Toad® Intelligence Central 4.3

Deployment 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

The Deployment Guide is intended for Administrators and provides information about how to install Toad Intelligence Central and how to configure server options. It also provides information about managing users and objects, as well as other Administrator activities.

This guide describes procedures that can be performed by users with the Administrator role, including the Administrator (root) user. Non-Administrators should refer to the *Toad Intelligence Central Quick Start Guide* for functionality available only to non-Administrator roles.

Install Toad Intelligence Central

The components of Toad Intelligence Central are as follows.

Component	Description
Intelligence Central server	The Toad Intelligence Central server stores objects published to Toad Intelligence Central and account information for users of Intelligence Central. Follow the steps to Install the Intelligence Central server. See also Install Toad Data Point and ODBC Drivers.
Web Server	The Toad Intelligence Central Web Server is used for administrative and general user access. It also hosts Web-based applications for collaborative Toad products. The Toad Intelligence Central Web Server is installed on the same computer as the Intelligence Central server. For more information, see Install the Web Server on page 9.

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.

Install the Intelligence Central server

Use the Toad Intelligence Central Server Installer.

i | **TIP:** If installing on a virtual machine, see Use Virtual Disk (VMDK) in Virtual Machine Installation for additional information.

To install the Toad Intelligence Central server

1. Run the Toad Intelligence Central Server Installer.

2. Select to install **Toad Intelligence Central**.

3. Agree to the license agreement.

4. Provide details if connections to data sources outside your organization need to go through a proxy server.

Field	Description
Proxy host address	Type the DNS or IP address of the proxy server within your organization. HTTP and HTTPS secure proxy servers are supported.
Proxy port number	Type the port on which the proxy server operates. The standard proxy port number is 8080. Sometimes port 80 is used. Less commonly an entirely different port may be used.

5. Make a note of the port numbers.

> **i** **NOTE:** These port numbers can be modified during installation to resolve port conflicts on the target host. However, all three port numbers are reserved for Toad with the Internet Assigned Numbers Authority and the default values should be valid for most installations.

Field	Description	Default
Intelligence Central server Port number	This port can be used by third party applications to connect to Toad Intelligence Central. All other applications should use the *Application server port number* to connect to Toad Intelligence Central.	3566
Internal port number	This is an internal port used by Toad Intelligence Central and should only be changed in the case of port number conflicts.	2166
Application server port number	Client applications use this port to connect to Toad Intelligence Central. Make sure you note down this port number. You will be required to enter this port number to connect Toad Data Point to Toad Intelligence Central.	8066

6. Create a password to connect to Toad Intelligence Central. This is the administrator (root) password to the Intelligence Central server.

7. Accept or change the installation folder (C:\Program Files\Quest Software\Toad Intelligence Central).

    If you change the installation folder be sure to document the new location. This folder is referred to in server maintenance.

8. Accept or change the Data Files Folder (C:\ProgramData\Quest Software\Toad Intelligence Central).

> **i** **TIP:** Ensure this folder has room to grow. All Toad Intelligence Central data will be stored in the ProgramData\Quest Software\Toad Intelligence Central\ folder and its subfolders. This folder will potentially grow quite large if lots of users publish lots of objects and take snapshots. You may choose to change the default folder location. For example, you may choose to direct the data files folder to a separate drive. If you do change the location of the data files folder be sure to document this as the data files folder is referred to in server maintenance. See Toad Intelligence Central Data Folder for more information.

9. Help improve Toad Intelligence Central. Optionally, select to provide anonymous user experience feedback. Refer also to the Privacy Statement.

> **i** **NOTE:** Beginning with Toad Intelligence Central 4.3, the Admin Console is no longer required and is not included in the installation. If an earlier version of the Admin Console exists, it is recommended that you uninstall it.

Upon successful installation, the Intelligence Central server will run as three services that start automatically when Windows® starts. For more information, see Toad Intelligence Central services on page 48.

Install Toad Data Point and ODBC Drivers

When Toad Data Point is used to publish objects and Automation scripts to Toad Intelligence Central, ensure the following requirement is met.

Install Toad Data Point on the same host computer as Toad Intelligence Central.

Beginning with Intelligence Central 3.0, if the Toad Intelligence Central Server Installer is used, Toad Data Point and applicable ODBC drivers are automatically installed immediately following the Intelligence Central installation. This ensures compatibility of features and drivers for objects published through Toad Data Point and is required in order for Toad Data Point Automation Scripts to execute on Toad Intelligence Central.

> **i** | **NOTE:** Following installation of Toad Data Point on the Toad Intelligence Central host computer, start the Toad Data Point application and add your Toad Data Point Professional license key. Adding your license key to Toad Data Point is required, however Toad Data Point installed via the Toad Intelligence Central installer is not counted in the Toad Data Point license count.

In addition, if Toad Data Point is used to publish Automation scripts to Intelligence Central, ensure the following requirements are met (if applicable).

Does the Toad Intelligence Central server have access to an email SMTP port?

If an 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.

Is Microsoft® Excel® installed on the Toad Intelligence Central host computer?

If an Automation Script scheduled to execute on the Toad Intelligence Central server includes an instruction to run a macro in an Excel spreadsheet, then Microsoft Excel must be installed on the Toad Intelligence Central host computer. Other Automation script uses of Excel do not have this requirement. For example, Excel is not required to execute an Automation script that *exports* to Excel.

Install the Web Server

Use the Toad Intelligence Central installer to install the Web Server on the same computer as the Intelligence Central server.

IIS Express	The Web Server requires Microsoft® IIS Express be installed. Installation of IIS Express is included in the installer and will run only if required and by your agreement.
	You can run the Web Server on Microsoft IIS, if necessary. See Run Web Server on Microsoft IIS for important configuration instructions.

Web Server Port Number	Port 80 is reserved for the web port. During installation, you can change this if required.
	i | **NOTE:**
	• The installer will let you know if there is a conflict in using the default port 80.
	• It is not advisable to install other web servers on the Toad Intelligence Central server host.
	• A port number other than 80 must be included in the web browser address as per **http://hostName:port/**.
	• Ensure the port is open for TCP inbound connection. Ensure the Windows® firewall and any other firewalls affecting the Toad Intelligence Central server host allow access to the Web Server.

Run Web Server on Microsoft IIS

If necessary, you can run the Web Server on Microsoft IIS instead of Microsoft IIS Express.

To run the Web Server on IIS

1. Allow the Toad Intelligence Central installer to install IIS Express along with the Web Server.

2. After successful installation, stop the Toad Web Server (Toad Intelligence Central) and change its Startup type to *Disabled*.

    a. Go to **Control Panel | Administrative Tools | Services** to open the services.msc dialog.

    b. Right-click Toad Web Server and select **Stop**.

    c. Right-click Toad Web Server and select **Properties** to open the Properties dialog. In the **Startup type** field, select **Disabled**.

