Therefore™ Security

www.therefore.net

Therefore™

PEOPLE PROCESS INFORMATION

VERSION: 2020 - 01

Table of Contents

1. Introduction

The purpose of this document is primarily to help people ensure that their Therefore™ system is as secure as possible. In addition we have also provided some general information on security in Therefore™.

2. User Accounts

Therefore™ supports Active Directory®, Windows local security, LDAP and Therefore™ Internal users.

- See Minimum User Privileges for details on minimum required privileges.
- See Document Permissions for tips on setting security for some sample situations.

2.1 Active Directory

By default user authentication uses Windows® Active Directory® (Active DS Mode : 0 in the Therefore™ Solution Designer advanced settings).

2.2 Windows Local Security

In addition accounts from Windows local security can be used. When allowed, a user account on a Therefore™ Client can connect to the Therefore™ Server if the same user account is created on the Therefore™ Server. This is typically used in Windows workgroup scenarios.

Allow LocalComputer Accounts mode must be allowed (Therefore™ Solution Designer advanced settings).

2.3 LDAP

Then as an alternative to Active Directory users, user accounts from LDAP are also supported. The Linux server needs a domain controlled by SAMBA and clients authenticating against it must be running a supported Windows® version.

For LDAP support the Active DS Mode (Therefore™ Solution Designer advanced settings) needs to be set to 1.

2.4 Internal Users

Then finally it is possible to create users and groups directly in Therefore™.

For Therefore™ internal users Mixed Security (Therefore™ Solution Designer advanced settings) must be enabled. There are some further advanced settings that can be configured for internal Therefore™ users.

Account Lockout Duration	This is the time a user's account will remain locked after it has been locked due to too many unsuccessful login attempts. If an administrator changes the password while the account is locked, this will also unlock the account.	Time in minutes	Default is 30 minutes
Account Lockout Threshold	This locks a users account after the specified number of unsuccessful login attempts.	Number of times	Default is 5 times
Password Minimum Length	The minimum length of passwords for Therefore™ Internal users can be set. Once this setting is changed every new password has to be longer than or equal to this setting.	Integer	Minimum is 4 Default is 8
Complex Passwords	If this is active, every new password has to fulfill at least 3 of the following 4 rules: - include lower case characters (a…z) - include upper case characters (A…Z) - include numbers (0…9) - include special characters (!§%$&/(# etc.)	True False	Activated (default) Deactivated

Active Directory® or LDAP users and groups, that are associated with Therefore™ (e.g. used in a workflow), will also be listed and can be used. In addition users from Windows or LDAP can be placed in Therefore™ Internal User groups. See How do I grant certain users advanced permissions?

If a user or group name is changed in Active Directory or LDAP, then then this name needs to be changed directly in the Therefore™ database in the TABLE: TheUser.

2.5 Portal Users

Within the Therefore™ system, permissions for Therefore™ Portal users are set differently than those of normal users. Whereas a normal user is granted rights to objects and documents directly, Portal users' permissions are managed for each user individually. Portal users can only be assigned searches, and conditions must be set for each search on each user.

It is very important to set search conditions correctly to ensure that users only see their own documents. For example, at minimum a condition should be set based on a Customer ID or other unique identifier, so a user can only see documents that belong to him/her. Instructions on setting conditions can be found in the online help.

2.6 Single Sign-on

Users from Windows or LDAP
When using users from Windows, Therefore™ supports single for clients connecting via DCOM, Therefore™ XML Web Service and also Therefore™ Web Service with Internet Explorer® and Mozilla® FireFox® (with configuration).

Therefore™ Internal Users

- By default when a user logs in to Therefore™ using a mobile, web or XML connection they have the option setting automatic login to yes. They will then not have to input their details when logging in to a future session.
- Administrators can remove this option for users. The expiry time for automatic log in tokens (that are not used) can also be configured. These settings can be configured under the Advanced settings in the Solution Designer.
- While a user is logged on to a Therefore™ client the session requires a Therefore™ user license. By default a session will automatically disconnect if not used for about 60 minutes. A user can also manually disconnect, or sign out from their session. Both of these actions will immediately free a concurrent or read-only licenses for use by another user. Or, in the case of named license for use by the same user on another device. (See the Therefore™ Licensing whitepaper for more information on release times of licenses).

The number of times a named user can move their active session is restricted by two security settings under the advanced server settings: Session Move Limit and Session Move Timeout.

2.6.1 Turn Off Integrated Security

In hosted environments or environments where only Therefore™ internal users should be used, an administrator may want to prevent users connecting via XML Web Service from signing in with integrated security credentials.

To turn off integrated security, browse to C:\Program Files\Therefore directory and edit TheXMLServer.exe.config file. The highlighted lines below in yellow simply need to be deleted and then the file re-saved.

```
<!-- Uncomment the following to turn of the integrated security support-->
<!--
<add key="IntSecOff" value="1"/>
-->
```

With the IntSecOff value set to 1, users will be prompted to enter their credentials at every login, unless they choose to stay signed in.

2.7 List of allowed domains

When Therefore™ is used in an environment with multiple domains, it's possible to define the list of allowed domains in the Therefore™ Solution Designer. This prevents users from other domains from connecting to the Therefore™ Server. The list of allowed domains has no effect on local user accounts and Therefore™ internal users.

Right-click and the Therefore™ object in the Solution Designer and click on Settings / Advanced / Security / Allowed Domains to enter the list of allowed domains.

2.7.1 Systems with no domain

For example hosting environments where only Therefore™ internal users are supported.

The Active DS Mode (Therefore™ Solution Designer advanced settings) needs to be set to 3.

2.8 Listing System Users

To allow/deny viewing all users and groups, the "Read" permission in the Users and Groups node in the Therefore™ Solution Designer has to be set to allow/deny.

This permission is inherited by the "User/Read" permission of the Solution Designer's root node (Therefore). Users that have the "Read" permission in the Users and Groups or root node are able to view users and user groups (delegating workflows, assigning tasks, etc.)

An "Access Denied" error message appears when a user tries to view users or groups without permission.

3. Minimum Privileges

To minimize the damage resulting from a breach of the system, we recommend the following minimum privileges.

3.1 Minimum Privileges for Therefore™ Server Service

Scenario 1
In a domain environment the Therefore™ Server service can be run with a domain user account with the following minimum privileges.

Scenario 2
In a non-domain environment the Therefore™ Server service can be run with a local user account with the following minimum privileges.

3.1.1 Database Server

3.1.1.1 SQL Server

Server Level:
To achieve the minimum required permissions it is necessary to manually create the Therefore™ database before installing Therefore™ (typically with the name Therefore).

Security
Logins: the account needs to be added to the Logins
User mapping: The account needs to be mapped to the Therefore database.
Other settings can be left as default.

Server Properties
Permissions: The account requires the Connect SQL and the View any database permission.

Therefore Database Level:

Database Properties
Permissions: The account requires CONNECT and CREATE TABLE permissions.
Extended properties: The account requires no extended properties.

Schemas
Create a schema with name 'Therefore' and make the Therefore™ Server service account the owner of the schema.

- To be able to install Therefore™ tables into the manually created schema the Therefore™ setup has to be run with the account that will be used for the Therefore™ Server service.
- For systems where the database is not on the same server as the Therefore™ Server Service, the user running the Therefore™ Server Service needs to have enough privileges on the database.

3.1.1.2 Oracle Server

An Oracle administrator must create a schema (user account) for a Therefore™ database instance.

The administrator must grant the following rights to a schema (user account) to use the database with Therefore™:

GRANT CREATE session TO <schema name>;
GRANT CREATE table TO <schema name>;
GRANT UNLIMITED TABLESPACE TO <schema name>;

3.1.2 Windows® Active Directory®

At least READ access (A normal Domain User account meets the requirements).


This only applies to Scenario 1.

3.1.3 LDAP

At least READ access (A normal Domain User account meets the requirements).


This only applies to Scenario 1.

3.1.4 Therefore Server Machine

The Therefore™ Server service account requires full access on the following objects:

MachineKeys folder
Windows Server® 2008/Windows Vista®/Windows® 7
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys

Windows Temp folder
Make sure that the Therefore™ Server service account has full access to this folder.

Registry
HKEY_LOCAL_MACHINE\SOFTWARE\Therefore

Therefore™ installation folder
C:\Program Files\Therefore


If Therefore™ is installed to a different folder, the account has to have Read & execute, List folder contents, Read and Write permissions to that location.

Therefore system folders (Buffer, Cache etc.)
It is recommended that these are not installed on the same drive as the operating system. The Therefore™ Server service account requires full access to these folders.

3.1.5 Storage folders

The Therefore™ Server service account requires full control on all folders where documents are migrated to.

3.2 Minimum Privileges for other Therefore™ Services

The accounts for the other Therefore™ Services can be run with a local account with the following minimum privileges:

3.2.1 Therefore™ Content Connector Service

The account for the Therefore™ Content Connector service account needs connect permission to the Therefore™ database.

3.2.2 Therefore™ Conversion Service

The account for the Therefore™ Conversion service requires the same permissions as a normal user (e.g. member of the Domain User group), but with read/write permission to the Windows Temp directory.

3.2.3 Therefore™ Easy Updater Service

The account for the Therefore™ Conversion service requires the same permissions as a normal user (e.g. member of the Domain User group).

3.2.4 Therefore™ Full-text Service

Scenario 1: Therefore™ Server and Therefore™ database are on the same machine.
The account for the Therefore™ Full-text service must be run with the Local System account.

Scenario 2: Therefore™ Server and Therefore™ database are on different machines.
The Therefore™ Full-text service must run with same account as the Therefore™ Server service.

3.2.5 Therefore™ MFP Manager Service

The account for Therefore™ MFP Manager Service requires access to the machine on which the Therefore™ Server is running (DCOM level).

3.2.6 Therefore™ Replication Service

The account for the Therefore™ Replication Service or the internal Therefore™ user account, set for the service (link) requires read permission in Therefore™.

3.2.7 Therefore™ Services for Connector to Microsoft® Exchange Server

Please see the documentation for the Therefore™ connector for Microsoft® Exchange Server.

3.2.8 Therefore™ Web Service

The account for Therefore™ Web service requires access to the machine on which the Therefore™ Server is running (DCOM level).

3.2.9 Therefore™ XML Web Service

The account for Therefore™ XML Web service requires access to the machine on which the Therefore™ Server is running (DCOM level). Unsecure endpoints should not be used in the production environment.

3.3 Minimum User Privileges

Therefore™ has an extensive rights access system which is managed via the Therefore™ Solution Designer. Objects are displayed using a tree-view, which enables rights to be given and inherited at various levels, including folders, sub folders, category, sub-category and then right down to single document level using the Therefore™ Viewer. Integration with Windows® integrated security (Active Directory®, or local security), and also LDAP, simplifies selection of users and groups. In addition, however, Therefore™ User Management allows independent users and groups to be created within the Therefore™ system. By default permissions are passed down from a parent to a child object, but inheritance can of course be broken where required.

3.3.1 Therefore™ Object

The minimum required permissions for a user of the Therefore™ system is User/Read. To edit documents they would also need User/Write.

3.3.2 Therefore™ Server Object

In the case of a multi-server environment, the tree structure also contains a Server object. The minimum permissions for a user is User/Connect

3.3.3 Categories Object

The categories object controls access to the document repository.

Customizable permission sets, which group related rights, further simplifies the process of rights assignment. The table below details all permissions. Furthermore, Therefore™ offers a rights server which makes it possible to implement an external rights server and enforce customer specific access rules.

The minimum permission set for a user to find documents is the Read set.
For editing documents they would require the Write set.
For deleting documents they would need the Delete set.
For creating/editing folders and categories they would need the Admin set.

However, it is possible to further refine the users permission by checking the Advanced permissions check box, which then displays the full permission list as detailed in the table below.

See http://www.therefore.net/help/2017/en-us/sd_r_theobject_settings_permissionsets.html for more details.

3.3.4 Keyword Dictionary Object

For a user to simple use a keyword dictionary in a category index field for which they have permission, no extra permission are required here. To restrict a users right on a keyword dictionary on a category for which the user has rights, the index field permissions can be restricted.

3.3.5 Referenced Tables Object

For a user to simply use a Referenced Table in a category index field for which they have permission, no extra permissions are required.

3.3.6 Cross Category Template Object

For a user to simply use a global cross category template that has been created in the Therefore™ Navigator, they only require rights to the categories involved. For the user to be able to create their own cross category searches in the Navigator with a specific template, they would require Read permission.

3.3.7 Users and Groups Object

No permissions are required here for a general user.

3.3.8 Capture Client Profiles Object

For a user to use a Capture Profile in the Therefore™ Capture Client, they require Read permission.

3.3.9 Document Loader Object

For a user to use a Document Loader Profile, they require Read permission.

3.3.10 Workflow Object

The minimum permission for a user to take part in a workflow is the Participate permission.

