accruent

Onsite Application Admin Guide

Advanced TMS Setup & Configuration

Table of Contents

1 Introduction

1.1 Purpose

This document is provided to serve as a template for application administrators that maintain, install, or otherwise have technical ownership of the TMS Onsite application server.

The objective of this document is to help these administrators install and configure TMS Onsite to have improved performance, reliability and improve overall system health.

1.2 Scope

This document is intended for individuals responsible for supporting and maintaining, installing, & troubleshooting TMS Onsite only. It will not cover the TMS Onsite installation process and is intended to supplement all TMS Onsite installation documents and does not replace them.

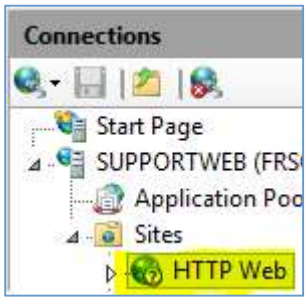
2 TMS Onsite post installation configuration

2.1 TMS HTTPS / SSL configuration

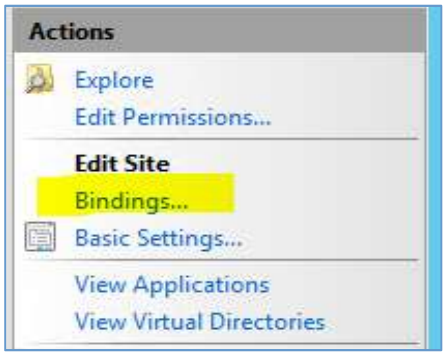
Before going further, please note that there will be some interruption to any users currently on the system. Also, prior to making any changes to your TMS system files, first create a backup of the original files.

IIS Bindings

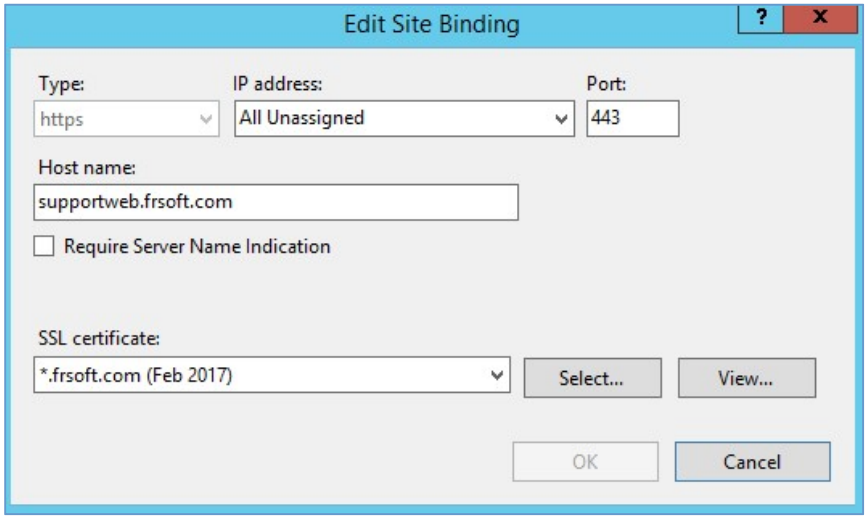
Open **Internet Information Services (IIS)** manager, expand sites and highlight your site that is hosting **TMS Onsite**:



On the right-hand side of the screen select **Bindings**:



