



Diver Platform 7.0 Installation Guide for Linux

Diver Platform 7.0 Installation Guide for Linux

Revision: Doc-DPIL-70-062521-05

June, 2021

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

60 Burlington Mall Road, Burlington, Massachusetts 01803

www.dimins.com

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

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

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

More Information

More information about trademarks, product warranty, and third-party license notices is available in your DI software Help system. At the bottom of any Help page, click **Product Information**, and then click **Disclaimers, Trademarks, Warranty, and Third-Party Licenses**.

Contents

| | |
|--|-----------|
| Diver Platform 7.0 Overview | 1 |
| About This Installation Guide | 1 |
| About Roles and Environments | 2 |
| About Installing DI Software on a Linux Platform | 4 |
| About Diver Platform Server 7.0 | 5 |
| About Diver Platform Developer 7.0 | 6 |
| Software Requirements | 7 |
| About the DI Directory Structure | 10 |
| Building the DI Directory Structure | 12 |
| About Diver Platform and Solution 7.0 Licenses | 14 |
| Diver Platform Licenses | 14 |
| Diver Solution Licenses | 14 |
| What Is Named User Licensing? | 15 |
| About License Types | 15 |
| Perpetual Licenses | 15 |
| Trial Licenses | 15 |
| Installing Diver Platform Server | 16 |
| Downloading the Server Installation Package | 16 |
| Extracting the Server Installation Package | 19 |
| Obtaining a License for the DI Software | 20 |
| Using the exportinfo Utility to Obtain Machine Information | 20 |
| Obtaining the Licensing Package | 21 |
| Requesting a License | 25 |
| Using the register Utility to Install a License File | 28 |

| | |
|---|-----------|
| About Installing DiveLine | 30 |
| Installing and Configuring DiveLine | 31 |
| Creating an Administrator and a Test User | 36 |
| Creating a DiveLine Linux System User | 37 |
| Creating and Configuring an Encryption Key | 41 |
| Starting and Stopping the DiveLine Service | 42 |
| Verifying the DiveLine Installation | 43 |
| Starting DiveLine Automatically at System Boot | 44 |
| Downloading Java | 44 |
| Installing Java Development Kit | 46 |
| About Setting up an HTTPS Connection | 47 |
| Downloading Apache Tomcat | 48 |
| Installing Apache Tomcat | 51 |
| Generating an SSL Self-Signed Certificate | 55 |
| Enabling the Default HTTPS Connector | 56 |
| Verifying the HTTPS Connection | 59 |
| Installing DivePort | 60 |
| Verifying the DivePort Installation | 69 |
| Installing NetDiver | 71 |
| Verifying the NetDiver Installation | 74 |
| Installing Diver Platform Developer | 77 |
| Downloading and Extracting the Developer Installation Package | 77 |
| Installing ProDiver | 78 |
| ProDiver Installation Silent Option | 82 |
| Verifying the ProDiver Installation | 83 |

| | |
|--|----|
| Installing Workbench | 88 |
| Verifying the Workbench Installation | 91 |

Diver Platform 7.0 Overview

About This Installation Guide

This guide contains installation, configuration, and verification procedures to install the Diver Platform Server 7.0 package for Linux and Diver Platform Developer 7.0 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.

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

- **Diver Platform**—The Dimensional Insight software suite that contains Diver 7.0 software, including Workbench and Spectre. User categories are: Developer, ProDiver, DivePort, and DiveTab.
- **Diver Solution**—The Dimensional Insight software suite that contains Diver 7.0 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 or a PC. 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 on your machine.

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/customer-support/>
- 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 ETL (extract, transform, load) 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 on how to install the Diver Platform 7.0 Server software for Linux on a Virtual Machine (VM) using the following versions of VMware and Ubuntu:

- VMware version 10.0.3
- Ubuntu version 16.04

NOTE: Check the versions of Java and Apache Tomcat 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. DiveLine authenticates users and controls access to data through Diver clients such as DivePort and NetDiver.
- **DivePort** – The software component used to build portals that display 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 7.0 software on a Linux server while all Windows-based clients install on Windows laptops. To install DI Windows clients, such as ProDiver and Workbench, refer to [Installing Diver Platform Developer on page 77](#).

This guide assumes that a Linux administrator may perform the following pre-installation actions:

- Builds the DI directory structure and downloads the 3rd party and DI software to the DI downloads directory.
- Sets the permissions on the DI directories (note that the instructions in this guide will often identify where you may need to update the permissions on a directory or file).

NOTES:

- Installing the DI Platform Server for Linux is a manual process; it does not provide a wizard feature 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.

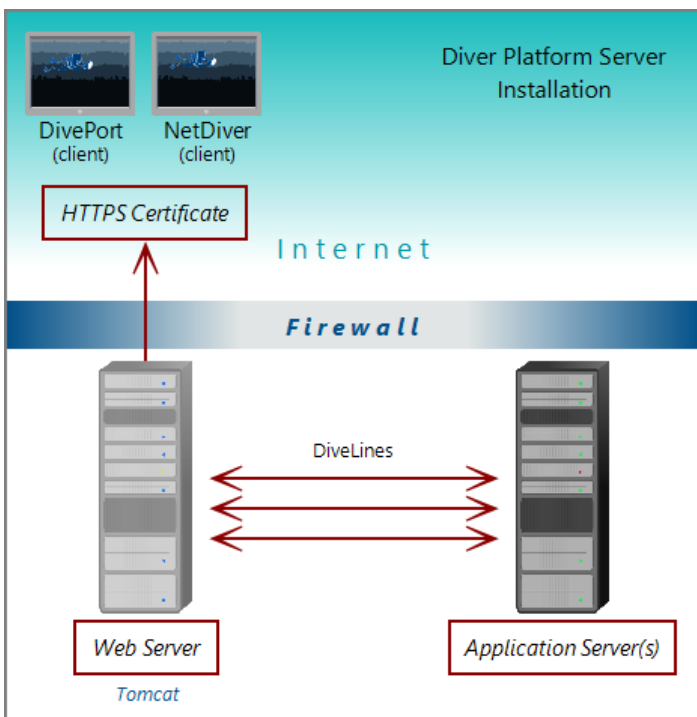
About Diver Platform Server 7.0

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 machines with VM capabilities. In some cases, several roles can share a single server environment by assigning different DiveLine port numbers to each role.

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

| Environment | Port Number |
|-------------|-------------|
| Production | 2130 |
| Test | 2131 |
| Development | 2132 |
| Build | 2135 |
| Bridge | 3330 |

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 DiveLines are installed on a virtual server machine.



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

About Diver Platform Developer 7.0

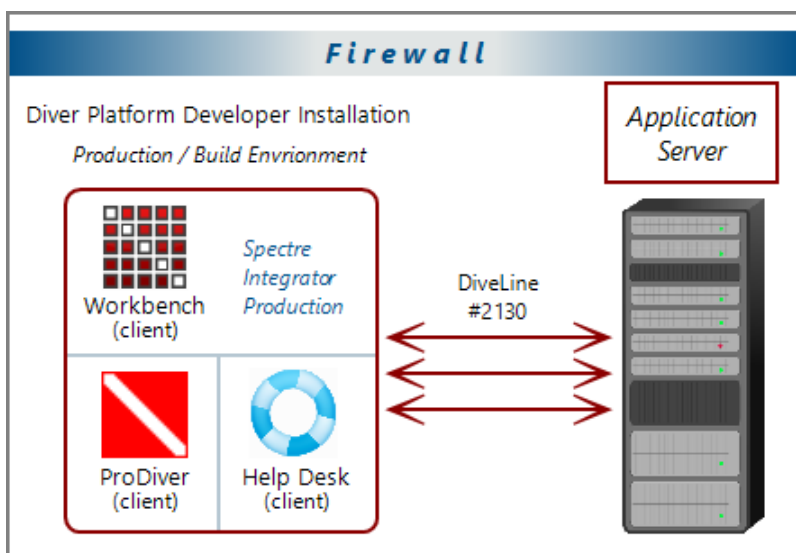
The Diver Platform Developer 7.0 package includes the following executables:

- **di-broadcast.exe**—A DiveLine client used to deliver 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 using a Windows user interface. Included to ease transition from version 6.x to 7.0. In 7.0, DI-Config functionality is part of the Workbench Server Settings.
- **di-scheduler.exe**—A DiveLine subcomponent that allows administrators to schedule jobs using a Windows user interface. Included to ease transition from version 6.x to 7.0. 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 machines independent of the machines that contain the server software. The developer software typically resides on machines 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 machines behind the company firewall.



Software Requirements

Before you install and operate Diver Platform 7.0 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.

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

| Application and Web Server | Support Notes |
|--|--|
| Linux | <p>Fully supported in the following configurations: Red Hat Enterprise Linux, CentOS, Debian, Ubuntu, SuSE.</p> <p>Latest version is recommended .64-bit is required.</p> <p>The Mono component is required to run Diver Solution and Diver Platform on Linux systems.</p> <p>DI recommends that you download the latest release from http://www.mono-project.com/download/.</p> |
| Microsoft Windows Server 2008 R2 | <p>Minimum version required to run DiveLine version 7.0 with Spectre. Server 2008 and later includes Microsoft .NET Framework which is needed for Workbench.</p> |
| Microsoft Windows Server 2012 | <p>Fully supported.</p> |
| Microsoft Windows Server 2016 or later | <p>Fully supported.</p> |

| Desktop Operating System | Support Notes |
|--------------------------|-------------------------|
| Microsoft Windows 7 | <p>Fully supported.</p> |
| Microsoft Windows 8 | <p>Fully supported.</p> |
| Microsoft Windows 8.1 | <p>Fully supported.</p> |
| Microsoft Windows 10 | <p>Fully supported.</p> |

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 | Fully supported. Version 11 or later recommended. |
| Google Chrome, Mozilla Firefox | Fully supported. Latest version recommended. |

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

| Java | Support Notes |
|------------------------------|--|
| Java 1.7.0.51 | Minimum version required for use of DIAL in 7.0. |
| latest version of OpenJDK 11 | Recommended version. NOTE: Diver Platform 7.0 is compatible with Java 11 and later, and OpenJDK. |

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.

TIP: On Tomcat 8, make sure to remove the `unpackWAR` attribute from the `Context` tag in DivePort's context *xml* file. The `unpackWAR` attribute is removed for Tomcat 8 and later using the Dimensional Insight installers.

| Apache Tomcat | Support Notes |
|------------------------------|---|
| Tomcat 7.0.67 | Minimum version required for use of web clients. |
| latest version of Tomcat 9.0 | Recommended version. NOTE: 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 4.0 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

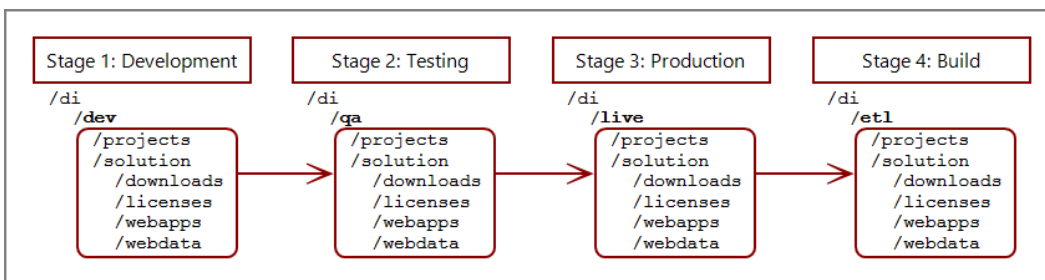
Prior to downloading and installing DI Platform server and developer software for 7.0, DI recommends that you create the following directory structure on your machine:

```

/di
  /projects
  /solution
    /downloads
    /licenses
    /webapps
    /webdata
    
```

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

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



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 is created manually. |
| /di | /solution | Folders and files created by DI product installations. This is created manually. |
| /di/solution | /downloads | Default location for DI software downloads. This is created manually. |
| /di/solution | /licenses | Folder for licenses and key files. This is created manually. |
| /di/solution | /diveline | Subdirectory with program files required by the DiveLine service. Each installed DiveLine instance can have its own <code>/diveline</code> directory. |
| /di/solution | /dl-dataroot | Top level directory for the DiveLine server for configuration information, cache, and log files. Each DiveLine installed can have its own <code>/dl-dataroot</code> instance. |
| /di/solution | /executables | Default location for many DI executables. |
| /di/solution | /webapps | Program, configuration, and setup files for DivePort and NetDiver. This is created manually. |

| Directory | Subdirectory | Description |
|--------------|--------------|---|
| /di/solution | /webdata | Data and customization files for DivePort and NetDiver. This is created manually. |

Building the DI Directory Structure

NOTE: You must have root user privileges (for example, type `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 Developer Linux installation, without different environments.

Complete the following steps:

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

```

jsmith@ubuntu:~$

```

3. Go to the root directory.

```
cd /
```

4. Create the `di` folder

```
sudo mkdir di
```

NOTE: Enter the user password if prompted.

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

```
ls
```

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

```

jsmith@ubuntu:/$ sudo mkdir di
[sudo] password for jsmith:
jsmith@ubuntu:/$ ls
bin  dev  home  lib64  mnt  root  snap  vmlinux
boot di  initrd.img  lost+found  opt  run  srv  usr
cdrom  etc  lib      media      proc  sbin  sys  var

```

6. Change to the `di` folder:

```
cd di
```

7. Optionally, create a directory for each environment.

- a. Create a directory (for example, `live`) by typing the following command and pressing **Enter**:

```
sudo mkdir live
```

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

```
ls
```

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

- 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 and pressing **Enter**:

- `sudo mkdir solution`
- `sudo mkdir projects`

9. Confirm that the folders were created successfully:

```
ls
```

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

10. Navigate to the `solution` directory:

```
cd solution
```

11. Add the following subdirectories by typing each of the following commands and pressing **Enter**:

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

12. Confirm that the folders were created successfully.

```
ls
```

A list of files and directories in the `solution` directory opens.

About Diver Platform and Solution 7.0 Licenses

Diver Platform 7.0 is the paid upgrade path for customers who want to use the Spectre engine, DiveTab, or Measure Factory. Diver Solution 7.0 is the free, standard software upgrade path for Diver Solution 6.4 customers on a maintenance plan. The way users are licensed depends 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 7.0 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 so they can make user account changes without consuming a Developer license

Diver Solution Licenses

Diver Solution 7.0 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 7.0 are:

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

What Is Named User Licensing?

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

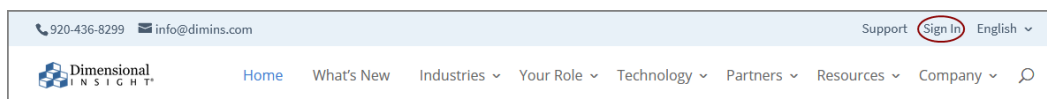
Installing Diver Platform Server

Downloading the Server Installation Package

You can download purchased software from the Dimensional Insight website. Dimensional Insight recommends that you download the software using a graphical web browser, rather than by invoking the `wget` command. Keep in mind that you might need to use another computer to download the server package, and then transfer the files onto your server.

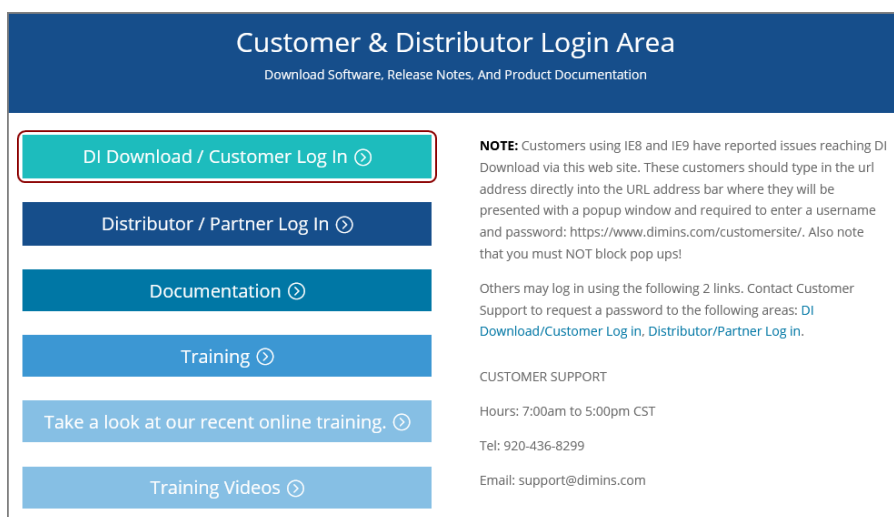
NOTE: Administrative privileges are required to install the software.