3.3.11 Device Object

General users need no permissions here.

3.3.12 Storage Policy Object

General users need no permissions here.

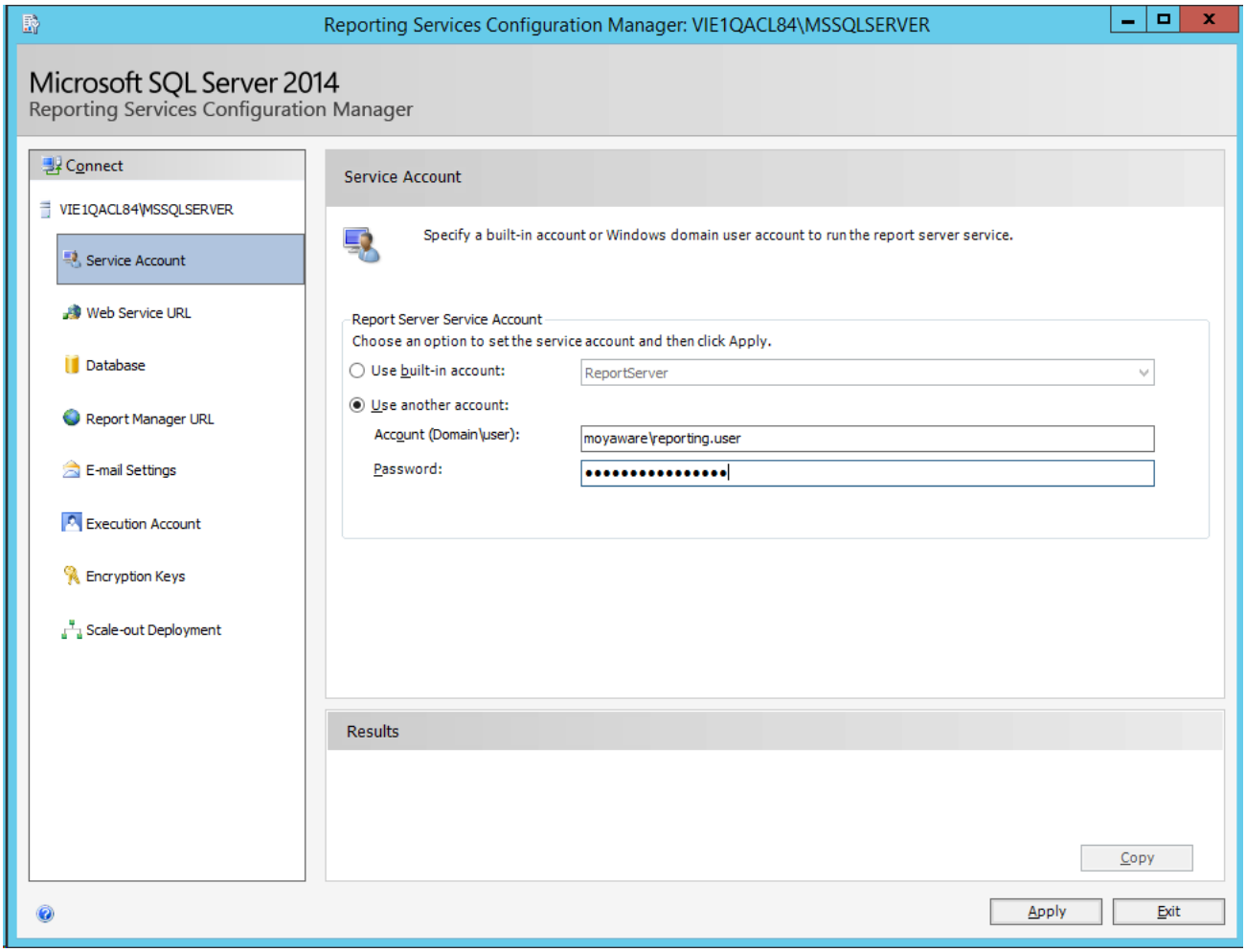
3.3.13 Retenion Policy Object

General users need no permissions here.

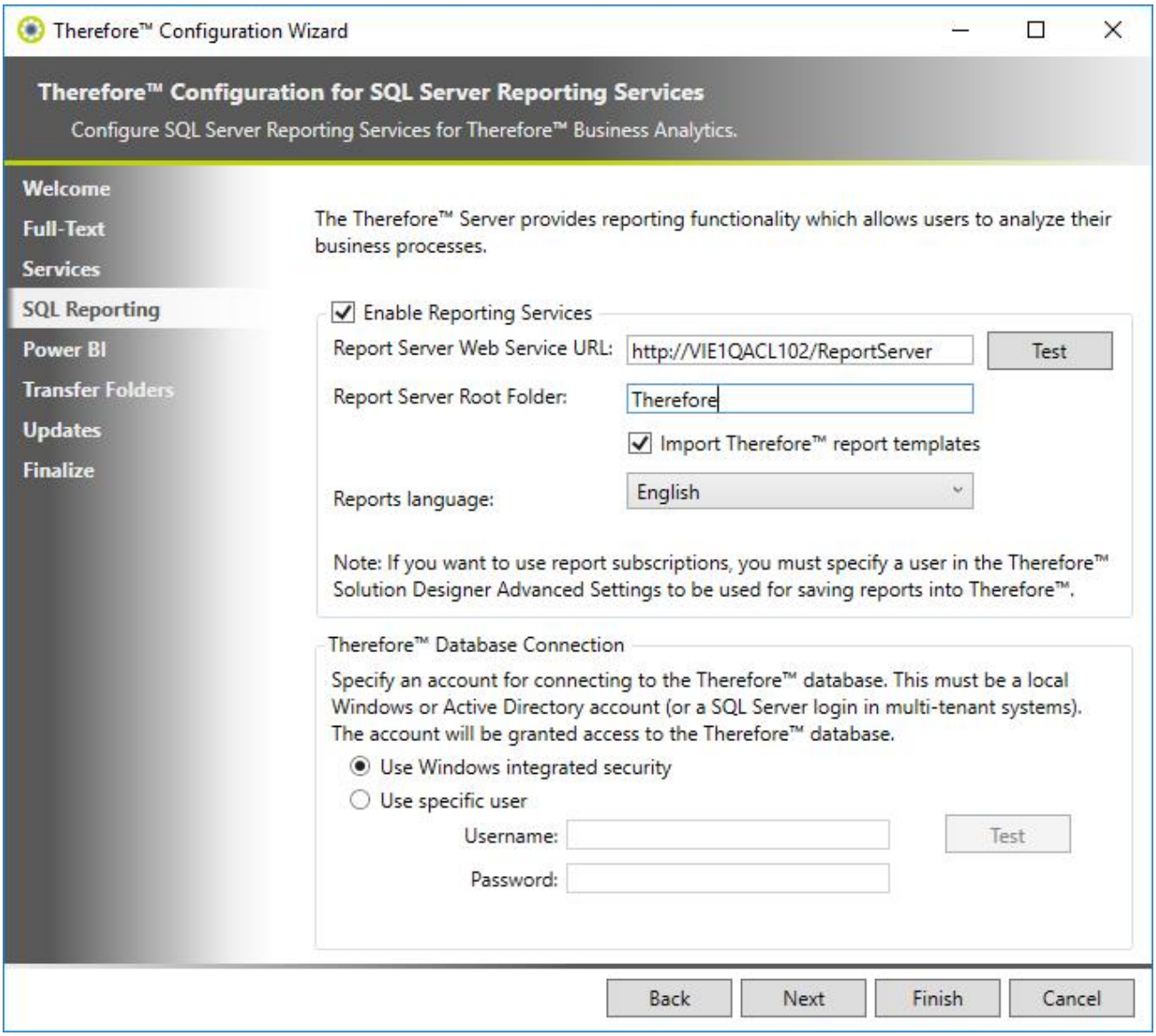
3.4 Minimum Priviliges for Reporting

Therefore's Reporting feature also allows report subscriptions to be defined. This requires defining the account that should be used to save automatically generated reports in Therefore™. We recommend creating an Active Directory user account specifically for this purpose. The minimum permissions for this account are Write access on Therefore's Reports category, and SELECT access on the Therefore™ database.

This user's credentials must be entered while configuring the Microsoft SQL Server Reporting Services (see the Installation Guide for more details).



This user's credentials should also be entered as the datasource user in the Configuration Wizard's Reporting tab.


Therefore™ Configuration Wizard
Therefore™ Configuration for SQL Server Reporting Services
Configure SQL Server Reporting Services for Therefore™ Business Analytics.
Welcome
Full-Text
Services
SQL Reporting
Power BI
Transfer Folders
Updates
Finalize
The Therefore™ Server provides reporting functionality which allows users to analyze their business processes.
Enable Reporting Services
Report Server Web Service URL:
http://VIE1QACL102/ReportServer
Test
Report Server Root Folder:
Therefore
Import Therefore™ report templates
Reports language:
English
Note: If you want to use report subscriptions, you must specify a user in the Therefore™ Solution Designer Advanced Settings to be used for saving reports into Therefore™.
Therefore™ Database Connection
Specify an account for connecting to the Therefore™ database. This must be a local Windows or Active Directory account (or a SQL Server login in multi-tenant systems). The account will be granted access to the Therefore™ database.
Use Windows integrated security
Use specific user
Username:
Password:
Test
Back
Next
Finish
Cancel

4. Storage of Therefore™ Documents

4.1 Managing External Audit Permissions

Immediate Access (Z1)
An auditor is given direct access to the system and provided with the appropriate access permissions. A Therefore™ user can be created for the auditor with appropriate permissions. The auditor can then access the documents at the company or via the Internet using the Therefore™ Navigator or Therefore™ Web Access.

Indirect Access (Z2)
An auditor can request that certain documents be retrieved from the system and made available for inspection. In Therefore™ an employee with the appropriate permissions can search for documents using standard searches or predefined search masks, and then allow the auditor to inspect them live on the system.

Mobile Access (Z3)
An auditor is provided with a Therefore™ Client software and permission to take the required documents offline. The required documents are taken offline and user permissions allow the auditor to view these documents.

4.2 Therefore™ Signature

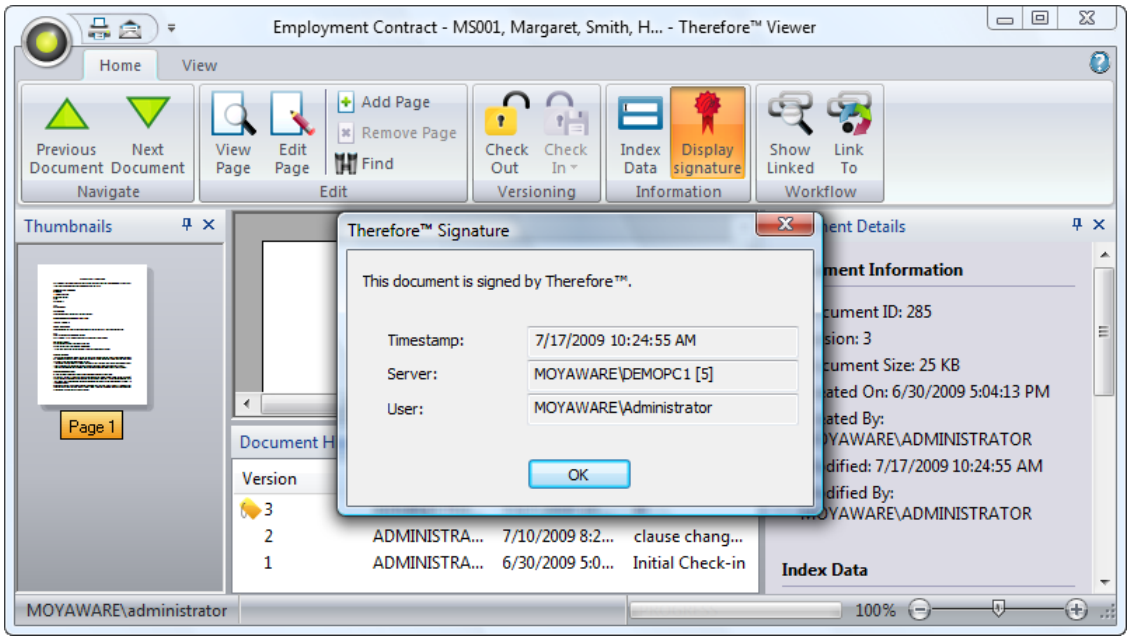
Therefore™ signs every document immediately after receiving it. When a user retrieves a document, the signature is verified by Therefore™ to guarantee that it is the original. Even the customer's system administrator cannot sign a changed document. The signature comprises the following data, which cannot be changed without invalidating the signature.

- Hash value for all files of the document (tiff, pdf, word, …)
- Timestamp
- Name of the Therefore™ Server
- ID of the used key
- Public key
- Username who triggered the archive operation
- Document number
- Alert (in case of Removed Signature or Invalid Timestamp) This is set by the Therefore™ Server.

