Dimensional INSIGHT

Diver Platform 7.2 Installation Guide for Linux

Diver Platform 7.2 Installation Guide for Linux

Revision: Doc-DPIL-72-022924-01

February, 2024

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

60 Burlington Mall Road, Burlington, Massachusetts 01803

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

Diver Platform 7.2 Overview

The Diver Platform is the Dimensional Insight software suite that contains all Diver 7.x software, including Workbench and Spectre. DiveTab is optional. User categories are: Developer, ProDiver, DivePort, DiveTab, and HelpDesk.

About This Installation Guide

This guide contains installation, configuration, and verification procedures to install the Diver Platform Server 7.2 package for Linux and Diver Platform Developer 7.2 package 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:

- **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.

- **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.

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

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

- North America: 920-436-8299 or **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.

About Installing DI Software on a Linux Platform

There are many flavors of Linux and many ways to install the DI software.

This guide provides general instructions, guidelines, and examples about how to install the Diver Platform 7.2 Server software for Linux on a Virtual Machine (VM) using the following versions of VMware and Ubuntu:

- VMware version 10.0.3
- Ubuntu version 20.04

NOTE: Check the versions of Java and Apache Tomcat that your Linux machine supports before installation.

The Diver Platform Server package contains DiveLine and the DivePort and NetDiver web clients.

- **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.
- **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
- **NetDiver** – The zero-footprint web-based analytics client of the Diver Platform. NetDiver provides ad hoc reporting and analytics tools in a web browser. NetDiver requires a connection to the DiveLine server software to access data.

It is important to note that the licenses for using DI software reside on the server. In a Linux environment, you can install Diver Platform Server 7.2 software on a Linux server while all Windows-based clients install on Windows laptops. To install DI Windows clients, such as ProDiver and Workbench, see Installing Diver Platform Developer on page 83.

When using this guide, command line commands are formatted as follows:

```
This is a command that is typed into the Linux command
line.
```

This guide assumes that a Linux administrator has access to perform the following pre-installation actions:

- Build the DI directory structure and download the third-party and DI software to the DI downloads directory.

- Set the permissions on the DI directories. (The instructions in this guide identify where you might need to update the permissions on a directory or file.)

In the course of installing DI software, the following permissions might need to be added to files or directories:

Character	Permission
r	Read permission to open and read a file or to list the contents of a directory.
w	Write permission to modify the contents of a file or to change the contents of a directory.
x	Execute permission to run an executable file or to navigate a directory with the `cd` command.

NOTES:

- Installing the DI Platform Server for Linux is a manual process; Linux installation does not use a wizard such as is available with the Windows installation.
- When installing to a virtual machine, it is a best practice to use a fixed Media Access Control (MAC) address. This prevents licenses issues if the VM is relocated.

About Diver Platform Server 7.2

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.

Workbench

Environment	Port Number
Production	2130
Test	2131
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

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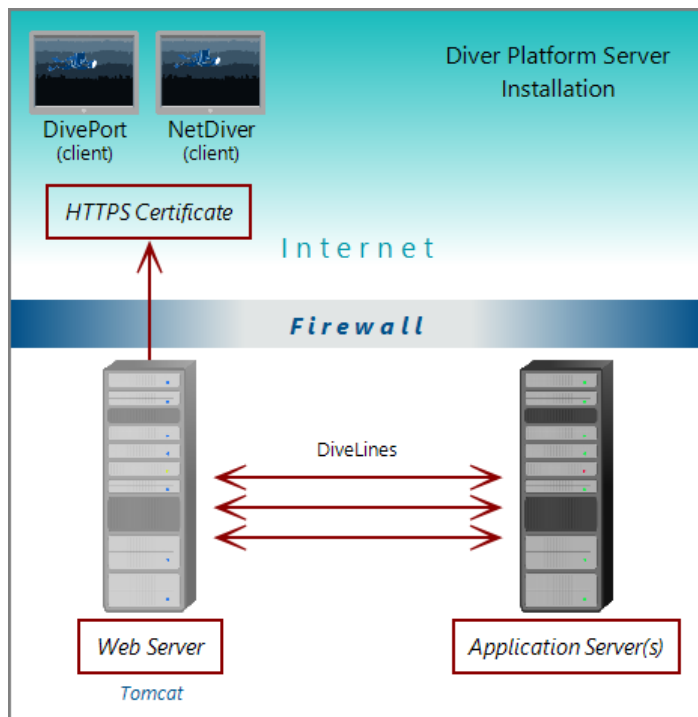
NOTE: When using Unicode for one component, make sure all components are Unicode. For example, you must have a Unicode DiveLine server to serve Unicode encoded content to a Unicode client.

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.
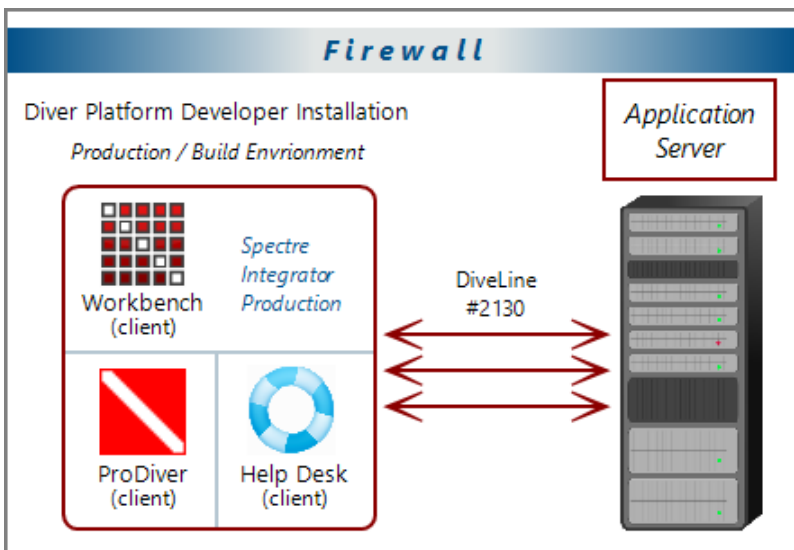
Software Requirements

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
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 Platform and Diver Solution on Linux systems.
	DI recommends that you download the latest release from **http://www.mono-project.com/download/**.
	The libodbc.so.1 library does not ship with the installer. It must be installed separately.
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.

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.

Workbench

Desktop Operating System	Support Notes
Microsoft Windows 8	Not supported. Browser compatibility may impact 7.2.
Microsoft Windows 7	Browser compatibility issues might impact web clients. **IMPORTANT**: 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 its 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**.

About 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
    /platform
        /downloads
        /licenses
        /webapps
        /webdata
```

NOTE: Make sure the directory structure is created from the root directory.

Workbench

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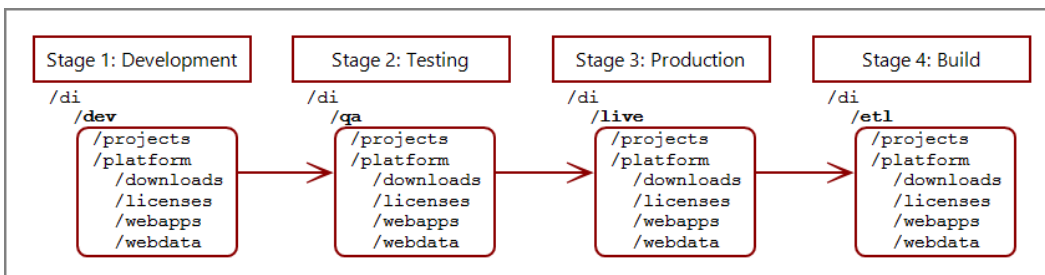
NOTE: This reflects the environments used on a single server so the `di` directory has subdirectories for each environment.

You can install server and developer software on a single machine or different machines using the same directory structure.

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

Directory	Subdirectory	Description
/di	/projects	Default location for Workbench projects. This directory is created manually.
/di	/platform	Default location for directories and files created by DI product installations. This directory is created manually.
/di/platform	/downloads	Default location for DI software downloads. This directory is created manually.
/di/platform	/licenses	Directory for licenses and key files. This directory is created manually.

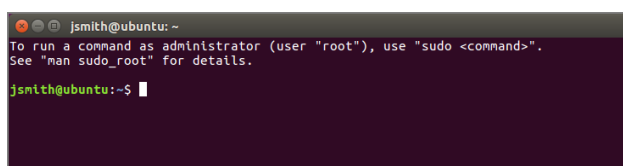| Directory	Subdirectory	Description
/di/platform	/diveline	Subdirectory with program files required by the DiveLine service. Each installed DiveLine instance can have its own `/diveline` directory.
/di/platform	/dl-dataroot	Top level directory for the DiveLine server for configuration information, cache, and log files. Each installed DiveLine instance can have its own `/dl-dataroot` directory.
/di/platform	/executables	Default location for many DI executable files.
/di/platform	/webapps	Program, configuration, and setup files for DivePort and NetDiver. This directory is created manually.
/di/platform	/webdata	Data and customization files for DivePort and NetDiver. This directory is created manually.

About the DI Directory Structure

Building the DI Directory Structure

NOTE: You must have root user privileges (for example, enter `sudo bash`) to build out the DI directory structure from the root directory. Do not build the DI structure from the `home` directory.

This procedure creates the basic structure for Diver Platform Server Linux installation.

Complete the following steps:

1. Log in to your Linux machine.
2. Open a command line.

3. Go to the root directory.

```
cd /
```

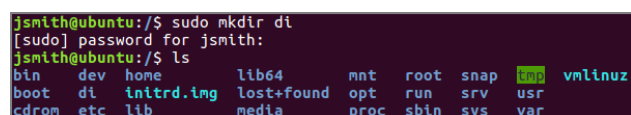4. Create the `di` directory.

```
sudo mkdir di
```

   NOTE: Enter the user password if prompted.

5. Confirm that the `di` directory was created successfully:

```
ls
```

   A list of files and directories in the root directory displays.

6. Change to the `di` directory:

```
cd di
```

7. Optionally, create a directory for each environment.

    a. Create a directory (for example, `live`).

```
sudo mkdir live
```

    b. Confirm that the directory or directories were created successfully:

```
ls
```

    A list of files and directories in the `di` directory displays.

    c. Navigate to the environment (for example, `live`) before creating the subdirectories:

```
cd live
```

NOTE: This guide does not use environments. Therefore, all subdirectories are contained within the `di` directory.

8. Add the following subdirectories by typing each of the following commands:

- `sudo mkdir platform`
- `sudo mkdir projects`

9. Confirm that the directories were created successfully:

```
ls
```

A list of files and directories in the `di` directory displays.

10. Navigate to the `platform` directory:

```
cd platform
```

11. Add the following subdirectories by typing each of the following commands:

- `sudo mkdir downloads`
- `sudo mkdir licenses`
- `sudo mkdir webapps`
- `sudo mkdir webdata`

12. Confirm that the directories were created successfully.

```
ls
```

A list of files and directories in the `platform` directory displays.

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 7.07.1 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 login information and can be logged in 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 do not specify environments. Be sure to alter file locations as required when you repeat these steps to create separate environments, for example, Test versus Production. See About the DI Directory Structure on page 11 and About Roles and Environments on page 2.

Downloading the Server Installation Package

You can download purchased software from the Dimensional Insight website. Dimensional Insight recommends that you download the software by using a graphical web browser rather than by invoking the `wget` command. Depending on your computer's internet access settings, you might need to use another computer to download the server package, and then transfer the files to your server.
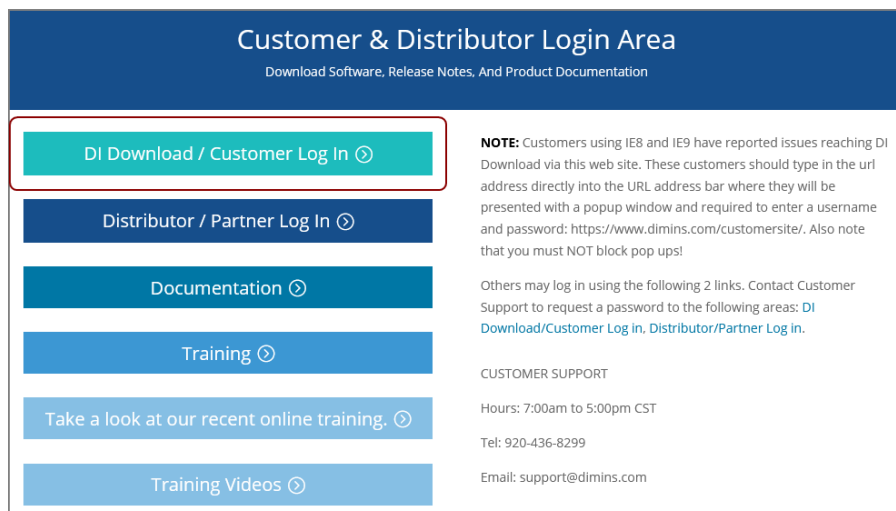
NOTE: Administrative privileges are required to install the software.

1. Using a web browser, go to the Dimensional Insight website: **http://www.dimins.com**.
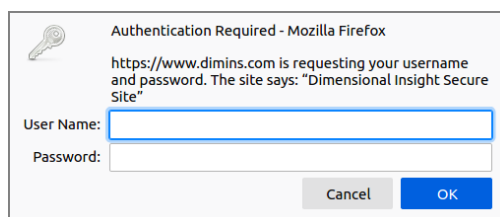
2. On the home page, click **Sign In**.
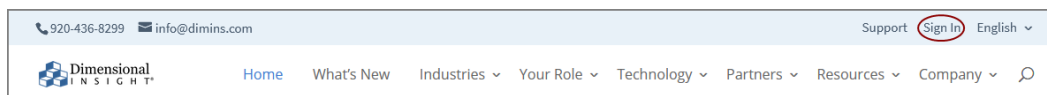
The **Customer & Distributor Login Area** page opens.

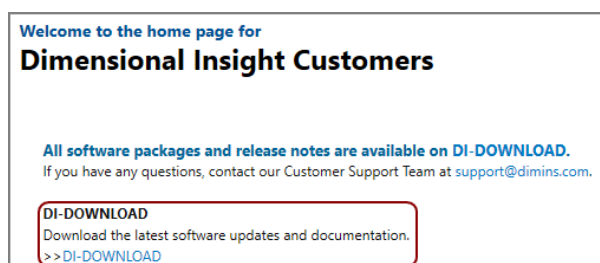3. Click **DI Download / Customer Log In**.

The **Authentication Required** dialog box opens.

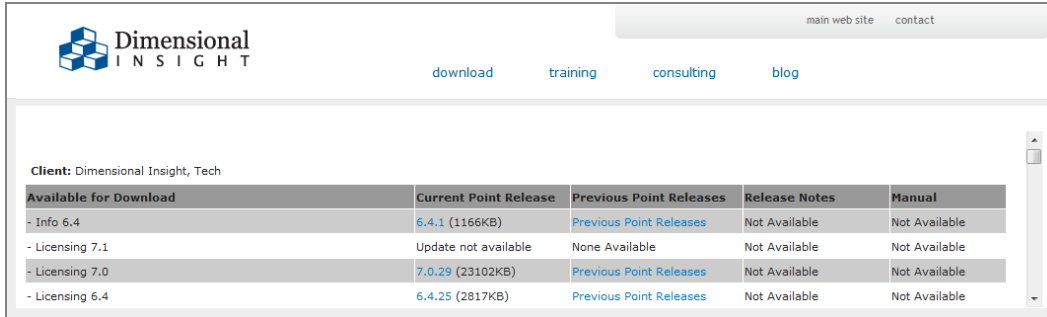4. Enter your **User Name** and **Password**, and click **OK**.

    The **Dimensional Insight Customers** home page opens.

5. Click **DI-DOWNLOAD**.

The software and documents download page opens.

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

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:
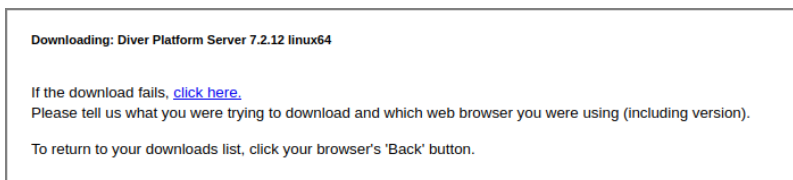
7. Select **Save File**, and click **OK**.
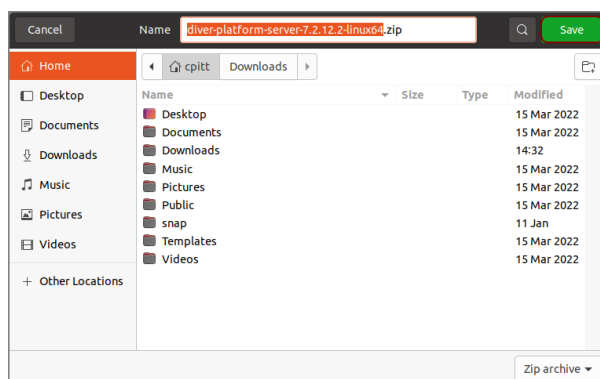
The Diver Platform Server software package *zip* file downloads to the `Downloads` directory on the local computer.

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 on Linux, you can choose **Edit** > **Preferences** and configure the download location.

8. If necessary, move the *zip* file to the Linux server.

9. On the Linux server, enter the following command to move the *zip* file to the `/di/platform/downloads` directory:

```
sudo mv diver-platform-server-<version number>-
linux64.zip /di/platform/downloads
```

Extracting the Server Installation Package

1. Go to the `/di/platform/downloads` directory by entering the following command:

```
cd /di/platform/downloads
```

2. Confirm that the *diver-platform-server-<version number>-linux64.zip* file is in this directory by entering the following command:

```
ls
```

3. Copy the file to the `/di/platform` directory by entering the following command:

```
sudo cp diver-platform-server-<version number>-
linux64.zip /di/platform
```

4. Navigate to the `/di/platform` directory by entering the following command:

```
cd ..
```

5. Confirm that the file is in this directory by entering the following command:

```
ls
```

6. Unzip the *diver-platform-server-<version number>-linux64.zip* file by entering the following command:

```
sudo unzip diver-platform-server-<version number>-
linux64.zip
```

7. After the processes finishes, list the files in the directory by entering the following command:

```
ls
```

Verify that the following files display:

- *di-diveline.tar.gz*
- *web-tools.zip*

8. Extract the *di-diveline.tar.gz* file by entering the following command:

```
sudo tar –xvf di-diveline.tar.gz
```

9. Verify that the files are extracted by entering the following command:

```
ls
```

The following new directories now display:

- `diveline`
- `executables`

Obtaining a License for the DI Software

You need to request and install a license, which enables you to run the software that you purchased.

For this part of the installation, you must use a computer with a Windows operating system that can access the Internet. If you do not have access, contact Dimensional Insight Customer Support.

Using the exportinfo Utility to Obtain Machine Information

You use the exportinfo utility to export your machine's name, operating system, and machine ID to a machine information (*info*) file. You need this information to request a license.

1. On the Linux server, go to the `/di/platform/executables` directory by entering the following command:

   ```
   cd /di/platform/executables
   ```

2. Confirm that the exportinfo utility is in the directory by entering the following command:

   ```
   ls
   ```

   The contents of the directory display, including the *exportinfo* file.

3. View the permissions for the exportinfo utility by entering the following command:

   ```
   ls -l exportinfo
   ```

   The permissions display. If an `x` displays within the first group of letters (for example, `-rwxr--r--`), you can run the utility.

   If you do not have permission to run the utility:

   a. Enable the execute permission.

      ```
      sudo chmod a+x exportinfo
      ```

   b. Verify that the permissions have changed.

      ```
      ls -l exportinfo
      ```

      The permissions display as `-rwxr-xr-x`.

4. Run the exportinfo utility by entering the following command:

   ```
   sudo ./exportinfo
   ```

   The exportinfo utility prompts you to specify a name for the machine information (*info*) file.

5. Specify a file name by doing one of the following:

   - Accept the default file name—*di_minfo_<your machine's name>.info* (for example, *di_minfo_ubuntu.info*)—by pressing the **Enter** key.

   - Enter a name for the file, including the *info* extension, and press the **Enter** key. For example, `di_minfo_jsmith-ubuntu.info`.

You can use any file name that is meaningful to you, but it is a good idea to identify your machine in the file name, so that you can recognize it later.

6. Confirm that the file was created successfully by entering the following command:

```
ls
```

The contents of the directory display, including the *info* file that you created.

7. (Recommended) Move the machine information file to the `/di/platform/licenses` folder by entering the following command:

```
sudo mv <file name>.info ../licenses
```

8. Go to the `/licenses` folder and confirm that the file was moved successfully by entering the following command:

```
ls
```

9. Copy the *info* file onto a Windows computer that can access the Internet, so that you can use it to request a license.

Obtaining the Licensing Package

1. On the Windows computer with the *info* file, open a web browser, and go to the Dimensional Insight website **www.dimins.com**.

2. On the home page, click **Sign In**.
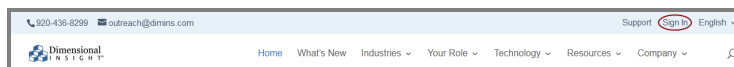
The **Customer & Distributor Login Area** page opens.
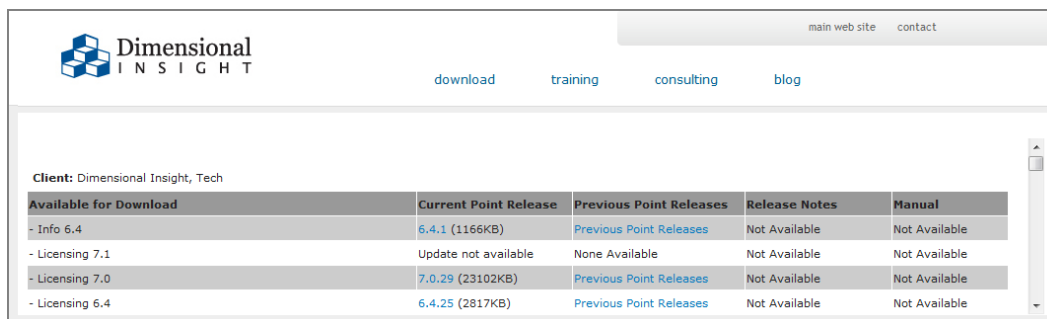
3. Click **DI Download / Customer Log In**.

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.

Workbench

6. Locate the latest version of the **Licensing** package, and click the blue version number.

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

7. On the Opening licensing confirmation box, select **Save File**, and click **OK**.

Obtaining the Licensing Package
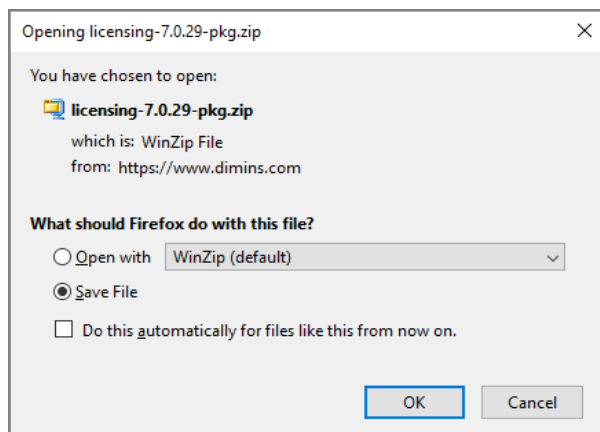
The licensing software package *zip* file is downloaded to the **Downloads** directory on the local computer.

NOTE: The Licensing package includes one file, called *licensing-<version number>-pkg.zip* (for example, *licensing-7.0.29-pkg.zip*).

8. Extract the package.

    A directory is created, called `licensing-<version number>` (for example, `licensing-7.0.29`).

    This directory contains several files. However, you only need *di-license-admin-<version number>-winnt.exe*.

Requesting a License

You can import a machine information (*info*) file to populate the DI-License-Admin utility with another machine's name, operating system, and machine ID. You use this option when you need to request a license for use on another machine (either Windows or Linux).

1. If you have not already, move the *info* file to the Windows computer with Internet access that can run the DI-License-Admin utility.

    NOTE: The *info* file is created in the section .

2. In the extracted licensing package you obtained from DI Download, double-click **di-license-admin-<version number>-winnt.exe** (for example, *di-license-admin-7.0.29-winnt.exe*).

    The **User Account Control** confirmation 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 DI-License-Admin utility starts.

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

5. Select **File** > **Import Machine Info**.
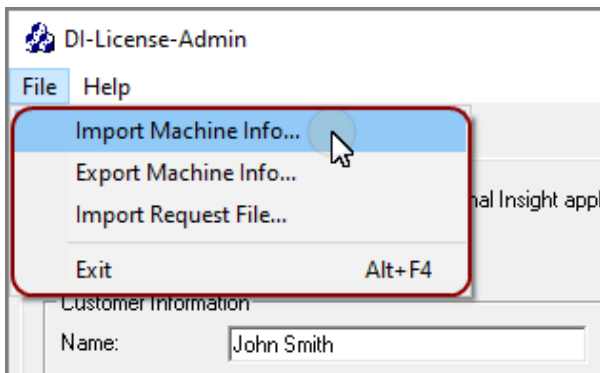
6. In the **Import Machine Info** dialog box, select the *info* file that you created and click **Open**.

   On the left side of the dialog box, the **Machine Name**, **Operating System**, and **Machine ID** boxes are populated with the machine information from the *info* file.

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

7. Complete the **Customer Information** section.
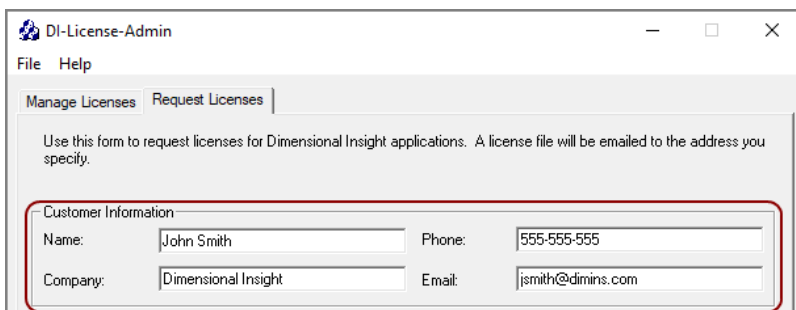
8. Specify details about the server-side licenses that you want to request:

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 Linux, 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.

9. 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**.

10. 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 the media access control (MAC) address of the machine that you want to request the licenses for (the one that was used to create the machine information file). For example:

Comments/Questions:
MAC Address: 28-D2-44-77-8A-E3

Save...   Submit

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**.

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

12. Click **Yes** to submit the license request.

13. Click **OK** to acknowledge the submission.

License Information Submitted   ✕

The license key request has been submitted

OK
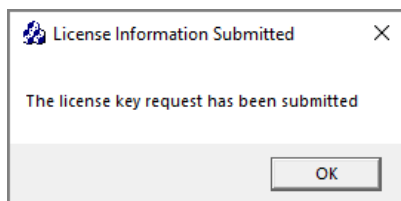
14. Click **Save** to store the license request file.

15. If necessary, move the *request* file to the Linux server.

16. On the Linux server, move the *request* file to the `/di/platform/licenses` directory by entering the following command:

```
sudo mv <request-file-name>.request
/di/platform/licenses
```

Using the Register Utility to Install a License File

After you receive your license file from Dimensional Insight, install it on your server, including the licenses that enable ProDiver and Workbench, which are installed on users' computers.

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

1. Copy the license *zip* file to the Linux server.

2. Copy the *zip* file to the `/di/platform/licenses` folder.

```
sudo mv <filename>.zip /di/platform/licenses
```

3. Navigate to the `/di/platform/licenses` folder.

```
cd /di/platform/licenses
```

4. Unzip the file.

```
sudo unzip <filename>.zip
```

5. Confirm that the *license* file is extracted

```
ls
```

```
chris@chris-VirtualBox:/di/platform/licenses$ ls
c3931_chris-virtualbox_platform71_p2130_m202211.license
Dimensional_Insight_Inc-chris-virtualbox-licenses-v7-20211115.zip
chris@chris-VirtualBox:/di/platform/licenses$
```

TIP: Take note the name of the license file. You will use it later in this procedure.

6. Navigate to the `/di/platform/executables` folder.

```
cd /di/platform/executables
```

7. Confirm that the register utility is in the directory.

```
ls
```

```
chris@chris-VirtualBox:/di/platform/licenses$ cd /di/platform/executables
chris@chris-VirtualBox:/di/platform/executables$ ls
dicfg   dictl   disch   exportinfo   genkey   libs   register
chris@chris-VirtualBox:/di/platform/executables$
```

8. View the permissions for the register utility.

```
ls -l register
```

The permissions display. If an `x` displays within the first group of letters (for example, `-rwxr--r--`), you can run the utility. Proceed to the next step

If you do not have permission to run the utility:

   a. Enable the execute permission.

```
sudo chmod a+x register
```

   b. Verify that the permissions have changed.

```
ls -l register
```

The permissions display as `-rwxr-xr-x`.

9. Move the register utility to the `/di/platform/diveline/bin` directory.

   ```
   sudo mv register diveline/bin
   ```

10. Go to the `/di/platform/diveline/bin` directory.

    ```
    cd ../diveline/bin
    ```

11. Confirm that the register utility is in the directory.

    ```
    ls
    ```

    The contents of the directory display, including the *register* file.

12. Run the register utility, and specify which *license* file to install.

    ```
    sudo ./register /di/platform/licenses/<license file
    name>.license
    ```

13. Confirm that the installation was successful.

    ```
    sudo ./register -l all
    ```

    A list of licenses that are currently installed on the server display, including the license file that you just installed.

14. Repeat this process for each license file that you want to install.

15. Repeat this procedure for each environment.

Installing DiveLine

Installing a DiveLine involves creating DiveLine users, using administer permissions, and modifying scripts using a text editor.

About Installing DiveLine

DiveLine is the server component of the Diver Platform. DiveLine authenticates users and controls access to data through Diver Platform clients such as Workbench, ProDiver, DivePort, and DiveTab.

DI recommends that you do the following before you install DiveLine for your site:

- Discuss the DiveLine Security and Authentication options with Technical Support to help determine the level and type of security for your DiveLine setup.
- If you expect your DiveLine clients to exchange information with users outside of the company firewall, discuss firewall requirements with Technical Support.

DiveLine typically resides behind a firewall on a corporate network. The system administrators need to configure the firewall and Domain Name System (DNS) so that internal and external customers can connect to DiveLine using the same host name and port number. Typically, you install DiveLine on port 2130, which needs to be open in the corporate firewall.

To set up and configure DiveLine inside a corporate network, consider the following:

- DiveLine communicates with clients using a proprietary protocol known as Dimensional Insight DiveLine Protocol (DIDP). You might need to configure your network to enable DIDP communications.
- Although configurable,by default, DiveLine accepts client connections on port 2130.
- Configure your routers and firewall so that DIDP traffic on port 2130 can reach the DiveLine service.
- Configure your firewall as a gateway for DIDP network traffic.
- Configure your firewall to transparently route two-way traffic on to the correct port to the DiveLine service.
- Typically, internal hosts (users inside the firewall) can connect directly to the DiveLine service, and external hosts connect to the network firewall, which then routes traffic to DiveLine.

- Clients connect to the DiveLine service using TCP/IP.
- If client computers are running Windows operating systems, ensure that the personal firewalls on these computers allow incoming connections from the port (for example, port 2130) that is used by DiveLine.

After installing DiveLine and Workbench, you can use Workbench tools to perform the following server-settings tasks:

- Reset the default authentication type
- Create users and groups and properties
- Set directory aliases
- Configure access controls

NOTE: The DiveLine service requires write access to Workbench projects (`/di/projects`), as well as to its data root (`/di/platform/dl-dataroot`).

Installing and Configuring DiveLine

Prerequisite: Uncompress the *di-diveline.tar.gz* file, as shown in <u>Extracting the Server Installation Package on page 21</u>, so that the `/di/platform/diveline` directory contains the following files and subdirectories:

- **bin**—Directory containing executable files used by the server
- **cgi-bin**—Directory containing the executable file for Web Server authentication
- **docs**—Directory containing a quick reference list for dicfg
- **html**—Directory containing *html* and *dlk* template files as well as a README file used with Web Server authentication
- **install-files**—Directory containing files that are used when installing DiveLine, some files of which need to be copied to other directories
- **samples**—Directory containing two sample models and DiveBooks for testing DiveLine
- **ENCRYPTION**—The OpenSSL license file
- **INSTALL**—Installation notes for 7.2
- **install-di-diveline**—The installation *shell* script
- **README**—Directory contents and support email address

NOTE: Text is case-sensitive in Linux.

To install and configure DiveLine:

1. Navigate to the `/diveline` directory by entering the following command:

   ```
   cd /di/platform/diveline
   ```

2. Check the directory contents for the *install-di-diveline* installation script by entering the following command:

   ```
   ls
   ```

3. View the permissions for the *install-di-diveline* installation script by entering the following command:

   ```
   ls -l install-di-diveline
   ```

   The permissions display. If the permissions are `-rwxr-xr-x`, you can run the utility. If you do not have permission to run the utility:

   a. Enable the execute permission.

      ```
      sudo chmod 755 install-di-diveline
      ```
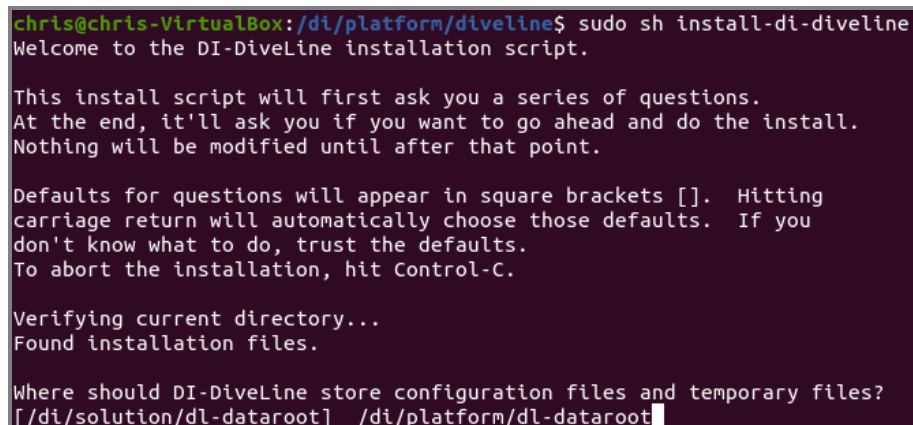
   b. Verify that the permissions have changed.

      ```
      ls -l install-di-diveline
      ```

      The permissions display as `-rwxr-xr-x`.

4. Run the install script by entering the following command:

   ```
   sudo sh install-di-diveline
   ```

```
chris@chris-VirtualBox:/di/platform/diveline$ sudo sh install-di-diveline
Welcome to the DI-DiveLine installation script.

This install script will first ask you a series of questions.
At the end, it'll ask you if you want to go ahead and do the install.
Nothing will be modified until after that point.

Defaults for questions will appear in square brackets [].  Hitting
carriage return will automatically choose those defaults.  If you
don't know what to do, trust the defaults.
To abort the installation, hit Control-C.

Verifying current directory...
Found installation files.

Where should DI-DiveLine store configuration files and temporary files?
[/di/solution/dl-dataroot]  /di/platform/dl-dataroot
```

The script begins with useful information about the question and answer process that follows including how to accept default suggestions or exiting the script. The answers given in this step are based on the fact that the server package was unzipped in the `/di/platform` directory.

NOTE: Press **Enter** to confirm the default, shown in brackets, or enter your response. Use **y** to answer yes and **n** to answer no.

The questions are:

- `Where should DI-DiveLine store configuration files and`
  `temporary files? [/di/solution/dl-dataroot]`

  The default location is `/di/platform/dl-dataroot` and needs manual entry if it is verified as the correct location.

  NOTE: Verify the location of your `dl-dataroot` directory before accepting the default or entering a new location.

- `What level of security should be configured for DI-`
  `DiveLine? [2]`

  The default security level is 2.

  There are three options to choose from:

  - **Level 0**—No security checking. All users have access to all models and DiveBooks in the models directory.
  - **Level 1**—Security checking is based on a web login. If a model is not listed in the configuration file, then all users have access to it.
  - **Level 2**—Security checking based on a web login. If a model is not listed in the ACL file, then no users have access to it.

- `Do you want to install a sample model and divebook? [y]`

  The default is `y`, or yes.

- `Go ahead and install? [y]`

  The default is `y`, or yes.

If not already installed, the script prompts you to create a new RSA private key and certificate files by entering information.

NOTE: A DI best practice is to create the private key and certificate files during the DiveLine installation.

For example:

- Country Code - **US**

  IMPORTANT: The country code must be two characters long.

- State/province - **MA**
- Location - **Burlington**
- Enter organization - **Dimensional Insight**

- Server name - **ubuntu**
- Email address - **jsmith@dimins.com**

```
OK.  Go ahead and install? [y]  y
Security Level: 2
Authentication Type: own
Debug Level: 0
One or both keypair files missing, generating new keypair
All fields are required.
Enter country code: US
Enter state/province: MA
Enter location: Burlington
Enter organization: Dimensional Insight
Enter server name: ubuntu
Enter email address: jsmith@dimins.com
Generating a 2048 bit RSA private key
Installing keypair
Done. You'll still need to:
 - edit bin/init-di-diveline to set the username, base directory, dataroot, and
port number
 - make sure you have a license installed
 - optionally configure the system to run bin/init-di-diveline on boot
 - Create a diveline admin user, with licensing set to Developer so you can logi
n
```

The script places the *privatekey.txt* and *certificate.pem* files in the `/di/platform/dl-dataroot/config` directory.

Alternatively, you can create the keypair files after the DiveLine installation. See **Creating and Configuring an Encryption Key** for instructions.

5. Navigate to the `/di/platform/dl-dataroot/` directory by entering the following command:

```
cd /di/platform/dl-dataroot/
```

6. View permissions for `/config` by entering the following command:

```
ls -l
```

The permissions display. If the permissions are `-rwxrwxrwx`, you can open and modify the directory and its contents. If you do not have permission:

a. Enable the execute permission.

```
sudo chmod a+rwx config
```

b. Verify that the permissions have changed.

```
ls -l config
```

The permissions display as `drwxrwxrwx`.

7. Verify that the keypair files (*privatekey.txt* and *certificate.pem*) are created successfully:

```
ls
```

8. Navigate to the `/di/platform/diveline/bin` directory by entering the following command:

```
cd /di/platform/diveline/bin
```

9. Confirm that the *init-di-diveline* file is in the directory by entering the following command:

```
ls
```

The contents of the directory display, including the *init-di-diveline* file.

10. View the permissions for the *init-di-diveline* file by entering the following command:

```
ls -l init-di-diveline
```

The permissions display. If the permissions are `-rwxrwxrwx`, you can modify the file. If you don't have permissions to edit the file:

a. Enable the execute permission.

```
sudo chmod a+rwx init-di-diveline
```

b. Verify that the permissions have changed.

```
ls -l init-di-diveline
```

The permissions display as `-rwxrwxrwx`.

11. Open the *init-di-diveline* script with a text editor, such as **gedit**, by entering a command similar to the following:

```
gedit init-di-diveline
```

The text editor opens.

```
###########################################################################
# Edit these variable assignments to suit your installation

# This is the user whose permissions will apply to everything the di-diveline
# does. (If not set, the script will not attempt to 'su')
DIDLUSER=diveline

# Important directory and port number settings
DIBASE=/di/solution

DIDATAROOT=$DIBASE/dl-dataroot
DIBINDIR=$DIBASE/diveline/bin
DISERVICE=di-service

# DiveLine clients such as ProDiver expect port 2130 unless told otherwise
DIPORTNUM=2131

# UMASK override. Uncomment if desired, leave alone if unsure.
#UMASK=002

# End of user-modifiable section
###########################################################################
```

The graphic displays the editable section of the script. The variable values are specific to the installation described in this guide.

12. For this installation, accept the variable defaults or make edits where necessary:

- `DIDLUSER=diveline`—The name of the user that runs the DiveLine server
- `DIBASE=/di/platform`—The location of the base DI Platform directory
- `DIDATAROOT=$DIBASE/dl-dataroot`—The location of the DiveLine `config`, `acl`, `cache`, `log`, and `data` directories
- `DIBINDIR=$DIBASE/diveline/bin`—The location of the DiveLine executable files
- `DISERVICE=di-service`—The name of the existing **di-service**
- `DIPORTNUM=2131`—The listening port for DiveLine on the server

  NOTE: Specify the port number that you chose when requesting a license. Port 2130 is the default.

13. Save and close the *init-di-diveline* file.

Creating an Administrator and a Test User

This procedure uses the **dicfg** command line tool to create an administrator and a test user for the initial DiveLine configuration.

NOTE: Setting environment variables is dependent on the shell you are using. This procedure uses the following **dicfg** format to create the administrator and test user:

```
./dicfg -dataroot $DIDATAROOT <dicfg commands>
```

`$DIDATAROOT` is the path to `/dl-dataroot` that is specified in the *init-di-diveline* file.

To create users for DiveLine:

1. Go to the `/executables` directory.
   ```
   cd /di/platform/executables
   ```
2. View the permissions for **dicfg**.
   ```
   ls -l dicfg
   ```

The permissions display. If the permissions are `-rwxrwxrwx`, you can create users. Proceed to step 3.

If you do not have permission to create users:

- Enable the execute permission.

```
sudo chmod a+rwx dicfg
```

- Verify that the permissions have changed.

```
ls -l dicfg
```

The permissions display as `-rwxrwxrwx`.

3. Create the administrator user ID.

```
sudo ./dicfg -dataroot /di/platform/dl-dataroot add
user -user <admin username> -password <admin password>
-administrator true
```

For example:

```
sudo ./dicfg -dataroot /di/platform/dl-dataroot add
user -user admin -password adminpassword -
administrator true
```

4. Create the test user ID.

```
sudo ./dicfg -dataroot /di/platform/dl-dataroot add
user -user <test user name> -password <test user
password>
```

For example:

```
sudo ./dicfg -dataroot /di/platform/dl-dataroot add
user -user tester -password testuserpassword
```

Creating a DiveLine Linux System User

To run the DiveLine service on a Linux machine, you must create an Administrative User account. For example, you might create a new user with the account name of "diveline." This user must have the right to "Log On As a Service" and have a strong password.

Your Linux administrator might have created a system user for DiveLine prior to the installation process. If so, record the name and password of the DiveLine user, or contact your administrator for assistance.

To create a Linux system user:

1. On the left panel, click the **System Settings** icon   .
   The **System Settings** page opens:
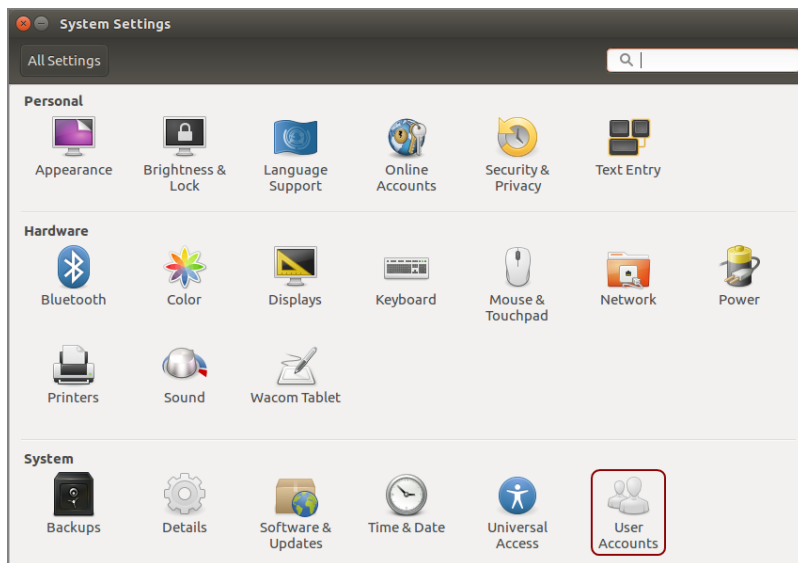
2. Double-click **User Accounts** .
   The **User Accounts** dialog box opens.
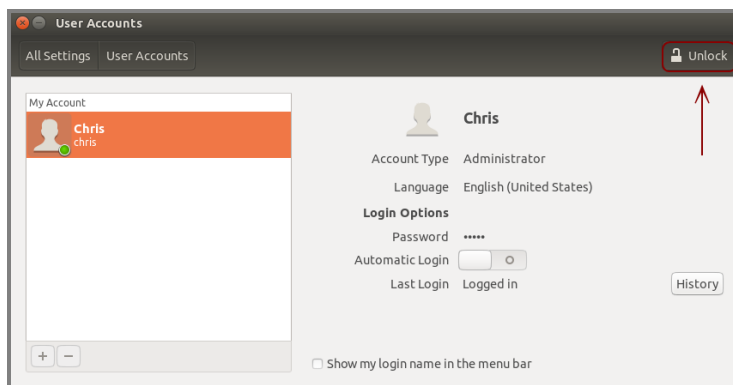
3. On the toolbar, click **Unlock** to enable editing.
   The **Authenticate** dialog box opens.

Creating a DiveLine Linux System User

41
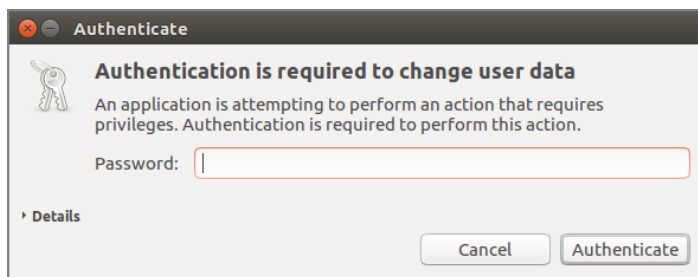
4. Enter your Password, and click **Authenticate**.

5. On the bottom left of the **User Accounts** window, click the plus sign .

   The **Add account** dialog box opens.
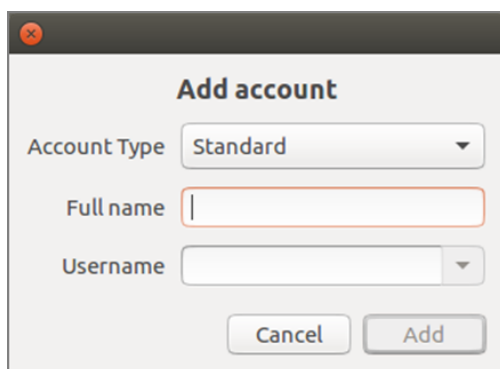
6. In the Add account dialog box:

   - Select the Account Type **Administrator**.

   - In the **Full name** and **Username** boxes, enter **diveline**, or another name of your choosing for running the DiveLine service.

     NOTE: Use the name that you identified for the `DIDLUSER` in Step 12 of Installing and Configuring DiveLine on page 34.

7. Click **Add**.

   Re-enter your password when prompted.

   The new account is now listed under **Other Accounts**.

8. Click **Account Disabled**.

   The changing password dialog box opens.

9. Enter a password in the **New password** and **Confirm password** boxes.

10. Click **Change** to display the updated **diveline** user account.

   The dialog box closes and the field next to **Password** changes to indicate a password is in use.

11. To enable automatic login for the DiveLine account, next to **Automatic Login**, click **OFF**.

   The option changes to **ON** and turns orange.
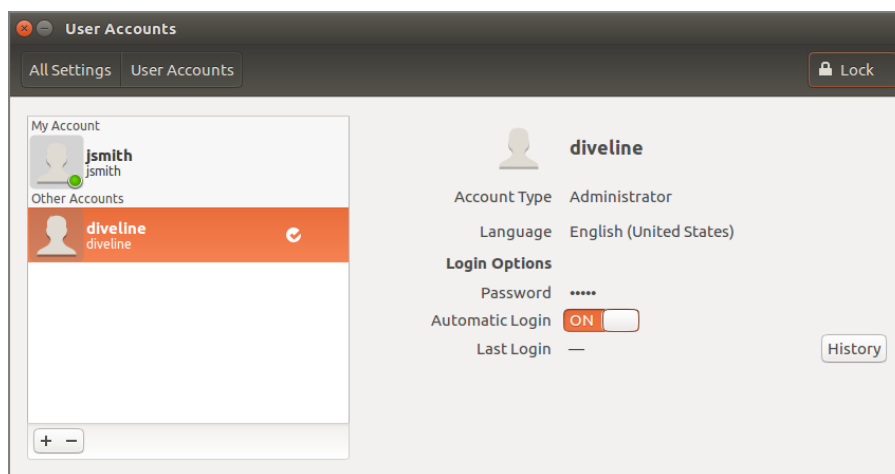
12. On the toolbar, click **Lock** and close the window.

Creating and Configuring an Encryption Key

Use the Java genkey tool, located in the `/executables` directory, to create an additional private key and certificate for encrypting software. Follow the instructions in this topic if you did not use the *install-di-diveline* script to create the *privatekey.txt* and *certificate.pem* files during the DiveLine installation.

Complete the following steps:

1. Go to the `/di/platform/executables` directory.

   ```
   cd /di/platform/executables
   ```

2. Use **genkey** and the following syntax to create an encryption key:

   ```
   ./genkey <country> <state> <location> <organization>
   <server name> <email address>
   ```

   For example:

   ```
   ./genkey US MA Burlington Dimensional Insight ubuntu
   jsmith@dimins.com
   ```

3. Go to the `/di/platform/dl-dataroot` directory.

   ```
   cd /di/platform/dl-dataroot
   ```

4. View permissions for `/config`.

   ```
   ls -l
   ```

   The permissions display.

If the permissions are `-rwxrwxrwx`, you can open and modify the directory and its contents. Proceed to step 5.

If you do not have permission:

    a. Enable the execute permission.