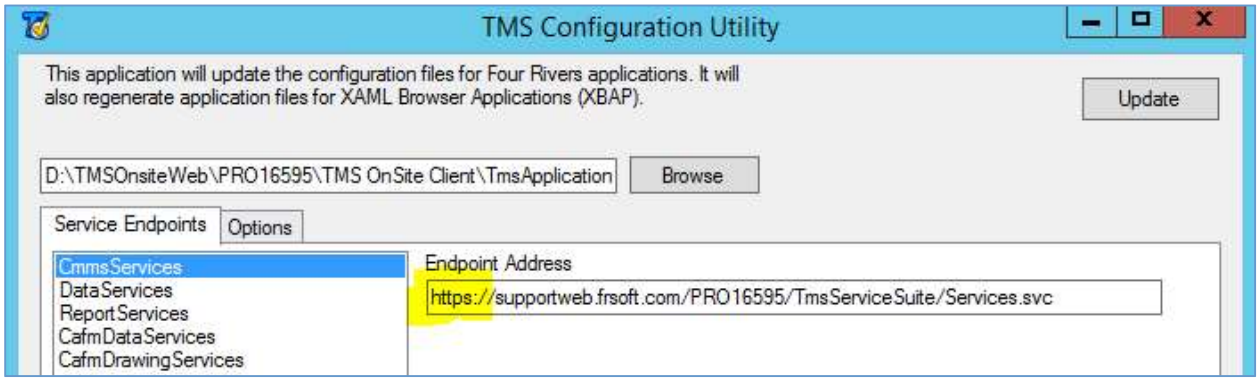
Click **Add** and then enter the following information verifying that the **Host name** is correct. Furthermore, if you do not have an SSL certificate one will need to be created by your organization. TMS Support cannot provide one for your organization.



TMS XBAP Utility

Launch the TMS XBAP utility and replace all instances of HTTP with HTTPS. This includes:

CmmsServices
DataServices
ReportServices
CafmDataServices
CafmDrawingServices



Once complete, click **Update** and click **OK** after the update is successful

Deployment File Update

Open Windows Explorer and navigate to your TMS Onsite installation directory. Locate the **\TMS Onsite Client** folder. Once there, open the **TmsApplication.exe.config.deploy** file with notepad. Once opened, update the file in the following manner:

Add an '**s'** to the FRSoft_binaryHTTPBinding:

```
</basicHttpBinding>
<customBinding>
  <binding name="FRSoft_binaryHttpBinding" receiveTimeout="01:00:00" sendTimeout="01:00:00">
    <binaryMessageEncoding maxSessionSize="250000000">
      <readerQuotas maxDepth="2000000" maxStringContentLength="20000000" maxArrayLength="250000000" maxBytesPerRead="2000000" maxNameTableCharCount="2000000" />
    </binaryMessageEncoding>
    <httpsTransport maxBufferSize="65536" maxReceivedMessageSize="250000000" transferMode="Streamed" />
  </binding>
</customBinding>
<netTcpBinding>
```

Save and close the file when complete.

Web Config File Update

Locate the **web.config** file found at **\TMS Onsite Services** and open the file with notepad. Once opened, update the file with the following information in the correct location (towards the top of the file):

```
  </system.codedom>
  <system.serviceModel>
      <serviceHostingEnvironment multipleSiteBindingsEnabled="true">
      </serviceHostingEnvironment>
      <services>
```

Exact text below:

<serviceHostingEnvironment multipleSiteBindingsEnabled="true">
</serviceHostingEnvironment>

Within the same **web.config** file, locate the **FRSoft_binaryHttpBinding** and update the transport binding to https:

```
  <binding name="FRSoft_binaryHttpBinding" receiveTimeout="01:00:00" se
          <binaryMessageEncoding maxSessionSize="50000000">
                  <readerQuotas maxDepth="2000000" maxStringContentLeng
lameTableCharCount="2000000"/>
          </binaryMessageEncoding>
          <httpsTransport maxBufferSize="65536" maxReceivedMessageSize=
  </binding>
```

Once complete, save and close the file. Then, **restart IIS** and login to the TMS client with HTTPS instead of HTTP.

 You may need to set your trusted sites in your IE browser to access the site successfully.

