Toad® Intelligence Central 6.0

Quick Start Guide

Legend

i | **IMPORTANT**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

! | **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

Contents

Welcome to Toad Intelligence Central

Toad Intelligence Central enables enterprise users to be far more productive with their tools including Toad Data Point by centralizing automation workflows, accessing data directly, collaborating and sharing on datasets, queries and Toad files and providing a secure and established way to manage your data sprawl.

- AUTOMATE - Toad users can schedule the regular automated execution of Toad Data Point automation scripts on Toad Intelligence Central.

- ACCESS - Toad users can access Toad files and basic data files published to Toad Intelligence Central that have been shared with them. An additional data connectivity license extends Toad Intelligence Central to work across a wide range of data stores including relational database models, data warehouses, No SQL and Business Intelligence data sources like OBIEE and SAP®.

- SHARE - Objects can be shared amongst users and groups and organized collectively in a familiar folder structure, assigned tags and given a description for easy search retrieval. Administration of users and groups can be managed locally or users and groups can be imported from Active Directory®.

- SECURE - Toad Intelligence Central provides a centrally managed, secure, stable and accessible system.

Distributions of Toad Intelligence Central include a Web Server for administrative and general user access. In addition, Toad Data Point and other collaborative Toad products can directly access Toad Intelligence Central. Data on Toad Intelligence Central can be accessed via a third party product such as Tableau for further data processing and visualization.

About This Guide

This Guide is Intended for Non-Administrators

The Quick Start Guide is intended for non-Administrators and describes how to use the Web Console (Web Server) to view and access objects and files in Toad Intelligence Central. This guide provides information about functionality that is available to Standard and Power users.

Users with the Administrator Role

- For functionality available to users with the Administrator role, see the *Toad Intelligence Central Deployment Guide*.

Additional Resources

- Product documentation - Find the complete set of Toad Intelligence Central technical documents.

- Toad Intelligence Central User Forum - Learn more about Toad Intelligence Central, find answers to

questions, and connect with the community.

- Toad Intelligence Central Blogs - Find articles describing how to use the features in Intelligence Central.

Find Help from Inside Toad Intelligence Central

- To go to product documentation from the Web Console, click 🛈 and select **Technical Documentation**. This actions opens the Technical Documentation page for Toad Intelligence Central on the Quest Support Portal.

  There you will find the Release Notes, User Guide, Deployment Guide (installation and Administrator information), and What's New in This Release for the current and earlier versions of Toad Intelligence Central.

- To go to the Toad Intelligence Central User Forum in Toad World, click 🛈 and select **User Forum**.

License Toad Intelligence Central

Toad Intelligence Central is shipped with a trial key that enables a 90 day open trial license to Toad Intelligence Central. Use this key to evaluate Toad Intelligence Central. At the end of the 90 day trial, if a Data Connectivity license has not been entered, your Toad Intelligence Central functionality will be limited to that of the Toad Intelligence Central Community Edition.

Data Connectivity License

A Toad Intelligence Central Data Connectivity license is required to enable data connectivity functionality in Intelligence Central. Data connectivity functionality is required for publishing data objects (views, snapshots, and datasets) to Intelligence Central and for filtering and downloading data objects through the Web Console.

To view / activate Toad Intelligence Central licenses

1. From a web browser, log in to Toad Intelligence Central. Any Toad Intelligence Central user can add a license. Administrator credentials are required to remove a license.

2. Select **Administration | Licensing**.

3. If Toad Intelligence Central has multiple licenses assigned, select the license to view or click **Add License** to add a license.

Connect to Toad Intelligence Central

Use one of the following methods to access Toad Intelligence Central:

- **Web Console**—Use the Web Console (Web Server) to access Intelligence Central. A Web browser is required.
- **Toad Applications**—Use a Toad application, such as Toad Data Point, to connect to Intelligence Central.
- **Third-Party Tool**—Use a third-party tool, such as Tableau or a MySQL command line interface.

Method	Description
Web Console	See Open the Web Console for more information about accessing Intelligence Central through the Web Console.
	The Web Console (Web Server) provides Standard users with the ability to view and perform operations on objects published to Intelligence Central from other Toad applications. To use the Web Console, the Web server must be installed on the same computer as Intelligence Central.
	The Web Console allows users with the Administrator role to perform advanced activities such as the management of users, groups, and objects, as well as Intelligence Central server configuration and maintenance. See the *Toad Intelligence Central Deployment Guide* to learn more about performing Administrator activities through the Web interface.
Toad Applications	Toad Data Point users can publish data objects, Automation scripts, Toad documents, and other resources created in Toad Data Point to Intelligence Central.
	For these users, their primary method to view, access, manage, and edit Intelligence Central objects is through their Toad application.
	For more information about using Toad applications and working with published objects through the Web Console, see Connect Using Other Toad Applications
Third-Party Tool	See Third-Party Connection to Toad Intelligence Central for more information.
	A Toad Intelligence Central user can create a MySQL connection to Toad Intelligence Central through a third party tool such as Tableau, MySQL command line interface, or MySQL Workbench. This connection can be used to query Data Connectivity objects stored in Toad Intelligence Central.

Open the Web Console

When the Web server is installed along with the Intelligence Central server, users can access Intelligence Central through a Web-based interface using a Web browser.

To open the Toad Intelligence Central Web Console

- Open your Web browser and enter the URL to the server hosting Intelligence Central. Review the following for additional information.

URL	The address of Toad Intelligence Central is **http://***hostName*/ where *hostName* is the name of the computer hosting the Web Server and Toad Intelligence Central. If the Web Server has been installed on a port other than port 80 then the address is **http://***hostName:port*/.
Log in	Toad Intelligence Central prompts you to login.
	If you login to Toad Intelligence Central using Windows credentials, then enter your login name at the login prompt. If necessary, include your Windows domain: **domain\username**. The computer you use to login to Toad Intelligence Central must be accessible to your Windows domain.

> **i**   **NOTE:** The login screen may include an option to **Register as a new user**. If you do not have a login to Toad Intelligence Central then click this link to add yourself as a new user. The availability of this link is dependent on local configuration. For more information on this feature, see Users and Groups

> **i**   **NOTE:** Toad Intelligence Central encrypts your login credentials when transmitted over the network.
>
> Refer to your local Toad Intelligence Central Administrator for more information.

Connect Using Other Toad Applications

You can connect to Toad Intelligence Central through other Toad applications. This allows users to publish data objects, scripts, files, and other resources to Intelligence Central through other Toad applications. The types of objects that can be published dependents on the Toad application used. Functionality for viewing, accessing, managing, and editing Intelligence Central objects may also be available in these applications.

For detailed information about how to connect to and use Intelligence Central from another Toad application, please see the product documentation for that Toad product.

After objects are published to Intelligence Central, users can view, access, manage, and work with these objects through the Intelligence Central Web Console.

> **i**   **NOTE:** A Toad Intelligence Central Data Connectivity license is required to enable data connectivity functionality in Intelligence Central.

Toad Applications Used to Publish Objects

To learn more about the objects and the functionality available to you based on the Toad application used to publish the object, see one of the following:

- Work with Toad Data Point Objects
- Toad Data Modeler

Third-Party Connection to Toad Intelligence Central

A Toad Intelligence Central user can create a MySQL connection to Toad Intelligence Central through a third-party tool, such as one of the following:

- Tableau
- MySQL command line interface
- MySQL Workbench

This connection can be used to query tables, views, snapshots and datasets stored in Toad Intelligence Central.

Requirements / Limitations

Third party tool	Ensure the authentication method you use to connect to Toad Intelligence Central is supported by the third party tool. This is straightforward if you login to Toad Intelligence Central using credentials local to Toad Intelligence Central. If you login to Toad Intelligence Central using Windows credentials then the third party tool must also support MySQL connection via Windows credentials.
Computer where the third party tool is installed	Ensure a MySQL driver is installed appropriate to the third party tool and Toad Intelligence Central. Ensure the default character set is UTF8.
Toad Intelligence Central Share / Manage rights	To see an object that you did not create yourself you must have Share or Manage rights to that object. These rights can be granted by any Toad Intelligence Central user with Manage rights to the object using the Web interface or an application such as Toad Data Point.
Data source authentication	Ensure the data source authentication you use to access the result set of a table or view is defined in Toad Intelligence Central. This can be done using the Web interface (Web server) or Toad Data Point. It cannot be done using the third party tool.

Connection

Create the MySQL connection.

Parameter	Description
Host name	The name of the Toad Intelligence Central server host.

Parameter	Description
Port	The connection port to the Toad Intelligence Central server. This is the Port number set during installation of the Toad Intelligence Central server, by default 3566.
Username and Password	Your username and password to Toad Intelligence Central. Alternatively, if you use Windows credentials to connect to Toad Intelligence Central then select the option to connect via Windows credentials.

MySQL database

Select the MySQL database where the object is stored. This is dependent on the application used to create the object.

Application	Description
Toad Data Point	The database is defined when the object is published to Toad Intelligence Central.
Admin Console	For a table, view or snapshot the MySQL database is the name of the data source. For a dataset the database is of the form **data_**_owner_. The owner is the user that created the dataset.
	i NOTE: Beginning with Toad Intelligence Central 4.3, the Admin Console is no longer installed by the Toad Intelligence Central Installer. The administrative functionality of the Admin Console is now superseded by the Web Server. The activity of mapping/editing data objects is best performed through Toad Data Point.

i   NOTE: Hidden, temporary and internal Toad Intelligence Central databases and MySQL databases may be visible.

Queries

Query tables, views, snapshots and datasets.

i   NOTE: When querying tables and views, execution of SQL may fail under some circumstances. If the SQL used by the third party tool has a MySQL dialect, then that SQL may fail if the query is shipped to a non-MySQL relational database for remote execution. As a workaround, you could use Toad Data Point to save the table or view as a snapshot and then access the snapshot via the third party tool.

