TARGIT Administrator

Back

Table of Contents

TARGIT Administrator

This section is intended for users who administrate a TARGIT solution.

Setup - Front-End

Number Format

By default this setting is checked on new installations and therefore all formatting is done on the client side according to the login (or browser) language. If this setting is disabled all number formatting is done on the server according to the system language and all clients will see the same number formatting. An advantage of using client-side formatting is the reductions in query result size, especially with cross tables. Both the server and client-side formatting may be overwritten by changing the number formatting on the individual data objects in the clients.

The currency setting decides what currency is used when using the currency number format.

Note: When upgrading from versions prior to build 4062, client-side formatting is disabled to ensure backward compatibility.

Statistics

Anonymous usage statistics are sent to TARGIT for improving and selecting future features. The statistics contains a list of features that users use in the client (ribbon content, right-click menu content and so on), but does not point out individual users nor does it contain any customer data. Click the Privacy policy link for details.

Splash screen

Display: May be set to Disabled, Default or Custom. Information on how to use the Splash screen settings are displayed when hovering the i to the right of the field.

URL: The URL for the custom website to display may be entered.

Menu name: The name of the Menu item that reopens the splash screen may be entered.

Enforce display in clients: If the display of the splash screen should be enforced, a check-mark may be set.

Data request cache

The following settings may be turned up or down for data request caching:

Cache size limit (Mb): Makes it possible to set the maximum size for the disk space allowed for caching (in Mb, default 1024 Mb).

Minimum free disk Space (Mb): Makes it possible to indicate the minimum size of free disk space required to enable the cache (in Mb, default 256 Mb).

File count limit: Makes it possible to set the maximum number of files in the cache. (Default 1000 files).

Idle file expiration (days): Makes it possible to indicate the number of days an idle cache file is kept before it is deleted (default 10 days).

Note that caching of data requests may be set to on or off on a database connection.

Client update

Update clients automatically: When end-users log on with the TARGIT Desktop App, the client version is checked against the server version. If the server version is newer, the TARGIT Desktop App will automatically be updated to match the server version.

Shortcut name and icon: As an Administrator you have the option to define the name and the icon of the TARGIT Desktop App as it should appear in the end-user's Windows Start menu.

Redirect to server: If the TARGIT installation is moved from one server to another, this option can be used to automatically redirect logins from the old server to the new server.

Setup - Back-End

Logging

The logging option allows requests to be logged in the auxiliary database. By default analysis requests are logged when checking the 'Log Analysis requests to auxiliary database' option, but it is possible to add storyboard requests to the logging by checking the 'Log storyboard requests' option. The counter adjust button ‘Keep data for’ is used for specifying the number of months to keep the logged requests in the database. If 0 (zero) is selected, the requests are kept until they are removed manually. If logging is disabled after being enabled the logging stops as soon as the currently running requests stops. If logging is enabled again, the logging does not start for the currently logged on users - only the ones logging on later. If the Auxiliary connection is changed while logging is enabled, the log will continue to use the old connection - until logging is stopped and restarted or the TARGIT Server is restarted.

Online License Update

Automatic license update may be enabled and a one hour period may be selected for the update to take place. The current license is sent, at a random time within the given time period, to the licensing server and a check for an updated license is made. If an update is needed e.g. due to expiration or update to a later version, the license will automatically be updated.

Criteria request cache

The following settings may be turned up or down for criteria request caching:

Cache size limit (Mb): Makes it possible to set the maximum size for the disk space allowed for caching (in Mb, default 1024 Mb).

Minimum free disk Space (Mb): Makes it possible to indicate the minimum size of free disk space required to enable the cache (in Mb, default 256 Mb).

File count limit: Makes it possible to set the maximum number of files in the cache. (Default 1000 files).

Idle file expiration (days): Makes it possible to indicate the number of days an idle cache file is kept before it is deleted (default 10 days).

Note that caching of criteria requests may be set to on or off on a database connection.

Multiple Logins

The default setting is that only one user can be logged on to the TARGIT Management client at a time. Use this setting to enable multiple simultaneous logins to the TARGIT Management client. However, if enabled, a warning will be displayed if a user attempts to log in while another user is already logged in. You will be warned that your work may potential be lost if another user is working on and saving the same settings that you are working on.

Setup - Alerts and Notifications

The Alerts and Notifications option is used to send e-mails if TARGIT Server errors occur and to specify the mail server to be used when scheduling notifications and Reports. It lets you specify the mail server to be used for outgoing mails. The server name may be followed by a colon and a port number.

