



# User Guide

## Table of Contents

Table of Contents .....	2
I'm an administrator and need to install and configure Application Manager ....	6
Apps Dashboard .....	17
Configuration Wizard .....	19
Downloads .....	24
I'm a new user and want to learn the basics of Application Manager .....	25
Application Resources .....	26
Application Tokens .....	27
Overview of User Roles and User Access .....	29
Register New User .....	30
User Sign In .....	32
Reset Password .....	34
Security .....	35
Authentication .....	36
Configure Portal for ArcGIS .....	38
No Security .....	44
Built In Security .....	45
Windows Security .....	46

Security Token Service .....	47
Configure TDS with Azure AD .....	51
OpenID Connect .....	59
Roles .....	61
Role Privileges .....	64
Description of Access Levels .....	67
App Restrictions .....	68
Profile Restrictions .....	70
Templates .....	72
Users and User Roles .....	76
Map User Claims .....	79
Security Settings .....	80
Access Tokens .....	86
Databases .....	89
Configuration Store .....	90
Data Sources .....	95
LRS Metadata .....	103
Import Seed Data .....	106
Export Seed Data .....	107
Editing Seed Files .....	108
Domains .....	109

Profiles .....	115
Support .....	117
Server Logs .....	118
Web Service Tool .....	121
Settings .....	122
Mail Server .....	123
Licensing .....	124
General Server Settings .....	125
SQL Command Settings .....	131
File Path Settings .....	136
Load Balancer File Path Settings .....	138
Scheduling Service Settings .....	142
Applications .....	145
Installed Applications .....	146
Application Profiles .....	148
Application Settings .....	150
Publishing ESRI Service Definition Files .....	156
Integrations .....	159
Actions .....	163
I'm seeking to expand my knowledge of Application Manager .....	165
Advanced Configurations .....	166

Setting Up Configuration Store Permission .....	172
Application Architecture .....	177
Application Security .....	182
Installation Errors .....	183
Installing TDS to a new (non-default) Website in IIS .....	188
Manual Installation .....	192
Options and Silent Installs .....	194
Scalability and Performance .....	196
WCAG and 508 Compliance .....	201
Services API Reference .....	202
Frequently Asked Questions (FAQs) .....	203



# I'm an administrator and need to install and configure Application Manager

Take a look at the following to install and set up Application Manager and your other Rizing Geospatial applications in a flash.

## Installation Requirements

---

Please review and familiarize yourself with the following requirements below prior to installation.

Review the [Application Architecture](#) requirements and recommendations.

Requirements:

### System Requirements

.NET 4.7.2 (or higher)

[.NET 4.7.2 Download](#)

Windows Server 2012 (or higher)

[Windows Server Documentation](#)

Internet Information Services 8.5 (or higher)

[The Official Microsoft IIS Site](#)

### User Requirements

Modern web browser

Chrome

Firefox

Safari

Edge

IE 11+

### Software Requirements

	No ESRI		ESRI Software				
Products	An LRS	Database Connection	ArcGIS Server	Roads & Highways	ESRI Geodatabase	ArcGIS Desktop	Rizing Software

Web	HPMS Assistant	Required	Required	Optional	Optional	Optional		TDS, SA, VA
	Job Execution Manager			Optional	Optional	Optional		
	MAVRIC			Optional	Optional	Optional		TDS
	Report Engine		Required					TDS
	Road Analyzer	Required		Required	Optional	Optional		TDS, RE (for printing)
	Road Video Viewer	Required						TDS
	Segment Analyzer	Required	Required	Optional	Optional	Optional		TDS
	Validation Assistant	Optional	Required	Optional	Optional	Optional		TDS
Desktop	Intersection Manager	Required	Required		Optional		Required	

**Note:** Depending on what products you will be installing, and running, a map service may be required to be published through ArcGIS Server and accessible from applications to consume data through the map service – see “[Data Sources](#)” for more information on configuring the map service URL.

#### ArcGIS Product Version Compatibility

ArcGIS Version	Web						Desktop
	Road Analyzer	Segment Analyzer	Validation Assistant	HPMS Assistant	Report Engine	Road Video Viewer	Intersection Manager
Pro 2.8	Supported	Supported	Supported	Supported	Supported	Supported	TBD
Pro 2.9	Supported	Supported	Supported	Supported	Supported	Supported	TBD
Pro 3.0	Supported	Supported	Supported	Supported	Supported	Supported	TBD
Enterprise 10.9	Supported	Supported	Supported	Supported	Supported	Supported	TBD
Enterprise 10.9.1	Supported	Supported	Supported	Supported	Supported	Supported	TBD
Enterprise 11.0	Supported	Supported	Supported	Supported	Supported	Supported	TBD
Enterprise 11.1	Supported	Supported	Supported	Supported	Supported	Supported	TBD

<b>Compatible</b>	The product is no longer fully supported against this version, but is likely still compatible. Rizing Geospatial does not offer any guarantee of compatibility.
<b>Supported</b>	The product is tested and fully functional. Product modifications will be made if an incompatibility is discovered.
<b>Not Supported</b>	The product is not compatible.
<b>*Not Supported</b>	The product is under development and may become compatible in the future.
<b>**Not Supported</b>	The product is not compatible due to an ESRI defect that was fixed in a later version.

### ArcGIS Desktop Compatibility

**Note:** You can not publish a map service from desktop to ArcGIS Enterprise past 10.8.1.

Version	Web						Desktop
	Road Analyzer	Segment Analyzer	Validation Assistant	HPMS Assistant	Report Engine	Road Video Viewer	Intersection Manager
ArcGIS 10.2	Compatible	Compatible	Compatible	Compatible	Compatible	Compatible	Not Supported
ArcGIS 10.2.1	Compatible	Compatible	Compatible	Compatible	Compatible	Compatible	Not Supported
ArcGIS 10.3	Compatible	Compatible	Compatible	Compatible	Compatible	Compatible	Compatible
ArcGIS 10.3.1	Compatible	Compatible	Compatible	Compatible	Compatible	Compatible	Compatible
ArcGIS 10.4	Compatible	Compatible	Compatible	Compatible	Compatible	Compatible	Compatible
ArcGIS 10.4.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported
ArcGIS 10.5.0	Compatible	Compatible	Compatible	Compatible	Compatible	Compatible	**Not Supported
ArcGIS 10.5.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported
ArcGIS 10.6.0	Supported	Supported	Supported	Supported	Supported	Supported	Supported
ArcGIS 10.6.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported
ArcGIS 10.7.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported
ArcGIS 10.8.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported
ArcGIS 11.1	Supported	Supported	Supported	Supported	Supported	Supported	Supported



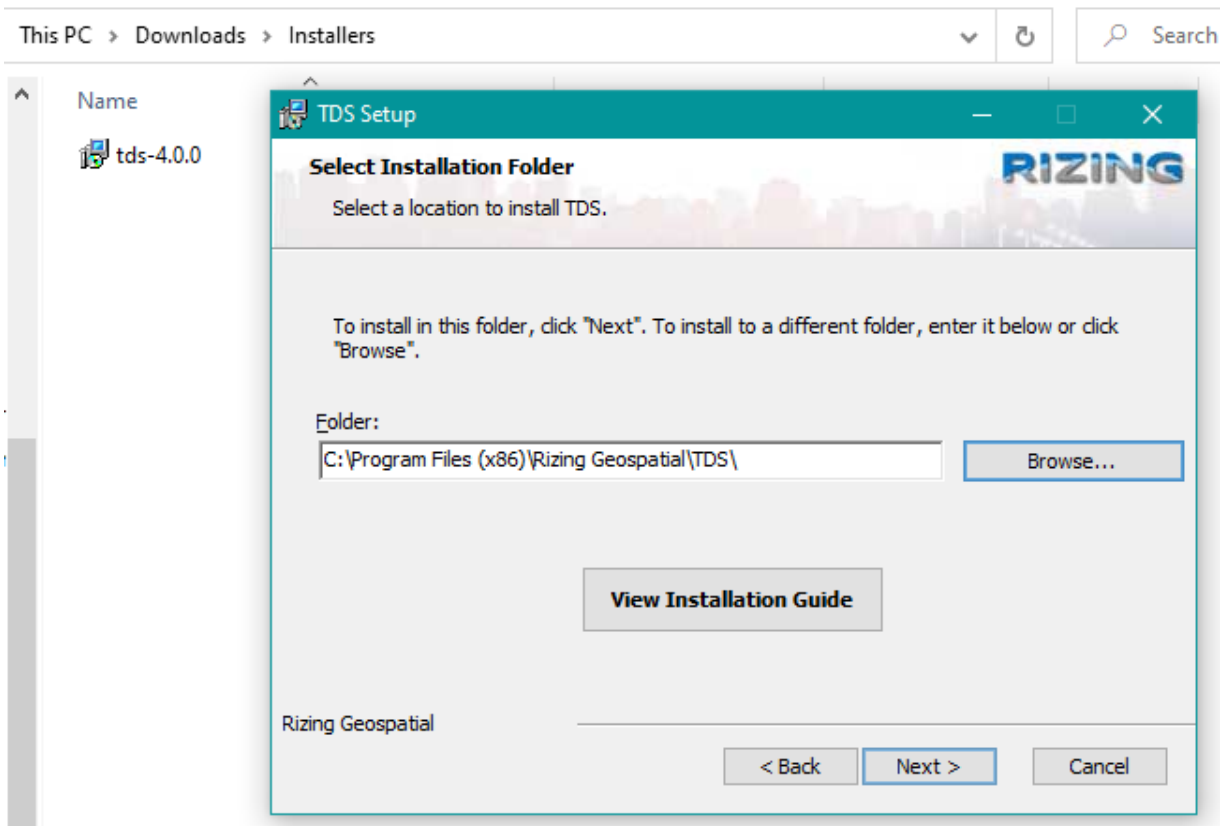
<b>Compatible</b>	The product is no longer fully supported against this version, but is likely still compatible. Rizing Geospatial does not offer any guarantee of compatibility.
<b>Supported</b>	The product is tested and fully functional. Product modifications will be made if an incompatibility is discovered.
<b>Not Supported</b>	The product is not compatible.
<b>*Not Supported</b>	The product is under development and may become compatible in the future.
<b>**Not Supported</b>	The product is not compatible due to an ESRI defect that was fixed in a later version.

## For New Installations

Follow the installation steps below to install TDS (App Manager) and our web applications.

### 1. Run the TDS (App Manager) Installer

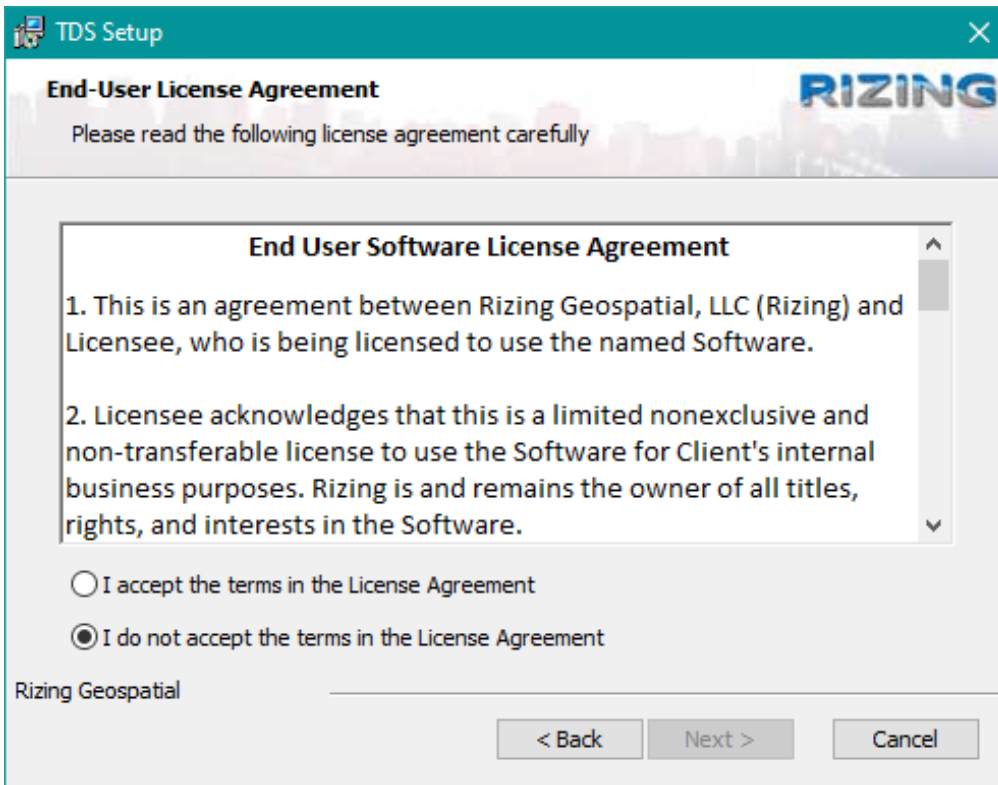
Double click the **installer** to run it. The TDS installer will be named tds-<version> (ex: tds-3.9.0). Then browse to the location you wish to install TDS and click **Next**.



**Tip:** Clicking **View Installation Guide** will bring up this topic in the User Guide.

## 2. Agree to the End-User License Agreement

Read and agree to the license agreement then click **Next**.



The screenshot shows a dialog box titled "TDS Setup" with a close button (X) in the top right corner. The main heading is "End-User License Agreement" with the "RIZING" logo to the right. Below the heading is the instruction "Please read the following license agreement carefully". A scrollable text area contains the "End User Software License Agreement" with two numbered points:

1. This is an agreement between Rizing Geospatial, LLC (Rizing) and Licensee, who is being licensed to use the named Software.
2. Licensee acknowledges that this is a limited nonexclusive and non-transferable license to use the Software for Client's internal business purposes. Rizing is and remains the owner of all titles, rights, and interests in the Software.

Below the text area are two radio button options:

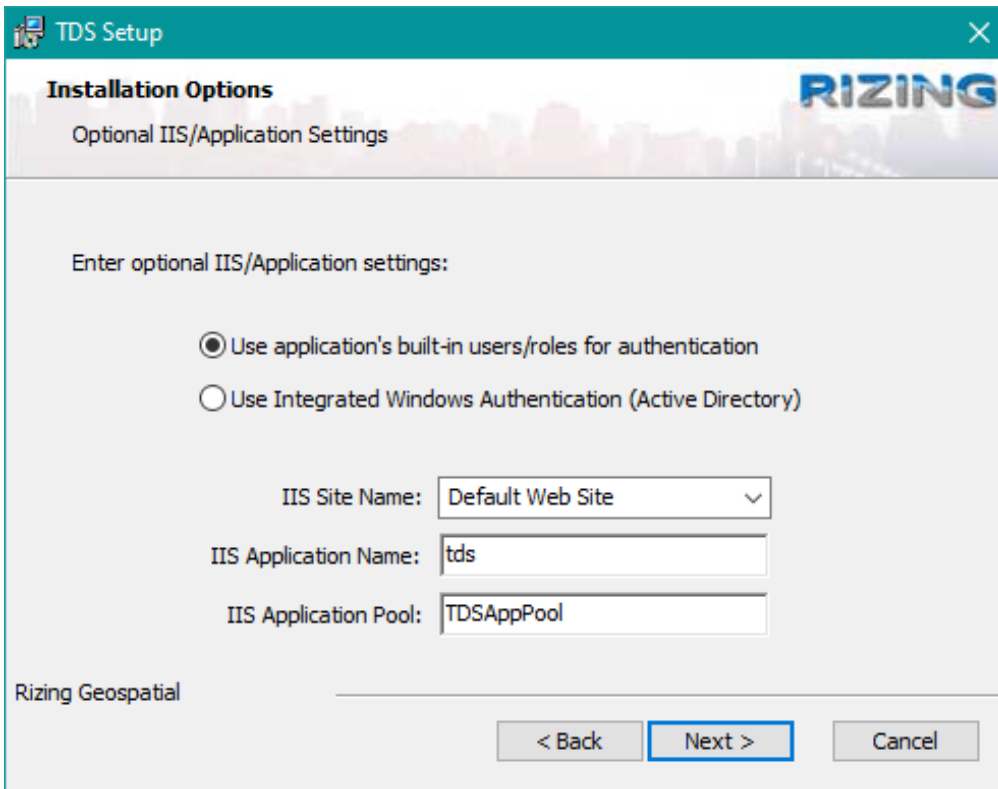
- I accept the terms in the License Agreement
- I do not accept the terms in the License Agreement

At the bottom left, the text "Rizing Geospatial" is followed by a horizontal line. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

**Note:** You can preview the license agreement [here](#).

## 3. Select your authentication method

Choose your authentication method and rename the IIS (Internet Information Services) Site, Application and/or Application Pool if desired then click **Next**. An overview of each option is outlined below.



Selecting **Use application's built-in users/roles for authentication** will allow you to register and create user roles that will be stored in the applications database.

Selecting **Use Integrated Windows Authentication (Active Directory)** will allow you to use Active Directory users/roles across your applications.

**IIS Site Name:** leave default or enter a new name. This is set to Default Web Site ("WEBAPP") by default.

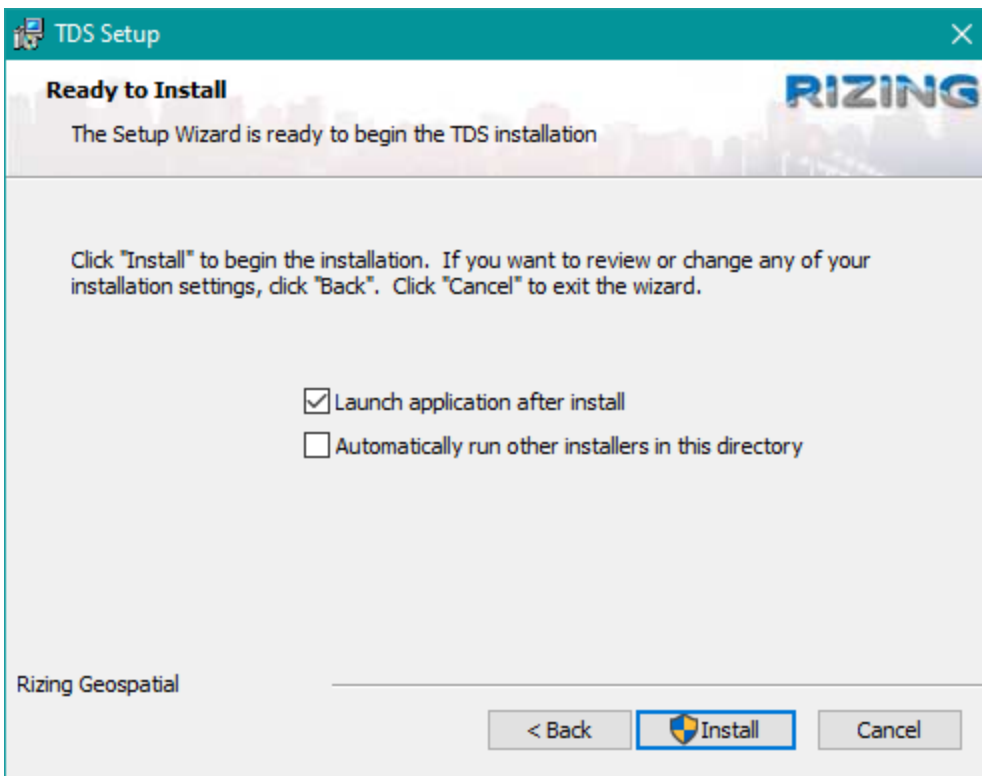
**IIS Application name:** leave default or enter a new name. This is set to tds by default.

**IIS application pool:** leave default or enter a new pool. This is set to TDSAppPool by default.

**Note:** *Recommended:* Leave **Launch application after install** checked to launch App Manager once installation is complete.

#### 4. Install the application

If you'd like the installer to install all other Rizing Geospatial web applications located in the selected installation directory (or sub-directories), select the option to **Automatically run other installers in this directory**. Otherwise, click **Install** to run the TDS installation.



Once you click Install, a series of confirmation prompts will open. Click **OK** to confirm each prompt.

The application should now load in your default browser window if **Launch application after install** was left checked.

#### 5. Run Application Installer(s)

Repeat steps 1-3 above for each web application installer.

**Tip:** While this step is not required, it will make the configuration process in App Manager go more smoothly if all of the applications are installed prior to running through the Configuration Wizard.

#### 6. Run the App Manager Configuration Wizard

**Tip:** This is the quickest and easiest way to get started with App Manager. The Configuration Wizard will walk you through importing your seed data file (if we provided you one) and all the core configuration settings needed to get up and running with all of our web applications.

Further detailed information on the underlying web application framework that App Manager sits on top of, including additional installation guidelines and technical specifications, see the [Expanding Knowledge](#) section.

### Updating an Existing Installation

---

**Heads Up!** Rizing recommends that you install the latest versions of each product as it is released. If support is requested related to a bug that has been fixed, Rizing requires that the software be updated to the most recent version before continued support related to that bug can be provided.

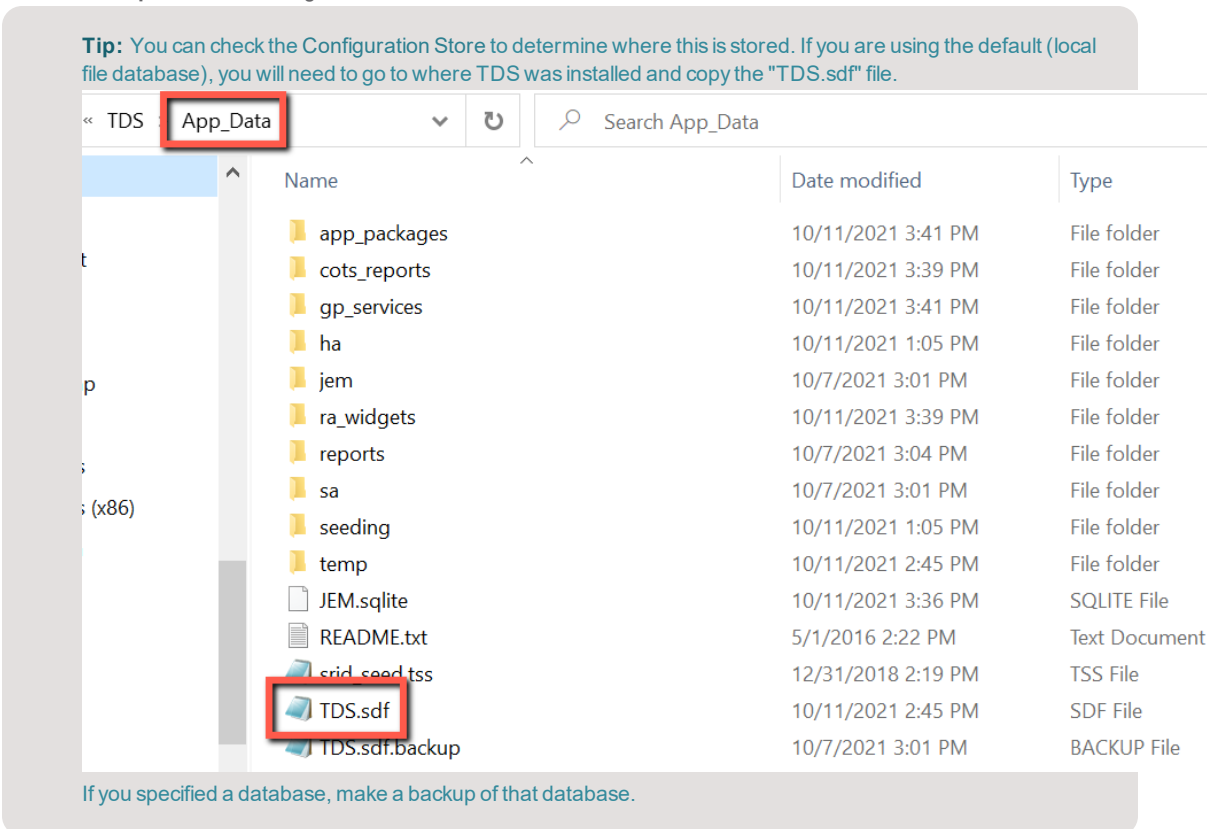
To update the application, simply run the new installer and the previous application version will automatically be updated to the new one. Create a backup of the configuration store database prior to upgrading any software.

### To upgrade the application in a replicated environment (behind a load balancer)

When upgrading software in a replicated environment (multiple machines running TDS), the following steps should be taken:

1. Make a **backup** of the TDS configuration store database.

**Tip:** You can check the Configuration Store to determine where this is stored. If you are using the default (local file database), you will need to go to where TDS was installed and copy the "TDS.sdf" file.



Name	Date modified	Type
app_packages	10/11/2021 3:41 PM	File folder
cots_reports	10/11/2021 3:39 PM	File folder
gp_services	10/11/2021 3:41 PM	File folder
ha	10/11/2021 1:05 PM	File folder
jem	10/7/2021 3:01 PM	File folder
ra_widgets	10/11/2021 3:39 PM	File folder
reports	10/7/2021 3:04 PM	File folder
sa	10/7/2021 3:01 PM	File folder
seeding	10/11/2021 1:05 PM	File folder
temp	10/11/2021 2:45 PM	File folder
JEM.sqlite	10/11/2021 3:36 PM	SQLITE File
README.txt	5/1/2016 2:22 PM	Text Document
grid_seed.tss	12/31/2018 2:19 PM	TSS File
<b>TDS.sdf</b>	10/11/2021 2:45 PM	SDF File
TDS.sdf.backup	10/7/2021 3:01 PM	BACKUP File

If you specified a database, make a backup of that database.

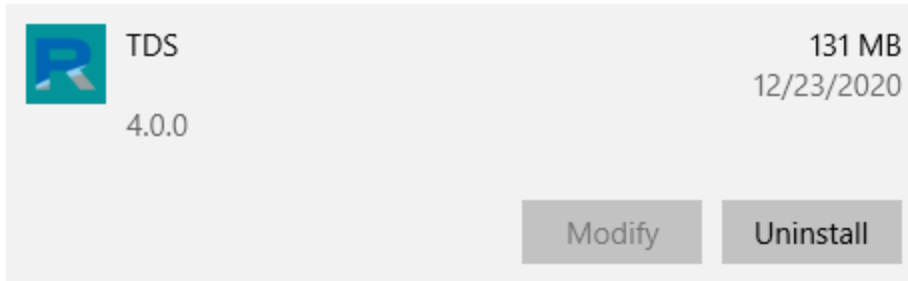
2. In IIS Manager, **stop the application pool** for each replicated instance.

**Note:** The default TDS app pool is TDSAppPool.

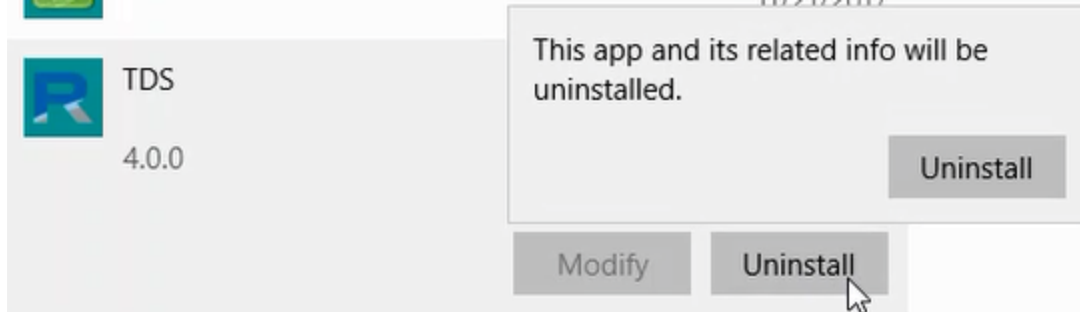
3. **Install** the latest applications (run all installers) on one of the replicated servers.
  - a. **Repeat** this steps for each of the replicated servers.
  - b. Test each server independently and then test access through the load balancer (once all servers have been brought back online).

### To uninstall the application

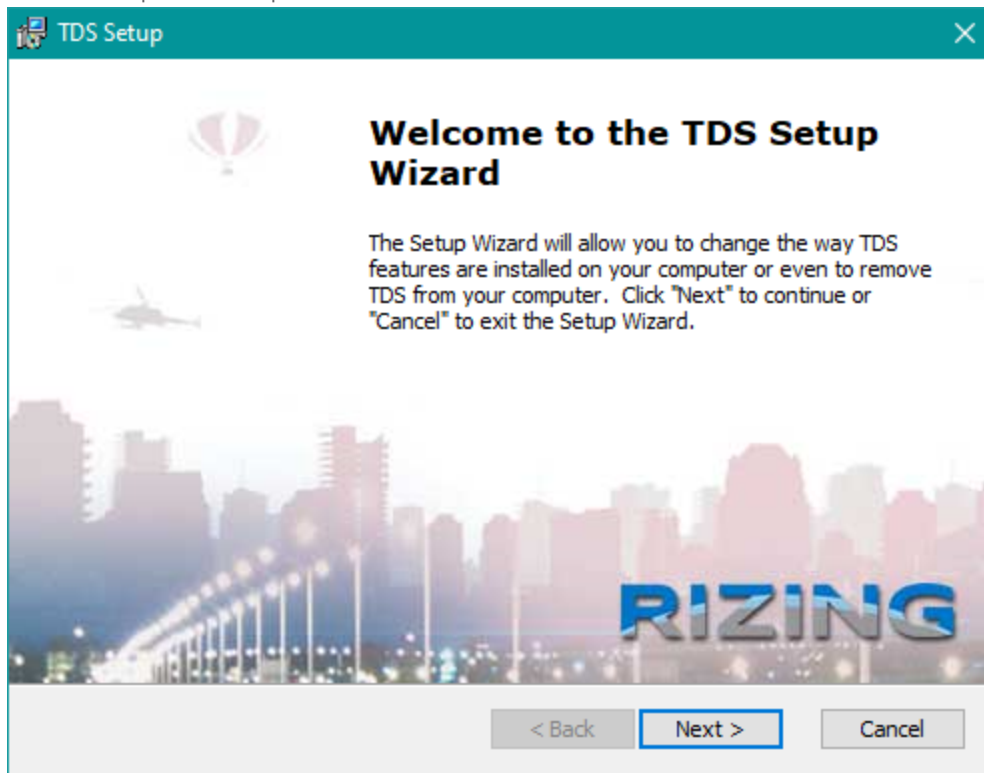
1. Navigate to Programs and select **Uninstall** for TDS.



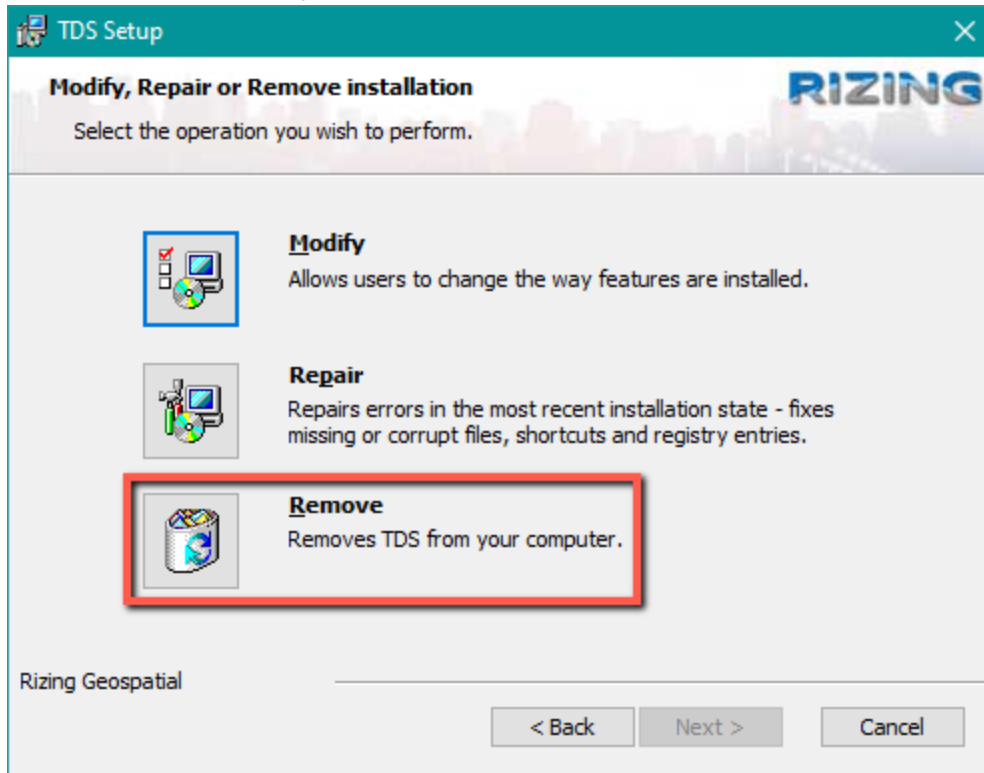
2. Click **Uninstall** on the confirmation popup.



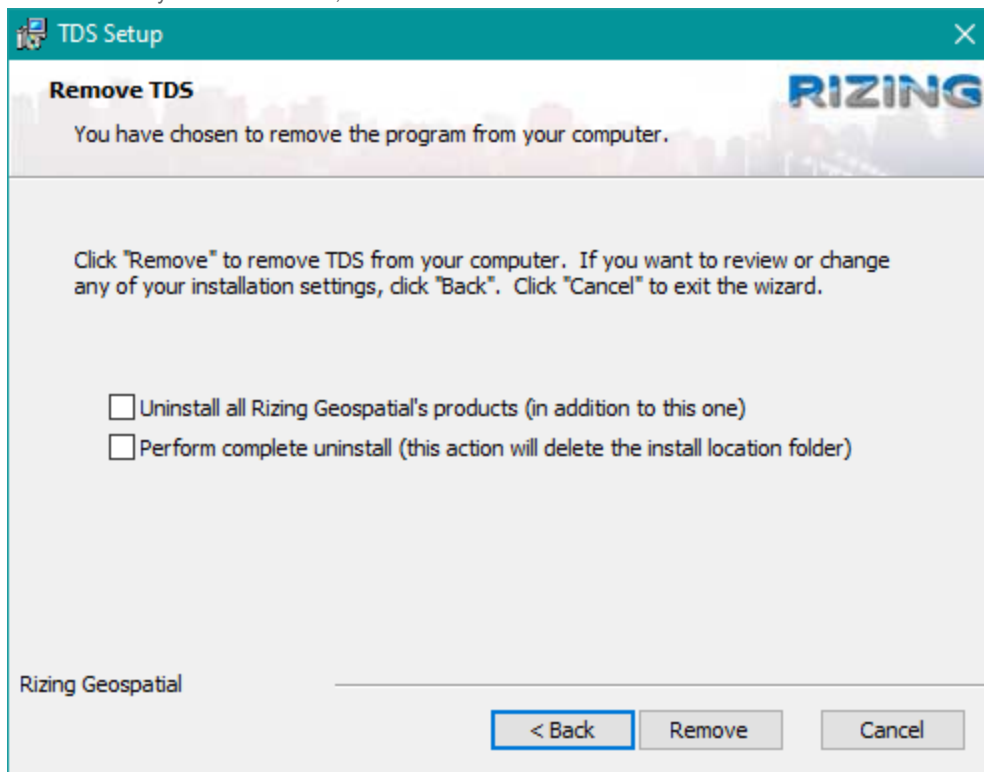
3. The TDS Setup Wizard will open. Click **Next**.



4. Select **Remove** from the list of options then click **Next**.



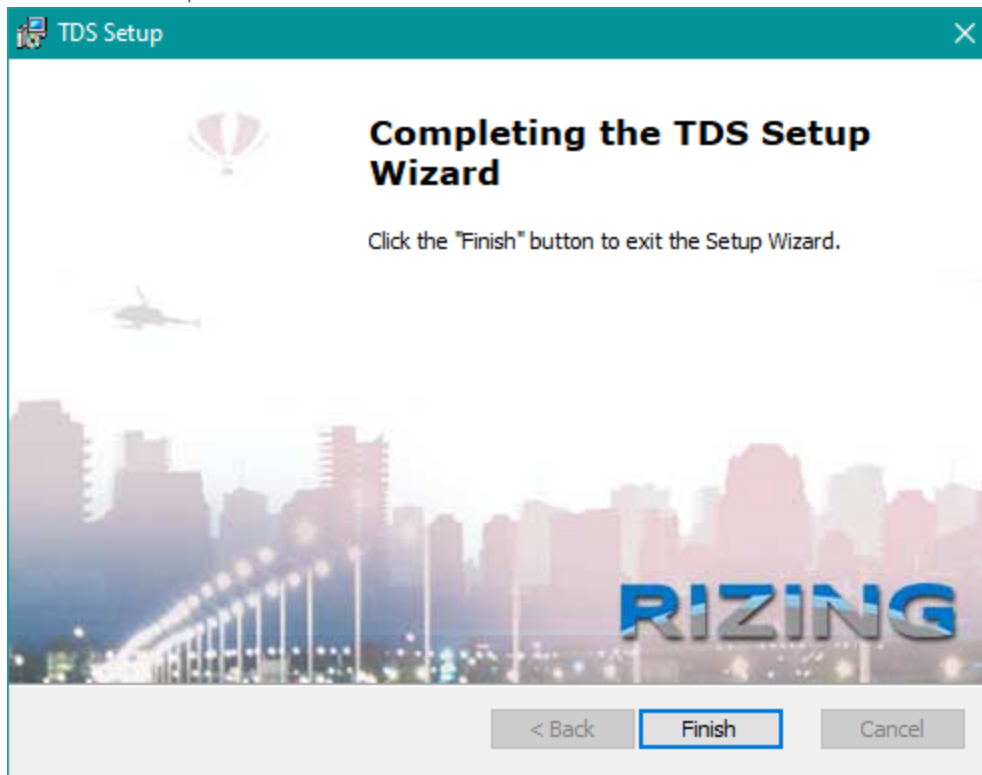
5. Select the items you wish to remove, then click **Remove**.



To uninstall all Rizing Geospatial products, select **Uninstall all Rizing Geospatial's products (in addition to this one)**.

To automatically remove the TDS folder (including any data or files/folders contained therein) after uninstalling, select **Perform complete uninstall (this action will delete the location folder)**

6. Click **Finish** to complete the uninstall.



**Note:** The application installer will automatically make a copy of the application's web.config and configuration database (if it is using SQL Server Compact) before performing the upgrade. If you are not running a standard configuration, backup your files manually.

**Heads Up!** Whenever a product installer is run, the application will automatically be taken offline. If you are not running a standard configuration, manually take the application offline. This will ensure it is not accessible to the public which could interfere with the installation process.

## Google Maps and Bing Maps API Disclaimer

---

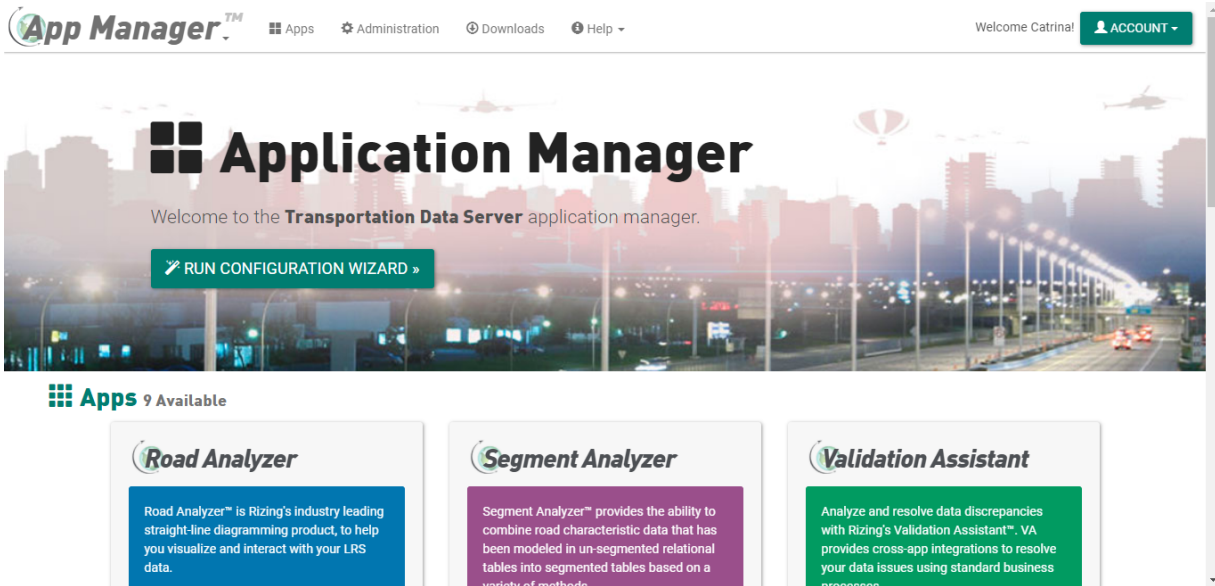
Google Maps: All Google Maps JavaScript API applications are subject to the limitations of Google's [Terms of Service](#). Therefore to use any imbedded Google Map tools within the applications, you will need to adhere to Google's [Terms of Service](#) - this typically means you need to purchase an enterprise license. To learn more please visit Google Maps' [Get a Key/Authentication](#) page.

Bing Maps: Using the Bing Maps API in authentication restricted applications may require the purchase of the Bing Maps API License. Please refer to their [Bing Maps API licensing options](#) for more information.



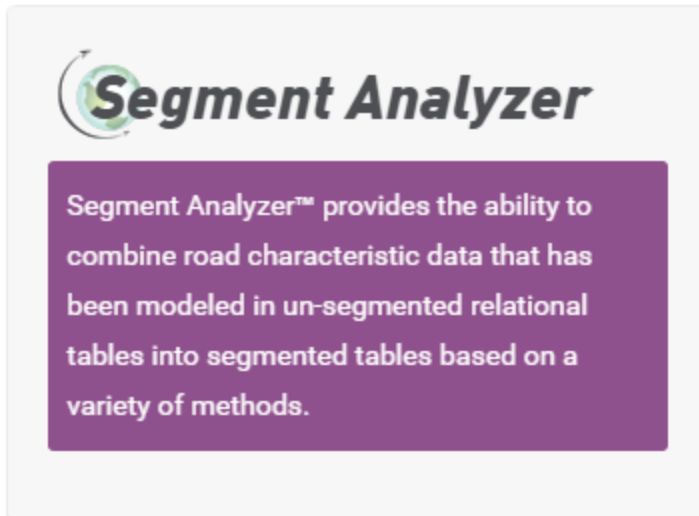
## Apps Dashboard

The Apps Dashboard is found on the main screen of App Manager and provides quick access to all your installed applications and application profiles.

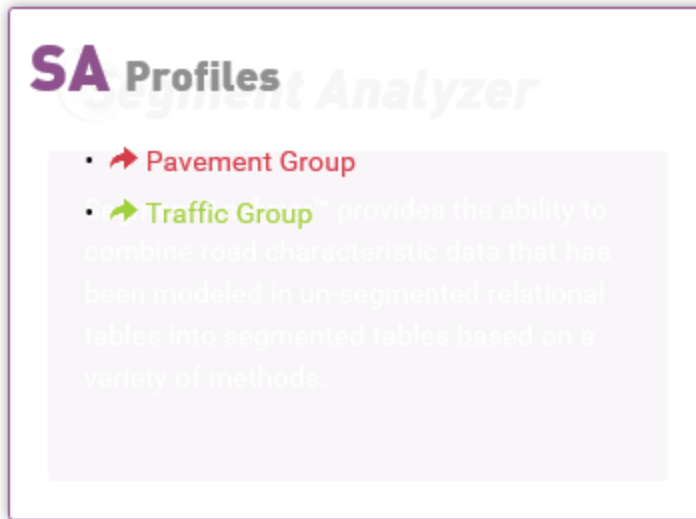


### Usage

1. Hover over the application you wish to launch.



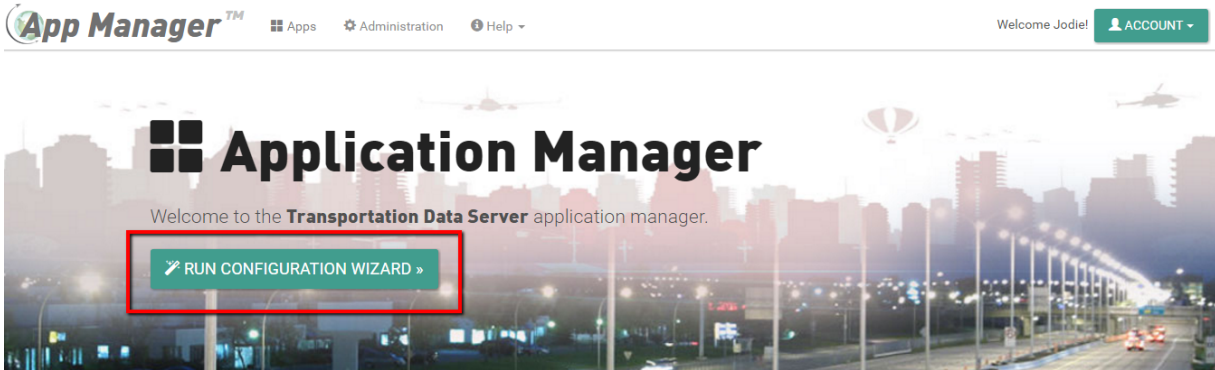
2. Select the application profile from the list of available profiles and click the link to launch that profile.



**Tip:** If you do not see an application or application profile you expect to see in the Apps Dashboard, contact your site administrator. If you are an administrator, you can also Run the Configuration Wizard if you are installing apps for the first time or create a new Application Profile.

## Configuration Wizard

The Configuration Wizard is the quickest way to get up and running with our web applications in your environment.

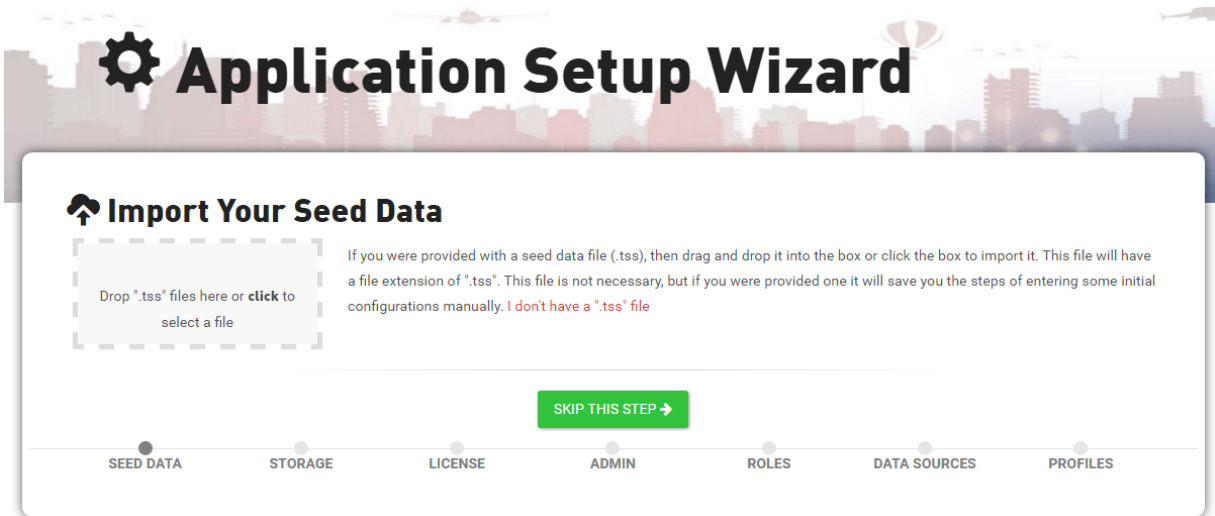


### Usage

To get started, simply click the **RUN CONFIGURATION WIZARD** button on App Manager's main screen and follow the instructions on screen to complete each of the following steps:

#### 1. Import Your Seed Data

If we provided you a seed data file, drag and drop the file into the dashed import box.



**Note:** The seed data file is a json file that contains details for any application configurations that we have pre-configured for you.

Click **SKIP THIS STEP** if you do not have a seed data file.

## 2. Configuration Database

Click **Use the Default** if you wish to use the default database. By default App Manager will store your configurations in a local file database (.sdf file) on the server.

