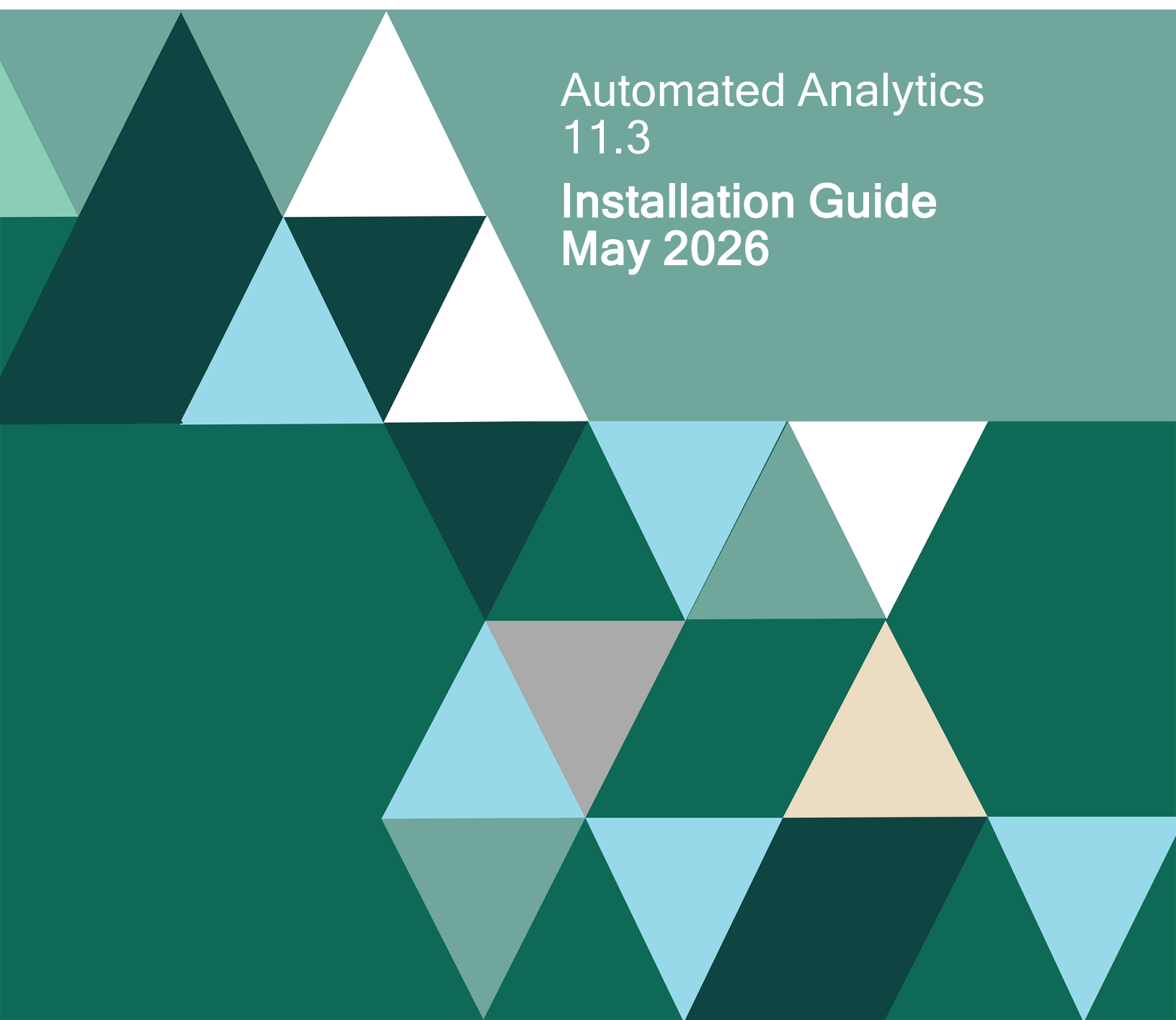


FORTRA



Automated Analytics
11.3
Installation Guide
May 2026

Copyright Terms and Conditions

Copyright © Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.

The content in this document is protected by the Copyright Laws of the United States of America and other countries worldwide. The unauthorized use and/or duplication of this material without express and written permission from Fortra is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given to Fortra with appropriate and specific direction to the original content.

202605181209

Table of Contents

Before You Begin	5
Base and Patch Releases	5
Product License Keys	5
System Requirements	6
Hardware and Software Requirements	6
Public Cloud Environments	6
Software Dependency	7
System Recommendations	7
Supported Databases	7
Tivoli Module Driver Requirements	8
Installing the Base Release	9
Preparing for Installation	9
Automated Analytics Base Release Installation	10
After You Are Done	11
Patch Releases	19
Preparing to Install a Patch on Microsoft Windows Systems	19
After You Are Done	20
After You Are Done	24
Configuring Audit Logging and Message Formatting	24
Updating SSL Certificates	25
Updating Platform-Discovery Mode Modules	29

Upgrading From a Previous Release 29

Uninstalling Automated Analytics 40

Contacting Fortra 43

Fortra Portal 43

Before You Begin

Read and understand this section before you install Automated Analytics.

Base and Patch Releases

You must install a base release of Automated Analytics. The base release contains all of the directory and folder structures, services, and applicable software needed for Automated Analytics to function properly.

Patch releases are installed after a base release or after another patch release. Patch releases contain software enhancements, predefined views and modules, and additional features.

Product License Keys

Automated Analytics requires a license key to function correctly. Provide the system information required to create a license key to your distributor. The system name is required for the license key; this is not the fully qualified domain name for the system.

System Requirements

This section provides information on the minimum requirements for installing and running Automated Analytics. Before installing Automated Analytics, read, understand, and agree to the terms of the enclosed License Agreement.

Hardware and Software Requirements

To install and run Automated Analytics components, your configuration must meet the following minimum requirements:

Package	Platform	Operating System Level	Disk Space Requirements	
Microsoft Windows (win-x64)	Microsoft Windows Server on x64 systems	2012, 2012 R2, 2016, 2019, 2022, 2025	Web Application	1.5 GB
Linux (linux-x64)	RedHat Enterprise Linux on x64 systems*	7, 8, 9	Web Application	2 GB
* Contact Global Services - Capacity Management before installing on this platform level if SELinux is enabled.				

Automated Analytics also requires the following to run:

- A current generation, multi-core processor.
- 500 MB of disk space. Additional disk space is required for published reports. A typical installation requires 3 to 5 GB.
- A minimum of 2 GB of RAM in addition to your existing RAM if Automated Analytics is installed on systems that run other applications. Otherwise, Automated Analytics requires 2 GB of RAM.

Public Cloud Environments

Automated Analytics runs on Amazon EC2, Microsoft Azure, and any other public cloud environment that supports the operating systems listed in this document.

Software Dependency

Automated Analytics uses PhantomJS to transform interactive charts into .png files. The .png files are included in Automated Analytics view exports. The FreeType and FontConfig packages and their dependencies are required for PhantomJS. For more information on the PhantomJS requirements, see <http://phantomjs.org/build.html>.

