



You are viewing content for Planview Hub version 22.4. [View another version](#) ▼



On This Page

Beginning in May 2024 (Planview Hub version 24.2), support for the MySQL database will be dropped and extended support for operational databases will be ended. If using a MySQL database, a migration procedure will be provided to move to a supported database.

If you have any questions, please contact customer care.

General Requirements

Planview Hub is a web application which runs centrally on a server. Users interact with it through a web browser from any computer that has network access to the server.

For best results, Hub should be deployed in an environment that has good network throughput and low latency to its operational databases and all repositories involved in an integration.

Below are general requirements to meet the needs of typical deployment scenarios.

- Hub **must** be installed in a server environment and only **one** instance of Hub should be installed on each server.
- The Hub operational database should have its own machine and should be co-located with the Hub server to reduce latency.

Note: TLS 1.2 is required for all encrypted connections. The database used for storing Hub operational data and any repositories being used must support TLS 1.2

User Requirements

To install and configure Hub, you need an account with administrative privileges on your server. The account must also have read/write access to the default file locations.

Supported Operating Systems

Note: For Windows, Powershell 4 must be installed on your server.

The following 64-bit operating systems and versions are supported:

- Windows 10
- Windows 11
- Windows Server 2019
- Windows Server 2022
- Oracle Enterprise Linux 7+
- Oracle Enterprise Linux 8+
- Red Hat Enterprise Linux 8.x
- Ubuntu Linux 18.04 LTS
- Ubuntu Linux 20.04 LTS
- Ubuntu Linux 22.04 LTS
- SUSE Linux Enterprise Server 12.x
- SUSE Linux Enterprise Server 15.x

Available under Extended support:

- Windows Server 2016 (*End-of-Service-Life Date: January 18, 2023*)
- Red Hat Enterprise Linux 7.x (*End-of-Service-Life Date: January 18, 2023*)
- Ubuntu Linux 16.04 LTS (*End-of-Service-Life Date: January 18, 2023*)

Note: Certain connectors (e.g., IBM DOORS) only run on Windows operating systems. Before installing Planview Hub, we recommend consulting with your customer care to determine which operating system best fits your integration scenario.

Supported Browsers

Note: Planview Hub runs with a minimum screen resolution of **1280 pixels x 800 pixels**.

The Planview Hub web interface is supported on the following browsers:

- Firefox 111+
- Google Chrome 111+
- Microsoft Edge 111+

Available under Extended Support:

- Firefox 101 (*End-of-Service-Life Date: January 17, 2024*)
- Google Chrome 102-105 (*End-of-Service-Life Date: January 17, 2024*)
- Microsoft Edge 102-105 (*End-of-Service-Life Date: January 17, 2024*)
- Firefox 102 (*End-of-Service-Life Date: March 14, 2024*)
- Google Chrome 106+ (*End-of-Service-Life Date: March 17, 2024*)
- Microsoft Edge 106+ (*End-of-Service-Life Date: March 17, 2024*)

If you are interested in extended support, please reach out to customer care.

Supported Databases for storing Hub Operational Data

Planview automatically stores operational data to a pre-configured Derby database. This is suitable for evaluation purposes *only*, and is not supported for production environments. Configuring Hub to utilize an external database enables you to perform frequent back-ups without stopping Hub, and ensures that your Hub practices are consistent with your existing disaster and recovery process.

Note: The database used for Hub operational data must support **TLS 1.2**.

To reduce latency, the Hub operational database should have its own machine and should be co-located with the Hub server.

Minimal User Permissions

For all supported databases, the user **must** have sufficient permissions to connect, create, alter and drop tables and indexes and create temporary tables. Users must also have sufficient permissions to select, insert, update, delete, and truncate tables.

to select, insert, update, delete, and truncate tables.

Hub supports this operational database policy for scenarios where your database is on **any** cloud infrastructure like AWS or Azure. You can refer to the resources below for more information on encrypting communication between Hub and Database:

- For AWS, we recommend implementing a VPC. Click [here](#) for more information.
- For Azure, we recommend a VPN gateway. Click [here](#) for more information.

Note: A separate database must be used for Hub Operational Data and Enterprise Data Stream integrations.

Operational Database Recommendations

The recommendations below offer a **general guideline** only. We recommend consulting with customer care to determine the exact needs for your integration scenario, and for guidance on how to efficiently configure Hub.

You can see [guidelines regarding external database sizing here](#).

We strongly recommend using the latest supported version of **PostgreSQL** for storing Hub Operational Data. At scale, Hub performs better, more reliably, and requires fewer resources with PostgreSQL than with the other available database options.

Supported Versions and Configuration Details

In the sections below, you will find supported database versions for storing Hub Operational Data and configuration details for each database.

PostgreSQL

[Supported Versions](#)

- 11
- 12
- 13
- 14
- 15

[Extended Support](#)

- 10 (End-of-Service-Life Date: July 31, 2024)

If you are interested in extended support, please reach out to [customer care](#).

[Configuration Settings](#)

- The database must be case-sensitive (this is the default configuration).
- The database must be configured with the **UTF8** character set.

```
CREATE DATABASE tasktop_hub
ENCODING 'UTF8'
LC_COLLATE = 'en_US.UTF-8'
LC_CTYPE = 'en_US.UTF-8'
TEMPLATE template0
```

[Necessary User Permissions](#)

The following provides sufficient permissions for the `tasktop_hub` user on the `tasktop_hub` database, when using a [public](#) schema:

```
CREATE USER tasktop_hub;

REVOKE ALL PRIVILEGES ON DATABASE tasktop_hub
FROM tasktop_hub;

GRANT CONNECT, TEMP ON DATABASE tasktop_hub
TO tasktop_hub;

GRANT CREATE ON SCHEMA public
TO tasktop_hub;

GRANT SELECT, INSERT, UPDATE, DELETE, TRUNCATE
ON ALL TABLES IN SCHEMA public
TO tasktop_hub;
```

The following provides sufficient permissions for the `tasktop_hub` user on the `tasktop_hub` database, when using a [custom](#) schema:

Note: If you use a custom schema, please note that when configuring the external database connection you will need to add `?currentSchema=tasktop` to the database connection URL, e.g. `jdbc:postgresql://example.com:5432/dbName?currentSchema=tasktop`

```
CREATE USER tasktop_hub;

\connect tasktop_hub;

CREATE SCHEMA TASKTOP;

REVOKE ALL PRIVILEGES ON DATABASE tasktop_hub
FROM tasktop_hub;

GRANT CONNECT, TEMP ON DATABASE tasktop_hub
TO tasktop_hub;

GRANT CREATE ON SCHEMA Tasktop
TO tasktop_hub;

GRANT SELECT, INSERT, UPDATE, DELETE, TRUNCATE
ON ALL TABLES IN SCHEMA Tasktop
TO tasktop_hub;
```

Microsoft SQL Server

[Supported Versions](#)

- 2019

[Extended Support](#)

- 2017 (End-of-Service-Life Date: July 31, 2024)

[Configuration Settings](#)

- The database must be case sensitive. We recommend Latin1_General_100_CS_AS_KS_WS.

- This can be configured using the following command (replace **dbName** with the name of your database):

```
ALTER DATABASE dbName COLLATE Latin1_General_100_CS_AS_KS_WS;
```

- We recommend monitoring the size of your transaction log, as very large transaction logs can cause database connection errors.
- We recommend using JDBC driver `mssql-jdbc-7.0.0.jre8.jar` when transferring from operational database to SQL Server.

Necessary User Permissions

- The user must be a SQL authenticated user (not a Windows authenticated user)
- Additionally, the user must have the following roles granted:
 - `db_datareader`
 - `db_datawriter`
 - `db_ddladmin`

Note: Instance and Database name options can be specified by attaching `”;instanceName=;databaseName=` to the end of the JDBC URL in Hub. If using JDBC driver `mssql-jdbc-10.2.x` or later, the `”;trustServerCertificate=` parameter and its corresponding value is required by the driver.

Oracle

Supported Versions

- 19c
- 21c

Extended Support

- N/A

If you are interested in extended support, please reach out to customer care.

Configuration Settings

- The database must be case-sensitive (this is the default configuration).
- The database must be configured with the **AL32UTF8** character set.

```
ALTER DATABASE dbName CHARACTER SET AL32UTF8;
```

Necessary User Permissions:

User must have `CREATE SEQUENCE`, `CREATE TABLE`, `CREATE SESSION` permissions, as well as sufficient quota. Typical user creation might look as follows:

```
CREATE USER tasktop_hub IDENTIFIED BY a_password DEFAULT TABLESPACE tasktop_hub;

GRANT CREATE SESSION TO tasktop_hub;

GRANT CREATE SEQUENCE, CREATE TABLE TO tasktop_hub;
ALTER USER tasktop_hub QUOTA UNLIMITED ON tasktop_hub;
```

Troubleshooting

- To resolve error **ORA-30036 (UNABLE TO EXTEND SEGMENT BY 8 IN UNDO TABLESPACE)**, please refer to the following documentation.

MySQL

Supported Versions

- 5.7.7+ (excluding 5.7.0 - 5.7.6) (Enterprise Edition only)
- 8.0 (Enterprise Edition and Community Edition)

Extended Support

- N/A

Configuration Settings

The following settings must be applied before connecting Hub to MySQL:

- The database default charset must be UTF-8, `ALTER DATABASE dbName CHARACTER SET = 'utf8'`
 - You can also create the database with these settings: `CREATE DATABASE dbName CHARACTER SET = 'utf8'`
- `innodb_buffer_pool_size` must be minimum 1G
 - This size is highly dependent on customer hardware and data size — the number above is only a recommendation. Please consult with customer care if you have any questions.
- `max_allowed_packet` property must be minimum 64M
 - If this is set too low, you will see a **Packet for query is too large** error on the Activity screen.
- `max_connections` property should be minimum 500
 - **Note:** The number of connections Hub uses is highly dependent on customer configuration, hardware, and load — the number above is only a recommendation. Please consult with customer care if you have any questions.
- The database must be case sensitive.
 - This can be configured using the following command (replace **dbName** with the name of your database):

```
ALTER DATABASE dbName COLLATE = 'utf8_bin'
```

- We recommend using JDBC driver version 8.0 or later when transferring from an operational database to MySQL Server.
- `innodb_default_row_format` must be `DYNAMIC`
- `innodb_file_format` must be `Barracuda`
- `innodb_file_per_table` must be `ON`
- `innodb_large_prefix` must be `ON`

Note: `innodb` settings are the default settings for MySQL, so you will not need to make any changes to those settings unless they have been changed previously. The `innodb` settings apply globally to all MySQL databases on the server, while the `character set` is specific to the database.

Note: Configuring Hub with the MySQL external operational database will prohibit the synchronization of 4-byte characters due to MySQL's default UTF8 encoding being limited to 3 bytes. Examples of 4-byte characters include but are not limited to some emojis and some Chinese characters. If you may be synchronizing 4-byte characters, consider using another supported database.

Necessary User Permissions

The following provides sufficient permissions for the tasktop_hub user on the tasktop_hub database:

```
REVOKE ALL PRIVILEGES, GRANT OPTION FROM tasktop_hub;  
GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, ALTER, INDEX, LOCK TABLES, REFERENCES ON tasktop_hub.* TO tasktop_hub
```

Supported Databases for use in Enterprise Data Stream Integrations

The Planview Hub Database add-on allows you to create integrations that send artifact information to one central database.

Note: A separate database must be used for Hub Operational Data and Enterprise Data Stream integrations.

You can see guidelines regarding external database sizing [here](#).

Supported Versions

If your license includes the Hub Database add-on and you would like to configure an Enterprise Data Stream Integration, the following databases and versions are supported:

PostgreSQL

General Support

- 11
- 12
- 13
- 14
- 15

Extended Support

- 10 (End-of-Service-Life Date: July 31, 2024)

If you are interested in extended support, please reach out to customer care.

Microsoft SQL Server

General Support

- 2019

Extended Support

- 2017 (End-of-Service-Life Date: July 31, 2024)

Oracle

General Support

- 19c
- 21c

Extended Support

- N/A

We recommend using JDBC driver version 8.0 or later when creating a SQL connection for Enterprise Data Stream integrations.

MySQL

General Support

- 5.7.7+
- 8.0

Extended Support

- N/A

Note: The user must be a SQL authenticated user (and not a Windows authenticated user)

Database Connections and Encryption

The following section describes different ways to configure your database connection. If you choose not to encrypt your connection, data will be transmitted over the network unprotected and will be at risk of being intercepted. Likewise use of self-signed certificates or other certificates not signed by a trusted Certificate Authority puts your data at risk as Hub cannot verify the identity of the server at the end of the connection.

Please ensure your connection is configured in a way that is aligned with your security policy and the associated risks are understood and accepted.

Configuration Details

PostgreSQL

For PostgreSQL, please refer to [PostgreSQL documentation](#) for more information.

Location

- Example Format: `jdbc:postgresql://hostServerName:port/MyDatabaseName`

You can enable encrypted connections by setting 'ssl=true' (e.g., `jdbc:postgresql://<server-name>:<port>/?ssl=true`).

If the certificate for the PostgreSQL server is self-signed you'll need to set 'sslfactory=org.postgresql.ssl.NonValidatingFactory' and 'sslmode=require' (e.g., `jdbc:postgresql://<server-name>:<port>/?ssl=true&sslmode=require&sslfactory=org.postgresql.ssl.NonValidatingFactory`).

If the certificate for the PostgreSQL server is not self-signed you'll need to add the certificate to the JDBC's truststore.

Microsoft SQL Server

For SQL Server, please refer to [Microsoft documentation](#) for more information.

Location

- Example Format: `jdbc:sqlserver://hostServerName;instanceN...MyDatabaseName`

You can enable encrypted connections by setting 'encrypt=true' (e.g., `jdbc:sqlserver://<server-name>;1433;encrypt=true;trustServerCertificate=false`). If the certificate for the MySQL server is self-signed you'll need to set 'trustServerCertificate=true' (e.g., `jdbc:sqlserver://<server-name>;1433;encrypt=true;trustServerCertificate=true`).

If using JDBC driver `msql-jdbc-10.2.x` or later, the "trustServerCertificate=" parameter and its corresponding value is required by the driver.

Note: Some older editions may be missing security updates and will need to apply security service packs to use a self-signed certificate and encryption. You may experience certificate errors if the SQL Server is using a self-signed or corporate certificate. To work around this, you will need to disable certificate validation in the JDBC driver or add the certificate to the JDBC's truststore.

Oracle

For Oracle, please refer to this [whitepaper](#) for an overview of how to set up connections to encrypted Oracle server. For a guide to configuring the Oracle server to support SSL, please refer to [Oracle documentation](#).

Location

- Example Format: `jdbc:oracle:thin:@hostServerName:oracleServerPort/SID`

For the most part assuming that the server is set up properly, you can follow Case#2 in the white paper and simply use a URL with the following format: `jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(PORT=2484)(HOST=<hostname>))(CONNECT_DATA=(SERVICE_NAME=<servicename>)))`. On the server, make sure to disable client authentication by setting 'SSL_CLIENT_AUTHENTICATION=FALSE' in the listener.ora and sqlnet.ora files.

For unencrypted connections, the protocol should be TCP and the port would generally be 1521, but the URL would otherwise be the same. The above example connection string is formatted in the 'Oracle Net connection descriptor' format, but Hub also accepts 'Thin-style service name' connection strings such as `jdbc:oracle:thin:@<hostname>:1521:<servicename>`.

If the certificate for the Oracle server is self-signed, but you still want to use SSL, you will need to follow Case#1 in the white paper. As described in the paper, only anonymous cipher suites are permitted when trying to use SSL without server authentication. You can specify the cipher suites in the sqlnet.ora file on the Oracle server.

Note: Some versions of Oracle do not by default support anonymous cipher suites. Thus, they will need to be imported to the server before enabling them.

MySQL

For MySQL, refer to [MySQL documentation](#) for the details on how to set up your connection.

Location

- Example Format: `jdbc:mysql://hostServerName:mysqlServerPort/MyDatabaseName`

To enable encryption on older MySQL servers (5.6.25 and earlier or 5.7.5 and earlier) you need to set the connection property 'useSSL=true' (e.g., `jdbc:mysql://<server-name>:3306?useSSL=true`). Later versions will implicitly try to connect using an encrypted connection. Regardless of the version, the client will only enforce that the server uses TLS if the property 'requireSSL=true' is set.

If the certificate for the MySQL server is self-signed you will need to set 'verifyServerCertificate=false' (e.g., `jdbc:mysql://<server-name>:3306?useSSL=true&verifyServerCertificate=false`).

Java Runtime Environment

Planview Hub is packaged with a JRE; there is no need to install a JRE separately. Planview Hub uses and ships with Oracle Java.

Note: Partner branded editions of Planview Hub use and ship with **Azul OpenJDK**.

Deploying Hub on a Cloud Environment

To ensure reliable performance, all virtual machines (on-prem and private cloud) **must** meet the requirements listed in the [General Requirements](#) section.

Hub can be deployed in operating systems on physical servers within virtual machines hosted on dedicated on-prem virtual machine hosts. Hub can also be deployed within private cloud deployments, such as AWS or Azure. If deploying on a private cloud environment, Hub and its operational database must be deployed using a full image and not a container, with the exception of AWS RDS PostgreSQL. Hub **cannot** run in containerized deployments (Kubernetes, OpenShift, etc.).

Planview has qualified AWS RDS PostgreSQL deployments for use as the operational database for Hub instances hosted in AWS private cloud environments. Planview does not offer direct support for private cloud hosting infrastructure (i.e., AWS networking and configuration) beyond the operation of Planview's own products within the hosted environment. See the section below for recommended configuration settings.

AWS RDS PostgreSQL Recommendations

The recommendations below offer a **general guideline** only. We recommend consulting with customer care to determine the exact needs for your integration scenario, and for guidance on how to efficiently configure Hub.

Note: Planview does not troubleshoot or maintain AWS RDS PostgreSQL. Please ensure your database is configured in a way that is aligned with your security policy and that the associated risks are understood and accepted.

Setting	Recommended Value
"DBInstanceClass"	"db.t3.small"
"Engine"	"postgres"
"AllocatedStorage"	50
"BackupRetentionPeriod"	30
"MultiAZ"	true
"EngineVersion"	"13.6"
"AutoMinorVersionUpgrade"	false
"PubliclyAccessible"	false
"StorageType"	"gp2"
"StorageEncrypted"	true
"CopyTagsToSnapshot"	true

Hardware Sizing for Deployment Scenarios

General Notes and Considerations

Below are recommendations on sizing hardware and virtual machine capacity to meet the needs of typical deployment scenarios.

These recommendations are guidelines intended to provide a starting point when deciding on hardware allocation for a specific deployment. We recommend monitoring system load including CPU usage, memory pressure and disk queue length, and adjusting the system sizing accordingly.

For best results, Hub should be deployed in an environment that has good network throughput and low latency to all repositories and databases involved in an integration.

Based on real-life metrics, we approximate database sizing at about 40 KB per artifact. For 100,000 artifacts total (including artifacts on both sides of an integration), that equates to about 4 GB of database storage, not including log files, rollback space, etc.

This is a rough estimate, and will depend on customer-specific configuration and usage. For example, artifacts that have hundreds of fields and many large comments will require more space. Likewise, short change detection intervals, frequent full scans, or frequent changes to large numbers of artifacts will require more processing power.

Hub Server Sizing Recommendations

Note: The recommendations below offer a **general guideline** only. The performance needs of Hub integrations depend on how integrations are configured, the specifications of connected end systems, and the volume and type of changes made in the end systems.

Note that it is possible for a deployment to have a low number of integrations and users, but a high number of artifact updates (or vice versa). We recommend consulting with [customer care](#) to

determine the exact sizing needs for your integration scenario, and for guidance on how to efficiently configure Hub.

Small Deployment

A deployment managing up to 20,000 artifacts in up to 100 projects with up to 10,000 updates/month (typically up to 200 active users, and up to 5 integrations).

- 4 GB system memory
- 3 GHz processor, 2 cores
- 50 GB free disk space

Medium Deployment

A deployment managing up to 150,000 artifacts in up to 500 projects with up to 50,000 updates/month (typically up to 1,000 active users, and up to 15 integrations).

- 8 GB system memory
- 2 x 3 GHz processor, 4 cores
- 150 GB free disk space

Large Deployment

A deployment managing up to 1,000,000 artifacts in up to 2000 projects with up to 200,000 updates/month (typically more than 2,000 active users, and 20+ integrations).

- 16 GB system memory
- 4 x 3 GHz processors, 8 cores
- 250 GB free disk space

Extra-Large Deployment

If your deployment exceeds any of the guidelines from the **Large Deployment**, please consult with [customer care](#).

For extra-large deployments, the specific characteristics of the integrations are crucial when determining proper instance sizing. As a result, no general recommendations can be offered for extra-large deployments.

External Database Sizing

The system that the external database is deployed on should also follow the sizing recommendations listed above. For example, the database for a large deployment should run on a separate machine with 16 GB of memory, 8 cores, and 250 GB of disk space.

Java Heap Size

We recommend setting the maximum Java heap size value to 50-75% of your system's memory.

Learn more about setting Java heap size [here](#).



You are viewing content for Planview Hub version 22.4. [View another version](#) ▼



Sandbox Environment

On This Page

It is recommended that you prepare a sandbox environment to test your Planview Hub configuration before deploying it in production.

The sandbox environment should include the following:

- A sandbox server to install Hub on
- Sandbox instances of all repositories you will be integrating
 - These instances should include the same project structure and customizations as your production repositories.
 - These instance should also include a comparable number of artifacts to your production repositories.