```
sudo chmod a+rwx config
```

    b. Verify that the permissions have changed.

```
ls -l config
```

       The permissions display as `drwxrwxrwx`.

5. Move the *privatekey.txt* and *certificate.pem* files to the `/dl-dataroot/config` directory.

```
mv privatekey.txt certificate.pem /di/platform/dl-dataroot/config
```

6. Go to the `/config` directory.

```
cd /di/platform/dl-dataroot/config
```

7. Verify that the *privatekey.txt* and *certificate.pem* files are present in the `/config` directory.

```
ls
```

Starting and Stopping the DiveLine Service

You can manually start, stop, and check the status of the DiveLine service by using the *init-di-diveline* file in the `/di/platform/diveline/bin` directory.

IMPORTANT: Before you start DiveLine for the first time, check the permissions of your `/di/platform/dl-dataroot` directory and the contents. If the permissions are `-rwxrwxrwx`, you can run the utility. If you do not have permission:

1. Navigate to the /di/platform directory by entering the following command:

```
cd /di/platform
```

2. Check the permissions by entering the following command:

```
ls -l dl-dataroot
```

```
chris@chris-VirtualBox:/di/platform$ ls -l dl-dataroot
total 36
drwxr-xr-x 3 root root 4096 Jan 18 13:51 acl
-rw-r--r-- 1 root root  122 Jan 18 13:51 acl.dir
drwxr-xr-x 2 root root 4096 Jan 18 13:51 cache
drwxr-x--- 2 root root 4096 Jan 18 13:51 config
drwxr-xr-x 3 root root 4096 Jan 18 13:51 data
drwxr-xr-x 3 root root 4096 Jan 18 13:51 logs-dicfg
drwxr-xr-x 2 root root 4096 Jan 18 13:51 security
drwxr-xr-x 2 root root 4096 Jan 18 13:51 temp
drwxr-xr-x 2 root root 4096 Jan 18 13:51 webdir
chris@chris-VirtualBox:/di/platform$
```

3. Enable the execute permission.

```
sudo chmod -R a+rwx dl-dataroot
```

NOTE: This changes the permissions for the dl-dataroot directory and it's contents.

4. Verify that the permissions have changed.

```
ls -l dl-dataroot
```

Navigate to the `/di/platform/diveline/bin` directory and enter the following commands to start, stop, restart, and check the status of the DiveLine service:

- Start DiveLine by entering the following command:

```
sudo sh init-di-diveline start
```

- Stop DiveLine by entering the following command:

```
sudo sh init-di-diveline stop
```

- Restart DiveLine by entering the following command:

```
sudo sh init-di-diveline restart
```

- Check the status of a running DiveLine (returns pid, port #, and path to `dl-dataroot` directory) by entering the following command:

```
sudo sh init-di-diveline status
```

Verifying the DiveLine Installation

Now that you can start and stop DiveLine, you can test the service to verify that it is running properly.

To verify DiveLine:

1. If it is not running, start DiveLine.:

```
sudo sh /di/platform/diveline/bin/init-di-diveline
start
```

2. Connect to the DiveLine port on the server using the following command syntax:

```
telnet <servername> <port number>
```

For example:

```
telnet ubuntu 2131
```

3. When you are connected, enter `?`.

   The DiveLine point release displays and validates the DiveLine installation.

```
?
DI-DiveLine 7.0 (56.2) SSL 64-bit
Start-up was completed successfully.
0
```

4. Enter `quit`.

   The connection closes.

NOTE: Alternatively, you can confirm a successful installation by connecting to your server using a client, such as ProDiver. When connecting from a client, enter the IP address of the Linux server.

Starting DiveLine Automatically at System Boot

To enable DiveLine to start automatically at system boot, you must configure your system startup scripts to include the path to the *init-di-diveline* file. Various versions of Linux have their own files where an administrator can list commands to run at startup. For more information, see to your system administrator or vendor documentation.

Installing Java and Tomcat

To use DiveLine and most client applications such as Workbench, DivePort, DiveTab, and more, you need to install Java and Tomcat software.

Downloading Java

At this point in the installation process, you must install (or have already installed) Java SE version 10 or later on your machine.

Prerequisite: Uninstall any older versions of Java SE.

This procedure uses OpenJDK.

NOTE: Consult with your Linux administrator to verify if they have downloaded the JDK package to your `/di/platform/downloads` directory, as well as set permissions on all directories in the DI structure.

NOTE: The following procedure is only necessary if JDK is not already installed on your computer.

To download the software, complete the following steps:

1. Open a web browser.
2. Open the Java Development Kit Builds page:

   https://jdk.java.net/21/

   NOTE: The appearance of the website can change over time.

   The OpenJDK JDK 21 General-Availability Release page opens.

3. Click **Linux/x64**, and download the file.

   The **Opening** download verification dialog box opens.
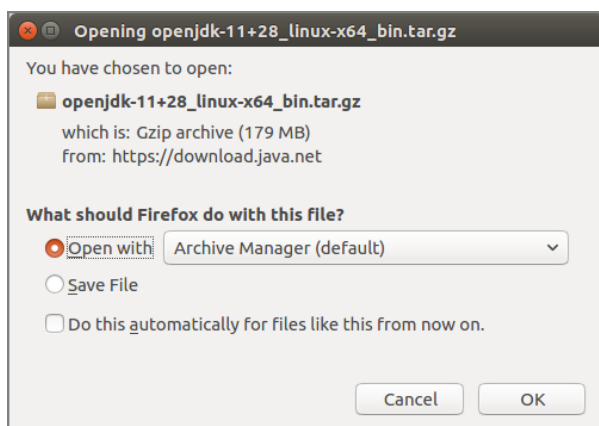
4. Select **Save File**.

5. Click **OK**.

   The software is saved to the default download directory.

6. Navigate to the file and move it to the `/di/platform/downloads` directory on your Linux server or VM.

```
sudo mv [openJDK file name].tar.gz
/di/platform/downloads
```

7. Navigate to the `/di/platform/downloads` directory.

```
cd /di/platform/downloads
```

8. Verify that the file copied correctly.

```
ls
```

9. Close the browser.

See **Installing the Java Development Kit** for instructions on how to install the Java software on a Linux server.

Installing Java Development Kit

Complete the following steps to install the software on a Linux machine. This procedure describes how to install the *openjdk-11+28_linux-x64_bin.tar.gz* package file.

Prerequisite: Download the latest version of the Java SE development kit.

NOTE: The individual steps required to install the software might vary at your site.

To install Java:

1. Go to the `/di/platform/downloads` directory.

```
cd /di/platform/downloads
```

2. Extract the JDK file.

```
sudo tar -xvzf openjdk-11+28_linux-x64_bin.tar.gz
```

The `-xvzf` arguments do the following:

- **x**—Extracts the files from the archive
- **v**—Lists all files as they are processed
- **z**—Uncompresses the files
- **f**—Names the file you are uncompressing

Press **Enter** to unpack the JDK package and create the `jdk-11` subdirectory.

3. Change to the `jdk-11` directory by entering the following command:

```
cd jdk-11
```

4. View the directory contents by entering the following command:

```
ls
```

```
chris@chris-VirtualBox:/di/platform/downloads$ cd jdk-11
chris@chris-VirtualBox:/di/platform/downloads/jdk-11$ ls
bin   conf   include   jmods   legal   lib   release
chris@chris-VirtualBox:/di/platform/downloads/jdk-11$
```

About Setting up an HTTPS Connection

The DivePort and NetDiver clients, can reside outside of the company firewall, must run over a secure Hypertext Transfer Protocol (HTTPS) with Transport Layer Security (TLS) connections to protect and ensure the integrity of data passing over the network.

An important part of the secure connection is obtaining, or creating, a certificate that guarantees message privacy and integrity. You must purchase and install a certificate on all servers that interact with DI web clients.

A certificate authority creates a digital TLS certificate, to establish a secure encrypted connection between a browser and a server. Whenever you run DivePort or NetDiver, the web browser points to a secured domain that requires a TLS handshake to authenticate both the server and the client.

A digital certificate verifies the identity of the requester and certifies that the requester meets all requirements to receive the certificate. The certificate provides the following security benefits:

- It contains personal information to help identify and trace the owner.
- It contains the information that is required to identify and contact the issuing authority.
- It is designed to be tamper-resistant and difficult to counterfeit.

A digital certificate issued by a certificate authority provides proof for verifying the identity of online entities using public and private keys.

Before enabling an TLS connection, you must install a site certificate using one of the following options:

- Purchase and install a certificate from a standard Certificate Authority, such as VeriSign or DigiCert. To request a certificate, you must create a Certificate Signing Request (CSR) from your server. Working with the issuer or instructions available, install the certificate in the Tomcat directory.

- Create a self-signed certificate using the Java genkey tool. Typically, you might generate and install a temporary self-signed certificate if you are in a trial or test phase and not concerned about receiving browser security warnings.

Before enabling the HTTPS connector, be sure that you have already installed the digital certificate in the Tomcat directory. This task is detailed in **Enabling the Default HTTPS Connector**.

Downloading Apache Tomcat

You must install (or have already installed) Apache Tomcat on your machine.

Dimensional Insight recommends that DivePort, NetDiver, and DiveTab software run on a Tomcat web server.

NOTE: DI recommendsTomcat 9.0.

To download Apache Tomcat:

1. Open a web browser.

2. Open the **Apache Tomcat** home page at:

   http://tomcat.apache.org

   The URL for this web site can change over time, but the home page is similar to the following:
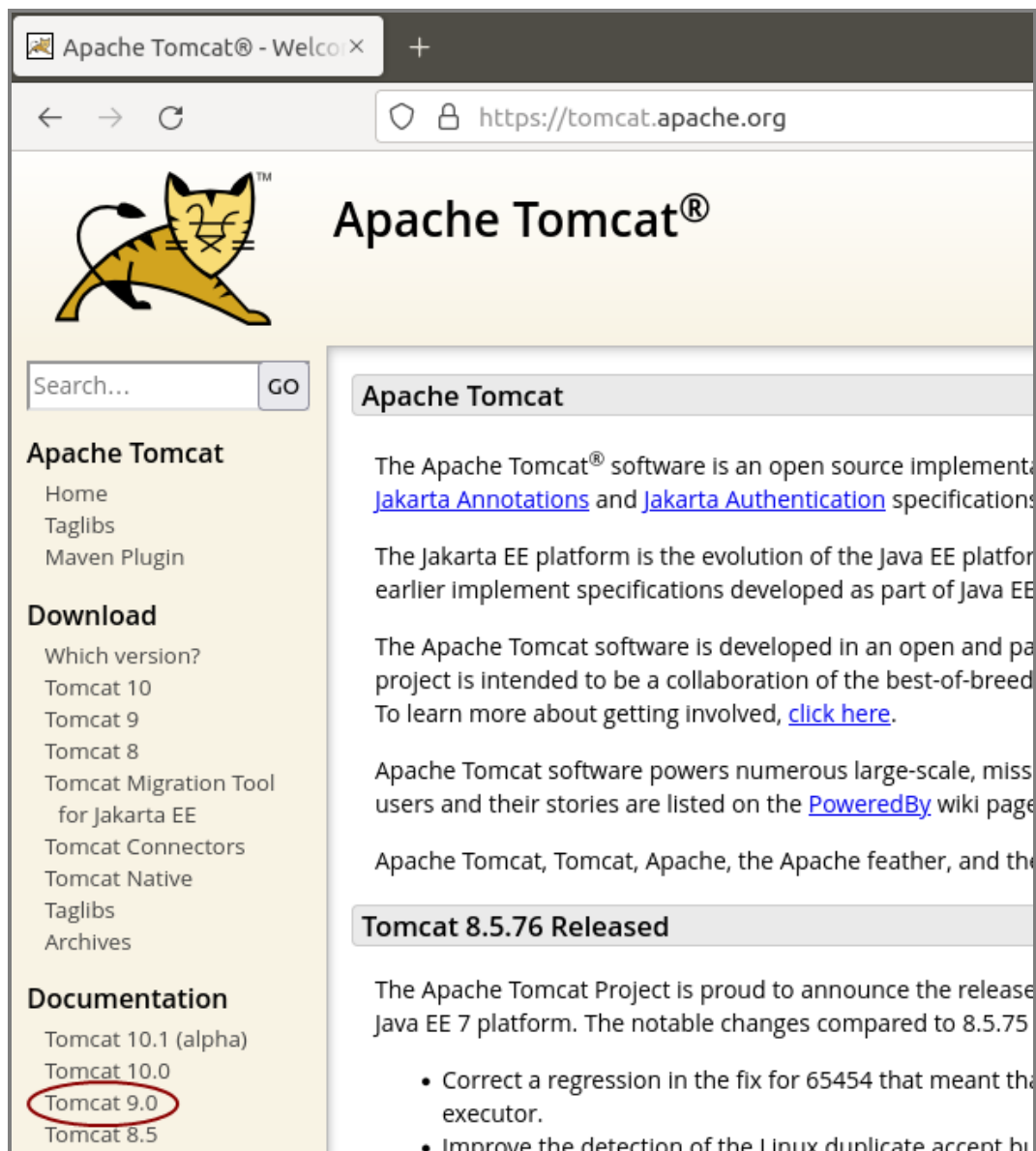
3. On the left pane, under Download, click **Tomcat <version number>** .

   The **Tomcat <version number> Software Downloads** page opens:

4. In the **Quick Navigation** section, click **the <version number>** to open the **Binary Distributions** section:

5. Click the **tar.gz** link.

   The **Opening** download verification dialog box opens.
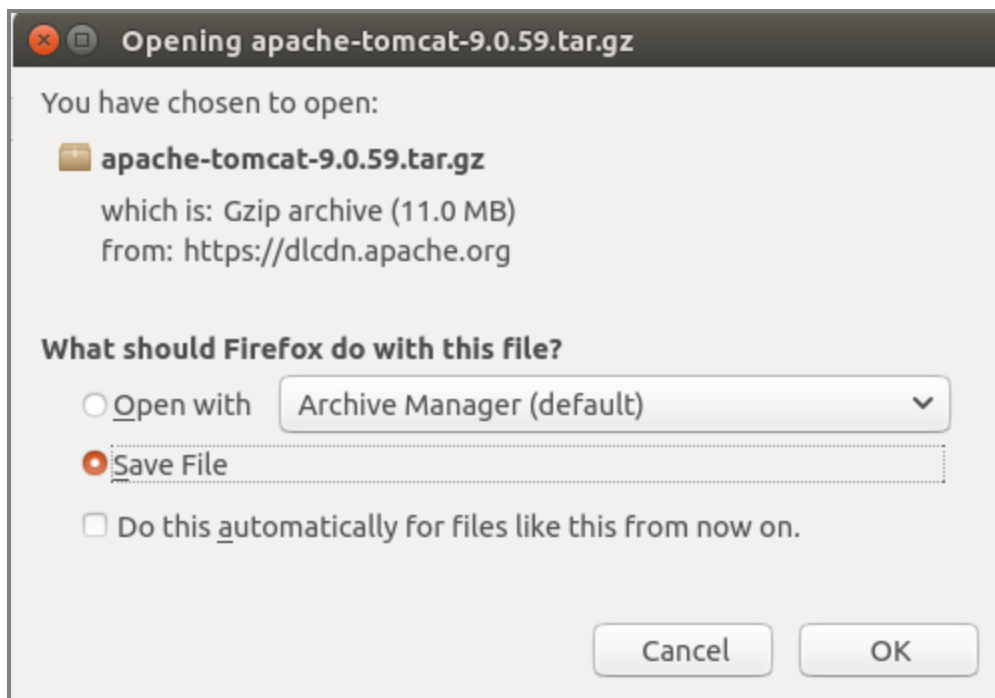
6. Select **Save File**.

7. Click **OK**.

   The file is downloaded to the `Downloads` directory on your local computer.

8. Navigate to the file location.

9. Move the file to the `/di/platform/downloads` directory

   ```
   sudo mv apache-tomcat-<version number>.tar.gz
   /di/platform/downloads
   ```

10. Navigate to the `/di/platform/downloads` directory

    ```
    cd /di/platform/downloads
    ```

11. Verify that the file moved correctly by entering the following command:

    ```
    ls
    ```

12. Close the web browser.

Installing Apache Tomcat

This page describes how to install Apache Tomcat using the apt-get utility. Apt-get is a free package management command line program. Apt-get works with Ubuntu's APT (Advanced Packaging Tool) library to perform the installation, deletion, or upgrading of new or existing software packages.

IMPORTANT: Individual steps required to install the software can vary at your site. depending on the distribution and version you are using.

NOTE: DI recommends Tomcat 9.0.

To install Apache Tomcat:

1. Navigate to the `/di/platform/downloads` directory.

   ```
   cd /di/platform/downloads
   ```

2. Decompress the *apache-tomcat-<version number>.tar.gz* file.

   ```
   sudo tar -xvzf apache-tomcat-<version number>.tar.gz
   ```

   The `-xvzf` arguments do the following:

   - **x**—Extracts the files from the archive
   - **v**—Lists all files as they are processed
   - **z**—Uncompresses the files
   - **f**—Names the file you are uncompressing
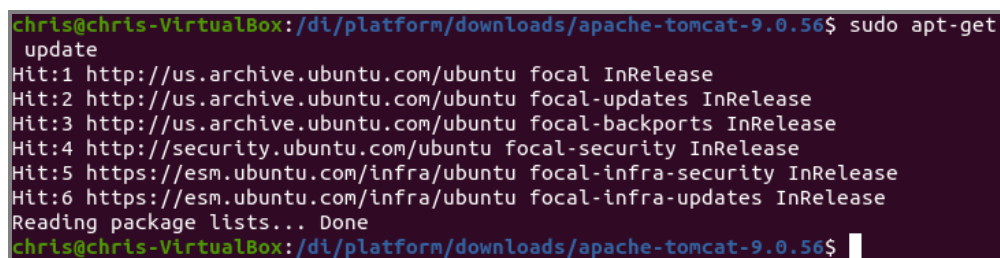
   The file unpacks and creates the `apache-tomcat-<version number>` subdirectory.

3. Go to the Apache Tomcat folder.

   ```
   cd apache-tomcat-<version number>
   ```

4. Update your apt-get package lists by entering the following command:

   ```
   sudo apt-get update
   ```

   ```
   chris@chris-VirtualBox:/di/platform/downloads/apache-tomcat-9.0.56$ sudo apt-get
    update
   Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
   Hit:2 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
   Hit:3 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
   Hit:4 http://security.ubuntu.com/ubuntu focal-security InRelease
   Hit:5 https://esm.ubuntu.com/infra/ubuntu focal-infra-security InRelease
   Hit:6 https://esm.ubuntu.com/infra/ubuntu focal-infra-updates InRelease
   Reading package lists... Done
   chris@chris-VirtualBox:/di/platform/downloads/apache-tomcat-9.0.56$
   ```

   NOTE: The apt-get utility works on a database of available packages. This command updates the database with any newer packages.

5. Start the Tomcat installation by entering a command similar to the following:

   ```
   sudo apt-get install tomcat<version number>
   ```

> **NOTE**: Apt-get installs Tomcat to the `/etc/tomcat<version number>` directory.

6. Navigate to the `/etc/default` directory .

```
cd /etc/default
```

7. View the permissions for the *tomcat<version number>* configuration file by entering a command similar to the following:

```
ls -l tomcat<version number>
```

The permissions display. If the permissions are `-rwxrwxwx`, you can run the utility. Proceed to step 9.

If you do not have permission to run the utility:

   a. Enable the execute permission.

```
sudo chmod a+rwx tomcat<version number>
```

   b. Verify that the permissions have changed.

```
ls -l tomcat<version number>
```

   The permissions display as `-rwxrwxrwx`.

> **NOTE**: If you are using SELinux on Red Hat 7.x, ensure that the webdata and webapps folders have the appropriate filesystem labels for Tomcat to be able to access them (for example, `tomcat_var_lib_t`). For more information, see Red Hat documentation.

8. Open the *tomcat<version number>* configuration file with a text editor, such as **gedit**, by entering a command similar to the following:

```
gedit tomcat<version number>
```

Here is an example of the configuration file:

TOMCAT9_USER=tomcat9 indicates the Tomcat user name on the machine.

9. Locate the JAVA_OPTS parameter (last line in the above figure) and replace it with the following:

```
JAVA_OPTS="-Djava.security.egd=file:/dev/./urandom –
Djava.awt.headless=true –Xms512m –Xmx1024m –
XX:MaxPermSize=256m –XX:+UseConcMarkSweepGC"
```

10. Change the TOMCAT9_SECURITY variable value to **no**, and remove the comment tag, #, at the beginning of the line.

11. Save and close the changed configuration file.

12. Change the ownership of webdata and operate on its files and sub-directories to enable Tomcat to write files to the DI webdata directory.