System Recommendations

The following are recommended add-ons to allow you to view reports in other formats:

- Adobe PDF Plugin for Mozilla Firefox or Microsoft Internet Explorer
Install this plugin to view PDF reports in a browser window. This plugin is available from the Adobe website.
- Microsoft Word or Microsoft Word Viewer
Install a full version of Microsoft Word or the Microsoft Word Viewer to view reports saved in a Microsoft Word (.doc or .docx) format. The Microsoft Word Viewer is available from the Microsoft website.

Supported Databases

Automated Analytics can connect to the following types of databases:

- Microsoft SQL Server*
- Microsoft SQL Server* (using Microsoft Authentication)

NOTE:

For information on connecting to a Microsoft SQL Server database using Microsoft Authentication, contact Fortra.

- Oracle Database
- PostgreSQL*
- Oracle RAC
- IBM DB2*
- MySQL*

* These databases require ODBC or JDBC drivers. Fortra recommends using jTDS for all Microsoft SQL Server connections.

Automated Analytics is extensible and can connect to any JDBC compliant or ODBC compliant database. ODBC is only supported on Microsoft Windows systems. For information on how to connect to other database types, contact Fortra.

Tivoli Module Driver Requirements

The Tivoli module requires an ODBC or JDBC driver to connect to the IBM DB2 database. To determine which driver is appropriate for your database, see your DB2 administrator.

To install the JDBC driver:

1. Stop **Automated Analytics**.
2. Copy the **db2jcc4.jar** file to the **TQDIR\Automated Analytics\webapps\surveyor\WEB-INF\lib** directory.
3. Restart **Automated Analytics**.

Installing the Base Release

NOTE: You must install the base release for the software to run.

This section provides information on available platforms, system requirements and recommendations, supported databases, required permissions and accounts, and how to install and configure a base release of Automated Analytics.

Preparing for Installation

There are several things that you must consider before installing Automated Analytics in your environment. For example, verify that the required accounts and datasources are available before installing.

Permissions and Accounts to Install and Run Automated Analytics

To install or run Automated Analytics or to access the external databases that Automated Analytics analyzes, the following account types and privileges are required:

On Microsoft Windows Systems

- An account with administrator privileges is required to install and configure Automated Analytics.
- An account with administrator privileges is required to run Automated Analytics.
- Although not mandatory, Fortra strongly recommends that you create a dedicated, unique, local database user account on each system that hosts a database used by Automated Analytics.

NOTE: For Microsoft SQL Server access, you cannot use Microsoft Windows Authentication.

NOTE: Fortra strongly recommends the use of read-only identifiers for accounts that access databases.

On Linux Systems

- Use root to install the RPM package of Automated Analytics. The product will be installed in /opt/vityl.

- A local database user account with read-only privileges is required for each database to which Automated Analytics connects to when accessing stored data.

Deployment Planning

Read this section if you plan on deploying Automated Analytics in multiple environments, such as production, development, and testing.

Fortra recommends the following, whenever possible:

- Create your reports in development environments and run those reports in production environments. Ideally, the development environment is a close representation of the production environment, ensuring that your results are similar.
- Copy data from a production environment to a development environment, export data files from the production environment, and import them into the development environment. After you develop views and reports, you can export them from the development environment and import them into the production environment for deployment.
- Develop reports using data copied from the production environment. In addition to creating a data sample with which to start developing views and reports, this allows you to work with data from your own systems while protecting your production data from errors that can occur in development.

Automated Analytics Base Release Installation

You can install Automated Analytics on a Linux system or a Microsoft Windows system.

Installing the RPM on Linux Systems

To install the RPM:

1. Download the Vityl Data Analytics package from the Forta Community Portal.
2. Move the vityl-data-analytics RPM package to the target system.
3. Open a terminal window on the target system.
4. Install the vityl-data-analytics package using the following command:

```
yum install vityl-data-analytics-11.3.xx-x.ely.x86_64.rpm
```
5. Enable the vityl-data-analytics service.

```
systemctl enable vityl-data-analytics.
```

6. Start the vityl-data-analytics service.

```
systemctl start vityl-data-analytics
```

After You Are Done

Before using Automated Analytics, do the following:

- If available, install the most recent patch release.

You must apply the most recent patch to have up-to-date product functionality and views. For information on installing a patch release, see [Installing Patch Releases on page 20](#).

- Optionally, stop or restart the Fortra Automated Analytics Service.

If Automated Analytics does not open or if you do not start the service during the installation process, start the Fortra Automated Analytics Service manually. For information on stopping or starting the service, see [Stopping and Starting the Fortra Automated Analytics Service on page 11](#).

- Apply a product license.

You receive a license when you purchase Automated Analytics. For a copy of your license, contact Fortra. For information on applying a license, see [Applying a License on page 13](#).

- Optionally, activate a module.

By default, the TeamQuest module is the only module activated at installation. All other modules are deactivated by default. You must activate a module before you can connect to a datasource. For information on activating a module, see [Activating Modules on page 14](#).

- Connect to a datasource.

Datasources are connections to a database. Before you can run views to create reports, create connections to the data on which your reports are based. For information on connecting to a datasource, see [Connecting to Datasources on page 14](#).

Stopping and Starting the Fortra Automated Analytics Service

If Automated Analytics does not open or if you do not start the service during the installation process, you must start the Fortra Automated Analytics service manually.

NOTE:

You should close Automated Analytics before stopping and starting the Fortra Automated Analytics service.

To start or stop the Fortra Automated Analytics service from a graphical user interface (GUI) on Microsoft Windows Systems:

1. From the **Control Panel** window, double-click the **Administrative Tools** icon.
2. From the **Administrative Tools** window, double-click the **Component Services** icon.
3. From the **Component Services** window, select **Services (Local)**.
4. From the **Services (Local)** list, select **Fortra Automated Analytics service**.
5. From the **Action** menu item, click **Start** or **Stop**.

NOTE:

You can also select the service, right-click, and select Start or Stop from the menu.

6. Close the **Services** window.

To stop or start the Fortra Automated Analytics service using a command prompt:

Run the following commands:

```
net stop automatedanalyticstv113
```

```
net start automatedanalyticstv113
```

To stop or start the Fortra Automated Analytics service on Linux Systems:

Run the following commands:

```
systemctl stop vityl-data-analytics
```

```
systemctl start vityl-data-analytics
```

Changing Port Settings

Port numbers are assigned during the Automated Analytics base installation. You can change the port numbers after installation if you have a port conflict.