Using SMTP authentication is possible, user name and password may be entered in the appropriate fields. It is also possible to enable SSL /TLS encryption if the server supports it.

Error reports by email are by default sent from ‘antserver@computer name’. Some mail servers however requires that sender address is a fully qualified domain name. An edit field allows specifying a correct sender address.

An example of an error could be that the TARGIT Server could not process a request or that the given request is invalid. When enabling the Administrative alerts option, it becomes possible to set an option to report different kinds of errors and write one or more e-mail addresses of the recipients.

Note: To send e-mails to external addresses the mail server needs to be configured to allow relay from the TARGIT Server. The simplest way to do this is to add the IP address of the TARGIT Server to the mail server's "Relay Allowed" list.

Setup - Performance

Performance

Maximum number of active threads determines the number of concurrent threads the TARGIT Server will use to serve the clients. Each client will use its own thread, but this setting can be used to limit the number of active threads. An active thread is defined as a thread currently processing a request. If the number of actual requests is higher than the number of available threads, the requests are queued. Performance can be increased by raising the number of concurrent threads, but at the cost of system resources (memory, CPU power, disk access, etc.). If this setting is 0 there is no upper limit to the number of concurrent active threads. Default is set to 4 times the number of CPU cores.

The maximum number of Sentinels threads may also be set and is used to specify how many threads should be used for searching for Sentinels. The default value is 1 on a single CPU server and half the number of CPU cores on a multi-core server. This is to avoid that all processing power is used on searching for Sentinels. The number may be changed, but no more threads than the number of CPU cores can be assigned to the Sentinel search even though a higher number may be entered. A value of 0 threads is the same as default.

Network Load Balancing

When multiple TARGIT Servers are configured in a Network Load Balancing (NLB) environment, this option may be enabled and the NLB parameters may be specified. The basic principle of operation is that requests may be rejected a maximum number of times, depending on the actual load of the TARGIT Server and below ‘Maximum Rejections’ setting. The actual thresholds triggering rejections may be based on either a CPU load percentage over a certain time period, on the number of Active Queries or a combination hereof. If both thresholds are set, request rejection will take place if one of them is fulfilled.

CPU Load

Check this to activate the threshold and specify the CPU percentage and time period that the actual CPU load has to be higher than in order to initiate a request rejection. The default values are 95% over 10 seconds.

Active Queries

Check this to activate the threshold and specify the Maximum Queries that will trigger a request rejection. The default value is four times the number of CPU cores on the server running the TARGIT Server.

Setup - Server Trace

Server trace consists of two options that will change the registry settings. Log requests logs analysis requests in the event log (this is in addition to the log in the auxiliary database if enabled in the Backend module). Log to file is only relevant when the TARGIT Server is running as a service. The option enables the possibility to log to a file (.LOG) rather than the application event log. The log file is date stamped and if the file exceeds 2GB during one day, more files are created. . LOG files are located in the folder: ...\ProgramData\ANTserver\TARGIT\LOG. MDX queries sent to the database may also be logged by checking the MDX check box.

Note: These options should only be used for debugging purposes, because of the large amount of data sent to the event log or log file. Logging data requests requires an Enterprise Server license.

Setup - Change Service Account

Choose the Service Account, according to your organisation's security policy, that should run the TARGIT Server.

Connections

Clicking the Connections module shows a list of current connections and their properties. Rightclicking a connection opens a menu with options to add, delete, disable and see the properties for the connection. When adding a new connection a new dialogue opens with options to create a MultiDimensional, Relational or Other connection.

Database setup dialogs for databases may have the following options:

Impersonation: (Windows Security Impersonation / Delegation)

Used to specify that user's access to the database should be controlled by the cube security. This option is only active for Microsoft Analysis Services cubes, and when using Windows authentication. Using impersonation on a database connection has the disadvantage of not being able to use scheduling since the users' credentials are needed to do the impersonation and these credentials are not known when the scheduled job is executed. Microsoft Analysis Services 2005 has introduced an alternative to 'Standard' impersonation called 'Effective user'. By supplying just the user name (and not the password) Analysis Services will behave as if the user was authenticated and any security set up in the database will be considered. Furthermore, this allows scheduled jobs to be executed. Note that this requires the user that logs into Analysis Services (i.e. the user running the TARGIT Server) to have administrator rights.

