


9. Rename the copied `cfg` file to `dlcgi.cfg` and open the file to verify the `d1-dataroot` directory path, or the server and port number.

**NOTE:** Repeat Step 1 to 8 for each virtual directory.

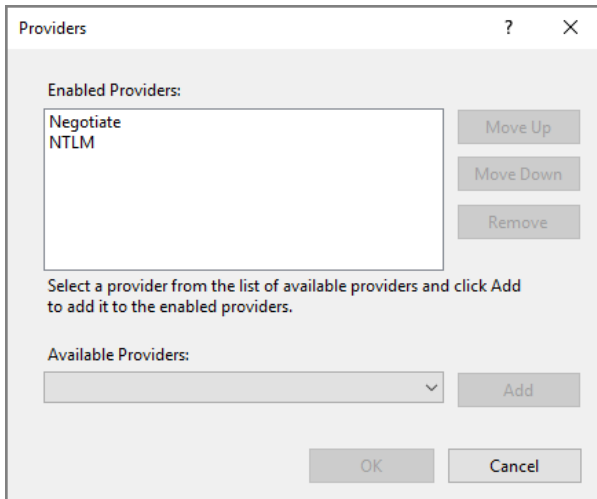


- To set permissions, select the virtual directory after creating it.
- On the center pane, double-click **Authentication**.  
The Authentication options open.

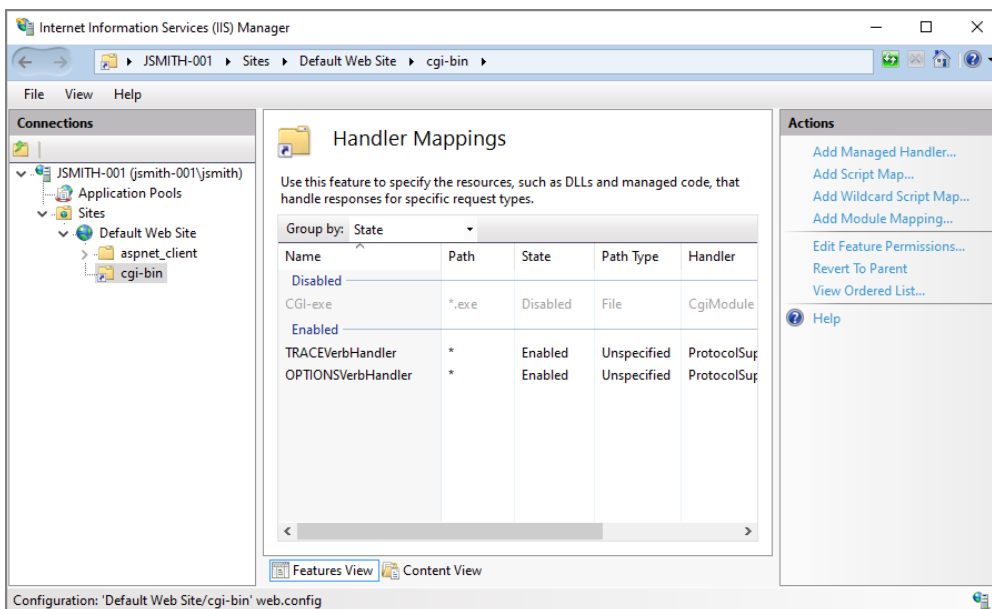


- Disable all authentication methods except **Windows Authentication**.  
Enable Windows Authentication if it is disabled.
- Right-click **Windows Authentication**, and select **Providers** from the menu.

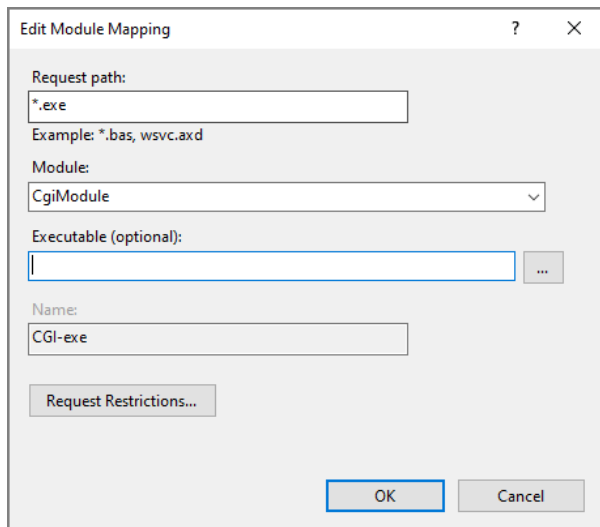
The **Providers** dialog box opens.



14. Remove **Negotiate** from the Enabled Providers and click **OK**.
15. Select the virtual directory again, and double-click **Handler Mappings**.  
The Handler Mappings options open.

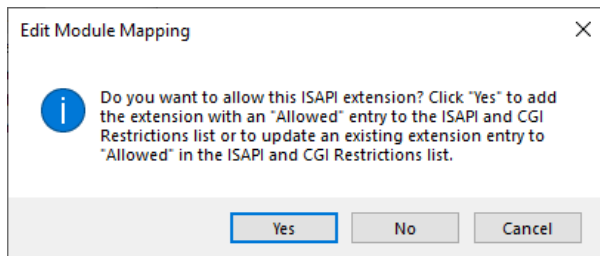


16. Double click **CGI-exe**.  
The **Edit Module Mapping** dialog box opens.

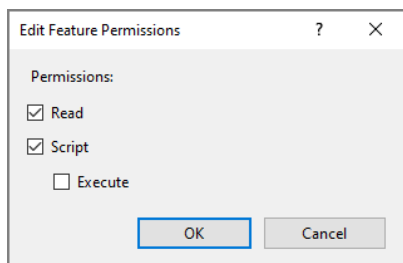


17. Click the browse button for the **Executable** box, and browse to the location of the *dlcgi.exe* file. The default value is `C:\DI\Solution\diveline\cgi-bin\dlcgi.exe`. If you cannot see the executable, select **exe** from the file type pull-down menu.
18. Click **OK**.

The **Edit Module Mapping** window opens.



19. Click **Yes** to accept the changes.  
The dialog box closes.
20. Right-click **CGI-exe**, and select **Edit Feature Permissions** from the menu.  
The **Edit Feature Permissions** dialog box opens.



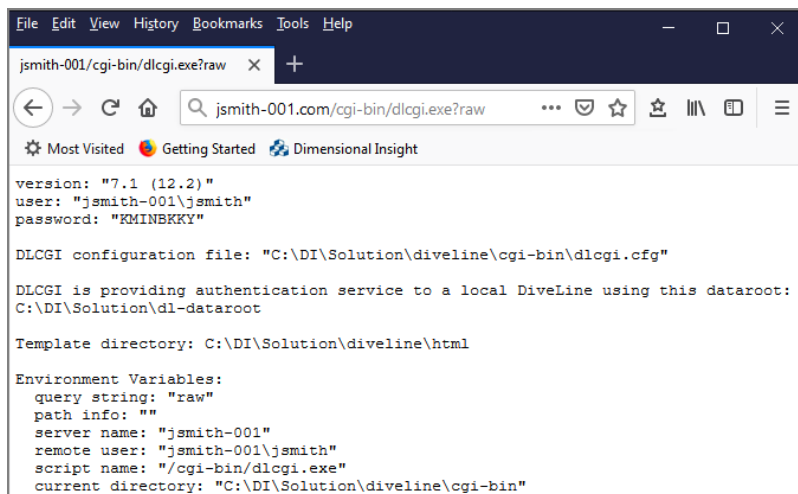
21. Select the **Read**, **Script**, and **Execute** check boxes, and click **OK**. This enables **CGI-exe**.

22. Test this configuration by running **dlcgi.exe?raw**:

Open a web browser and enter in *http://<servername>/cgi-bin/dlcgi.exe?raw*.

**NOTE:** This page might ask for a username and password. Use the server username. For this example, the username is *jsmith*.

Here is the resulting page:



IIS is now configured for DiveLine’s Web Server authentication under Windows 10.

## Configuring IIS Windows 8 / Server 2012

Microsoft’s Internet Information Services (IIS), or Internet Information Server, is a Web Server for use with Windows NT. IIS is not active by default when Windows is installed; the IIS Manager is accessed through the Microsoft Management Console or the Administrative Tools in the Control Panel. This section applies to IIS 8.0 which comes standard in Windows 8 and Server 2012. These steps might not be exact—refer to the latest Microsoft documentation.

To verify the IIS installation:

1. Navigate to `Control Panel\Programs\Programs and Features`.

**NOTE:** There are multiple ways to navigate the Windows operating system. This method uses a path in the Windows Explorer.

The **Programs and Features** window opens.

2. On the left column, click **Turn Windows Features on or off**.
3. Expand **Internet Information Services**.
4. Select your options. The ones listed below are required.
  - **Web Management Tools > IIS Management Console**
  - **World Wide Web Services > Application Development Features > CGI**
  - **World Wide Web Services > Security > Windows Authentication**
5. Click **OK**.

6. The dialog box closes.

**NOTE:** You might need to restart your computer for these features to take effect.

To create a virtual directory and set permissions to allow DL CGI to run:

1. Navigate to `Control Panel\System and Security\Administrative Tools`.

**NOTE:** There are multiple ways to navigate the Windows operating system. This method uses a path in the Windows Explorer.

2. Click **Internet Information Services (IIS)**.

The **Internet Information Services (IIS) Manager** opens.

3. On the **Connections** pane on the left, expand the local computer and **Sites**.

The **Default Web Site** displays.

4. Right-click **Default Web Site** and select **Add Virtual Directory** from the menu.

The **Add Virtual Directory** dialog box opens.

5. For the **Alias**, enter **cgi-bin** and for the **Physical Path**, browse for the path to the *dlcgi.exe* file. The default path is `C:\DI\Solution\diveline\cgi-bin`.
6. Click **Connect as**.

The **Connect As** dialog box opens.

7. Select **Specific User** and **Set**, fill in the credentials for the user account running DiveLine, and click **OK**.
8. Do one of the following:
  - If DiveLine and the Web Server are on the same machine, copy the `\diveline\install-files\dlcgi-local.cfg` file to the `diveline\cgi-bin` directory.

```

dlcgi-local.cfg - Notepad
File Edit Format View Help
version "1";
// Computer generated object language file
object 'DCFG' "main" {
    dataroot="c:\\di_solution\\dl-dataroot",
    template_directory="c:\\di_solution\\diveline\\html",
};
    
```

- If DiveLine and the Web Server are on different machines, copy the `\diveline\install-files\dlcgi-remote.cfg` file to the `diveline\cgi-bin` directory.

```

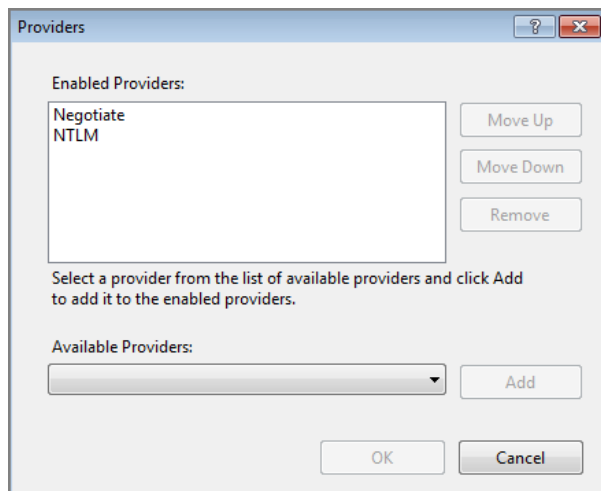
dlcgi-remote.cfg - Notepad
File Edit Format View Help
version "1";
// Computer generated object language file
object 'DCFG' "main" {
    diveline="server[:port]",
    template_directory="C:\\di_solution\\diveline\\html",
};
|
    
```

9. Rename the copied `cfg` file to `dlcgi.cfg` and open the file verify the `dl-dataroot` directory path, or the server and port number.

