Dimensional INSIGHT

Diver Platform 7.1 Installation Guide for Linux

Diver Platform 7.1 Installation Guide for Linux

Revision: Doc-DPIL-71-031522-01

March, 2022

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 7.1 Overview

About This Installation Guide

This guide contains installation, configuration, and verification procedures to install the Diver Platform Server 7.1 package for Linux and Diver Platform Developer 7.1 package for Windows. The server package contains DiveLine and web clients DivePort, NetDiver, Bridge, and DIAL; the developer package contains the desktop clients Workbench, ProDiver, and Help Desk. All Dimensional Insight products in these packages are listed as follows:

- **Diver Platform**—The Dimensional Insight software suite that contains Diver 7.1 software, including Workbench and Spectre. User categories are: Developer, ProDiver, DivePort, and DiveTab.
- **Diver Solution**—The Dimensional Insight software suite that contains Diver 7.1 software, including Workbench. User types are tiered: Developer, Advanced, General, and Casual.
- **DiveLine**—The server component of the Diver Platform and Diver Solution. DiveLine authenticates users and controls access to data through Diver clients such as Workbench, ProDiver, DivePort, and DiveTab.
- **Spectre**—The data analysis software in the Diver Platform. Spectre processes data from a database or file to build a column-oriented database (cBase) that caches efficiently on both the server and client device. Spectre is integrated with DiveLine.
- **Workbench**—An integrated development environment to develop, test, and manage projects associated with a Diver application.
- **ProDiver**—The desktop analytics client of the Diver Platform and Diver Solution.
- **NetDiver**—The zero-footprint web-based analytics client that provides ad hoc reporting.
- **DivePort**—The client used to build and display portals that present your Diver data and any other content you need to share over the web.
- **Help Desk**—A desktop component that provides access to user maintenance for the DI client-server applications on the DiveLine server.
- **DiveTab**—The client that provides mobile users access to unstructured content and structured data. It uses guided data navigation and one-touch access on an iPad, PC, or phone. DiveTab is distributed separately.

- **Bridge**—A web application based on DivePort technology that you can use to navigate your DI applications from one central place.

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

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

- North America: 920-436-8299 or **support@dimins.com**
- United States: **https://www.dimins.com/dimensional-insight-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 extract, transform, and load (ETL) process involving the creation of up-to-date cBase and model files on a regular, usually nightly, schedule

Roles are independent of machines or engines and more than one role can be performed in the same environment. For example, if the people responsible for content development are also responsible for testing and validation, you can combine the Development and Test roles in the same environment. However, Test and Development environments should be isolated from the Production environment to prevent untested content from reaching users.

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

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

About Installing DI Software on a Linux Platform

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

This guide provides general instructions, guidelines, and examples about how to install the Diver Platform 7.1 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 that your Linux machine supports before installation.

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

- **DiveLine** – The server component of the Diver Platform and Diver Solution. DiveLine authenticates users and controls access to data through Diver clients such as Workbench, ProDiver, DivePort and DiveTab.
- **DivePort** – The client used to build and display portals that present your Diver data and any other content you need to share over the web
- **NetDiver** – The zero-footprint web-based analytics client of the Diver Platform. NetDiver provides ad hoc reporting and analytics tools in a web browser. NetDiver requires a connection to the DiveLine server software to access data.

It is important to note that the licenses for using DI software reside on the server. In a Linux environment, you can install Diver Platform Server 7.1 software on a Linux server while all Windows-based clients install on Windows laptops. To install DI Windows clients, such as ProDiver and Workbench, see Installing Diver Platform Developer on page 79.

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

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

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

- Build the DI directory structure and download the third-party and DI software to the DI downloads directory.
- Set the permissions on the DI directories. (The instructions in this guide identify where you might need to update the permissions on a directory or file.)

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

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

NOTES:

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

About Diver Platform Server 7.1

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

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

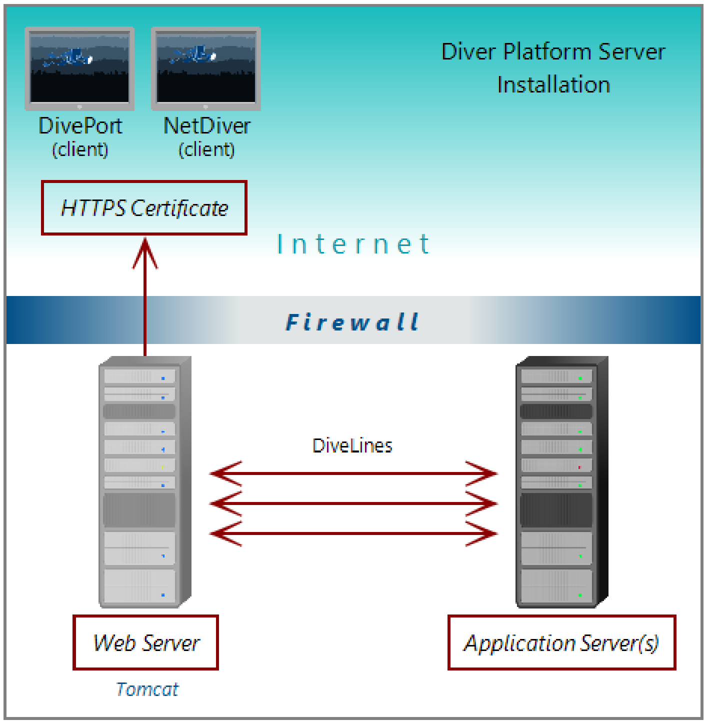
Environment	Port Number
Production	2130
Test	2131

Environment	Port Number
Development	2132
Build	2135
Bridge	3330

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

Environment	Port Number
Production	2130
Development/Test	2131

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



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

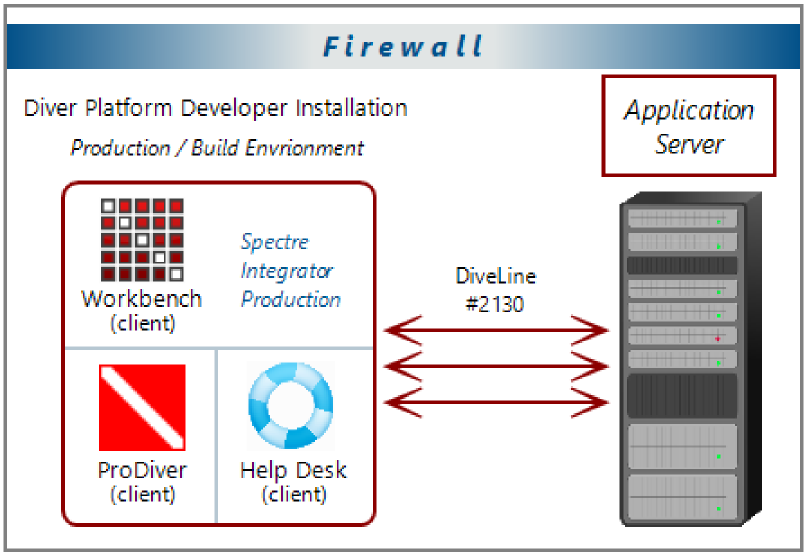
About Diver Platform Developer 7.1

The Diver Platform Developer 7.1 package includes the following executable files:

- **di-broadcast.exe**—A DiveLine client that delivers data to selected users through email. Deliveries can be scheduled on an episodic or periodic basis, or triggered by a specific event.
- **di-config.exe**—A DiveLine subcomponent that allows an administrator to configure DiveLine options by using a Windows user interface. Included to ease transition from version 6.x to 7.1. In 7.1, DI-Config functionality is part of the Workbench Server Settings.
- **di-scheduler.exe**—A DiveLine subcomponent that allows administrators to schedule jobs by using a Windows user interface. Included to ease transition from version 6.x to 7.1. DI-Scheduler functionality is integrated into Workbench.
- **HelpDesk-Setup.exe**—Installation software for the desktop component of the Diver Platform. Help Desk provides access to user maintenance for client-server applications on DiveLine. It requires a separate license.
- **ProDiver-Setup.exe**—Installation software for the desktop analytics client of the Diver Platform. ProDiver is the client in a client–server architecture, which means it requires a connection to a DiveLine server to access data.
- **Workbench-Setup.exe**—Installation software for the integrated visual development environment to develop, test, and manage projects associated with Diver Platform software.

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

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



Software Requirements

Before you install and operate Diver Platform 7.1 software, ensure that the following application server, web server, and desktop client requirements are met. In general, DI recommends that you use the latest versions.

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

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

Application and Web Server	Support Notes
Linux	Fully supported in the following configurations: Red Hat Enterprise Linux, CentOS, Debian, Ubuntu, SuSE. Latest version is recommended. 64-bit is required. The Mono component is required to run Diver Platform and Diver Solution on Linux systems. DI recommends that you download the latest release from **http://www.mono-project.com/download/**. The libodbc.so.1 library does not ship with the installer. It must be installed separately.
Microsoft Windows Server 2016 or later	Minimum version for 7.1. Fully supported. For more information about memory limits of specific versions, please refer to Microsoft's guidelines.

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

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

Web Browser	Support Notes
Internet Explorer 11 or later	Fully supported. Some dashboard features might not run in versions 10 and earlier.
Google Chrome, Microsoft Edge, Mozilla Firefox, Safari	Fully supported. Latest version recommended.

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

Java	Support Notes
OpenJDK 11	Latest version is recommended.
Java 10	Minimum version required. Some features might not function.

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

Apache Tomcat	Support Notes
Tomcat 9.0	Latest version is recommended.
Tomcat 8.5.0	Minimum version required for for 7.1. On Tomcat 8 and later, 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 by using the Dimensional Insight installers.
Tomcat 7.0	Tomcat 7.0 reached it's end-of-life as of March 2021, and no longer receives updates. DI recommends updating to Tomcat 9.0.

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

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

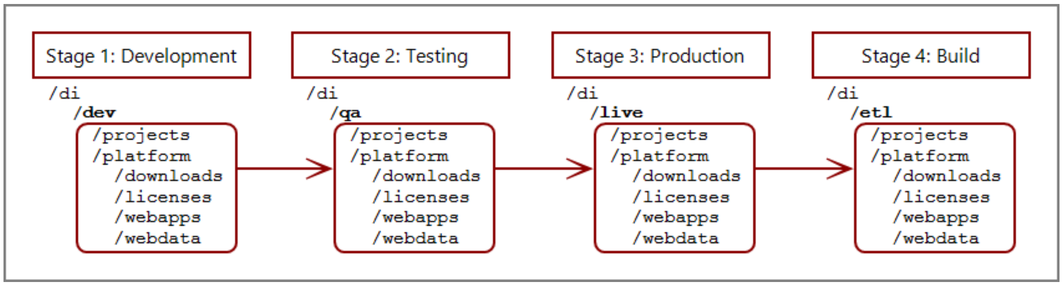
About the DI Directory Structure

Prior to downloading and installing DI Platform server and developer software for 7.1, DI recommends that you create the following directory structure on your machine:

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

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

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



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

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

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

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

Directory	Subdirectory	Description
/di/platform	/webapps	Program, configuration, and setup files for DivePort and NetDiver. This directory is created manually.
/di/platform	/webdata	Data and customization files for DivePort and NetDiver. This directory is created manually.

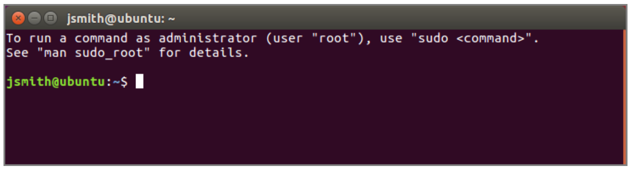
Building the DI Directory Structure

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

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

Complete the following steps:

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



```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

jsmith@ubuntu:~$
```

3. Go to the root directory.

```
cd /
```

4. Create the `di` directory.

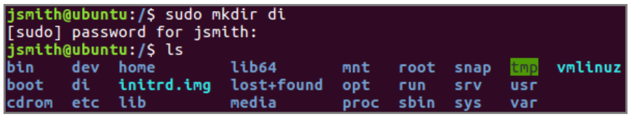
```
sudo mkdir di
```

NOTE: Enter the user password if prompted.

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

```
ls
```

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



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

6. Change to the `di` directory:

   ```
   cd di
   ```

7. Optionally, create a directory for each environment.

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

      ```
      sudo mkdir live
      ```

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

      ```
      ls
      ```

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

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

      ```
      cd live
      ```

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

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

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

9. Confirm that the directories were created successfully:

   ```
   ls
   ```

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

10. Navigate to the `platform` directory:

    ```
    cd platform
    ```

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

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

12. Confirm that the directories were created successfully.

```
ls
```

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

About Diver Platform and Solution 7.1 Licenses

Diver Platform 7.1 is the paid upgrade path for customers who want to use the Spectre engine, DiveTab, or Measure Factory. Diver Solution 7.1 is the free, standard software upgrade path for Diver Solution 7.0 customers on a maintenance plan. Users licenses differ depending on whether you use Diver Platform or Diver Solution.

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

Diver Platform Licenses

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

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

The user license types for Platform 7.1 are:

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

Diver Solution Licenses

Diver Solution 7.1 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 7.1 are:

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

What Is Named User Licensing?

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

About License Types

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

Perpetual Licenses

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

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

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

Trial Licenses

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

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

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

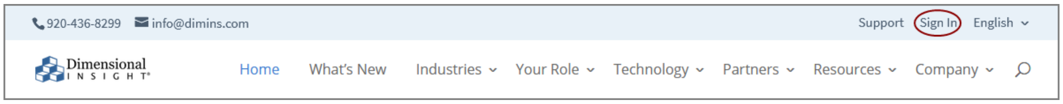
Installing Diver Platform Server

Downloading the Server Installation Package

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

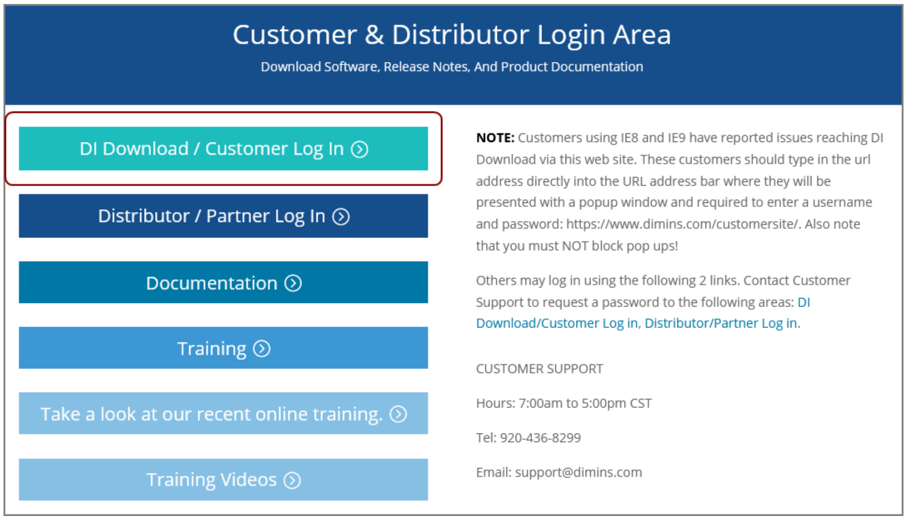
NOTE: Administrative privileges are required to install the software.

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



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

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


Customer & Distributor Login Area
Download Software, Release Notes, And Product Documentation
DI Download / Customer Log In
Distributor / Partner Log In
Documentation
Training
Take a look at our recent online training.
Training Videos

NOTE: Customers using IE8 and IE9 have reported issues reaching DI Download via this web site. These customers should type in the url address directly into the URL address bar where they will be presented with a popup window and required to enter a username and password: https://www.dimins.com/customersite/. Also note that you must NOT block pop ups!

Others may log in using the following 2 links. Contact Customer Support to request a password to the following areas: DI Download/Customer Log in, Distributor/Partner Log in.

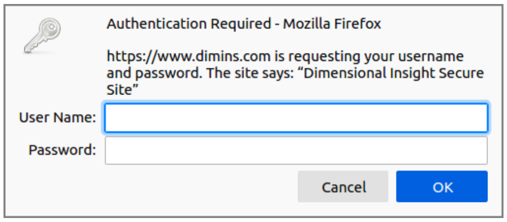
CUSTOMER SUPPORT

Hours: 7:00am to 5:00pm CST

Tel: 920-436-8299

Email: support@dimins.com

   The **Authentication Required** dialog box opens.



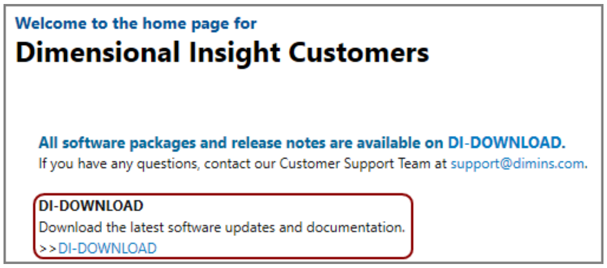
Authentication Required - Mozilla Firefox

https://www.dimins.com is requesting your username and password. The site says: “Dimensional Insight Secure Site”

4. Enter your **User Name** 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.

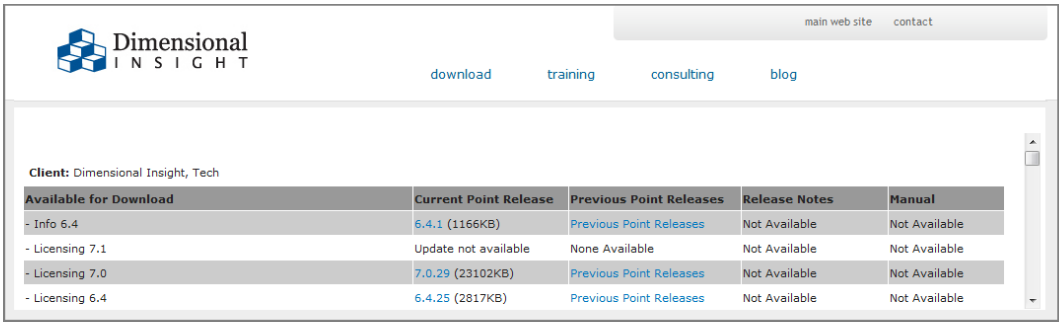
If you have any questions, contact our Customer Support Team at support@dimins.com.

DI-DOWNLOAD

Download the latest software updates and documentation.

>>DI-DOWNLOAD

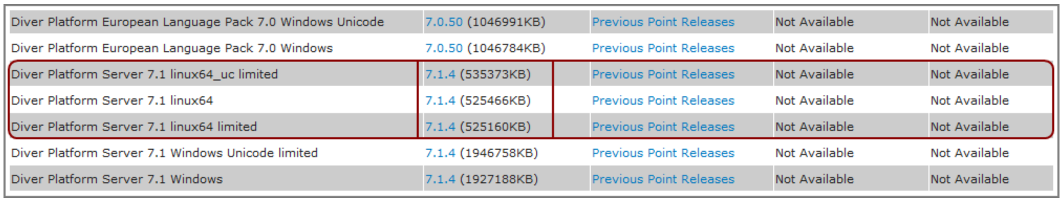
The software and documents download page opens.



Client: Dimensional Insight, Tech

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 7.1 software that you purchased, and click the blue version number.



Diver Platform European Language Pack 7.0 Windows Unicode	7.0.50 (1046991KB)	Previous Point Releases	Not Available	Not Available
Diver Platform European Language Pack 7.0 Windows	7.0.50 (1046784KB)	Previous Point Releases	Not Available	Not Available
Diver Platform Server 7.1 linux64_uc limited	7.1.4 (535373KB)	Previous Point Releases	Not Available	Not Available
Diver Platform Server 7.1 linux64	7.1.4 (525466KB)	Previous Point Releases	Not Available	Not Available
Diver Platform Server 7.1 linux64 limited	7.1.4 (525160KB)	Previous Point Releases	Not Available	Not Available
Diver Platform Server 7.1 Windows Unicode limited	7.1.4 (1946758KB)	Previous Point Releases	Not Available	Not Available
Diver Platform Server 7.1 Windows	7.1.4 (1927188KB)	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 box does not open automatically, follow the instructions on the page:

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

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

   NOTE: Most browsers enable you to configure the download location for files downloaded from the Internet. For example, if you are using the Firefox browser on Linux, you can choose **Edit** > **Preferences** and configure the download location.