Note: If TARGIT Server and Analysis Services are on separate servers, they must be on the same domain and the TARGIT Server PC must have "delegate" rights. Also note that the TARGIT login option "Specify credentials" does not work in connection with "Impersonate users" if TARGIT Server and Analysis Services are on separate servers, so in this case the Client PC's must be on the same domain as the servers.

Non empty criteria

This property is enabled by default and ensures that dimensions on the criteria bar are filtered such that members causing empty results are removed from the dimensions displayed in the criteria bar. This option is only available in connection with Multi-Dimensional databases.

Non empty queries

This property is enabled by default and filters dimension members with empty results from the data set. This option is only available in connection with Multi-Dimensional databases.

Use subcubes

A subcube is a subset of a cube based on the criteria applied to the data set. The use of subcubes is enabled by default and will in most cases result in a performance increase. Use of subcubes has both pros and cons which should be considered. This option is only available in connection with MultiDimensional databases.

Max active connections

Used to limit the number of active connections to the backend database server.

Accumulated query time before reconnect (seconds)

In order to reduce Pivot Table Services memory requirements when accessing large databases, it is recommended to disconnect and reconnect from the database at certain intervals. The number of seconds of accumulated query time between each disconnect may be specified here. Default setting is 0 (zero) for no automatic disconnect / connect.

Generate SQL based on consistent data (Only relational databases)

This option indicates to the TARGIT Server if data are consistent or not. Specifically if all foreign keys lead to a proper result. This option is on by default, but can be cleared if data are known to be inconsistent, e.g. when connecting to a real-time source. Note that if this option is cleared the query performance may be reduced.

Check for Desktop and Touch notifications

This option is on by default. Clearing it prevents notifications from being displayed for Desktop and Touch when processing the data model related to the connection. If a connection is very often processed and the connection is not used for Desktop or Touch, performance may be improved by clearing this option, since the TARGIT Server does not have to check for notifications.

Cache data requests

Data request cache works in connection with data requests in order to reduce the time it takes to fetch and display data when data requests are repeated. Note that default is on on multidimensional database and Xbone connections and off on relational database connections. Every time a cube is processed, the cache is flushed in order to prevent outdated results, which means that cache on close to real-time connections may have little or no effect.

Data request cache files for the Windows client are placed in the following folder on the local computer:

<drive\path>\users\\Appdata\Local\Temp\cache\

Data request cache files for Web and Touch clients are placed on the server in folders similar to this:

<drive\path>\windows\temp\cache_\

The data request cache is updated in case of cube processing and when colors are changed.

Cache criteria requests on server

Criteria request cache works in connection with criteria requests in order to reduce the time it takes to fetch and display criteria when criteria requests are repeated. Note that default is on on multidimensional database and Xbone connections and off on relational database connections. Every time a cube is processed, the cache is flushed in order to prevent outdated results, which means that cache on close to real-time connections may have little or no effect.

Criteria request cache files are placed in the following folder on the server:

<drive\path>\Program Data\TARGIT\ANTserver\cache

The criteria request cache is updated when processing the cube, when changing colors and in case of changing forced criteria in roles or changing decorations.

Select Into SQL: (Only relational databases)

This field makes it possible to enter an SQL statement that the TARGIT Server uses when aggregation tables are created. The statement consists of SQL keywords and placeholders e.g. (SELECT INTO). The TARGIT Server replaces the placeholders with SQL when working on the aggregation tables. Other SQL statements that copies data from one table to another may also be used (e.g. CREATE TABLE AS SELECT).

License

When connected to a TARGIT Server and clicking the license module, a list of the license values is shown e.g. expiration date, version and number of named users for each application.

The license information may be altered by using one of the options under the license values; Download License, Import License and Check Online Now. A License is supplied as a 16 character License Key which may be entered here and used to download the license data from the license portal. In case the PC running the TARGIT Management application does not have access to the Internet, it is possible to download the license information from the license portal as an XML file which may then be used with above Import License option. Older license keys and license files may be used to register the license as long as the old key or file is valid and there is an update subscription for the license.

The last option is to check for license updates. This is done by sending the current license to the licensing server, which checks for updates. If an update is needed the license will automatically be updated.

Note: Incorrect License information will disable the TARGIT Server, and all other Server modules and settings will be unavailable.