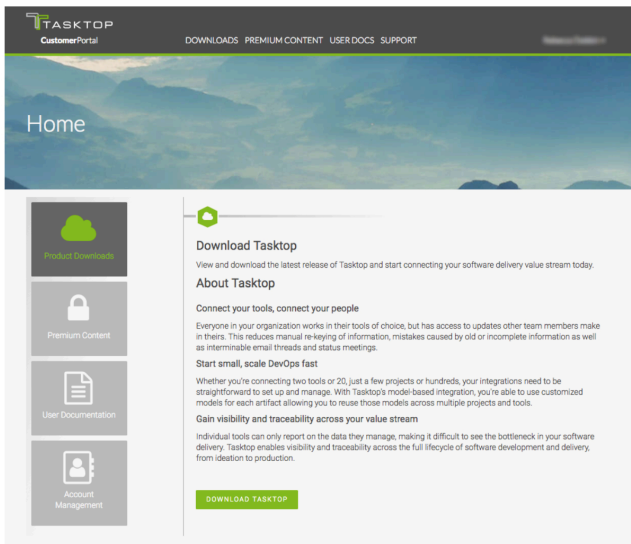
After you have configured Hub on the sandbox server and are satisfied with the way it is running with your sandbox repositories, you can install Hub on your production server and recreate the configuration for your production repositories.

Installation

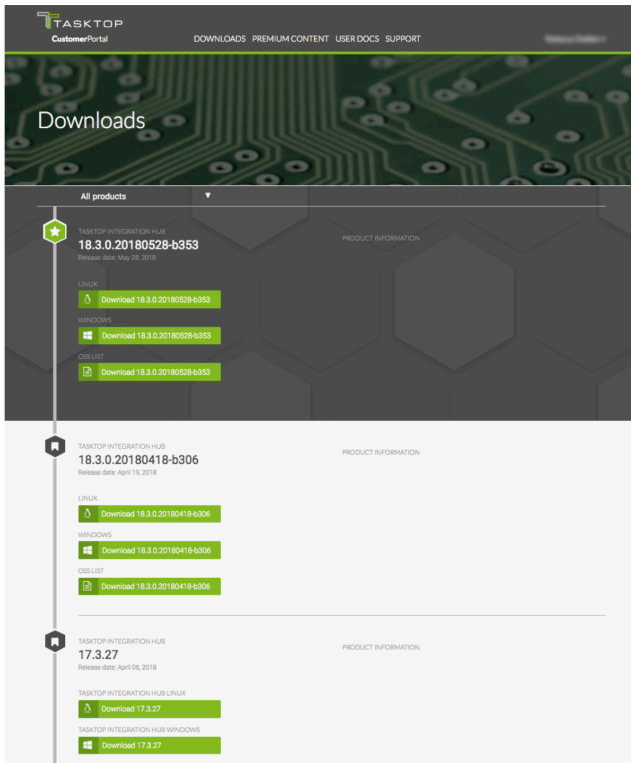
Where to Download Planview Hub

To get the latest version of Planview Hub, create an account on our [Customer Portal](#), then contact your Solutions Architect or customer care.

Once logged in to the Customer Portal, click **Product Downloads**.



This will lead you to the **Downloads** section, where you can download the latest version of Planview Hub.

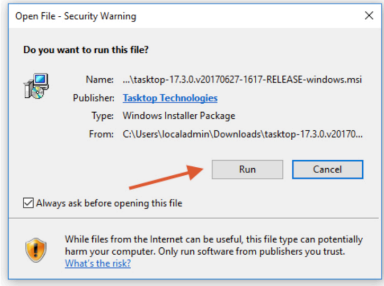


Installation on Windows

Click the **Windows** download link on the **Product Downloads** page of the **Customer Portal**.

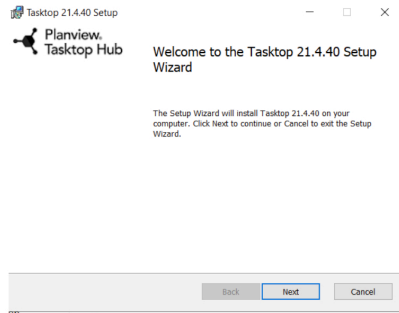
You will be provided with an installation package for Hub as a standard Windows MSI installer.

If prompted, click **Save File** and open the file once downloaded.

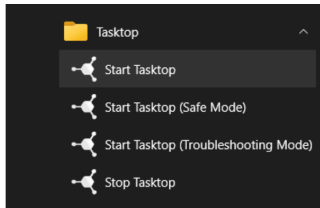


The Setup Wizard will guide you through the installation process.

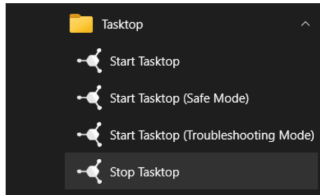
Note: If you decide to change the location of the ProgramData directory, do **not** include spaces in the new directory name. If the directory includes spaces, Hub's UI will **not** be accessible.



After installing Hub, open the **Start** menu and click **Start Tasktop** to start both Hub and User Management services.



To stop both Hub and User Management services, click **Stop Tasktop**.



Note: The Planview Hub application is available via HTTPS on port 8443. A default SSL certificate is provided for testing purposes, however this SSL certificate is insecure. **Before using in a production environment, the provided SSL certificate must be replaced.** Please see details in the [SSL Certificate Installation](#) section below.

Please follow the steps in the [Getting Started](#) section when starting Hub for the first time.

Powershell

Planview Hub supports Windows environments that require PowerShell scripts to be signed, but Tasktop must be added to the Trusted Publishers store to run on such environments. To do this, see the steps below.

1. Install the latest version of Hub on the machine.
2. Log in as the user that will be used to run Hub.
3. Run PowerShell as administrator and navigate to `C:\Program Files\Tasktop\container\bin\setenv.ps1`
4. Type 'A' and press enter.

Alternatively, PowerShell commands can be used to add Tasktop to the Trusted Publishers store for the entire machine.

Note that the following commands can be run by any user once Hub is installed and must be entered into a PowerShell terminal and not run as a PowerShell script.

```
$Cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$Cert.Import((((Get-AuthenticodeSignature "C:\Program Files\Tasktop\container\bin\setenv.ps1").SignerCertificate).Export([System.Security.Crypt
$store = Get-Item "cert:\LocalMachine\TrustedPublisher"
$store.Open([System.Security.Cryptography.X509Certificates.OpenFlags] "ReadWrite")
$store.Add($Cert)
$store.Close()
```

Installation on Linux

For Direct Customers

Click the **Linux** download link on the **Product Downloads** page of the **Customer Portal**.

You will be provided with an installation package for Hub as a `.tar.gz` archive.

To extract this archive to your desired location, copy the archive to the correct location on your Linux system.

You must choose a location with `no spaces` in its path and use the following command to extract:

You must choose a location with **no spaces** in its path and use the following command to extract.

```
$ tar -xzf tasktop-linux-x64-<version>.tar.gz
```

After extracting, run the `start-tasktop.sh` script from the installation directory (see note on permissions below) to start Hub and User Management services.

To stop Tasktop and User Management services, use the `stop-tasktop.sh` script in the same folder.

Please follow the steps in the [Getting Started](#) section when starting Hub for the first time.

For OEM Customers

You will be provided with a `.bin` installation package for Hub.

To execute the file, run these commands:

```
chmod +x tasktop-linux-x64.bin
```

```
./tasktop-linux-x64.bin
```

After approving the End User License Agreement, the file will automatically unzip, allowing you to run Hub.

Run the `start-tasktop.sh` script from the installation directory (see note on permissions below) to start Tasktop and Keycloak User Management services.

To stop Tasktop and User Management services, use the `stop-tasktop.sh` script in the same folder.

Note: The Tasktop application is available via HTTPS on port 8443. A default SSL certificate is provided for testing purposes, however this SSL certificate is insecure. **Before using in a production environment, the provided SSL certificate must be replaced.** Please see details in the [SSL Certificate Installation](#) section below.

Please follow the steps in the [Getting Started](#) section when starting Planview Hub for the first time.

Note on Permissions

We recommend creating a dedicated user for running Planview Hub. We do **not** recommend running Planview Hub as root, as it may create files that cannot be accessed when running Hub as another user. Running an application on a Linux system as root may also interfere with your system's security.

For this reason, `start-tasktop.sh` will not start if it detects the current user is root.

If you would like to run Planview Hub as root despite these risks, you can do so by deleting or commenting lines 3-7 of `call-catalina.sh` in the installation directory as shown below:

```
#!/bin/sh
# if [ "$id -u" -eq "0" ]
# then
#   echo "Tasktop should not be run as root"
#   exit 1
# fi
```

Planview Hub Service on Linux

There are several ways to configure a Planview Hub Service that starts automatically on system startup. We recommend using a dedicated account for running Planview Hub.

You can see the examples below for **Systemd** and **SysVinit**.

Planview Hub Service with Systemd

- Paste the following into the file:

```
# Systemd unit file for tasktop
[Unit]
Description=Tasktop Hub
After=syslog.target network.target

[Service]
Type=forking

ExecStart=/path/to/tasktop/start-tasktop.sh
ExecStop=/path/to/tasktop/stop-tasktop.sh

User=user
Group=group

[Install]
WantedBy=multi-user.target
```

- Change both instances of `/path/to/tasktop` to the full path to your Planview Hub installation directory
- Change the User and Group variables to the username and group of the account you want to run the Hub service

- Reload Systemd

```
$ systemctl daemon-reload
```

1. Navigate to `/etc/systemd/system`
2. Create a file named `tasktop.service`
3. Enable the new Planview Hub service to start on system startup

```
$ systemctl enable tasktop
```

To manually start and stop the Planview Hub Service, use the following commands:

```
$ systemctl start tasktop
$ systemctl stop tasktop
```

Planview Hub Service with SysVinit

- Paste the following into the file:

```
#!/bin/bash
# description: Tasktop Start Stop Restart
# processname: tasktop
# chkconfig: 2345 20 80
TASKTOP_HOME=/path/to/tasktop
case $1 in
start)
sh $TASKTOP_HOME/start-tasktop.sh
;;
stop)
sh $TASKTOP_HOME/stop-tasktop.sh
;;
*)
;
```

```
restart)
sh $TASKTOP_HOME/stop-tasktop.sh
sh $TASKTOP_HOME/start-tasktop.sh
;;
esac
exit 0
```

- Change the TASKTOP_HOME variable to the full path to your Planview Hub installation directory
- If you'd like, you can change the chkconfig run levels and start and stop priorities

- Set the permissions of Hub to make it executable:

```
$ chmod 755 tasktop
```

- Navigate to /etc/init.d
- Create a file named tasktop
- Use the chkconfig utility to enable Planview Hub start at system startup

```
$ chkconfig --add tasktop
$ chkconfig --level 2345 tasktop on
```

- If you'd like, you can change the run levels in this command

To manually start and stop the Planview Hub Service, use the following commands:

```
$ service tasktop start
$ service tasktop stop
$ service tasktop restart
```

Externalized Configuration

Planview Hub enables you to externalize configurations from Tomcat, Jboss/Keycloak, and certain application properties in a single place. This allows you to use property files to override default values such as:

- Jboss:** ports (e.g., http, https, management port), Keycloak database paths, Keycloak trust stores, java memory variables, and custom system properties
- Tomcat:** ports (e.g., http https), keystores (e.g., files, passwords, types), java memory variables, and custom system properties
- Application Properties:** Derby, Tasktop Hub, Liquibase, log4j, and keycloak host

To override default values through a properties file, you must provide the tasktop-hub.properties file in a directory that Hub can scan and read.

This can be done as follows:

- Rename the file tasktop-hub.properties.default to tasktop-hub.properties.
 - For **Windows**, this file can be found in the **App Data Directory**.
 - For **Linux**, this file can be found in the root level of the .tar.gz package.
 - Note:** For Linux users, we recommend creating an environment variable named TASKTOP_HOME with its value pointing to an exclusive directory where the tasktop-hub.properties file will be placed.
- Provide values to properties that need to be overridden.
 - For example, if you'd like to change the Tomcat https port to port 9443, uncomment the property from #server.port=8443 to server.port=9443

Good to Know:

- Only properties/lines uncommented within the <AppDataDirectory>/tasktop-hub.properties file will be applied, otherwise Hub will assume default values for commented properties.
- Only properties at <AppDataDirectory>/tasktop-hub.properties file will be used; the file <AppDataDirectory>/tasktop-hub.properties.default is just a template and will not work in Hub.

Upgrading

Upgrading on Windows

The tasktop-hub.properties file will not be replaced or deleted during the installation/upgrade process. For this reason, newer versions of Hub can retain settings automatically after upgrading.

Upgrading on Linux

Because the properties file is placed in the \$TASKTOP_HOME directory, newer versions of Planview Hub will automatically apply all configurations.

If the properties file is not placed in the \$TASKTOP_HOME directory, it is necessary to copy the properties file from the old installation directory to the new installation directory.

Upgrading from a Version Earlier than 20.4

If you have made manual changes to Tomcat and/or Jboss files, you have two options upon upgrading to 20.4:

- You can apply all configurations that have been applied manually to server.xml, standalone.xml, standalone.conf, standalone.conf.bat, setenv.sh, and Manage Tasktop -> Java -> Java Options to the tasktop-hub.properties file.

During an upgrade, it is not necessary to override the server.xml file from the old version to the new installation directory. This can be done by simply providing the tasktop-hub.properties file in a directory that Hub is able to read and ensuring that there is an uncommented line as shown below:

```
...
server.port=9443
...
```

Other properties can be configured the same way as shown in the example above.

- You can copy all configuration files from Tomcat and/or Jboss that were previously modified and override them in the new version directories.

Port Configuration

By default, Planview Hub utilizes the ports listed in the table below.

If any of those ports are already being utilized for other purposes, you will need to change them. To view a list of all ports being used on your system, you can use the netstat-a command. This will help you determine which available ports you would like to use for Hub.

Here is a summary of each port Hub utilizes and the location where you can change it if it is already being used:

Port	Location	Purpose
8080	tasktop-hub.properties	Default port Hub uses for HTTP (8080) / HTTPS (8443)
8443	#server.port=8443	

	#server.redirect.port=8080	
	More details here	
8081	tasktop-hub.properties	User Management (Keycloak) HTTP Ports
8444	#jboss.http.port=8081	
	#jboss.https.port=8444	
	More details here	
Additional Keycloak Ports:	tasktop-hub.properties	User Management (Keycloak)
• 9990	#jboss.ajp.port=8009	More details here
• 9993	#jboss.management.http.port=9990	
• 8009	#jboss.management.https.port=9993	
• 4712	#jboss.txn.recovery.environment.port=4712	
• 4713	#jboss.txn.status.manager.port=4713	
• 25	#jboss.mail.smtp.port=25	
	More details here	
(Note: The following ports have been modified from the Keycloak defaults: 8080→8081, 8443→ 8444)		
8005	tasktop-hub.properties	Tomcat Shutdown Port
	#server.shutdown.port=8005	

Planview Hub Port

The default port Hub uses is 8443 for HTTPS and 8080 for HTTP, which redirects to HTTPS. If you'd like to change these ports to ease access for your users, or to accommodate a proxy, follow these instructions:

1. Open the tasktop-hub.properties file and configure the following properties:

- a. `server.port` - The http or https port
- b. `server.redirect.port` - The port that, if accessed, redirects to **server.port**

2. After changing the port, the address used to access Hub (i.e., <http://localhost:8080>) will need to be updated with the new port number in place of '8080.'

Please refer to the [official documentation](#) for additional configuration options.

To learn more about creating a tasktop-hub.properties file, please see the section below.

User Management (Keycloak) Port

The default port for User Management is 8081. If you'd like to change the port that User Management (Keycloak) utilizes, follow the instructions [here](#). If your User Management (Keycloak) utilizes a port other than 8081, you can instruct Hub to access User Management (Keycloak) via the correct port by following the instructions below.

1. Open the tasktop-hub.properties file and configure the following properties:

- a. `jboss.http.port` - Jboss http port
- b. `jboss.https.port` - Jboss https port

Note: If you change the default jboss management-http port setting in the `/keycloak/standalone/configuration/standalone.xml` to something other than 9990, you must also update the port referenced in `/keycloak/bin/jboss-cli.xml`.

To learn more about creating a tasktop-hub.properties file, please see the section below.

Getting Started

Once installation is complete, you can begin using Hub by opening <https://localhost:8443/> in any of our supported browsers.

Before logging on to Hub, you must log into the **User Administration Console** in order to create your admin user(s). The User Administration Console can be accessed via the **User Administration Console link** at the bottom of the Hub login page. Please review the [User Management](#) section for detailed instructions on how to create a user, login, and manage your user accounts.

Once logged in, you will be prompted to set a **Master Password**, which will be used to encrypt your repository credentials.

You will also need to apply your license before configuring your integrations. You can learn how to apply your license [here](#).

Providing Limited Public Access to Hub

To ensure optimal protection, we recommend only allowing intended traffic to access your Hub instance. Numerous network techniques and scenarios exist for configuring a web application with restricted public access.

Port Forwarding

Port forwarding enables traffic from the internet or an external network to reach a specific device or service within a private local network.

Planview offers limited support for configuring port forwarding. See [details here](#) to learn more.

Reverse Proxies

A reverse proxy acts as an intermediary between clients (typically web browsers) and backend servers, working on behalf of the backend servers to handle client requests. It serves as a robust protective barrier within networking techniques, making it a widely adopted solution for enhancing security and safeguarding backend servers from direct exposure to external clients.

Planview offers limited support for configuring reverse proxies. See [details here](#) to learn more.

Externalized Configuration

Planview Hub enables you to externalize configurations from Tomcat, Jboss/Keycloak, and certain application properties in a single place. This allows you to use property files to override default values such as:

- **Jboss:** ports (e.g., http, https, management port), Keycloak database paths, Keycloak trust stores, java memory variables, and custom system properties
- **Tomcat:** ports (e.g., http https), keystores (e.g., files, passwords, types), java memory variables, and custom system properties
- **Application Properties:** Derby, Tasktop Hub, Liquibase, log4j, and keycloak host

To override default values through a properties file, you must provide the tasktop-hub.properties file in a directory that Hub can scan and read.

This can be done as follows:

1. Rename the file tasktop-hub.properties.default to tasktop-hub.properties.

- a. For **Windows**, this file can be found in the **App Data Directory**.
- b. For **Linux**, this file can be found in the root level of the `.tar.gz` package.

- a. **Note:** For Linux users, we recommend creating an environment variable named `TASKTOP_HOME` with its value pointing to an exclusive directory where the `tasktop-hub.properties` file will be placed.

2. Provide values to properties that need to be overridden.

- a. For example, if you'd like to change the Tomcat https port to port 9443, uncomment the property from `#server.port=8443` to `server.port=9443`

Good to Know:

- Only properties/lines uncommented within the `<AppDataDirectory>/tasktop-hub.properties` file will be applied, otherwise Hub will assume default values for commented properties.
- Only properties at `<AppDataDirectory>/tasktop-hub.properties` file will be used; the file `<AppDataDirectory>/tasktop-hub.properties.default` is just a template and will not work in Hub.

Upgrading

Upgrading on Windows

The `tasktop-hub.properties` file will not be replaced or deleted during the installation/upgrade process. For this reason, newer versions of Hub can retain settings automatically after upgrading.

Upgrading on Linux

Because the properties file is placed in the `$TASKTOP_HOME` directory, newer versions of Planview Hub will automatically apply all configurations.

If the properties file is not placed in the `$TASKTOP_HOME` directory, it is necessary to copy the properties file from the old installation directory to the new installation directory.

Upgrading from a Version Earlier than 20.4

If you have made manual changes to Tomcat and/or Jboss files, you have two options upon upgrading to 20.4:

1. You can apply all configurations that have been applied manually to `server.xml`, `standalone.xml`, `standalone.conf`, `standalone.conf.bat`, `setenv.sh`, and `Manage Tasktop -> Java -> Java Options` to the `tasktop-hub.properties` file.

During an upgrade, it is not necessary to override the `server.xml` file from the old version to the new installation directory. This can be done by simply providing the `tasktop-hub.properties` file in a directory that Hub is able to read and ensuring that there is an uncommented line as shown below:

```
...
server.port=9443
...
```

Other properties can be configured the same way as shown in the example above.

2. You can copy all configuration files from Tomcat and/or Jboss that were previously modified and override them in the new version directories.

Properties

The `tasktop-hub.properties` file contains three main blocks:

- Keycloak Properties
- Tomcat Properties
- Planview Hub Properties

Keycloak

The properties listed in the table below are used only if Hub is using Keycloak as an Authentication Provider.

Note: Starting in 23.2, Keycloak runs on the Quarkus framework instead of the Jboss application server. This change led to the deprecation or renaming of certain properties as noted in the table.

Property	Purpose	Notes
<code>keycloak.http.port</code>	Use this property to select a custom HTTP port for keycloak.	Formerly named <code>jboss.http.port</code> . Please update all properties prefixed with <code>jboss</code> .
<code>keycloak.https.port</code>	Use this property to select a custom HTTPS port for keycloak.	Formerly named <code>jboss.https.port</code> .
<code>keycloak.server.data.dir</code>	Use this property if you want to place the keycloak database in a custom directory.	This is the directory where the keycloak database lives. Formerly named <code>jboss.server.data.dir</code> . The name of the database file must not be changed (it should be <code>keycloak.h2.db</code>). For both Windows and Linux, the directory separator needs to be <code>'/'</code> .
<code>keycloak.java.memory</code>	Use this property to change memory settings.	We recommend setting the maximum Java heap size value to 50-75% of your system's memory. Formerly named <code>jboss.java.memory</code> .
<code>keycloak.custom.system.properties</code>	Use this property to load custom system properties. For example: <code>-keycloak.*=value, -Dkey=value, -XX:key=value, -javaagent:value, -agentlib:value</code>	Formerly named <code>jboss.custom.system.properties</code> .
<code>keycloak.custom.auth-server-url</code>	Use this property to override the default authentication server URL detection	This is only needed in rare scenarios with proxies or load balancers where Planview Hub is unable to determine the externally accessible URL for Keycloak. It is recommended to host Hub and Keycloak on the same machine and restrict access to Keycloak via firewall.