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

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

Extracting the Server Installation Package

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

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

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

   ```
   ls
   ```

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

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

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

   ```
   cd ..
   ```

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

   ```
   ls
   ```

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

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

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

   ```
   ls
   ```

   Verify that the following files display:

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

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

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

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

   ```
   ls
   ```

   The following new directories now display:

   - `diveline`
   - `executables`

Obtaining a License for the DI Software

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

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

Using the exportinfo Utility to Obtain Machine Information

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

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

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

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

   ```
   ls
   ```

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

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

   ```
   ls -l exportinfo
   ```

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

   If you do not have permission to run the utility:

   a. Enable the execute permission.

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

   b. Verify that the permissions have changed.

      ```
      ls -l exportinfo
      ```

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

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

   ```
   sudo ./exportinfo
   ```

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

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

   - Accept the default file name—*di_minfo_<your machine's name>.info* (for example, *di_minfo_ubuntu.info*)—by pressing the **Enter** key.
   - Enter a name for the file, including the *info* extension, and press the **Enter** key. For example, `di_minfo_jsmith-ubuntu.info`.

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

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

   ```
   ls
   ```

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

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

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

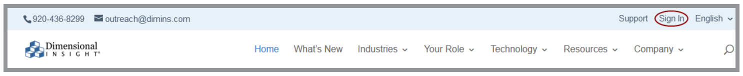
8. Go to the `/licenses` folder and confirm that the file was moved successfully by entering the following command:

   ```
   ls
   ```

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

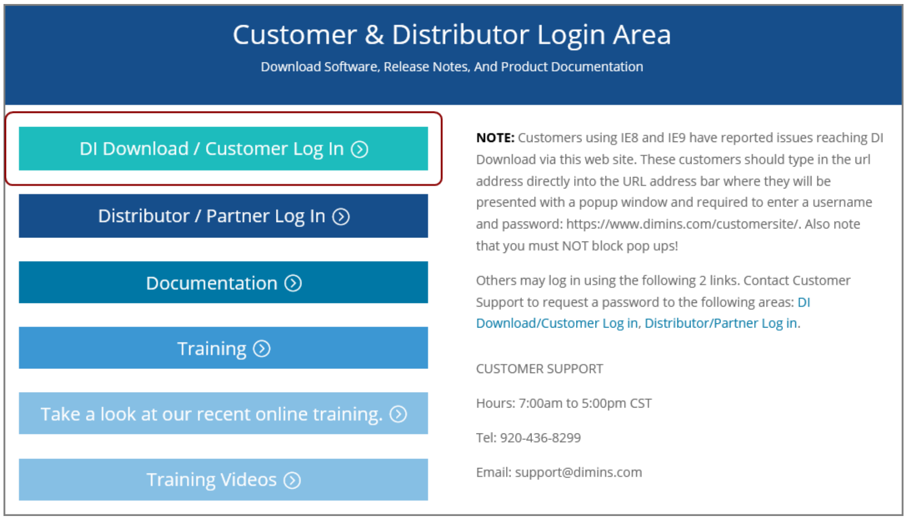
Obtaining the Licensing Package

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



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

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



Customer & Distributor Login Area

Download Software, Release Notes, And Product Documentation

DI Download / Customer Log In
Distributor / Partner Log In
Documentation
Training
Take a look at our recent online training.
Training Videos

NOTE: Customers using IE8 and IE9 have reported issues reaching DI Download via this web site. These customers should type in the url address directly into the URL address bar where they will be presented with a popup window and required to enter a username and password: https://www.dimins.com/customersite/. Also note that you must NOT block pop ups!

Others may log in using the following 2 links. Contact Customer Support to request a password to the following areas: DI Download/Customer Log in, Distributor/Partner Log in.

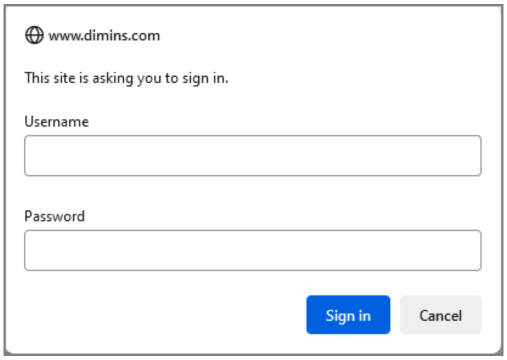
CUSTOMER SUPPORT

Hours: 7:00am to 5:00pm CST

Tel: 920-436-8299

Email: support@dimins.com

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



www.dimins.com

This site is asking you to sign in.

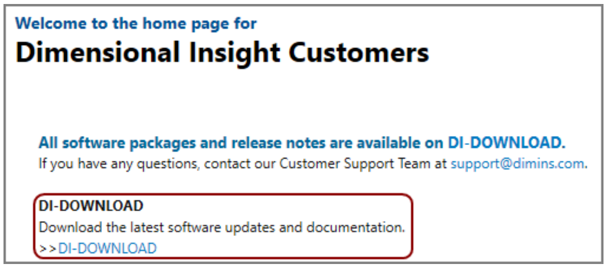
Username

Password

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.

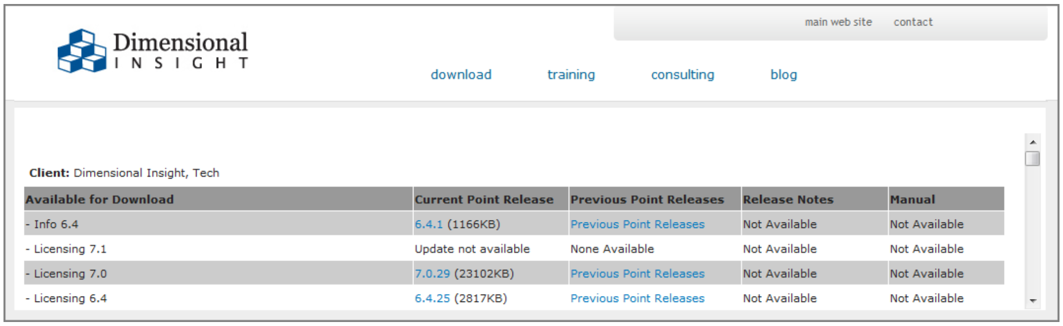
If you have any questions, contact our Customer Support Team at support@dimins.com.

DI-DOWNLOAD

Download the latest software updates and documentation.

>>DI-DOWNLOAD

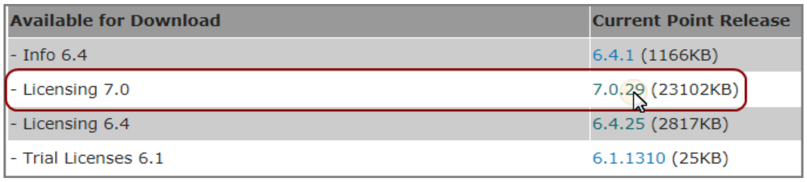
The software and documents download page opens.



Client: Dimensional Insight, Tech

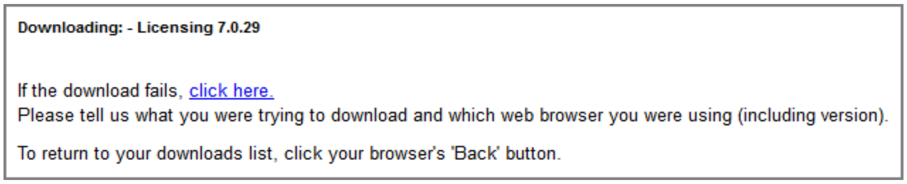
Available for Download	Current Point Release	Previous Point Releases	Release Notes	Manual
- Info 6.4	6.4.1 (1166KB)	Previous Point Releases	Not Available	Not Available
- Licensing 7.1	Update not available	None Available	Not Available	Not Available
- Licensing 7.0	7.0.29 (23102KB)	Previous Point Releases	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 **Downloading** page opens in the browser. If the **Opening** confirmation box does not open automatically, follow the instructions on the page:

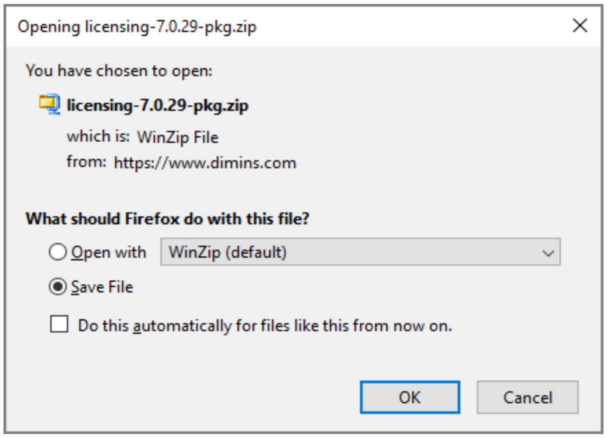


Downloading: - Licensing 7.0.29

If the download fails, click here.
Please tell us what you were trying to download and which web browser you were using (including version).

To return to your downloads list, click your browser's 'Back' button.

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



Opening licensing-7.0.29-pkg.zip

You have chosen to open:

licensing-7.0.29-pkg.zip

which is: WinZip File
from: https://www.dimins.com

What should Firefox do with this file?

○ Open with WinZip (default)

● Save File

□ Do this automatically for files like this from now on.

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

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. You use this option when you need to request a license for use on another machine (either Windows or Linux).

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

   NOTE: The *info* file is created in the section Using the exportinfo Utility to Obtain Machine Information on page 19.

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

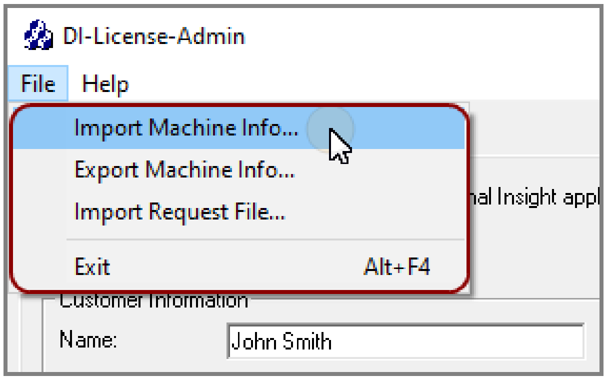
   The **User Account Control** confirmation box opens, asking you to confirm making changes to your device.

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

3. Click **Yes**.

   The DI-License-Admin utility starts.

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



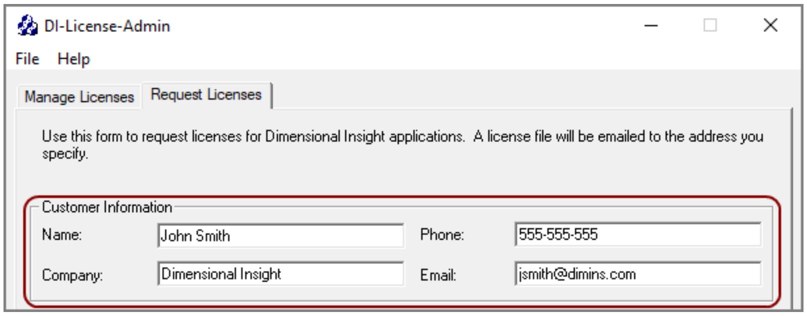
Name: John Smith

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

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

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

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



Use this form to request licenses for Dimensional Insight applications. A license file will be emailed to the address you specify.

Customer Information

Name:	John Smith	Phone:	555-555-555
Company:	Dimensional Insight	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 that you purchased. For example, if you purchased Diver Platform Server 7.1 for Linux, select **Diver Platform 7.1 BI – DiveLine <port>**.

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

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

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

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

   c. If you know the number of users of each type that you purchased access for, complete the remaining fields. Otherwise, Dimensional Insight Customer Support can find this information when they create your license.
   d. Click **OK**.

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

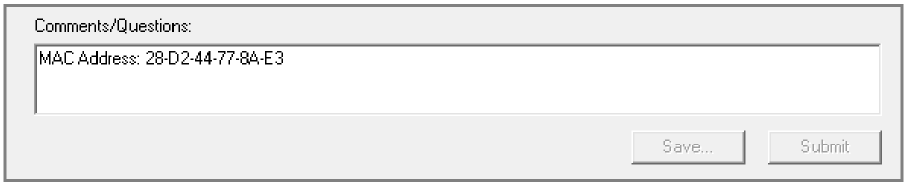
   e. Repeat Steps **a** through **d** to request a server-side license for each virtual environment on your machine.

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

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

   For example, if you purchased Diver Platform, select **Developer Package 7.1**.

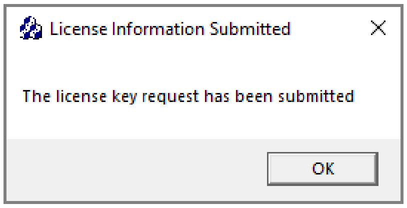
10. In the **Comments/Questions** box, specify any additional purchases, such as Input Tables, Measure Factory, or Help Desk, and include any comments or questions that you have. Dimensional Insight recommends that you also provide the media access control (MAC) address of the machine that you want to request the licenses for (the one that was used to create the machine information file). For example:


Comments/Questions:

MAC Address: 28-D2-44-77-8A-E3

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

11. Click **Submit** to open the **Submit License?** dialog box showing your selections.
12. Click **Yes** to submit the license request.
13. Click **OK** to acknowledge the submission.


License Information Submitted

The license key request has been submitted

14. Click **Save** to store the license request file.
15. If necessary, move the *request* file to the Linux server.
16. On the Linux server, move the *request* file to the `/di/platform/licenses` directory by entering the following command:

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

Using the register Utility to Install a License File

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

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

1. Copy the license *zip* file to the Linux server.
2. Copy the *zip* file to the `/di/platform/licenses` folder.

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

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

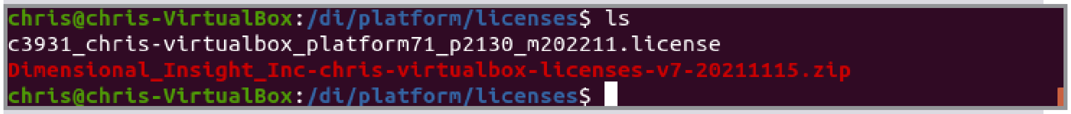
   ```
   cd /di/platform/licenses
   ```

4. Unzip the file.

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

5. Confirm that the *license* file is extracted

   ```
   ls
   ```

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

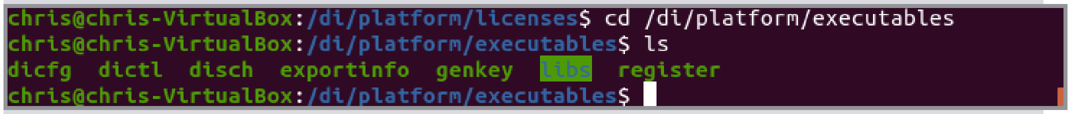
   TIP: Take note the name of the license file. You will use it later in this procedure.

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

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

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

   ```
   ls
   ```

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

8. View the permissions for the register utility.

   ```
   ls -l register
   ```

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

If you do not have permission to run the utility:

a. Enable the execute permission.

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

b. Verify that the permissions have changed.

```
ls -l register
```

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

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

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

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

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

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

```
ls
```

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

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

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

13. Confirm that the installation was successful.

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

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

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

15. Repeat this procedure for each environment.

Installing DiveLine

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

About Installing DiveLine

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

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

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

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

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

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

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

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

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

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

Installing and Configuring DiveLine

Prerequisite: Uncompress the *di-diveline.tar.gz* file, as shown in Extracting the Server Installation Package on page 18, so that the `/di/platform/diveline` directory contains the following files and subdirectories:

- **bin**—Directory containing executable files used by the server
- **cgi-bin**—Directory containing the executable file for Web Server authentication
- **docs**—Directory containing a quick reference list for dicfg
- **html**—Directory containing *html* and *dlk* template files as well as a README file used with Web Server authentication
- **install-files**—Directory containing files that are used when installing DiveLine, some files of which need to be copied to other directories
- **samples**—Directory containing two sample models and DiveBooks for testing DiveLine
- **ENCRYPTION**—The OpenSSL license file
- **INSTALL**—Installation notes for 7.1
- **install-di-diveline**—The installation *shell* script
- **README**—Directory contents and support email address

NOTE: Text is case-sensitive in Linux.

To install and configure DiveLine:

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

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

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

```
ls
```

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

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

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

   a. Enable the execute permission.

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

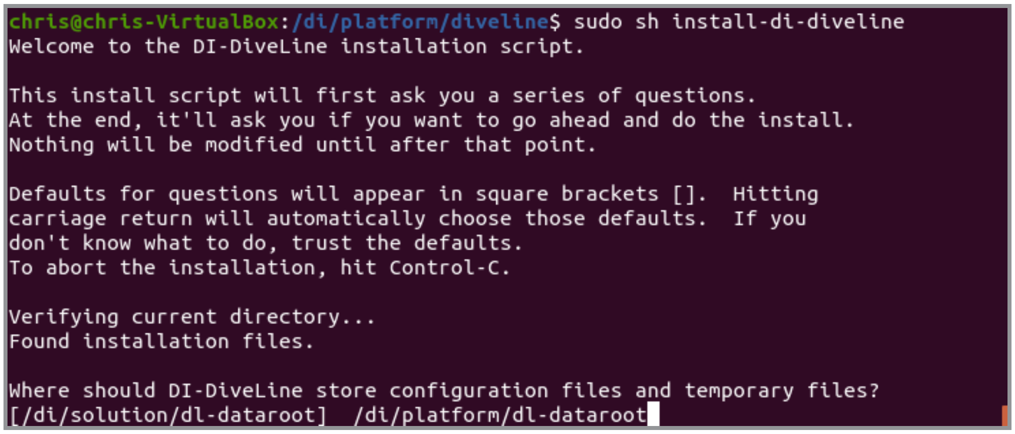
   b. Verify that the permissions have changed.

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

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

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

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



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

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

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

Verifying current directory...
Found installation files.

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

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

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

The questions are:

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

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

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

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

  The default security level is 2.

  There are three options to choose from:

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

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

  The default is `y`, or yes.

- `Go ahead and install? [y]`

  The default is `y`, or yes.

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

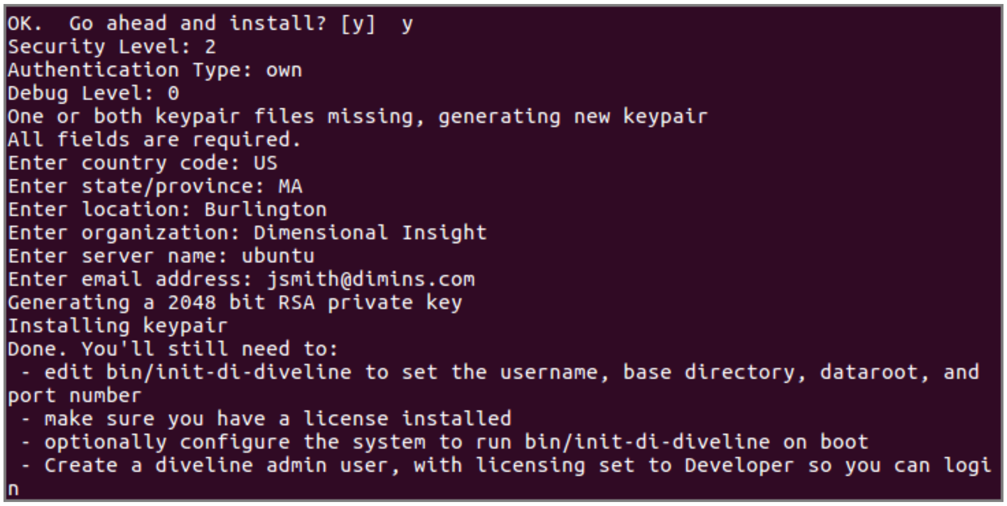
NOTE: A DI best practice is to create the private key and certificate files during the DiveLine installation.

For example:

- Country Code - **US**

  IMPORTANT: The country code must be two characters long.

- State/province - **MA**
- Location - **Burlington**
- Enter organization - **Dimensional Insight**
- Server name - **ubuntu**
- Email address - **jsmith@dimins.com**



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

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

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

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

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

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

```
ls -l
```

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

   a. Enable the execute permission.

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

   b. Verify that the permissions have changed.

   ```
   ls -l config
   ```

   The permissions display as `drwxrwxrwx`.

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

```
ls
```

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

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

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

   ```
   ls
   ```

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

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

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

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

    a. Enable the execute permission.

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

    b. Verify that the permissions have changed.