Logins

The Logins module provides an overview of the logins for the license. For each of the licensed applications, the number of available, used and connected logins are shown. The Logins overview may be refreshed by right-clicking and selecting 'Refresh list'. For a more detailed view of the logins, double-click one of the applications for a view of logins to all applications or right-click an application and select to view logins for the selected application or for all applications. This opens a new window, where the list of users who have logged in is shown in the leftmost column. Users with a grey dot are not currently logged in and users with a green dot is currently logged in. Unfolding the plus-character next to each user reveals the logins performed for the user and for users currently logged in, another plus-character may be unfolded to see the IP-address of the user. For each of the logins, the last logon time, the user level and the client version of last login are shown in the other columns. Columns may be sorted by clicking them.

To the right of the logins overview filters may be applied. This is done by selecting the permission rights of the users who should be shown and /or select if disconnected, connected or both kind of users should be shown. The filters are applied instantly.

At the bottom of the window three buttons allow for a refresh of the logins, disconnecting users and deleting users. Deleting users may be used to free up some of the used logins and make room for new users.

Language

The language module is used for customizing business terms in relation to the TARGIT databases. The database terms, including names of databases, measures, dimensions and dimension levels may be translated. Also names of folders and files in TARGIT Smartpad Documents Shared section may be customized.

Each implemented language is represented by an entry in the list of languages. Double clicking a language entry opens a Language Properties dialog with options to edit business terms. A right-click menu is also available for opening the Language Properties dialog for the selected language.

The left column of the Language Properties dialog displays a tree structure for each database and Smartpad Documents, where nodes are preceded by plus or minus signs, which is used to expand or collapse the nodes. The tree may be browsed by using the arrows keys. The middle column 'Translated Name' of the Language Properties dialog is used for translation of the business terms. After having selected an original element of the database tree in the left column, pressing the Enter key will prepare the corresponding edit field in the middle column for entering the translation. Press the Enter key again to accept the translation. The right column 'Translated Description' is used to add a description of the business term. Content of this field will be displayed as a hint when the cursor is hovered over the field in Smartpad Source data tab or the folder or file in Smartpad Documents.

To edit a translated element, press F2 or Enter and type the translation. If the translation is the same as the original use the right-click menu and select 'Copy Original'.

The Suggestion field below the tree structures is filled if an identical original with a different translation is found anywhere in the list. This can be used to make the translations consistent and the suggestion can be applied by clicking the Apply button or right-click an entry in the language list and select 'Copy Suggestion' (Shortcut is Ctrl S). Other options in the right-click menu include 'Copy Default' (Ctrl D), which copies the translation of the default language and 'Copy Original' (Ctrl O), which copies the original text. 'Expand Recursive' expands all the nodes in the database tree and 'Remove Translation' removes the translation.

Decorations

The decorations editor is used to add information to the metadata coming from the underlying backend databases. Decorations are added before metadata is further processed. The benefits of using decorations includes improved performance, easier and better data overview and additional information not available in the database.

When clicking 'Manage decorations' a dialog opens with a list of all databases on the left and a list of properties on the right. In the top of the dialog a filter for each of the properties may be applied and a check box 'Show only specified decorations' to display only the decorations that have been changed from the default values. The check box is checked by default when the decorations editor is opened if decorations have been specified. Each database to the left may be expanded to display containing cubes and each cube may be expanded to display dimensions and measures. When an element is clicked, the properties that may be set for the element are displayed to the right. Default values are displayed for all properties. Changing the default value displays a small '-' button, which may be used to remove the decoration. Note that some of the properties have several values, which may be cycled by clicking them several times and other properties have multi-select values selectable from a list once the default value is clicked. Changes to the properties of an element overrides any values of the property specified elsewhere in TARGIT Management and any values specified on higher levels.

Please refer to the 'TARGIT Management user guide', available in the Download Center, for further details on Decorations.

Export Folders

As an end-user you can schedule various documents or outputs to be send out as an email or to be saved to a folder. The latter option, to save the output to a folder, is where the Export Folders gets into the equation.

A newly installed TARGIT solution will have only one Export Folder, the Default folder, which is pointing to a local folder on the TARGIT Server: C:\ProgramData\TARGIT\ANTServer\Exported Reports\

As an Administrator, you can add as many extra Export Folders as you need. One thing to consider though: The added folders should preferably be folders that are accessible by end-users as well as by the TARGIT Server.

Rights

This module is used to create and edit rights for users and groups regardless of the security model. A good practice is to create different, properly named rights according to the wanted security levels and then add users/groups to the rights.