3. Now you can deploy the Toad Web Server to IIS. The site content path is the path to the Toad Intelligence Central Web Server installation folder, for example:

    C:\Program Files\Quest Software\Toad Intelligence Central Web Server

4. You must include the following Role Services for the Web Server (IIS) Role:

    • Web Server | Common HTTP Features

        • Default Document

        • HTTP Errors

        • Static Content

    • Web Server | Application Development

        • .NET Extensibility 4.5

        • ASP.NET 4.5

        • ISAPI Extensions

        • ISAPI Filters

5. When finished, restart the Toad Web Server.

Authenticated proxy server connections

The following is required if the host on which the Toad Intelligence Central server is installed connects to the Internet via a proxy server and the proxy server is authenticated. Execute this SQL statement after the Toad Intelligence Central server is installed.

INSERT INTO hub_information_schema.hub_proxies VALUES ('*http*', '*http://proxyAddress:proxyPort/*', '*username*', '*password*');

Variable	Value
http	The protocol under which the proxy server operates. The protocol may be http or https or both http and https. If both http and https are used then execute the SQL statement twice, once per protocol.
proxyAddress	The IP address of the proxy server.
proxyPort	The port on which the proxy server operates.
username	The username to the proxy server.
password	The password to the proxy server.

Use Virtual Disk (VMDK) in Virtual Machine Installation

If you plan to install Toad Intelligence Central in a virtual machine (VM) environment, and you require more space than is available, you might choose to utilize a virtual disk (VMDK) to store the Toad Intelligence Central Data Files Folder.

Create the virtual disk and mount a drive on the VM to the virtual disk (if remote) prior to installing Toad Intelligence Central. Then during installation, specify the virtual disk as the location for the Data Files Folder.

The following procedure describes how to add a virtual disk for a VMware® virtual machine.

Add new virtual disk (VMDK) to VMware VM

1. Open the VMware virtual machine.

2. Select the virtual machine and select **VM | Settings**.

3. Select the **Hardware** tab.

4. Click **Add**.

5. In the Add Hardware Wizard, select **Hard Disk** and click **Next**.

6. On the Select a Disk page, select **Create a new virtual disk**. Click **Next**.

7. On the Select a Disk Type page, use the defaults. Click **Next**.

8. On the Specify Disk Capacity page, enter a value for the disk size. Select **Store virtual disk as a single file**. Click **Next**.

9. On the Specify Disk File page, specify a location for the virtual disk file. Click **Browse**.

    a. Specify the remote server address, if creating the disk on a remote server.

    b. Enter a file name.

    c. Click **Open**.

10. After adding the virtual disk, you must initialize it.

    a. In the VMware virtual machine, go to **Computer Management | Storage | Disk Management**.

    b. Initialize the uninitialized virtual disk.

    c. After it is initialized, right-click the disk and select **New Simple Volume**.

11. The new virtual disk should now be listed under Drives on the computer where it is located.

Access Toad Intelligence Central

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

- **Web Interface**—Log in to the Web Server using a Web browser
- **Toad Applications**—A Toad application, such as Toad Data Point or Toad for Oracle
- **Third-Party Tool**—A third-party tool, such as Tableau or a MySQL command line interface

i | **NOTE:** Toad Intelligence Central is a server that runs as three services that start automatically when Windows starts. For more information, see Toad Intelligence Central services on page 48.

Method	Description
Web Interface	See Log In From a Web Browser for more information about accessing Intelligence Central through the Web interface.
	The Web interface (Web Server) provides Standard users with the ability to view and perform limited operations on objects published to Intelligence Central from other Toad applications. To use the Web interface, the Web server must be installed on the same computer as Intelligence Central. The *Toad Intelligence Central Quick Start Guide* provides the Standard user with information on how to use the Web interface.
	The Web interface 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.
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. Toad for Oracle users can publish Automation apps, files, and other resources created in Toad for Oracle. For these users, their primary method to view, access, manage, and edit Intelligence Central objects is through their Toad application.
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.

Log In From a Web Browser

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 log in to Toad Intelligence Central using a web browser

- In a Web browser, 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. To login to Toad Intelligence Central as the Administrator (root), in the username field type **root**. In the password field type your Administrator password. The initial Administrator password is as per the password you entered when you installed the Intelligence Central server. 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 To set local configuration, see Configure New User Registration.

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.

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.
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.

Application	Description
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

4

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 Data Connectivity license is required to use Toad Intelligence Central with Data Connectivity. Any Toad Intelligence Central license from a prior release can serve as a Data Connectivity license for this release.

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.

After licensing Toad Intelligence Central, you can elect to provide anonymous user feedback to help influence the design of future releases. See Enable User Experience Feedback to learn how to easily enable this feature.

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.

To enable/disable self-registration, specify who can add new users, and configure other registration parameters, see Configure New User Registration.

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, see Add Active Directory Users and Groups. Your local configuration may require login with an Administrator role to add Active Directory users. See Configure New User Registration.
	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**. See Add Active Directory Users and Groups. Your Intelligence Central configuration may require login with an Administrator role to add Active Directory groups. See Configure New User Registration.
	Intelligence Central Groups Any logged in user can create an Intelligence Central group. For more information, see Create Intelligence Central Groups on page 22.

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 Configure New User Registration 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 Log In From a Web Browser on page 14.

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

- 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.

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. For more information, see Synchronize Active Directory on page 31.
- 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.

To view a list of domains configured for Active Directory synchronization, in the Web interface go to **Administration | Server | Users**. Log in with Administrator role is required to view this information. You can also change the credentials used for synchronization from this page. See Synchronize Active Directory for more information.

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. See Synchronize Active Directory for more information.

   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. See User Roles for more information. 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.

6

Manage Users and Groups

The Toad Intelligence Central Administrator (root) user account is created during the installation of the Toad Intelligence Central server. This Administrator user account has access to all administrative privileges. In the Web interface, other users can be granted an Administrator role with the same privileges for managing users and groups. See User Roles for more information.

View User and Group Information

Use a web browser to view users and groups on Toad Intelligence Central. Users and groups are listed alphabetically by username. Disabled users are listed in italics. Properties of a user include the user's name and email address.

To view user/group information

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

2. Select a user or group to display details in the right pane.

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

Users	Groups	Description
		Active Directory® users and groups.
		Log in to a web browser to view the properties of Active Directory users and groups. Use Active Directory to edit the properties of Active Directory users and groups. Users with an Administrator role (User Roles) manage that Intelligence Central is synchronized with Active Directory user and group information. For more information, see Synchronize Active Directory on page 31.
		Intelligence Central users and groups.
		The properties of an Intelligence Central user can be edited by the user themselves and by any user with an Administrator role (User Roles). The properties of an Intelligence Central group can be edited by the owner (creator) of the group and by any user with an Administrator role.

Following login from a web browser, click **Administration | Users** or **Administration | Groups**. Select a user or group to show properties.

i **TIP:** Show / hide Active Directory users and Intelligence Central users using the on screen options. Search for users using the search bar.