To change the Automated Analytics port numbers:

1. Shut down the **Fortra Automated Analytics** service (see [Stopping and Starting the Fortra Automated Analytics Service on page 11](#)).
2. In a text editor, open the **server.xml** file from the **TQDIR/Automated Analytics/conf** directory.
3. Edit the settings as needed and save the file by doing the following:

- a. In the **Connector** tag for the **http** scheme, change the application port. For example,

```
<Connector port="8000" acceptorThreadCount="5"
compression="on"
```

- b. In the **Connector** tag for **scheme="http"**, change the SSL redirectPort. For example,

```
<Connector port="8000" acceptorThreadCount="5"
compression="on"
  compressionMinSize="512" maxPostSize="1"
  enableLookups="false" redirectPort="8443"
acceptCount="100"
  protocol="org.apache.coyote.http11.Http11Protocol"
scheme="http"
  secure="false"
```

- c. In the **Connector** tag for **scheme="https"**, change the port entry. For example,

```
Connector port="8443" SSLEnabled="true"
acceptorThreadCount="5"
  maxPostSize="-1" enableLookups="false" acceptCount="100"
  compression="on" compressionMinSize="512"
  protocol="org.apache.coyote.http11.Http11Protocol"
  keystoreFile="webapps/surveyor/WEB-INF/, keystore"
scheme="https" secure="true"
```

- d. In the **Server shutdown** tag, change the shutdown port. For example,

```
Server shutdown="SHUTDOWN" port="8007"
```

4. Restart the **Fortra Automated Analytics** service (see [Stopping and Starting the Fortra Automated Analytics Service on page 11](#)).

Applying a License

Automated Analytics requires a product license. You receive a license when you purchase the product. For a copy of your license, contact Fortra.

To apply a license to Automated Analytics:

1. Log into **Automated Analytics** as a SuperAdmin (**sa**).
2. Select **Tools > Licensing**.
3. Type or paste your license key into the **Enter New License** field.
4. Click **OK**.
5. Click **OK** again.

If your key is accepted, you are returned to the Administrator interface. Information on your license is displayed in the Status Bar at the bottom of the interface.

If your key is invalid, you are returned to the Licensing dialog to enter a valid license.

Activating Modules

Modules define how a datasource connects to a database. They contain queries and instructions that Automated Analytics uses to retrieve data from databases.

By default, the TeamQuest module is the only module activated at installation. All other Automated Analytics modules are deactivated by default. You must activate a module before you can connect to a datasource.

To activate a module:

1. From the **Administrator Interface**, select **Edit > Modules**.

Deactivated modules are displayed with  icon.

2. Select the module to activate.
3. From the right pane, click **Activate**.

The module is activated and displayed at the top of the module hierarchy with  icon. Activated modules are listed alphabetically.

NOTE:

You can also right-click the module and select Activate from the menu.

Connecting to Datasources

Datasources are connections to a database. Before you can run views to create reports, you must create connections to the data on which your reports are based.

NOTE:

You cannot connect to a datasource for a deactivate module. The TeamQuest module is the only module activated by default at installation. All other modules are deactivated by default.

To add a datasource:

1. Log in with an account that has the Edit Datasources permission assigned to it.
2. Select **Edit > Datasources**.
3. Select **File > New Datasource** and select the type of datasource to connect to.
4. In the **Name** text box, type the datasource name.

5. From the **dbType** list, select the database type to connect to.

Different options are displayed in the dialog, depending which database you selected.

NOTE:

Because of performance and scalability issues, Fortra recommends that you avoid using ODBC datasources for production environments. They are included for backward compatibility, development purposes, and to support databases that only support this connection method.

6. Specify the options for the selected database type. Options that are not required for your database type are shaded.

- **host**

Specifies the name or IP address of the server where the database resides (only required for the Oracle and jTDS drivers). Host names must be resolved by a local host entry or datasource name (DSN) for the connection to succeed.

- **hosts**

Lists the Oracle RAC hosts to which you want to connect. Separate each server name with a comma (,).

- **port**

Specifies the port number that the database server is listening. Default port numbers are specified when you select a suitable database type, but these values can be different for your environment. Ask your database administrator for the non-default port number.

- **database**

Specifies the name of the datasource name (DSN) defined to connect to the database (for ODBC datasources). For Microsoft SQL Servers through jTDS, this is the database container to use on the database server.

- **instance**

Specifies the database instance, or SID, to which you connect on the database server (for Oracle databases). If instances are configured to run with jTDS drivers, this is the specific database instance to which you want to connect on the database server.

- **user**

Specifies the user. All datasources require a username (schema in Oracle) and password to authenticate to the database server.

- **password**

Specifies the password. All datasources require a username (schema in Oracle) and password to authenticate to the database server.

- **priority**

Specifies how to handle data that exists for the same system in multiple datasources. Automated Analytics attempts to use the datasource with the most recently updated data first and only attempts to use other datasources if data is not found for the requested interval. If the last updated data is the same for multiple datasources, the datasource priority setting is used. The higher-priority datasource is used first and the lower-priority datasource is used only if data is not found for the requested interval. Higher values represent a higher priority to Automated Analytics. The default value is 10. The `get-*-data` function `datasource-selection-criteria` property overrides the default selection.

- **timezone**

Specifies the timezone of the database server.

NOTE:

If the Automated Analytics server is in a different timezone from the database server, report results can be affected. The datasource timezone can be configured to adjust the date and timestamp strings for all data in the datasource.

- **dataset**

Allows you to classify your data according to whether it is from a production, testing, or a development environment. These classifications can help you distinguish the day-to-day production data collection from more granular data collection from the same systems for testing purposes, such as load testing. By default, only production databases are queried when a request is made.

- **mode**

Specifies how current the data in the database is, the time frame that Automated Analytics searches, and how aggressively the datasource properties are interrogated. Automated Analytics datasource modes can be static, real-time, historical, or future.

- **Static**

- Data in the database is no longer updated.
- The interval range is limited to the dates in the database.
- System discovery runs once a day and stops if nothing new is found.
- Property discovery only runs when datasources are created or if new data is found.

- **Realtime**

- Data is added to the database regularly throughout the day.
- The interval range includes everything from the start date to the end of the current day.
- System discovery runs once a day and retries hourly until new data is found.
- Property discovery runs once a day.
- **Historical**
 - Data is added to the database once a day from the previous day.
 - The interval range includes everything from the start date to the end of the day before the current day.
 - System discovery runs once a day and retries hourly until new data is found.
 - Property discovery runs once a day and only when new systems are found.

NOTE:

Historical mode is the default mode for most datasources.

- **Future**
 - Data can include future projections.
 - The interval range includes everything in the database and can include intervals that overlap other datasources and dates in the future.
 - System discovery runs once a day and retries hourly until new data is found.
 - Property discovery runs once a day and only when new systems are found.
- **dataFrequency**

Indicates the size of the gaps between data points and is indicative of the current state of your database. Leave this field blank unless specifically instructed otherwise by Fortra.
- **inputDateFormat**

Specifies the date format of the data.
- **usingTeamQuestStorage**

Indicates whether you are using the TeamQuest Storage module. If you are using this module, additional metrics are discovered. Connecting to the datasource takes more time when this field is set to True.
- **useEndTime**

Specifies how time labels are displayed in your charts. Points can be labeled with either the start of the time period or the end of the time period. By default, time labels show the start time of the time period.

7. Click **Create/Connect** to create, verify, and connect to the datasource.

NOTE:

Optionally, click Create to create the connection to the datasource. The datasource is displayed as inactive. Click Connect to activate the datasource. After it is activated, right-click the datasource and click Connect to create the connection to the datasource.