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

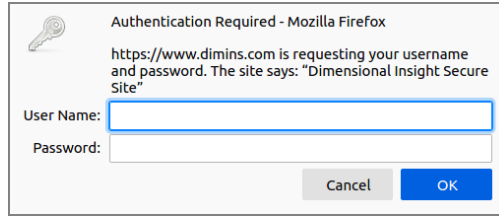


The **Customer & Distributor Login Area** page opens.

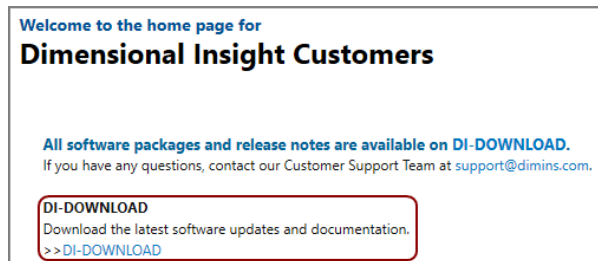
3. Click **DI Download / Customer Log In**.



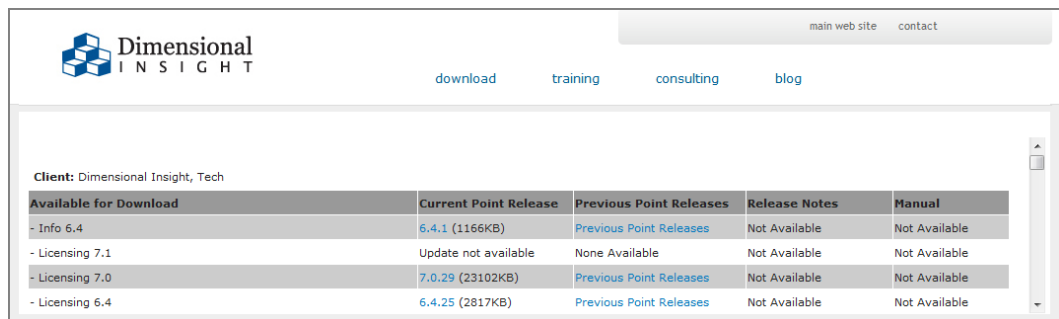
The **Authentication Required** dialog box opens.



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.

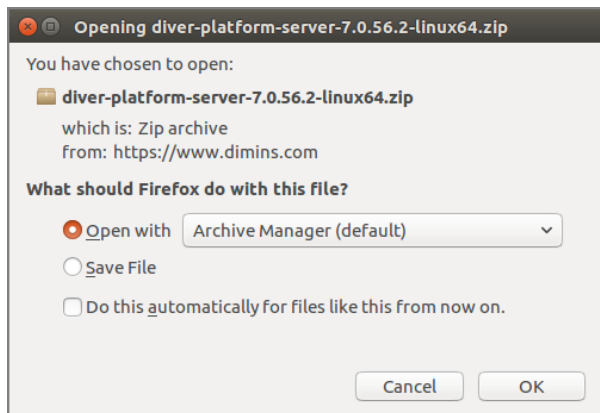


6. Locate the latest version of the 7.0 software that you purchased, and click the blue version number.

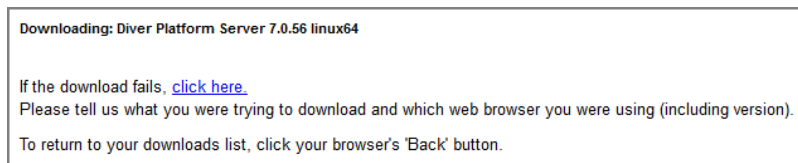
| | | | | |
|---|--------------------|---|---------------------------------------|---------------------------------|
| Diver Platform Server 7.1 Windows Unicode limited | 7.1.19 (1617944KB) | Previous Point Releases | Release Notes (212KB) | Not Available |
| Diver Platform Server 7.1 Windows | 7.1.19 (1699460KB) | Previous Point Releases | Release Notes (212KB) | Not Available |
| Diver Platform Server 7.1 Windows limited | 7.1.19 (1699462KB) | Previous Point Releases | Release Notes (212KB) | Not Available |
| Diver Platform Server 7.0 linux64_uc limited | 7.0.56 (499775KB) | Previous Point Releases | Release Notes (890KB) | Manual (9143KB) |
| Diver Platform Server 7.0 linux64 | 7.0.56 (499719KB) | Previous Point Releases | Release Notes (890KB) | Manual (9143KB) |
| Diver Platform Server 7.0 linux64 limited | 7.0.56 (499723KB) | Previous Point Releases | Release Notes (890KB) | Manual (9143KB) |
| Diver Platform Server 7.0 Windows Unicode limited | 7.0.56 (1258822KB) | Previous Point Releases | Release Notes (890KB) | Manual (9143KB) |

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

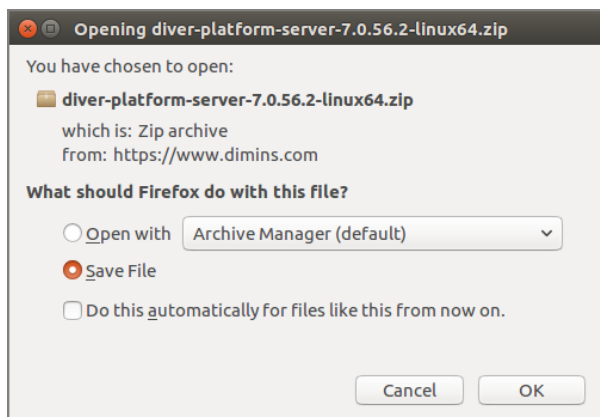
Diver Platform 7.0



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 is downloaded to the `Downloads` directory on the local machine.

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

8. If necessary, move the *zip* file onto the Linux server.
9. On the Linux server, move the *zip* file to the `/di/solution/downloads` folder using the following command:

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

Extracting the Server Installation Package

1. Go to the `/di/solution/downloads` folder using the following command:

```
cd /di/solution/downloads
```

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

```
ls
```

3. Copy the file to the `/di/solution` folder using the following command:

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

4. Navigate to the `/di/solution` folder using the following command:

```
cd /di/solution
```

5. Confirm that the file is in this folder using the following command:

```
ls
```

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

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

7. After the processes finishes, view the files that were extracted using the following command:

```
ls
```

The following files now display:

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

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

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

9. Verify that the files are extracted using 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/solution` folder using the following command:

```
cd /di/solution
```

2. Confirm that the `exportinfo` utility is in the directory using the following command:

```
ls
```

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

3. View the permissions for the `exportinfo` utility using 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. Modify the execute permission using the following command:

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

- b. Verify the permission change using the following command:

```
ls -l exportinfo
```

The permissions display as `-rwxr-xr-x`, which means that you can run the utility.

4. Run the `exportinfo` utility using 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 using 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/solution/licenses` folder using the following command:

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

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

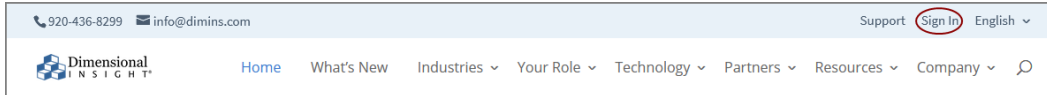
```
ls
```

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

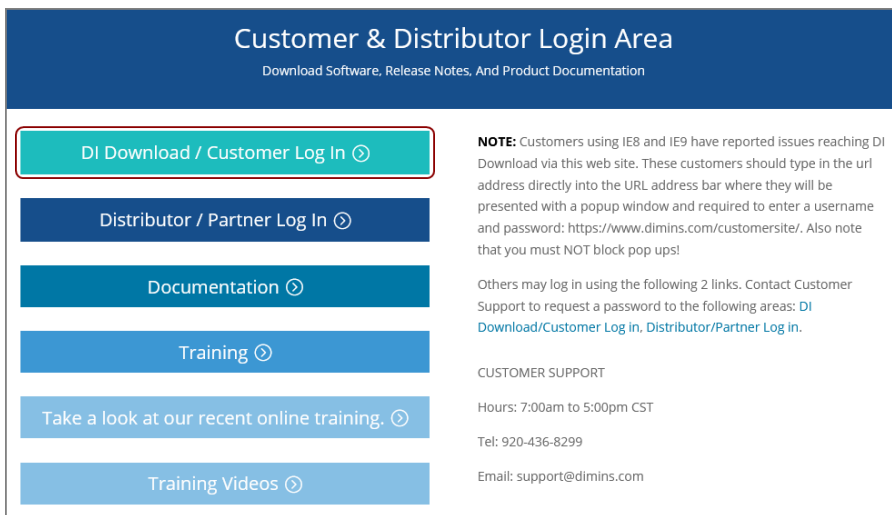
1. On the Windows computer with the *info* file, open a web browser, and go to the Dimensional Insight website (www.dimins.com).
2. On the home page, click **Sign In**.

Diver Platform 7.0



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**.

Welcome to the home page for
Dimensional Insight Customers

All software packages and release notes are available on **DI-DOWNLOAD**.
 If you have any questions, contact our Customer Support Team at support@dimins.com.

DI-DOWNLOAD
 Download the latest software updates and documentation.
[>>DI-DOWNLOAD](#)

The software and documents download page opens.

The screenshot shows the Dimensional Insight website. The navigation menu includes 'download', 'training', 'consulting', and 'blog'. Below the menu is a table with the following data:

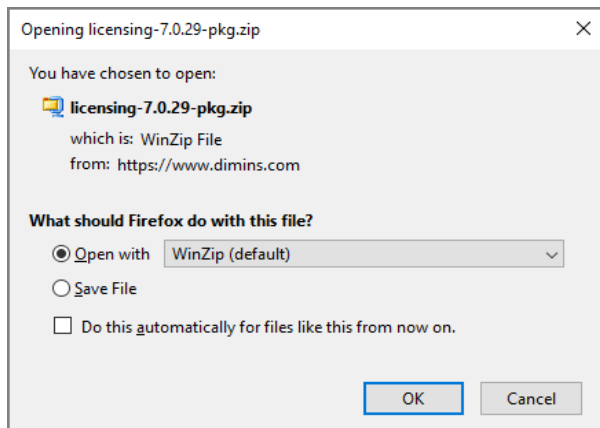
| Available for Download | Current Point Release | Previous Point Releases | Release Notes | Manual |
|------------------------|----------------------------------|---|---------------|---------------|
| - Info 6.4 | 6.4.1 (1166KB) | Previous Point Releases | Not Available | Not Available |
| - Licensing 7.1 | Update not available | None Available | Not Available | Not Available |
| - Licensing 7.0 | 7.0.29 (23102KB) | Previous Point Releases | Not Available | Not Available |
| - Licensing 6.4 | 6.4.25 (2817KB) | Previous Point Releases | Not Available | Not Available |

6. Locate the latest version of the **Licensing 7.0** package, and click the blue version number.

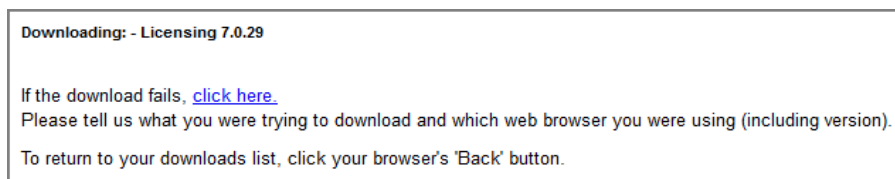
| Available for Download | Current Point Release |
|------------------------|----------------------------------|
| - Info 6.4 | 6.4.1 (1166KB) |
| - Licensing 7.0 | 7.0.29 (23102KB) |
| - Licensing 6.4 | 6.4.25 (2817KB) |
| - Trial Licenses 6.1 | 6.1.1310 (25KB) |

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

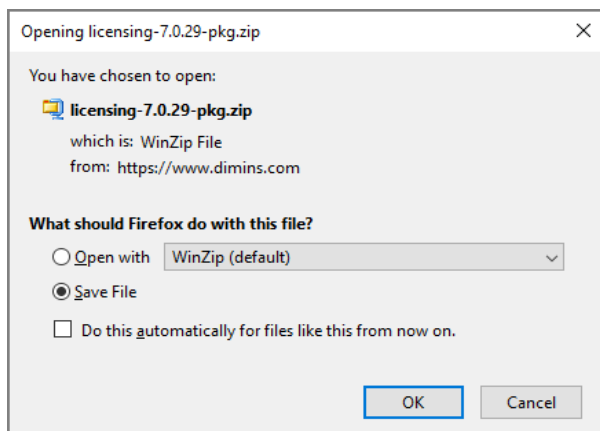
Diver Platform 7.0



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 licensing software package *zip* file is downloaded to the **Downloads** directory on the local machine.

NOTE: The Licensing 7.0 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.

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

NOTE: The *info* file is created in Step 5 of [Using the exportinfo Utility to Obtain Machine Information on page 20](#).

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*).

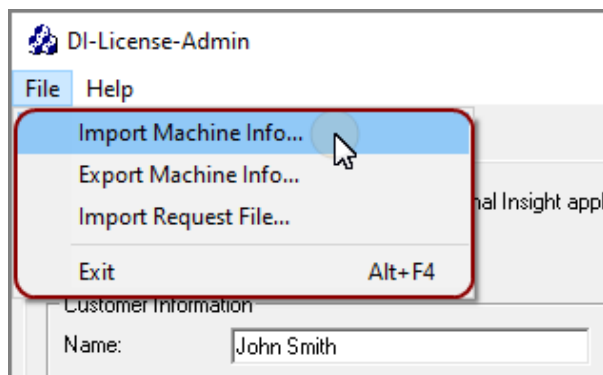
The **User Account Control** dialog box opens, asking you to confirm making changes to your device.

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

3. Click **Yes**.

The DI-License-Admin utility starts.

4. Click the **Request Licenses** tab.
5. Click **File > Import Machine Info**.

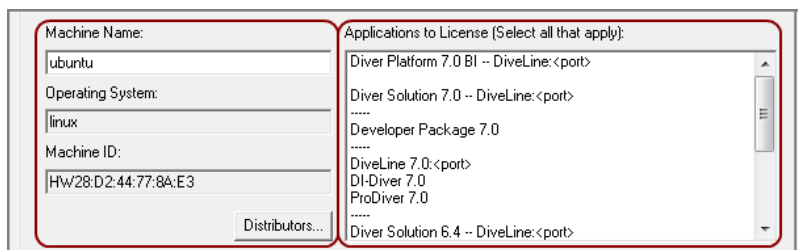


6. In the **Import Machine Info** dialog box, select the *info* file that you created and click **Open**.

Diver Platform 7.0

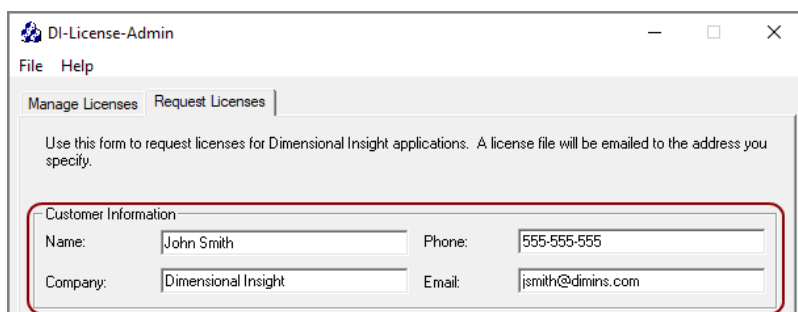
On the left, the **Machine Name**, **Operating System**, and **Machine ID** boxes are populated with the machine information from the *info* file.