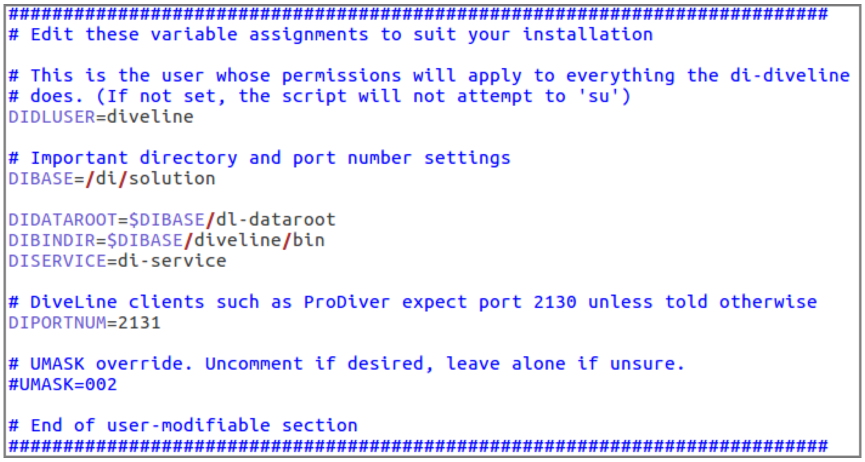
       ```
       ls -l init-di-diveline
       ```

       The permissions display as `-rwxrwxrwx`.

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

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

    The text editor opens.



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

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

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

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

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

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

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

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

12. For this installation, accept the variable defaults or make edits where necessary:
    - `DIDLUSER=diveline`—The name of the user that runs the DiveLine server
    - `DIBASE=/di/platform`—The location of the base DI Platform directory
    - `DIDATAROOT=$DIBASE/dl-dataroot`—The location of the DiveLine `config`, `acl`, `cache`, `log`, and `data` directories
    - `DIBINDIR=$DIBASE/diveline/bin`—The location of the DiveLine executable files
    - `DISERVICE=di-service`—The name of the existing **di-service**
    - `DIPORTNUM=2131`—The listening port for DiveLine on the server

      NOTE: Specify the port number that you chose when requesting a license. Port 2130 is the default.
13. Save and close the *init-di-diveline* file.

Creating an Administrator and a Test User

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

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

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

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

To create users for DiveLine:

1. Go to the `/executables` directory.

   ```
   cd /di/platform/executables
   ```
2. View the permissions for **dicfg**.

   ```
   ls -l dicfg
   ```

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

   If you do not have permission to create users:
   - Enable the execute permission.

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

- Verify that the permissions have changed.

  ```
  ls -l dicfg
  ```

  The permissions display as `-rwxrwxrwx`.

3. Create the administrator user ID.

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

   For example:

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

4. Create the test user ID.

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

   For example:

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

Creating a DiveLine Linux System User

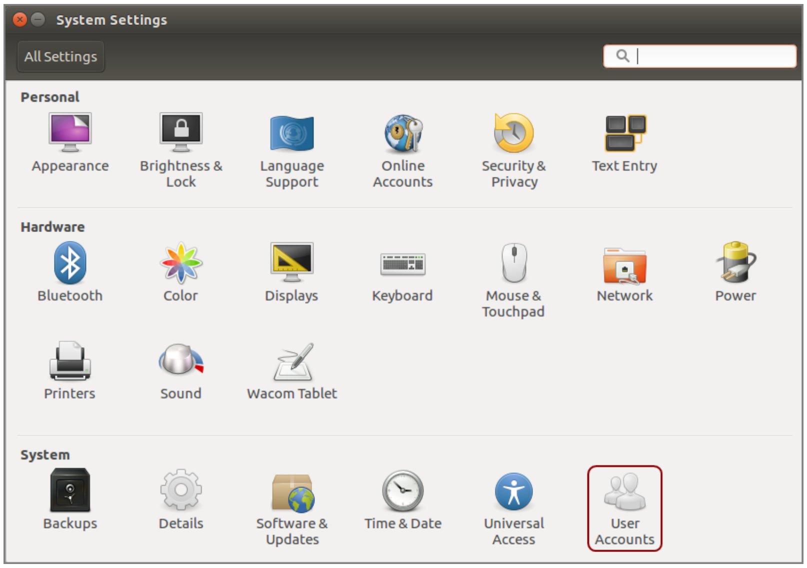
To run the DiveLine service on a Linux machine, you must create an Administrative User account. For example, you might create a new user with the account name of "diveline." This user must have the right to "Log On As a Service" and have a strong password.

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

To create a Linux system user:

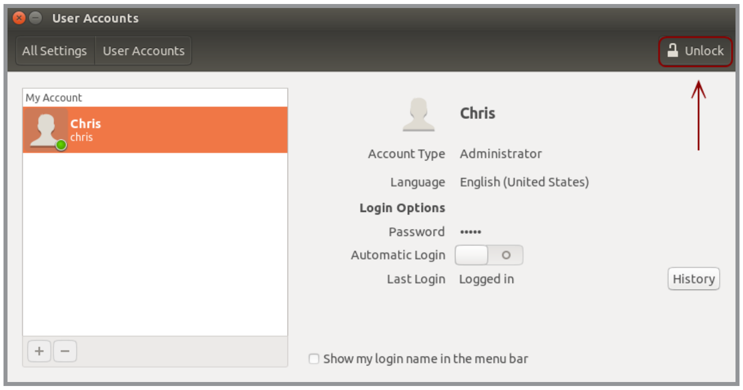
1. On the left panel, click the **System Settings** icon .

   The **System Settings** page opens:



2. Double-click **User Accounts** .

   The **User Accounts** dialog box opens.



Chris
chris

Chris

Account Type Administrator

Language English (United States)

Login Options

Password •••••

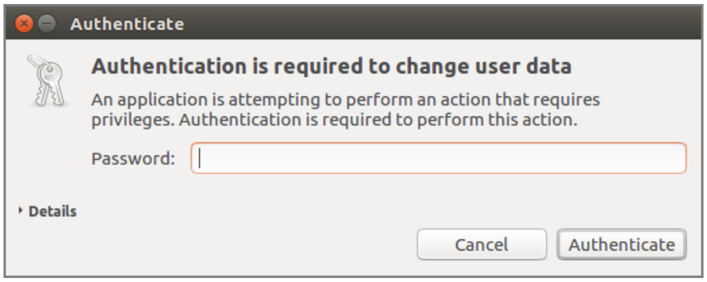
Automatic Login ○

Last Login Logged in

□ Show my login name in the menu bar

3. On the toolbar, click **Unlock** to enable editing.

   The **Authenticate** dialog box opens.



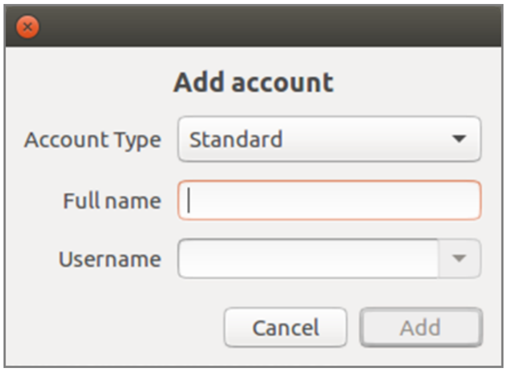
Authentication is required to change user data

An application is attempting to perform an action that requires privileges. Authentication is required to perform this action.

Password:

4. Enter your Password, and click **Authenticate**.
5. On the bottom left of the **User Accounts** window, click the plus sign .

   The **Add account** dialog box opens.



Add account

Account Type: Standard

Full name

Username

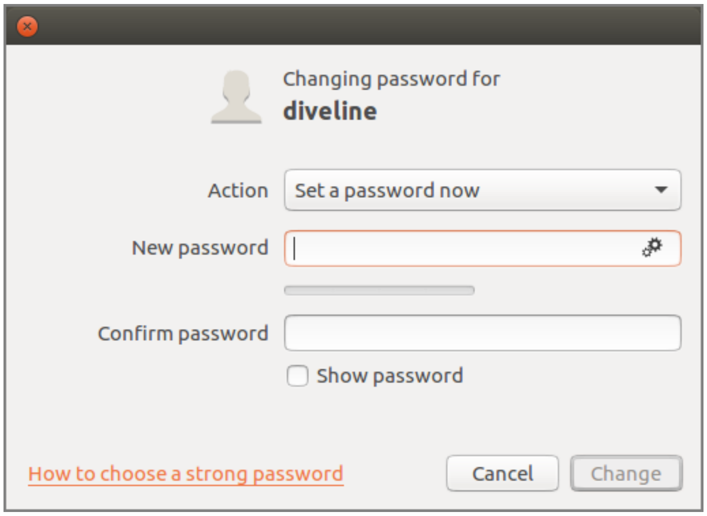
6. In the Add account dialog box":
   - Select the Account Type **Administrator**.
   - n the **Full name** and **Username** boxes, enter **diveline**, or another name of your choosing for running the DiveLine service,

     NOTE: Use the name that you identified for the `DIDLUSER` in Step 12 of Installing and Configuring DiveLine on page 30.
7. Click **Add**.

   Re-enter your password when prompted.

   The new account is now listed under **Other Accounts**.
8. Click **Account Disabled**.

   The changing password dialog box opens.



Changing password for
diveline

Action: Set a password now

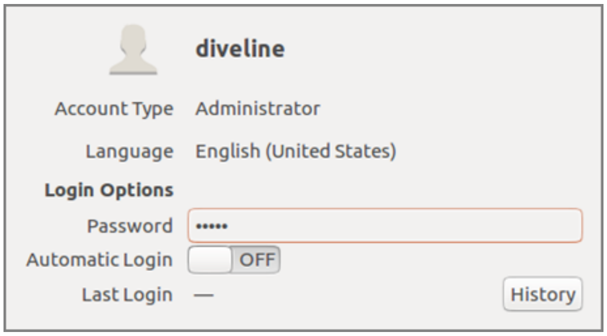
New password:

Confirm password:

□ Show password

9. Enter a password in the **New password** and **Confirm password** boxes.
10. Click **Change** to display the updated **diveline** user account.

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



diveline

Account Type: Administrator

Language: English (United States)

Login Options

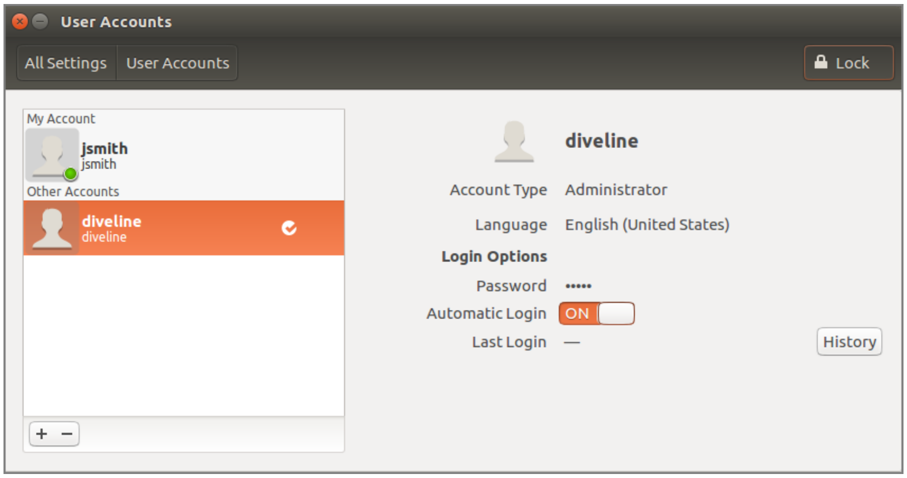
Password: •••••

Automatic Login: OFF

Last Login: —

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

    The option changes to **ON** and turns orange.



diveline

Account Type Administrator

Language English (United States)

Login Options

Password •••••

Automatic Login ON

Last Login —

12. On the toolbar, click **Lock** and close the window.

Creating and Configuring an Encryption Key

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

Complete the following steps:

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

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

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

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

   For example:

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

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

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

4. View permissions for `/config` .

   ```
   ls -l
   ```

   The permissions display.

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

If you do not have permission:

a. Enable the execute permission.

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

b. Verify that the permissions have changed.

```
ls -l config
```

The permissions display as `drwxrwxrwx`.

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

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

6. Go to the `/config` directory.

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

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

```
ls
```

Starting and Stopping the DiveLine Service

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

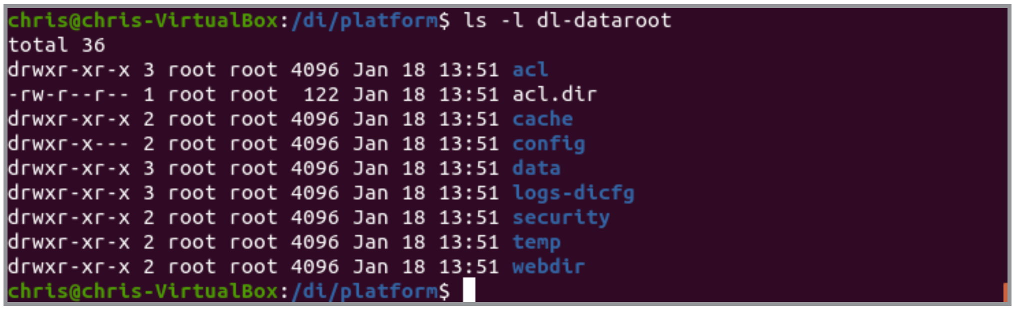
IMPORTANT: Before you start DiveLine for the first time, check the permissions of your `/di/platform/dl-dataroot` directory and the contents. If the permissions are `-rwxrwxrwx`, you can run the utility. If you do not have permission:

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

```
cd /di/platform
```

2. Check the permissions by entering the following command:

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



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

3. Enable the execute permission.

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

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

4. Verify that the permissions have changed.

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

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

- Start DiveLine by entering the following command:

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

- Stop DiveLine by entering the following command:

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

- Restart DiveLine by entering the following command:

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

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

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

Verifying the DiveLine Installation

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

To verify DiveLine:

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

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

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

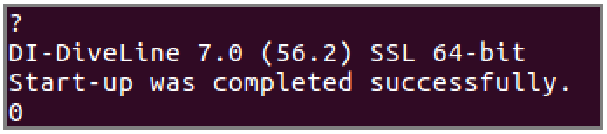
   ```
   telnet <servername> <port number>
   ```

   For example:

   ```
   telnet ubuntu 2131
   ```

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

   The DiveLine point release displays and validates the DiveLine installation.

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

4. Enter `quit`.

   The connection closes.

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

Starting DiveLine Automatically at System Boot

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

Installing Java and Tomcat

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

Downloading Java

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

Prerequisite: Uninstall any older versions of Java SE.

This procedure uses OpenJDK.

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

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

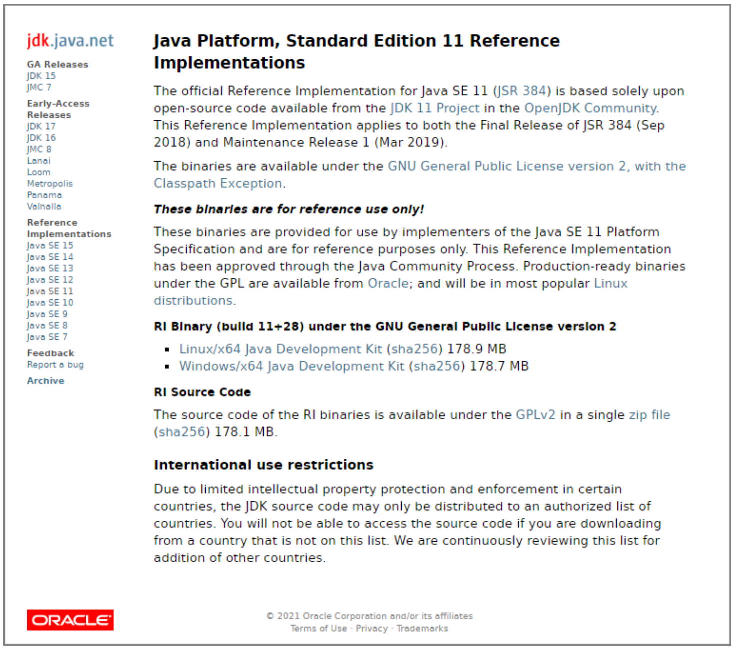
To download the software, complete the following steps:

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

   https://jdk.java.net/java-se-ri/11/

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

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



Java Platform, Standard Edition 11 Reference Implementations

The official Reference Implementation for Java SE 11 (JSR 384) is based solely upon open-source code available from the JDK 11 Project in the OpenJDK Community. This Reference Implementation applies to both the Final Release of JSR 384 (Sep 2018) and Maintenance Release 1 (Mar 2019).

The binaries are available under the GNU General Public License version 2, with the Classpath Exception.

These binaries are for reference use only!

These binaries are provided for use by implementers of the Java SE 11 Platform Specification and are for reference purposes only. This Reference Implementation has been approved through the Java Community Process. Production-ready binaries under the GPL are available from Oracle; and will be in most popular Linux distributions.

RI Binary (build 11+28) under the GNU General Public License version 2

- Linux/x64 Java Development Kit (sha256) 178.9 MB
- Windows/x64 Java Development Kit (sha256) 178.7 MB

RI Source Code

The source code of the RI binaries is available under the GPLv2 in a single zip file (sha256) 178.1 MB.

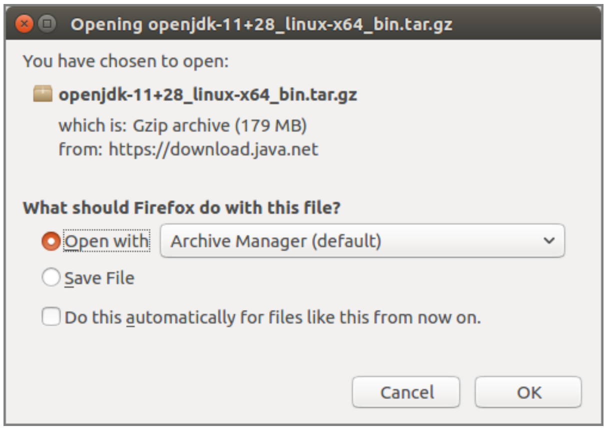
International use restrictions

Due to limited intellectual property protection and enforcement in certain countries, the JDK source code may only be distributed to an authorized list of countries. You will not be able to access the source code if you are downloading from a country that is not on this list. We are continuously reviewing this list for addition of other countries.

© 2021 Oracle Corporation and/or its affiliates
Terms of Use · Privacy · Trademarks

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

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


Opening openjdk-11+28_linux-x64_bin.tar.gz

You have chosen to open:

openjdk-11+28_linux-x64_bin.tar.gz

which is: Gzip archive (179 MB)
from: https://download.java.net

What should Firefox do with this file?

● Open with Archive Manager (default)

○ Save File

□ Do this automatically for files like this from now on.

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

   The software is saved to the default download directory.
6. Navigate to the file and move it to the `/di/platform/downloads` directory on your Linux server or VM.

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

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

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

8. Verify that the file copied correctly.

   ```
   ls
   ```

9. Close the browser.

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

Installing Java Development Kit

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

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

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

To install Java:

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

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

2. Extract the JDK file.

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

   The `-xvzf` arguments do the following:

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

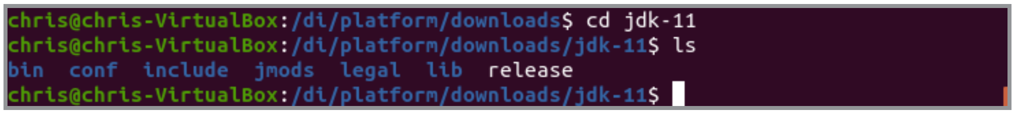
   Press **Enter** to unpack the JDK package and create the `jdk-11` subdirectory.

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

   ```
   cd jdk-11
   ```

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

```
ls
```



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

About Setting up an HTTPS Connection

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

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

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

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

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

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

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

- Purchase and install a certificate from a standard Certificate Authority, such as VeriSign or DigiCert. To request a certificate, you must create a Certificate Signing Request (CSR) from your server. Working with the issuer or instructions available, install the certificate in the Tomcat directory.
- Create a self-signed certificate using the Java genkey tool. Typically, you might generate and install a temporary self-signed certificate if you are in a trial or test phase and not concerned about receiving browser security warnings.