If you'd like to specify the database used, click **Specify a Database** and enter your database details into the provided form.

Where would you like to store your configuration?

Use the default

Specify a database

**Database Type:**

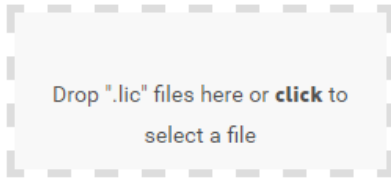
**Connection String:**

You can test that your database connection is successful by clicking **TEST CONNECTION**.

## 3. Import Your License

Drag and drop the ".LIC" file we provided to you into the dashed import box to add your software license information. Once added, you'll be able to see your license ID, license type, who it's registered to, when it expires as well as all the products and features included in your license.

## Import Your License



**License ID:** f3d10350-4bb6-4829-b594-9bdca6140e28  
**Type:** Standard  
**Registered To:** Rusty Green ([rgreen@tssgis.com](mailto:rgreen@tssgis.com))  
**Expires:** Never  
**Features:**

- ✓ App Manager
- ✓ Security
- ✓ License Server
- ✓ Data Sources
- ✓ Jobs
- ✓ LRS
- ✓ Road Analyzer
- ✓ Segment Analyzer
- ✓ Validation Assistant
- ✓ HPMS Assistant
- ✓ Report Engine
- ✓ Video Log
- ✓ File Access

← BACK

SKIP THIS STEP →

#### 4. Administrator Account

This step asks you to set up the main admin user for App Manager. This account is the backup account and has complete administrator privileges to this application. To add, simply provide a User Name, First Name, Last Name, Email, and Password in the provided fields and click "Register."

## Administrator Account Create a system admin account



**Create a built in admin account.** This account will be the backup account that will have complete administrator privileges to this application. You can configure other user/roles and assign privileges in the next step. You'll want to make this a good password.

User Name:	<input type="text" value="siteadmin"/>
First Name:	<input type="text" value="Admin"/>
Last Name:	<input type="text" value="User"/>
Email:	<input type="text" value="Example: jsmith@example.com"/>
Password:	<input type="password" value="Enter a password"/>
Confirm Password:	<input type="password" value="Confirm password"/>

REGISTER

### 5. Define Roles

Roles provide a method in which to group application privileges by App Manager allows you to pre-set roles for a standard users group and an admin group across all your applications. Use the form to create a standard user group and an admin group role name.

## Define Roles

**Define Your Roles!** Roles provide a method in which to group application privileges by. All functionality throughout the app have their own distinct privilege, and these privileges can be assigned to any number of roles in order to grant access to individuals within those roles. To help with the assigning of privileges to roles, you can define role names that represent the typical breakdown of privilege grouping, and the application will automatically assign newly installed privileges accordingly.

**Note:** If you are, or will be using, active directory roles then you must prefix your role/group names with the domain name. For example: `MY_DOMAIN\Admins`

**Note:** Leave role names blank to prevent the application from automatically assigning privileges.

Standard Users Group Role Name:	<input type="text" value="Standard Users"/>
	The role name that represents a "standard" authenticated user.
Admin Group Role Name:	<input type="text" value="Admin Users"/>
	The role name that represents a grouping of "administrators".

BACK

SAVE AND CONTINUE

**Note:** If you are, or will be using, active directory roles then you must prefix your role/group names with the domain name. For example: `MY_DOMAIN\Admins`. Also, leave role names blank to prevent the application from automatically assigning privileges.

### 6. Enter Your Data Sources

Data sources provide access to your data from all your applications and tools. See the [Data Sources](#) topic for step-by-step instructions on how to add a data source.

Q | Refresh + Add New

Status	Name	Provider	Description	Actions
	TSS			
	Demo Data Set	SQL Server	Generic TSS Demo Transactional DB	
	Demo Data Set Output Workspace	SQL Server	Generic TSS Demo Output Workspace DB	

## 7. Setup Application Profiles

Application profiles provide the ability to create multiple configurations for the same application. See the [Application Profiles](#) topic for step-by-step instructions on how to add and manage profiles.

Q | Refresh + Add New

Application	Profile ID	Name	Description	Actions
HPMS Assistant	CW16	Testing		
HPMS Assistant	tes	Tss		

## Downloads

The Downloads feature is accessible from the top menu and allows you to download available supporting software and application files provided by Rizing Geospatial. The available downloads listed is dependent on the applications you have installed.

Product	File Name	Creation Date	Description	Download	Actions
Road Analyzer	SLD Print.mrt	12/28/17 10:56 AM	RE template for SLD print...	DOWNLOAD	Help   Actions
Road Analyzer	event-editor-widget.zip	12/29/17 09:54 AM	RA widget for Event Edito...	DOWNLOAD	Help   Actions

## Usage

### Download Supporting Software or an Application File

1. Click the **Download** button for the item you wish to download.

Product	File Name	Creation Date	Description	Download	Actions
Road Analyzer	SLD Print.mrt	12/28/17 10:56 AM	RE template for SLD print...	DOWNLOAD	Help   Actions
Road Analyzer	event-editor-widget.zip	12/29/17 09:54 AM	RA widget for Event Edito...	DOWNLOAD	Help   Actions

2. The file will then download to your computers downloads folder.

### Seed a File

If the file is typically "seeded" in App Manager or an application, it will have an **Actions** option listed next to it.

1. Click the **Actions** dropdown.
2. Confirm the option to seed the file listed in the dropdown.

Description	Download	Actions
RE template for SLD print...	DOWNLOAD	Help   Actions
RA widget for Event Edito...	DOWNLOAD	Help

Seed the COTS report template into RE (overwrite existing)

**Note:** For full instructions on how to download and publish the SD files available here, please see the [Publishing ESRI Service Definition Files](#) topic.





## I'm a new user and want to learn the basics of Application Manager

Sound like you? You've landed in the right place. You're new to App Manager and want to learn the key components. Delve into the information below and you'll be an experienced user in no time!

[Application Resources](#) - various topics covering global application features and settings

[Overview of User Roles and User Access](#)

### Administration Console

The Administration Console provides access to all configuration settings available in App Manager.

[Security](#) - configure your authentication mechanism, security settings, roles, privileges, and assign users to roles

[Databases](#)- configure where to save your data, add database connections, and import seed data

[Support](#)- view server logs and execute web service calls

[Settings](#)- configure your general server, file path settings, and many more

[Applications](#) - create and manage application profiles

[Actions](#) - options that affect the entire application

## Application Resources

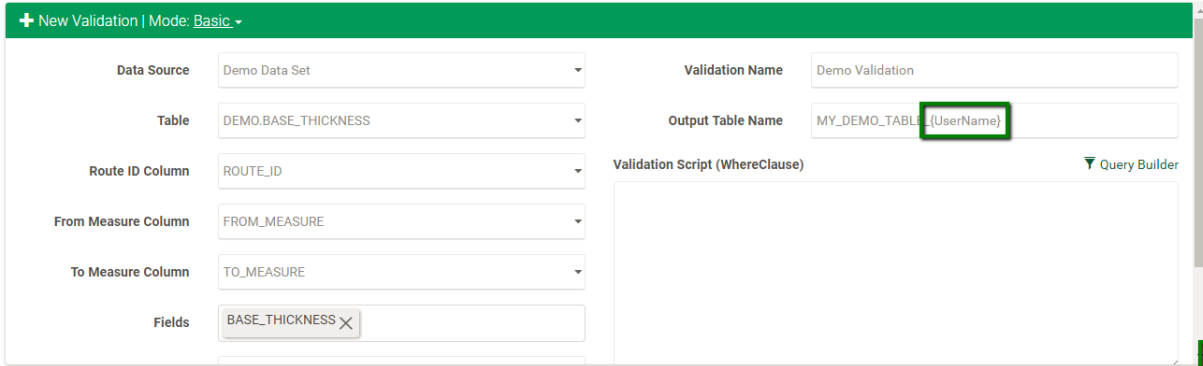
The following topics cover various application features and functionality that are utilized across our applications.

[Output Table Tokens](#) - use tokens in output tables names to dynamically name output tables using a variety of tokens

[Geodatabase Versioning Workflows](#) - overview of how geodatabase versions are managed in workflows utilizing both transactional data, mash up tables and views across multiple applications

## Application Tokens

Several of our applications already support the use of tokens to dynamically name output tables and the rest of our applications will support this feature in the near future. The tokens are used to construct the table name in the application's user interface and then server-side code is used to rename the table once it is output.



### Usage

To use, simply include the token in the table name.

#### Available tokens:

The following tokens can be used in a table name as part of a string *or* by themselves:

{Username} - The authenticated username

**Note:** Since special characters like ! "" SPACE # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ ] ^ ` { | } ~ cannot be part of a table name, if your username includes any of them this token can not be used.

{UserFirstName} - The authenticated user's first name

{UserLastName} - The authenticated user's last name

{AuthType} - The type of authentication used for the authenticated user

{Unique} - Will insert a unique string (it will be a new GUID)

The following tokens can be used in a table name as the suffix of a string:

{Timestamp} - Will insert an EPOCH timestamp (current time)

{Date} - Will insert the current date

#### Token manipulation:

You can add ":upper" or ":lower" to force the token value to be upper case or lower case.

{Username:lower} - will lower case the username value

{Username:upper} - will upper case the username value

**Example:**

**MY\_TABLE\_{UserName} becomes MY\_TABLE\_rgreen**

**MY\_TABLE\_{UserName:upper} becomes MY\_TABLE\_RGREEN**

**MY\_TABLE\_{UserName:lower} becomes MY\_TABLE\_rgreen**

**{UserName}\_{Unique} becomes rgreen\_F10F88CD-AF38-4AD5-A290-3CA3E3BAFBF8**

## Overview of User Roles and User Access

All features, actions, and service calls, are tied to a specific permission or privilege in the application. [Privileges](#) can be granted or denied to any role, and users can only access functions assigned to their role. Rather than assigning application privileges to each user, [roles](#) are created and assigned privileges to ensure the appropriate level of security. [Users](#) are then assigned to the role appropriate for their job function.

### Anonymous Access

If a role with the name "Anonymous Access" exists, then any privilege assigned to that role will be accessible by anyone (no authentication necessary). This "Guest Access" should typically be configured to restrict access to any configuration components, and only grant access to "view-only" operations.

### Authenticated Users

If you have credentials for the application you can enter them in the User Sign In area. Once you have successfully signed in, any features available to you (depending on your user role(s)) will be made available/visible. See the [Roles](#), [Role Privileges](#), and [User Roles](#) sections for information on configuring authenticated user roles.

**Note:** If you do not see functionality that you expect to see, please contact the site's administrator and request to have the particular functionality made available to you.

[Register New User](#)

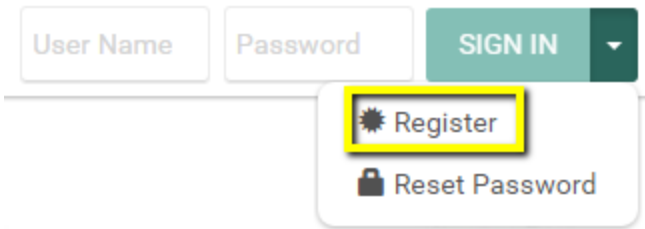
[User Sign In](#)

[Reset Password](#)

## Register New User

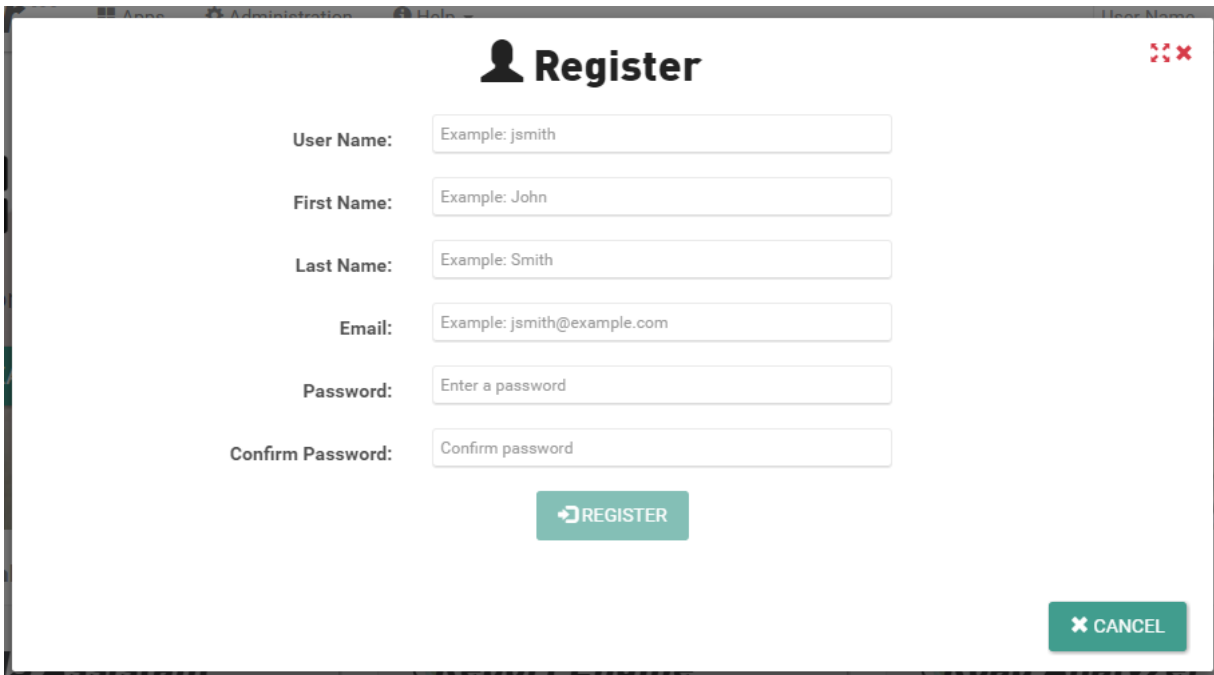
The New User dialog provides the ability to add a new user to gain access to basic functionality in the application, as well as personalized/customized layout and settings. Administrators, or others with the privilege, can also register a new user in [User Roles](#).

**Heads Up!** If Windows authentication or Security Token Service (STS) is the chosen security setting and you are part of an Active Directory or other STS you will not need to register as a new user. When you are already signed in on an Active Directory or STS network, App Manager will pick up your credentials and automatically sign you in.



### Usage

To register as a new user:



A screenshot of the 'Register' dialog box. The dialog has a title bar with a person icon and the word 'Register'. It contains several input fields: 'User Name' (with example 'jsmith'), 'First Name' (with example 'John'), 'Last Name' (with example 'Smith'), 'Email' (with example 'jsmith@example.com'), 'Password' (with placeholder 'Enter a password'), and 'Confirm Password' (with placeholder 'Confirm password'). At the bottom, there are two buttons: 'REGISTER' and 'CANCEL'.

1. Click the **down arrow** beside the Sign In box.
2. Click **Register** from the dropdown menu.

3. Fill in **User Name**, **First Name**, **Last Name**, **Email**, **Password**, and **Confirm Password**.

**Tip:** Make note of your **User Name** and **Password** for future use.

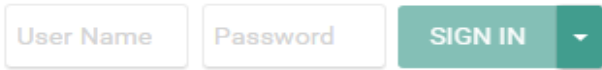
4. Click **Register**.

## User Sign In

The "User Sign In" tool provides the ability to enter your user credentials and gain access to additional functionality in the application, as well as personalized/customized layout and settings.

### Signing In

To sign in:



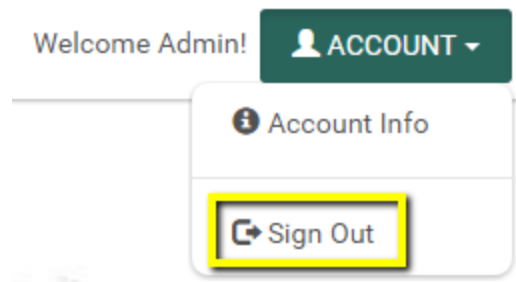
The image shows a user sign-in form with three input fields: "User Name", "Password", and a "SIGN IN" button. The "SIGN IN" button is green with a white downward arrow on its right side.

1. Locate the login input boxes in the upper right corner of the app.
2. Enter your username in the **User Name** input box.
3. Enter your password in the **Password** input box.
4. Click **Sign in** to authenticate.
5. Wait for confirmation that you were successfully signed in.

**Note:** If you log into the app and do not log out before closing the browser session, the app will remember you and keep you logged in the next time the app is started. You must log out of the application if you do not want the application to remember your login across sessions.

### Signing Out

To sign out:

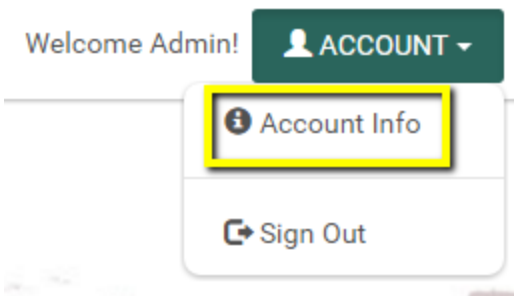


1. Locate the login input boxes in the upper right corner of the app.
2. Click the **Account** drop-down button.
3. Click **Sign Out**.
4. Wait for confirmation that you were successfully signed out.

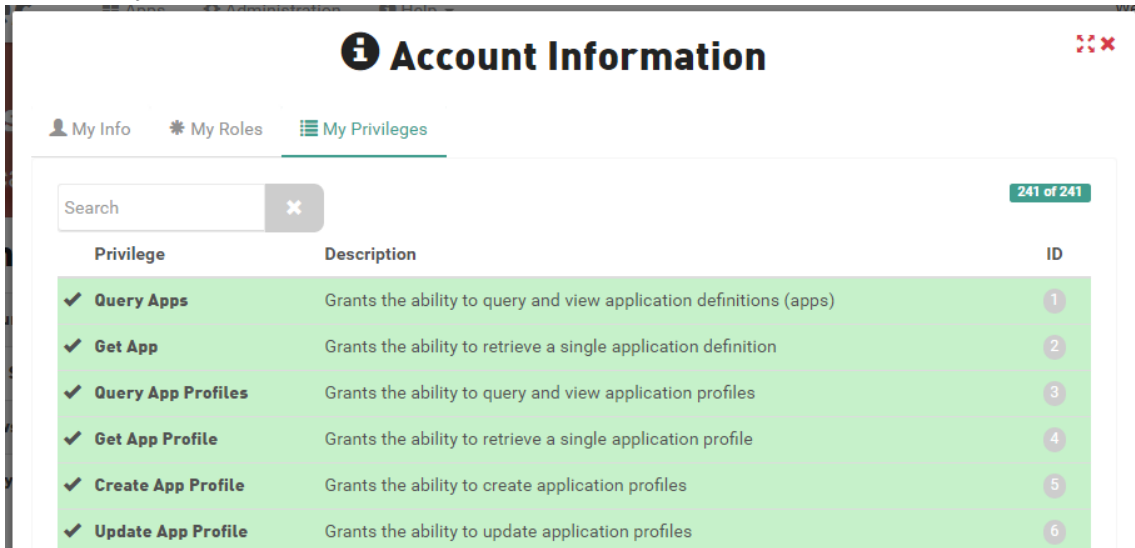
### Account Info

Once you are signed in, you can view/edit your user information by:





1. Click the **Account** drop-down button.
2. Select the tab you want to view.



Options include:

My Info - basic account info including: User Name, First Name, Last Name and Email

My Roles - lists of all Roles you are in and their description

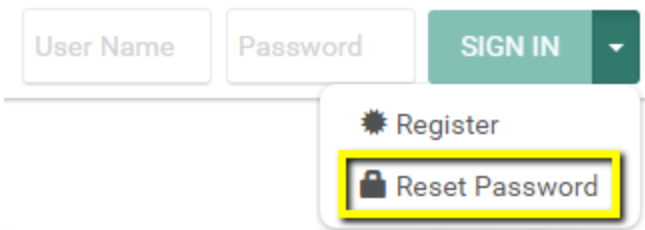
My Privileges - view all privileges (features) that you have access to in the application

3. Click **Close** to close the Account Information dialog.

## Reset Password

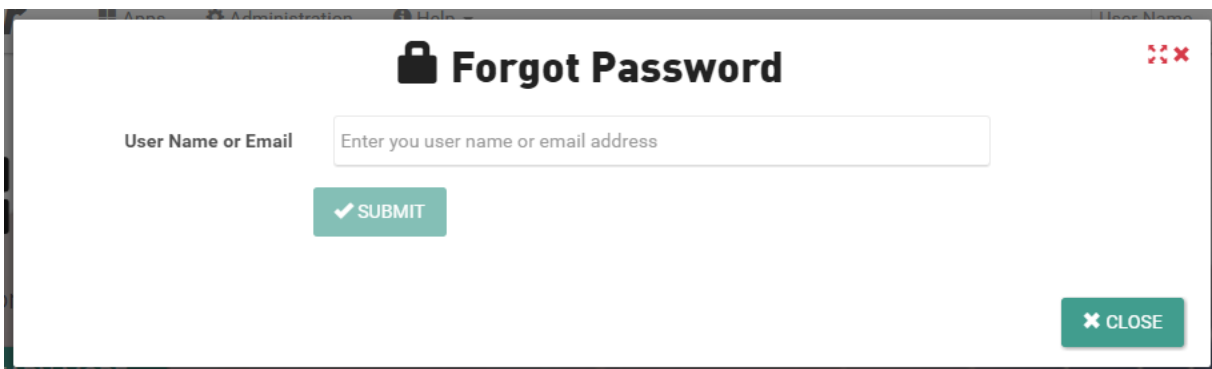
The Reset Password dialog provides the ability to reset a user's password if forgotten or lost.

**Heads Up!** If Windows authentication is the chosen security setting and you are part of an Active Directory you will need to contact your Active Directory administrator to change your password.



### Usage

You can reset your password by:



1. Click the **down arrow** beside the Sign In box.
2. Click **Reset Password** from the dropdown menu.
3. Fill in your **User Name** or the **Email** you registered with.
4. Click **Submit**.
5. Go to the email you registered with and open the message.
6. Follow the instructions in the email to complete resetting your password.

## Security

[Authentication](#) - learn about the available authentication mechanism options

[Configure Portal for ArcGIS](#) - configure TDS to consume Portal for ArcGIS content

Workflows for setting up the following authentication options:

[No Security](#)

[Built In Security](#)

[Windows Security](#)

[Security Token Service](#)

[IdentityServer](#)

[Roles](#) - create roles to assign application privileges

[Role Privileges](#) - assign application privileges to defined roles

[App Restrictions](#) - assign restrictions to applications to defined roles

[Profile Restrictions](#) - assign restrictions to profiles to defined roles

[Templates](#) - manage templates and define sharing privileges

[Users and User Roles](#) - assign your configured users to roles

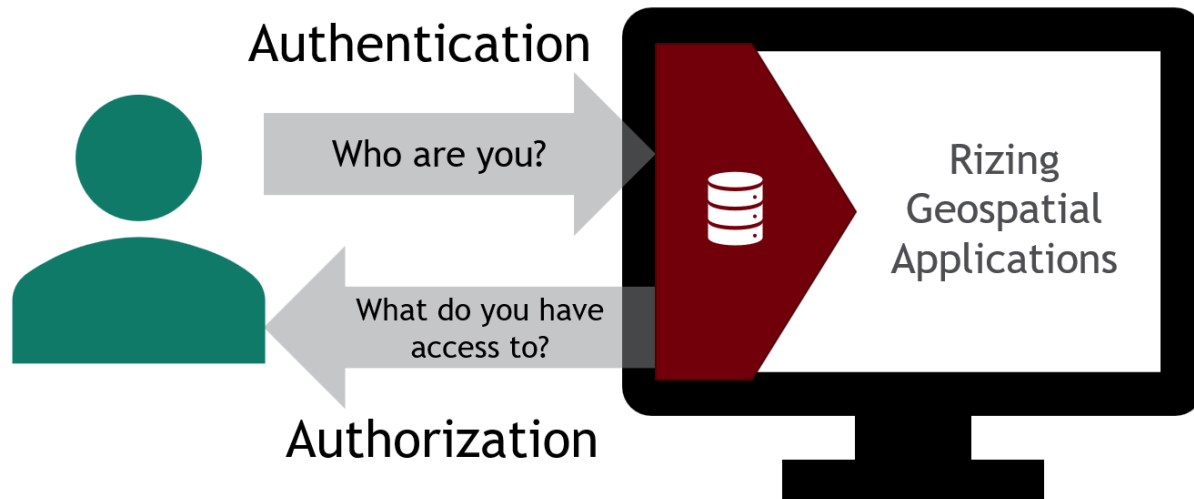
[Map User Claims](#) - map custom user claims

[Security Settings](#) - set up error handling, user access and roles, etc.

[Access Tokens](#) - manage privilege authorization via access tokens

## Authentication

User authentication (the determining who you are) and authorization (determining what you have access to) for all your Rizing Geospatial applications is selected in App Manager's Authentication feature.



**Note:** For information regarding authenticating with ArcGIS Portal, please refer to the [Configure Portal for ArcGIS](#) topic.

Options include:

### No Security

This option will disable any security checks and leave all functionality open to anyone who has access to the application and services. This option should only be used during testing or on a secure network.

To implement this option, follow the steps found here: [No Security](#).

### Built In Security

This option will use the application's security mechanism and all users, roles, and privileges will be stored internally. Application features are shown/hidden based on user privileges and services are secured through token-based authentication based on registered users and defined roles; all of which can be managed through the application interface.

To implement this option, follow the steps found here: [Built In Security](#).

### Windows Security

This option will authenticate users and roles based on Integrated Windows Authentication. This option requires that the application server (IIS) is on the same domain and has read access to the domain's Role/Group store. The users and roles that drive this security policy can be read from Active Directory or configured using the application server's user/groups functionality. Application privileges

are still stored using the applications built in security mechanism, but the users and roles are stored and checked using windows authentication - privileges are simply mapped to windows roles/groups.

To implement this option, follow the steps found here: [Windows Security](#).

### Security Token Service (STS)

This option will authenticate users and verify roles based on the configured Security Token Service (STS) metadata. An STS is the service component that builds, signs, and issues security tokens according to the WS-Trust and WS-Federation protocols. A Security Token Service can be a cloud STS such as a LiveIDSTS, a pre-built STS such as Active Directory Federation Services (ADFS) or a custom STS. On authentication, STS should return identity information such as name, e-mail address and roles as claims.

To implement this option, follow the steps found here: [Security Token Service](#).

### IdentityServer

This option will authenticate users and roles against IdentityServer3. IdentityServer is a framework and a hostable component that allows implementing single sign-on and access control for modern web applications and APIs using protocols like OpenID Connect and OAuth2. It supports a wide range of clients like mobile, web, SPAs and desktop applications and is extensible to allow integration in new and existing architectures. You can learn more about this option here: [IdentityServer Documentation](#).

To implement this option, follow the steps found here: [IdentityServer](#).

**Note:** More details and information regarding security can be found in the [Application Security](#) topic.

## Configure Portal for ArcGIS

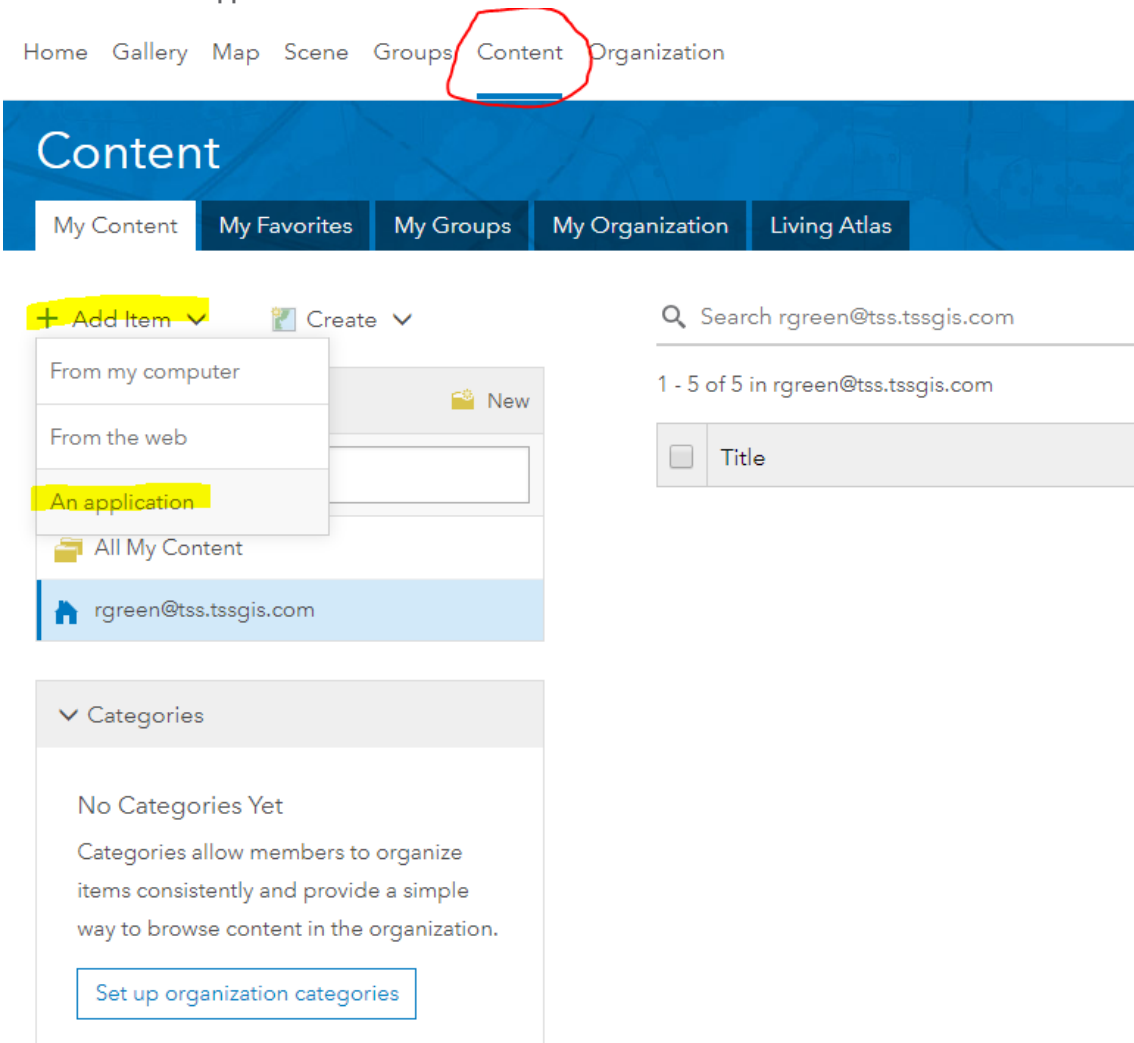
The Rizing web applications can be configured to allow its applications to consume map service data from a secured map server federated with an ArcGIS Portal.

### Configuration

To allow the applications to consume data from a secured map service which is federated with Portal for ArcGIS, the following steps must be taken:

#### Setup Application within Portal

1. Sign into your **Portal for ArcGIS** instance.
2. Go to **Content**.
3. Click **Add Item > An Application**.



4. Select **Application**.

5. Enter a **Title**.
  1. Suggestions:
    1. DEV Environment TDS Portal App
    2. STG Environment TDS Portal App
    3. PRD Environment TDS Portal App
    4. etc
6. Enter **Tags**.
7. Click **Add Item**.

**Add an application** ? X

Add an item from your computer or reference an item on the Web.

Type:

Web Mapping  Mobile  Desktop  Application

Application Extension (Operations Dashboard)

Application Extension (AppBuilder)

Title:

DEV Environment TDS Portal App

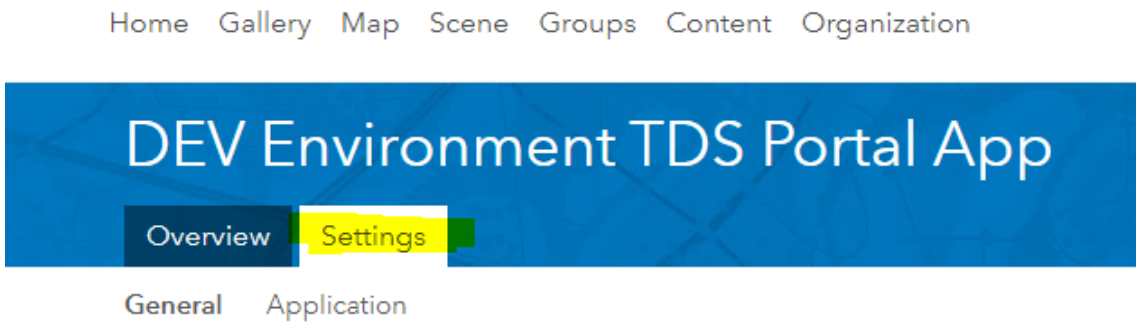
Tags:

TDS x

Add tag(s)

Add Item Cancel

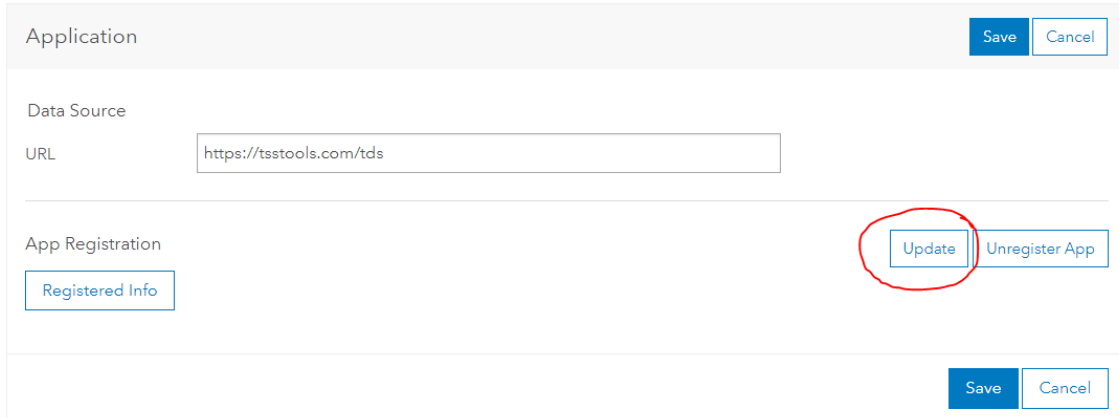
8. On the newly created Application page, click the **Settings** tab.



9. Under the **Application** panel, enter the **URL** the to Application Manager site.

**Note:** This will allow users to quickly launch App Manager from within your Portal for ArcGIS site.

10. Click the **Update** button.



The screenshot shows the 'Application' configuration page. At the top right are 'Save' and 'Cancel' buttons. Below is the 'Data Source' section with a 'URL' field containing 'https://tsstools.com/tds'. The 'App Registration' section contains a 'Registered Info' button and an 'Update' button (circled in red), along with an 'Unregister App' button. At the bottom right are 'Save' and 'Cancel' buttons.

11. Enter in a redirect **URL** that will point back to the following URL:

YOUR\_TDS\_URL/apps

**Example:**

1. https://YOUR\_TDS\_URL/apps

**Note:** This URL must match the exact URL that will be used to access TDS.

**Note:** It is recommended to add both http and https protocols.

2. http://YOUR\_TDS\_URL/apps  
https://YOUR\_TDS\_URL/apps

**Note:** It is recommended to add both the external domain (if applicable) as well as the PC name of the TDS server (or whatever URLs will be used to access the TDS site), to cover both internal and external access (if applicable).

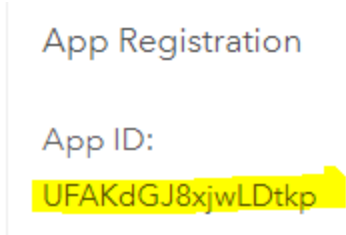
3. https://YOUR\_TDS\_URL/apps  
http://YOUR\_TDS\_URL/apps

**Note:** Ensure that you click "Add" to add the Redirect URI to the list

12. Click **Update** to accept the added Redirect URIs.

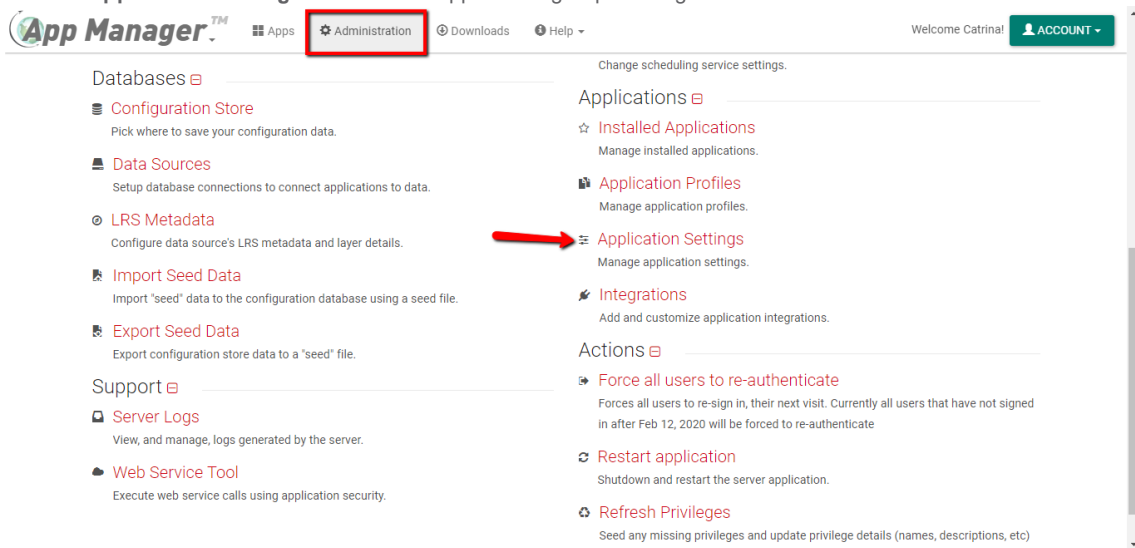


13. Make note of the **App ID** value. You will need it to enable Portal for ArcGIS authentication for your data source in App Manager.



### Configure Portal Settings in App Manager

1. Load App Manager (TDS) application and log in with an Administrator account.
2. Go to the **Administration** page (button is accessible from the top navigation bar).
3. Click the **Application Settings** link under the Applications group heading.



4. Enter an **ArcGIS Server Geometry Service URL** that is hosted on the secured map service (federated with Portal for ArcGIS).

**ArcGIS Server Geometry Service URL:**

The URL to ArcGIS Server's Geometry service (for doing things like projections, buffering, etc). This service is typically found in the "Utilities" folder on ArcGIS Server.

5. Enter an **ArcGIS for Portal URL**.
6. Enter a **Portal App ID** which is the **App ID** value noted in the previous step above.

**ArcGIS for Portal URL:**

The ArcGIS Server URL used to authenticate applications.

**ArcGIS for Portal App ID:**

The App ID for the TDS application setup in ArcGIS Portal.

7. Click the **Save** button (located in the bottom right corner of the page).
8. Portal is now configured within TDS, however an application will only try to authenticate with Portal for ArcGIS when a data source is marked as "Service requires ArcGIS for Portal authorization". See below to enable that setting.

### Enable Portal for ArcGIS Authentication for a Data Source

1. Navigate to the **Administration** page within TDS's App Manager.
2. Select the **Data Sources** link under the **Databases** group heading.

## Databases

### Configuration Store

Pick where to save your configuration data.

### Data Sources

Setup database connections to connect applications to data.

### LRS Metadata

Configure data source's LRS metadata and layer details.

3. Edit (or create) the data source that is configured to use a secure map service (federated with Portal for ArcGIS).
4. Ensure that the **Associated Service URL** is configured to point directly to the secure map service.
5. Check the **Service requires ArcGIS for Portal authorization** check box option.

Associated Service URL:

Test URL



Service requires ArcGIS for Portal authorization

6. Click **Save**.
7. Any application that uses this data source will now initiate the sign in process with Portal (when applicable).

#### Test Portal for ArcGIS Authentication for an Application

1. Load an application profile that is using a data source that is marked as **Service requires ArcGIS for Portal authorization**.
2. Ensure that the application prompts the user to authenticate with Portal for ArcGIS (as described in the "Functionality Overview" section above).

#### Diagnose Portal for ArcGIS Authentication Issues

If an issue occurs during portal authentication, review the message that will be displayed in the Portal popup window or review the application logs (found under Help > Logs). The following is a list of common misconfiguration and diagnostic steps:

##### Redirect page stuck on ArcGIS Page with message of "Invalid redirect\_uri"

**Issue:** This message means that the redirect URL configured within Portal for ArcGIS is not the same URL that the user is accessing the site from.

ArcGIS Portal Directory | [Home](#)

Error

**Invalid redirect\_uri**

**Error: 400**

**Solution:** Compare the base of the URL from the browser of the application with the URL that was configured with Portal for ArcGIS. Update the “Redirect URI” to include a valid URL.

**Tip:** You can copy the URL of the popup window and run the URL through any HTML/URL decoder to see what the exact redirect URL is being passed to Portal (it will be present as a query parameter named “redirect\_uri”).

## Workflow

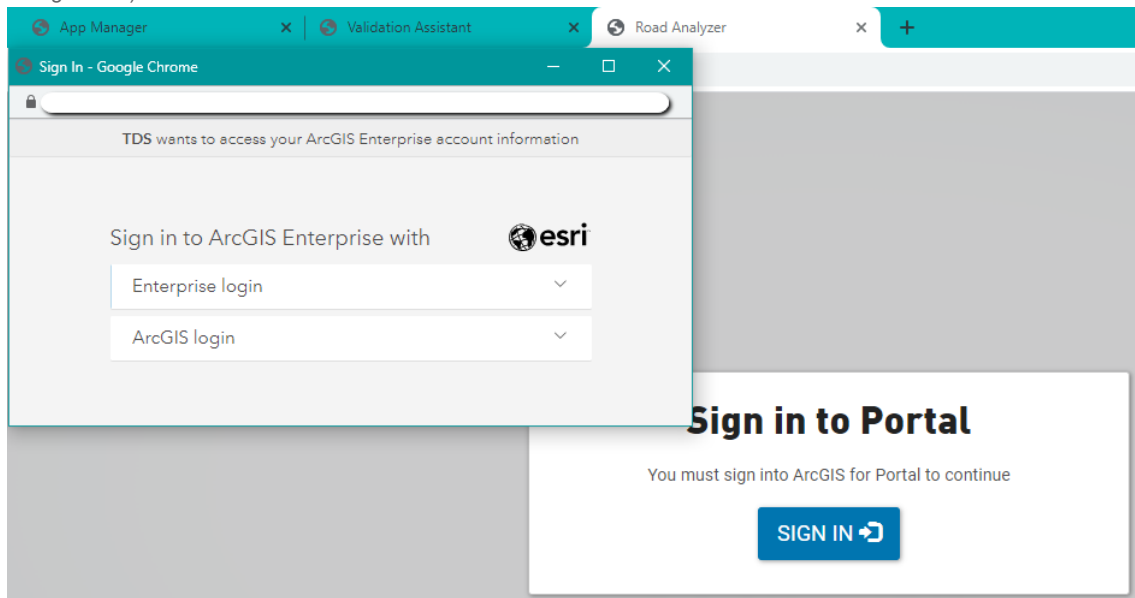
After App Manager has been properly configured, you will do the following steps when accessing an application that consumes this data.

**Heads Up!** If the application does not have a map interface or does not have any Profile Configuration settings that use the map service, you will not need to sign in to Portal.

1. You launch an application from App Manager that has a data source which is pointing to a secure [Map Server that is federated with Portal for ArcGIS](#).
2. The application opens to a dialog asking you to **Sign in to Portal**.

**Note:** It is necessary to confirm this action in order to prevent the browser popup blocker from blocking the next step.

3. Click **SIGN IN**.
4. A popup window will open with the Portal for ArcGIS authentication method (the exact method varies based on your Portal configuration).



5. After you are authenticated within Portal for ArcGIS, the popup window and dialog will close and the application will continue loading as normal.

**Tip:** The token will automatically be refreshed behind the scenes with Portal for as long as it can. However, once the token can no longer be refreshed you will be required to repeat steps 2 through 4 to obtain a new access token.

## No Security

This mechanism can be enabled by removing any previously configured security configurations and setting the “appSettings” key “BypassSecurity” to “True”.

### Steps to use No Security for Authentication:

1. **Check** the No Security option.
2. Click **Save**.
3. Click **Change** to confirm your changes..

## Built In Security

### Steps to use Built In Security for Authentication:

1. Add any **Roles** needed.
2. Assign **Privileges** to those roles.
3. Add any **Users** needed.
4. **Assign** your users to a role.
5. Adjust the following **Security Settings** as desired:
  - System Administrator "Username"** - this sets the username of the System Administrator for TDS. If you used the Configuration Wizard, this will already be filled in with the 'siteadmin' user you registered. If you did not, you will need to enter the username of your System Administrator here.
  - Anonymous Access Role Name** - this will set the role any anonymous users will receive when accessing any of your Rizing Geospatial web applications.
  - Auto-managed Role Privileges** - if this is checked App Manager will automatically assign role privileges based on Rizing Geospatial's suggested privilege levels and the defined roles you select below that setting.
  - Admin and Standard User's Group Roles** - if you checked Auto-managed role privileges, here you can select the Role that represents the "administrators" group and the "standard user's" group. When you install any new applications, these groups will automatically be assigned the privileges set for the selected roles.
  - New User's Default Role** - if you checked the **Auto-managed Role Privileges** option, here you can select the Role that will be assigned to all new users.
6. On the Authentication page, **check *Built In Security***, click **Save** and then click **Change** to confirm your changes.

**Note:** After changing the authentication method, you will need to *refresh* the application. If you were not signed in with a built-in account, your access will be limited or blocked. You can sign in by entering your username and password then clicking **Sign In**.

## Windows Security

### Steps to use Windows Security for Authentication:

1. Add [Roles](#) to mimic your Active Directory roles.

**Heads Up!** These new roles in App Manager must have the *exact name* of the Active Directory role/group, so that you will be able to assign application privileges to that role.

2. Assign [Privileges](#) to those roles.
3. Enable Windows Authentication within [Internet Information Services \(IIS\)](#).
4. If any of your [Data Sources](#) will be authenticating with ArcGIS Portal, you will need to [configure Portal for ArcGIS](#).
5. Adjust the following [Security Settings](#) as desired:
  - [Anonymous Access Role Name](#) - this will set the role any anonymous users will receive when accessing any of your Rizing Geospatial web applications.
  - [Auto-managed Role Privileges](#) - if this is checked App Manager will automatically assign role privileges based on Rizing Geospatial's suggested privilege levels and the defined roles you select below that setting.
  - [Admin and Standard User's Group Roles](#) - if you checked Auto-managed role privileges, here you can select the Role that represents the "administrators" group and the "standard user's" group. When you install any new applications, these groups will automatically be assigned the privileges set for the selected roles.
  - [New User's Default Role](#) - if you checked the **Auto-managed Role Privileges** option, here you can select the Role that will be assigned to all new users.
6. On the Authentication page, **check Windows Security**, click **Save** and then click **Change** to confirm your changes.

## Security Token Service

This topic provides the steps for configuring TDS to use the [Security Token Service \(STS\)](#) authentication mechanism. This authentication mechanism is typically used for protocols such as ADFS, [Azure AD](#), WS-Trust, SAML, etc. Below are general configuration steps. If you want specific configuration steps to use Azure AD as your STS, please see the [Configure TDS with Azure AD](#) topic.

### Configuration Steps

#### Backup existing TDS & data

You will want to back up the TDS application state so that it can be restored to this point in case the authentication mechanism change does not complete as intended. You can skip this step if you are not applying this change to an already configured/established TDS environment.

If you are making these changes to an existing TDS instance:

1. Completely backup your existing TDS and TDS configuration store before making any changes.

**Note:** You could stand up a new instance for this purpose, if that is easier for your scenario.

#### Ensure Integrated Windows Authentication is disabled

The following steps remove the Integrated Windows Authentication configuration from TDS in preparation for the switch to an STS authentication mechanism. You can skip this section if you are not making these changes to an existing TDS instance that already has Windows Authentication setup.

