

TARGIT

Data Discovery

Installation and Configuration Guide

Decision Suite 2019 RTM

Contents

- TARGIT 1
- Data Discovery 1
 - Introduction 3
 - Architecture 3
 - Requirements 4
 - Installing the TARGIT Data Discovery (Single server setup) 5
 - Installing the TARGIT Data Discovery (Separate server setup)..... 6
 - Configuring network level security 8
 - Securing the data 8
 - Filtering browsing of files and folders..... 8
 - Securing Communications 9

Introduction

TARGIT Data Discovery enables a TARGIT customer to instantly consume data from a wide range of data sources. The product can be installed on the same server hosting the TARGIT Server component.

The goal with this guide is to provide you with tools and methods to install and utilize the TARGIT Data Discovery in your environment.

Please note that installation and configuration require knowledge of Windows Server, IIS configuration.

The user guide is available at online at <http://doc.targit.com/data-service>

Architecture

The TARGIT Data Discovery will require the ports 9095 (for the administrative interface) and 9090 (for database communications) to be available.

The TARGIT Data Discovery contains a full IP filter service where connections from other network entities can be limited additionally Windows Security can be applied to minimize access to the administrative interface.

TARGIT Data Discovery can in addition to the schematic below be installed on a separate server, please see the section “Installing the TARGIT Data Discovery (Separate server setup)” for further guidance.



Requirements

The following requirements must be present for successful installation of the TARGIT Data Discovery:

- TARGIT Decision Suite 2015 or newer
- A newer browser (IE10 and newer)
- A valid license that includes the Data Discovery-module
- .NET Framework 4.7.1 or newer
- Windows Server 2008 SP2 and newer
- Enabled Windows Features for:
 - WCF Activation over port and http
 - IIS ASP.NET 4.5

Installing the TARGIT Data Discovery (Single server setup)

1. A server running TARGIT Server must be configured and running with a valid license for the “Data Discovery”-module.
2. Ensure you have upgraded the browser on the servers where you want to test/utilize Data Discovery (at least IE10 and newer). Also, for servers the secure browser mode must be turned off for the UI to be shown.
3. Ensure the following components (Windows Features) are installed
 - a. WCF Activation over port and http
 - b. IIS ASP.NET 4.5
4. Download the TARGIT Data Discovery installer from the TARGIT Download Center and execute the installer and fill out the prompts on the installer pages.
5. Specify the URL for which the clients should be able to access the Data Discovery interface. Please ensure that the firewall on the machine is open for the port tcp/9090 and tcp/9095. It is recommended not to change the ports.
6. Modify the proxy settings if they are required for the network environment. The installer tries to autodetect this and if it does find a proxy it will default to that option and suggest you fill out the fields for proxy address, user and password to connect through the proxy.
7. Choose the appropriate locales for your environment. If you primarily work with English files add English as the first option in the locale selection screen and add additional locales that you would meet, e.g. German. You can add as many as necessary and the parsing of dates etc. will be done according to the list.
8. Choose the installation option for local TARGIT Server.
9. Finish the installation
10. Start TARGIT Management, go to rights and give the current user permissions to be Data Discovery administrator

You should now be able to launch the TARGIT client and launch the Data Discovery tool from the ribbon

Installing the TARGIT Data Discovery (Separate server setup)

1. A server running TARGIT Server must be configured and running with a valid license for the “Data Discovery”-module.
2. An accessible Windows Share must be created and be given full write permissions for the service account that TARGIT Server is running under, this share must point to the path for the TARGIT settings folder (default c:\ProgramData\TARGIT\ANTserver\)
3. Ensure you have upgraded the browser on the servers where you want to test/utilize Data Discovery (at least IE10 and newer). Also, for servers the secure browser mode must be turned off for the UI to be shown.
4. Ensure the following components (Windows Features) are installed
 - a. WCF Activation over port and http
 - b. IIS ASP.NET 4.5
5. Download the TARGIT Data Discovery installer from the TARGIT Download Center and execute the installer and fill out the prompts on the installer pages.
6. Specify the URL for which the clients should be able to access the Data Discovery interface. Please ensure that the firewall on the machine is open for the port tcp/9090 and tcp/9095. It is recommended not to change the ports.
7. Modify the proxy settings if they are required for the network environment. The installer tries to autodetect this and if it does find a proxy it will default to that option and suggest you fill out the fields for proxy address, user and password to connect through the proxy.
8. Choose the appropriate locales for your environment. If you primarily work with English files add English as the first option in the locale selection screen and add additional locales that you would meet, e.g. German. You can add as many as necessary and the parsing of dates etc. will be done according to the list.
9. Choose the installation option for remote TARGIT Server and specify the name including the port (default port is 1300) in the form of servername:portnumber e.g. myTARGIT Server:1300 as well as the path to the share created earlier in the form [\\nameofanserver\TARGIT](#).
10. Start the Windows Services control panel and stop the service TARGIT Data Discovery. Change the service account credentials to an account with full permissions to modify the file share created earlier and restart the service
11. Finish the installation