Tomcat

The properties listed in the table below are used to override some properties from Tomcat

Property	Purpose	Notes
<code>server.port</code>	Use this property to provide a value for the attribute port in the tag <code><Connector></code> within the <code>server.xml</code> descriptor.	After changing the port, if Keycloak is being used, you will need to go into the User Administration Console and adjust the client to the new port.
<code>server.redirect.port</code>	Use this property to provide a value for the attribute redirectPort in the tag <code><Connector></code> within the	

	server.xml descriptor.	
server.shutdown.port	Use this property to provide a value for the attribute port in the tag <Server/> within the server.xml descriptor.	
server.tomcat.connection-timeout	Use this property to provide a value for the attribute connectionTimeout in the tag <Connector/> within the server.xml descriptor.	
server.ssl.key-store=/path/to/keystore-file	Use this property to provide a value for the attribute keystoreFile in the tag <Connector/> within the server.xml descriptor.	This property is shared with Keycloak.
server.ssl.key-store-password=changeit	Use this property to provide a value for the attribute keystorePass in the tag <Connector/> within the server.xml descriptor.	This property is shared with Keycloak.
server.ssl.key-store-type=JKS	Use this property to provide a value for the attribute keystoreType in the tag <Connector/> within the server.xml descriptor.	
server.ssl.key-alias	Use this property to provide a value for the attribute keyAlias in the tag <Connector/> within the server.xml descriptor.	Enable this property only if your custom Keystore has an alias and it is different than Tomcat.
tomcat.java.memory=-Xms256M -Xmx2118M	Use this property to change memory settings.	<p>We recommend setting the maximum Java heap size value to 50-75% of your system's memory.</p> <p>For Windows: Initial memory pool size (-Xms) and maximum memory pool size (-Xmx) needs to be in MB. That means that the value needs to be suffixed with 'M'.</p> <p>Values suffixed with 'G' will cause an error at the start of Hub.</p> <p>For Linux: Values can be specified in MB or GB. Both suffixes 'M' and 'G' work.</p>
tomcat.java.errorFile=/path/to/hs_err_pid%p.log	Use this property to provide a custom path for -XX:ErrorFile.	
tomcat.java.io.tmpdir=path/to/temp	Use this property to provide a custom path for java.io.tmpdir directory.	
tomcat.java.util.logging.config.file=path/to/logging.properties	Use this property to provide a custom path for Tomcat's logging.properties file.	
tomcat.jdk.tls.rejectClientInitiatedRenegotiation=true	Use this property to provide jdk.tls.rejectClientInitiatedRenegotiation value.	
tomcat.custom.system.properties	Use this property to load custom system properties such as: -XX:key=value, -javaagent:value, -agentlib:value	

Tasktop Hub

The properties listed in the table below are used to override some Hub values.

Property	Purpose	Notes
derby.storage.pageCacheSize	Use this property to change the data page cache in the database.	Reference
derby.system.home=/path/to/db	Use this property to provide a custom path to the Derby database directory.	Providing the Derby database directory is useful for Linux environments when upgrading, as you do not need to copy files from the old installation directory to the new installation directory.
hub.database.configuration.directory=/path/to/db	Use this property to provide a custom path to the Derby database.	
liquibase.ignoreRecycleBinWarning=true	Use this property to whether or not suppress liquibase warnings.	
log4j.configuration=file:/path/to/log4j2.xml	Use this property to provide a custom path to the log4j2.xml file.	
log4j.configuration.verbose=file:/path/to/log4j2-troubleshooting.xml	Use this property to provide a custom path to the log4j2-troubleshooting.xml file.	
hub.security.cors.exclusionPaths	Use this property to provide a list of paths that will be excluded from the CORS verification. For example:/first-path,/second-path	Prior to version 21.1, this property was configured in /tasktop/container/webapps/root/WEB-INF/web.xml

Good to Know

Windows

- It is not possible to use environment variables to compound values. Properties related to paths must be configured using an absolute path.
- Properties must be modified in the tasktop-hub.properties file as this file has more priority than properties modified in Manage Tasktop > Java > Java Options | Initial memory pool | Maximum memory pool.

Linux

It is possible to use environment variables to compound a specific value. As an example, it is possible to use \$CATALINA_BASE to compound a path.

```
hub.database.configuration.directory=$CATALINA_BASE/../../directory
log4j.configuration.verbose=file:$CATALINA_BASE/../../log4j2-troubleshooting.xml
```

Default File Locations

Windows

When Planview Hub is installed on Windows using the MSI installer, the program files (i.e., the executable files and binaries) are located in C:\Program Files\Tasktop; configuration files and logs are located in C:\ProgramData\Tasktop.

Tip: ProgramData may be a hidden folder, so you will need to change your Windows Explorer settings to show hidden files and folders to find it.

Note: If you change the location of the ProgramData directory to an alternate location, do **not** include spaces in the name of the new directory. If the directory has spaces in its name, Hub's UI will not be accessible.

Linux

When Planview Hub is installed on Linux, the program files (i.e., the executable files and binaries), configuration files, and logs are all located in the installation directory where you extracted the distribution archive.

Note: You must choose a location with **no spaces** in its path, or Hub's UI will not be accessible.

Repository Preparations

Preparing Your Repositories

In Hub, the term **repository** refers to the external tools Hub connects to (e.g., Atlassian Jira, ServiceNow, BMC Remedy, etc).

Before connecting Hub to your external repositories, you will need to perform some simple preparation on each repository you will be integrating. This preparation includes creating a user account for Hub with the appropriate permissions. Please refer to our Connector Documentation for detailed instructions for each repository.

Firewalls and Proxies

If Planview Hub is installed behind a firewall, you may need to connect to external repositories (e.g., hosted or cloud ALM tools) through a proxy. To create a connection to such external repositories in Planview Hub, you can make Hub connect through your proxy by configuring the proxy settings when creating a new repository connection. It is recommended to create login credentials specifically for Hub on the proxy server.

Note: The Proxy Location must be a URL in order for the proxy connection to work. If a .pac script is used in your browser, you will need to open the script and find the URL/port to enter in the Location field.

To use a proxy server, check the **user proxy server** box and fill in your proxy details in the **Proxy Server** section on the New Repository Screen:

Proxy Server Use proxy server

Proxy Host Address	<input type="text" value="https://proxy.example.com:8080"/>
Username	<input type="text" value="TasktopUser"/>
Password	<input type="password" value="*****"/>

Proxy Server
If your organization uses a proxy server to access the above repository, please provide the proxy server credentials.

Troubleshooting

Troubleshooting Mode

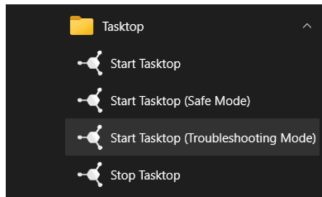
Troubleshooting Mode allows you to turn on verbose logging when the UI doesn't appear due to issues upon startup.

To start Hub in Troubleshooting Mode, see the following instructions:

- **For Linux:** Run the following script from the command line in the installation folder:

```
start-tasktop-troubleshooting-mode.sh
```

- **For Windows:** Click **Start Tasktop (Troubleshooting Mode)** in the Start menu.



Note: The default troubleshooting duration is set to two hours when Troubleshooting Mode is enabled. You can view the Troubleshooting timer in the Troubleshooting tab on the Settings screen

SafeMode

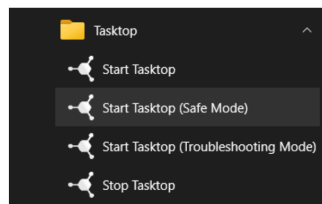
SafeMode allows you to start Hub without running your integrations (i.e., no synchronization or change detection will occur).

To start Hub in SafeMode, see the following instructions:

- **For Linux:** Run the following script from the command line in the installation folder:

```
start-tasktop-safe-mode.sh
```

- **For Windows:** Click **Start Tasktop (Safe Mode)** in the Start Menu.





You are viewing content for Planview Hub version 22.4. [View another version](#) ▼



Container Configuration

On This Page

Planview Hub is distributed with the **Apache Tomcat Servlet Container**.

For information on configuring the container, refer to [Apache Tomcat documentation](#).

On **Windows**, configuration and log files are installed under `C:\ProgramData\Tasktop` while program files are located under `C:\Program Files\Tasktop`.

For information on configuring the service, refer to [Apache Tomcat Service How to](#).

Further configuration, including JVM options and memory allocation, can be performed for the Windows service by launching **Tasktop Properties** located at `C:\Program Files\Tasktop\container\bin\tasktopw.exe`.

Increasing Available Memory

Beginning in Hub version 20.4, configurations are externalized from **Tomcat, Jboss/Keycloak**, and certain application properties in a single place. This allows you to use property files to override memory variables and custom system properties.

For more information on changing memory settings, please refer to the [properties table](#).

Logging

Logging is configured with `log4j2`. See the included `log4j2.xml` to configure log levels, location, and rolling policy.

The included `log4j2-troubleshooting.xml` configures `log4j2` for the troubleshooting log level when set via the Settings screen.


[On This Page](#)

When upgrading from a version earlier than 23.2.0 with Keycloak customization:

- Refer to the properties table [here](#) to update the Keycloak Jboss properties.

When upgrading from earlier versions to 21.1.x:

- As 21.1.x is a [checkpoint release](#), be aware that you **must** upgrade to version 21.1.x **before** upgrading to a later version.
- If you do not follow instructions [here](#), you may encounter issues with artifact association management that prevent you from viewing and deleting artifact pairs.
- Note:** Be aware that upgrading to 21.1.x from an earlier version may take longer than usual.

Backup

A working backup strategy is a critical element of disaster recovery, since only backups can mitigate complete hardware failure and user error. A strategy that ensures correct and current backups is essential. Backups of the Hub database include both configuration and operational data.

Backup frequency should mirror your practices for all software tools your organization utilizes. Backup frequency should be daily, ideally with incremental backups performed more frequently.

General Application Configuration

The recommended practice is to back up the entire installation/program data directory to cover all customizations (excluding logs)

- Back up Tomcat customizations (in Linux install directory or Windows Program Data)
 - container/conf/server.xml
 - Any keystores for certificates
 - For **Linux**: bin/setenv.sh
 - For **Windows**: Any changes to the Java section of the Manage Planview Hub application (e.g., memory, command line parameters, etc)
- Back up keycloak data and customizations
 - keycloak/data/h2 (on Linux from 23.2 and later)
 - keycloak/standalone/data

Note: The location of keycloak or operation data are configurable in `tasktop-hub.properties`. If the defaults are overridden by this configuration, please back up the configured directories.

Operational Data Configuration

Default Derby Database

Planview automatically stores operational data to a built-in database. However, for production environments, we strongly recommend that operational data is stored to an external database for improved maintainability. This enables you to perform frequent backups without stopping Hub and ensures that your Hub practices are consistent with your existing disaster and recovery process. For details on how to store your operational data to an external database rather than Planview's built-in database, please refer [here](#).

If utilizing Planview's built-in Derby Database, ensure you've backed up the following:

- File backup of db directory (in Linux install directory or Windows Program Data)

External Database

In order to back up Hub, follow the instructions below:

- Ensure that you have migrated your operational data to an external database. For details on how to set up your external database, please see [here](#).
- Back up the following folders

a. on Linux:

- ./tasktop/db
- ./tasktop/drivers
- ./tasktop/libraries

b. on Windows:

- The Hub data folder, typically C:\ProgramData\Tasktop

- Back up the external database using that database's backup tools.
- Back up the Tomcat and Catalina configuration

Note: This is only applicable if changes are made to the Tomcat and Catalina configuration.

Restore from Backup

If Planview Hub fails to restart after an upgrade or if there are unresolvable errors preventing your integrations from running, Planview Hub may need to be returned to the previous version. Please ensure to stop Hub before restoring to a previous version.

Note: If restoring from backup, you should be cautious as the state of the integration is maintained in the database and restoring to an older version could result in duplicated items and data (e.g., comments and attachments). It is recommended to only restore when directed by Planview support or after a failed upgrade where no items were processed.

Tip: If integrations were resumed individually during an upgrade, you can prevent duplicating items and data when restoring to an earlier version by utilizing the upgrade from backup file feature described below.

General Configuration

You should restore any changes identified in the backup.

Operational Data

Default Derby Database

In order to restore Hub, follow the instructions below:

- Copy the database directory from backup to the Hub data folder.
- Restore the backed up Tomcat and Catalina configuration files from part 4 of the backup instructions.

External Database

In order to restore Hub, follow the instructions below:

1. Restore the external database backup using the tools from that database.
2. Restore the backed up Tomcat and Catalina configuration files from part 4 of the backup instructions.

Operating Systems

Windows Backup

1. Shut down Hub.
2. Uninstall Hub, then run the previous installer.
3. Restore from backup as described in section above.
4. Restart Hub.
 - a. If you'd like, you can restart Hub in 'safe mode' which ensures all integrations are paused.

Linux Backup

1. Shut down Hub.
2. Remove the new Hub installation folder and restore the old Hub installation folder from step 3 of the upgrade steps.
3. If you are using an external database for Hub's configuration, restore the external database as described above.
4. Restart Hub.
 - a. If you'd like, you can restart Hub in 'safe mode' which ensures all integrations are paused.

Upgrading

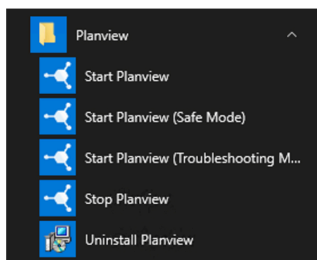
Before you Upgrade

Before upgrading Planview Hub, be sure to do the following:

1. Shut down Hub and afterwards follow the [backup instructions](#) outlined above. The first time that Hub restarts after an upgrade, the internal database will be migrated to the new version and it will no longer be possible to return to the prior version without the backup.
2. Additionally, ensure that backups are made of the Tomcat, Catalina, and Keycloak configuration files that have been customized. The upgrade process will overwrite these configuration files and customizations will need to be re-applied.
3. When Hub is upgraded, a service-downtime for the Hub service is required in order to upgrade the database. Note that a second instance cannot be running while the first instance is attempting to upgrade the database.
 - To understand implications of Hub downtime, please see [here](#).
4. Please review the [release notes](#) for all Planview Hub versions that have been released after the version you are upgrading from. Ensure that any upgrade steps outlined in the release notes are followed.

Windows

1. Ensure a copy of the old installer is available in case a roll-back is required.
2. Click the **Stop Planview** button on your desktop, and make sure services are stopped:



2. Backup as described in section above.
3. Run the installer of the new version of Planview Hub.
4. Re-apply Tomcat/Keycloak configurations.
 - Upgrading from versions *earlier* than 20.4:
 - Apply all customizations done in `<install-location>/container/conf/server.xml` to the `tasktop-hub.properties` file. More details about translating configurations from `server.xml` to the new properties file can be found [here](#).
 - Upgrading from versions *earlier* than 21.1:
 - If any configuration was applied to `exclusion-paths` property in the `web.xml`, it needs to be migrated to the `tasktop-hub.properties` file. See the following example:

- Copy `/auth/realms/Tasktop/broker/saml` and `/auth/realms/Tasktop/login-actions` from the `web.xml` file.

```
<filter>
  <filter-name>CORSFilter</filter-name>
  <filter-class>com.tasktop.servlet.cors.CorsHeaderScrutinyServletFilter</filter-class>
  <init-param>
    <description>A comma or whitespace separated list of paths to exclude from the CORSFilter</description>
    <param-name>exclusion-paths</param-name>
    <param-value>
      /auth/realms/Tasktop/broker/saml
      /auth/realms/Tasktop/login-actions
    </param-value>
  </init-param>
</filter>
```

Place them in the `tasktop-hub.properties` file.

- ```
A list of paths that will be excluded from the CORS verification.
This list is separated by comma. Example: /first-path,/second-path
hub.security.cors.exclusionPaths=/auth/realms/Tasktop/broker/saml,/auth/realms/Tasktop/login-actions
```

Upgrading from version 20.4 and later:

- No action needs to be taken. Tomcat/Keycloak configurations will be applied automatically.

## Linux

- Shut down Hub and Keycloak.
- Back up as described in section above.
- Move the old Hub installation folder to an archive folder.
- Unzip the new Hub distribution archive.
- Restore drivers, copy the `/tasktop/drivers` directory from the old installation into the new installation folder `<install-location>/tasktop`.
- Restore DB.
  - If you are using Hub's internal configuration database, copy the `tasktop/db` folder from the old installation into the new installation folder `<install-location>/tasktop`.
  - If you are using an external database for Hub's configuration, copy the `tasktop-db.json` file, and the `/tasktop/db` from the old installation into the new installation folder `<install-location>/tasktop`.
- Re-apply Tomcat/Keycloak configurations.
  - Upgrading from versions earlier than 20.4:
    - Apply all customizations done in `<install-location>/container/conf/server.xml` to the `tasktop-hub.properties` file. More details about translating configurations from `server.xml` to the properties file can be found [here](#).
    - Apply all customizations done in `<install-location>/keycloak/standalone/configuration/standalone.xml` to the `tasktop-hub.properties` file. More details about translating configurations from `standalone.xml` to the properties file can be found [here](#).
  - Upgrading from versions earlier than 21.1:
    - If any configuration was applied to `exclusion-paths` property in `web.xml`, it will need to be migrated to the `tasktop-hub.properties` file. See the following example:
      - Copy `/auth/realms/Tasktop/broker/saml` and `/auth/realms/Tasktop/login-actions` from the `web.xml` file:

```
<filter>
 <filter-name>CORSFilter</filter-name>
 <filter-class>com.tasktop.servlet.cors.CorsHeaderScrutinyServletFilter</filter-class>
 <init-param>
 <description>A comma or whitespace separated list of paths to exclude from the CORSFilter</description>
 <param-name>exclusion-paths</param-name>
 <param-value>
 /auth/realms/Tasktop/broker/saml
 /auth/realms/Tasktop/login-actions
 </param-value>
 </init-param>
</filter>
```

- Place them in the `tasktop-hub.properties` file:

```
A list of paths that will be excluded from the CORS verification.
This list is separated by comma. Example: /first-path,/second-path
hub.security.cors.exclusionPaths=/auth/realms/Tasktop/broker/saml,/auth/realms/Tasktop/login-actions
```

- Upgrading from version 20.4 and later:
  - If any customization has been applied to the `tasktop-hub.properties` file, copy it into the new installation folder `<install-location>/tasktop`.
- Restore Keycloak (user management) configuration. Note that keycloak's database and Hub's database are separate.
  - If you are using Keycloak's internal configuration database, restore the database (`<install-location>/keycloak/standalone/data/keycloak.h2.db`) after installation.
  - If you are using an external database for Keycloak's configuration, reconfigure the external database as described [here](#)
    - **Note:** You must create an account to access these.
- If you have connected to the Microsoft TFS repository in the past:
  - Remove all files and folders, [except for the com.tasktop files](#), under `<install-location>\Tasktop\libraries\microsoft-tfs`.
  - Once Hub is started up again, navigate to the TFS repository connection screen. There, you will see instructions on how to provide the updated SDK and CLC files to Hub by adding them to the `connector-requirements` directory on the machine that hosts Hub.
  - Restart Hub after uploading the files.
- Start Hub.
- Navigate to the Activity screen.
  - Review the **Background Jobs** tab to review status on Integration Data Migration jobs.
    - Resolve any associated issues shown here. These issues will need to be resolved and their associated data migration jobs completed before the affected integrations can run (unrelated integrations should continue to process).
    - Once the associated issue is resolved, failed Integration Data Migration processes can be prioritized using the 'prioritize' button on the Background Jobs tab. Ensure that these jobs complete successfully.
  - Review the **Issues** tab to resolve any configuration issues.
    - If there are configuration migration issues, those will be shown in the Issues tab. They will block affected integrations from running (but unrelated integrations should continue to process). Once the source of the issue is resolved, configuration migration issues can be retried using the 'retry' button on the Issues tab.
  - Review the **Errors** tab to resolve any errors related to specific integration activities.
    - Once all issues and errors are resolved, the internal upgrade will complete and information will begin processing for those affected integrations.

1. If you are upgrading from a version earlier than 19.4.1, please see details regarding the [Troubleshooting User](#) [here](#).

## Upgrade from Backup File

This feature is only available when upgrading from Planview Hub versions 20.1 and later. To utilize this feature, please see the section below.

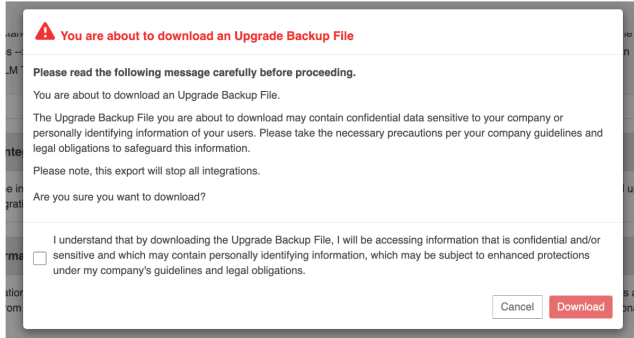
To restore Hub to a previous version in cases where integrations were resumed individually during an upgrade, you must use the upgrade backup file available on the **Advanced Configuration** screen. The downloaded data in the file corresponds to artifacts that may have been modified when migrations were still running to ensure artifact updates aren't duplicated when restoring.