The signature is stored within ".thex" document and is created using a standard signing algorithm which computes the SHA 256 Hash and then encrypts this hash value with the RSA algorithm. Therefore™ generates an RSA key using the Microsoft® Crypt API (length is configurable, default=800 bit). The private key is stored in the operating system only and is not exportable (i.e. no one can export the key and store it for later abuse). A key-pair is re-created every 30 days (time configurable) and the old private key is deleted, making it impossible to sign a document with the old key. The public key is stored in the Therefore™ database and is used during signature verification. After a document is retrieved the client verifies that the signature is valid. If the signature is not valid, an error message will be shown to the user.

If valid, the SHA 256 Hash values for individual files within the document are re-computed and verified. If one of the hashes is invalid then the user is notified that the document is corrupt. Contact support@therefore.net for help recovering corrupt documents.

Users with sufficient rights can check a document out, edit it, and check it back in as an edited version. This edited version is saved as a new document version with a new digital signature. Old document versions together with their digital signatures are retained and can be inspected using the Therefore™ Viewer.



These digital signatures should not be confused with signing a PDF with a personal signature or signature via a DTM provider.

4.3 Composite Files

- Composite files are compliant with Open Packaging Conventions (OPC), documented in the ISO/IEC 29500 and ECMA 376 standards.
- Used by Microsoft® Office (.docx, .xlsx, .pptx, …)
- This allows a single document to consist of multiple single files (e.g. a Microsoft Word document and Microsoft Excel® sheet can make up one Therefore™ composite document).
- Files greater than the Large File threshold are stored as links (the threshold is 1024Mb but can be changed under Advanced settings in the Solution Designer).
- Index information and digital signatures form part of the composite file which carries the extension ".thex".

In the case of the Therefore™ database being lost, without a backup, it is possible to recover information from the stored composite documents. But, this is a complicated process and there are limitations on what can be recovered. Hence it is recommended that proper backup procedures be followed.

4.4 Blocked and Allowed Extensions

List of Blocked Extensions
To prevent users from saving potentially dangerous files to the system, a number of default extensions are blocked. In current versions of Therefore™, these include:

ade; adp; app; asax; ascx; ashx; asmx; asp; aspx; axd; bas; bat; browser; cer; chm; cla; class; cmd; cnt; com; compile; cpl; crt; cs; csh; der; dhtml; dll; exe; fxp; gadget; grp; hlp; hpj; hta; htm; html; hxt; inf; ins; isp; its; jar; jhtml; js; ksh; lnk; mad; maf; mag; mam; maq; mar; mas; master; mat; mau; mav; maw; mda; mdb; mcf; mde; mdt; mdw; mdz; mhtml; msc; msh; msh1; msh2; mshxml; msh1xml; msh2xml; msi; msp; mst; ocx; ops; osd; pcd; phtml; pif; pl; plg; prf; prg; pst; reg; rhtml; scf; src; sct; shb; shs; shtml; xhtml; zhtml; ps1; ps1xml; ps2; ps2xml; psc1; psc2; tmp; url; vb; vbe; vbs; vsmacros; vsw; ws; wsc; wsf; wsh; xbap; xnk.

List of Allowed Extensions
To restrict the file format in which documents are saved to Therefore™, it's possible to set a white-list of allowed extensions in the Therefore™ Solution Designer under Settings / Advanced / Security / Allowed extensions.

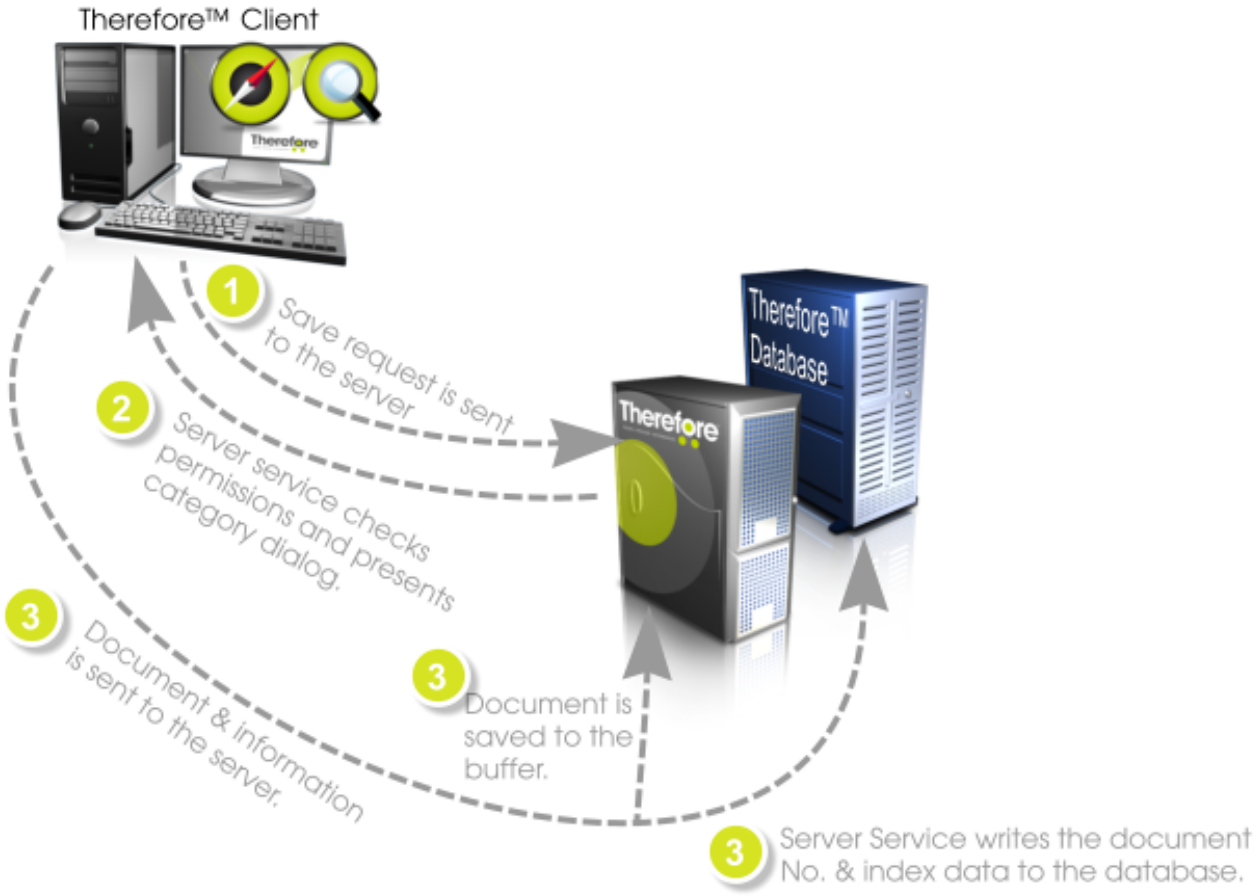
For best security it is recommended to configure a white list explicitly listing all allowed extensions, e.g. *bmp; docx; dotx; gif; jpg; pdf; png; pptx; tif; txt; xlsx; xltx*; the user can add any other secure file types to save into their system.

This will prevent users from saving documents to the system in any other format besides those in the list. Note that this list overrides the list of blocked extensions. This setting may also be useful for compliance reasons.

4.5 Saving to Therefore™

Documents can be saved to Therefore™ and can either be paper based and scanned via DR scanners or MFP devices or they can be electronic documents already saved to a PC. Irrespective of their origin, the saving process is the same:

1. The save request is sent to the Therefore™ Server.
2. The Server service checks permissions and presents the category dialog.
3. Once the category and index information have been entered, the information is sent to the Server. The document itself, including the digital signature, is saved to the Buffer folder and the document information is written to the database.



Documents remain in the Buffer until the migration schedule triggers a migration policy which moves documents from the buffer to storage. It is important to ensure that the "waiting" time of documents in the buffer be kept as short as possible, and to regularly backup the buffer folder and all its sub-folders.

Therefore™ allows for, and recommends, the use of both primary and backup storage. The advantage of double storage is that it replaces the need for the classic backup scenario. Therefore™ verification tools enable administrators to ensure that all documents are accessible on primary and backup media. In the case of the primary storage location being corrupted or destroyed (e.g. disk crash), it can be repaired or replaced using the backup. Modern RAID/NAS/DAS/SAN devices, network or local, are well suited as storage devices. In addition Therefore™ supports NetApp® SnapLock® which allows WORM storage. Some storage devices have internal backup technology and when used, could replace a Therefore™ backup storage.

Security of documents stored on external devices is ensured by requiring that only the Therefore™ Server service needs access to these locations. All normal users can be barred from accessing the documents directly from these storage locations.

4.6 Transfer Folders

Starting from Therefore™ 2014, transfer folders have been implemented to improve the speed of saving and retrieving large files. Transfer folders can be defined for clients connecting via DCOM, XML Web Service and Therefore™ Web Access.

Security is one of the most important aspects to consider when configuring transfer folders. Since these folders may contain confidential files, we recommend restricting access to them by keeping permissions to a minimum, see the online help.

4.7 Document History

Any changes to a Therefore™ document result in a new version being created. This includes:

1. Adding files to a document.
2. Adding annotations to a page within the document.
3. Editing the contents of any of the files within a document.

If check box Create a new document version on index data change is checked (Cateory->Properties->Advanced), then a new version will also be created when index data is changed.

All old versions remain accessible via the document history pane in the Therefore™ Viewer. In addition check-in comments can be activated to record what changes a user makes. The retention policy feature makes it possible for administrators to delete old document versions should this be required.

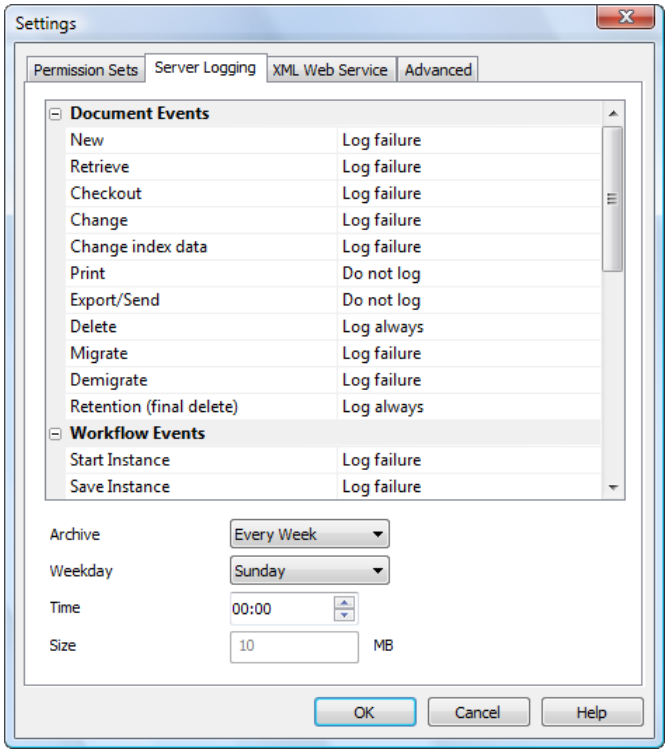
4.8 Document Retention

Therefore™ retention policies allow documents to be permanently deleted from both the database and the storage locations. Retention policies are defined in the Solution Designer based on the date of creation, modification or a date stored in an index field. The Retention feature in the Therefore™ Console allows administrators to search categories for documents that exceed the retention period. These documents can then be checked and confirmed for deletion. The server service will then delete these documents from the database and write them to the retention queue. The next time migration occurs, these documents will be permanently deleted from all storage media.