If you are making these changes to an existing TDS instance and it is currently using Windows Authentication:

2. Go to App Manager > Administration > [Authentication](#).
3. Change the Authentication Mechanism to **No Security**.
4. Click **Save** and then click **Change** to confirm your changes.

**Note:** It may take a few moments for the application to save. Wait for it to complete.

5. Disable Windows Authentication from the TDS application within IIS.
  - a. Set **Anonymous Authentication** to Enabled.
  - b. Set **Windows Authentication** to Disabled.
6. Ensure App Manager loads properly.

**Note:** At this point there is no security/authentication being applied to TDS.

#### Setup Administrator role in preparation for switch to STS

The following steps will set up a non-externally managed role for global site administrators. This role will be used to place the initial STS authenticated user in, so that after the initial switch to the STS authentication mechanism, the user will be able to continue administering App Manager. If a role like this already exists, skip to step 12 to ensure the role has all the needed privileges.

7. Go to App Manager > Administration > [Roles](#).
8. Create a non-externally managed role for global site administrators.


- Do not check the **Is role externally managed** checkbox for the role.

### Add application roles (to group privileges) i

**Role name:**

The name of the application role to create. This can be a completely new, arbitrary role name, or it can mirror the name of an external role (such as an Active Directory group). Note, when using an Active Directory group name, prefix the role name with domain and a backslash. Example: **MY\_DOMAIN\Admin Users**

**Copy privileges from:**

**Is role externally managed?**  

Check this option if this role name is mirroring an external role (such as an Active Directory group). Checking this option will prevent assigning users to this role within this application (instead the users must be assigned roles within the external system). Note, this is dependent on your selected **Authentication Profile**.

**Role description**

- Click **Save**.
- Go to App Manager > Administration > [Role Privileges](#).
- Select the **Administrator**, or equivalent, role.
- Ensure that the role has all privileges with a suggested type of **Super Admin and below** assigned to it.

**Note:** There are a few privileges that do **not** fall into this category.

**Note:** Your exact number or privileges will depend on what applications you have installed.

#### Setup security configuration in preparation for switch to STS

The following steps will configure App Manager to automatically add the first user provisioned through the new STS authentication mechanism to the Administrator role. This needs to be done to prevent being locked out of the application after making the initial switch to STS authentication.

- Go to App Manager > Administration > [Security Settings](#).
- Find the **New users's default role** setting and select the role that represents "Administrators" (from the previous section).

**Tip:** This will ensure that the first time you load the application after changing the authentication mechanism you will be registered as an administrator with full permissions.

- Find the **Enable just-in-time user provisioning** setting and check it.
- Click **Save**.

#### Change the authentication mechanisms to STS


The following steps will change the authentication mechanism to STS security.



- Go to App Manager > Administration > **Authentication**.
- Check Security Token Service**, then enter in the following information:

<b>STS Metadata Location:</b>	<input type="text" value="ex: https://app.your-company.com/federationmetadata/2007-06/federationmetadata.xml"/>
<b>Realm:</b>	<input type="text" value="ex: https://app.your-company.com/app"/>
<b>Audience URL:</b>	<input type="text" value="ex: https://app.your-company.com/app"/>
<b>WHR:</b>	<input type="text" value="ex: https://app.your-company.com/app"/>

#### Add Protocol Message Parameters (optional)

**Name:**  **Value:**  

#### Add Redirect Response Cookies (optional)

**Cookie Key:**  **Cookie Value:**  

**STS Metadata Location** - where the service is located

**Example:** For Azure AD: `https://login.microsoftonline.com/YOUR_TENANT_ID/federationmetadata/2007-06/federationmetadata.xml`

**Realm** - the website of your Rizing Geospatial applications

**Example:** `https://demo.rizing.com`

**Audience URL** - where the STS will reply to after it authenticates the user

**Heads Up!** The **Realm** and **Audience URL** were used to set up the service and *must match* or there will be an error.

*Optional:* Protocol message **Name** and **Value** parameters, then click **Add** (the plus icon)

**Note:** To remove a Protocol Message Parameter, click the **remove param** button (x icon).

*Optional:* To have TDS set a cookie directly before the user gets redirected to the Identity Provider, enter the **Cookie Key** and **Cookie Value**, then click **Add** (the plus symbol)

**Note:** To remove a Redirect Response Cookie, click the **remove cookie** button (x icon).

- Click **Save** and then click **Change** to confirm your changes.

**Note:** It may take a few moments for the application to save. Wait for it to complete.

- Load App Manager in a new browser window.

22. The application should redirect you to your IDP's sign in and then redirect you back to App Manager with you signed in.

**Tip:** You should see your name in the upper right corner.

#### Remove the temporary "New user's default role" setting

Now that you can successfully access the application as an administrator, this step will walk you through changing the "New user's default role" setting back to the desired role.

23. Go to App Manager > Administration > [Security Settings](#).
24. Find the **New user's default role** setting and select the desired **Role** from the dropdown.

**Tip:** This is the role that any new users who authenticate through your IDP will be automatically assigned to. It is typically set to a restricted user type of role, such as *Standard Users*.

**Note:** If you do not wish to have any new users automatically assigned to a role, then select **Prevent automatic role assignment (for new users)**.

25. Test the application and make any additional configurations for your specific needs.

**Note:** You can view users who have accessed the site and adjust their role assignment from the [User Roles](#) page.

## Configure TDS with Azure AD

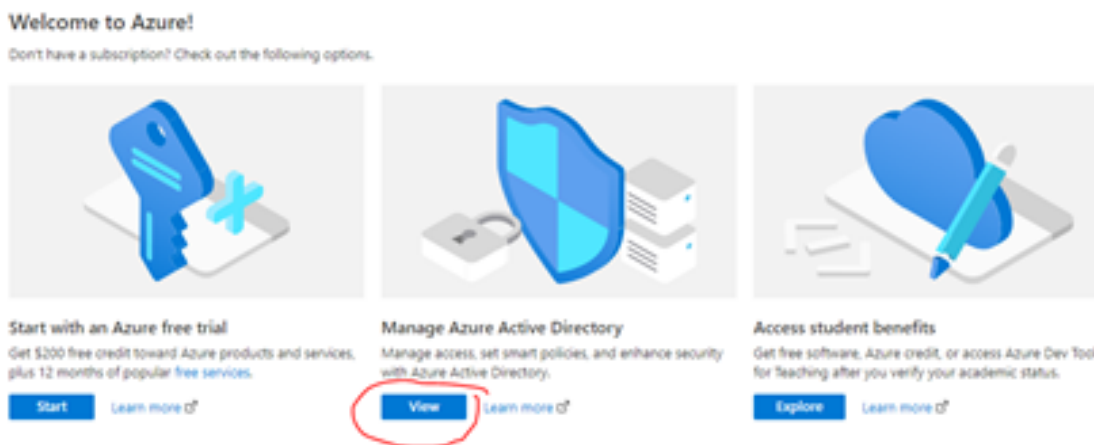
This topic provides the steps for configuring TDS to use Azure AD as the STS (Security Token Service) authentication mechanism.

### Configuration Steps

#### Azure Steps

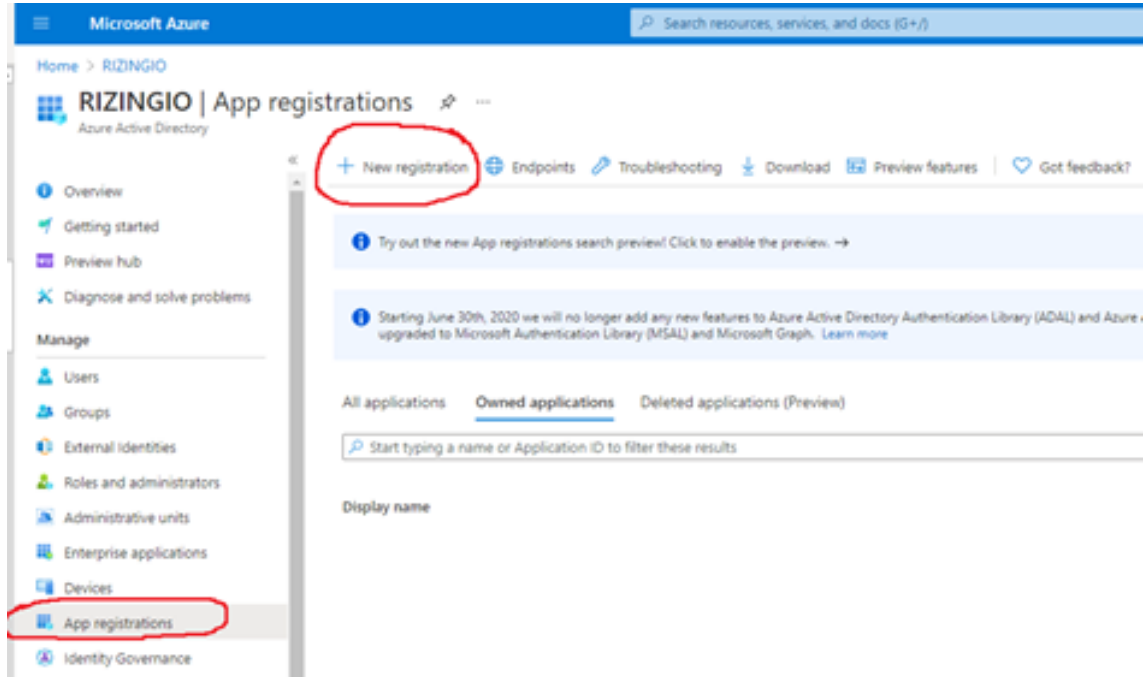
##### Create App Registration

1. Go to [Azure Portal](#).
2. Click the **View** button under Manage Azure Active Directory.



3. Click **App Registrations** from the menu panel on the left.

4. Click New registration.



5. Fill in application details:

- a. Redirect URI must point to App Manager's URL

Example: `https://test.rizing.com/tds`

### Register an application

#### Name

The user-facing display name for this application (this can be changed later).

TDS With Azure AD ✓

#### Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (RIZINGIO only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

#### Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web `http://localhost/tds` ✓

6. Click **Register**.

## Set Application ID

1. Go to the **Expose an API** section in the side menu.
2. Click the **Set** link next to the Application ID URI.

The screenshot shows the Microsoft Azure App Manager interface. The top navigation bar includes the Microsoft Azure logo and a search bar. The breadcrumb trail indicates the current location: Home > TDS With Azure AD. The main heading is 'TDS With Azure AD | Expose an API'. On the left, a navigation menu lists various options, with 'Expose an API' highlighted and circled in red. The main content area shows the 'Application ID URI' field with a 'Set' button circled in red. Below this, there are sections for 'Scopes defined by this API' and 'Authorized client applications'.

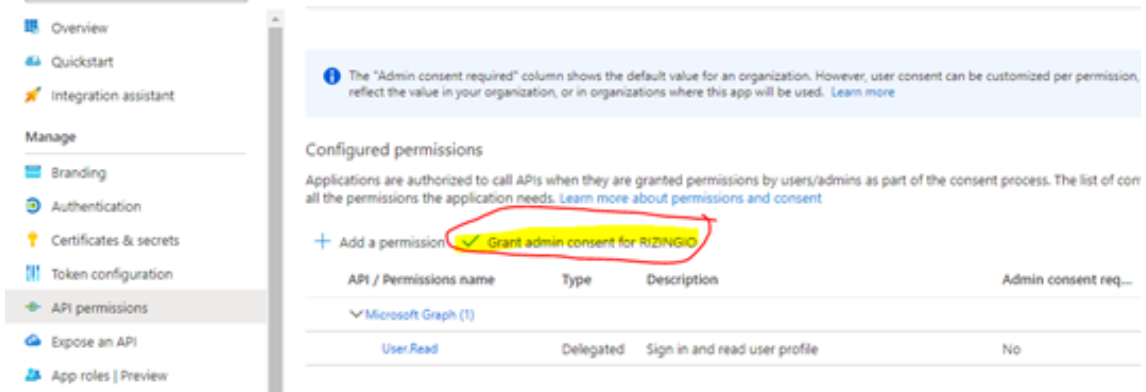
3. Enter the URL to the TDS application.

The dialog box is titled 'Set the App ID URI'. It contains a text input field labeled 'Application ID URI' with the value 'http://localhost/tds'. Below the input field are two buttons: 'Save' and 'Discard'.

**Heads Up!** Copy this URL as it will be entered into App Manager in a later step and it *must match exactly*.

### Grant API Permissions

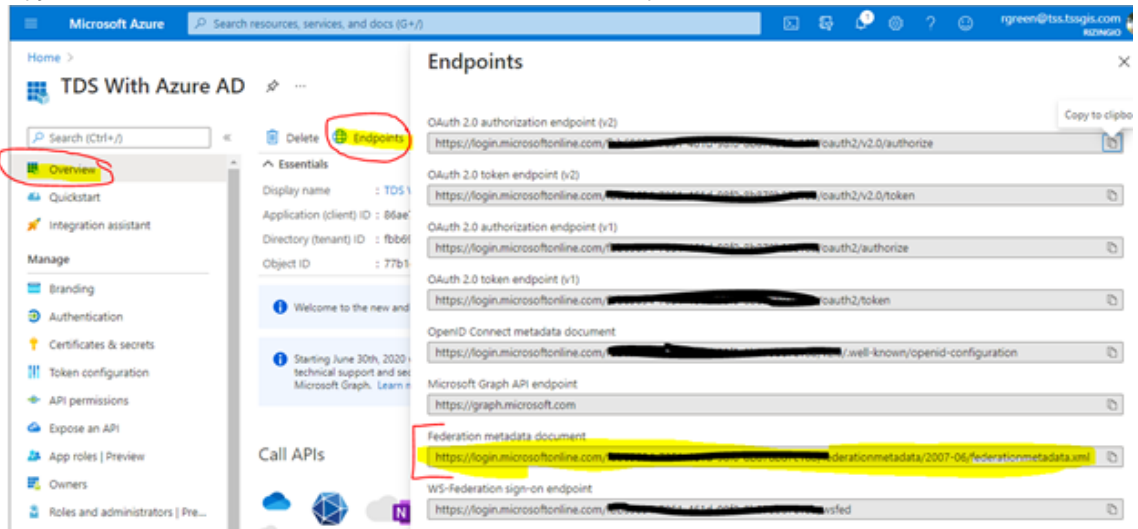
1. Go to the **API permissions** section in the side menu.
2. Click **Grant admin consent for YOUR\_ORG**.
3. Click **Yes**.



**Note:** This will give User.Read permissions to your users.

### Obtain Metadata Document URL

1. Go to the **Overview** section in the side menu.
2. Click **Endpoints**.
3. Copy the **Federation metadata document URL** for use in a later step.



**Heads Up!** This URL will be entered into App Manager in a later step.

### TDS Configuration Steps

#### Backup existing TDS & data

This step is to back up the TDS application state so that it can be restored to this point in case the authentication mechanism change does not complete as intended. Skip this step if you are not applying this change to an already configured/established TDS environment.

If you are making these changes to an existing TDS instance:

1. Completely backup your existing TDS and TDS configuration store before making any changes.

**Note:** You could stand up a new instance for this purpose, if that is easier for your scenario.

### Ensure Integrated Windows Authentication is disabled

The following steps remove the Integrated Windows Authentication configuration from TDS in preparation for the switch to an STS authentication mechanism. You can skip this section if you are not making these changes to an existing TDS instance that already has Windows Authentication setup.

If you are making these changes to an existing TDS instance and it is currently using Windows Authentication:

1. Go to App Manager > Administration > [Authentication](#).
2. Change the Authentication Mechanism to **No Security**.
3. Click **Save** and then click **Change** to confirm your changes.

**Note:** It may take a few moments for the application to save. Wait for it to complete.

4. Disable Windows Authentication from the TDS application within IIS.
  - a. Set **Anonymous Authentication** to Enabled.
  - b. Set **Windows Authentication** to Disabled.
5. Ensure App Manager loads properly.

**Note:** At this point there is no security/authentication being applied to TDS.

### Setup Administrator role in preparation for switch to STS

The following steps will set up a non-externally managed role for global site administrators. This role will be used to place the initial STS authenticated user in, so that after the initial switch to the STS authentication mechanism, the user will be able to continue administering App Manager. If a role like this already exists, skip to step 12 to ensure the role has all the needed privileges.

1. Go to App Manager > Administration > [Roles](#).
2. Create a non-externally managed role for global site administrators to have full access to TDS – if one does not exist already


- Do not check the **Is role externally managed** checkbox for the role.

### Add application roles (to group privileges) i

**Role name:**

The name of the application role to create. This can be a completely new, arbitrary role name, or it can mirror the name of an external role (such as an Active Directory group). Note, when using an Active Directory group name, prefix the role name with domain and a backslash. Example: **MY\_DOMAIN\Admin Users**

**Copy privileges from:**

**Is role externally managed?**  

Check this option if this role name is mirroring an external role (such as an Active Directory group). Checking this option will prevent assigning users to this role within this application (instead the users must be assigned roles within the external system). Note, this is dependent on your selected **Authentication Profile**.

**Role description**

- Click **Save**.
- Go to App Manager > Administration > [Role Privileges](#).
- Select the **Administrator**, or equivalent, role.
- Ensure that the role has all privileges with a suggested type of **Super Admin and below** assigned to it.

**Note:** There are a few privileges that do **not** fall into this category.

**Note:** Your exact number or privileges will depend on what applications you have installed.

#### Setup security configuration in preparation for switch to STS

This step will configure the TDS application to automatically add the first user provisioned through the new STS authentication mechanism to the Administrator role. This needs to be done to prevent being locked out of the application after making the initial switch to STS authentication.

- Go to App Manager > Administration > [Security Settings](#).
- Find the **New users's default role** setting and select the role that represents "Administrators" (from the previous section).

**Tip:** This will ensure that the first time you load the application after changing the authentication mechanism you will be registered as an administrator with full permissions.

- Find the **Enable just-in-time user provisioning** setting and check it.
- Click **Save**.

#### Change the authentication mechanisms to STS

These steps will change the TDS authentication mechanism to STS security.



1. Go to App Manager > Administration > **Authentication**.
2. **Check Security Token Service**, then enter in the following information:

<b>STS Metadata Location:</b>	<input type="text" value="ex: https://app.your-company.com/federationmetadata/2007-06/federationmetadata.xml"/>
<b>Realm:</b>	<input type="text" value="ex: https://app.your-company.com/app"/>
<b>Audience URL:</b>	<input type="text" value="ex: https://app.your-company.com/app"/>
<b>WHR:</b>	<input type="text" value="ex: https://app.your-company.com/app"/>

#### Add Protocol Message Parameters (optional)

**Name:**  **Value:**

#### Add Redirect Response Cookies (optional)

**Cookie Key:**  **Cookie Value:**

**STS Metadata Location** - the [Federation metadata document URL](#) copied from Azure Portal in a previous step.

**Example:** For Azure AD: [https://login.microsoftonline.com/YOUR\\_TENANT\\_ID/federationmetadata/2007-06/federationmetadata.xml](https://login.microsoftonline.com/YOUR_TENANT_ID/federationmetadata/2007-06/federationmetadata.xml)

**Realm** - the [Application ID](#) set in Azure Portal from a previous step

**Example:** <https://demo.rizing.com>

3. Click **Save** and then click **Change** to confirm your changes.

**Note:** It may take a few moments for the application to save. Wait for it to complete.

4. Load App Manager in a new browser window.  
The application should redirect you to your IDP's sign in and then redirect you back to App Manager with you signed in.

**Tip:** You should see your name in the upper right corner.

#### Remove the temporary “new user’s default role” setting

Now that you can successfully access the application as an administrator, this step will walk you through changing the “New user’s default role” setting back to the desired role (usually a “General User” role).

1. Go to App Manager > Administration > **Security Settings**.
2. Find the **New user’s default role** setting and select the desired **Role** from the dropdown.

**Tip:** This is the role that any new users who authenticate through your IDP will be automatically assigned to. It is typically set to a restricted user type of role, such as *Standard Users*.

**Note:** If you do not wish to have any new users automatically assigned to a role, then select **Prevent automatic role assignment (for new users)**.

Your swap to STS authentication in TDS is completed. Test the application and make additional configurations for your specific needs.

**Note:** You can view users who have accessed the site and adjust their role assignment from the [User Roles](#) page.

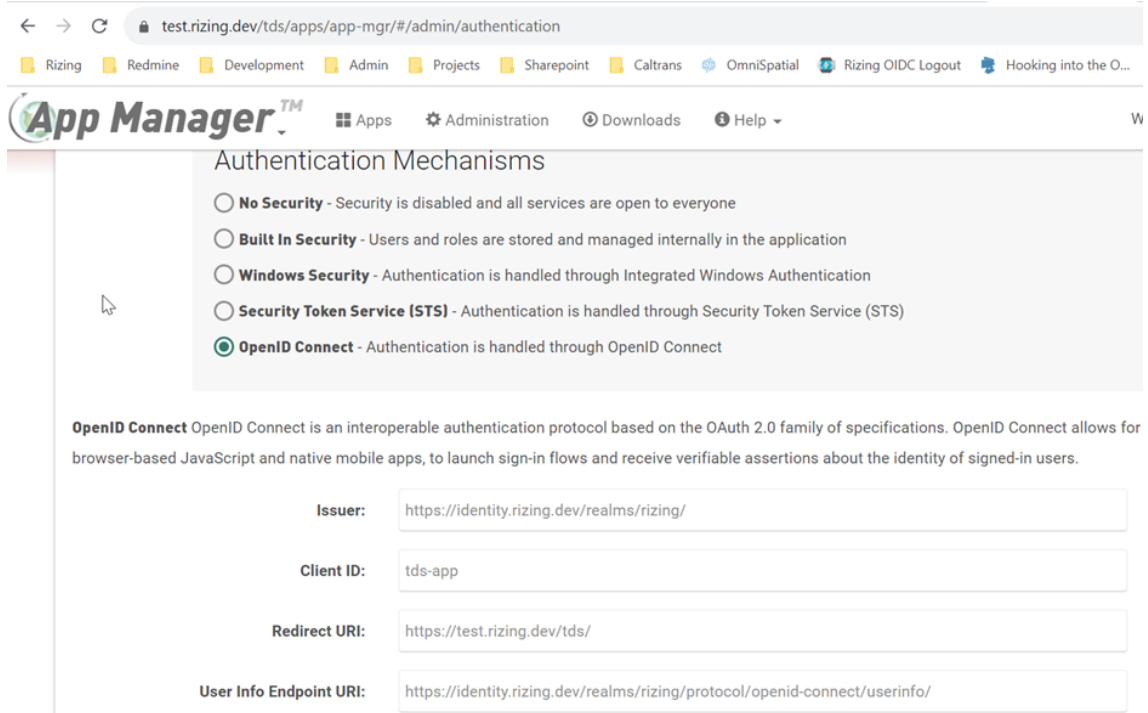
## OpenID Connect

**Note:** If you plan to use OpenID Connect as your authentication method you'll need to start by creating the application in Auth0 that will be used to authenticate your users. Please see the [Setting Up Okta Powered by Auth0](#) topic first to create and setup your Auth0 application before continuing with the steps below.

### Setting Up Application Manager (TDS) to use Auth0/Okta with OpenID Connect for Authentication For the First Time:

Before proceeding, you need to ensure that the Admin role is set as the default New user's role.

1. Open Application Manager and navigate to **Administration > Security Settings > Access and Roles** and confirm **Admin Users** is selected.
2. Next set up your [Roles](#), [Role Privileges](#) and [User Claims](#) as preferred. Once those are set up proceed to step 3.
3. Navigate to **Administration > Authentication** and select **OpenID Connect**.
4. Enter the **Issuer**, **Client ID**, and **User Info Client URI** noted while [setting up the Auth0 application](#).



5. Use your Application Manager (TDS) base URL as the **Redirect URI**.
6. Click **Save** and then click **Change** to confirm your changes.
7. The application will now restart. Lastly, you need to update the default role back to a standard user role.

8. Navigate to **Administration > Security Settings > Access and Roles** and select Standard Users (or your organization's equivalent) as the **New user's default role**.

**New user's default role:**

The role name that will be assigned to all new users. This role will be assigned to registering users (when application's security profile is set to Built-In) or user accounts automatically created during Just-In-Time Provisioning. Leave this role blank if you do not want the application to automatically assign roles for new users.

9. Click **Save**.

## Roles

The Roles feature provides the ability to create roles to assign application privileges to, or to enter Active Directory (Windows Security) roles (see note on windows security below). When you use the [RUN CONFIGURATION WIZARD](#) tool, you are prompted to create a standard authenticated user group role and an admin user group role. However, you have the freedom to create as many roles, internal or external, as you like and assign privileges to those roles as you see fit for your organization.



The screenshot shows the 'Administration' window with the 'Roles' tab selected. The main heading is 'Add application roles (to group privileges)'. Below this is a search bar with a 'Refresh' button and an 'Add New' button. A table lists the existing roles:

Role	Description	External	Actions
Admin Users	Administrator role	<input type="checkbox"/>	
Anonymous	Anonymous user acces	<input type="checkbox"/>	
Standard Users	Standard authenticated user acces	<input type="checkbox"/>	

If you are using Active Directory or Security Token Service your Role Names for these groups must match the equivalent role name in your Active Directory or Security Token Service. Under certain AD configurations you may need to delete all roles that are not in Active Directory even if they are not being used by the user. The application does not know what role the user is in, it only knows what roles are necessary to gain access to each privilege and then asks Active Directory if the user is in each of those roles.

## Usage

### Add New Role

**Role name:**

The name of the application role to create. This can be a completely new, arbitrary role name, or it can mirror the name of an external role (such as an Active Directory group). Note, when using an Active Directory group name, prefix the role name with domain and a backslash. Example: `MY_DOMAIN\Admin Users`

**Copy privileges from:**

**Is role externally managed?**

Check this option if this role name is mirroring an external role (such as an Active Directory group). Checking this option will prevent assigning users to this role within this application (instead the users must be assigned roles within the external system). Note, this is dependent on your selected **Authentication Profile**.

**Role description**

1. Click **+ Add New**. A new role form opens.
2. Enter a name in the **Role name** input box.
3. Select a role in the **Copy privileges from** dropdown list to populate a default set of privileges for the new role.

**Note:** Once the role is created, use the Role Privileges tab to modify the privileges assigned to the new role.

4. If the role is mirroring an external role, check the box beside **Is role externally managed?**

**Note:** This is dependent on your selected **Authentication mechanism**.

5. Enter a description in the **Role description** input box.
6. Click **Save** to save the new role.

### Edit a Role

🔍 | 🔄 Refresh ➕ Add New







Role	Description	External	Actions
Admin Users	Administrator role	<input type="checkbox"/>	
Anonymous	Anonymous user acces	<input type="checkbox"/>	
Standard Users	Standard authenticated user acces	<input type="checkbox"/>	

1. Click the **Edit icon** in the Actions column for the role to be edited.
2. Edit the **Role name**, **Is role external** selection, and/or **Role description**.

3. Click **Save** to save your changes, or **Cancel** to cancel the operation.

### Delete a Role

🔍 | [Refresh](#) ➕ Add New

Role	Description	External	Actions
Admin Users	Administrator role	<input type="checkbox"/>	 
Anonymous	Anonymous user acces	<input type="checkbox"/>	 
Standard Users	Standard authenticated user acces	<input type="checkbox"/>	 

1. Click the **Delete icon** next to the role to be deleted. A confirmation dialog is displayed.
2. Click **Delete** to delete the role, or **Cancel** to cancel the operation.

**Heads Up!** When the application is configured to use "Windows Security", you must still "create" the roles within this component, that you want to use from Active Directory. When using active directory roles you must also prefix your role/group names with the domain name. You must enter the exact name of the Active Directory role/group that you want to assign "privileges" to. The workflow is identical to setting up internal roles, except you do not need to assign the user to the role because the user/role relationship is already configured in Active Directory (groups). Creating the role within this component, that matches the Active Directory role is necessary because you need to be able to assign application privileges to that role.

**Note:** Leave role names blank to prevent the application from automatically assigning privileges.

## Role Privileges

The Role Privileges feature provides the ability to select and assign privileges to roles that have been defined in [Roles](#). All available application privileges are listed and managed from this tool. They are categorized and can be filtered by:

Group - the application or component the privilege belongs to

Suggested Level - the suggested user access level for the privilege ("Description of Access Levels" on page 67)

**Role Privileges**

**Assign privileges to roles**

Role: Standard Users

194 of 260 Privileges Assigned

Group	Privilege	Suggested Level	Description
app-mgr (23)			
app-mgr	Query Apps	Anonymous	Grants the ability to query and view application
app-mgr	Get App	Anonymous	Grants the ability to retrieve a single applicatio
app-mgr	Query App Profiles	Anonymous	Grants the ability to query and view application
app-mgr	Get App Profile	Anonymous	Grants the ability to retrieve a single applicatio
app-mgr	Create App Profile	Admin	Grants the ability to create application profiles
app-mgr	Update App Profile	Admin	Grants the ability to update application profiles
app-mgr	Delete App Profile	Admin	Grants the ability to delete application profiles
app-mgr	Apply Seed Data	Super Admin	Grants the ability to apply seed data to the data
app-mgr	Get Configuration Store	Admin	Grants the ability to get/view the configured da

### Usage

To modify the privileges assigned to a role:

1. Select a role from the **Role** dropdown list.
2. **Check/uncheck** the privileges you wish to assign/unassign to that role.
3. Click **Save** button.

**Heads Up!** The roles set for the Admin group and Standard user's group in [Security Settings](#) are automatically managed, so any changes you make to their privileges will not hold.

### List Options

#### Search the list

1. Click the **search icon** to expand the search field.
2. **Start typing** the name of an app, privilege or keyword.
3. The list will update to show matching items.

#### Filter



The Filter options lets you filter the groups, privileges, suggested levels, and/or descriptions you want shown in the list.

Role:

🔍 | **Filter** | 🔄 Refresh | + Add to Selection ▾ 0 of 260 Privileges Assigned

Group	Privilege	Suggested Level	Description
data-source (2)			table
data-source	Query Tables	User	Grants the ability to query for tables (discover 1
data-source	Query Columns	User	Grants the ability to query for table columns (vi
ha (1)			
ha	Build Submittal	User	Grants the ability to Build Submittal Table

1. Click **Filter**.
2. Enter the criteria for the groups, privileges, suggested levels, and/or descriptions you want filtered into the applicable box.

**Tip:** Click **Filter** again to close the filter and refresh the privileges list.

### Add to Selection

The Add to Selection option lets you filter to list by suggested level.

🔍 | Filter | 🔄 Refresh | **+ Add to Selection ▾**

Group	Suggested Levels
app-mgr (23)	<ul style="list-style-type: none"> <li> Admin</li> <li> Anonymous</li> <li> None</li> <li> Super Admin</li> <li> User</li> </ul>
app-mgr	
app-mgr	
app-mgr	
app-mgr	
app-mgr	

1. Click **Add to Selection**.
2. Select a level from the dropdown.
3. The list will update to show all privileges that match the selected level.

### Close/Open Privilege Groups

You can filter the privilege list by group.

Q | Filter | Refresh | Add to Selection | 0 of 260 Privileges Assigned

<input type="checkbox"/>	Group	Privilege	Suggested Level	Description
<input type="checkbox"/>	app-mgr (23)			
<input type="checkbox"/>	data-source (17)			
<input checked="" type="checkbox"/>	drawing (4)			
<input type="checkbox"/>	drawing	Generate Imagery	User	Grants the ability to generate, and store, image
<input type="checkbox"/>	drawing	Merge Imagery	User	Grants the ability to manipulate, and store, ima
<input type="checkbox"/>	drawing	Get Imagery	Anonymous	Grants the ability to retrieve generated imagery
<input type="checkbox"/>	drawing	Delete Imagery	User	Grants the ability to delete generated imagery (
<input checked="" type="checkbox"/>	ha (22)			
<input type="checkbox"/>	io (11)			

1 / 1 | 100 items per page | 1 - 22 of 21 items

Click the + or - to open/close the group

Click the + or - icon in the table header to open/close all the groups

### Select All/Deselect All

1. Click the **checkmark** in the table header to check all items in the list at once.
2. Click the **checkmark** in the table header again to uncheck all items in the list at once.

## Description of Access Levels

### **Anonymous**

General unauthenticated access. Provides read access and basic functionality. Typically the access level provided to public, non-logged in users.

### **User**

Provides all Anonymous privileges, plus general authenticated access. Extends read functionality with the ability to send emails, perform queries, update some items as well as other functionality typical of a standard logged in user.

### **Admin**

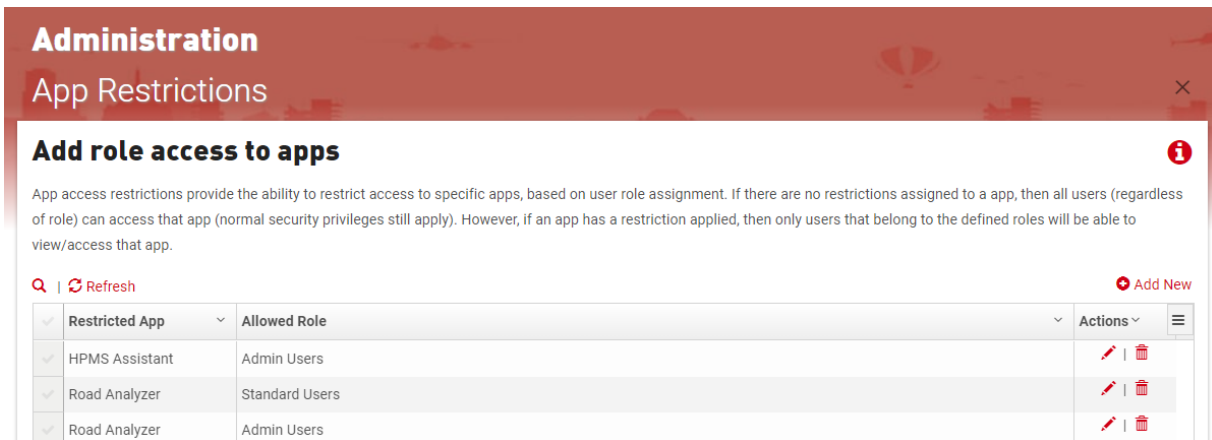
Provides all Anonymous and User level privileges, plus general admin access, such as the ability to edit and delete some items as well as manage data sources and profiles.

### **Super Admin**

Provides all Anonymous, User and Admin level privileges, plus super admin access, such as the ability to add apps, manage application configuration as well as edit databases if applicable.

## App Restrictions

App access restrictions provide the ability to restrict access to specific apps, based on user role assignment. If there are no restrictions assigned to an application, then all users (regardless of role) can access that application (normal security privileges still apply). However, if an application has a restriction applied, then only users that belong to the defined roles will be able to view and/or access that application.



**Administration**  
App Restrictions

**Add role access to apps**

App access restrictions provide the ability to restrict access to specific apps, based on user role assignment. If there are no restrictions assigned to a app, then all users (regardless of role) can access that app (normal security privileges still apply). However, if an app has a restriction applied, then only users that belong to the defined roles will be able to view/access that app.

🔍 | 🔄 Refresh ➕ Add New

Restricted App	Allowed Role	Actions
HPMS Assistant	Admin Users	✎   🗑️
Road Analyzer	Standard Users	✎   🗑️
Road Analyzer	Admin Users	✎   🗑️

### Usage

#### Add New

To add a new app restriction:

**Restrict App:**

**Allowed Role:**

Any users that belong to the selected role will be granted access to the selected app.

1. Click **Add New**.
2. Select the application you want to restrict from the **Restrict App** dropdown.
3. Select the **role** you want to have access from the **Allowed Role** dropdown.

**Note:** You will need to create a new restriction for each role you want to have access to the restricted application.

**Example:** If you have 5 total roles and want to restrict 3 of those roles from accessing an application, you will need to add a new app restriction for each of the 2 roles that are allowed access to that application.

4. Click **Save**.

#### **Edit Existing**

To edit an existing app restriction:

1. Click the **pencil icon** in the Action column of the App Restriction you want to edit.
2. Make your edit(s).
3. Click **Save**.

#### **Delete Existing**

To delete an existing app restriction:

1. Click the **trashcan icon** of the App Restriction you want to delete.
2. Click **Delete** in the popup confirmation.

## Profile Restrictions

Profile access restrictions provide the ability to restrict access to specific profiles, based on user role assignment. If there are no restrictions assigned to a profile, then all users (regardless of their role) can view and access that profile (normal security privileges still apply). However, if a profile has a restriction applied, then only users that belong to the defined roles will be able to view and/or access that profile.

Administration

Profile Restrictions
×

### Add profile access to roles i

Profile access restrictions provide the ability to restrict access to specific profiles, based on user role assignment. If there are no restrictions assigned to a profile, then all users (regardless of role) can view that profile (normal security privileges still apply). However, if a profile has a restriction applied, then only users that belong to the defined roles will be able to view/access that profile.

Q | Refresh Add New

	Restricted App	Restricted Profile	Allowed Role	Actions
✓	Road Analyzer	Portal Test	Standard Users	✍   🗑
✓	Road Analyzer	Portal Test	TSS\TSS Users	✍   🗑
✓	Segment Analyzer	Portal Test	Standard Users	✍   🗑
✓	Segment Analyzer	Portal Test	TSS\TSS Users	✍   🗑
✓	Validation Assistant	HPMS TEST Oracle - All	TSS\TSS Users	✍   🗑
✓	Validation Assistant	HPMS TEST SQL Server - All	TSS\TSS Users	✍   🗑

## Usage

### Add New

To add a new profile restriction:

Restrict App:

Restrict Profile:

Allowed Role:

Any users that belong to the selected role will be granted access to the selected profile.

✕ CANCEL
✓ SAVE

1. Click **Add New**.
2. Select the application you want to restrict from the **Restrict App** dropdown.
3. Select the **profile** that you want to restrict from the **Restrict Profile** dropdown.

4. Select the **role** you want to have access from the **Allowed Role** dropdown.

**Note:** You will need to create a new restriction for each role you want to have access to the restricted profile.

**Example:** If you have 5 total roles and want to restrict 3 of those roles from accessing a profile, you will need to add a new profile restriction for each of the 2 roles that are allowed access to that profile.

5. Click **Save**.

#### **Edit Existing**

To edit an existing profile restriction:

1. Click the **pencil icon** in the Action column of the Profile Restriction you want to edit.
2. Make your edit(s).
3. Click **Save**.

#### **Delete Existing**

To delete an existing profile restriction:

1. Click the **trashcan icon** to the left of the Name of the Profile Restriction you want to delete.
2. Click **Delete** in the Delete Profile Restriction popup.

## Templates

Template management provides the ability for Administrators, with the proper role privileges, to manage access to Segment Analyzer and Road Analyzer templates, based on a user role assignment. If there are no shares assigned to a template it is marked as "Public" and all users, regardless of role, can view that template in read-only mode. Templates can also be deleted and ownership of a template can be changed, even if they have not been shared. Only the **users in roles** with template shares **privileges** will be able to manage the share access of any template. See [Template Share Privileges](#) below for configuration details.

**Administration**

**Templates**

### Manage Templates

Template management provides the ability to restrict access to specific templates, based on a user role assignment. If there are no shares assigned to a template, then all users, regardless of role, can view that template in read-only mode.

[Refresh](#) | 
 [Delete Selected Templates](#) | 
 [Change Ownership](#) | 
 [Change Selected Sharing](#)
[Add New Template Share](#)

Name	App Name	Profile ID	Owner Name	Shared	Role	Actions
TOPS - Full SQL	Segment Analyzer	test_1071_sql	Catrina Wingate	Public		
KDOT Standard Temp 3	Segment Analyzer	test_kdot_standard	Jodie Locklear	Read	TEST_RH Editor	
SA-TC-05 Oracle - Output wit...	Segment Analyzer	test_1061_ora	Jodie Locklear	Public		
KDOT User Temp 1	Segment Analyzer	test_kdot_user	Jodie Locklear			

## Usage

### Template Share Privileges

The ability to view, save, update and manage template sharing is managed at the **user role** level by the following **role privileges**:

**Note:** The owner of a template will have full access to the template, even if they are not in the shared role(s).

### Manage Template Shares at the Template Level:

**Share Templates** (ID: 164) - grants the ability to share Road Analyzer templates when saving them, and the ability to update the share access of any templates shared with the user's role

**Share Templates** (ID: 214) - grants the ability to share Segment Analyzer templates when saving them, and the ability to update the share access of any templates shared with the user's role

### Manage Template Shares from Application Manger at the Admin Level:

**Manage All Templates And Shares** (ID: 43) - grants the ability to manage all templates and template sharing in App Manager, as well as, the ability to edit the share access of any *shared* template in the Road Analyzer and Segment Analyzer **Manage Templates** dialogs

### Search the list

1. Click the **search icon** to expand the search field.



2. **Start typing** the name of a template.
3. The list will filter to show all matching template(s).

### Add New Template Share

To add a new template share:

**Application:** Road Analyzer

**Profile:** TEST 1071 SQL

**Template:** Base Template

**Share Access:**

Not shared  
 Share with everyone (read-only)  
 Share with role

**+ ADD ROLE ACCESS**

	Role	Access
<input type="checkbox"/>	Standard Users	Write
<input type="checkbox"/>	Anonymous	Read

1. Click **Add New Template Share**.
2. Select the application you want from the **Application** dropdown.
3. Select the **profile** that you want from the **Profile** dropdown.
4. Select the template you want to set the share access from the **Template** dropdown.
5. Select the **Share Access** from the options listed:

**Not Shared** - only the owner can use and edit the template within the application

**Share with everyone (read-only)** - every user can use the template, but they will not be able to make changes to the template share access or overwrite the template

**Share with role** - the Role(s) selected will have the selected access to the template

**Note:** Any administrators with the [Manage All Templates And Shares](#) privilege can manage any template from within App Manager.

#### Add Role Access:

1. Click **Add Role Access**.
2. Select the role you want to have access to the selected template from the **Role** dropdown.

**Heads Up!** Unless **Just-in-Time Provisioning** is enabled, only **built-in roles** will be available in the dropdown.

4. Select the type of access you want the selected role to have for the selected template from the **Access** dropdown.

**Read** - the users in the selected role can use the template

**Write** - the users in the selected role can use and edit the template

6. Click **Save**.

#### Edit Template Sharing

##### To edit a single template share:

1. Click the **pencil icon** in the Action column of the template you want to edit.
2. Make your edit(s).
3. Click **Save**.

##### To edit multiple template shares:

1. Click the check boxes beside the templates you want to edit the share access of.
2. Click **Change Selected Sharing** at the top of the table.
3. Make your edit(s) to the **Share Access**.
4. Click **Save**.

#### Delete Template

##### To delete a single template:

1. Click the **trashcan icon** to the left of the Name of the template you want to delete.
2. Click **Delete** in the Delete Template popup.

##### To delete multiple templates:

1. Click the check boxes beside the templates you want to delete.
2. Click **Delete Selected Templates** at the top of the table.
3. Click **Delete** in the Delete Template popup.

#### Remove Template Sharing

##### To remove a single template share:

1. Click the **trashcan icon** to the left of the Name of the template you want to remove the template share access.
2. Click **Remove** in the Remove Template popup.

##### To remove multiple template shares:

1. Click the check boxes beside the templates you want to remove the share access of.
2. Click **Change Selected Sharing** at the top of the table.
3. Select **Not Shared**.
4. Click **Save**.

#### Change Ownership

**To change the ownership of a single template:**

1. Click the check box beside the template you want to change the ownership of.
2. Click **Change Ownership** at the top of the table.
3. Select the new **Owner** from the dropdown.
4. Click **Save**.

**To change the ownership of multiple templates:**

1. Click the check boxes beside the templates you want to change the ownership of.
2. Click **Change Ownership** at the top of the table.
3. Select the new **Owner** from the dropdown.
4. Click **Save**.

## Users and User Roles

The User Roles feature provides the ability to search, add, and manage users in your defined roles.

### User Roles

#### Assign users to roles

🔍 Refresh
➕ Register New User

✓	Last Name	First Name	Username	# Assigned Roles	Email	Source	Actions
✓			cwingate	0	cwingate@tss.tssgis.c...	Built-in	✎   🗑
✓		Jodie	jodieTest	0	locklear_j@yahoo.com	Built-in	✎   🗑
✓	User	Admin	siteadmin	1	rgreen@tssgis.com	Built-in	✎   🗑
✓			jlocklear	0	jlocklear@tss.tssgis.co...	Built-in	✎   🗑

**Note:** To be able to assign of internal roles to external users, you will need to enable Just-in-time (JIT) provisioning in the [Security Settings](#). That will enable the application to create an internal application user based on an external user's information.

### Usage

Add New

#### Assign users to roles

🔍 Refresh
➕ Register New User

✓	Last Name	First Name	Username	# Assigned Roles	Email	Source	Actions
✓			cwingate	0	cwingate@tss.tssgis.c...	Built-in	✎   🗑

To add a new user:

1. Click **+ Register New User** to open the new user registration form.

**First Name:**   
**Last Name:**   
**User Name:**   
**Email:**   
**Password:**   
**Confirm Password:**

2. Fill in the **First Name**, **Last Name**, **User Name**, and **Email**.
3. Enter a password in the **Password** field and then enter it again in the **Confirm Password** field.
4. Click **Register**.

#### Search User list

1. Click the **search icon** to expand the search field.
2. **Start typing** the name of a user.
3. The list will update to show the matching user(s).
4. Click **Refresh** to refresh the user list.

#### Assign User to Role(s)

To assign, or edit, the role(s) assigned to a user:

🔍 Refresh ➔ Register New User


✓ Last Name	First Name	Username	# Assigned Roles	Email	Source	Edit user
✓ Smith	Mike	msmith	2	mbanick@tssgis.com	Built-In	✎ 🗑

1. Locate the row for the User whose roles you want to edit and click **Edit** (pencil icon), or click **the number** (in the **# Assigned Roles** column).
2. Check the role(s) you want to add the user to by clicking the **checkmark** in the far left field beside the Role. To remove the user from any role(s), click the **checkmark** to uncheck the role(s).
3. Click **Save** and then click **Save** in the popup.

## Delete User

To delete a single existing user:









Q | Refresh Register New User

Last Name	First Name	Username	# Assigned Roles	Email	Act <b>Delete user</b>
Walden	Tim	Timmy	1	mbanick@tssgis.com	

1. Locate the row for the user you wish to delete and click the **Delete** icon.
2. Click **Delete** in the confirmation popup.

To delete multiple users:

Q | Refresh **Delete Selected** Register New User

Last Name	First Name	Username	# Assigned Roles	Email	Actions	
<input checked="" type="checkbox"/>	Walden	Tim	Timmy	1	mbanick@tssgis.com	 
<input checked="" type="checkbox"/>	Banick	Matthew	mattb	1	mbanick@tssgis.com	 
<input checked="" type="checkbox"/>	Jimmerson	Jim	Jimmy	1	mbanick@tssgis.com	 
<input type="checkbox"/>	User	Admin	siteadmin	1	rgreen@tssgis.com	 

1. In the users list, find the users you wish to delete and click the **checkmarks** to the left of them.
2. Click **Delete Selected** in the Template table header.
3. Click **Delete** in the confirmation popup.

## Map User Claims

The Map Claims feature provides the ability to map custom user claims.



**Administration**  
Map Claims

### Map Custom Claims

Q | Refresh Add New

System Claim	Custom Claim	Actions
Name	http://schemas.tssgis.com/ws/2017/01/identity/claims/customemailaddress	

### Usage

#### Add New

**System claims:**

**Custom claim:**

1. Click **+ Add New** to open the new claim form.
2. Select a claim in the **System claims** dropdown list.
3. Enter the custom claim in the **Custom claim** input box.
4. Click **Save** to save the new claim.

#### Search Existing

1. Click the **search icon** to expand the search field.
2. **Start typing** the name of a claim.
3. The list will update to show the matching claim(s).
4. Click **Refresh** to refresh the list.