**Note:** You must download the backup file from your Planview Hub instance **before** beginning the steps to restore.

To use this feature, you will first need to download the upgrade backup file. This file can be downloaded on the **Advanced Configuration** screen.

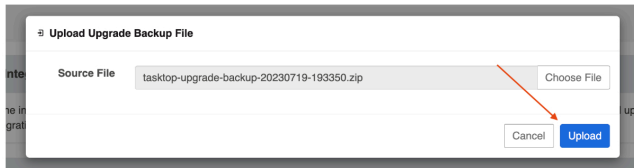


After clicking **Download**, the following message will appear:

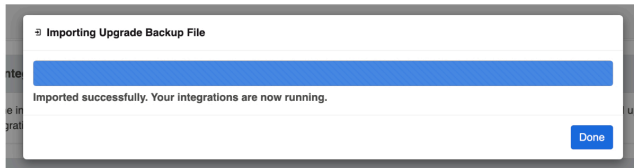


Once the file has been downloaded, you will need to restore Hub to the prior version. Please see the [section above](#) for more details on how to restore to a prior version.

After restoring to the earlier version, you can then select the backup file you would like to import and click **Upload**.



If the backup file is imported successfully, the following message will appear and your integrations will resume.



**Note:** If the backup file fails to upload, you will need to contact customer care for further assistance.

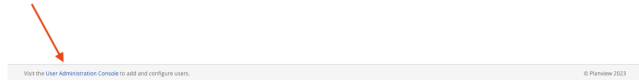
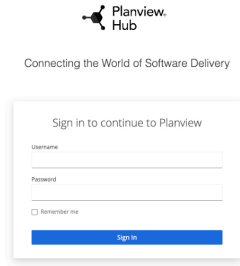


## Getting Started

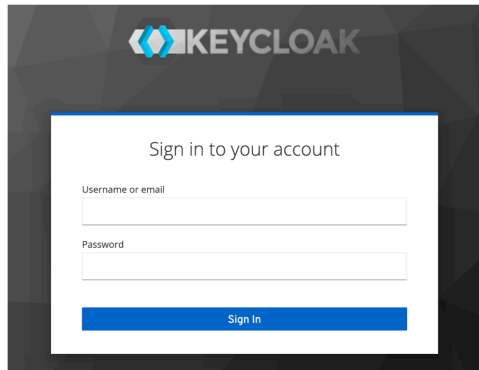
[On This Page](#)

Once installation is complete, you can begin using Planview Hub by opening <http://localhost:8080/> or <https://localhost:8443/> in any of our supported browsers.

Before logging in to Hub, you must log in to the **User Administration Console** to create your admin user(s). This can be accessed via the **User Administration Console link** at the bottom of the Hub login screen.



After clicking the link, the Keycloak login screen will appear.



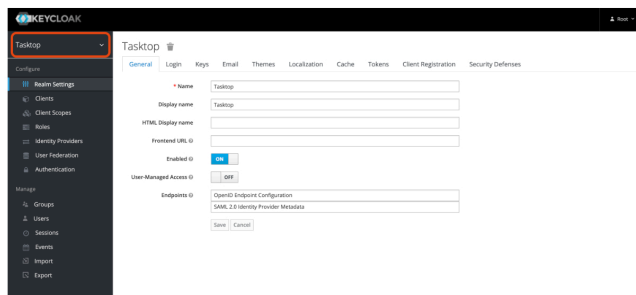
The Hub User Administration Console comes pre-configured with a root user and password. You can use the following credentials to log in to Keycloak:

- **Username:** root
- **Password:** Tasktop123

**Note:** There is only **one** initial root user. If the credentials for this user are lost, access to the advanced User Management features will also be lost. All functionality of Hub will continue uninterrupted. You can learn how to create additional root users and manage existing root users here.

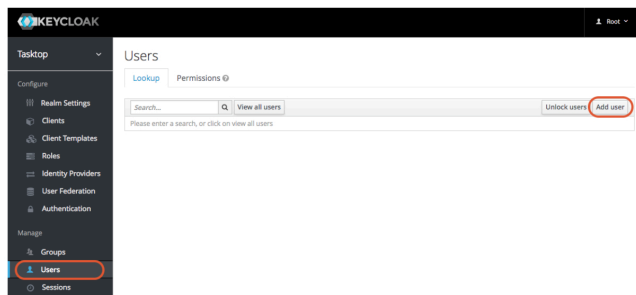
After logging in, you will be prompted to change your root password and you will need to make at least **one** new Hub Admin user for Planview Hub. After this first user is created, you can create additional users directly from the Hub interface.

To create a Hub Admin, ensure the **Tasktop** realm is selected here:

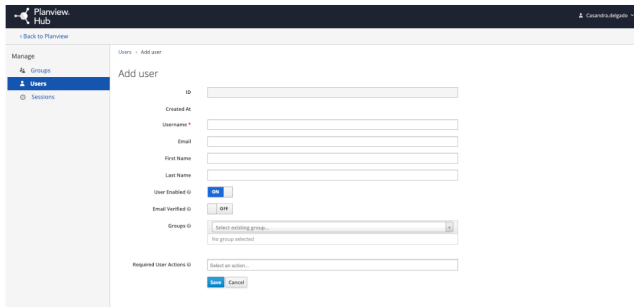


**Note:** Do not rename the realm (**Tasktop**), as this will result in errors upon Hub log in. If you must rename the realm, please also edit `{tasktop workspace}/webapps/ROOT/WEB-INF/keycloak.json`, update the 'realm' parameter, and then restart Hub.

Select the **User** section in the left column and click **Add user**.



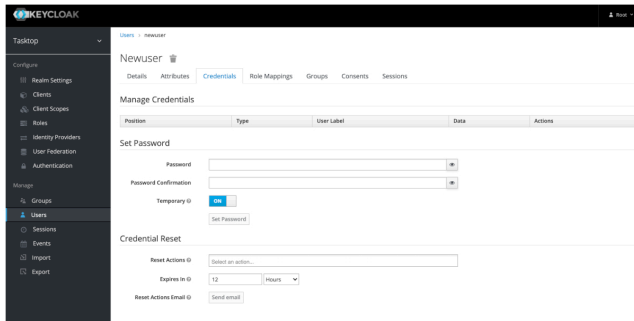
On this screen, enter the username, email, first name, and last name for your new user — the rest of the fields are **not** required. Once you've entered the required fields, click **Save**.



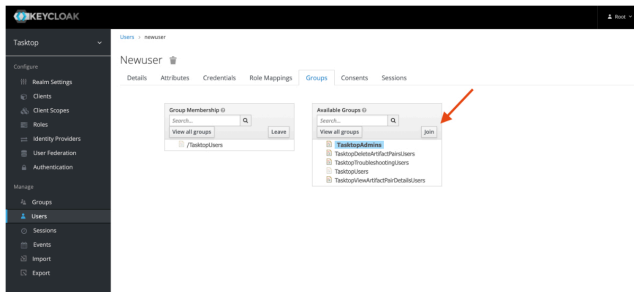
After you have saved the user, select the **Credentials** tab and provide a temporary password for the new user.

**Tip:** Please ensure the Temporary toggle is set to **On**. This will allow the user to set a new password upon their first log in.

Once you have entered the temporary password, click **Set Password**.



Next, select the **Groups** tab to assign the user as a Hub Admin. Highlight **TasktopAdmins** and click **Join**. By becoming a Hub Admin, the user can add new users directly from the Hub interface.



**Tip:** You can ignore the Attributes, Role Mappings, Consents and Sessions tabs.

That's it! Your Hub Admin user has been added.

Now, you can sign out of the User Administration console, navigate to <http://<server>:8080>, and log in with your newly created user account.

## Types of Users

There are several types of user roles in Hub:

- **Users:** This user has all permissions needed to create, modify, and run integrations.
- **Admins:** This user has the same permissions as a **User** and also includes the following permissions:
  - Create new users
  - Update users' passwords
  - Change users' group membership (from user to admin or vice-versa)
- **Troubleshooting Users:** This user can review Hub errors, logs, usage reports, and configurations, but cannot alter Hub integration configurations or user management.
  - **Note:** Troubleshooting Users may require additional steps if you'd like to update specific settings. For more information on configuring the Troubleshooting User role, please see the section below.
- **View Artifact Pair Details Users:** This user can view artifact pair details.
  - Note that this user role must be used in conjunction with the User, Admin, or Troubleshooting user role.
  - **Note:** Any users upgrading from versions prior to 21.1 will need to follow the steps outlined [here](#) for the View Artifact Pair user role to appear. All Hub Cloud users or users installing Planview Hub after 21.1 will have the Artifact Pair user roles by default and will not need to follow any additional steps.
- **Delete Artifact Pair Users:** This user can delete artifact pairs.
  - Note that this user role must be used in conjunction with the User, Admin, or Troubleshooting user role.
  - **Note:** Any users upgrading from versions prior to 21.1 will need to follow the steps outlined [here](#) for the Delete Artifact Pair user role to appear. All Hub Cloud users or users installing Planview Hub after 21.1 will have the Artifact Pair user roles by default and will not need to follow any additional steps.
- **Repository Write Access Users:** This user can create and edit repositories.
  - Note that this user role must be used in conjunction with the User, Admin, or Troubleshooting user role.
  - **Note:** Any users upgrading from versions prior to 23.4 will need to follow the steps outlined [here](#) for the Repository Write Access user role to appear. All users installing Planview Hub after 23.4 will have this role available by default and will not need to follow any additional steps.
- **Non Repository Write Access Users:** This user can create and edit all configuration except for repositories.
  - Note that this user role must be used in conjunction with the User, Admin, or Troubleshooting user role.
  - **Note:** Any users upgrading from versions prior to 23.4 will need to follow the steps outlined [here](#) for the Non Repository Write Access user role to appear. All Hub Cloud users or users installing Planview Hub after 23.4 will have this role available by default and will not need to follow any additional steps.

## Best Practices

We recommend configuring **at least two admin users** — that way if one admin forgets their password, the other admin can log in and reset the other admin user's password.

We also recommend changing the default password of the **Advanced User Administration** console. See the [Getting Started](#) section above for information on how to reset passwords.

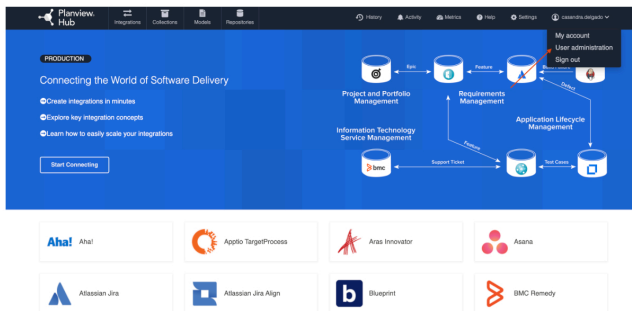
## User Role Permissions

Capability	Admin	User	Troubleshooting User	View Artifact Pair User	Delete Artifact Pair User	Repository Write Access User	Non Repository Write Access User
Access to the Hub Application	✓	✓	✓	✗	✗	✗	✗
Create New User	✓	✗	✗	✗	✗	✗	✗
Reset Any User's Password	✓	✗	✗	✗	✗	✗	✗
View and Modify Any User's Group Membership	✓	✗	✗	✗	✗	✗	✗
Reset Own Password, Name, or E-mail	✓	✓	✓	✗	✗	✓	✓
Create and Modify Repository Connections	✓	✓	✗	✗	✗	✓	✗
Create and Modify Models	✓	✓	✗	✗	✗	✗	✓
Create and Modify Collections	✓	✓	✗	✗	✗	✗	✓
Create, Modify, and Run Integrations	✓	✓	✗	✗	✗	✗	✓
Download Troubleshooting Reports (logs, usage reports, etc)	✓	✓	✓	✗	✗	✗	✓
Change Logging Frequency	✓	✓	✓	✗	✗	✗	✓
Review Errors & Configurations	✓	✓	✓	✗	✗	✗	✓
Retry, Prioritize, and Recreate Errors	✓	✓	✗	✗	✗	✗	✓
View artifact pair details	✗	✗	✗	✓	✗	✗	✗
Delete artifact pairs	✗	✗	✗	✗	✓	✗	✗
Access to <code>/api/v1/integrations/delete-integration-data</code> public API	✓	✗	✗	✗	✗	✗	✗
Access to <code>/api/v1/integrations/delete-all-integration-data</code> public API	✓	✗	✗	✗	✗	✗	✗

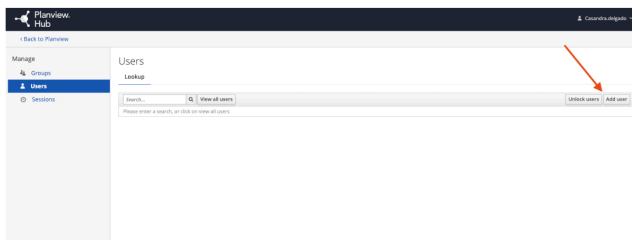
## Creating Additional Users

To create a user, select **User Administration**.

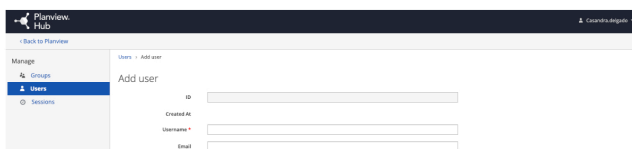
**Note:** You must have **admin** capabilities to create an additional user.



From the **User Administration** screen, select **Add user**.



On the **Add User** screen, enter the username, email, first name, and last name for your new user — the rest of the fields are **not** required. Once you've entered the required fields, click **Save**.



First Name:

Last Name:

User Enabled:

Email Verified:

Groups:

Required User Actions:

After you have saved the user, select the **Credentials** tab and provide a temporary password for the new user.

**Note:** Please ensure the Temporary toggle is set to **On**. This will allow the user to set a new password upon their first log in.

Once you have entered the temporary password, click **Set Password**.

Planview Hub - Manage Users - Hubuser

Manage Credentials

Set Password

Password:

Password Confirmation:

Temporary:

Next, click the **Groups** tab and add the user to a group — based on the permissions you'd like the user to have.

**Note:** If the new user is not added to a group, they will not be able to successfully access Hub.

Planview Hub - Manage Users - Hubuser

Groups

Group Membership:

Available Groups:

**Tip:** You can ignore the Attributes, Role Mappings, Consents, and Sessions tabs.

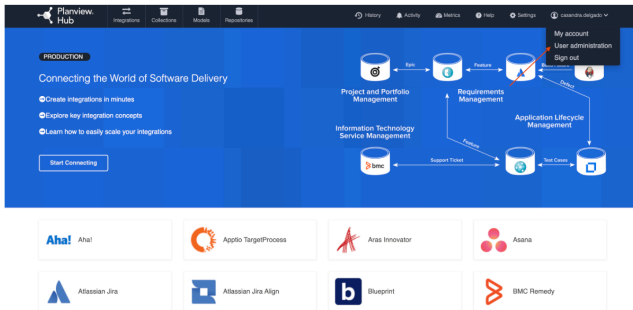
That's it! Your user has been added and can log in with their temporary password.

**Note:** Hub will not send the new user an email notification. The **admin** must notify the user of the new account and password.

## Resetting a User's Password

To reset a user's password, select **User Administration** from the upper right corner of the application.

**Note:** You must have **admin** capabilities to reset a user's password.



Click **View all users**. Next, click on the ID for the user whose password you'd like to reset.

Planview Hub - Manage Users - Users

Users

ID	Username	Email	Last Name	First Name	Actions	Unlink users	Address
97949297-531e-40c1-9484-...	user@nu.digiparis				Edit	Delete	
97970297-088-8461-8877-...	Hubuser				Edit	Delete	
525665197-488-8527-...	test@nuuser		User	Test@nu	Edit	Delete	

Then, click the **Credentials** tab and provide a temporary password for the user.

**Note:** Please ensure the Temporary toggle is set to **On**. This will allow the user to set a new password upon their first log in.

Once you have entered the temporary password, click **Set Password**.

Planview Hub - Manage Users - Hubuser

Manage Credentials

Set Password

Password:

Password Confirmation:



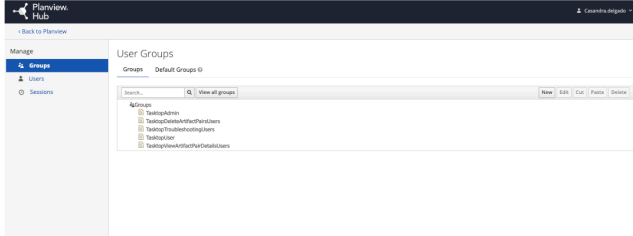
**Note:** Hub will not send the user an email notification. The **admin** must notify the user of the new temporary password. The user will be prompted to set a new password upon their next log in.

## Managing Groups

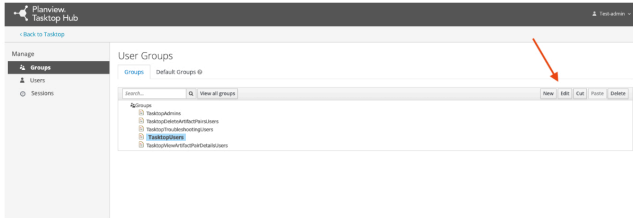
### Viewing Members of a Group

To view the members of a group, click **Groups** on the left side of the **User Management** screen.

**Note:** You must have **admin** capabilities to view members of a group.

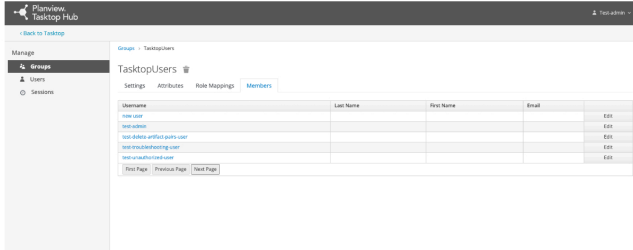


Next, select the group you'd like to review, and click **Edit**.



To view the group's current members, click the **Members** tab.

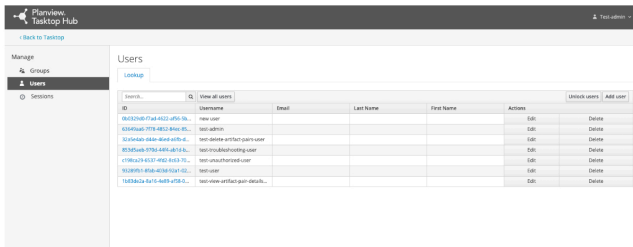
**Tip:** A user can be a member of multiple groups.



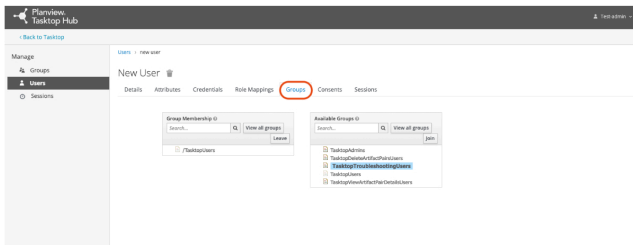
### Adding or Removing Users From a Group

Select **Users** from the left sidebar of the **User Administration** screen. Then, click **View all Users** and select the **ID** of the user you'd like to modify.

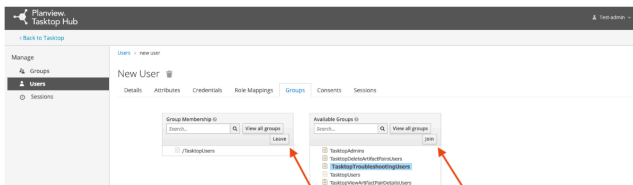
**Note:** You must have **admin** capabilities to modify a user's group membership.



Click the **Groups** tab and select the group whose membership you'd like to modify.



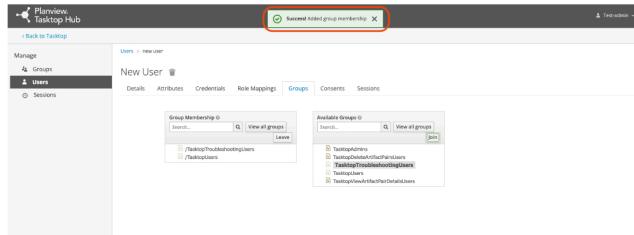
Then, use the **Leave** and **Join** buttons to modify their group membership.





There is no saving necessary here. Once you click **leave** and/or **join**, you will see a notification at the top of the screen informing you that your change has been made.

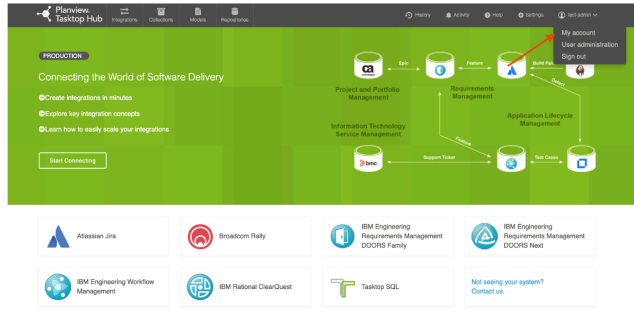
**Note:** A user must be a member of at least **one** group in order to be able to log in to Hub successfully.



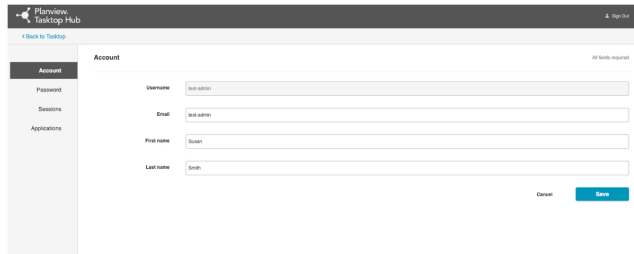
## Modifying Your Own User Information

To change your own password or other user information, click your username at the upper right corner of the screen, and select **My Account**.