```
sudo chown –R tomcat<version number>
/di/platform/webdata
```

For example:

13. To start, restart, and stop the Tomcat server, navigate to the apache-tomcat-<version number>/bin directory with the following command:
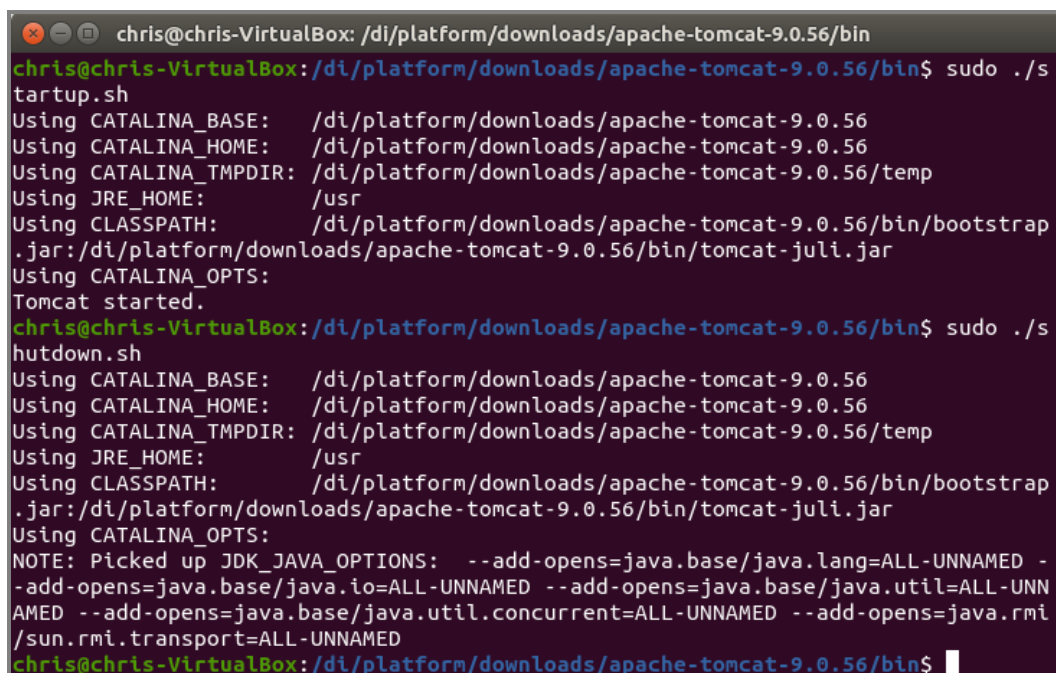
```
cd /di/platform/downloads/apache-tomcat-<version-
number>/bin
```

- Start Tomcat by entering the following command:

```
sudo ./startup.sh
```

- Stop Tomcat by entering the following command:

```
sudo ./shutdown.sh
```


14. With Tomcat running, open a web browser and enter the URL to test the Tomcat installation. Use the following format:

```
http://<server name>:8080
```

For example, `http://localhost:8080`

Press **Enter** to display a page similar to the following:
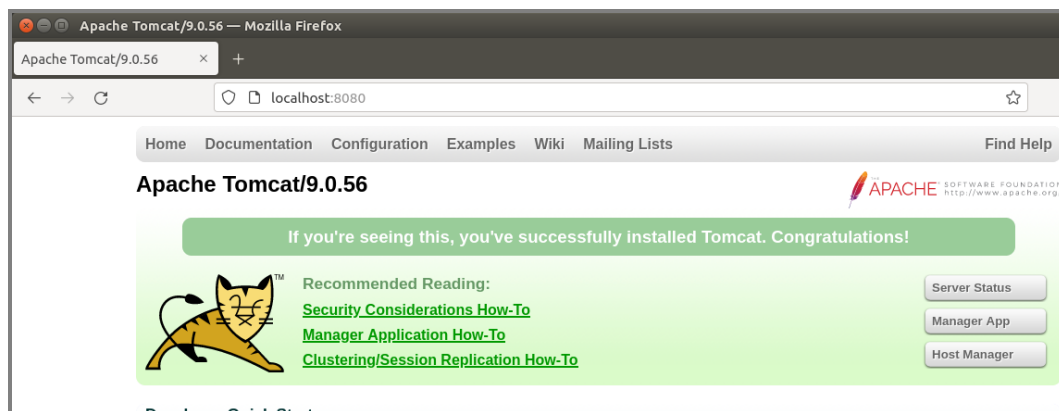
NOTE: It is possible to install Tomcat using a system account that is not an administrator, but this prevents full access to the machine. Be sure the user that Tomcat runs as has file system access to Tomcat's installation folder and subfolders, plus the DI `webapps` and `webdata` folders.

Generating an SSL/TLS Self-Signed Certificate

If you decide to generate your own self-signed certificate, adhere to the following prerequisites:

- Use a non-root user configured with **sudo** privileges
- Verify that the server has an installed Apache Tomcat web server
- Stop the Apache Tomcat service before beginning this process

NOTE: A self-signed certificate encrypts communication between your server and any web-based clients. However, because this certificate is not signed by any of the trusted certificate authorities included with web browsers, users cannot use the certificate to validate the identity of your server automatically.

SSL/TLS works by using a combination of a public certificate and a private key. The SSL/TLS key is kept secret on the server and is used to encrypt content sent to clients. The SSL/TLS certificate is publicly shared with anyone requesting content stored on the server. The certificate can also be used to decrypt the content signed by the associated SSL/TLS key.

To generate a self-signed certificate:

1. Change to the JDK `/bin` directory by entering a command similar to the following:

   ```
   cd /di/platform/downloads/jdk-<version number>/bin
   ```

2. Generate a certificate for Tomcat with the keytool utility by entering a command similar to the following:

```
sudo keytool -genkey -alias tomcat -keyalg RSA -
validity 1460 -keystore /etc/tomcat<version
number>/keystore -keypass tomcat -storepass tomcat
```

After pressing **Enter**, the command prompts you to enter information about your server that will be incorporated into the self-signed certificate and visible to anyone viewing the certificate. Accept any defaults or enter information specific to your server. The prompts appear as questions in the following order:

- `What is your first and last name?` – Do not enter your common name, instead enter the Fully Qualified Domain Name (FQDN) of the server. For example, `portal.mycompany.com`, where `portal` is the host name and `mycompany.com` is the domain name. For this example, enter the host name of the server, **ubuntu**.

  NOTE: Responses to the remaining command prompts are optional but recommended.

- `What is the name of your organizational unit?` – For example, **BI Software**.

- `What is the name of your organization?` – For example, **Dimensional Insight**.

- `What is the name of your City or Locality?` – For example, **Burlington**.

- `What is the name of your State or Province?` – For example, **MA**.

- `What is the two-letter country code for this unit?` – For example, **US**.

- At the confirmation prompt, for example:

  Is CN=ubuntu, OU=BI Software, O=Dimensional Insight, L=Burlington, ST=MA, C=US correct? [no]

  Type `Y` to confirm, and press **Enter**. `N`, or no, is the default.

3. Change to the Tomcat `etc` directory by entering a command similar to the following:

```
cd /etc/tomcat<version number>
```

4. Verify the creation of the *keystore* file by entering the following command:

```
ls
```

The *keystore* certificate file is valid for 1460 days and can be renewed upon expiration following the directions in this topic.

NOTE: You can restart the Tomcat service or leave it closed and move to the **Enabling the Default HTTPS Connector** for instructions on how to edit the *server.xml* file.

Enabling the Default HTTPS Connector

To establish a connection between DivePort and NetDiver clients and Tomcat, you must enable the HTTPS connector by editing the *server.xml* file.

1. If Tomcat is running, stop it.
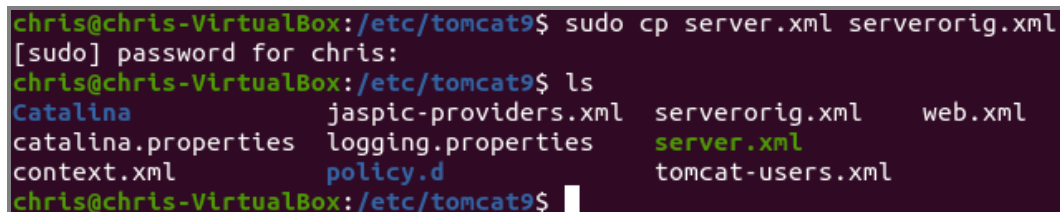
```
sudo /di/platform/downloads/apache-tomcat-<version-
number>/bin ./shutdown.sh
```

2. Go to the Tomcat directory (`/etc/tomcat<version-number>`)

```
cd /etc/tomcat<version-number>
```

3. Make a backup copy of the *server.xml* file called *serverorig.xml*

```
sudo cp server.xml serverorig.xml
```


4. Verify that the file is copied correctly by entering the following command:

```
ls
```

5. View the permissions of the *server.xml* file

```
ls -l server.xml
```

The permissions display. If the permissions are `-rwxrwxrwx`, you can edit the file.

If you do not have permissions:

- Enable the execute permission.

```
sudo chmod a+rwx server.xml
```

- Verify that the permissions have changed.

```
ls -l server.xml
```

6. Open the *server.xml* file using a text editor, such as gedit.

```
gedit server.xml
```

7. Locate the section beginning with `Define an SSL/TLS HTTP/1.1 Connector on port 8443.`

```
    <!-- Define an SSL/TLS HTTP/1.1 Connector on port 8443
         This connector uses the NIO implementation. The default
         SSLImplementation will depend on the presence of the APR/native
         library and the useOpenSSL attribute of the
         AprLifecycleListener.
         Either JSSE or OpenSSL style configuration may be used regardless of
         the SSLImplementation selected. JSSE style configuration is used below.
    -->
    <!--
    <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="200" SSLEnabled="true" secure="true" scheme="https" clientAuth="false"
sslProtocol="TLS" maxHttpHeaderSize="8192" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true" acceptCount="100" URIEncoding="UTF-8"
keystorePass="tomcat" keystoreFile="etc/tomcat9/keystore">
```

8. In the "Define an SSL/TLS HTTP/1.1 Connector on port 8443" and "Connector port" sections of the *server.xml* file, make the following edits:

   a. Remove the commented lines beginning with "This connector..." and ending with "used below".

   b. After `<Connector port= "8443"`, add the following attributes:

```
        SSLEnabled="true"
        maxHttpHeaderSize="8192"
        minSpareThreads="25"
        maxSpareThreads="75"
        enableLookups="false"
        disableUploadTimeout="true"
        acceptCount="100"
        URIEncoding="UTF-8"
        keystorePass="tomcat"
        keystoreFile="/etc/tomcat9/keystore"
```

9. Remove the comment symbols, (`<!--` and `-->`) around the `<Connector Port= ... />` section. The file appears as follows:

```
    <!-- Define an SSL/TLS HTTP/1.1 Connector on port 8443-->

    <Connector port="8443" SSLEnabled="true" maxHttpHeaderSize="8192" minSpareThreads="25"
maxSpareThreads="75"  enableLookups="false" disableUploadTimeout="true" acceptCount="100"
URIEncoding="UTF-8"  keystorePass="tomcat" keystoreFile="/etc/tomcat9/keystore">
    </Connector>
```

10. Save and close the *server.xml* file.

11. Start Tomcat.

    ```
    sudo /di/platform/downloads/apache-tomcat-<version-
    number>/bin ./startup.sh
    ```

NOTES:

- When DivePort software generates URLs, non-ASCII characters are encoded to ensure that the URL only contains ASCII characters. For these generated strings, ISO-8859-1 or UTF-8 encoding is acceptable.

- If users intend to enter URLs that contain non-ASCII characters, set the URIEncoding on the Tomcat connector according to the encoding that they intend to use.

Verifying the HTTPS Connection

You can verify the HTTPS connection for Tomcat by opening a browser window and connecting through the TLS port URL. The first time you attempt to connect to your Tomcat web server through a self-signed certificate using HTTPS, you can expect warnings from the browser when it attempts to authenticate with Tomcat. You might encounter the following:

- A browser might display a warning message similar to "There is a problem with this website's security certificate".

- The Microsoft Internet Explorer browser asks you to click the **Continue to this website (not recommended)** warning message before opening the Tomcat home page on the secure port.

- Most browsers allow you to accept the self-signed certificate permanently.

- If you restart the browser and enter **https://<servername>:<portnumber>**, the default Tomcat home page should display without a security warning.

NOTE: If you encounter any HTTPS errors when logging into Tomcat, refer to your logs for troubleshooting information.

This procedure uses the Mozilla Firefox browser.

To verify the HTTPS connection, complete the following steps:

1. Open a browser window, and enter a URL with the following syntax:

   `https://<servername or IP address>:8443`

   For example:
   `https://localhost:8443`

2. Press **Enter** to display the following security screen in the Firefox browser:
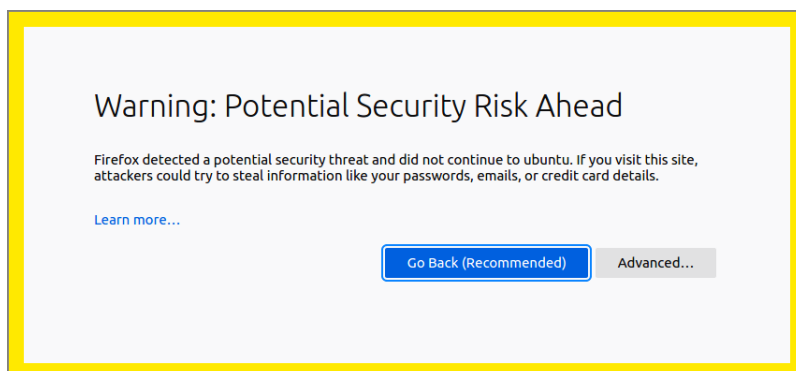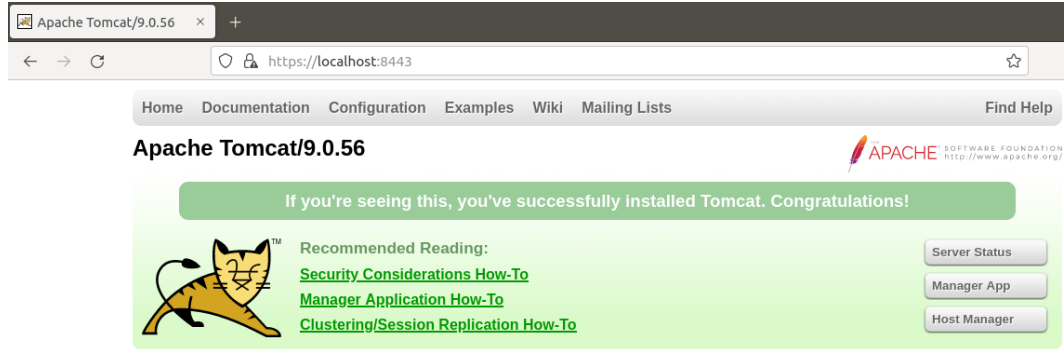
3. Click **Advanced** to view additional information.
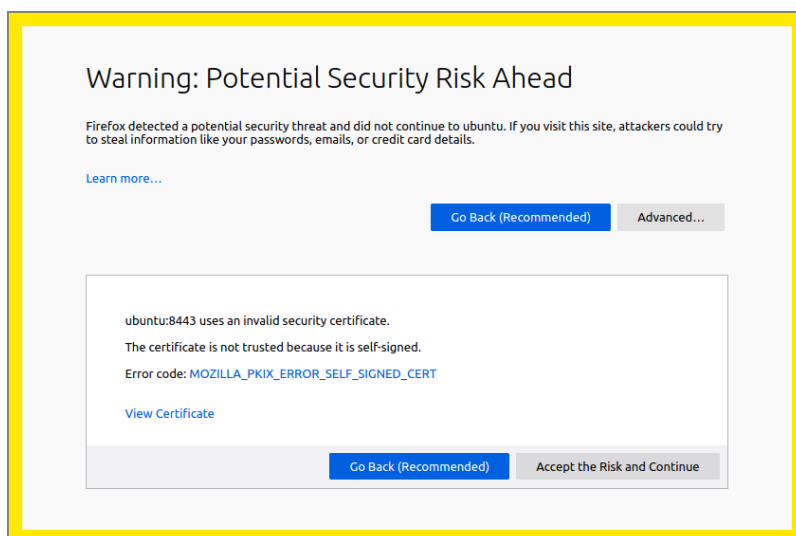
4. Click **Accept the Risk and Continue** to enable the connection to the Tomcat web server.

   The confirmation page displays.

   NOTE: The confirmation page might differ depending on the version of Tomcat.

Verifying the HTTPS Connection

DivePort

Installing DivePort

DivePort is a web client that employs portlet web technology. A DivePort portal consists of pages that contain portlet instances. DivePort enables you to create and configure pages and their portlet instances. DivePort typically resides on Apache Tomcat, a web application server, which you can access by using a web browser.

Prerequisite: The successful installation of Apache Tomcat and DiveLine. The DivePort installation files are in the *web-tools.zip* file which comes bundled with the Diver Platform Server package.

To extract and copy the DivePort installation files:

1. If Tomcat is running, stop it.

2. Navigate to the `/di/platform` directory .

   ```
   cd /di/platform
   ```

3. Verify that the *web-tools.zip* file is present.

   ```
   ls
   ```

4. Unzip *web-tools.zip* file.

   ```
   sudo unzip web-tools.zip
   ```


5. View the unpackaged *web-tools.zip* file in the directory.

   ```
   ls
   ```


6. Unzip *diveport.zip*.

   ```
   sudo unzip diveport.zip
   ```

7. Navigate to the `diveport` directory.

```
cd diveport
```

8. View the unpackaged *diveport.zip* file.

```
ls
```

The unzipped DivePort package creates the following directories and file in the `diveport` directory:

- `/appdir`
- `/datadir`
- *context-file-template.xml*

9. Copy the `appdir` directory to the `/di/platform/webapps` directory and rename it to assign a DivePort portal name (for example, **mydiveport**).

```
sudo cp -r appdir /di/platform/webapps/mydiveport
```

10. Copy the `datadir` directory to the `/di/platform/webdata` directory and rename it to the same DivePort portal name (for example, **mydiveport**).

```
sudo cp -r datadir /di/platform/webdata/mydiveport
```

11. Verify that the files were renamed and copied.

- `ls /di/platform/webapps`
- `ls /di/platform/webdata`

12. Navigate to the `/etc/init.d` directory.

```
cd /etc/init.d
```

13. Determine the IP address of your Linux machine

```
ifconfig
```

```
jsmith@ubuntu:/etc/init.d$ ifconfig
ens33     Link encap:Ethernet  HWaddr 28:d2:44:77:8a:e3
          inet addr:192.168.179.140  Bcast:192.168.179.255  Mask:255.255.255.0
          inet6 addr: fe80::d72e:2c81:95c2:a46e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:18456 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5458 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19805591 (19.8 MB)  TX bytes:608962 (608.9 KB)
```

14. Note the IP address (`inet addr`) that displays.

For example, 192.168.179.140 is the IP address that displays in the figure.

15. Specify whether you want the DivePort name to display in the URL to your portal (for example, **https://www.<your server>.com/<DivePort name>**).

(Recommended) To display `<DivePort name>` in the URL:

a. Navigate to the `/di/platform/diveport` directory.

```
cd /di/platform/diveport
```

b. Create a copy of the *context-file-template.xml* file and rename it to the name of your DivePort portal file (for example, *mydiveport.xml*).

```
sudo cp -i context-file-template.xml
mydiveport.xml
```

c. Verifythe permissions of the *<DivePort name>.xml* file.

```
ls -l mydiveport.xml
```

The permissions display. If the permissions are `-rwxrwxrwx`, you can open and modify the directory and its contents. Proceed to step 15 d.

If you do not have permission:

i. Enable the execute permission.

```
sudo chmod a+rwx mydiveport.xml
```

ii. Verify that the permissions have changed.

```
ls -l mydiveport.xml
```

The permissions display as `-rwxrwxrwx`.

d. Open the *<DivePort name>.xml* file with a text editor, such as **gedit**.

```
gedit mydiveport.xml
```

The file opens in the text editor.

```
<Context docBase="Enter DivePort War File Path Here" unpackWAR="false"
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 DLCGI
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" />
    -->
        <!-- For Tomcat 8.5.42+ or 9.0.12+, the following is recommended:
    <CookieProcessor sameSiteCookies="lax" />
    -->
</Context>
```

e. Edit the *<DivePort name>.xml* file to include the following changes:

- "`Enter DivePort War File Path Here`" – The path to the *diveport.war* file

    For example:

    `/di/platform/webapps/mydiveport/diveport.war`

- "`Enter DivePort Webdata Directory Here`" – The path to the `webdata` directory (`dataroot`)

    For example:

    `/di/platform/webdata/mydiveport`

- "`Enter DivePort WebApp Directory Here`" – The path to the `webapps` directory (`approot`)

    For example:

    `/di/platform/webapps/mydiveport`

- "`Enter DiveLine Server String Here`" – The DiveLine server name

    For example:

    `ubuntu:2131`

- "`Enter Admin Username Here`" – The DiveLine administrator name, which is defined in [Creating an Administrator and a Test User on page 39](#).

    For example:

    `admin`

f. Remove `uncomment this and set the following parameters:` and the surrounding comment markers (`<!--` and `-->`).

    For example:

```
<Context
docBase
="/di/platform/webapps/mydiveport/diveport.war"
 unpackWAR="false" sessionCookiePathUsesTrailingSlash="false">
      <Parameter
name="dataroot" value="/di/platform/webdata/mydiveport" />
      <Parameter
name="approot" value="/di/platform/webapps/mydiveport" />
      <Parameter name="diveline.server" value="ubuntu:2131" />
      <Parameter name="diveline.admin-username" value="admin" />
      (Optional) for single-sign-on with a CGI-mode
installation, set these parameters:
      <Parameter name="diveline.web-auth-start-url" value="Enter DLCGI
DivePort URL Here"/>
      <Parameter name="diveline.web-auth-finish-url" value="Enter Logoff
URL Here"/>
      (Optional) If you need to permit HTTP connections:
      <Parameter name="require-confidentiality" value="false" />
      <CookieProcessor sameSiteCookies="lax" />
</Context>
```

IMPORTANT: If you do not require HTTP connections, comment out the **require-confidentiality** parameter. If you permit HTTP connections, you are allowing unsecured communications with DiveLine.

g. Save your changes and close the file.

16. Move the file that you just created (either *mydiveport.xml* or *ROOT.xml*) to the Tomcat `localhost` directory.

```
sudo mv <file name>.xml /etc/tomcat<version-
number>/Catalina/localhost
```

17. Navigate to the `/etc` directory.

```
cd /etc
```

18. Change the ownership for the `tomcat<version>` directory to the Tomcat user, identified in .

```
sudo chown -R tomcat<version-number> ./tomcat<version-
number>
```

19. Change to the directory holding the *atlcfg.cfg* file.

```
cd /di/platform/dl-dataroot/config
```

20. Check the permissions of the *atlcfg.cfg* file.

```
ls -l atlcfg.cfg
```

The permissions display. If the permissions are `-rwxrwxrwx`, you can open and modify the directory and its contents. If you do not have permission:

   a. Enable the execute permission.

```
sudo chmod a+rwx atlcfg.cfg
```

   b. Verify that the permissions have changed.

```
ls -l atlcfg.cfg
```

   The permissions display as `-rwxrwxrwx`.

21. Open the file with a text editor, such as **gedit**.