MySQL Views

You can use the following MySQL commands to verify the third party tool.

- SHOW [FULL] TABLES command
- DESC[RIBE] command
- EXPLAIN command
- SHOW [FULL] COLUMNS command

- SELECT query against information_schema.views
- SELECT query against information_schema.tables

Getting Started with the Web Console

The Toad Intelligence Central Web Console (Web Server) is a Web-based interface used to access Toad Intelligence Central.

The Web Console is a collection of pages/modules that provide access to the objects in Intelligence Central and provide functionality for managing objects, users, and the server.

In the Web Console you can do the following:

- Access data objects, files and other resources stored in Intelligence Central
- Filter and download data objects published from Toad Data Point
- Manage objects
- Generate and view reports
- Manage users and groups
- Perform administrative tasks on the Intelligence Central server

See Open the Web Console to learn how to connect to Intelligence Central using the Web Console.

Navigating the Web Console

When you log in to the Web Console, the main window opens displaying the **Home** page. The main menu is displayed on the left and provides a means to navigate to other pages and sections of the Web Console.

Click an item in the main menu to navigation to that page of the Web Console. The **Server** page of the Web Console (**Administration | Server**) is available only to users with the Administrator role.

Web Console Navigation - Main Menu

Section	Page	Page/Section Description
Home		The **Home** page allows you to view and access the objects shared with you. See Home Page.
Reports	**Data Objects**	The **Data Objects** page allows users to view and create reports about Intelligence Central object usage. See Data Object Usage Report.
Reports	**User Activity**	The **User Activity** page allows users to view and export user activity statistics. See User Activity Report.
Administration	**Users**	Use the **Users** page to view user information or to edit your user account details. See View and Edit Users.
Administration	**Groups**	Use the **Groups** page to view group information or edit a group you own. See View and Edit Groups.
Administration	**Licensing**	Use the **Licensing** page to view, add, or remove licenses. See License Toad Intelligence Central.
Administration	**Server**	The **Server** page is available only to users with the Administrator role. See the *Toad Intelligence Central Deployment Guide* for more information.

Home Page

The **Home** page is the default landing page presented when you open the Web Console. The Home page allows you to view and access the objects in Intelligence Central that have been shared with you.

You can use the Home page to organize the objects and folders for which you have Manage privileges. To determine if you have Manage privileges to an object or folder, select the object or folder to display the **Details** pane. The **Manager** field displays a list of managers. See Manager Privileges for more information about who can manage an object or secured folder.

Objects Visible to You

In the **Home** page of the Web Console, you see the objects and files in Intelligence Central that have been shared with you.

- Double-click a folder to open it.

- Select an object and click **Visibility** in the **Details** pane to see a list of users that share the object.

- You can see all the non-secured folders in Intelligence Central.

- You can see the secured folders that have been shared with you. You can see the parent folder of a secured folder that has been shared with you.

- Select a secured folder and click **Visibility** in the **Folder Details** pane to see a list of users that share the folder.

i | NOTE: A Toad Intelligence Central Data Connectivity license is required to enable data connectivity functionality in Intelligence Central.

Identify Objects by Icon

Icon	Description
	Non-secured folder—Visible to all users.
	Secured folder—Secured folders are visible only to users with visibility (sharing) privileges and can be managed only by users with manage privileges.

Icon	Description
	Automation script
	Dataset
	Snapshot
	View

Find, View and Work with Objects

See the following for additional information:

- Find Objects—To learn how to locate objects in Intelligence Central

- View Object Details—To learn how to view object information

- Work with Toad Data Point Objects—To learn how to download objects and data published from Toad Data Point

Move and Delete Objects

The Home page allows you to move and delete objects. Users with the Administrator role or manage privileges to the object can move or delete an object (unless the object is locked by another user).

- To move the selected object, select a destination folder from the **Folder** drop-down list (Details pane). Or drag-and-drop the object to another folder.

- Select an object and click to delete it.

- To move an object into a secured folder, the user must have the Administrator role or manage privileges to the object and the secured folder.

View Object Managers

- To view object managers, select an object to display its **Details** pane. Then click **Managers** in the Details pane to see which users have been granted manage privileges to the object.

See Manager Privileges for a list of actions enabled for object (and folder) managers.

Folders

Objects published to Intelligence Central are organized into folders. The object's publisher selects an existing folder or creates a new folder during the publishing process. You can also create folders through the Web Console.

Intelligence Central provides two types of folders: secured folders and non-secured folders. An Intelligence Central server can contain one or both types of folders. See About Secured Folders for more information.

- —Non-secured folders are visible to all users.

- —Secured folders are visible to users with visibility privileges to the folder.

- To create a new folder, select a folder and click in the **Folder Details** pane. See Create Folders for more information.

- You can drag-and-drop a folder to move it. See Move Folders for more information.

- To delete the selected folder, click in the **Folder Details** pane. See Delete Folders for more information.

- To view managers of a secured folder, select a folder and click **Managers** in the **Folder Details** pane. See View Folder Details for more information.

Toad Applications Used to Publish Objects

The types of objects and files in Intelligence Central depend on which Toad applications are being used to publish to Intelligence Central. For example, Toad Data Point users can publish data objects (views, snapshots, and datasets), Toad documents, Automation scripts, and other resources created in Toad Data Point.

To learn more about the objects and the functionality available to you based on the Toad application used to publish the object, see one of the following:

- Work with Toad Data Point Objects

- Toad Data Modeler

See Additional Documentation in the Toad Application

If your primary method to view and access Intelligence Central objects is through one of the Toad applications listed above, see the application's online Help for more-detailed information about the full range of functionality that is available to you through that Toad application.

Toad Data Point

Work with Toad Data Point Objects

Toad Data Point allows users to publish data objects (views, snapshots, and datasets), Toad documents (Query Builder, SQL Editor), Automation scripts, database connections, Project Manager projects, and other resources created in Toad Data Point to Intelligence Central.

If you are a Toad Data Point user, your primary method to view and access Intelligence Central objects is through the Toad Data Point application. However, both Toad Data Point users and non-users can view and perform limited operations on Intelligence Central objects using the Web Console.

i | **NOTE:** A Toad Intelligence Central Data Connectivity license is required to enable data connectivity functionality in Intelligence Central.

Download Objects

Users of Toad Intelligence Central can log in through a web browser and download Toad Data Point objects that have been shared with them.

1. Log in through a web browser. See Open the Web Console.

2. Click **Home**.

3. Locate the object. See Find Objects.

4. Select the object to show details. See View Object Details.

5. **Download object.** Click ⬇ in the Details pane to download the object. The location of the downloaded object is determined by your Web-browser settings.

   - **Enter Variables**—For views containing a variable, Intelligence Central prompts you for a variable value. Enter a new value or use the default. The new value applies to this download only. The default value is specified when the view is published from Toad Data Point and can be modified through Toad Data Point or Intelligence Central. To edit the default value, see Modify Variable Default Value.

     To enter the NULL value, select NULL from the drop-down list.

   - **Data objects**—For data objects (view, snapshot, or dataset), Intelligence Central prepares the object and displays a Success message when the object is ready to download. Click **Download** in the Success message to download the result set. For more information about data objects, see Data Connectivity Objects.

> **i** | **NOTE:** If authentication is required, Intelligence Central prompts you for credentials. For example, you might be required to authenticate the first time you access a View that was published with a personal key, instead of a shared key. See Add Authentication.

6. **Filter data.** For data objects, you can filter the data before downloading. Click ▼ in the Details pane to filter data. See Filter Data Before Downloading for more information.

Automation Scripts

The Intelligence Central Web interface allows you to view and execute Automation scripts that have been shared with you.

> **i** | **NOTE:** If the Automation Script scheduled to execute on the Toad Intelligence Central server includes an instruction to send an email then in order for that email to be sent the Toad Intelligence Central server must have access to an email SMTP port. If the Automation Script scheduled to execute on the Toad Intelligence Central server includes an instruction to create an Excel spreadsheet then Microsoft® Excel® must be installed on the Toad Intelligence Central host computer for the Excel spreadsheet to be created. Refer to your Toad Intelligence Central Administrator for more information.

View Script Details

Select a script to view script details in the Details pane. See View Object Details for a description of the Details fields. For Automation scripts, the following additional details are provided.

- **Schedule**—Displays the script execution schedule. Click **Schedule** to edit the schedule. See Modify Execution Schedule for more information.

- **Credentials**—Displays the name of the user account specified to run the Automation script. Click **Credentials** to select or modify the run account. See Alter Automation Script Credentials for more information.

- **Logs tab**—Displays script execution history. Click **Expand** to expand the Logs tab. This action allows you to view run duration, results, and exit code. Select a run (in the expanded tab) to view the individual execution log.

  > **i** | **NOTE:** Only Administrators and users with Manage privileges to the script can view the detailed execution logs.

Run Automation Scripts

You can execute an Automation script from the Web Console. You can execute scripts that have been shared with you.

1. Log in through a web browser. See Open the Web Console

2. Click **Home**.

3. Select the Automation script to execute.

4. Click ▶ in the Details pane.

- **Enter Variables**—If the Automation script executes SQL containing a variable, Intelligence Central prompts you for a variable value. Enter a new value or use the default. The new value applies to this run only. The default value is specified when the script is published from Toad Data Point and can be modified through Toad Data Point or Intelligence Central. To edit the default value, see Modify Variable Default Value.

  To enter the NULL value, select NULL from the drop-down list.

5. To cancel script execution, click the Stop button in the Details pane. You can also click the down arrow in the progress message (located in the page header) and then click **Cancel** in the Background Tasks pane.

6. In the Success (or Error) message, click **View Log** to display the execution log.

For more-detailed information about publishing, using, creating, and managing Automation scripts, see the Toad Data Point online Help.