**NOTE:** Repeat Step 1 to 8 for each virtual directory.

10. To set permissions, select the virtual directory.
11. On the center pane, double-click **Authentication**.  
The Authentication options open.
12. Disable all authentication methods except **Windows Authentication**.  
Enable Windows Authentication if it is disabled.
13. Right-click **Windows Authentication**, and select **Providers** from the menu.

The **Providers** dialog box opens.



14. Remove **Negotiate** from the Enabled Providers and click **OK**.
15. Select the virtual directory again, double-click **Handler Mappings**, and double click **CGI-exe**.

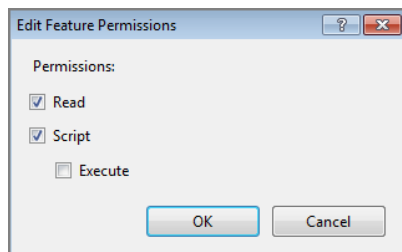
The **Edit Module Mapping** dialog box opens.

16. Click the browse button for the **Executable** box, and browse to the location of the *dlcgi.exe* file. The default value is `C:\DI\Solution\diveline\cgi-bin\dlcgi.exe`. If you cannot see the executable, select **exe** from the file type pull-down menu.
17. Click **OK**.

The dialog box closes.

18. Right-click **CGI-exe**, and select **Edit Feature Permissions** from the menu.

The Edit Feature Permissions dialog box opens.



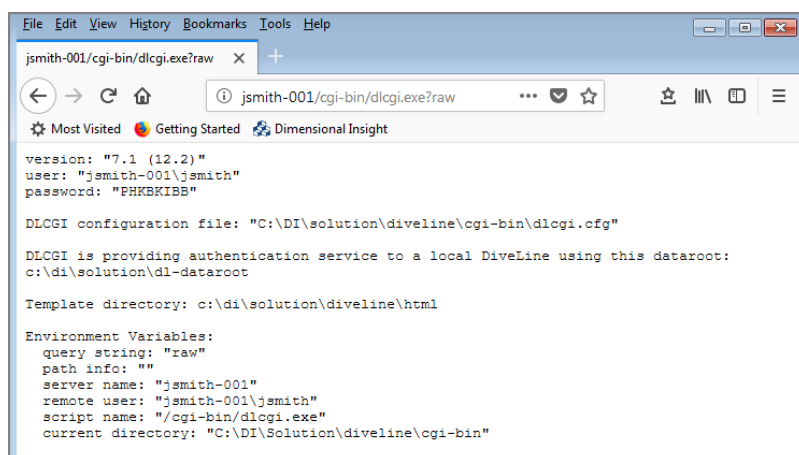
19. Select the **Read**, **Script**, and **Execute** check boxes, and click **OK**. This enables **CGI-exe**.

20. Test this configuration by running **dlcgi.exe?raw**:

Open a web browser and enter in *http://<servername>/cgi-bin/dlcgi.exe?raw*.

**NOTE:** This page might ask for a username and password. Use the server username. For this example, the username is *jsmith*.

Here is the resulting page:



IIS is now configured for DiveLine's Web Server authentication under Windows 8.

## Configuring IIS Windows 7 / Server 2008

Microsoft's Internet Information Services (IIS) or Internet Information Server, is a Web Server for use with Windows NT. IIS is not turned on by default when Windows is installed and can be accessed through the Microsoft Management Console or Administrative Tools in the Control Panel. This section applies to IIS 7.0 which comes standard in Windows 7 and Server 2008. These steps might not be exact—refer to the latest Microsoft documentation.

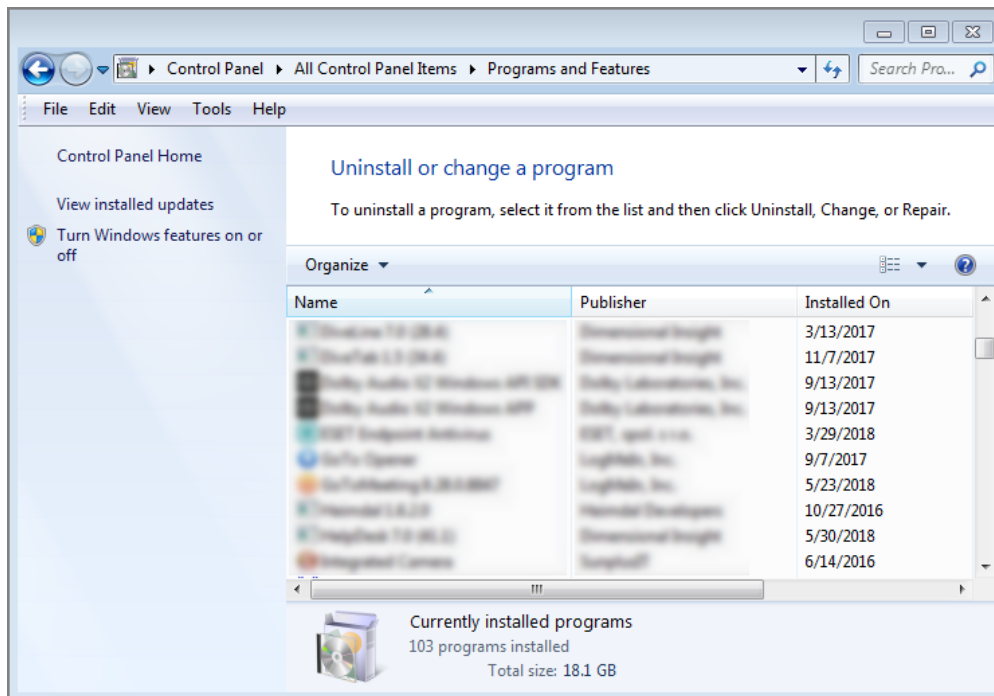
To verify the IIS installation:

1. Navigate to Control Panel\Programs\Programs and Features.

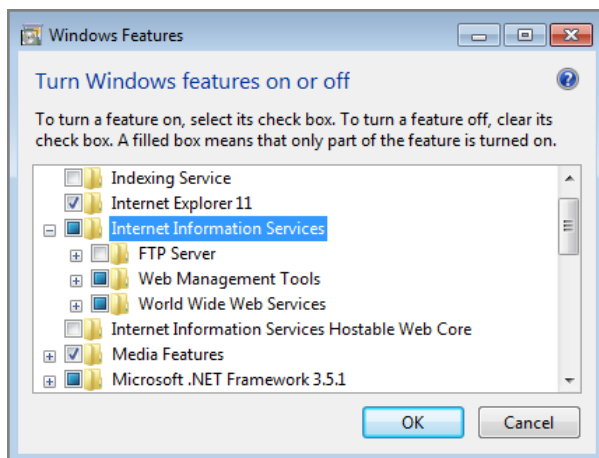
**NOTE:** There are multiple ways to navigate the Windows operating system. This method uses a path in the Windows Explorer.

The **Programs and Features** window opens.





2. On the left column, click **Turn Windows Features on or off**.  
The **Windows Features** window opens.
3. Expand **Internet Information Services**.



4. Select your options. The ones listed below are required.
  - **Web Management Tools > IIS Management Console**
  - **World Wide Web Services > Application Development Features**

> **CGI**

- **World Wide Web Services > Security > Windows Authentication**

5. Click **OK**.

The dialog box closes.

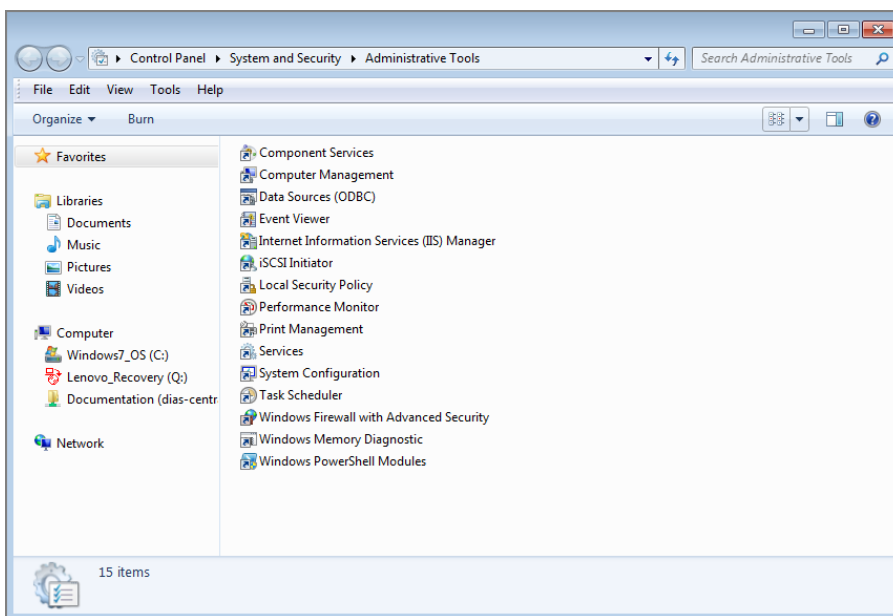
**NOTE:** You might need to restart your computer for these features to take effect.

To create a virtual directory:

1. Navigate to Control Panel\System and Security\Administrative Tools.

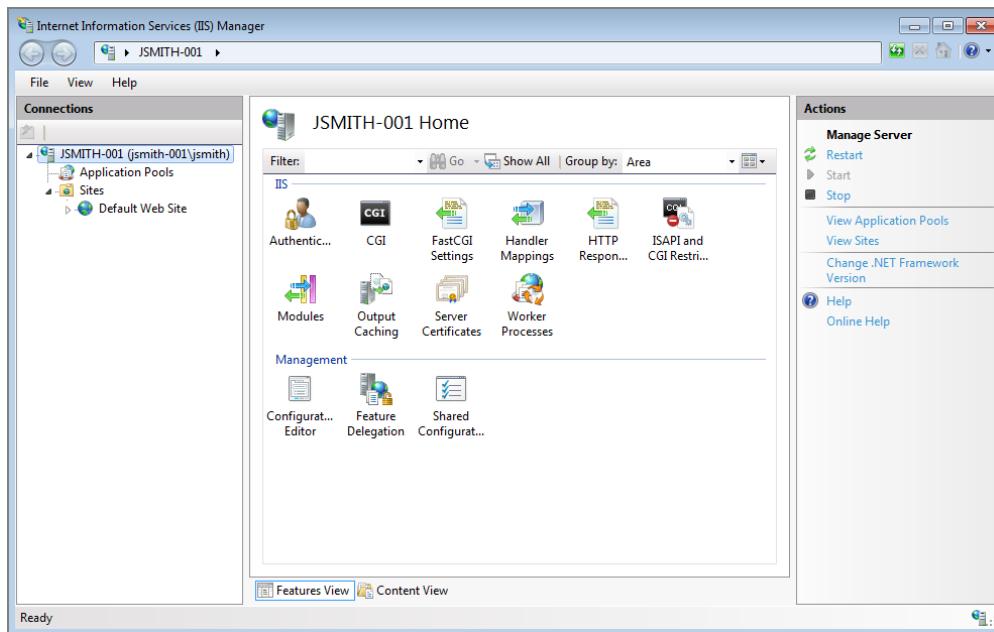
**NOTE:** There are multiple ways to navigate the Windows operating system. This method uses a path in the Windows Explorer.