Patch Releases

NOTE:

Patch releases cannot be rolled back. Contact Fortra if you encounter problems.

Preparing to Install a Patch on Microsoft Windows Systems

Before you install a patch, consider the following:

- The 11.3 base release of Automated Analytics must be installed.
- Export files not included in the Restore functionality before you install.
Files not included in the Restore functionality are generated reports, spreadsheets, HTML templates, model files, custom images, css files, and js files. Exporting these files minimizes the amount of data that you can lose by overwriting your data with a full restore. For more information on exporting files, see the *Automated Analytics Administrator Guide*.
- Optionally, stop the Fortra Automated Analytics Service.
- If you are installing on a Microsoft Windows system, check the service to see if it is running. Stop the Fortra Automated Analytics Service prior to installing.

NOTE:

Close Automated Analytics before stopping the Fortra Automated Analytics Service.

To stop the Fortra Automated Analytics Service from a Graphical User Interface (GUI):

1. From the **Control Panel** window, double-click the **Administrative Tools** icon.
2. From the **Administrative Tools** window, double-click the **Component Services** icon.
3. From the **Component Services** window, select **Services (Local)**.
4. From the **Services (Local)** list, select **Fortra Automated Analytics Service**.
5. From the **Action** menu, click **Stop**.

NOTE:

You can also select the service, right-click to display a pop-up menu, and select **Stop** from the menu.

6. Close the **Services** window.

To stop or start the Fortra Automated Analytics service from a command prompt:

Run the following commands:

```
net stop automatedanalyticstv113
```

```
net start automatedanalyticstv113
```

Installing Patch Releases

You can install a patch on a previously installed base release or patch release on a Microsoft Windows system.

Version 11.3 is the base version of Automated Analytics. You must have this version installed before you can install a patch release of Automated Analytics. For example, if you are installing Automated Analytics for the first time or are upgrading from a release prior to 11.3, do the following:

1. Install the base release (11.3).
2. Check to see if any instance of Automated Analytics is running, and if it is, stop it.
3. Install the patch version of Automated Analytics.

Patch releases are cumulative and contain all features and fixes from all patch releases subsequent to the base release of Automated Analytics.

To install a patch release:

1. Double-click the patch file. For example,
`tqpf-surveyor-11.3.x-wub.exe`
2. Follow the prompts. When the installation is complete, the Select Additional Tasks dialog displays.

The Restart Service? checkbox is selected by default. If you do not want to restart the Fortra Automated Analytics Service with this installation, clear the checkbox. You can start the service at a later time.

NOTE: For information on installing on Linux systems, see [Installing the RPM on Linux Systems on page 10](#).

After You Are Done

If you do a restore operation, import the Automated Analytics package files and delete the old view categories.

These package files are automatically installed but are overwritten during the restore operation.

NOTE:

If you perform a restore operation after deleting old view categories, all old view categories are restored and you must delete them again.

View Category Tree Structure

The 11.2 PF 20150323 Performance Surveyor patch release introduced a new view category tree structure. The reorganization of the view categories makes navigation to views easier. Views in the old view categories are not supported. Fortra recommends that you rename predefined views that you are modifying.

New View Category	Old View Category
System	Dashboards
	AutoPredict Reports
	TeamQuest Model
Storage	Storage Reports
Examples	Advanced Charts
	Base Charts
	Calendar Samples
	Categorizations
	Correlation
	Distributions
	Filters
	Instance Level Data
	Iteration
	Loop Samples
	Monthly Report Samples
	Percentile
	Period over Period

New View Category	Old View Category
	Problem Detectors
	Projections
	Raw Data
	Spreadsheets
	Table Reports

- The names of the views from the old Dashboards view category have not changed for the System view category.
For example, the view IO Trouble under the old Dashboards view category is called IO Trouble in the new System view category.
- The previous AutoPredict Reports category views have changed to have (AutoPredict) at the end of the view name so you can easily find the previous views.
For example, the Predicted Response Time view was in the AutoPredict Reports view category. Now the Predicted Response Time view is in the System view category and is called Predicted Response Time (AutoPredict).
- The previous TeamQuest Model category views are now called Multiple Systems Model Export and Single System Model Export.
- The names of the old Storage Reports view category did not change.
- All predefined sample views are now located in the Examples single view category.
The predefined sample views are named with the previous view category name prefixed to the name of the view so you can easily find view examples.
For example, the view Group Line Chart moved from the Basic Charts category to the Group Line Chart in the Examples category and are now called Basic Charts - Group Line Chart.

Deleting View Categories

NOTE:

If you are using the Tivoli or bpa modules with views within the Dashboards view category, do not delete this view category.

Fortra recommends deleting the old predefined view categories. For example, delete the Dashboards view category and all of the views within it. If you modify schedules for the deleted view categories, reconfigure the schedules for those views in the new view category tree structure. Only views in new view categories are supported. Fortra recommends that you rename the predefined views you are modifying.

NOTE:

When you delete a view category, the views under it are also deleted. To avoid unintentionally deleting views, rename, move, or copy your views to another category. You can only recover views that are backed up. For more information, see the *Automated Analytics Administrator Guide*.

To delete a view category:

1. Select **Edit > Views**.
2. From the view tree, right-click the view category.
3. Select **Delete**.

One of the following occurs:

- The *Delete category name* dialog is displayed if the view category contains views used in schedules and instances.
 - a. To delete the schedules that use views in the view category that you are deleting, select the Delete schedules option.
 - b. To delete the reports that the affected schedules and instances generate, select the Delete schedule reports from disk option.
 - c. Click Yes. The view category, and all views under it, are deleted.
 - The Delete Category confirmation prompt is displayed.
4. Click **Yes**.

Importing Package Files

If you perform a full restore of your backups, every change since the backup is lost. You can restore individual items by exporting files before you install a patch and import them. This minimizes the amount of data that you can lose by overwriting your data with a full restore.

If you performed a restore operation from a backup created before you installed this patch, new groups and views in the Automated Analytics package files are removed. Use the import functionality to import these new views and groups for use with this patch.

To import an Automated Analytics package file:

1. Select **File > Import Package**.
2. From the list, select the Automated Analytics package to import.
3. Clear the check boxes for the items that you do not want to import and clear the Overwrite existing items check box to avoid overwriting items you are importing.
4. Click **OK**.
5. Review the log details and click **Close**.

After You Are Done

Congratulations! Automated Analytics is now installed. Read the following for additional information and your next steps.

Configuring Audit Logging and Message Formatting

You can configure audit logging and message formatting to ensure proper logging of user activities for compliance and troubleshooting. Configuration for User Access Logging is stored in `/opt/vityl/data-analytics/webapps/surveyor/WEB-INF/classes/log4j.properties`. Audit logs are written to `/opt/vityl/data-analytics/logs/audit.log`.

Default Configuration

- `log4j.appender.audit.File=${catalina.home}/logs/audit.log`
- `log4j.appender.audit.MaxFileSize=3MB`
- `log4j.appender.audit.MaxBackupIndex=20`

where:

- **log4j.appender.audit.File** is the audit log file path.
- **log4j.appender.audit.MaxFileSize** - triggers rotation when the limit is reached. The maximum size for each audit log file is 3 megabytes.
- **log4j.appender.audit.MaxBackupIndex** - is the number of backup audit files after rotation.