Right-clicking the white space opens a menu with the option to add a new set of rights. By right-clicking on an existing set of rights it is possible to add a new set of rights, delete the rights or edit the properties for the rights.

Adding a new set of rights causes a Rights Properties dialog to be displayed. In the name field a name for the set of rights may be entered. Below the name field there are three tabs: Members, License and Rights.

The options when clicking the tabs are:

Members

Clicking on the Add tab makes it possible to select and add members to the set of rights. The dialog displayed depends on the security model. If Windows security is selected, a Windows Select Users and Groups dialog is displayed. If Standard security is selected a Select Users/Groups dialog with the defined users and groups is displayed. When members have been added to a set of rights it is possible to remove members by selecting one or more members and then clicking the Remove tab.

License

For each client type a field with a drop-down list makes it possible to set the license level for the rights. The number of purchased licenses of each license type is displayed in parentheses after the license name. Note that it is not the number of unused licenses of the type that is displayed. A short general description of the license levels is given in the table below. For detailed information about licenses see the License Overview document (not available in this user guide).

License	Windows and Web Client
Designer User	All rights to Analyses and Reports
Consumer User	Mostly read rights for Analyses, Reports and Storyboards without any editing rights

In addition to the rights obtained through the license level, the right to Manage the TARGIT Server via TARGIT Management and to Touch access may be managed in the license tab dialog.

Note: If e.g. two Designer User licenses have been purchased and installed and these are the only licenses available, then when selecting a lower license level for a set of rights (e.g. Consumer User), the Designer User licenses will be used when logging on, but the user logs on with Consumer rights.

Rights

This module makes it possible to remove permissions to the Windows with a license level as starting point. A set of features is related to each license level. For each higher license level the set of features is expanded (a Designer user has all the features that a Consumer user has plus extra features). Each of the features related to a license level may be disabled. E.g. if the license level is set to Designer User, it is possible to remove the permission to save analyses in shared documents by clicking on the 'Allow in these rights' link aligned with this feature. Clicking on the link changes the text displayed to 'None in these rights' and another click changes the text to 'Deny in all rights'.

By denying in these rights it may still be possible to obtain the permission through another set of rights. By Denying in all rights the permission cannot be obtained unless it is edited in this set of rights.

If a license module is necessary in order to have access to a feature, the name of the module is displayed in the License modules column. If the module is not purchased, 'not available' is displayed in parentheses after the module name.

Note that the features displayed do not represent a definition of the difference between the license levels. They are only a selection of features that have been assessed to be relevant in relation to rights.

Roles

The Roles module is used to allow or deny access to selected parts of the data in the TARGIT environment including Data Warehouse data and subfolders and their content in the 'Shared' folder.

Roles can be added, edited, copied and deleted by using the right-click menu. Editing a role by clicking the properties menu item brings up the Role Properties dialog. Copying a Role makes it easy to create roles with slightly different properties than the source role. Note: Give roles meaningful names. Often the name could match the title of the group of users the role is intended for, e.g. the name of a department.

Members

The Members tab is used to select which users/groups that should belong to this role. Clicking the Add button will do one of two things depending on the security model of the server. In the case of standard security a dialog will appear where the users/groups from the Users module can be selected as members of the role. In the case of Windows security a standard Windows dialog will appear where names of Windows users and groups may be entered. A user may be member of more than one Role, but it should be noted that Deny in one Role element overrules Allow for that element in all other Roles.

Look Up User Permissions

Provides the possibility to view combined permissions set through roles for a specific user.

A dialog with a user name field is presented when clicking the text, and a user name may be entered or selected from the drop-down list. The drop-down list displays users having logged in to the TARGIT Windows client.

After a user is selected and then clicking OK, a dialog with a Role name field to the left and a Role details field to the right is displayed. In the Role name field the names of the roles the user is a member of is displayed. At the top of the field the standard role tabs are displayed. By using the tabs and then browsing to select a specific item, the role permissions for the item selected are displayed in the Role details field.

Note that when a sub element is disallowed access, the parent element displays an information icon with the tool-tip "Sub elements have different permission".

Databases

The Databases tab can be used to select which data should be visible to members of this role. Access can be granted on database (top), cube and measure/dimension level. This is done by setting the permission level to 'Allow in this role' in the 'Permission' column for the element. Other permission types are 'None in this role', which denies access to the specific element for all users in this role and 'Deny in all roles', which denies access to this element in all roles e.g. if the user is included in more than one role. Next to each element an 'Inherit' checkbox is checked. This allows all sub elements to automatically gain the same access rights.