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

Downloading Apache Tomcat

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

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

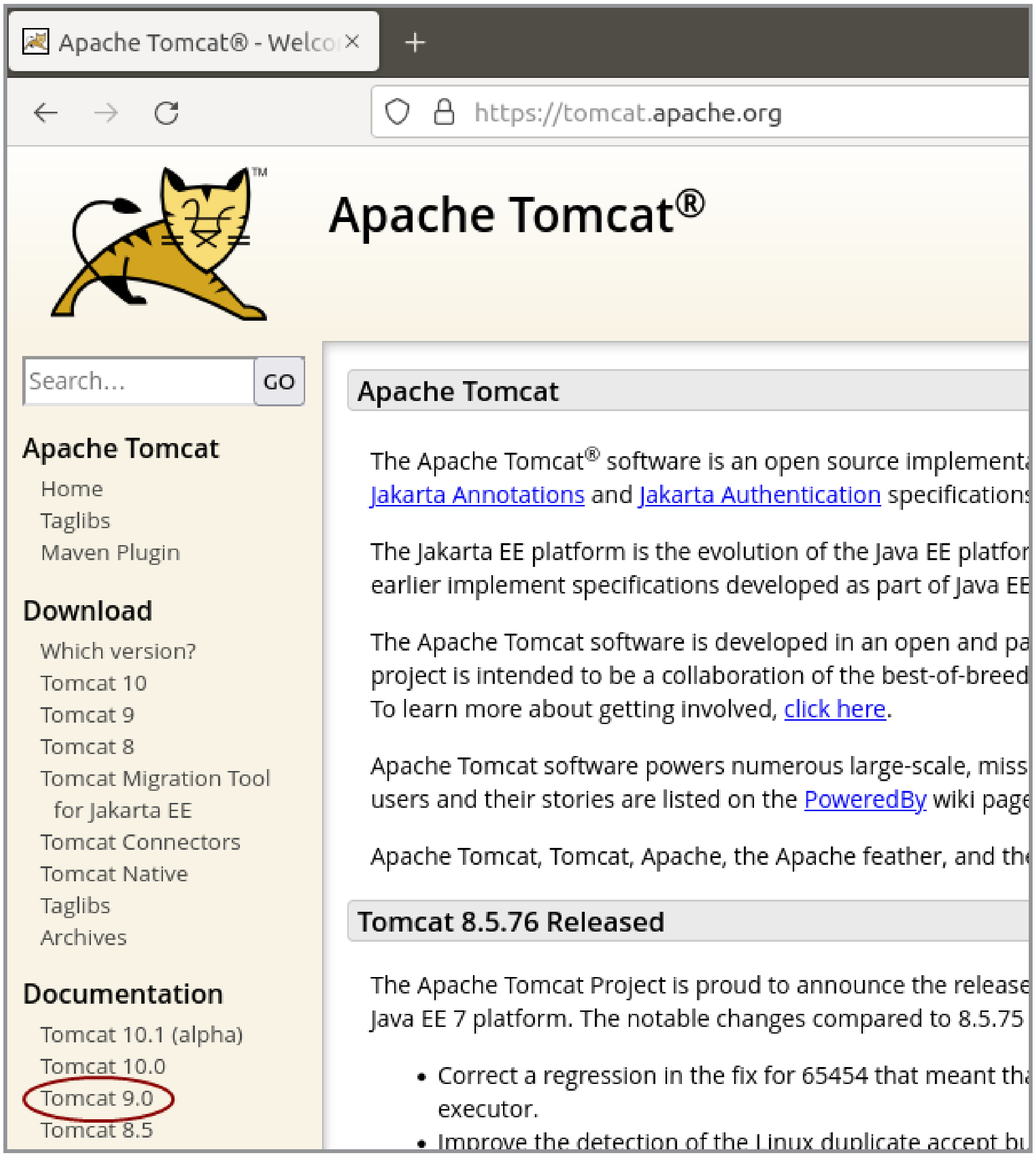
NOTE: DI recommendsTomcat 9.0.

To download Apache Tomcat:

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

   http://tomcat.apache.org

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



Apache Tomcat®

Apache Tomcat
Home
Taglibs
Maven Plugin

Download
Which version?
Tomcat 10
Tomcat 9
Tomcat 8
Tomcat Migration Tool for Jakarta EE
Tomcat Connectors
Tomcat Native
Taglibs
Archives

Documentation
Tomcat 10.1 (alpha)
Tomcat 10.0
Tomcat 9.0
Tomcat 8.5

Apache Tomcat

The Apache Tomcat® software is an open source implement
Jakarta Annotations and Jakarta Authentication specification

The Jakarta EE platform is the evolution of the Java EE platfor
earlier implement specifications developed as part of Java EE

The Apache Tomcat software is developed in an open and pa
project is intended to be a collaboration of the best-of-breed
To learn more about getting involved, click here.

Apache Tomcat software powers numerous large-scale, miss
users and their stories are listed on the PoweredBy wiki page

Apache Tomcat, Tomcat, Apache, the Apache feather, and th

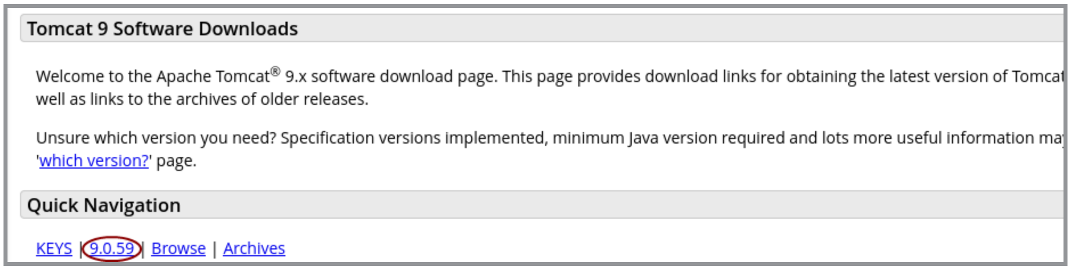
Tomcat 8.5.76 Released

The Apache Tomcat Project is proud to announce the release
Java EE 7 platform. The notable changes compared to 8.5.75

- Correct a regression in the fix for 65454 that meant th executor.
- Improve the detection of the Linux duplicate accept bu

3. On the left pane, under Download, click **Tomcat <version number>** .

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



Tomcat 9 Software Downloads

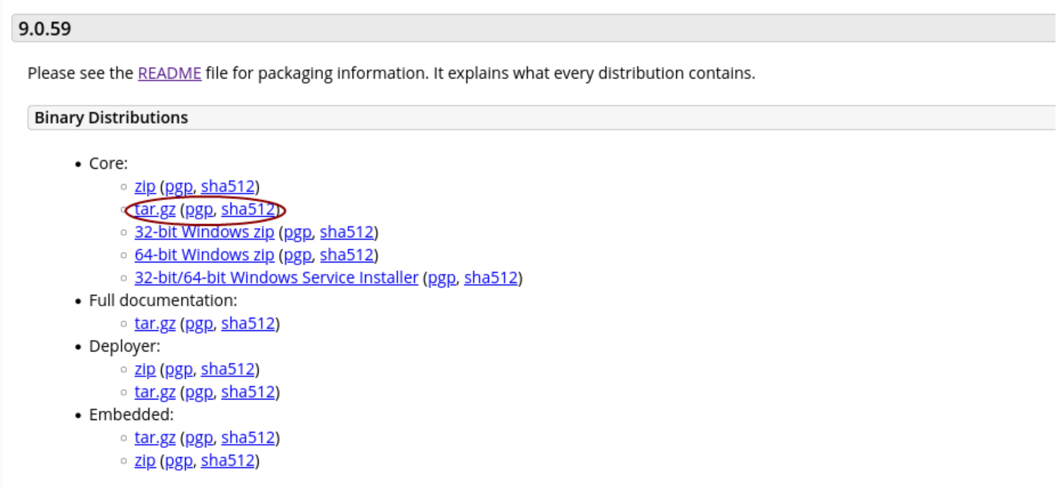
Welcome to the Apache Tomcat® 9.x software download page. This page provides download links for obtaining the latest version of Tomcat well as links to the archives of older releases.

Unsure which version you need? Specification versions implemented, minimum Java version required and lots more useful information ma 'which version?' page.

Quick Navigation

KEYS | 9.0.59 | Browse | Archives

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



9.0.59

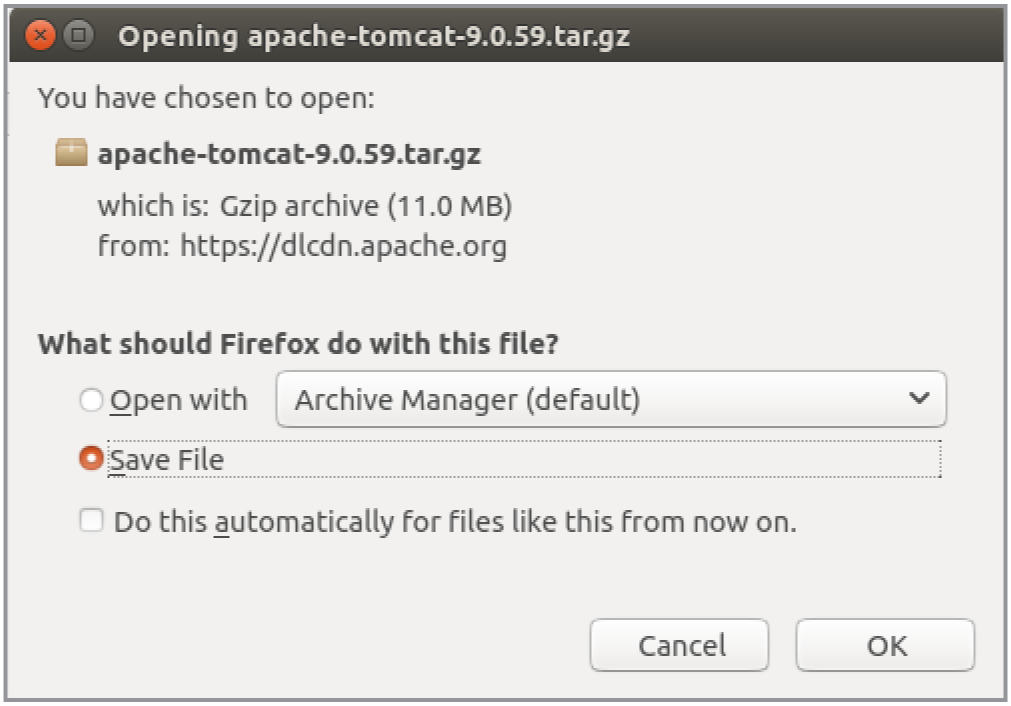
Please see the README file for packaging information. It explains what every distribution contains.

Binary Distributions

- Core:
  - zip (pgp, sha512)
  - tar.gz (pgp, sha512)
  - 32-bit Windows zip (pgp, sha512)
  - 64-bit Windows zip (pgp, sha512)
  - 32-bit/64-bit Windows Service Installer (pgp, sha512)
- Full documentation:
  - tar.gz (pgp, sha512)
- Deployer:
  - zip (pgp, sha512)
  - tar.gz (pgp, sha512)
- Embedded:
  - tar.gz (pgp, sha512)
  - zip (pgp, sha512)

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

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



Opening apache-tomcat-9.0.59.tar.gz

You have chosen to open:

apache-tomcat-9.0.59.tar.gz

which is: Gzip archive (11.0 MB)
from: https://dlcdn.apache.org

What should Firefox do with this file?

○ Open with Archive Manager (default)

● Save File

□ Do this automatically for files like this from now on.

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

   The file is downloaded to the `Downloads` directory on your local computer.
8. Navigate to the file location.
9. Move the file to the `/di/platform/downloads` directory

   ```
   sudo mv apache-tomcat-<version number>.tar.gz
   /di/platform/downloads
   ```
10. Navigate to the `/di/platform/downloads` directory

    ```
    cd /di/platform/downloads
    ```
11. Verify that the file moved correctly by entering the following command:

    ```
    ls
    ```
12. Close the web browser.

Installing Apache Tomcat

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

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

NOTE: DI recommends Tomcat 9.0.

To install Apache Tomcat:

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

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

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

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

   The -`xvzf` arguments do the following:

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

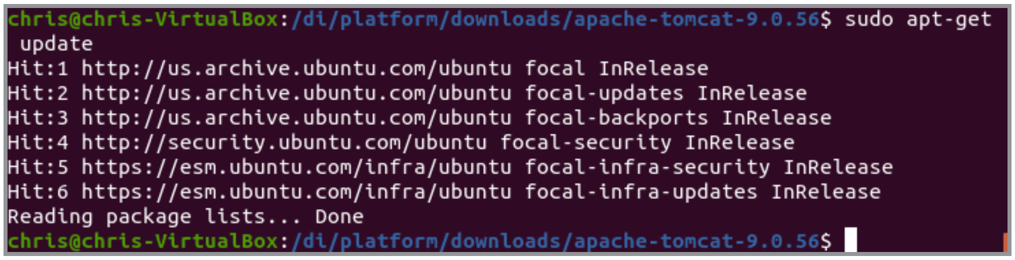
   The file unpacks and creates the `apache-tomcat-<version number>` subdirectory.

3. Go to the Apache Tomcat folder.

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

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

   ```
   sudo apt-get update
   ```

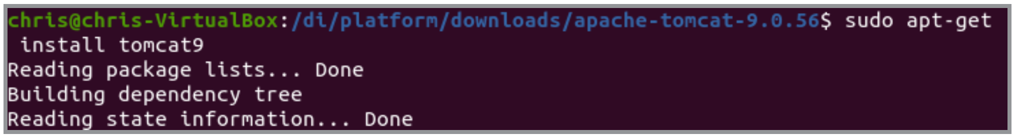


```
chris@chris-VirtualBox:/di/platform/downloads/apache-tomcat-9.0.56$ sudo apt-get
 update
Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu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

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

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

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



```
chris@chris-VirtualBox:/di/platform/downloads/apache-tomcat-9.0.56$ sudo apt-get
 install tomcat9
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 .

   ```
   cd /etc/default
   ```

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

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

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

   If you do not have permission to run the utility:

   a. Enable the execute permission.

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

   b. Verify that the permissions have changed.

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

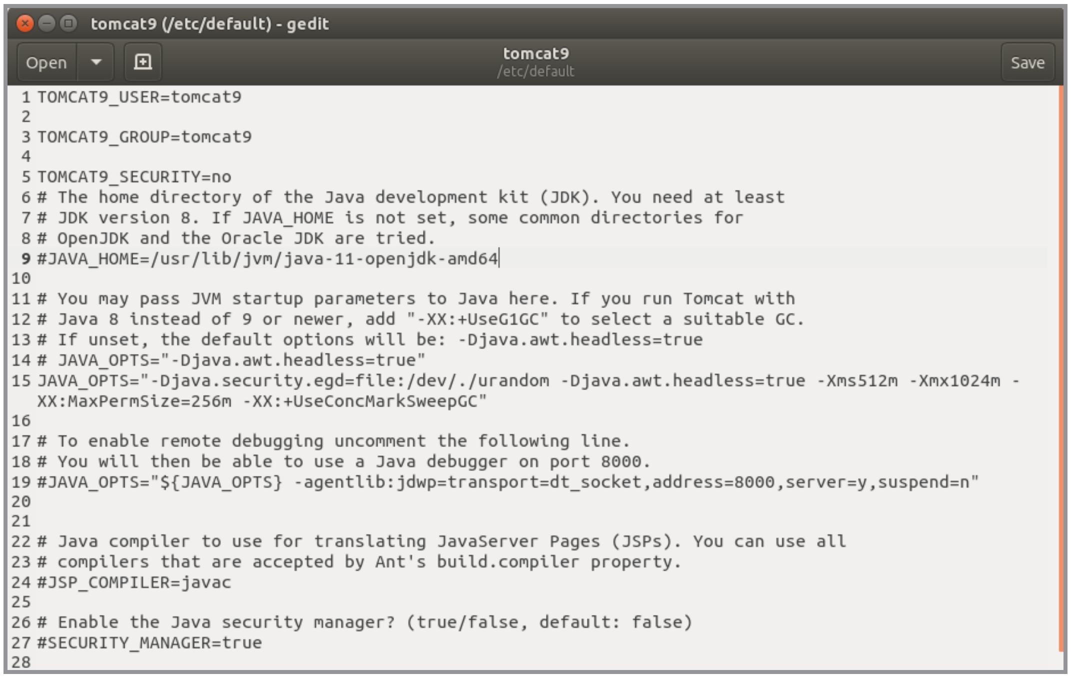
      The permissions display as `-rwxrwxrwx`.

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

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

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

   Here is an example of the configuration file:



```
TOMCAT9_USER=tomcat9

TOMCAT9_GROUP=tomcat9

TOMCAT9_SECURITY=no
# The home directory of the Java development kit (JDK). You need at least
# JDK version 8. If JAVA_HOME is not set, some common directories for
# OpenJDK and the Oracle JDK are tried.
#JAVA_HOME=/usr/lib/jvm/java-11-openjdk-amd64

# You may pass JVM startup parameters to Java here. If you run Tomcat with
# Java 8 instead of 9 or newer, add "-XX:+UseG1GC" to select a suitable GC.
# If unset, the default options will be: -Djava.awt.headless=true
# JAVA_OPTS="-Djava.awt.headless=true"
JAVA_OPTS="-Djava.security.egd=file:/dev/./urandom -Djava.awt.headless=true -Xms512m -Xmx1024m -
XX:MaxPermSize=256m -XX:+UseConcMarkSweepGC"

# To enable remote debugging uncomment the following line.
# You will then be able to use a Java debugger on port 8000.
#JAVA_OPTS="${JAVA_OPTS} -agentlib:jdwp=transport=dt_socket,address=8000,server=y,suspend=n"


# Java compiler to use for translating JavaServer Pages (JSPs). You can use all
# compilers that are accepted by Ant's build.compiler property.
#JSP_COMPILER=javac

# Enable the Java security manager? (true/false, default: false)
#SECURITY_MANAGER=true

```

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

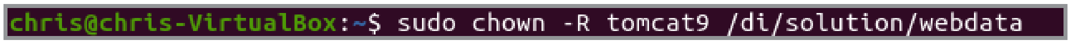
9. Locate the `JAVA_OPTS` parameter (last line in the above figure) and replace it with the following:

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

10. Change the `TOMCAT9_SECURITY` variable value to **no**, and remove the comment tag, `#`, at the beginning of the line.
11. Save and close the changed configuration file.
12. Change the ownership of `webdata` and operate on its files and sub-directories to enable Tomcat to write files to the DI `webdata` directory.