**Tip:** Both **users** and **admins** can modify their own account information.



This will bring you to the **Account Info** screen, where you can update your name or email address.



Click **Password** on the left sidebar to change your password.

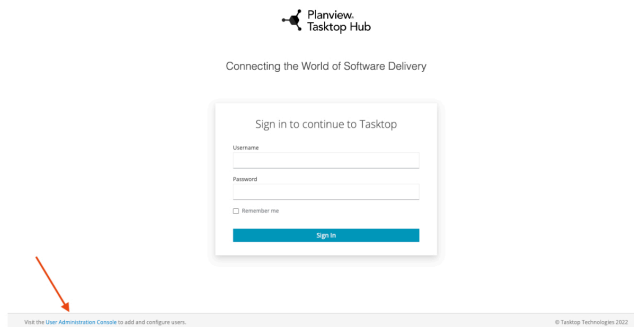


**Tip:** The **Sessions** and **Applications** sections can be ignored.

## Advanced User Management

Planview Hub has advanced user management capabilities that are not accessible via the Hub interface.

To access advanced user management capabilities, click the **User Administration Console** link at the bottom of the Hub login screen.



You can log in using the credentials you set when you first installed and began using Planview Hub.

**WARNING:** There is only one initial root user. If the credentials for this user are lost, access to the advanced User Management features will be lost. All functionality of Planview Hub, however, will continue uninterrupted.

Some of the advanced features include:

Some of the advanced features include:

- User Federation Configuration for:
  - LDAP
  - Kerberos
- Identity Provider login for:
  - SAML v2.0
  - OpenID Connect v1.0
- Enforcing custom password policies such as:
  - Set password expiration
  - Require special characters
  - Setting minimum password length

**Note:** While Planview Hub officially supports LDAP, other advanced features (including but not limited to Kerberos Federation and IDP) are not supported or tested by Planview.

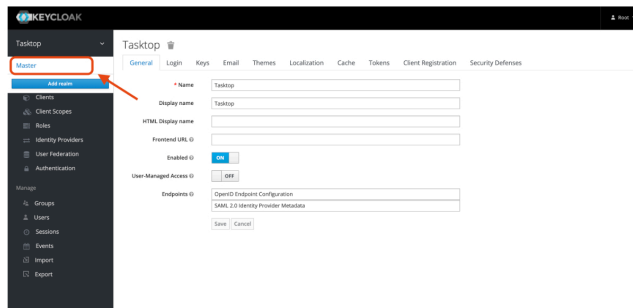
To learn more about these advanced features, click [here](#).

**WARNING:** Do not make changes or updates to the Roles or Groups section. Altering these settings may prevent your Planview Hub users from accessing the tool.

## Creating and Managing Root Users

A **root user** refers to a user who can log in to the **User Administration Console**. Hub comes with one root user, but if you'd like to create additional root users or to manage existing users, you can do so from the **User Administration Console**.

Once logged in, click the arrow next to **Tasktop** (in the upper left panel) and select **Master**.



Next, click **Users** in the left panel.

From here, you can follow the [same instructions used to create Hub users](#) to create and manage root users (ignoring the **Groups** section).

## Configuring the Troubleshooting User

### Upgrades to 19.4

This section is only applicable when upgrading from versions earlier than Planview Hub version 19.4.

#### Creating the Troubleshooting User Role using a Script

To configure the troubleshooting user role, we provide a script that will create the **TasktopTroubleshootingUser** role in your Keycloak instance, and replace the default **TasktopUsers** group with the **TasktopTroubleshootingUsers** group.

**Note:** This script can only be used if you have provided a valid SSL certificate as described in the [SSL Certificate Installation](#) section. If you have not provided such a certificate, skip to the [Creating the troubleshooting user role via the Keycloak admin console](#) section below.

#### Windows

Run the `add-troubleshooting-user.bat` script in `C:\Program Files\Tasktop\utility-scripts`, providing the relevant information when prompted.

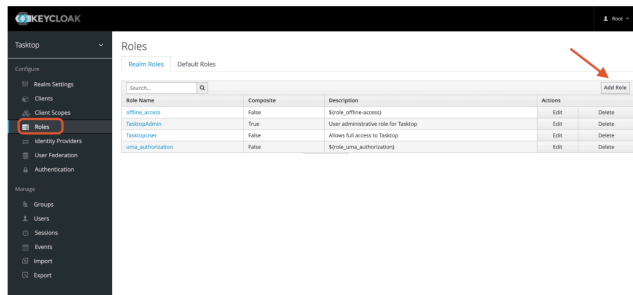
#### Linux

Run the `add-troubleshooting-user.sh` script in `<installation location>/Tasktop/utility-scripts`, providing the relevant information when prompted.

#### Creating the Troubleshooting User Role via the Keycloak Admin Console

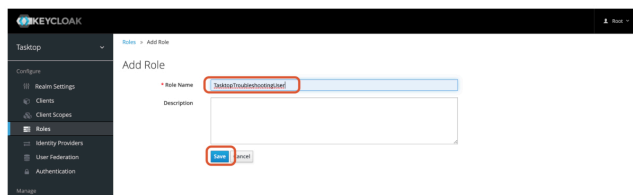
If you have not provided a valid SSL certificate, you can create a troubleshooting user via the **User Administration Console**. This console can be accessed by following the instructions in the [Getting Started](#) section.

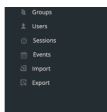
After logging in, navigate to the **Roles** section in the left column and click **Add Role**.



On this screen, enter **TasktopTroubleshootingUser** in the Role Name field. Then, click **Save**.

**Tip:** The Role Name is case-sensitive and must match exactly.



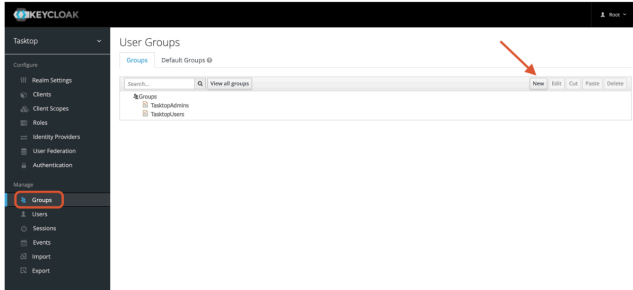


That's it! The troubleshooting user role has been created. Next, you'll need to add the troubleshooting user to a group.

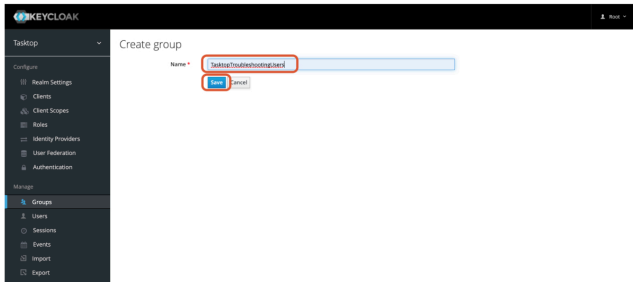
### Adding Troubleshooting Users to a Group

We recommend that you create a group for troubleshooting users and set it as the default group.

To do this, navigate to the **Groups** section in the left column and click **New**.

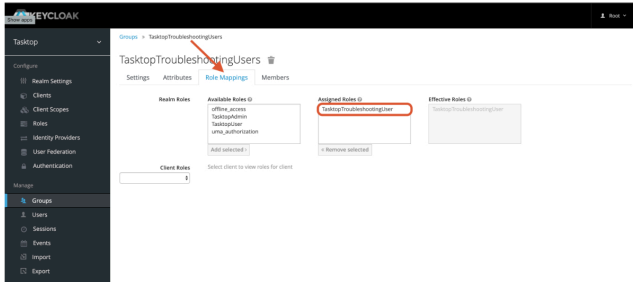


On the Create Group screen, enter **TasktopTroubleshootingUsers** in the Name field. Then, click **Save**.



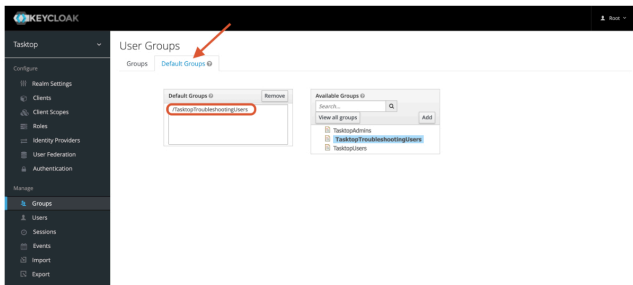
After saving the group, the new group screen will appear.

Next, select the **Role Mappings** tab and add **TasktopTroubleshootingUser** to Assigned Roles.



After you have added the user to Assigned Roles, navigate back to the **User Groups** screen and select the **Default Groups** tab.

Next, remove any groups under **Default Groups** and add the **TasktopTroubleshootingUsers** group.



### 19.4 - 21.1

This section is only applicable to Planview Hub version 19.4 - 21.1.

Upon installation, new users will default to having the **TasktopUser** role. If you'd like to set the default to **TasktopTroubleshootingUser**, please follow either set of instructions below.

#### Setting the Default Troubleshooting User Group Using a Script

To configure the troubleshooting user role, we provide a script that will create the **TasktopTroubleshootingUser** role in your Keycloak instance, and replace the default **TasktopUsers** group with the **TasktopTroubleshootingUsers** group.

**Note:** This script can only be used if you have provided a valid SSL certificate as described in the [SSL Certificate Installation](#) section. If you have not provided such a certificate, skip to the [Creating the troubleshooting user role via the Keycloak admin console](#) section below.

#### Windows

Run the `add-troubleshooting-user.bat` script in `C:\Program Files\Tasktop\utility-scripts`, providing the relevant information when prompted.

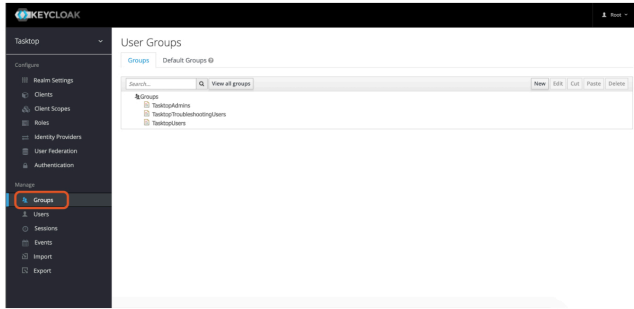
#### Linux

Run the `add-troubleshooting-user.sh` script in `<installation location>/Tasktop/utility-scripts`, providing the relevant information when prompted.

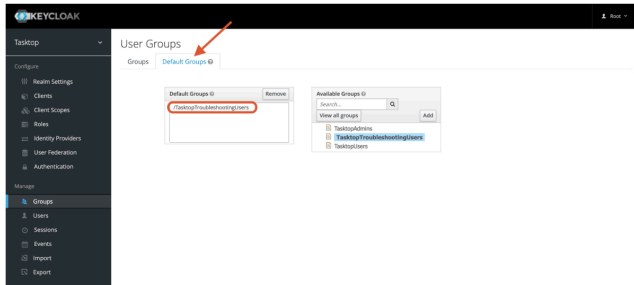
#### Setting the Default Troubleshooting User Group via the Keycloak Admin Console

If you have not provided a valid SSL certificate, you can set the troubleshooting user group as the default via the **User Administration Console**. The console can be accessed by following the instructions in the Getting Started section.

After logging in, navigate to the **Groups** section in the left column.



Select the **Default Groups** tab. Remove any groups under **Default Groups** and add **TasktopTroubleshootingUsers**.



## 21.2 and later

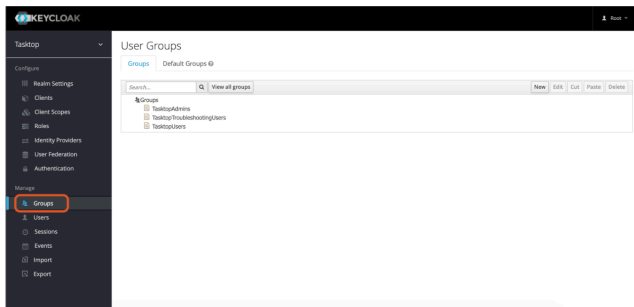
This section is only applicable to Planview Hub version 21.2 and later.

Upon installation, new users will default to having the **TasktopUser** role. If you'd like to set the default to **TasktopTroubleshootingUser**, please follow the instructions below.

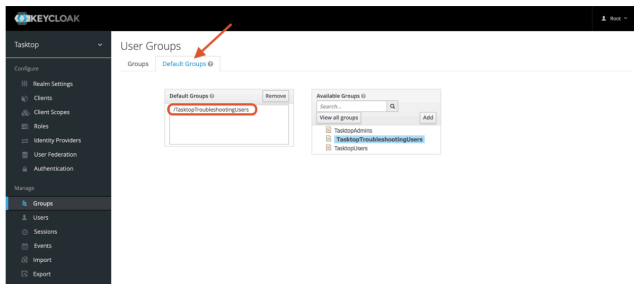
### Setting the Default Troubleshooting User Group via the Keycloak Admin Console

If you have not provided a valid SSL certificate, you can set the troubleshooting user group as the default via the **User Administration Console**. The console can be accessed by following the instructions in the Getting Started section.

After logging in, navigate to the **Groups** section in the left column.



Select the **Default Groups** tab. Remove any groups under **Default Groups** and add **TasktopTroubleshootingUsers**.



## Configuring LDAP User Management

### Required Directory Information

Before configuring LDAP, please check you have the following required pieces of information available for your specific Active Directory (AD) domain.

- The **fully qualified domain name** (FQDN) for the AD service,
  - *example: 'demo.tasktop.com'*
- An AD **user** account and credentials; The user will need read / view access to Users, Groups and Organizational Units (OU). We suggest a specific restricted account be setup in AD for this purpose.
  - *example: 'service\_tasktop'*
- An AD **user group**. The group(s) will be used to store specific users, who will have access to Planview Hub.
  - *example: 'Tasktop Users'*
- A tool such as **ADSIEdit**, which is able to give you the specific information about the structure of your AD domain setup.
  - **ADSIEdit** is part of Microsoft Windows Remote Server Administration Toolset (RSAT). This can be downloaded from [Microsoft RSAT page](#), or enabled on a server by adding the RSAT feature.

- Alternatively, ask your Domain Administrators for all of the following information:
  - CN/DN for Hub User (mentioned above)
  - CN/DN for the Hub User Group (mentioned above)
  - User, mail; username and name attributes (the specific name for each attribute)
  - OU root for all users
  - LDAP FQDN server URL

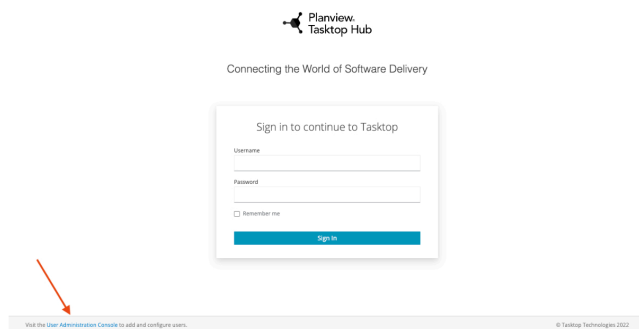
### Importing SSL Certificates

If you would like to connect to an LDAP server, you will need to import the SSL certificate into the keystore of your Hub product and restart it. To import the certificate to the keystore, see the following:

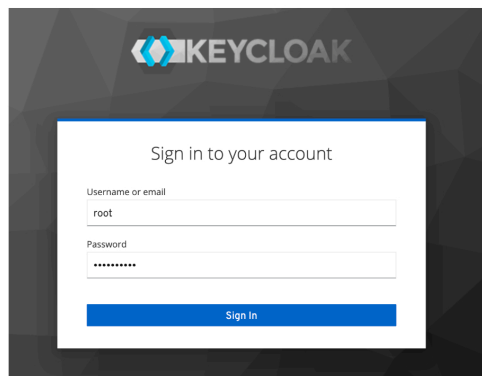
- Shut down your Planview Hub instance (including Keycloak)
- Obtain the certificate and certificate chain for your LDAP server. You may be able to do this using a command like the following on Linux
  - `echo -n | openssl s_client -connect <ldap-server>:636 | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > Idapserver.pem`
- In command prompt enter the following:
  - `<path_to_jre>/bin/keytool -import -trustcacerts -keystore <path_to_keystore> -storepass <password> -alias ldap -file Idapserver.pem`
    - `<path_to_jre>` refers to the jre folder in the Hub install location.
    - `<path-to-keystore>` refers to the path to the truststore referenced [here](#).
    - `<password>` is the password of your keystore or changeit if you are using the default
    - the keytool command should be run for each certificate exported. Each will need to have a unique alias.
  - the default password is: changeit
- Start your Hub product.
- Try again to connect to LDAP Server.

### Accessing Keycloak Configuration Tool

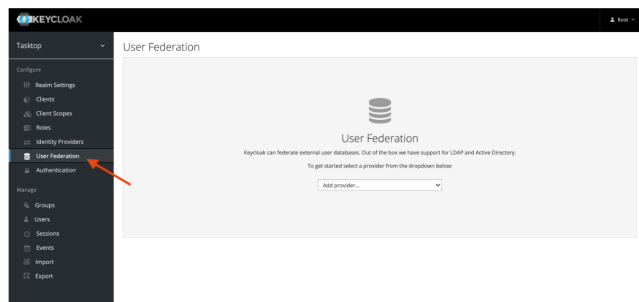
1. To access advanced user management capabilities, click the **User Administration Console** link at the bottom of the Planview Hub login screen.



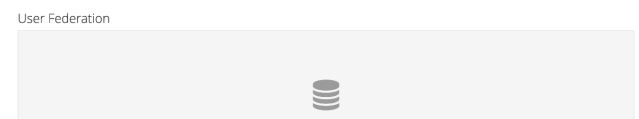
2. Log in using the default credentials listed in the Getting Started section above.

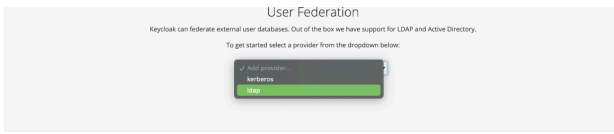


3. Select the **User Federation** link from the left side panel.

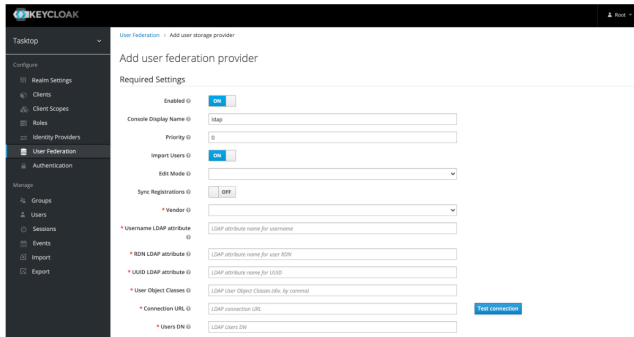


4. Choose the **ldap** option from the dropdown for **Add provider...**





5. The **LDAP configuration** screen should now be displayed.



### Configuring LDAP for Active Directory

This section will guide you through creating a connection to an LDAP authentication server.

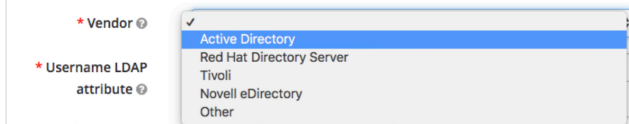
**Note:** Images provided are only a sample of settings — please ensure that you enter information specific for your environment.

#### Required Settings

**Note:** Follow the steps above to access the **LDAP configuration** page.

See the required settings below:

- **Console Display name:** This is the name you'd like to give your connection.
- **Priority:** If you have more than one User Federation configured, this setting specifies in which order to search each user federation service, **0** is first.
- **Edit Mode:**
  - **READ\_ONLY:** This setting reads the attributes from Active Directory (AD). It will not attempt to modify the AD service or store any local changes to user information.
  - **WRITABLE:** This setting may enable some changes to be written back to AD. The user account communication with AD will need access to modify the specific objects attribute.
  - **UNSYNCED:** This setting reads the attributes from AD and synchronizes them to a local store in the internal Keycloak database. **Users** and **Administrators** can make changes to the user objects, but those changes will only be stored for the local Hub instance. This will not write back to Active Directory.
- **Tip:** The recommended mode is **READ\_ONLY**.
- **Sync registrations:** If a new user is created in Planview Hub, this will allow that user to also be created in AD if you have **WRITABLE** selected and access to create user objects in the AD domain. The default setting is **OFF**.
- **Vendor:** Specifies which vendor software to use for this LDAP configuration. If you are using something other than Active Directory, the attributes and locations may be different. This will also pre-fill some default values.



- **Username LDAP attribute:** This should be the default username attribute as specified in your domain. The default for Microsoft AD is **sAMAccountName**.

\* Username LDAP attribute

- **RDN LDAP attribute:** The Relative Distinguished Name LDAP attribute is a list of attributes which will be searched when a user attempts to authenticate to Planview Hub. The attributes listed here should be unique within an OU level or unique within a domain. The following options are a good base to use:

- **cn** (canonical name): the full name (e.g., *John Doe*)
- **sAMAccountName**: the username (e.g., *john.doe*)
- **mail**: the email address (e.g., *john.doe@demo.tasktop.com*)

\* RDN LDAP attribute

- **UUID LDAP attribute:** The User Unique Identification attribute is a complicated long string of characters which uniquely identify a single object within AD. For unix based LDAP this is often **uid**. The default for Microsoft AD is **objectGUID**.