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



The screenshot shows a form with two main sections. The left section, titled 'Machine Information', contains three text boxes: 'Machine Name' with 'ubuntu', 'Operating System' with 'linux', and 'Machine ID' with 'HW28:D2:44:77:8A:E3'. Below these is a 'Distributors...' button. The right section, titled 'Applications to License (Select all that apply):', is a list box containing several items: 'Diver Platform 7.0 BI -- DiveLine:<port>', 'Diver Solution 7.0 -- DiveLine:<port>', '.....', 'Developer Package 7.0', '.....', 'DiveLine 7.0:<port>', 'DI-Diver 7.0', 'ProDiver 7.0', '.....', and 'Diver Solution 6.4 -- DiveLine:<port>'. A vertical scrollbar is visible on the right side of the list box.

7. Complete the **Customer Information** section.



The screenshot shows a window titled 'DI-License-Admin' with a menu bar 'File Help'. Below the menu bar are two tabs: 'Manage Licenses' and 'Request Licenses'. A message reads: 'Use this form to request licenses for Dimensional Insight applications. A license file will be emailed to the address you specify.' Below this is a section titled 'Customer Information' with four text boxes: 'Name' (John Smith), 'Phone' (555-555-555), 'Company' (Dimensional Insight), and 'Email' (jsmith@dimins.com).

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 you purchased. For example, if you purchased Diver Platform Server 7.0 for Linux, select **Diver Platform 7.0 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 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.

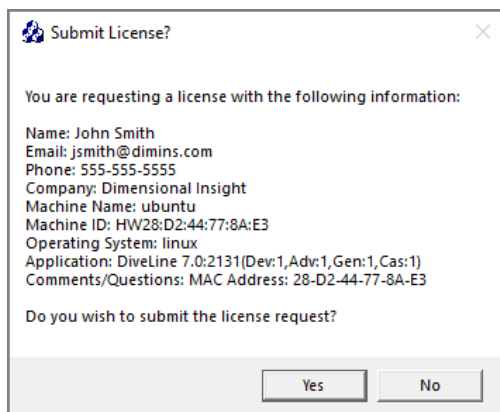
For example, if you purchased Diver Platform, select **Developer Package 7.0**.

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:

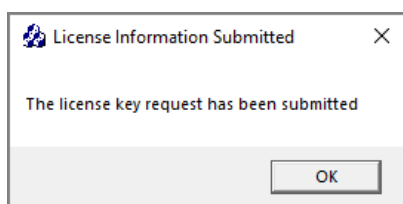
NOTE: If installed on a virtual machine and that machine is relocated, a new license is required. This can be avoided by ensuring the virtual

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.



14. Click **Save** to store the license request file.
15. If necessary, move the *request* file onto the Linux server.
16. On the Linux server, move the *request* file to the `/di/solution/licenses` folder using the following command:

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

Using the register Utility to Install a License File

After you receive your license from Dimensional Insight, you must install it on your server.

As of version 7.0, all licenses are installed on the server. This includes 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/solution/licenses` folder using a command similar to the following:

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

3. Navigate to the `/di/solution/licenses` folder using a command similar to the following:

```
cd /di/solution/licenses
```

4. Unzip the file using the following command:

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

5. Confirm that the *license* file is extracted using the following command:

```
ls
```

TIP: Take note the name of the license file. This is used when running the register utility.

6. Navigate to the `/di/solution` folder using the following command:

```
cd /di/solution
```

7. Confirm that the register utility is in the directory using the following command:

```
ls
```

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

8. View the permissions for the register utility using the following command:

```
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.

If you do not have permission to run the utility:

- a. Modify the execute permission using the following command:

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

- b. Verify the permission change using the following command:

```
ls -l register
```

The permissions display as `-rwxr-xr-x`, which means that you can run the utility.

9. Move the register utility to the `/di/solution/diveline/bin` directory using the following command:

NOTE: You cannot run the register utility successfully unless it is in this directory.

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

10. Go to the `/di/solution/diveline/bin` directory using the following command:

```
cd diveline/bin
```

11. Confirm that the register utility is in the directory using the following command:

```
ls
```

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

12. Run the register utility, and specify which *license* file to install using the following command:

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

13. Confirm that the installation was successful using the following command:

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

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

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

NOTE: Repeat this process for each environment.

About Installing DiveLine

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

Please be aware of the following before installing and configuring 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 your installed DiveLine clients exchange information with users on the other side 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 hostname and port number. Typically, you install DiveLine on port 2130, which needs to be open in the corporate firewall.

The following list provides some suggestions on how to set up and configure DiveLine inside a corporate network:

- DiveLine communicates with clients using a proprietary protocol known as Dimensional Insight DiveLine Protocol (DIDP). You may need to configure your network to enable DIDP communications.
- Although configurable, DiveLine, by default, 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 to act as gateway for DIDP network traffic.
- Configure your firewall to transparently route two-way traffic on the correct port to the DiveLine service.
- Typically, internal hosts (users inside the firewall) can connect directly to the DiveLine service, while external hosts connect to the network firewall, which then routes traffic to DiveLine.
- Clients connect to the DiveLine service using TCP/IP.
- If client machines are running Windows operating systems, ensure that the personal firewalls on these machines allow incoming connections from the port (for example, 2130) 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/solution/dl-dataroot`).

Installing and Configuring DiveLine

After decompressing the `di-diveline.tar.gz` file in [Extracting the Server Installation Package on page 19](#), the `/di/solution/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 *dlk* template file used with Web Server authentication
- **install files**—Directory containing files that are used when installing DiveLine, some 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 7.0
- **install-di-diveline**—The installation *shell* script
- **README**—Directory contents and support email address

NOTE: Words are case sensitive in Linux.

To install and configure DiveLine on your machine:

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

```
cd /di/solution/diveline
```

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

```
ls
```

3. View the permissions for the *install-di-diveline* installation script using 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. Modify the execute permission using the following command:

```
sudo chmod 755 install-di-diveline
```

- b. Verify the permission change using the following command:

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

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

4. Run the install script using the following command:

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

```

jsmith@ubuntu:/di/solution/diveline$ sudo sh install-di-diveline
[sudo] password for jsmith:
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]

```

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/solution` 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/solution/dl-dataroot`.

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**
- State/province - **MA**
IMPORTANT: The country code must be two characters long.
- 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/solution/dl-dataroot/config` directory.

Alternatively, you can create the keypair files after the DiveLine installation. Refer to [Creating and Configuring an Encryption Key](#) for instructions.

5. Navigate to the `/di/solution/dl-dataroot/config` directory:

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


6. Verify the keypair files are created successfully:

```
ls
```

7. Navigate to the `/di/solution/diveline/bin` directory using the following command:

```
cd /di/solution/diveline/bin
```

8. Confirm that the `init-di-diveline` file is in the directory using the following command:

```
ls
```

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

9. View the permissions for the `init-di-diveline` file using 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. Modify the execute permission using the following command:

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

- b. Verify the permission change using the following command:

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

The permissions display as `-rwxrwxrwx`.

10. Open the `init-di-diveline` script with a text editor, such as **gedit**, using the following command:

```
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.

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

- DIDLUSER=diveline—DiveLine runs as the user "diveline"
- DIBASE=/di/solution—The location of the base DI Solution directory
- DIDATAROOT=\$DIBASE/dl-dataroot—The directory where DiveLine stores the config, acl, cache, log, and data directories
- DIBINDIR=\$DIBASE/diveline/bin
- DISERVICE=di-service—The name of the existing **di-service**
- DIPORTNUM=2131—The listening port for DiveLine on the server
NOTE: This is the port number you chose when requesting a license. Port 2130 is the default.

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

Creating an Administrator and a Test User

This topic 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` specified in the *init-di-diveline* file.

To create users for DiveLine:

1. Change to the `/executables` directory using the following command:

```
cd /di/solution/executables
```

2. View the permissions for **dicfg** using the following command:

```
ls -l dicfg
```

The permissions display. If the permissions are `-rwxrwxrwx`, you can create users. If you do not have permission to create users:

- Modify the execute permission using the following command:

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

- Verify the permission change using the following command:

```
ls -l dicfg
```

The permissions display as `-rwxrwxrwx`.

3. Create the administrator user ID using the following command:

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

For example:

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

4. Create the test user ID using the following command:

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

For example:

```
sudo ./dicfg -dataroot /di/solution/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 should have the right to "Log On As a Service" and have a strong password.

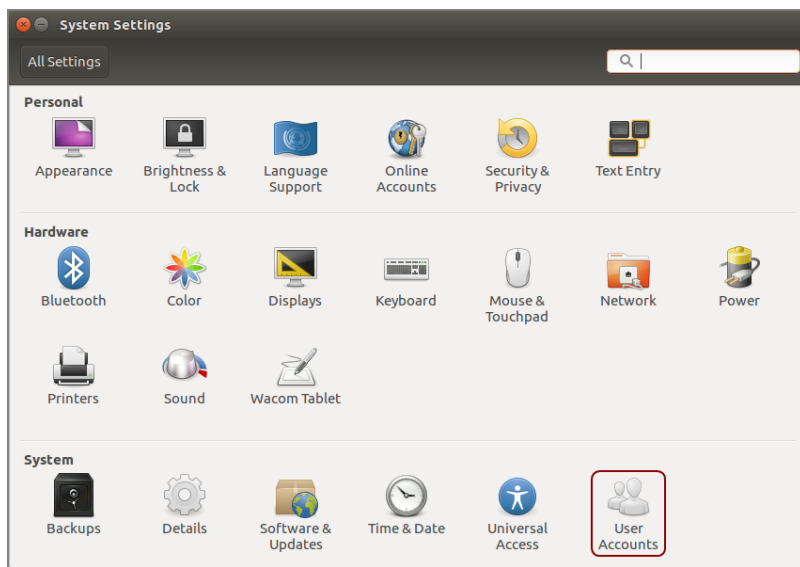
Your Linux administrator may have previously created a system user for DiveLine prior to the installation process. If so, record the name and password of the DiveLine user, or contact your administrator for assistance.

Diver Platform 7.0

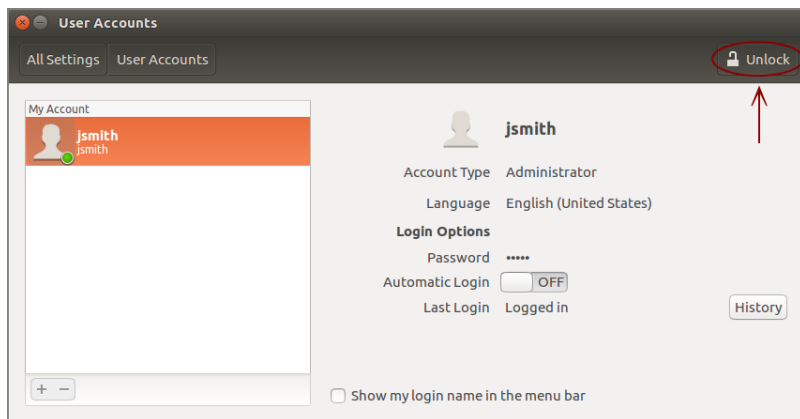
To create a Linux system user:



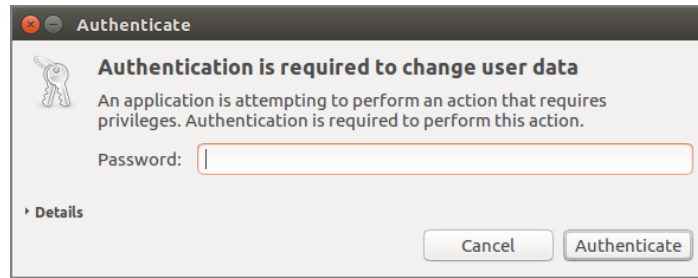
1. Click the **System Settings** icon, , in the left-hand panel. A page similar to the following opens:



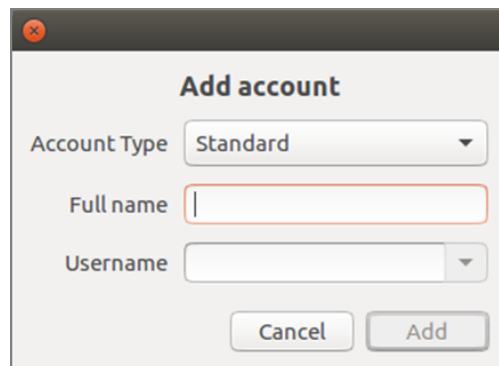
2. Double-click the **User Accounts** icon. The **User Accounts** dialog box opens.



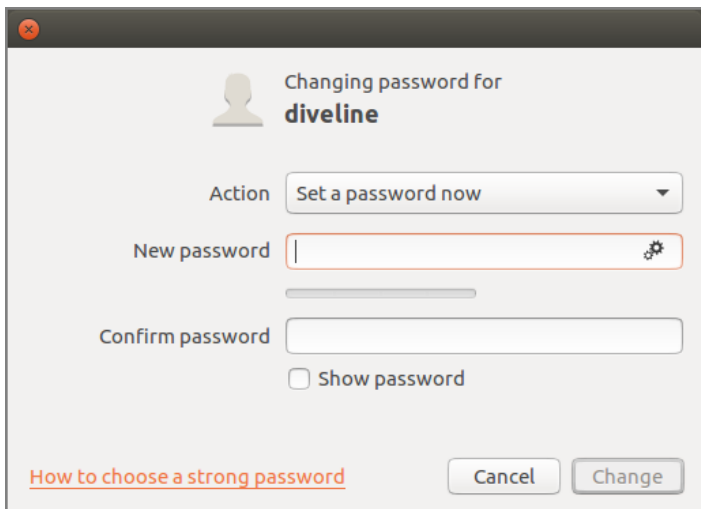
3. Click the **Unlock** icon to enable editing. The **Authenticate** dialog box opens.



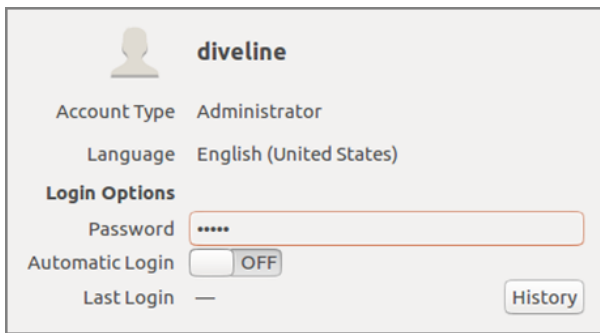
4. Enter your password, and click the **Authenticate** button.
The dialog box closes.
5. On the bottom left of the **User Accounts** window, click the plus sign button.
The **Add account** dialog box opens.



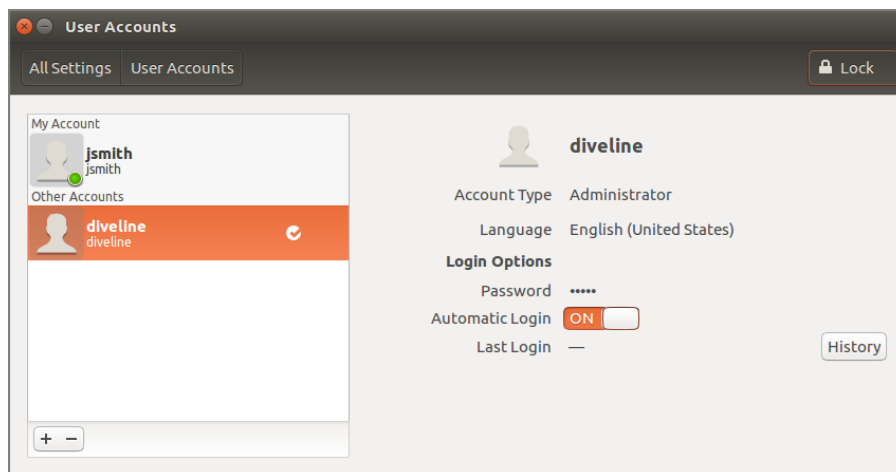
6. Do the following:
 - Select the Account Type **Administrator**.
 - Enter **diveline**, or another name of your choosing for running the DiveLine service, in the **Full name** and **Username** fields.
NOTE: This is the same name identified for the `DIDLUSER` in Step 10 of [Installing and Configuring DiveLine on page 31](#).
7. Click **Add**.
NOTE: Re-enter your password when prompted.
The **diveline** account is now listed under **Other Accounts**.
8. Click **Account Disabled** next to **Password**.
The changing password dialog box opens.



9. Enter a password in the **New password** and **Confirm password** fields.
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, click the **OFF** button next to **Automatic Login**.
The button changes to **ON** and turns orange.



12. Click the **Lock** button and close the window.

Creating and Configuring an Encryption Key

Use `genkey`, 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 in [Installing and Configuring DiveLine on page 31](#).

Complete the following steps:

1. Go to the `/di/solution/executables` directory using the following command:

```
cd /di/solution/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/solution/dl-dataroot` directory using the following command:

```
cd /di/solution/dl-dataroot
```

4. View permissions for `/config` using 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. Modify the execute permission using the following command:

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

- b. Verify the permission change using the following command:

```
ls -l config
```

The permissions display as `drwxrwxrwx`.

