Quest

Toad® Intelligence Central 2026 R2

Deployment Guide

Copyright© 2026 Quest Software Inc.
ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at www.quest.com/legal.

Trademarks

Quest, Toad, and the Quest logo are trademarks of Quest Software Inc. in the U.S.A. and other countries. For a complete list of Quest Software trademarks, please visit our website at www.quest.com/legal. Microsoft, Windows, Windows Server, Excel, SQL Server, Active Directory and SharePoint are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Oracle is a registered trademark of Oracle and/or its affiliates in the United States and other countries. Google® and Google Analytics™ are registered trademarks of Google Inc. SAP® and SYBASE® are the trademark or registered trademark of SAP AG in Germany and in several other countries. Salesforce.com and Salesforce are trademarks of salesforce.com, inc. and are used here with permission. Apache, Apache Hadoop, Hadoop, Apache Cassandra, Cassandra, Apache HBase, HBase, Apache Hive and Hive are trademarks of the Apache Software Foundation. Amazon SimpleDB™ and SimpleDB™ are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries. MongoDB is a trademark of MongoDB, Inc. Kerberos is a trademark of the Massachusetts Institute of Technology (MIT). Snowflake® is a registered trademark of Snowflake Inc. in the United States and/or other countries. Other trademarks are property of their respective owners.

Legend

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.

Toad Intelligence Central Deployment Guide
Updated - Wednesday, September 2, 2026
Software Version - 2026 R2

Contents

Welcome to Toad Intelligence Central **8**
About This Guide 8
Additional Resources 9
Find Help from Inside Toad Intelligence Central 9

Install Toad Intelligence Central **10**
Install Toad Intelligence Central 10
Install Toad Data Point and ODBC Drivers 12
Authenticated proxy server connections 13
Use Virtual Disk (VMDK) in Virtual Machine Installation 13
Deploy Toad Intelligence Central in Microsoft Azure 14
Deploy Intelligence Central from Azure Marketplace 14
Install Toad Intelligence Central in Azure 14

License Toad Intelligence Central **17**

Connect to Toad Intelligence Central **18**
Open the Web Console 19
Connect Using Other Toad Applications 19
Third-Party Connection to Toad Intelligence Central 20
Requirements / Limitations 20
Connection 20
MySQL database 21
Queries 21
MySQL Views 21
Connecting to Toad Intelligence Central from Excel (2019 and later) file 22

Users and Groups **24**
Types of Users 24
Types of Groups 25
Add Active Directory Users and Groups 25
Requirements 26
Known issues and Limitations 26
Authenticate to Active Directory 27
Add from Active Directory 28
Add Single Sign-On Users and Groups 29
Requirements 29
Authenticate to Single Sign-On Provider 30

Add from Single Sign-On Provider 30
Create Intelligence Central Groups 31

Manage Users and Groups 33
View User and Group Information 33
Edit User and Group Information 34
Reset User Password 34
Change a User's Role 34
Change User's Email Subscriptions 35
Disable a User Account 35
Enable a Disabled User Account 35
Remove a User 36
Remove a Group 36
User Roles 37
Privileges by Role 37
User Management Privileges 37
Object Management Privileges 38
Misc Privileges 39
Licensing Privileges 39
Configure New User Registration 40
Enable/Disable Add Users and Self-Registration 40
Specify Default User Role 40
Restrict Registration to Active Directory or SSO Users 41
Configure New Group Creation 41
Synchronize Active Directory and Single Sign-On 41
Synchronize status 42
Synchronize rules 42

Email Notifications 44
How to Configure Notifications 44
Types of Email Notifications 44
Server Email Notification Settings 44
Specify User Email Subscriptions 45

Misc Administrator Activities 46
Configure Session 46
Configure New Group Creation 46
Download Audit Log 46
Enable User Experience Feedback 47

Manage Objects 48
View Objects 48

View Objects by User or Group ... 48
Move Objects and Folders ... 49
Data Connectivity and Data Objects ... 49
Authentication ... 50
Specify Visibility and Manage Privileges for Objects ... 51
Specify Visibility Privileges ... 51
Specify Manager Privileges ... 52
Toad Data Point Automation Scripts ... 52
Alter Automation Script Credentials ... 53
Alter Authentication ... 54

Folders in Intelligence Central ... 56
Special Folders ... 56
Secured and Non-Secured Folders ... 56

Create Folders ... 57

Move Folders ... 58

Delete Folders ... 59
View Folder Details ... 59
About Secured Folders ... 60
Secured Folder Characteristics ... 60
Why Use Secured Folders ... 60
Server-Level Configuration ... 60
Rules and Restrictions for Secured Folders ... 61
Specify Visibility, Manage and Publish Privileges for Folders ... 62
Specify Sharing Privileges ... 62
Specify Manage and Publish Privileges ... 63
Configure Server for Folder Security ... 63

Manager Privileges ... 65
Manager Privileges for Objects ... 65
Manager Privileges for Secured Folders ... 66
Who Can Manage Objects/Folders ... 66

Reports ... 67
Data Object Usage Report ... 67
Dashboard View ... 67
What's popular? ... 67
What's been used? ... 68
What's been published? ... 68
User Activity Report ... 68

Landing Page ... 69
Drill Down to Additional Data ... 69

Health Check Dashboard ... 70
Run a Health Check ... 70
Data Integrity ... 70
Exceptions ... 71
Transfer Object Owner ... 71
Specify Settings ... 72

Support Bundle ... 74
Create a Support Bundle ... 74

Server Maintenance ... 75
Toad Intelligence Central services ... 75
Stop the Toad Intelligence Central server ... 75
Restart the Toad Intelligence Central server ... 76
Toad Intelligence Central Data Folder ... 76
Backup the Toad Intelligence Central server ... 77
Manual backup ... 77
Executable backup ... 77
Scheduled backup ... 78
Restore Toad Intelligence Central ... 78
Migrate Toad Intelligence Central ... 79
Troubleshooting ... 79
Migration Prerequisites ... 80
To migrate Toad Intelligence Central ... 80
Configure Web Server for HTTPS ... 81
Configure Toad Intelligence Central for SSO Authentication ... 82
Corporate Identity Providers supported in Toad Intelligence Central ... 82
Microsoft Entra ID ... 82
Required Configuration on the Microsoft Entra ID Portal ... 83
Required Setup on the Machine that Hosts the Toad Intelligence Central Server ... 84
Configure SSO in the TIC Web Interface ... 86
Self-Registration Workflow ... 88

Upgrade Toad Intelligence Central ... 90
Upgrade Toad Intelligence Central from a deprecated operating system ... 91

Uninstall Toad Intelligence Central ... 92
Backup / Remove Data ... 92

About Us ... 93

Contact Quest 93
Technical Support Resources 93

1

Welcome to Toad Intelligence Central

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

- AUTOMATE - Toad users can schedule the regular automated execution of Toad Data Point automation scripts on Toad Intelligence Central.
- ACCESS - Toad users can access Toad files and basic data files published to Toad Intelligence Central that have been shared with them. An additional data connectivity license extends Toad Intelligence Central to work across a wide range of data stores including relational database models, data warehouses, No SQL and Business Intelligence data sources like OBIEE and SAP®.
- SHARE - Objects can be shared amongst users and groups and organized collectively in a familiar folder structure, assigned tags and given a description for easy search retrieval. Administration of users and groups can be managed locally or users and groups can be imported from Active Directory®.
- SECURE - Toad Intelligence Central provides a centrally managed, secure, stable and accessible system.

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

About This Guide

This Guide is Intended for Administrators

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

Users with the Administrator Role

- This guide describes procedures that can be performed by users with the Administrator role, including the Administrator (root) user.

Standard and Power Users

- Non-Administrators should refer to the *Toad Intelligence Central Quick Start Guide* for functionality available only to the non-Administrator roles.

Additional Resources

- Product documentation - Find the complete set of Toad Intelligence Central technical documents.
- Toad Intelligence Central User Forum - Learn more about Toad Intelligence Central, find answers to questions, and connect with the community.
- Toad Intelligence Central Blogs - Find articles describing how to use the features in Intelligence Central.

Find Help from Inside Toad Intelligence Central

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

  There you will find the Release Notes, User Guide, Deployment Guide (installation and Administrator information), and What's New in This Release for the current and earlier versions of Toad Intelligence Central.
- To go to the Toad Intelligence Central User Forum in Toad World, click and select **User Forum**.

2

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 Toad Intelligence Central. 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. The Toad Intelligence Central Web Server is installed along with the Toad Intelligence Central server.