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

    For example:

    ```
    chris@chris-VirtualBox:~$ sudo chown -R tomcat9 /di/solution/webdata
    ```

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

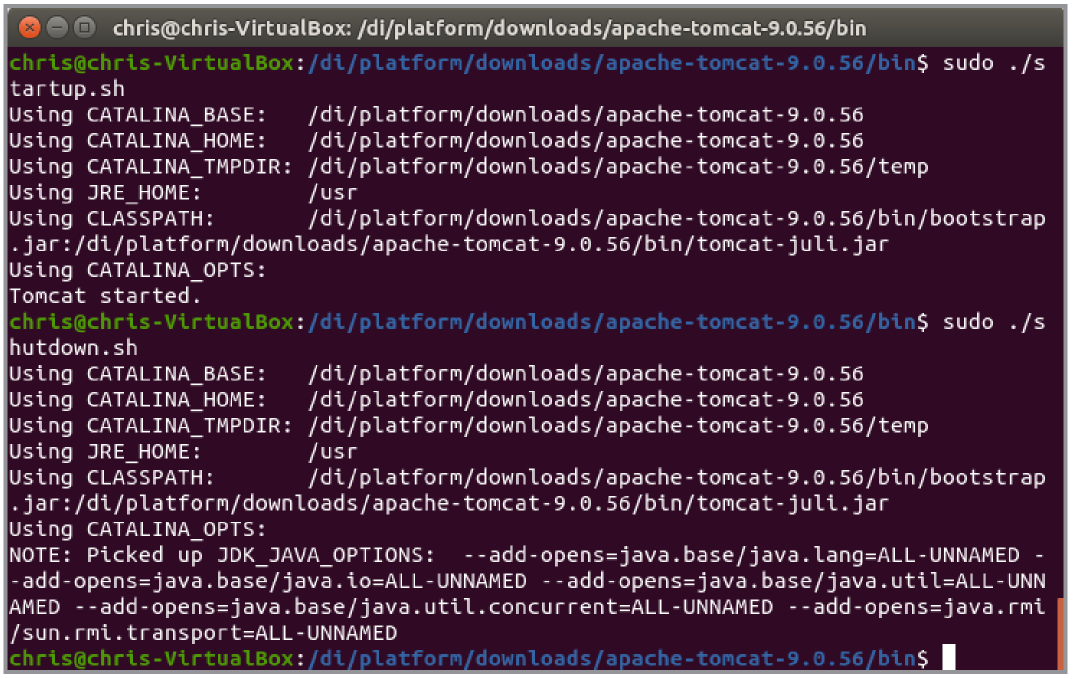
```
cd /di/platform/downloads/apache-tomcat-<version-
number>/bin
```

- Start Tomcat by entering the following command:

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

- Stop Tomcat by entering the following command:

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



chris@chris-VirtualBox: /di/platform/downloads/apache-tomcat-9.0.56/bin

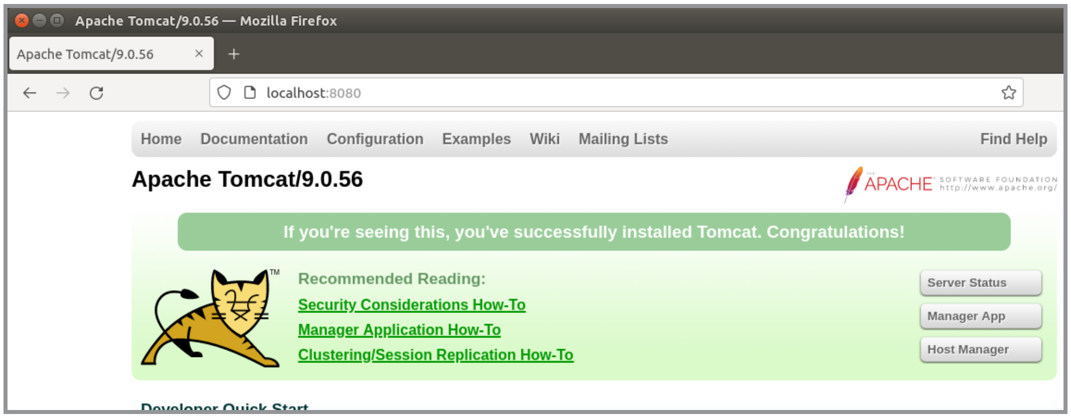
```
chris@chris-VirtualBox:/di/platform/downloads/apache-tomcat-9.0.56/bin$ sudo ./s
tartup.sh
Using CATALINA_BASE:   /di/platform/downloads/apache-tomcat-9.0.56
Using CATALINA_HOME:   /di/platform/downloads/apache-tomcat-9.0.56
Using CATALINA_TMPDIR: /di/platform/downloads/apache-tomcat-9.0.56/temp
Using JRE_HOME:        /usr
Using CLASSPATH:       /di/platform/downloads/apache-tomcat-9.0.56/bin/bootstrap
.jar:/di/platform/downloads/apache-tomcat-9.0.56/bin/tomcat-juli.jar
Using CATALINA_OPTS:
Tomcat started.
chris@chris-VirtualBox:/di/platform/downloads/apache-tomcat-9.0.56/bin$ sudo ./s
hutdown.sh
Using CATALINA_BASE:   /di/platform/downloads/apache-tomcat-9.0.56
Using CATALINA_HOME:   /di/platform/downloads/apache-tomcat-9.0.56
Using CATALINA_TMPDIR: /di/platform/downloads/apache-tomcat-9.0.56/temp
Using JRE_HOME:        /usr
Using CLASSPATH:       /di/platform/downloads/apache-tomcat-9.0.56/bin/bootstrap
.jar:/di/platform/downloads/apache-tomcat-9.0.56/bin/tomcat-juli.jar
Using CATALINA_OPTS:
NOTE: Picked up JDK_JAVA_OPTIONS:  --add-opens=java.base/java.lang=ALL-UNNAMED -
-add-opens=java.base/java.io=ALL-UNNAMED --add-opens=java.base/java.util=ALL-UNN
AMED --add-opens=java.base/java.util.concurrent=ALL-UNNAMED --add-opens=java.rmi
/sun.rmi.transport=ALL-UNNAMED
chris@chris-VirtualBox:/di/platform/downloads/apache-tomcat-9.0.56/bin$
```

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

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

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

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



Apache Tomcat/9.0.56

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:
Security Considerations How-To
Manager Application How-To
Clustering/Session Replication How-To

Developer Quick Start

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

Generating an SSL/TLS Self-Signed Certificate

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

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

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

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

To generate a self-signed certificate:

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

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

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

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

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

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

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

- `What is the name of your organizational unit?` – For example, **BI Software**.
- `What is the name of your organization?` – For example, **Dimensional Insight**.
- `What is the name of your City or Locality?` – For example, **Burlington**.
- `What is the name of your State or Province?` – For example, **MA**.
- `What is the two-letter country code for this unit?` – For example, **US**.
- At the confirmation prompt, for example:

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

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

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

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

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

```
ls
```

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

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

Enabling the Default HTTPS Connector

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

1. If Tomcat is running, stop it.

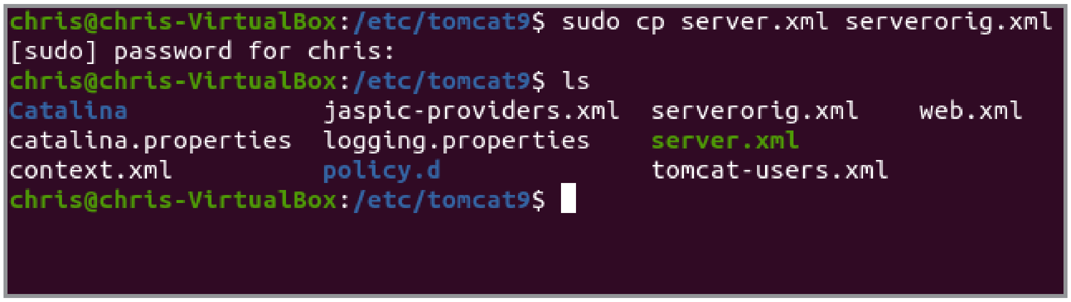
   ```
   sudo /di/platform/downloads/apache-tomcat-<version-number>/bin ./shutdown.sh
   ```

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

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

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

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



```
chris@chris-VirtualBox:/etc/tomcat9$ sudo cp server.xml serverorig.xml
[sudo] password for chris:
chris@chris-VirtualBox:/etc/tomcat9$ ls
Catalina            jaspic-providers.xml  serverorig.xml    web.xml
catalina.properties logging.properties    server.xml
context.xml         policy.d              tomcat-users.xml
chris@chris-VirtualBox:/etc/tomcat9$
```

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

   ```
   ls
   ```

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

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

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

   If you do not have permissions:

   - Enable the execute permission.

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

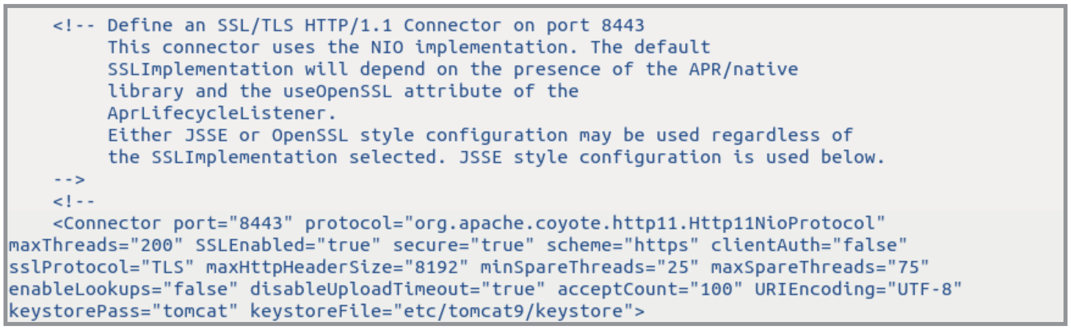
   - Verify that the permissions have changed.

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

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

```
gedit server.xml
```

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

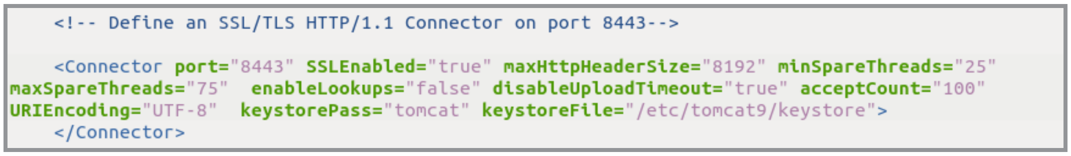


```
    <!-- Define an SSL/TLS HTTP/1.1 Connector on port 8443
         This connector uses the NIO implementation. The default
         SSLImplementation will depend on the presence of the APR/native
         library and the useOpenSSL attribute of the
         AprLifecycleListener.
         Either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

8. In the "Define an SSL/TLS HTTP/1.1 Connector on port 8443" and "Connector port" sections of the *server.xml* file, make the following edits:
   a. Remove the commented lines beginning with "This connector..." and ending with "used below".
   b. After `<Connector port= "8443"`, add the following attributes:

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

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



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

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

10. Save and close the *server.xml* file.
11. Start Tomcat.

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

NOTES:

- When DivePort software generates URLs, non-ASCII characters are encoded to ensure that the URL only contains ASCII characters. For these generated strings, ISO-8859-1 or UTF-8 encoding is acceptable.
- If users intend to enter URLs that contain non-ASCII characters, set the `URIEncoding` on the Tomcat connector according to the encoding that they intend to use.

Verifying the HTTPS Connection

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

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

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

This procedure uses the Mozilla Firefox browser.

To verify the HTTPS connection, complete the following steps:

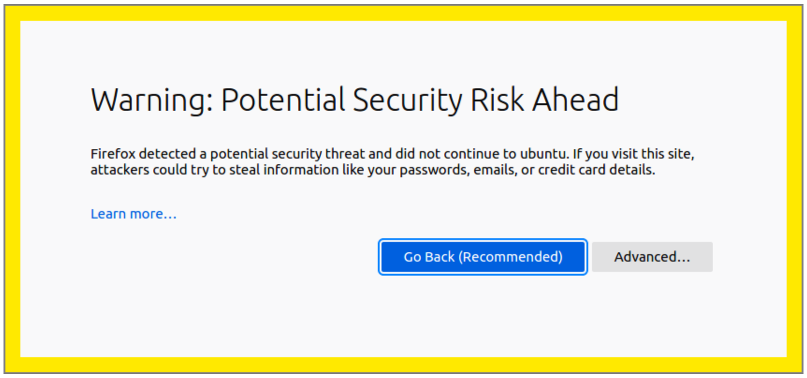
1. Open a browser window, and enter a URL with the following syntax:

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

   For example:

   ```
   https://localhost:8443
   ```

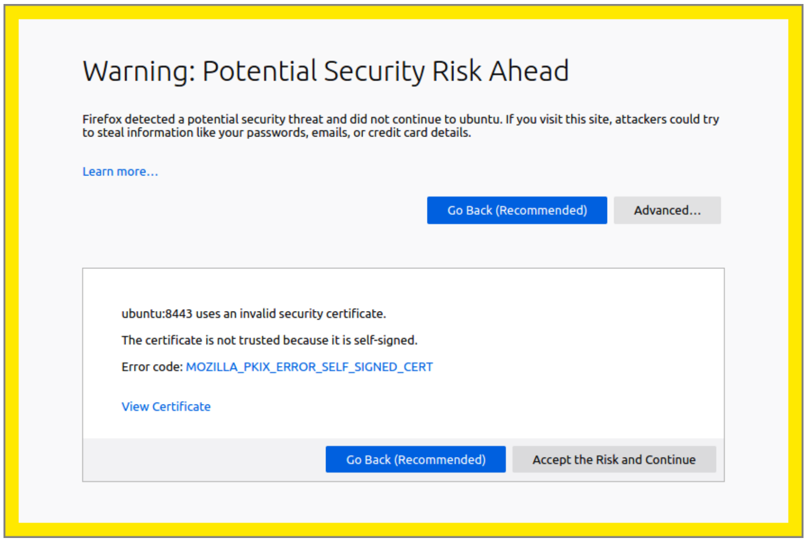
2. Press **Enter** to display the following security screen in the Firefox browser:



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to ubuntu. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

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



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to ubuntu. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

ubuntu:8443 uses an invalid security certificate.

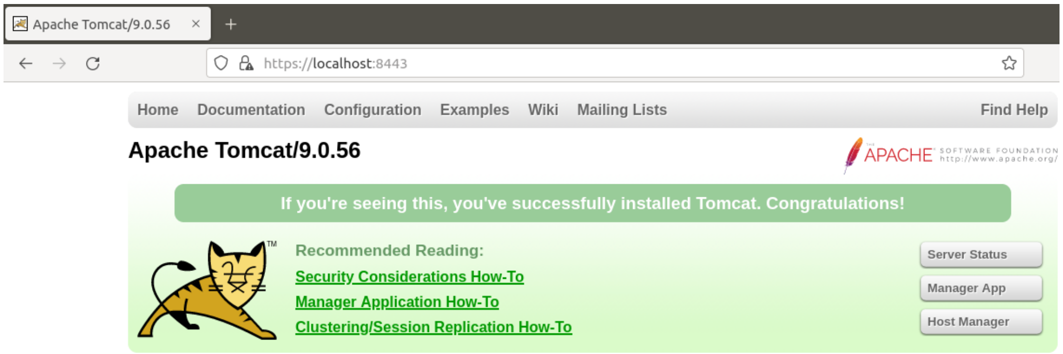
The certificate is not trusted because it is self-signed.

Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

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

   The confirmation page displays.

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



Apache Tomcat/9.0.56

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:

Security Considerations How-To

Manager Application How-To

Clustering/Session Replication How-To

DivePort

Installing DivePort

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

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

To extract and copy the DivePort installation files:

1. If Tomcat is running, stop it.
2. Navigate to the `/di/platform` directory .

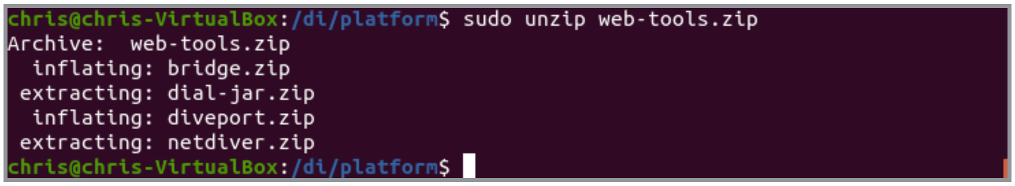
   ```
   cd /di/platform
   ```

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

   ```
   ls
   ```

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

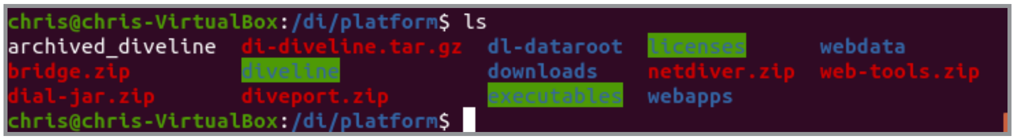
   ```
   sudo unzip web-tools.zip
   ```



```
chris@chris-VirtualBox:/di/platform$ sudo unzip web-tools.zip
Archive:  web-tools.zip
  inflating: bridge.zip
 extracting: dial-jar.zip
  inflating: diveport.zip
 extracting: netdiver.zip
chris@chris-VirtualBox:/di/platform$
```

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

   ```
   ls
   ```



```
chris@chris-VirtualBox:/di/platform$ ls
archived_diveline  di-diveline.tar.gz  dl-dataroot  licenses     webdata
bridge.zip         diveline            downloads    netdiver.zip  web-tools.zip
dial-jar.zip       diveport.zip        executables  webapps
chris@chris-VirtualBox:/di/platform$
```

6. Unzip *diveport.zip.*

   ```
   sudo unzip diveport.zip
   ```

7. Navigate to the `diveport` directory.

   ```
   cd diveport
   ```

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

   ```
   ls
   ```

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

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

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

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

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

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

11. Verify that the files were renamed and copied.

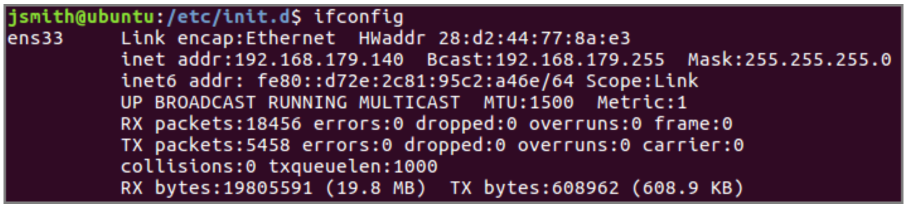
    - `ls /di/platform/webapps`
    - `ls /di/platform/webdata`

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

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

13. Determine the IP address of your Linux machine

    ```
    ifconfig
    ```

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

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

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

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

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

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

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

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

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

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

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

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

If you do not have permission:

i. Enable the execute permission.

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

ii. Verify that the permissions have changed.

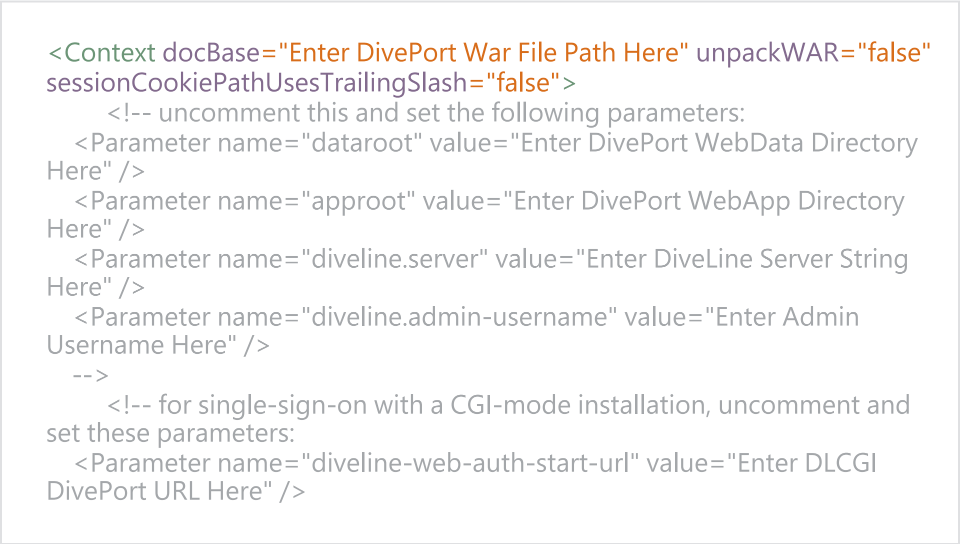
```
ls -l mydiveport.xml
```

The permissions display as `-rwxrwxrwx`.

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

```
gedit mydiveport.xml
```

The file opens in the text editor



```
<Context docBase="Enter DivePort War File Path Here" unpackWAR="false"
sessionCookiePathUsesTrailingSlash="false">
        <!-- uncomment this and set the following parameters:
    <Parameter name="dataroot" value="Enter DivePort WebData Directory
Here" />
    <Parameter name="approot" value="Enter DivePort WebApp Directory
Here" />
    <Parameter name="diveline.server" value="Enter DiveLine Server String
Here" />
    <Parameter name="diveline.admin-username" value="Enter Admin
Username Here" />
    -->
        <!-- for single-sign-on with a CGI-mode installation, uncomment and
set these parameters:
    <Parameter name="diveline-web-auth-start-url" value="Enter DLCGI
DivePort URL Here" />
```

```
  <Parameter name="diveline.web-auth-finish-url" value="Enter Logoff
URL Here" />
  -->
     <!-- If you need to permit HTTP connections:
  <Parameter name="require-confidentiality" value="false" />
  -->
     <!-- For Tomcat 8.5.42+ or 9.0.12+, the following is recommended:
  <CookieProcessor sameSiteCookies="lax" />
  -->
</Context>
```

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

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

  For example:

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

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

  For example:

  `/di/platform/webdata/mydiveport`

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

  For example:

  `/di/platform/webapps/mydiveport`

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

  For example:

  `ubuntu:2131`

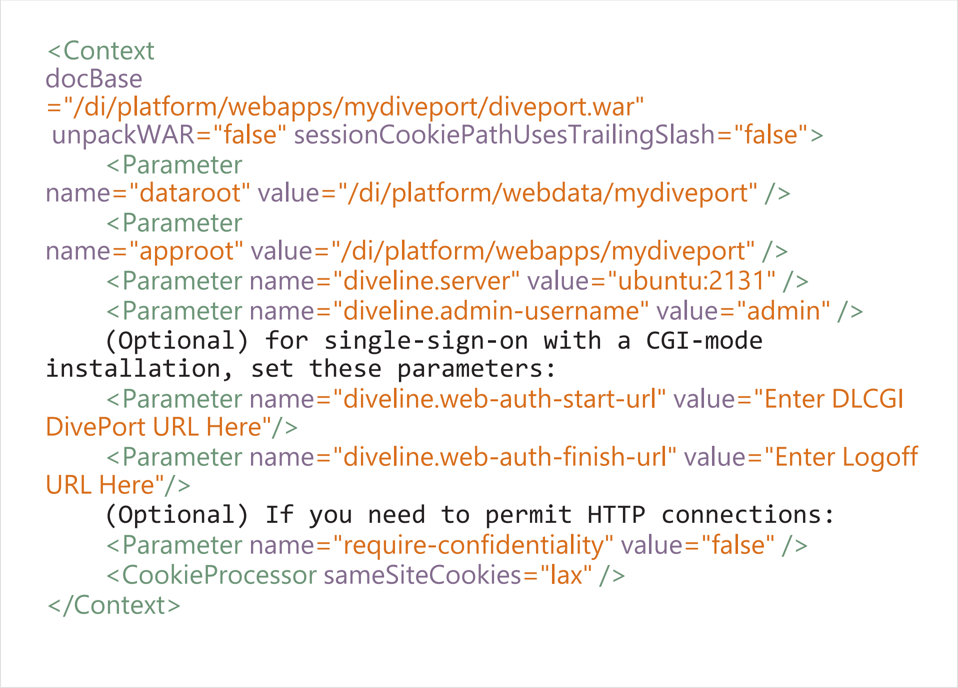
- `"Enter Admin Username Here"` – The DiveLine administrator name, which is defined in Creating an Administrator and a Test User on page 35.

  For example:

  `admin`

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

For example:



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

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

g. Save your changes and close the file.

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

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

17. Navigate to the `/etc` directory.