The **Administrative Tools** window opens.

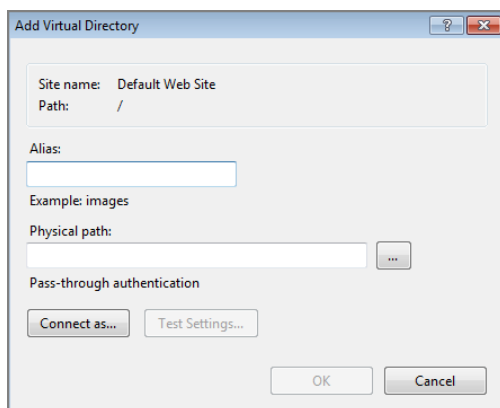


2. Click **Internet Information Services (IIS)**.

The **Internet Information Services (IIS) Manager** opens.

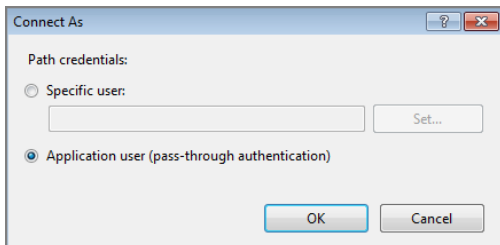


3. On the **Connections** pane on the left, expand the local computer and **Sites**.  
The **Default Web Site** displays.
4. Right-click **Default Web Site** and select **Add Virtual Directory** from the menu.  
The **Add Virtual Directory** dialog box opens.

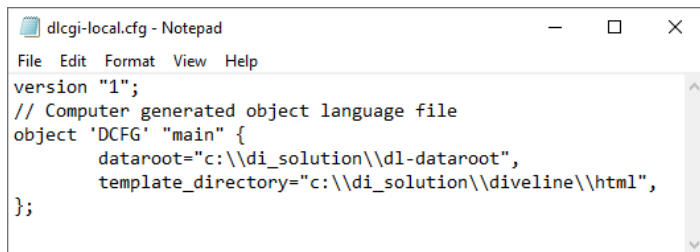


5. For the **Alias**, enter **cgi-bin** and for the **Physical Path**, browse for the path to the *dlcgi.exe* file. The default path is C:\DI\Solution\diveline\cgi-bin.
6. Click **Connect as**.

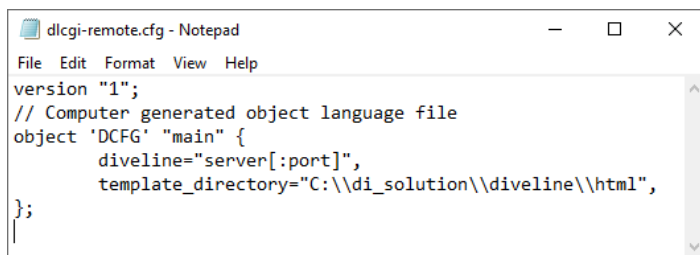
The **Connect As** dialog box opens.



7. Select the **Specific User** radio button, **Set**, fill in the credentials for the user account running DiveLine, and click **OK**.
8. Do one of the following:
  - If DiveLine and the Web Server are on the same machine, copy the `\diveline\install-files\dlcgi-local.cfg` file to the `diveline\cgi-bin` directory.



- If DiveLine and the Web Server are on different machines, copy the `\diveline\install-files\dlcgi-remote.cfg` file to the `diveline\cgi-bin` directory.



9. Rename the copied `cfg` file to `dlcgi.cfg` and open the file to verify the `dl-dataroot` directory path, or the server and port number.

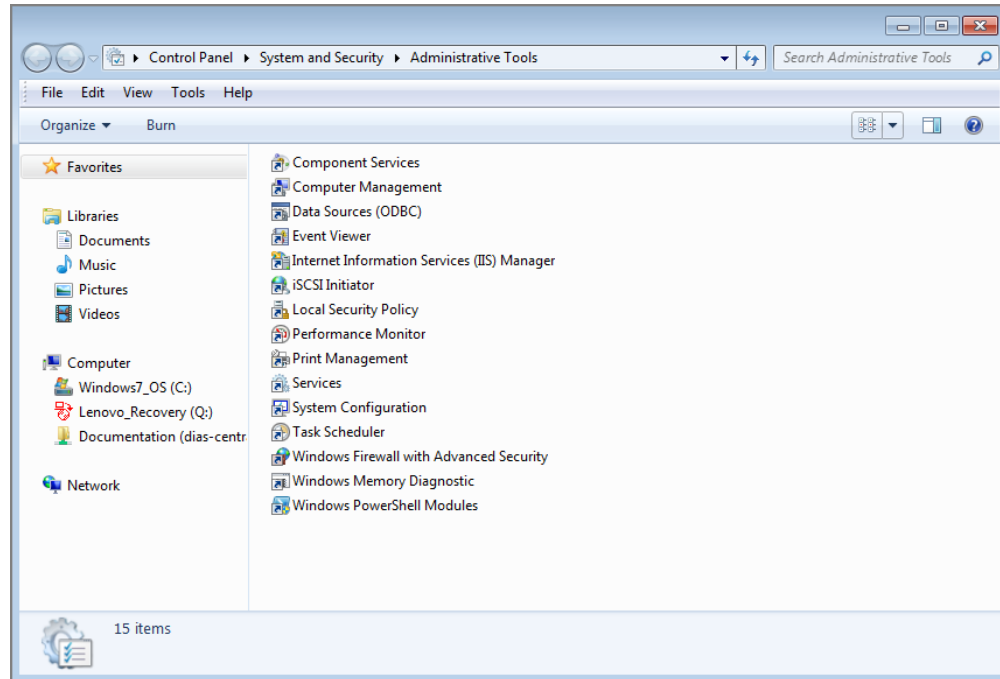
**NOTE:** Repeat Step 1 to 8 for each virtual directory.

To set the permissions to allow DL CGI to run:

1. Navigate to Control Panel\System and Security\Administrative Tools.

**NOTE:** There are multiple ways to navigate the Windows operating system. This method uses a path in the Windows Explorer.

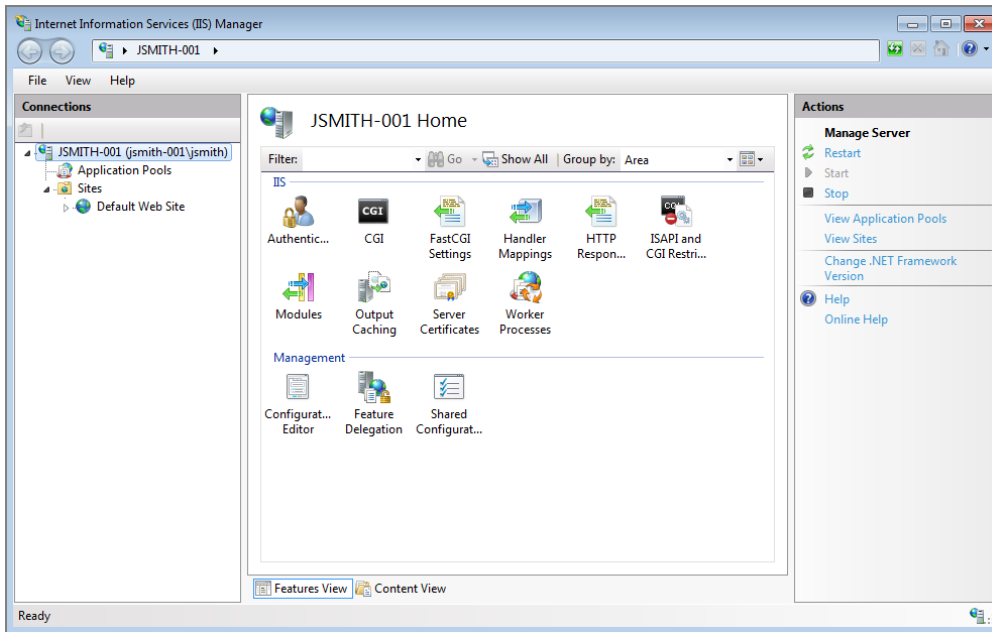
The **Administrative Tools** window opens.



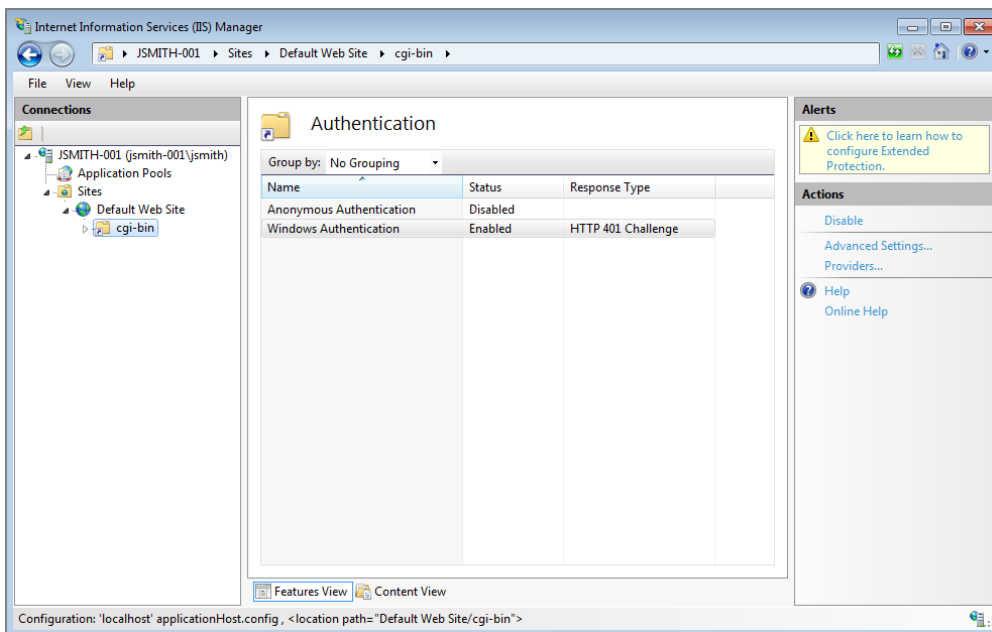
2. Click **Internet Information Services (IIS)**.

The **Internet Information Services (IIS) Manager** opens.