Edit User and Group Information

Use a web browser to edit user and group information on Toad Intelligence Central.

Reset User Password

Users	Description
	The Toad Intelligence Central Administrator cannot reset the password for Active Directory users. The user should follow the standard procedure in their Active Directory environment to reset their Active Directory password.
	Users with an Administrator role (User Roles) can reset the password for Intelligence Central users (authentication by Intelligence Central). • A new password is randomly generated for the user. • The Administrator can see the password. • The Administrator can copy the password to the clipboard. • If an email client is installed, the Administrator can email the password to the user. Following log in from a web browser, select **Administration | Users** to list the users of Toad Intelligence Central. Select the user and in the **Details** pane click **Reset Password**.
	The Administrator (root) password cannot be reset. If the Administrator password is lost then the procedure is to uninstall and reinstall the Intelligence Central server. During reinstall the Administrator is prompted to enter their password (they can enter a new password).

Change a User's Role

Users with an Administrator role (User Roles) can change a user's role. Following log in from a web browser, click **Administration \| Users** to list the users of Toad Intelligence Central. Select the user whose role you want to change so their details are visible on screen. In the **Details** pane click **Edit** to change their role.

For more information on each of the user roles, see User Roles.

i | **NOTE:** The Administrator (root) role cannot be changed.

Change User's Email Subscriptions

Intelligence Central can send email notifications to users to provide information about object activities, as well as error reports. Users can select which types of email notifications they want to receive. See Email Notifications for more information.

To change a user's email subscriptions

1. Log in using a Web browser and select **Administration | Users**.

2. Select a user name.

3. Click **Change subscription** and then select which email notifications this user should receive.

Disable/Enable a User

Users with an Administrator role (User Roles) can disable users from Intelligence Central. Disabled users cannot login to Toad Intelligence Central until an Administrator chooses to enable them. Objects owned by the disabled user remain on Toad Intelligence Central and can be used by users with rights to those objects.

i | **NOTE:**

- The Administrator (root) cannot be disabled.

- The Administrator cannot disable a user while that user is connected to Toad Intelligence Central.

Following log in from a web browser click **Administration | Users** to list the users of Toad Intelligence Central. Select the user to disable so their details are visible on screen and click **Disable User**.

Enable a Disabled User

Users with an Administrator role (User Roles) can enable disabled users. When the user is enabled all their data (objects and authentication, sharing and manage rights) are as before.

Users	Password when enabled
👤	When the Active Directory user is enabled their password is as per their current Active Directory password.
👤	When the Intelligence Central user is enabled their password is randomly generated. The Administrator can see the password. It is up to the Administrator to notify the user of their new password. The Administrator can copy the password to the clipboard. If an email client is installed, the Administrator can email the password to the user.

Following log in from a web browser click **Administration | Users** to list the users of Toad Intelligence Central. Select the user so their details are visible on screen and click **Enable User**.

Remove a User

Users with an Administrator role (User Roles) can remove users from Intelligence Central.

i | **NOTE:**

- The Administrator (root) cannot be removed.

- The Administrator cannot remove a user while that user is connected to Toad Intelligence Central.

- When the user is removed their objects are also removed. Other Intelligence Central users who may have had access rights to those objects will no longer be able to access those objects.

Following log in from a web browser click **Administration | Users** to list the users of Toad Intelligence Central. Select the user to remove so their details are visible on screen and click **Remove User**.

Remove a Group

Groups	Description
👥	Users with an Administrator role (User Roles) can remove Active Directory groups. Users in the group who are inactive on Toad Intelligence Central are automatically deleted when the group is deleted. Inactive users are users who have no published objects, no objects shared with them and are part of no other group.
👤	Intelligence Central groups can be removed by any user with an Administrator role or the owner (creator) of the group.

Following log in from a web browser click **Administration | Groups** to list the groups on Toad Intelligence Central. Select the group so the group details are visible on screen and click **Remove Group**.

i | NOTE: When the group is removed, Share and Manage rights assigned to the group are also removed. The ability for members of the group to see / manage objects may be affected dependent on the other rights assigned to them. A user is given the highest level of rights applied to them either individually or to the group(s) they are a member of.

User Roles

There are three user roles available in Toad Intelligence Central: Standard user, Power user, and Administrator. During installation of the Toad Intelligence Central server, the Toad Intelligence Central Administrator (root) user account is created. This account has access to all administrative privileges.

The root Administrator account (or any account with the Administrator role) can grant/edit the role for another user account. This can be done when creating a new account or when editing an existing account. See Users and Groups and Manage Users and Groups 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.

Privileges by Role

Review the following privileges for each role.

User Management Privileges

The following table lists the user management privileges that are provided by each role. See Manage Users and Groups for more information.

Privilege/Action	Administrator	Power user	Standard user
Add users. This privilege is configuration dependent. See Configure New User Registration.	Y	configuration dependent	configuration dependent
View users and groups	Y	Y	Y
Change a user's role to Administrator, Power user, or Standard user. See Manage Users and Groups.	Y	N	N
Change a user's email subscriptions. See Specify User Email Subscriptions.	Y	user's profile only	user's profile only
Disable/enable a user	Y	N	N
Remove a user	Y	N	N
Edit Intelligence Central users	any user	user's profile only	user's profile only
Reset the password of Intelligence Central users	any Intelligence Central user	user's password only	user's password only
Create Intelligence Central groups	Y	Y	Y
Edit/remove Intelligence Central group	any group	groups owned by user	groups owned by user
Remove an Active Directory group	Y	N	N
Synchronize Active Directory	Y	N	N

Object Management Privileges

The following table lists the object management privileges that are provided by each role.

Privilege/Action	Administrator	Power user	Standard user
Publish objects	Y	Y	Y
View objects on Home page and view object details	all objects	objects owned by or shared with the user	objects owned by or shared with the user

Privilege/Action	Administrator	Power user	Standard user
(View or snapshot) Display the text for the underlying query	Y	objects owned by or managed by the user	objects owned by or managed by the user
(Automation script) Display the detailed execution logs	Y	objects owned by or managed by the user	objects owned by or managed by the user
Edit an object, grant/revoke access rights to the object, lock the object, delete the object, rename the object	all objects	objects owned by or managed by the user	objects owned by or managed by the user
Move an object or folder	Y	N	N
Modify authentication key for an object	Y	objects owned by or managed by the user	objects owned by or managed by the user
(View or Automation script) Edit the default value for a variable	Y	objects owned by or managed by the user	objects owned by or managed by the user
(Automation script) Change script run account	Y	objects owned by or managed by the user	objects owned by or managed by the user
Force consumers to take a shared object published or managed by the user	Y	Y	N
Publish Toad for Oracle analysis results to Toad Intelligence Central	Y	Y	Y
Access Toad for Oracle analysis Web Modules	Y	Y	Y

Misc Privileges

Only a user with the Administrator role can view and access the Server page (**Administration | Server**) in the Web interface. The Server page contains the following miscellaneous features:

- Configure New User Registration

- Synchronize Active Directory

- Download the Download Audit Log

- Configure Enable User Experience Feedback

- Enable/disable email notifications on server. See Server-Level Configuration for Notifications.