```
cd /etc
```

18. Change the ownership for the `tomcat<version>` directory to the Tomcat user, identified in Installing Apache Tomcat on page 51.

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

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

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

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

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

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

a. Enable the execute permission.

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

b. Verify that the permissions have changed.

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

The permissions display as `-rwxrwxrwx`.

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

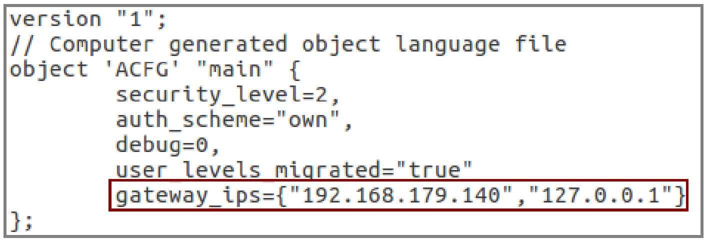
```
gedit atlcfg.cfg
```

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

    For example:

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

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



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

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

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

24. Save and close the file.

25. Start Tomcat

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

Verifying the DivePort Installation

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

Prerequisite: Download, install, and configure DivePort.

1. Enter your DivePort URL with the following syntax:

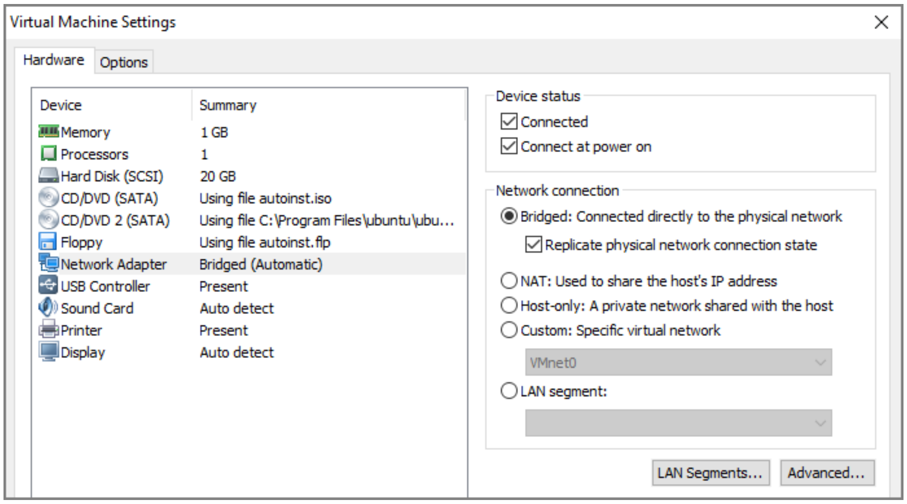
   ```
   https://<servername or IP address>:8443/<DivePort name>
   ```

   For example:

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

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

   If you have problems connecting to DivePort, review your logs and the configuration changes made to the *mydiveport.xml* and *atlcfg.cfg* files. The example URL reflects changes made in the **Installing DivePort** section. Additionally, if the Linux server is running in a VM, verify that you have configured the network connection options correctly. For example, the **Virtual Machine Settings** > **Network Adapter** options for an Ubuntu server appear as follows:



Device	Summary
Memory	1 GB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Using file autoinst.iso
CD/DVD 2 (SATA)	Using file C:\Program Files\ubuntu\ubu...
Floppy	Using file autoinst.flp
Network Adapter	Bridged (Automatic)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

● Bridged: Connected directly to the physical network

☑ Replicate physical network connection state

○ NAT: Used to share the host's IP address

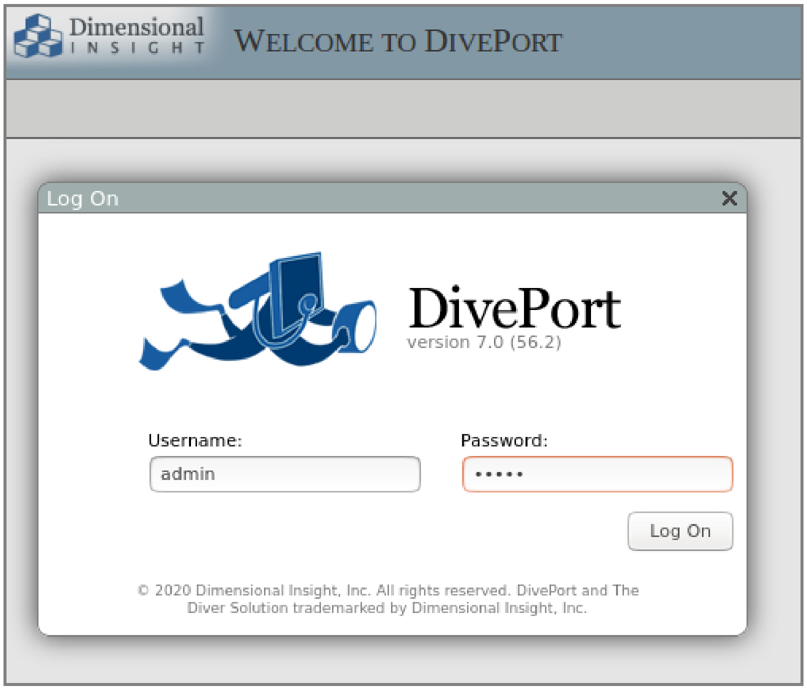
○ Host-only: A private network shared with the host

○ Custom: Specific virtual network

VMnet0

○ LAN segment:

2. In the Network connection section, enable the following options:
   a. Bridged: Connected directly to the physical network
   b. Replicate physical network connection state
3. If you have successfully installed DivePort, the **Welcome to DivePort** page opens.

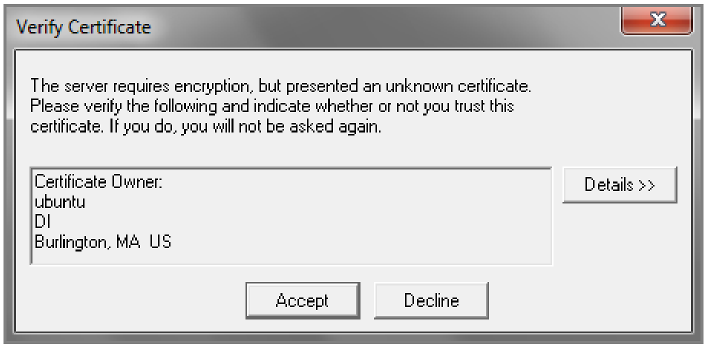


Username: admin

Password: •••••

© 2020 Dimensional Insight, Inc. All rights reserved. DivePort and The Diver Solution trademarked by Dimensional Insight, Inc.

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



The server requires encryption, but presented an unknown certificate. Please verify the following and indicate whether or not you trust this certificate. If you do, you will not be asked again.

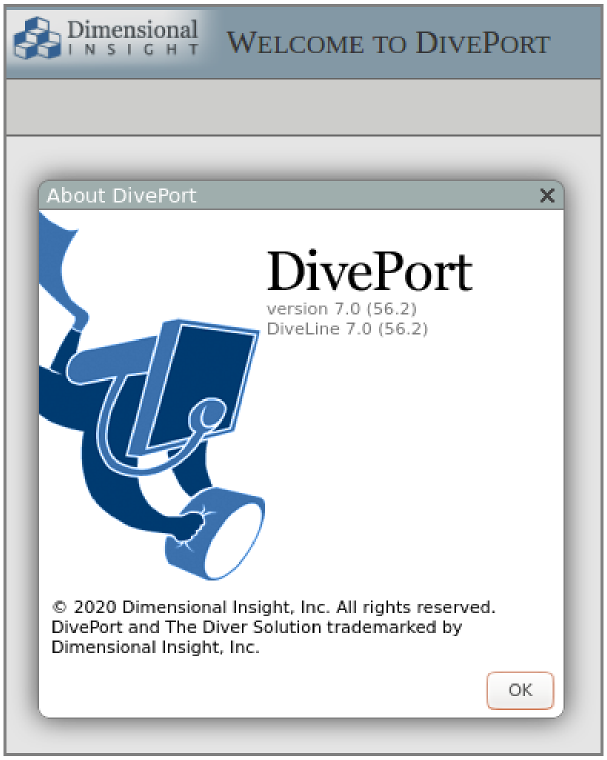
Certificate Owner:
ubuntu
DI
Burlington, MA US

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

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

6. Once connected and logged in to DivePort, click **HELP** > **About** to open the **About DivePort** dialog box that lists the current version numbers of DiveLine and DivePort.

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



version 7.0 (56.2)
DiveLine 7.0 (56.2)

© 2020 Dimensional Insight, Inc. All rights reserved.
DivePort and The Diver Solution trademarked by
Dimensional Insight, Inc.

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

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

Appendix: DivePort Installation

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

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

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

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

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

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

```
gedit ROOT.xml
```

```
<Context docBase="Enter DivePort War File Path Here" unpackWAR="false"
sessionCookiePathUsesTrailingSlash="false">
        <!-- uncomment this and set the following parameters:
    <Parameter name="dataroot" value="Enter DivePort WebData Directory Here"
/>
    <Parameter name="approot" value="Enter DivePort WebApp Directory Here" />
    <Parameter name="diveline.server" value="Enter DiveLine Server String Here" />
    <Parameter name="diveline.admin-username" value="Enter Admin Username
Here" />
    -->
        <!-- for single-sign-on with a CGI-mode installation, uncomment and set
these parameters:
    <Parameter name="diveline-web-auth-start-url" value="Enter DLCGI DivePort
URL Here" />
    <Parameter name="diveline.web-auth-finish-url" value="Enter Logoff URL Here"
/>
    -->
        <!-- If you need to permit HTTP connections:
    <Parameter name="require-confidentiality" value="false" />
    -->
</Context>
```

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

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

     For example:

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

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

     For example:

     `/di/platform/webdata/mydiveport`

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

     For example:

     `/di/platform/webapps/mydiveport`

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

     For example:

     `ubuntu:2131`

   - `"Enter Admin Username Here"` – The DiveLine administrator name, which is defined in Creating an Administrator and a Test User on page 35.

For example:

`admin`

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

  For example:

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

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

   For example:

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

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

6. Save your changes and close the file.

NetDiver

Installing NetDiver

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

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

To install NetDiver:

1. If running, stop the Tomcat web server.
2. Navigate to the `/di/platform` directory
   ```
   cd /di/platform
   ```
3. Unzip the *netdiver.zip* file.
   ```
   sudo unzip netdiver.zip
   ```
4. Navigate to the `netdiver` directory.
   ```
   cd netdiver
   ```
5. View the unzipped *netdiver.zip* file.
   ```
   ls -l
   ```
   The unzipped NetDiver package creates the following directories and file in the `netdiver` directory:
   - `/appdir`
   - `/datadir`
   - *context-file-template.xml*
6. Copy the `appdir` directory to the `/di/platform/webapps` directory and rename it to assign a NetDiver portal name (for example, **mynetdiver**).
   ```
   sudo cp -r appdir /di/platform/webapps/mynetdiver
   ```
7. Copy the `datadir` directory to the `/di/platform/webdata` directory and rename it to the same NetDiver portal name (for example, **mynetdiver**).
   ```
   sudo cp -r datadir /di/platform/webdata/mynetdiver
   ```
8. Navigate to the `/di/platform/netdiver` directory.
   ```
   cd /di/platform/netdiver
   ```
9. Create a copy of the *context-file-template.xml* file and rename it to the name of your NetDiver portal (for example, *mynetdiver.xml*).
   ```
   sudo cp -i context-file-template.xml mynetdiver.xml
   ```

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

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

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

a. Enable the execute permission.

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

b. Verify that the permissions have changed.

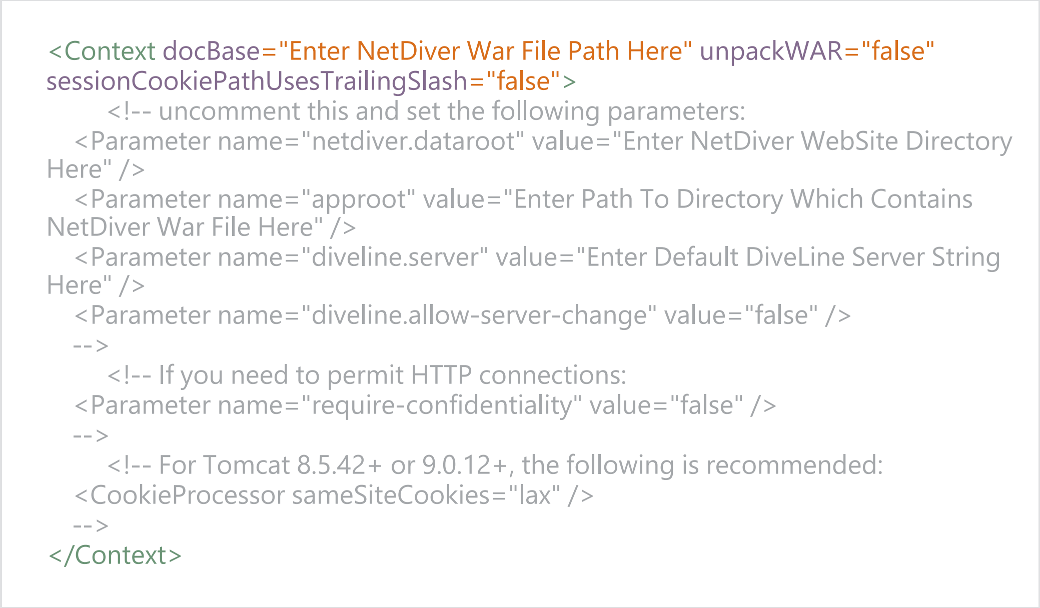
```
ls -l mynetdiver.xml
```

The permissions display as `-rwxrwxrwx`.

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