## Diver Platform 7.2



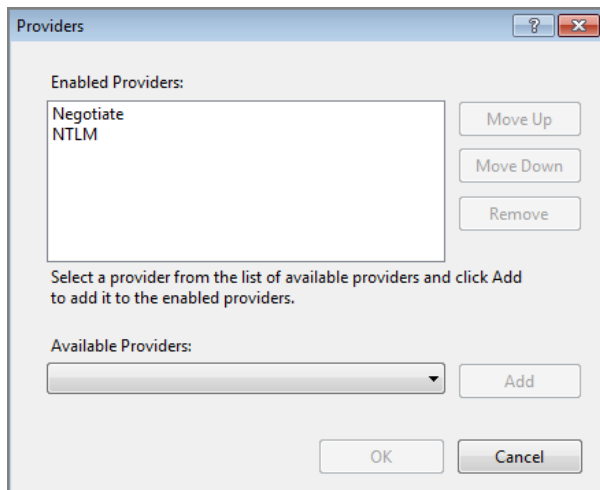
3. Navigate to the virtual directory you created previously, `cgi-bin`.
4. On the center pane, double-click **Authentication**.  
The Authentication options open.



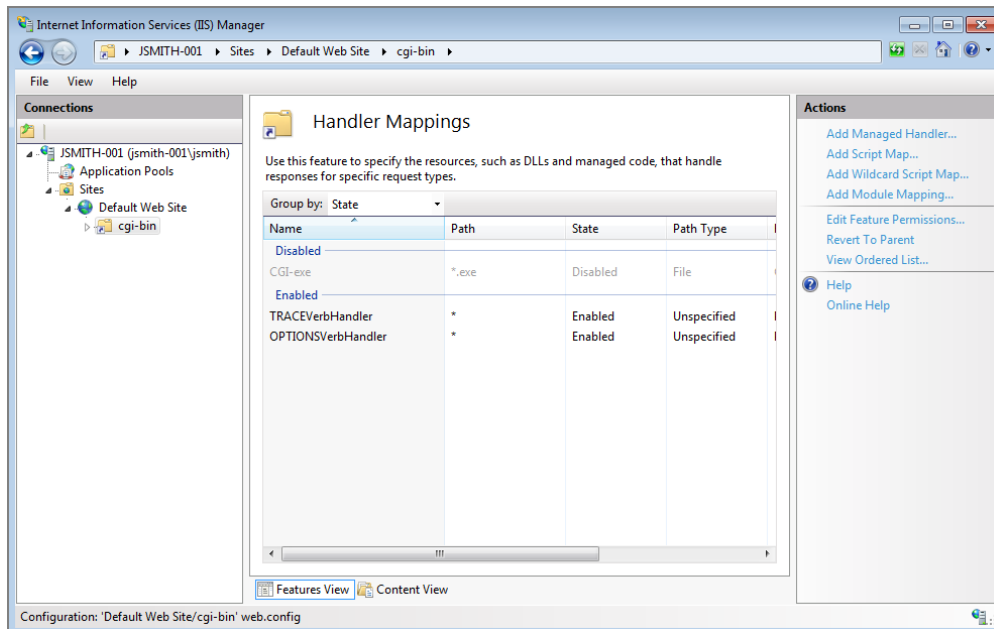
5. Enable **Windows Authentication** and disable all other authentication methods.

- Right-click **Windows Authentication**, and select **Providers** from the menu.

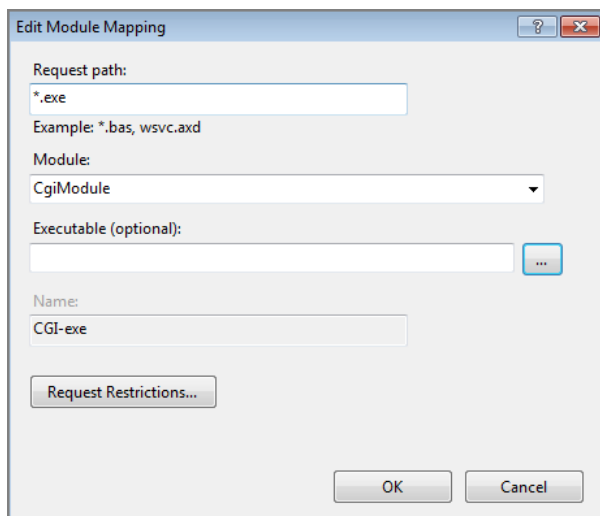
The **Providers** dialog box opens.



- Remove **Negotiate** from the Enabled Providers and click **OK**.
- Select the virtual directory again, double-click **Handler Mappings**.



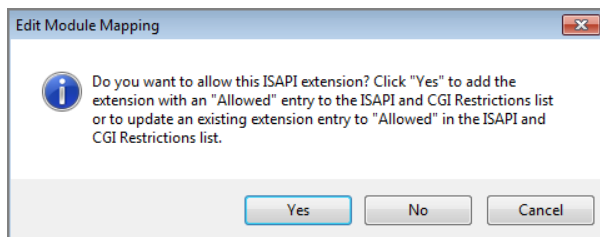
- Double click **CGI-exe**.  
The **Edit Module Mapping** dialog box opens.



10. Click the browse button for the **Executable** box, and browse to the location of the *dlcgi.exe* file. The default value is `C:\DI\Solution\diveline\cgi-bin\dlcgi.exe`. If you cannot see the executable, select **exe** from the file type pull-down menu.

11. Click **OK**.

The **Edit Module Mapping** window opens.



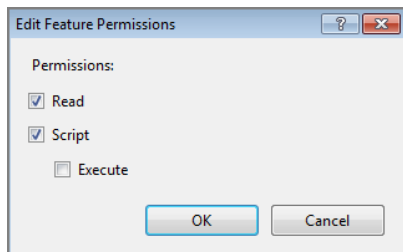
12. Click **Yes** to accept the changes.

The dialog box closes.

13. Right-click **CGI-exe**, and select **Edit Feature Permissions** from the menu.

The **Edit Feature Permissions** dialog box opens.



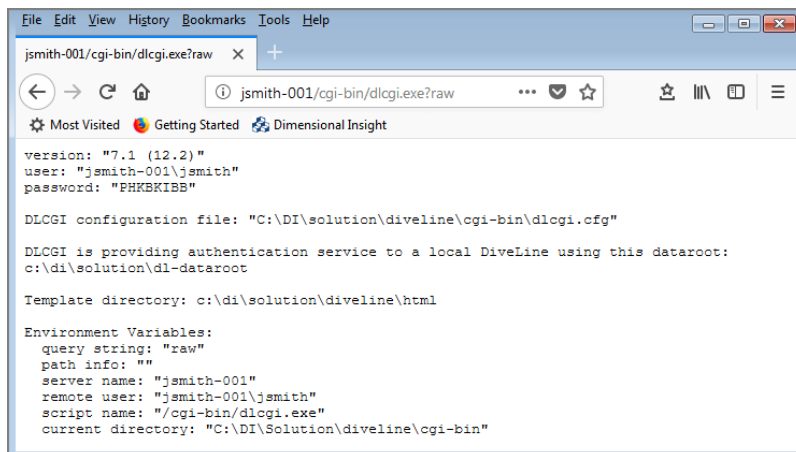


14. Select the **Read**, **Script**, and **Execute** check boxes, and click **OK**. This enables **CGI-exe**.
15. Test this configuration by running **dlcgi.exe?raw**:

Open a web browser and enter in *http://<servername>/cgi-bin/dlcgi.exe?raw*.

**NOTE:** This page might ask for a username and password. Use the server username. For this example, the username is *jsmith*.

Here is the resulting page:



IIS is now configured for DiveLine's Web Server authentication under Windows 7.

## Domain Issues

If you configured both Integrated and Basic authentication for IIS, you may have a situation where internal users are recognized as `<mydomain>\<username>`, while external users are recognized as just `<username>`. If so, try defining a default domain.

For example, to enable Basic Authentication in IIS 7.0:

1. Start the **Internet Information Services (IIS) Manager**.
2. Expand the **Sites** container for the **Enterprise Vault Web Access** application computer.
3. Click the **EnterpriseVault** folder.
4. Double-click **Authentication** in the IIS area at the right.
5. Verify that Anonymous Authentication is disabled and **Basic Authentication** is enabled.
6. Right-click **Basic Authentication**, and then click **Edit**.
7. Enter the name of the domain that contains the majority of the user accounts using the Web Access application.
8. Click **OK**.

If you encounter difficulties, add the following line to your *dlcgi.exe* file:

```
default_domain="<mydomain>"
```

In this case, <mydomain> is the domain name to be prepended with a backslash to the username anytime the Web Server provides a username without a domain. Users that IIS authenticates as <mydomain>\<username> stay as <mydomain>\<username>, while users that authenticate as <username> are changed to <mydomain>\<username>.

Note that when using this method, the Active Directory groups that define who can access the directory containing *dlcgi.exe*, and therefore who is allowed to reach DiveLine, need to contain all the users twice, once with and once without the domain part.

Alternatively, the file system security can change to allow everyone to access *dlcgi.exe*, with the DiveLine configuration determining who can log on.

## Configuring Web Server Authentication

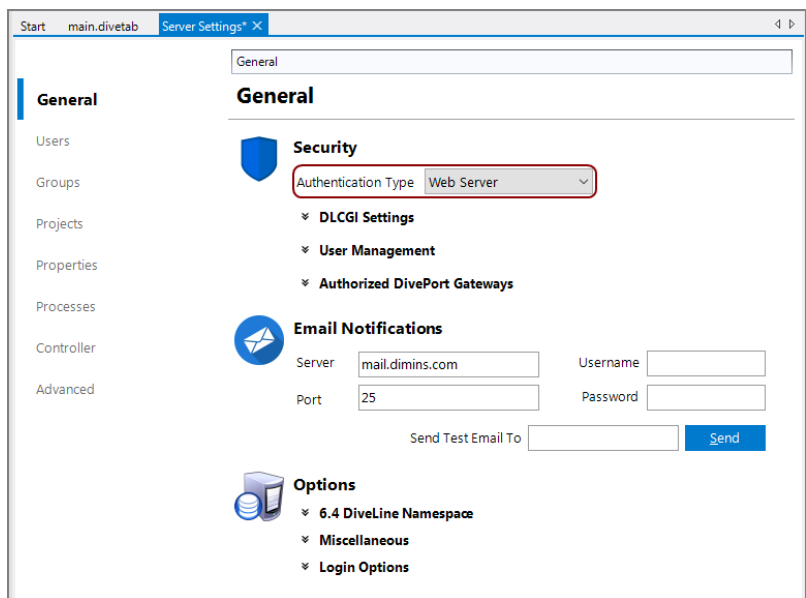
After the Web Server is configured, you need to complete the DiveLine settings in Workbench. If the Web Server has not been configured, see [Configuring the Web Server on page 134](#).

A user connects to the Web Server, enters a username and password, and is connected to the DLCGI object on the Web Server. The DLCGI object dynamically creates the HTML that is returned to the user's browser. At the same time, it creates a DiveLine password for the user. This password is stored in a directory on the DiveLine machine in the `webdir` directory. The password is good for five minutes, or until the first time it is used. The Web Server must have permission to write to the `webdir` directory and DiveLine (or the user the service is running as) must have read access to the directory.