- Enable/disable email notification for a user (subscribe/unsubscribe a user). See Server-Level Configuration for Notifications.

Privilege/Action	Administrator	Power user	Standard user
View/access **Administration	Server**	Y	N	N

Licensing Privileges

The following table lists the licensing privileges provided by each role. See License Toad Intelligence Central for more information.

Privilege/Action	Administrator	Power user	Standard user
View licenses	Y	Y	Y
Enter new licenses	Y	Y	Y
Delete licenses	Y	N	N

Configure New User Registration

The root Administrator account (or any account with the Administrator role) can place some restrictions on how new users are registered and how accounts are created in Intelligence Central.

Enable/Disable Add Users and Self-Registration

By default anyone can self-register and add users to Toad Intelligence Central. Any user with an Administrator role can disable self-registration.

To enable/disable add users and self-registration

1. Use a web browser to log in to Intelligence Central as a user with the Administrator role.
2. Select **Administration | Server | Users**.
3. In the **New User Registration** section, select one of the following options.

Only the Administrator can add users	Select this option to allow only users with an Administrator role to add users to Intelligence Central.
Anyone can self-register and add users	Select this option to allow anyone to self-register and add users. A pre-existing account on Toad Intelligence Central will not be required when self-registering.
	• **Allow browser self-registration**—Select this option to allow self-registration through the Intelligence Central Web interface (browser). This option is enabled by default. Depending on your security requirements, you may choose to disable this ability.

For more information about Administrator privileges, see User Roles.

Specify Default User Role

You can specify a default role for new accounts.

To specify default user role

1. Use a web browser to log in to Intelligence Central as a user with the Administrator role.

2. Select **Administration | Server | Users**.

3. In the **Default user role** field, select a role from the drop-down list.

Restrict Registration to Active Directory Users

You can require that new accounts use only Active Directory credentials.

To restrict new accounts to Active Directory users

1. Use a web browser to log in to Intelligence Central as a user with the Administrator role.

2. Select **Administration | Server | Users**.

3. Select **New users can register with Active Directory (Windows) credentials only**. When selected, only Active Directory users can be added to Toad Intelligence Central. No new Intelligence Central users can be added.

Synchronize Active Directory

When a domain in the Active Directory® forest is synchronized with Intelligence Central, changes to users and groups in the domain are replicated on Intelligence Central. Any user with an Administrator role (User Roles) can manage synchronizing Toad Intelligence Central with Active Directory.

Synchronize status

From a web browser login to Intelligence Central as a user with an Administrator role. Click **Administration | Server | Users**.

Table 1: Domains in the Active Directory forest synchronized with Toad Intelligence Central

Field / Action	Description
Domain	Show all domains in the Active Directory forest synchronized with Toad Intelligence Central.
Last synchronized	Show the time the domain was last synchronized with Toad Intelligence Central. If the last attempt was unsuccessful then the error is reported in red.
Edit	Click to Show / Change the username and password used to connect to the domain. This username / password pair is used to synchronize Toad Intelligence Central with Active Directory. The credentials are saved on Toad Intelligence Central.
Remove	Click to remove the domain from this list. The users and groups added from this domain will remain on Toad Intelligence Central, but will not be synchronized again. The Active Directory credentials saved on Toad Intelligence Central are removed.

Field / Action	Description
Synch Now	Click to synchronize Toad Intelligence Central with the domain now. Note that if a Synchronization operation is already in progress then Toad Intelligence Central must wait till that is finished before it can synchronize again.
Add Domain	Click to add a domain to this list. You will be prompted for credentials to Active Directory. These credentials will be used to synchronize Toad Intelligence Central with the domain.

Synchronize rules

Changes to users and groups in Active Directory are replicated on Intelligence Central according to the following rules.

Synchronization is scheduled for daily at 12:00 AM (Intelligence Central server time). The time of this automated synchronization schedule cannot be changed.

Table 2: Synchronization rules

Active Directory	Toad Intelligence Central
User details updated	Update the user details from Active Directory (name and email address).
User disabled	Disable the user in Intelligence Central
User deleted	Delete the user from Intelligence Central if the user is inactive. Inactive users have no published objects, no objects shared with them as an individual and are part of no other group. Otherwise, disable the user in Intelligence Central. This is to ensure that if the user owns any objects that they will be kept.
User renamed	Delete or disable the old user in Intelligence Central (as above). A new user account is not automatically created in Toad Intelligence Central.
User enabled	Enable the user in Intelligence Central.
Group details updated	Update the group details in Intelligence Central (name and description).
Group deleted	Remove the group from Intelligence Central. Users in the group who are inactive on Toad Intelligence Central are automatically deleted. Inactive users are users who have no published objects, no objects shared with them and are part of no other group.
Group membership updated (User added to the group)	Add the user to the group in Intelligence Central. Create a the new Intelligence Central user account if the user does not already have one.
Group membership updated (User removed from the group)	Remove the user from the group in Intelligence Central. Delete the user if the user is inactive. Inactive users have no published objects, no objects shared with them as an individual and are part of no other group.

Email Notifications

Intelligence Central can send activity reports and error alerts to users for objects they own or manage. A user with the Administrator role can receive an additional report—the Daily or Weekly Digest—that summarizes activities relevant to the Administrator role.

How to Configure Notifications

Email notification can be configured at three different levels.

- **Server level**—Enable/disable email service at the server. Only users with the Administrator role can perform this configuration. See Server-Level Configuration for Notifications.
- **User level**—Subscribe/unsubscribe an individual user to the email notification service. Only users with the Administrator role can perform this configuration. See Server-Level Configuration for Notifications.
- **Email notification level**—Select which email notifications each individual user receives. Users with the Administrator role can configure email notifications for other users. Each user can edit their own profile. See Specify User Email Subscriptions.

Types of Email Notifications

There are four types of email notifications.

- Personal Digest—Provides a summary of activity for the objects a user owns or manages.
- Error Alerts—Sent when an error occurs during script execution or snapshot refresh for objects a user owns or manages. Also available to Administrators.
- Daily Admin Digest—Provides a daily summary of activities relevant to the Administrator role. Available to Administrators only.
- Weekly Admin Digest—Provides a weekly summary of activities relevant to the Administrator role. Available to Administrators only.

Server-Level Configuration for Notifications

Before Intelligence Central can start sending email notifications, the email notifications service must be enabled on the Intelligence Central server. In addition, the SMTP mail server must be configured. Both of these actions can be performed by a user with the Administrator role.

A user with the Administrator role can also subscribe/unsubscribe individual users to the email notification service.