\* UUID LDAP attribute

- **User Object Classes:** These are the 'types' of objects which can be used to authentication against. You can specify more if your organization has other specific identifiers such as 'staff' or 'contractor'. The default for Microsoft AD is: **person, organizationalPerson, user**.

\* User Object Classes

- **Connection URL:** This is the specific string which should be the FQDN of your LDAP service. It's default format for AD will be 'ldap://demo.tasktop.com'. If you have SSL configured then you can also use ldaps://demo.tasktop.com (SSL is not enabled by default in Microsoft AD).

\* Connection URL

**Tip:** At this point, we recommend selecting the **Test connection** button to check that Planview Hub is able to communicate with your LDAP server. You should see a green message at the top of your screen indicating a successful connection to your LDAP server.

- **Users DN:** This is the Distinguished Name for the location where you can find your users. You can find the Users DN (and any other Distinguished Names) via the **ADSIEdit** tool in Windows. Once the tool is open, you will need to connect to the AD domain for your organization. Once connected, the domain will be presented in a tree-view on the left, where you can drill down to the specific branches until you find the specific OU or User object you want details for. We recommend using this utility as it will allow you to copy/paste the specific DN information directly (any typing mistakes will result in error when testing).

The format for this string will be a number of **OU=** followed by a number of **DC=** separated by a comma.

**Tip:** Spaces are allowed in this string if they exist in your structure.

• **Users DN**

- **Authentication Type:** If using Microsoft Active Directory, you will be required to authenticate. Some non-Microsoft systems do not require authentication—if this is the case, select **none**.
- **Bind DN:** This is the Distinguished Name for the user account which you will use to authenticate against your LDAP service to allow Planview Hub to authenticate users. The Bind DN user account can be anywhere within the AD domain, however, we suggest that you have a dedicated account specifically for Planview Hub. The format for this string will be a singular **CN=** for the Canonical Name of the user account, followed by possible **OU=** which is followed by the **DC=** items all separated by a comma.

**Tip:** Spaces are allowed in the string if they exist in your structure.

• **Bind DN**   
• **Bind Credential:**

- **Bind Credential:** This is the password for the user account configured in the Bind DN.
- Tip:** Once you have entered the password, click **Test authentication** to confirm that Planview Hub is successful in authenticating itself against your Active Directory domain. You should see a green message at the top of your page as an indication of a successful authentication.

- **LDAP Filter:** This is where you will configure a filter to specify which user accounts will have access to authenticate in Planview Hub. If you leave this blank, all users within your **Users DN** OU in the AD environment will have access. The structure of the string is as follows:

- `()`: braces to start and finish
- Either
  - `&()`: for performing an 'AND' operation (i.e., all items must match)
  - `|()`: for performing an 'OR' operation (i.e., where any items can match)
- Specific attribute related condition (e.g., matching objects in a group)
- Users in a specific group can use **memberOf=**
  - `memberOf=CN=Tasktop Hub Users,OU=Resource Groups,OU=Groups,OU=Tasktop,DC=demo,DC=tasktop,DC=com`
- Users and (nested) Groups in a specific group require **memberOf:1.2.840.113556.1.4.1941:=**
  - `memberOf:1.2.840.113556.1.4.1941:=CN=Tasktop Hub Users,OU=Resource Groups,OU=Groups,OU=Tasktop,DC=demo,DC=tasktop,DC=com`
- You can also specify that a particulate attribute is equal to some value (e.g., `objectCategory=Person`)

Custom User LDAP Filter

- **Search Scope:** The Configuration of this depends on whether you have all of your AD users in a single OU, or if you'd like to search through the OU hierarchy structure. If searching, the Users DN field configured above will need to be the root or lowest-level OU.

- If all users are in a single OU, set this to **One Level**.
- If users are hierarchically organized in OUs, set this to **Subtree**.

Search Scope

- **Use Trusted SPI:** This is used if your environment uses SSL and a client certificate is required. This is not a default AD configuration.
- **Connection Pooling:** This will allow connections to your AD server to remain open if set to **ON**, (for specific timeframe) rather than creating a new connection each time a user authenticates.
- **Pagination:** This allows you to page (or cache) information for active connections from your AD servers.
- **Mappers:** Go to the **Mappers** tab at the top of the LDAP user federation you just created. Click **Username**. Ensure that **LDAP Attribute** is the same as what you entered in **Username LDAP attribute** here.

#### Kerberos

**Note:** Hub does **not** include instructions for Kerberos setup.

#### Sync Settings

- **Batch Size:** Indicates how many accounts will process at once
- **Periodic Full Sync:** Allows for a sync of all users to occur between Planview Hub and Active Directory. If you have a large number of users constantly authenticating into Hub, it may be useful to enable this. Default is set to **OFF**.
- **Periodic Changed Users Sync:** Allows for newly created or updated users to be synced from Active Directory to Planview Hub. If you have the Periodic Full Sync enabled, you should also enable this. Default is set to **OFF**.

**Tip:** Save your configuration by clicking **Save** at the bottom of the page. A green message at the top will indicate that your save was successful.

#### Additional LDAP Information

##### Testing

**Note:** The configuration utility for LDAP requires its own internal authentication. As such, when you test account access it is recommended that you use a separate browser or select a **private** or **incognito** browser. If you are already logged in to Planview Hub, you will first need to log out before testing.

1. Direct your browser to the default web address of your Hub server, such as <https://demo.tasktop.com/>
2. Enter credentials which should be allowed access to authenticate from the LDAP connection you have just setup
3. Retry with a set of credentials which should **not** have access to Hub. If you are able to log in, check the **filter** settings again.

##### Default User Access

By default, all LDAP users will be granted **user** level access to Planview Hub. If you have configured the troubleshooting user functionality (by running the script or performing manual configuration through the admin console), LDAP users will by default be granted **troubleshooting user** level access instead. If desired, you can set all new accounts, including LDAP user accounts, to default into a specific group. You can also assign different **members** to either of the **TasktopUsers** or **TasktopAdmins** groups.

To change the default group, use the following instructions:

1. Select **Groups** (under the **Manage** section) of the right-side bar menu.
2. Select the **Default Groups** tab.
3. Add or Remove the **TasktopUsers** and/or the **TasktopAdmins** groups to the **Default Groups** list.

#### User Management and Security Constraints

Planview Hub's User Management uses Security Constraints as described in the Java Servlet Specification to limit access to authenticated users. Adding additional Security Constraints to the Apache Tomcat configuration can interfere with Security Constraints provided by Planview and enable unauthenticated users to access Planview Hub.

#### DNS Settings

## DNS Settings

The server Planview Hub in installed on must be able to resolve the hostname clients will use to access it. This can be accomplished through the DNS configuration. A less preferred option is to configure using the server's hosts file.

The hostname clients use to access Planview Hub must be a valid hostname according to RFC 952. This means it may only contain letters, digits, hyphens, and periods, and may not contain underscores.

## Alternative User Management

By default, Planview Hub comes with a user management solution. In the rare scenario where your organization decides not to use Planview Hub's provided user management solution and you still need to ensure that only authorized users are able to access your Planview Hub instance, you can set up Basic Authentication for the Tomcat web server.

Additional information on configuring Tomcat authentication can be found [here](#).

**Note:** Using this style of user management will mean that all of your users will have the exact same permissions within Planview Hub. There will be no separate roles or permissions within the application.





## Introduction

On This Page

General (Settings) can be accessed by clicking the **General** tab on the **Settings** screen.

Under **General (Settings)**, you can access:

- Configuration
- Master Password Configuration
- Storage Settings

## Configuration

The **Configuration** section allows the administrator to set the change detection intervals of the connected repositories and to create a label for their Planview Hub instance identifying the environment name and type (i.e., testing or production).

\*Environment Type

Environment Name

## Change Detection

### Repeat Method

This is the method in which Hub detects changed artifacts in your external repositories.

You can configure repeat method to run on a time interval (e.g., 1 minute or 5 minutes) or an advanced schedule using cron expression (e.g., every 30 minutes from 9am-5pm from Monday to Friday).

**Configuration**

\* Change Detection

Repeat Method

Interval

\* Full Scan  Full Scan Enabled

Note: Some Planview Hub capabilities require full scans to run. Please see the [User Guide](#) for more details.

Repeat Method

Note: Please see the [User Guide](#) for more information on the differences between time interval and cron expression.

Interval

\*Integration Maximum Concurrency

\*Environment Type

Environment Name

### Change Detection Interval

This is the time between polling requests made by Hub to your external repositories to detect **only changed artifacts**.

**Note:** This defaults to **1 minute**, but can be customized as desired. This global setting can also be overridden with an integration-specific change detection interval, by updating the Change Detection settings for that integration.

**Configuration**

\* Change Detection

Repeat Method

Note: Please see the [User Guide](#) for more information on the differences between time interval and cron expression.

Interval

\* Full Scan  Full Scan Enabled

Note: Some Planview Hub capabilities require full scans to run. Please see the [User Guide](#) for more details.

Repeat Method

Note: Please see the [User Guide](#) for more information on the differences between time interval and cron expression.

Interval

\*Integration Maximum Concurrency

**\*Environment Type** Production

**Environment Name**

Cancel Restore Defaults Save

### Full Scan Interval

This is the time between polling requests to detect changed artifacts, in which all artifacts that have previously synchronized in the integration are scanned.

**Note:** The Full Scan Interval defaults to **24 hours** on the General (Settings) screen, but can be overridden with an integration-specific full scan interval, by updating the [Change Detection](#) settings for that integration.

**Configuration**

**\* Change Detection**

**Repeat Method** Time Interval

Note: Please see the [User Guide](#) for more information on the differences between time interval and cron expression.

**Interval** 1 Minutes

**\* Full Scan**  Full Scan Enabled

Note: Some Planview Hub capabilities require full scans to run. Please see the [User Guide](#) for more details.

**Repeat Method** Time Interval

Note: Please see the [User Guide](#) for more information on the differences between time interval and cron expression.

**Interval** 24 Hours

The length of time between the end of the prior scan and the beginning of the next scan.

**\*Integration Maximum Concurrency** 10

**\*Environment Type** Production

**Environment Name**

Cancel Restore Defaults Save

Not all changes to an artifact will register as a change. Some repositories do not mark items as changed — for example, when a relationship is added or an attachment has changed. These changes may **not** be picked up by regular Change Detection, but **will** be picked up by a Full Scan.

**Tip:** Review our [connector docs](#) to determine the type of updates that will require a full scan.

### Disable Full Scan

Full scans can be disabled globally on the General (Settings) screen, or on a per-integration basis via the [Change Detection](#) screen. This feature is especially useful for users that do not want to overload their repositories.

To disable full scan, uncheck the **Full Scan Enabled** box for the desired collection.

**Note:** If you choose to disable full scans, [Twinless Artifact Updates](#) will not work and some artifact updates may be missed.

**Configuration**

**\* Change Detection**

**Repeat Method** Time Interval

Note: Please see the [User Guide](#) for more information on the differences between time interval and cron expression.

**Interval** 1 Minutes

**\* Full Scan**  Full Scan Enabled

Note: Some Planview Hub capabilities require full scans to run. Please see the [User Guide](#) for more details.

**Repeat Method** Time Interval

Note: Please see the [User Guide](#) for more information on the differences between time interval and cron expression.

**Interval** 24 Hours

**\*Integration Maximum Concurrency**

**\*Environment Type**

**Environment Name**

**Process All Artifacts**

Since the Full Scan only scans artifacts that have previously synchronized, artifacts that are newly eligible for synchronization due to updated artifact filtering or routing will not be picked up by the Full Scan.

These artifacts will only be processed by clicking [Process All Artifacts](#) on the [Field Flow](#) screen, or when a new integration-eligible change is made to them.

**Integration Maximum Concurrency**

This limits the number of events processed concurrently by each integration. Increasing this value will enable more artifact changes to flow concurrently, whereas decreasing this value will reduce the level of concurrent changes. Changing this value has the potential to affect the load on the end-points of an integration, and may have an adverse effect on performance if set too high.

**Note:** The default setting is **10**, and should be used unless advised otherwise by customer care.

**Configuration**

**\* Change Detection**

**Repeat Method**

Note: Please see the [User Guide](#) for more information on the differences between time interval and cron expression.

**Interval**

**\* Full Scan**  Full Scan Enabled

Note: Some Planview Hub capabilities require full scans to run. Please see the [User Guide](#) for more details.

**Repeat Method**

Note: Please see the [User Guide](#) for more information on the differences between time interval and cron expression.

**Interval**

**\*Integration Maximum Concurrency**

**\*Environment Type**

**Environment Name**

Limits the number of events processed concurrently by each integration.

**Environment Type and Name**

Hub administrators can also set an environment type (testing or production) and name for their instance in the Configuration panel. This will create a label visible in the upper left corner of the screen while navigating throughout the Hub UI, to allow users to easily identify which Hub instance they are utilizing.

**Configuration**

**\* Change Detection**

**Repeat Method**

Note: Please see the [User Guide](#) for more information on the differences between time interval and cron expression.

**Interval**

**\* Full Scan**  Full Scan Enabled

Note: Some Planview Hub capabilities require full scans to run. Please see the [User Guide](#) for more details.

**Repeat Method**

Note: Please see the [User Guide](#) for more information on the differences between time interval and cron expression.

**Interval**

\*Integration Maximum Concurrency: 10

\*Environment Type: Testing

Environment Name: Testing Sandbox

Buttons: Cancel, Restore Defaults, Save

Once set, you will see the environment type and name label displayed in Hub.

The screenshot shows the Planview Hub interface. At the top left, there's a navigation bar with 'Planview Hub' and icons for Integrations, Collections, Models, and Repositories. On the right, there are icons for History, Activity, Metrics, Help, and Settings. The main content area has a blue background with the text 'Connecting the World of Software Delivery'. Below this, there are three bullet points: 'Create integrations in minutes', 'Explore key integration concepts', and 'Learn how to easily scale your integrations'. A 'Start Connecting' button is at the bottom left. On the right, there's a diagram showing the flow of software delivery: Project and Portfolio Management (Epic) -> Requirements Management (Feature) -> Application Lifecycle Management (Build Failure) -> Test Cases (Defect) -> Information Technology Service Management (Support Ticket) -> Project and Portfolio Management (Epic). The diagram also includes icons for BMC and codebeamer.

Aha!	Apptio TargetProcess	Aras Innovator	Asana
Atlassian Jira	Atlassian Jira Align	Blueprint	BMC Remedy
Broadcom Clarity	Broadcom Rally	Cherwell Service Management	codebeamer
Digital.ai Agililty	Digital.ai Release	Git	GitHub Issues

## Master Password Configuration

After installation, you will be prompted to set a Master Password.

**Settings**  
View and manage your application settings.

**Master Password Configuration**

Before continuing, you must configure the master password that Tasktop will use for credential encryption.

Master Password: [password field]

Confirm Password: [password field]

Save

The Master Password is used to encrypt the credentials used in your repository connections and proxy settings, along with any other configuration values that are considered secret, which could include API keys and tokens.

**Note:** 256 bit AES encryption is used.

Hub will automatically use the stored Master Password to decrypt repository credentials.

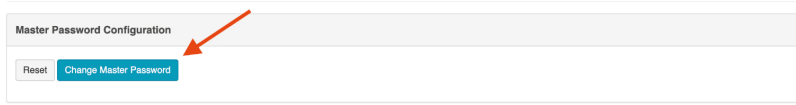
Normally you will not need to re-enter your Master Password. However, if the stored Master Password is missing, or if you'd like to change your Master Password from the General (Settings) screen, you will need to enter your current Master Password.

The Master Password is encrypted and stored separately from the encrypted repository credentials.

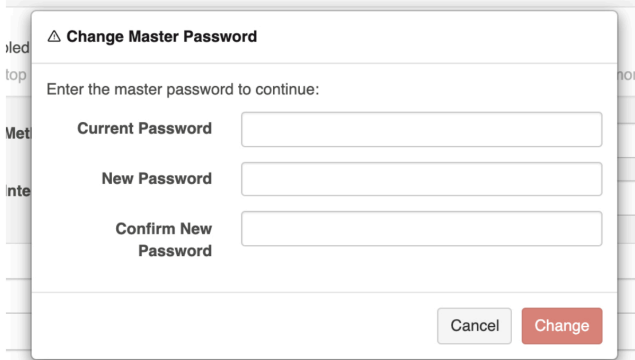
- On **Windows**, the encrypted Master Password is stored in the Windows Registry, encrypted using the Windows Data Protection (DPAPI).
- On **Linux**, the encrypted Master Password is stored in the Home Directory of the User running Hub.

If desired, you can change or reset the Master Password from the General (Settings) screen.

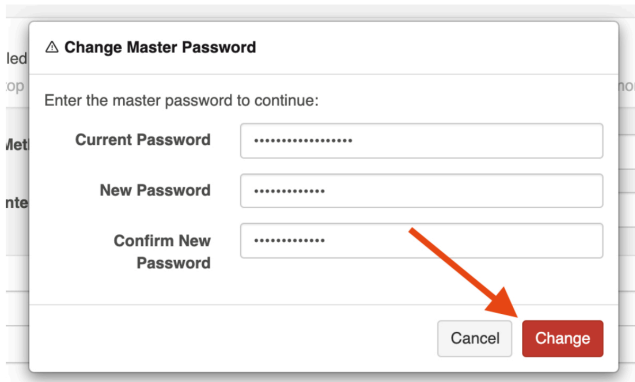
To do this, click **Change Master Password**.



Enter your current Master Password and new Master Password.

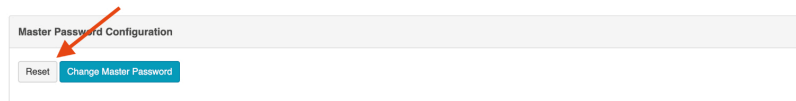


Click **Change** to update the Master Password.



To reset your master password, click **Reset**.

**Note:** If resetting the Master Password, you will not need to enter your current Master Password, but previously encrypted repository passwords will be lost, and must be provided after resetting.



## Storage Settings

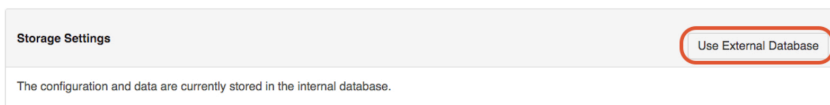
Planview automatically stores operational data to a pre-configured Derby database. This is suitable for evaluation purposes only, and is **not** supported for production environments. Configuring Hub to utilize an external database will enable you to perform frequent back-ups without having to stop Hub, and ensure that your Hub practices are consistent with your existing disaster and recovery process.

**Tip:** See our [Hardware Requirements](#) to determine which databases are supported for storing operational data.

## Migrating Databases

### Internal to External

To migrate your Hub operational data from the internal database to an external database, click **Use External Database**.



Next, click **Configure JDBC Driver** to select the JDBC driver for your database.

To download the JDBC driver:

### Microsoft SQL Server

The JDBC driver for Microsoft SQL Server can be downloaded from the [Microsoft support site](#).

**Note:** Planview Hub currently supports the 9.4 version.

### MySQL

The JDBC driver for MySQL can be downloaded from the [MySQL download site](#).

**Note:** Upon downloading the JDBC driver from the MySQL download site, select **Platform Independent** to download the correct file.

### Oracle

The JDBC driver for Oracle can be downloaded from the [Oracle support site](#). Note that it is best if the Oracle JDBC driver that is used matches the version of the Oracle server that you are connecting to.

### PostgreSQL

The JDBC driver for PostgreSQL can be downloaded from the [PostgreSQL download site](#).

To upload the JDBC driver to Hub, a system administrator (a user with file system access to the machine that hosts Hub) must extract the **\*.jar** file from the downloaded driver file and add the file to the designated directory:

- On **Windows**, the default folder is `C:\ProgramData\Tasktop\jdbc-drivers`
- On **Linux**, the `jdbc-drivers` folder can be found in the Hub installation directory

**Note:** If needed, the user can change the location in which Hub looks for the files. This is done by changing the system property `jdbc.libraries.path`

Once the JDBC driver is uploaded, select it from the **Choose File** field on the Configure JDBC Driver pop-up.

Next, fill out the Database Connection credentials — enter the location, username, and password.

**Note:** Authentication credentials **must** be in SQL server authentication mode (i.e., mixed-mode with SQL credentials). Windows authentication mode is **not** supported.

Location formats are as follows:

### Microsoft SQL Server

`jdbc:sqlserver://hostServerName;instanceN...MyDatabaseName`

### MySQL

`jdbc:mysql://hostServerName:mysqlServerPort/MyDatabaseName`

### Oracle

`jdbc:oracle:thin:@hostServerName:oracleServerPort/SID`

## PostgreSQL

`jdbc:postgresql://hostServerName:postgresServerPort/MyDatabaseName`

**Note:** If you use a custom schema, you will need to add `?currentSchema=tasktop` to the URL (e.g., `jdbc:postgresql://example.com:5432/dbName...Schema=tasktop`).

If you'd like, you can also update the **Backoff Interval** setting.

The **Backoff Interval** is the time Hub will wait after a database connection failure (e.g., invalid username or password) before retrying the connection. This feature is especially useful for databases with a lockout or brute force policy configured.

**Note:** While backoff is in effect, processing artifacts will display an error and some operations may not work (e.g., you may be automatically redirected to the Settings screen). Once the backoff interval expires, artifacts will resume processing and operations will return to normal.

Storage Settings

Configuring External Database for Storage  
Need help? Please refer to the [Tasktop Integration Hub User Guide](#).

JDBC Driver

Database Connection

Location

Username

Password

Backoff Interval  Hours

The backoff interval defaults to **one hour**, but can be customized as desired.

Storage Settings

Configuring External Database for Storage  
Need help? Please refer to the [Tasktop Integration Hub User Guide](#).