```
gedit atlcfg.cfg
```

22. Locate the `ACFG` object, and insert the `gateway_ips` attribute with IP address information.

    For example:

```
gateway_ips={"192.168.179.140","127.0.0.1"}
```

    Here is an example of the attribute in the *atlcfg.cfg* file:

```
version "1";
// Computer generated object language file
object 'ACFG' "main" {
        security_level=2,
        auth_scheme="own",
        debug=0,
        user_levels_migrated="true"
        gateway_ips={"192.168.179.140","127.0.0.1"}
};
```

23. Optionally, if not already configured, add an administrative user to the *atlcfg.cfg* file.

    NOTE: Remember to enter a comma at the end of all lines within the **ACFG** object except the last one.

24. Save and close the file.

25. Start Tomcat.

NOTE: The server IP address can change when you restart the server. The server IP address shown in examples might change in different topics due to restarting the test server.

Verifying the DivePort Installation

Verify that your DivePort installation is working by entering the DivePort URL in a web browser.

Prerequisite: Download, install, and configure DivePort.

1. Enter your DivePort URL with the following syntax:

```
https://<servername or IP address>:8443/<DivePort name>
```

For example:

```
https://ubuntu:8443/mydiveport
```

NOTE: If the server name does not work, use the IP address of the DiveLine server.

If you have problems connecting to DivePort, review your logs and the configuration changes made to the *mydiveport.xml* and *atlcfg.cfg* files. The example URL reflects changes made in the **Installing DivePort** section. Additionally, if the Linux server is running on a VM, verify that you have configured the network connection options correctly. For example, the **Virtual Machine Settings** > **Network Adapter** options for an Ubuntu server appear as follows:
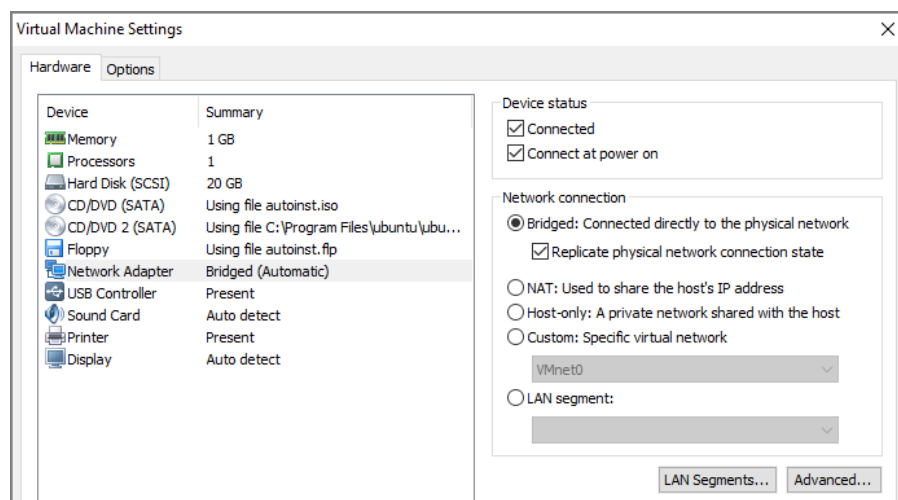
2. In the Network connection section, enable the following options:
   - Bridged: Connected directly to the physical network
   - Replicate physical network connection state
3. If you have successfully installed DivePort, the **Welcome to DivePort** page opens.

Verifying the DivePort Installation

73
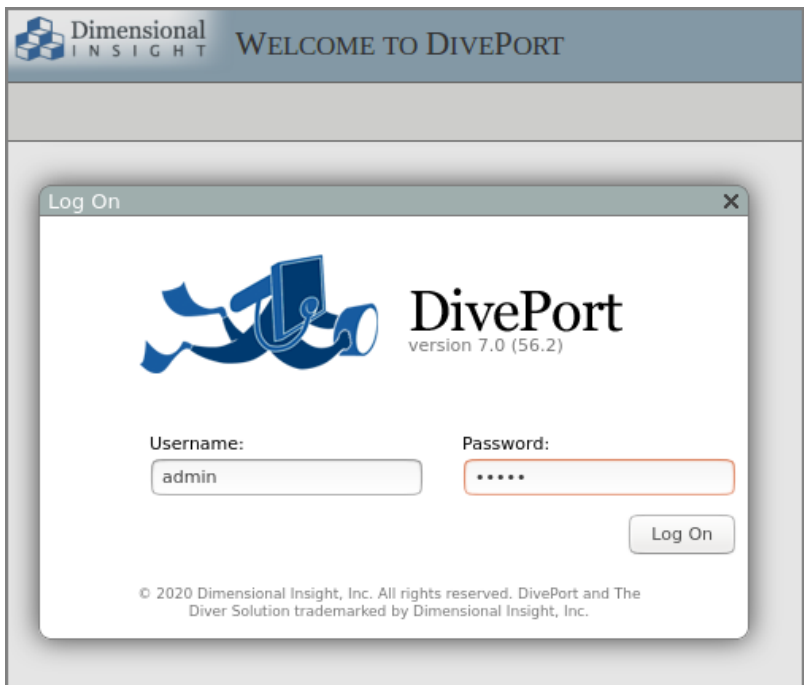
4. If you installed a self-signed certificate and you have not previously logged in to the Linux server with a DI client, such as DivePort, the client displays a **Verify Certificate** dialog box:

5. Different browsers display different security warnings the first time you log in to the server with a web-based DI client. If the dialog box presented is different from the one shown above, follow the online instructions to permanently accept the certificate.

   Click **Accept** to trust the certificate.

6. When connected and logged in to DivePort, click **HELP** > **About** to open the **About DivePort** window and verify the version numbers of DiveLine and DivePort.

7. Click **OK**.
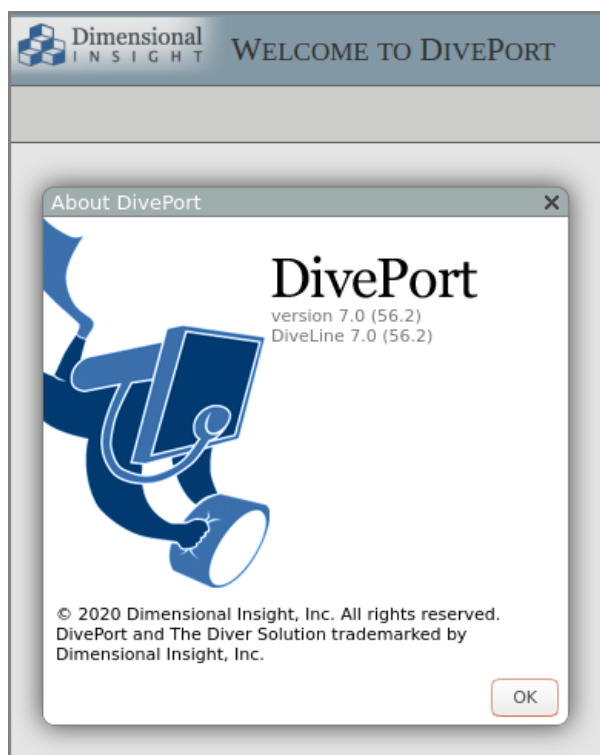
8. ClSelect **HELP** > **View User Help** to open the Help system in a new tab in your browser.

NOTE: DivePort administrators have access to *DivePort Administrator Help*, as well as *DivePort User Help*.

Appendix: DivePort Installation

The following optional process suppresses the name of your DivePort in the URL:

1. Go to the `/di/platform/diveport` directory by entering the following command:

```
cd /di/platform/diveport
```

2. Create a copy of the *context-file-template.xml* file and rename it *ROOT.xml* by entering the following command:

```
sudo cp -i context-file-template.xml ROOT.xml
```

3. Open the *ROOT.xml* file with a text editor, such as **gedit**, by entering a command similar to the following:

```
gedit ROOT.xml
```

```xml
<Context docBase="Enter DivePort War File Path Here" unpackWAR="false"
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 DLCGI 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" />
   -->
</Context>
```

4. Edit the *ROOT.xml* file to include the following changes:

   - `"Enter DivePort War File Path Here"` – The path to the *diveport.war* file

     For example:

     `/di/platform/webapps/mydiveport/diveport.war`

   - `"Enter DivePort Webdata Directory Here"` – The path to the `webdata` directory (`dataroot`)

     For example:

     `/di/platform/webdata/mydiveport`

   - `"Enter DivePort WebApp Directory Here"` – The path to the `webapps` directory (`approot`)

     For example:

     `/di/platform/webapps/mydiveport`

   - `"Enter DiveLine Server String Here"` – The DiveLine server name

     For example:

     `ubuntu:2131`

- **"Enter Admin Username Here"** – The DiveLine administrator name, which is defined in [Creating an Administrator and a Test User on page 39](#).

  For example:

  ```
  admin
  ```

- To suppress the `<diveport name>` in the URL, add the `node-id` parameter with a value of `Servername (/)`.

  For example:

  ```
  <Parameter name="node-id" value="ubuntu:2131" />
  ```

5. Remove `uncomment this and set the following parameters:` and the surrounding comment markers (`<!--` and `-->`).

   For example:

   ```
   <Context
   docBase
   ="/di/platform/webapps/mydiveport/diveport.war"
   unpackWAR="false" sessionCookiePathUsesTrailingSlash="false">
       <Parameter name="dataroot" value="/di/platform/webdata/mydiveport" />
       <Parameter name="approot" value="/di/platform/webapps/mydiveport" />
       <Parameter name="diveline.server" value="ubuntu:2131" PR 39377/>
       <Parameter name="diveline.admin-username" value="admin" />
       <Parameter name="node-id" value="ubuntu:2131" />
       (Optional) for single-sign-on with a CGI-mode installation,
   set these parameters:
       <Parameter name="diveline.web-auth-start-url" value="Enter DLCGI DivePort
   URL Here"/>
       <Parameter name="diveline.web-auth-finish-url" value="Enter Logoff URL
   Here"/>
       (Optional) If you need to permit HTTP connections:
       <Parameter name="require-confidentiality" value="false" />
   </Context>
   ```

   IMPORTANT: If you do not require HTTP connections, comment out the `require-confidentiality` parameter. If you permit HTTP connections, you are allowing unsecured communications with DiveLine.

6. Save your changes and close the file.

NetDiver

Installing NetDiver

NetDiver is the web-based analytics client of the Diver Platform. NetDiver provides ad hoc reporting and analytics tools in a web browser.

Prerequisite: Install Apache Tomcat and DiveLine before you install NetDiver.

To install NetDiver:

1. If running, stop the Tomcat web server.

2. Navigate to the `/di/platform` directory.

   ```
   cd /di/platform
   ```

3. Unzip the *netdiver.zip* file.

   ```
   sudo unzip netdiver.zip
   ```

4. Navigate to the `netdiver` directory.

   ```
   cd netdiver
   ```

5. View the unzipped *netdiver.zip* file.

   ```
   ls -l
   ```

   The unzipped NetDiver package creates the following directories and file in the `netdiver` directory:

   - `/appdir`
   - `/datadir`
   - *context-file-template.xml*

6. Copy the `appdir` directory to the `/di/platform/webapps` directory and rename it to assign a NetDiver portal name (for example, **mynetdiver**).

   ```
   sudo cp -r appdir /di/platform/webapps/mynetdiver
   ```

7. Copy the `datadir` directory to the `/di/platform/webdata` directory and rename it to the same NetDiver portal name (for example, **mynetdiver**).

   ```
   sudo cp -r datadir /di/platform/webdata/mynetdiver
   ```

8. Navigate to the `/di/platform/netdiver` directory.

   ```
   cd /di/platform/netdiver
   ```

9. Create a copy of the *context-file-template.xml* file and rename it to the name of your NetDiver portal (for example, *mynetdiver.xml*).

   ```
   sudo cp -i context-file-template.xml mynetdiver.xml
   ```

10. Check the permissions of the *mynetdiver.xml* file.

```
ls -l mynetdiver.xml
```

The permissions display. If the permissions are `-rwxrwxrwx`, you can open and modify the directory and its contents. If you do not have permission:

    a. Enable the execute permission.

```
sudo chmod a+rwx mynetdiver.xml
```

    b. Verify that the permissions have changed.

```
ls -l mynetdiver.xml
```

The permissions display as `-rwxrwxrwx`.

11. Open the *<NetDiver name>.xml* file with a text editor, such as **gedit**.

```
gedit mynetdiver.xml
```

The file opens in the text editor.

```xml
<Context docBase="Enter NetDiver War File Path Here" unpackWAR="false"
sessionCookiePathUsesTrailingSlash="false">
    <!-- uncomment this and set the following parameters:
  <Parameter name="netdiver.dataroot" value="Enter NetDiver WebSite Directory
Here" />
  <Parameter name="approot" value="Enter Path To Directory Which Contains
NetDiver War File Here" />
  <Parameter name="diveline.server" value="Enter Default DiveLine Server String
Here" />
  <Parameter name="diveline.allow-server-change" value="false" />
  -->
    <!-- If you need to permit HTTP connections:
  <Parameter name="require-confidentiality" value="false" />
  -->
    <!-- For Tomcat 8.5.42+ or 9.0.12+, the following is recommended:
  <CookieProcessor sameSiteCookies="lax" />
  -->
</Context>
```

12. Edit the *<NetDiver name>.xml* file to include the following changes:

- `"Enter NetDiver War File Path Here"` – The path to the *netdiver.war* file

  For example:

  ```
  /di/platform/webapps/mynetdiver/netdiver.war
  ```

- `"Enter NetDiver WebSite Directory Here"` – The path to the `webdata` directory (`dataroot`)

  For example:

```
/di/platform/webdata/mynetdiver
```

- **"Enter Path to Directory Which Contains NetDiver War File Here"** – The path to the `webapps` directory (`approot`)

  For example:

  ```
  /di/platform/webapps/mynetdiver
  ```

- **"Enter Default DiveLine Server String Here"** – The DiveLine server name

  For example:

  ```
  ubuntu:2131
  ```

- Change the **"diveline.allow-server-change"** parameter value to `true`

Optionally, you can permit unsecured HTTP connections and export to *xlsx* instead of *xls* Excel file extensions.

13. Remove `uncomment this and set the following parameters:` and the surrounding comment markers (`<!--` and `-->`).

    For example:

    ```
    <Context
    docBase
    ="/di/platform/webapps/mynetdiver/netdiver.war"
     unpackWAR="false" sessionCookiePathUsesTrailingSlash="false">
        <Parameter
    name="netdiver.dataroot" value="/di/platform/webdata/mynetdiver" />
        <Parameter name="approot" value="/di/platform/webapps/mynetdiver" />
        <Parameter name="diveline.server" value="ubuntu:2131" />
        <Parameter name="diveline.allow-server-change" value="true" />
        <!-- (Optional) If you need to permit HTTP connections -->
        <Parameter name="require-confidentiality" value="false" />
    </Context>
    ```

    NOTE: If you do not require HTTP connections, comment out the **require-confidentiality** parameter. If you permit HTTP connections, you are allowing unsecured communications with DiveLine.

14. Save and close the file.

15. Navigate to the `/di/platform/netdiver` directory.

    ```
    cd /di/platform/netdiver
    ```

16. Copy the *<NetDiver name>.xml* file to the Tomcat directory.

```
sudo cp mynetdiver.xml /etc/tomcat<version-
number>/Catalina/localhost
```

17. Start Tomcat.

Verifying the NetDiver Installation

Verify that your NetDiver installation is working by entering the NetDiver URL in a web browser.

Prerequisite: Download, install, and configure NetDiver.

1. Enter your NetDiver URL with the following syntax:

```
https://<servername or IP address>:8443/<NetDiver name>
```

For example:

```
https://ubuntu:8443/mynetdiver
```

NOTE: If the server name does not work, use the IP address of the DiveLine server.

NOTE: If you have problems connecting to NetDiver, check your logs and the configuration changes made to the *mynetdiver.xml*. The example URL reflects changes made in the **Installing NetDiver** topic. Additionally, if the Linux server is running in a VM, you need to verify that you have configured the network connection options correctly. Refer to **Verifying the DivePort Installation** for additional information.

2. If you have successfully installed NetDiver, the NetDiver start page with a log in dialog box opens.
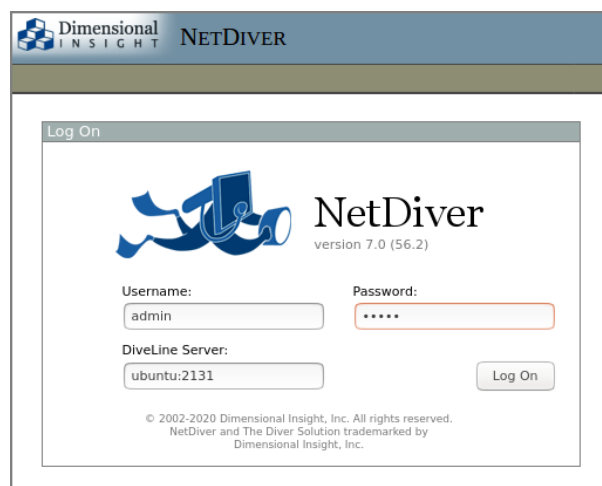
3. If you installed a self-signed certificate and you have not previously logged in to the Linux server with a DI client, the client might ask you to verify the self-signed certificate. Refer to **Verifying the DivePort Installation** for additional information.

4. Once connected and logged in to NetDiver, click **About** to open the **About NetDiver** dialog box that lists the current version numbers of DiveLine and NetDiver.
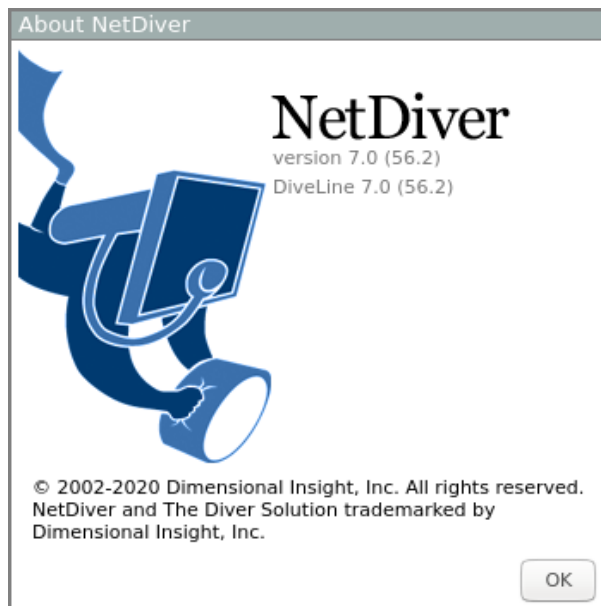
5. Click **OK** to close the dialog box.

6. Click **HELP** to open the *NetDiver Help* system in a new tab in your browser.

Installing Diver Platform Developer

The following installation process requires a computer with Windows installed. This installation cannot be done on a Linux operating system.

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 18 for information on how to locate DI installation files.

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

See About the DI Directory Structure on page 11 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)	Previous Point Releases	Not Available	Not Available
Diver Platform Asian Language Pack 7.0 Windows Unicode	7.0.56 (132524KB)	Previous Point Releases	Not Available	Not Available
Diver Platform Developer Pack 7.2 Windows Unicode limited	7.2.10 (432203KB)	Previous Point Releases	Not Available	Not Available
Diver Platform Developer Pack 7.2 Windows	7.2.10 (432198KB)	Previous Point Releases	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)	Previous Point Releases	Release Notes (1586KB)	Not Available
Diver Platform Developer Pack 7.1 Windows	7.1.33 (417990KB)	Previous Point Releases	Release Notes (1586KB)	Not Available

The **Opening** download verification dialog box opens.
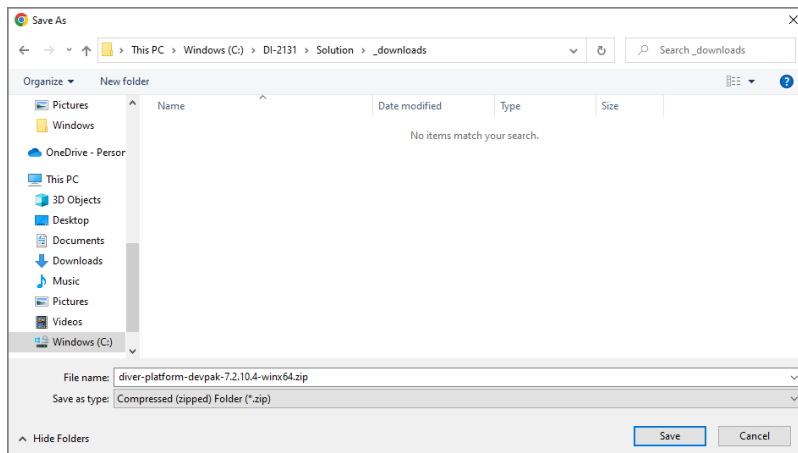
The **Downloading** page opens in the browser. If the **Opening** dialog does not open automatically, follow the instructions on the page.
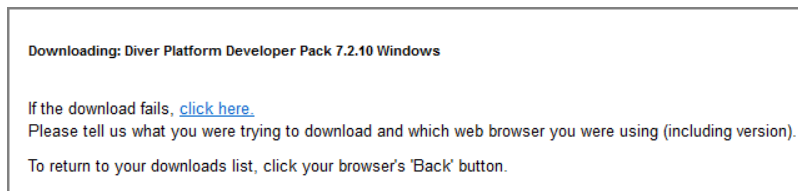
2.   Enter a file name and then click **Save**.
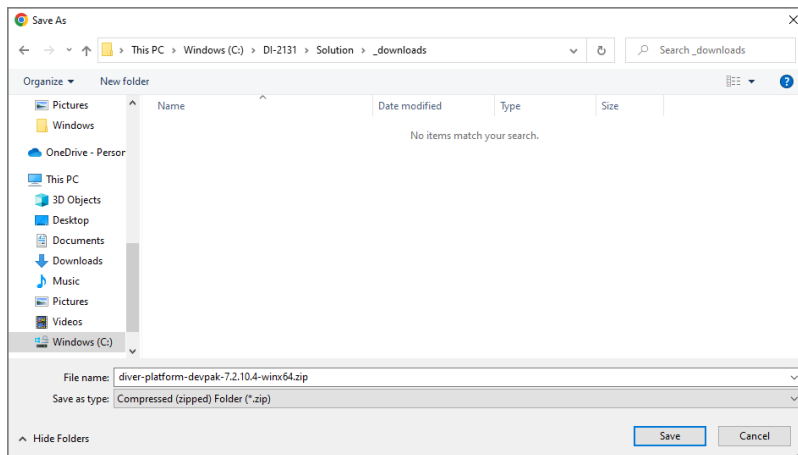
The Diver Platform Developer 7.2 software package is saved to the **Downloads** directory on your local computer.

3.   Move the developer package to the `DI\Solution\downloads` directory.

Downloading and Extracting the Developer Installation Package

84

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:
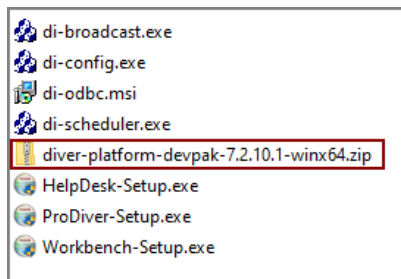
Installing ProDiver

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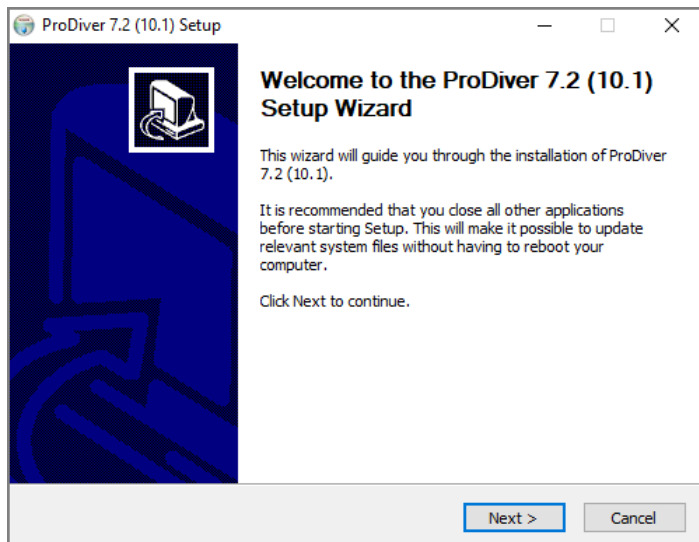
4. Review the setup instructions, and click **Next**.

   The **Installed ProDivers** page displays.
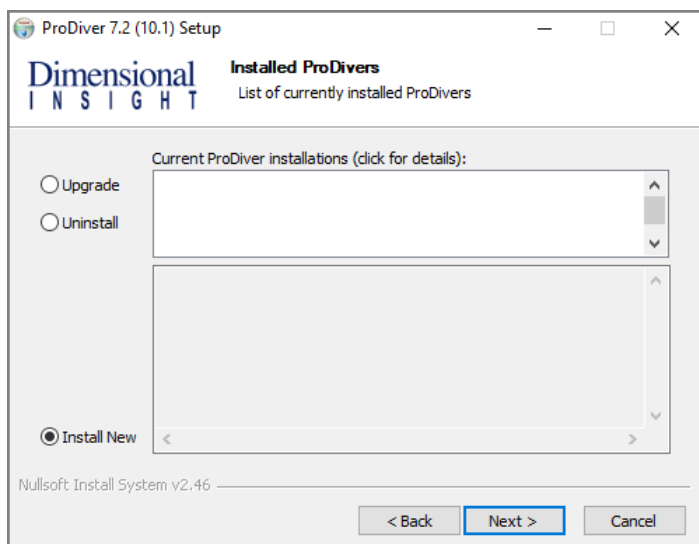
5. Select the **Install New** option.
   This page lists any existing ProDiver installations, which you can choose to
   Upgrade or **Uninstall**. If this is the first installation, **Install New** is selected
   by default.

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.
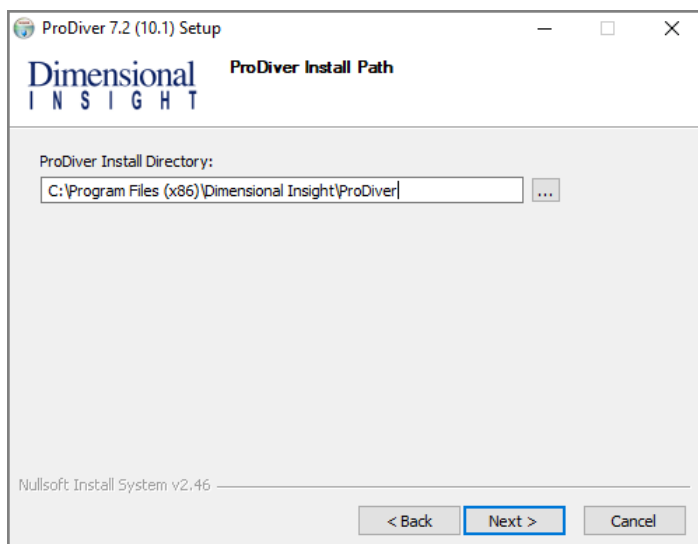
7. Click **Next**.

The **Ready to Install** page displays a summary of the pending installation.
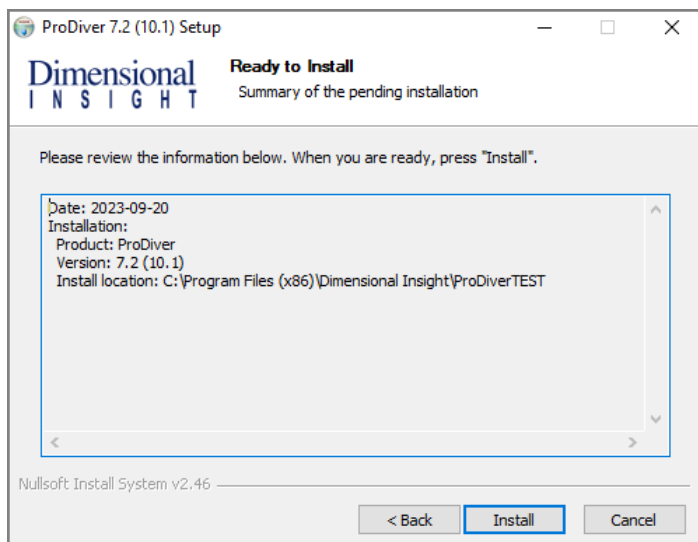
8. Click **Install** to install the ProDiver software.
   When complete, the wizard displays the **Installation Complete** dialog box.
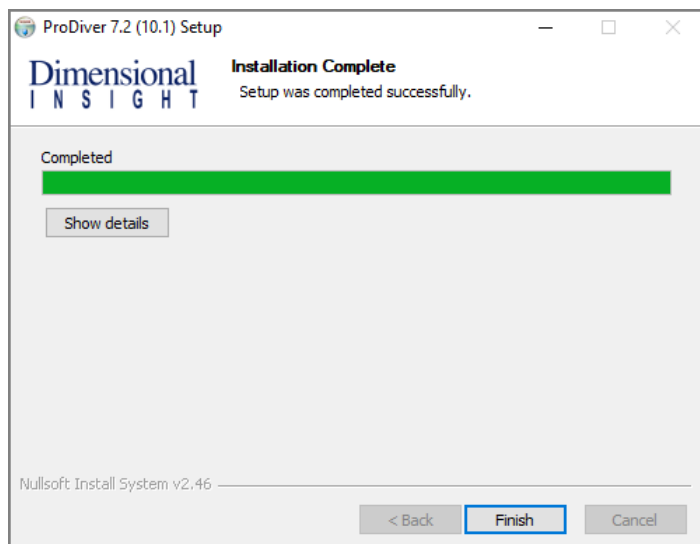
NOTE: To view a running summary of the installation process, click the **Show details** button.

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
/mode=	Indicates the action for the installer. Values are: • `install` • `upgrade` • `uninstall` • `list` 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 list option to see existing installations.
/path=	Indicates the target location. The default value for the path is: `"C:\DI\Solution\executables\prodiver"` The installer writes a log file called *installation.log* to the user-specified or default path with information about the installation.
/installation=	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").

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**.

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**.

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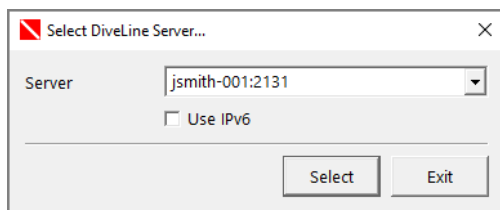
NOTE: The default port number is 2130. If you are using another port, specify it in the **Server** box by using the format **<server name>:<port number>**.

The **Verify Certificate** window opens.
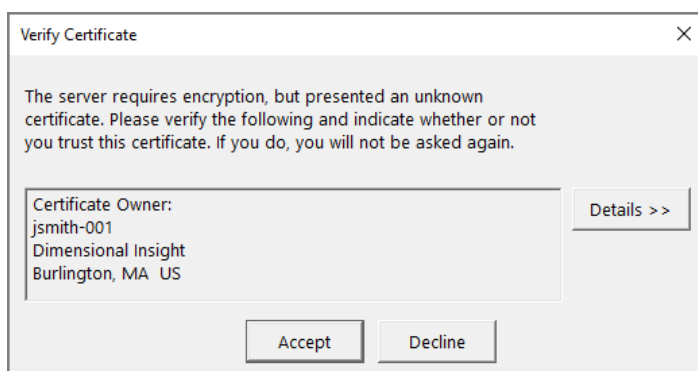
5. Review the certificate, and click **Accept**.

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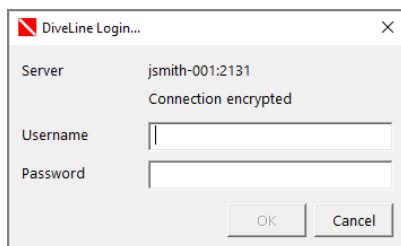
6. On the **DiveLine Login** dialog box, enter the **Username** and **Password** and click **OK**.

Verifying the ProDiver Installation

91
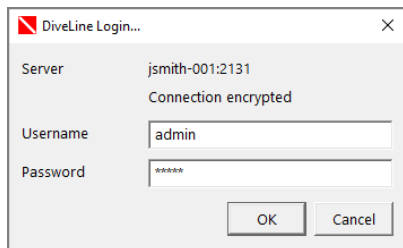
TIP: If you want to use a different server, click **Cancel**, and return to **Step 4**.

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.
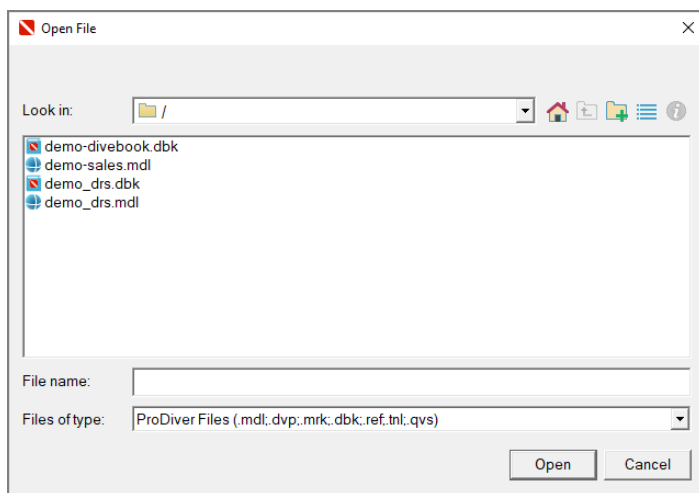
8. Select a *dbk* file, and click **Open**. For example, *demo-divebook.dbk*.
9. Select an Area and a Topic, for example **Tabulars** and **Sales Region**, and click **OK**.
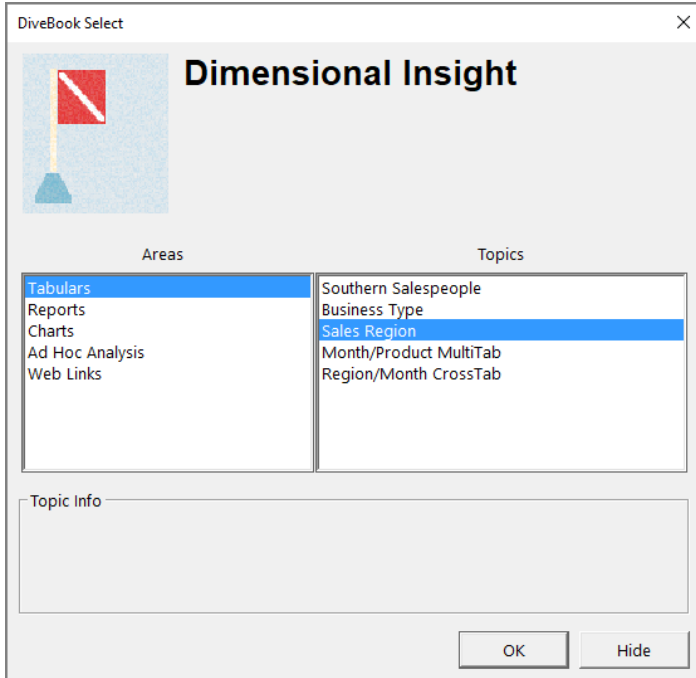
If you see a tabular display similar to the following, ProDiver is functioning correctly.

10. To view the installed version of ProDiver and the DiveLine server name and version, select **Help** > **About ProDiver**.
Confirm the versions and click **OK**.
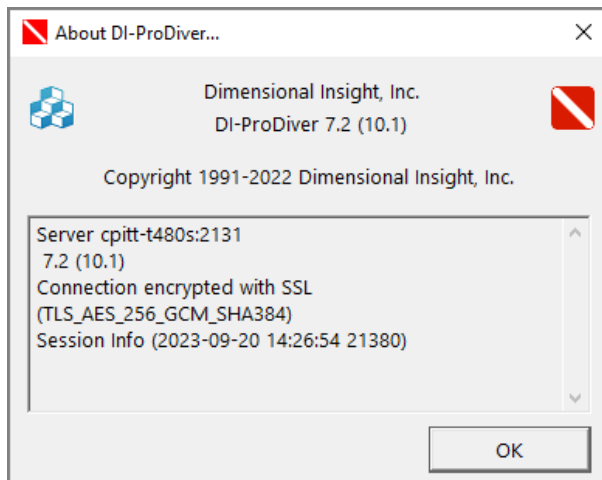
11. To open *ProDiver Help* select **Help** > **View Help**.
    ProDiver Help opens in your default browser.
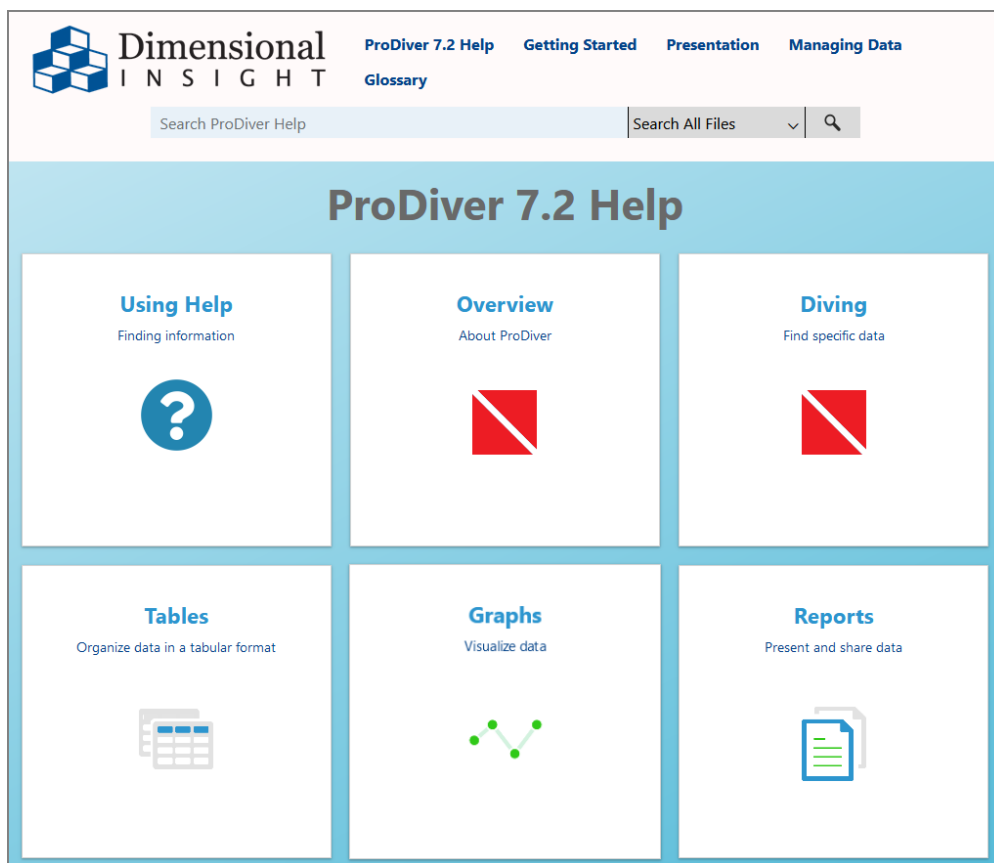
Installing Workbench

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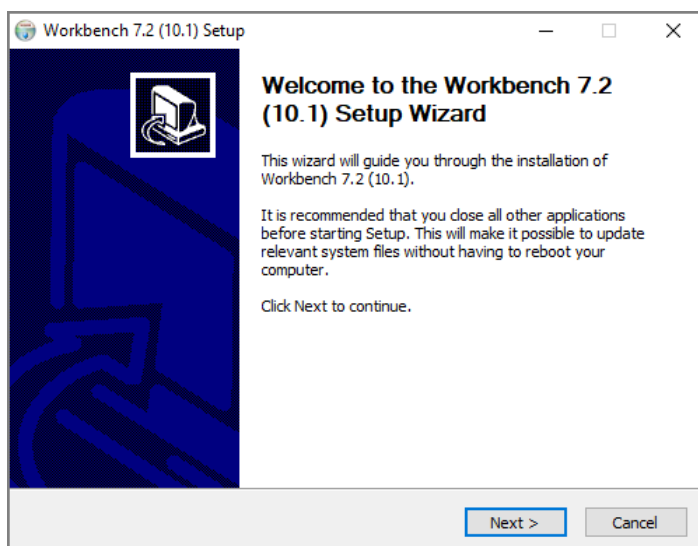
4. Review the setup instructions and click **Next**.

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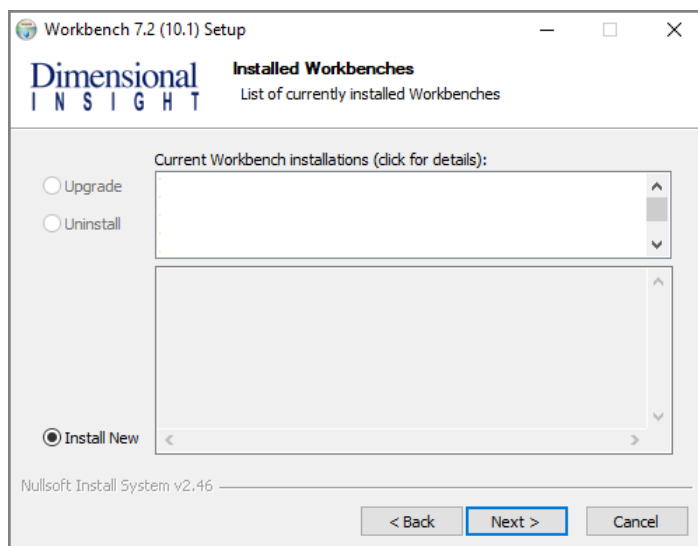
5. Select the **Install New** option. This page lists any existing Workbench installations, which you can choose to **Upgrade** or **Uninstall**. If this is the first installation, **Install New** is selected by default.

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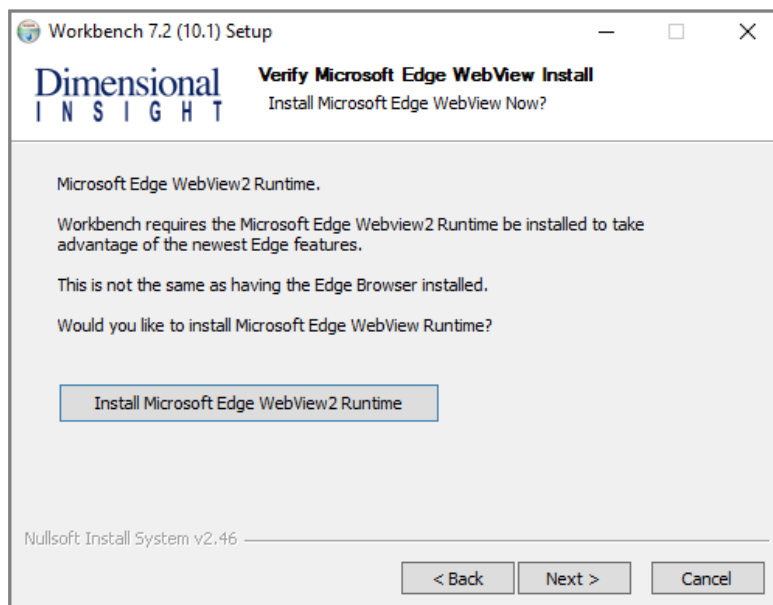
b. Click **Next** when the installation process finishes.

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.
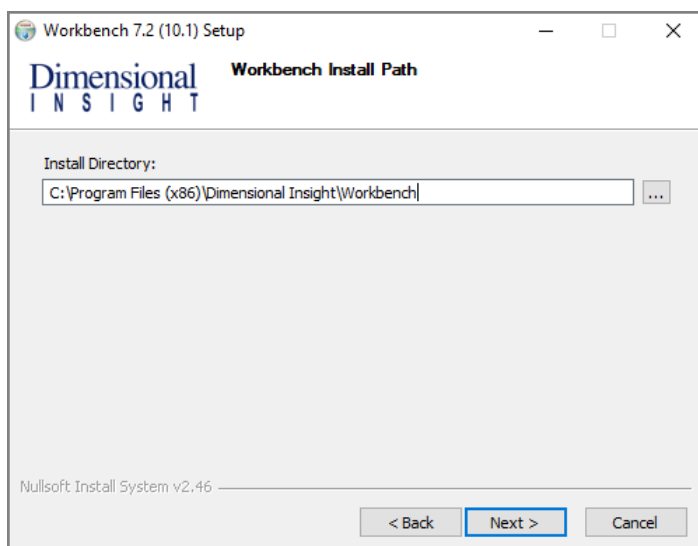
7. Click **Next**.

The **Ready to Install** page opens and displays a summary of the pending installation.
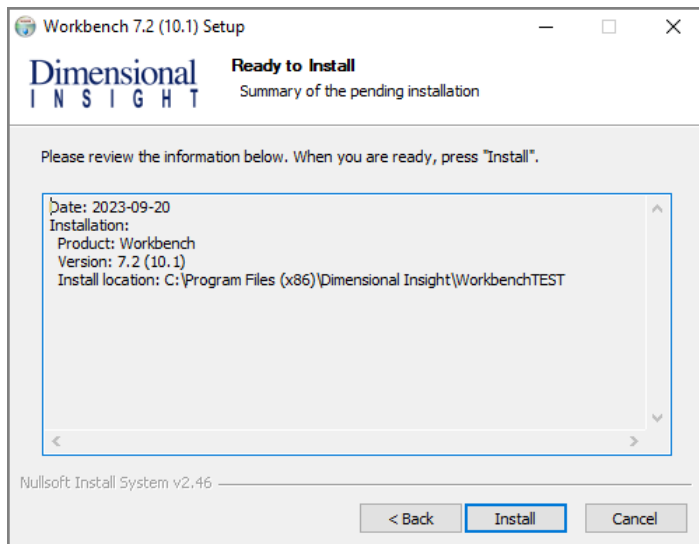
8. Click **Install** to install the Workbench software. When complete, the wizard displays the **Installation Complete** page.
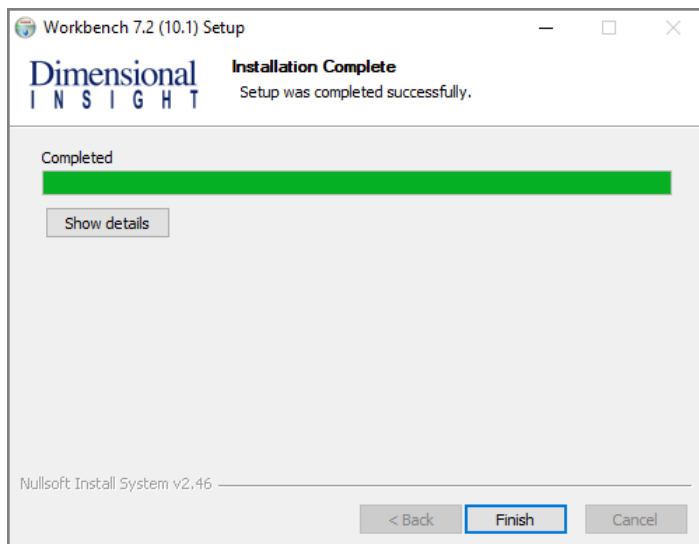
NOTE: To view a running summary of the installation process, click the **Show details** button.

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**.
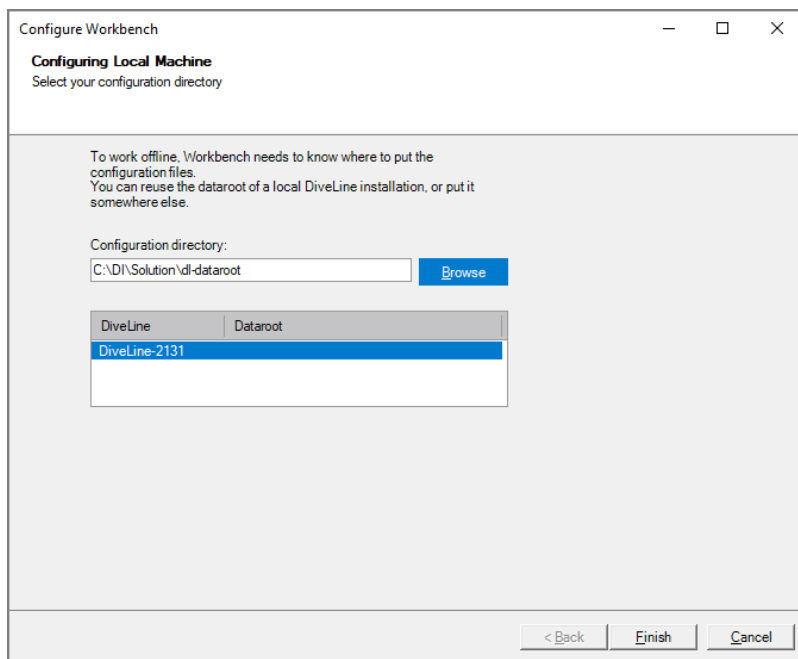
3. If successfully installed, the **Workbench** Start page opens.
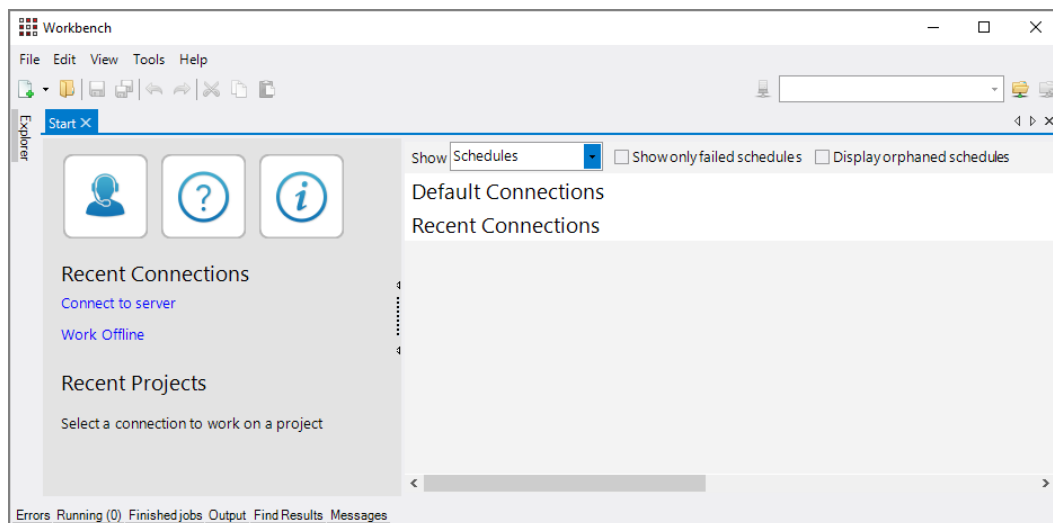
4. To view the Workbench version number, click **Help** > **About Workbench**. Confirm the version, and click **OK**.

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

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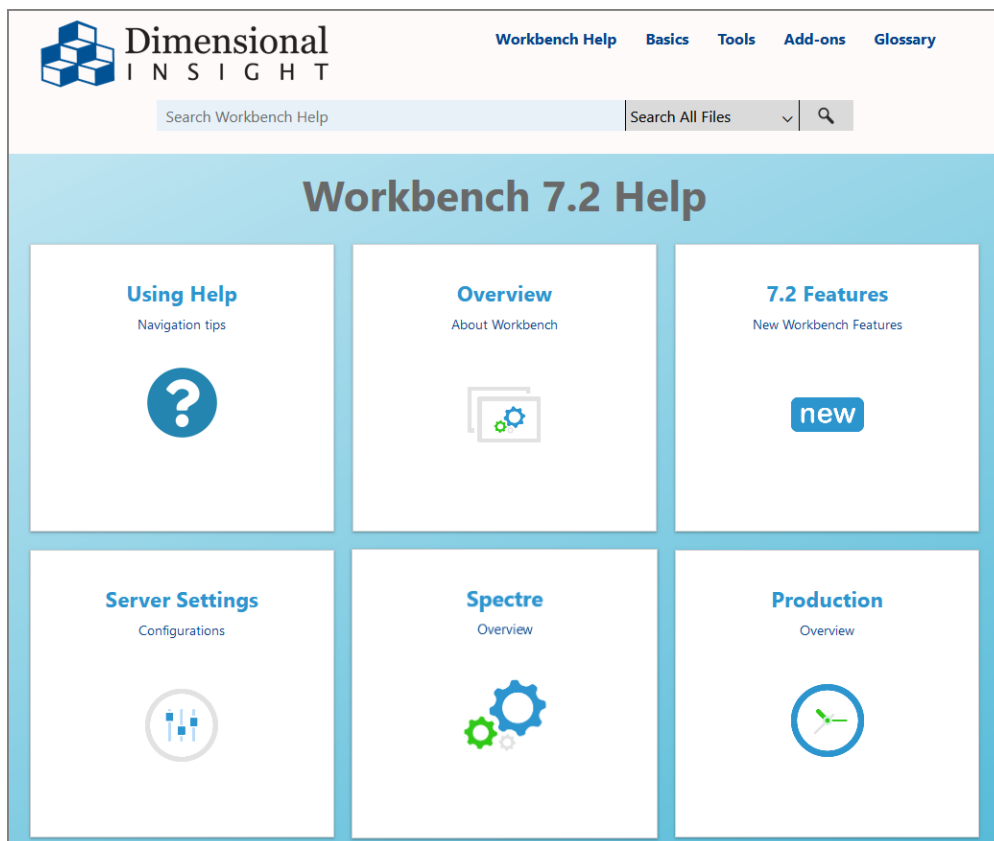
The *Workbench Help* opens in your default browser. Here you can find topics that explain how to connect to a server.

Glossary

6

6.4 DiveLine namespace

A virtual project that allows 7.x Diver clients to access the data area that was created by DiveLine 6.4.

6.4 Production sandbox

A virtual project that allows Workbench to access scripts created in Diver Solution 6.4. It is created when a 6.4 installation is upgraded to 7.x. The sandbox uses the rules applied by DI-Production 6.4 and Visual Integrator 5.1 to create aliases and paths to data.

A

access control

The collection of rules that restricts or allows user access to data in a directory or project. Rules fall into the following categories: file, cBase, model, audit, and DiveTab.

access control file

The mechanism Workbench uses to control user and group access to the contents of the server. Access control files grant or restrict access within project files, cBases, models, and DiveTab areas.

ACL

access control list. The security tool that DiveLine 6.x uses to control user and group access to the server. DiveLine 7.x applies access control rules to projects and can apply ACLs to non-project resources that use the 6.4 DiveLine namespace.

ad hoc page

A tabular DiveTab page type that serves as a starting point for analysis. Ad hoc pages allow switching dimensions, and diving on dimensions and DimCounts.

advanced user

A tiered license type for Diver Solution customers. Advanced users have access to ProDiver, DivePort, NetDiver, DI-Config, Broadcast, Scheduler, and DIAL.

analysis portlet

The DivePort portlet type used to display information about the Measure Factory source data. There are two types: default and custom.

anchor date

A reference point for a Spectre date range. A Workbench developer can set the expression dynamically with a parameter, import a calculation from a text file, or use the last date in the cPlan.

Apache Tomcat

An open source web application server developed by the Apache Software Foundation. DivePort and NetDiver are designed to run on an Apache Tomcat WAS.

application template

A file containing a set of properties that defines the look-and-feel of a specific Diver Platform component.

area

The DiveBook component that groups topics, similar to how a folder groups files.

assisted analytics

A DivePort analysis portlet feature that performs automatic dives and summarizes the results to provide information that you can use for further data analysis. Assisted analytics requires a separate license.

authentication

The process of identifying and approving access to the server for valid users. Diver offers four possible authentication methods: Own, System, Web Server (CGI), and LDAP. Two-factor

authentication is available using DI Cloud.

aux measure

A value typically derived from applying a calculation to a measure, and used as a threshold that is compared to the measure value.

auxiliary measure

A value typically derived from applying a calculation to a measure, and used as a threshold that is compared to the measure value.

B

background portlet

A DivePort portlet type that is used to draw simple images or add text to a portal page.

breaklevel

Points in a ProDiver report where the flow of data breaks to create a subtotal.

build description file

The configuration file types (.dsc or .desc) that control the process of building a DI model using the classic Builder engine.

build file

The configuration file type (.build) that controls the process of building a cBase using the Spectre engine.

Builder

The Diver Platform component that summarizes and preprocesses data to create classic DI models.

C

calc rule

A Measure Factory rule type that processes an expression and returns a value of any Spectre data type.

calculated column

A column that is defined within a dive window using the set of calculations built into ProDiver. Calculated columns modify model, cBase, or cPlan data using a combination of operators, functions, counts, DimCounts, and Named Groups.

calculation reference string

A means for identifying information in a ProDiver report palette cell definition.

calculation rule

A Measure Factory rule type that processes an expression and returns a value of any Spectre data type.

calendar QuickView

A QuickView type in DivePort whose selections are in the form of a calendar. Selecting an available date on the calendar displays the data associated with that date.

cascade dive

A method of changing the results of a multilevel dive by changing the dimension value in an earlier step in the dive path. The resulting changes cascade through the following steps until the new data is updated in the dive window.

casual user

A tiered license type for Diver Solution customers. Casual users have access to DivePort only.

categories

Optional folders in a ProDiver console used to organize model or cBase data. Categories are defined in Workbench using DiveMaster and stored in a DivePlan.

cBase

The file type (.cbase) that stores Diver Platform data generated by the Spectre engine. A cBase is a columnar data structure optimized to aggregate (summarize) large volumes of data.

cell reference

A means to refer to individual cells in a ProDiver report palette. The reference can be absolute: $(a1), relative: $(a#), $(#1), or relative with an offset: $(a#[-1]), $(#[-1]1), $(#[1]#[-1]).

CellDiver

An add-in for Microsoft Excel that allows a DiveLine user to dive from an Excel-based console in order to pull data directly from a classic model into an Excel spreadsheet.

central page

In DivePort or DiveTab, a page type that focuses on a single dimension value. Central pages can link to the dimension value on other pages.

chart portlet

The DivePort portlet type used to create and format Spectre-based graphs and charts. Chart portlets provide formatting options for cBases and cPlans in the same way that measures portlets provide formatting options for tabular markers, cBases, or cPlans.

child page

A DivePort page that inherits its settings from an existing page. A page can be a child of one page and the parent of others.

child window

The window in ProDiver that displays the results of the last step of a dive. The windows displaying the results of the previous steps are all parents to the child window.

click action

DivePort developer-defined action that occurs when a user clicks specified points on a page. Click actions are defined within portlet instances.

click action menu

A DivePort pop-up menu that lists possible click actions on a portlet instance.

client

An application running on a workstation (desktop computer, laptop, or mobile device) that must connect to a server to obtain some functionality. Diver clients include Workbench, ProDiver, DivePort, and DiveTab.

combobox

A text box that provides a pull-down menu for selections and also accepts user-entered selections. Comboboxes are commonly used within QuickViews that have hundreds of options.

conditional click action

A click action whose availability is determined by the value of a given row. Only row-scoped click actions can be defined as conditional.

connection

A communication channel between a client and its server. Diver Platform connections are between the various components and DiveLine. Each connection has its own process ID.

console

The window in a Diver Platform client in which the diving process is managed. The console displays the dive path and the dimensions available for diving.

consolidated DivePlan

A DivePlan that merges multiple models with similar structures and transaction levels. Consolidated DivePlans generally combine models that span different periods of time, and minimize build times by reducing the data contained in any individual model.

context menu

> A menu that is accessed from within the body of a Diver Platform client whose options vary based on which part of the client a user is interacting with.

Controller

> In Diver, the server settings component that provides administrators with access to DiveLine tracking data (connected users, open models, memory usage), and with the ability to message or disconnect users.

core dimension

> Any dimension defined in a classic model at build time. Core dimensions are indexed during the build for rapid retrieval.

core model

> One of the components of a detail model. The core model contains the dimensions that are presummarized and indexed within the detail model.

count

> The field containing the total number of rows in the current view of a cBase or model.

cPlan

> The Spectre file type (.cplan) for defining input sources and data calculations for cBase data. cPlans specify which columns and calculations are available for a dive into a cBase.

cross page

> A tabular DiveTab page type that presents data from two dimensions. The primary dimension displays vertically with its values as rows, and the cross dimension displays horizontally with its values as columns.

CrossLink click action

> A DivePort click action type that links two or more portlets by a common dimension. Selecting a row in the common dimension in one portlet updates the data displayed in all other portlets on the

page that contain the common dimension.

CrossPlot

A ProDiver graph type that contains summary data relating to two different dimensions.

CrossTab

A tabular display that contains summary data relating to two different dimensions.

D

dashboard

An integrated display of high-level data points from multiple sources. A dashboard provides an at-a-glance view of KPIs relevant to a specific goal.

data governance

The process of managing the authority, control, and collaboration of data assets to ensure data usability, integrity, and security.

Data Integrator

The Diver Solution extract, transform, and load scripting tool. In version 7.x, Visual Integrator/Integrator is an integral part of Workbench.

data page

A DiveTab page type that contains the business data that users work with. DiveTab has six types of data pages: the free form overview and central pages, plus the tabular report, ad hoc, cross, and dive pages.

data set

A collection of related data elements that is composed of separate elements but can be manipulated as a unit.

dataroot

The directory specified as the top level directory of the DiveLine file system. The dataroot is usually named dl-dataroot.

date data

The value of a date in integer form. The date data value is the number of days since December 31, 1899.

date rollup

A method for creating and adding time-base dynamic dimensions to DivePlans and cPlans. Date roll-ups generally create longer time periods from existing time-based dimensions, such as quarterly data rolled up from monthly data.

default port

The server port where a component is expected to connect. The DiveLine default port is 2130; SSL (for DivePort) is 8443.

delete

An ACL setting within DiveLine 6.x. Delete hides selected dimensions, summaries, or info fields from the specified user or group.

detail dimension

A model dimension containing focused data that is accessible for diving only after dives on core dimensions have narrowed the data to 256,000 records or fewer. Detail dimensions are created using the Detail option in Builder.

detail info field

An info field defined as part of a detail model.

detail model

A classic model in which only a subset of dimensions, info fields, and summaries are presummarized. Detail models contain presummarized core dimensions and un-summarized

detail dimensions, which can only be accessed when core dives have narrowed the data to 256,000 records or fewer.

detail summary

A summary field defined as part of a detail model.

developer user

A tiered license type for Diver Platform customers, and a user category for Diver Solution customers. Developer users have access to Workbench and all DiveLine clients.

DI-Broadcast

The Diver component used to deliver data to selected users via email. Deliveries can be scheduled on an episodic or periodic basis, or triggered by a specific event.

DI-Config

The DiveLine subcomponent that allows an administrator to configure DiveLine options using a Windows user interface. In 7.x, DI-Config functionality is part of Workbench server settings.

DI-Controller

In Diver Solution, the subcomponent that provides administrators with access to DiveLine tracking data (connected users, open cBases and models, memory usage), and with the ability to message and disconnect users. In version 7.x, Controller functionality is part of Workbench server settings.