To enable notifications and configure the SMTP mail server

1. Select **Administration | Server | Notifications**.

2. Select *On* in the **Email notifications** field.

3. Click **Configure SMTP Mail Server**.

4. In the Configure SMTP Mail Server dialog, enter the mail server host name.

5. If your SMTP mail server supports TLS/SSL, select **Use TLS/SSL**. This will encrypt email communications between Intelligence Central and your SMTP mail server.

6. If the SMTP server requires authentication, select the check box and enter credentials.

7. **From address**—Enter an email address to use as the sender address in each email.

8. **Subject prefix**—Enter a prefix to use at the beginning of the Subject line of each email.

9. Click **Send Test Email** to test your email configuration.

10. Click **Save** to save your settings and close the dialog.

To subscribe/unsubscribe users

- To unsubscribe a user, select the user name in the **Subscribers** list (left pane) and click the right arrow to move the user to the **Unsubscribed** list (right pane).

- To resubscribe a user, select the user name in the **Unsubscribed** list and move the user to the **Subscribers** list.

Specify User Email Subscriptions

A user with the Administrator role can specify which types of email notifications each individual user can receive.

Any user can specify the email notification options for their own user account.

To change a user's email subscriptions

1. Log in using a Web browser and select **Administration | Users**.

2. Select a user name.

3. Click **Change subscription** and then select which email notifications this user should receive. See Email Notifications for a description of each notification type.

ℹ️ | **NOTE:** Email Notifications must be enabled on the Intelligence Central server before the Admin Digest can be sent. See Server-Level Configuration for Notifications for more information.

Misc Administrator Activities

In addition to the other server-related activities described elsewhere in this document, users with the Administrator role can also perform the following.

Download Audit Log

The Audit Log allows you to download a log of activity on Toad Intelligence Central for a specific time period.

The log is a simple spreadsheet and includes the following information:

- Time of event
- Type of event
- Event description
- Object name or database name, if applicable

To download the audit log

1. From a web browser, log in to Toad Intelligence Central as a user with an Administrator role. For more information about the Administrator role, see User Roles.
2. Click **Administration | Server | Logging**.
3. In the Audit Log section, select a time period.
4. Then click **Prepare Download**. This converts the log to a CSV file. The time to prepare the file for download depends on the time span selected and the usage volume during the time span.
5. Track the preparation of the download on the web browser display.
6. Intelligence Central displays a Success message when the object is ready to download. Click the link in the Success message to download the audit log. The location of the log file on download will be as per your web browser settings.

Enable User Experience Feedback

You can influence the design of future versions of Toad Intelligence Central and help us improve its quality, reliability and performance.

To enable/disable user experience feedback

1. From a web browser, log in to Toad Intelligence Central as a user with the Administrator role. For more information about the Administrator role, see User Roles.

2. Click **Administration | Server | Logging**.

3. Select or clear the **Provide anonymous user experience feedback to help improve Toad Intelligence Central** option.

Refer also to the Privacy Statement.

Manage Objects

Users with an Administrator role are automatically granted **Manage** privileges to all objects on Toad Intelligence Central. See User Roles for more information.

In addition to the following object-management activities, the Web interface provides object usage reports. See View and Download Reports for more information.

View Objects

In the Web interface, use the Home page to view the objects in Intelligence Central. You can also view a list of objects per user (or group) on the Users page (or Groups page).

Users can see only the objects that they own or that have been shared with them, with the exception of the Administrator. The Administrator can view all objects on Intelligence Central.

To view objects and object details

1. From a web browser, log in to Intelligence Central.

2. Click **Home** to show objects in their folder structure.

3. Enter a partial text string in the Search text box to filter objects.

4. Select an object to display details in the right pane.

5. To view objects associated with a user, go to **Administration | Users**. Select a user to display a list of objects shared with the user and a list of objects published by the user.

6. To view objects shared with a group, go to **Administration | Groups** and select a group.

View Objects by User or Group

When a user with an Administrator role generates a list of objects they see all objects on Toad Intelligence Central. When any other user generates a list of objects they see the objects for which they have **Share** or **Manage** rights. Another user may not see all the objects that the Administrator can see.

Show the objects owned by a particular user

From a web browser with log in to Intelligence Central, click **Administration | Users** and select the user. The objects owned by that user are listed in the **Published Objects** pane. Tabs show the number of objects that are **Private** (to that user) and **Shared** (with other Toad Intelligence Central users). Click the Private / Shared tabs to show / hide these objects.

Show the objects shared with a particular user

From a web browser with log in to Intelligence Central, click **Administration | Users** and select the user. The objects shared with that user are listed in the **Shared Objects** pane.

Show the objects shared with a particular group

From a web browser with log in to Intelligence Central, click **Administration | Groups** and select the group. Objects shared with that group are listed in the **Shared Objects** pane.

Move Objects and Folders

To move objects

On the Home page, you can drag-and-drop an object to move it to another folder. Only users with the Administrator role can move an object (unless the object is locked by another user).

Restrictions:

- You cannot move objects into or out of the *Common_Transformation_Repository*.
- You cannot sort or reorganize objects in a folder.
- You cannot move an object to a folder where the name exists.

To move folders

On the Home page, you can drag-and-drop a folder to move it. Only users with the Administrator role can move folders (unless 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.

Data Connectivity and Data 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. See License Toad Intelligence Central for more information.

ODBC Connectivity

When data is published from a remote data source by a Toad Data Point user, the connection information is stored on Intelligence Central. Intelligence Central uses ODBC connectivity to connect to relational database sources that have been defined by Toad Data Point.

ℹ | **NOTE:** To connect to data sources using ODBC connectivity, supporting ODBC drivers and necessary client files must be installed on the Toad Intelligence Central server host. See Install Toad Data Point and ODBC Drivers for more information.

User Access to Remote Data Source - Authentication

When a Toad Data Point user publishes a data object to Intelligence Central, the object is associated with a particular data source connection. This data source connection in Intelligence Central must have a login ID (or authentication key) to use when connecting to the remote data source. This ID / authentication key is created when the object is published and can be either shared or personal. A shared ID / authentication key can be used by any user when accessing the remote source. A personal ID / authentication key requires that each user log in using their own personal login credentials when accessing the remote source.

Users can provide login credentials through the Web interface (Web server) for an object that requires authentication.

1. From the **Home** page, select an object to display the Details pane.

2. In the **Details** pane, click the data source link in the **Source** field to open the Alter Authentication dialog.

   For an object with a shared key applied, only users with Manage privileges to the object can open the Alter Authentication dialog through the data source link. For other users, the data source link is disabled.

See Alter Authentication for more information.

Authentication

The ability of any user, including a user with an Administrator role, to download an object where data is sourced from a remote data source is dependent on the authentication granted to that user. The Administrator role is not automatically granted authentication to view data sourced directly from remote data sources.

The following table describes the origin of data and the authentication requirements for the data objects in Intelligence Central.