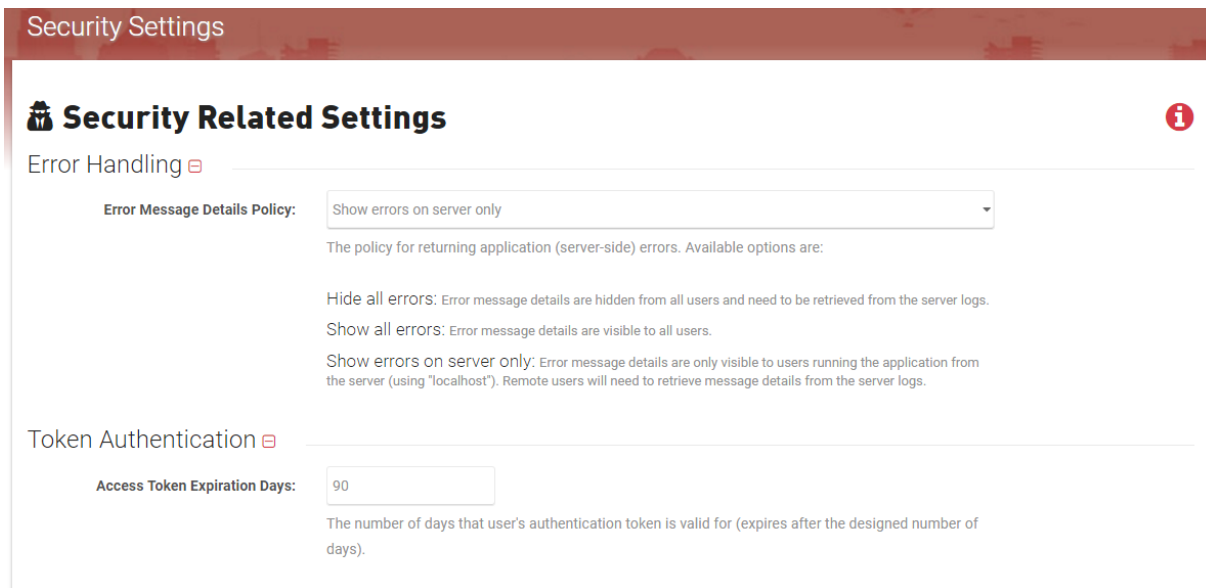
#### Delete Existing

To delete an existing claim:

1. Click the **trashcan icon** on the line of the Custom Claim you want to delete.

## Security Settings

Changes to security related configurations, such as token expiration time or what servers the applications can make requests from, are set in Security Settings.



**Security Settings**

### Security Related Settings

**Error Handling**

**Error Message Details Policy:** Show errors on server only

The policy for returning application (server-side) errors. Available options are:

- Hide all errors: Error message details are hidden from all users and need to be retrieved from the server logs.
- Show all errors: Error message details are visible to all users.
- Show errors on server only: Error message details are only visible to users running the application from the server (using "localhost"). Remote users will need to retrieve message details from the server logs.

**Token Authentication**

**Access Token Expiration Days:** 90

The number of days that user's authentication token is valid for (expires after the designed number of days).

**Tip:** If you want to hide or expand one of the sections, click the square at the end of the section name.

## Usage

### Error Handling

#### Error Message Details Policy

This sets the policy for returning application (server-side) errors. When errors are hidden, the application will give a generic "An error occurred" message, but when errors are shown the user will get a detailed error message. Available options are: Hide all errors, Show all errors, and Show errors on server only.

#### To Use:

1. Select the desired option from the dropdown.
2. Click **Save** at the bottom of the page.

### Token Authentication

#### Access Token Expiration Days

This sets the number of days that a user can stay logged in without needing to sign in.

#### To Use:



1. Enter the desired number of days.
2. Click **Save** at the bottom of the page.

#### Enable sliding expiration for authentication cookies

Enabling this will re-issue a new cookie with a new expiration time when a request is made more than halfway through the expiration window.

#### To Use:

1. Check/uncheck the box beside **Enable sliding expiration for authentication cookies**.
2. Click **Save** at the bottom of the page.

#### Prevent Auto Sign Out Feature

This prevents the default behavior of the application forcing all users to re-authenticate the next time they sign into the application when changes are made to any role or role's privileges.

#### To Use:

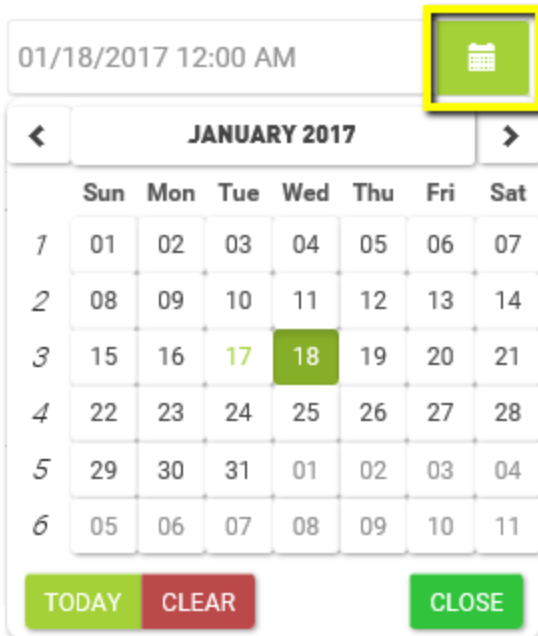
1. Check/uncheck the box beside **Prevent auto sign out feature**.
2. Click **Save** at the bottom of the page.

#### Invalidate All Tokens Before

This sets the date and time all tokens will expire, so that all users must be re-authenticated.

#### To Use:

1. Click the calendar and select a date.



The image shows a date selection interface. At the top, a text box displays the current date and time: "01/18/2017 12:00 AM". To the right of this text box is a green square button with a white calendar icon, which is highlighted with a yellow border. Below the text box is a calendar for "JANUARY 2017". The calendar has a header row for the days of the week: Sun, Mon, Tue, Wed, Thu, Fri, Sat. The dates are arranged in a grid. The date "18" is highlighted in green, indicating it is the selected date. At the bottom of the calendar, there are three buttons: "TODAY" (green), "CLEAR" (red), and "CLOSE" (green).

**Tip:** The time will be defaulted to **12:00 AM** unless changed.

2. Or Enter in the desired date and time.

**Heads Up!** The expected format is **MM/dd/yyyy h:mm a**.

3. Click **Save** at the bottom of the page.

### Reset Password Token Expiration Hours

This sets the number of hours the link to reset a user's password will remain valid.

#### To Use:

1. Enter the desired number of hours.
2. Click **Save** at the bottom of the page.

### Cross Origin Resource Sharing

#### Disable same site mode for cookies authentication

Sets the SameSite cookie to none to indicate that same site restrictions should be disabled by the client and to allow cross-site cookie use. When using TDS (or any of the applications within TDS) in an iframe, it may experience issues if using sameSite=Lax or sameSite=Strict cookies, because iframe is treated as cross-site scenario. Hence, its recommended to disable it and set the same-site mode to 'None'. Note: Cookies that assert SameSite=None must also be marked as Secure. In this case, TDS will need to be secure site accessed using 'https'.

#### To Use:

1. Check/uncheck the box beside **Disable same site mode for cookies authentication**.
2. Click **Save** at the bottom of the page.

### Allowed CORS Settings

These options allow you to specify what servers the application(s) can make requests from. For more information: [HTTP access control\(CORS\)](#).

**Example:** If you have tds on one server and Road Analyzer on a separate server, this will allow Road Analyzer to make requests to the server tds is on. Enter "\*" to allow requests from all servers, or enter in the specific server(s) that you will allow requests from.

#### To Use:

1. Enter the **Allowed CORS Origins, Headers, and/or Methods**.
2. Click **Save** at the bottom of the page.

### Access and Roles

#### System Administrator "Username"

The System Admin is built-in and has global access to everything no matter what role/privilege they are in and will be available no matter security you choose for the application. If you used the [Configuration Wizard](#) this will already be filled in.

**To Use:**

1. Enter the desired **System administrator "username"**.
2. Click **Save** at the bottom of the page.

**Anonymous Access Role Name**

You can select the role name that has the privileges anonymous users will receive.

**To Use:**

1. Select the desired role name from the **Anonymous access role name** dropdown list.
2. Click **Save** at the bottom of the page.

**Auto-managed role privileges**

You can select whether or not to have the role privilege mapping to be handled automatically within the application itself, or be based on the suggested privilege levels and semantically defined role types you set.

**To Use:**

1. To enable, check the box beside **Auto-managed role privileges**.
2. Click **Save** at the bottom of the page.

**Admin and Standard Group Role Names**

You can assign roles to admin and standard users with default privileges. If you install any new applications, these roles will be automatically assigned privileges.

**Heads Up!** If you are using Active Directory or Security Token Service your Role Names for these groups *must* match the equivalent role name in your Active Directory or Security Token Service. If they do not, the application will not recognize you and will be locked out.

**To Use:**

1. Select the desired **Role Name** from each of the dropdowns.

**Note:** The options available in the dropdowns for these roles are from the [Roles](#) section. If you do not want a role, you can select **Prevent automatic privilege assignment** options.

2. Click **Save** at the bottom of the page.

**New User's Default Role**

You can set the role name that will be assigned to all new users or prevent automatic assignment of a role.

**To Use:**

1. Select the desired **Role Name** from the dropdown.

**Note:** The options available in the dropdowns for these roles are from the [Roles](#) section. If you do not want a role, you can select **Prevent automatic privilege assignment** options.

2. Click **Save** at the bottom of the page.

## Users and Registration

### Enable Just-in-time Provisioning

To create a user account for external users, enable this setting. With Just-in-time (JIT) provisioning, an internal application user will automatically be created based on the external user information.

#### To Use:

1. To enable, check the box beside **Enable Just-in-time provisioning**.

**Note:** The options available in the dropdowns for these roles are from the [Roles](#) section. If you do not want a role, you can select **Prevent automatic privilege assignment** options.

2. Click **Save** at the bottom of the page.

### Max Users to Return

In [Users and User Roles](#), this will set the maximum number of users the application will search for and display in the list.

#### To Use:

1. Enter the desired number of users.
2. Click **Save** at the bottom of the page.

### New User Registration Notification Email

When a new user registers in any of the TDS applications an email will be sent if the following information is filled out. Further configure this email content by adjusting the subject line and template to suit your needs.

**New User Registration Notification  
Email:**

ex: admin@example.com

The "email address" to send notifications to, when a new user registration occurs.

**New User Registration Notification Email  
Subject Line:**

New User Registered

The "subject" of the email that will be sent when a new user is registered.

**New User Registration Notification Email  
Template:**

A new user, {{firstName}} {{lastName}} ({{userName}}), has registered. This user will need to be assigned to a security group, in order for them to fully access application functionality.<br><br>You can contact {{firstName}} {{lastName}} at {{userEmail}}.

The "body" of the email that will be sent when a new user is registered.

#### To Use:

1. Enter the desired **Email**.
2. *Optional:* Edit the default **Subject Line** and/or **Email Template**.
3. Click **Save** at the bottom of the page.

## Password Reset

In these settings you can specify the subject line and body of the password reset email for your organization.

### Password Reset

**Reset Password Email Subject Line:**

The "subject" of the email that will be sent when resetting a password.

**Reset Password Email Template:**

```
{{firstName}},<br><br>Here is the reset password link:<br><a href="{{redirectTo}}?resetToken={{resetToken}}&resetUserName={{userName}}">{{redirectTo}}?resetToken={{resetToken}}&resetUserName={{userName}}</a><br><br>Simply click or paste the above link into your browser's address bar to reset your account's password. This is a one-time use link, it will instantly expire once
```

The "body" of the email that will be sent when resetting a password.

### To Use:

1. Enter the desired **Subject Line** and/or **Email Template**.
2. Click **Save** at the bottom of the page.

### Reset to Default



Should you want to reset to default all security settings, click **Reset** and select **Save** on the confirmation popup.

**Heads Up!** Be aware that a few other security settings that are not visible in this form will also be reset.

## Access Tokens

Access Tokens are mechanisms to create a security token to access specific TDS REST services. For example, you could have an external service or process that needs to:

- kick off an SA template
- get a report
- or any other TDS API request

The Access token tool provides the ability to generate a token and then pass the token as a parameter when the service is called without the need for additional authentication. Authentication is provided by the token.

**Manage Access Tokens**

Create and manage security access tokens. Access tokens provide the ability to pre-authenticate services, so that an access token can be generated and passed through a URL in a stateless manner, bypassing the normal token authentication mechanism.

Q | Filter | Refresh Add New

Token	Description	Created By	Behavior	Expires	# Privileges	Actions
b73b4bfba79849198b89...	Test the Demo database ...		Never Delete		1	
48d2f2973371486bbbf3...	get report		Delete On Expire	12/29/17 06:28 PM	1	

## Usage

### Add New

To add a new access token:

1. Click **+ Add New** to expand the new Access Token form.

**+ Enter New Access Token**

**Description:**

**Behavior:**

**Expiration Date:**

Token will expire in **1 day**

2. Fill in the **Description**, **Behavior** and **Expiration Date**.

*Behavior Options include:*

- Token expires on specified data - this is the default setting and will auto set the token to expire in 24 hours
- Delete on first use (one time use only) - token can only be used once and will expire itself immediately after use
- Token never expires (valid until manually deleted - token must be manually deleted to expire)

**Tip:** Deleting a token also expires it.

- Select the privileges in the **Available Privileges** table that you wish the token to provide authorization for. Available privileges are based on your user role.

Available Privileges Privileges that are accessible when using this token

Q | Filter | Refresh 2 of 330

ID	Product	Name	Access Level
12003	data-source	Create Data Source	Admin
12004	data-source	Delete Data Source	Admin
✓ 12005	data-source	Test Data Source	User
12006	data-source	Recreate Data Source	Super Admin
✓ 12007	data-source	Query Tables	User
12008	data-source	Query Columns	User
12009	data-source	Query Data	User

- Click **Save**. Once saved the token will display under the list of privileges.

Items per page: 1000 Super Admin

1 - 330 of 330 items

Token:

Usage Example: `https://YOUR_SERVER/tds/api/YOUR_ENDPOINT?_token=b73b4bfa79849198b8914ae9782484b2850d[REDACTED]`

- To use the token, suffix your endpoint URL with the token provided.

### Updating Existing

To update an existing access token:

Q | Filter | Refresh Add New

Token	Description	Created By	Behavior	Expires	# Privileges	Actions
✓ b73b4bfa79849198b89...	Test the Demo database ...		Never Delete		1	
✓ 48d2f2973371486bbbf3...	get report		Delete On Expire	12/29/17 06:28 PM	1	

- Locate the row for the token you wish to edit and click **Edit** (pencil icon).
- Make desired changes to the form.
- Click **Save**.

### Delete Existing

To delete an existing access token:

Q | Filter | Refresh Add New

Token	Description	Created By	Behavior	Expires	# Privileges	Actions
✓ b73b4bfa79849198b89...	Test the Demo database ...		Never Delete		1	
✓ 48d2f2973371486bbbf3...	get report		Delete On Expire	12/29/17 06:28 PM	1	



1. Locate the row for the token you wish to delete and click **Delete**.
2. Click **Delete** in the confirmation popup.



## Databases

[Configuration Store](#) - pick where to save your configuration data

[Data Sources](#) - setup database connections for your applications

[LRS Metadata](#) - setup and configure non-ArcGIS Server Extension layers and metadata

[Import Seed Data](#) - makes importing configurations easy

[Export Seed Data](#) - easily export application configurations as a seed file

[Editing Seed Files](#) - learn how to update your domains and profiles using a seed file

## Configuration Store

Your applications need somewhere to keep your settings and application changes so they are persisted across sessions. By default App Manager will store your configurations in a local file database (.SDF file) on the server. However, the Configuration Store feature provides the ability for you to manage this setting and specify a specific database if you choose.

### Config Store

#### Configuration Database

**Where would you like us to store your configuration data?** The application needs somewhere to keep your settings and application changes so that we can persist them across sessions. Typically the amount of data that needs to be stored is very minimal, and includes things like; user preferences, saved templates, and application profiles. By default, the application will store your configuration in a local file database (.sdf file) on the server. This is typically an acceptable solution, however you have the ability to store this information in an enterprise database as well (such as SQL Server or Oracle).

Where would you like to store your configuration?

Use the default

Specify a database

**Note:** See the [Advanced Configurations](#) section for details on configuration architecture, database requirements, and other technical details.

### Choosing a Storage Mechanism

The default Configuration Store, a SQL Server Compact Edition database (.SDF file), is only recommended to be used when the physical storage demands for the applications is expected to be relatively lightweight. SQL Server Compact Edition DB is a file-based database which is restricted by the limitations of the operating system's file system. Such as: file size, read/write time, availability, etc. The default configuration store (SQL Server Compact Edition) will typically perform satisfactorily under normal circumstances. However, if it is expected that the applications will be heavily used by many concurrent users or if a large amount of data will be stored (for example, the use of Road Video Viewer) then it is highly recommended to use an enterprise configuration storage mechanism (such as SQL Server or Oracle). The information below can be used to help decide which storage mechanism is right for you.

#### Reasons to use SQL Server Compact Edition (default) Configuration Store

- If only a few profiles and associated data (templates, settings, etc) are expected to be used
- If you are evaluating TDS or associated software
- If you plan to migrate to another environment or platform in the near future
- If an enterprise database is not available

#### SQL Server Compact Edition Configuration Store

##### Pros

- Easy setup (no separate database required)
- Light weight
- Easy to backup and restore

#### Cons

- Limited to up to 4 GB in data storage (not heavily scalable)
- Database performance will degrade if considerable storage is used (+- 2GB)
- Cannot be “tuned” like an enterprise database

#### Enterprise Configuration Store

#### Pros

- Best option for optimal performance
- Supporting staff have familiarity
- Backup and restoration process can be adopted from existing procedures
- Easier scalability

#### Cons

- Requires more setup time and maintenance effort

## Usage

#### To use the default:

1. Click **Use the Default**.
2. Click **Save**.

#### To specify a database:

1. Click **Specify a Database**.
2. Enter the data source ID in the **Data Source ID** input box.
3. Select a database type from the **Database Type** dropdown.
4. Enter your database connection string in the **Connection String** input box.
5. Click **Test Connection** to verify the connection works.
6. Click **Save**.

#### To migrate TDS from one Configuration Store to another:

This exercise demonstrates migrating a TDS configuration store from SQL Server Compact Edition (the default) to an enterprise database (SQL Server or Oracle).

#### Prerequisites:

When using an enterprise database (such as SQL Server or Oracle) as a configuration store, the database should be a new empty database and the connection to this database should use a database user that is the schema owner of its own schema (a user with read/write to its own schema only). When configuring this Configuration Store connection string, it is important to use a database user that does not have access to anything outside of this "TDS" configuration database to mitigate any risk of inadvertently modifying or accessing other data. [Click here for more details](#).

Make sure the new configuration store database is empty.

Make sure the connection, which will be configured in App Manager, to connect to the new configuration store database has

privileges to read, create, and delete objects (only to the desired schema though).  
 Make a backup of the application and existing configuration store, as a precaution.

**Procedure Steps:**

**Step One - Export current Configuration Store to a seed file**

1. Install the latest available Rizing Geospatial software to insure you're running the most up to date versions.
2. Open **App Manager** and click the **Administration** tab.
3. Click **Export Seed Data**.
4. Select all items you want to migrate to the new configuration store.

**Heads Up!** Any items that have approximately 1,000 or more records should not be exported. This seed export step will export to a single text file and it is not practical to export extremely large amounts of data this way. If you have Road Video Viewer, do *not* select **Camera Images** or **Event Points** – these items should only be seeded using the original seed files generated through the [TIM processing tool](#).

5. Click the **Download Selected** button and then **Continue**.

**Export Your Seed Data** Configuration store export

Select the data items that you would like to export to a "seed file" (.tss file). The available data items are derived from the currently installed applications. You can export the entire configuration store, by not selecting anything, or you can pick and choose specific items to export.

**Heads up!** There are tables with a large number of records available. It is recommended that these tables be exported and migrated directly through the database rather than through exporting a seed file. Writing large amounts of data to a seed file can result in slow or unresponsive application performance.

Product	Entity Alias	Record Count
security	Security Configuration	1
security	Users	1
Validation Assistant	Profiles	11
Validation Assistant	Validation Groups	14
Validation Assistant	Validations	340
Road Video Viewer	Camera Images	2,869,762
Road Video Viewer	Cameras	
Road Video Viewer	Event Points	
Road Video Viewer	Profiles	

Download Seed Data

Are you sure you want to download a seed data file?

CONTINUE CANCEL

CLOSE DOWNLOAD SELECTED (25)

Wait for the seed file to finish downloading before proceeding to the next section.

**Step Two - Change the TDS Configuration Store**

1. Launch **App Manager** and click on the **Administration** tab.
2. Click **Configuration Store**.
3. If it is not already selected, click the **Specify a database** option.

**Note:** You may want to copy the original connection string in case you need to revert to this configuration store at any point.

4. Enter the data source ID in the **Data Source ID** input box.

5. Select a database type from the **Database Type** dropdown.
6. Select the database type to change the configuration store to.
7. Enter the **Connection String** to the new configuration database (see prerequisites for details on this database).

**Heads Up!** When using Oracle as the Configuration Store, your Connection String should include "Direct=true" to ensure proper connection.

**Example: Oracle Connection (without TNS names entry)**

```
Data Source=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=YOUR_HOST)(PORT=1522)))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=YOUR_SERVICE)));Direct=true;User Id=YOUR_USER;Password=YOUR_PASSWORD;
```

**Oracle Connection (with TNS names entry)**

```
Data Source=YOUR_SOURCE;Direct=true;User Id=YOUR_USER;Password=YOUR_PASSWORD;
```

**Oracle Connection (without TNS names entry)**

```
Data Source=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=YOUR_HOST)(PORT=1522)))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=YOUR_SERVICE)));Direct=true;User Id=YOUR_USER;Password=YOUR_PASSWORD;
```

**Oracle Connection (with TNS names entry)**

```
Data Source=YOUR_SOURCE;Direct=true;User Id=YOUR_USER;Password=YOUR_PASSWORD;
```

**Tip:** Use the **Examples** dropdown menu to see available connection string examples.

8. Click **Test Connection** and verify that the connection succeeded.
9. Click **Save** and then **Confirm**.  
The application may take several minutes to swap to the new configuration store and setup the new database objects. It should take you back to the **Administration** page once it is complete.

**Note:** If you receive an error message, and are locked out of Application Manager, you can swap the configuration store connection back to the original connection by opening the TDS web.config file and updating the connection string and provider name for the "DefaultConnection" connection string.

10. Click the **Configuration Store** link and verify that the correct new database connection information is showing.

### Step Three - Apply Seed File (from previous configuration store)

1. Launch **App Manager** and click on the **Administration** tab.
2. Click the **Import Seed Data** link.
3. Drop the **seed file** (the one that was exported earlier) into the gray box (optionally you can click on the gray box and select the file).
4. Click **Save** and then **Save** the confirmation dialog.
5. After a moment, the page will show a **Seeding Job History** list and you should see the status of the seed file import. Remain on this page until it is complete – this may take several minutes depending on the amount of data being imported.
6. Once the seed file process is complete, click on the **Details** link to check for any import errors.
7. Check the **Last Message** details to verify that there are 0 errors.

**Last Message:** ✕

Total records added: 1474  
Total records updated: 33  
Total records deleted: 0  
Total number of errors: 0

8. At this point the new configuration store should be restored to the previous (based on what you selected to export to the seed file).



9. Navigate through the App Manager **Administration** and **Apps** pages to verify that all the expected profiles and settings are in place.
10. Test each application and verify that all data and settings are present.

# Data Sources

Data Sources provide a way to add, remove, and update the data sources that you wish to have access to within the application.

**Administration**  
Data Sources

**Enter Your Data Sources** Connect to your data

Data sources provide access to your data from various applications and tools. Data sources can consist of a simple database connection string and provider name, and/or a service URL that points to a map service that is published with the specified connection string. A data source does not have to have both a database connection and a service URL, but if both are provided the two must point to the same database.

Filter Refresh Add New

Status	Name	Provider	Description	Actions
✓	TEST 1060 SQL	SQL Server	Test 1060 SQL Server Database Conne...	[Icons]
✓	TEST 1060 ORACLE	Oracle	Test 1060 Oracle Database Connection	[Icons]
✓	TEST 1051 SQL	SQL Server	Test 1051 SQL Database Connection	[Icons]
✓	TEST 1051 ORACLE	Oracle	Test 1051 Oracle Database Connection	[Icons]
✓	TEST 1041 SQL	SQL Server	Test 1041 R&H Database connection	[Icons]
✓	TEST 1041 ORACLE	Oracle	Test 1041 Oracle Database Connection	[Icons]

## Usage

### Add New

To add a new data source:

1. Click **+ Add New** to expand the new Data Source form.

**Enter Your Data Sources** Connect to your data

Data sources provide access to your data from various applications and tools. Data sources can consist of a simple database connection string and provider name, and/or a service URL that points to a map service that is published with the specified connection string. A data source does not have to have both a database connection and a service URL, but if both are provided the two must point to the same database.

Filter Refresh Add New

Status	Name	Provider	Description	Actions
✓	TEST 1060 SQL	SQL Server	Test 1060 SQL Server Database Conne...	[Icons]
✓	TEST 1060 ORACLE	Oracle	Test 1060 Oracle Database Connection	[Icons]

**Note:** For different data base connection examples, click Examples in the upper right corner and select the example that best matches your connection type.

**+ Enter New Data Source**

Name:

Description:

Database Type:

Examples

- SQL Server Connection
- SQL Server Compact (SQL CE) Connection
- Oracle Connection (without TNS names entry)
- Oracle Connection (with TNS names entry)

2. Fill in the **Name**, **Description**, and **Database Type**.
3. Enter the **Connection String**. Use the **Test Connection** button to verify the string.

**Click if entering a data source for a Configuration Store**

1. You have the option here for App Manager to automatically create a **Configuration Store** database for you on your selected database.
2. Click the down arrow on the **TEST CONNECTION** button and click **Test and create database if none exists**.



4. Enter the **Associated Service URL**.

**Note:** Once entered the URL will be tested and the result will be displayed below the input box.

5. If you want the application to authenticate with ArcGIS for Portal, check the box beside **Service requires ArcGIS for Portal authorization**.

**Heads Up!** If you selected this option, you will need to ensure that TDS has been configured to use Portal for ArcGIS. See the [Configure Portal for ArcGIS](#) topic for more details. You will also need to add your **ArcGIS for Portal URL** in the [Application Settings](#) of App Manager.

6. If the map service using branch versioning, check the box beside **Data source uses ArcGIS Branch Versioning**.

**Heads Up!** If you selected this option, you will need to add your **Map Services Account Username** and **Password** in [Application Settings](#).

7. *Optional:* Click **More Options** to enter the following information about your data source:
  - a. **Service URL LRS Extension** - configure which extension the application should use for any given data source. If left blank, the application will default to the standard extension value of "LRSServer". If a map service is using ArcGIS Pro and Roads & Highways, then you must enter "LRServer" for the respective data source
  - b. **Description** - enter a description of the data source.
  - c. **Database Schema/Owner** - enter the schema or owner of the database.
  - d. **Spatial Reference ID (SRID)** - enter the spatial reference ID (SRID) assigned to the database.
8. Click **Save**.

**Search the list**

1. Click the **search icon** to expand the search field.
2. **Start typing** the name of a data source.
3. The list will filter to show matching data sources.

**Filter**













The Filter options lets you filter the data source table by Name, Provider, and/or Description.

1. Click **Filter**.
2. Enter the criteria for the name, provider, and/or description you want filtered into the applicable box.

**Tip:** Click **Filter** again to close the filter and refresh the privileges list.

**Test Existing**















Status	Name	Provider	Description	Actions
✓	TEST 1060 SQL	SQL Server	Test 1060 SQL Server Database Connec...	               
✓	TEST 1060 ORACLE	Oracle	Test 1060 Oracle Database Connection	               

1. Locate the row for the Data Source you wish to test.
2. Click the **test icon** pictured above.

**Heads Up!** This will only test the database connection. If the data source you want to test only has the associated service URL, it will fail this test even if that URL is correct.

### Updating Existing

To update an existing data source:

Status	Name	Provider	Description	Actions
✓	TEST 1060 SQL	SQL Server	Test 1060 SQL Server Database Connec...	               
✓	TEST 1060 ORACLE	Oracle	Test 1060 Oracle Database Connection	               

1. Locate the row for the Data Source you wish to edit and click **Edit** (pencil icon).
2. Make desired changes to the form input and then use the **Test Connection** button to verify the string still connects.
3. Click **OK**.













### Import Data

This feature can be used to import an appropriately configured table (e.g., routeid, from/to measure, biz data, etc.) to be used in the other Rizing Geospatial applications such as Segment Analyzer. You can import CSV, Excel, or Access tables.

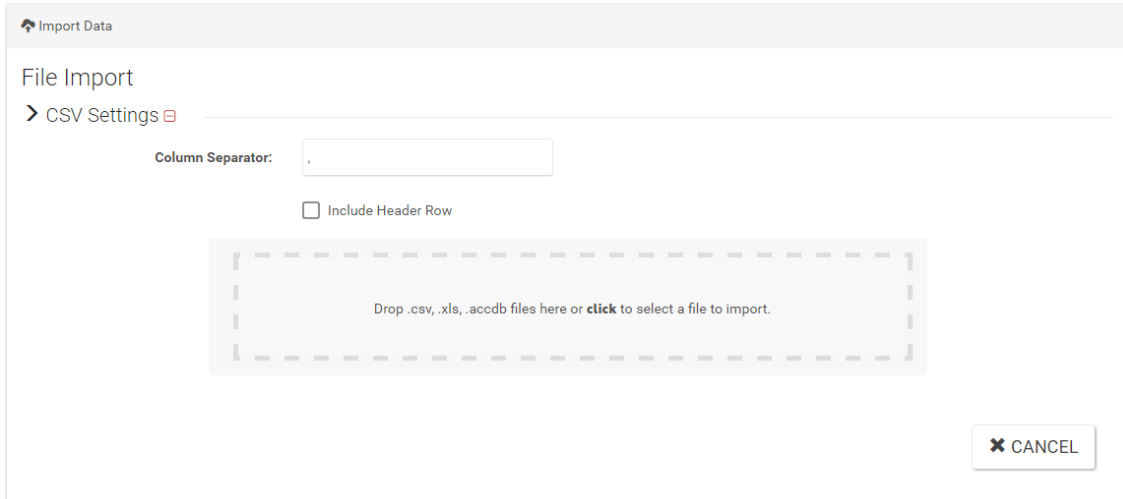
**Heads Up!** In order to use this functionality, [Microsoft Access database engine 2010](#) must be installed on the TDS application server. This is a driver that allows external applications (like TDS) to read/consume Microsoft office files (like Excel and Access). If the proper version of these components is not installed on the server, the **Import** button will remain "disabled." Once installed, you'll need to either recycle the TDS Application App Pool in IIS, restart IIS, or Restart the Application on the Administration page under Actions for the **Import** icon button to become "enabled".

### Usage

To import data to an existing data source:

Status	Name	Provider	Description	Actions
✓	TEST 1060 SQL	SQL Server	Test 1060 SQL Server Database Connec...	               
✓	TEST 1060 ORACLE	Oracle	Test 1060 Oracle Database Connection	               

1. Locate the row for the Data Source you to import a table to and click the **Import** icon.
2. Check the box beside **Include Header Row** to include the header row of the table.



Import Data

File Import

> CSV Settings

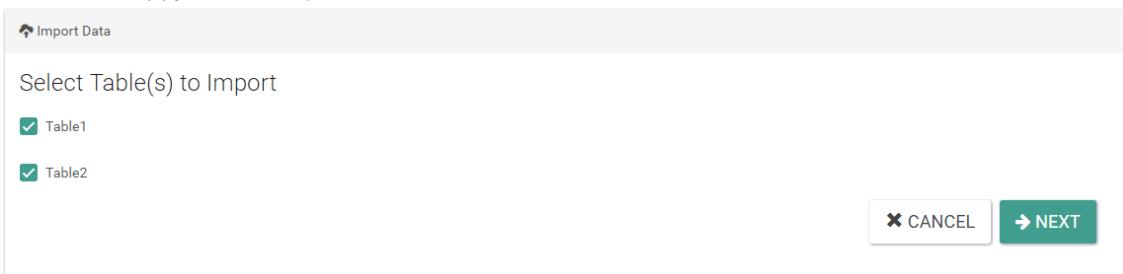
Column Separator: ,

Include Header Row

Drop .csv, .xls, .accdb files here or **click** to select a file to import.

CANCEL

3. Drag the table (or multiple tables) into the File Import area, or click inside the File Import area and navigate to the table you want to import.
4. Check the table(s) you want to import then click **Next**.



Import Data

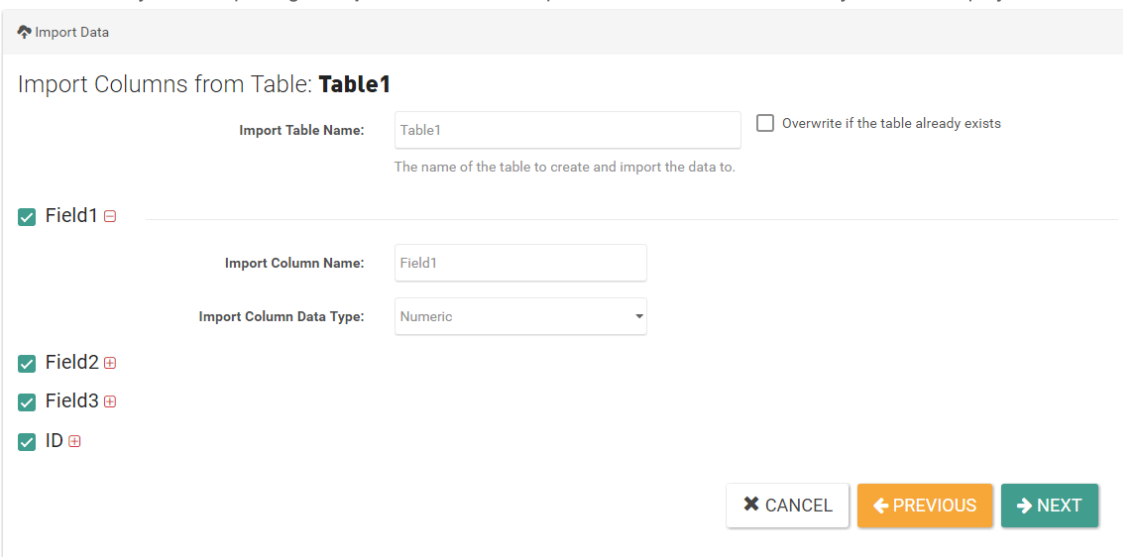
Select Table(s) to Import

Table1

Table2

CANCEL NEXT

5. For each table you are importing, in **Import Table Name** input box enter the table name as you want it displayed.



Import Data

Import Columns from Table: **Table1**

Import Table Name: Table1  Overwrite if the table already exists

The name of the table to create and import the data to.

Field1

Import Column Name: Field1

Import Column Data Type: Numeric

Field2

Field3

ID

CANCEL PREVIOUS NEXT

6. Uncheck any columns you do not want included in the import (all columns are checked by default).

- For each column in the table you are importing, enter the **Import Column Name** and **Import Column Data Type** as you want it to be displayed.
- Click **Next** to go to the next table.
- When finished editing the tables, review your selections and when finished click **Import**.

**Import Data**

Table(s) to Import

Table	Fields	Actions
Table1	Field1, Field2, Field3, ID	
Table2	Field12, Field22, Field33, ID2	

1 - 3 of 2 items

250 items per page

**CANCEL** **IMPORT**

**Tip:** If you need to make further edits to the tables and/or columns, click the **Edit** icon in the **Actions** column.

### Export Data

This feature can be used to export a CSV file containing records from a selected data source.

**Heads Up!** In order to use this functionality, [Microsoft Access database engine 2010](#) must be installed on the TDS application server. This is a driver that allows external applications (like TDS) to read/consume Microsoft office files (like Excel and Access). If the proper version of these components is not installed on the server, the **Export** button will remain "disabled." Once it is installed the **Export** button will become "enabled."

### Usage

To export data from an existing data source:

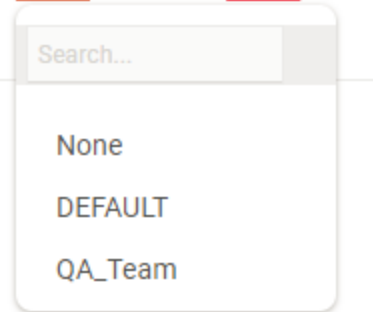
Status	Name	Provider	Description	Actions
	TEST 1060 SQL	SQL Server	Test 1060 SQL Server Database Connec...	
	TEST 1060 ORACLE	Oracle	Test 1060 Oracle Database Connection	

1. Locate the row for the Data Source you to export and click the **Export** icon.
2. Select the **Version** and **Table** from their respective dropdown lists.

## CSV Export

**Data Source:** TEST 1060 ORACLE **Version:** None ▾ **Table:** None ▾

> Settings ⊕



A dropdown menu is open, showing a search bar at the top with the text "Search...". Below the search bar, three options are listed: "None", "DEFAULT", and "QA\_Team". A thin line connects the "Settings" button to the top of the dropdown menu.

3. Check any columns you want to include in the export (all columns are unchecked by default).

## CSV Export

**Data Source:** TEST 10.6.0 Oracle **Version:** DEFAULT ▾ **Table:** SA\_PAVEMENT ▾ (26 records)

### Select Columns To Export

- OBJECTID
- ID
- ROUTEID
- FROMMEASURE
- TOMEASURE
- COMPLEX\_INTXN\_INFL\_SEGM\_ID
- COMPLEX\_INTXN\_ID
- STREET\_NAME
- D\_ROUTE\_STATUS\_ID
- D\_SURFACE\_TYPE\_ID

4. *Optional:* Click on **Settings** to configure the following settings:

> Settings

Column Separator:

Limit Records?

Limit:

Note: data will be sorted by table primary key(s).

Include Header Row

**Column Separator** - enter the character the export will use to separate the columns (a comma is used by default)

**Limit Records** - to limit the number of records exported, check this box and enter the number of records to export

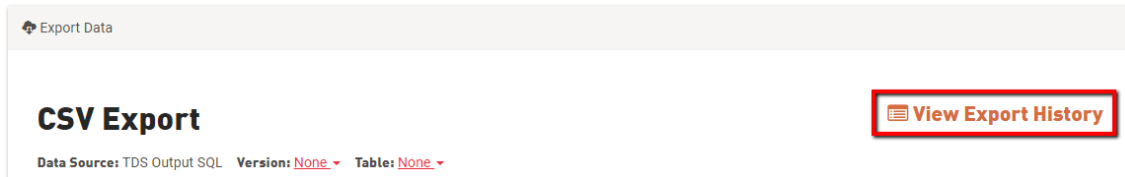
**Include Header Row** - uncheck to not include the header row (this is checked by default)

5. Click **Export** to start the export of the csv table.

### Export History Table

To view the Export History table:

1. Click **View Export History** in the upper right corner of the Export Data form.



2. Within the table, you have the following options:

**Search the Table** - click the **search icon**, then **start typing** the name of a job

**Filter the Table** - click **Filter**, then enter the criteria for the job or other column you want filtered

**Download a Job** - click the **download options icon**, then select the output from the dropdown list

**Delete a Job** - click the **trashcan icon**, then click **Delete** in the confirmation popup

**View Job Details** - click **Details** and the job's details will be opened

3. Click **Hide Export History** to close the table and return to the Export Data form.

### Delete Existing

To delete an existing data source:

Status	Name	Provider	Description	Actions
	TEST 1060 SQL	SQL Server	Test 1060 SQL Server Database Connec...	
	TEST 1060 ORACLE	Oracle	Test 1060 Oracle Database Connection	

1. Locate the row for the Data Source you wish to delete and click the **trashcan icon**.

2. Click **Delete** in the confirmation popup.

**Note:** If the users of the Data Source(s) will need to make changes to the network and update any tables that they are not the owner of, your database administrator will need to ensure that they have editor privileges so they can make changes to the network and update the tables.

## LRS Metadata

LRS metadata provides the ability to assign required LRS "semantics" to your data - such as "Route ID Field Names", "From Measure Field Names", "To Measure Field Names", and other LRS information, which is necessary for various applications to consume the data. If your map service has LRS metadata exposed via *LRS Server extension for ArcGIS Server* for a given event layer, no additional LRS metadata configuration is required for standard functionality.

If your map service does not have layer metadata exposed via the LRS Server extension, you'll need to add and configure any layers here that your applications need to consume data from.

### 🔗 LRS Metadata & Layer Details i

Configuring LRS metadata provides the ability to assign required LRS "semantics" to your data - requirements such as "Route ID Field Names", "From Measure Field Names", "To Measure Field Names", and other LRS information, which is necessary for various applications to consume the data. If the associated map service already has LRS metadata exposed for a given layer, then no additional LRS metadata configuration is required for standard functionality. To get started, select a data source, and then create, edit, or delete the data sources LRS metadata.

**Data Source:**  Refresh List

**Description:** Generic TSS Demo Transactional DB

**Service URL:** //stg-app.tsstools.com/arcgis/rest/services/tss/lrs/MapServer

#### LRS Metadata

CLEAR ALL DELETE ADVANCED EDITOR

Metadata Details
Network Layers (1)
Event Layers (3)
Intersection Layers (1)

Add New

Network ID	Layer ID	Table	Route ID Field	From Measure Field	To Measure Field	From Date Field	To Date Field	Actions
8	232		ROUTE_ID	MEASURE				<>   🗑️
8	233		ROUTE_ID	MEASURE				<>   🗑️
8	121		ROUTE_ID	MEASURE				<>   🗑️

### Usage

**Data Source:**  Refresh List

- Select a data source --
- Configuration Store
- Demo Data Set
- Demo Data Set Output Workspace

To start, select the data source from the dropdown that you wish to configure LRS metadata for, then follow the instructions below for each layer option.

#### Metadata Details

## LRS Metadata

[CLEAR ALL](#)
[DELETE](#)
[ADVANCED EDITOR](#)

[Metadata Details](#)
[Network Layers \(1\)](#)
[Event Layers \(3\)](#)
[Intersection Layers \(1\)](#)

Name

Service URL has additional LRS metadata

[CLOSE](#)
[SAVE](#)

### If your map service has LRS metadata exposed via *LRS Server extension for ArcGIS Server*

1. Enter a **Name** for your metadata details.
2. Check the box for **Service URL has additional LRS metadata**.

**Note:** When this box is checked, it will notify your applications to query the LRS Server to pull and access layer metadata.

### If your map service does not have LRS metadata exposed via *LRS Server extension for ArcGIS Server*

1. Enter a **Name** for your metadata details.
2. Insure the check the box for **Service URL has additional LRS metadata** is not checked.

**Note:** When this box is not checked, your applications will not query the LRS Server for layer metadata. You will need to add any layers you wish to query in the appropriate sections of this tool.

### Network Layers, Event Layers and Intersection Layers

For non- ArcGIS LRS Server Extension users, all layers and layer fields you want applications to have access to, must be configured in these tabs. Remember, if you're using the LRS Server extension, layers exposed through that extension don't need to be added. However, that doesn't mean you won't have any layers configured here. For example, you may have multiple network layers or tables added to the map service that aren't exposed through the extension. Those items would still need to be set up here.

The minimum requirement when adding a new layer is the Network ID, layer ID, Route ID field and the From Measure field. Some applications may also require additional fields to function correctly. For example, in addition to the above required fields, Segment Analyzer also needs to know the Table Name so it knows where to write the output to.

#### Layer Options:

[Network Layers](#)  
[Event Layers](#)  
[Intersection Layers](#)

#### To Add a New Layer

Click the tab you wish to add the layer too.

Click **+Add New** or **+Add New Layer Configuration** to add an empty row to the list of layers.

Double click fields to enter layer details into the table.



Click **Save**.

#### **To Edit a Layer**

##### **Table Method**

1. Double click the field you wish to edit.
2. Enter your changes.
3. Click **Save**.

##### **JSON Method**

1. To open the editor, click `</>` in the Actions column of the row you wish to edit.
2. Click the JSON code you wish to edit, and make your edits.
3. Click **Apply**.

#### **To Delete a Layer**

1. Click the tab you wish to remove the layer from.
2. Click **Delete** (trashcan) in the Actions column of the row you wish to delete.
3. Click **Delete** to confirm.

#### **Advanced Editor**

The Advanced Editor gives you a JSON view of all configured metadata layers and allows you to edit the raw JSON code.

1. Click the JSON code you wish to edit, and make your edits.
2. Click **Apply**.

## Import Seed Data

The Import Seed Data tool allows you to import "seed" data to the configuration database using a seed file. Using this feature saves you the step of entering in some of the configurations manually. If any updates to the original seed file are made, you can reload it using this tool.

### Administration

#### Seed Data

### Import Your Seed Data i

Drop ".tss" files here or **click** to select a file

If you were provided with a seed data file (.tss), then drag and drop it into the box or click the box to import it. This file will have a file extension of ".tss". This file is not necessary, but if you were provided one it will save you the steps of entering some initial configurations manually.

✕ CLOSE ✓ SAVE

### Usage

Drag and drop the seed data file into the box


or

Click inside the box to select the file

## Export Seed Data


The Export Seed Data tool provides the ability to export TDS, as well as various application configurations to a single seed file. This feature is useful for backing up configurations and other application settings prior to updating or other maintenance.

### Export Your Seed Data Configuration store export



Select the data items that you would like to export to a "seed file" (.tss file). The available data items are derived from the currently installed applications. You can export the entire configuration store, by not selecting anything, or you can pick and choose specific items to export.

**Heads up!** There are tables with a large number of records available. It is recommended that these tables be exported and migrated directly through the database rather than through exporting a seed file. Writing large amounts of data to a seed file can result in slow or unresponsive application performance. ✕

🔍 |  Refresh

Product ▲2 ▼	Entity Alias ▲3 ▼	Record Count ▼	☰
App Manager	Application Details	11	▲
App Manager	Application Integrations	5	▲
App Manager	Application Settings	34	▲
App Manager	Server Configuration	1	▲
data-source	Data Sources	53	▲
HPMS Assistant	Profiles	20	▲
ia	File Path Settings	0	▲

### Usage

#### Search Seed Data list

1. Click the search icon to expand the search field.
2. Start typing the name of an app or item you wish to export.
3. The list will update to show matching items.

#### Export Seed Data

1. Check the items that you wish to export.
2. Click Download Selected to export the selected items.

**Heads Up!** Be sure to note the Record Count of your selected items prior to export. Some of the items available for export have a large number of records and for best performance it is recommended that you export/migrate those items directly through your database rather than using this tool.

## Editing Seed Files

If your database is not set up as an ESRI enterprise geodatabase, some items will be configured through the [LRS Metadata](#) in the Transportation Data Server (TDS) Administration settings. The following can be edited through the [LRS Metadata](#) seed file:

[Domains](#)

[Profiles](#)

## Domains

Domains provide an easy way to constrain the valid values that can be populated for an event layer. If your database is not set up as an ESRI enterprise geodatabase, domains will be populated through the **LRS Metadata** in App Manager's Administration settings. The steps below will guide you through the process of adding and editing domains through the **LRS Metadata** seed file.

### Download Existing Metadata

To edit domains in the LRS Metadata, you will first need to download the relevant seed file that references domains. This can be done using the **Export Seed Data** functionality. LRS Metadata has a stand-alone seed file that can be exported to the user's desktop and edited directly.

**Heads Up!** The seed file is formatted as JSON, so users should be familiar with JSON formatting prior to editing the seed file.

**Tip:** Ensure that any pop-up blockers are disabled on this page or the user will not be able to download the file.

1. Select the LRS Metadata seed file and click **Download Selected**.

The screenshot shows a table with columns for Product, Entity Alias, and Record Count. The 'Irs' row is selected. Below the table are navigation controls and a 'DOWNLOAD SELECTED (1)' button.

Product	Entity Alias	Record Count
HPMS Assistant	Profiles	5
Irs	LRS Metadata	54
Road Analyzer	Profiles	25
Road Analyzer	SLD Templates	74
Road Video Viewer	Camera Images	286,425
Road Video Viewer	Cameras	24
Road Video Viewer	Event Points	40,581
Road Video Viewer	Profiles	3
Road Video Viewer	Route Metadata	0

1 of 12 of 12 items

**DOWNLOAD SELECTED (1)**

2. The file will download to the default downloads folder; you can open it using any text editor.

### Adding a Domain

The easiest way to add a domain is to copy and paste the formatting for an existing domain, then update the new domain with its code and name values.