```
gedit mynetdiver.xml
```

The file opens in the text editor.



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

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

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

  For example:

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

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

  For example:

`/di/platform/webdata/mynetdiver`

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

  For example:

  `/di/platform/webapps/mynetdiver`

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

  For example:

  `ubuntu:2131`

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

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

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

    For example:

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

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

14. Save and close the file.
15. Navigate to the `/di/platform/netdiver` directory.

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

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

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

17. Start Tomcat.

Verifying the NetDiver Installation

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

Prerequisite: Download, install, and configure NetDiver.

1. Enter your NetDiver URL with the following syntax:

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

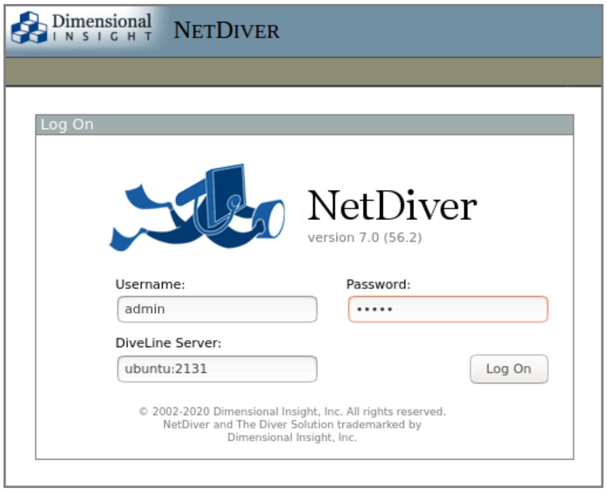
   For example:

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

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

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

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



version 7.0 (56.2)

Username: admin

Password: •••••

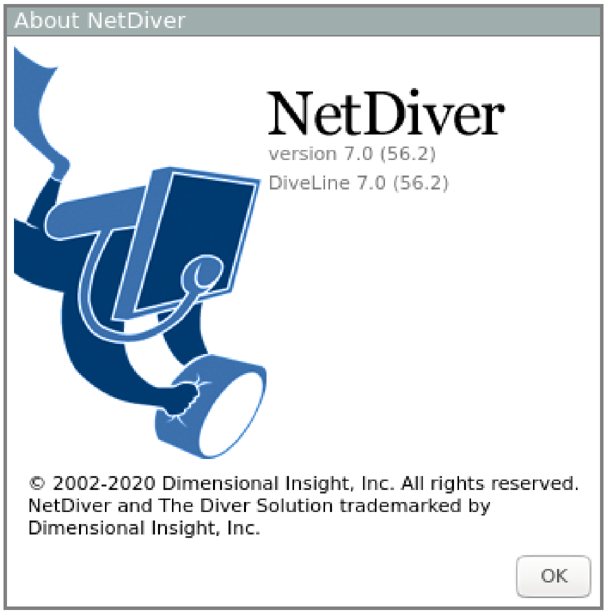
DiveLine Server: ubuntu:2131

© 2002-2020 Dimensional Insight, Inc. All rights reserved.
NetDiver and The Diver Solution trademarked by
Dimensional Insight, Inc.

3. If you installed a self-signed certificate and you have not previously logged in to the Linux server with a DI client, the client might ask you to

verify the self-signed certificate. Refer to **Verifying the DivePort Installation** for additional information.

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



version 7.0 (56.2)
DiveLine 7.0 (56.2)

© 2002-2020 Dimensional Insight, Inc. All rights reserved.
NetDiver and The Diver Solution trademarked by Dimensional Insight, Inc.

5. Click **OK** to close the dialog box.
6. Click **HELP** to open the *NetDiver Help* system in a new tab in your browser.

Installing Diver Platform Developer

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

Downloading and Extracting the Developer Installation Package

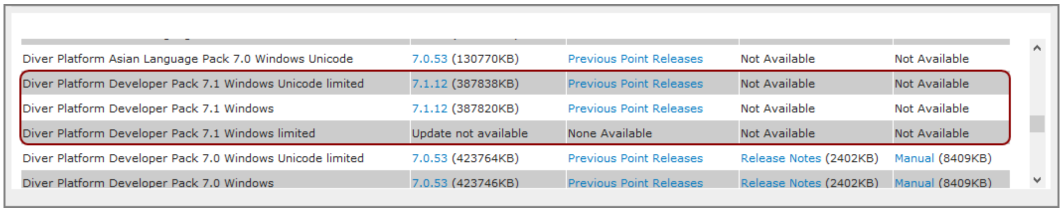
This topic describes how to download and extract the Diver Platform Developer 7.1 Windows software package. See Downloading the Server Installation Package on page 16 for information on how to locate DI installation files.

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

See About the DI Directory Structure on page 10 to prepare the client computers.

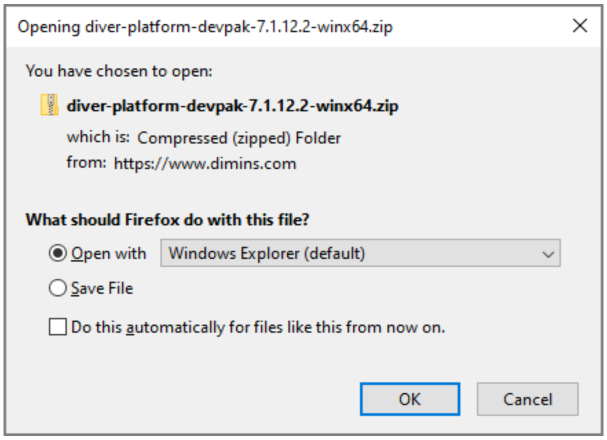
Complete the following steps:

1. On the software and documents download page on DI-Download, locate the latest version of the Diver Platform Developer 7.1 Windows installation package, and click the version number.



Diver Platform Asian Language Pack 7.0 Windows Unicode	7.0.53 (130770KB)	Previous Point Releases	Not Available	Not Available
Diver Platform Developer Pack 7.1 Windows Unicode limited	7.1.12 (387838KB)	Previous Point Releases	Not Available	Not Available
Diver Platform Developer Pack 7.1 Windows	7.1.12 (387820KB)	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 (423764KB)	Previous Point Releases	Release Notes (2402KB)	Manual (8409KB)
Diver Platform Developer Pack 7.0 Windows	7.0.53 (423746KB)	Previous Point Releases	Release Notes (2402KB)	Manual (8409KB)

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


Opening diver-platform-devpak-7.1.12.2-winx64.zip

You have chosen to open:

diver-platform-devpak-7.1.12.2-winx64.zip

which is: Compressed (zipped) Folder
from: https://www.dimins.com

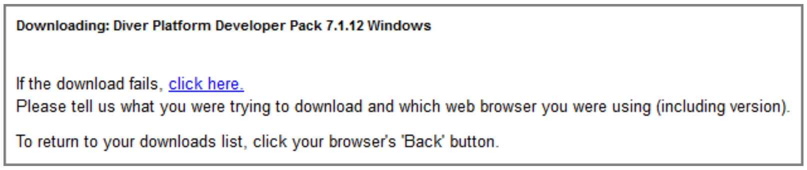
What should Firefox do with this file?

● Open with Windows Explorer (default)

○ Save File

□ Do this automatically for files like this from now on.

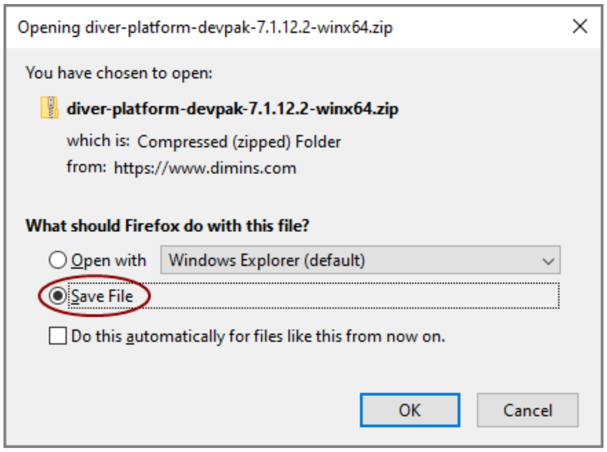
The **Downloading** page opens in the browser. If the **Opening** dialog does not open automatically, follow the instructions on the page.


Downloading: Diver Platform Developer Pack 7.1.12 Windows

If the download fails, click here.
Please tell us what you were trying to download and which web browser you were using (including version).

To return to your downloads list, click your browser's 'Back' button.

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


Opening diver-platform-devpak-7.1.12.2-winx64.zip

You have chosen to open:

diver-platform-devpak-7.1.12.2-winx64.zip

which is: Compressed (zipped) Folder
from: https://www.dimins.com

What should Firefox do with this file?

○ Open with Windows Explorer (default)

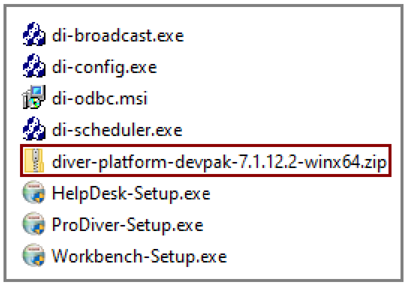
● Save File

□ Do this automatically for files like this from now on.

The Diver Platform Developer 7.1 software package is saved to the **Downloads** directory on your local computer.

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

The following executable files are extracted to the directory:



di-broadcast.exe
di-config.exe
di-odbc.msi
di-scheduler.exe
diver-platform-devpak-7.1.12.2-winx64.zip
HelpDesk-Setup.exe
ProDiver-Setup.exe
Workbench-Setup.exe

Installing ProDiver

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

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

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

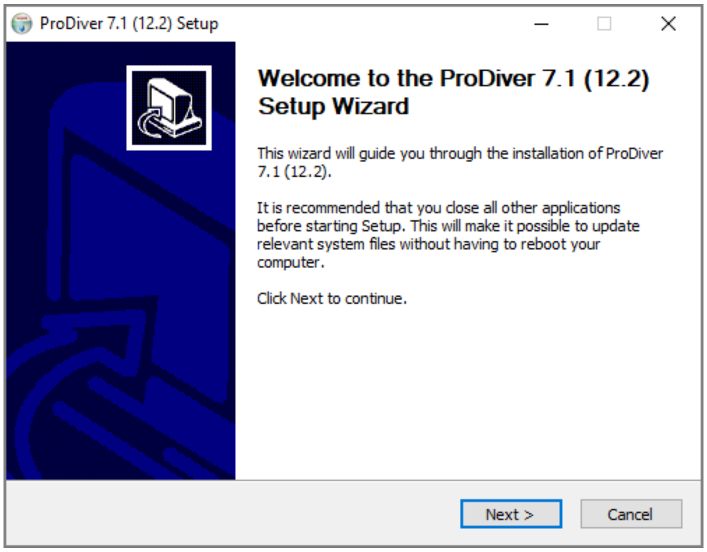
To install ProDiver:

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

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

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

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



ProDiver 7.1 (12.2) Setup

Welcome to the ProDiver 7.1 (12.2) Setup Wizard

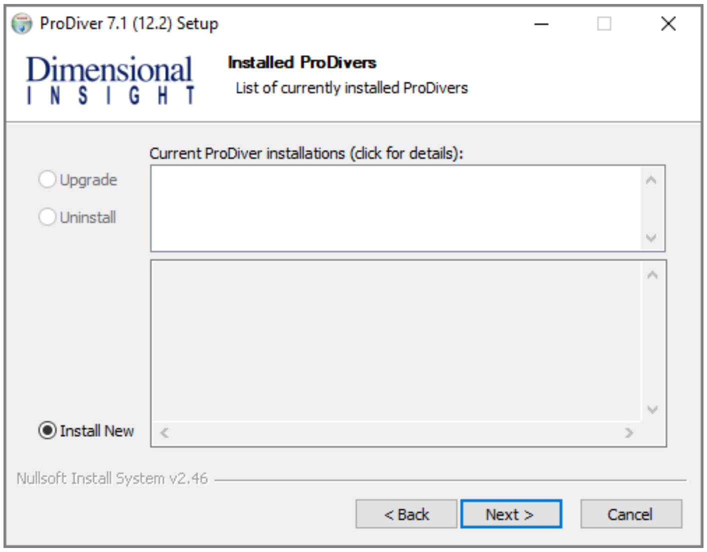
This wizard will guide you through the installation of ProDiver 7.1 (12.2).

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

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

   The **Installed ProDivers** page displays.



ProDiver 7.1 (12.2) Setup

Installed ProDivers

List of currently installed ProDivers

Current ProDiver installations (click for details):

○ Upgrade

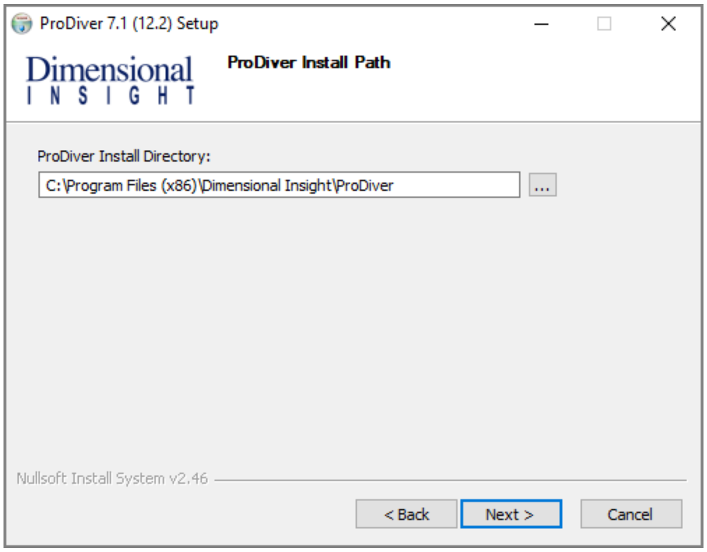
○ Uninstall

● Install New

Nullsoft Install System v2.46

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

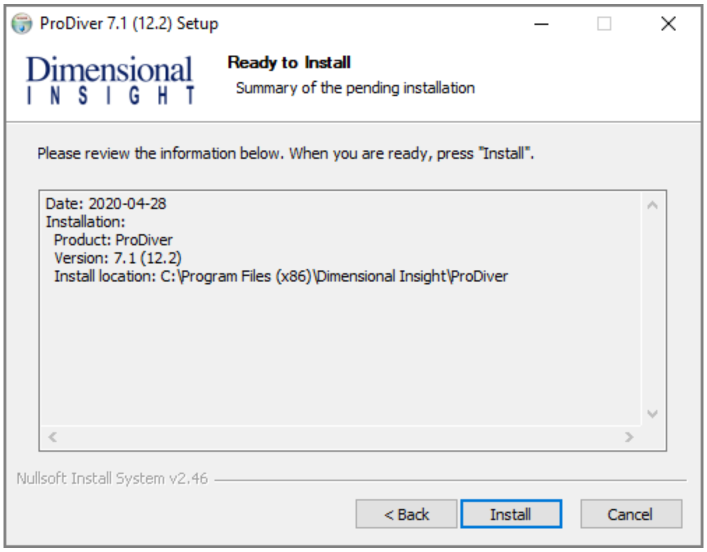
The **ProDiver Install Path** page displays the default installation path. For example, `C:\Program Files (x86)\Dimensional Insight\ProDiver`. Make changes if necessary.



ProDiver Install Directory: C:\Program Files (x86)\Dimensional Insight\ProDiver

7. Click **Next**.

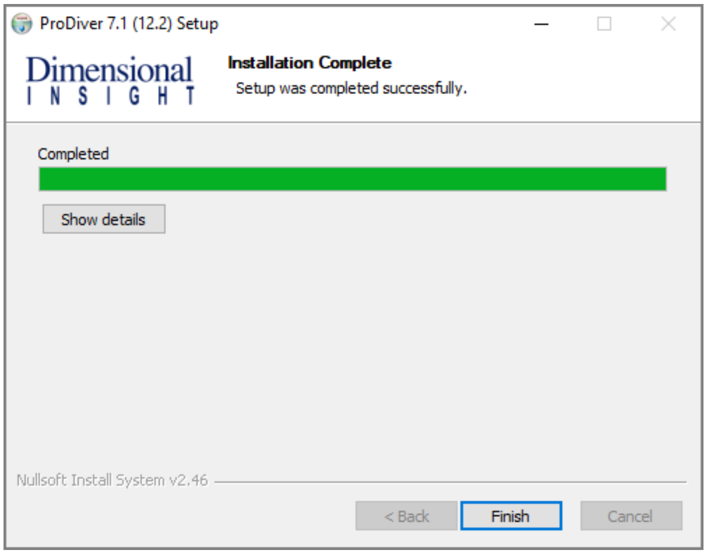
   The **Ready to Install** page displays a summary of the pending installation.


ProDiver 7.1 (12.2) Setup
Dimensional INSIGHT
Ready to Install
Summary of the pending installation
Nullsoft Install System v2.46
< Back
Install
Cancel

Please review the information below. When you are ready, press "Install".

```
Date: 2020-04-28
Installation:
  Product: ProDiver
  Version: 7.1 (12.2)
  Install location: C:\Program Files (x86)\Dimensional Insight\ProDiver
```

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


ProDiver 7.1 (12.2) Setup

Installation Complete

Setup was completed successfully.

Completed

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

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

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

ProDiver Installation Silent Option

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

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

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

The following options can be used for more control.

Option	Description
/mode=	Indicates the action for the installer. Values are: • `install` • `upgrade` • `uninstall` • `list` If there are no existing installations, the installer defaults to doing a new install. If there is one existing installation, the installer defaults to doing an upgrade. If there are multiple installations, there is no default mode—to perform an upgrade or uninstall, you must specify the installation. Use the list option to see existing installations.
/path=	Indicates the target location. The default value for the path is: `"C:\DI\Solution\executables\prodiver"` The installer writes a log file called *installation.log* to the user-specified or default path with information about the installation.
/installation=	On computers with multiple installations, indicates which installation to upgrade or uninstall. The format used is that of the GUI installer (for example "ProDiver-2019-02-26-17-41-29").

NOTE: When output is sent to the console to display a list of errors encountered when running, you might be prompted to press **Enter** to continue. If the message does not indicate that the installer has completed, the process might still be running in the background. If you need to perform other tasks, use a separate command window.

Examples:

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

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

That installation can be upgraded using the same command line:

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

A new installation to a non-standard path:

```
ProDiver-Setup.exe /S /path=c:\di\solution71\executables\prodiver71
```

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

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

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

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

To see a list of installed versions:

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

An upgrade to a particular version:

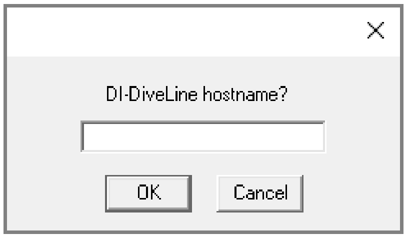
```
ProDiver-Setup.exe /S /mode=upgrade /installation=ProDiver-2019-
0804-12-58-26
```

Verifying the ProDiver Installation

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

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

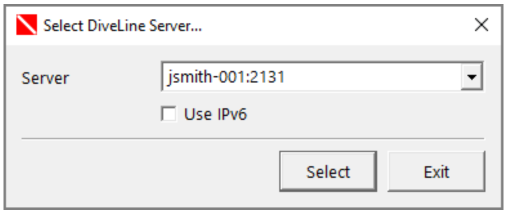
   The **DI-DiveLine hostname** dialog box opens.

   DI-DiveLine hostname?

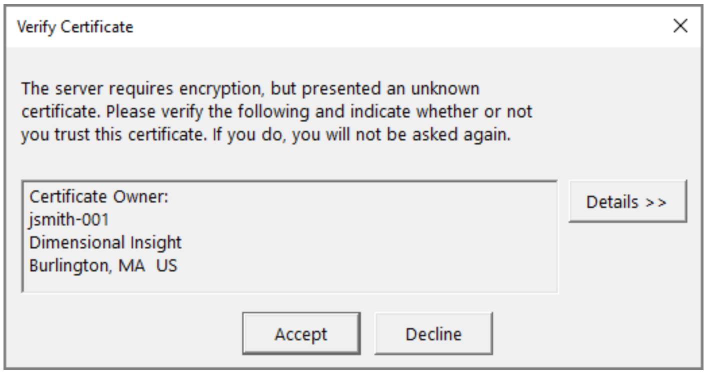
   NOTE: If you used ProDiver to check the DiveLine installation, this is not the initial use of ProDiver. The **DiveLine Login** dialog box opens directly. Skip to **Step 6**.
3. If you are using the default port number 2130, enter **<server>**. If you are using another port number, enter **<server>:<port number>**. For example, **jsmith-001:2131**.

   If the connection fails, the **Select DiveLine Server** dialog box opens. If successful, skip to **Step 6**.
4. Enter or select the name of the server and click **Select**.



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

The **Verify Certificate** window opens.

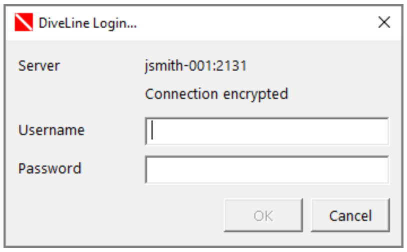


The server requires encryption, but presented an unknown certificate. Please verify the following and indicate whether or not you trust this certificate. If you do, you will not be asked again.

Certificate Owner:
jsmith-001
Dimensional Insight
Burlington, MA US

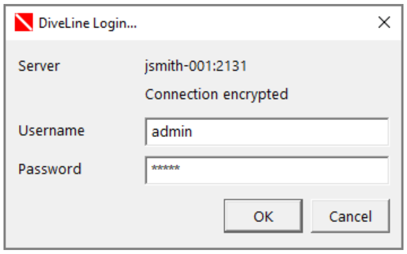
5. Review the certificate, and click **Accept**.

   The **DiveLine Login** dialog box opens.



Server jsmith-001:2131
Connection encrypted

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



Server jsmith-001:2131

Connection encrypted

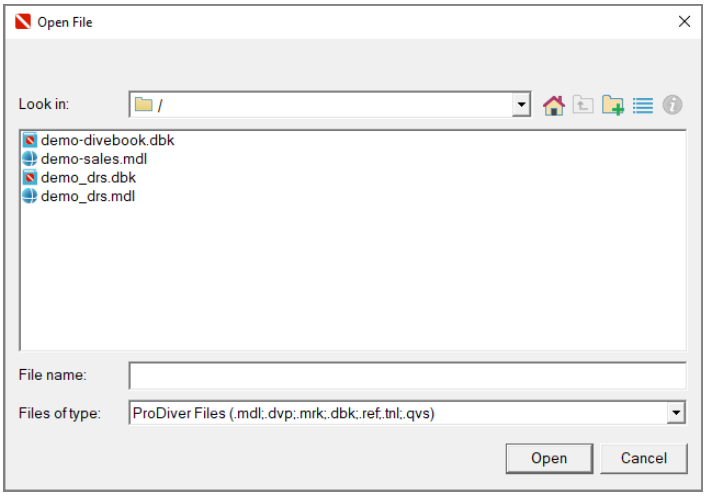
Username admin

Password *****

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

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

   NOTE: Your display might contain different files.



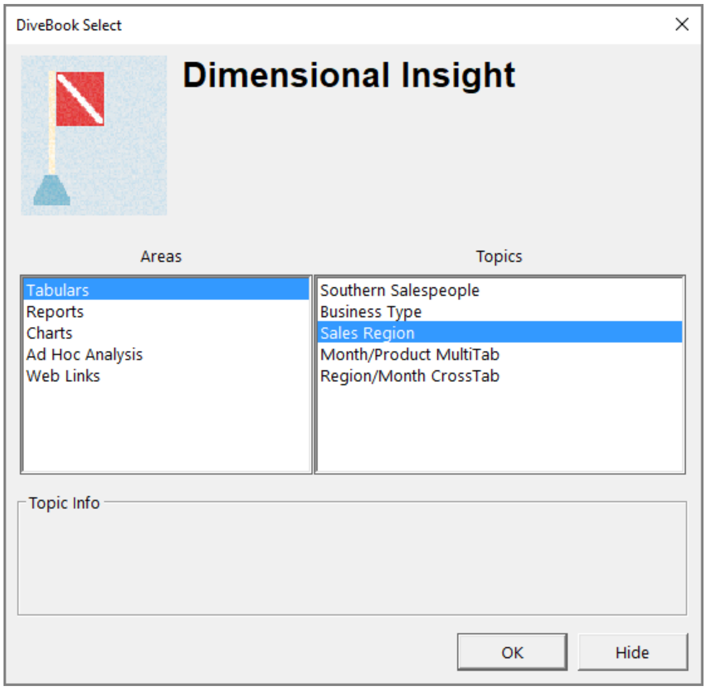
Look in: /

- demo-divebook.dbk
- demo-sales.mdl
- demo_drs.dbk
- demo_drs.mdl

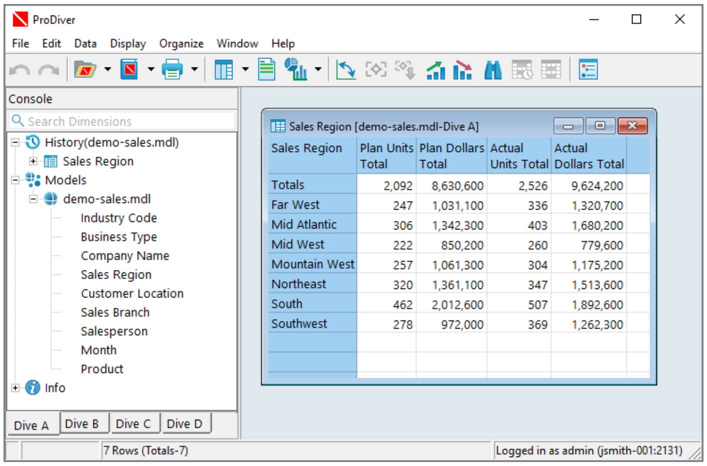
File name:

Files of type: ProDiver Files (.mdl;.dvp;.mrk;.dbk;.ref;.tnl;.qvs)

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



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

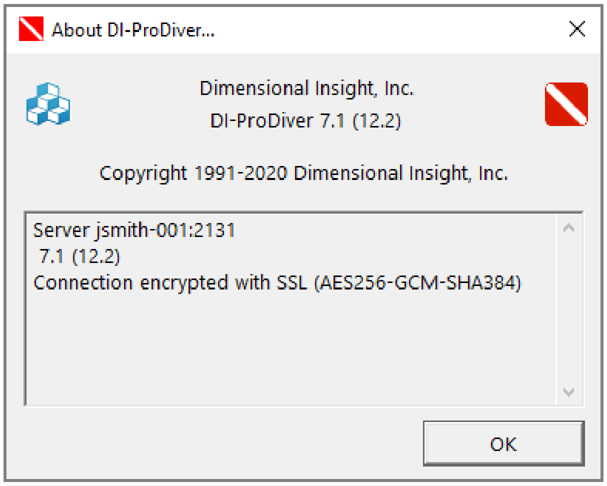


Sales Region	Plan Units Total	Plan Dollars Total	Actual Units Total	Actual Dollars Total
Totals	2,092	8,630,600	2,526	9,624,200
Far West	247	1,031,100	336	1,320,700
Mid Atlantic	306	1,342,300	403	1,680,200
Mid West	222	850,200	260	779,600
Mountain West	257	1,061,300	304	1,175,200
Northeast	320	1,361,100	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-001:2131)

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



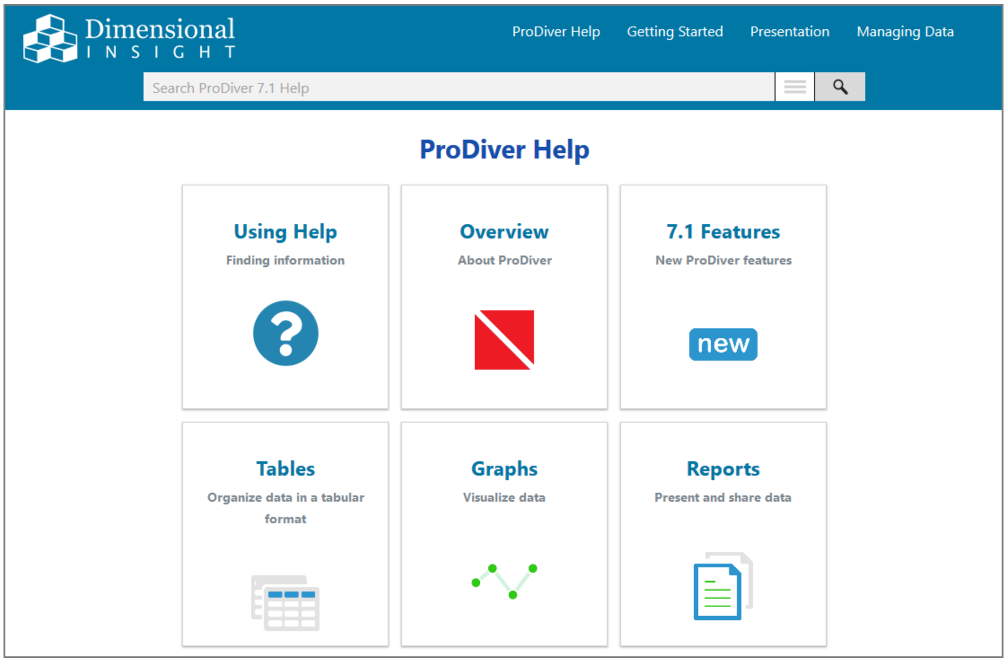
About DI-ProDiver...

Dimensional Insight, Inc.
DI-ProDiver 7.1 (12.2)

Copyright 1991-2020 Dimensional Insight, Inc.