DI-Launcher

An application that manages computers with multiple configurations of Diver client programs or multiple versions that connect to different DiveLine servers. DI-Launcher ensures that the correct instance of the client is started.

DI-License-Admin

A Windows application used to request and manage DI product registration and user licenses.

DI-ODBC

Dimensional Insight open database connectivity. A module of the Diver Platform, an ODBC driver that can retrieve Spectre data from a DiveLine server via ODBC-capable applications.

DI-Production

The Diver Solution graphical component used by back-end developers to design workflows and schedule and monitor ongoing processes. In version 7.x, DI-Production functionality is integrated as the Production component of Workbench.

DI-Scheduler

In 6.x, the DiveLine subcomponent that is used to automate tasks within the Diver Solution, including building models and running Integrator scripts. DI-Scheduler is used to manage jobs, events, and tasks. DI-Scheduler functionality has been replaced with Production Job Schedules in Workbench.

DI-Updater

The Diver Platform component that creates a package for managing downloads from the DiveLine server.

DI Bridge

A web application that is used to navigate to multiple DI applications from one central place.

DI Cloud

Dimension Insight platform as a service (PaaS) cloud hosting option. With DI Cloud, customers manage applications and data; and DI supports the network, servers, and server software.

DI Download

The website used to distribute Dimensional Insight software. DI Download is accessed by licensed users via the Dimension Insight website, https://dimins.com.

DI SDL

Dimension Insight Simplified Declarative Language. DI SDL is used for Spectre, DiveTab, and access control scripts. Its syntax is made up of tags, attributes, and variables.

DIAL

Dimensional Insight Access Language. DIAL is a high-level Java programming language for processing, analyzing, and distributing information contained in cBases and models.

dictionary file

A Diver file (.dic or .dict) that defines the format of an input or output file for Integrator or the classic Builder.

DIDP

Dimensional Insight DiveLine Protocol. DIDP is a proprietary protocol for communication between the DiveLine server and its clients (such as ProDiver and DivePort). Networks must be configured to allow DIDP communication to occur.

DimCount

The number of unique values in a dimension, a shortened form of dimension count.

dimcount dimension

A dive dimension that displays dimcount values by default.

dimension

A collection of related data within a model or cBase used for sorting and filtering data (diving).

Dimensional Insight Object Language

The scripting language used by Diver to represent complex objects to its ETL components (Integrator and Builder), configuration settings for the server, and data access directions for its clients.

DIUX

Dimensional Insight user experience. A DI dashboard design toolkit.

dive arrows

Arrows appearing in the ProDiver console that indicate diveable dimensions.

dive dimension

A DiveTab dimension that is diveable.

dive page

A tabular DiveTab page type that serves as a starting point for analysis. Dive pages allow diving on dimensions.

dive path

The sequence of steps taken to access the data displayed in the dive window. In ProDiver, the dive path is displayed in the console history.

dive selectors

The tabs on the ProDiver console that allow you to retain up to four active dives.

dive window

The window in ProDiver that displays data retrieved in a dive.

DiveBook

Diver files (.dbk) that are used for organizing DivePlans, cPlans, markers, and dive files for easy access. DiveBooks are organized by area (similar to a file folder) and topic (the files in the folder).

DiveBook portlet

The DivePort portlet type that presents the contents of a DiveBook within a portal page.

DiveLine

The server component for Diver software. DiveLine authenticates users and controls access to data through Diver clients such as Workbench, ProDiver, DivePort, and DiveTab.

DiveLine administrator

A DiveLine user that has full access to server configuration tools and all data managed by that DiveLine.

DiveMaster

The Workbench component used to create DivePlans, which specify how model or cBase data is presented in client applications.

DivePlan

A Diver configuration file type (.dvp) that determines the organization and presentation of DI model and cBase data to Diver clients. DivePlans are used to categorize data into folders.

DivePort

The web portal environment of Diver Solution and Diver Platform.

DivePort | IN

An alternate name for the DivePort Input-all license.

DivePort administrator

The DivePort user type with permission within a portal to add, edit, or delete content, set access rights for pages, and set user types. A DiveLine administrator is a DivePort administrator by default.

DivePort classic interface

The tab-based interface used in DivePort 6.x. The classic interface is available as an option in DivePort 7.x.

DivePort simplified interface

The button-based interface that is the default for DivePort 7.x. The simplified interface mimics a mobile environment.

DivePort user

The Diver Platform user category that gives named users access to DivePort and NetDiver.

DivePort user type

A DivePort-specific user type that controls user access to a portal. The user types are Disabled, which hides the portal from the user; User, which allows the user to view the portal; and Administrator, which allows the user to edit the portal.

Diver Gateway

An application that links DI applications together to allow one entry point to customer data. You can access Diver Gateway from your desktop, laptop, tablet, or mobile phone.

Diver Platform

The Dimensional Insight software suite that contains all Diver 7.x software, including Workbench and Spectre. DiveTab is optional. User categories are: Developer, ProDiver, DivePort, DiveTab, and HelpDesk.

Diver Solution

The Dimensional Insight software suite that contains all Diver 7.x software, including Workbench. Spectre is not included. User types are tiered: Developer, Advanced, General, and Casual.

DiveTab

An information delivery platform designed to provide mobile users access to unstructured data, such as presentations and documents, and structured data, such as reports and dashboards. DiveTab runs on an iPad, iPhone, Android, or PC.

DiveTab bookmark

A DiveTab feature that saves the path to a specific page, providing direct access to that page. Bookmarks are available for all DiveTab pages except the menu.

DiveTab module

A Diver Platform file type (.divetab) that defines a portion of a DiveTab instance. Menu, data, document, repository, and web page areas are all defined using DiveTab modules.

DiveTab user

The Diver Platform user category that gives named users access to a DiveTab project.

diving

The process of accessing smaller segments of data in greater detail using a DiveLine client.

document library

In DivePort and DiveTab, a specific directory used to collect and organize files on the server for delivery to end users. DivePort document libraries require an additional license to use.

document manager portlet

The DivePort portlet type that provides access to a document repository via the portal. Document manager portlets can contain documents of any type recognized by DivePort, the web server, and the browser.

document viewer portlet

A DivePort portlet type used to embed a specific document from a document library onto a portal page. Document viewer portlets require an additional license to use.

downlink and maximize click action

A DivePort click action that causes a new marker portlet to fill the portal page.

downlink click action

A click action that causes a new marker to display in place of the current marker on a DivePort page.

DTAP

development, testing, acceptance, and production. A phased approach for software development and testing.

dual-factor authentication

An alternate term for two-factor authentication.

dynamic dimension

An info field that has been promoted to a diveable dimension.

E

encryption

A method of securing data by adding code that makes the data unreadable to unauthorized users. The Diver Platform employs the industry-standard Transport Layer Security (TLS) encryption protocol which uses the AES-256 cipher. This applies to communication between DiveLine and its clients, and between DI clients and third-party software such as web browsers.

environment

A collection of DivePort pages that share a hierarchy and portal settings. Multiple environments can exist in a single portal.

ETL

extract, transform, load. A process in which data is extracted from one or more sources, transformed into a format suitable for analysis, and loaded to a cBase or model.

Excel click action

A click action that exports data from a DivePort portlet into a Microsoft Excel spreadsheet.

external DivePlan

A DivePlan that is not saved within a single marker, but to an external file. External DivePlans are useful when multiple markers reference them, because editing the DivePlan updates all of the markers.

F

factory explore portlet

The DivePort portlet type used to display a diagram that shows the definition or composition of a Measure Factory measure or rule.

factory file

The configuration file type (.factory) that controls the Measure Factory build process.

filtered calc

A ProDiver calculation in which a dimension value is specified as part of the column definition. You can specify values for more than one dimensions.

flag rule

For Measure Factory data sets, a flag rule brings in a Boolean value using a single lookup key.

flex QuickView

A QuickView type that provides flexibility when designing QuickViews. Flex QuickView lists can be collapsible like a pull-down, searchable like a combobox, multi-select like a picklist, or a combination of list styles.

form portlet

A DivePort portlet type that allows you to create custom data entry forms for adding and validating rows in DivePort tables. Form portlets require an additional license to use.

free entry QuickView

A QuickView type that allows a user to supply custom options as values in a text box, rather than select from a predetermined set of options.

G

Gateway

An information delivery platform designed to provide desktop and mobile users access to unstructured data, such as presentations and documents, and structured data, such as reports and dashboards using MyLibrary. Gateway runs on an iPad, iPhone, Android, or PC.

general user

A tiered license type for Diver Solution customers. General users have access to web-based DiveLine clients (NetDiver and DivePort), plus DI-Config.

geocoded layer

A dimension containing geographic data that is used to find latitude, longitude, and center points in a map layer file.

geocoding

The process of identifying geographic coordinates (usually expressed as latitude and longitude) based on other information such as street address or postal code.

geographic key

A field contained in a classic model that enables the creation of maps. If a geographic key is present, ProDiver creates an info field for each map layer and promotes them to dynamic dimensions to create diveable maps.

graph

A diagram that represents data. Diver supports more than four dozen graph types.

graph templates

A Diver file type (.gtpl) that applies uniform appearance settings to graphs.

graph toolbar

A toolbar available on a ProDiver graph dive window that you can use to edit the graph.

group

A ProDiver option that combines multiple diveable values into a single unit for diving.

group with others

A ProDiver option that aggregates selected rows in a tabular into a group and puts the unselected rows into another diveable value called Others. Grouped rows are displayed individually, while the others row is summarized.

guest page

The home or welcome page for a DivePort portal, seen before the user is authenticated.

guest user

A type of DivePort user who can view portal pages that do not contain DiveLine data. An additional license is required to create guest users.

GUID

globally unique identifier. A 128-bit hexadecimal number used to identify information in computer systems.

H

help click action

A click action that displays a pop-up window containing help text. Help click actions accept DivePort variables and HTML formatting.

Help Desk

A Diver application that provides a subset of Workbench server settings for user and group maintenance. Help Desk users do not have access to data.

HelpDesk user

The Diver Platform user category that gives named users access to Help Desk and DI-Config.

home directory

The directory on a server that contains the files for a specific user. It is the standard starting point when a client is opened as well as the location to store and retrieve DiveLine content.

home project

A special Workbench project on a DiveLine server used to organize user files into individual home directories.

hotspot

A rectangular area within a DivePort Image Portlet designated to display text (a tooltip) when a user places the pointer over it.

HTML portlet

A DivePort portlet type that is used to display HTML-formatted information on a portal page.

I

image portlet

The DivePort portlet type that is used to upload images to the DivePort image library and portal pages. The image portlet hotspot functionality allows you to add tooltips.

indicator

A graphical representation of a single value in DivePort. Along with the value, indicators can show positive or negative relationships to user-defined thresholds.

indicator portlet

The DivePort portlet type that is used to add an indicator (a single-value graph) to a portal page.

indicator template

A group of settings that determines the look and feel of a specific indicator type. Users can create, save, and reuse multiple indicator templates for each indicator type.

info click action

A click action that displays a pop-up window containing information about a portlet. Info click actions accept DivePort variables and HTML formatting.

info field

A model or cBase component that contains data that supplements or supports dimension data. Info fields are not diveable, but they can be promoted to dynamic dimensions, which are diveable.

Input-all license

A DivePort licensing option, sometimes called DivePort | IN, which permits full use of all tables, forms, documents, and document libraries.

input table

An interactive page element that allows users to enter row-based data in DivePort. Input tables require an additional license to use.

instance

An individual portlet that exists on a DivePort page. DivePort pages can contain multiple instances of the same or different portlet types.

Integrator

The Diver Solution extract, transform, and load scripting tool. In version 7.x, Visual Integrator/Integrator is an integral part of Workbench.

Integrator date format

Integrator processes dates in the date format (YYYY/MM/DD) as well as the ISO date format (YYYY-MM-DD).

InterReport

Dimensional Insight software as a service (SaaS) cloud offering, in which DI manages the customer's data and applications as well as the network, servers, and server software.

J

jump

A single cascading dive between multiple models or cBases. Jumps are possible when open models or cBases share a dimension.

K

knowledge base

An integrated collection of datasets, enhanced with business rules and quantitative measures, interactive dashboards, analytical models, and metadata that, when used together, provides analytical insight into a particular problem domain.

KPI

key performance indicator. A measure used by an organization to define and evaluate success.

L

limit

An ACL setting within DiveLine 6.x. Limit restricts which values in a particular dimension or info field can be seen by the specified user or group.

link portlet

A DivePort portlet type that creates hyperlinks between a portal page and other web pages, inside or outside the portal.

link rule

For Measure Factory data sets, a link rule moves data from one data set to another. There must be a key: a rule in one data set that matches a rule in another data set. When records are connected, data is summarized in one set and added to the corresponding records in the other set.

list QuickView

A QuickView type that allows the user to assign values from a text file, rather than relying on model or cBase data.

location bar

In the DivePort classic interface, the area just below the page tabs and toolbar. The location bar contains the navigation breadcrumbs and multiple icons representing key DivePort functions.

logon portlet

A DivePort portlet type that is used to customize a DivePort logon page. The logon portlet contains fields for entering username and password, and can share a page with images, graphics, text, and links.

lookup manager portlet

A DivePort portlet type through which users can access and modify lookup tables contained on the DiveLine server. Lookup manager portlets require an additional license to use.

lookup model

A model format containing one core dimension (key) with related info fields. Lookup models are used to add info fields to a model after the build, and have mostly been replaced by lookup tables.

lookup rule

For Measure Factory data sets, a lookup rule brings in columns from a lookup file by matching certain values from each record with values on a particular row of the lookup file. Common use is to convert codes into text descriptions.

lookup table

An external table that can be linked to a cBase or model after the build. Lookup tables contain a primary value that matches a dimension in the cBase or model and secondary values (info fields).

M

map portlet

A DivePort portlet type that is used to analyze data by location. Map portlets sort data based on latitude–longitude pairs or custom settings for display in boundary maps, point maps, heat maps, and web map service maps.

MapData set

A set of ProDiver files representing layers of information rendered on a ProDiver map. Layers can be areas on a world map (such as countries, cities, or postal codes) or areas of a building (such as rooms and shelves) using a reduced area scale. The set includes .mid/.bmi file pairs and a map_data configuration file.

marker

A Diver file type (.mrk) that stores the actions taken during a dive and the state of the dive window. Reopening a marker displays the most recent build of the model or cBase data in the state the marker was in when it was saved.

marker portlet

A DivePort portlet type that loads a marker from DiveLine and displays the data in a portlet. Markers are defined in ProDiver.

matrix portlet

In a Measure Factory-licensed DivePort, matrix portlets display tabular views of cPlan data.

max clump

A Builder value defined as the most frequently encountered value for a dimension in a classic model dataset.

measure

Numbers computed at a point in time by the application of rules against an enhanced data set often sourced from different systems. For correct interpretation, a measure needs context.

measure dictionary

A DivePort portlet type that provides details about the methods used to apply business rules to data to determine measures.

Measure Factory

An add-on for Diver Platform that automates the process of specifying and producing business rules. Measure Factory includes a business rules engine that transforms data as defined.

Measure Factory editor

The Workbench component that is used to create and edit rules and measures in a Measure Factory script.

measures portlet

The DivePort portlet type used to display and customize marker or Spectre dive file data. Measures portlet data can be customized in DivePort.

menu portlet

A DivePort portlet type that provides links to user-specified pages. The menu portlet displays large button-style links to mimic a mobile environment and is used with the simplified interface only.

mockup portlet

A DivePort portlet type that shows potential elements of a portal page without requiring data. Mockup portlets are used to test page design.

model