Snapshots

In the Web Console, you can view and refresh Toad Data Point snapshots. You can view snapshots that have been shared with you (any folder) or snapshots that you own (non-secured folder). You can refresh snapshots to which you have Manage privileges.

View Snapshot Details

Select a snapshot to view snapshot information in the Details pane. See View Object Details for a description of the Details fields. For snapshots, the following additional details are also provided.

- **Schedule**—Displays the snapshot execution schedule. Click **Schedule** to edit the schedule. See Modify Execution Schedule for more information.

- **Columns tab**—Displays columns included in the snapshot. Select the **Columns** tab and click **Expand** to view more details.

- **Query tab**—Displays the snapshot's underlying query.

  ℹ | NOTE: Only Administrators and users with Manage privileges to the object can view the query text.

Refresh Snapshots

You can refresh a Toad Data Point snapshot from the Web interface.

1. Log in through a web browser. See Open the Web Console

2. Click **Home**.

3. Select the snapshot to refresh.

4. Click 🔄 in the Details pane.

5. You can view the refresh progress in the Background Tasks pane. Click the down arrow in the progress message (located in the page header) to open the Background Tasks pane.

For more-detailed information about creating, publishing, using, scheduling, and automating snapshots, see the Toad Data Point online Help.

Filter Data Before Downloading

You can filter the data in a view, snapshot, or dataset before downloading the data. This is useful for large data sets as it allows you to download only the data you need, instead of the entire data set.

i | **NOTE:** A Toad Intelligence Central Data Connectivity license is required to enable data connectivity functionality in Intelligence Central.

To filter data before download

1. In the Web interface, select an object to download on the Home page. See Work with Toad Data Point Objects for more information.

2. In the object's Details pane, click ![filter icon] to filter the data.

   - **Enter Variables**—For views containing a variable, Intelligence Central prompts you for a variable value. Enter a new value or use the default. The new value applies to this download only. The default value is specified when the view is published from Toad Data Point and can be modified through Toad Data Point or Intelligence Central. To edit the default value, see Modify Variable Default Value.

     To enter the NULL value, select NULL from the drop-down list.

   - **Download pane**—A data grid opens displaying a preview of the data. In this window you can quickly filter a column or you can create a filter in the filter editor.

   i | **NOTE:** If authentication is required, Intelligence Central prompts you for credentials. For example, you might be required to authenticate the first time you access a View that was published with a personal key, instead of a shared key. See Add Authentication.

3. To quickly filter a column, do the following:

   a. Enter a value in the text box below the column header. For date/time columns, click the down-arrow to select a date.

   b. Then click ![key icon] beside the text box to change the operator.

   c. Press **Enter** to apply the filter.

   d. The text of your filter displays in the upper-left, above the data grid. Click the filter text to open the filter editor and modify the filter further.

   i | **TIP:** Filter one or more columns to quickly create the framework for your filter. Then refine it in the filter editor.

4. To create/edit a filter in the filter editor, click **Create Filter** or click the filter text if you already started a filter.

   a. In the filter editor, click ![plus icon] to add an initial condition. The **And** operator is used by default. To use a different Boolean operation, click **And** and select a different operator.

   b. To modify an existing condition, click the operator or the value to edit it.

   c. To add another condition, click ![plus icon] .

d. To add another group of conditions, click the operator in the parent group and select **Add Group**.

e. Click **Save** to save your changes and close the editor.

> **i** | **TIP:** To create a complex filter, plan out your filter before building it in the filter editor. Identify grouped conditions (those in parentheses). Identify the Boolean operator for the main expression. Add parentheses to your expression if necessary to help clarify which conditions should be evaluated first.

5. The data grid displays a preview of the filtered data.

6. Click **Download** in the data grid window to begin the download process.

> **i** | **NOTE:** This action closes the data grid window containing your filter and preview of filtered data.

Intelligence Central prepares the filtered data and displays a Success message when the data is ready.

7. Click **Download** in the Success message to download the filtered data as a .csv file. The location of the download is determined by your Web-browser settings.

Add Authentication

If you attempt to access an object that requires authentication, such as a view published with a personal key for which you have not yet authenticated, Intelligence Central prompts you for credentials to the remote data source.

To add Authentication

1. If you attempt to access an object that requires authentication, the Add Authentication dialog opens. Enter your user name and password to the remote data source.

2. **Apply this to other view objects for this source that need authentication**—If setting your personal key for a view, select this option to apply these credentials to other views sourced from this data source with a personal key that also require authentication

3. If the object is a cross-connection query, perform the previous steps for each data source in the drop-down list that requires authentication.

See also, Alter Authentication.

Troubleshooting

Issue	Description
Unable to access earlier version view with shared key	In some cases, if a user attempts to access a view published from Toad Data Point 4.2 (or earlier) from multiple tables in one data source with a shared key, the Add Authentication dialog opens. **Solution:** Enter the password for the shared key in the Add Authentication dialog.

6

Toad Data Modeler

HTML Reports

HTML Report are created in Toad Data Modeler.

HTML Reports can be published from Toad Data Modeler to Toad Intelligence Central. From Toad Data Modeler they can be shared with users of Toad Intelligence Central. Refer to your Toad Data Modeler documentation for more information.

Users of Toad Intelligence Central can log in to the web browser, view and download Toad Data Modeler HTML Reports that have been shared with them.

1. Log in to the web browser.

2. Click **Home**.

3. Locate the object (Find Objects).

4. Select the object to show details (View Object Details).

5. Click **View** to view the HTML Report in your web browser.

6. Click to download the HTML report. The location of the report on download will be as per your web browser settings.

> **i** | **NOTE:** A Toad publisher can choose to share and update objects in a mandatory way on Toad Intelligence Central. This ensures consumers of the objects always have the latest updates. For more detail, refer to the Toad application used to publish.

7

Objects

Find Objects

Use the Web Console to find objects on Toad Intelligence Central.

Method	Description
By folder	Click **Home** to show objects in their folder structure. The objects you see are the objects that have been shared with you.
	The folders you see include all non-secured folders and the secured folders that have been shared with you.
	The folder tree is used to organize the objects published to Intelligence Central. A folder is created, or an existing folder is selected, when an object is published. Folders can also be created through the Web Console. For more information about folders, see Folders.
	See View Object Details for more information about the Details pane.
	The *No folder assigned* folder is a special folder.
	• The **No folder assigned** folder holds all objects not yet moved (or assigned) to other folders.
	• The **No folder assigned** folder cannot be moved, renamed or deleted.
	• The **No folder assigned** folder cannot have sub folders.
By search	Click **Home**. Use the search bar. The search results highlight text in the object name, object publisher, modified date, and object type fields that match the search string.
List just the objects you own	From your username, select **My Profile**. Alternatively, click **Administration | Users** and select your username.
	The objects owned by you that are in folders visible to you are listed in the **Published Objects** pane.
	• **Private**—Click to hide/show the objects that are visible only to you (as the owner) and the Administrators.
	• **Shared**—Click to hide/show the objects that are also shared with other Toad Intelligence Central users.
	i | **TIP:** Secured folder visibility privileges override object owner (publisher) visibility privileges.

Method	Description
List objects shared with you	From your username, select **My Profile**. Alternatively, click **Administration | Users** and select your username. The objects shared with you are listed in the **Shared Objects** pane. **i** **TIP:** Select a username other than your own. The objects this user has shared with you are listed in the **Published Objects** pane. The objects shared with both you and this user are listed in the **Shared Objects** pane.
List objects shared with a group	Click **Administration | Groups** and select the group. Objects shared with this group are listed in the **Shared Objects** pane. If you are a member of this group then you will see all shared objects. If you are not a member of this group then you will only see the objects shared with you; there may be additional objects shared with this group that you do not have the right to see.

View Object Details

Use the Details pane to view information about an object. You can also modify object properties from the Details pane. See Edit Object Details for more information.

To view object details

In the Web Console, click **Home**. Select an object to show object details.

Table 1: Object Details - Upper Pane

Detail	Description
Name	Object name. Managers of the object can rename the object. No two data objects can have the same name within the same folder. For Toad documents, the name must be unique within a folder per Toad document type. A script name must be unique among scripts. No two scripts can have the same name within an Intelligence Central instance. **i** **NOTE:** Tables and Mappable Objects cannot be renamed.
Description	The object's description. This is a short textual description of the object. The description is written when the object is published and can be edited by Managers of the object.
Tags	Tags are applied when an object is published and are editable by Managers. Tag names are created by the users of Intelligence Central. Typical examples of tag names include: the product name, the project name, or version number. Tags help the users of Toad Intelligence Central locate or group similar objects. Tags are an organizational tool. Tags are collectively managed by the users of Toad Intelligence Central. Valid characters are letters, numbers, space ( ), dash (-), underscore (_) or dot (.). Letters entered in upper case are converted to lower case.

Detail	Description
Folder	The folder in which the object is located. The folder is selected or created when the object is published. Folders can also be created through the Web Console. This field can be used to move an object by a user with the proper privileges. See Folders.
	To move the object, click within the **Folder** field and select a folder from the drop-down list.
	See Getting Started with the Web Console for more information about the folder structure.
	See About Secured Folders for more information about secured folders.
Object Type	Several types of objects can be published (or mapped) to Intelligence Central. Use this field to identify the type of object. An icon (Name column in grid) also indicates the object type.
	Toad artifacts are created in a Toad product then published to Toad Intelligence Central. There are many types of artifact. Each type is identifiable by icon.
	Data objects (views, snapshots, datasets), Automation scripts, and Toad documents are published from Toad Data Point.
	Data Connectivity object types are Tables, Views, Snapshots, Mappable Objects and Datasets. Use of Data Connectivity requires a Toad Intelligence Central Data Connectivity License.
Database	The underlying Intelligence Central database that contains the object. This can vary dependent on the application used to publish the object to Toad Intelligence Central.
	For example, Toad Data Point users can personalize the database when they publish the object to Toad Intelligence Central for all object types except Automation scripts. If the database is not personalized from Toad Data Point the object is stored in database **published_objects** or <folder name>. For Data Connectivity objects created in the Admin Console, **Database** is the display name of the data source in Toad Intelligence Central.
Source	For Data Connectivity objects, the Source is the actual name of the originating data source.
	• Click the data source link to modify the Authentication key or to update credentials. See Alter Authentication for more information.
	• When the data source has a shared key applied, the link is enabled only for users with Manage privileges to the object.
	For Automation scripts, this field displays the connections included in the script.
	i **TIP:** From a Web browser, where the name of the source is long, click the arrow to show/hide the full name.
Status	(Automation scripts and snapshots) Displays the last run or refresh time.
Schedule	(Automation scripts and snapshots) Displays the script or snapshot execution schedule.
	Click **Schedule** to edit the schedule. See Modify Execution Schedule for more information.
Publisher	The user on Intelligence Central who created the object.
Created	The date and time the object was created.
Updated	The date and time the object was last modified, and the user who last modified the object.