JDBC Driver

Database Connection

Location

Username

Password

Backoff Interval  Hours ▾

- Milliseconds
- Seconds
- Minutes
- Hours

After you've added your database connection credentials, click **Test Connection** to confirm that your credentials have been accepted by Hub.

**Note:** If backoff is in effect, the Test Connection button will continue to work so you can test and save updated credentials.

Storage Settings

Configuring External Database for Storage  
Need help? Please refer to the [Tasktop Integration Hub User Guide](#).

JDBC Driver

Database Connection

Location

Username

Password

Backoff Interval  Hours

Once confirmed, click **Save**.

Storage Settings

Configuring External Database for Storage  
Need help? Please refer to the [Tasktop Integration Hub User Guide](#).

JDBC Driver

Database Connection

Location

Username

Password

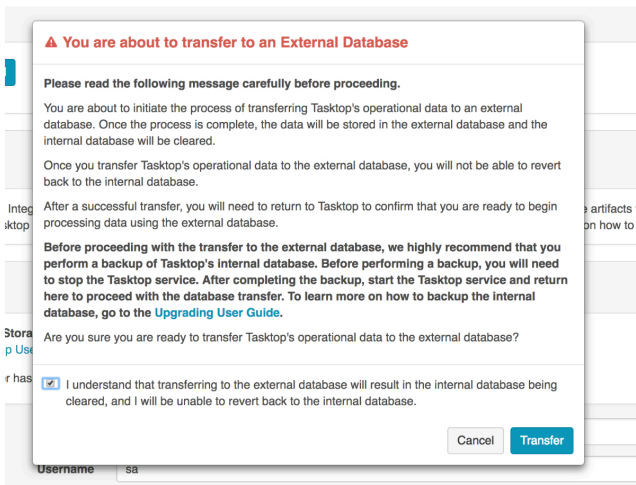
Backoff Interval  Hours

A warning message will appear telling you that you are about to transfer to an External Database. Review the entire message, **ensuring that you have performed the recommended data backup**.

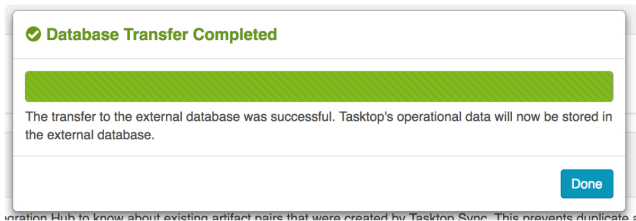
If you'd like to continue the transfer, click the checkbox and then click **Transfer**.



If you click to continue the transfer, click the checkbox and then click **Transfer**.



A **Database Transfer Completed** message will appear once the transfer is complete, informing you that your operational data has been successfully transferred from Hub's internal database to your own external database.



## External to External

If you'd like to migrate your data from one external database to a different external database, **you will need to manually transfer the data from the current database to the new target database**. If you do not manually transfer the data, Hub will not work properly once you switch to the target database settings. **Hub will not automatically transfer this data for you.**

If you are simply updating the location or credentials of your current external database and will continue using the same database, you do not need to transfer any data. Hub will continue to work properly.

### Moving between databases of the same type...

If you are migrating to a database of the same type (e.g., moving from one MySQL database to a different MySQL database), follow the instructions below:

1. Transfer data from the old database to the new database.
2. Update the Location, Username, and/or Password fields in the Database Connection section.
3. Click **Test Connection** and then **Save**.
4. A warning message will then appear, ensuring you have taken all necessary steps. After reviewing the message, click the checkbox and then **Save**.

### Moving between databases of different types...

If you are migrating to a database of a different type (for example, moving from a MySQL database to an Oracle database), follow the instructions below:

1. Create a new empty database in the new database.
2. Stop Hub.
3. Manually replace the jdbc driver jar in `<program data>/Tasktop/drivers` with the correct driver for the new database (not in `<program data>/Tasktop/jdbc-drivers`, because the new driver cannot be selected in the UI), and make sure it is named `database-driver.jar`.
4. Manually edit `<program data>/Tasktop/db/tasktop-db.json` with the URL and credentials for the new database.
5. Start Hub.
6. Hub will create new empty tables in the new database.
7. Stop Hub.
8. Copy all the data from the tables in the old database to the tables in the new database, except the tables `DATABASECHANGELOG` and `DATABASECHANGELOGLOCK` (copying data for these two tables will cause errors).
9. Start Hub.

## If your Database Transfer Fails or is Aborted

If your database transfer fails or is aborted, Hub will continue to use its internal database to store operational data. The internal database is not cleared until a successful transfer is completed, so you should not notice any change in performance.

However, we do recommend reviewing the external database and clearing any data and tables that were created as part of the failed data transfer before starting the transfer process again.

## Overriding Database Access

In order to prevent risk of collisions, duplicates, and other errors, Hub has functionality to ensure that multiple Hub instances cannot run on the same operational database.

If you connect your instance to a database that is already in use by Hub (this is **not** recommended), upon start-up of the new instance, the prior instance will lose database access and stop processing events. When you login to the prior instance, you will see an error message prompting you to either update your credentials to connect to a different database, or to override database access. If you override database access, this means that the other instance of Hub will lose access to that database.

When overriding, be sure to confirm that no other Hub instance is using the database before moving forward. If another Hub instance is actively using the database, it is recommended that you shut down the other instance of Hub before proceeding.

### Settings

View and manage your application settings.

[Back to Database Transfer](#)

**⚠** The database appears to currently be in use and is denying access to your Tasktop instance. To resolve this, you can change your external database settings to point to another external database, or you can "Override Database Access" to allow your current instance to use the database.

---

### Storage Settings

**Using External Database for Storage**  
Need help? Please refer to the [Tasktop User Guide](#).

**JDBC Driver** Driver has been uploaded. [Change](#)

**Database Connection**

**Location** jdbc:sqlserver://database:1433;databaseName=tasktop

**Username** databaseUser

**Password** \*\*\*\*\*

[Cancel](#)  [Test Connection](#) [Save](#)

---

**Database Access**

[Override Database Access](#)

**⚠** The database is in use by another instance of the application. Tasktop's database is in use by another instance of the application. (CCRRTT-30012E)

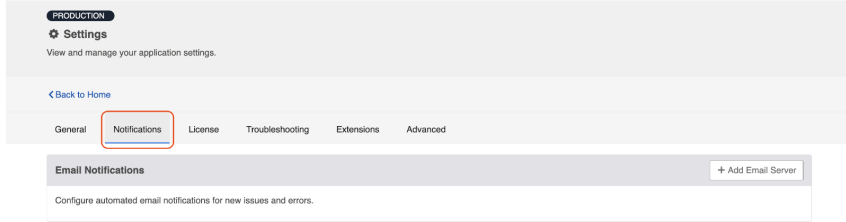
[Show less](#)



## Introduction

On This Page

Notifications can be accessed by clicking the **Notifications** tab on the **Settings** screen.



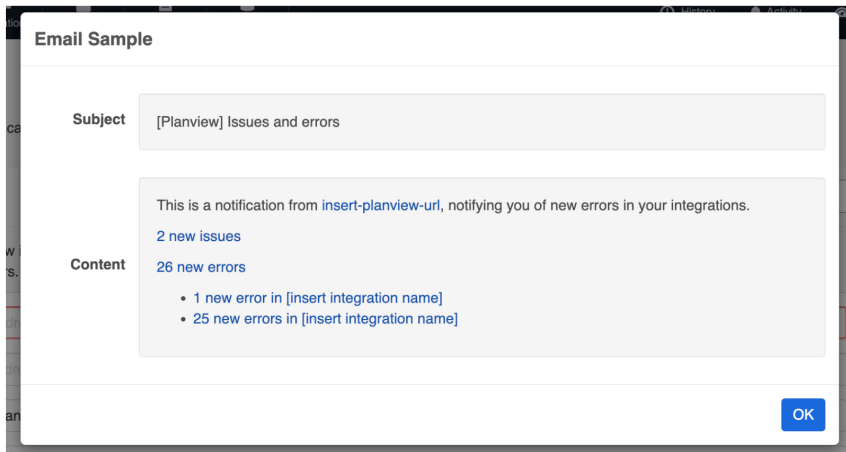
Under **Notifications**, you can access:

- Email Notifications

## Email Notifications

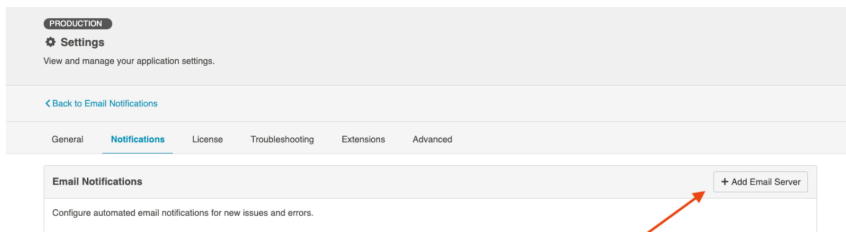
To facilitate troubleshooting, you can configure automated email notifications for new errors and issues encountered in Planview Hub.

Emails will contain a count of new issues and errors (excluding **ignored errors**) since the last email notification, and a link to the Activity screen to view the errors/issues. Emails will be sent only if a new error or issue occurs.

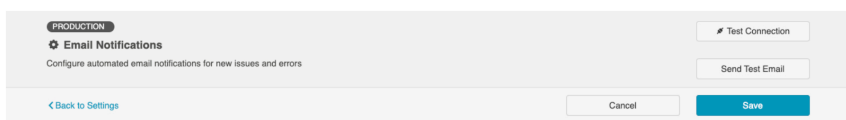


## Configuring Email Notifications

To configure email notifications click **+Add Email Server**.



This will bring you to the **Email Notifications** screen.



Emails will contain a count of new issues and errors since the last email notification, and a link to the Activity screen to view the errors/issues. Emails will be sent only if a new error or issue occurs. ([View Email Sample](#))

**To Email Addresses**

**From Address**

**Subject Prefix**

**Tasktop Server URL**

**Notification Frequency**  **Minutes** -

---

**Username**

**Password**

**SMTP Server**

**SMTP Port**

**Connection Timeout**  **Minutes** -

**Protocol**

**Basic Details**

Configure basic details for email notifications. Multiple email addresses separated by commas can be added to receive notifications.

**Email Server Settings**

Configure email server settings to allow Tasktop Integration Hub to send notifications.

The form requires that the following fields be filled out:

**Basic Details**

- **To Email Address:** The email address that will receive the notifications. This field is limited to one email address.
- **From Email Address:** The email address listed in the 'sender address' (or 'from') field of notification emails sent by Hub. In many cases, this will match the email whose settings are configured in the 'Email Server Settings' section below, though a different email (such as `no-reply@email.com`) can be configured here. If a user were to hit 'reply' on an email notification, this is the email the reply would be sent to.
- **Subject Prefix (optional):** The prefix appended to the subject line of the Error Notification emails. This defaults to [Tasktop] but can be edited if needed. This can help users filter email notifications from Tasktop based on prefix.
- **Tasktop Server URL:** The URL used to access your instance of Hub. This is used to construct links to errors and issues in the notification emails.
- **Notification Frequency:** The frequency of email notifications. Emails will contain a count of new issues and errors since the last notification and will only send if a new error or issue has occurred since the prior email.

**Email Server Settings**

These are the email server settings that allow Hub to send notifications.

- **Username (optional):** Username for the authenticated SMTP server.
- **Password (optional):** Password for the authenticated SMTP server.
- **SMTP Server:** The SMTP host name of your mail server.
- **SMTP Port:** The SMTP Port number to use.
  - If Protocol = SMTP, the value for this will typically be 25.
  - If Protocol = SMTPS, the value for this will typically be 465.
  - If Protocol = SMTP\_STARTTLS, the value for this will typically be 587, but can also be port 25.
- **Connection Timeout:** Specifies the maximum period, in seconds, that establishing an email server connection is permitted to take. This defaults to 60 seconds, which should cover most scenarios.
- **Protocol**
  - **SMTP:** Basic unencrypted SMTP Protocol.
  - **SMTPS:** A more advanced, encrypted SMTP Protocol (SMTP Secure), which will perform server certificate validation.
  - **SMTP\_STARTTLS:** A modern protocol that wraps the unencrypted SMTP protocol in TLS (formerly known as SSL encryption), and will perform server certificate validation. This will attempt the STARTTLS wrapper, but if it is not supported by the server, the client will fall back to basic SMTP.

**Note:** Google email users should select SMTP\_STARTTLS.

Here's an example of a filled in form:

**PRODUCTION** Test Connection

**Email Notifications** Send Test Email

Configure automated email notifications for new issues and errors

[Back to Settings](#) Cancel Save

Email Notifications are off. Turn On Notifications

Emails will contain a count of new issues and errors since the last email notification, and a link to the Activity screen to view the errors/issues. Emails will be sent only if a new error or issue occurs. ([View Email Sample](#))

**To Email Addresses**

**From Address**

**Subject Prefix**

**Tasktop Server URL**

**Notification Frequency**  **Minutes** -

---

**Username**

**Password**

**SMTP Server**

**SMTP Port**

**Connection Timeout**  **Minutes** -

**Protocol**

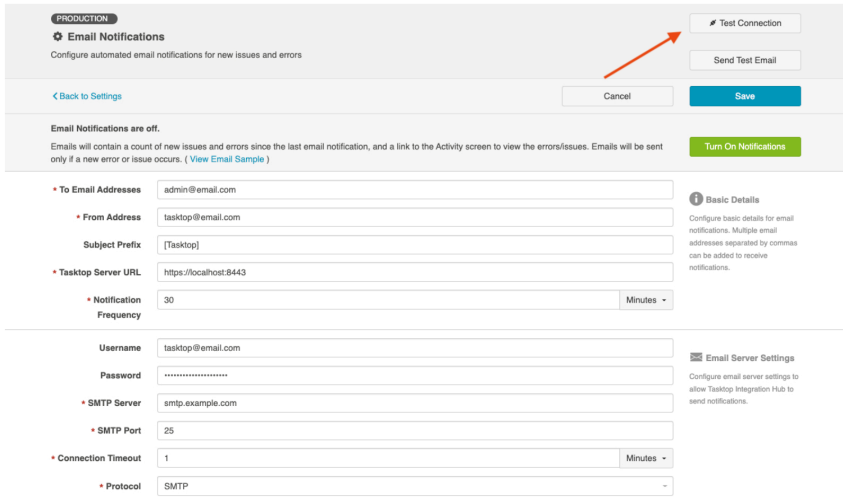
**Basic Details**

Configure basic details for email notifications. Multiple email addresses separated by commas can be added to receive notifications.

**Email Server Settings**

Configure email server settings to allow Tasktop Integration Hub to send notifications.

You can test your email server settings by clicking **Test Connection**.



**PRODUCTION**  
**Email Notifications**  
Configure automated email notifications for new issues and errors

[Back to Settings](#)

**Email Notifications are off.**  
Emails will contain a count of new issues and errors since the last email notification, and a link to the Activity screen to view the errors/issues. Emails will be sent only if a new error or issue occurs. ([View Email Sample](#))

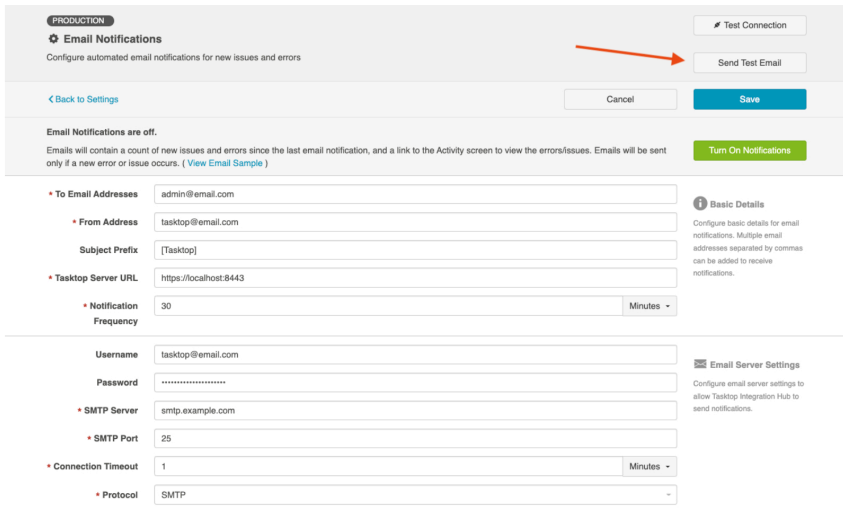
**To Email Addresses**   
**From Address**   
**Subject Prefix**   
**Tasktop Server URL**   
**Notification Frequency**  Minutes

**Basic Details**  
Configure basic details for email notifications. Multiple email addresses separated by commas can be added to receive notifications.

**Email Server Settings**  
Configure email server settings to allow Tasktop Integration Hub to send notifications.

**Username**   
**Password**   
**SMTP Server**   
**SMTP Port**   
**Connection Timeout**  Minutes  
**Protocol**

Or, send a test email by clicking **Send Test Email**.



**PRODUCTION**  
**Email Notifications**  
Configure automated email notifications for new issues and errors

[Back to Settings](#)

**Email Notifications are off.**  
Emails will contain a count of new issues and errors since the last email notification, and a link to the Activity screen to view the errors/issues. Emails will be sent only if a new error or issue occurs. ([View Email Sample](#))

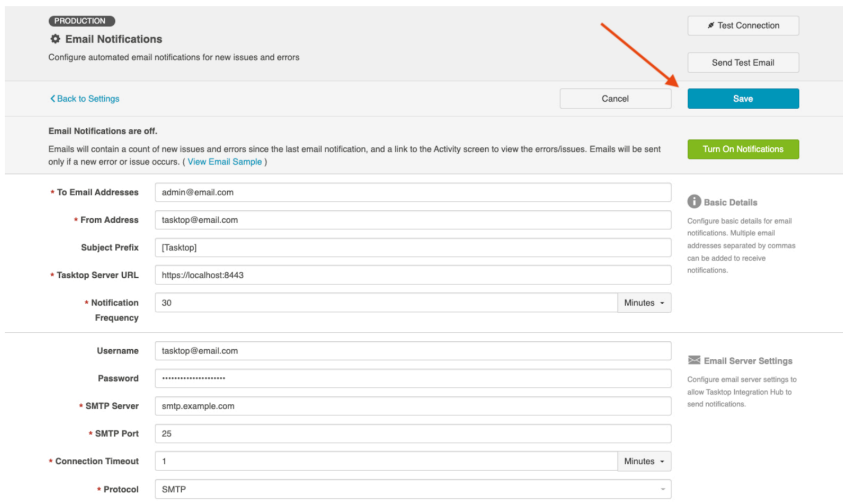
**To Email Addresses**   
**From Address**   
**Subject Prefix**   
**Tasktop Server URL**   
**Notification Frequency**  Minutes

**Basic Details**  
Configure basic details for email notifications. Multiple email addresses separated by commas can be added to receive notifications.

**Email Server Settings**  
Configure email server settings to allow Tasktop Integration Hub to send notifications.

**Username**   
**Password**   
**SMTP Server**   
**SMTP Port**   
**Connection Timeout**  Minutes  
**Protocol**

Once settings are filled in and the connection has been tested, click **Save** to save your settings.



**PRODUCTION**  
**Email Notifications**  
Configure automated email notifications for new issues and errors

[Back to Settings](#)

**Email Notifications are off.**  
Emails will contain a count of new issues and errors since the last email notification, and a link to the Activity screen to view the errors/issues. Emails will be sent only if a new error or issue occurs. ([View Email Sample](#))

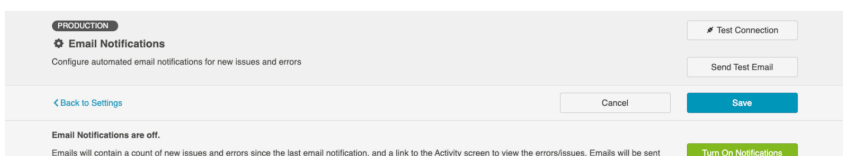
**To Email Addresses**   
**From Address**   
**Subject Prefix**   
**Tasktop Server URL**   
**Notification Frequency**  Minutes

**Basic Details**  
Configure basic details for email notifications. Multiple email addresses separated by commas can be added to receive notifications.

**Email Server Settings**  
Configure email server settings to allow Tasktop Integration Hub to send notifications.

**Username**   
**Password**   
**SMTP Server**   
**SMTP Port**   
**Connection Timeout**  Minutes  
**Protocol**

Click **Turn On Notifications** to enable email notifications.



**PRODUCTION**  
**Email Notifications**  
Configure automated email notifications for new issues and errors

[Back to Settings](#)

**Email Notifications are off.**  
Emails will contain a count of new issues and errors since the last email notification, and a link to the Activity screen to view the errors/issues. Emails will be sent only if a new error or issue occurs. ([View Email Sample](#))

only if a new error or issue occurs. ( [View Email Sample](#) )

• **To Email Addresses**

• **From Address**

**Subject Prefix**

• **Tasktop Server URL**

• **Notification Frequency**  **Minutes** ▾

---

**Username**

**Password**

• **SMTP Server**

• **SMTP Port**

• **Connection Timeout**  **Minutes** ▾

• **Protocol**

**Basic Details**

Configure basic details for email notifications. Multiple email addresses separated by commas can be added to receive notifications.

**Email Server Settings**

Configure email server settings to allow Tasktop Integration Hub to send notifications.