Default child permission

For the elements, databases, cubes and dimensions a default child permission may be set. This option makes sure that any additions e.g. a new dimension gets appropriate permission instead of uncritically allowing it in the role. The permission options include:

Permission	Description
Inherit	Added children of the element inherits the permission of the element in this role.
Allow	Added children of the element are allowed permission in this role.
None	Added children of the element are disallowed permission in this role.
Deny	Added children of the element are disallowed permission in all roles.

E.g. if a Sales cube has default child permission set to 'None' in a role and the database administrator adds a new dimension to the cube, the users in this role are automatically denied permission to the new dimension. When creating a role it is convenient to set appropriate default child permissions on as many elements as possible, such that the role accommodates later additions.

Note: By default the default child permission is set to 'Inherit', hence, if a child is added and gets the permission 'Deny' the children of this child inherits the 'Deny' permission.

Documents

The Documents tab can be used to select which folders of the Shared Documents section that should be visible to the members of this role. This can effectively be used to deny access to Analyses and Reports. The permission options are the same as in the Database tab with the extension that each element has columns for both read and write permissions. The read and write columns may be set individually such that write permissions are stricter than read permissions. The other way around is not possible. Also the default child permission may be used to control how added folders and subfolders are assigned permissions. This is done in the same way as for databases, but note that the permissions affect both read and write permissions, hence, 'Deny' default child permission denies both read and write permission.

Note: If elements, e.g. a folder, in roles are deleted , the permissions for the folder is not deleted from the roles. Therefore, creating a new folder with the same name gets the same permission as the old folder with that name.

Forced Criteria and Initial Criteria

In order to control which dimension values should be available to users the Criteria tab provides options to set forced and initial criteria. When setting forced criteria on a dimension, the dimension will have preset criteria when used in TARGIT. For example, if the forced criteria Period = 2008 and 2009 has been set in one role, members of that role may only see data for this period and no other period values are selectable - it is as if other periods do not exist in the data that the user browses. Initial criteria, on the other hand, are criteria that are preset for the data source, but may be changed or removed by the user. Initial criteria are visible to the user in the client.

Both forced and initial criteria are set by clicking the 'Add forced/initial criteria' text, then selecting a data source and the dimension where the criteria must be applied. This opens a view of the dimension members equal to the one shown in TARGIT clients. Members may either be included (green equal character) or exclude (red not equal character) by clicking them one or several times. Sometimes selections may conflict. For example if Period = 2009 has been selected, it does not make any sense to select Period != 2008 since the Period is already set to 2009 only. Conflicts like this appear in the box to the right of the selection area and may be resolved directly by clicking the text 'Resolve all conflicts' in the bottom of the box. Conflicts may also be resolved by manually changing the selections that caused the conflicts. To pinpoint the conflicts in the member list click the conflicting members in the conflicts list. An already selected member may also be located in the member list by clicking its name in the selection list over the member list.

In hierarchies selected members may not be easy to spot. Therefore an option, 'Show selected', is available in the bottom of the member list. If the link is clicked only selected members and their upper levels are shown. 'Show all' returns to the full view of all members. If a dimension level contains more than 50 members only the first 50 are shown. To see the rest click the 'Show all xx members' in the bottom of the list.

When the appropriate members have been selected the OK text must be clicked, which returns to the forced and initial criteria overview.

Export Folders

Makes it possible to select which Export folders the role provides access to. The folders allowed are presented in the Delivery |'Export to folder' drop-down list in the Schedule Job dialog.

Startup Document

Provides the possibility to set a specific document that should load at startup for the members of the role. If the startup document is set in a role, the 'Load on startup' choice on documents is dimmed for the members of the role. If 'Load on startup' is selected on a document before it is set in a role, the setting remains but have no effect. If a startup document is set in more than one role, an automatic choice is performed based first on permissions and then alphabetically. Folders are displayed first and there's a search field available at the bottom of the dialog.

Managed Documents

The Administrator can force specified documents into a Managed Documents folder on the end-user's Start page.

Role Based Menu

With the concept of the *Role based menu* you can have one group of end-users seeing one menu when they work with the TARGIT analyses, while another group of end-users will see another menu - even when working on the very same analysis.

To achieve this, you must

- **a.** Define and save the number of different menus you plan to use.
- **b.** In the analysis/analyses, insert a menu object as a *Role based menu.*
- **c.** In the management client, assign the different menus to their respective Roles.