Detail	Description
Visibility	Displays the sharing (visibility) privileges for the selected object. Sharing privileges are specified when the object is published. Managers can modify the sharing (visibility) privileges.
	Click **Visibility** to open the Alter Visibility dialog where you can modify sharing and Manage privileges for the object. See Specify Visibility and Manage Privileges for Objects for more information.

	Private	The object can be seen by the owner and Administrator.
	Shared	The object can be seen by the owner, Administrator, and selected users and groups.
	Public	The object can be seen by all Intelligence Central users.

Detail	Description
Managers	Displays the list of users and groups with Manage privileges for the selected object. Manage privileges are specified when an object is published. Managers can modify the Manage privileges for the object.
	Click **Managers** to open the Alter Visibility dialog where you can modify the Manage privileges for the object. See Specify Visibility and Manage Privileges for Objects for more information.
Locked by	Displays the user who locked the object. See Edit Object Details for more information about locked objects.
Credentials	(Automation scripts) Displays the name of the user account specified to run the Automation script. The run account is initially specified at the time the script is published.
	Click **Credentials** to open the Alter Credentials dialog where you can select or modify the user account used to run the Automation script. See Alter Automation Script Credentialsfor more information.
Row Count	(Dataset and snapshot) Displays the row count for the data object.

Table 2: Object Details - Lower Pane

Click **Expand** to display the full contents of each tab. This action opens the lower pane in a separate window.

Tab	Description
Columns	(Views, snapshots, datasets, tables) The Columns tab displays the columns and data types for the object.
Query	(Views, snapshots) The Query tab displays the underlying query for the object.
	i **NOTE:** Only Administrators and users with Manage privileges to the object can view the query text.
Variables	(Views, Automation scripts) If the object includes one or more variables, the Variables tab displays and provides each variable name and default value. To edit default values, see Modify Variable Default Value.
Logs	(Automation script) The Logs tab provides execution times and results.
	i **NOTE:** Only Administrators and users with Manage privileges to the script can view the detailed execution logs.

Edit Object Details

You can edit object details in the Details pane for objects to which you have Manage privileges. The editable object details include name, description, tags, and folder. From the Details pane you can also move the object to another folder.

Edit Object Details

To edit object details

1. In the Web Console, click **Home**.

2. Select an object to display object details.

3. In the **Details** pane, select the property to edit. Modify the value and then click .

4. To move the selected object, select a folder from the **Folder** drop-down list.

Lock/Unlock Object

You can lock an object to prevent the object from being dropped by other users or to prevent certain attributes from being modified by other users. Users with Manage privileges for an object can lock it.

To lock an object

1. In the Web Console, click **Home**.

2. Select an object to display object details.

3. In the Details pane, click in the **Locked by** field.

Which Object Operations Are Locked

Once an object is locked, it cannot be modified or dropped, except by the user who locked it or by the Administrator. Only the user who locked it and the Administrator can unlock it.

Locking an object prevents users (except the user who locked it and the Administrator) from performing the following actions:

- Dropping an object

- Modifying an object's sharing or manage options

- Modifying a snapshot's refresh schedule

- Manually refreshing a snapshot

Which Object Activities Are Not Locked

- If a locked snapshot has a refresh schedule, it will continue to refresh at the scheduled time.

- Locked tables and views continue to reflect current data from the source. When you access a locked view, the query executes and retrieves the current data.

Move Objects

On the Home page, you can drag-and-drop an object to move it to another folder. You can also relocate an object by selecting the destination folder in the selected object's **Details** pane. Users with the Administrator role or manage privileges to the object can move an object (between non-secured folders). An object cannot be moved if it is locked by another user.

Restrictions:

- You cannot move rules out of the ***Common_Transformation_Repository***.

- You cannot sort or reorganize objects within a folder.

- You cannot move an object to a folder where the name exists.

- To move an object, you must have manage privileges to the object.

- To move an object to a secured folder, you must have manage privileges to the object and to the secured folder.

Specify Visibility and Manage Privileges for Objects

Users with Manage privileges to an object can modify the object's Visibility/Sharing and Manage privileges. See Manager Privileges for additional information.

To modify visibility and manage settings for a secured folder, see Specify Visibility, Manage and Publish Privileges for Folders.

Specify Visibility Privileges

You can modify the Visibility/Sharing options for an object to which you have Manage privileges.

To alter Visibility for an object

1. In the Web Console, click **Home**.

2. Select an object to display details.

3. In the Details pane, click **Visibility** to open the Alter Visibility dialog.

4. Select to either keep the object private, make it public, or share it with a list of users you specify. Review the following for additional information.

Sharing Option	Description
Keep this data private	Select to keep the object private.

Sharing Option	Description
Share this data with any user	Select to make the object public.
	Allow any user to manage this object—Select this option to grant Manage privileges to all users.
Share this data with selected users and groups	Select this option to make the object available to a list of users you specify. Then add users and groups to the right pane. You can include both individual users and groups.
	Manage—Select this option for each user (or group) to which you want to grant Manage privileges.

i | **NOTE:** When privileges are assigned to a group, a new member added to the group is automatically assigned the privileges of the group. When the user is removed from the group, any rights associated with that group are removed for that user. A user is given the highest level of privileges applied to them, whether it is as an individual user or as a member of a group.

Specify Manager Privileges

You can modify the Manage privileges for an object to which you have Manage privileges.

To modify Manage privileges for an object

1. In the Web Console, click **Home**.

2. Select an object to display object details.

3. In the Details pane, click **Managers** to open the Alter Visibility dialog.

4. Select a Manage option based on the specified Visibility setting:

Visibility Setting	Manage Option
Share this data with any user	**Allow any user to manage this object**—Select this option to provide manage privileges to all users.
Share this data with selected users	Select the check box in the **Manage** column for each user (or group) to which you want to grant Manage privileges.

Users with **Manage** privileges to an object can do the following (unless the object is locked):

- Lock the object

- Delete the object

- Modify the object's sharing options

- Modify the object's manage options

- Rename the object

- (Automation script) Change user account for script execution

- (Snapshot) Refresh snapshot or modify refresh schedule

- (Automation script) Modify schedule

- (View or Automation script) Modify variable default value
- Change a shared key password
- Change Authentication key type

Alter Authentication

Use the Alter Authentication dialog to set your personal authentication key, to update keys when your remote data source password changes, or to change authentication key type for a view.

You can use the Alter Authentication dialog to perform the following tasks:

- **To set your personal authentication key**—You are required to authenticate the first time you attempt to download a view that was published with a personal key. Enter your personal login credentials to access the remote source.

- **To change your personal authentication key password**—If your password changed for a remote data source, you must also change the password in your authentication key.

- **To change a shared key password**—If the password changed for the shared account in the remote data source, you must also change the password for the shared authentication key. Users with Manage privileges can modify a shared key.

- **To change personal key to shared key**— Change the type of key applied to an object from personal to shared. All personal keys are removed. Users with Manage privileges to the object can change the authentication key type.

- **To change shared key to personal key**— Change the type of key applied to an object from shared to personal. After the personal key is applied, users with which the object is shared are required o set a personal key by providing personal login credentials to the remote source. Users with Manage privileges to the object can change the authentication key type.

  > **i** | **NOTE:** This action is not available for snapshots. You can apply only a shared key to a snapshot.

To modify Authentication

1. In the Web interface (Web server), select the **Home** page.

2. Select an object to display object details.

3. In the **Details** pane, click the link in the **Source** field. If the object has multiple data sources, multiple links are displayed. Select a link to open the Alter Authentication dialog.

4. In the Alter Authentication dialog, select the data source for which you want to modify authentication.

5. (Views) To set your personal key, enter your login credentials for the remote data source.

6. If you are updating your password, enter the new password.

7. (Views) To change a personal key to a shared key, select **Share authentication**.

8. (Views) To change a shared key to a personal key, clear the **Share authentication** check box.

   > **i** | **NOTE:** This option is not available for snapshots. You can apply only a shared key to a snapshot.

9. (Views) **Apply this to other view objects for this source that need authentication**—If setting your personal key, select this option to apply these credentials to other views sourced from this data source with a

personal key that also require authentication.

> **i** | **TIP:** If your password changed for a remote data source, you must also change the password in your personal authentication keys. If you are using the Alter Authentication dialog to change a personal authentication key password, select this option to apply the change to all applicable views.

Specify this option separately for each data source in the drop-down list.

> **i** | **NOTE:** This option is disabled for a shared key.

Email Users from Details Pane

You can send an email to a user by clicking the user's name when it is displayed in the Details pane. A user name can be displayed in one or more fields in the Details pane.

1. In the Details pane, click a user name displayed in one of the fields, such as Publisher, Updated, Visibility, or Managers.

2. This action opens an email pre-populated with the user's address and the object name. Add a message and additional information before sending the email.

Modify Execution Schedule

You can modify the execution schedule for a snapshot or an Automation script through the Web Console (Web Server). A user with Manage privileges to the object can modify its schedule.