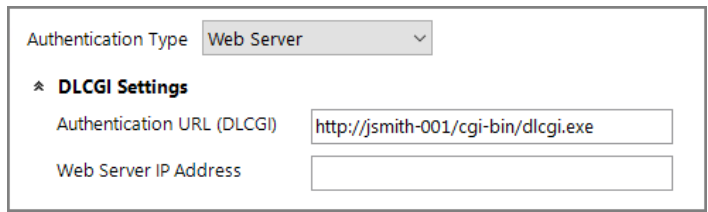
The Web Server authentication method uses a Web Server to authenticate users, and streamline maintenance of client start pages. For more information, see [Web Server Authentication on page 133](#).

To configure Web Server authentication:

1. Open **Workbench** and open a DiveLine connection.
2. Select to **Tools > Server Settings > General**.
3. In the **Security** section, select **Web Server** from the **Authentication Type** pull-down menu.



4. Click the chevron next to **DLCGI Settings**.  
The DLCGI Settings display.



5. In the **Authentication URL (DLCGI)** box, enter the URL to the DLCGI executable for the web site that users are authenticating against. The basic format of a valid URL is *http://<server name>/cgi-bin/dlcgi.exe*.

6. In the **Web Server IP Address** box, enter the IP address of the machine on which the Web Server is installed and configured.
7. **Save** the Server Settings, using **File > Save** or **Ctrl+S**.

**NOTE:** If authenticating using CGI within a domain environment, the domain name must be part of the DiveLine username. For example, `dimins\jsmith`.

In order for DivePort to work, it needs to be reconfigured. For more information, see [Configuring DivePort for Web Server Authentication below](#).

## Configuring DivePort for Web Server Authentication

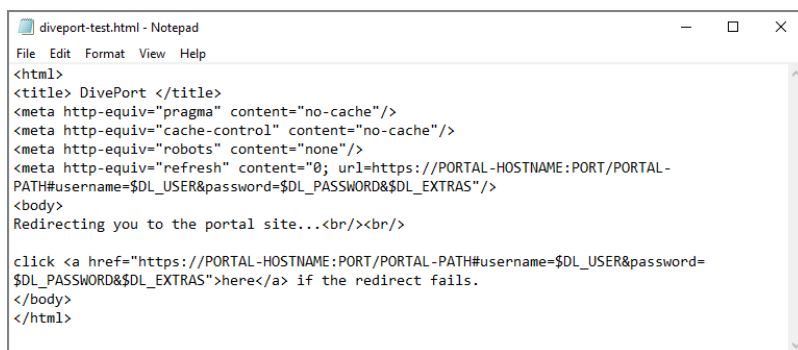
DivePort needs to be configured so it knows the URL for DL CGI, allowing it to forward unauthenticated users to that address for authentication. This insures a single sign-on procedure for the end users.

If DiveLine is using Web Server authentication, you need to update two files:

- `diveport.html`
- `<diveport>.xml`

To update the `diveport.html` file:

1. Copy the `diveport.html` template file located in `\DI\Solution\webapps\<diveport>\dlcgi` to the `\DI\Solution\<diveport>\html` directory.
2. Rename the file, replacing `diveport` with the name of your installed instance of the DivePort application.
3. From the `html` directory, open the `<diveport>.html` in a text editor.



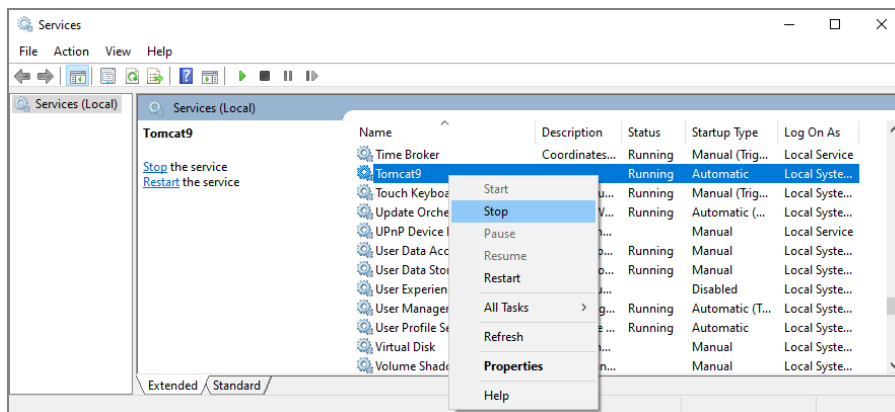
```
File Edit Format View Help
<html>
<title> DivePort </title>
<meta http-equiv="pragma" content="no-cache"/>
<meta http-equiv="cache-control" content="no-cache"/>
<meta http-equiv="robots" content="none"/>
<meta http-equiv="refresh" content="0; url=https://PORTAL-HOSTNAME:PORT/PORTAL-
PATH#username=$DL_USER&password=$DL_PASSWORD&$DL_EXTRAS"/>
<body>
Redirecting you to the portal site...<br/><br/>
click <a href="https://PORTAL-HOSTNAME:PORT/PORTAL-PATH#username=$DL_USER&password=
$DL_PASSWORD&$DL_EXTRAS">here</a> if the redirect fails.
</body>
</html>
```

4. Replace the two instances of `https://PORTAL-HOSTNAME:PORT/PORTAL-PATH` with `https://<servername>:8443/<diveport>`.

Use your DivePort `<servername>` and `<diveport>` so the `html` file points to the correct URL.

To update the `<diveport>.xml` file:

1. Select **Control Panel > Administrative Tools**.
2. Open the **Services** window.
3. **Stop** the Tomcat service.



4. Locate the context file `<diveport>.xml` in the Tomcat directory. For example:

`C:\DI\Tomcat\Tomcat 9.0\conf\Catalina\localhost\diveport-test.xml`

5. Open the file in a text editor.

```

diveport-test.xml - Notepad
File Edit Format View Help
<Context docBase="C:\DI\Solution\webapps\diveport-test\diveport.war"
sessionCookiePathUsesTrailingSlash="false">
  <!-- uncomment this and set the following parameters:
  <Parameter name="dataroot" value="Enter DivePort WebData Directory Here" />
  <Parameter name="approot" value="Enter DivePort WebApp Directory Here" />
  <Parameter name="diveline.server" value="Enter DiveLine Server String Here" />
  <Parameter name="diveline.admin-username" value="Enter Admin Username Here" />
  -->
  <!-- for single-sign-on with a CGI-mode installation, uncomment and set these parameters:
  <Parameter name="diveline.web-auth-start-url" value="Enter DL CGI DivePort URL Here"/>
  <Parameter name="diveline.web-auth-finish-url" value="Enter Logoff URL Here"/>
  -->
  <!-- If you need to permit HTTP connections:
  <Parameter name="require-confidentiality" value="false" />
  -->
  <Parameter name="dataroot" value="C:\DI71\Solution\webdata\diveport-test" />
  <Parameter name="approot" value="C:\DI71\Solution\webapps\diveport-test" />
  <Parameter name="diveline.server" value="jsmith-001:2131" />
  <Parameter name="diveline.admin-username" value="admin" />
</Context>

```

6. Change the following parameters and values to match your `DI\Solution` directory and DiveLine Admin user setup:

- `Parameter name="dataroot"`

For example:

```
Parameter name="dataroot"  
value="C:\DI\Solution\webdata\diveport-test"
```

- Parameter name="aproot"

For example:

```
Parameter name="aproot"  
value="C:\DI\Solution\webapps\diveport-test"
```

- Parameter name="diveline.server"

For example:

```
Parameter name="diveline.server" value="jsmith-  
001:2131"
```

- Parameter name="diveline.admin-username"

For example:

```
Parameter name="diveline.admin-username" value="admin"
```

7. Within the comment tags, delete the comment and enclosing tags, and set the following parameter and value lines:

- Parameter name="diveline.web-auth-start-url"

This points to the DLCGI DivePort URL, which is the *diveport.html* file.

For example:

```
Parameter name="diveline.web-auth-start-url"  
value="http://jsmith-001/cgi-bin/dlcgi.exe/diveport-  
test.html"
```

**NOTE:** If some users are not using single sign-on, redirect users using an authentication override of OWN to the logon dialog box by using one of the following formats instead:

- `https://<servername>:8443/<diveport>/login`
- `https://<servername>:8443/<diveport>/#login=true`

This avoids the CGI-authentication redirect.

- Parameter name="diveline.web-auth-finish-url"

This points to the Logoff URL, that is, where DivePort users are directed after log off.

For example:

```
Parameter name="diveline.web-auth-finish-url"  
value="http://www.dimins.com"
```

8. Save your file changes and restart Tomcat.

If you require more information on using the DivePort DLCGI, contact Technical Support.

## LDAP Authentication

DiveLine supports use of the Lightweight Directory Access Protocol (LDAP) as defined by RFC 2255. When DiveLine is using LDAP authentication, for each user that attempts to log in, in real time, DiveLine:

- Requests credentials
- Connects to an LDAP directory server
- Performs a search for the given user
- Authenticates that user with the given password

If it succeeds, then the username attribute specified is passed back to DiveLine. That user then has access based on profile settings in Workbench. Note that you do need to define your users within Workbench, and the user names assigned in the DiveLine user profile must exactly match the user names in the LDAP.

LDAP authentication is supported in DiveLine running on:

- All Windows platforms
- Solaris
- Linux

The Microsoft version of LDAP is Active Directory (AD). LDAP authentication is tested against both Microsoft Active Directory and OpenLDAP directories. On supported UNIX platforms, the OpenLDAP libraries must be installed on the server in order for it to work.

**NOTE:** When configuring DiveLine LDAP authentication, the database schema must be known. On Windows, if it is unknown, the LDAP Data Interchange Format (LDIF) utility can be used to provide the necessary information.

DiveLine also supports LDAP over TLS (LDAPS). The LDAP server certificate must be installed and trusted. The DiveLine Events logs indicate if there are problems with the certificate. LDAPS is a good option when DiveLine is on one server environment and the authentication is being done on a remote server.

The key to DiveLine's ability to make use of LDAP servers is the attributes defined in the *atlcfg.cfg* file. These attributes determine whether LDAP is supported, how a user's credentials are matched against the directory, and the scope of a search that an application conducts in the LDAP tree. The *atlcfg.cfg* file is updated when you use the Workbench GUI.

There are three steps to configuring DiveLine to use LDAP authentication:

- [Obtaining Information below](#)
- [Exporting the LDAP Database Listing below](#)
- [Configuring LDAP Authentication on the facing page](#)

## Obtaining Information

It is recommended that the following information be obtained prior to configuring LDAP:

- LDAP server name or IP address and port number.
- Account for an application to access the LDAP server, typically an LDAP administrator.
- LDAP schema; this can be provided in the form of an *LDIF* file.
- LDAP user distinguished name (DN) components that map to the base search for DiveLine.
- LDAP user attribute that maps to the DiveLine user name.

**NOTE:** It is often the case that the DiveLine administrator is not an LDAP expert, so a trial and error period might occur when configuring DiveLine for LDAP authentication. DiveLine session logs prove very useful in these cases, as they provide helpful information on authentication failures.

## Exporting the LDAP Database Listing

When configuring DiveLine to use LDAP authentication, it is useful to have a database listing to ensure that the names given to DiveLine match those in the LDAP configuration. The database contents can be exported in LDAP Interchange Format (LDIF) by using the LDIFDE utility as follows:

1. Start a Command Prompt on the server.
2. Run the *ldifde -f output.ldf* file.

The *output.ldf* file contains all the objects in the LDAP configuration, separated by blank lines. Each object begins with the Distinguished Name (dn); this is considered the primary name for the object and has a form similar to:

```
dn: cn=Users,dc=jsmith-001
```

Notice that the names for objects contain the local domain.