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 Toad Intelligence Central

Use the Toad Intelligence Central Server Installer to install the Intelligence Central server and the Web Server.

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

To install Toad Intelligence Central

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.

> **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
Web server port number	Port 80 is reserved for the web port. During installation, you can change this if required. **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.	80

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).

> **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. Click **Install**.

> **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.

Product registration is optional. Register as a Toad user to receive product news and updates. If you register at the time of installation, you can unsubscribe at: https://www.quest.com/unsubscribe.

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 75.

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.

> **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.

> **NOTE:** Starting with Toad Intelligence Central 2025 R2, the 32-bit edition is no longer available. Toad Intelligence Central and Toad Data Point are delivered exclusively as 64-bit editions.

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.

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.

Deploy Toad Intelligence Central in Microsoft Azure

The following methods are available for deploying Toad Intelligence Central in Microsoft Azure:

- Deploy Toad Intelligence Central from Azure Marketplace as a pre-installed application.
- Install Toad Intelligence Central in your virtual machine environment in Azure.

Deploy Intelligence Central from Azure Marketplace

Toad Intelligence Central is now available in the Azure Marketplace. This pre-installed offering provides a quicker, more-simplified deployment of Intelligence Central. If you do not need to customize your installation, this method might be preferable to manually installing Intelligence Central in a new or existing Azure VM.

To locate Toad Intelligence Central in the Azure Marketplace, go to Microsoft Azure Marketplace and search for Quest Toad Intelligence Central.

To deploy Toad Intelligence Central from Azure Marketplace

1. From the Azure Portal home page, click **Create a resource** and then *Search the Marketplace* for Toad Intelligence Central.
2. Select Toad Intelligence Central and then click **Create**.
3. On the Create a Virtual Machine page, select the desired options to create a virtual machine with a Toad Intelligence Central image pre-installed. Some options are pre-configured. Some options are customizable.

Install Toad Intelligence Central in Azure

Use these guidelines to help you set up and install Toad Intelligence Central in your own virtual machine environment in Microsoft Azure. Use this manual method if you have any of the following requirements:

- If you must customize your installation, such as specifying a custom location for the Toad Intelligence Central Data Folder or modifying a port number.
- If you must use a version of Toad Intelligence Central other than the one available through Azure Marketplace.

To install Toad Intelligence Central in Azure

1. Go to the Microsoft Azure portal at https://portal.azure.com and log in.
2. Create a resource on Azure. It is recommended to use Windows Server 2016 VM.
    a. On the Microsoft Azure home page, click **Create a resource**.
    b. Click **Windows Server 2016 VM**. If the option is visible, select the **Get started** category in the left pane to display the **Windows Server 2016 VM** option in the right pane.
3. Enter the basic information in the Create Virtual Machine page. Review the following for additional information.
    - Subscription—A Windows Azure subscription grants you access to Windows Azure services and to the Windows Azure Platform Management Portal. This shipped with your Azure account.
    - Resource group—A resource group is a collection of resources that share the same life cycle, permissions, and policies.

      Select **Use existing** to select an existing resource group or select **Create new** to create a new one.
4. Click **Size** in the left pane to select a size for the VM. It is recommended to select at least 8 GB of memory.
5. Click **Settings** in the left pane to configure optional features. Review the following for additional information.
    - High availability—None.
    - Storage use managed disks—Yes.
    - Network—You can use an existing virtual network in your subscription or create a new virtual network automatically by default.
    - Public IP—Static. If assignment is dynamic, the IP address may change after restart.
    - Network | Network security group—If you select **Basic**, add *RDP (3389)* to the public inbound ports list to enable remote access to the Windows Server virtual machine. If you select **Advanced**, create a new network security group or use an existing security group.
6. Specify the remaining settings:
    a. Auto-shutdown—Off
    b. Monitoring | Boot diagnostics—Disabled
    c. Monitoring | Guest OS diagnostics—Disabled
    d. Managed service identity—No
    e. Backup—Disabled
7. Click **Create** to deploy the VM. The virtual machine takes a few minutes to deploy.
8. After deployment is successful, connect to the virtual machine using the RDP file.
9. When prompted, enter credentials using the user name and password you created when you configured the basic settings in step 3.

10. After logging in to the virtual machine, go to the Properties page for the local server (Server Manager\Local Server) and set **IE Enhanced Security Configuration** to **Off** .
11. Install Toad Intelligence Central. See Install Toad Intelligence Central for further instructions.
12. If you intend to access the Intelligence Central service locally from the same virtual machine, you must configure the network security group.
    a. Return to the deployment page for your virtual machine in the Azure portal. Then go to **Settings | Networking**.
    b. Add the Application server port and the Web server port to the inbound port rules list and the outbound port rules list.
13. Update Windows Firewall rules on the virtual machine.
    a. Open Windows Firewall with Advanced Security (or run **wf.msc**).
    b. Create a new inbound rule. Select **Port** and click **Next**. Select **Special local ports** and enter 80, 8066, 3566. Click **Next**. Select **Allow the connection** and click **Next**. Select these three options for applying the rule: **Domain**, **Private**, and **Public**. Click **Next**. Enter a name for the new rule and click **Finish**.

3

License Toad Intelligence Central

Toad Intelligence Central is shipped with a trial key that enables a 30 day open trial license to Toad Intelligence Central. Use this key to evaluate Toad Intelligence Central. At the end of the 30 day trial, if a Data Connectivity license has not been entered, your Toad Intelligence Central functionality will be limited to that of the Toad Intelligence Central Community Edition.

Data Connectivity License

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

To view / activate Toad Intelligence Central licenses

1. From a web browser, log in to Toad Intelligence Central. Any Toad Intelligence Central user can add a license. Administrator credentials are required to remove a license.
2. Select **Administration | Licensing**.
3. If Toad Intelligence Central has multiple licenses assigned, select the license to view or click **Add License** to add a license.

After licensing Toad Intelligence Central, you can select to provide anonymous user feedback to help influence the design of future releases. See Misc Administrator Activities to learn how to easily enable this feature.

4

Connect to Toad Intelligence Central

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

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

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 75.

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

Open the Web Console

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

To open the Toad Intelligence Central Web Console

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

URL	The address of Toad Intelligence Central is **http://*hostName*/** where *hostName* is the name of the computer hosting the Web Server and Toad Intelligence Central. If the Web Server has been installed on a port other than port 80 then the address is **http://*hostName:port*/**.
Log in	Toad Intelligence Central prompts you to login. If you login to Toad Intelligence Central using Windows credentials, then enter your login name at the login prompt. If necessary, include your Windows domain: **domain\username**. The computer you use to login to Toad Intelligence Central must be accessible to your Windows domain. If you login to Toad Intelligence Central using Single Sign-On credentials, then click Login with Single Sign-On at the login prompt. The computer you use to login to Toad Intelligence Central must be accessible to your Corporate Identity Provider for authentication. See Configure Toad Intelligence Central for SSO Authentication for more information about configuring supported Corporate Identity Providers with TIC. 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 the password you entered when you installed the Intelligence Central server. **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.

NOTE: Toad Intelligence Central encrypts your login credentials when transmitted over the network.

Refer to your local Toad Intelligence Central Administrator for more information.

Connect Using Other Toad Applications

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

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

After objects are published to Intelligence Central, users can view, access, manage, and work with these objects through the Intelligence Central Web Console. See the *Toad Intelligence Central Quick Start Guide* for more information about functionality available to Standard users through the Web Console.

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.

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.

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

Queries

Query tables, views, snapshots and datasets.