1. The section for domains should be near the top of the file; if not, you will need to search for the relevant section. The domains will be represented as an array with the "domains" heading, as highlighted in the below picture.

```
seed_export_2_4_2019 (1).tss x
1  {
2    "dropAndRecreate": false,
3    "license": "<License>\r\n <Id>f3d10350-4bb6-4829-b594-9bdca614",
4    "restartOnComplete": true,
5    "seeds": [
6      {
7        "type": "Transcend.Spatial.Web.Lrs.LrsMetadata",
8        "idFieldName": "DataSourceId",
9        "deleteAll": false,
10       "addIfNotExists": true,
11       "addOrUpdate": true,
12       "dontSkipNullUpdates": false,
13       "useIndividualSave": false,
14       "skip": false,
15       "adds": [
16         {
17           "creationDate": "2018-04-18T10:50:07.633",
18           "dataSourceId": "ctdot",
19           "name": "CtDOT MAVRIC LRS Metadata",
20           "serviceHasLrsMeta": false,
21           "domains": [
22             {
23               "type": "codedValue",
24               "name": "ROUTE_PREFIX",
25               "description": "",
26               "codedValues": [
```

2. Your text editor should highlight where the code for that domain begins and ends.

```
{
  "type": "codedValue",
  "name": "ROUTE_PREFIX",
  "description": "",
  "codedValues": [
    {
      "name": "CT - Connecticut",
      "code": "CT"
    },
    {
      "name": "SR - State Route",
      "code": "SR"
    },
    {
      "name": "US - US Route",
      "code": "US"
    },
    {
      "name": "I - Interstate",
      "code": "I"
    }
  ]
}
```

3. Copy and paste the entire selection, then enter a name for the new domain and clear out the 'name' and 'code' values, to avoid accidental duplication.

```
{
  "type": "codedValue",
  "name": "NEW_DOMAIN_NAME",
  "description": "",
  "codedValues": [
    {
      "name": "",
      "code": ""
    },
    {
      "name": "",
      "code": ""
    },
    {
      "name": "",
      "code": ""
    },
    {
      "name": "",
      "code": ""
    }
  ]
},
```

4. Enter the respective code and name values for the new domain. The *code* value represents the value that will actually be stored in the database, while the *name* is the textual representation of that code. Typically, the name is used to provide you an explanation for an abstract code value.



```
{
  "type": "codedValue",
  "name": "TOWN_CODE",
  "description": "",
  "codedValues": [
    {
      "name": "ANDOVER",
      "code": "001"
    },
    {
      "name": "ANSONIA",
      "code": "002"
    },
    {
      "name": "ASHFORD",
      "code": "003"
    },
    {
      "name": "AVON",
      "code": "004"
    },
    {
      "name": "BARKHAMSTED",
      "code": "005"
    }
  ]
}
```

**Tip:** Save the file regularly.

Repeat the steps above to create all the new domains you need.

### Associating Domains with Layers

Once the domain has been created, you will need to associate the domain with the appropriate layer(s) and field(s). There are several sub-headings referencing data used by Rizing Geospatial's applications. These are:

"networkLayers"

"eventLayers"

"nonLRSLayers"

1. Use these sub-headings to navigate to the appropriate layers. Domain information will be referenced in the 'fields' array associated with the layer.

```
"networkLayers": [
  {
    "featureClassName": "EXOR.RoadsRoutesCombined",
    "targetFeatureClassName": "FIELD.RoadsRoutesCombined",
    "compositeRouteIdFieldName": "RoadRouteID",
    "toDateFieldName": "END_DATE",
    "modifiedDateFieldName": "Modified_Date",
    "modifiedByFieldName": "Modified_By",
    "id": 15,
    "hierarchyFilter": [
      {
        "isRoot": true,
        "networkLayerIdFieldName": "RoadRouteType",
        "label": "Route Type"
      },
      {
        "isRoot": true,
        "networkLayerIdFieldName": "TownName",
        "label": "Town Name"
      },
      {
        "isRoot": false,
        "networkLayerIdFieldName": "RoadRouteId",
        "label": "Route Number"
      }
    ],
    "fields": [
      {
        "name": "ID",
        "type": "id"
      },
      {
        "name": "TownName",
        "domainName": "TOWN_CODE"
      }
    ]
  }
]
```

2. Associate all new domains with the correct layer(s) and field(s).
3. Save the file and begin the import process.

### Importing Seed Files

Once the seed files have been updated, they will need to be imported into TDS so that the new domains can take effect. You can find those steps in the [Import Seed Data](#) topic.

## Profiles

Occasionally, there may be a need to [create a new profile](#) for any of the applications on TDS. While this can be done manually through App Manager, it is quite simple to use a seed file to create a new profile with all of the needed data.

Profile information can be either part of a larger seed file – this is the case with the metadata file that is currently being used to store event, domain and other metadata – or it can be created in a stand-alone file. Once a profile has been created through the seed file, it can be updated as needed in the Profile Configuration page within the application.

### Example

The picture below shows all of the attributes associated with creating a profile. This file is self-contained; it has only the valid JSON needed to create a profile.

```
1  {
2    "dropAndRecreate": false,
3    "license": null,
4    "restartOnComplete": false,
5    "seeds": [
6      {
7        "type": "Transcend.Data.Collection.Mavric.Web.MavricProfile",
8        "idFieldName": "AppId,Id",
9        "deleteAll": false,
10       "addIfNotExists": true,
11       "addOrUpdate": true,
12       "dontSkipNullUpdates": false,
13       "useIndividualSave": false,
14       "skip": false,
15       "adds": [
16         {
17           "appId": "mavric",
18           "id": "ctdot",
19           "name": "CtDOT MAVRIC",
20           "templateId": "ctdot-base",
21           "dataSourceId": "ctdot"
22         }
23       ],
24       "updates": [],
25       "deletes": []
26     }
27   ]
28 }
```

Some caveats:

Data source information may also need to be provided, either through this file or through an additional stand-alone seed file

Template information may also need to be provided, either through this file or through an additional stand-alone seed file

In this case, the profile created by this seed file is for the MAVRIC application. This is specified by the 'type' attribute.

The "adds" array contains information specific to the profile being created:

"appld": the foreign key value for the application that is having a new profile created

"id": the profile ID which essentially acts as the primary key for the profile

"name": the name is an alias for the profile and will be how the profile appears in the list of [application profiles](#) on the [Apps Dashboard](#)

"templated": this references the default template associated with the profile

**Note:** This template should be supplied within the seed file, or as a separate seed file import.

"dataSourceId": This references the data source used by the profile

**Note:** The data source ID is created when a new data source is added to the App Manager. If this data source does not exist, it can be created with a seed file as well.

The image below shows the attributes associated with a [Data Source](#) within a seed file. This data source may be created during this process, or it may be updated by adding new properties to an existing data source.

```
{
  "type": "Transcend.Data.DataSource",
  "idFieldName": "Id",
  "deleteAll": false,
  "addIfNotExists": true,
  "addOrUpdate": true,
  "dontSkipNullUpdates": false,
  "useIndividualSave": false,
  "skip": false,
  "adds": [
    {
      "id": "ctdot",
      "name": "CtDOT MAVRIC Data Source",
      "description": "Connecticut DOT's TED data source",
      "connectionString": "data source=MAVRIC-WS, 1433;initial catalog=MAVRIC;persist",
      "providerName": "System.Data.SqlClient",
      "serviceUrl": "//mavric-ws/1061gis/rest/services/ctdot/mavric/MapServer",
      "srId": 3857
    }
  ],
  "updates": [],
  "deletes": []
},
```

## Support

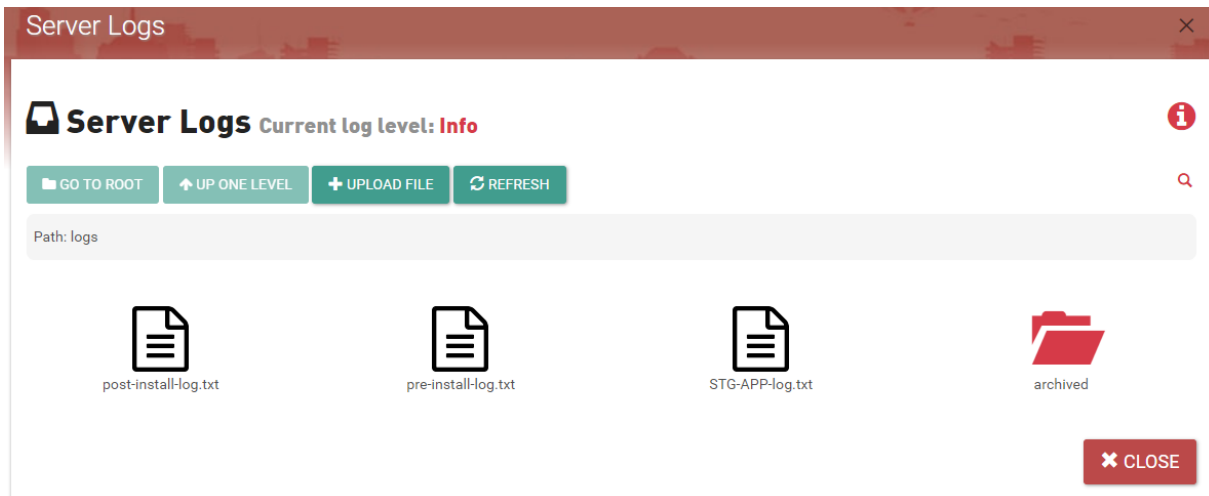
[Server Logs](#) - view and manage logs generated by the server

[Web Service Tool](#) - execute web service calls using application security

**Tip:** We've added notification messages throughout App Manager (as all our web applications) to alert you when there is an error or warning. The notifications will appear on the application screen bottom left. These notification are designed to appear for a few seconds, then disappear on there own. However, you can hover over a notification to keep it from disappearing and also double-click a notification to close it immediately.

## Server Logs

The Server Logs feature is a web interface that allows system administrators to view the server log activity and diagnose errors. The Server Log includes the time stamp, log level, and detailed messages from the application including a post-install-log.txt, pre-install-log.txt and a primary [app-name]-log.txt file. The saved logs from the previous day are automatically sent to an archived folder.



## Usage

### View a log

#### To view the most recent log

1. Double click the **log.txt** file to view the server log in a Grid View.

Q | Filter Text View

Level	Time	Message	Actions
INFO	09:31:02	Creating new 'VaProfile' in 0 millis	View Details
INFO	09:31:02	Creating new 'VaProfile' in 0 millis	View Details
ERROR	08:14:54	Failed to retrieve RA profile by ID 'test_1071_sql' in 0 millis System.InvalidOperationException: The specified cast from a materialized 'Sy...	View Details
ERROR	08:14:54	Failed to find single 'RaProfile' by primary key(s) 'ra_test_1071_sql' in 0 millis System.InvalidOperationException: The specified cast from ...	View Details
DEBUG	08:04:37	Retrieving anonymous privilege IDs in 0 millis	View Details
INFO	08:04:33	Added scheduling admin dashboard at path: 'scheduler'	View Details

2. You can change the view to text by clicking **Text View**.

Grid View

```

10:23:02 INFO:Added scheduling admin dashboard at path: 'scheduler'
10:23:02 INFO:Hangfire SQL objects installed.
10:23:02 INFO:Start installing Hangfire SQL objects...
10:23:02 INFO:Configuring scheduling service with storage mechanism 'SQLite' and worker count 1
10:23:02 INFO:Initializing site in 0 millis
10:23:02 INFO:Auto-seeding role privileges in 0 millis
    
```

3. Click **Grid View** to return to the original view.
4. Click **View Details** next to an item in the log to view more details.
5. Click **Refresh** to refresh the log.
6. Click **Close File** to return to the main log directory.

### To view an archived log

1. Double click the **archived** folder to open it.
2. Double click the **log.txt** file to view the server log in a Grid View.

**Note:** You can change the view to text by clicking **Text View**.

3. Click **View Details** next to an item in the log to view more details.
4. Click **Refresh** to refresh the log.
5. Click **Close File** to return to the main log directory.

### Search a log

1. Double click the **log.txt** file to view the server log in a Grid View.
2. Click the **search icon** to expand the search field.
3. **Start typing** the name of an item in the log.
4. The list will update to show all matching items.

### Filter a log

The Filter options lets you filter the log level, times, and messages in the log.

Q | Filter Text View

Level	Time	Message	Actions
DEBUG	09:47:37	Setting connection timeout to: 0 seconds	View Details
INFO	09:47:34	Updating 'VaProfile' with ID: test_profile in 0 millis	View Details
INFO	09:31:02	Creating new 'VaProfile' in 0 millis	View Details
INFO	09:31:02	Creating new 'VaProfile' in 0 millis	View Details

1. Double click the **log.txt** file to view the server log in a Grid View.
2. Click **Filter**.
3. Enter the criteria for the log level, times, and/or messages you want filtered into the applicable box.

**Tip:** Click **Filter** again to close the filter and refresh the log.

### Export a log

1. Double click the **log.txt** file to view the server log in a Grid View.
2. Click **hamburger icon** in the top right hand corner of the grid and select **Export all data as csv** from the dropdown.

STG-APP-log.txt Text View

CLOSE FILE REFRESH

Q | Filter

Level	Time	Message	Actions
INFO	15:55:11	Initialization site in 0 millis	<div style="border: 2px solid red; padding: 2px;">Export all data as csv</div> Export visible data as csv Columns: <input checked="" type="checkbox"/> Level <input checked="" type="checkbox"/> Time <input checked="" type="checkbox"/> Message <input checked="" type="checkbox"/> Actions

3. The log will download to your computers downloads folder in csv format.

**Tip:** If server log does not download, check your browser settings to verify that pop-up blocker is not on.

#### Delete a log or folder

1. Right click on the log/folder you want to delete.

**Heads Up!** If you delete a log in this interface, it will be deleted in the application's server logs too.

2. Click **Delete**.
3. In the Confirm Delete popup, click **Delete**.

#### Rename a log or folder

1. Right click on the log/folder you want to rename.
2. Click **Rename**.
3. Once clicked, the report name will become an editable field.
4. Enter your changes.
5. Click any blank space on the page to exit editing mode.

**Tip:** Did you make a mistake and need to change it? No worries. Just repeat the steps above.

#### Download a log

1. Right click on the log you want to download.
2. Click **Download**.
3. The log will download to your computers downloads folder in txt format.

**Tip:** If server log does not download, check your browser settings to verify that pop-up blocker is not on.

#### Upload a file

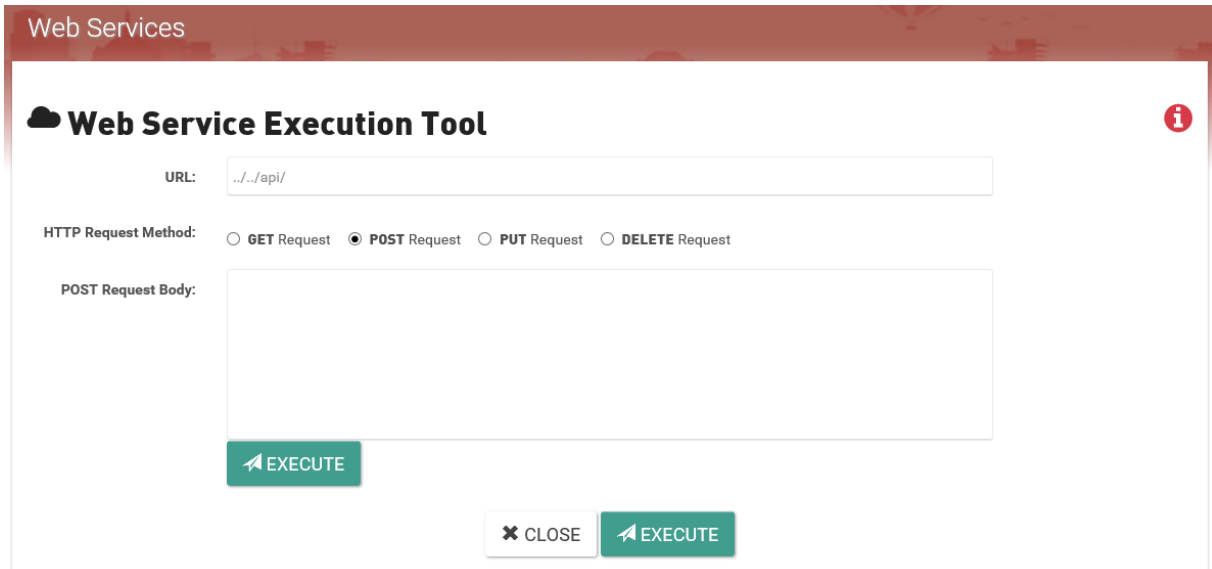
1. Click the **+Upload File** button.
2. Select the file you wish to upload.
3. Click **Open** to upload the file.

**Note:** You can change the logging level on the [General Server Settings](#) page.



## Web Service Tool

The Web Service Tool feature enables you to execute HTTP requests against TDS.



The screenshot shows a web interface titled "Web Services" with a sub-header "Web Service Execution Tool". It features a "URL:" input field containing " ../api/". Below it, the "HTTP Request Method:" section has four radio buttons: "GET Request", "POST Request" (which is selected), "PUT Request", and "DELETE Request". A "POST Request Body:" text area is positioned below the radio buttons. At the bottom of the form, there are three buttons: a green "EXECUTE" button with a play icon, a white "CLOSE" button with an 'x' icon, and another green "EXECUTE" button with a play icon. An information icon (i) is located in the top right corner of the tool's content area.

### Usage

1. Enter your HTTP request in the **URL** input box
2. Select desired **HTTP Request Method**.
3. *For POST and PUT requests:* Enter the **Request Body**.
4. Click **Execute**.

## Settings

[Mail Server](#) - configure settings your applications use to send emails

[Licensing](#) - manage your software license

[General Server Settings](#) - configure the server logging level, cache policy, expiration dates and more

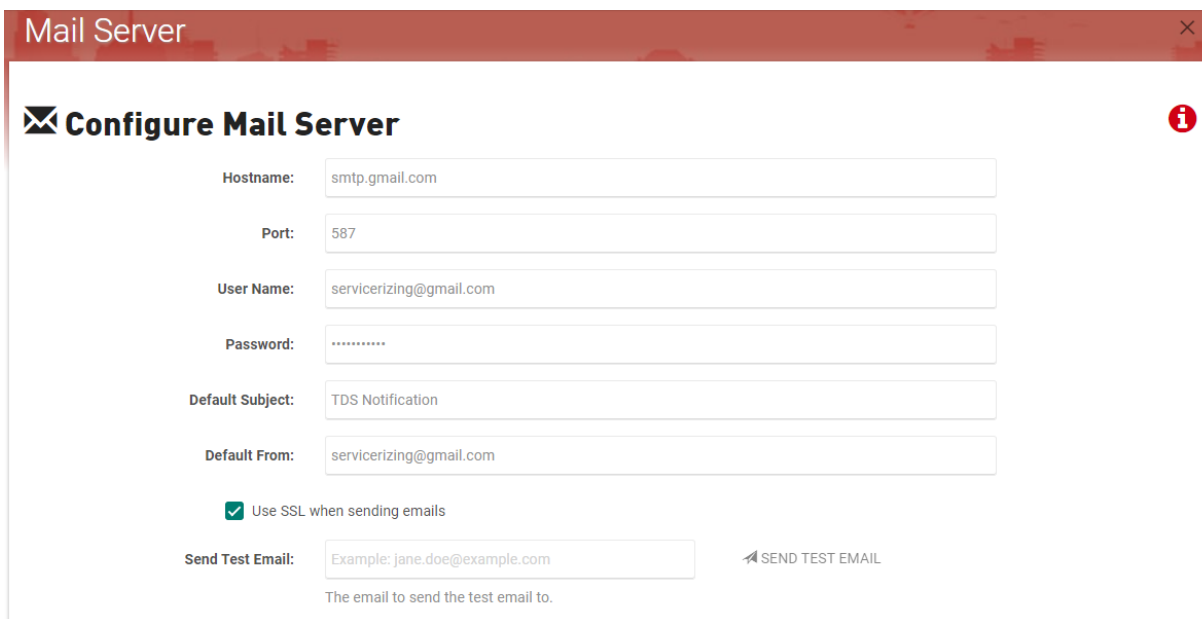
[SQL Command Settings](#) - configure the internal application SQL queries

[File Path Settings](#) - choose where to store physical files on the server

[Scheduling Service Settings](#) - configure the storage mechanism, connection string and more for the Job Execution Manager scheduler

## Mail Server

The Mail Server feature allows you to manage the default mail server you'd like your applications to use and to set a default email subject line and default from email address.



The screenshot shows a window titled "Mail Server" with a close button (X) in the top right corner. Below the title bar is a header area with a mail icon and the text "Configure Mail Server" and an information icon (i). The main content area contains several input fields and a checkbox:

- Hostname:** smtp.gmail.com
- Port:** 587
- User Name:** servicerizing@gmail.com
- Password:** .....
- Default Subject:** TDS Notification
- Default From:** servicerizing@gmail.com
- Use SSL when sending emails
- Send Test Email:** Example: jane.doe@example.com
- SEND TEST EMAIL** button
- Text below the field: "The email to send the test email to."

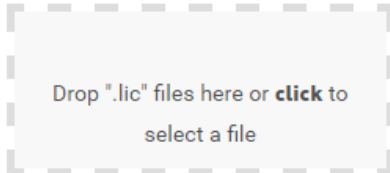
### Usage

1. Enter your email provider's host name (also called server name) in the **Hostname** field.
2. Enter the port number used to connect to your host's server in the **Port** field.
3. Enter the user name for your account in the **User Name** field.
4. Enter your account password in the **Password** field.
5. Enter the default subject line you wish to use in the **Default Subject** field.
6. Enter a default from email address in the **Default From** field.
7. Click **Use SSL when sending emails** if you wish to add SSL encryption to emails sent from your applications.
8. Enter a test email address in the **Send Test Email** field and click **SEND TEST EMAIL** to test these settings. (optional)
9. Click **Save** when done.

## Licensing

The Licensing feature provides the ability to add your software license details for all your applications using a .LIC file provided to you by Rizing Geospatial.

### Import Your License



**License ID:** f3d10350-4bb6-4829-b594-9bdca6140e28  
**Type:** Standard  
**Registered To:** Rusty Green ([rgreen@tssgis.com](mailto:rgreen@tssgis.com))  
**Expires:** Never  
**Features:**

- ✓ App Manager
- ✓ Security
- ✓ License Server
- ✓ Data Sources
- ✓ Jobs
- ✓ LRS
- ✓ Road Analyzer
- ✓ Segment Analyzer
- ✓ Validation Assistant
- ✓ HPMS Assistant
- ✓ Report Engine
- ✓ Video Log
- ✓ File Access

← BACK

SKIP THIS STEP →

### Usage

Drag and drop the ".LIC" file we provided to you into the dashed import box to add your software license information. Once added, you'll be able to see your license ID, license type, who it's registered to, when it expires as well as all the products and features included in your license.

## General Server Settings

General server functions and basic settings you'd like the server to use when making calls, logging, etc. are set in the General Server Settings.

### General Server Settings

#### Server Settings

##### Logging and Errors

**Log Level:** Info (import information only)  
The level of detail the server should log information.

**Log File Name Template:** \${machinename}-log.txt  
The template used for log file names. See [here](#) for details on template options.

**Archived Log Location:** archived/{#}.txt  
The template used to store "archived" log files. See [here](#) for details on template options.

**Max Log File Size (in bytes):** 2000000 1.9 MB  
The maximum file size per log file (in Megabytes). Once this limit is reached, the log file will be archived and a new log file will be started.

**Max Number of Logs to Keep:** 90 Max possible log storage usage: 171.7 MB  
The maximum number of log files to keep "archived". Once the threshold is met, the system will delete the oldest log file.

**Log Format Template:** \${date:format=HH:mm:ss} \${level:uppercase=true}:\${message} \${exception:format=toString}  
The log template to be used when logging to text files. See [here](#) for details on template options.

**Tip:** If you want to hide or expand one of the sections, click the plus / minus sign at the end of the section name.

## Usage

### Logging and Errors

#### Log Level

The log level setting sets the level at which the server will write message logs and how granular the logs are written. The levels are listed hierarchically based on the amount of information & messages logged, meaning that each successive level will include the messages of the log levels below it. For example, the default setting is Info, so in addition to Info messages, Warn, Error and Fatal messages are also included.

**Log Level:**

The level of detail the server should log information.

**To Use:**

1. Select the log level you wish to use from the dropdown.

*Options include:*

Trace – very fine details and ALL log messages available will be logged

Debug – all messages that may be of value in order to debug and troubleshoot

Info – informational messages only

Warn – only errors and warnings

Error - (errors only)

Fatal – fatal errors only

2. Click **Save**.

**Heads Up!** Performance may be impacted when using Trace or Debug due to the increased number of messages logged.

**Log File Name Template**

**Log File Name Template:**

The template used for log file names. See [here](#) for details on template options.

The Log File Template allows you to configure the layout renderer macro template used for log file names. The default is `$(machinename)` which will use the name of the machine the process is running on in the name. You can find more info [here](#) about the different layout renderer macros that can be used.

**To Use:**

1. Enter the desired layout renderer macro following by `-log.txt`.
2. Click **Save**.

**Archived Log Location**

**Archived Log Location:**

The template used to store "archived" log files. See [here](#) for details on template options.

The Archived Log Location setting allows you to configure the location and file name for archived logs. By default, the logs are saved to the archived folder and named with the date of the log, for example: 2017-08-09.0.txt. You can find more info [here](#) about the different layout renderer macros that can be used.

**To Use:**

1. Enter the desired layout renderer macro into the curly braces and update the folder location if desired.
2. Click **Save**.

**Max Log File Size (in bytes)**

**Max Log File Size (in bytes):**  1.9 MB

The maximum file size per log file (in Megabytes). Once this limit is reached, the log file will be archived and a new log file will be started.

The Max Log File Size setting allows you to configure the maximum size a log be in megabytes. As stated in the above image, once the limit is reached, the log is archived and a new log file is started.

**To Use:**

1. Enter the desired size limit in megabytes.
2. Click **Save**.

**Max Number of Logs to Keep**

**Max Number of Logs to Keep:**  Max possible log storage usage: 171.7 MB

The maximum number of log files to keep "archived". Once the threshold is met, the system will delete the oldest log file.

The Max Number of Logs to Keep setting allows you to set a maximum number of logs to keep archived. Once the threshold is met, the system will delete the oldest log file.

**To Use:**

1. Enter the desired number of logs to keep.
2. Click **Save**.

**Log Format Template**

**Log Format Template:**

The log template to be used when logging to text files. See [here](#) for details on template options.

The Log Format Template setting allows you to configure the layout renderer macro template used for logging text files. You can find more info [here](#) about the different layout renderer macros that can be used.

**To Use:**

1. Update the layout renderer macros in the template string.
1. Click **Save**.

**Data Processing**

The following settings affect the various limits of data processing for all the applications.

Data Processing

---

**Max Records to Return:**

The max number of records that can be returned through a web request, at one time. Enter 0 for no limit.

**Bulk Record Query Threshold:**

The max number of records (or groups of data) to query for, when processing data in chunks.

**Database Connection Timeout:**

The max number of seconds a database connection will remain open (before timing out). Enter "0" for no timeout. Current configuration will never timeout.

**Bulk Record Insert Threshold:**

When inserting data in bulk, the max number of records to keep in memory before committing to the database.

**Max Records to Return**

The number set here represents the max number of records that can be returned through a web request, at one time. Enter 0 for no limit.

**To Use:**

1. Enter your desired max number of records into the field.

**Bulk Record Query Threshold**

The number set here represents the max number of records (or groups of data) to query for, when processing data in chunks.

**To Use:**

1. Enter your desired max number of records into the field.

**Database Connection Timeout**

The max set here determines the max number of seconds a database connection will remain open before timing out. For no timeout, enter "0."

**To Use:**

1. Enter your desired max seconds into the field.

**Bulk Record Insert Threshold**



When inserting data in bulk, the number set here determines the max number of records to keep in memory before committing to the database.

**To Use:**

1. Enter your desired max number of records into the field.

**Prevent Field Quotes**

Check this option if you want to prevent the system from automatically adding quotes around database field names, when executing SQL statements.

**To Use:**

1. Check/uncheck the box to turn on/off.

**Job Expiration Days**

The number set here determines the default number of days you wish to keep job information. After the specified number of days has expired the job (and any associated files) will be deleted. A job typically consists of exported files, reports, etc.

**To Use:**

1. Enter your desired default number of days to keep a job into the field.

**Job Update Interval**

The number set here determines the number of seconds to update the status of a job. For example, a value of "30" will update the progress of a long running job every 30 seconds (will update the progress of the job).

**To Use:**

1. Enter your desired default number of seconds in the field.

**Tuning and Performance**

This setting determines whether the server can cache commonly requested resources so that it doesn't need to continually make requests to the database, unless a change is found.

**Enable Caching:**     **Enable Server Side Caching**

**To Use:**

1. Check the checkbox to enable.
2. Uncheck the checkbox to disable.

**Reset**

The reset button can be used to reset all the general server settings back to the defaults.


**Heads Up!** Be aware that a few other settings that are not visible in this form, such as the mail server settings, will also be reset.

## SQL Command Settings

The applications make use of many SQL statements internally that are pre-defined, yet dynamic SQL query configurations. These "parameterized queries" are expected to contain specific parameters (@SomeParamName) in order to function. It is recommended that these queries do not get changed, unless a specific environment setting/configuration warrants a modification.

/

### Sql Commands

 **SQL Query Statements Configuration**
i

**Attention!** Query configurations are pre-defined, yet dynamic, SQL statements that are used within various applications. These "parameterized queries" are expected to contain specific parameters (@SomeParamName) in order to function. It is recommended that these queries do not get changed, unless a specific environment setting/configuration warrants a modification. The most typical change that would be required to these statements is adding an SDE user/schema prefix - or removing the prefix.

<b>Column Filter:</b>	<input type="text" value="(*Shape\$) (*Shape.Length\$) (*Geometry\$)"/>
<b>Copy Table:</b>	<input type="text" value="SELECT @Fields INTO @ToTable FROM @FromTable"/>
<b>Copy Table Oracle:</b>	<input type="text" value="CREATE TABLE @ToTable AS SELECT @Fields FROM @FromTable"/>
<b>Copy Table Sql Ce:</b>	<input type="text" value="CREATE TABLE @ToTable AS SELECT @Fields FROM @FromTable"/>
<b>Create Table:</b>	<input type="text" value="CREATE TABLE @TableValue (@ColumnDeclarations)"/>
<b>Date Query Formatter:</b>	<input "="" type="text" value="{0}"/>
<b>Date Query Formatter Oracle:</b>	<input type="text" value="TO_DATE('{0}','YYYY-MM-DD HH24:MI:SS')"/>
<b>Delete Rows:</b>	<input type="text" value="DELETE FROM @TableValue WHERE @WhereClause"/>

The most typical change that would be required to these statements is modifying the user/schema prefix for SDE-related objects - adding, updating or removing the prefix.

**Example:** ...sde.table\_registry...  
 To...  
 dbo.table\_registry...  
 Or...  
 table\_registry...

### Usage

1. Click inside the text field and update the SQL statement as needed.
2. Use the Reset button to reset all SQL statements back to the defaults.

**Heads Up!** It is possible that other SQL statements not listed, may also be reset.

## Default SQL statements

Description	SQL Statement
Column Filter:	<code>(^Shape\$)   (^Shape.Length\$)   (^Geometry\$)</code>
Copy Table:	<code>SELECT @Fields INTO @ToTable FROM @FromTable</code>
Copy Table Oracle:	<code>CREATE TABLE @ToTable AS SELECT @Fields FROM @FromTable</code>
Copy Table SQL Ce:	<code>CREATE TABLE @ToTable AS SELECT @Fields FROM @FromTable</code>
Create Table:	<code>CREATE TABLE @TableValue (@ColumnDeclarations)</code>
Date Query Formatter:	<code>'{0}'</code>
Date Query Formatter Oracle:	<code>TO_DATE('{0}', 'YYYY-MM-DD HH24:MI:SS')</code>
Delete Rows:	<code>DELETE FROM @TableValue WHERE @WhereClause</code>
Drop Table:	<code>DROP TABLE @TableValue</code>
Insert Row:	<code>INSERT INTO @TableValue (@ColumnNames) VALUES (@InsertValues)</code>
Select Column Info:	<pre> SELECT c.COLUMN_NAME, c.DATA_TYPE, c.IS_NULLABLE,        c.CHARACTER_MAXIMUM_LENGTH, c.NUMERIC_PRECISION,        c.NUMERIC_SCALE, c.ORDINAL_POSITION, CASE WHEN pk.COLUMN_NAME IS NOT NULL THEN 1 ELSE 0 END AS PRIMARY_KEY FROM INFORMATION_SCHEMA.COLUMNS c LEFT JOIN (     SELECT ku.TABLE_CATALOG, ku.TABLE_SCHEMA, ku.TABLE_NAME, ku.COLUMN_NAME     FROM INFORMATION_SCHEMA.TABLE_CONSTRAINTS AS tc     INNER JOIN INFORMATION_SCHEMA.KEY_COLUMN_USAGE AS ku     ON tc.CONSTRAINT_TYPE = 'PRIMARY KEY'     AND tc.CONSTRAINT_NAME = ku.CONSTRAINT_NAME ) pk ON c.TABLE_CATALOG = pk.TABLE_CATALOG    AND c.TABLE_SCHEMA = pk.TABLE_SCHEMA    AND c.TABLE_NAME = pk.TABLE_NAME    AND c.COLUMN_NAME = pk.COLUMN_NAME WHERE c.TABLE_NAME = @TableName AND c.TABLE_SCHEMA = @SchemaName ORDER BY c.COLUMN_NAME </pre>

<p>Select Column Info No Schema:</p>	<pre>SELECT c.COLUMN_NAME, c.DATA_TYPE, c.IS_NULLABLE,        c.CHARACTER_MAXIMUM_LENGTH, c.NUMERIC_PRECISION,        c.NUMERIC_SCALE, c.ORDINAL_POSITION, CASE WHEN pk.COLUMN_NAME IS NOT NULL THEN 1 ELSE 0 END AS PRIMARY_KEY FROM INFORMATION_SCHEMA.COLUMNS c LEFT JOIN (   SELECT ku.TABLE_CATALOG,ku.TABLE_SCHEMA,ku.TABLE_NAME,ku.COLUMN_NAME   FROM INFORMATION_SCHEMA.TABLE_CONSTRAINTS AS tc   INNER JOIN INFORMATION_SCHEMA.KEY_COLUMN_USAGE AS ku   ON tc.CONSTRAINT_TYPE = 'PRIMARY KEY'   AND tc.CONSTRAINT_NAME = ku.CONSTRAINT_NAME ) pk ON c.TABLE_CATALOG = pk.TABLE_CATALOG    AND c.TABLE_SCHEMA = pk.TABLE_SCHEMA    AND c.TABLE_NAME = pk.TABLE_NAME    AND c.COLUMN_NAME = pk.COLUMN_NAME WHERE c.TABLE_NAME = @TableName ORDER BY c.COLUMN_NAME</pre>
<p>Select Column Info No Schema Oracle:</p>	<pre>select c.COLUMN_NAME, c.DATA_TYPE, c.NULLABLE,        c.DATA_LENGTH, c.DATA_PRECISION,        c.DATA_SCALE, c.COLUMN_ID, CASE WHEN i.COLUMN_NAME IS NOT NULL THEN 1 ELSE 0 END AS PRIMARY_KEY from user_tab_columns c LEFT JOIN (   SELECT cols.COLUMN_NAME, cols.TABLE_NAME   FROM all_constraints cons, all_cons_columns cols   WHERE cols.table_name = UPPER(@TableName)   AND cons.constraint_type in ('P')   AND cons.constraint_name = cols.constraint_name   AND cons.owner = cols.owner ) i ON c.TABLE_NAME = i.TABLE_NAME    AND c.COLUMN_NAME = i.COLUMN_NAME WHERE c.TABLE_NAME = UPPER(@TableName) ORDER BY c.COLUMN_NAME</pre>
<p>Select Column Info No Schema SQL Ce:</p>	<pre>select c.COLUMN_NAME, c.DATA_TYPE, c.IS_NULLABLE,        c.CHARACTER_MAXIMUM_LENGTH, c.NUMERIC_PRECISION,        c.NUMERIC_SCALE, i.ORDINAL_POSITION, i.PRIMARY_KEY from INFORMATION_SCHEMA.COLUMNS c LEFT JOIN INFORMATION_SCHEMA.INDEXES i ON c.TABLE_NAME = i.TABLE_NAME    AND c.COLUMN_NAME = i.COLUMN_NAME WHERE c.TABLE_NAME = @TableName    AND c.TABLE_SCHEMA = @SchemaName ORDER BY c.COLUMN_NAME</pre>

<b>Select Column Info Oracle:</b>	<pre>select c.COLUMN_NAME, c.DATA_TYPE, c.NULLABLE,        c.DATA_LENGTH, c.DATA_PRECISION, c.DATA_SCALE, c.COLUMN_ID, CASE WHEN i.COLUMN_NAME IS NOT NULL THEN 1 ELSE 0 END AS PRIMARY_KEY from all_tab_columns c LEFT JOIN (     SELECT cols.COLUMN_NAME, cols.TABLE_NAME     FROM all_constraints cons, all_cons_columns cols     WHERE cols.table_name = UPPER(@TableName)     AND cons.constraint_type in ('P')     AND cons.constraint_name = cols.constraint_name     AND cons.owner = cols.owner     ) i ON c.TABLE_NAME = i.TABLE_NAME    AND c.COLUMN_NAME = i.COLUMN_NAME WHERE c.TABLE_NAME = UPPER(@TableName)    AND c.OWNER = @SchemaName ORDER BY c.COLUMN_NAME</pre>
<b>Select Column Info SQL Ce:</b>	<pre>select c.COLUMN_NAME, c.DATA_TYPE, c.IS_NULLABLE,        c.CHARACTER_MAXIMUM_LENGTH, c.NUMERIC_PRECISION,        c.NUMERIC_SCALE, i.ORDINAL_POSITION, i.PRIMARY_KEY from INFORMATION_SCHEMA.COLUMNS c LEFT JOIN INFORMATION_SCHEMA.INDEXES i ON c.TABLE_NAME = i.TABLE_NAME    AND c.COLUMN_NAME = i.COLUMN_NAME WHERE c.TABLE_NAME = @TableName    AND c.TABLE_SCHEMA = @SchemaName ORDER BY c.COLUMN_NAME</pre>
<b>Select Count:</b>	<pre>SELECT COUNT(*) from @TableValue where @WhereClause</pre>
<b>Select Distinct From Table:</b>	<pre>SELECT DISTINCT @Columns from @TableValue where @WhereClause</pre>
<b>Select From Table:</b>	<pre>SELECT @Columns from @TableValue where @WhereClause</pre>
<b>Select From Table Paged:</b>	<pre>SELECT @Columns from @TableValue where @WhereClause ORDER BY @OrderBy OFFSET @OffsetRows ROWS FETCH NEXT @PageSize ROWS ONLY</pre>
<b>Select From Table Paged Oracle:</b>	<pre>SELECT @Columns FROM (select @Columns, row_number()                         OVER (order by @OrderBy)rn FROM @TableValue where @WhereClause                         WHERE rn BETWEEN @StartRow AND @EndRow order by rn</pre>
<b>Select Version View:</b>	<pre>SELECT imv_view_name FROM sde.SDE_table_registry WHERE table_name = @TableName</pre>
<b>Select Version View Oracle:</b>	<pre>SELECT imv_view_name FROM sde.table_registry WHERE table_name = @TableName</pre>
<b>Select Versions:</b>	<pre>SELECT name, owner, version_id, status, state_id, description, parent_name, parent_owner, parent_version_id, creation_time FROM [sde].[SDE_versions]</pre>

Select Versions Oracle:	SELECT NAME, OWNER, VERSION_ID, STATUS, STATE_ID, DESCRIPTION, PARENT_NAME, PARENT_OWNER, PARENT_VERSION_ID, CREATION_TIME FROM sde.VERSIONS
Set Version Proc:	sde.set_current_version
Set Version Proc Oracle:	sde.VERSION_UTIL.set_current_version
Set Version Proc Param:	version_name
Table Filter:	(^A[0-9])(^D[0-9])(^I[0-9])(^KEYSET_)(^REV_)(^SDE_)(ID\\$\\$)(^GDB_)(^DR\\$\\$)(^eww\$)(^SDO_)(^ST_)(^SERVER_CONFIG\$)(^TABLE_LOCKS\$)(^DBTUNE\$)(^COLUMN_REGISTRY\$)(^GEOMETRY_COLUMNS\$)(^INSTANCES\$)(^LAYER_LOCKS\$)(^LINEAGES_MODIFIED\$)(^LOCATORS\$)(^METADATA\$)(^MBTABLES_MODIFIED\$)(^LAYERS\$)(^LINEAGES_MODIFIED\$)(^OBJECT_LOCKS\$)(^PROCESS_INFORMATION\$)(^RASTER_COLUMNS\$)(^SPATIAL_REFERENCES\$)(^STATE_LINEAGES\$)(^STATE_LOCKS\$)(^TABLE_REGISTRY\$)(^VERSION\$)(^VERSIONS\$)
Table Type Filter:	(^System\$)
Truncate Table:	TRUNCATE TABLE @TableValue
Update Rows:	UPDATE @TableValue set @ColumnNames = @UpdateValue WHERE @WhereClause

## File Path Settings

File Paths are pre-defined application data or storage folder locations. These paths are expected to be relative or complete paths to a physical folder location accessible to the application. These paths are automatically generated when App Manager and other Rizing Geospatial applications are installed. With this feature you can view and edit the physical location on the server that the applications use to store any output.

### File Path Settings

**Attention!** File Paths are pre-defined application data or storage folder locations. These paths are expected to be relative or complete paths to a physical folder location accessible to the application.

🔍 | 🔄 Refresh

ID	Name	Path	Physical Path	Actions
ha	HPMS Assistant	{{DataDirectory}}\ha	C:\Program Files (x86)\Transcend Spatial So...	
logs	Site Logs Storage	{{DataDirectory}}\..logs	C:\Program Files (x86)\Transcend Spatial So...	
re	Report Templates Storage Location	{{DataDirectory}}\reports	C:\Program Files (x86)\Transcend Spatial So...	
sa	Segment Analyzer	{{DataDirectory}}\sa	C:\Program Files (x86)\Transcend Spatial So...	
temp	General Temporary Storage	{{DataDirectory}}\output	C:\Program Files (x86)\Transcend Spatial So...	

### Usage

#### Edit a File Path

To edit an existing file path:



Edit File Path

### File Path Settings

**ID:**

**Name:**

**Description:**

**Path:**   
Physical Path: C:\Program Files (x86)\Transcend Spatial Solutions\TDS\App\_Data\ha\

**URL:**

1. Locate the row for the File Path you wish to edit and click **Edit** (pencil icon).
2. Make desired changes to the form input.
3. Click **Save**.

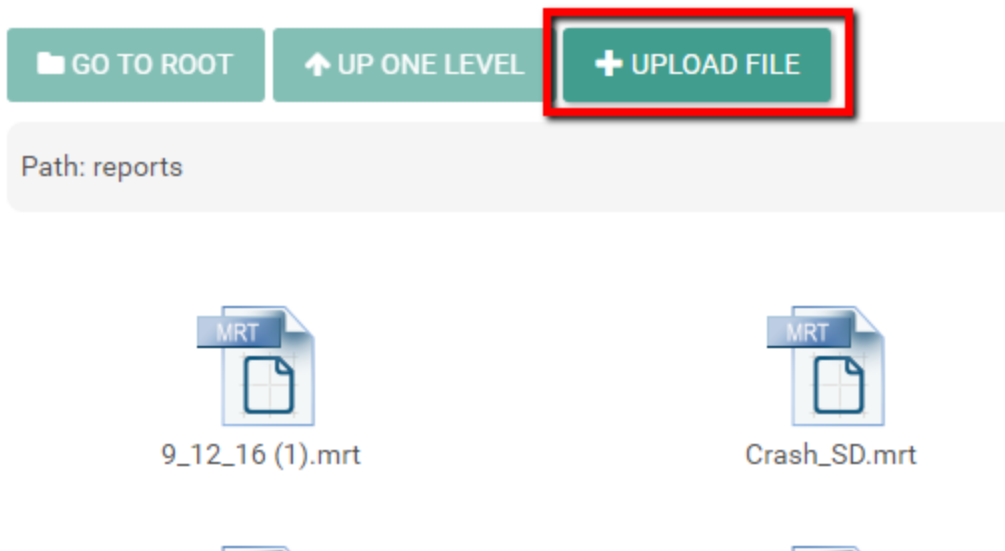
#### Explore a File Path

To explore an existing file path:

1. Locate the row for the File Path you wish to edit and click **Explore** (folder icon).
2. When finished, click **Back to List** (located at the top and bottom of the page).

#### Upload a New File

1. Locate the row for the File Path you wish to edit and click **Explore** (folder icon).
2. Click the **Upload File** button.



3. Navigate to the file you wish to upload and click **Open**.
4. The selected file will be uploaded to the selected destination.

## Load Balancer File Path Settings

When configuring TDS behind a load balancer it is often necessary to point the File Path Settings to a shared network folder (which all the replicated TDS servers would point to). In this scenario, there are various methods for sharing a network drive with an IIS application/process. Below are the two most common methods.

### Option 1 - Change Application Pool Identity to AD Account

One option is to change the TDS application pool to run under an Active Directory account which can then be set to have read and write privileges to the shared drive. The following steps will guide you through changing the TDS application pool identity to run under an AD account.

#### Change App Pool Identity

1. Create or chose an AD service account to run TDS under.
2. Share the desired network drive with the chosen AD service account.
3. Open IIS Manager on one of the replicated TDS application servers.

**Note:** The following process will need repeated on each TDS application server.

4. Navigate to the Application Pools list, under the appropriate site.
5. Right click on **TDSAppPool**.

6. Click **Advanced Settings**.

The screenshot shows the IIS Manager interface. On the left, the tree view shows 'Application Pools' expanded to 'Sites' and then 'Default Web Site'. Under 'Default Web Site', several application pools are listed: '1051-event-editor', '1051gis', '1051pub', 'aspnet\_client', and 'tds'. The main pane shows a table of application pools. The 'TDSAppPool' is selected, and a context menu is open over it. The 'Advanced Settings...' option is highlighted in yellow.

Name	Status	.NET CLR V...	Managed P
.NET v2.0	Started	v2.0	Integrated
.NET v2.0 Classic	Started	v2.0	Classic
.NET v4.5	Started	v4.0	Integrated
.NET v4.5 Classic	Started	v4.0	Classic
ArcGISWebAda...	Started	v4.0	Integrated
Classic .NET Ap...	Started	v2.0	Classic
DefaultAppPool	Started	v4.0	Integrated
<b>TDSAppPool</b>	Started	v4.0	Integrated

7. Select the options button in the **Identity** row.

The screenshot shows a configuration table for the 'Identity' row. The 'Identity' row is selected, and the options button (three dots) is circled in red.

Property	Value
Identity	ApplicationPoolIdentity
Idle Time-out (minutes)	0
Idle Time-out Action	Terminate

8. Select **Custom** account.

9. Click the **Set...** button.

10. Enter the AD service account (prefixed with the domain) and password.

**Example:** DOMAIN\admin.service

11. Click **OK**.

### Test the individual TDS server

1. Load the URL to the specific TDS application (not the URL through the proxy).
  1. We want to test that the configuration is working for this specific instance.
2. Go to **Administration > File Path Settings**.

3. Modify each of the file path's to point to the shared folder.

**Example:** \\YOUR\_SHARED\_SERVER\YOUR\_SHARED\_FOLDER\logs.

4. Click the **test** icon to verify that TDS has proper permissions to the shared folder.

**Administration**  
File Path Settings

**File Path Settings**

**Attention!** File Paths are pre-defined application data or storage folder locations. These paths are expected to be relative or complete paths to a physical folder location accessible to the application.