To modify the schedule for a snapshot or Automation script

1. In the Web interface, click **Home**.

2. Select an object to display object details.

3. In the Details pane, click **Schedule** to open the Alter Schedule dialog.

4. (Automation script) To execute the script immediately, select the **Execute once at** option.

5. (Snapshot and Automation script) To schedule a recurring execution, select a frequency and a start date.

   - To schedule more than one execution within one day, select **Other** and specify a frequency.

6. (Automation script) To disable the script, select **Disable this scheduled automation**.

Alter Automation Script Credentials

An Automation script running in Intelligence Central runs under a specified user account. Initially, this run account is specified at the time the script is published. After the script is published, you can use the Alter Credentials dialog to perform the following tasks:

- Change the account under which the script runs

- Change the password for the current run account

Only users with the Administrator role or with Manage privileges to the Automation script can change the account under which the script runs.

Alter Automation script user account

1. In the Web interface, click **Home**.

2. Select an Automation script to display object details.

3. In the Details pane, click **Credentials** to open the Alter Credentials dialog. Select one of the following:

   - **Specify user to execute automation script**—Select to specify a Windows user account. Then enter account credentials.

   - **Use default user to execute automation script**—Select to use the default user account, which is the account under which the Toad Intelligence Central App Server is currently running.

     For best results when using the default user (App Server) account to run scripts, give this account all the necessary permissions to successfully execute the scripts. Normally, the Intelligence Central App Server uses the server's Local System user account.

   To limit the script run time, enter a maximum run time in **Script execution limit**.

4. If you want to change the password for the current run account (if Windows user account), enter the new password and click **Save**. This action updates the password for each script that runs under this user account.

Modify Variable Default Value

A view or Automation script can contain one or more variables. Each variable has a default value. The initial default value is specified when the view or script is published from Toad Data Point.

You can modify a variable default value for a view or Automation script through the Web Console (Web Server). You can modify the default value for objects to which you have Manage privileges.

When downloading a view or manually running an Automation script that contains a variable, Intelligence Central allows users to enter a variable value. This run-time value applies to the current download or execution and does not change the default value. See Work with Toad Data Point Objects for more information.

To modify variable default value

1. In the Web interface, click **Home**.

2. Select an object containing a variable to modify.

3. In the lower portion of the Details pane, select the **Variables** tab or click **Expand** and then select the **Variables** tab.

   > **i** | **NOTE:** The Variables tab displays only for objects containing one or more variables.

4. Enter a new value in the **Default Value** column.

- For a view, the new value will be used when the result set is returned.

- For a script, the new value is used when the scheduled script is executed.

Data Connectivity Objects

Data connectivity functionality allows Toad Data Point users to publish data objects (views, snapshots, and datasets) to Intelligence Central. Data objects are published to Intelligence Central as a way to store and share data from remote data sources.

i | **NOTE:** A Toad Intelligence Central Data Connectivity license is required to enable data connectivity functionality in Intelligence Central.

Users of Toad Intelligence Central can log in to the Web Console (Web Server) to view and download Data Connectivity objects that have been shared with them.

1. Log in to the Web Console (Web Server).

2. Click **Home**.

3. Locate the object. See Find Objects for more information.

4. Select the object to show details. See View Object Details for more information.

5. Click ⬇ to download the object. The location of the object on download will be as per your Web browser settings.

For more information about working with objects published from Toad Data Point, see Work with Toad Data Point Objects.

Object type	Download, view		
Table	Tables are tables of data mapped from data source mappable objects.		
	Download	Click ⬇ to prepare download of the table result set.	
		Data is retrieved direct from the data source. Some time may be required to prepare the data for download.	
		ℹ NOTE: If authentication is required, Intelligence Central prompts you for your credentials.	
		Track the preparation of the download on the web browser display. Success is an indicator that the table is ready for download.	
		✓ Success:	
		Click **Download** in the Success message. The location of the table on download will be as per your Web browser settings.	
	Source	The source is one of the object details listed on the **Details** pane. Where the name of the data source is long, the web browser has the facility to expand/ contract your view. Table data is retrieved from this source.	
		Click the data source link to alter authentication. See Alter Authentication for more information.	
	Columns	Show the table structure, column names, and data types.	
	Expand	Click to expand and show column details: data type, data size and Not Null status.	

Object type	Download, view	
View 👓	Views are saved SQL statements.	
	Download	Click 📥 to execute the SQL statement on the data source and prepare the result set for download. Some time may be required to prepare the data for download.
		ⅈ | **NOTE:** If authentication is required, Intelligence Central prompts you for your credentials. For example, you might be required to authenticate the first time you access a View that was published with a personal key, instead of a shared key.
		Track the preparation of the download on the web browser display. Success is an indicator that the result set is ready for download.
		✔ Success:
		Click **Download** in the Success message. The location of the result set on download will be as per your web browser settings.
	Source	The source is one of the object details listed on the **Details** pane. The SQL statement is executed against this data source. Where the name of the data source is long, the web browser has the facility to expand/ contract your view.
		Click the data source link to alter authentication. See Alter Authentication for more information.
		ⅈ | **NOTE:** When the data source has a shared key applied, the link is enabled only for users with Manage privileges to the object.
	Query	Show the query that is executed to produce the result set.
		ⅈ | **NOTE:** Only Administrators and users with Manage privileges to the object can view the query text.
	Expand	Click to expand and show column details: data type, data size and Not Null status.

Object type	Download, view	
Snapshot	Snapshots are the result set from an executed SQL statement (View) or table. Snapshots capture data at a specific point in time and can be scheduled to execute once or repeatedly. Snapshot data is stored in Intelligence Central so it is fast to load and does not require data source authentication to view. Snapshots are published with a shared key.	
	Download	Click ![icon] to prepare download of the snapshot result set. This converts the snapshot to a CSV file. Depending on the size of the snapshot, this can take some time. Track the preparation of the download on the web browser display. Success is an indicator that the snapshot is ready for download. ✓ Success: Click **Download** in the Success message. The location of the snapshot on download will be as per your web browser settings.
	Source	The source is one of the object details listed on the **Details** pane. The SQL statement is executed against this data source. Where the name of the data source is long, the web browser has the facility to expand/ contract your view. Click the data source link to alter authentication. See Alter Authentication for more information. ℹ **NOTE:** When the data source has a shared key applied, the link is enabled only for users with Manage privileges to the object.
	Status	Status is an object detail that indicates the execution status of the snapshot. It may be success, error, running (currently taking the snapshot) or pending (where Toad Intelligence Central is waiting to take the snapshot). If there was an error taking the last snapshot then expand to see the error details.
	Schedule	When was the last snapshot taken? When will the next snapshot be taken? The snapshot is scheduled to refresh (the result set) at the given date and time.
	Query	Show the query that is executed to produce the result set. ℹ **NOTE:** Only Administrators and users with Manage privileges to the object can view the query text.
	Expand	Click to expand and show column details: data type, data size and Not Null status.

Mappable Objects	Mappable objects are objects from the data source that can be potentially mapped to tables. Mappable objects are not available for download and not visible from a web browser.	

Object type	Download, view

Datasets	Datasets are tables of data published to Toad Intelligence Central.
	
	From a web browser, click **Home**. Locate the dataset.
	
	    1. Select the dataset to show details.
	
	    2. Click in the Details pane. This converts the dataset to a CSV file. Depending on the size of the dataset, this can take some time.
	
	    3. Track the preparation of the download on the web browser display. Success is an indicator that the dataset is ready for download.
	
	    4. Click **Download** in the Success message. The location of the dataset on download will be as per your web browser settings.

Folders

Objects published to Intelligence Central are organized into folders. The object's publisher selects an existing folder or creates a new folder during the publishing process in Toad Data Point. Intelligence Central users can also create folders through the Web Console.

Folders in Intelligence Central

Intelligence Central can contain several different types of folders. These folders can differ by purpose, origin, contents, and characteristics. Review the following descriptions for different folder types in Intelligence Central.

Special Folders

The following folders are created by Intelligence Central and have specific functionality.

No folder assigned

The *No folder assigned* folder is a special folder.

- The **No folder assigned** folder holds all objects not yet moved (or assigned) to other folders.
- The **No folder assigned** folder cannot be moved, renamed or deleted.
- The **No folder assigned** folder cannot have sub folders.

Common_Transformation_Repository

Toad Data Point users can publish Transform and Cleanse Rules to Intelligence Central to share with other users. These Transform and Cleanse Rules are stored in the **Common_Transformation_Repository** folder. See the *Toad Data Point Help* for more information about this feature.

- The **Common_Transformation_Repository** folder and its subfolders cannot be moved, renamed or deleted.
- You cannot move rules out of the **Common_Transformation_Repository** folder.

Secured and Non-Secured Folders

Aside from the special folders listed above, Toad Intelligence Central provides two types of folders for storing objects: secured folders and non-secured folders. Secured folders have visibility (sharing) and manage privileges assigned to them. Non-secured folders do not. See About Secured Folders for additional information.

An Intelligence Central server can provide one or both types of folders. A user with the Administrator role can configure which types of folders can be created and which user role/roles are allowed to create secured folders. For more information about configuring Folder Security, see the *Toad Intelligence Central Deployment Guide*.

Icon	Description
	Non-secured folder—Visible to all users.
	Secured folder—Secured folders are visible only to users with visibility (sharing) privileges and can be managed only by users with manage privileges.

Create Folders

You can create a new folder using the Web Console (Web Server). A folder can also be created through Toad Data Point when an object is published. Only alpha, numeric, and the underscore (_) characters are allowed in folder names. A name cannot begin with the underscore character.

Restrictions

- You cannot create a secured folder in a non-secured folder.

- You cannot create a non-secured folder in a secured folder.

- To create a subfolder in a secured folder, you must have manage privileges to the parent secured folder.