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

Connecting to Toad Intelligence Central from Excel (2019 and later) file

To create the connection:

- Create a self-signed certificate or obtain a certificate from Certification Authority for Toad Intelligence Central (TIC) **URL** or **IP address**
- Install the certificate in Trusted Root Certification Authorities store on the server where Toad Intelligence Central (TIC) is installed
- Bind the certificate to **port 8066** by running one of the following commands in elevated

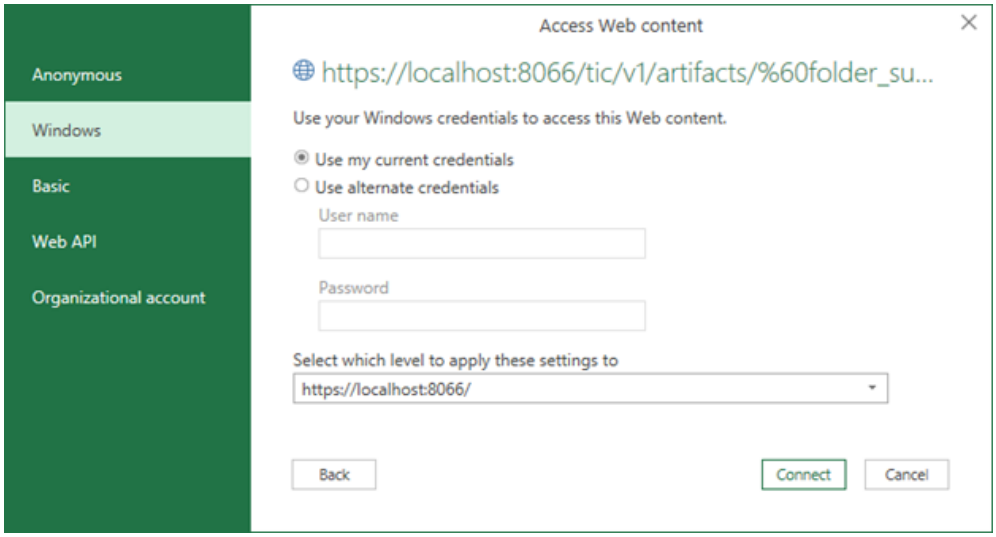
  - If connecting to TIC via IP address use the following PowerShell command:
  `netsh http add sslcert ipport={tic IP}:8066 certhash={certificate thumbprint} appid={00112233-4455-6677-8899-AABBCCDDEEFF}`

  - If connecting to TIC via the domain name use the following PowerShell command:
  `http add sslcert hostnameport={tic URL}:8066 certhash={certificate thumbprint} appid={00112233-4455-6677-8899-AABBCCDDEEFF} certstorename=MY`

> **NOTE:**
> `{tic IP}` replace with IP address e.g., 127.0.0.1
> `{tic URL}` replace with TIC URL e.g., ticserver.mydomain.com
> `{certificate thumbprint}` replace with certificate thumbprint, which can be viewed in Certificate Manager in Windows by opening the certificate, switching to the details tab, and copying the value for the Thumbprint property

- If using a self-signed certificate, it needs to be installed in Trusted Root Certification Authorities store on every client that needs to connect to TIC from an Excel file; alternative is to set up Domain Controller to distribute the certificate to all clients
- From TIC, select the desired object and note the name and database properties in the details panel
- From Excel, go to the Data tab and select Get Data | From Other Sources | From Web
- Type the URL as follows (replace text in bold with appropriate values) and press OK:
https://{tic URL/IP}:8066/tic/v1/artifacts/`{database}`.`{name}`/content

- In the next dialog, select Windows or Basic authentication, depending on what authentication method is used to connect to TIC



- After this is done, data can be imported and refreshed on demand

5

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.
	Single Sign-On Users To self-register from a web browser, click **Register as a new user** at the login prompt, and then click **Register with Single Sign-On**. The computer you use to login to Toad Intelligence Central must be accessible to your corporate identity provider for authentication. This option is visible only if your local configuration allows self-registration via a web browser. To register new users post login, see ***Add Single Sign-On Users and Groups***. Your local configuration may require login with an Administrator role to add Single Sign-On 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.
	Single Sign-On Groups Following login to Intelligence Central from a web browser, to add a group from Single Sign-On provider, select **Administration | Groups | Add Group | Add Single Sign-On Group**. See *Add Single Sign-On Users and Groups*. Your Intelligence Central configuration may require login with an Administrator role to add Single Sign-On 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 31.

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 Open the Web Console on page 19.
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.

Issue	More information
Active Directory names containing characters not allowed by Toad Intelligence Central	Active Directory names containing the following characters cannot be imported to Intelligence Central. You will be notified of any users and groups who cannot be imported. • Forward slash (/) • Backward slash (\) • Left square bracket ([) • Right square bracket (]) • Colon (:) • Semicolon (;) • Vertical bar (|) • Equal sign (=) • Plus sign (+) • Asterisk (*) • Question mark (?) • Left angle bracket (<) • Right angle bracket (>) • Double quote (") • At symbol (@) • Comma (,)
Active Directory supports sub groups (groups within groups). Intelligence Central does not.	When importing an Active Directory group with sub groups the sub groups and users in sub groups are not imported to Intelligence Central.

Authenticate to Active Directory

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

To authenticate to Active Directory

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

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

2. **Remember these credentials on server for future Active Directory access and synchronization**—Select this option to instruct Intelligence Central to do the following:
   - Automatically and regularly synchronize imported Active Directory users and groups. For more information, see Synchronize Active Directory and Single Sign-On on page 41.
   - 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 | Settings**. 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 and Single Sign-On for more information.
3. **Schedule AD synchronization.** If you selected **Remember these credentials...**, you can schedule the Active Directory synchronization. Enter the scheduling details in the fields provided. After scheduling a synchronization, the scheduling information and status are displayed in **Administration | Server | Settings**.

Add from Active Directory

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

To add users/groups from Active Directory

1. In the Add Users/Groups from Active Directory dialog, select a domain from the drop-down list. Intelligence Central retrieves the list of users in that domain.
2. You can filter the list by entering a partial text string in the text box.
3. To refresh the list, click **Refresh**. The refresh option is available only for domains that are selected for synchronization in Intelligence Central. See Synchronize Active Directory and Single Sign-On for more information.

   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.

   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.

Add Single Sign-On Users and Groups

Users with certain privileges can add new users and groups to Toad Intelligence Central by importing users/groups from Single Sign-On Provider (Corporate Identity Provider). 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 Single Sign-On User or Group using the Web interface

1. Use a web browser to log in to Intelligence Central. For more information, see Open the Web Console on page 19.
2. Click **Administration** and then select either **Users** or **Groups**.
3. Then select **Add User | Add Single Sign-On User** or **Add Group | Add Single Sign-On Group**.
   - If the Authenticate to Single Sign-On dialog opens, enter the Tenant ID, Client ID and Client Secret in order to access a list of users and groups. See Authenticate to Single Sign-On Provider for more information.
4. In the Add Users and Groups from Single Sign-On Provide dialog, select the users/groups to add to Intelligence Central. SeeAdd from Single Sign-On Provider for more information.

Requirements

1. Toad Intelligence Central (Toad Web Server) must be configured to use HTTPS protocol for network communication. See Configure Web Server for HTTPS for more information.
2. The Corporate Identity Provider that is being used must be supported by Toad Intelligence Central. See Configure Toad Intelligence Central for SSO Authentication to review the list of supported identity providers.

3. The Toad Intelligence Central server host must be accessible for authentication via your Corporate Identity Provider.

Authenticate to Single Sign-On Provider

Use the Authenticate to Single Sign-On Provider dialog to enter the Tenant ID, Client ID and Client Secret in order to access a list of users and groups when attempting to add Single Sign-On users (or groups) to Intelligence Central.

To authenticate to Single Sign-On

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

Field	Description
Tenant ID	Identifies the Corporate Identity Provider directory where the application is registered. It ensures authentication requests are directed to the correct tenant identity.
Client ID	A unique identifier for the registered application. It tells the Corporate Identity Provider which application is requesting authentication.
Client Secret	A secure value (similar to a password) used by the application to authenticate itself to the Corporate Identity Provider when requesting tokens.

2. **The credentials provided are saved by default on server for future Single Sign-On access and synchronization** - allowing Intelligence Central to do the following:
   - Automatically and regularly synchronize imported Single Sign-On users and groups. For more information, see Synchronize Active Directory and Single Sign-On on page 41.
   - Cache Single Sign-On user and group data on Toad Intelligence Central. This improves performance of Toad Intelligence Central when looking up Single Sign-On users and groups.

   To view the Single Sign-On Provider (tenant) configured for Single Sign/On synchronization, in the Web interface go to **Administration | Server | Settings**. Log in with Administrator role is required to view this information. You can also change the credentials used for synchronization from this page.For more information, see Synchronize Active Directory and Single Sign-On on page 41.
3. **Schedule Single Sign-On synchronization**. You can schedule the Single Sign-On synchronization. Enter the scheduling details in the fields provided. After scheduling a synchronization, the scheduling information and status are displayed in **Administration | Server | Settings.**

Add from Single Sign-On Provider

This dialog is used to add users and groups from Single Sign-On Provider to Toad Intelligence Central.