Icon	Object	Description
▦	Tables	Tables are tables of data mapped from data source mappable objects. The data is sourced direct from the data source. Authentication is required to view the contents of the object.
👓	Views	Views are saved SQL statements. When the SQL statement is executed, data is sourced direct from the data source.
		Authentication is required to view the result set if the object was published with a personal key. Authentication is not required if published with a shared key.
		Beginning with Intelligence Central 4.3, a view can have either a personal key or a shared key applied, but not both.
🖼	Snapshots	Snapshots are the result set of an executed SQL statement (View) or table. The data is stored on Toad Intelligence Central.
		Authentication is not required to view the result set, as snapshots are published with a shared key.
🔲	Mappable Objects	Mappable objects are data source objects that can be potentially mapped to tables. Authentication is required to list mappable objects and map tables.

Toad Data Point Automation Scripts

Prerequisites for Automation Script Execution

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 run a macro in an Excel spreadsheet, then Microsoft Excel must be installed on the Toad Intelligence Central host computer for the macro to successfully execute.

Change Account Used for Script Execution

Automation scripts execute in Intelligence Central under a user account. Users with the Administrator role can change the account under which a script executes.

1. From the **Home** page, select an Automation script to display the Details pane.

2. In the **Details** pane, click **Credentials** to open the Alter Credentials dialog. See Alter Automation Script Credentials for more information.

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.

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.

View and Download Reports

The Web server provides a Reports section which allows you to view and create reports about Intelligence Central object usage. The Reports landing page provides a dashboard-type view that displays top-level usage statistics. The Reports feature is designed mainly for Administrators, but all users can view and export usage reports.

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**.

Health Check Dashboard

You can run a health check on the Intelligence Central server to check for object integrity anomalies and other issues with data objects stored on the server.

Use the Health Check Dashboard page to run a health check, review the health check results, repair anomalies, and specify health check settings.

Users with the Administrator role can run a health check, repair objects, and specify settings.

To run a Health Check

1. In the Intelligence Central Web server, select **Administration | Server | Health Check Dashboard**.

2. In the Health Check Dashboard page, click **Run Health Check**.

3. After the Health Check process finishes, the Data Integrity tab displays the results of the Health Check.

   a. If an object is found to have an anomaly, it is listed along with the object details, a description of the impact to the user, and a description of the solution.

   b. Screen tips display more information. Place your cursor over the information icon, as well as the Impact and Solution descriptions, to display more information.

4. To repair an object, select the object and click **Repair**. You can select one object or multiple objects to repair. Select the check box beside a category to select all objects in that category.

5. If a repair is successful, the object is removed from the report. If a repair is unsuccessful, an error message is displayed.

To specify Health Check settings

1. In the Intelligence Central Web server, select **Administration | Server | Health Check Dashboard**.

2. Select the **Settings** tab. Review the following:

3. **Auto run health check weekly**—Enable this option to instruct Intelligence Central to automatically run a health check once per week (2 am on Sunday).

4. **Send out email to Admin if any anomalies found after auto run**— If enabled, an email is sent to users with the Administrator role after each automatic health check. The email contains a link to the Health Check Dashboard page to allow users to open the dashboard and review the latest report.

   • Before Intelligence Central can send email notifications, the SMTP mail server must be configured. See Server-Level Configuration for Notifications for more information.

12

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.

Server Maintenance

Toad Intelligence Central services

The Toad Intelligence Central server runs as three Windows® services that start automatically when the server host starts.

The Toad Intelligence Central server services are:

- Toad Application Server
- Toad Database Server
- Toad Optimization Server

The Toad Intelligence Central Web Server service is:

- Toad Web Server

Stop the Toad Intelligence Central server

To stop the Toad Intelligence Central server (from the server host):

1. Open **Windows® Control Panel**.
2. Click **Administrative Tools | Services**.
3. Stop ALL of the following services. Right click on each service and select **Stop**.

   - Toad Application Server
   - Toad Database Server
   - Toad Optimization Server

i | **NOTE:** If an Automation Script is executing when services are stopped then execution of that script stops when the Toad Intelligence Central server is stopped.

Restart the Toad Intelligence Central server

After the Toad Intelligence Central server has stopped (Stop the Toad Intelligence Central server), follow these instructions to restart the Toad Intelligence Central server.

On the server host:

1. Open **Windows® Control Panel**.

2. Click **Administrative Tools | Services**.

3. Start ALL of the following services. Right click on each service and select **Start**.

    - Toad Application Server

    - Toad Database Server

    - Toad Optimization Server

Toad Intelligence Central Data Folder

ProgramData\Quest Software\Toad Intelligence Central\ stores all user information, data source connection information and mappings for the Toad Intelligence Central server. This folder will potentially grow quite large if there are lots of snapshots and published objects.

The location of this folder was defined when the Toad Intelligence Central server was installed. See Install the Intelligence Central server for more information.

The default location for the folder is **C:\ProgramData\Quest Software\Toad Intelligence Central** however the actual location may be quite different. For instance, due to the nature of this folder a decision may have been made to locate this folder on a separate drive.

> **i**   **NOTE:** If you upgraded from Intelligence Central 3.2 (or earlier), the location of this folder might be ProgramData\Dell\Toad Intelligence Central.

If installing in a virtual machine environment, see Use Virtual Disk (VMDK) in Virtual Machine Installation for information about locating this folder on a virtual disk.

The folder has three sub folders. When making a copy of this folder ensure you copy all content (files and subfolders):

- ProgramData\Quest Software\Toad Intelligence Central\appserver

- ProgramData\Quest Software\Toad Intelligence Central\conf

- ProgramData\Quest Software\Toad Intelligence Central\data

> **i**   **NOTE:** The C:\ProgramData folder is hidden by default. To see the folder, from Windows® Explorer click **Tools | Folder Options**, from the Folder Options dialog click **View | Show hidden files, folders, and drives**.

Backup the Toad Intelligence Central server

All user information, data source connection information and mappings for the Toad Intelligence Central server are stored in ProgramData\Quest Software\Toad Intelligence Central\. A backup of the Toad Intelligence Central server is a backup of this folder including sub folders.

i | **NOTE:** If you upgraded from Intelligence Central 3.2 (or earlier), the location of this folder might be ProgramData\Dell\Toad Intelligence Central.

The Toad Intelligence Central server must be stopped while the backup is made. You may want to ensure the time of the backup does not conflict with tasks Toad Intelligence Central has been scheduled to do, such as refreshing a snapshot or executing a Toad Data Point automation script.

If a backup is taken while Toad Intelligence Central services are still running the backup will be corrupted; **you will not be able to restore or recover from the corrupted backup**.

If your standard backup procedure involves taking an image or full backup of the hard disk then use Windows® Scheduler as documented in this section to schedule the Toad Intelligence Central backup.

Please make a note of the Toad Intelligence Central version when you create the backup. The backup can only be restored to this version of Toad Intelligence Central. For example, a backup from Toad Intelligence Central 3.3 can only be restored to Toad Intelligence Central 3.3. It cannot be restored to Toad Intelligence Central 4.3. If you need to restore the backup data, refer to Restore Toad Intelligence Central.