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

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

6. Change to the `/config` directory using the following command:

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

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

```
ls
```

Starting and Stopping the DiveLine Service

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

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

- a. Navigate to the `/di/solution` directory using the following command:

```
cd /di/solution
```

- b. Check the permissions using the following command:

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



```

jsmith@ubuntu:/di/solution$ ls -l dl-dataroot
total 36
drwxrwxrwx 3 root root 4096 Mar 17 11:22 acl
-rwxrwxrwx 1 root root 122 Mar 17 11:22 acl.dir
drwxrwxrwx 2 root root 4096 Mar 17 11:18 cache
drwxrwxrwx 2 root root 4096 Mar 17 13:44 config
drwxrwxrwx 3 root root 4096 Mar 17 11:22 data
drwxrwxrwx 3 root root 4096 Mar 17 11:18 logs-dicfg
drwxrwxrwx 2 root root 4096 Mar 17 11:18 security
drwxrwxrwx 2 root root 4096 Mar 17 11:18 temp
drwxrwxrwx 2 root root 4096 Mar 17 11:18 webdir
jsmith@jsmith-001:/di/solution$

```

- c. Modify the execute permission using the following command:

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

NOTE: This changes the permissions for the dl-dataroot directory and its contents.

- d. Verify the permission change using the following command:

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

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

- Start DiveLine using the following command:

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

- Stop DiveLine using the following command:

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

- Restart DiveLine using 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) using 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 using the following command:

```
sudo sh /di/solution/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. Once connected, type `?`.

The installed 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. Type `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 execute at startup. Depending on the flavor of Linux that you are running, refer to your system administrator or vendor documentation for more information.

Downloading Java

At this point in the installation process, you must install (or have already installed) a Java SE version 7 or higher on your machine. Additionally, if you want to create a self-signed certificate, you must install the JDK version of the Java software. Before proceeding with these download instructions, uninstall any older versions of Java SE.

This procedure uses OpenJDK.

NOTE: The Linux administrator may already have downloaded the JDK package to your `/di/solution/downloads` directory. In addition, the administrator may need to set permissions on all the directories in the DI structure.

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/>

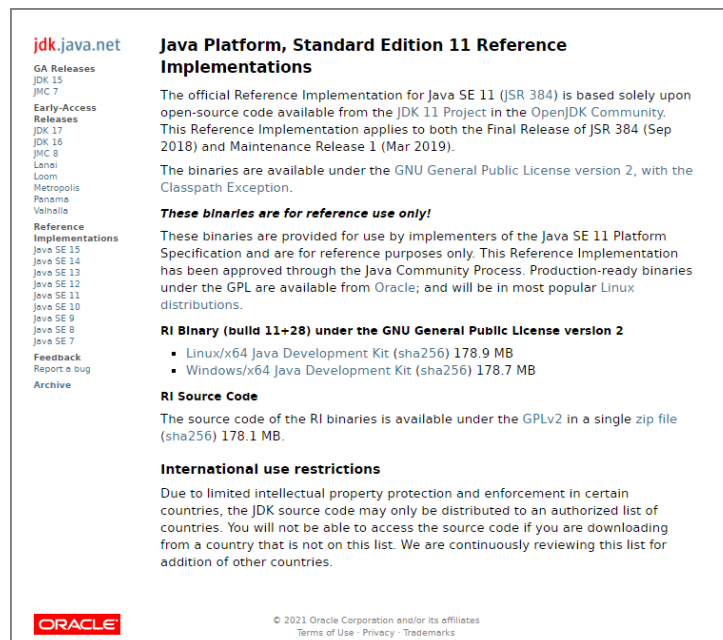
NOTE: The appearance of the website can change over time.

The home page appears similar to the following:



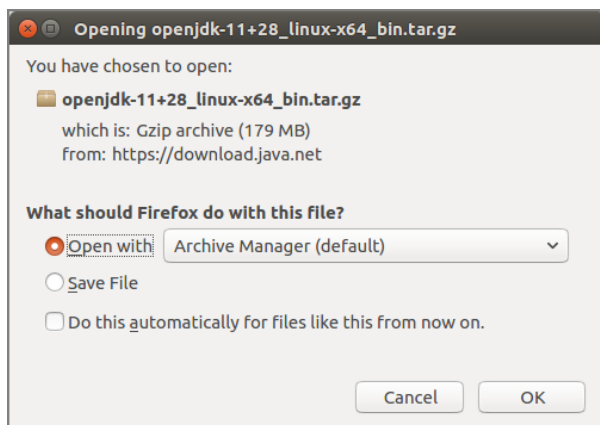
3. Click the Java SE 11 reference implementation.

The Java Platform, Standard Edition 11 Reference Implementations page opens.



4. Click **Linux/x64 Java Development Kit**, and download the file to your machine.

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



5. Select **Save File**.
6. Click **OK**.

The software is saved to the default download directory.

7. Navigate to the file and move it to the `/di/solution/downloads` directory on your Linux server or VM using a command similar to the following:

```
sudo mv openjdk-11+28_linux-x64_bin.tar.gz  
/di/solution/downloads
```

8. Navigate to the `/di/solutions/downloads` directory using the following command:

```
cd /di/solution/downloads
```

9. Verify that the file copied correctly using the following command:

```
ls
```

10. 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

After downloading the latest version of the Java SE 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.

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

To install Java:

1. Go to the `/di/solution/downloads` directory using the following command:

```
cd /di/solution/downloads
```

2. Extract the JDK file using a command similar to the following:

```
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` sub-directory.

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

```
cd jdk-11
```

4. View the directory content using the following command:

```
ls
```

```
jsmith@ubuntu:/di/solution/downloads$ cd jdk-11
jsmith@ubuntu:/di/solution/downloads/jdk-11$ ls
bin  conf  include  jmods  legal  lib  release
jsmith@ubuntu:/di/solution/downloads/jdk-11$
```

About Setting up an HTTPS Connection

The DivePort and NetDiver clients, which can reside outside of the company firewall, need to run over a secure HyperText Transfer Protocol (HTTPS) with Secure Socket Layer (SSL) 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.

Whenever you run DivePort or NetDiver, the web browser points to a secured domain that requires an SSL handshake to authenticate both the server and client. You must purchase and install a certificate on all servers that interact with DI web clients. A certificate authority creates an SSL certificate, also called a digital certificate, to establish a secure encrypted connection between a browser and a server.

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 SSL 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

At this point in the installation process, you must install (or have already installed) Apache Tomcat on your machine.

Dimensional Insight recommends that the DivePort, NetDiver, and DiveTab software runs on the Tomcat web server.

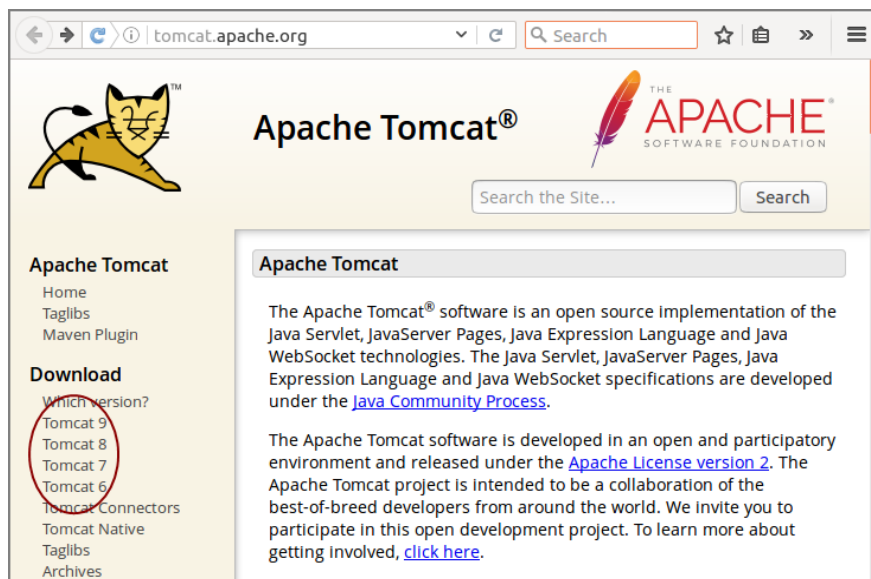
NOTE: Tomcat 7.0 reached its end-of-life as of March 2021, and no longer receives updates. DI recommends updating to Tomcat 9.0.

To download Apache Tomcat:

1. Open a web browser.
2. Open the **Apache Tomcat** home page at:

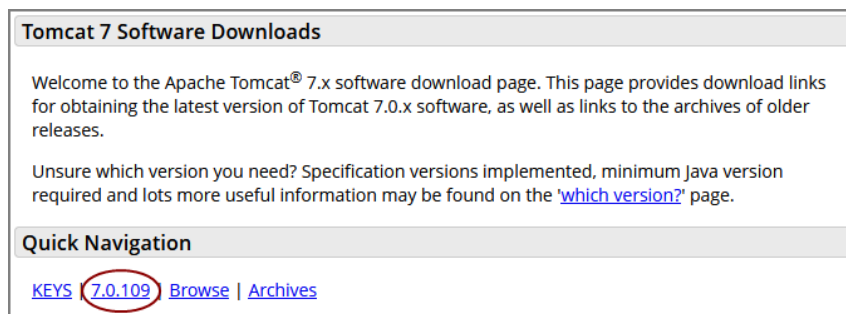
<http://tomcat.apache.org>

The URL for this web site can change over time, but the home page is similar to the following:

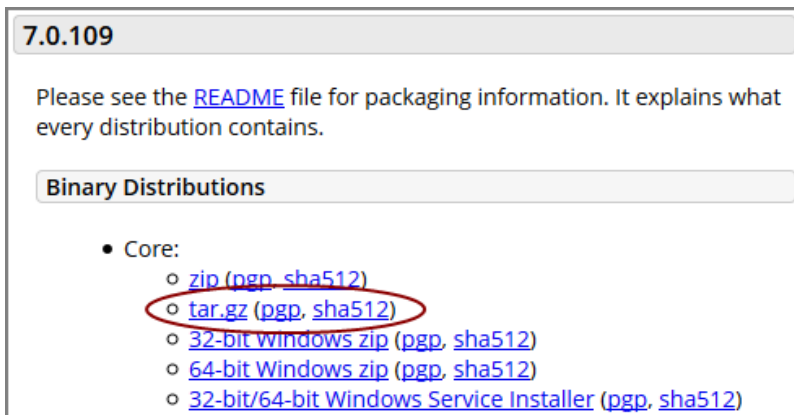


3. Click the **Tomcat <version number>** button.

The **Tomcat <version number> Software Downloads** page opens, and appears similar to the following:

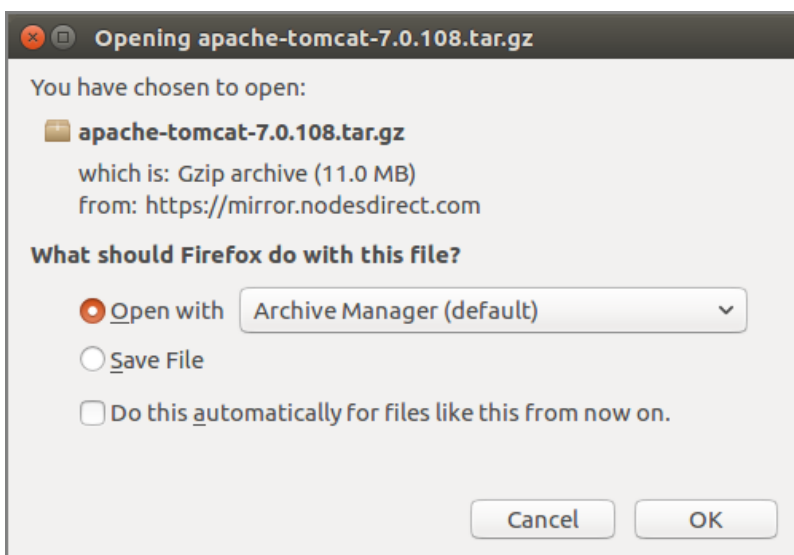


4. In the **Quick Navigation** section, click **<version number>** button to open the **Binary Distributions** section shown below:



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 the local machine.

8. Navigate to the file location.

9. Move the file to the `/di/solution/downloads` directory using the following command:

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


10. Navigate to the `/di/solution/downloads` directory using the following command:

```
cd /di/solution/downloads
```

11. Verify that the file moved correctly using the following command:

```
ls
```

12. Close the web browser.

Installing Apache Tomcat

This topic 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 may vary at your site.

NOTE: Tomcat 7.0 reached its end-of-life as of March 2021, and no longer receives updates. DI recommends updating to Tomcat 9.0.

To install Apache Tomcat:

1. Navigate to the `/di/solution/downloads` directory using the following command:

```
cd /di/solution/downloads
```

2. Decompress the `apache-tomcat-<version number>.tar.gz` file using the following command:

```
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 using the following command:

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

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

```
sudo apt-get update
```

```
jsmith@ubuntu:/di/solution/downloads/apache-tomcat-7.0.109$ sudo apt-get update
Hit:1 http://us.archive.ubuntu.com/ubuntu xenial InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu xenial-updates InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu xenial-security InRelease
Reading package lists... Done
jsmith@ubuntu:/di/solution/downloads/apache-tomcat-7.0.109$
```

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 using a command similar to the following:

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

```
jsmith@ubuntu:/di/solution/downloads/apache-tomcat-7.0.109$ sudo apt-get ins
tall tomcat7
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

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

6. Navigate to the `/etc/default` directory using the following command:

```
cd /etc/default
```

7. View the permissions for the `tomcat<version number>` configuration file using a command similar to the following:

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

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

- a. Modify the execute permission using the following command:

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

- b. Verify the permission change using the following command:

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

The permissions display as `-rwxrwxrwx`.