Once saved, you can turn email notifications on or off and delete the notification settings from the Notifications screen. You can also click **Configure Notification Settings** to modify your existing settings:

**Email Notifications** [Configure Notification Settings](#)

**Email Notifications are on.**

Emails will contain a count of new issues and errors since the last email notification, and a link to the Activity screen to view the errors/issues. Emails will be sent only if a new error or issue occurs. ( [View Email Sample](#) )

**From Email:** tasktop@email.com  
**To Email:** admin@email.com

[Turn Off Notifications](#) [Delete Notification Settings](#)

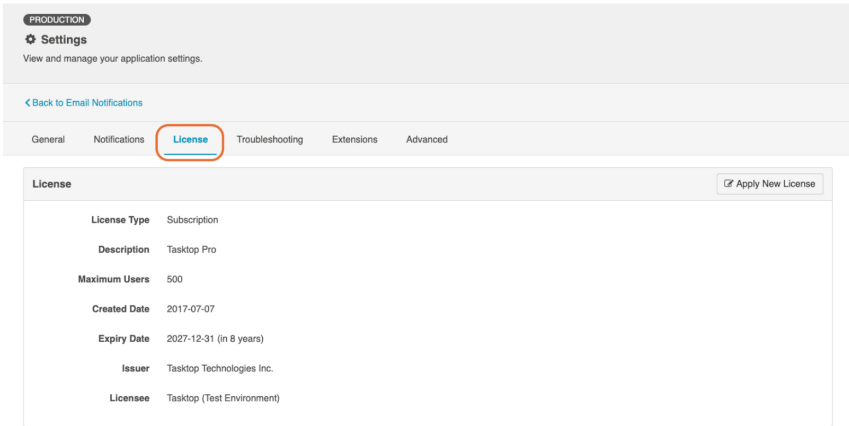
**Note:** If an email notification fails, an issue will be surfaced on the [Activity](#) screen in Hub.



## Introduction

On This Page

You can access your License details by clicking the **License** tab on the **Settings** screen.

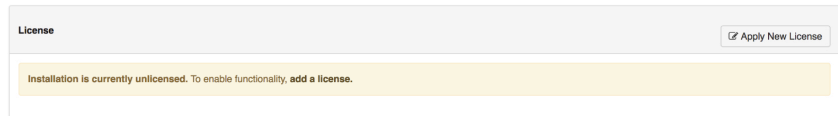


Under **License**, you can access:

- License
- Logging

## License

A license is required to run the application. Upon initial log-in, you will see that your product is currently un-licensed:

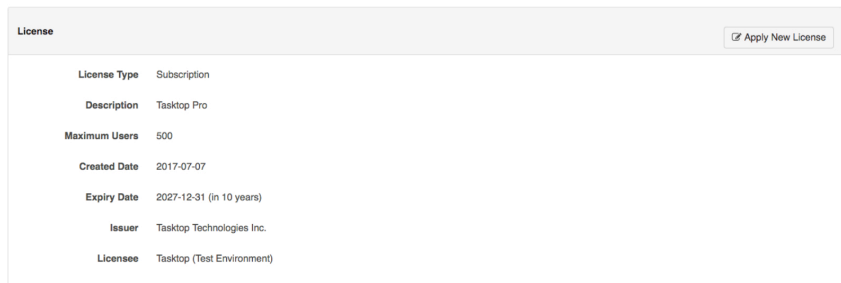


Click **Apply New License** to enter your license.

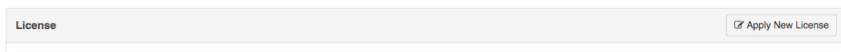
The **Master Password** must be set and the License must be entered before the application can be used.

On the License panel, you will see the following information:

- License Type
- Description
- Maximum Users
- Created Date
- Expiration Date
- Issuer
- Licensee



You will also see a warning if your license is expired:



**License Expired**  
To renew your license, please contact [Tasktop Support](#).

License Type	Trial
Description	Tasktop Ultimate
Maximum Users	500
Estimate of Connected Users	1
Created Date	1969-12-31
Expiry Date	2018-07-23 (expired)
Issuer	Tasktop Technologies Inc.
Licensee	Tester

Should your license expire, in addition to seeing a warning on the License screen, you'll also see that an issue is surfaced on the Activity screen:

**Activity**  
See detailed information about activity across your integrations and about any configuration issues with your integration components.

[Back to Settings](#)

Issues: 3
Current Activity: 0
Pending: 0
Processing: 0
Errors: 0
Past Activity: 0

**Issue Details:**

**ID:** CCRRTT-15008E **Created:** 35 minutes ago

**Message:** Integration services cannot be started since the current license has expired. License expiry date is 2014-12-31.  
**Related Configuration Elements:**

**Description**  
Tasktop integration services cannot be started because the current license has expired.

**User Action**  
This problem can be resolved by installing a valid license using the following steps:

1. Obtain a valid license by contacting the [Tasktop Support Center](#)
2. Navigate to the settings page
3. Press the Apply New License button under License
4. Paste in the license text and press Save

When your license is expired, you can still navigate within the Planview Hub UI, but your integrations will be stopped from running. Note that though they will still display the **Run** or **Stopped** state they were in at the time your license expired, no artifacts will process in an integration until a new license is applied.

**Note:** Please consult your license agreement or contact your account representative if you have any questions about your license settings or usage policy.





## Introduction

[On This Page](#)

Advanced (Settings) can be accessed by clicking the **Advanced** tab on the **Settings** screen.

**PRODUCTION**  
Settings  
View and manage your application settings.

[Back to Home](#)

General Notifications License Troubleshooting Extensions **Advanced**

**Flow External Workflow Changes**

'Flow external workflow changes' ensures that Planview Hub detects and flows workflow changes more robustly, especially those triggered by external sources like repositories.

Flow external workflow changes in the following integrations:

Filter Integrations

Jama Defects ↔ Jira Defects  
 Xray Tests ↔ Jama Test Cases  
 TestResults-TestExecution  
 DOORS Next Requirements → Polarion Requirem...  
 Jama Requirements ↔ Jira Stories  
 WhiteHat Vulnerabilities → Jira Defects

Jama Stories ↔ Jira Stories  
 TestSet Folder ↔ Test Set  
 Asana Tasks ↔ LeanIX Stories  
 AgilePlace Cards to Ahal Ideas  
 Jira Stories ↔ qTest Requirements

Jama Requirements ↔ Jira Epics  
 JamaDefects ↔ XrayDefects  
 Asana Tasks ↔ Jira Stories  
 Ahal Features to Jira Epics  
 Jira to Jama Defects

**Move Routes Between Integrations** [Move Routes](#)

Move existing routes from one integration to another. Integrations must share the same artifact types and repositories. This feature can be used to facilitate ALM upgrades or to merge or split existing synchronization integrations.

**Import Artifact Pair Information** [Import](#)

Importing artifact pair information allows Planview Hub to recognize existing artifact pairs created by another Planview Hub instance and determine if the artifacts are current. This prevents duplicate artifacts and data from being created when moving existing artifact pairs between Planview Hub instances. Please contact Planview Support for additional information on how to use

Under **Advanced**, you can access:

- Flow External Workflow Changes
- Move Routes Between Integrations
- Import Artifact Pair Information
- Upgrade Backup Files
- Import Configuration

## Flow External Workflow Changes

Flowing external workflow changes allows you to specify the integrations that should receive high-fidelity scans to ensure that changes that might have been missed during a regular change detection interval are detected.

**Note:** Enabling this setting for all integrations may have a negative impact on Planview Hub's performance.

## Move Routes Between Integrations

There may be rare scenarios when you must move routes from an existing integration to another integration. For example, you may have configured Hub incorrectly and mistakenly created multiple integrations which should be combined into one. Or you could be upgrading Micro Focus ALM, which requires moving projects from an instance running an old version of ALM to a server running a newer instance of ALM. Since existing projects are moved to a completely new ALM instance with a different URL, users must create a new repository connection, collection(s), and integration(s) in Hub. Once the new integration is created, existing routes must be migrated to prevent the risk of duplicate artifacts. This feature will allow users to easily migrate routes from an existing integration to a new one.

To move routes from one integration to another, they must both:

- Be synchronize integrations
- Use the same artifact types
- Use the same repository connections (except for Micro Focus ALM connections used in an upgrade scenario)

We recommend stopping both integrations before moving routes so that you can review your mappings and configuration before running.

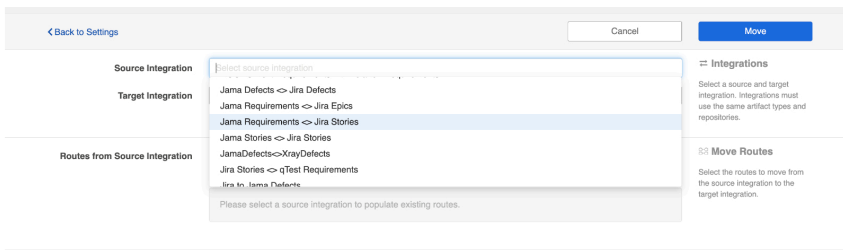
To use this feature, click **Move Routes**.

**Move Routes Between Integrations** [Move Routes](#)

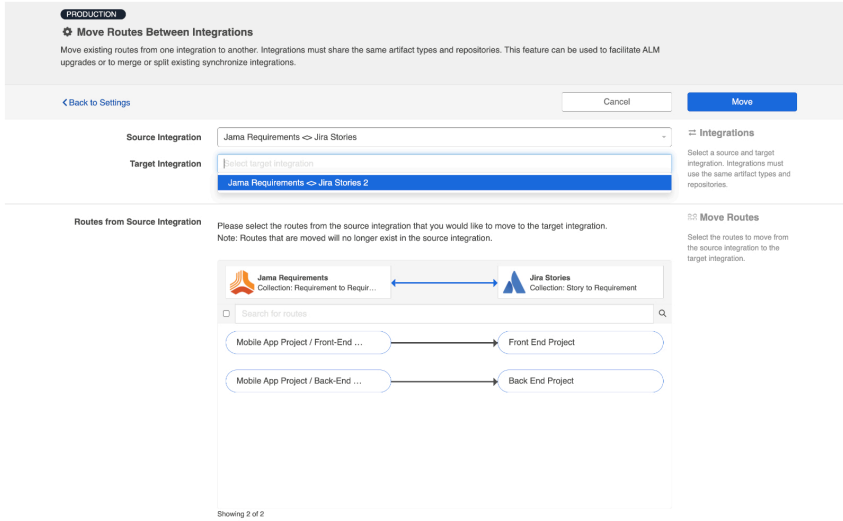
Move existing routes from one integration to another. Integrations must share the same artifact types and repositories. This feature can be used to facilitate ALM upgrades or to merge or split existing synchronization integrations.

Select your source integration:

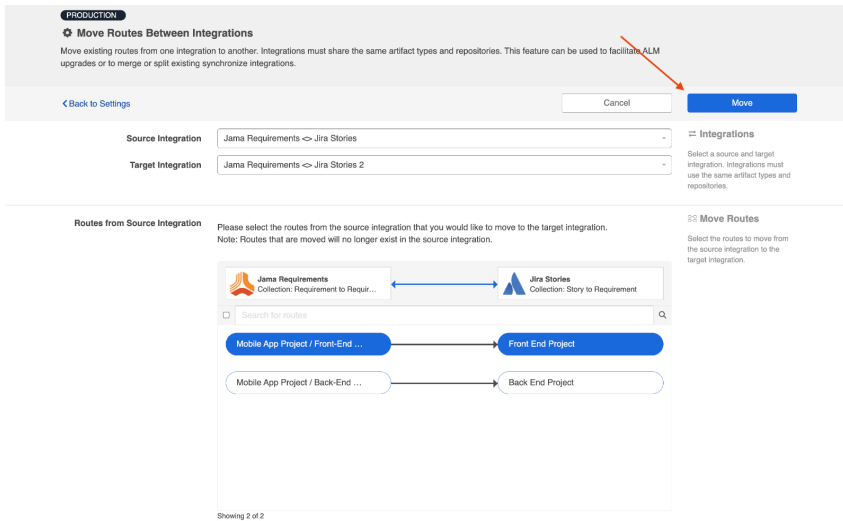
**PRODUCTION**  
Move Routes Between Integrations  
Move existing routes from one integration to another. Integrations must share the same artifact types and repositories. This feature can be used to facilitate ALM upgrades or to merge or split existing synchronization integrations.



Then select your target integration:



Select the routes from the source integration that you'd like to move to the target integration. Once moved, they will no longer exist in the source integration. Click **Move** in the upper right corner.



Review the pop-up message and if approved, click **I understand...** and **Move**. This process may take some time. Progress can be tracked on the Background Jobs tab of the **Activity Screen**.

Once the move is complete, review your integration configuration, field mappings, etc, before clicking **run** on the target integration.

## Import Artifact Pair Information

Importing artifact pairs allows Hub to import existing artifact pairs that were created by Tasktop Sync. This prevents duplicate artifacts from being created when you switch from using Tasktop Sync to Planview Hub to administer your integrations.

Please [contact customer care](#) for additional information on how to use this capability.

## Upgrade Backup Files

*This feature is only available when upgrading from Planview Hub versions 20.1 and later.*

Upgrading backup files enables you to download and upload artifact data in cases where integrations were resumed individually during an upgrade. The downloaded data corresponds to artifacts that were modified when migrations were still running. These files capture any synchronization activity that occurred on individually running integrations, so that you can ensure no updates are duplicated if restoring from backup.

# Supported Repository Versions

You are viewing content for Planview Hub version 22.4. [View another version](#) ▼



## Planview Hub 22.4 (October 18, 2022)

If you are interested in extended support, please reach out to [customer care](#) before the date specified here.

Repository	General Support (Planview Hub 22.4)
Aha!	Current On Demand (Cloud) Version
Apptio Targetprocess	Current On Demand (Cloud) Version
Aras Innovator	11.0 SP15
Asana	Current On Demand (Cloud) Version
Atlassian Jira Core	8.22, 9.0, 9.1, 9.2, 9.3 Support All Patch Versions Current On Demand (Cloud) Version
Atlassian Jira Software	8.22, 9.0, 9.1, 9.2, 9.3 Support All Patch Versions Current On Demand (Cloud) Version
Xray Test Management for Jira	6.x Support All Patch Versions Current On Demand (Cloud) Version
Atlassian Jira Service Management	4.22, 5.0, 5.1, 5.2 Support All Patch Versions
Atlassian Jira Align	Current On Demand (Cloud) Version
Blueprint	13.1, 13.2, 13.3 Support All Patch Versions Current On Demand (Cloud) Version <b>Note:</b> With the release of Blueprint version 11.2, Blueprint Storyteller has been rebranded as Blueprint. Blueprint Storyteller versions 4.0 - 5.1 remain supported.
BMC Helix ITSM (formerly Remedy)	19.02, 19.08, 19.11, 20.02

Support All Patch Versions



Broadcom Clarity

16.0.0

Support All Patch Versions

Current On Demand (Cloud) Version

Broadcom Rally

2018.1, 2.0, 2.1.0

Support All Patch Versions

Current On Demand (Cloud) Version



Cherwell Service Management

10.0.2

(Only available for Planview OEM)



codebeamer

Support All Patch Versions



Digital.ai Agility

Support All Patch Versions

Current On Demand (Cloud) Version

Digital.ai Release

22.3



Git

All

**\*Note:** If using a supported Git Hosting Service, the version of the service used does not impact functionality. It is used to determine commit location.



GitHub Issues

Current On Demand (Cloud) Version



GitLab

GitLab Issues

Enterprise and Community Edition:

14.x, 15.x

Support All Patch Versions

Current On Demand (Cloud) Version



IBM Rational ClearQuest

9.1.0

IBM Engineering Requirements  
Management DOORS Family

9.7, 9.7.1, 9.7.2, 9.7.2.4

IBM Engineering Requirements  
Management DOORS Next

7.0.2

IBM Engineering Workflow  
Management

7.0.2



Jama  
software

Jama Connect

8.66, 8.71, 8.74

Support All Patch Versions

Current On Demand (Cloud) Version



Micro Focus ALM/Quality Center  
On Premise and SaaS versions:  
15.5, 15.5.1, 16.00, 16.0.1

Micro Focus ALM Octane  
15.1.20, 15.1.40, 15.1.60, 15.1.90, 16.0.100, 16.0.200,  
16.0.300, 16.0.400  
Current On Demand (Cloud) Version

Micro Focus Dimensions RM  
Support All Patch Versions

Micro Focus PPM  
9.62, 9.63, 9.64, 9.65, 9.66, 10.0  
Support All Patch Versions

Micro Focus Solutions Business Manager  
11.8, 12.0  
Support All Patch Versions



Microsoft Azure DevOps Server  
2019, 2020, 2020.1  
Support All Patch Versions  
Current On Demand (Cloud) Version

Microsoft Azure DevOps Services  
Current On Demand (Cloud) Version\*  
Support All Patch Versions  
\*Please note limitations in [Connector Documentation](#)

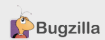
Microsoft Project Server  
2019\*, Project Online\*  
\*Please note limitations in [Connector Documentation](#)

Microsoft SharePoint  
2019, Sharepoint Online

Microsoft Test Manager  
Client Based Application accessing any supported version of Microsoft Team Foundation Server



Modern Requirements4DevOps  
Plug-in for all supported Microsoft Azure DevOps and Microsoft Azure DevOps Server versions



Mozilla Bugzilla  
5.0, 5.0.1, 5.0.2, 5.0.3, 5.0.4, 5.0.5, 5.0.6  
Support All Patch Versions



Pivotal Tracker  
Current On Demand (Cloud) Version



Planview AdaptiveWork (formerly Clarizen)  
Current On Demand (Cloud) Version

Planview AgilePlace (formerly LeanKit)  
Current On Demand (Cloud) Version

Planview Portfolios (formerly Enterprise)  
18 On Demand

One)

Support All Patch Versions

Planview PPM Pro

Current On Demand (Cloud) Version



Polarion ALM

22 R1

Support All Patch Versions



PTC Windchill

12.0.2, 12.1.0, 12.1.1

PTC Windchill RV&S

13.0, 13.1



Salesforce: Sales Cloud, Service Cloud,  
Marketing Cloud

Current On Demand (Cloud) Version



ServiceNow:  
IT Service Management,  
IT Business Management (Agile  
Development/SDLC, PPM)

San Diego On Demand, Tokyo On Demand

ServiceNow Express

Current On Demand (Cloud) Version



SmartBear QAComplete

11.2, 11.3, 11.4, 11.5, 11.6, 11.7 (for versions  
11.7.1990 and later), 11.8, 11.9, 12.0, 12.1, 12.11,  
12.12, 12.13, 12.14, 12.20, 12.21, 12.31, 12.40, 12.50,  
12.60, 12.71, 12.80, 12.90, 14.0

Current On Demand (Cloud) Version



Sparx Systems Pro Cloud Server

4.0, 4.1, 4.2

\*Premium Editions only



Targetprocess

Current On Demand (Cloud) Version



TestRail

7.0

Current On Demand (Cloud) Version



Tricentis qTest

11.0

Support All Patch Versions

Current On Demand (Cloud) Version

Tricentis Tosca

14.2, 14.3, 15.0, 15.1, 15.2

Support All Patch Versions



Trello

Current On Demand (Cloud) Version - Business  
Class Edition



Whitehat Sentinel

Current On Demand (Cloud) Version

Zendesk

Current On Demand (Cloud) Version



Zephyr Squad for Jira

5.x, 6.x, 7.x, 8.x, 9.x

Support All Patch Versions

Current On Demand (Cloud) Version

[collapse section](#)[expand section](#)

## Tasktop Sync

	Repository	General Support (Tasktop Sync 4.32)
	Atlassian Jira Core	8.22, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 Support All Patch Versions Current On Demand (Cloud) Version
	Atlassian Jira Software	8.22, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 Support All Patch Versions Current On Demand (Cloud) Version
	BMC Helix ITSM (formerly Remedy)	19.02, 19.08, 19.11, 20.02 Support All Patch Versions
<b>Borland</b>	Borland Star Team	11, 12, 13
	Broadcom Rally	2018.1, 2.0, 2.1.0 Support All Patch Versions Current On Demand (Cloud) Version
	Broadcom Clarity Agile/Requirements	Current On Demand (Cloud) Version
	Broadcom Clarity	16.0.0, 16.1 Support All Patch Versions Current On Demand (Cloud) Version
	Digital.ai Agility	Enterprise and Ultimate: 22.3 Support All Patch Versions Current On Demand (Cloud) Version
	GitHub Issues	Current On Demand (Cloud) Version
	IBM Rational ClearQuest	9.1.0

IBM Engineering  
Requirements  
Management DOORS  
Next

7.0.2

IBM Engineering  
Workflow  
Management

7.0.2



Micro Focus  
ALM/Quality Center

On Premise and SaaS versions:  
15.5, 15.5.1, 16.00, 16.0.1

Micro Focus ALM  
Octane

15.1.20, 15.1.40, 15.1.60, 15.1.90, 16.0.100, 16.0.200,  
16.0.300, 16.0.400, 16.1.100  
  
Current On Demand (Cloud) Version

Micro Focus Solutions  
Business Manager

11.8, 12.0  
  
Support All Patch Versions



Microsoft Azure  
DevOps Server

2019, 2020, 2020.1  
  
Support All Patch Versions  
  
Current On Demand (Cloud) Version

Microsoft Azure  
DevOps Services

Current On Demand (Cloud) Version  
  
Support All Patch Versions  
  
\*Please note limitations in Connector Documentation

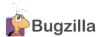
Microsoft Test  
Manager

Client Based Application accessing any supported  
version of Microsoft Team Foundation Server



Modern  
Requirements4DevOps

Plug-in for all supported Microsoft Azure DevOps and  
Microsoft Azure DevOps Server versions



Mozilla Bugzilla

5.0, 5.0.1, 5.0.2, 5.0.3, 5.0.4, 5.0.5, 5.0.6  
  
Support All Patch Versions



Polarion ALM

22 R1, 22 R2  
  
Support All Patch Versions