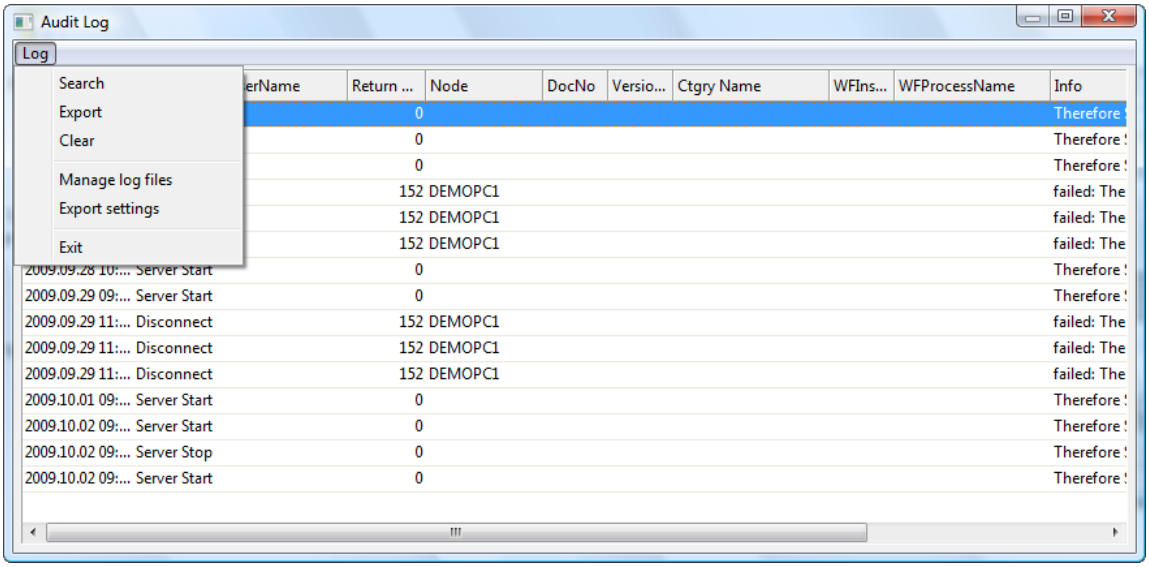
4.9 Audit Trail

The console makes it possible to check what a user has been doing on the Therefore™ system or to see what has happened to a particular document. A permanent audit trail is written to the Therefore™ system log as events occur. When a current log file reaches a defined limit it is then saved to the Logfiles category in Therefore™ system. For more details see the Administration Manual.

Events to be logged can be configured in Solution Designer under Server Logging. See the Administration Manual -> Solution Designer for a table detailing the individual events that can be logged.



Log files can then be loaded, reports can be created and exported in the Therefore™ Console.



To prevent documents being printed or exported in an offline state, and hence without logging, two registry entries should be entered and set to "1" on all Client PCs.
HKLM\Software\User\Therefore
AbortExportOnLogFail
AbortPrintONLogFail

4.10 Document/Case Permissions

During installation an administrator and user group must be defined. These two groups are then added by default to Therefore™.

The Admin group will by default have admin rights on the Therefore™ object and all objects below.

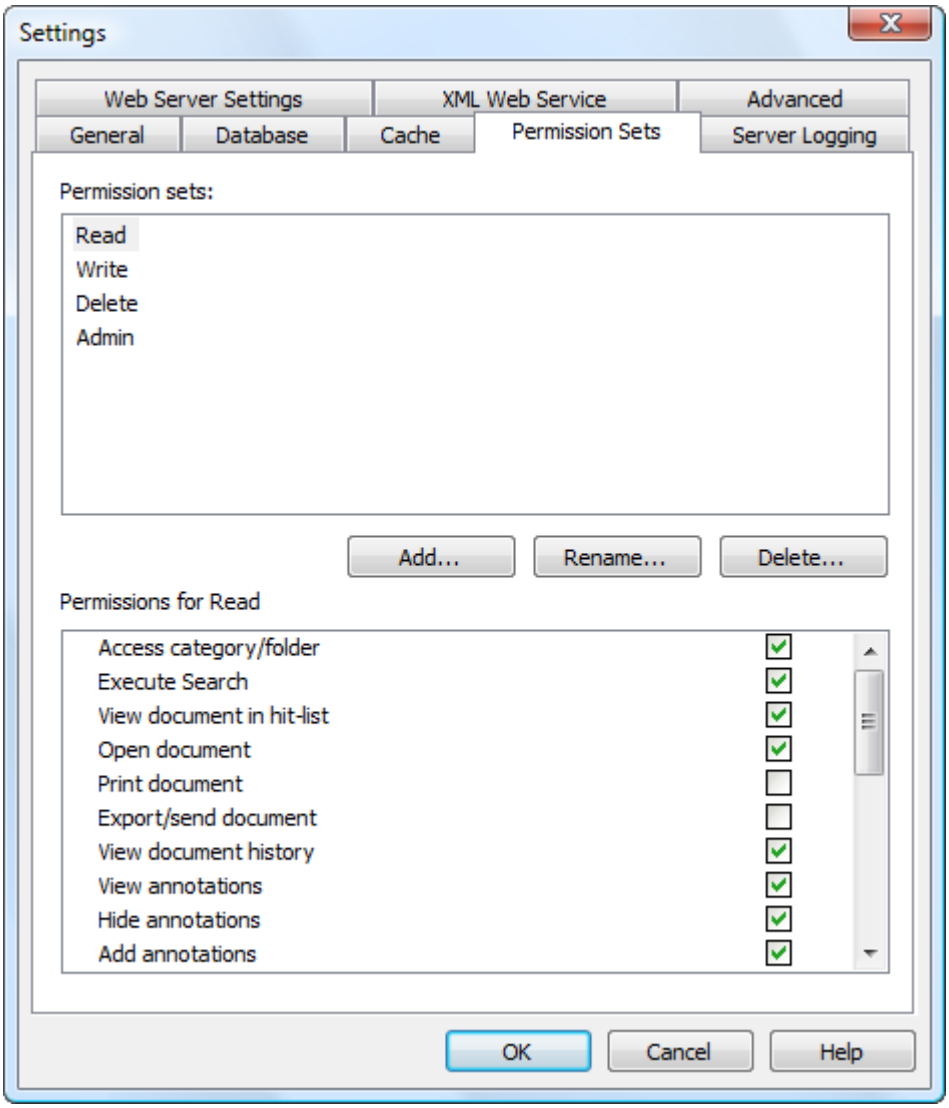
The User group has typical read/write permissions on the Therefore™ object and objects below. Note however, that on the Category object, in addition to the Read and Write permission sets this default User group also has one permission from the Delete set: "Delete document pages" and one from the Admin set: "Retention policy" (which allows a user to remove an individual document from a retention policy).

See Minimum User Privileges for details on minimum required privileges.

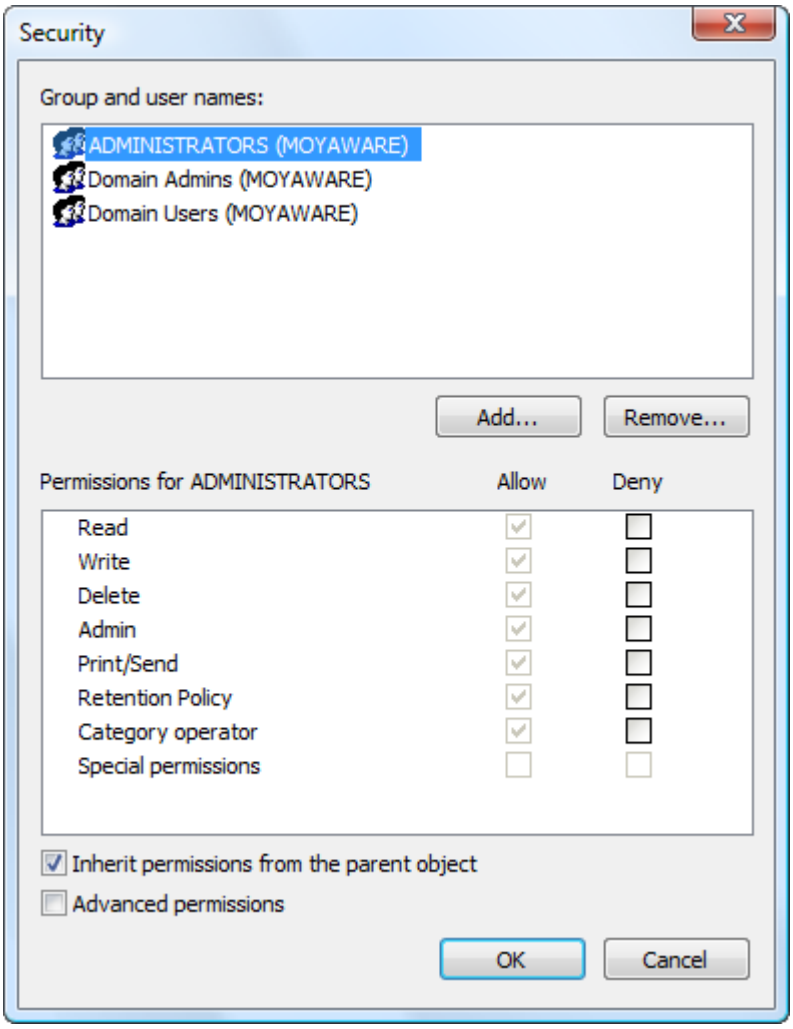
By default permissions are inherited by objects lower down in the hierarchy, but the inheritance can be broken if required.

4.10.1 How do I set advanced permissions?

To make permission administration easier, permissions have been grouped into sets. Administrators can then configure permissions on categories by defining which user has permissions for the Read, Write, Delete and Admin set instead of managing the entire list of individual permissions. These permission sets are configurable and can be changed to suit a customers requirements. New sets can be added, existing ones deleted, renamed or changed.



Permissions for documents can be set on various levels and is then by default inherited by objects below. For example a folder could be created. Then right-click and choose Security...



If the folder should have different permissions than its parent, deselect the Inheritance check box. Clicking on Advanced permissions will expand the permissions sets and show all available permissions.

If you need permissions in addition to those listed, the Therefore™ Rights Server can be used. Please contact support@therefore.net for more information.

4.10.2 How can I give only selected users certain permissions?

Simply create an internal Therefore™ users group (e.g. Advanced permissions). Then add the required users to this group and then add this group where advanced permissions are required.

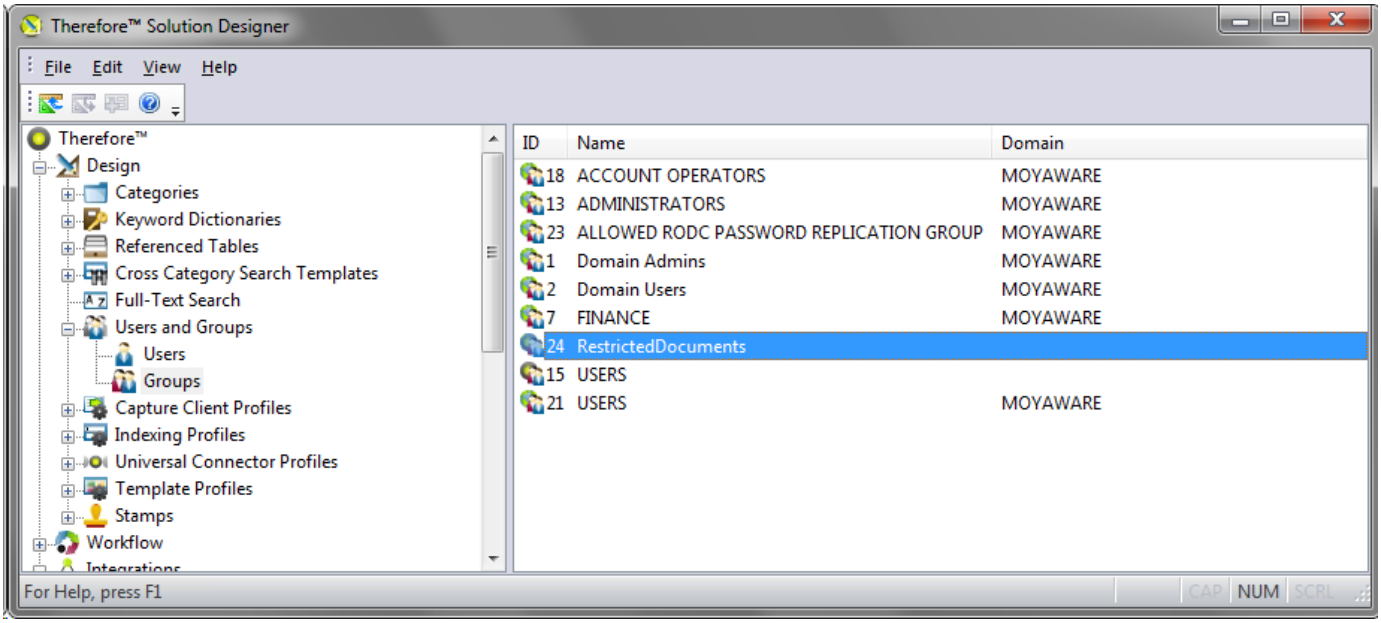
Note these can also be users from Windows or LDAP.