For example:

Rotation: `audit.log` → `audit.log.1` → `audit.log.2` → ... → `audit.log.20`
 Total audit storage: 21 files × 3MB = ~63MB maximum

Log File Format

```
{
  "timeStamp":"2025-12-17T18:56:11.9761846Z",
  "source":"10.60.154.131",
  "userId":"admin",
  "eventType":"login",
  "componentName":"Authentication",
```



```
"status": "success"
}
```

where

- **timeStamp** is the date and time that the event occurred.
- **source** is the source IP address of the request.
- **userId** is the authenticated user performing the action.
- **eventType** is the specific audit event type.
- **componentName** is the system component handling the event.
- **status** is the outcome of the action.

Updating SSL Certificates

This section provides information on how to update the SSL certificate in Automated Analytics. When Automated Analytics is installed, HTTPS connections are enabled and a self-signed SSL certificate is generated.

You can replace the self-signed SSL certificate with one generated by a Certificate Authority (CA).

When Automated Analytics is installed, HTTPS connections are enabled and a self-signed SSL certificate is generated. If your organization requires a certificate signed by a Certificate Authority (CA), replace the self-signed certificate with a certificate signed by a CA.

NOTE:

If your organization does not require a certificate signed by a CA, you can connect securely using the self-signed certificate. For information on accepting self signed certificates, see the Help in your browser.

To update the SSL certificate on Microsoft Windows Systems:

1. From a command prompt, enter the following command to generate the Certificate Signing Request (CSR):

```
TQDIR/Automated Analytics/jre/bin/keytool -certreq -alias
tomcat -sigalg SHA256withRSA -keystore
TQDIR/Automated Analytics/webapps/surveyor/WEB-INF/.keystore -
file tomcat.csr -storepass password
```

where:

TQDIR is the path of the directory where Automated Analytics is installed

password is the password for the keystore. The default password for the keystore created by the setup process is changeit. Unless you change the password, enter changeit

2. Email or upload the **tomcat.csr** file to your **Certificate Authority (CA)**.

After signed, a file named tomcat.cer and the CA's certificate chain file are sent to you.

3. Do the following to save the certificate:

- a. Save the CA certificate chain file and all files contained in this file as **Base-64 encoded X.509.cer** in the following location:

TQDIR/Automated Analytics/conf

- b. Save the **tomcat.cer** file to the following location:

TQDIR/Automated Analytics/conf

4. From a command line, do the following to import files into the keystore, which is a container that holds public and private keys for Java:

- a. Run the following command to ensure that the CA that signed your certificates is accepted to build certificate chains:

```
TQDIR/Automated Analytics/jre/bin/keytool -importcert -
alias CAName
-file
TQDIR/Automated Analytics/conf/CACer -keystore
TQDIR/Automated Analytics/webapps/surveyor/WEB-
INF/.keystore
```

The certificate file is installed in the keystore.

- b. Store the returned certificate in the keystore used by Apache Tomcat using the following command:

```
TQDIR/Automated Analytics/jre/bin/keytool -importcert -
alias tomcat -trustcacerts
-file
TQDIR/Automated Analytics/conf/CER -keystore
TQDIR/Automated Analytics/webapps/surveyor/WEB-
INF/.keystore
```

where *CER* is the name of the signed certificate response file. For example, clrh12.cer.

The certificate reply is installed in the keystore.

NOTE:

If you receive multiple certificate files from the Certificate Authority, run this command for each certificate file and use a unique alias. For example, if you receive a top-level certificate from Verisign and an intermediate certificate from your local CA, signed by Verisign.

- Restart the **Fortra Automated Analytics Service** to apply the changes using the following commands, depending on your system:

NOTE:

Close any Automated Analytics sessions before restarting the Fortra Automated Analytics service.

```
net stop automatedanalyticssv113
net start automatedanalyticssv113
```

To update the SSL certificate on Linux Systems:

- From a command prompt, enter the following command to generate the Certificate Signing Request (CSR):

```
/usr/bin/keytool -certreq -alias tomcat - sigalg SHA256withRSA
-keystore
TQDIR/data-analytics/webapps/surveyor/WEB-INF/.keystore - file
tomcat.csr - storepass password
```

where:

password is the password for the keystore. The default password for the keystore created by the setup process is changeit. Unless you change the password, enter changeit

- Email or upload the **tomcat.csr** file to your **Certificate Authority (CA)**. After signed, a file named tomcat.cer and the CA's certificate chain file are sent to you.
- Do the following to save the certificate:
 - Save the CA certificate chain file and all files contained in this file as **Base-64 encoded X.509.cer** in the following location:
`TQDIR/Automated Analytics/conf`
 - Save the **tomcat.cer** file to the following location:
`TQDIR/Automated Analytics/conf`

4. From a command line, do the following to import files into the keystore, which is a container that holds public and private keys for Java:
 - a. Run the following command to ensure that the CA that signed your certificates is accepted to build certificate chains:

```
/usr/bin/keytool -importcert -alias
CAName
-file
TQDIR/Automated Analytics/conf/CACer -keystore
TQDIR/data-analytics/webapps/surveyor/WEB-INF/.keystore
```

where:

<i>CAName</i>	is the name of the CA that signed your certificate. For example, Verisign.
---------------	---

<i>CACer</i>	is the name of the certificate authority's certificate file. For example, verisign.cer.
--------------	--

- b. Store the returned certificate in the keystore used by Apache Tomcat using the following command:

```
/usr/bin/keytool -importcert -alias tomcat -trustcacerts
- file
TQDIR/Automated Analytics/conf/CER - keystore
TQDIR/data-analytics/webapps/surveyor/WEB-INF/.keystore
```

where *CER* is the name of the signed certificate response file. For example, clrh12.cer.

The certificate reply is installed in the keystore.

NOTE:

If you receive multiple certificate files from the Certificate Authority, run this command for each certificate file and use a unique alias. For example, if you receive a top-level certificate from Verisign and an intermediate certificate from your local CA, signed by Verisign.

5. Restart the **Fortra Automated Analytics Service** to apply the changes using the following commands, depending on your system:

NOTE:

Close any Automated Analytics sessions before restarting the Fortra Automated Analytics service.

```
systemctl stop vityl-data-analytics
systemctl start vityl-data-analytics
```

Updating Platform-Discovery Mode Modules

The platform-discovery mode is no longer available in all modules. The affected modules are pnet, mvpa, cme, and user-created modules using platform-discovery mode.

Predefined modules are displayed with green icons. User-created modules are displayed with blue icons. Modules that use the platform-discovery mode are displayed with a red icon until they are updated to the current release.

Datasource support for these modules is no longer available. You cannot activate datasources when a module is in platform-discovery mode. You can easily update user-created modules from platform-discovery mode to system-discovery mode.