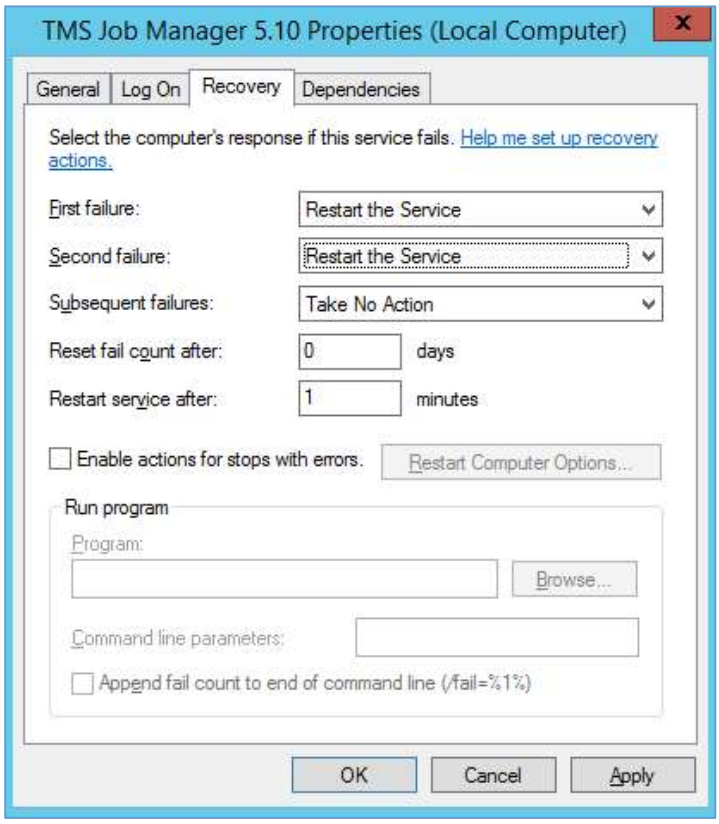
2.2 TMS Onsite services configuration

There are some services that are installed onto your TMS Application server during the installation of TMS. These include:

TMS Job Manager
TMS OnSite Agent
TMS Onsite Print Agent (If installed)
TMS Interface Engine (does not apply)

These services control the automation processes, printing reports within TMS, emailing and other operations. To prevent interrupting these services during configuration, follow these steps:

1. Open the services on your TMS application server.
2. Open the **TMS OnSite Agent** service properties.
3. Verify (or change) **the Startup Type** to **Automatic**.
4. Click on the **Recovery** tab and choose the following options:

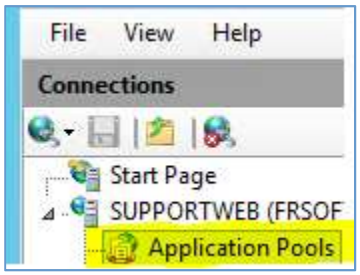


5. Click **Apply** and then **OK**.
   Complete the same actions for the remaining TMS Services.

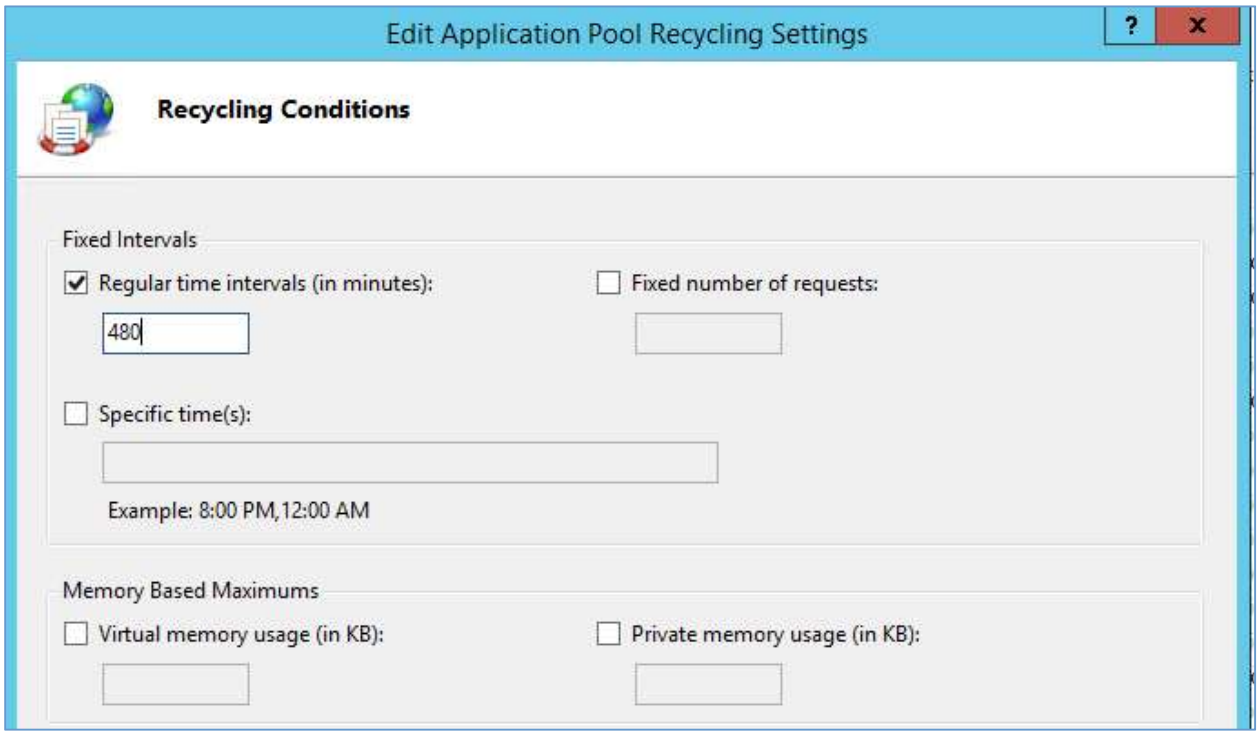
2.3 IIS application pool recycling

After installing TMS the default application pool recycle occurs every 29 hours. To increase the stability of IIS (especially for high traffic environments) this setting can be changed to increase the number of times the application pool is recycled. Please note that when an application pool recycles, it will not interrupt any users currently engaged or idle in the application. Because of this, there is no risk, but a high reward to application pool recycling.

To set this up, open **Internet Information Services (IIS) Manager** and click on **Application Pools**:



Find your TMS Onsite application pool, highlight it and click on **Recycling** on the right-hand side of the screen. Edit the **recycling conditions** and reduce the **regular time intervals (in minutes)** to a lower number. For example, the value for once every 8 hours would be 480:



Alternatively, you can also set the recycling to occur at specific time intervals throughout the day.

Click **OK**.

2.4 Automatic service restart

The TMS Onsite services can be setup to automatically restart on their own via the task scheduler. This can be done for many reasons including verifying the services are running before they are needed the most (i.e. restart one day prior to the monthly PM generation). To set this up, please complete this via **Windows Task scheduler**.

The instructions for using **Windows Task Scheduler** are not included here, however, the action that will be done is running a batch file. The batch file contents are as follows:

NET STOP TmsJobManager5105
NET STOP TmsOnSiteAgent5105
NET STOP TmsOnsitePrintAgent510

NET START TmsOnSiteAgent5105
NET START TmsJobManager5105
NET START TmsOnsitePrintAgent510

 Depending on your TMS Onsite version, you may need to update the batch file contents to match your TMS Onsite service names.