To add users/groups from Single Sign-On

1. In the Add Users/Groups from Single Sign-On Provider dialog, Intelligence Central retrieves the list of users from the corporate identity provider.
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 the identity provider that has been authenticated for synchronization in Intelligence Central. For more information, see Synchronize Active Directory and Single Sign-On on page 41..

   NOTE: This process could take several minutes, depending on the number of users and groups that need to be synchronized.

4. Select available Single Sign-On users/groups and move them to the **users/groups to be added** list.

   TIPS:

   - Use SHIFT to select multiple users/groups in sequence. Use CTRL to select multiple users/groups not in sequence.
   - The number of Single Sign-On users displayed is limited to 10,000. If the list exceeds 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.

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

   When a group is added, a Single Sign-On 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).

6. 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.

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 and Single Sign-On on page 41.
		Single Sign-On users and groups. Log in to a web browser to view the properties of Single Sign-On users and groups. Use the Corporate Identity Provider's administration portal to edit the properties of Single Sign-On users and groups. Users with an Administrator role (User Roles) manage that Intelligence Central is synchronized with Single Sign-On user and group information. For more information, see Synchronize Active Directory and Single Sign-On on page 41.

Users	Groups	Description
		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.

> **TIP:** Show / hide Active Directory/ SSO 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

User	Description
	The Toad Intelligence Central Administrator cannot reset the password for Active Directory\SSO users. The user should follow the standard procedure in their Active Directory\SSO environment to reset their Active Directory\SSO 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.

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 a User Account

Users with the Administrator role (User Roles) can disable a user account in Intelligence Central. When an account is disabled, the user cannot log in to Intelligence Central until the account is enabled again.

Objects owned by the disabled user account remain in Toad Intelligence Central and can be used by users with rights to those objects.

- Log in to the Web Console and click **Administration | Users** to list the users of Toad Intelligence Central. Select the user account to disable so account details are visible on screen and then click **Disable User**.

  To review objects owned by the disabled user account and to transfer objects to a new owner, run a Health Check. See Health Check Dashboard for more information.

NOTE:

- The Administrator (root) cannot be disabled.
- The Administrator cannot disable a user while that user is connected to Toad Intelligence Central.

Enable a Disabled User Account

Users with the Administrator role (User Roles) can enable a disabled user account.

- Log in to the Web Console and click **Administration | Users** to list the users of Toad Intelligence Central. Select the user to re-enable to display account details and then click **Enable User**.
- When the user is re-enabled, their data (including objects, authentication, and sharing and manage rights) is as it was before.
- When an Intelligence Central account is re-enabled, a new password is generated. The Administrator is given the opportunity to send an email notifying the user. Review the following for more information.

User	Password for re-enabled account
	When an Active Directory\SSO user is re-enabled in Intelligence Central, the account uses the current Active Directory\SSO account password.
	When an Intelligence Central user is re-enabled, a new password is randomly generated. The Administrator can see the password and copy it to the clipboard. If an email client is installed, the success message allows the Administrator to send an email notifying the user of their new password. Otherwise it is up to the Administrator to provide the password to the user.

Remove a User

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

CAUTION: When a user is removed from Intelligence Central, objects owned by the user are also removed.

To remove a user

- Log in to the Web Console and 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**.

NOTES:

- 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.

Remove a Group

Groups	Description
	Users with an Administrator role (User Roles) can remove Active Directory\SSO 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**.

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. In particular, all actions performed through the **Administration | Server** section of the Web Console are available only to users with the Administrator 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
Add groups. This privilege is configuration dependent. See Misc Administrator Activities.	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

Privilege/Action	Administrator	Power user	Standard user
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
Remove an SSO group	Y	N	N
Synchronize Active Directory and Single Sign-On	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 (non-secured folder)	Y	Y	Y
Publish objects to a secured folder	Y	folders for which user has publish privilege	folders for which user has publish privilege
View objects on Home page and view object details	all objects	objects shared with the user	objects shared with the user
View a secured folder and its contents	Y	folders shared with the user	folders shared with the user
(View or snapshot) Display the text for the underlying query	Y	objects managed by the user	objects managed by the user
(Automation script) Display the detailed execution logs	Y	objects managed by the user	objects 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 managed by the user	objects managed by the user
Move an object	all objects	objects managed by the user	objects managed by the user
Move a non-secured folder and its contents	Y	folders in which all objects are owned by or managed by the user	folders in which all objects are owned by or managed by the user
Move a secured folder and its contents	Y	folders managed by the user	folders managed by the user
Create a secured folder. This privilege is configuration dependent. See Configure Server for Folder Security.	configuration dependent	configuration dependent	configuration dependent

Privilege/Action	Administrator	Power user	Standard user
Delete a folder	Y	folders in which all objects are managed by the user	folders in which all objects are managed by the user
Modify authentication key for an object	Y	objects managed by the user	objects managed by the user
(View or Automation script) Edit the default value for a variable	Y	objects managed by the user	objects managed by the user
(Automation script) Change script run account	Y	objects managed by the user	objects managed by the user
Force consumers to take a shared object published or managed by the user	Y	Y	N

Privileges Based on User-Object Relationship

In addition to granting object manage privileges by user role, manage privileges to an object are also granted based on the user's relationship to the object, for example, the object's publisher. For more information about privileges based on object relationship, see Manager Privileges.

Misc Privileges

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

- Configure New User Registration
- Synchronize Active Directory and Single Sign-On
- Download the Misc Administrator Activities
- Configure Misc Administrator Activities
- Enable/disable email notifications on server. See Server Email Notification Settings.
- Enable/disable email notification for a user (subscribe/unsubscribe a user). See Server Email Notification Settings.
- Health Check Dashboard
- Configure Server for Folder Security

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 | Permissions**.
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 user role for all new accounts. The default role is applied when a new user account is created. Only Administrators can specify a default user role. Administrators can then change the new account's role later.

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 | Permissions**.

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

Restrict Registration to Active Directory or SSO Users

You can require that new accounts use only Active Directory or Single Sign-On credentials.

To restrict new accounts to Active Directory or Single Sign-On users

1. Use a web browser to log in to Intelligence Central as a user with the Administrator role.
2. Select **Administration | Server | Permissions**.
3. Select **New users can register with Active Directory (Windows) or Single Sign-On credentials only**. When selected, only Active Directory or Single-Sign-On users can be added to Toad Intelligence Central. No new Intelligence Central users can be added.

Requirements for Single Sign-On Registration

1. The Corporate Identity Provider that is being used must be supported by Toad Intelligence Central. See Configure Toad Intelligence Central for SSO Authenticationto review the list of supported identity providers.
2. Toad Intelligence Central requires additional configuration for Single Sign-On authentication and registration. See Configure Toad Intelligence Central for SSO Authentication for more information.

Configure New Group Creation

By default anyone can create group, and any user with Administrator role can update this rule.

To specify default user role who can create group

1. Use a web browser to log in to Intelligence Central as a user with the Administrator role
2. Select **Administration | Server | Permissions**
3. In the New Group Creation section, select a role from the drop-down list

Synchronize Active Directory and Single Sign-On

When a domain in the Active Directory® forest / Single Sign-On Provider (corporate identity provider) is synchronized with Intelligence Central, changes to domain/SSO users and groups are replicated on Intelligence Central. Any user with an Administrator role (User Roles) can manage synchronizing Toad Intelligence Central with Active Directory / Single Sign-On Provider.

Synchronize status

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

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

Field / Action	Description
Last synchronized	Show the time the domain\SSO provider was last synchronized with Toad Intelligence Central. If the last attempt was unsuccessful then the error is reported in red.
Edit	Click to edit the schedule or to show/change the username and password used to connect to the domain, or Tenant ID, Client ID and Client secret to authenticate to the SSO (corporate identity) provider. This username/password pair is used to synchronize Toad Intelligence Central with Active Directory or Single Sign-On provider. The credentials are saved on Toad Intelligence Central.
Remove	Click to remove the domain or SSO provider from this list. The users and groups added from this domain\SSO provider will remain on Toad Intelligence Central, but will not be synchronized again. The Active Directory\SSO provider credentials saved on Toad Intelligence Central are removed.
Synch Now	Click to synchronize Toad Intelligence Central with the domain\SSO provider 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.

Synchronize rules

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

Table 2: Synchronization rules

Active Directory / Single Sign-On	Toad Intelligence Central
User details updated	Update the user details from Active Directory/Single Sign-On (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.

Active Directory / Single Sign-On	Toad Intelligence Central
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.

7

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 notifications can be enabled or configured on three different levels.