4.10.3 How do I restrict rights on a certain document(s)?

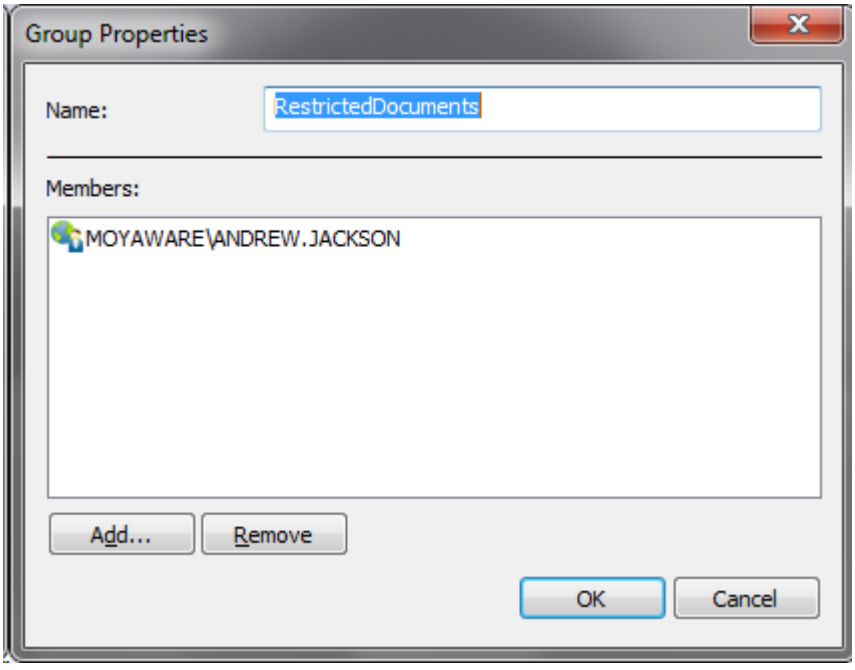
This could of course be done on a per document level, by opening the document in the Therefore™ Viewer and then setting the permissions.

But, it could also be done using subcategories.

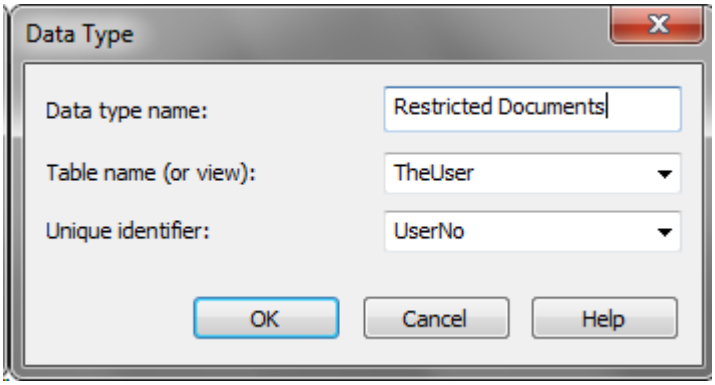
1. Create an internal Therefore™ users groups (e.g. Restricted documents)



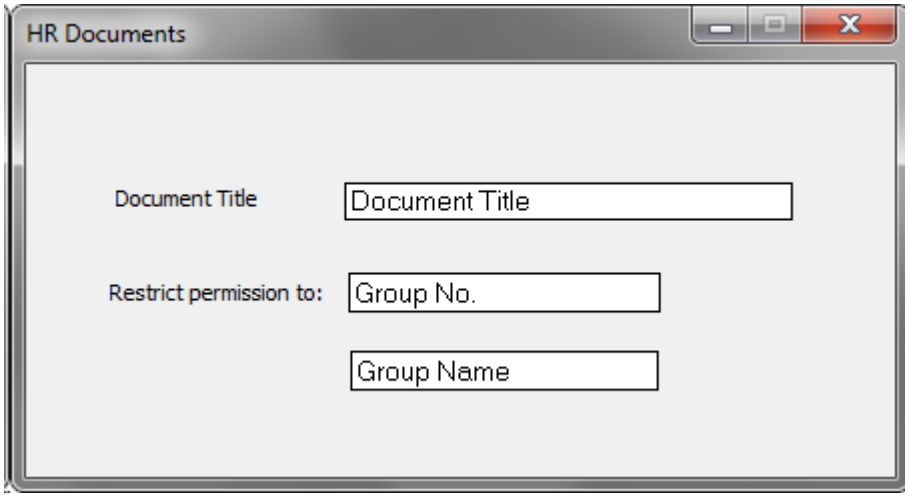
2. Add the users who should have permissions to this group. Note: these can be from Windows, LDAP or Therefore™ Internal users.



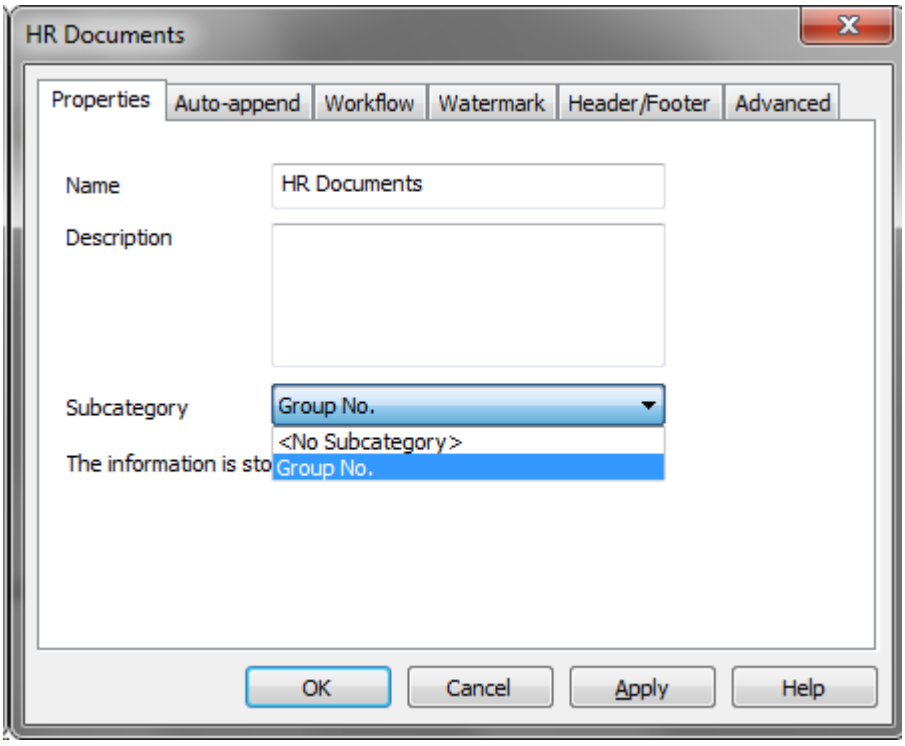
3. Create a referenced table that links to the Table : TheUser, set the Unique identifier as UserNo.



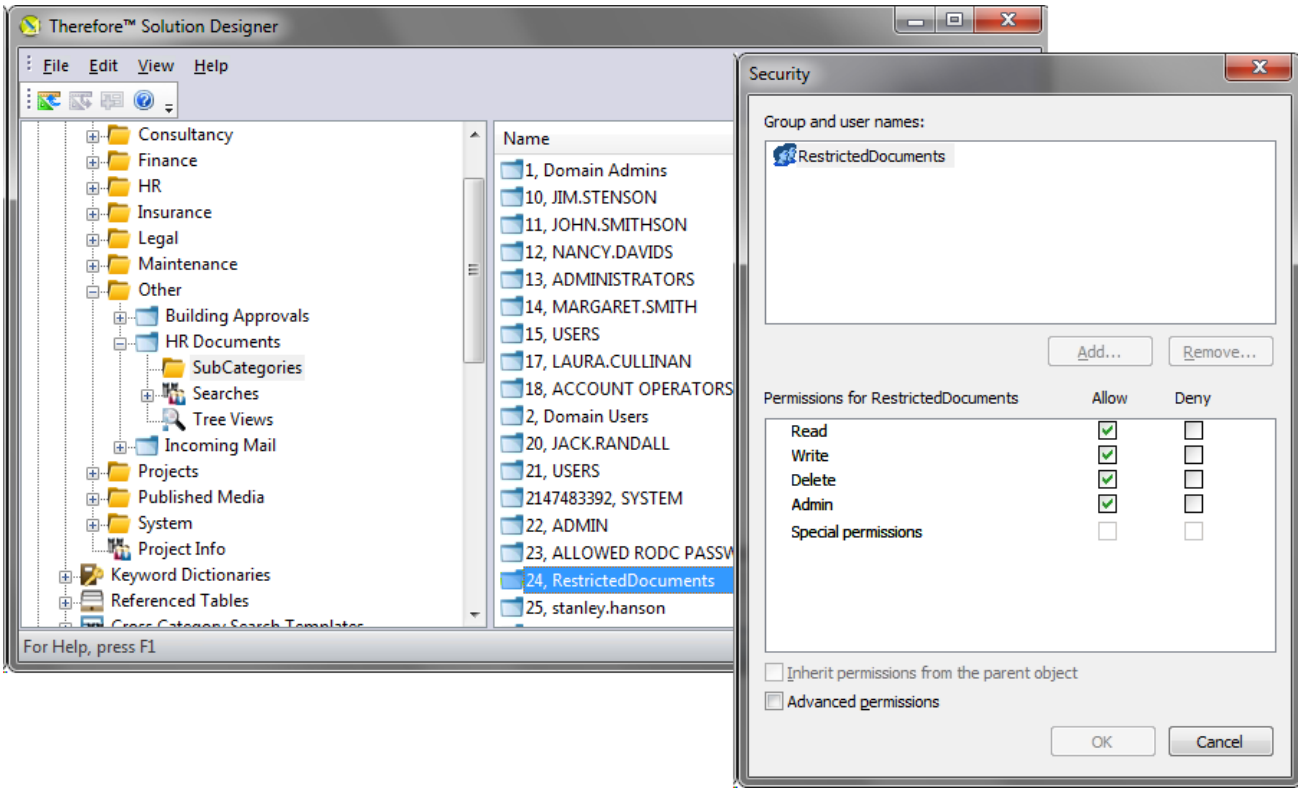
4. Add a Primary field to the category that uses this Referenced table. Also add a dependent field so that you can see the Name of the group.



5. Under the category properties define a subcategory for the Primary field. Then save the category.



6. Click on the Subcategories folder and then on the group we created earlier. Remove inheritance and then add the internal group that should see the documents.



7. Now when a document is saved to this group and the permission is set to Restricted HR documents, only users in this group will be able to see the documents.

4.10.4 How do I grant rights on a certain case?

Permissions can be granted to cases in a similar way as documents.

In the Therefore™ Navigator hit-list, right-click on a case and select Security... from the context menu. Set the permissions for individual users or groups as required.

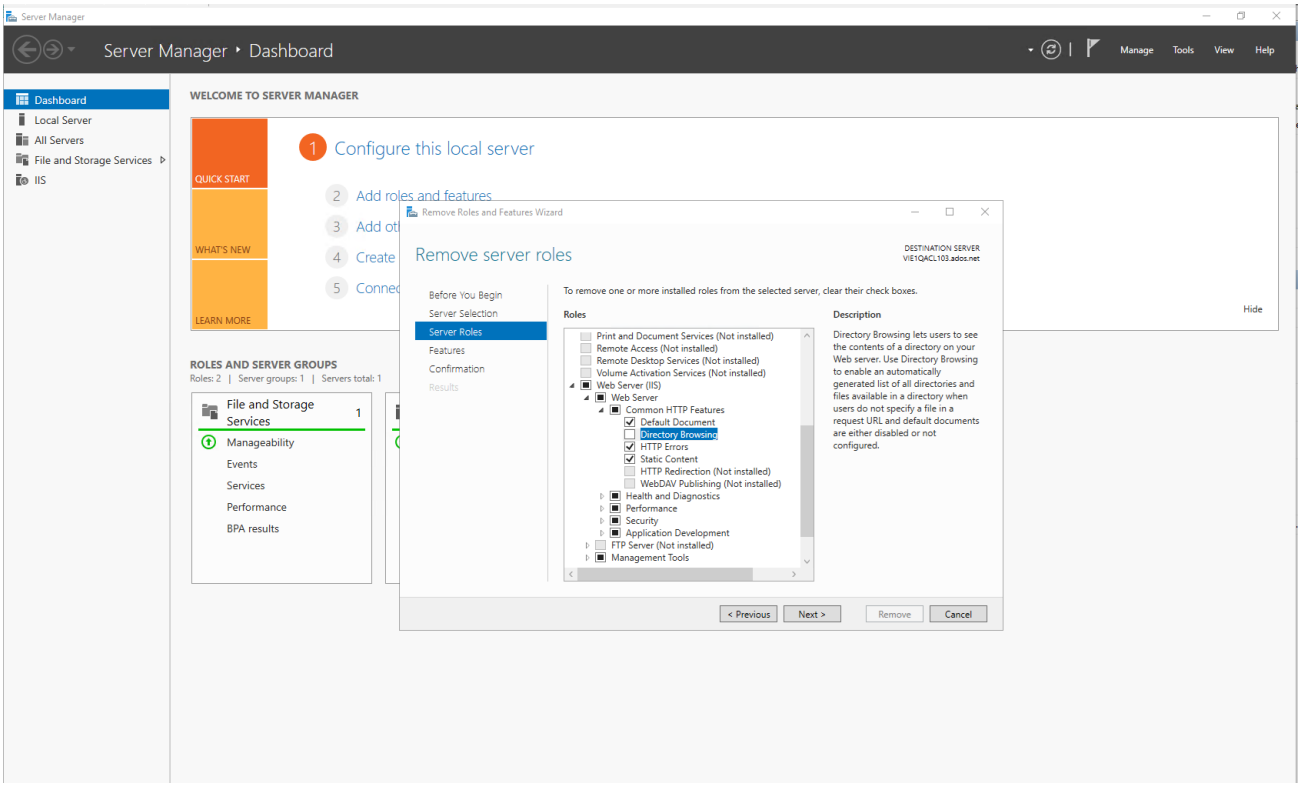
Note that the documents contained in a certain case are also not visible to users without the correct permissions. Permissions are also automatically applied on a case document level, so the documents are not available to non-authorized users even if they perform a direct query on the case category from the Therefore™ Navigator.