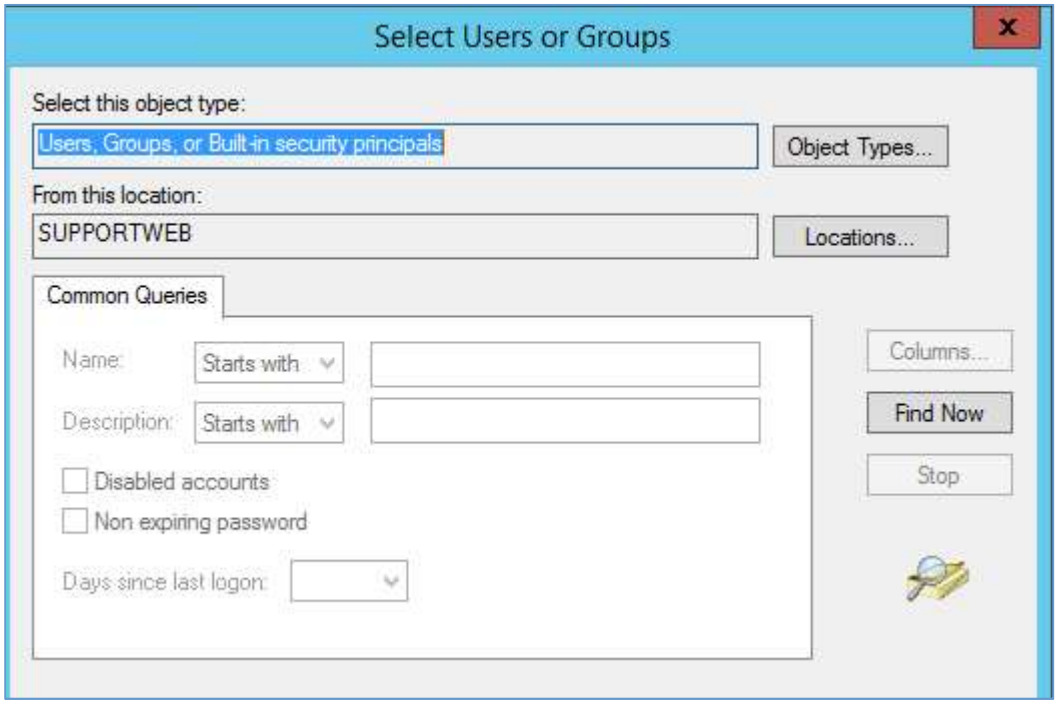
2.5 TMS Onsite folder permissions

To avoid possible IIS permission issues for end users within TMS, the security on the root TMS installation folder can be configured. There are 3 user accounts that are built into windows that can be added to avoid these potential issues. They are as follows:

NETWORK SERVICE
IIS_IUSRS
IUSR

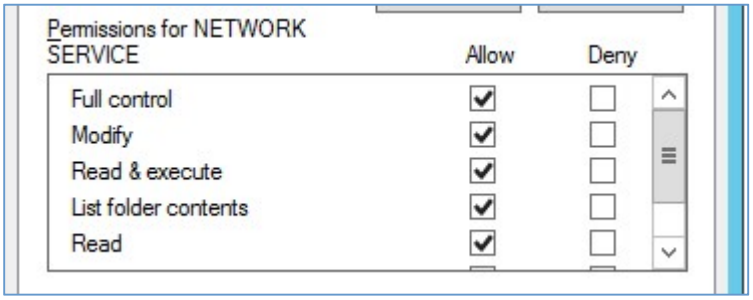
The following actions will prevent potential permission related issues for end users while within the core application or any of the add-on modules.

1. Using Windows Explorer, navigate to your core installation folder.
   Normally, this is **C:\Program Files (x86)\FRSoft**.
2. Right click on the folder and choose **Properties**.
3. Click the **Security tab** and click **Edit**.
4. Click the **Add** button.
5. Click the **Locations** button and choose **your local server** from the menu and click **OK**.
6. Click **Advanced** and then **Find Now**.



7. Select the 3 user accounts listed above by finding them in the list and holding down the left CTRL key while clicking on each.
   This will enable you to add all 3 at once.

8. Click **OK** and then **OK** again. Once the names appear in the properties screen, click through the users added and select the checkbox for **Full control** for all three users.



9. Click **Apply** and then click **OK**.

Onsite Application Server Admin Guide – September 2018

Accruent, LLC

11500 Alterra Parkway
Suite 110
Austin, TX 78758

www.accruent.com