- **Server Level**—You can enable email service for the server and configure server email settings. Only users with the Administrator role can perform this configuration. See Server Email Notification Settings.
- **User Level**—You can subscribe individual users to the email notification service. Only users with the Administrator role can perform this configuration. See Server Email Notification Settings.
- **Email Notification Level**—You can 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 Email Notification Settings

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 email 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 (server-level)

- After enabling email notifications, you can specify which users are subscribed to email notifications.
    - To subscribe a user, make sure the user's name is listed in the **Subscribers** list. To specify which emails an individual user should receive, go to **Administration | Users**. See Specify User Email Subscriptions.
    - To unsubscribe a user, move the user to the **Unsubscribed** 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 to the Web Console 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.

NOTE: Email Notifications must be enabled on the Intelligence Central server before the Admin Digest can be sent. In addition, the user must be on the **Subscribers** list (Administration | Server | Notifications). See Server Email Notification Settings for more information.

8

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:

Configure Session

By default the session time out value is 60 minutes and the remember me interval is 30 days (when remember me option is enabled , user do not need to input credential again when login Toad Intelligence Central Web Console during the remember me interval).

To specify the value of session time out and remember me interval

1. Use a web browser to log in to Intelligence Central as a user with the Administrator role
2. Select **Administration | Server | Settings**
3. In the Session section, input the value in the field Session Time Out and Remember me Interval

Configure New Group Creation

Admin users now can specify which user roles are allowed to create user groups. For more information about Roles, see User Roles.

1. Use a web browser to log in to Intelligence Central as a user with the Administrator role
2. Select **Administration | Server | Permissions**
3. Select an option in **New Group Creation**

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 | Settings**.
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

1. You can influence the design of future versions of Toad Intelligence Central and help us improve its quality, reliability and performance.
2. ***To enable/disable user experience feedback***
3. a. 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.
   b. Click **Administration | Server | Settings**.
   c. Select or clear the **Provide anonymous user experience feedback to help improve Toad Intelligence Central** option.
4. Refer also to the Privacy Statement.

9

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 Data Object Usage Report 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. You can also relocate an object by selecting the destination folder in the selected object's **Details** pane. Users with the Administrator role or manage privileges to the object can move an object (between non-secured folders). An object cannot be moved if it is locked by another user.

Restrictions:

- You cannot move rules out of the ***Common_Transformation_Repository***.
- You cannot sort or reorganize objects within a folder.
- You cannot move an object to a folder where the name exists.
- To move an object, you must have manage privileges to the object.
- To move an object to a secured folder, you must have manage privileges to the object and to the secured folder.

To move folders

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

Restrictions:

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

See About Secured Folders for more information about secured folders.

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.

> **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.

> **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
	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.

Icon	Object	Description
	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.

Specify Visibility and Manage Privileges for Objects

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

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

Specify Visibility Privileges

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

To alter Visibility for an object

1. In the Web Console, click **Home**.
2. Select an object to display details.
3. In the Details pane, click **Visibility** to open the Alter Visibility dialog.
4. Select to either keep the object private, make it public, or share it with a list of users you specify. Review the following for additional information.

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

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

Specify Manager Privileges

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

To modify Manage privileges for an object

1. In the Web Console, click **Home**.
2. Select an object to display object details.
3. In the Details pane, click **Managers** to open the Alter Visibility dialog.
4. Select a Manage option based on the specified Visibility setting:

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

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

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

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.

NOTE: Beginning with Toad Intelligence Central 5.1.5 Toad would add the user account that executes automation scripts to a new OS (Windows server) group called TIC Automation. This new group's permissions are similar to normal Users group with some additional permissions necessary to execute automation scripts. Toad Application Server (ToadBIAppServer), is the service that triggers execution of Toad Data Point Automation Scripts in Toad Intelligence Central, its default login is Local System account.

If the login is changed from Local System account to another account , e.g. a domain user that belongs to the Windows Administrators group, the following change is needed:

1. Open **Windows Control Panel | Administrative Tools | Local Security Policy | Local Policies | User Right Assignment**
2. Double-click **Replace a process level token** and click **Add User or Group** button to input that account that would be the login for the ToadBIAppServer

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.

  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.

   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.

> **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.

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

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

Folders in Intelligence Central

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

Special Folders

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

No folder assigned

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

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

Common_Transformation_Repository

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

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

Secured and Non-Secured Folders

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

An Intelligence Central server can provide one or both types of folders. A user with the Administrator role can configure which types of folders can be created and which user role/roles are allowed to create secured folders. To configure these server-level settings for secured folders, see Configure Server for Folder Security.

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

Create Folders

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

Restrictions

- You cannot create a secured folder in a non-secured folder.
- You cannot create a non-secured folder in a secured folder.
- To create a subfolder in a secured folder, you must have manage privileges to the parent secured folder.
- Folder creation is restricted to the folder types specified by the server-level Folder Security settings.
- To create a secured folder, the user's *role* must have permissions granted by the server-level Folder Security settings.

For more information, see About Secured Folders.

To create a new folder

1. On the **Home** page, select a folder and click in the **Folder Details** pane.
2. In the Create Folder dialog, select a folder to serve as the parent folder. To create a folder at the root level, select **Folders**.
3. Click the button corresponding to the type of folder you want to create.
    - **New Non-Secured Folder**—Select to create a non-secured folder.
    - **New Secured Folder**—Select to create a secured folder.

    NOTE: If a button is disable, creation of that folder type is not allowed, either at the server level or in the selected parent folder. See the Restrictions listed above.
4. Enter a folder name and click **OK**.
5. (Secured folder only) After a secured folder is created, you can then modify the visibility (sharing) and manage privileges, if necessary. Initially, only the folder creator and users with the Administrator role have visibility and manage privileges to the folder. The folder creator is automatically listed under folder Managers. See Specify Visibility, Manage and Publish Privileges for Folders for more information.

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

Move Folders

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

Restrictions:

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

See About Secured Folders for more information about secured folders.

Delete Folders

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

To delete a folder

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

You cannot delete the ***No folder assigned*** folder.

View Folder Details

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

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

To view folder details

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

Detail	Description
Name	Folder name. For a secured folder, managers of the folder can rename the folder.
Creator	Folder creator. This is the name of the user who initially created the folder.
Visibility	(Secured folders) Displays the visibility (sharing) privileges for the selected folder. Managers can modify the visibility privileges. Click **Visibility** to open the Alter Folder Visibility dialog where you can modify visibility and manage privileges for the folder. See Specify Visibility, Manage and Publish Privileges for Folders for more information.
Managers	(Secured folders) Displays the list of users and groups with manage privileges for the selected folder. Managers can modify the visibility and manage privileges for the object. Click **Managers** to open the Alter Folder Visibility dialog where you can modify the manage privileges for the folder. See Specify Visibility, Manage and Publish Privileges for Folders for more information.

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

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

About Secured Folders

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

Secured Folder Characteristics

Secured folders have the following special characteristics:

- Secured folders have visibility, manage, and publish privileges assigned to them.
- The sharing and manage privileges specified for a secured folder are also applied to all objects in the folder.
- When an object is published to a secured folder, the object automatically inherits the visibility and manage privileges applied to the secured folder.

Why Use Secured Folders

The special characteristics of secured folders provide the following advantages:

- Object publishers can automatically define visibility and manage privileges for an object by publishing it to the desired folder. In this way, the task of specifying object privileges can be transferred from the individual user to a group of folder managers.
- A folder manager can change the visibility and manage privileges for all objects in a secured folder at one time by simply changing the privileges for the secured folder itself.

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

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

Server-Level Configuration

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

To learn how to configure the server settings for secured folders, see Configure Server for Folder Security.

Rules and Restrictions for Secured Folders

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

Visibility Privileges

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

Privileges Based on User or Role

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

Subfolder Privileges

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

Publishing

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

Creating and Moving Folders

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

Object Privileges

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

Moving and Deleting Secured Folders

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

Rules for Moving Objects into or out of a Secured Folder

- To move an object into a secured folder, the user must be an Administrator or have manage privileges to the object and the secured folder.
- If an object is moved into a secured folder, the object inherits the privileges of the secured folder, regardless of the object's original privileges.
- When an object is moved into a secured folder, the object publisher does not retain manage privileges unless the publisher is a *folder manager*.