5. Web Security

5.1 Microsoft® IIS

To ensure that the content of the directories cannot be listed with a browser, make sure that Directory Browsing is not installed on Microsoft® IIS .

1. Open Windows® Server Manager and expand the Roles object. Select Web Server (IIS) and scroll down and click Remove Role Services (right-hand column). In the Remove Role Services dialog, make sure that Directory Browsing is not selected.



If directory browsing is required, for example, by another application, then it can be deactivated just for Therefore™ Web Access. Go to Internet Information Services (IIS) Manager and under Default Web Site click on TWA. In the options in the center pane open Directory Browsing and then click Disable in the right-pane.

5.1.1 Web.Config

To prevent hackers gaining control over the server by executing server scripts embedded in Therefore™ documents, the following settings should be configured in the web.config files, by default in the folder C:\inetpub\wwwroot\TWA.

1. For Therefore™ Web Access make sure that following section is included in the <configuration> section of the web.config file in the TWA directory.

```
<!-- BEGIN: CLIENT SETTINGS - PREVENT ASP.NET SERVER SCRIPTS -->
   <location path="Client/WebCache">
     <system.web>
       <compilation>
         <assemblies><clear /></assemblies>
         <buildProviders><clear /></buildProviders>
         <expressionBuilders><clear /></expressionBuilders>
       </compilation>
     </system.web>
   </location>
 <!-- END CLIENT SETTINGS -->
```

2. For Therefore™ MFP Print make sure that following section is included in the <configuration> section of the web.config file in the TWA directory.

```
<!-- BEGIN: MFP SETTINGS - PREVENT ASP.NET SERVER SCRIPTS -->
      <location path="Mfp/WebCache">
        <system.web>
          <compilation>
            <assemblies><clear /></assemblies>
            <buildProviders><clear /></buildProviders>
            <expressionBuilders><clear /></expressionBuilders>
          </compilation>
        </system.web>
      </location>
    <!-- END MFP SETTINGS -->
```

To prevent an endless redirection loop, which can cause high sever load (denial of service), being triggered, make sure that the following entry is included in the "web.config" file by default in the folder C:\inetpub\wwwroot\TWA.

```
<system.web>
...

   <customErrors mode="RemoteOnly" defaultRedirect="error.html" /><!--CUSTOM ERROR
   MESSAGES (mode="On"     or "RemoteOnly" to enable friendly error message, "Off"
   to disable)-->

...
...
</system.web>
```

To make sure that form data which was entered by a user cannot be read by hackers, ensure that the following entry is included in the web.config file in the by default C:\inetpub\wwwroot\TWA\Client directory:

```
<system.web>

...
...
```

```
<pages controlRenderingCompatibilityVersion="3.5" clientIDMode="AutoID"
viewStateEncryptionMode="Always">

...
...
</system.web>
```

5.1.1.1 Prevent Frameable Response

To prevent frameable response the following settings should be activated in the web.config files, by default in the folders

- C:\inetpub\wwwroot\TWA
- C:\inetpub\wwwroot\TWA\Client
- C:\inetpub\wwwroot\TWA\Portal

To do this remove the comment (highlighted characters below) in each web.config file. Then restart IIS.

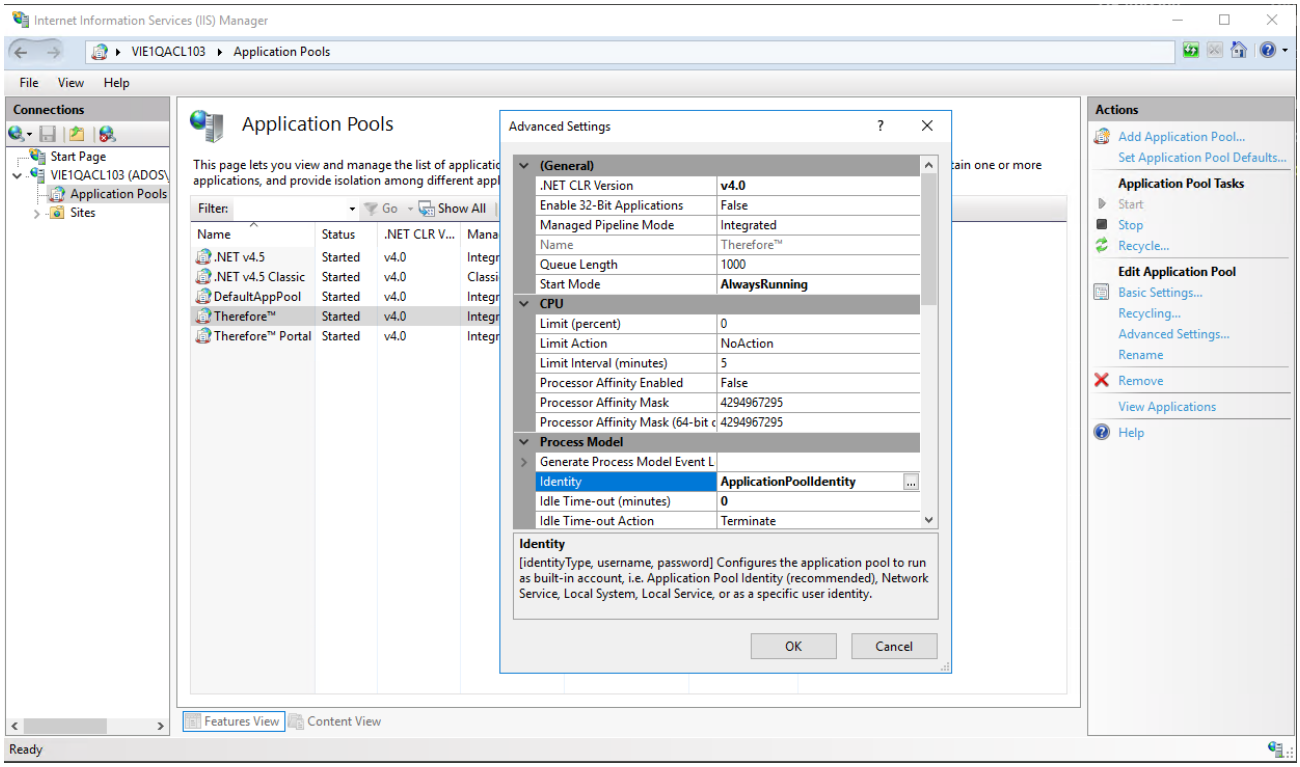
```
<!--add name="X-Frame-Options" value="SAMEORIGIN" /-->
```

5.1.2 Therefore™ Web Application

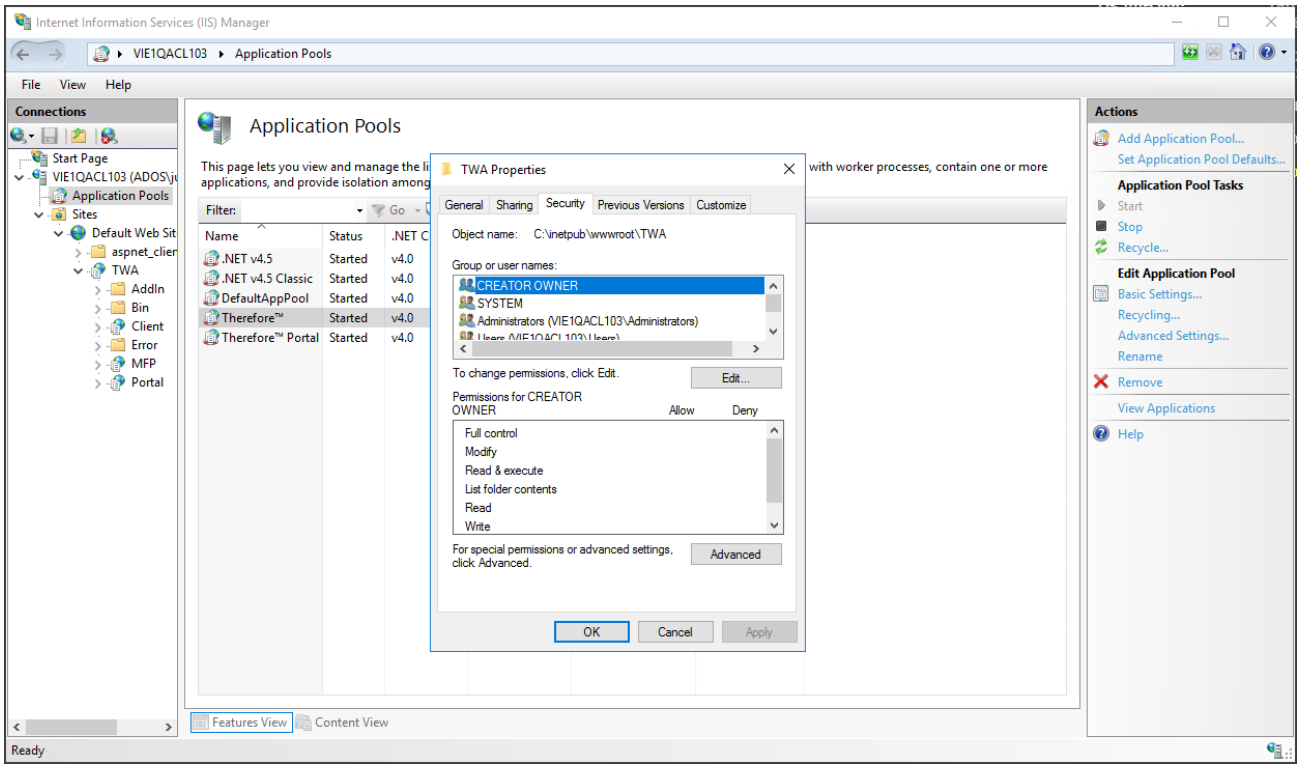
To ensure that the Therefore™ Web Access application has minimum required permissions on the server run the Best Practices Analyzer for IIS which is included in Windows® Server 2008 R2. The BPA will then report "Application pools should be set to run as application pool identities".

To solve this issue the following can be done:

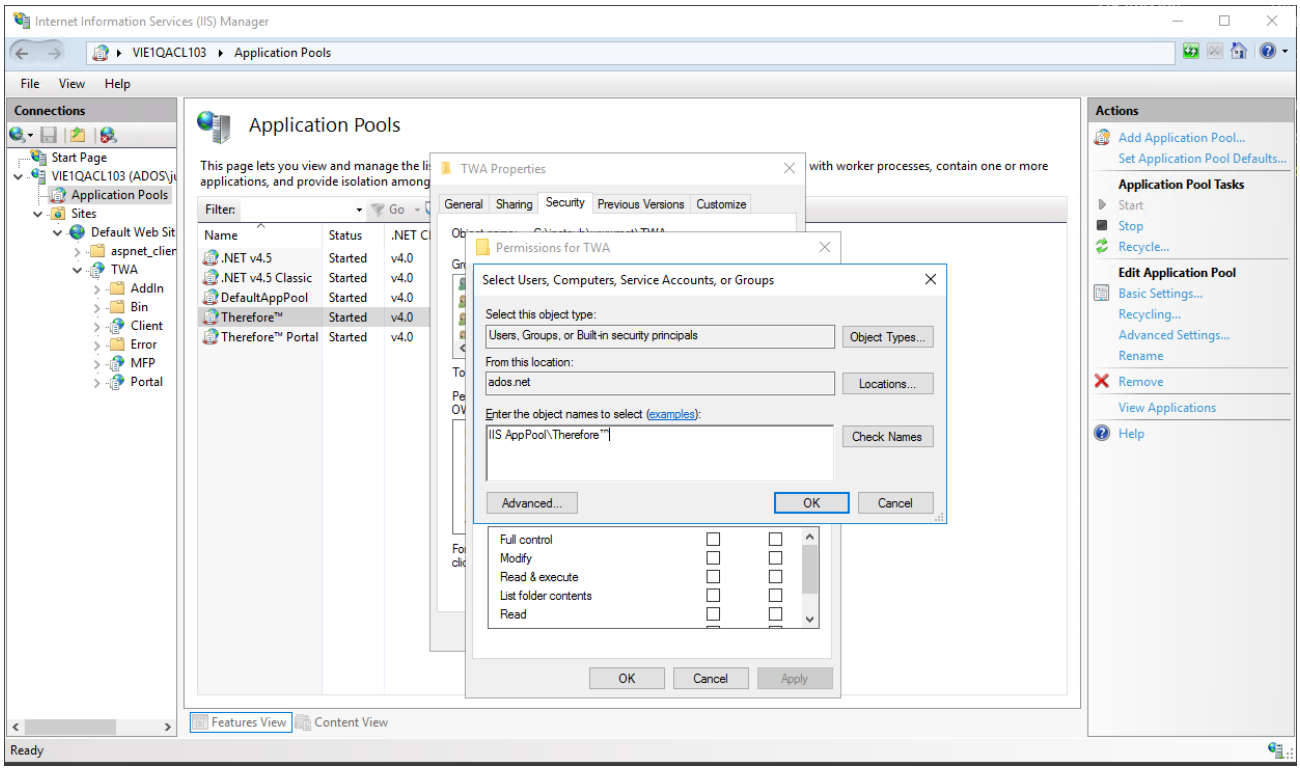
1. Go to Internet Information Services (IIS) Manager under Application Pools right click on Therefore™ and choose Advanced Settings... Set the application pool's identity to ApplicationPoolIdentity.