12. Restart the TARGIT Server service account on the server where the service resides.

13. Start TARGIT Management, go to rights and give the current user permissions to be Data Discovery administrator

You should now be able to launch the TARGIT client and launch the Data Discovery tool from the ribbon

Configuring network level security

Securing the data

Data access for end users is configured through the TARGIT Management-application and does not differ from configuring security on other connection types. Please refer to the TARGIT Management User Guide.

Filtering browsing of files and folders

An administrator can limit browsing for files or folders in the Data Sources plugins by specifying a filter in the Data Service's settings.

These can be used ONCE within the browsing-section

Allow *	Allows access to all resources
Deny *	Denies access to all resources

These can appear multiple times as necessary

Allow <u>c:\resource</u>	Allows access to a resource
Deny <u>c:\resource</u>	Denies access to a resource

In the example below browsing in all folders are disabled by the deny * and browsing C:\DSTraining end up being allowed.

Data Service Settings

Main

Managing access to the files and folders. You need to enter the name of directory or file storage and specify access to it.

Plugins

Plugin Manager

Cache

Proxy

Database Engine

Logging

File Storage

File Browser

Notifications

Add File Path

Allow ▼ C:\DSTraining

Deny ▼ *

Back Save

Securing Communications

The TARGIT Data Discovery comes with a built in IP filtering functionality that can limit the request to the service. This can be configured by editing the file C:\Program Files\TARGIT\TARGIT Data Discovery\Target.DataService.Exe.Config (make a backup before editing!)

By default the functionality is disabled but can be enabled by simply uncommented the entries in the configuration file.

➔ Please note that help related to configuration of this is only provided as billable support

By default the filter is set to the name "Default" and the corresponding filter with the same name, however the FilterName can be changed to any of the other filter examples, to only allow connections for both administrative and queries for the server the TARGIT Data Discovery is installed on the following settings must be changed:

1. Remove comments from the `<!-- <HttpModule FilterName="Default" /> -->` line (the `<!--` and the `-->`)
2. Change `<HttpModule FilterName="Default" />` to `<HttpModule FilterName="LoopbackOnly" />`
3. Remove comments for the loopback section, leaving it like this

```
<!-- A filter than only allows traffic from loopback -->
<add Name="LoopbackOnly">
  <allow hosts="127.0.0.1/8" />
  <deny hosts="*" />
</add>
```
4. Restart the TARGIT Data Discovery from the Windows Services.

Below are the individual sample configurations – also found in the default configuration file, please note that comments have been removed from all irrelevant places in the sample below:

```
<IPFilter>
  <HttpModule FilterName="Default" />
  <Filters>
    <add Name="Default" DefaultBehavior="Deny">
      <deny hosts="192.168.11.12,192.168.1.*" />
      <allow hosts="192.168.0.0/16" />
      <deny hosts="*" />
    </add>

    <!-- A filter than only allows traffic from local network -->
    <add Name="LocalOnly">
      <allow hosts="10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,127.0.0.1/8" />
      <deny hosts="*" />
    </add>

    <!-- A filter than denies traffic from local network -->
    <add Name="DenyLocal">
      <deny hosts="10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,127.0.0.1/8" />
      <allow hosts="*" />
    </add-->

    <!-- A filter than only allows traffic from loopback -->
    <add Name="LoopbackOnly">
```

```
<allow hosts="127.0.0.1/8" />
<deny hosts="*" />
</add>

<!-- A filter than denies traffic from loopback -->
<add Name="DenyLoopback">-->
  <deny hosts="127.0.0.1" />-->
</add>-->
</Filters>

</IPFilter>
```