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

Notifications of Secured Folder Activity

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

Specify Visibility, Manage and Publish Privileges for Folders

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

Specify Sharing Privileges

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

To alter Visibility for a secured folder

1. In the Web Console, click **Home**.
2. Select a secured folder to display details.
3. In the Folder Details pane, click **Visibility** to open the Alter Visibility dialog.
4. In the Alter Visibility dialog, select the users and groups with which you want to share the folder.
    - Add users and groups to the right pane. You can include both individual users and groups.
5. For each user (or group) specify manage and publish privileges.

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

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

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

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

Specify Manage and Publish Privileges

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

For more information about manage privileges, see Manager Privileges.

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

To modify Manage and Publish privileges for a secured folder

1. In the Web Console, click **Home**.
2. Select a secured folder to display folder details.
3. In the Folder Details pane, click **Managers** to open the Alter Visibility dialog.
4. In the Alter Visibility dialog, do the following:
    - Select the **Manage** check box for each user (or group) to which you want to grant Manage privileges.
    - Select the **Publish** check box for each user (or group) to which you want to grant Publish privileges.

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

- Modify the folder's sharing (visibility), manage, and publish options
- Rename or delete the folder
- Create a subfolder

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

Configure Server for Folder Security

Toad Intelligence Central provides two types of folders: secured folders and non-secured folders. An Intelligence Central server can use one type of folder exclusively, or use both types. This specification is made at the server level.

Only users with the Administrator role can configure folder security. Once the secured folder feature is enable for a server, the Administrator can then specify which user roles are allowed to create secured folders.

Secured folders are a special type of folder in Toad Intelligence Central. To learn more about secured folders and how to use them, please see About Secured Folders.

To specify folder security

1. In the Web Console, select **Administration | Server | Permissions**.
2. On the Folder Security page, specify the following options:

Allow creation of	Select one of the following: • **Secured folders only**—Select to allow users to create only secured folders. • **Non-secured folders only**—Select to allow users to create only non-secured folders. • **Both secured and non-secured folders**—Select to allow users to create both types of folders.
Who can create secured folders?	If creation of secured folders is allowed, select one of the following: • **Admins only**—Select to allow only users with the Administrator role to create secured folders. • **Admins and Power users**—If selected, only Admins and Power users can create secured folders. • **All users**—Select to allow all users to create secured folders. The restriction does not apply to non-secured folders. When non-secured folders are allowed, all users can create them.

10

Manager Privileges

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

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

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

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

Manager Privileges for Objects

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

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

Manager Privileges for Secured Folders

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

- Modify the folder's sharing (visibility), manage, and publish options
- Rename or delete the folder
- Create a subfolder

Who Can Manage Objects/Folders

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

Management Privileges to Objects

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

Management Privileges to Secured Folder

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

11

Reports

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

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

The following reports are provided:

- Data Object Usage Report
- User Activity Report

Data Object Usage Report

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

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

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

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

to see data for all publishers. Click a publishers name to filter the data grid by that publisher. Click a value to filter the data grid by that criteria.
6. To sort by a column in the data grid, click the column header.
7. To export the data in the data grid, click **Download CSV**.

User Activity Report

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

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

Landing Page

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

To filter the landing page

1. Select a time period from the **Active Users Over the...** drop-down list.
2. Then select the activity for which you want to view user statistics.
    - Select **Published** to view the most-active publishers.
    - Select **Consumed** to view the most-active consumers. Consumer activities include downloading files, downloading data objects, querying data objects from Toad Data Point, and running Automation scripts.

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

Other actions

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

Drill Down to Additional Data

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

To drill down to additional data

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

    On the TIC Active Users page, you can do the following:
    - Click a column header to sort the data grid by that column.
    - Click **Download CSV** to export the data to a .csv file.
    - Select a different time period from **Active Users Over the...**.
2. Click a user name to drill down to a list of the user's activities.
    - On the user's page, click a column header to sort the list by that column.
    - Click **Download CSV** to export the data to a .csv file.
3. Click a link in the breadcrumb navigation to go back to a previous page.

12

Health Check Dashboard

Run a health check on the Intelligence Central server to check for object integrity anomalies, current errors, and other object issues.

Users with the Administrator role can access the Health Check Dashboard page and its functionality.

From the Health Check Dashboard page you can do the following:

- View and repair existing data object anomalies
- View a summary of current errors
- Identify objects owned by an account that no longer exists or is no longer enabled
- Specify health check settings

Run a Health Check

To run a Health Check

1. In the Intelligence Central Web Console, select **Administration | Server | Health Check Dashboard**.
2. On the Health Check Dashboard page, click **Run Health Check**.
3. When the Health Check process is finished, select one of the following tabs to view the specific results and take action:
    - Data Integrity
    - Exceptions
    - Transfer Object Owner

Data Integrity

To view data integrity results and repair objects

1. Select **Administration | Server | Health Check Dashboard**. Click **Run Health Check**.
2. After the Health Check process finishes, the **Data Integrity** tab displays results of the Health Check.
    - If an object is found to have an anomaly, the object is listed along with details about the object, including a description of the impact to the user and a description of the solution.
    - Objects are grouped into categories, based on the type of anomaly found.

- If an unused temp table is found, it is listed in the *Unused Temp Table* category along with table details.

3. Tooltips provide descriptions for each category of anomalies. Place your cursor over the category issue count to display the description.
4. Review the **Impact** and **Solution** descriptions to determine which objects you want to repair.
    - Place your cursor over the description field to display the full text when a long description is truncated.
5. To repair objects, do one or more of the following:
    - To repair a single object, click **Repair** in the row for that object.
    - To delete an unused temp table, click **Repair** in the row for that table.
    - To repair all objects in a category, click the **Repair all issues** link for that category.
    - To repair all objects, click **Repair all** at the top of the tab/page.
6. If the repair process is successful, the object is removed from the report.
7. If the repair process is unsuccessful, an error message is displayed.

Exceptions

To view errors / exceptions

1. Select **Administration | Server | Health Check Dashboard**.
2. Select the **Exception** tab. To ensure the error information is up-to-date, click **Refresh**.
3. Objects with current errors are listed along with the error message and the time the last error occurred. For objects with consecutive errors, only the last error is displayed.
    - Objects are grouped by object type.
    - Object lists are sorted by error time. The latest error is at the top.

    An object is automatically removed from the list after a subsequent successful execution or download.
4. Click the object name to go to the object in the Home page. There you can find more information about the object, such as the execution logs for an Automation script. Use this information to help troubleshoot the issue.

    Intelligence Central can automatically send error alerts when a script execution or snapshot refresh fails. For more info about email notifications, including error alerts, see Email Notifications.

Transfer Object Owner

Use **Object Owner Transfer** tab to identify objects owned by an account that no longer exists or is no longer enabled in Intelligence Central. For example, a user account may no longer exist because the user is no longer in your organization. This tab allows you to transfer the objects owned by that user to a new owner.

To transfer object owner

1. Select **Administration | Server | Health Check Dashboard**. Click **Run Health Check**.
2. After the Health Check process finishes, select the **Object Owner Transfer** tab.
3. If a user account no longer exists or is no longer enabled in Intelligence Central, objects owned by that account are listed along with object details.
    - Objects are sorted by object owner (publisher).
    - Click the object name to go to the object in the Home page.

    > **NOTE:** This process does not identify objects in which the owner was removed using the **Remove User** action on the Users page of the Web Console (Administration | Users). When a user is removed, objects owned by the user are also removed. See Remove a User.
4. Review the list and the object descriptions.
5. To transfer an object to another owner, click **Transfer to new owner** in the row for that object.
6. To transfer all objects, click **Transfer all to new owner**.
7. In the **Transfer to** dialog, select a user to serve as the object's new owner. Click **OK**.
8. If the transfer is successful, a success message is displayed and the object is removed from the report.
9. If the transfer is not successful, an error message is displayed.
10. New owner visibility and manage privileges to the object are dependent on the folder type.
    - **Non-secured folder**—If the object is in a *non-secured* folder, the new owner is granted visibility and manage privileges to the object as the object owner.
    - **Secured folder**—Secured folder privileges override object privileges. If the object is in a *secured* folder, the folder's visibility and manage privileges apply to the object. To see the object, the folder must be shared with the new owner. The new owner must be a folder manager to have manage privileges to the object. See About Secured Folders for more information.

      To ensure the new owner has visibility or manage privileges, review the folder's privileges in the Folder Details pane and modify if necessary.
11. Upon successful transfer of the object, the new owner is notified by email.

Specify Settings

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 settings:
    - **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).
    - **Email Admin when health check auto run results in issues**

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 Email Notification Settings for more information.

13

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.

14

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

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 Toad Intelligence Central 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.