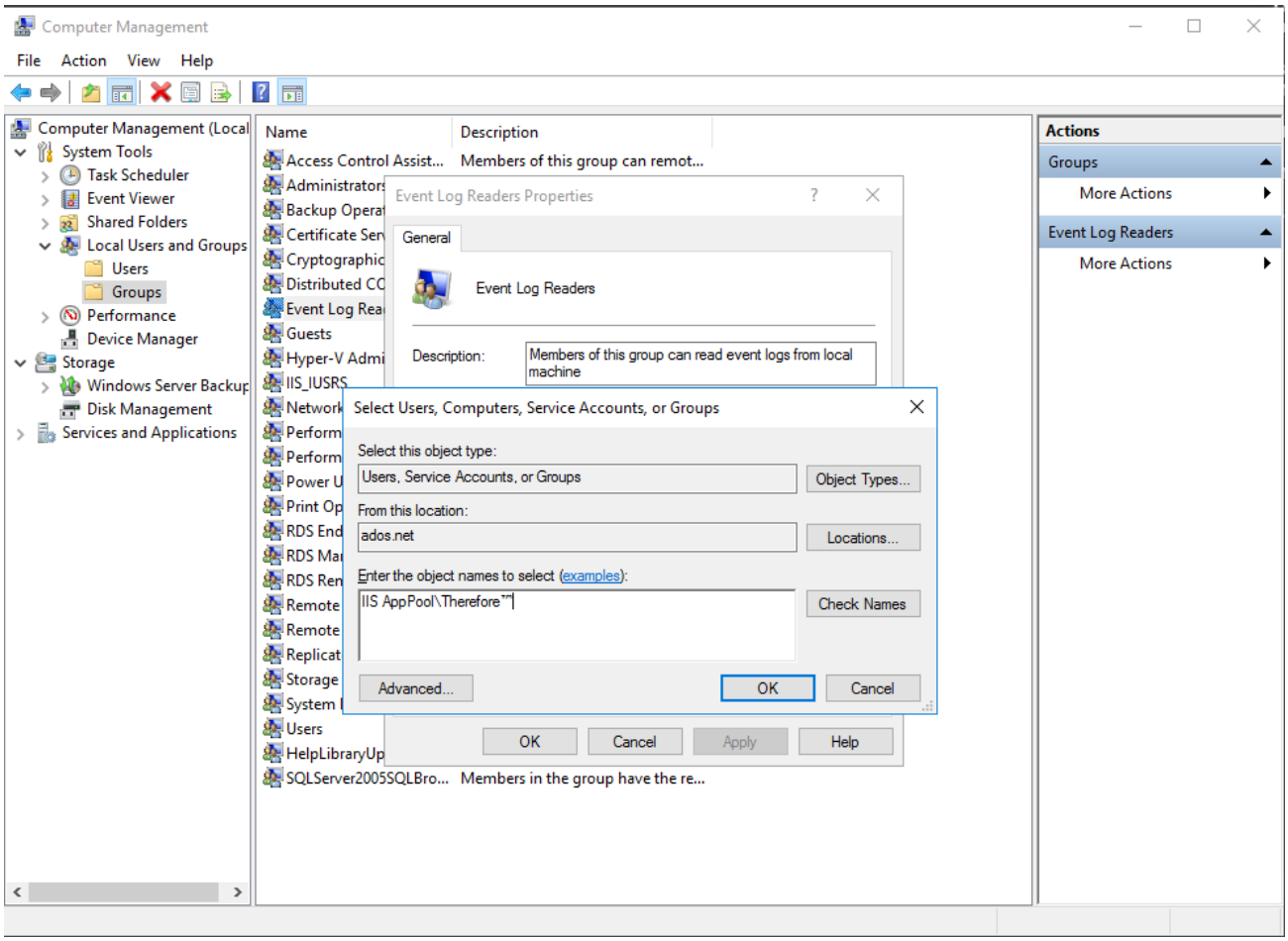
2. Go to Sites then expand Default Web Site, right-click on TWA, select Edit Permissions... and then select the Security tab.



3. Add the user for the site's application pool. By default the application pool is named Therefore™ and in this case the user would be "IIS AppPool\Therefore™" (the pool user is located on the server itself, so you have to set the Location to <servername>).



4. Grant the user Read & Write permissions only.
5. Add the IIS AppPool\Therefore™ user to the Distributed COM Users group. If you get an access denied in event log, please see the Therefore™ Installation Guide for information on DCOM configuration.
6. Create the eventlog source by executing the Powershell statement: *New-EventLog -Source 'Therefore Web Access' -LogName 'Application' -MessageResourceFile 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\EventLogMessages.dll'*
7. Add the IIS AppPool\Therefore™ to the local 'Event Log Readers' group.



8. Restart Therefore™ services.
9. Restart Microsoft® IIS.

5.1.2.1 Removal of HTTP Response Headers

HTTP response headers can be removed to avoid the client displaying them in the response, to do this:

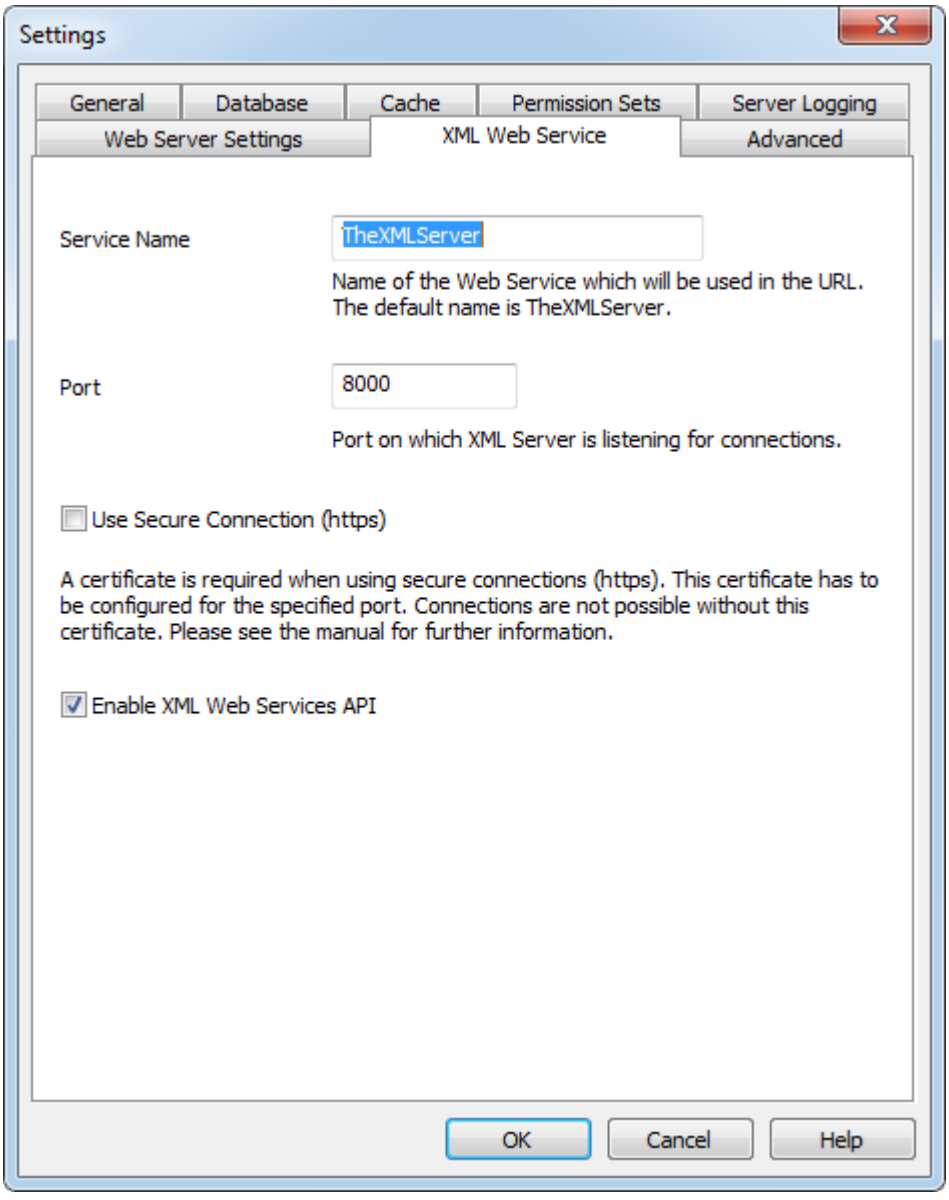
1. Select 'HTTP Response Headers".
2. Select the "X-Powered-By" HTTP Header.
3. Select Remove.

5.2 Https

Non encrypted protocols enable network traffic to be read. So to ensure the security on systems reachable via the Internet, https is required.

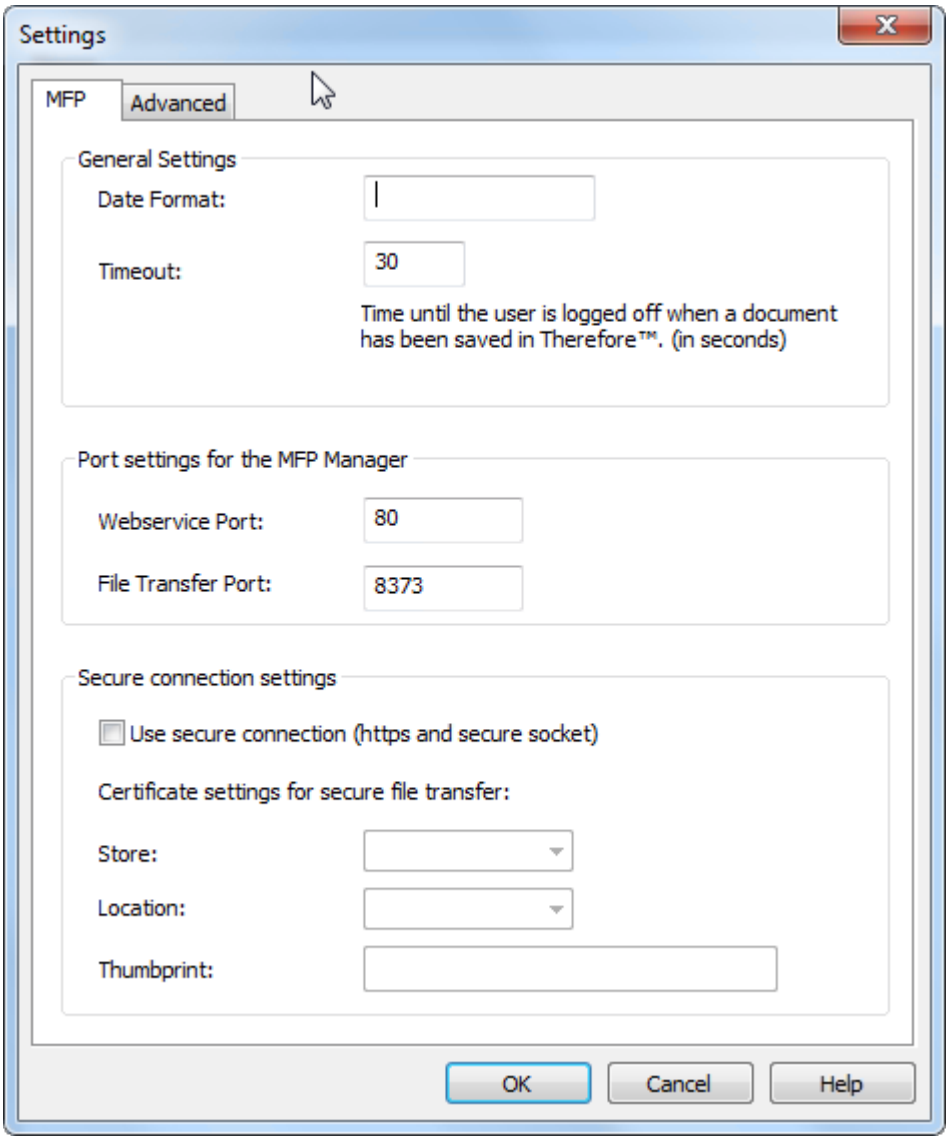
5.2.1 XML Web Service

Https for The XML Web Service can be configured in the Solution Designer under the Settings of the Therefore Object. For information on creating self-signed certificates and configuring SSL certificates, refer to the Therefore™ documentation.