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

```
gedit tomcat7
```

Here is an example of the configuration file:

```
# Run Tomcat as this user ID. Not setting this or leaving it blank will use the
# default of tomcat7.
TOMCAT7_USER=tomcat7 ←

# Run Tomcat as this group ID. Not setting this or leaving it blank will use
# the default of tomcat7.
TOMCAT7_GROUP=tomcat7

# The home directory of the Java development kit (JDK). You need at least
# JDK version 6. If JAVA_HOME is not set, some common directories for
# OpenJDK, the Oracle JDK, and various Java SE 6+ versions are tried.
#JAVA_HOME=/usr/lib/jvm/openjdk-6-jdk

# You may pass JVM startup parameters to Java here. If unset, the default
# options will be: -Djava.awt.headless=true -Xmx128m -XX:+UseConcMarkSweepGC
#
# Use "-XX:+UseConcMarkSweepGC" to enable the CMS garbage collector (improved
# response time). If you use that option and you run Tomcat on a machine with
# exactly one CPU chip that contains one or two cores, you should also add
# the "-XX:+CMSIncrementalMode" option.
JAVA_OPTS="-Djava.awt.headless=true -Xmx128m -XX:+UseConcMarkSweepGC"
```

TOMCAT7_USER=tomcat7 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 TOMCAT7_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/solution/webdata
```

For example:

```
jsmith@ubuntu:/$ sudo chown -R tomcat7 /di/solution/webdata
```

13. To start and stop the Tomcat server, change to the init.d directory using the following command:

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

- To start Tomcat, type the following:

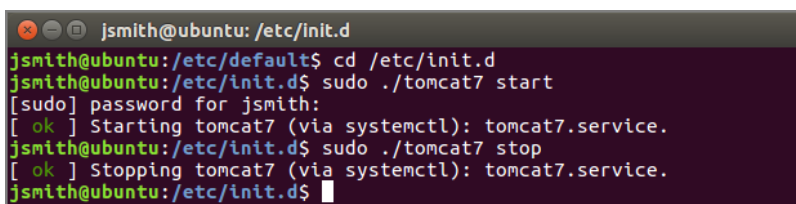
```
sudo ./tomcat<version number> start
```

- To stop Tomcat, type the following:

```
sudo ./tomcat<version number> restart
```

- To stop Tomcat, type the following:

```
sudo ./tomcat<version number> stop
```



```
jsmith@ubuntu: /etc/init.d
jsmith@ubuntu:/etc/default$ cd /etc/init.d
jsmith@ubuntu:/etc/init.d$ sudo ./tomcat7 start
[sudo] password for jsmith:
[ ok ] Starting tomcat7 (via systemctl): tomcat7.service.
jsmith@ubuntu:/etc/init.d$ sudo ./tomcat7 stop
[ ok ] Stopping tomcat7 (via systemctl): tomcat7.service.
jsmith@ubuntu:/etc/init.d$
```

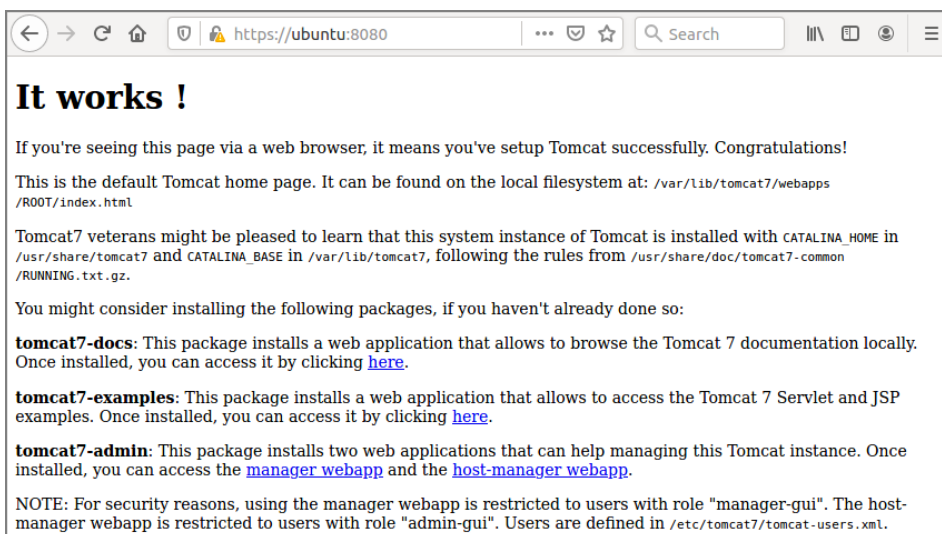
NOTE: The `/etc/init.d` directory holds shell scripts that respond to start, stop, and restart commands to manage a particular service.

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

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

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

Press **Enter** to display a page similar to the following:



NOTE: It is possible to install Tomcat using a system account which is not an administrator. This would prevent 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 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 (`sudo /etc/init.d/tomcat<version number> stop`)

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 works by using a combination of a public certificate and a private key. The SSL key is kept secret on the server and is used to encrypt content sent to clients. The SSL 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 key.

To generate a self-signed certificate:

1. Stop the Apache Tomcat service using a command similar to the following:

```
sudo /etc/init.d/tomcat<version number> stop
```

2. Change to the JDK `/bin` directory using a command similar to the following::

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

3. Generate a certificate for Tomcat with the `keytool` utility using 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.

4. Change to the Tomcat `etc` directory using a command similar to the following:

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

5. Verify the creation of the `keystore` file using 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 the connection link between DivePort and NetDiver clients and Tomcat, you must enable the HTTPS connector. The following procedure describes how to enable the HTTPS connector by editing the `server.xml` file.

Complete the following steps:

1. Check the status of Tomcat using the following command:

```
sudo /etc/init.d/tomcat7 status
```

2. If Tomcat is running, shut down Apache Tomcat by typing the following command:

```
sudo /etc/init.d/tomcat7 stop
```

3. Change to the Tomcat directory (`/etc/tomcat7`) using the following command:

```
cd /etc/tomcat7
```

4. Make a backup copy of the `server.xml` file called `serverorig.xml` using the following command:

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

5. Verify the file is copied correctly using the following command:

```
ls
```

6. View the permissions of the `server.xml` file using the following command:

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

The permissions display. If the permissions are `-rwxrwxrwx`, you can edit the file. If you do not have permissions:

- Modify the execute permission using the following command:

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

- Verify the permission change using the following command:

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

7. Open the `server.xml` file in a text editor using a command similar to the following:

```
gedit server.xml
```

8. Locate the section beginning with `Define a SSL HTTP/1.1 Connector on port 8443`.

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443
This connector uses the BIO implementation that requires the JSSE
style configuration. When using the APR/native implementation, the
OpenSSL style configuration is required as described in the APR/native
documentation -->
<!--
<Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" />
```

9. In the above `server.xml` section, make the following edits:
 - a. Remove the commented lines beginning with "This connector..." and ending with "documentation".

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

- `maxHttpHeaderSize="8192"`
- `minSpareThreads="25"`
- `maxSpareThreads="75"`
- `enableLookups="false"`
- `disableUploadTimeout="true"`
- `acceptCount="100"`
- `URIEncoding="UTF-8"`
- `keystorePass="tomcat"`
- `keystoreFile="/etc/tomcat7/keystore"`

After you add the attributes in the above list, the "Define a SSL HTTP/1.1 Connector on port 8443" section of the *server.xml* file should appear similar to the following:

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

<Connector port="8443" maxHttpHeaderSize="8192" maxThreads="150"
minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" URIEncoding="UTF-8"
scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
keystorePass="tomcat" keystoreFile="/etc/tomcat7/keystore" SSLEnabled="True"
/>
```

10. Remove the comment symbols, (`<!--` and `-->`) around the `<Connector port= ... />` section.
11. Save and close the *server.xml* file.
12. Restart Tomcat using the following command:

```
sudo /etc/init.d/tomcat7 start
```

NOTES:

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

It is possible that a user might want to enter a URL directly, which could contain non-ASCII characters. If those characters are high bit ISO-8859-1 characters, then a `URIEncoding="UTF-8"` would not be accurate. If a user intends to enter URLs that contain non-ASCII characters, they should set the `URIEncoding` on their Tomcat connector according to the encoding they intend to use.

Verifying the HTTPS Connection

You can verify the HTTPS installation for Tomcat by opening a browser window and connecting through the SSL 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 may encounter the following:

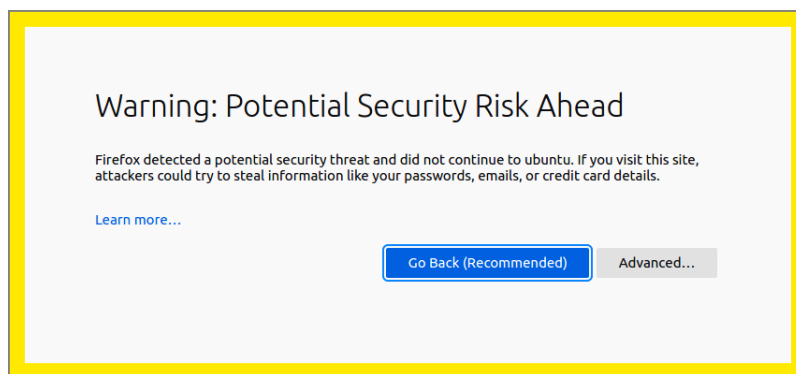
- A browser may display a warning message similar to "There is a problem with this website's security certificate".
- The IE browser asks you to click the **Continue to this website (not recommended)** warning message before opening the Tomcat home page on the secure port.
- Most browsers allow you to accept the self-signed certificate permanently.
- If you restart the browser and enter **https://<servername>:<portnumber>**, the default Tomcat home page should display again without a security warning.

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

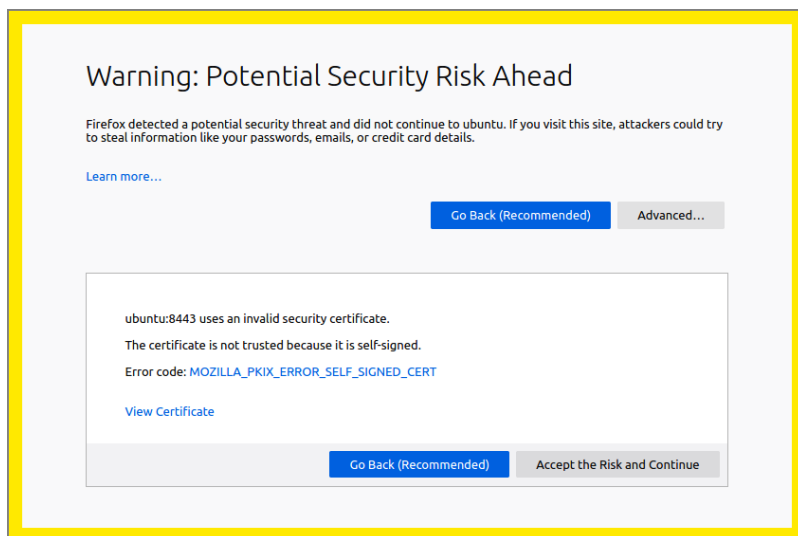
This procedure uses the Mozilla Firefox browser.

To verify the HTTPS connection, complete the following steps:

1. Open a browser window, and type the following URL:
https://ubuntu:8443
2. Press **Enter** to display the following security screen in the Firefox browser:



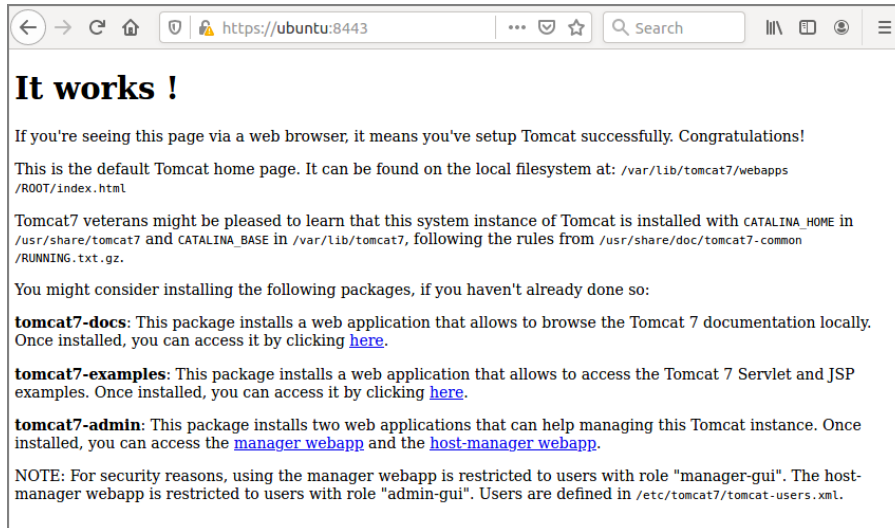
3. Click the **Advanced** button to view additional information.



4. Click **Accept the Risk and Continue** to enable the connection to the Tomcat web server.

The confirmation page displays.

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



Installing DivePort

After the successful installation of Apache Tomcat and DiveLine, you can begin the DivePort installation.

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 both pages and their portlet instances. DivePort typically resides on Apache Tomcat, a Web Application Server, which you can access using a web browser.

DivePort typically resides in the *web-tools.zip* which comes bundled with the Diver Platform Server package.

To install DivePort:

1. If running, stop the Tomcat web server using a command similar to the following:

```
sudo /etc/init.d/tomcat7 stop
```

NOTE: The `/etc/init.d` directory holds shell scripts that respond to `start`, `stop`, and `restart` commands to manage a particular service.

2. Navigate to the `/di/solution` directory using the following command:

```
cd /di/solution
```

3. Verify that the *web-tools.zip* file is present using the following command:

```
ls
```

4. Unzip *web-tools.zip* file using the following command:

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

```
jsmith@ubuntu:/di/solution$ sudo unzip web-tools.zip
Archive:  web-tools.zip
  inflating: bridge.zip
 extracting: dial-jar.zip
  inflating: diveport.zip
 extracting: netdiver.zip
```

5. View the unpackaged *web-tools.zip* file in the directory using the following command:

```
ls
```

```
jsmith@ubuntu:/di/solution$ ls
bridge.zip          diver-platform-server-7.0.56.2-linux64.zip  license
dial-jar.zip       libdataapi.jar                               netdiver.zip
di-diveline.tar.gz downloads                                     webapps
diveport.zip       exportinfo                                    webdata
diveport.zip       exportinfo                                    web-tools.zip
```

6. Unzip *diveport.zip* using the following command:

```
sudo unzip diveport.zip
```

7. Navigate to the `diveport` directory using the following command:

```
cd diveport
```

8. View the unpackaged `diveport.zip` file using the following command:

```
ls
```

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

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

9. Copy the `appdir` directory to the `/di/solution/webapps` directory and rename to assign a DivePort portal name (for example, **mydiveport**) using a command similar to the following:

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

10. Copy the `datadir` directory to the `/di/solution/webdata` directory and rename it to the same DivePort portal name (for example, **mydiveport**), using a command similar to the following::

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

11. Verify that the files were renamed and moved using the following commands:

- `ls`

NOTE: Only the `context-file-template.xml` file remains in the `/di/solution/diveport` directory.

- `ls /di/solution/webapps`
- `ls /di/solution/webdata`

12. Navigate to the `/etc/init.d` directory using the following command:

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

13. Determine the IP address of your Linux machine using the following command:

```
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`) displayed.
For example, 192.168.179.140 is the IP address displayed in the above 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/solution/diveport` directory using the following command:

```
cd /di/solution/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`) using a command similar to the following:

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

- c. Check the permissions of the `<DivePort name>.xml` file using a command similar to the following:

```
ls -l mydiveport.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. Modify the execute permission using the following command:

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

- b. Verify the permission change using the following command:

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

The permissions display as `-rwxrwxrwx`.

- d. Open the `<DivePort name>.xml` file with a text editor, such as **gedit**, using a command similar to the following:

```
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 DL CGI DivePort URL Here"/>
<Parameter name="diveline.web-auth-finish-url" value="Enter Logoff URL Here"/>
-->
<!-- If you need to permit HTTP connections:
<Parameter name="require-confidentiality" value="false" />
-->
</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/solution/webapps/mydiveport/diveport.war`
 - "Enter DivePort Webdata Directory Here" – The path to the webdata directory (`dataroot`)
For example:
`/di/solution/webdata/mydiveport`
 - "Enter DivePort WebApp Directory Here" – The path to the webapps directory (`approot`)
For example:
`/di/solution/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 36](#).
For example:
`admin`

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

For example:

```
<Context
docBase="/di/solution/webapps/mydiveport/diveport.war"
unpackWAR="false"
sessionCookiePathUsesTrailingSlash="false">
  <Parameter name="dataroot"
value="/di/solution/webdata/mydiveport" />
  <Parameter name="approot"
value="/di/solution/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 DL CGI 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>
```

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

- g. Save your changes and close the file.

To suppress <diverport name> in the URL:

- a. Navigate to the /di/solution/diveport directory using the following command:

```
cd /di/solution/diveport
```

- b. Create a copy of the *context-file-template.xml* file and rename it *ROOT.xml* using the following command:

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

- c. Open the *ROOT.xml* file with a text editor, such as **gedit**, using a command similar to the following:

```
gedit ROOT.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 DL CGI DivePort URL Here"/>
<Parameter name="diveline.web-auth-finish-url" value="Enter Logoff URL Here"/>
-->
<!-- If you need to permit HTTP connections:
<Parameter name="require-confidentiality" value="false" />
-->
</Context>

```

d. 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/solution/webapps/mydiveport/diveport.war
```

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

For example:

```
/di/solution/webdata/mydiveport
```

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

For example:

```
/di/solution/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 36](#).

For example:

```
admin
```

- node-id parameter with a value of Servername (/) (this parameter suppresses <diveport name> in the URL)

For example:


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

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

For example:

```
<Context
docBase="/di/solution/webapps/mydiveport/diveport.war"
unpackWAR="false"
sessionCookiePathUsesTrailingSlash="false">
  <Parameter name="dataroot"
value="/di/solution/webdata/mydiveport" />
  <Parameter name="approot"
value="/di/solution/webapps/mydiveport" />
  <Parameter name="diveline.server" value="ubuntu:2131"
/>
  <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>
```

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

- f. 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 using a command similar to the following:

```
sudo mv <file name>.xml
/etc/tomcat7/Catalina/localhost
```

17. Navigate to the `/etc` directory using the following command:

```
cd /etc
```

18. Change the ownership for the `tomcat<version>` directory to the Tomcat user, identified in Step 8 of [Installing Apache Tomcat on page 51](#), using a command similar to the following:

```
sudo chown -R tomcat7 ./tomcat7
```

19. Change to the directory holding the *atlcfg.cfg* file using the following command:

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

20. Check the permissions of the *atlcfg.cfg* file using the following command:

```
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. Modify the execute permission using the following command:

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

- b. Verify the permission change using the following command:

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

The permissions display as `-rwxrwxrwx`.