- Folder creation is restricted to the folder types specified by the server-level Folder Security settings.

- To create a secured folder, the user's *role* must have permissions granted by the server-level Folder Security settings.

For more information, see About Secured Folders.

To create a new folder

1. On the **Home** page, select a folder and click ➕ in the **Folder Details** pane.

2. In the Create Folder dialog, select a folder to serve as the parent folder. To create a folder at the root level, select **Folders**.

3. Click the button corresponding to the type of folder you want to create.

    - **New Non-Secured Folder**—Select to create a non-secured folder.

    - **New Secured Folder**—Select to create a secured folder.

    ℹ️ | **NOTE:** If a button is disable, creation of that folder type is not allowed, either at the server level or in the selected parent folder. See the Restrictions listed above.

4. Enter a folder name and click **OK**.

5. (Secured folder only) After a secured folder is created, you can then modify the visibility (sharing) and manage privileges, if necessary. Initially, only the folder creator and users with the Administrator role have visibility and manage privileges to the folder. The folder creator is automatically listed under folder Managers. See Specify Visibility, Manage and Publish Privileges for Folders for more information.

ℹ️ | **NOTE:** A folder can be created by an object's publisher during the publishing process in Toad Data Point. See the *Toad Data Point Help* for more information.

Move Folders

On the Home page, you can drag-and-drop a folder to move it. To move a folder, a user must have the Administrator role or manage privileges to all objects in the folder. A folder cannot be moved if an object in the folder is locked by another user.

Restrictions:

- You cannot move the *Common_Transformation_Repository* or its sub-folders.
- You cannot move the *No folder assigned* folder.
- You cannot move a folder while a snapshot in the folder is refreshing.
- You cannot move a secured folder into a non-secured folder.
- You cannot move a non-secured folder into a secured folder.

See About Secured Folders for more information about secured folders.

Delete Folders

You can delete a folder if you have the Administrator role or have manage privileges to all objects in the folder (unless an object is locked by another user).

To delete a folder

- On the **Home** page, select a folder and click in the Folder Details pane.

You cannot delete the *No folder assigned* folder.

View Folder Details

You can view information about a folder in Intelligence Central through the Folder Details pane. This is useful, especially for secured folders, which have sharing (visibility) and manage privileges assigned to them.

You can view the secured folders that have been shared with you. You can also view the parent folder of a secured folder that has been shared with you.

To view folder details

- In the **Home** page of the Web Console, select a folder to display the **Folder Details** pane. Review the following for additional information.

Detail	Description
Name	Folder name. For a secured folder, managers of the folder can rename the folder.
Creator	Folder creator. This is the name of the user who initially created the folder.

Detail	Description
Visibility	(Secured folders) Displays the visibility (sharing) privileges for the selected folder. Managers can modify the visibility privileges.
	Click **Visibility** to open the Alter Folder Visibility dialog where you can modify visibility and manage privileges for the folder. See Specify Visibility, Manage and Publish Privileges for Folders for more information.
Managers	(Secured folders) Displays the list of users and groups with manage privileges for the selected folder. Managers can modify the visibility and manage privileges for the object.
	Click **Managers** to open the Alter Folder Visibility dialog where you can modify the manage privileges for the folder. See Specify Visibility, Manage and Publish Privileges for Folders for more information.
Publishers	(Secured folders) Displays the list of users and groups allowed to publish objects to the selected folder. Users with manage privileges can modify publish privileges for the folder through the Alter Folder Visibility dialog. See Specify Visibility, Manage and Publish Privileges for Folders for more information.

For additional information about manage privileges for secured folders, see Manager Privileges.

About Secured Folders

Secured folders are special folders in Toad Intelligence Central. Secured folders have visibility (sharing), manage, and publish privileges assigned to them. Non-secured folders do not.

Secured Folder Characteristics

Secured folders have the following special characteristics:

- Secured folders have visibility, manage, and publish privileges assigned to them.

- The sharing and manage privileges specified for a secured folder are also applied to all objects in the folder.

- When an object is published to a secured folder, the object automatically inherits the visibility and manage privileges applied to the secured folder.

Why Use Secured Folders

The special characteristics of secured folders provide the following advantages:

- Object publishers can automatically define visibility and manage privileges for an object by publishing it to the desired folder. In this way, the task of specifying object privileges can be transferred from the individual user to a group of folder managers.

- A folder manager can change the visibility and manage privileges for all objects in a secured folder at one time by simply changing the privileges for the secured folder itself.

These characteristics, along with the server-level Folder Security settings, allow companies to customize the way they define and manage object accessibility in Intelligence Central.

Use this feature to develop and implement a methodology for controlling and regulating the sharing and management of objects, files, and data.

Server-Level Configuration

Intelligence Central allows you to specify which type of folders users can create: secured, non-secured, or both. You can also specify which users are allowed to create and configure secured folders. These settings are specified at the server level by a user with the Administrator role.

To learn how to configure secured folder settings for the server, see the *Toad Intelligence Central Deployment Guide*.

Rules and Restrictions for Secured Folders

Review the following rules and restrictions that apply to secured folders and their objects.

Visibility Privileges

- You can see secured folders that have been shared with you.
- You can see the parent folder of a secured folder that has been shared with you.

Privileges Based on User or Role

- By default, the folder creator and users with the Administrator role have visibility and manage privileges to a newly-created secured folder.
- Users with the Administrator role retain visibility and manage privileges to secured folders.

Subfolder Privileges

- A subfolder is not required to have the same visibility or manage privileges as the parent folder.
- A subfolder is not affected by changes to privileges for the parent folder.

Publishing

- In order to publish an object to a secured folder, the publisher must be an Administrator or have publish privileges to the secured folder.

Creating and Moving Folders

- A non-secured folder cannot be created in or moved into a secured folder.
- A secured folder cannot be created in or moved into a non-secured folder.
- A secured folder can be created at the root level.

Object Privileges

- All objects in a secured folder have the same manage and visibility privileges as the folder.

Moving and Deleting Secured Folders

- To move a secured folder, a user must have the Administrator role or manage privileges to the secured folder and all its subfolders.
- To delete a secured folder, a user must have either the Administrator role or visibility and manage privileges to the secured folder and all its subfolders.

Rules for Moving Objects into or out of a Secured Folder

- To move an object into a secured folder, the user must be an Administrator or have manage privileges to the object and the secured folder.

- If an object is moved into a secured folder, the object inherits the privileges of the secured folder, regardless of the object's original privileges.

- When an object is moved into a secured folder, the object publisher does not retain manage privileges unless the publisher is a *folder manager*.

- When an object is moved from a secured folder into a non-secured folder, the object's manage privileges are retained. For visibility privileges, only users with manage privileges to the object will retain visibility, others will not.

Notifications of Secured Folder Activity

- If a secured folder's objects or subfolders are moved, users with visibility or manage privileges to the folder receive an email notification.

- If an object is moved into a secured folder, the object publisher and users with visibility or manage privileges to the object will receive an email notification.

Specify Visibility, Manage and Publish Privileges for Folders

Secured folders have visibility (sharing), manage, and publish privileges assigned to them. Users with manage privileges to a secured folder can modify the visibility, manage, and publish privileges.

To learn how to modify privileges for an object, see Specify Visibility and Manage Privileges for Objects.

Specify Sharing Privileges

You can modify the visibility (sharing) options for a secured folder to which you have manage privileges. The sharing options you specify for a secured folder are applied to all objects in the folder.

To alter Visibility for a secured folder

1. In the Web Console, click **Home**.

2. Select a secured folder to display details.

3. In the Folder Details pane, click **Visibility** to open the Alter Visibility dialog.

4. In the Alter Visibility dialog, select the users and groups with which you want to share the folder.

   - Add users and groups to the right pane. You can include both individual users and groups.

5. For each user (or group) specify manage and publish privileges.

   Manage—Select this option for each user (or group) to which you want to grant Manage privileges.

   Publish—Select this option for each user (or group) to which you want to grant Publish privileges.

i   **NOTE:** When privileges are assigned to a group, a new member added to the group is automatically assigned the privileges of the group. When the user is removed from the group, any rights associated with that group are removed for that user. A user is given the highest level of privileges applied to them, whether it is as an individual user or as a member of a group.

i   **TIP:** Refresh or reload through your Web browser if changes to folder visibility are not immediately reflected in the Web Console.

Specify Manage and Publish Privileges

You can modify the manage and publish privileges for a secured folder to which you have Manage privileges. The manage options you specify for a secured folder are applied to all objects in the folder.

For more information about manage privileges, see Manager Privileges.

You can also specify publish privileges to allow users to publish objects to the secured folder. Users with or without the manage privilege can be granted the publish privilege.

To modify Manage and Publish privileges for a secured folder

1. In the Web Console, click **Home**.

2. Select a secured folder to display folder details.

3. In the Folder Details pane, click **Managers** to open the Alter Visibility dialog.

4. In the Alter Visibility dialog, do the following:

    - Select the **Manage** check box for each user (or group) to which you want to grant Manage privileges.

    - Select the **Publish** check box for each user (or group) to which you want to grant Publish privileges.

Users with **Manage** privileges to a secured folder can do the following:

- Modify the folder's sharing (visibility), manage, and publish options

- Rename or delete the folder

- Create a subfolder

Users with **Publish** privileges to a secured folder can publish objects to the folder from Toad Data Point.

Manager Privileges

When an object is published to Intelligence Central, the publisher specifies visibility (sharing) and manage privileges for the published object.

After an object is published, the object's managers are allowed to modify the visibility and manage privileges for the object.

When a secured folder is created, the folder creator and users with the Administrator role have visibility and manage privileges to the folder. After the folder is created, the secured folder's managers can modify the visibility and manage privileges, if necessary.

To learn how to modify visibility and manage settings for an object or folder, see Specify Visibility and Manage Privileges for Objects and Specify Visibility, Manage and Publish Privileges for Folders.