When authenticating user "John Smith", DiveLine connects to the server at **dimins.com**, and then searches the users under *cn=Users,dc=jsmith-001* for a user with a common name (cn) of "John Smith". If it is preferred that the user log in to DiveLine with a short name (jsmith), then pick another attribute (for example, *sAMAccountName*) that contains this value, for example:



```
ldap://jsmith-
001:389/cn=Users,dc=dimins,dc=com?sAMAccountName?sub?obje
ctClass=user
```

The LDIF dump should indicate what the values for various attributes are. By not specifying a port, the example URL above uses the default port 389. If this is not the port in use, the URL should take the general form:

```
ldap://<server>:<port>/<dn>?<attribute>?<scope>?<filter>
```

DiveLine can connect to only one LDAP directory server. If that directory server has been set up to switch to a standby computer server, DiveLine accepts the returned URL and searches the new directory server.

If the Active Domain administrator has set up **Organization Units**, users may be in a different part of the hierarchy based on their organization unit. This displays in the LDIF dump. In this case, the username might have an "OU" attribute giving the organization unit. For example:

```
cn=John Smith,OU=Documentation,dc=dimins,dc=com
```

To only search users in the Administration organizational unit, give that as the base DN in the URL:

```
ldap://jsmith-
001:389/ou=Administration,dc=dimins,dc=com?cn?sub?objectClass=user
```

When using LDAP, please note the following:

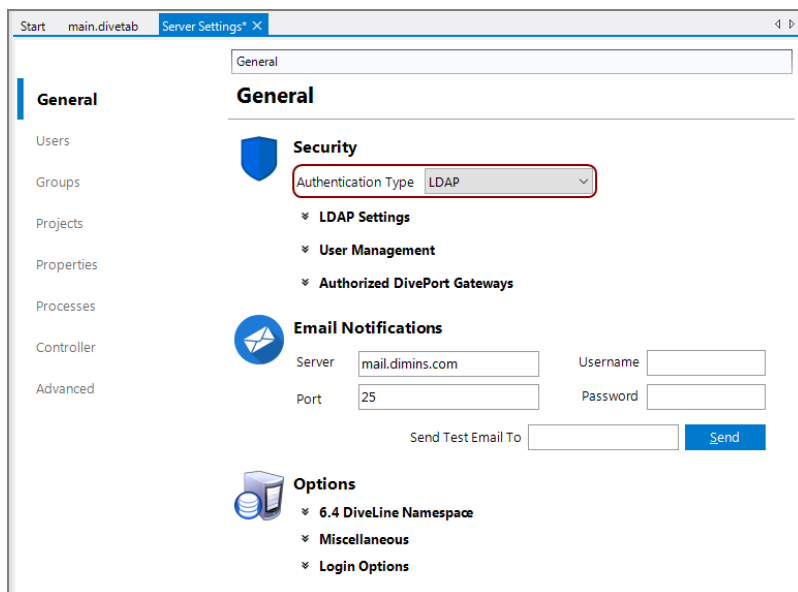
- URLs should be entered without spaces or line breaks.
- LDAP Group attributes are not recognized as Groups in DiveLine. Groups in DiveLine are established using Workbench.
- DiveLine LDAP authentication requires challenging the user credentials. Single sign-on is possible only with DiveLine Web Server authentication. See [Configuring LDAPS on page 165](#).

## Configuring LDAP Authentication

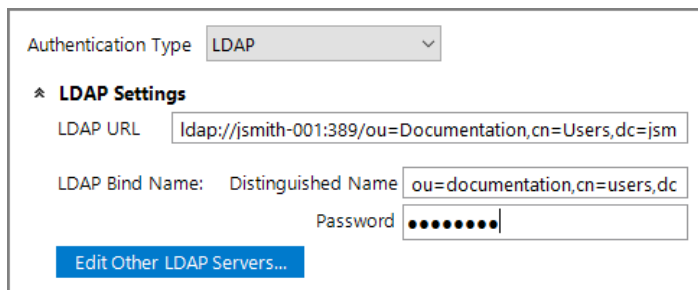
Once you have collected your LDAP information, you need to configure LDAP authentication in Workbench.

To configure LDAP authentication:

1. Open **Workbench** and open a connection.
2. Select **Tools > Server Settings > General**.



3. Select **LDAP** from the **Authentication Type** pull-down menu.



4. Enter the **LDAP URL**. The LDAP URL defines the LDAP server, the username attribute, and the filter for searching the LDAP database. This URL is an LDAP URL as defined by RFC 2255, and takes the general form:

`ldap://<server>:<port>/<dn>?<attribute>?<scope>?<filter>`

- **server**—The LDAP server hostname or IP address.
- **port**—The Transmission Control Protocol (TCP) port number to use to connect to the LDAP server. The default is 389.
- **dn**—The distinguished name used to start the search for the user.
- **attribute**—Used to match the given user name to DiveLine. If there are multiple attributes specified, only the first one is used. If no attributes are specified, the default attribute, *uid*, is used. DiveLine can also match an attribute and return a different attribute. Multiple attributes are separated by commas.

- **scope**—Defines the scope of the search, and should be either *one* to search the children of the given base, or *sub* to search all descendants of the given base. The *sub* option is recommended.
  - **filter**—A string representation of the filter to apply in the search. It is appended to the username search using an *AND* condition, such as *(&(user=attr)(filter))*. This is optional.
5. Enter the **Distinguished Name**. This field needs to contain the Distinguished Name of an LDAP administrator to use to log in to the server. This user must have permission to search the database. The Distinguished Name is passed in clear text.
  6. Enter the **Password**. This field must contain the password for the Distinguished Name given in the Distinguished Name field. The password is stored and passed in clear text.
  7. **Save** the Server Settings, using **File > Save** or **Ctrl+S**.
  8. Restart the DiveLine service for the LDAP settings to take effect.

## Configuring LDAPS

When using LDAP authentication, a URL starting with *ldaps://* can be specified to cause DiveLine to negotiate a secure TLS connection before sending passwords to the LDAP server.

When configuring LDAPS on Windows, note the following:

- The SSL/TLS certificate presented by the LDAP server must be considered trusted by Windows. If it is not, the logon fails. The DiveLine Events log indicates that the cause is the LDAP server is down or the certificate was rejected. In some Active Directory or Windows Domain environments, the necessary certificates can be distributed and trusted automatically.
- To troubleshoot LDAPS connections, you can tell DiveLine to not attempt Certificate Verification, blindly accepting any and all certificates. To do this, manually add the following line to the **main** block of the *atcfg.cfg* file:
 

```
ldaps_debug_skip_cert_verification="true"
```

Then start a new ProDiver session.

**CAUTION:** This creates a security risk from man-in-the-middle attacks and should be undone at the conclusion of your troubleshooting.

If LDAPS only works with this switch enabled, then there is a problem with the certificate. It might be one of the following:

- The certificate is expired.

- The certificate common name does not match the name of the machine specified as the LDAP server. Note that "machine" and "machine.domain.com" do not match.
- The Certificate Authority (CA) is not trusted. This is the case for self-signed certificates or certificates signed by a corporate CA where the CA certificate has not been imported.
- To install a new Certificate Authority (CA) certificate in Windows, use the Certificates snap-in of the Microsoft Management Console (*mmc.exe*). See <http://msdn.microsoft.com/en-us/library/ms788967.aspx> for instructions on starting that interface and importing the third-party root certificate.

When configuring LDAPS for Linux, note the following:

- It is possible to modify *atlcfg.cfg* to require encryption through STARTTLS on the normal port by setting `ldap_tls="always"`. Use of an ordinary *ldap://* URI is then encrypted.

Other options:

- **ldap\_tls="none"**—Do not attempt STARTTLS; it is treated as if the option is not present.
- **ldap\_tls="optional"**—Encryption is not required. Never use this except for debugging.
- The TLS certificate presented by the LDAP server must be trusted. The */etc/ldap/ldap.conf* file specifies, using its **TLS\_CACERT** attribute, a file containing the trusted Certificate Authorities. Position the certificate here to enable both STARTTLS and LDAPS.
- It is also possible to temporarily set "TLS\_REQCERT never" in the LDAP configuration file during debugging to see if the certificate is in fact the problem.

**CAUTION:** This should not be left set, however, because it disables certificate checking and protection from man-in-the-middle attacks.

- Verification of the TLS certificate settings can also be done from the command-line, using the **ldapsearch** tool. For example:

TLS on LDAPS port:

```
ldapsearch -x -H ldaps://ldap1.dimins.com -b  
"ou=people,dc=dimins,dc=com" uid=joe
```

STARTTLS on normal LDAP port:

```
ldapsearch -ZZ -x -H ldap://ldap1.dimins.com -b  
"ou=people,dc=dimins,dc=com" uid=joe
```

You see a **Connection error** message if the certificate is rejected or if the network connection cannot be made.

## Implementing SSO on Linux

If you are using LDAP on Linux, and are trying to implement SSO (single sign-on), consider using *dlcgi.exe* for Web Authentication. The standard use of *dlcgi.exe* allows you to implement SSO.

For standard SSO from an LDAP Active Directory login, configure a Windows server or virtual machine (VM) with Internet Information Server (IIS) running *dlcgi.exe*. You can then configure the *dlcgi.exe* to refer to the Linux DiveLine as the target to forward authentication information to.

## OIDC Authentication

DiveLine supports use of the OpenID Connect (OIDC) authentication scheme for connections. OpenID Connect allows you to specify a third-party provider to redirect to for user authentication. Issuers can be anything from a Microsoft Azure site to Google to Facebook. When you configure an OIDC provider in DiveLine, users can connect to that DiveLine through the provider's website. The process works as follows:

1. A user attempts to log onto their DiveLine user account.
2. DiveLine detects that the user should connect through OIDC.
3. The user is redirected to the OIDC identity provider's website.
4. The user logs onto the OIDC identity provider's website.
5. A verification token is sent to DiveLine and DiveLine gives access to the user.

This process ensures that DiveLine never handles a password. Instead, it sends the username to the identity provider, which then verifies the password. The usernames assigned in the Workbench user accounts must exactly match the usernames for the identity providers. Setting up OIDC requires configuring OIDC identity providers. This can be done either in the *atlcfg.cfg* file or through the interface in Workbench server settings.