21. Open the file with a text editor, such as **gedit**, using a command similar to the following:

```
gedit atlcfg.cfg
```

22. Insert the `gateway_ips` attribute with IP address information in the `ACFG` object.

```
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 the lines ending with "true".

24. Save and close the file.
25. Start Tomcat using the following command:

```
sudo /etc/init.d/tomcat7 start
```

NOTE: The server IP address can change when you restart the server. The server IP address used in this documentation may change in different topics due to restarting the test server.

Verifying the DivePort Installation

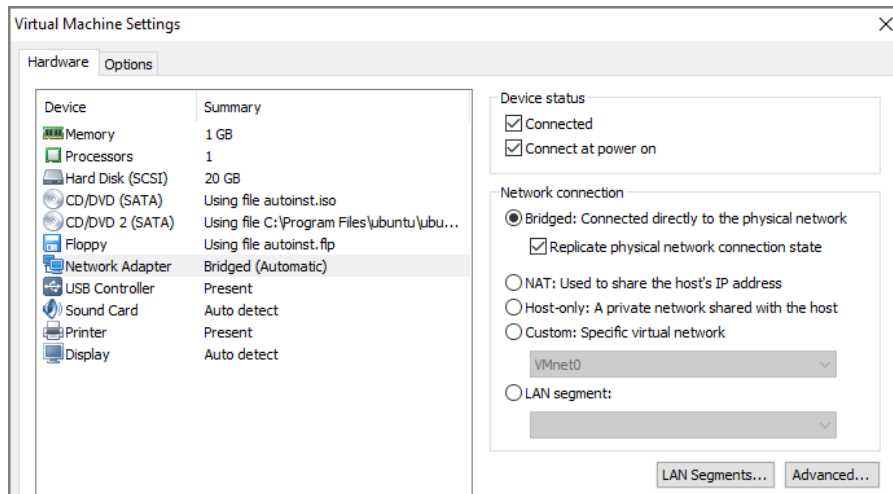
After you have downloaded, installed and configured DivePort, you can verify that it is working by opening a web browser and entering a URL with the following syntax:

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

For example:

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

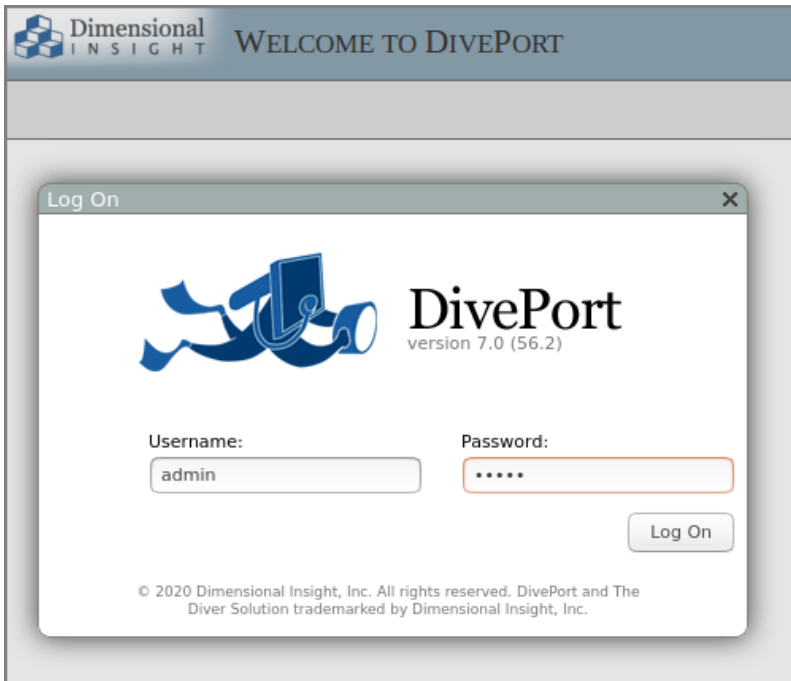
NOTE: If the server name does not work, try entering the IP address of the DiveLine server. If you have problems connecting to DivePort, check your logs and the configuration changes made to the *mydiveport.xml* and *atcfg.cfg* files. The example URL reflects changes made in the [Installing DivePort](#) topic. Additionally, if the Linux server is running inside a VM, you need to 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:



In the Network connection section, enable the following options:

- Bridged: Connected directly to the physical network
- Replicate physical network connection state

If you have successfully installed DivePort, the **Welcome to DivePort** page opens.



NOTE: If you have not previously logged on to the Linux server with a DI client (and you installed a self-signed certificate), the client (for example, DivePort) displays a **Verify Certificate** dialog box similar to the following:

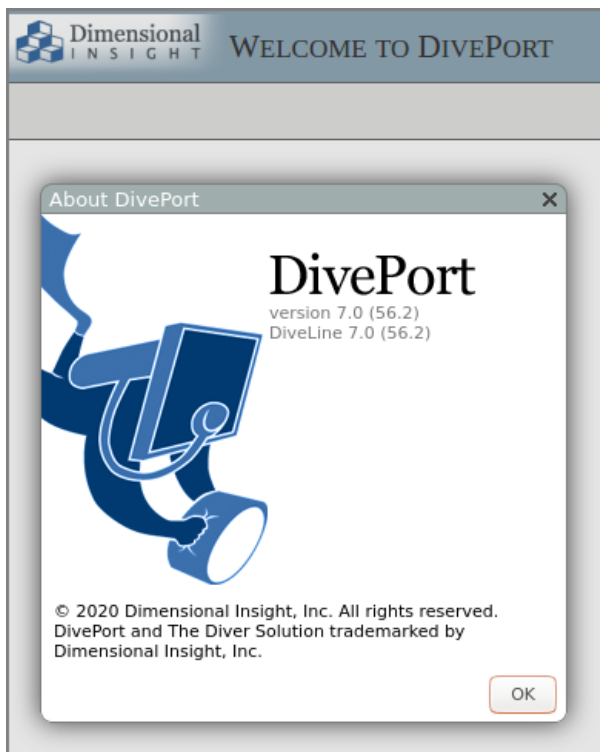


Click **Accept** to trust the certificate now and for all future logons.

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

Once connected and logged in to DivePort, click **HELP > About** to open the **About DivePort** dialog box listing the current version number for both DiveLine and DivePort.

Click **OK** to close the dialog box.



Click **HELP** > **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 the *DivePort User Help*.

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. You can install NetDiver after the installations of Apache Tomcat and DiveLine.

NOTE: The instructions in this topic use a different server IP address than in the [Installing DivePort](#) topic.

To install NetDiver:

1. If running, stop the Tomcat web server using a command similar to the following:

```
sudo /etc/init.d/tomcat7 stop
```

2. Navigate to the `/di/solution` directory using the following command:

```
cd /di/solution
```

3. Unzip the *netdiver.zip* file using the following command:

```
sudo unzip netdiver.zip
```

4. Navigate to the `netdiver` directory using the following command:

```
cd netdiver
```

5. View the unpackaged *netdiver.zip* file using the following command:

```
ls -l
```

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

- `/appdir`
 - `/datadir`
 - *context-file-template.xml*
6. Copy the `appdir` directory to the `/di/solution/webapps` directory and rename it to assign a NetDiver portal name (for example, **mynetdiver**) using a command similar to the following::

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

7. Copy the `datadir` directory to the `/di/solution/webdata` directory and rename it to the same NetDiver portal name (for example, **mynetdiver**) using a command similar to the following::

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

8. Navigate to the `/di/solution/netdiver` directory using the following command:

```
cd /di/solution/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*) using a command similar to the following:

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

10. Check the permissions of the *mynetdiver.xml* file using the following command:

```
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. Modify the execute permission using the following command:

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

- b. Verify the permission change using the following command:

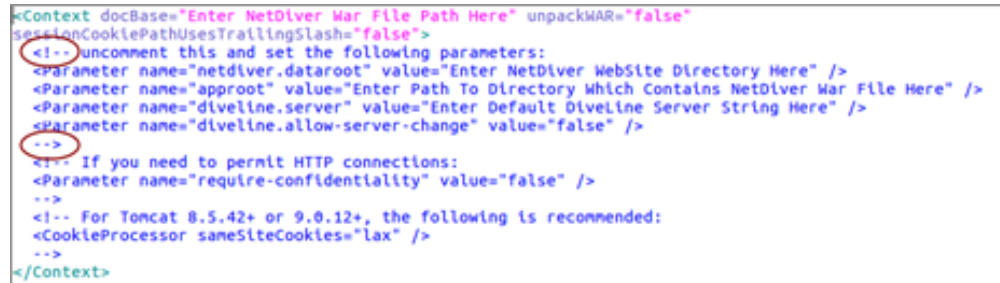
```
ls -l mynetdiver.xml
```

The permissions display as `-rwxrwxrwx`.

- Open the `<NetDiver name>.xml` file with a text editor, such as **gedit**, using a command similar to the following:

```
gedit mynetdiver.xml
```

The file opens in the text editor.



```
<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>
```

- 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/solution/webapps/mynetdiver/netdiver.war
```

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

For example:

```
/di/solution/webdata/mynetdiver
```

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

For example:

```
/di/solution/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/solution/webapps/mynetdiver/netdiver.war"
unpackWAR="false" sessionCookiePathUsesTrailingSlash="false">
  <Parameter name="netdiver.dataroot"
value="/di/solution/webdata/mynetdiver" />
  <Parameter name="approve"
value="/di/solution/webapps/mynetdiver" />
  <Parameter name="diveline.server" value="ubuntu:2131" />
  <Parameter name="diveline.allow-server-change" value="true" />
</Context>
```

(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 above parameter. If you permit HTTP connections, you are allowing unsecured communications with DiveLine.

14. Save and close the file.
15. Navigate to the `/di/solution/netdiver` directory using the following command:

```
cd /di/solution/netdiver
```

16. Copy the `<NetDiver name>.xml` file to the Tomcat directory using a command similar to the following:

```
sudo cp mynetdiver.xml
/etc/tomcat7/Catalina/localhost
```

17. Start Tomcat using the following command:

```
sudo /etc/init.d/tomcat7 start
```

Verifying the NetDiver Installation

After you have downloaded, installed and configured NetDiver, you can verify that it is working by opening a web browser and entering a URL with the following syntax:

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

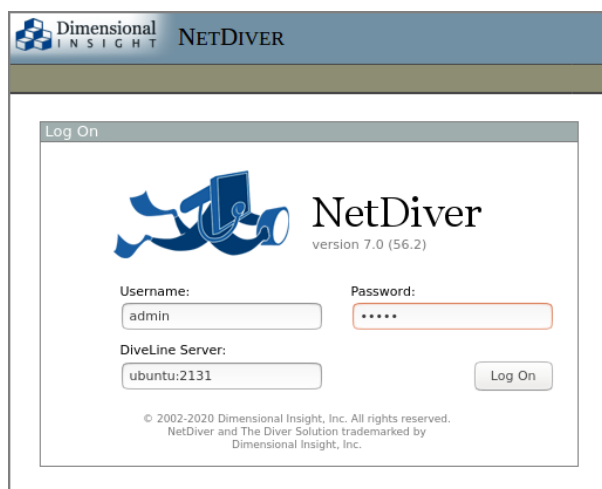
For example:

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

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 inside a VM, you need to verify that you have configured the network connection options correctly. Refer to [Verifying the DivePort Installation](#) for additional information.

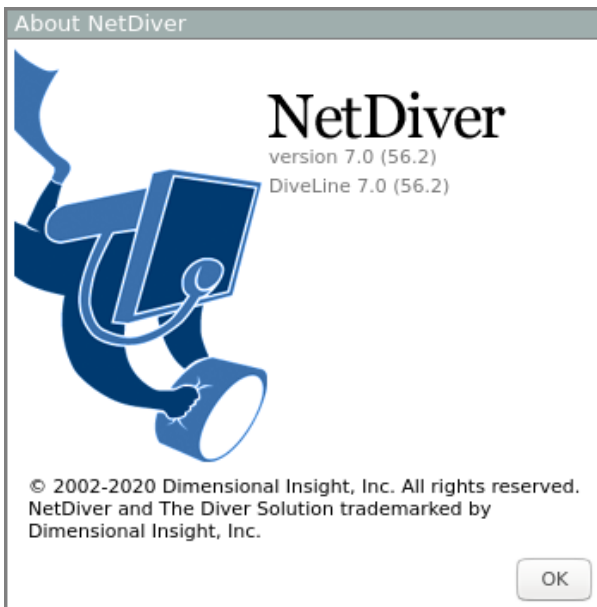
If you have successfully installed NetDiver, the NetDiver start page with a log on dialog box opens.



NOTE: If you have not previously logged on to the Linux server with a DI client (and you installed a self-signed certificate), the client may ask you to verify the self-signed certificate. Refer to [Verifying the DivePort Installation](#) for additional information.

Once connected and logged in to NetDiver, click **About** to open the **About NetDiver** dialog box listing the current version number for both DiveLine and NetDiver.

Diver Platform 7.0



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

Installing Diver Platform Developer

Downloading and Extracting the Developer Installation Package

This topic describes how to download and extract the Diver Platform Developer 7.0 Windows software package. See [Downloading the Server Installation Package on page 16](#) for information on how to locate DI installation files.

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

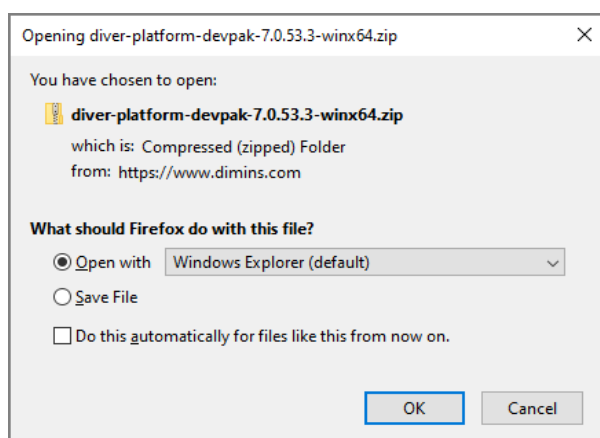
See [About the DI Directory Structure on page 10](#) to prepare the client machines.

Complete the following steps:

1. On the software and documents download page on DI-Download, locate the latest version of the Diver Platform Developer 7.0 Windows installation package, and click the version number.

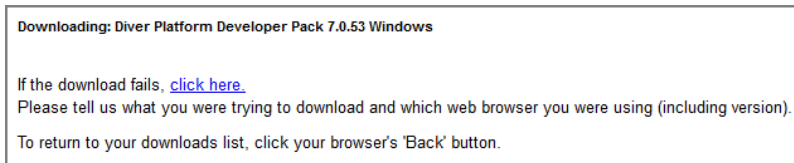
| | | | | |
|---|----------------------|---|--|---------------------------------|
| Diver Platform Developer Pack 7.1 Windows | 7.1.11 (382502KB) | Previous Point Releases | Not Available | Not Available |
| Diver Platform Developer Pack 7.1 Windows limited | Update not available | None Available | Not Available | Not Available |
| Diver Platform Developer Pack 7.0 Windows Unicode limited | 7.0.53 (423763KB) | Previous Point Releases | Release Notes (2405KB) | Manual (8409KB) |
| Diver Platform Developer Pack 7.0 Windows | 7.0.53 (423747KB) | Previous Point Releases | Release Notes (2405KB) | Manual (8409KB) |
| Diver Platform Developer Pack 7.0 Windows limited | Update not available | None Available | Release Notes (2405KB) | Manual (8409KB) |
| Diver Platform European Language Pack 7.1 Windows Unicode | 7.1.11 (2276070KB) | Previous Point Releases | Not Available | Not Available |

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

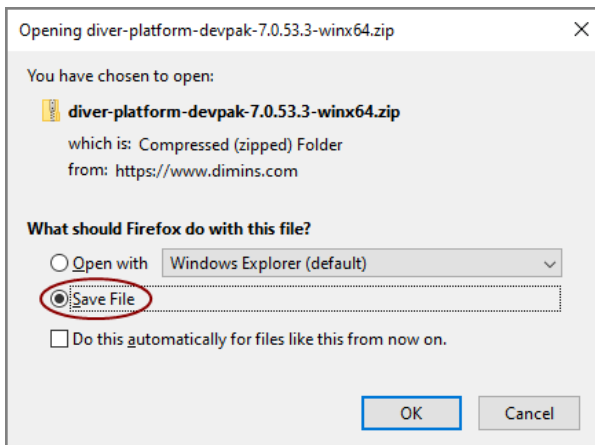


The **Downloading** page opens in the browser. If the **Opening** dialog does not open automatically, follow the instructions on the page.