Manager Privileges for Objects

Users with **Manage** privileges to an object can do the following (unless the object is locked):

- Lock the object
- Delete the object
- Modify the object's sharing options
- Modify the object's manage options
- Rename the object
- (Automation script) Change user account for script execution
- (Snapshot) Refresh snapshot or modify refresh schedule
- (Automation script) Modify schedule
- (View or Automation script) Modify variable default value
- Change a shared key password
- Change Authentication key type

Manager Privileges for Secured Folders

Users with **Manage** privileges to a secured folder can do the following:

- Modify the folder's sharing (visibility), manage, and publish options

- Rename or delete the folder

- Create a subfolder

Who Can Manage Objects/Folders

The following tables describe some important details about manage privileges based on a user's relationship to an object or folder.

Management Privileges to Objects

User	Details
Object Publisher	**For objects in a *non-secured* folder**—The object publisher has (and retains) manage privileges. **For objects in a *secured* folder**—Secured folder privileges override object privileges. • In order to publish an object to a secured folder, the publisher must have publish privileges to the folder. • All objects in a secured folder have the same manage and visibility privileges as the folder. See About Secured Folders. • When an object is moved into a secured folder, the object publisher does not automatically retain manage privileges. The object publisher must also be a *folder manager* to retain manage privileges to the object.
Object Managers	**For objects in a *non-secured* folder**—Users who have been granted manage privileges to the object can manage the object. **For objects in a *secured* folder** • Users who have been granted manage privileges to the secured folder can manage all objects in the secured folder.
Administrators	Users with the Administrator role can manage all objects.

Management Privileges to Secured Folder

User	Details
Secured Folder Managers	Users who have been granted manage privileges to a secured folder can manage the folder.
Administrators	Users with the Administrator role can manage all secured folders.

10

Reports

The Web Console provides a Reports section which allows you to view and create reports about Intelligence Central objects and user activity.

Reports are designed mainly for Administrators, but all users can view and export reports.

The following reports are provided:

- Data Object Usage Report
- User Activity Report

Data Object Usage Report

The **Data Objects** page of the Reports section allows you to view, create, and download reports about Intelligence Central object usage. The Data Objects landing page provides a dashboard-type view that displays top-level object usage statistics. This report is designed mainly for Administrators, but all users can view and export object usage reports.

To open the Data Objects page, select **Reports | Data Objects**.

i | **NOTE:** Standard and Power users can view statistics for all objects. However, for these users, access to an object from a report page is limited to objects shared with or owned by the user.

Dashboard View

The dashboard displays top-level usage statistics. Use the dashboard to drill down to more-detailed information or object details. The dashboard graphs group data into the following categories:

- Most-popular objects
- Percentage of objects used
- Most-often published objects

To Filter the Dashboard View

- Select a time period from **What's happened over the ...**.

What's popular?

This chart displays the most popular objects, i.e., the objects that have been downloaded or queried the most. You can click an object name to view object details.

1. Click an object name to open the **Home** page with the object selected.

2. In the **Home** page you can view the object details or perform additional actions on the object, such as download the object.

What's been used?

This graph displays the percentage of objects used (downloaded or queried) in Intelligence Central. Click a graph data point to see the data broken down into usage statistics for the individual objects. Use filtering to narrow your results.

1. Click either the **Objects Used** or **Objects Not Used** section of the graph to view a breakdown of the data.

2. In the **Objects Used** or **Objects Not Used** page, you can filter results by selecting a different time period.

3. **Filter results by object.** (Objects Used) In the Object Downloads and Queries chart, click an object's bar or value to filter the data grid by that object.

4. **Filter results by date.** (Objects Used) In the Daily Downloads and Queries graph, click a data point to filter the data grid by that date.

5. To sort by a column in the data grid, click the column header.

6. To export the data in the data grid, click **Download CSV**.

What's been published?

This graph shows what types of objects have been published during the selected time period, as well as the percentage for each object type. Click a graph section to view publishing statistics related to each object type.

1. Click a section of the graph to view a breakdown of the data for that object type.

2. In the object type page, you can filter results by selecting a different time period.

3. **Change object type.** To see results for a different object or for all objects simultaneously, select an option from the second drop-down list.

4. **Top 10 Publishers.** Click ![Top 10] to see data for the top 10 publishers. In the Top 10 Publishers chart, hover the cursor over a bar to see a breakdown by Sharing option. Click a bar to filter the data grid by that publisher. To clear the filter, click the highlighted bar again.

5. **All Publishers.** Click ![All] to see data for all publishers. Click a publishers name to filter the data grid by that publisher. Click a value to filter the data grid by that criteria.

6. To sort by a column in the data grid, click the column header.

7. To export the data in the data grid, click **Download CSV**.

User Activity Report

The **User Activity** page of the Reports section allows you to view statistics related to Toad Intelligence Central user activity. This report is designed mainly for Administrators, but all users can view and export user activity data.

- To open the User Activity page, select **Reports | User Activity**.

Landing Page

The landing page for this report provides a summary of user activity in Toad Intelligence Central.

To filter the landing page

1. Select a time period from the **Active Users Over the...** drop-down list.

2. Then select the activity for which you want to view user statistics.

    - Select **Published** to view the most-active publishers.

    - Select **Consumed** to view the most-active consumers. Consumer activities include downloading files, downloading data objects, querying data objects from Toad Data Point, and running Automation scripts.

    Users are sorted according to the number of objects published or consumed, highest to lowest. The top 10 most-active users (for the selected activity) are displayed.

Other actions

- Click the *N* **Total Users** link to go to the **Users** page of the Web Console (Administration | Users) where you can view a list of Intelligence Central users, as well as user details (including objects associated with a user).

- Click the *N* **Total Groups** link to go to the **Groups** page of the Web Console (Administration | Groups) where you can view a list of Intelligence Central groups, as well as group details and a list of objects shared with the group.

Drill Down to Additional Data

From the landing page, you can drill down to view more data about user activity.

To drill down to additional data

1. Click the *N* **Active Users** link to view an expanded list of user activity. The time period is preserved. You can also export data from this page.

    On the TIC Active Users page, you can do the following:

    - Click a column header to sort the data grid by that column.

    - Click **Download CSV** to export the data to a .csv file.

    - Select a different time period from **Active Users Over the...**.

2. Click a user name to drill down to a list of the user's activities.

    - On the user's page, click a column header to sort the list by that column.

    - Click **Download CSV** to export the data to a .csv file.

3. Click a link in the breadcrumb navigation to go back to a previous page.

Users and Groups

New users and groups can be added to Toad Intelligence Central. Which user role is required before adding new users is dependent on how Intelligence Central is configured. A user with the Administrator role can configure registration parameters through the Web interface. To learn how to configure new user registration, see the *Toad Intelligence Central Deployment Guide*.

Use the following icons to identify the type of user or group wherever users/groups are displayed, for example the Users or Groups pages. Review the following descriptions.

Types of Users

Icon	Description
	Active Directory® Users
	To self register from a web browser, click **Register as a new user** at the login prompt. The computer you use to login to Toad Intelligence Central must be accessible to your Windows® domain. This option is visible only if your local configuration allows self registration via a web browser.
	To register new users post login, select **Administration | Users | Add User | Add Active Directory User**. Your local configuration may require login with an Administrator role to add Active Directory users.
	Intelligence Central Users
	To self register from a web browser, click **Register as a new user** at the login prompt. Deselect the option to **Use my Active Directory details**. Fill in your user details. The options in this procedure may not be visible or selectable, depending on your local configuration. Your local configuration may not allow self registration from a web browser or registration of new Intelligence Central users.
	Following login to Intelligence Central from a web browser, to add users, select **Administration | Users | Add User | Create Intelligence Central user**. The availability of these steps depends on your Intelligence Central configuration.

Types of Groups

Icon	Description
	Active Directory Groups
	Following login to Intelligence Central from a web browser, to add a group from Active Directory, select **Administration | Groups | Add Group | Add Active Directory Group**.
	Your Intelligence Central configuration may require login with an Administrator role to add Active Directory groups.
	Intelligence Central Groups
	Any logged in user can create an Intelligence Central group.

View and Edit Users

In Toad Intelligence Central, new user accounts are created using one or both of the following methods:

- Add (import) accounts from Active Directory®
- Create accounts within Intelligence Central

Use the following icons to identify the source of a user account.

Icon	Description
	Active Directory® user (imported from Active Directory). This type of account uses Windows® credentials.
	Intelligence Central user (created on Toad Intelligence Central). This type of user account exists only on Toad Intelligence Central and uses Intelligence Central credentials.

View User Information

You can view a list of users, as well as user details (including objects associated with a user), on the **Users** page of the Web interface.

To view user information

1. In the Web interface, click **Administration \| Users** to display the list of users on Toad Intelligence Central.
2. Select a user to view details in the right pane. The following useful information is available:

   - Account details, email address, and user role.
   - Groups in which the user is a member.
   - Objects shared with the user.
   - Objects published by the user.

i | **TIP:** You can see only the objects shared with you. When viewing a user other than yourself, this user may have objects shared with them that you cannot see.

User Roles

Each user is granted a role. By default, a new user is granted the Standard role. A user with the Administrator role can change the default role for new users and can change the role of any existing user. See the *Toad Intelligence Central Deployment Guide* for more information.

Review the following role descriptions.

- **Administrator**—Users with an Administrator role are granted all privileges in the administration of users, groups and objects. They are also granted some server and licensing privileges. The role of the Administrator (root user) cannot be changed.

- **Power User**—Power users have all the privileges of the Standard user. In addition, Power users can force consumers to take a shared object that is published or managed by the Power user.

- **Standard User**—All new users are granted the Standard role, by default.

Edit Your Account / Change Your Password

If your account is an Intelligence Central user account, you can edit some account details (profile) or change your password.