To update a platform-discovery module:

1. Select **Edit > Modules**.

The Edit Module dialog is displayed. Modules that need to be updated are displayed with a red icon.

2. Click a module.

The Edit Modules dialog is displayed with information about the module displayed in the pane for the General tab.

The discovery mode for this module is Platform. This discovery type is deprecated in the Performance Surveyor 11.2 PF 20140304 base release.

3. From the **Discovery Mode** area, select **System**.

4. Click **Apply Changes**.

The Module Updated dialog is displayed.

5. From the **Module Updated** dialog, click **Yes**.

The Migration Complete dialog is displayed with information about the migrated queries.

6. From the **Migration Complete** dialog, click **OK**.

You are returned to the Edit Modules dialog. The updated module is displayed with a blue icon.

Upgrading From a Previous Release

This section provides information on the required permissions and accounts, how to upgrade TeamQuest Performance Software, how to upgrade Automated Analytics, how to upgrade PostgreSQL servers, and how to configure Automated Analytics. It also describes how to install multiple releases of Automated Analytics to run concurrently or individually on the same system.

Preparing for an Upgrade

There are several things that you must consider before upgrading Automated Analytics. For example, verify that the required accounts and data sources are available before you upgrade Automated Analytics.

Before Updating to the Current Version

All Automated Analytics backup files are migrated by the installer to the new release, allowing you to restore your settings and customizations.

To update to the current base release of Automated Analytics, do the following:

- Create a backup file of the data on the earlier release of Automated Analytics.
You can restore the backup from the previous night and use that data. For information on creating backups, see the *Automated Analytics Administrator Guide*.
- Export files not included in the Restore functionality before installing.
Files not included are generated reports, spreadsheets, HTML templates, model files, custom images, css files, and js files. Exporting these files minimizes the amount of data that can be lost by overwriting your data with a full restoration.
- Determine if you still need the previous level of Automated Analytics.
If you no longer need the previous level of Automated Analytics, stop the previous service before installing the new level of Automated Analytics, see [Stopping and Starting the Fortra Automated Analytics Service on page 36](#).
For information on using the previous level of Automated Analytics, see [Considerations for Multiple Releases Installed Concurrently on page 30](#).

Considerations for Multiple Releases Installed Concurrently

You can install and run the current version of Automated Analytics alongside previous versions of Automated Analytics. This allows you to verify the output of your reports before using the new release in your production environment.

Running multiple versions of Automated Analytics on the same system

You can run multiple versions of Automated Analytics on the same system at the same time. Before installing the current version, do the following:

- Create a backup of the data on the earlier version of Automated Analytics.
You can restore the backup from the previous night and use that data. For information on creating backups, see the *Automated Analytics Administrator Guide*.

- Export files not included in the restore functionality before installing.
Files not included are generated reports, spreadsheets, HTML templates, model files, custom images, css files, and js files. Exporting these files minimizes the amount of data that can be lost by overwriting your data with a full restoration.
- Determine the application, shutdown, and HTTPS port numbers.
The port numbers used by Automated Analytics versions cannot be the same; they each must use a unique port number.
The default application port is 8000, the default shutdown port is 8007, and the default HTTPS port number is 8443. When you install a new version, assign different port numbers when requested to do so in the installation wizard. For information on changing Automated Analytics port settings, see [Changing Port Settings on page 37](#).
- Verify that there is enough memory to run multiple Automated Analytics applications and your other applications at the same time.
Automated Analytics requires a minimum of 2 GB of RAM. For example, if you typically run two Automated Analytics applications on a system where these are the only two applications running, you need a minimum of 4 GB of RAM. If you run two Automated Analytics applications on a system where other applications are running, you must add at least 4 GB of RAM to the existing system RAM.

Running multiple versions of Automated Analytics on one system

You can run multiple versions of Automated Analytics (that do not run at the same time) on the same system. If you use each version of Automated Analytics individually, port number and RAM changes are not required.

You do not need to change the default application and shutdown port numbers for each release, because port conflicts only result if you run multiple versions of Automated Analytics on a single system at the same time.

You do not need to add RAM beyond that specified in the system requirements, because only one version of Automated Analytics runs at a time. You need only the minimum 2 GB of RAM for a single installation of Automated Analytics.

Upgrades

You can upgrade Automated Analytics your installation to other versions.

About Linux Upgrades

The RPM version of Automated Analytics is not packaged with Java. However, since the product requires Java 11, yum will automatically install Java if it does not already exist on the system.

If you install Automated Analytics on a Linux system, it is configured to automatically start when your system starts or reboots.

NOTE:

While the current release use ports 3708 and 3709, previous versions of Automated Analytics use ports 8000 and 8443 respectively. You can change ports as needed (see [Changing Port Settings on page 12](#)).

Upgrading Automated Analytics

To upgrade Automated Analytics on Microsoft Windows System:

1. From the Fortra website, download the Automated Analytics base release installation file by clicking **Downloads > My Product Downloads – By Brand** or the **Automated Analytics Downloads > My Product Downloads – By Hardware**.
2. Navigate to the directory where you saved the installation file.
3. Double-click the installation file. For example:
`Fortra-Automated-Analytics-11.3.xx.exe`
4. From the **Select Destination Directory** dialog, accept the default or type a destination folder.
The destination directory is the folder where Automated Analytics is installed. By default, C:\Program Files\Fortra\Automated Analytics.
5. From the **Select Start Menu Folder** dialog, specify if you want to create a shortcut in the start menu.
By default, a start menu item and shortcut is created for all users.
6. From the **Configuration Information** dialog, accept the default ports or type new ports.
By default, the application port is 8000, the shutdown port is 8007, and the SSL port is 8443.

NOTE:

Verify that the ports are not in use. If Automated Analytics and TeamQuest Administration Console are installed on the same system and use the default ports, you must change the ports for one of the products. Fortra recommends that you change the Automated Analytics SSL port to 9443.

If you specify a port for Automated Analytics that is used by a non-running application, a port conflict is not detected during installation. After installation, you can encounter a port conflict if you try to use Automated Analytics and the other application at the same time. To avoid this, change the port for one of the applications.

If you specify a port for Automated Analytics that is used by a running application, a port conflict is detected. Type a different port to continue the installation.

For information on changing port settings in Automated Analytics, see [Changing Port Settings on page 37](#).

7. From the second **Configuration Information** dialog, do the following:

- a. In the **SuperAdmin (sa) Password** text box, type a password for the SuperAdmin account.

The password is case-sensitive. The SuperAdmin account is the first account that Automated Analytics creates. The username is sa and is case-sensitive. Use this to log into Automated Analytics for the first time, import the license, create other administrator and user accounts, run reports from the Administrator and End User interfaces, manage the environment, and perform other configuration tasks.

- b. In the **Confirm Password** text box, retype the SuperAdmin account password.
- c. From the **Memory Configuration** area, specify the memory configuration.
 - Select **Systems with up to 4GB of total System RAM** if your system has less than 4 GB of RAM or if the system has a lot of memory, but hosts memory intensive applications. This option prevents Automated Analytics processes from being swapped out to the paging file, resulting in poor performance. This option is not recommended for production environments.
 - Select **Systems with 4-8GB of total System RAM** if your system has an x64 architecture and 4 to 8 GB of RAM. This is the default.
 - Select **Systems with 8GB+ of total System RAM** if your system has an x64 architecture and more than 8 GB of RAM.