NOTE: If you upgraded from Intelligence Central 3.2 (or earlier), the Toad Intelligence Central data folder could be located here: 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

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.

> **NOTE:** If you upgraded from Intelligence Central 3.2 (or earlier), the Toad Intelligence Central data folder could be located here: 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 2026 R1 can only be restored to Toad Intelligence Central 2026 R1. It cannot be restored to Toad Intelligence Central 2026 R2. 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.

NOTE: Restore to the same version of Toad Intelligence Central as the backup. For example, a backup from Toad Intelligence Central 2026 R1 can only be restored to Toad Intelligence Central 2026 R1. It cannot be restored to Toad Intelligence Central 2026 R2.

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

NOTE: If you upgraded from Intelligence Central 3.2 (or earlier), the Toad Intelligence Central data folder could be located here: 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.

NOTE: If you upgraded from Intelligence Central 3.2 (or earlier), the Toad Intelligence Central data folder could be located here: 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 Kestrel section to the Toad Web Server appsettings.json file. 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 Kestrel section to the Toad Web Server configuration file.
    a. Locate the Toad Web Server installation directory. The default path is: C:\Program Files\Quest Software\Toad Intelligence Central\webserver.
    b. In this directory, open appsettings.json in an editor, such as Notepad.
    c. Add Kestrel section using the following format:

```
"Port": 8080,
"Kestrel": {
"EndpointDefaults": {
"SslProtocols": ["Tls12", "Tls13"]
},
"Certificates": {
"Default": {
"Path": "C://MyCert//exportCert.pfx",
"Password": "123"
}
}
}
}
```

    NOTE: **Path** is for the full path of the pfx file. **Password** is for the password when export the certificate to the pfx file. The example above adds an https binding on port 8080, uses the certificate file - *C://MyCert//exportCert.pfx* , the Password for this certificate is **123** .
3. Start 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 Start.

NOTE:

"ERR_HTTP2_INADEQUATE_TRANSPORT_SECURITY" error is encountered in Google Chrome browser when connecting to Web Server via HTTPS

Troubleshooting:

- In C:\Program Files\Quest Software\Toad Intelligence Central\webserver\ open appsettings.json using any text editor (administrator privileges are required to edit this file)
- Update kestrel section in appsettings.json file with following:

```
"Kestrel": {
 "EndpointDefaults":
 { "Protocols": "Http1",
 "SslProtocols": ["Tls12", "Tls13"]
 }
```

- After saving appsettings.json please restart Toad Web Portal (ToadIntelligenceCentralWebServer) service through Task Manager or Services Management Console

Configure Toad Intelligence Central for SSO Authentication

Toad Intelligence Central requires additional configuration for Single Sign-On authentication and registration. The setup is dependent on the specific Corporate Identity Provider that is being used.

Corporate Identity Providers supported in Toad Intelligence Central

Toad Intelligence Central currently supports Microsoft Entra ID for Single Sign-On autentication.

Microsoft Entra ID

To enable Single Sign-On (SSO) with **Microsoft Entra ID**, you must register Toad Intelligence Central (TIC) as an application in your organization's identity provider tenant. This registration establishes trust between TIC and Entra ID and enables secure authentication and user synchronization.

Prerequisites

Before registering the application, ensure the following:

- Toad Intelligence Central is configured to use **HTTPS**. For more details about setting up Toad Intelligence Central for HTTPS, see the **Configure Web Server for HTTPS**.

- You have sufficient permissions in Entra ID to register applications, for example, the **Application Administrator** or **Global Administrator** role.
- The TIC server URL and intended callback path are defined.

Required Configuration on the Microsoft Entra ID Portal

Application Registration Requirements

When registering the Toad Intelligence Central application in the Entra ID portal, configure the following settings:

1. **Application Name**
    - Provide a recognizable display name for the application, for example, **Toad Intelligence Central.**
    - This name is used for identification within the Entra ID portal.
2. **Supported Account Types**
    - Select the account types that will be allowed to authenticate.
3. **Redirect URI**
    - Select **Public client/native (mobile & desktop)** as the platform.
    - Specify a redirect URI that points to the TIC server endpoint responsible for handling authentication responses, also known as the callback path, in the following format:

      `https://<tic-server-host>/<callback-path>`
    - Example:

      `https://tic-server.company.com/signin-oidc`
    - This endpoint is used by Entra ID to return the authentication code to TIC.

Additional Redirect URI Configuration

After registration, additional redirect URIs need to be configured under **Authentication | Redirect URI configuration**:

- Configure the redirect URI that will be used for SSO provider, Entra ID, authorization when connecting to Toad Intelligence Central from Toad Data Point and Toad Workbook in the following format:

  `http://localhost:<port>`

  The recommended port range is **49152–65535**. Ensure that the selected port is not used by another application.
- **Multiple TIC environments** optional:
    - Add additional redirect URIs for each TIC server instance as needed.

Client Credentials

The following step is to add a client secret that will be used to authenticate Toad Intelligence Central on Microsoft Graph API. This allows the import and synchronization of Entra ID users and groups to TIC.

Client Secret

- Create a client secret under **Certificates & secrets**.
- Store the **Value** securely immediately after creation.
- This value is required for TIC configuration.

Application Identifiers

From the application **Overview** page, record the following values:

- **Tenant ID** – Identifies your Entra ID directory.
- **Client ID** – Identifies the registered TIC application.

These values should be stored securely along with the Client Secret. They are also required for configuring SSO in TIC.

API Scope Configuration

To ensure authentication tokens are issued specifically for TIC:

- Define a **custom API** scope under **Expose an API**.
- Use the suggested Application ID URI or define a custom one.
- Create a scope name that will later be referenced in TIC configuration.

This step ensures that access tokens are issued with TIC as the intended audience, rather than default Microsoft services.

API Permissions

To enable user and group synchronization from Entra ID:

1. Navigate to **API permissions** > **Add a permission**.
2. Select **Microsoft Graph**.
3. Choose **Application permissions**.
4. Add the following permissions:
    - `User.Read.All`
    - `Group.Read.All`
    - `GroupMember.Read.All`
5. Grant admin consent after adding the permissions.

These permissions allow TIC to read users, groups, and group memberships required for synchronization.

Required Setup on the Machine that Hosts the Toad Intelligence Central Server

To enable Single Sign-On (SSO) authentication using **Microsoft Entra ID**, you must configure Toad Intelligence Central (TIC) on the server by defining OpenID Connect settings in a configuration file.

Configure SSO Settings File

On the TIC server machine, create or update the following configuration file:

```
%ProgramData%\Quest Software\Toad Intelligence Central\appserver\ssosettings.json
```

Add the OpenID Connect configuration in the following format:

```
{
        "OpenIdConnectSettings": {
        "Authority": "https://login.microsoftonline.com/<tenant_id>/v2.0",
        "ClientId": "<client_id>",
        "CallbackPath": "/<callback_path>",
        "Scope": "openid offline_access profile email api://<client_id>/<scope_
name>",
        "DesktopRedirectUri": "http://localhost:<port>/",
        "ProviderName": "EntraID"
                                }
 }
```

Configuration Properties

Configure each property as described below:

Authority

- Specifies the identity provider endpoint used to obtain tokens.
- Retrieve this value from the OpenID configuration endpoint:

  `https://login.microsoftonline.com/<tenant_id>/v2.0/.well-known/openid-configuration`
- Use the **issuer** value from the response.

ClientId

- The Application Client ID from the registered TIC application in Entra ID.

CallbackPath

- The callback path defined during application registration in Entra ID.
- This endpoint is used by TIC to receive the authentication response.

Scope

Defines the permissions requested during authentication. Include:

- `openid` – Required for authentication.
- `offline_access` – Enables token refresh.
- `profile` – Retrieves user profile information.
- `email` – Retrieves user email.
- `api://<client_id>/<scope_name>` – Custom API scope defined during app registration.

DesktopRedirectUri

- Must match the redirect URI configured in Entra ID for desktop clients:
  `http://localhost:<port>/`
- Use a port in the recommended range **49152–65535**.
- Ensure the selected port is:
  - Not in use by another application.
  - Accessible from client machines, for example, Toad Data Point or Toad Workbook.

ProviderName

- Specifies the external identity provider.
- Must be set to: `EntraID`
- Do not modify this value.