If your account was created by importing it from Active Directory, you cannot change the password through Toad Intelligence Central. However, Intelligence Central can be configured to synchronize with Active Directory. See the *Toad Intelligence Central Deployment Guide* for more information about synchronization.

To edit your Intelligence Central user details

1. In the Web interface, click **Administration | Users** to display the list the users on Toad Intelligence Central.

2. Select your user name.

3. Click **Edit** in the Details pane to change your full name or email address.

4. Click **Reset Password** to change your Intelligence Central account password.

Change Your Email Subscriptions

Intelligence Central can send activity reports and error alerts to users for objects they own or manage. Individual users can subscribe/unsubscribe to these email notifications through their user account details.

To modify your email subscriptions

1. In the Web interface, click **Administration | Users**.

2. Select your user name.

3. Click **Change subscription** and then select which email notifications to receive. See the *Toad Intelligence Central Deployment Guide* for more information about Email Notifications.

View and Edit Groups

In Toad Intelligence Central, new groups are created using one or both of the following methods:

- Add (import) groups from Active Directory®
- Create groups within Intelligence Central

Use the following icons to identify the source of a group.

Group	Description
	Active Directory group (imported from Active Directory).
	Intelligence Central group (created on Toad Intelligence Central). Groups with this icon exist only on Toad Intelligence Central.

Note that on Toad Intelligence Central, groups are a flat structure containing any number of users. A group on Toad Intelligence Central cannot contain sub-groups or nested groups.

View Group Information

You can view a list of groups, as well as group details, on the Groups page of the Web interface.

To view group information

1. In the Web interface, click **Administration | Groups** to display the list of groups on Toad Intelligence Central.

2. Select a group to display details in the right pane. The following useful information is displayed.

   - The group's source: local or Active Directory
   - A list of members in the group
   - Details of each member in the group: username, full name, and email address
   - A list of objects shared with the group

Edit an Intelligence Central Group

You can modify the list of members of an Intelligence Central group you own. You can remove an Intelligence Central group you own.

You cannot use Intelligence Central to modify a group imported from Active Directory. However, Intelligence Central can be configured to synchronize with Active Directory. See the *Toad Intelligence Central Deployment Guide* for more information about synchronization.

Administrator login is required to remove Active Directory groups.

To edit an Intelligence Central group

1. In the Web interface, click **Administration | Groups** to display the list the groups on Toad Intelligence Central.

2. Select a group.

3. Click **Edit** in the Details pane to modify the list of members in the group.

4. Click **Remove Group** to remove the group from Intelligence Central.

   Share and Manage rights assigned to the group are removed with the group. The ability of individual members of the group to see/manage objects might be affected and is dependent on other rights assigned to them. A user is given the highest level of rights assigned to them, either as an individual or as a member of a group.

Add Active Directory Users and Groups

Users with certain privileges can add new users and groups to Toad Intelligence Central by importing users/groups from Active Directory®. Which type of user (role) is allowed to add new users is dependent on how Intelligence Central is configured. See the *Toad Intelligence Central Deployment Guide* for more information.

To add Active Directory User or Group using the Web interface

1. Use a web browser to log in to Intelligence Central. For more information, see Open the Web Console on page 10.

2. Click **Administration** and then select either **Users** or **Groups**.

3. Then select **Add User | Add Active Directory User** or **Add Group | Add Active Directory Group**.

   - If the Authenticate to Active Directory dialog opens, enter the credentials for your Active Directory account (including the domain name) in order to access a list of domains and users. See Authenticate to Active Directory for more information.

4. In the Add Users and Groups from Active Directory dialog, select the users/groups to add to Intelligence Central. See Add from Active Directory for more information.

Requirements

1. The Toad Intelligence Central server host must be in a valid Windows® domain.

2. If the Windows domain of the Toad Intelligence Central host and the Windows domain of the user are different then a two-way trust relationship must exist between the Windows domains.

Known issues and Limitations

Users and groups imported from Active Directory are given the same name in Intelligence Central.

Review the following known issues and limitations.

Issue	More information
Duplicate names	If an Active Directory name already exists on Toad Intelligence Central then that Active Directory name is not imported. You will be notified of any users and groups who cannot be imported.
Long Active Directory usernames	For Active Directory usernames longer than 16 characters, the Intelligence Central username will be a truncated form of the Active Directory name. If the Active Directory username has a numeric suffix then up to three digits of that numeric suffix is preserved. For example, Active Directory username very_long_username12 transforms to Intelligence Central username very_long_user12.
Active Directory names containing characters not allowed by Toad Intelligence Central	Active Directory names containing the following characters cannot be imported to Intelligence Central. You will be notified of any users and groups who cannot be imported. • Forward slash (/) • Backward slash (\) • Left square bracket ([) • Right square bracket (]) • Colon (:) • Semicolon (;) • Vertical bar (|) • Equal sign (=) • Plus sign (+) • Asterisk (*) • Question mark (?) • Left angle bracket (<) • Right angle bracket (>) • Double quote (") • At symbol (@) • Comma (,)
Active Directory supports sub groups (groups within groups). Intelligence Central does not.	When importing an Active Directory group with sub groups the sub groups and users in sub groups are not imported to Intelligence Central.

Authenticate to Active Directory

Use the Authenticate to Active Directory dialog to enter your Active Directory credentials in order to access a list of domains and users when attempting to add Active Directory users (or groups) to Intelligence Central.

To authenticate to Active Directory

1. In the Authenticate dialog, enter the following information:

Field	Description
Domain	A domain in the Active Directory forest.
Username	Your username to that domain.
Password	Your password to that domain.

2. **Remember these credentials on server for future Active Directory access and synchronization**—Select this option to instruct Intelligence Central to do the following:

   - Automatically and regularly synchronize imported Active Directory users and groups.

   - Cache Active Directory user and group data on Toad Intelligence Central. This has the potential to improve performance of Toad Intelligence Central when looking up Active Directory users and groups.

   If you do not select this option, the list of imported users and groups might not be kept in sync with Active Directory.

3. **Schedule AD synchronization.** If you selected **Remember these credentials...**, you can schedule the Active Directory synchronization. Enter the scheduling details in the fields provided. After scheduling a synchronization, the scheduling information and status are displayed in **Administration | Server | Settings**.

Add from Active Directory

This dialog is used to add users and groups from Active Directory® to Toad Intelligence Central.

To add users/groups from Active Directory

1. In the Add Users/Groups from Active Directory dialog, select a domain from the drop-down list. Intelligence Central retrieves the list of users in that domain.

2. You can filter the list by entering a partial text string in the text box.

3. To refresh the list, click **Refresh**. The refresh option is available only for domains that are selected for synchronization in Intelligence Central.

   i | **NOTE:** This process could take several minutes, depending on the size of the domain.

4. If the domain you want to view is not listed, click **Add Domain**.

   - Enter the name of the domain to add. Then enter credentials for an account in that domain. Click **Authenticate**. See Authenticate to Active Directory for more information.

5. Select available Active Directory users/groups and move them to the **users/groups to be added** list.

i | **TIPS:**

- Use SHIFT to select multiple users/groups in sequence. Use CTRL to select multiple users/groups not in sequence.

- The number of Active Directory users displayed is limited to 10,000. For domains containing more than 10,000 users, a message informs the user that the list is not displayed in full. To find users not displayed, use the search box.

- Enter a name or partial text string in the search box to filter the list of users and groups. Intelligence Central returns users that contain matching text in the username or full name fields. Clear the search box to clear this filter.

6. Click **Add Users** to add the users/groups to Intelligence Central.

   When a group is added, an Active Directory user account is created on Toad Intelligence Central for anyone in the group who does not already have an account on Toad Intelligence Central (in addition to the group account).

7. A Success message displays if the users were successfully added.

Create Intelligence Central Groups

Intelligence Central allows you to create a group from existing users. You can include user accounts from both Active Directory and Intelligence Central in one group. Intelligence Central groups are identified by the following icon: .

The user creating the group is the owner of the group. The owner and users with an Administrator role are able to remove the group and edit group properties. If the owner is deleted, then the Administrator (root) becomes the group owner.

i | NOTE: Intelligence Central groups use a flat structure and contain any number of users. A group cannot contain sub-groups or nested groups.

To create an Intelligence Central group

1. Using a web browser, select **Administration | Groups | Add Group | Create Intelligence Central Group**.

2. In the Create Group dialog, enter a name and add users. Review the following for additional information.

Field	Description
Group name	Give the group a name. A group name can be up to 128 characters: letters, numbers, space ( ), hyphen (-), underscore (_), period (.). The name is case insensitive.
Description	(Optional) Enter a description.

Field	Description
Group members	Any enabled user on Toad Intelligence Central can potentially be a group member. Select the Intelligence Central users to add to the group. Move these users to the **Users in this group** list. You (the user creating the group) are added to this list by default and can be removed. The number in brackets following **Group Members** indicates the number of users in the group. If the number of users on Toad Intelligence Central is extensive then you may like to filter the list of potential users. You can do this by typing text in the *Start typing to find available users* box. Remove the text to remove the filter.

Support Bundle

A support bundle can assist in the diagnosis of issues such as data connectivity and query performance. To help troubleshoot these issues, you might want to generate a support bundle to send to Quest Software Technical Support. See the following for more information:

- Create a Support Bundle

Create a Support Bundle

You can create a support bundle and send it to Quest Software Support. The support bundle contains information about the status, logs, and configuration of Toad Intelligence Central and the Toad Intelligence Central Web server. The support bundle provides information that is used to help troubleshoot problems.

To generate and send a support bundle

1. In the Web interface, click 🛈 to open the **About** box.

2. In the About box, click **Contact** to open the Quest Software contact details tab.

3. Then click **Generate support bundle**.

4. A file of type ZIP will be created and then downloaded as per your web-browser settings. You can save this zip file and then attach it to an email to Quest Software Support.

About Us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Contact Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical Support Resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product