Filter | Refresh | Check Directory Permissions

Status	ID	Name	Path	Physical Path	Actions
<span style="color: green;">✔</span>	logs	Site Logs Storage	\\DEV-APP\tds_test_data\logs	\\DEV-APP\tds_test_data\logs	<span style="border: 1px solid yellow; border-radius: 50%; padding: 2px;">Test</span>   Edit   Delete
<span style="color: red;">✘</span>	seeding	Seed File Storage	\\DEV-APP\tds_test_data\seeding	\\DEV-APP\tds_test_data\seeding	Test   Edit   Delete
<span style="color: red;">✘</span>	temp	General Temporary Storage	\\DEV-APP\tds_test_data\temp	\\DEV-APP\tds_test_data\temp	Test   Edit   Delete

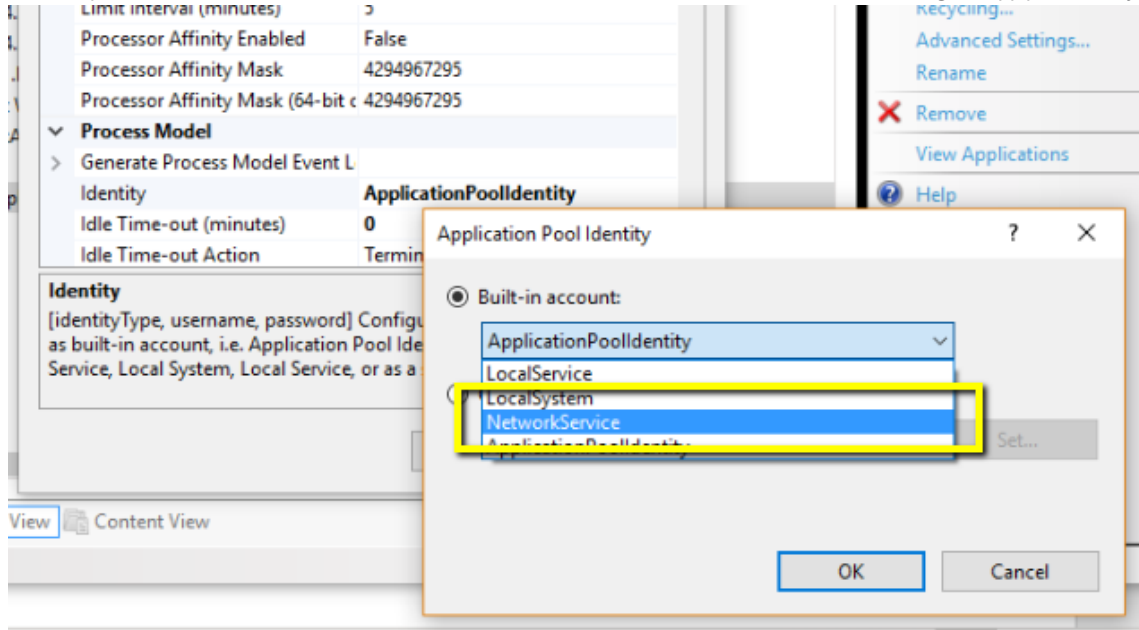
5. If the shared folder is accessible and has read/write privileges the status will become green.
6. If the shared folder does not have the necessary privileges (status of red), verify the following:
  1. Ensure that the folder is shared with Read and Write privileges with the AD service account.
  2. Ensure that the TDS Application pool is set to use the AD service account (has the domain filled in and has proper password entered).
  3. Ensure that you are running the proper TDS instance (should be directly running the specific replicated TDS server that you changed the app pool identity for).

### Option 2 - Change Application Pool Identity to Network

An alternative option is to change the TDS application pool to run under “Network” instead of an AD service account (as described in Option 1). In this case, access to the network will use the domain account for the server.

The following steps can be used in conjunction with the Option 1 steps:

1. Follow Option 1 instructions but select **NetworkService** rather than **Custom account** when selecting the app pool identity.



2. Set the shared driver permissions to grant Read/Write access to the server's domain account.

**Example:** DOMAIN\YOUR\_SERVER\_NAME.

**Note:** This option has not been confirmed or tested. This configuration option is based off Microsoft's documentation. Read more about this option's configuration [here](#).

## Scheduling Service Settings

General settings for the Job Execution Manager scheduler service are configured here.

**Scheduling Service Settings**

Scheduler Settings

**Scheduling storage mechanism:** SQLite Database  
The storage mechanism used to store scheduled job history details.

**Storage DB connection string:** Data Source=|DataDirectory|\JEM.sqlite;  
The database connection string to store scheduled job history details.

**Worker Count:** 1  
The number of workers to create on each application server.

Enable advanced administrator scheduling dashboard  
Check this option if you want to access an advanced administrator job scheduling dashboard.

Internally, Job Execution Manager (JEM) uses a library called [HangFire](#) to schedule and run tasks. By default, the HangFire implementation uses an internal SQLite database stored locally on the application server. This storage mechanism can/should be changed depending on the deployment configuration and desired functionality. Specific documentation on HangFire can be found [here](#).

**Heads Up!** After making any changes within this section, the TdsAppPool application pool within IIS must be recycled. If you are running a load balanced environment, then each TDS instance's application pool must be recycled.

**Note:** If JEM is running in a load balanced environment, then a shared database between the TDS instances must be used so the instances can stay in sync. The instances can use SQL Server (recommended) or they can be pointed to a single shared SQLite database file by making the SQLite database accessible to all TDS instances.

### Usage

#### Scheduling storage mechanism

Select where to store scheduled job history details.

**Scheduling storage mechanism:**

#### To Use:

1. Select the storage mechanism you wish to use from the dropdown.

#### Scheduling Storage Mechanism Options

There are 3 scheduling storage mechanisms that can be used – each with their own benefits and limitations.

**In Memory** – a fully functional storage mechanism that does not persist job history.

This option is good for testing environments or instances where persisted job history is not desired.

**SQLite Database** – a file-based database which is the default choice when installing JEM.

This option is good for single TDS instances or where an enterprise SQL Server database is not available.

**SQL Server Database** – an enterprise SQL Server database.

This option is good for production environments or when there are multiple TDS instances within a load balanced environment.

2. If using one of the SQL database options, enter the **Storage DB connection string** in the text box.

Storage DB connection string:

3. Click **Save**.

### Worker Count

The number of workers to create on each application server. This should match the number of processors that the TDS application has.

Worker Count:

### To Use:

1. Enter the desired number of workers.

**Note:** Increasing the number of workers may effect CPU speed

2. Click **Save**.

### Advanced administrator dashboard

Checking this option exposes an advanced administrator job scheduling dashboard at the specified path.

Enable advanced administrator scheduling dashboard

Check this option if you want to expose an advanced administrator job scheduling dashboard.

Advanced admin dashboard path:

[../scheduler](#)

The URL path to the advanced administrator job scheduling dashboard.

### To Use:

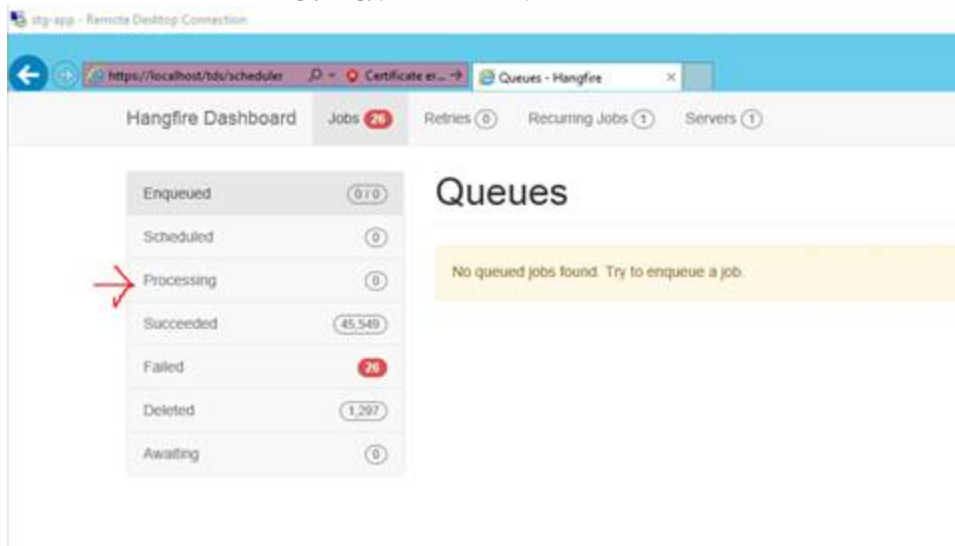
1. Click the checkbox next to **Enable advanced administrator scheduling dashboard**.
2. Enter desired path to scheduler in the **Advanced admin dashboard path** field.
3. Click **Save**.

### View HangFire Scheduler Dashboard

1. Log into the application server that TDS is installed on.

2. Go to <http://localhost/tds/scheduler>.

This will bring up the native HangFire dashboard, which is the underlying scheduling software used in JEM. From this dashboard you should be able to see the running (hung) process and stop it from there.





## Applications

[Installed Applications](#) - manage application settings

[Application Profiles](#) - create and manage application profiles

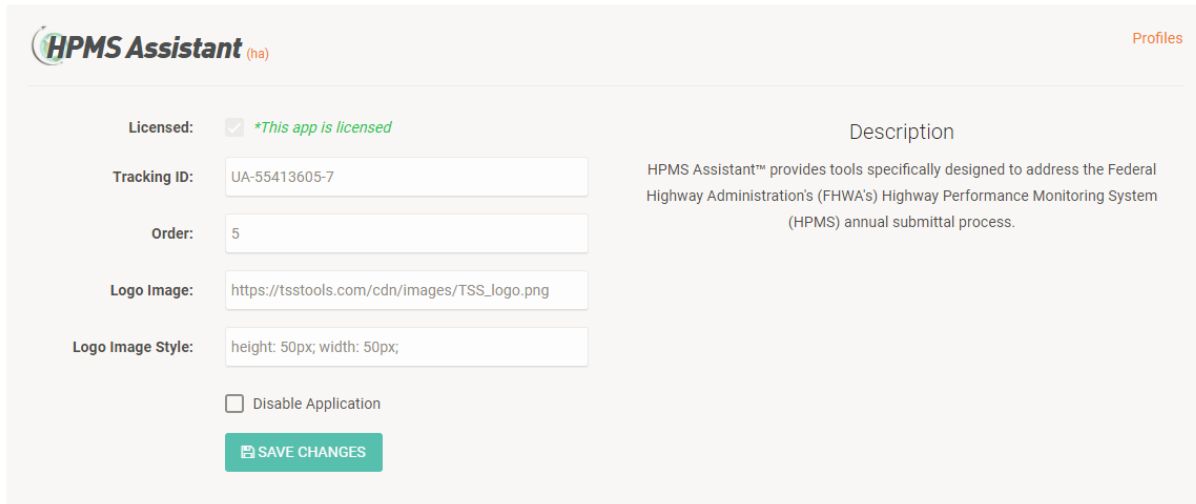
[Application Settings](#) - manage general settings used by the applications

[Publishing ESRI Service Definition Files](#) - retrieve and publish SD files for application input/export geometry services

[Integrations](#) - manage custom links and external application integrations

## Installed Applications

The Installed Applications feature allows you to see a list of all the applications that are currently installed. This is where you can change each applications tracking code, display order and visibility on the Apps Dashboard. You can also easily check if the application is licensed and how many profiles the application has.



The screenshot shows the configuration page for the 'HPMS Assistant' application. The page header includes the application logo 'HPMS Assistant (ha)' and a 'Profiles' link. The configuration is divided into two columns. The left column contains several settings: 'Licensed' with a checked checkbox and the text '\*This app is licensed'; 'Tracking ID' with a text input field containing 'UA-55413605-7'; 'Order' with a text input field containing '5'; 'Logo Image' with a text input field containing 'https://tsstools.com/cdn/images/TSS\_logo.png'; and 'Logo Image Style' with a text input field containing 'height: 50px; width: 50px;'. Below these fields is a checkbox for 'Disable Application' which is unchecked, and a green 'SAVE CHANGES' button. The right column is titled 'Description' and contains the text: 'HPMS Assistant™ provides tools specifically designed to address the Federal Highway Administration's (FHWA's) Highway Performance Monitoring System (HPMS) annual submittal process.'

### Usage

#### Tracking ID

This setting allows you to enter your tracking ID in order to send out the Google Analytics metrics for that application to your ID.

#### To Use:

1. Enter your Google Analytics tracking ID.
2. Click **Save Changes**.

#### Order

This setting allows you to change the order of the applications shown on the Apps Dashboard. For example, if you use the Road Analyzer application most frequently, you can specify it to have the order of 1 and then it will be the first application listed on the Apps Dashboard.

#### To Use:

1. Enter an order value (from 1 - 6).
2. Click **Save Changes**.

#### Disable Application

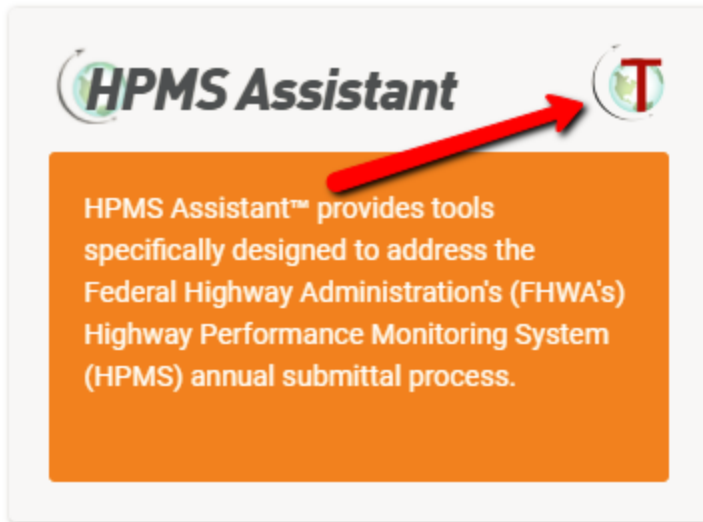
This setting disables the application so it is no longer visible on the Apps Dashboard. This does not uninstall the application.

## To Use:

1. Check the checkbox to disable visibility or uncheck the checkbox to enable visibility.
2. Click **Save Changes**.

## Logo Image and Logo Image Style

With these settings you can add a logo image to the top right corner of application on the [Apps Dashboard](#) and have the option to add styling for the logo using inline CSS.



## To Use:

1. Enter your logo image path in the **Logo Image** text box.
2. *Optional:* Enter any desired inline CSS into the **Logo Image Styling** text box.
3. Click **Save Changes**.

## Application Profiles

Application profiles provide the ability to create multiple configurations for the same application. By creating multiple configurations (profiles) you can change defaults and application behavior to better suite the target user's needs. For example, let's say you have a Pavement group, a Traffic group and an Inventory group and you'd like each group to have their own version of the application that uses a different map service, default configurations, etc. Application Profiles gives you the flexibility to provide this functionality.

+
App Profiles

### Setup Application Profiles

Further configuration will occur within the application

i

Application profiles provide the ability to create multiple configurations for the same application. By creating multiple configurations (profiles) you can change defaults and application behavior to better suite the target user's needs.

🔍 | ↻ Refresh
➕ Add New

Application	Profile ID	Name	Description	Actions
Road Analyzer	pavement_group	Pavement Group		↔   ✎   🗑️
Road Analyzer	traffic-group	Traffic Group		↔   ✎   🗑️
Segment Analyzer	pavement_group	Pavement Group		↔   ✎   🗑️

## Usage

### Add New

+
Enter New Profile

**Application:**

**Profile Name:**

**Profile ID:**

✖ CANCEL
✔ SAVE

To add a new profile:

1. Click **Add New**.
2. Fill in the **Profile Name** and **ID**.

**Heads Up!** If you are creating a new profile for HPMS Assistant, the **Profile ID** needs to be 10 characters or less. If the Profile ID is longer than 10 characters, the validation tables names will be too long causing the validations to fail to run.

3. Click **Save**.

### Run Profile

To view a profile:

1. Click the **run arrow icon** in the Action column of the Name of the Profile you want to view.
2. A new browser tab will open and load the profile of the application you selected.

#### **Edit Existing**

To edit an existing profile:

1. Click the **pencil icon** in the Action column of the Name of the Profile you want to edit.
2. Make your edit(s).
3. Click **Save**.

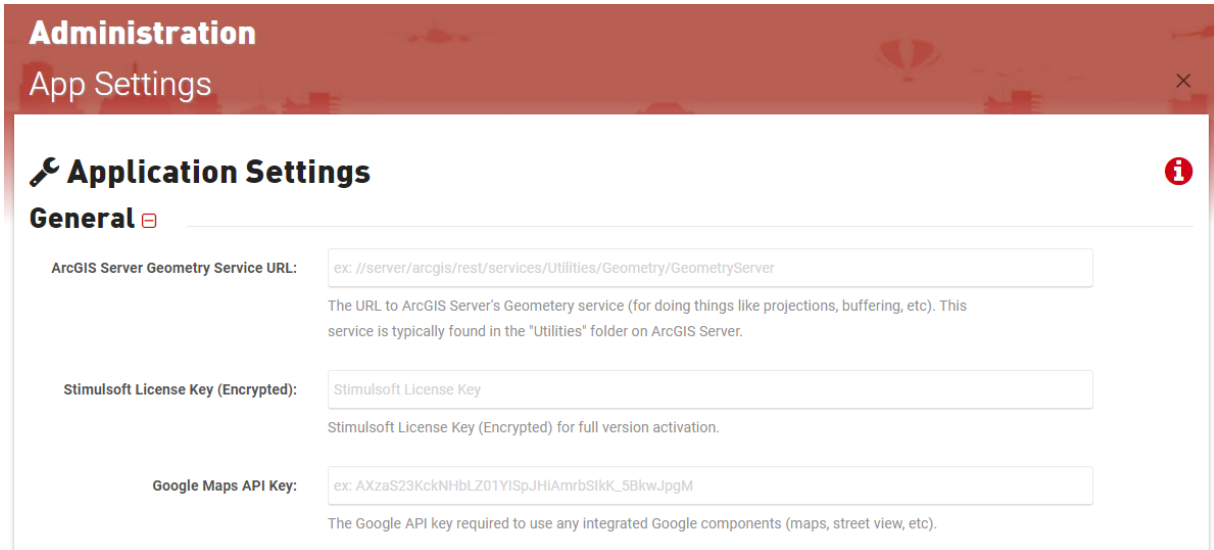
#### **Delete Existing**

To delete an existing profile:

1. Click the **trashcan icon** in the Action column of the Name of the Profile you want to delete.
2. Click **Delete** in the Delete Profile popup.

## Application Settings

The Application Settings feature allows you to manage general settings used by the applications such as the geometry service URL and Google API credentials.



The screenshot shows the 'Administration' section with a sub-tab for 'App Settings'. The main heading is 'Application Settings' with a wrench icon and an information icon. Under the 'General' section, there are three settings:

- ArcGIS Server Geometry Service URL:** A text input field containing the example URL 'ex: //server/arcgis/rest/services/Utilities/Geometry/GeometryServer'. Below the field is a descriptive text: 'The URL to ArcGIS Server's Geometry service (for doing things like projections, buffering, etc). This service is typically found in the "Utilities" folder on ArcGIS Server.'
- Stimulsoft License Key (Encrypted):** A text input field containing the placeholder 'Stimulsoft License Key'. Below the field is a descriptive text: 'Stimulsoft License Key (Encrypted) for full version activation.'
- Google Maps API Key:** A text input field containing the example key 'ex: AXzaS23KckNHbLZ01YISpJHiAmrbSikk\_5BkwJpgM'. Below the field is a descriptive text: 'The Google API key required to use any integrated Google components (maps, street view, etc).'

### Usage

#### General Application Settings

##### ArcGIS Server Geometry Service URL

The URL set here will be used by the applications for doing geometry operations, such as projecting map extents.

##### To Use:

1. Enter the geometry service URL.
2. Click **Save**.

##### Stimulsoft License Key (Encrypted)

The Stimulsoft License Key provides full access to functionality found in the [Reports](#) tool as well as [Report Engine](#).

##### To Use:

1. Enter your Stimulsoft license key.
2. Click **Save**.

##### Google API

As explained in the [Google Maps API Disclaimer](#), using Google Maps API components in authentication restricted applications requires the purchase of the Google Maps API Premium Plan. Once purchased, Google will supply you with a Google Maps API

Client ID and a Google Maps API Key, and possibly a Maps API Signature and/or Maps API Channel to use in conjunction with the key.

**To Use:**

1. Enter your information in the fields provided.
2. Click **Save**.

**Heads Up!** Per Google, you may receive error messages and Google may block your Maps API access if a Google API Client ID and Maps Key are not provided and you use the Maps API anyway.

**Note:** You can leave these fields blank if you do not plan to use the Google Maps API (Street View).

**Error Report Email**

The email address set here is where all error messages reported by users will be sent.

**Note:** Individual "application profiles" can specify their own error report email addresses which will override this default recipient address.

**To Use:**

1. Enter the desired email address.
2. Click **Save**.

**Bing Maps API Key**

As explained in [Bing Maps API licensing options](#), using the Bing Maps API in authentication restricted applications may require the purchase of the Bing Maps API License Plan. Once purchased, Microsoft will supply you with a Bing Maps API Key.

**To Use:**

1. Enter your Bing Maps license key.
2. Click **Save**.

**ArcGIS for Portal URL and App ID**

The ArcGIS for Portal URL and App ID will be used to authenticate applications.

**Note:** This is needed if you checked the **Service requires ArcGIS for Portal authorization** option when adding a [Data Source](#). See the [Configure Portal for ArcGIS](#) topic for full details on setting up ArcGIS for Portal.

**To Use:**

1. Enter your Portal URL and Portal App ID.
2. Click **Save**.

**Application Base URL**

This field should contain the URL used to access your TDS application. This should be configured since some tools, such as JEM's

generate and email report action, rely on using it as a token for api requests.

**Example:** <https://server-name/tds>.

**To Use:**

1. Enter the URL used to access your TDS application.
2. Click **Save**.

**ArcGIS Portal Fetch Credentials**

This field defaults to “same-origin” when left blank which meets most use cases when using ArcGIS for Portal. In certain scenarios however (for example when using Integrated Windows Authorization), you may need to set the credentials option to “include”, or “omit”.

**To Use:**

1. Enter the desired credential option: [“same-origin”, “include”, “omit”].
2. Click **Save**.

**Include Geometry Service URL**

Allows you to enter a geoprocessing service URL for the 'Include Geometry' geoprocessing service. This will be needed to use the "[Create geometry in output table \(add shape field\)](#)" option in Segment Analyzer.

**To Use:**

1. Enter the URL to the "include geometry" geoprocessing service.

**Tip:** The exact name of the "include geometry" service may vary, depending on if the defaults were used when publishing the service.

2. Click **Save**.

**Note:** To publish an ESRI Service Definition file (.sd file), refer to the [ESRI documentation](#) (links below). Additional details and steps are also provided in the [Publishing ESRI Service Definition Files](#) topic.

[Publishing a service definition to the server in ArcGIS for Desktop](#)

[Publishing a service definition to the server in Manager](#)

**Test Schema Lock GP Service URL**

Allows you to enter a URL for the 'Test Schema Lock' geoprocessing service. This will be needed to use the "[Test for table schema lock prior to running process](#)" option in Segment Analyzer.

**To Use:**



1. Enter the URL to the "test schema lock" geoprocessing service.

**Tip:** The exact name of the "test schema lock" service may vary, depending on if the defaults were used when publishing the service.

2. Click **Save**.

**Note:** To publish an ESRI Service Definition file (.sd file), refer to the ESRI documentation. Additional details and steps are also provided in the [Publishing ESRI Service Definition Files](#) topic.

<http://server.arcgis.com/en/server/latest/publish-services/windows/publishing-a-service-definition-to-the-server-in-arcgis-for-desktop.htm>

<http://server.arcgis.com/en/server/latest/publish-services/windows/publishing-a-service-definition-to-the-server-in-manager.htm>

### Geoprocessing Services Polling Rate

The number of milliseconds you want the service to wait between checking geoprocessing service job statuses (the service check rate).

#### To Use:

1. Enter a wait time in milliseconds.
2. Click **Save**.

### Geoprocessing Services Account Username and Password

The service account username and password which will be used to authenticate against any geoprocessing services executed from the server.

**Heads Up!** This is only required if the Geoprocessing Service is not shared with everyone, otherwise the applications will not be able to access the service.

**Note:** If using **ArcGIS for Portal** authorization, TDS will attempt to authenticate geoprocessing services through Portal as well. Therefore, you'll need to ensure that the "Geoprocessing Services Account Username/Password" is also a built-in ArcGIS Portal account. See the [Configure Portal for ArcGIS](#) topic for full details on setting up ArcGIS for Portal.

#### To Use:

1. Enter the username and password for the account.
2. Click **Save**.

### Map Services Account Username and Password

The service account username and password which will be used to authenticate against any map services consumed from the server. This is required if the map service is secured and/or is using ArcGIS branch versioning. If you add multiple map services for the applications to use, this account must have access to them all. These credentials will be used to authenticate with Portal and then query ArcGIS server for the data.

#### To Use:

1. Enter the username and password for the account.
2. Click **Save**.

## HPMS Assistant Settings

### FHWA Validation Seed File Version

The version of the current seed file included for seeding the FHWA validations for HPMS Assistant. This value is auto populated when a new version of HPMS Assistant is installed - or - the seed data is updated manually or by [importing a new validations seed file](#).

### HPMS Metadata Seed File Versions

The HPMS Metadata includes all settings related to Data Groups and Items that will be used to create data tables and CSVs for FHWA submittal. The **HPMS Metadata Seed File Version (latest release)** value is auto populated when the application or the seed data file is updated. The **HPMS Metadata Seed File Version (last used)** value is the last version of the seed file that is currently being used in HPMS Assistant.

When a profile in HPMS Assistant is opened, the application will automatically compare these versions and if the version numbers do not match, you will be notified that updates are available.

### Remove HPMS Validations on HA Profile Delete

When a HPMS Assistant profile is deleted, this setting will affect whether or not the HPMS validations created in the associated Validation Assistant profile are also deleted. If set to **true**, the validations will be deleted. If set to **false**, the validations will not be deleted.

**Example:** Multiple HPMS Assistant profiles are associated to the same Validation Assistant profile, then the validations should not be deleted, so you would enter **false** into this setting.

### HPMS Data Table Section Cutoff Length

When the HPMS Data Table is built, sections having a length less than or equal to the value set here will not be included in the table.

### Certified Mileage Calculation

The SQL statement entered in these settings will be used to calculate the certified mileage which is used to [Validate Certified Mileage](#). Unless any edits are made, HPMS Assistant will use a calculation based on the standard logic outlined in the FHWA documentation.

### Summary Table Calculations

The SQL statement entered in these settings will be used to produce the [County, Urban, and Statewide Summary Tables](#). Unless any edits are made, HPMS Assistant will use a calculation based on the standard logic outlined in the FHWA documentation.

### Job Execution Manager Settings

This setting provides the ability to set the Maximum number of records per translate request. This setting is only available in the app-mgr UI and as there is no Application Setting UI in the JEM app. The default value is 1000.

#### To Use:

1. Enter a desired number between 1 and 1000.
2. Click **Save**.

### Segment Analyzer Settings

#### Avoid Spaces as a Delimiter

When entering any route(s) into Segment Analyzer, if **Avoid Spaces as a Delimiter** is set to "true" the Route IDs will not split or trim the spaces in the Route ID. If your Route IDs do not have spaces, you can enter "false" for this setting.

**To Use:**

1. Enter true/false.
2. Click **Save**.

**Column Names**

The following settings provide the ability to override Segment Analyzer's default column names for ID, Route ID, From Measure and To Measure and configure them to custom field names.

<b>ID Column Name:</b>	<input type="text" value="Id"/>
	Column name that will used for Segment Analyzer output table ID field.
<b>Route ID Column Name:</b>	<input type="text" value="RouteId"/>
	Column name that will used for Segment Analyzer output table route ID field.
<b>From Measure Column Name:</b>	<input type="text" value="FromMeasure"/>
	Column name that will used for Segment Analyzer output table from measure field.
<b>To Measure Column Name:</b>	<input type="text" value="ToMeasure"/>
	Column name that will used for Segment Analyzer output table to measure field.

**To Use:**

1. Enter your information in the fields provided.
2. Click **Save**.

**Heads Up!** If these settings are changed, you will need to load and rerun any existing [Segment Analyzer templates](#), then update the corresponding column names in any existing [HPMS Assistant mappings](#) and [Validation Assistant validations](#).

## Publishing ESRI Service Definition Files

In order to utilize geometry input/export features in Rizing Geospatial's applications such as the "Include Geometry GP Service" and "Test for Table Schema Lock" in Segment Analyzer, as well as the "Export Geometry" feature in HPMS Assistant, a geoprocessing service must be published and configured in TDS. Once published, the service URL must also be configured in the [Application Settings](#) for each app utilizing the service. The SD files available to publish the services are available from the TDS App Manager [Downloads](#) page.

### Usage

#### Download and Publish a Service

1. Click the **Downloads** tab in top menu of App Manager. There are 2 different **include-geometry.sd** files; one for ArcGIS Desktop and another for ArcGIS Pro. Find the file that matches your environment and click **DOWNLOAD**.

Q | Filter | Refresh

Product	File Name	Creation Date	Description	Download	Actions
HPMS Assistant	route-geometry-export.sd	03/31/21 01:47 PM	Route geometry export G...	DOWNLOAD	Help   Actions
HPMS Assistant	hpms_metadata.tss	04/16/20 08:58 AM	File used by HPMS Assis...	DOWNLOAD	Help   Actions
HPMS Assistant	validations.tss	03/31/21 01:45 PM	File used by HPMS Assis...	DOWNLOAD	Help   Actions
Road Analyzer	SLD Print.mrt	04/26/19 09:15 AM	RE template for SLD print...	DOWNLOAD	Help   Actions
Road Analyzer	event-editor-widget.zip	04/01/21 12:01 PM	RA widget for Event Edito...	DOWNLOAD	Help   Actions
Segment Analyzer	include-geometry.sd	04/01/21 10:54 AM	ArcGIS Desktop include g...	DOWNLOAD	Help   Actions
Segment Analyzer	include-geometry-pro.sd	04/01/21 10:52 AM	ArcGIS Pro include geom...	DOWNLOAD	Help   Actions
Segment Analyzer	test-schema-lock.sd	04/01/21 10:55 AM	Test schema lock GP ser...	DOWNLOAD	Help   Actions

2. Publish the **SD file**. This can be done either from ArcGIS Desktop or through the ArcGIS Manager web interface. Links for detailed steps from ESRI are provided below as well as brief step-by-step instructions for each method.

[Publishing a service definition to the server in ArcGIS for Desktop](#)

[Publishing a service definition to the server in Manager](#)

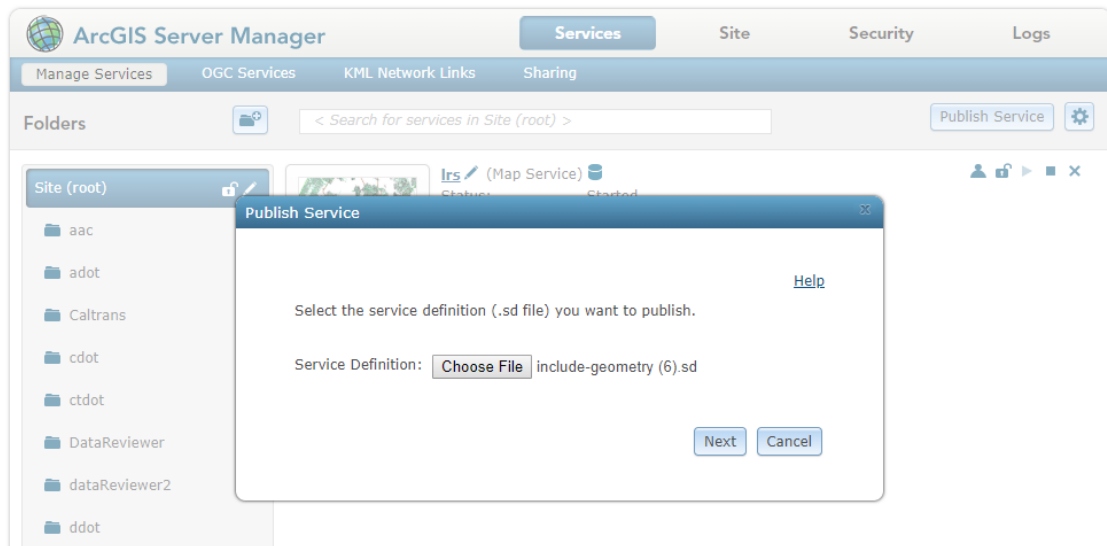
3. Enter the URL into the [Application Setting](#) for that feature.

**Example:** For the includegeometry.sd, after publishing the SD file, you would enter the URL into the "Include Geometry Service URL" setting.

#### Publishing from ArcGIS Server Manager

1. Launch **ArcGIS Server Manager**.
2. Click **Publish Service** in the upper right corner.

3. Select the downloaded **SD file** (ex: includegeometry.sd).

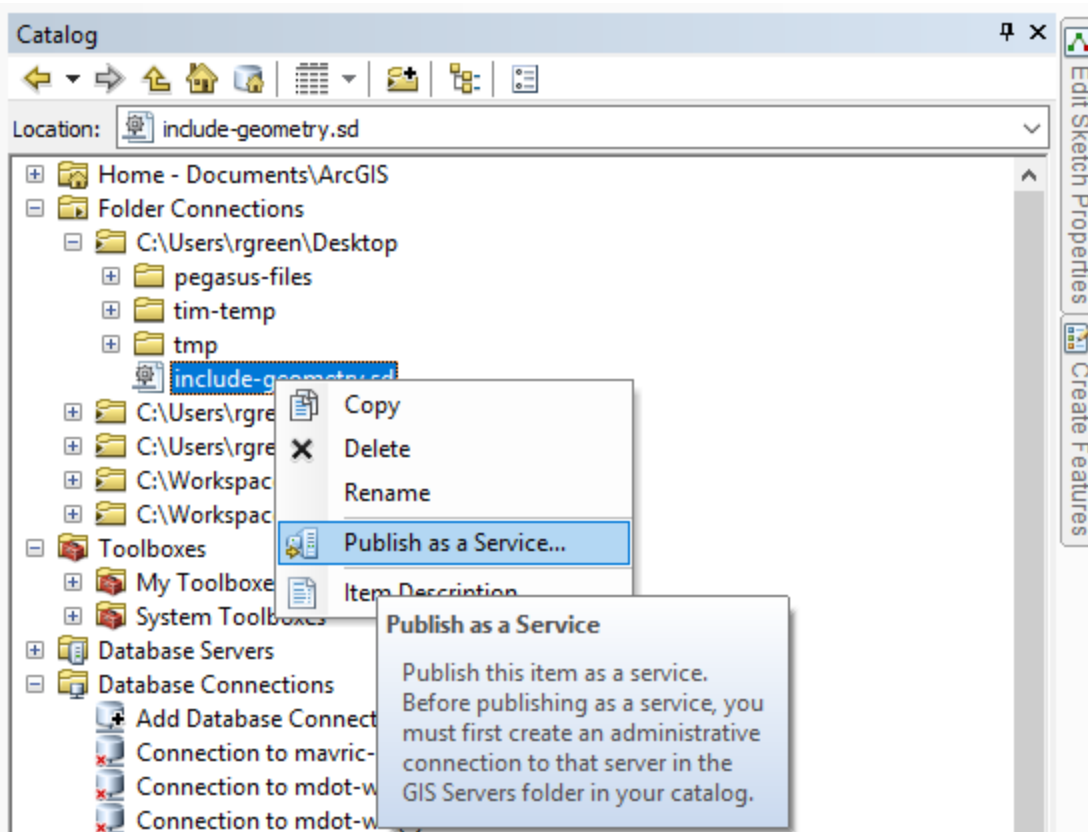


4. Click the **Next** button.
5. Select a **folder location** and make any desired changes (if applicable).
6. Click **Next**.
7. Click **Publish**.

#### Publishing from ArcGIS Desktop

1. Open **ArcMap** or **ArcCatalog**.
2. Connect to the **folder location** where the service definition file has been downloaded to.
3. Navigate to, and right click the **SD file**.

4. Click **Publish as a Service...**



5. Select the **connection**, **folder**, and other details.
6. Click **Finish**.

## Integrations

Integrations allows you to add and manage custom links as well as application integrations that are external to the Transportation Data Server application. Integrations can be embedded or added as links that displays on App Manager's home page.

The screenshot shows the App Manager interface with a navigation bar at the top containing 'App Manager', 'Apps', 'Administration', and 'Help'. A user greeting 'Welcome Jodie!' and an 'ACCOUNT' dropdown are on the right. Three application cards are displayed:

- HPMS Assistant** (orange): HPMS Assistant™ provides tools specifically designed to address the Federal Highway Administration's (FHWA's) Highway Performance Monitoring System (HPMS) annual submittal process.
- Validation Assistant** (green): Analyze and resolve data discrepancies with Transcend's Validation Assistant™. VA provides cross-app integrations to resolve your data issues using standard business processes.
- Segment Analyzer** (purple): Segment Analyzer™ provides the ability to combine road characteristic data that has been modeled in un-segmented relational tables into segmented tables based on a variety of methods.

Below the applications is a 'Links' section with '3 Available' links:

- SharePoint**: Includes the SharePoint logo.
- IM User Guide**: Includes a blue square icon.
- Google Maps**: Includes a light green square icon with the text 'Click to launch integration' and 'Google Maps'.

## Usage

### Add New

To add a new integration:

### Manage Custom Integrations

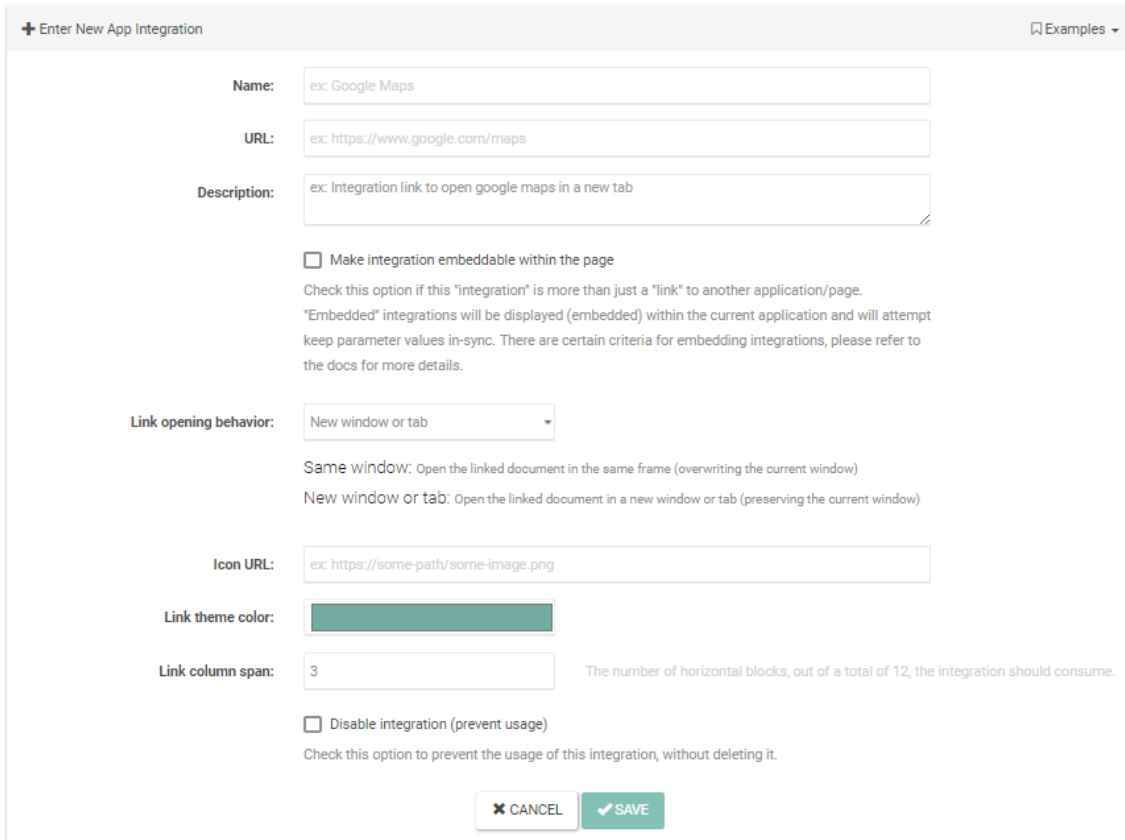
Add and edit custom web applications and links that are external to the Transportation Data Server application.

🔍 | Filter | Refresh

Add New

Name	URL	Embedded	Disabled	Actions
SharePoint	https://www.office.com/?auth=2&home=1			↑   ↓   ✎   🔄   🗑️
IM User Guide	https://docs.tsstools.com/im/Content/Home.htm			↑   ↓   ✎   🔄   🗑️
Google Maps	https://google.com			↑   ↓   ✎   🔄   🗑️

1. Click **+ Add New** to open the new Integration form.



**+ Enter New App Integration** Examples ▾

**Name:**

**URL:**

**Description:**

**Make integration embeddable within the page**  
Check this option if this "integration" is more than just a "link" to another application/page. "Embedded" integrations will be displayed (embedded) within the current application and will attempt keep parameter values in-sync. There are certain criteria for embedding integrations, please refer to the docs for more details.

**Link opening behavior:**

**Same window:** Open the linked document in the same frame (overwriting the current window)  
**New window or tab:** Open the linked document in a new window or tab (preserving the current window)

**Icon URL:**

**Link theme color:**

**Link column span:**  The number of horizontal blocks, out of a total of 12, the integration should consume.

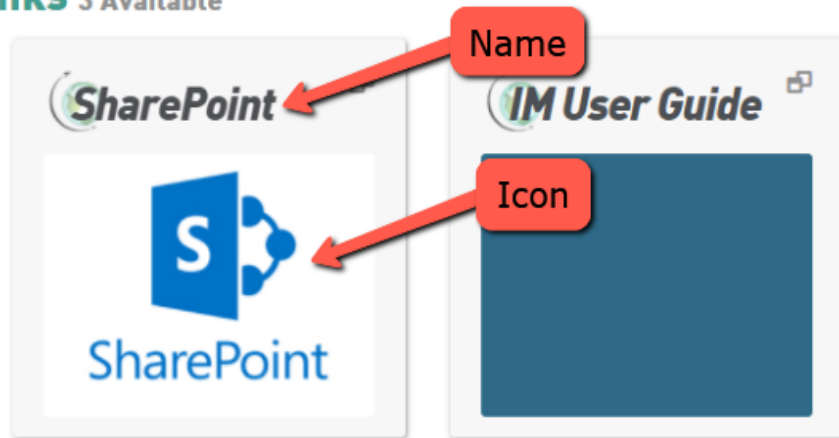
**Disable integration (prevent usage)**  
Check this option to prevent the usage of this integration, without deleting it.

**Note:** To view examples of popular integrations, such as ArcGIS Map and Google Street View, click Examples in the top right corner and select the integration you would like.

2. Enter a name for the link or integration in the **Name** field.
3. Enter the URL for your external link or integration in the **URL** field.
4. Enter a description for the link or integration in the **Description** field.
5. Check the box beside **Make integration embeddable within the page** to make the integration embedded within the application. If unchecked, the integration will be a click-able external link.
6. Select the **Link Opening Behavior** from the dropdown. Options include:
  1. Same window - Integration will load in the current browser window
  2. New window or tab - Integration will load in a separate browser window
7. If you'd like an image or icon to display for the link or integration, enter a URL for the image in the **Icon URL** field. (image will display inside the link as shown below)



## Links 3 Available



**Note:** If no Icon URL is added, the link will display the link theme color selected below.

- Click on the **Link theme color** selector to select a color for the link or integration. (selected color will show in the background of the link icon, or behind the image if you've added an Icon URL)
- Enter the number of horizontal blocks (1-12) you wish the link or integration to take up across the display in the **Link Column span** field.
- You can disable the link or integration by checking the **Disable integration (prevent usage)** checkbox.
- Click **Save**.

### Change Order

To change the order of existing integrations in the Integrations menu:

- Click the **up or down arrow** in the Actions column of the integration you want to reorder.

### Update Existing

To update an existing integration:

- Click the **pencil icon** in the Action column of the integration you want to update.
- Make the needed updates in the form.
- Click **Save**.

**Heads Up!** Disclaimer: All Google Maps JavaScript API applications are subject to the limitations of Google's [Terms of Service](#). Therefore to use any imbedded Google Map tools within the applications, you will need to adhere to Google's [Terms of Service](#) - this typically means you need to purchase an enterprise license. To learn more please visit Google Maps' [Get a Key/Authentication](#) page.

### Test Integration

🔍 | ▼ Filter | ↻ Refresh ➕ Add New

Name	URL	Embedded	Disabled	Actions
SharePoint	https://www.office.com/?auth=2&home=1			↑ ↓ ↻ ↗ 🗑️
IM User Guide	https://docs.tsstools.com/im/Content/Home.htm			↑ ↓ ↻ ↗ 🗑️
Google Maps	https://google.com			↑ ↓ ↻ ↗ 🗑️

To Test an integration:

1. Click the **angled arrow icon** in the Action column of the link or integration you want to test.
2. The integration should open in a separate browser window.

### Delete Existing

Q | Filter | Refresh Add New

Name	URL	Embedded	Disabled	Actions
SharePoint	https://www.office.com/?auth=2&home=1			↑   ↓   ↗   ↻   🗑️
IM User Guide	https://docs.tsstools.com/im/Content/Home.htm			↑   ↓   ↗   ↻   🗑️
Google Maps	https://google.com			↑   ↓   ↗   ↻   🗑️

To delete an existing integration:

1. Click the **trashcan icon** in the Action column of the link or integration you want to delete.
2. Click **Delete** in the Delete Integration popup.

## Actions

The Actions section holds a few options that affect all the applications and users. These may be needed by administrators when making changes that affect users or an application.

### Actions

---

#### Force all users to re-authenticate

Forces all users to re-sign in, their next visit. Currently all users that have not signed in after Mar 16, 2018 will be forced to re-authenticate

#### Restart application

Shutdown and restart the server application.

#### Refresh Privileges

Seed any missing privileges and update privilege details (names, descriptions, etc) to the latest. No action will be taken if no privilege updates are found.

## Usage

### Force all users to re-authenticate

This action will require all users in their next visit to re-sign in.

**Example:** If you need to change the [Role Privileges](#) for a User Group and then this will force the application to sign everyone out so that the application has to go back and re-query their privileges.

1. Click on the **Force all users to re-authenticate** text.
2. Click **Continue**.

**Note:** The date will be updated on the Administration page and the **Invalidate All Tokens** date and time on the [Security Settings](#) page.

### Restart application

This action will shutdown and restart the application on the server.

**Example:** An application has been installed but it not showing on the Apps Dashboard, then this could recycle the application pool to force it to find all the applications installed.

1. Click on the **Restart application** text.
2. Click **Continue**.

### Refresh Privileges

Privilege names and descriptions are seeded when TDS is initially installed and do not automatically get "reseeded" when a new version of TDS (App Manager) is installed. This action "reseeds" the privilege list and will add any missing privileges, remove any non-licensed (or uninstalled) privileges, prune any duplicate privileges, and update privilege names and descriptions with the latest installed version. The number of privileges updated will be displayed to the right of the **Refresh Privileges** text. If no privilege updates are found, it will display "0 privileges updated."

### Refresh Privileges

4 privileges updated

Seed any missing privileges and update privilege details (names, descriptions, etc) to the latest. No action will be taken if no privilege updates are found.

1. Click on the **Refresh Privileges** text.
2. Click **Refresh**.

## I'm seeking to expand my knowledge of Application Manager

You've got the fundamentals down, now's the time to explore the topics below to broaden your knowledge. The following sections cover system requirements, application configuration and everything you need to know to get the underlying web application framework (.NET MVC) up and running in your environment.