8. Optionally, from the **Optional User Accounts** dialog, configure the passwords for the Administrative or Analyst accounts.

NOTE:

If you do not configure passwords for these accounts at this time, you can configure them later. For more information, see the *Automated Analytics Administrator Guide*.

- a. Clear the **Locked by default** check box for the **Admin Account** or the **Analyst Account**.
 - b. In the **Admin Password** or **Analyst Password** text box, type the password.
 - c. Click **Next**.
9. From the **Advanced Configuration Settings** dialog, accept the default settings. The default settings are suitable for most environments. By default, the Unlock check box is selected and you cannot change the settings.

NOTE:

These settings allow you to change the run-time settings of the Java Virtual Machine (JVM) to match how they are configured in existing systems. Do not change these settings unless you have advanced knowledge of run-time settings or are advised to do so by Fortra.

- a. From the **Migrate Publisher Configuration Information?** dialog, select how to handle reports and schedules from previous versions.
- b. Follow the prompts in the wizard.
- c. From the **Completing the Performance Surveyor Setup Wizard** dialog, specify how you want Automated Analytics to start.

- **Start service on exit** starts the Fortra Automated Analytics Service.
- **Launch Surveyor on Exit** opens Automated Analytics in a browser.

Both options are selected by default.

NOTE:

If you plan on installing a patch release after the base upgrade, clear the Start service on exit and Launch Surveyor on Exit options.

10. Click **Finish**.

To upgrade Automated Analytics on Linux System:

1. From the Fortra website, download the Automated Analytics base release installation file by clicking **Downloads > My Product Downloads – By Brand or the Downloads > Automated Analytics > My Product Downloads – By Hardware**.

2. Navigate to the directory where you saved the installation file.
3. Install the vityl-data-analytics package using the following command:

```
yum update vityl-data-analytics-11.3.xx-x.el.y.x86_64.rpm
```
4. Start the vityl-data-analytics service.

```
systemctl start vityl-data-analytics
```

NOTE: If you are upgrading from version 11.3.31 and older, you must transition to the RPM version of Vityl Data Analytics. Contact Fortra Customer Support for more information.

Post Installation

After you install Automated Analytics, there are several steps that you must perform to complete the installation.

Before Using Automated Analytics

Before you use Automated Analytics, consider the following:

- Make sure you have the most current patch release (if one is available) installed before you restore your previous version of the Automated Analytics backup file. For example, you must have the Automated Analytics base release 11.3 and the most recent patch release installed before you can restore your previous version of Automated Analytics.
- If you perform a Restore operation, you must also import the Automated Analytics package files.
These files are automatically installed but are overwritten during restoration.
- Optionally, stop and restart the Fortra Automated Analytics Service.
If Automated Analytics does not open or if you do not start the service during the installation, manually start the Fortra Automated Analytics Service. For information on stopping or starting the service, see [*Stopping and Starting the Fortra Automated Analytics Service on page 36*](#).
- Optionally, activate a module.
By default, the TeamQuest module is the only module activated at installation. All other modules are deactivated by default. You must activate a module before you can connect to a datasource. For information on activating a module, see [*Activating Modules on page 38*](#).
- Optionally, import the Automated Analytics package files.

If you perform a Restore operation from a backup created before you installed the patch, new groups and views in the Automated Analytics package files are removed. For information on using the import functionality, see [Importing Package Files on page 39](#).

- Optionally, update your platform-discovery mode modules.

The platform-discovery mode is deprecated in all modules within Automated Analytics for the 11.3 base release. The affected modules are pnet, mvpa, cme, and any user-created module using platform-discovery mode. For information on updating these modules, see [Updating Platform-Discovery Mode Modules on page 29](#).

- Optionally, remove the old release version of Automated Analytics.

After testing and verifying the Automated Analytics upgrade, you can remove the old release. For information on removing the old release of Automated Analytics, see [Removing the Previous Release on page 39](#).

Stopping and Starting the Fortra Automated Analytics Service

You can stop and start the Fortra Automated Analytics Service if you are unable to connect to Automated Analytics.

NOTE:

Close Automated Analytics before stopping and starting the Fortra Automated Analytics Service.

To start or stop the Fortra Automated Analytics Service from a Graphical User Interface (GUI) on Microsoft Windows System:

1. From the **Control Panel** window, double-click the **Administrative Tools** icon.
2. From the **Administrative Tools** window, double-click the **Component Services** icon.
3. From the **Component Services** window, select **Services (Local)**.
4. From the **Services (Local)** list, select **Fortra Automated Analytics Service**.
5. From the **Action** menu, click **Start** or **Stop**.

NOTE:

You can also select the service, right-click, and select Start or Stop from the menu.

6. Close the **Services** window.

To stop or start the Fortra Automated Analytics Service from a command prompt:

Run the following commands:

```
net stop automatedanalyticsv113

net start automatedanalyticsv113
```

To stop or start the Fortra Automated Analytics Service on a Linux System:

Run the following commands:

```
systemctl stop vityl-data-analytics

systemctl start vityl-data-analytics
```

Changing Port Settings

Port numbers are assigned during the Automated Analytics base installation. You can change the port numbers after installation if you have a port conflict.

To change the Automated Analytics port numbers:

1. Shut down the **Fortra Automated Analytics Service** (see [Stopping and Starting the Fortra Automated Analytics Service on page 11](#)).
2. In a text editor, open the **server.xml** file from the **TQDIR/Automated Analytics/conf** directory.
3. Edit the settings as needed and save the file by doing the following:
 - a. In the **Connector** tag for scheme **http**, change the application port. For example,


```
<Connector port="8000" acceptorThreadCount="5"
compression="on"
```
 - b. In the **Connector** tag for **scheme="http"**, change the SSL redirectPort. For example,


```
<Connector port="8000" acceptorThreadCount="5"
compression="on"
compressionMinSize="512" maxPostSize="1"
enableLookups="false" redirectPort="8443"
acceptCount="100"
protocol="org.apache.coyote.http11.Http11Protocol"
scheme="http"
secure="false"
```
 - c. In the **Connector** tag for **scheme="https"**, change the port entry. For example,


```
Connector port="8443" SSLEnabled="true"
acceptorThreadCount="5"
maxPostSize="-1" enableLookups="false" acceptCount="100"
compression="on" compressionMinSize="512"
```

```
protocol="org.apache.coyote.http11.Http11Protocol"
keystoreFile="webapps/surveyor/WEB-INF/,keystore"
scheme="https" secure="true"
```

- d. In the **Server shutdown** tag, change the shutdown port. For example,

```
Server shutdown="SHUTDOWN" port="8007"
```

4. Restart the **Fortra Automated Analytics Service** (see [Stopping and Starting the Fortra Automated Analytics Service on page 36](#)).