Manual backup

These steps illustrate what is involved in the backup process. Ensure Toad Intelligence Central server services have stopped. Restart Toad Intelligence Central server services once backup is complete.

1. Stop the Toad Intelligence Central server
2. Copy the entire ProgramData\Quest Software\Toad Intelligence Central\ folder including subfolders to an appropriate back up media.
3. Restart the Toad Intelligence Central server

Executable backup

Toad Intelligence Central is distributed with an executable file that automatically follows the steps of the manual backup.

From the Windows Server® that hosts the Toad Intelligence Central server

1. Log in as Administrator.
2. Open a command prompt.
3. Change directory to the Toad Intelligence Central server bin folder (by default Program Files\Quest Software\Toad Intelligence Central\bin).
4. Execute the backup.bat command. For example: **backup.bat "c:\backup folder"**

Optionally, enclose the target folder for the backup in quotes. In the example the target folder is "c:\backup folder". If the target folder is not specified then the backup will be saved to: ProgramData\Quest Software\Toad Intelligence Central\backup

Verification:

- Open the backup folder to ensure Toad Intelligence Central data folders have been backed up. (See Toad Intelligence Central Data Folder)
- Verify Toad Intelligence Central server services restart once the backup is complete.

Scheduled backup

Use Windows Scheduler to schedule a local backup of the data files. Follow this procedure if your standard backup procedure involves taking an image or full backup of the hard disk.

1. Open the Windows Task Scheduler.

   From the Windows server that hosts Toad Intelligence Central, log in as Administrator. Click **Start | Control Panel | System and Security | Administrative Tools | Task Scheduler**.

2. Click **Action | Create task**.

   On the **General** tab, give the task a **Name** and select **Run with highest privileges**.

   On the **Triggers** tab, click **New**. Set your required back up schedule. As a consideration, ensure this schedule does not conflict with the schedules set for Toad Intelligence Central such as snapshot refresh and Toad Data Point automation script execution. Ensure the schedule is set to complete prior to the full machine backup.

   On the **Actions** tab, click **New**.

   - The required action is to **Start a program**.
   - The program is located in the bin folder in the Toad Intelligence Central server install folder (by default Program Files\Quest Software\Toad Intelligence Central\bin).
   - The name of the program is **backup.bat**.
   - Set the **Add arguments** field to the target folder for the backup.
   - Set the **Start in** field to the bin folder in the Toad Intelligence Central server install folder (by default Program Files\Quest Software\Toad Intelligence Central\bin).

Restore Toad Intelligence Central

Follow these instructions to restore a backup of the Toad Intelligence Central server. To backup the Toad Intelligence Central server see Backup the Toad Intelligence Central server.

i | NOTE: Restore to the same version of Toad Intelligence Central as the backup. For example, a backup from Toad Intelligence Central 3.3 can only be restored to Toad Intelligence Central 3.3. It cannot be restored to Toad Intelligence Central 4.3.

1. Stop the Toad Intelligence Central server
2. Copy the entire backed up ProgramData\Quest Software\Toad Intelligence Central\ folder to the

ProgramData\Quest Software\Toad Intelligence Central\ folder used by the installation.

- Merge the files to keep both current and backed-up content.
- Overwrite the files to replace content.

3. Restart the Toad Intelligence Central server

i | **NOTE:** If you upgraded from Intelligence Central 3.2 (or earlier), the location of this folder might be ProgramData\Dell\Toad Intelligence Central. See Toad Intelligence Central Data Folder for more information.

Migrate Toad Intelligence Central

Copy ProgramData\Quest Software\Toad Intelligence Central\ from one Toad Intelligence Central server installation to another. ProgramData\Quest Software\Toad Intelligence Central\ stores all user information, data source connection information and mappings. See Toad Intelligence Central Data Folder for more information.

i | **NOTE:** If you upgraded from Intelligence Central 3.2 (or earlier), the location of this folder might be ProgramData\Dell\Toad Intelligence Central.

Troubleshooting

Before migrating, review the following potential issues.

Issue	Issue Description and Workaround
Automation scripts fail to run successfully after migration	In Toad Intelligence Central 2.7.2 (or earlier), attempting to run an Automation script after migration can result in a null password database error (for example, "ORA-01005: null password given; logon denied"). If you encounter this issue, contact Support or implement the following workaround. **Workaround:** To prevent this issue, before migrating to another server, upgrade your current Toad Intelligence Central installation to version 3.0 (or later). Then perform the migration.
Automation scripts fail to run successfully after migration	In Toad Intelligence Central 4.3 (or earlier), after migrating data files from one Toad Intelligence Central server installation to another, the migrated Automation scripts set to run under an account other than the default user account do not run successfully. **Workaround:** Contact Quest Support for a workaround. See the following knowledge base article for more information: https://support.quest.com/toad-intelligence-central/kb/250694/migrating-the-tic-data-folder-causes-published-scripts-execution-to-fail.
Error fetching build_arch for Intelligence Central server	A known issue found when connecting to Toad Intelligence Central following migration generates the following error: "Error fetching build_arch for Intelligence Central server." **Solution:** If you encounter this error, right click the **Data** folder in ProgramData\Quest Software\Toad Intelligence Central\ and select **Properties**. On the **General** tab in the **Attributes** section ensure **Read-only** is NOT selected.

Migration Prerequisites

Ensure the version of Toad Intelligence Central is the same for both installations before migration. Upgrade one of the Toad Intelligence Central installations if necessary.

To migrate Toad Intelligence Central

1. **For the Toad Intelligence Central server you are migrating from:**

   a. Stop the Toad Intelligence Central server

   b. Make a copy of ProgramData\Quest Software\Toad Intelligence Central\.

2. **For the Toad Intelligence Central server you are migrating to:**

   a. Stop the Toad Intelligence Central server

   b. Replace ProgramData\Quest Software\Toad Intelligence Central\ with the copy you made in **Step 1.b.**

      - Merge the files to keep both the current and backed up content.

      - Overwrite the files to replace the current content.

   c. Restart the Toad Intelligence Central server

3. **For the Toad Intelligence Central server you are migrating from:**

   a. Optionally, Restart the Toad Intelligence Central server

4. **The Administrator connects to Toad Intelligence Central via a web browser**

   a. The Administrator password is the Administrator password for the Toad Intelligence Central server you migrated from.

   b. Reenter the Toad Intelligence Central License.

   c. Notify Toad Intelligence Central users of the change. If the host name or IP address of the Toad Intelligence Central server has changed then they will need to update their connection details as appropriate.

5. **Data connectivity**

   Some data source connections make use of drivers installed on the Intelligence Central server. Ensure all drivers required by the Intelligence Central server data source connections are installed on the new Intelligence Central server.

Configure Web Server for HTTPS

You can configure the Toad Web Server to use HTTPS protocol for network communication. To do this you must add an HTTPS binding to the Toad Web Server applicationhost.config file. Then bind a certificate to the port you specified to be used for the HTTPS communication.