[Advanced Configurations](#)

[Setting Up Configuration Store Permission](#)

[Application Architecture](#)

[Application Security](#)

[Diagnosing Installation Errors](#)

[Manual Installation](#)

[Options and Silent Installs](#)

[Scalability and Performance](#)

[WCAG and 508 Compliance](#)

[Services API Reference](#)

### We suggest the following steps when getting started:

1. Familiarize Yourself With RESTful Services:

Representational state transfer (REST) is a style of software architecture for distributed systems such as the World Wide Web. REST has emerged as a predominant web API design model. The term representational state transfer was introduced and defined in 2000 by Roy Fielding in his doctoral dissertation. Fielding is one of the principal authors of the Hypertext Transfer Protocol (HTTP) specification versions 1.0 and 1.1. Read about Representational State Transfer (REST) architectural principles and how to consume REST services. Learn more...

2. Consume the Services/Data:

You can easily consume endpoints marked as a "GET" request by simply navigating to the url in your browser. The browser will display the response from the service in your browser window. There are many clients and plug-ins available to help construct service requests:

[Chrome Advanced REST Client Plug-in](#)

[Firefox REST Client Add-On](#)

[Fiddler](#)

[.NET REST Client](#)

[Java REST Client](#)

## Advanced Configurations

All required system-level configurations will automatically be configured through the installation wizard. Other application settings can be configured directly through the application's Administration Interface. However, under certain scenarios (uncommon), it may be required to manually make system-level configuration changes directly on the application server (or servers if more than one) - rather than through the application's administration UI.

**Note:** If any changes are manually made to the application's web.config file (not recommended), then those same changes will have to be made after installing new versions of the software. The existing web.config file will be overwritten with every installation/update. Configuration settings will automatically be restored by the application, from the configuration database, upon application start.

### Configuration Storage Mechanism

The application needs a place to store application configurations, user preferences, saved templates, and other session persisted information. The default storage mechanism will use a "SQL Compact Edition" file database that will be located in the "App Data" directory of the application hosted on IIS.

The configuration data store, out of the box, can be configured to point to any of the following databases:

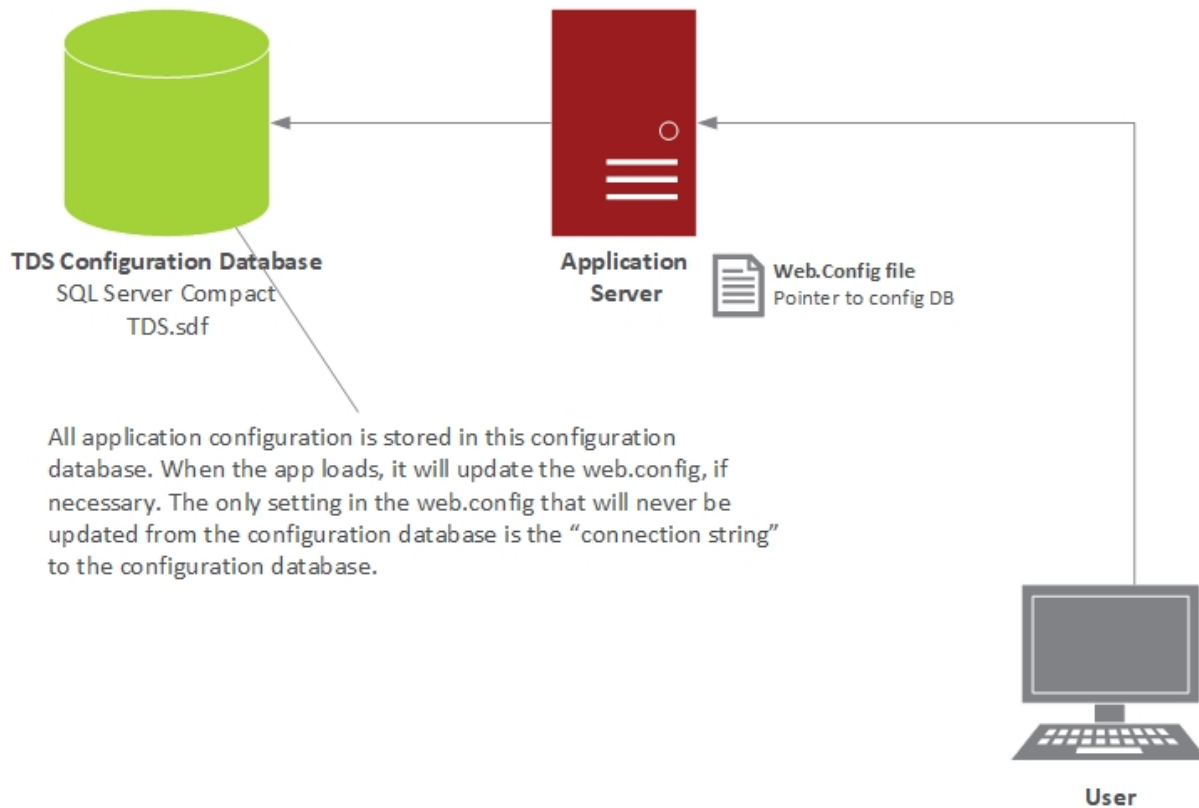
SQL Compact Edition

SQL Server

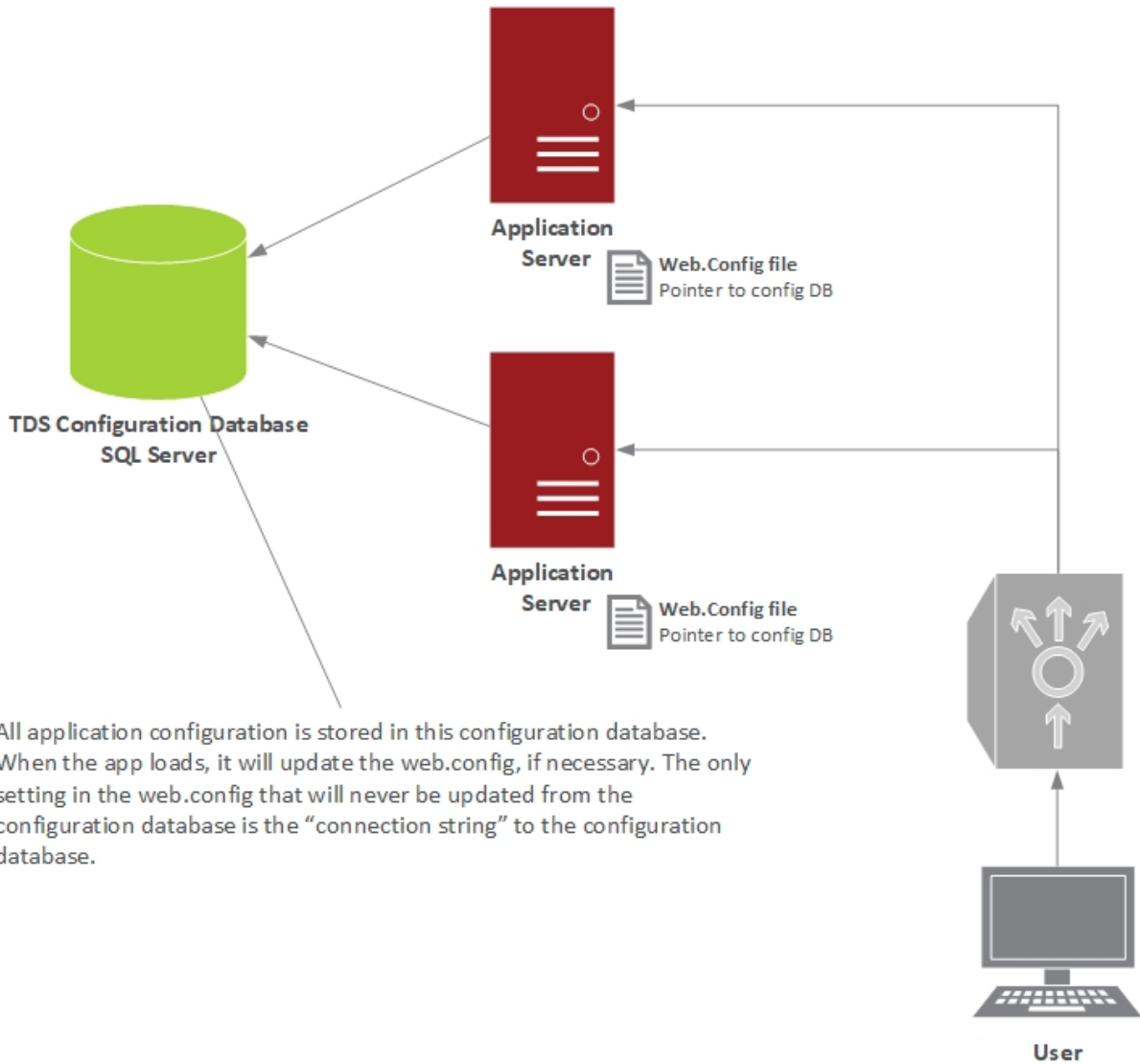
Oracle

**Note:** Detailed step-by-step instructions for setting up your configuration store can be found here: [Setting Up Configuration Store Permission](#)

## Default Configuration Database (Not Load Balanced)



## Configuration Database in a Load Balanced Environment



All application configuration is stored in this configuration database. When the app loads, it will update the web.config, if necessary. The only setting in the web.config that will never be updated from the configuration database is the “connection string” to the configuration database.

### Configuration for Load Balanced Environments

The application can be replicated to multiple application servers and function in a load balanced environment, however the following considerations should be taken:

The connection to the configuration database must have read/write permissions, in order to create objects (ONLY within that specific database/catalog).

The configuration database must be shared by all the replicated application servers, and therefore must be an enterprise database, so that all application instances can point to the same configuration store. See the [Configuration Storage Mechanism](#) section for details on changing this.

The web.configs, for each application instance, must be identical across all the applications. This can be done through the [Configuration Store](#) component (see steps below).



All [File Path Settings](#) must be pointed to a shared folder (which all TDS instances can access). The only exception is the "logs" file path.

*Server-side caching* must be turned off in the [General Server Settings](#).

#### Steps to follow, for setting up TDS behind a load balancer:

1. Install the first TDS instance on the first application server.
2. Navigate to the [Configuration Store](#) page under the [Administration Console](#).
3. Check the **Specify Database** check-box.
4. Enter in database connection info for the enterprise configuration database, which will be shared across TDS app instances.
5. Test the connection, to make sure it is valid; the connection must be valid before saving.
6. Click **Save** and confirm save in the confirmation popup.
  1. If saved successfully, this will reload the page and take you back to the **Administration** page.
  2. This process can take several minutes, please be patient.
7. Import your license (see [License](#) section).
8. Update all of your [File Path Settings](#) to point to shared folders.
  1. Example:  
Change "temp" from "{{DataDirectory}}\output" to: "k:\shared\_app\_files\tds\output"  
Change "temp" from "{{DataDirectory}}\seeding" to: "k:\shared\_app\_files\tds\seeding\  
Change "temp" from "{{DataDirectory}}\logs" to: "k:\shared\_app\_files\tds\logs\  
  
2. NOTE: there are several strategies that can be used to share a network drive with a particular application. One is to change the TdsAppPool identity to an AD service account
    1. IIS > Application Pools > Right click "TdsAppPool".
    2. Click "Advanced Settings".
    3. Change "Identity" to "Custom Account".
    4. Enter the service account you would like the application to run under.
    5. Share the network drive with the service account that the application is running under.
    6. After updating the [File Path Settings](#) to point to shared folders, test the privileges using the built in "Test" action in the [File Path Settings](#) grid.
9. Make any additional global application configuration/settings changes.

This step is optional (see the [Note](#) at the end of this list).
10. Install TDS on the second application server - this will be the replicated (second) instance of the TDS application.
11. Navigate to the [Configuration Store](#) page under the [Administration Console](#).
12. Check the **Specify Database** check-box.
13. Enter the exact same connection info that was entered in **Step 4** (connection to the enterprise configuration database).
14. Click **Save** (and confirm save in the confirmation popup).

If saved successfully, this will reload the page and take you back to the **Administration** page

This process can take several minutes, please be patient
15. Once the site has loaded you should see the same configuration settings that were set on the first TDS instance.
16. Repeat steps 9 through 14 for each additional replicated instance of TDS (each additional application server behind the load balancer).

**Note:** After making any global application configuration changes (things like [Authentication](#), [Roles](#), [Role Privileges](#), [Security Settings](#), [File Path Settings](#), etc) you may need to restart each of the TDS applications. You can perform this restart by clicking [Restart application](#) action in the [Administration Console](#) under [Actions](#).

## IIS Authentication

When running the installation wizard, it is recommended to check the [Use Integrated Windows Authentication \(Active Directory\)](#) option, if you plan to use Windows Authentication within the application. If you decide to change to or from Windows Authentication (or for some reason the installer could not automatically do this for you) then you will need to manually enable or disable Anonymous Authentication and enable or disable Windows Authentication from within IIS (depending on whether you are turning it on or off).

1. Open Internet Information Services (IIS) Manager.
2. Click on the application node.
3. Double click **Authentication** under the IIS section.
4. To turn **on** Windows Authentication:
  - Set Anonymous Authentication to *Disabled*
  - Set Windows Authentication to *Enabled*
5. To turn **off** Windows Authentication:
  - Set Anonymous Authentication to *Enabled*
  - Set Windows Authentication to *Disabled*
6. Reload the application. You should be prompted by the browser to enter your Windows credentials (depending on your browser, you may automatically be authenticated).

**Note:** By enabling Windows Authentication, within IIS, you are requiring authentication to happen at the IIS level (outside of the actual application). To get the application to recognize the IIS authentication mechanism, and use your Windows account, you must configure the appropriate authentication mechanism from within the application. See the [Authentication](#) section for details on changing this setting.

## IIS Permissions

In order for the application to be able to make configuration changes from the user interface (UI), the built in IIS account/user (typically IUSR or IIS\_USRS) must have full permissions on the root directory of the application. If this is not present, then configuration changes made from the client side application will not be successfully persisted. **This permission setting will automatically be configured by the installation wizard.** However, if for some reason this needs to be done manually, below are the following steps to set these permissions:

1. Open Internet Information Services (IIS) Manager.
2. Right click on the **application node**.
3. Click **Edit Permissions**.
4. Click the **Security** tab.
5. Make sure the user account/group that IIS is running under has Full Control.
  - This user is typically IUSR or IIS\_USRS
  - You can find more information about IIS built-in user and group accounts [here](#)

## IIS Application Pool Recycling

In order to run long server processes within the application IIS must be configured to not recycle the application pool automatically. Additionally this will keep the application from idling and will increase the response time of the first request to the application after no

use for an extended amount of time. **These related setting will automatically be configured in IIS by the installation wizard.** If you are manually deploying the application or if the installer was unable to make this change, they can be made with the following steps:

1. Open **Internet Information Services (IIS) Manager**.
2. Click on the **Application Pools** node.
3. Right click on the app pool that TDS is running under (the default is "TDSAppPool").
4. Click **Advanced Settings**.
5. Under the **Process Model** section, change the **Idle Time-out (minutes)** setting to "0."
6. Under the **Recycling** section, change **Regular Time Interval (minutes)** setting to "0."

## Setting Up Configuration Store Permission

When using an enterprise database (such as SQL Server or Oracle) as a configuration store, the database should be a new empty database and the connection to this database should use a database user that is the schema owner of its own schema (a user with read/write to its own schema only). When configuring this "Configuration Store" connection string, it is important to use a database user that does not have access to anything outside of this "TDS" configuration database - in order to mitigate any risk of inadvertently modifying or accessing other data.

### Steps for SQL

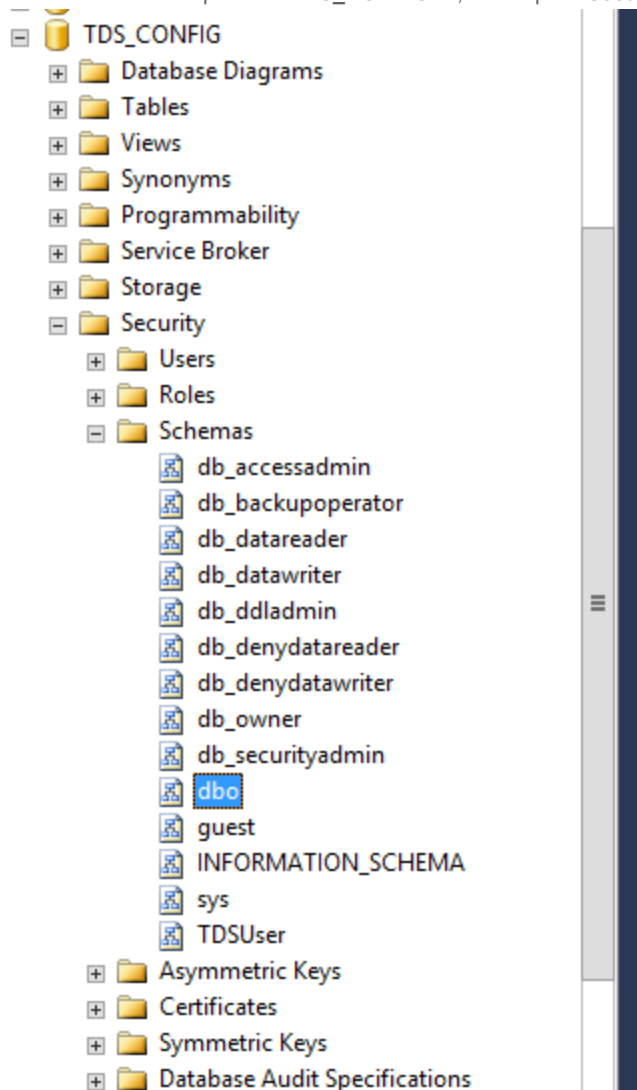
#### Grant DBO Permissions

The application, by default, uses the dbo schema and therefore needs to be granted dbo permissions.

This can be done with the following steps:

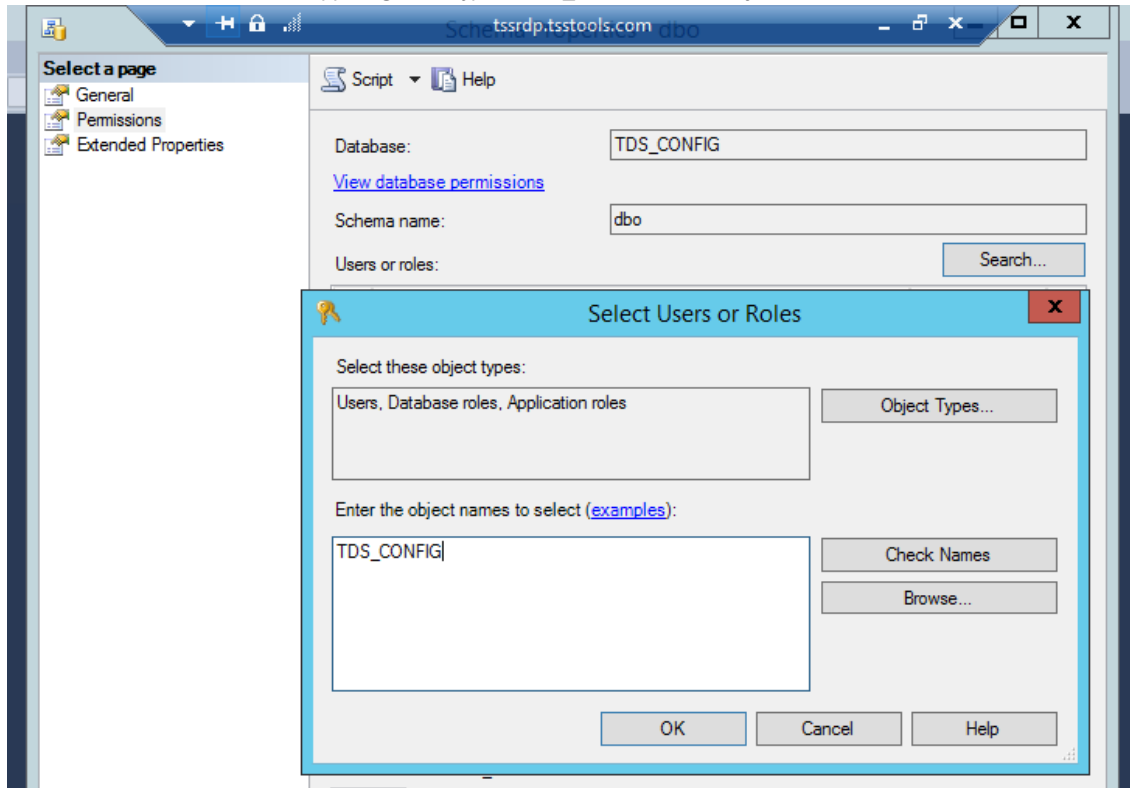
**Note:** The following steps will use the database/user name of TDS\_CONFIG, which could vary depending on your environment:

1. Log in as administrator and expand the **TDS\_CONFIG** db, then expand **Security**, and then **Schemas**.



2. Right click on **dbo** and select **Properties**, and click the **Permissions** tab.

3. Click the **Search** button towards upper right and type in **TDS\_CONFIG** as the object name and click **OK**.



4. The TDS\_CONFIG now shows up in your list of Users or Roles.

**Select a page**

- General
- Permissions**
- Extended Properties


Script Help

Database: TDS\_CONFIG

[View database permissions](#)

Schema name: dbo

Users or roles:

Name	Type
 TDS_CONFIG	User

Permissions for TDS\_CONFIG:

- Towards the bottom of the screen will be the permissions for the TDS\_CONFIG user to access the dbo schema.

Permissions for TDS\_CONFIG:

Explicit Effective

Permission	Grantor	Grant	With Grant	Deny
Alter		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Control		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Control	dbo	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Create sequence		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Execute		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Insert		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
References		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Take ownership		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Update		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
View change tracking		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
View definition		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK Cancel

**Note:** The Control option includes all CRUD operations.

- Point TDS's configuration store setting to point to this new database using the TDS\_CONFIG DB credentials.

### Other Notes

CRUD dbo permissions are required for the TDS application to work with a SQL Server instance as the configuration store.

### Steps for Oracle

COMING SOON



## Application Architecture

The "Transportation Data Server (TDS)" application is the "wrapper", server-side, application that hosts a number of supporting web services and all of the client-side web applications (which consume those web services) - for example: Road Analyzer (RA), Segment Analyzer (SA), Validation Assistant (VA), HPMS Assistant (HA), Road Video Viewer (RVV), etc.

TDS is typically hosted in a standard enterprise-level IT environment, with supporting LRS transactional components - such as an LRS geodatabase and GIS map services. TDS is compatible with most LRS models and is often used in conjunction with Esri's Roads & Highways product, however Roads & Highways is not required. There are many different infrastructure configurations and environments that TDS can be ran within. Below is a listing of the most common configurations:

### **Systems Architecture - no load balancing**

This option has no load-balancer in either the GIS or web tier. This is a fairly common architecture for Roads and Highways environments. It is not necessarily a big risk in that the most performance intensive component in this stack is ArcGIS Server (which could be setup to use clustering, instead of a load balancer). Most of the "web tier" components are simple HTML/JS/CSS applications that do not drastically benefit from a load balancer (unless you have hundreds of thousands of users).

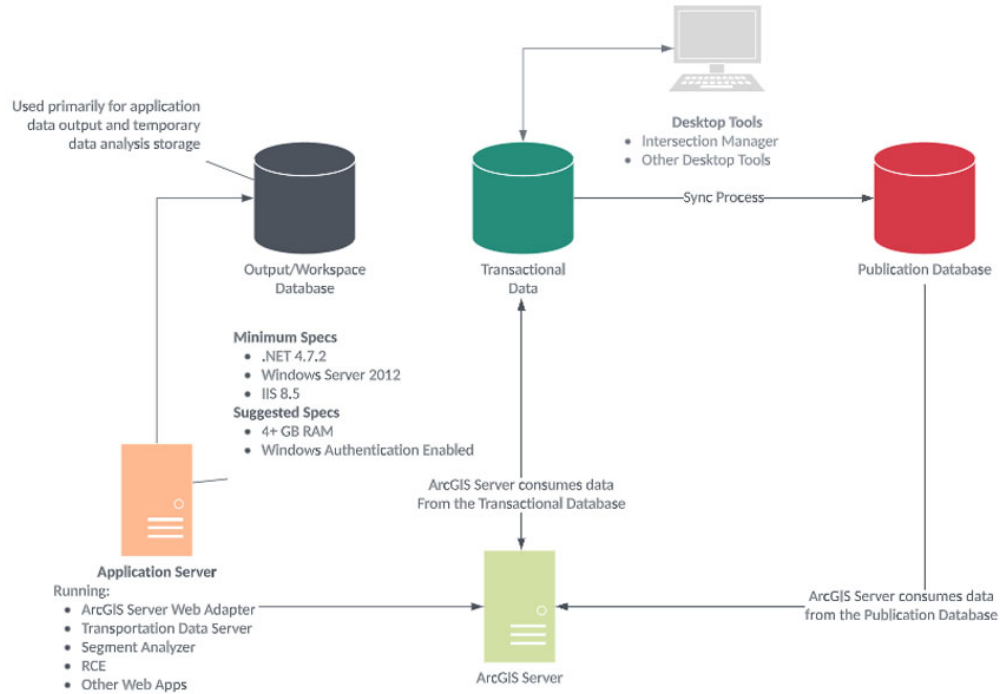
#### **Pros:**

- Simple to configure and understand.
- The GIS tier (ArcGIS Server) can still scale using clustering.
- Uses standard configurations in both web and GIS tiers.

#### **Cons**

- The web-tier is not easily scalable.
- The GIS-tier is not easily scalable, from a load balancer standpoint, but could scale via clustering.

### Standard System Architecture (non-load balanced)



**Application Server Notes**

- Apps can be split over multiple servers
- App server can be replicated (sit behind a load balancer)
- It is suggested that Web Adapter is installed on the Application Server if you are using Windows Authentication due to cross-machine authentication restrictions

**ArcGIS Server Notes**

Can be setup using clusters or with a load balancer

### Systems Architecture - load balanced GIS tier and non-load balanced web tier

This configuration provides load balancing for the most common "stress-point" - ArcGIS Server. This configuration provides the most benefit with the least amount of work (configuration), if a load balancer is already planned to be used.

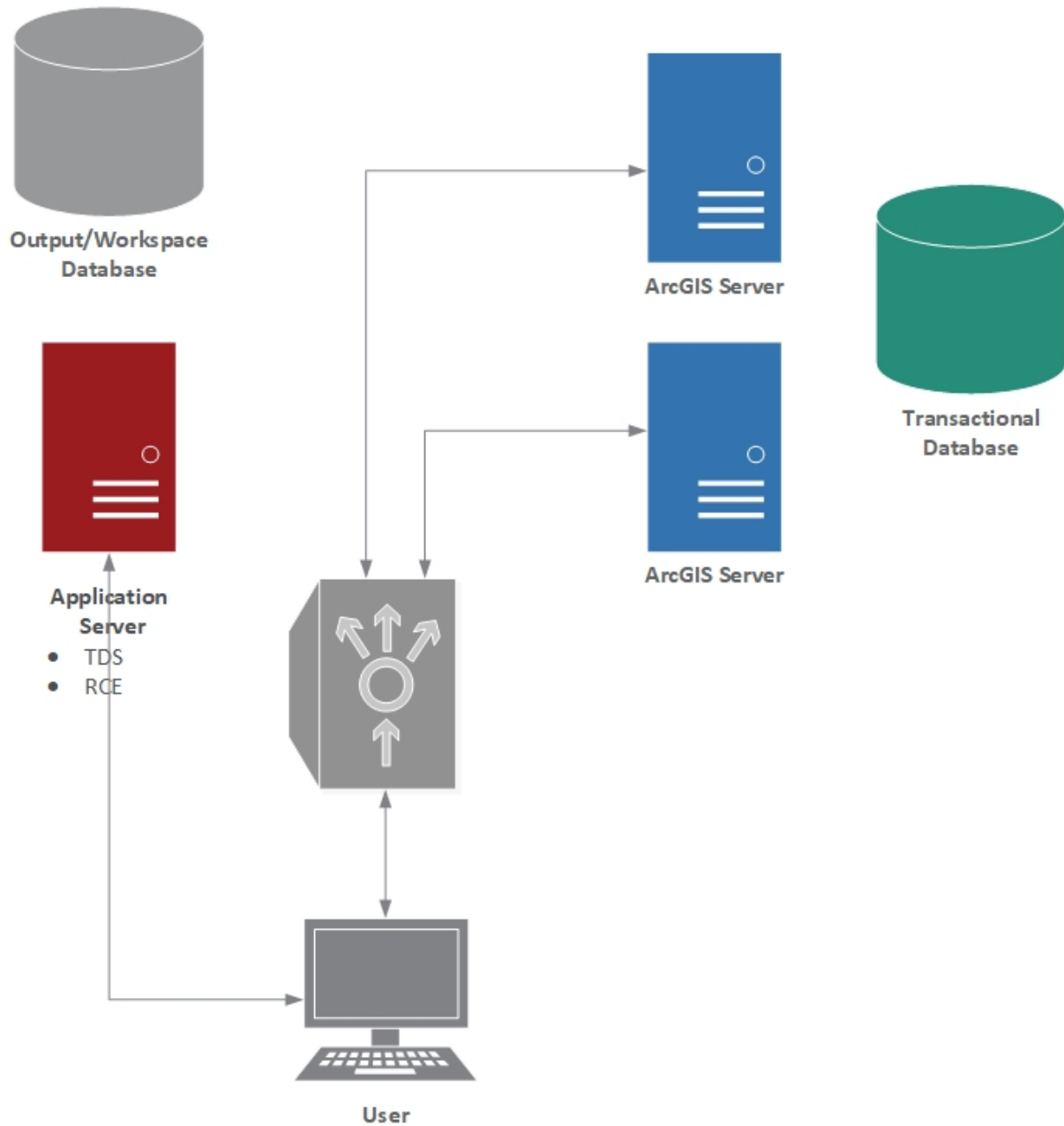
**Pros:**

- Simple web-tier configuration.
- Easily scalable GIS-tier.
- Uses standard configurations in both web and GIS tiers.

**Cons**

- More complex configuration for GIS-tier.
- Web-tier is not easily scalable (not necessarily a big deal unless you plan on having a very large user group).

## Load balanced GIS-tier and non-load balanced web-tier



### Systems Architecture - load balanced GIS tier and load balanced web tier

This option provides the most "scalable" and fail-safe solution, but also requires the most configuration and maintenance.

Pros:

Completely scalable.

Ability to do server updates without affecting users.

**Cons**

More difficult configuration.

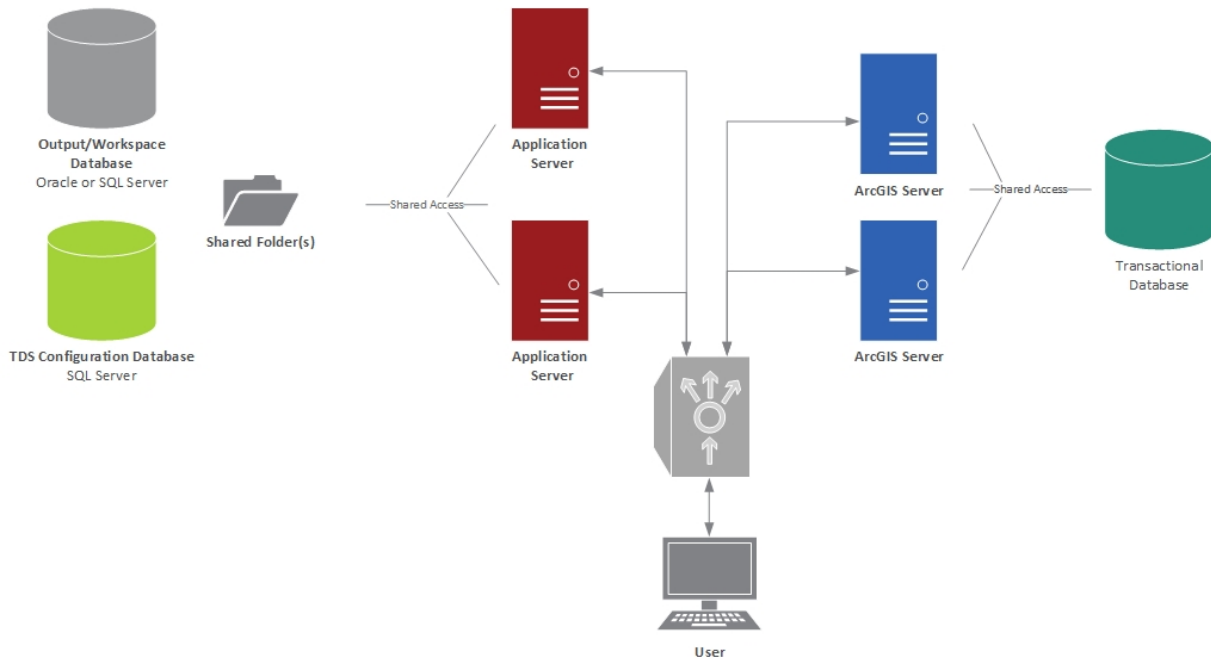
More difficult troubleshooting and diagnostics (both web and GIS tiers).

Increased maintenance (more servers to run installations, backups, Event Editor configuration sync, etc).

Must use a SQL Server database as a configuration database for TDS (which each TDS instance points to).

Must have shared network folders between TDS instances (if using print or reporting capability within RA).

**Fully load-balanced (GIS-tier and web-tier)**

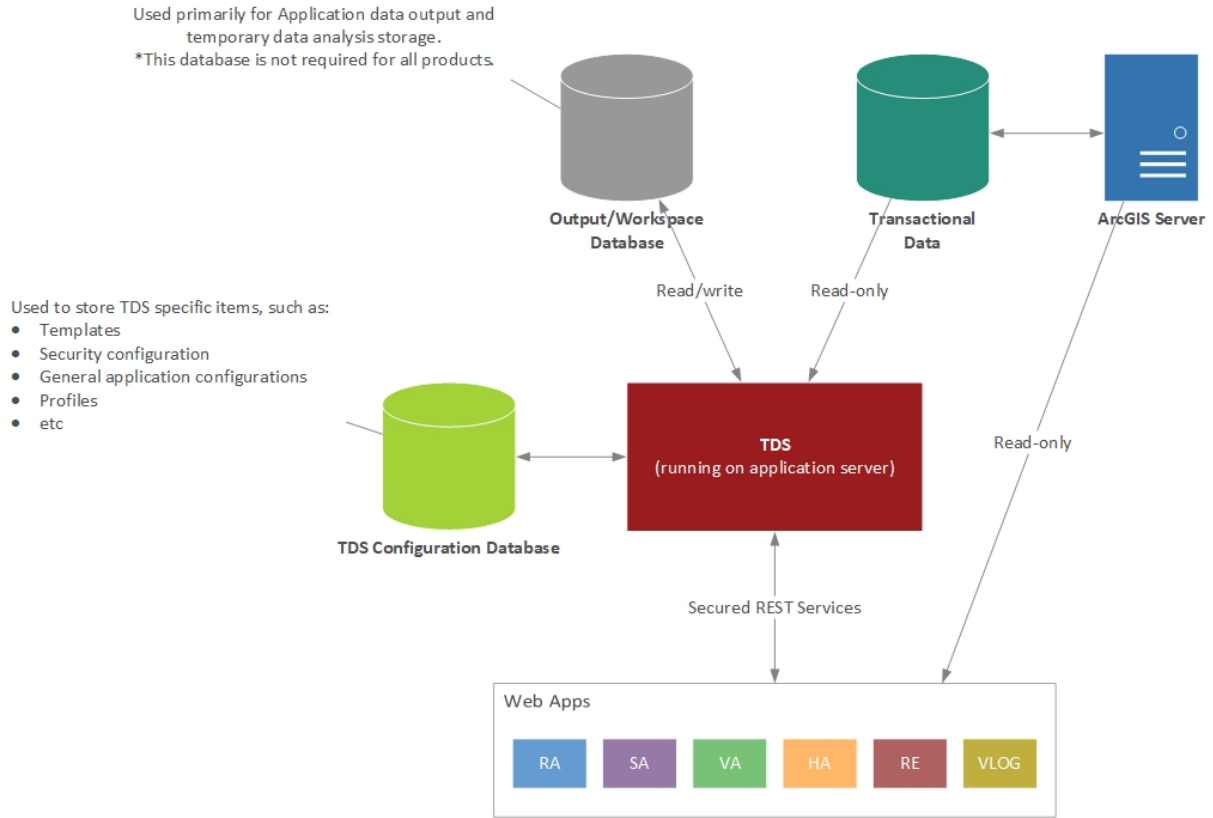


**Heads Up!** When placing TDS (the web-tier) behind a load balancer there are several configuration options that must be considered in order to keep the multiple instances in sync. See the "[Advanced Configurations](#)" page for details on configuring the application behind a load balancer.

**Data Flow and Connections**

Data is accessed and consumed in various ways, depending on the particular application running. The two most typical data connection types will read data from a "Map Service" (typically ArcGIS for Server) or by directly connecting to the database from TDS (through a set of secured REST services). TDS can be configured to point to many different data sources, both spatial (geodatabases) and non-spatial (standard RDBMS, no geodatabase).

**Heads Up!** It is highly recommended that the data source connection to your "Transactional Database" be read-only. You should configure the connection to use an account that has "read-only" access to the data. This will mitigate the risk of accidental edits or loss of important data.



## Application Security

### Application Security

All of Rizing Geospatial's products provide safeguards to help prevent SQL injection attacks by making use of parameterized SQL queries within the .NET framework. While there are safeguards in place to prevent SQL injection attacks, within Rizing Geospatial's products, the recommended data access architecture is intended to provide the greatest defense mechanism. Securing data access via connection account privileges and application user/role/privilege assignment is critical to mitigating the risk of unintended server and database access. This is particularly important due to the fact that some functionality in Rizing Geospatial's products do require some level of dynamic SQL input. It is critical that only authenticated and trusted users have access to this functionality. All database connections to the transactional data should be configured to use a read-only connection. See "Data Flow and Connections" on page 180 for more details.

**Note:** ArcGIS Server does include a security option to help prevent SQL injection attacks through the use of "standardized queries" functionality, which prevent the use of database-specific functions and syntax from being used within a supplied map service query "where clause". This security measure is turned on by default in ArcGIS Server. More information can be found here: [ArcGIS Server: About standardized queries](#)

The application's security policy can be configured to use a number of different authentication and authorization mechanisms. See the [Authentication](#) topic for details on the supported security settings and how to configure them, as well as the other [Security](#) section topics.

### Secured Services

Application security happens at the web service level. This means that authorization and authentication must be satisfied (based on the configuration) for any service/endpoint to be consumed. The application uses a token-based authentication system. This means that the user will first need to provide a set of credentials to verify who they are. The application will take those credentials and generate a token with an expiration date that can be passed by any subsequent requests to services for authentication. The application will cache the token that it receives after "logging in" and will pass that token as "Authorization" header in the HTTP request for every request made to the application services.

### Data Security

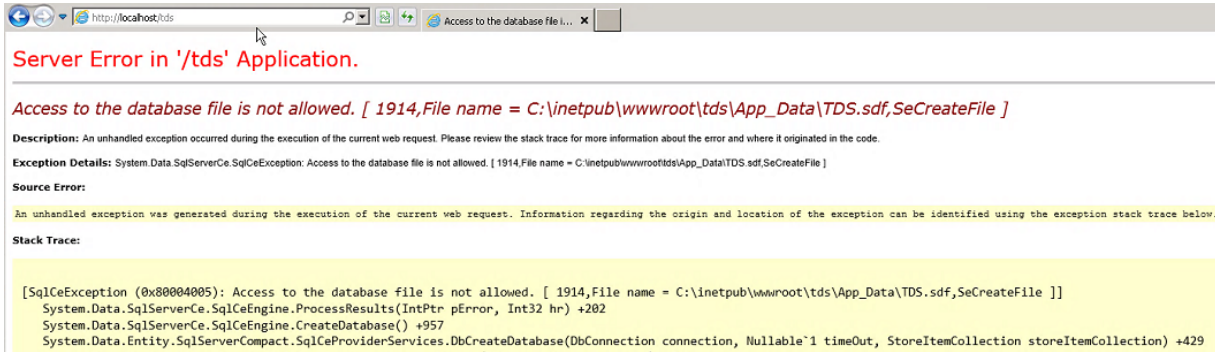
In order to properly secure the data transactions between the web application and the services, HTTPS (SSL) must be configured and used on the application server. If HTTPS is not used then the HTTP traffic could potentially be "sniffed" by anyone else on the network.

## Installation Errors

The following is a list of common application errors you may see when a component is not configured completely or correctly:

### Access to the database file is not allowed

If the TDS application is configured to use a local configuration file (SQL Compact Edition), and the correct permissions have not been set, you will see the following error message when you try to load the application:












This error can be resolved by setting “write” (full) access to the application (tds) directory for the user/group that IIS is running as (typically “IUSR” and “IIS\_IUSRS”). See [Advanced Configuration](#) for more information.

### Retrieving LRS Metadata / An Error Occurred

Typically when the “Retrieving LRS metadata” entry in the app log shows as an error, there is a problem with the configured map service. If the failed HTTP request provides a more detailed message, the application log will display it, otherwise it will simply log “An error occurred”. The following steps can be taken to diagnose this error:

1. Click the **Test URL** button and verify that the map service exists and you can access it.
2. If you are using `https`, verify that you have the proper certificate for the server that the map service is hosted on.

3. If you have the **Map Service Has LRS Capabilities** option checked, verify that the LRSServer extension is enabled on the map service and that there is a network layer and event layers in the map service.

Application Log		
 <b>Initializing application</b>	444 ms	✘
 Set approved roles for current user - total of 130	0 ms	✔
 Retrieving application configuration	251 ms	✔
 Set map service calls to use JSONP	0 ms	✔
 Configured default roles (guest roles) - total of 60	0 ms	✔
 <b>Retrieving LRS metadata</b>	172 ms	✘
 Retrieving template by ID '1'	72 ms	✔
 <b>An error occurred</b>	0 ms	✘
 <b>An error occurred</b>	0 ms	✘

#### Unauthorized: Access is denied due to invalid credentials

The "Unauthorized: Access is denied due to invalid credentials" error message is typically associated with Integrated Windows Authentication, within IIS, being incorrectly configured or IIS configuration being out of sync with the application's [security configuration](#).

### Server Error

**401 - Unauthorized: Access is denied due to invalid credentials.**

**You do not have permission to view this directory or page using the credentials that you supplied.**

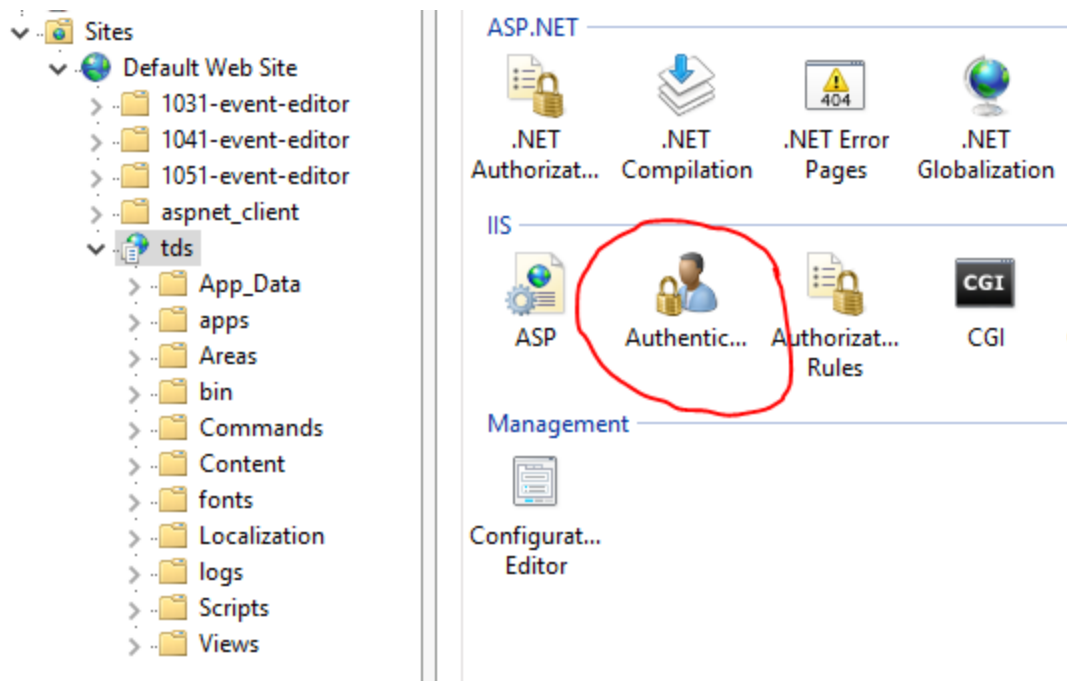
To resolve the issue the following procedures can be followed:

**If the desire is to use Windows Authentication and the application has already been configured with external roles (AD Groups):**

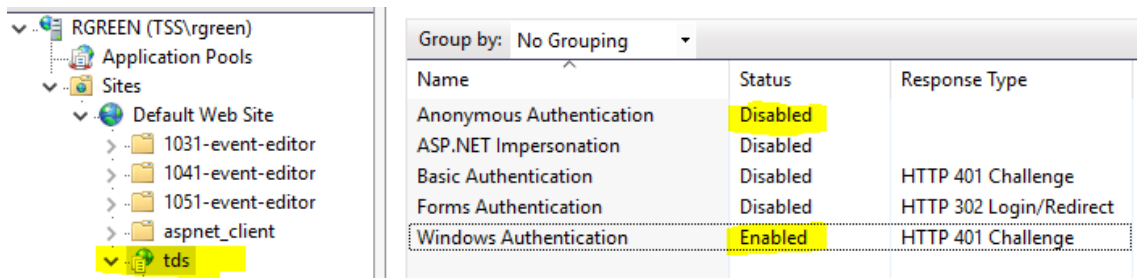
1. On the application server that TDS is installed, open **IIS Manager**.
2. Navigate to the "tds" application node (click the "tds" node).



3. Double-click the Authentication icon.



4. Enable Windows Authentication and disable all other types



5. Test the application by opening it in a browser. If it doesn't work, continue...

6. Navigate to the TDS application installation directory

This can be achieved by right-clicking the "tds" node in IIS and clicking **Explore**

7. Edit the **Web.config** in a text editor

- In the system.web tag, ensure that the "authorization" and "authentication" appear as follows:

```

15 <system.web>
16   <authorization>
17     <deny users="?" />
18   </authorization>
19   <authentication mode="Windows" />
20   <compilation targetFramework="4.5" />
21   <httpRuntime targetFramework="4.5" maxRequestLength="1048576" />
22   <customErrors defaultRedirect="~/apps/oops.html" mode="RemoteOnly">
23     <error statusCode="404" redirect="~/apps/oops.html?errorMessage=Sor
24     <error statusCode="401" redirect="~/apps/oops.html?errorMessage=Sor
25   </customErrors>
26 </system.web>
  
```

Copy/Paste:

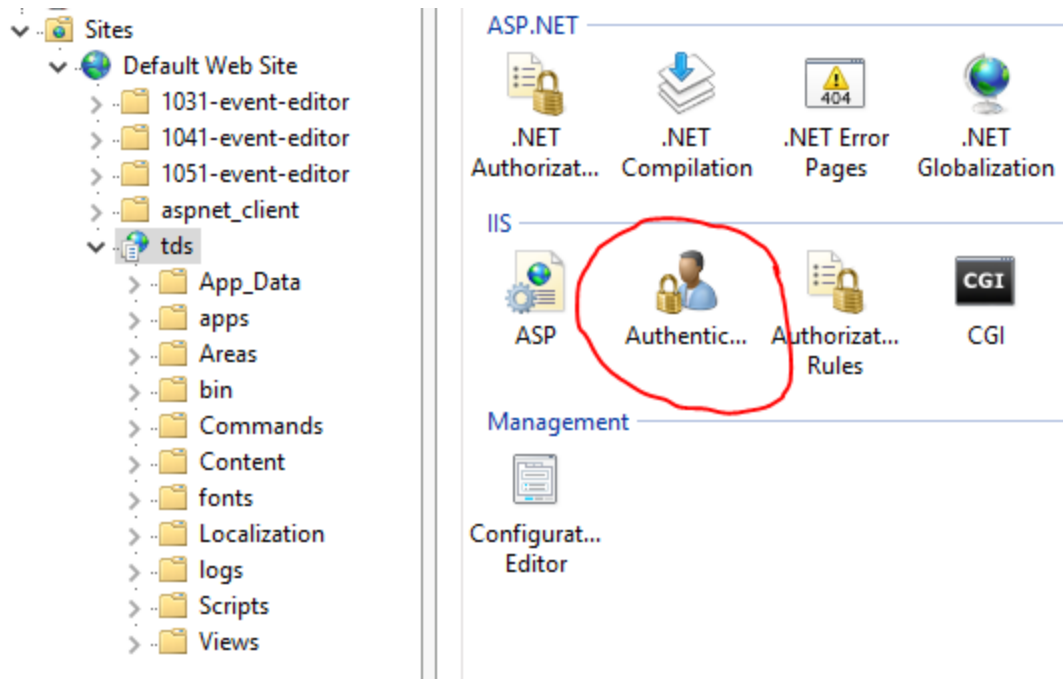
```

<authorization>
  <deny users="?" />
</authorization>
<authentication mode="Windows" />
  
```

- Save the edited "Web.Config" file.
- Test application by opening it in a browser.
- If the application doesn't work, move onto the "Manual reset of application authentication" steps.