Diver Platform 7.0



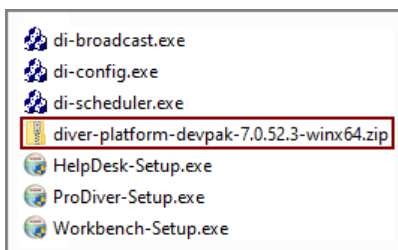
2. Select **Save File** and then click **OK**.



The Diver Platform Developer 7.0 software package is saved to the **Downloads** directory on your local machine.

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

The following executable files are extracted to the directory:



Installing ProDiver

ProDiver is the Diver Solution and Platform client working with the DiveLine server that allows users to view and analyze model and cBase data with a graphical user interface. Markers created in ProDiver are often used to build dashboards and presentations in DivePort.

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

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

To install ProDiver:

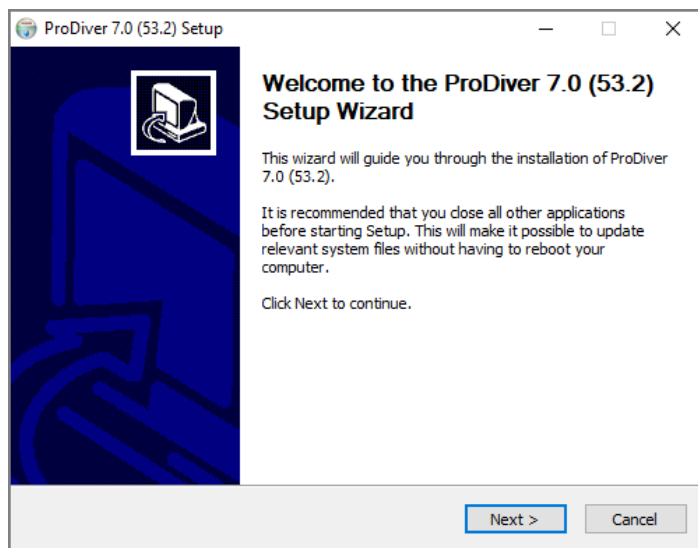
1. Navigate to the `DI\Solution\downloads` directory.
2. Double-click the **ProDiver-Setup.exe** file.

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.

3. Click **Yes**.

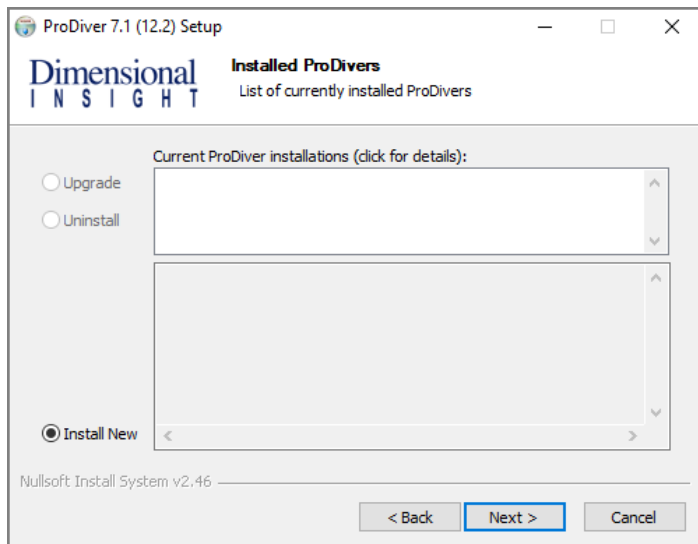
The **ProDiver <version number> Setup Wizard** dialog box opens.



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

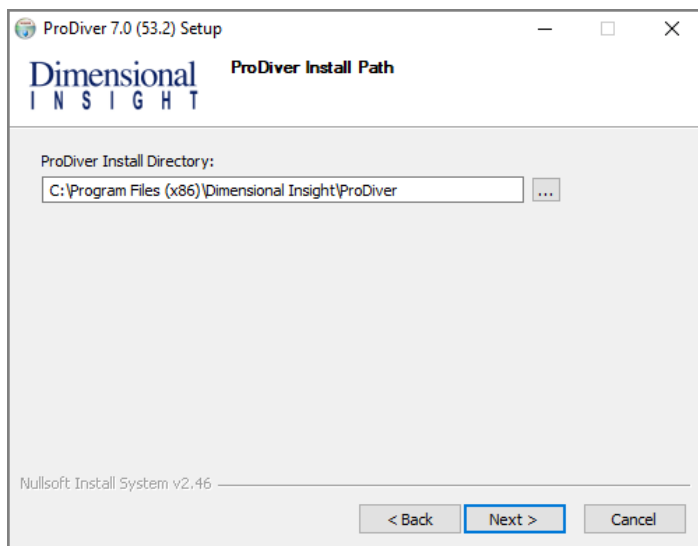
The **Installed ProDivers** page displays.

Diver Platform 7.0



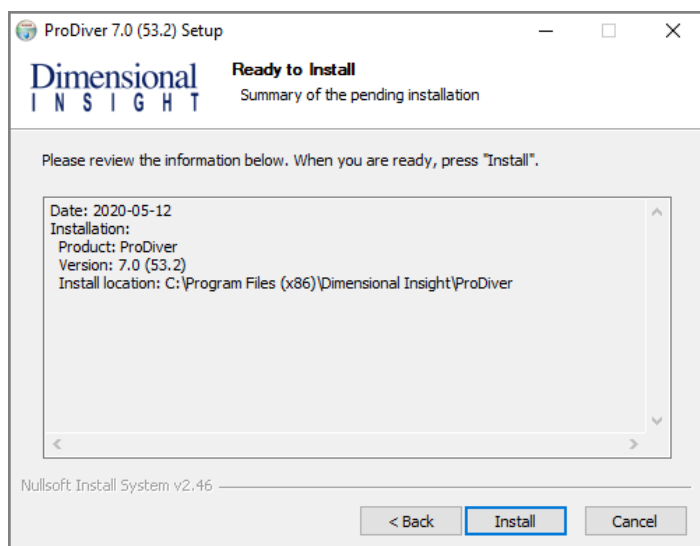
5. Select the **Install New** option. This page lists any existing ProDiver installations, which you can choose to **Upgrade** or **Uninstall**. If this is the first install, **Install New** is selected by default.
6. Click **Next**.

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

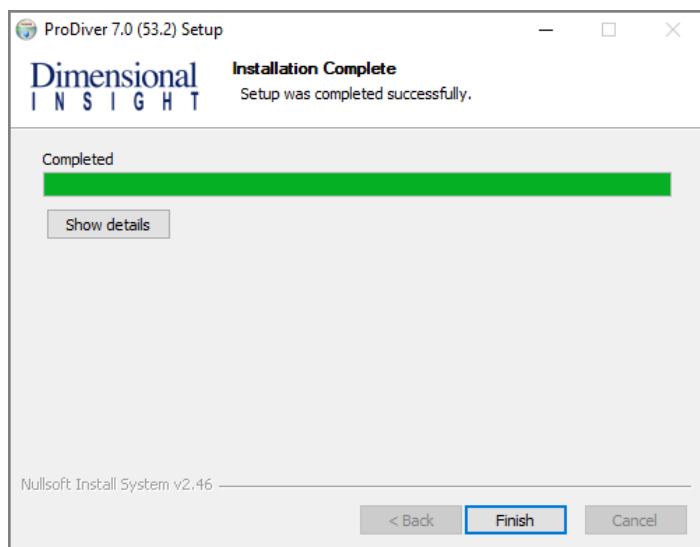


7. Click **Next**.

The **Ready to Install** page displays. It 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 for opening ProDiver from DivePort.

ProDiver Installation Silent Option

The ProDiver installer has a "silent option". This allows administrators to run the installer remotely on multiple workstations without interaction from the user. To run the installer in silent mode, use the `/S` option (case sensitive) on the command line. For example:

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

The following options can be used for more control.

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

NOTE: When output is sent to the console to display a list of errors encountered when running, you may be prompted to press **Enter** to continue. If the message does not indicate that the installer has completed, the process may still be

running in the background. If you need to perform other tasks, use a separate command window.

Examples:

A new install to the default path on a machine with no existing ProDiver:

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

That installation can be upgraded using the same command line:

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

A new install to a non-standard path:

```
ProDiver-Setup.exe /S /path=c:\di\solution70\executables\prodiver70
```

If it is the only ProDiver on that machine, you can upgrade just 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:

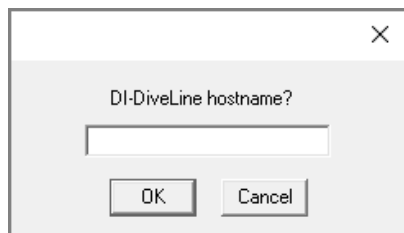
```
ProDiver-Setup.exe /S /mode=upgrade /installation=ProDiver-2019-0804-12-58-26
```

Verifying the ProDiver Installation

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

1. Open the Windows **Start** menu and type **ProDiver**.
2. Click the link to ProDiver that appears in the **Programs** list.

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



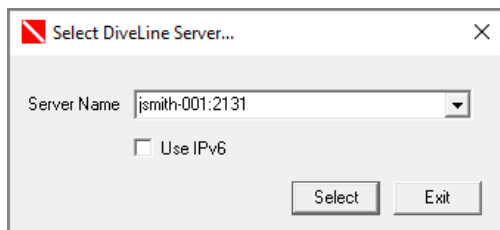
NOTE: If you used ProDiver to check the DiveLine installation, this is not the initial use of ProDiver. The **DiveLine Login** dialog box opens directly. Skip to [Step 6](#).

3. Enter **<server>** if you are using the default port number 2130, and **<server>:<port number>** if you are using another port number. For

example, **jsmith-001:2131**.

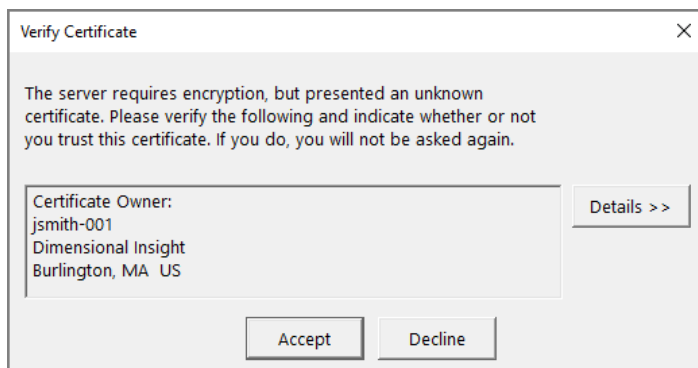
If the connection fails, the **Select DiveLine Server** dialog box opens. If successful, skip to [Step 6](#).

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



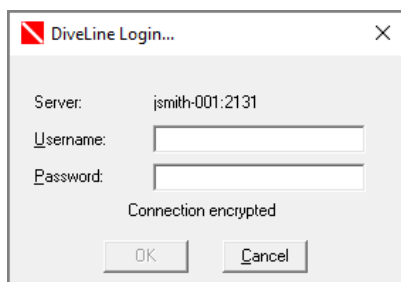
NOTE: The default port number is 2130. If another port is used, specify it in the server name using the format **<server name>:<port number>**.

The **Verify Certificate** window opens.

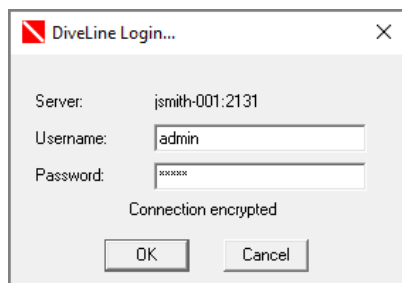


5. Review the certificate, and then click **Accept**. The window closes.


The **DiveLine Login** dialog box opens.



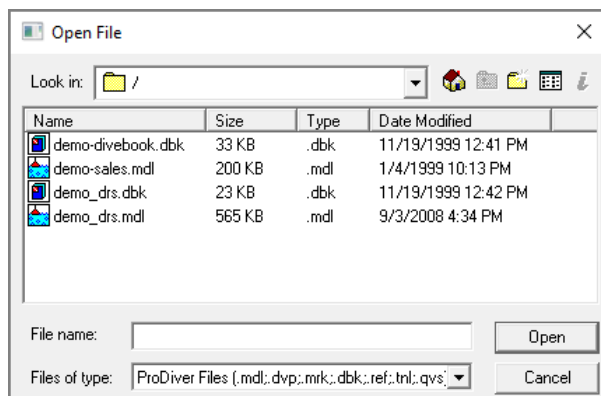
- On the **DiveLine Login** dialog box, enter the Username and Password and click **OK** to open ProDiver.



TIP: If you use a different server than the one that appears in the window, click **Cancel**, and return to [Step 4](#).

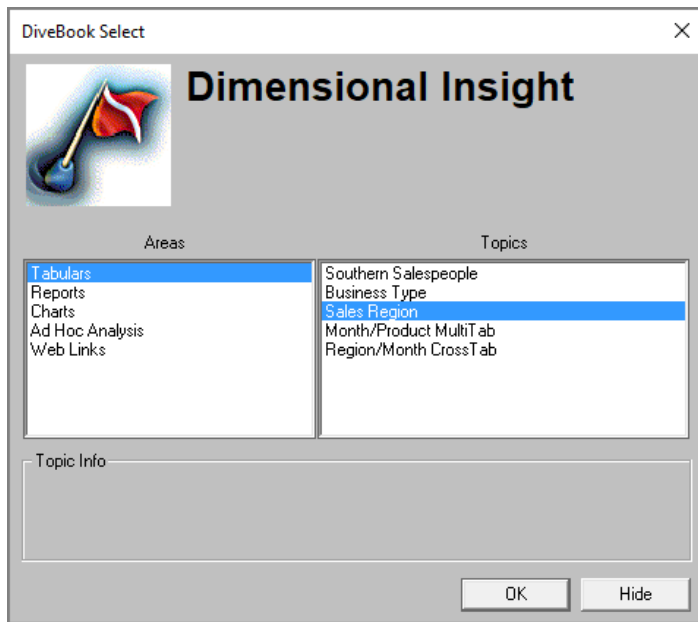
- Select **File > Open**, or click the Open icon, , to display the **Open File** dialog box with sample model and DiveBook files.

NOTE: Yours may differ and contain different files.



- Select a *dbk* file and click **Open**. For example, *demo-divebook.dbk*.
- Select an Area and a Topic, for example **Tabulars** and **Sales Region**, and click **OK** to open.