Activating Modules

Modules define how a datasource connects to a database. They contain queries and instructions that Automated Analytics uses to retrieve data from databases.

By default, the TeamQuest module is the only module activated on installation. All other modules are deactivated by default. You must activate a module before you can connect to a datasource.

In the 11.1 version of Performance Surveyor, the TeamQuest module discovered the data collected by the Oracle Agent, the DB2 UDB Agent, the Sybase ASE Agent, or the Network Device Agent of TeamQuest Manager when harvested into an open database. The TeamQuest module no longer discovers this data. With the release of version 11.2 of Performance Surveyor, two additional modules are used to discover this data; the TeamQuest Application module and the TeamQuest Network Device module.

NOTE:

Activate the TeamQuest Application module to view and analyze data collected by the Oracle Agent, the DB2 UDB Agent, or the Sybase ASE Agent.

Activate the TeamQuest Network Device module to view and analyze data collected by the Network Device Agent.

To activate a module:

1. From the **Administrator Interface**, select **Edit > Modules**.

The Edit Modules dialog is displayed. Deactivated modules are indicated by  icon.

2. Select a module.

The Module details are displayed in the right pane.

3. Click **Activate**.

The module is activated and displayed at the top of the module hierarchy with  icon. Activated modules are listed alphabetically.

NOTE:

You can also right-click the module and select Activate from the menu.

Importing Package Files

If you perform a full restoration of your backups, every change since the backup is lost. You can restore individual items by exporting files before you install a patch and import them. This minimizes the amount of data that you can lose by overwriting your data with a full restoration.

If you performed a restore operation from a backup created before you installed the patch, new groups and views in the Automated Analytics package files are removed. Use the import functionality to import these new views and groups into the patch.

NOTE:

Only views in the new view categories are supported. Fortra recommends deleting old view categories. For more information, see [View Category Tree Structure on page 21](#).

To import an Automated Analytics package file:

1. Select **File > Import Package**.
2. From the list, select the Automated Analytics package to import.
3. Clear the check boxes for the items that you do not want to import and clear the Overwrite existing items check box to avoid overwriting items that you are importing.
4. Click **OK**.
5. Review the log details and click **Close**.

Removing the Previous Release

After you run your tests, are satisfied with the performance of Automated Analytics in your environment, and validate the output of your reports in the new version, you might need to complete additional steps.

To remove the previous version when the two versions are installed on the same system:

1. Perform a backup operation of the data from the previous version of Automated Analytics.
2. Optionally, change the port settings (see [Changing Port Settings on page 37](#)).
3. Log into version 11.3 of Automated Analytics.
4. Select **Tools > System Mode**.
5. Restore the backup from the previous version.

For information on restoring a backup file, see the *Automated Analytics Administrator Guide*.

6. From the **Restore Schedules** prompt, click **Yes** to include the schedules in the restoration.
7. Uninstall the previous version of Automated Analytics.

To remove the old version when the two versions are on different systems:

1. Perform a backup operation of the data from the previous version of Automated Analytics
2. Install version 11.3 of Automated Analytics on the production server.
3. Accept the default application and shutdown ports or change them (see [Changing Port Settings on page 37](#)).
4. Copy the backup file from the previous version backups folder to the version 11.3 backups folder.
5. Log into version 11.3 of Automated Analytics.
6. Select **Tools > System Mode**.
7. Restore the backup from the previous version.

For information on restoring a backup file, see the *Automated Analytics Administrator Guide*.

8. From the **Restore Schedules** prompt, click **Yes** to include the schedules in the restoration.
9. Uninstall the previous version of Automated Analytics.

Uninstalling Automated Analytics

This section provides information on how to uninstall Automated Analytics and remove associated folders and files.

Removing Automated Analytics

Automated Analytics can be removed from your system using the uninstall process in the interface or using commands.

Some configuration and data folders and files are not deleted when you uninstall. If you reinstall the product at a later date, these files are used by the new installation to restore your original configuration. If you delete these folders and files, you need to reconfigure Automated Analytics when you reinstall it.

Uninstalling Using the Interface

The uninstaller for both Linux and Microsoft Windows systems leaves Automated Analytics customization data behind so you can archive, or, if you reinstall the product, reapply your customizations. The Linux uninstaller displays directory names that are left behind, but the Microsoft Windows version does not. For more information on the customization data or for instructions on removing it, see [Removing Data Folders and Files on page 42](#).

To uninstall Automated Analytics using the Control Panel:

Uninstall Automated Analytics on Microsoft Windows systems using **Add or Remove Programs** or **Programs and Features** in the **Control Panel**.

To uninstall Automated Analytics interactively:

1. From **Control Panel > Programs and Features**, right-click **Automated Analytics** and click **Uninstall/Change**.

The Automated Analytics 11.3 uninstall wizard is displayed.

2. Follow the prompts.

When the removal is complete, a Automated Analytics uninstall wizard is displayed.

3. Click **Finish**.
4. Archive the Automated Analytics subfolders under the Automated Analytics installation folder.

NOTE:

Fortra strongly recommends that you archive your data folders and files immediately after uninstalling Automated Analytics.

Uninstalling Using Commands

Some configuration and data folders and files are not deleted when you uninstall. If you reinstall the product at a later date, these files are used by the new installation to restore your original configuration. If you delete these folders and files, you need to reconfigure Automated Analytics if you reinstall.

To remove Automated Analytics from Microsoft Windows Systems:

1. Open the Control Panel and select **Uninstall a program**.
2. Right-click **Automated Analytics** and select **Uninstall**.
3. Click **OK**.
4. Click **OK** when prompted if you want to uninstall the program.

To remove Automated Analytics from Linux Systems

An uninstall command is available to remove any software within TeamQuest Performance Software installed with the `install.sh` script.

Removal of Automated Analytics must be completed using separate uninstall commands.

NOTE:

You must have superuser privileges to remove software with the `uninstall` command.

To remove Automated Analytics:

Run the following command:

```
yum remove vityl-data-analytics
```

where *version* is the version of Automated Analytics.

Removing Data Folders and Files

Uninstalling Automated Analytics removes program files and associated folders, but leaves behind Automated Analytics customization data. The customization data contain items such as user preferences, view and group definitions, user-defined and modified modules, and user and role definitions. You can archive the customization data and restore them at a later time, such as when moving Automated Analytics to another system or when restoring a backup file.

To remove Automated Analytics data folders and files:

1. Archive the folders under the Automated Analytics installation directory in both Microsoft Windows and Linux systems.
2. Delete the data folders and files. To delete all versions, delete the main installation path folder *TQDIR*. All files, subfolders, and versions of Automated Analytics are deleted.

Contacting Fortra

Please contact Fortra for questions or to receive information about Automated Analytics. You can contact us to receive technical bulletins, updates, program fixes, and other information via electronic mail, Internet, or fax.

Fortra Portal

For additional resources, or to contact Technical Support, visit visit [Support Portal](#).

For support issues, please provide the following:

- Check this guide's table of contents and index for information that addresses your concern.
- Gather and organize as much information as possible about the problem including job/error logs, screen shots or anything else to document the issue.