**Manual reset of application authentication:**

- On the application server that TDS is installed, open IIS Manager.
- Navigate to the "tds" application node (click the "tds" node).
- Double-click "Authentication" icon.



4. Enable "Anonymous Authentication" and Disable all other types.

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

5. Navigate to the TDS application installation directory.

This can be achieved by right-clicking the "tds" node in IIS and clicking **Explore**

6. Edit the "Web.config" in a text editor.

7. In the system.web tag, remove any existing "authorization" and "authentication" tags and add the following "authentication" tag:

```

15 <system.web>
16 <authentication mode="None" />
17 <compilation targetFramework="4.5" />
18 <httpRuntime targetFramework="4.5" maxRequestLength="1048576" />
19 <customErrors defaultRedirect="~/apps/oops.html" mode="RemoteOnly"
20 <error statusCode="404" redirect="~/apps/oops.html?errorMessage=
21 <error statusCode="401" redirect="~/apps/oops.html?errorMessage=
22 </customErrors>
23 </system.web>
  
```

Copy/Paste:

```

<authentication mode="None" />
>
  
```

8. Save the "Web.Config" file.

9. Open up the **TDS Configuration Store** database and open the **SecurityConfigs** table (there should only be 1 record).

10. Edit the **SecurityProfileId** columns for the one record by setting the value to **none**.

SystemAdminUserName	SecurityProfileId	CorsOrigins	CorsHeaders
	none	*	*

11. Test the application by opening it in a browser. You should now have full access to the site and it should be configured with "No Security."

12. Go through the **Authentication Configuration** steps to property configure the desired TDS security mechanism.

## Installing TDS to a new (non-default) Website in IIS

The steps below cover moving TDS from a standard "Default Web Site" IIS installation to a new non-default website in IIS.

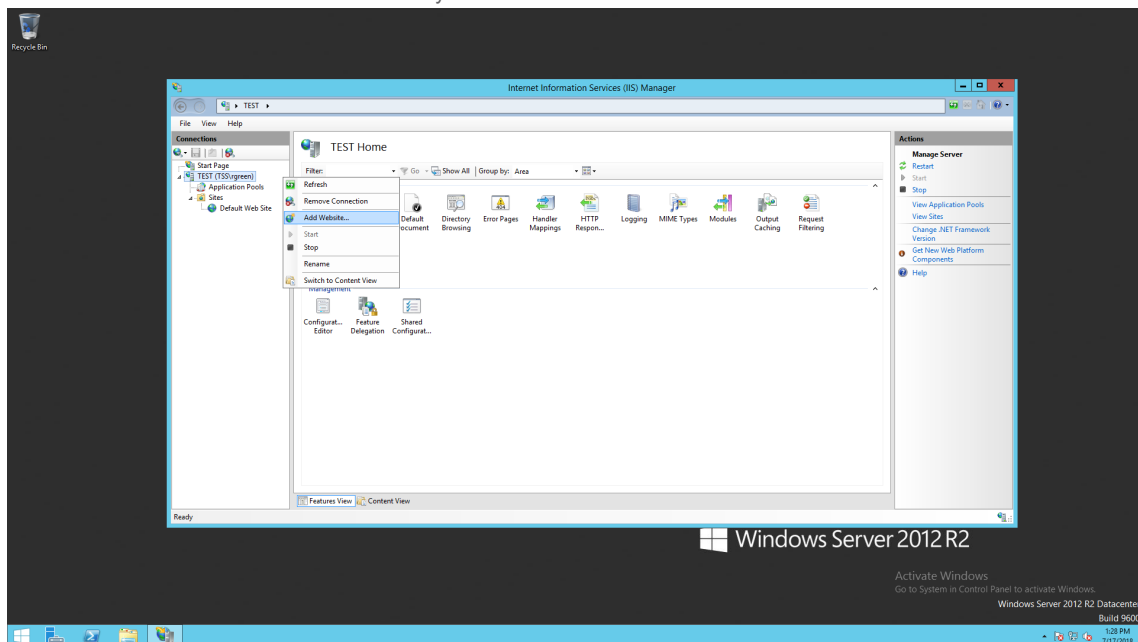
**Before migrating TDS from one website to another it is recommended to:**

1. Export the current TDS configuration to a seed file ([see migrate TDS configuration store docs](#))
2. Make a backup of the current application and data
3. Completely uninstall all Rizing Geospatial products from the respective web server ([see uninstalling the application docs](#))

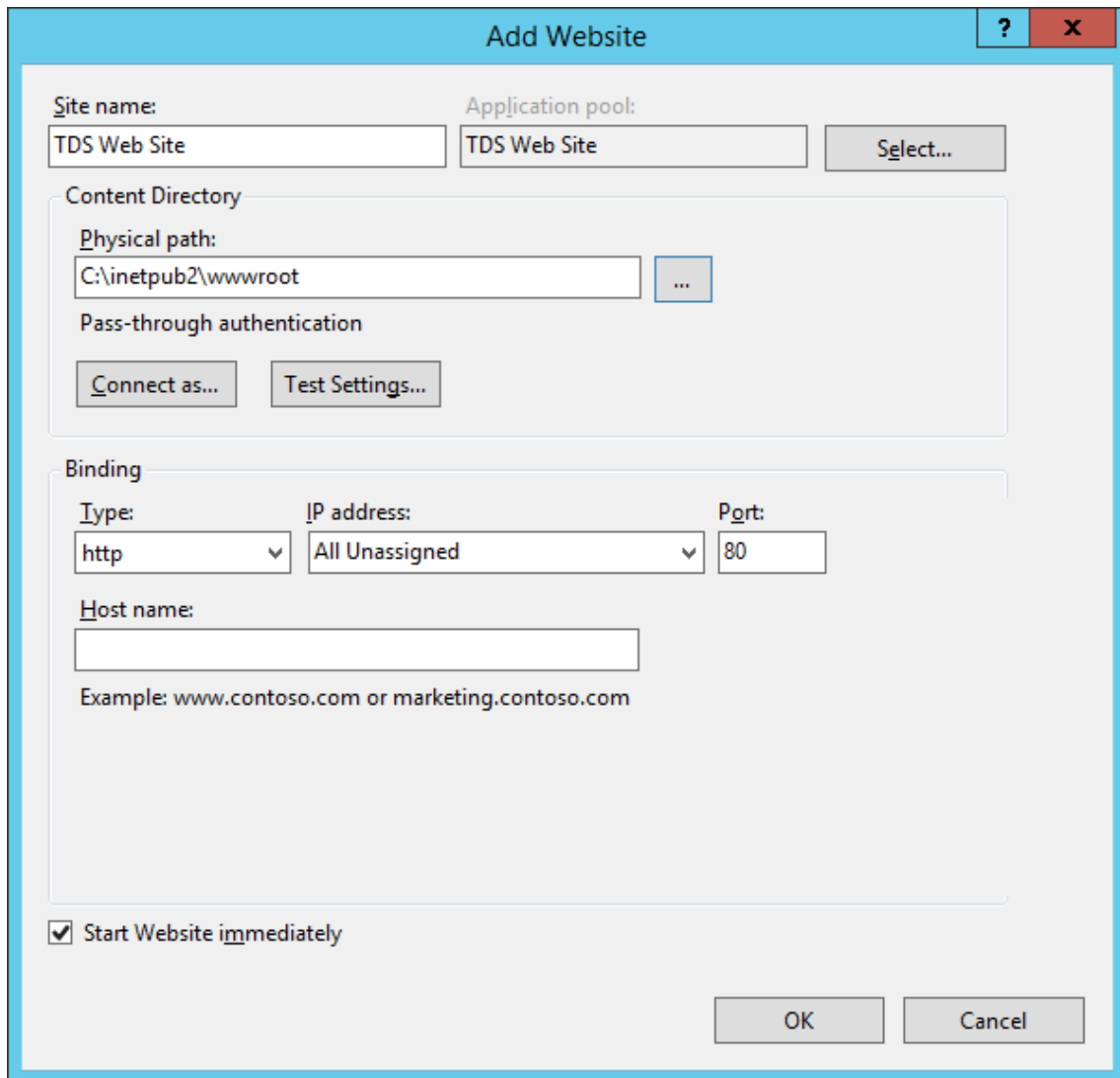
**Steps:**

### 1) Create new website in IIS

1. Create a new website in IIS if it does not already exist.



2. Fill in site details.



**Add Website** ? X

**S**ite name: TDS Web Site      **A**pplication pool: TDS Web Site      Select...

**C**ontent Directory

**P**hysical path: C:\inetpub2\wwwroot      ...

**P**ass-through authentication

Connect as...      Test Settings...

**B**inding

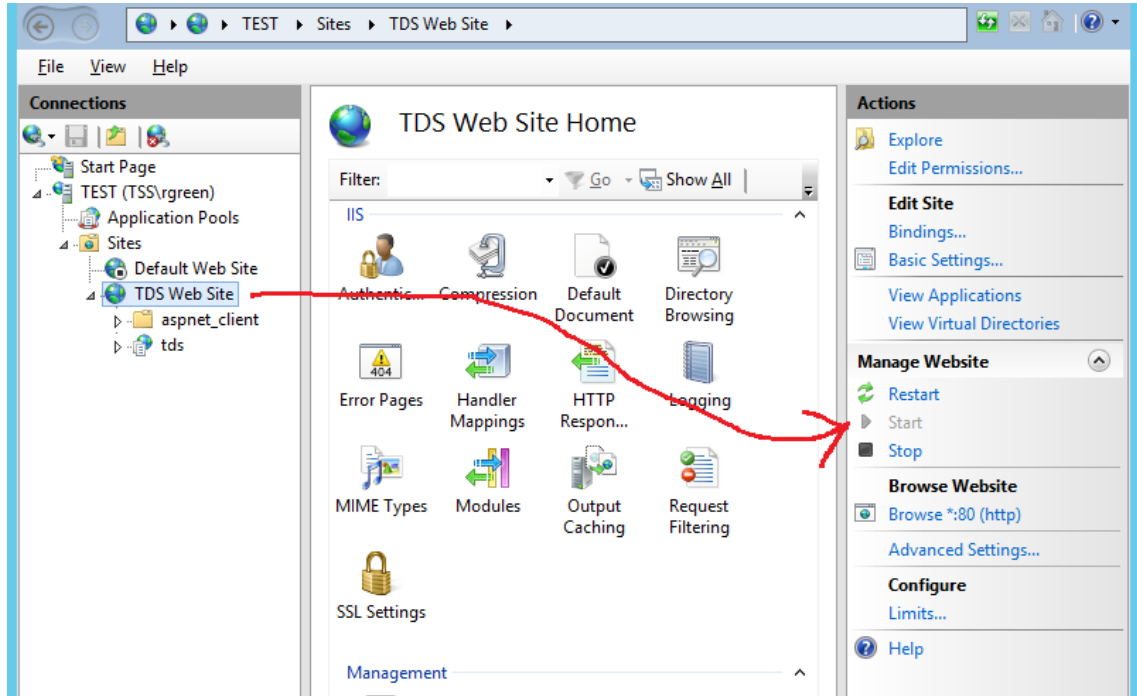
Type:	IP address:	Port:
http	All Unassigned	80

**H**ost name:  
Example: www.contoso.com or marketing.contoso.com

Start Website **i**mmediately

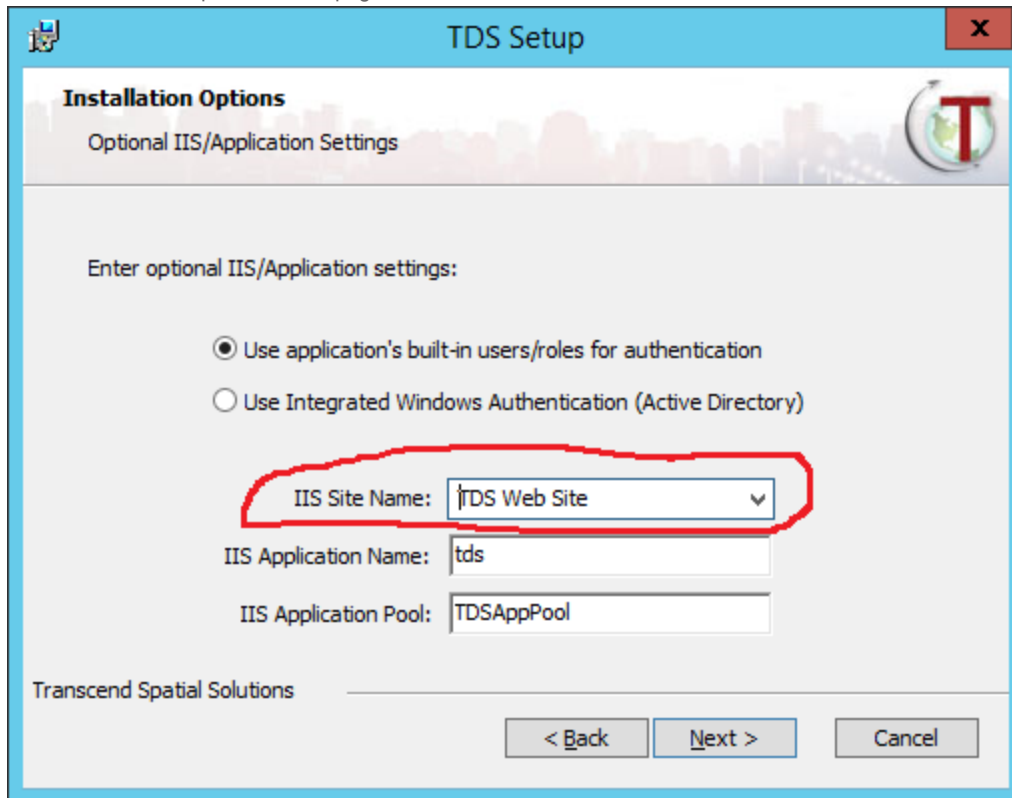
OK      Cancel

3. Ensure that the site is running.



## 2) Run the TDS Installer

1. Run the TDS Installer (for the latest TDS release).
2. On the "Installation Options" wizard page, select the desired IIS Site Name.



3. Run through the remainder of the installation wizard steps and complete the installation process.
4. Once the installation is complete, the application should be installed within the selected IIS Site.

### **3) Verify the applications were installed**

1. View the applications listed under the selected "IIS Site Name" to verify.
2. Install any remaining Rizing Geospatial products on the server (example: Road Analyzer, Segment Analyzer, etc).

### **4) Import the exported seed file**

Once the new website is installed correctly, import the exported seed file (from the previous website) to the new application which will restore TDS back to the previous site's application configuration.

## Manual Installation

The steps below are the typical, manual, deployment/installation steps followed to host the web application in a Windows environment (on IIS).

**Note:** If you are updating the application, see the **Updating Application** section below.

### 1) Verify Installation Requirements

#### Installation Requirements

### 2) Extract Deployment Package

The install package will contain a directory named "tds", this is the primary deployment folder that will be used in the following steps.

### 3) Deploy Application to IIS

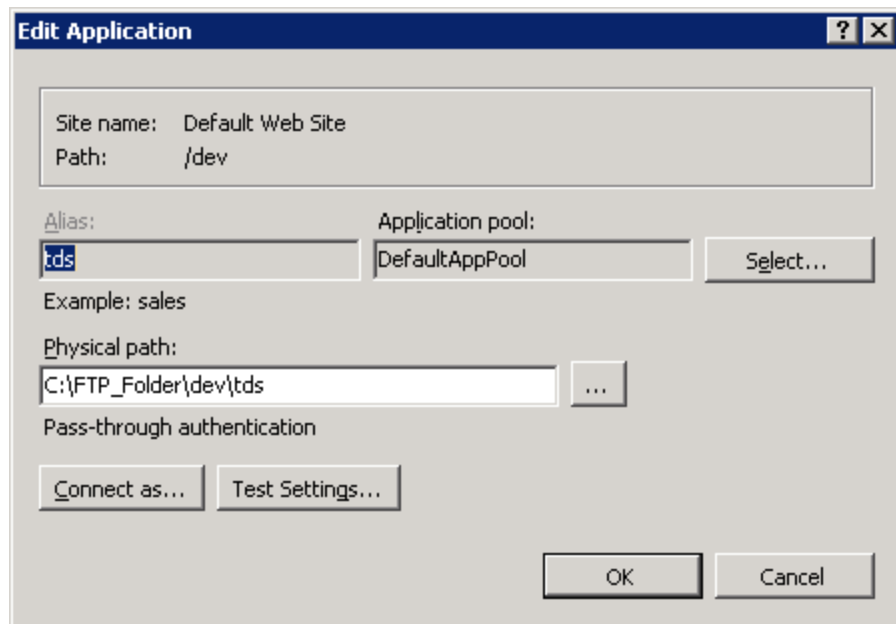
#### Create "tds" Application

Create a new application in IIS Manager called "tds" and point the "Physical path" to the "tds" directory that you copied/created in the previous step.

**Note:** If you copied the tds directory directly to "C:\inetpub\wwwroot" then you only need to right click on the "tds" folder in IIS Manager and click **Convert to Application**.

Use the "DefaultAppPool" if the default application pool is .NET 4.5 - if not you will need to create an app pool for .NET 4.5 and set that as the app pool for this application. After installing .NET 4.5 the default app pool should automatically be configured to use .NET 4.5.





**Edit Application** [?] [X]

Site name: Default Web Site  
Path: /dev

Alias:  Application pool:

Example: sales

Physical path:

Pass-through authentication

### Configure and Test Application

After the application is deployed, follow the remainder of the installation steps in the [Getting Started](#) section.

### Updating Application

If the application has already been deployed and you are trying to re-deploy a newer version of the application, manually, the following steps should be taken:

1. Extract deployment package.
2. Make a backup of the current application (tds directory).
3. Overwrite all of the content currently deployed (in IIS) with the contents of the "tds" directory in the deployment package.
4. Update the web.config to match your previous deployment configuration/settings.
5. Run the application and test.

## Options and Silent Installs

The installer can take in a number of options via the command line, in order to set default behavior and configuration – during the installation process.

### Command Line Options

The following is a list of arguments that can be passed to the installer via command line:

1. `/L*V <log file location>`
  - a. Will tell the installer where to log its progress.
  - b. Note, the log path and log file must already exist.
2. `APPDIR=<install directory>`
  - a. Will tell the installer where to install the application on the target machine.
3. `ENABLE_WIN_AUTH=1 or 0`
  - a. Will tell the installer to enable windows authentication and disable anonymous authentication, or not.
  - b. Defaults to 0.
4. `LAUNCH_BROWSER=1 or 0`
  - a. Will tell the installer to launch a browser, to the application, or not once the installation is complete.
  - b. Defaults to 1.
5. `APP_NAME=tds`
  - a. Will tell the installer what to “name” the application within IIS.
  - b. Defaults to “tds”.
6. `APP_POOL_NAME=TDSAppPool`
  - a. Will tell the installer what to name the “Application Pool” for the installed application.
  - b. Defaults to “TDSAppPool”.
7. `/qn, /quiet`
  - a. Will tell the installer to install “silently”.
8. Example:
  - a. `msiexec /i <msi location> /L*V <log file location> APP_NAME=<app name> APP_POOL_NAME =<app pool name> ENABLE_WIN_AUTH=<1 or 0>`
9. Working example:
  - a. `msiexec /i "C:\deployment-package\tds.msi" /L*V "C:\ deployment-package\install-log.txt" APP_NAME=tds APP_POOL_NAME =MyAppPool ENABLE_WIN_AUTH=1 APPDIR="C:\Program Files (x86)\TDS`

### Silent Installs

The installer can be run “silently”, meaning it will not ask for any input from the user. It will use all default values, unless a specific option/argument was passed in via the command line.

`/qn, /quiet`

Will tell the installer to install “silently”

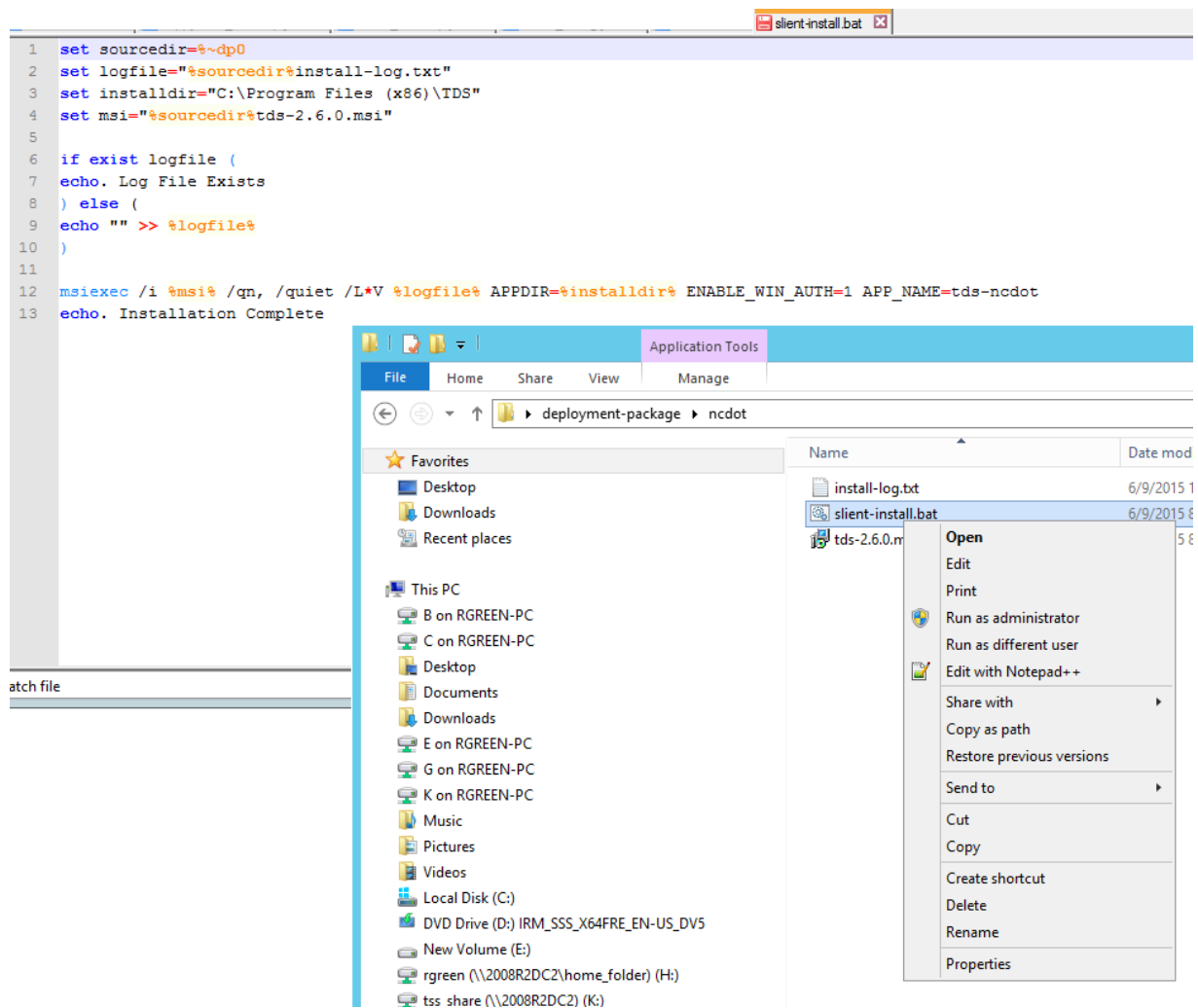
Example:

`msiexec /i <msi location> /qn, /quiet /L*V <log file location> APPDIR=<install directory> ENABLE_WIN_AUTH=1`

Working example:

```
msiexec /i "C:\deployment-package\tds.msi" /qn, /quiet /L*V "C:\deployment-package\install-log.txt" APPDIR-
R="C:\Program Files (x86)\TDS
```

The installation package will contain pre-filled batch script, "silent-install.bat", which you could add to, or edit, the arguments to pass to the "msi" file. Note, if you run the installer using the "silent-install.bat" file you must run it as an administrator.



## Scalability and Performance

### Application Performance

The application's performance is very dependent on external factors, such as ArcGIS Server configuration, hardware, software, networking, and bandwidth. The application stack is made up of a set of RESTful services and a web application. The application services do not typically query data themselves – but instead the web application will leverage an ArcGIS Server map service to query data. See [Application Architecture](#) for more details.

Since neither the web application (simple HTML site) nor the .NET MVC application (REST services) query data themselves, the biggest point of potential performance issues lies within the ArcGIS Server map service. ArcGIS Server performance is essential for the web application to perform adequately. See [ArcGIS Server performance documentation](#) for details.

### Scalability

In order to accommodate a very large number of concurrent users, the application server (REST services and web app) can be replicated/scaled to be placed in a load-balanced environment. This "replicating" of services will allow for spreading the load over multiple resources. There are however a number of configuration considerations that should be taken when using "replicating" of services. You can find these configuration considerations in [Configuration for Load Balanced Environments](#) located in the [Configuring the Application](#) section.

### Example Metrics

The following is a list of metrics gathered, and the hardware and software they were performed on.

#### Configuration 1

##### Description:

Application Server (Server #1)

Windows Server 2012

64-bit

Intel(R) Xeon(R) CPU E5-2670 v2 @ 2.50GHz, 2499 Mhz, 2 Core(s), 4 Logical Processor(s)

30.5 GB Physical Memory

Installed Software: ArcGIS Server, ArcGIS Desktop, SQL Server 2012

Configuration Database (SQL Compact Edition)

ArcGIS Server (Server #2)

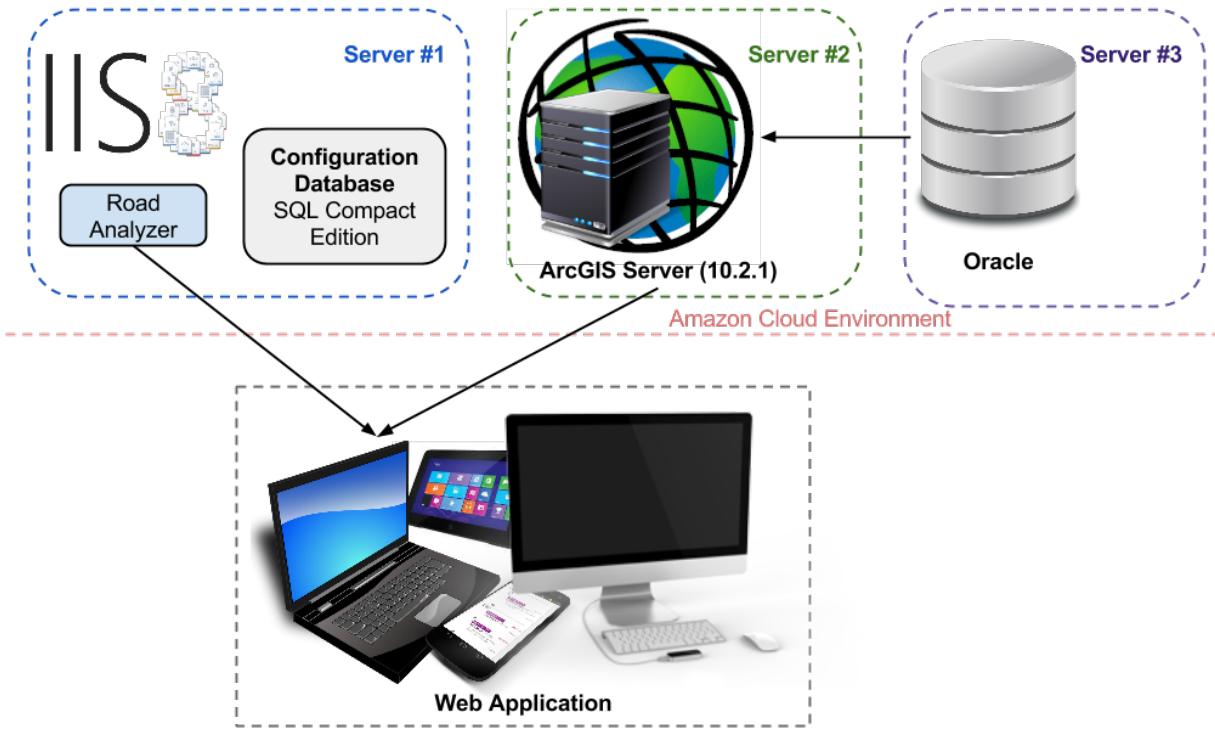
10.2.1

Default configuration

Database (Server #3)

Oracle

##### Infrastructure:

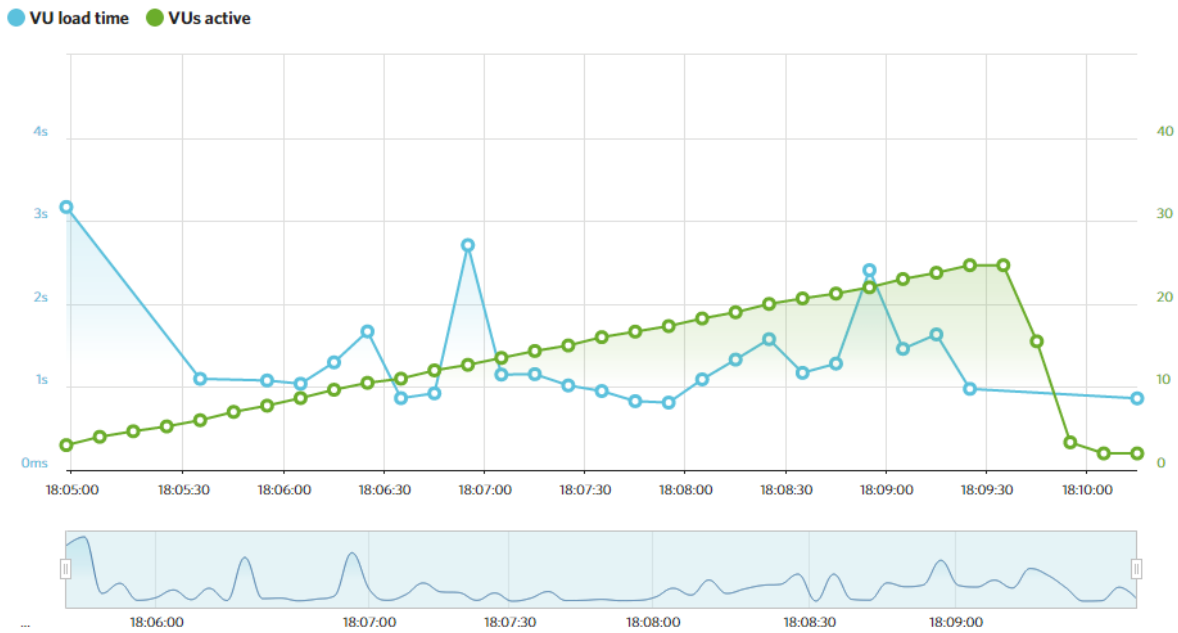


Performance Metrics:

Total Miles	Layers Queried	Features Queried	Symbology Complexity (1-10)	Total Query & Render Time (seconds)
3.5	15	26	7.5	5.98
25.07	8	319	7.5	9.91
25.07	9	416	9	22.87
20	9	258	9	13.05
5	15	125	7.5	3.68
5	4	19	4	1.1

25 Concurrent Users Metrics

### VU load time (Aggregated (World)) / VUs active (Aggregated (World))

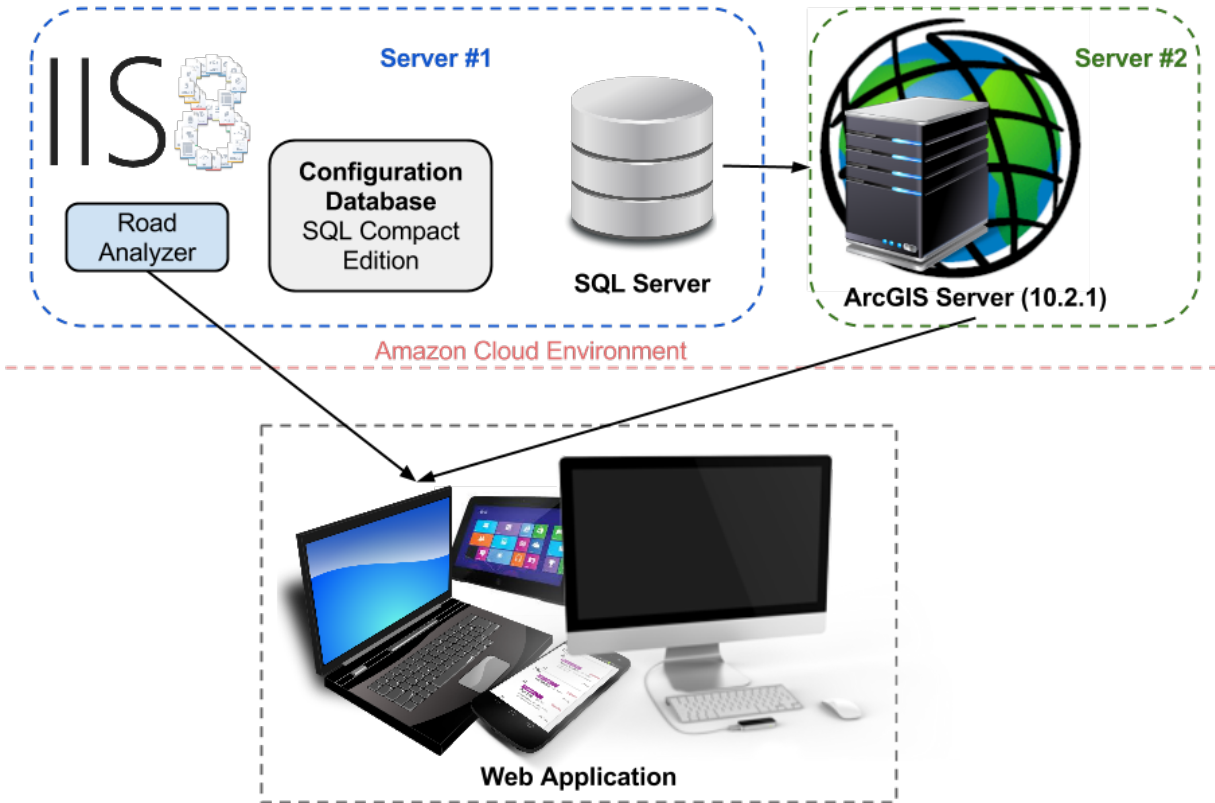


### Configuration 2

Description:

- Application Server (Server #1)
  - Windows Server 2012
  - 64-bit
  - Intel(R) Xeon(R) CPU E5-2670 v2 @ 2.50GHz, 2499 Mhz, 2 Core(s), 4 Logical Processor(s)
  - 30.5 GB Physical Memory
  - Installed Software: ArcGIS Server, ArcGIS Desktop, SQL Server 2012
  - Configuration Database (SQL Compact Edition)
- ArcGIS Server (Server #2)
  - 10.2.1
  - Default configuration
- Database (Server #1)
  - SQL Server 2012

Infrastructure:



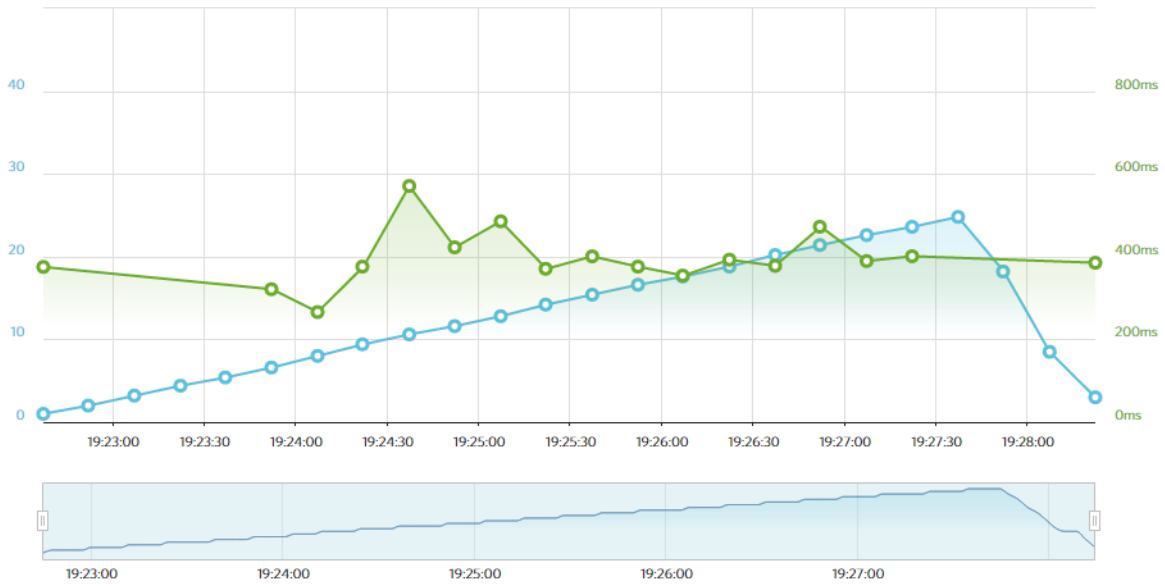
Performance Metrics:

Total Miles	Layers Queried	Features Queried	Symbology Complexity (1-10)	Total Query & Render Time (seconds)
12.525	13	40	5	1.96
3	13	103	8.5	4.39
5	13	148	148.9	3.85
18.68	13	14	4	2.07
40	4	12	2	2.09
4.662	13	15	3	1.44

25 Concurrent Users Metrics:

VUs active (Aggregated (World)) / VU load time (Aggregated (World))

● VUs active ● VU load time





## WCAG and 508 Compliance

Rizing Geospatial is committed to ensuring digital accessibility for people with disabilities. We are continually improving the user experience for everyone and applying the relevant accessibility standards.

### Measures to Support Accessibility

Rizing Geospatial takes the following measures to ensure accessibility across all our web applications:

- Includes accessibility as part of our routine quality assurance testing

- Runs automated tests through an updated accessibility engine

### Conformance Status

The [Web Content Accessibility Guidelines \(WCAG\)](#) defines requirements for designers and developers to improve accessibility for people with disabilities. It defines three levels of conformance: Level A, Level AA, and Level AAA. Rizing Geospatial is partially conformant to varying extent with WCAG levels A, AA and AAA for each of the WCAG principles. Partially conformant means that some parts of the content do not fully conform to the accessibility standard.

### Additional Accessibility Considerations

Our goal is to meet WCAG Levels A, AA and AAA conformance to the best of our ability recognizing that full compliance is unrealistic given the visual nature, complexity, and extensive code libraries utilized by our suite of web tools.

### Feedback

We welcome your feedback on the accessibility of Rizing Geospatial's web application products. Please let us know if you encounter accessibility barriers.

E-mail: [geosupport@rizing.com](mailto:geosupport@rizing.com)

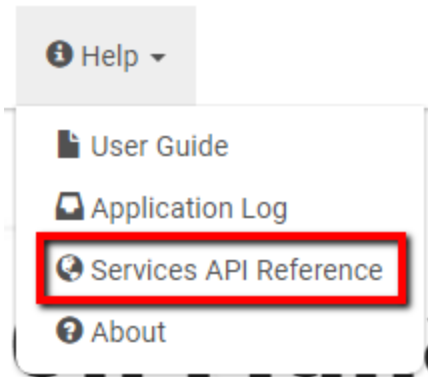
### Assessment Approach

Rizing Geospatial assesses the accessibility of our web applications using the following approaches:

- [Deque's axe](#) open source accessibility browser extension tool

## Services API Reference

The Services API Reference can be accessed from the **Help** dropdown menu found in the top navigation bar and clicking on the "Services API Reference" menu option.



The Services API Reference is a list of the available Transportation Data Server Web API services for most of Rizing Geospatial software solutions.

## Frequently Asked Questions (FAQs)

### **What browsers does App Manager support?**

Most modern web browsers like: Chrome, Firefox, Safari, Edge, and IE11+. For optimal performance, the product team recommends using the application in the most up to date versions of these.

### **What operating systems does App Manager support?**

Since App Manager is an HTML, JavaScript, and CSS web application any operating system with a modern web browser can run App Manager – even tablets, phones, and other devices.

### **Does App Manager support data encryption?**

Yes, the application requests/transactions can be encrypted by running over HTTPS (SSL).

### **Is App Manager scalable? Does it work in a load balanced environment?**

App Manager can be “replicated” to multiple application servers and function in a load balanced environment. See [Scalability and Performance](#) for more details.

### **Does App Manager provide role based separation of actions?**

Yes, every service endpoint and functionality in all our applications have an assigned privilege. Roles can be created dynamically and privileges can be assigned to, or removed from, any role. See the [Roles](#), [Role Privileges](#), and [User Roles](#) sections for information on configuring authenticated user roles.

### **Is App Manager configured to use Google Analytics?**

Yes, the Google tracking code can be entered into App Manager. See the [Installed Applications](#) topic under “Tracking ID” for instructions on how to configure this feature.

All Google Maps JavaScript API applications are subject to the limitations of [Google's Terms of Service](#). Therefore to use any imbedded Google Map tools within the applications, you will need to adhere to [Google's Terms of Service](#) - this typically means you need to purchase an enterprise license. To learn more, please visit [Google Maps' Get a Key/Authentication](#) page. Once you have that you can enter it in the [General Server Settings](#), along with your Client ID, Signature, and/or Channel.

### **Can I change where TDS stores its configuration data (the config store)?**

Yes, please see the [Configuration Store](#) topic for more information as well as step-by-step migration instructions.

### **What safeguards does TDS use for database access security and protection against SQL injection and other functions?**

All of Rizing Geospatial's products provide safeguards to help prevent SQL injection attacks by making use of parameterized SQL queries within the .NET framework. While there are safeguards in place to prevent SQL injection attacks, within Rizing Geospatial's products, the recommended data access architecture is intended to provide the greatest defense mechanism. Securing data access via connection account privileges and application user/role/privilege assignment is critical to mitigating the risk of unintended server and database access. This is particularly important due to the fact that some functionality in Rizing Geospatial's products do require some level of dynamic SQL input. It is critical that only authenticated and trusted users have access to this functionality. All database connections to the transactional data should be configured to use a read-only connection. See ["Data Flow and Connections"](#) on

page 180" for more details.

#### Do I need to install new releases in a particular order?

It depends on the type of release. Rizing uses the Major.Minor.Patch semantic versioning (for example, version 5.0.0 is a major release, version 5.1.0 is a minor release, and 5.1.1 is a patch release). Minor or patch releases can be installed in any order. For major releases, reference the Release Notes for the recommended installation instructions, which may include a specified order. It is best to install the all of latest products at the same time. and we strongly recommend [making a backup of the site/TDS configuration](#) before you begin.

Enhancements and bug fixes are provided in each release, so [keeping your application updated](#) to the most recent version ensures the best performance of the applications.

#### How do I uninstall one of the applications?

1. Navigate to *Programs* in your computer.
2. Click **Uninstall** for the application you want to uninstall.
3. Click **Uninstall** or **Yes** on the confirmation popup.
4. A confirmation prompts will open. Click **OK** to confirm.

See ""To uninstall the application" on page 13" under the [Updating an Existing Installation](#) heading in the [Getting Started](#) topic for more information.

#### Can I migrate TDS in IIS from the default website to a non-default website?

Yes, please see the [Installing TDS to a new Website in IIS](#) topic which will walk you through the process of uninstalling and backing up TDS, creating a new TDS website in IIS and migrating data from the previous install.

#### I'm unable to delete or update a data source, profile, etc. within the applications, how do I troubleshoot the issue?

IIS has many configurations and modules that can interfere with the HTTP requests from TDS applications to the TDS services. Typically, the default IIS configuration provides the necessary setup to allow for the required HTTP traffic to route through IIS and to the TDS web services (API). However, if certain requests (typically HTTP PUT or DELETE) are not being properly routed to the TDS API, the following steps can be used to troubleshoot the configuration issue.

##### Option 1 - Check and Remove WebDAV

1. Open **Programs and Features** on your computer.
2. Select the **Turn Windows features on or off** option.
3. Continue through the **Add/Remove Roles** wizard until you get to the option to edit **IIS features**.
4. Uncheck the following option found under **Internet Information Services > World Wide Web Services > Common HTTP Features**

##### WebDAV Information Services

5. If the option is not checked, proceed to **Option 2** below.
6. Click **OK**.
7. Test the application to see if it resolved the issue.

**Note:** You may need to restart the server for the change to take effect.

##### Option 2 - Add additional verbs to default IIS configuration

1. Navigate to the IIS `applicationHost.config` file.  
Typically located at `C:\Windows\System32\inetsrv\config`
2. Edit the `applicationHost.config` file in a text editor.
3. Navigate to the `system.webServer > security > requestFiltering > verbs tag`.
4. Ensure that **PUT** and **DELETE** are listed.

**Note:** If the `allowUnlisted="true"` property is set on the verbs tag then it is not necessary to specify "PUT" and "DELETE" explicitly.

**Tip:** If you do not want to apply this setting globally to IIS you can make this configuration specifically for the TDS application or website. <https://docs.microsoft.com/en-us/iis/configuration/system.webserver/security/requestfiltering/verbs/add>

5. Test the application to see if it resolved the issue.

**Note:** You may need to recycle the app pool or restart IIS.

#### Do Rizing Geospatial products meet WCAG and 508 accessibility guidelines?

Rizing Geospatial is committed to ensuring accessibility for people with disabilities. Due to the nature of some of our products not all accessibility rules are relevant or obtainable. Please see our [WCAG and 508 Compliance topic](#) for further details on how we are continually working to improve the user experience for everyone and apply the relevant accessibility standards across all our web applications.

#### Do Rizing Geospatial's applications support Esri's branch versioning option?

Yes, all of Rizing Geospatial's applications support [Esri's branch versioning](#). Branch Versioning means the application will query the versions *thru the map service*, not the database. So, when adding a [data source](#) for the applications to use that has branch versioning, you will need to check the **Data source uses ArcGIS Branch Versioning** option, then enter the **Map Services Account Username** and **Map Services Account Password** in [Application Settings](#).

In order for Rizing Geospatial's applications to load properly, the [Associated Service URL of the data source](#) configured in TDS needs to be at a minimum a *Viewer User Type* in Portal and have the map services used by the [Data Source](#) shared with it. The easiest way to do that is to add the user to the group that the map service is shared with, if the map services are not shared to the Organization.

You can have both types of versioning in a single database: traditional and branch. Traditional versions are managed within the database. Branch versions are managed from the feature service. Only one type of versioning can be used with a Data Source. If there is a need to pull branch versioned data and traditional versioned data from the same database, for example in a Segment Analyzer template, *two different Data Sources* will need to be used: one configured with just the database connection and map service and one configured with the map service and the [Data source uses ArcGIS Branch Versioning](#) option checked.