Diver Platform 7.0



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

ProDiver

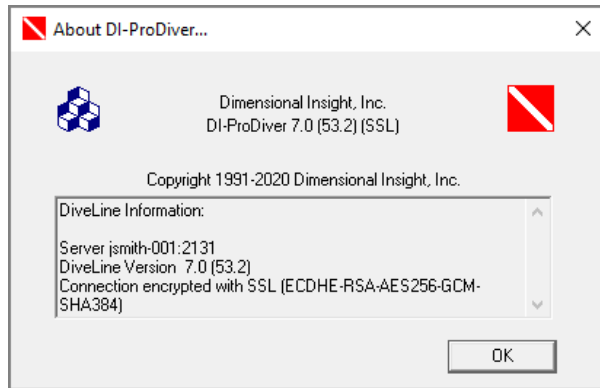
File Edit Organize Display Window Help

Sales Region [demo-sales.mdl-Dive A]

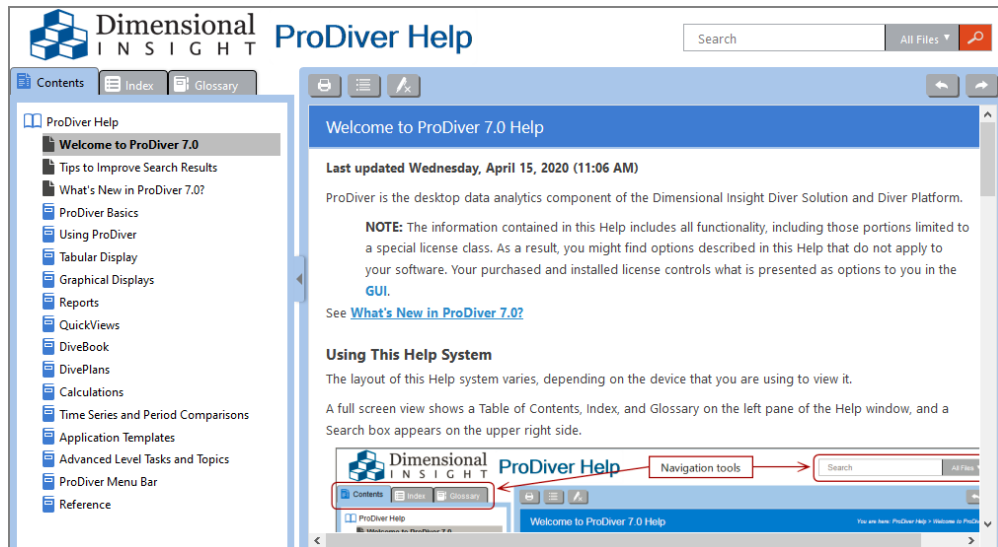
| Sales Region | Plan Units Total | Plan Dollars Total | Actual Units Total | Actual Dollars Total |
|---------------|------------------|--------------------|--------------------|----------------------|
| Totals | 2,092 | 8,630,600 | 2,526 | 9,624,200 |
| Far West | 247 | 1,031,100 | 336 | 1,320,700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

7 Rows (Totals-7) Logged in as admin (jsmith)

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



11. Click **Help** > **View Help** to view *ProDiver 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, easing the task of developing, testing, and managing multiple data projects.

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

Complete the following steps:

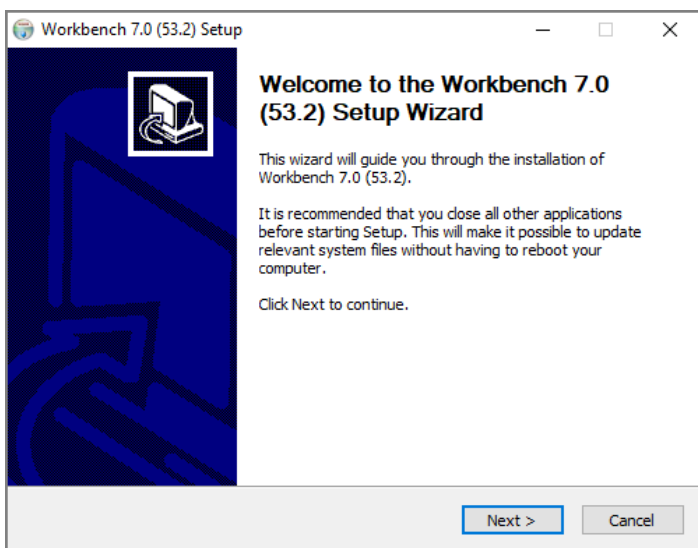
1. Navigate to the `DI\Solution\downloads` directory.
2. Double-click the **Workbench-Setup.exe** file.

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.

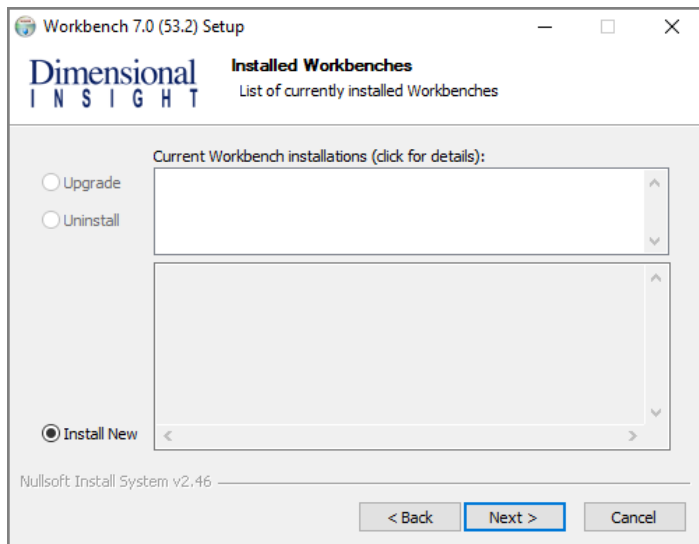
3. Click **Yes**.

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



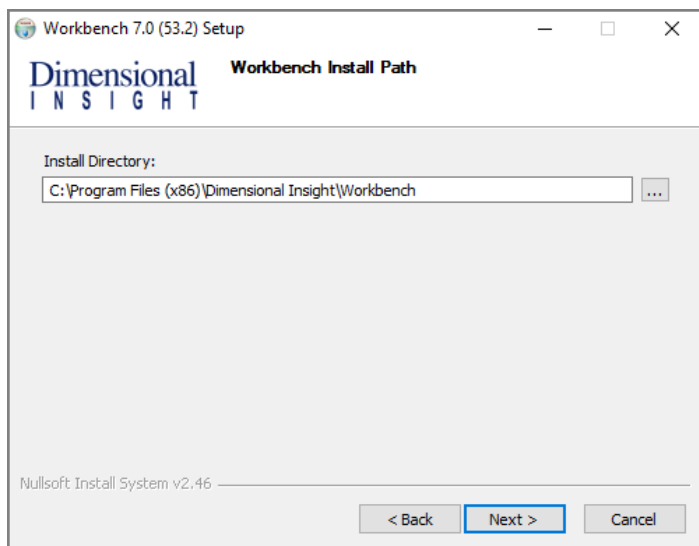
4. Review the setup instructions and click **Next**.

The **Installed Workbenches** page opens.



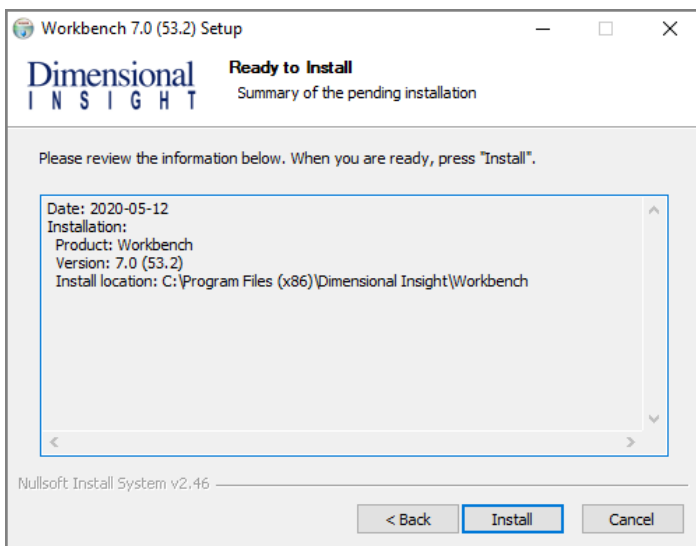
5. Select the **Install New** option. This page lists any existing Workbench installations, which you can choose to **Upgrade** or **Uninstall**. If this is the first install, **Install New** is selected by default.
6. Click **Next**.

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

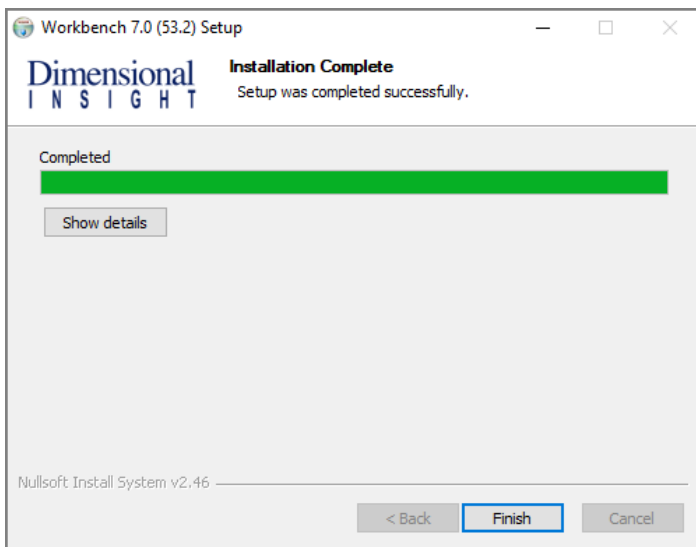


7. Click **Next**.

The **Ready to Install** page opens. It 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 installation wizard.

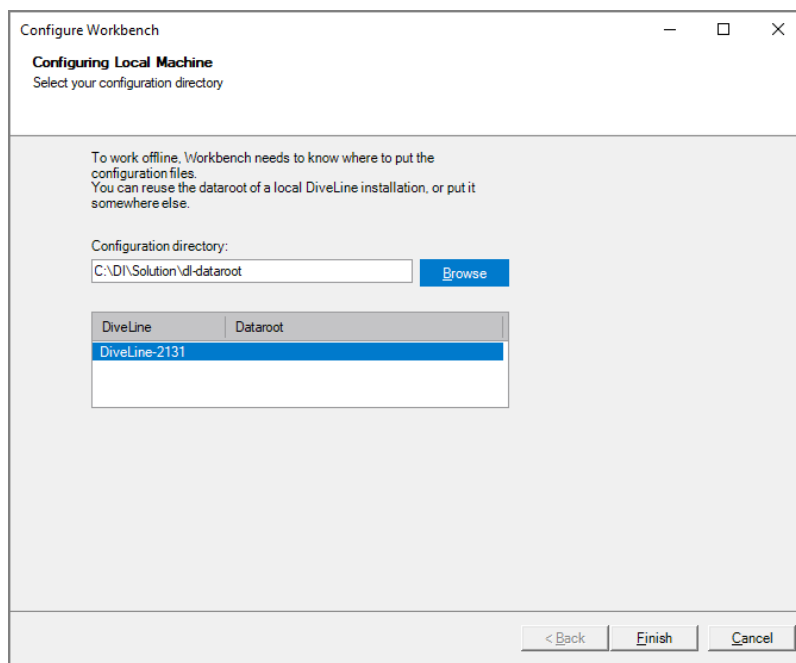
Verifying the Workbench Installation

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

1. Open the Windows **Start** menu and type **Workbench**.
2. Click the link to Workbench that appears in the **Programs** list.

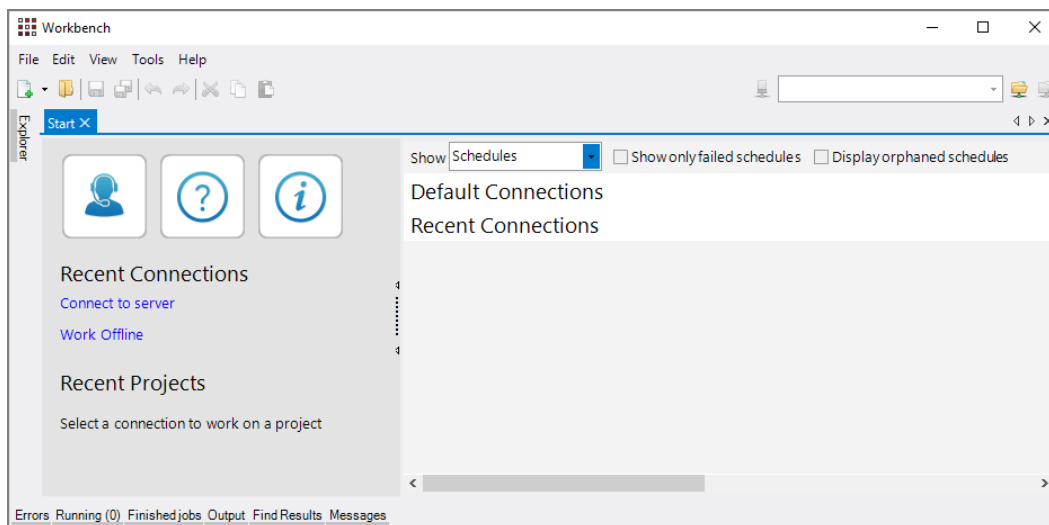
NOTE: When opening Workbench for the first time, it prompts you to select a directory for storing configuration files when you work offline. The default is the `C:\DI\Solution\dl-dataroot` directory for the local DiveLine installation.

- Click the **Browse** button to select a different Workbench configuration directory.
- Click **Finish** to complete this configuration step.

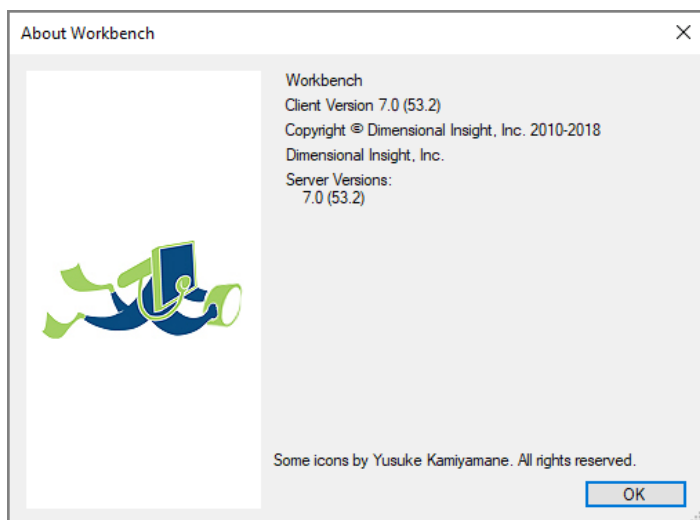


3. If successfully installed, the **Workbench** Start page opens.

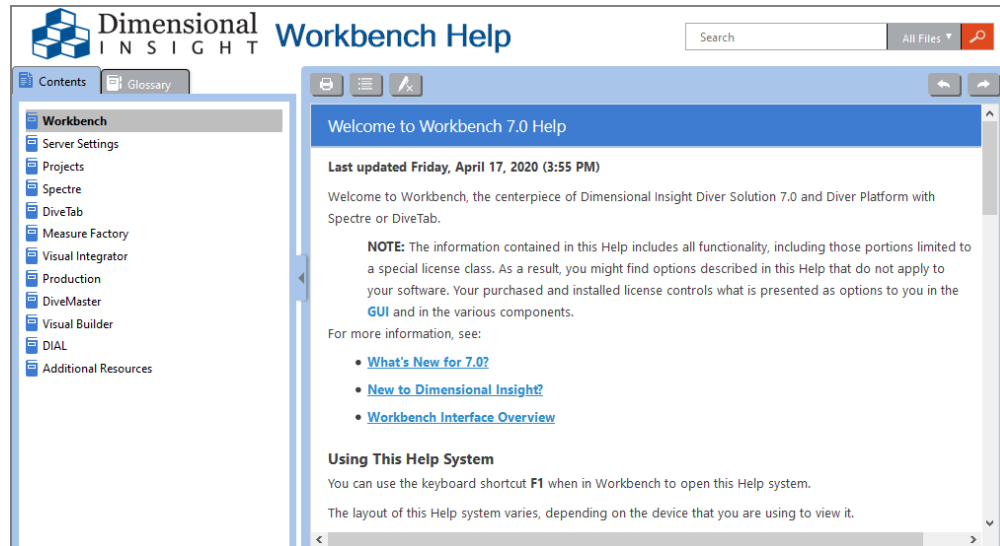
Diver Platform 7.0



4. Click **Help** > **About Workbench** to view the Workbench version number.



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



The *Workbench Help* opens in your default browser.