The following procedure describes general instructions. Instructions for your environment may vary.

To configure Web Server for HTTPS

1. Stop the Toad Web Server.

   a. Open the **Windows Control Panel**.

   b. Select **Administrative Tools | Services**.

   c. Right-click **Toad Web Server (Toad Intelligence Central)** and select **Stop**.

2. Add a site binding to the Toad Web Server config file.

   a. Locate the Toad Web Server installation directory. The default path is:

   C:\Program Files\Quest Software\Toad Intelligence Central Web Server.

   b. In this directory, open **applicationhost.config** in an editor, such as Notepad.

   c. Add a site binding using the following format:

   <bindings>

       <binding protocol="https" bindingInformation="*:443:"/>

   </bindings>

   Where:

   - *protocol* defines the protocol to use (in this case "https")

   - *bindingInformation* provides the following: [ip]:[port]:[host]

   The example above adds an https binding on port 443 for any IP address and any host.

3. View available public key certificates on host computer.

   a. To view public key certificates available on this computer, open the Microsoft Management Console (MMC.exe). (Open the Command Prompt, type mmc, and press ENTER.)

   b. In the Console, select **File | Add/Remove Snap-in**.

   c. Select **Certificates** and click **Add**.

   d. In the Certificates snap-in dialog, select **Computer account**. (Optionally, select My User account or Service account if applicable.)

   e. In the Select Computer dialog, click **Finish**.

   f. In the Add or Remove Snap-ins dialog, click **OK** to save your changes and close the dialog.

   g. In the Console, expand the **Certificates (Local Computer)** node (depending on the added snap-in) to display certificate stores.

   h. Select a store to display available certificates in that store.

4. Select certificate to use and copy thumbprint value.

   a. Select a certificate to bind to the https port number.

   b. Double-click the selected certificate to open it.

   c. In the Certificate dialog, select the **Details** pane.

   d. Scroll down and select **Thumbprint**. This hexadecimal value identifies the certificate.

   e. Copy the thumbprint value. You must remove the spaces before using it in a command.

f. Paste the value in an editor, such as Notepad, and remove the spaces. This is your certificate hash.

5. Bind certificate to port.

    a. Open a Command Prompt window.

    b. Run a command similar to the following to bind the certificate to the port:

```
netsh http add sslcert ipport=0.0.0.0:443 appid={00112233-4455-6677-8899-
AABBCCDDEEFF} certhash=YOURCERTHASH
```

    Where:

    - *ipport* is the IP address and port to bind

    - *appid* is a GUID that can be used to identify the owning application

    - *YOURCERTHASH* is the certificate hash (thumbprint) value

6. Start the Toad Web Server.

Upgrade Toad Intelligence Central

To upgrade, run the Toad Intelligence Central installer.

ℹ | **NOTE:** Beginning with Toad Intelligence Central 4.3, the Admin Console is no longer required and is not included in the installation. If an earlier version of the Admin Console exists, it is recommended that you uninstall it.

This release of Toad Intelligence Central has been tested with and supports an upgrade from either of the two previous versions. For example, an upgrade to Intelligence Central 4.3 from version 3.3 or 3.2 has been tested and is supported.

ℹ | **NOTES:**

- The Toad Intelligence Central Data folder stores user information, data source connection information and mappings, snapshots and datasets. This folder is not affected by the upgrade. See Toad Intelligence Central Data Folder for more information.

- By default, the location of the Toad Intelligence Central Data folder is ProgramData\Quest Software\Toad Intelligence Central\. If you upgraded from Intelligence Central 3.2 (or earlier), the location of this folder might be ProgramData\Dell\Toad Intelligence Central.

- To upgrade Toad Intelligence Central from a deprecated operating system, refer to Upgrade Toad Intelligence Central from a deprecated operating system.

Intelligence Central Automatically Upgrades Authentication Keys

If upgrading from Toad Intelligence Central 3.3 or earlier, authentication keys for some objects must be upgraded to support the more-simplified object Authentication process introduced in Intelligence Central 4.3. Specifically, if a view has both a shared key and a personal key, the personal key is removed. This process runs automatically during upgrade/installation.

ℹ | **IMPORTANT:** If an error occurs during the process of deleting the redundant authentication keys (deleting personal keys where a shared key exists), please contact Quest Support for further assistance.

Upgrade Toad Intelligence Central from a deprecated operating system

Follow these instructions to upgrade Toad Intelligence Central from a deprecated operating system.

1. Stop the Toad Intelligence Central server.

2. **Copy ProgramData\Quest Software\Toad Intelligence Central\ including subfolders to the location**

that will be used by Toad Intelligence Central 4.3

The default location is (C:\ProgramData\Quest Software\Toad Intelligence Central\). This folder will potentially grow quite large if lots of users publish lots of objects and take snapshots. You may choose to change the default folder location. For example, you may choose to direct the data files folder to a separate drive. If you do change the location of the data files folder be sure to document it as this folder is frequently referred to during server maintenance.

If you upgraded from Intelligence Central 3.2 (or earlier), the location of this folder might be ProgramData\Dell\Toad Intelligence Central.

See Toad Intelligence Central Data Folder for more information.

3. Install the Intelligence Central server 4.3 on a supported operating system.

   During installation you will be prompted for the Data Files Folder. Ensure this location is set to the place you copied ProgramData\Quest Software\Toad Intelligence Central\.

4. **The Administrator connects to Toad Intelligence Central 4.3 via the Web Server**

   a. The Administrator password is the Administrator password for the original Toad Intelligence Central installation.

   b. Reenter the Toad Intelligence Central License.

   c. Notify Toad Intelligence Central users of the change. As the host name / IP address of the Toad Intelligence Central server has changed then they will need to update their connection details as appropriate.

   > **i** | **NOTE:** A known issue on connecting to Toad Intelligence Central 4.3 following this upgrade is Error fetching build_arch for Intelligence Central server. If you see this error then right click the **Data** folder in ProgramData\Quest Software\Toad Intelligence Central\ and select **Properties**. On the **General** tab in the **Attributes** section ensure **Read-only** is NOT selected.

5. **Use Toad Intelligence Central 4.3 (Data Source Connections and Drivers)**

   Some data source connections make use of drivers installed on the Intelligence Central server. Ensure all drivers required by the Intelligence Central server data source connections are installed on the new Intelligence Central server.

Uninstall Toad Intelligence Central

Use the Toad Intelligence Central installer to uninstall each component.

Backup / Remove Data

Data from Toad Intelligence Central is stored in ProgramData\Quest Software\Toad Intelligence Central\. This folder is not removed automatically on uninstall. Backup or remove it manually as required.

> **i** | **NOTE:** If you upgraded from Intelligence Central 3.2 (or earlier), the location of this folder might be ProgramData\Dell\Toad Intelligence Central.

For more information see: Backup the Toad Intelligence Central server and Toad Intelligence Central Data Folder.

About Us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

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