Apply Configuration Changes

After saving the `ssosettings.json` file:

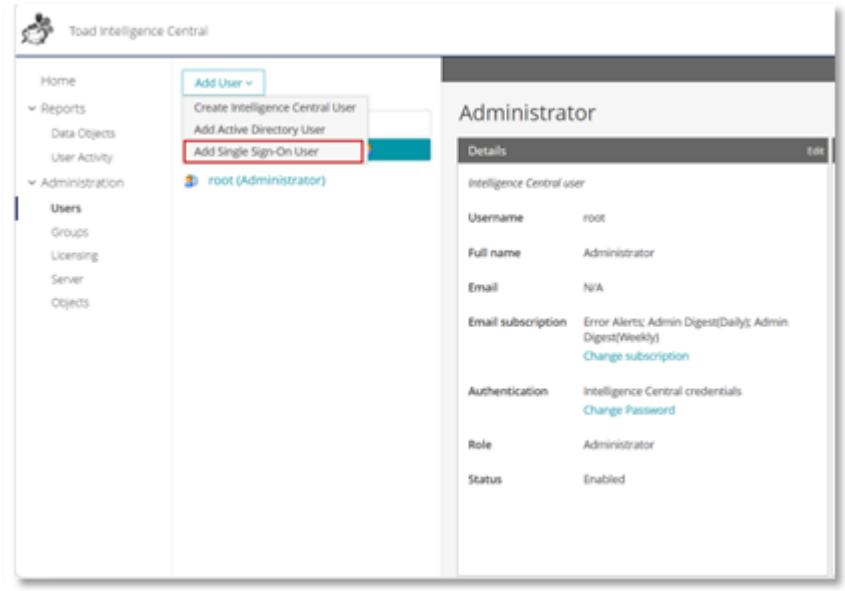
1. Open **Windows Services**.
2. Restart the **ToadApplicationServer** service.
   - This automatically restarts the **Toad Web Portal** service.

Once the service is restarted, TIC is configured to use SSO authentication.

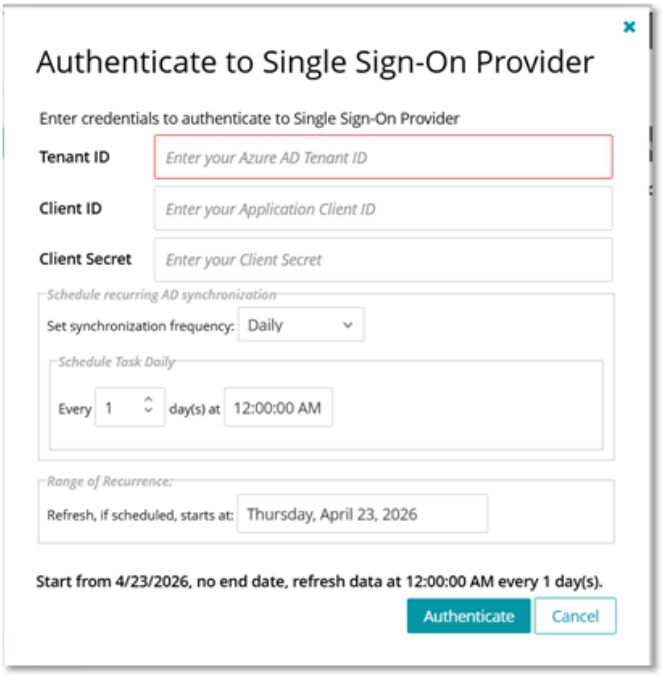
Configure SSO in the TIC Web Interface

To complete the setup:

1. Log in to TIC as an administrator.
2. Navigate to **Users** > **Add Single Sign-On User**.



3. In the authentication dialog, provide the following values:
   - **Tenant ID**
   - **Client ID**
   - **Client Secret**
4. Configure synchronization frequency and click **Authenticate**.



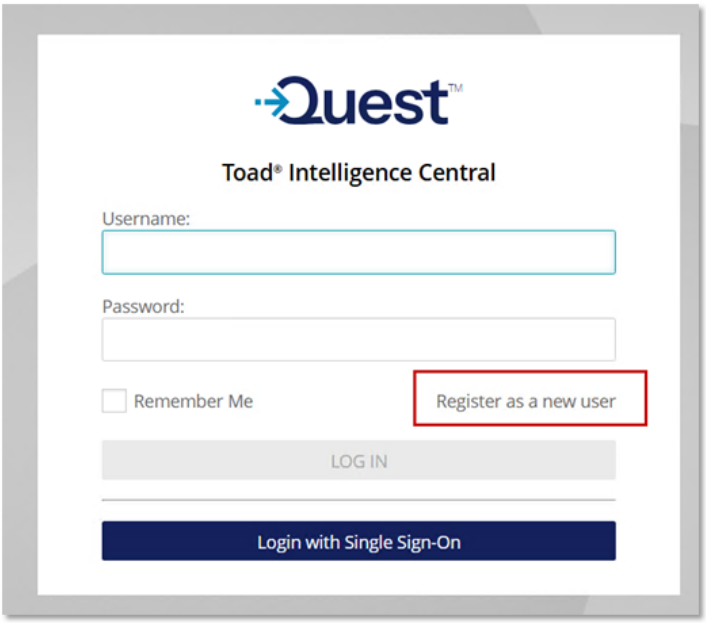
After successful authentication:

- Users and groups can be imported from Entra ID.
- Synchronization settings are available under **Server** > **Settings**.

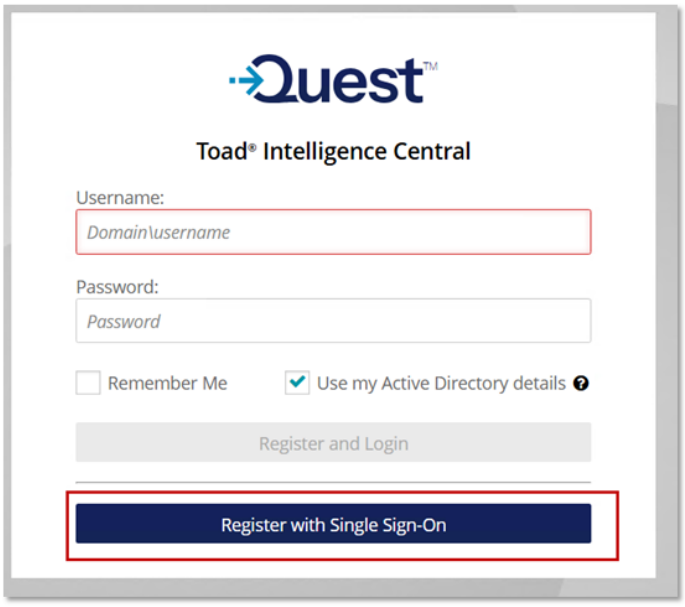
Self-Registration Workflow

Users can register using SSO from the TIC login page:

1. Select **Register as a new user**.



2. Click **Register with Single Sign-On**.



3. Complete authentication via Entra ID.

NOTE:

- SSO users can be assigned roles and fully interact with TIC, including running objects.
- SSO user accounts cannot be configured as default credentials for running Automation Scripts and Workbooks.

  This capability is currently supported only for Active Directory users.

15

Upgrade Toad Intelligence Central

To upgrade, run the Toad Intelligence Central installer.

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 5.0 from version 4.3 or 3.3 has been tested and is supported.

NOTES:

- The Toad Intelligence Central Data folder stores user information, data source connection information and mappings, snapshots and datasets. This folder might be affected by the upgrade (file contents and table schemas may be changed in new version). See Toad Intelligence Central Data Folder for more information.
- Backup your data folder before upgrade in case you needed to roll back to the previous version because of any upgrade failures.
- Beginning with version 5.1.3 you can use the upgrade wizard of Toad Intelligence Central to back up the data folder for you automatically. When an upgrade fails, TIC will auto rollback both the application and data folder.
- Remove the backup data folder when you do not need it anymore. Toad Intelligence Central will not remove it automatically.
- 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 Toad Intelligence Central data folder could be located here: 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.

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 2026 R2**

   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 Toad Intelligence Central data folder could be located here: ProgramData\Dell\Toad Intelligence Central.

   See Toad Intelligence Central Data Folder for more information.
3. Install Toad Intelligence Central 2026 R2 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 2026 R2 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.

   NOTE: A known issue on connecting to Toad Intelligence Central 2026 R2 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 2026 R2 (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.

16

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.

> **NOTE:** If you upgraded from Intelligence Central 3.2 (or earlier), the Toad Intelligence Central data folder could be located here: ProgramData\Dell\Toad Intelligence Central.

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

About Us

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

Contact Quest

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

Technical Support Resources

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

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

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