The file type (.mdl) that stores data generated by the classic Builder engine. A model is a presummarized, indexed data set designed for multidirectional drill-down without directional limits or predetermined drill paths.

multi-select CrossLink click action

A DivePort click action type that allows users to make multiple selections before refreshing portlet data. DI recommends using multi-select CrossLink click actions with picklists and tunnel scripts.

MultiCrossTab

A tabular display that combines two dimensions, displaying one horizontally and the other vertically, with the values of one or more summaries.

multilevel DivePlan

A DivePlan that merges models with different dimension and summary relationships. Models combined in a multilevel DivePlan must have a common dimension and maintain a 1:1 relationship between info fields and core dimensions.

MultiTab

A tabular display that vertically combines two or more dimensions.

MultiTabMultiCrossTab

A tabular display that presents three or more dimensions and one or more summaries. To create a MultiTabMultiCrossTab, first create a MultiTab, and then apply a MultiCrossTab to it.

My Library

A DivePort user interface that uses expandable menus to navigate portal pages.

N

named group

A collection of dimension values that are grouped under a specified label. Named groups are used in calculated columns to filter cBase or model data based on the values in the named group.

named group lookup

External files that specify named groups for a DivePlan. Named group lookups can be shared across markers that contain the appropriate core dimension.

named user

An individual specified by the customer as the holder of a user license to access Dimensional Insight software.

navigation bar

The bar on a DivePort page that contains the title and navigation buttons for the page, and the controls for locking and unlocking the page. The navigation bar is located directly above the page body.

NetDiver

The zero-footprint web-based analytics client of the Diver Platform. NetDiver provides ad hoc reporting and analytics tools in a web browser.

NetDiver click action

A click action associated with a DivePort portlet that opens the underlying marker in NetDiver.

O

ODBC

open database connectivity. A standard application programming interface used for accessing database management systems.

ODBC user

The Diver Platform user category that gives named users access to the DI-ODBC module.

OIDC

OpenID Connect. An open authentication protocol that works on top of the OAuth 2.0 framework.

OpenID connect

An authentication protocol that provides an identity layer to OAuth 2.0 protocol. DiveLine 7.1(23) and later supports OpenID connect.

other dimensions

A console category used when a developer assigns some, but not all dimensions, to categories in a DivePlan. Dimensions not explicitly assigned to a named category are assigned to the other dimensions category.

overview page

The DiveTab page type used to provide a high-level summation and view of a data set. Overview pages have a free-form layout, enabling graphs, web links, images, or presentation links to appear in addition to tabular dimension summaries.

P

page

A display area within a DivePort environment that can contain one or more portlets which display content. Each page has an ID and a specific URL.

page tab

A link to a top-level page in the DivePort classic interface. Page tabs appear in a row above the page body.

parameterized calculation

A calculated column defined with a variable that references the value of an external QuickView. The column values change when the value of the QuickView changes.

parent dimension

A dimension selected as an intermediate step in a dive. Each dimension selected in a dive is the parent of any subsequent dimension selected in the dive.

parent page

A DivePort page that provides its settings to a child page. A page can be a parent of many pages and the child of a page.

parent window

Any window in ProDiver that displays the results of an intermediate step in a dive. The window displaying the last step is the child of all the previous parent windows.

pdf click action

A click action that exports data from a DivePort portlet into a pdf file.

Period Comparison wizard

A ProDiver tool available from the toolbar and edit menu that creates time period-based summary values and comparisons such as year-to-date and last-year-to-date, or month-to-date and last-month-to-date, and the percent change between the two periods.

picklist

A selectable list with options that are always visible. Picklists can be used in QuickViews as an alternative to pull-down lists.

PID

process identifier. A unique identifier created for a process within a server/client connection. DiveLine processes, such as links to individual portlets on a DivePort page, are assigned PIDs.

plugin rule

For Measure Factory data sets, a plugin rule executes an external process to produce rules that are not included in the standard Measure Factory rule types.

pop-up click action

A click action that reveals a hidden DivePort portlet as a pop-up window. This click action does not pass data to the hidden portlet.

pop-up CrossLink click action

A click action that displays a hidden portlet that is the target of a CrossLink in a pop-up window in the center of the page. This click action passes the selected row to the portlet, which determines the values the portlet displays.

portal

A designated website that provides a single point of access to a set of web pages relating to a topic such as an organization or enterprise. DivePort is the portal environment of the Diver software suite.

portal page click action

A DivePort click action that links a page to another page within the portal. The linked page can open or display in a pop-up window without leaving the original page.

portal variable

A predefined variable available within DivePort. Portal variables are considered global macros and can be used anywhere within DivePort.

portlet

A content area within a DivePort portal page that processes requests and generates dynamic content. DivePort offers a number of different portlet types.

presentation

In DiveTab, a series of grouped slides that can be displayed serially or selected in a random order.

privileged user

A DivePort user who has been granted the ability to add, edit, or delete pages and portlets in a portal. Privileged user status is granted by a DivePort administrator.

ProDiver

The desktop analytics client of the Diver software suite that displays live views of model and cBase data as tabular displays, reports, or graphs.

ProDiver click action

A click action associated with a DivePort portlet that opens the underlying marker in ProDiver.

ProDiver user

The Diver Platform user category that gives named users access to ProDiver, Broadcast, and DIAL.

Production

The Diver graphical component used by back-end developers to design workflows and schedule and monitor ongoing processes. Production is an integral part of Workbench.

project

A set of related files within a single directory tree that are associated with a Diver application or DiveTab instance. Projects are self-contained and portable, and each project can have custom access control settings.

property

A name and value set defined and shared among all DiveLines using a particular dataroot. Properties are used primarily to define access control, and they are shared by Workbench projects on the same server. Properties are assigned to users and groups.

proxy

A user who logs into another user's account to view data from that user's perspective. Proxy logon is available to properly credentialed ProDiver, NetDiver, and DivePort users.

pull-down list

A list box that must be opened before you can view its contents and make a selection.

Q

QuickView

A data filtering feature of Diver clients. QuickViews are used to dynamically update displayed data by applying one or more filters.

QuickView portlet

A DivePort portlet used to consolidate and organize QuickViews on a portal page.

QuickView set

For 7.x, the file type (.qvset) that defines QuickViews for use with cPlans, cBases, and Spectre Dive Files. Workbench is used to create and edit qvset files. In 6.4, the file type (.qvs) that defines QuickViews for use with multiple markers. ProDiver is used to create and edit qvs files. Editing a QuickView set updates the attributes of the QuickView wherever it is used.

R

record

Individual sets of information in a database. Each row of data in a model or cBase is a record.

reference link file

The Diver file type (.ref) that contains window dive reference strings for use in the report palette.

report macro

A variable used to create and reuse complex item definitions in the ProDiver report palette.

report page

A DiveTab page type that displays tabular data. Report pages are usually linked from central or overview pages.

report palette

A report structure in ProDiver that can be used to link multiple data sources to create complex reports.

report reference item

In ProDiver, an item that combines a calculation reference and a dive window reference string. Report reference items are used in the ProDiver report palette.

report template

A set of specifications for standardizing the appearance of reports. ProDiver provides report templates and also allows users to create their own templates.

rollup

A method for creating and adding time-base dynamic dimensions to DivePlans and cPlans. Date roll-ups generally create longer time periods from existing time-based dimensions, such as quarterly data rolled up from monthly data.

rule

Specific manipulations applied to input data sets for Measure Factory projects that are used to create measures. Examples of rule types: source, calc, lookup, flag, link, and plugin.

rules engine

A software system that evaluates a collection of conditions and takes actions based on those conditions. The conditions or rules can be written in any order without affecting how the engine

evaluates them. The Measure Factory rules engine transforms data sets into knowledge bases that support the computation and presentation of measures in context.

S

scope

An abstraction layer on the Measure Factory source data set that limits the measure to a portion of the data.

scorecard

A portal page that uses multiple data visualizations to provide information on individuals or small groups for rating purposes.

script

A collection of DI Object Language commands that execute a process to produce a defined outcome. For example, Integrator executes scripts that yield flat files that can then be built into cBases or models, and DI-Production executes scripts that manage multiple ETL tasks sequentially or in parallel.

sections menu

A set of DiveTab pages linked from the current page, accessible by clicking the sections button in the lower left corner of the client. When the sections menu is used, all filters are ignored.

security certificate

A digital certificate that authenticates the identity of a website and ensures secure transactions between a browser and a server. DivePort and NetDiver use TLS security certificates for authentication and to ensure the security of the data over the internet.

self service

An optional feature in DivePort and DiveTab that non-adminisrtator users can use to access specific pages and create stamp dashboards. Self service requires a Measure Factory license.

server

A computer or other device that manages network resources. DiveLine is the server component for Diver Solution and Diver Platform.

session

The period during which a user is logged onto a Diver Platform client. The session begins when the user logs on and ends when the user logs off.

session ID

A unique identifier assigned to an individual user session. Session IDs are made up of the logon time and the PID of the DiveLine instance handling the connection, in the format YYYY-MM-DD HH:MM:SS ####, where #### is the PID.

setup rule

For Measure Factory data sets, setup rules initialize data from data input or plugin input sources.

sidebar

A navigational element in DivePort that displays the pages of an environment in a tree view.

signed software

Software with a digital signature that indicates ownership and copyright. Diver application files that run on Windows operating systems contain the digital signature of Dimensional Insight, Inc.

single model DivePlan

A DivePlan that contains only one cBase or model. Use single model DivePlans to group dimensions into categories in the console, promote info fields to dynamic dimensions, and define lookup files for adding additional info fields or named groups.

site map portlet

A DivePort portlet that displays a linked map of accessible pages within an environment. The site map portlet can also be configured to list the visible portlets on each page.

skin

A collection of color, font, and size settings that control the overall look and feel of a report, page, or portal in DivePort, NetDiver, or ProDiver.

slide show portlet

A DivePort portlet type that is used to create slide show presentations on a portal page. Slide show portlets require an additional license to use.

source rule

For Measure Factory data sets, the source rule makes all cBase columns automatically available.

Spectre

The data analysis software that is used to build cBases. It powers the DiveLine server software for efficient queries from DI clients against those cBases. Spectre has two parts: the scripting language and the calculation engine.

Spectre Dive file

A Diver Platform file type (.dive) that contains a script which specifies a window into Spectre cBase data by enumerating columns and values that appear in a tabular display. Spectre Dive files are used in DivePort in the same way as markers are.

squash

A process within Data Integrator or Builder that combines records for identical dimension values, summarizing totals and reducing the size of the data set. Spectre also has a squash function.

SSO

single sign-on. An access control property that allows users to gain access to multiple related software systems using a single ID and password.

stamp portlet

The Measure Factory-licensed DivePort portlet type that support easy duplication of a presentation layout for different measures. Stamp portlets enable the self service feature.

stamps

In a Measure Factory-licensed DivePort or DiveTab, a stamp is a template that defines a collection of portlets similar in appearance to a dashboard. Custom stamp template files can be created in Workbench and deployed in DivePort. DiveTab stamps are defined in the script.

structured dive

A form of diving that uses a predefined path. Developers can create structured dives in DivePort using a series of DownLink click actions.

subsets area

DiveTab functionality that allows end-users to save local filters and reapply them whenever the data is updated. Although the subsets area is available to all users, the saved filters are private.

summary

A column in a model or cBase containing numeric data.

T

table editor portlet

A DivePort portlet type that is used to display and edit input tables or document libraries. Table editor portlets require an additional license to use.

table of contents portlet

A DivePort portlet type that is used to create links between a page and its child pages. New child pages are automatically added to an existing table of contents portlet.

tabular

A format for presenting model or cBase data in a Diver client. A tabular display resembles a spreadsheet and is the most commonly used data format in Diver.

text variable

A variable in the report view that contains a string value. Text variables have names in the form $VARIABLE_NAME, such as $BUILD_DATE, $DIMVAL(n), $FIND_COLUMN, and $MAXPAGE.

tiered user licensing

The licensing method for The Diver Solution. The Diver Solution 7.x has four license tiers, which determine user access to Diver Solution components and clients: Developer, Advanced, General, and Casual.

time series

Diver Platform functionality that is used to define and calculate column data which is based on time periods.

time series template

A set of time period comparisons built into the time series functionality in ProDiver.

title bar

The banner at the top of a DivePort page.

TLS

Transport Layer Security. A security protocol for establishing an encrypted link between a server and a client, typically a web server and a browser, or a mail server and a mail client.

toolbar

A horizontal bar containing icons or buttons that are used as shortcuts to functions otherwise accessed from menus.

tooltip

A text box that displays when the pointer is placed over a hotspot for more than one second.

topic

The DiveBook construct that provides access to data. DivePlans, markers, links, Spectre dive files, and cPlans can be saved as topics. Topics are grouped in DiveBook areas, in the same way files are grouped in folders.

tunnel script

A Data Integrator script (.tnl) that connects to a data source to build a model or cBase in real time. Tunnel scripts are executed by a user action (such as selecting a QuickView item) in a DiveLine client (ProDiver, DivePort, NetDiver, or DiveTab).

two-factor authentication

A security process that requires two separate, distinct forms of identification to verify a user. Dive Platform 7.1(13) and later supports two-factor authentication.

two-step verification

An alternate term for two-factor authentication.

U

user category

The licensing method for Diver Platform. Diver Platform offers six categories: Developer, ProDiver, DivePort, DiveTab, HelpDesk, and ODBC; each of which provides access to specific Diver Platform functionality. Users can be assigned to more than one category to give them access to more functionality.

UUID

universally unique identifier. A 128-bit hexadecimal number used to identify information in computer systems.

V

view switcher

Clickable icons that allow users to switch between graphical editor and text editor views for some Workbench file types.

Visual Builder

The Workbench component used to create Builder Description files (.dsc) that describe the transformation of data into a model file (.mdl).

Visual Integrator

The graphical version of Data Integrator for the creation and testing of data manipulation scripts. The end user works with graphical objects, supplying attribute names and values in dialog boxes, while the application supplies the underlying syntax.

W

WAS

web application server. The platform for supporting a web-based client in a client/server architecture. DivePort and NetDiver are both designed to run on an Apache Tomcat WAS.

WCAG

web content accessibility guidelines. An internationally shared set of guidelines for web content accessibility published by the Web Accessibility Initiative of the World Wide Web Consortium (W3C).

web page click action

A DivePort click action that opens the page at the specified URL. Pages outside the portal open in a new browser tab; pages in the portal open in the current tab.

web page portlet

A DivePort portlet type that displays another web page within a frame on the current page. Links on the target page are active. Therefore, forms can be embedded using a web page portlet.

webapps

The Diver directory where web application code is installed. The webapps directory contains DivePort and NetDiver code, as well as fixed resources, such as built-in images and skins.

webdata

The Diver directory where DivePort and NetDiver configuration information is stored. Users can place customizations (user-created skins, icon images) in the webdata directory.

window dive reference string

A ProDiver tool that captures the dive window information for use as a report link in the report palette or report view. The string takes the form: diveref:window_type["model_name".dive_ dimension,(parent_dimension="parent_value"),(_attribute_name="attribute_value")], where the parentheses denote optional repetitive items.

Workbench

An integrated visual development environment to develop, test, and manage projects associated with Diver applications.

Workbench group

A collection of Workbench users (DiveLine accounts) that share similar access requirements. Use groups to simplify user administration.

Workbench users

Individual DiveLine accounts that are managed by Workbench or Help Desk. These accounts specify which Diver applications are available to users.