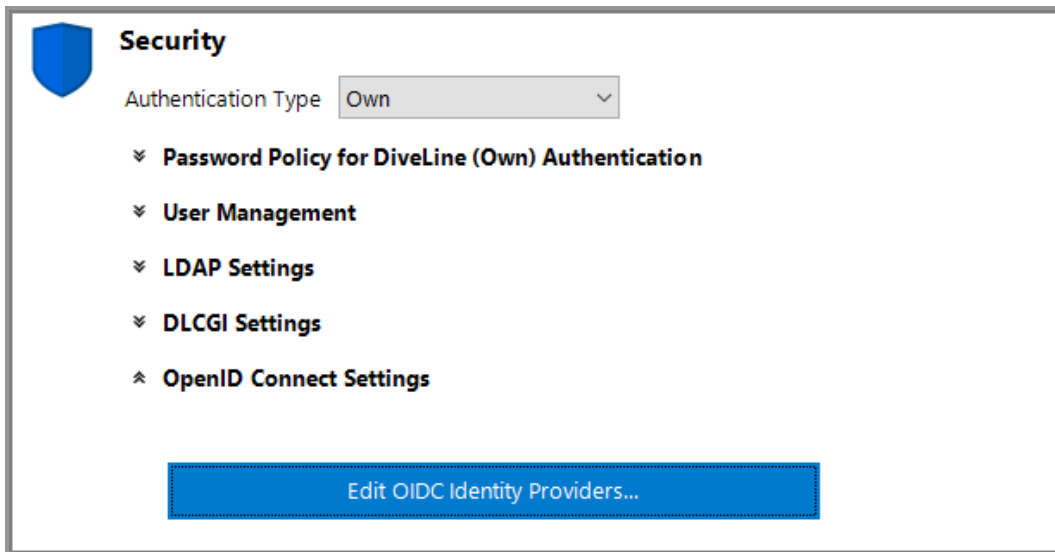
## Configuring OIDC Authentication

Setting the OIDC authentication type allows you to authenticate credentials using a third-party identity provider.

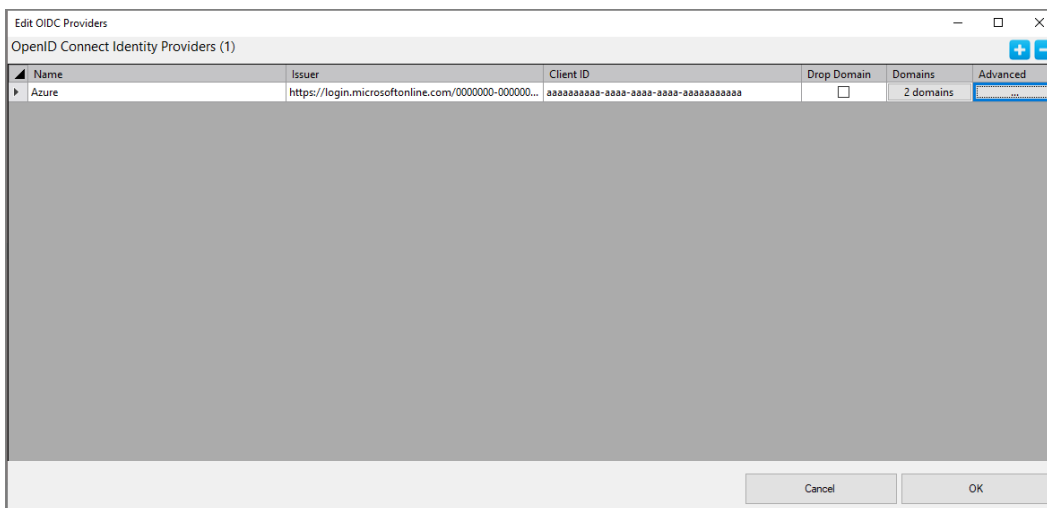
To configure OIDC authentication:

1. Open **Workbench** and open a DiveLine connection.
2. Select **Tools > Server Settings > General**.

- Expand the **OpenID Connect Settings** (click the expand chevron).



- Click **Edit OIDC Identity Providers**.  
The **Edit OIDC Providers** window opens.



The available columns are:

- **Name**—A user-provided name for the OIDC identity provider.
- **Issuer**—An OpenID Connect metadata URL or, alternatively, a URL that is supplied by the identity provider.
- **ClientID**—A unique token supplied by the identity provider.

- **Drop Domain**—If selected, any username formatted as *username@domain.com* has the *@domain.com* portion removed before looking for a matching user in the DiveLine user list. For example, if a username is *test@company.com*, only *test* is sent to the issuer; *@company.com* is removed.
  - **Domains**—Specifies which domains are used with the given Issuer and ClientID combination. Domains are generally only specified if there are multiple OIDC identity providers.
  - **Advanced**—Opens the OIDC Advanced Options window, where you can set the following attributes:
    - **Username Claims**—Certain identity providers send authorization responses with a name and value pair containing a username. This field defines names that might contain a DiveLine username as a value. This field accepts a comma-separated list for multiple potential names. This field accepts array notation. For example, given an array of usernames named *users*, providing `users[0]` returns the first element in the *users* array.
    - **Scopes**—Defines a comma-separated list of values that, when sent to an identity provider, determines what additional information, if any, needs to be sent back to assist in authorization.
    - **Client Secret**—This feature is specific to OIDC implementations that use Google as an identity provider. Stores a unique string of information only shared by the identity provider and DiveLine.
    - **Discovery Endpoint**—Stores the identity provider's metadata URI.
    - **Authorization Endpoint**—Stores the identity provider's authorization URI
    - **Token Endpoint**—Stores the identity provider's token URI.
    - **JWKS URI**—Stores the identity provider's JWKS URI.
    - **Web app response mode**—Stores the mode used when returning the OIDC response and parameters. The only available value is currently `query`.
5. When you are done adding identity providers, click **OK**.
  6. At the top of the Security section, click the **Authentication Type** menu.

- Each identity provider you created populates the Authentication Type menu in the format `OIDC:[Identity Provider Name]`.

The screenshot shows a web interface with a 'General' header. Below it is a 'Security' section with a blue shield icon. The 'Authentication Type' is a dropdown menu currently showing 'OIDC:Azure'. Below that is an expanded 'LDAP Settings' section with a chevron icon. It contains three input fields: 'LDAP URL', 'LDAP Bind Name: Distinguished Name', and 'Password'. At the bottom of the LDAP Settings section is a blue button labeled 'Edit Other LDAP Servers...'.

## Running DiveLine in Clustered Mode

Running DiveLine in clustered mode allows multiple DiveLine services, on multiple machines (or nodes), to share a dataroot. To run DiveLine in clustered mode, install all instances of DiveLine on the desired machines, being sure to point each instance to the same dataroot location. The dataroot needs to be on shared storage, such as a NAS or Windows file share. Once installed, you must explicitly tell each DiveLine service instance to run in clustered mode.

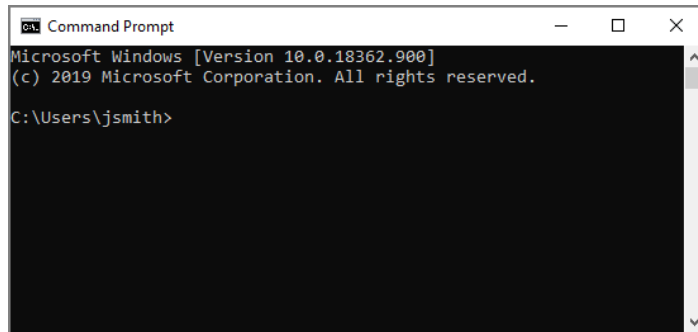
**NOTE:** Clustering requires the use of a separate load-balancer, as software or hardware, and is not supplied by DI.

For example, on Windows:

- Open the **Start** menu and type **cmd.exe**.
- Click the search box icon.
- Click **cmd.exe** from the results list.

The Command Prompt opens.





4. Navigate to the DiveLine utilities. For example:

```
cd \DI\Solution\diveline\bin
```

5. Enter **di-service -list** and press **Enter**.

A list of DiveLine instances on the machine appears.

6. To turn clustering mode on, use the following syntax for each instance:

```
di-service -edit <servicename> -cluster
```

Replace *<servicename>* with instances from [Step 5](#).

7. Repeat Steps 4 to 6 on each DiveLine server, for each DiveLine service instance. This ensures all instances of *di-service.exe* are set to run in clustered mode.
8. Stop and restart each service instance.

Each time you set a DiveLine to use clustering, it should return a message similar to the following:

```
Service: DI-DiveLine-2131
Status: Running
Start-up: Automatic, on system boot.
Executable: \\jsmith-001\DI\Solution\diveline\bin\di-
service.exe
Service runs as user: divelineuser
Dataroot: \\jsmith-001\DI\Solution\dl-dataroot
Port: 2131
Clustering support is enabled.
```

**NOTE:** The *di-service.exe -list* command indicates if clustering is in use. This is an easy way to verify the dataroot and cluster support settings.

The following points should be considered when using clustered mode:

- All DiveLines should be configured to use the same dataroot, on shared storage, such as a NAS or Windows file share. When installing the DiveLines, the dataroot would be something like

\\<server>\DI\dataroot.

- Configuring the DiveLines to use the same dataroot is how they can use the same configuration of users, same data, and how the nodes can find each other for presentation in **Workbench**.
- There is only one `atlcfg.cfg` file, in the shared dataroot, that all clustered nodes access.
- In cluster mode, logs are written to `logs-<nodename>-<portnum>` instead of just `logs-<portnum>`.
- If you are running **DI-Broadcast** or **DI-Scheduler** jobs, the `atljobs.cfg` file that the **di-scheduler-engine** looks for on the node uses the node name as well as the port number, so that each node does not run the same jobs.
- Once clustering is enabled, you can use **Workbench** to connect to any node in the cluster and see information about the use of all nodes.

# Appendix D: AntiVirus Exclusions List

The following information is provided in order to best optimize performance and security for an installation of the Diver Platform. Exclusions are presented as options rather than requirements, and the potential risks are presented to help you to make informed decisions best suited to your needs.

## Client Machines

No specific exclusions are required for normal operation. The following should be considered.

- ProDiver is a single stand-alone *exe* file. There are no *dlls* files and no exclusions are required. This is installed by default in `C:\Program Files (x86)\Dimensional Insight\ProDiver`, but this is configurable. If the executable source is trusted it can be specifically excluded.
- DiveTab-PC uses a number of *dlls* files. The install directory, which defaults to `C:\Program Files (x86)\Dimensional Insight\DiveTab`, can be excluded from real-time scans, or the *DiveTab.exe* binary can be specifically excluded.
- DivePort and NetDiver are web clients that run in a browser. No exclusions are required.

## Application Server

### Solution Directory

The Solution directory contains the executable components of the application server, as well as configuration files, logs and the cache. Many of these files are accessed and changed frequently during normal operation of the product.

All paths below are relative to the Solution installation directory set at install time. The default is `C:\DI\Solution`.

### DiveLine bin

The following core components of the application server should be permitted to execute recursively:

- `C:\DI\Solution\diveline\bin\`

Alternatively, the entire **diveline** directory can be excluded.

## DiveLine dataroot

The **dl-dataroot** directory and all subdirectories should be excluded from real-time scans. There are no executable files present, and the data files are modified often and continuously during normal operation of the server:

- C:\DI\Solution\dl-dataroot\

## Projects Directory

The Projects directory contains scripts and data files that define the nightly ETL process and other data processing as well as configuration and logs. The location is configurable at install time, but defaults to C:\DI\Projects.

Real-time scanning of the C:\DI\Projects directories should be disabled. There are no executable files here, and lots of modifications are made to data files on a continual basis. Enabling real-time scans carries a strong risk of impeding the timely and successful completion of nightly processing of data.

## Web Server

The web server can be installed on the same machine as the application server, but is not required.

## Webapps Directory

The following locations contain *dlls* files, executables and *war* files that are regularly called in the normal operation of the product. While it is not required that real-time scanning is disabled for these locations, it is advisable when using certain features (printing, certain features of the Spectre engine, among others).