```
Server jsmith-001:2131
 7.1 (12.2)
Connection encrypted with SSL (AES256-GCM-SHA384)
```

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



Installing Workbench

Workbench is an integrated development environment (IDE), designed to simplify and speed up development of applications to model your data. With Workbench on your desktop, you can manage projects on the server, and test and visually examine your data flows and processes. In addition, Workbench provides one point of entry for all your Diver data servers, consolidating the tasks of developing, testing, and managing multiple data projects.

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

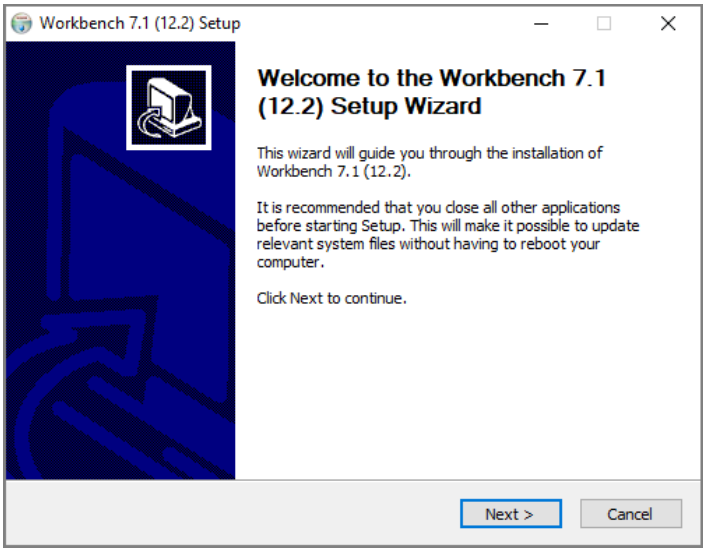
Complete the following steps:

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

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

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

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



Welcome to the Workbench 7.1 (12.2) Setup Wizard

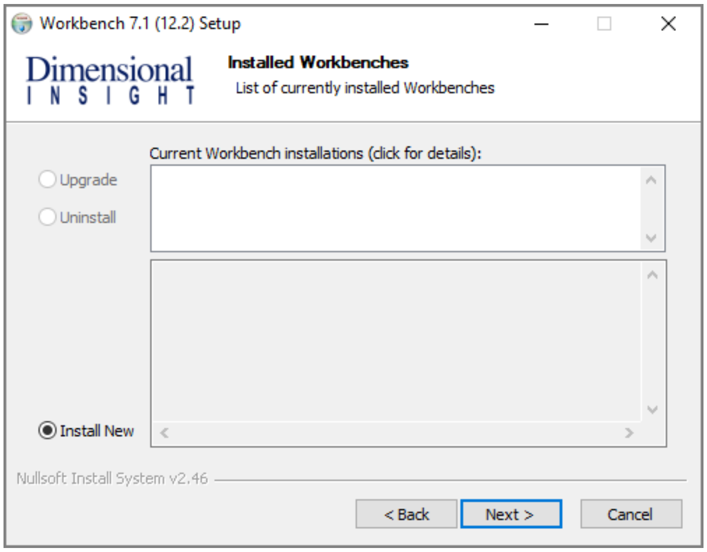
This wizard will guide you through the installation of Workbench 7.1 (12.2).

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

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

   The **Installed Workbenches** page opens.



Workbench 7.1 (12.2) Setup

Installed Workbenches

List of currently installed Workbenches

Current Workbench installations (click for details):

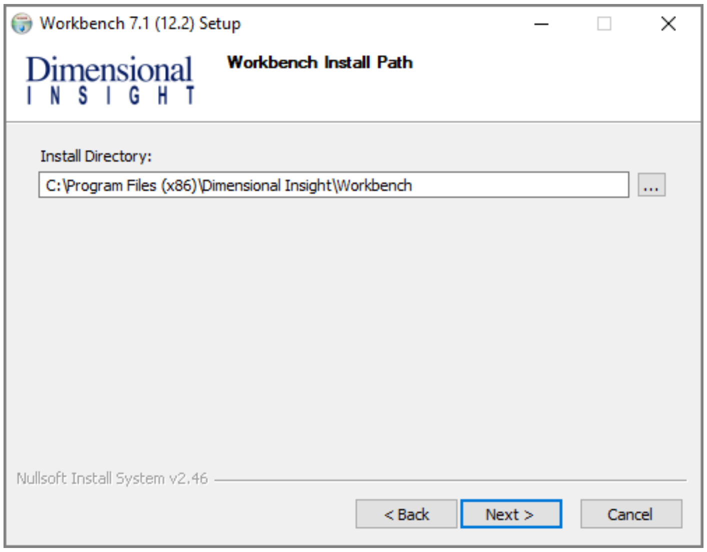
○ Upgrade

○ Uninstall

● Install New

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

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



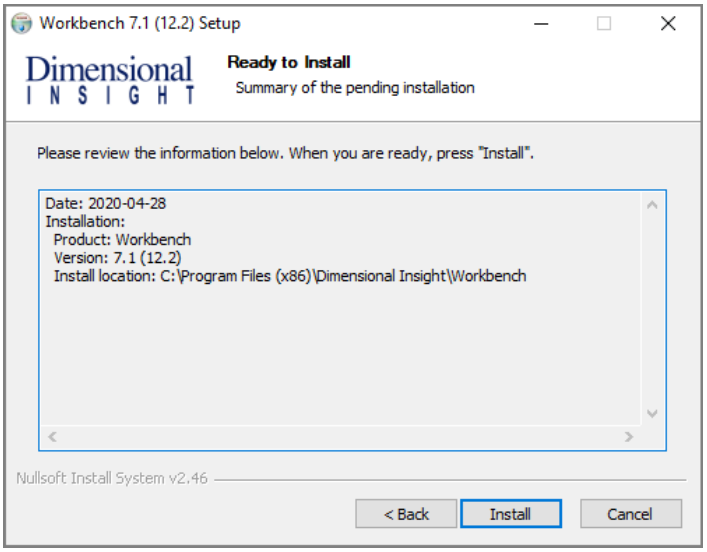
Workbench 7.1 (12.2) Setup

Workbench Install Path

Install Directory: C:\Program Files (x86)\Dimensional Insight\Workbench

7. Click **Next**.

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

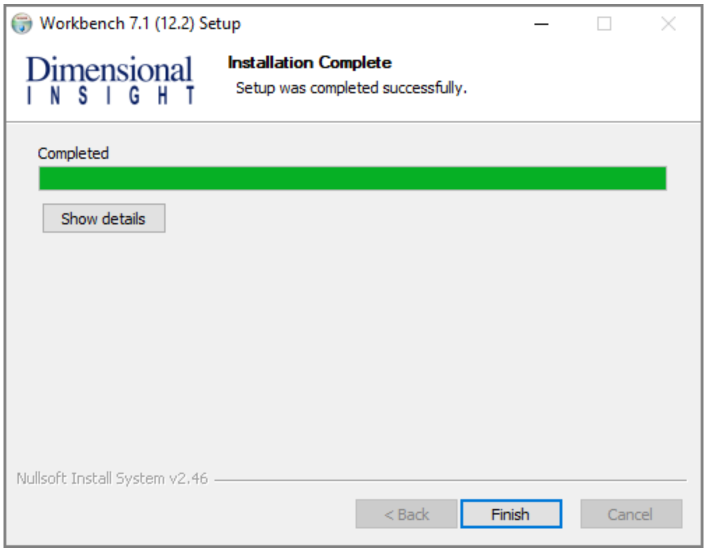


Workbench 7.1 (12.2) Setup
Dimensional INSIGHT
Ready to Install
Summary of the pending installation
Nullsoft Install System v2.46
< Back
Install
Cancel

Please review the information below. When you are ready, press "Install".

```
Date: 2020-04-28
Installation:
  Product: Workbench
  Version: 7.1 (12.2)
  Install location: C:\Program Files (x86)\Dimensional Insight\Workbench
```

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



Workbench 7.1 (12.2) Setup
Dimensional INSIGHT
Installation Complete
Setup was completed successfully.
Completed
Show details
Nullsoft Install System v2.46
< Back
Finish
Cancel

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

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

NOTE: The Workbench installer, starting with version 7.1(12), enables TLS 1.2 on Windows 7 if it was not explicitly disabled by the user.

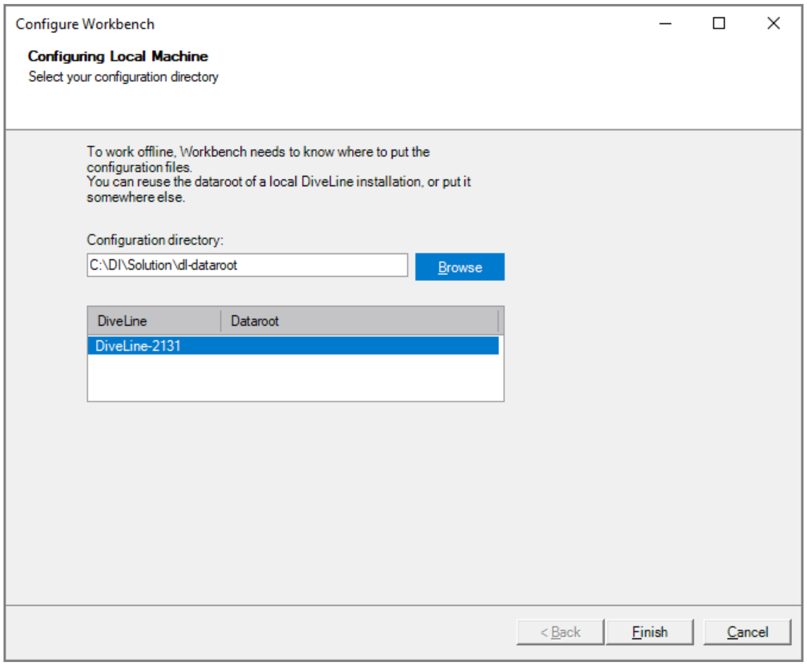
Verifying the Workbench Installation

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

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

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

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



Configure Workbench

Configuring Local Machine

Select your configuration directory

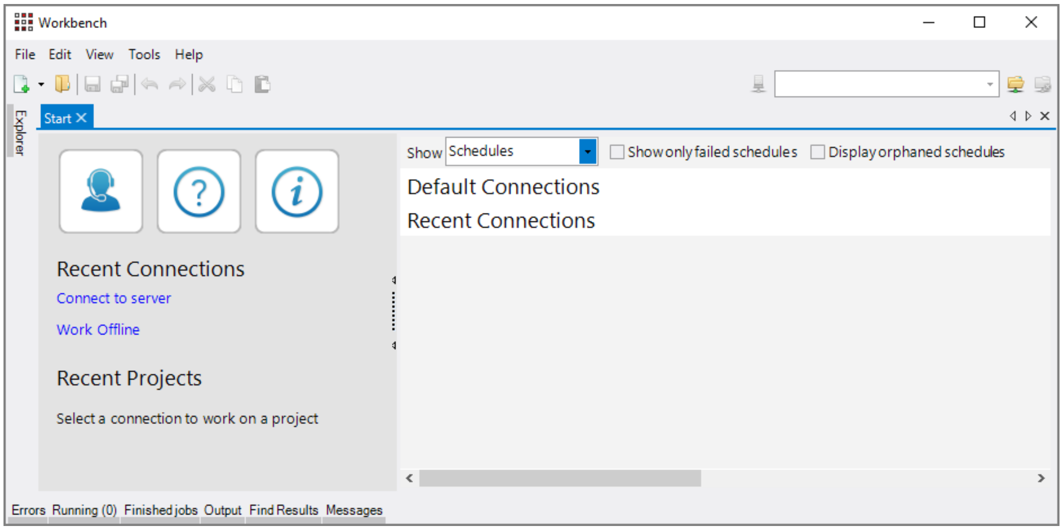
To work offline, Workbench needs to know where to put the configuration files.
You can reuse the dataroot of a local DiveLine installation, or put it somewhere else.

Configuration directory:

C:\DI\Solution\dl-dataroot

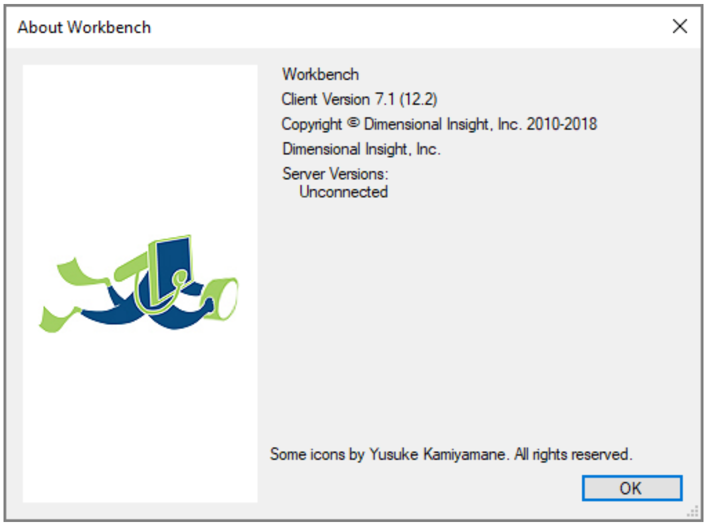
DiveLine	Dataroot
DiveLine-2131	

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


Workbench
File Edit View Tools Help
Explorer
Start
Show Schedules
□ Show only failed schedules □ Display orphaned schedules
Default Connections
Recent Connections
Recent Connections
Connect to server
Work Offline
Recent Projects
Errors Running (0) Finished jobs Output Find Results Messages

Select a connection to work on a project

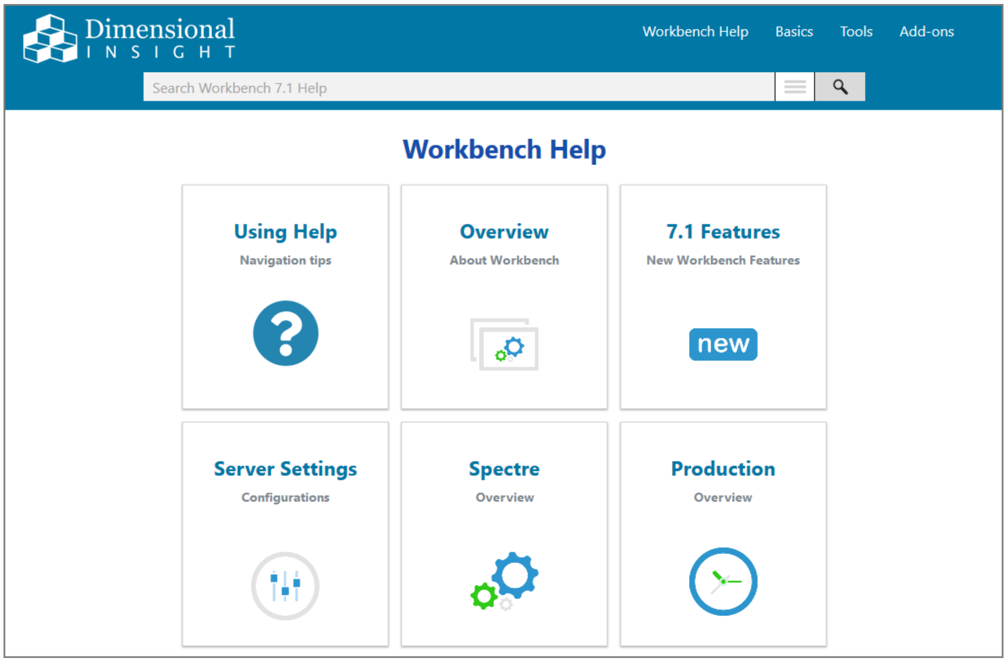
4. To view the Workbench version number, click **Help** > **About Workbench**. Confirm the version, and click **OK**.



Workbench
Client Version 7.1 (12.2)
Copyright © Dimensional Insight, Inc. 2010-2018
Dimensional Insight, Inc.
Server Versions:
Unconnected

Some icons by Yusuke Kamiyamane. All rights reserved.

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



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