- C:\DI\Solution\webapps\`<diveport>` for each DivePort being served
- C:\DI\Solution\webapps\`<netdiver>` for each NetDiver being served
- C:\DI\Solution\webapps\`<divetab>` for each DiveTab being served

Alternatively, the entire C:\DI\Solution\webapps directory can be excluded.

## Webdata Directory

The following locations contain data files that are regularly updated in the normal operation of the product. No executable files are present. While it is not required that real-time scanning is disabled for these locations, some performance can be lost if it is not.

- C:\DI\Solution\webdata\`<diveport>` for each DivePort being served
- C:\DI\Solution\webdata\`<netdiver>` for each NetDiver being served
- C:\DI\Solution\webdata\`<divetab>` for each DiveTab being served

Alternatively, the entire `<Solution>\webdata` directory may be excluded.

# Appendix E: Troubleshooting

Below are some common problems you may have during installation, and the way to solve them.

## Licenses

### **If a machine has multiple network adapters, each having a unique MAC address, which MAC address is used as the machine ID?**

When using the `exportinfo` tool, the network adaptor last returned by the system is used. Prior to Windows 10, the order of network adaptors can be controlled from **Control Panel > Network and Internet > Network Connections > Advanced Settings**. Starting with Windows 10, the order is unspecified.

**IMPORTANT:** If using a virtualization platform, verify that the hardware addresses are not changing upon machine restart.

When validating a license, DI looks at all installed adapters and matches it to the address in the license. You can specify multiple hardware addresses and provide them to DI Support if using the last returned network adapter, chosen by `exportinfo`, is not sufficient. This includes all the hardware addresses within the license.

## DiveLine

### **My AD account does not have the correct permissions.**

If after installing DiveLine, the service is set to run as an Active Directory account, you need to make sure it has the correct permissions. The service user requires write permissions to the `dataroot` directory and everything contained within it, as well as the `projects` root.

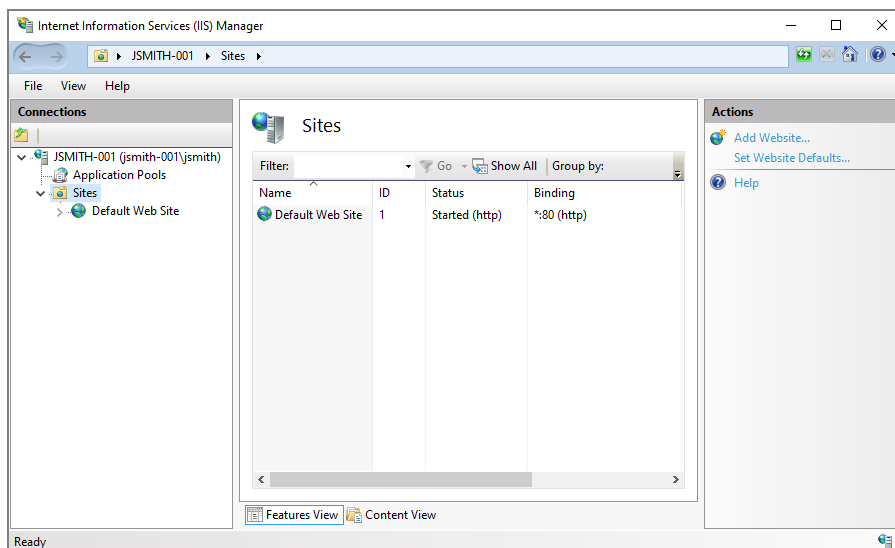
### **Windows security is having me authenticate when it should be authenticating for me.**

This happens when the basic settings are set to **user pass-through authentication** to run the `dlcgi.exe` file. To solve this issue, create a virtual directory and set the needed permissions.

**NOTE:** In many cases this is occurring even when they have read execute access to that directory.

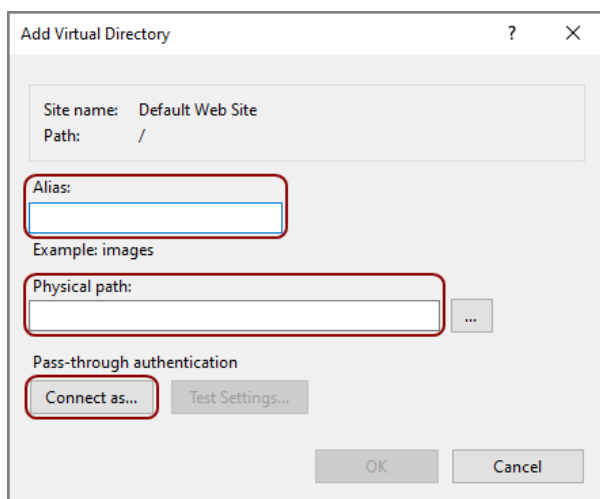
1. Navigate to **Control Panel > Administrative Tools**, and open the **Internet Information Services (IIS) Manager**.

## Diver Platform 7.2

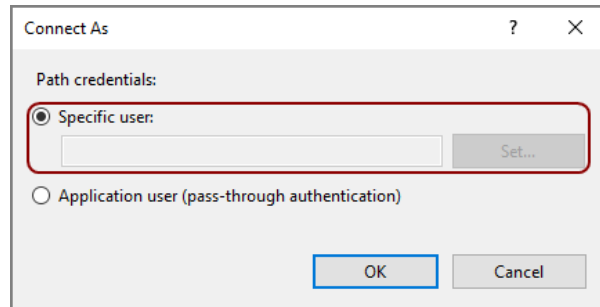


2. On the left panel, expand your connections and open the Sites directory.
3. Right-click the **Default Web Site** and select **Add Virtual Directory** from the menu.

The **Add Virtual Directory** window opens.



4. Enter **cgi-bin** for the **Alias**.
5. Enter the path to the *dlcgi.exe* file for the **Physical path**. The default path is C:\DI\Solution\diveline\cgi-bin.
6. Click **Connect as** and select **Connect as specific user**.



7. Fill in the credentials for the user account running DiveLine.
8. Click **OK**.

## DivePort

### I cannot resolve the `https://<servername>/<portal name>`.

It could be that port 443 is in use by another program. Do one of the following to check:

- Review the Apache Tomcat logs, typically found in `C:\DI\Tomcat\Tomcat 9.0\logs`. The logs may indicate that the address is already in use.
- Open the command prompt and run `netstat -ab`. This tells you if port 443 is in use.

If port 443 is in use, you can do one of the following:

- Figure out what is using the port and decide if that is something that can change.
- Modify the `server.xml` file to use port 8443 instead of 443. The file is typically found in `C:\DI\Tomcat\Tomcat 9.0\conf`.

### I am getting a `java.lang.OutOfMemoryError: PermGen space error` when using multiple DivePorts on the same DiveLine

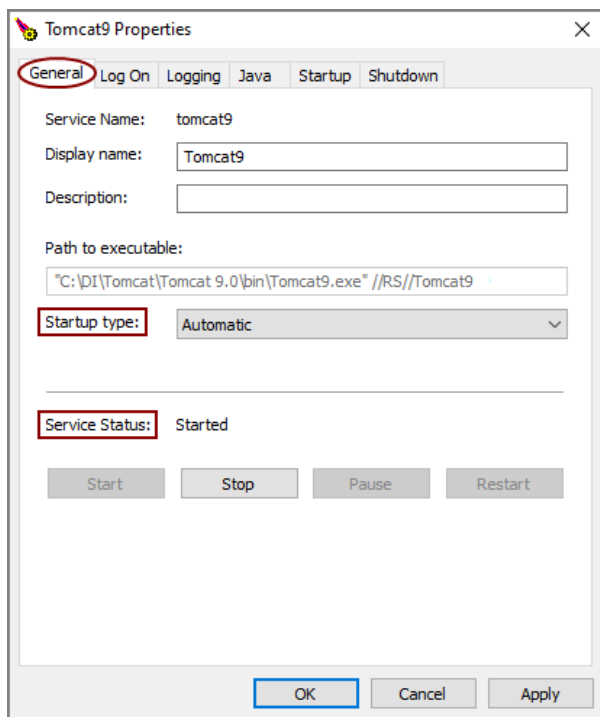
This error indicates that there is not enough space granted to Tomcat to store Java classes. To change this, the Java options for Tomcat must change to include more PermGen space.

To remedy this error:

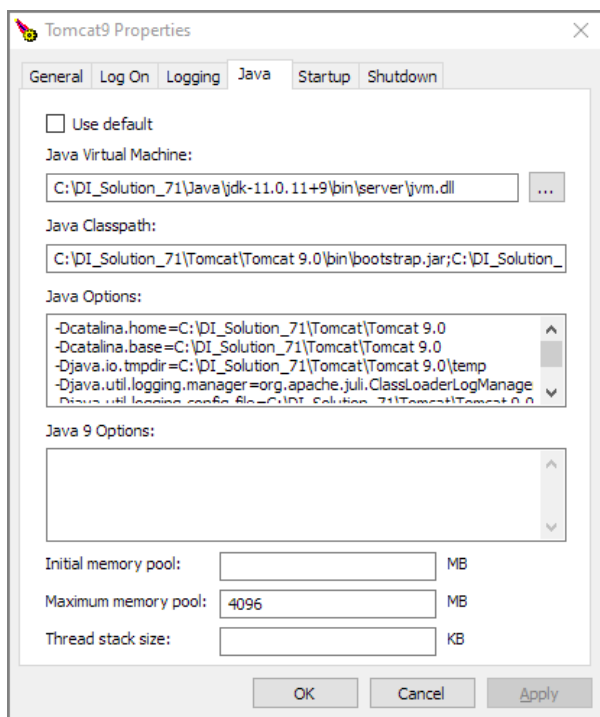
1. Open **Windows Explorer** and navigate to the Tomcat `bin` directory at `C:\DI\Tomcat\Tomcat 9.0\bin`.
2. In the `bin` directory, double-click the **tomcat9w.exe** file.

The **Tomcat9 Properties** dialog box opens.

## Diver Platform 7.2



3. Select the **Java** tab.



4. On the **Java** tab, add `-XX:MaxPermSize=128m` to the **Java Option**.



**TIP:** If 128 is not enough space, try 256.

**IMPORTANT:** If the `-XX:MaxPermSize` attribute is already in place, modify it with the new value.

5. To implement any changes, click **Stop** then **Start** in the **Service Status** section on the **General** tab.
6. Click **Apply**.

## Spectre

**Spectre.exe sometimes crashes even without arguments on the customer machine.**

If running *spectre.exe* without any arguments crashes, it could be your virus scanner. To check:

Try disabling the virus scanner and then running *spectre.exe*. If Spectre runs repeatedly without issue, add *spectre.exe* to its list of exclusions. Also review the section [Appendix D: AntiVirus Exclusions List on page 173](#).

## ProDiver

**My data is not displaying correctly.**

The ProDiver and DivePort clients are able to display text-based data in all languages. Some languages have characters which require "Unicode-enabled" versions of DiveLine and ProDiver in order to correctly display those characters.

If using a non-Unicode DiveLine and non-Unicode clients, set the system's **Language for Non-Unicode Programs**. In Windows 10, navigate to **Control Panel > Region**, select the **Administrative** tab, and then **Change system locale** under the **Language for non-Unicode programs** section.

## Diver Platform 7.2