5.2.2 MFP Manager Service

Https for the MFP Manager Service can be configured in the Solution Designer under the Therefore™ MFP Application Settings. For information on creating self-signed certificates and configuring SSL certificates, refer to the Therefore™ documentation.



5.2.3 Cryptographic Best Practices

By default SSL v2.0 is enabled on every server system. However, since this version has been hacked and hence non-secure, it is recommended to follow the instructions listed below on the servers where Microsoft® IIS, Therefore™ XML Web Service and Therefore™ MFP Manager Service are running, as a matter of best practice.

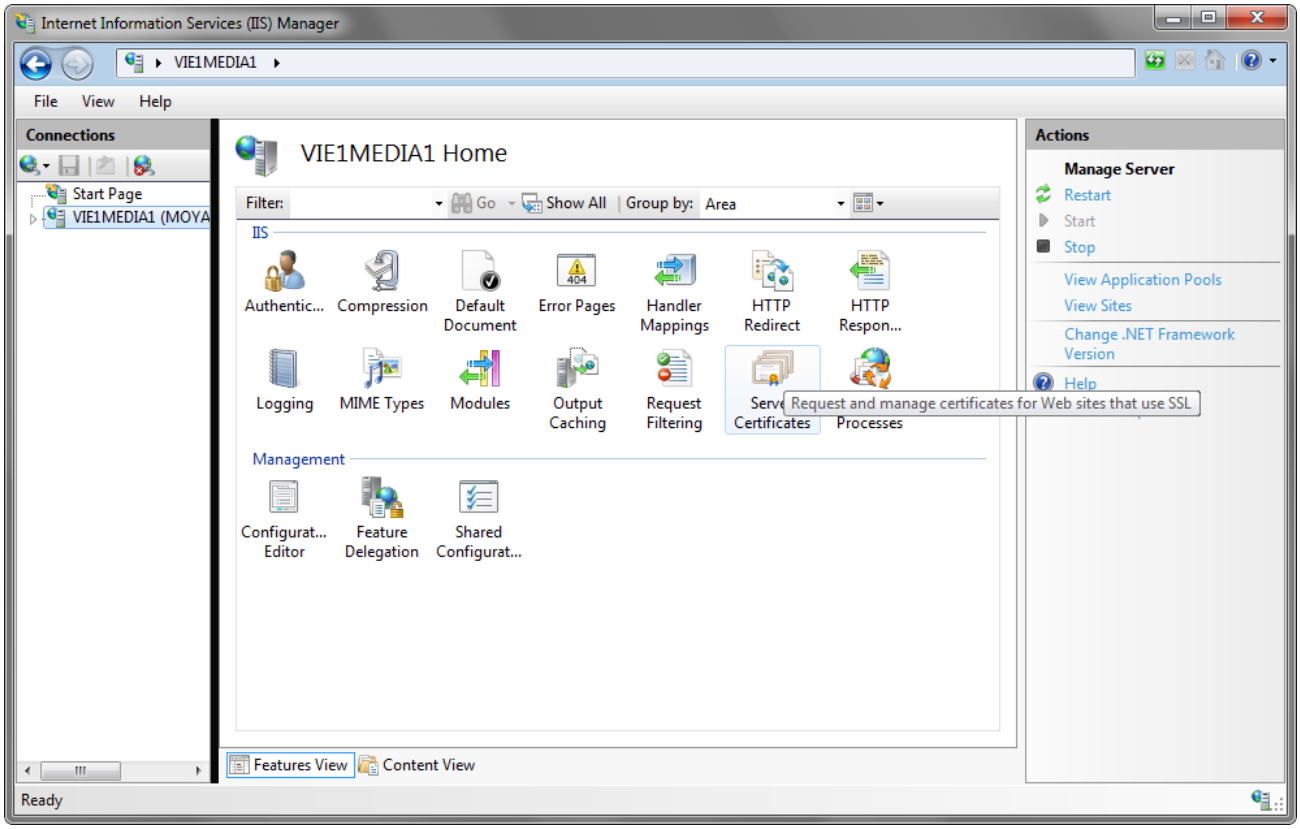
1. Download the free tool by 'Nartac Software' from https://www.nartac.com/Products/IISCrypto.
2. Under the Templates tab, select PCI 3.1.
3. Under the Cipher Suites tab, disable TLS_RSA_WITH_3DES_EDE_CBC_SHA.
4. Restart the computer.

Consider using Nartac's Best Practices templates that allow your system to follow certain standards and protocols.

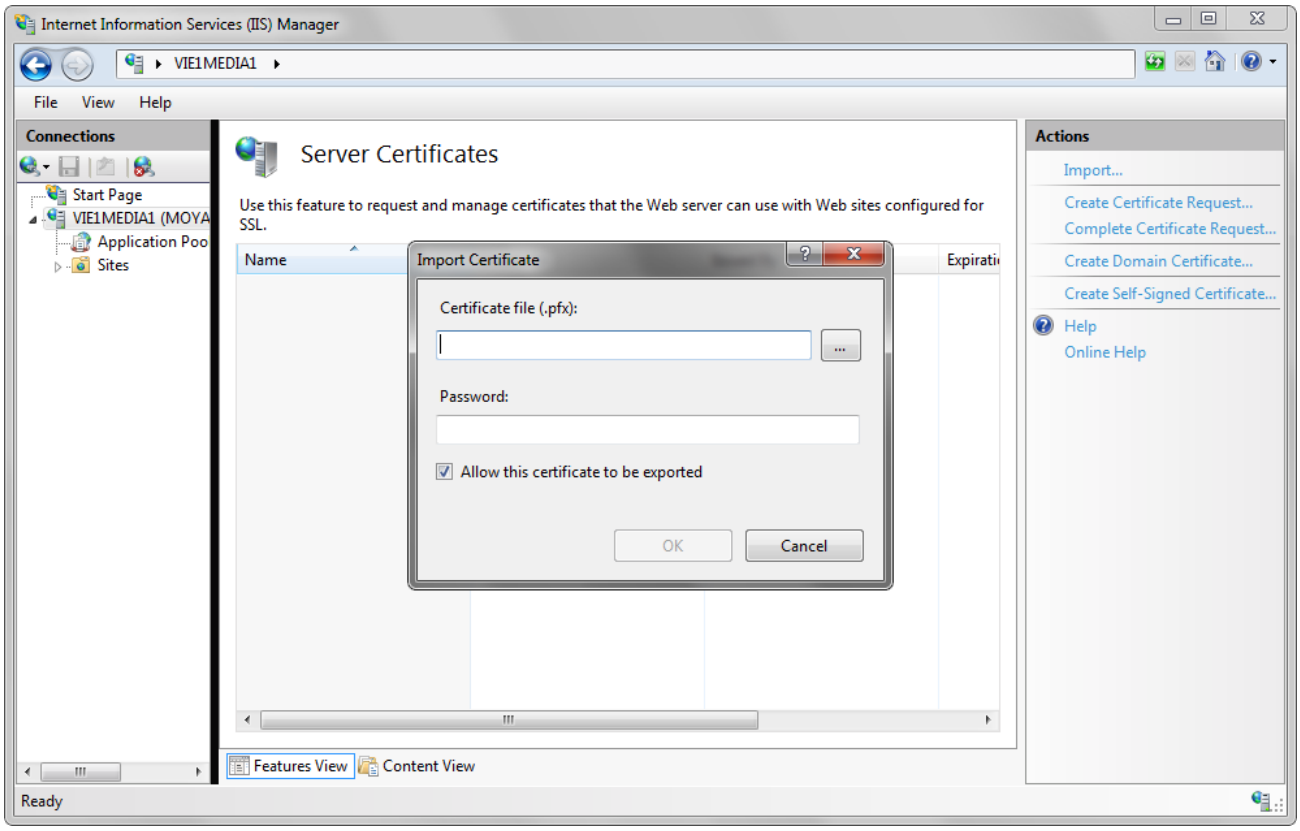
5.2.4 Microsoft® IIS

You can configure https for Microsoft® IIS as follows:

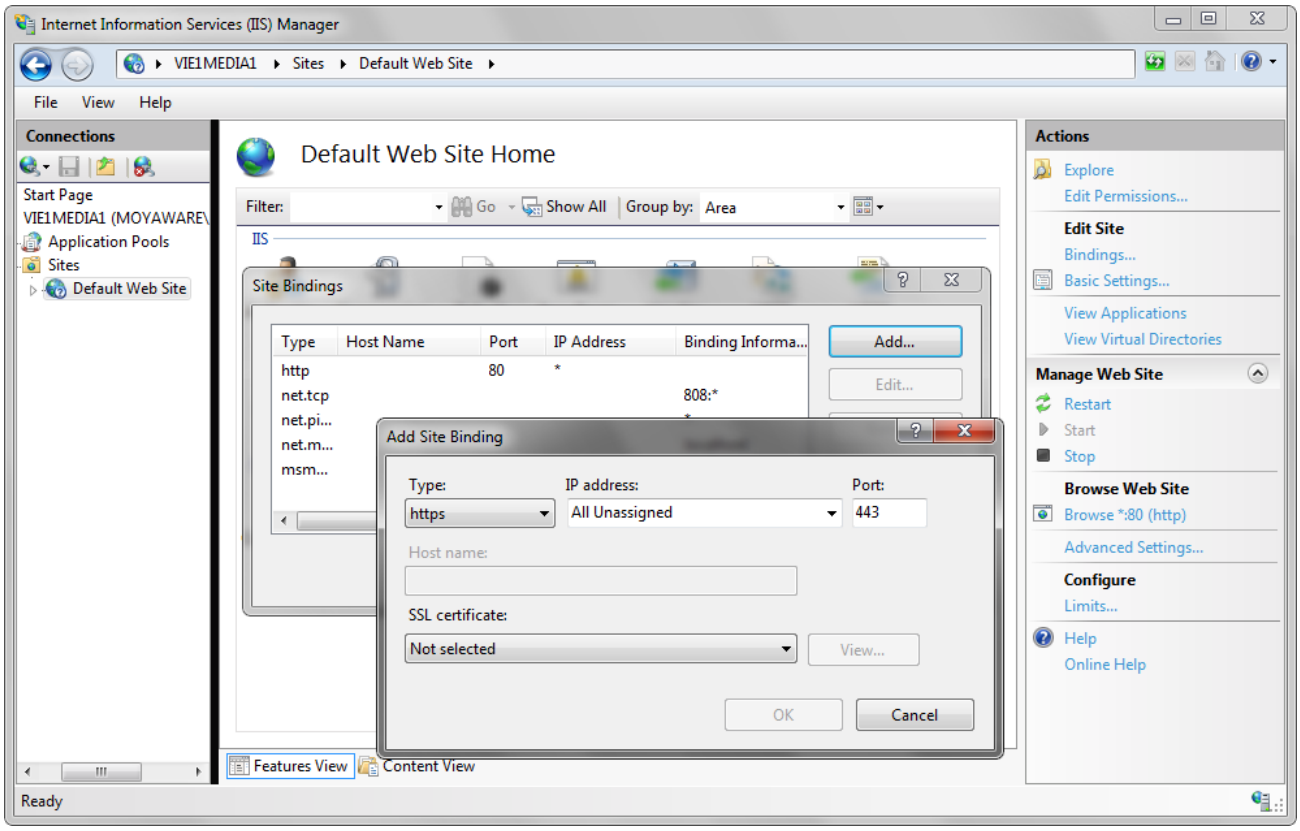
1. Go to Internet Information Services (IIS) Manager. Under the server Home, open Server Certificates.



2. Select Import... and then import your certificate.



3. Under the Default Website under Edit Site, select Bindings... and then click Add... Now specify https and the SSL certificate. Click OK when done.



4. Then you can either remove the http binding or, to avoid a connection error, you can set forwarding from http to https via utilities such Microsoft URL Rewrite.

5. Once switching to https, ensure that cookies make use of SSL by selecting web.config in the TWA folder and set: *requireSSL=true* for the forms and the cookies:

```
  <system.web>
    <httpCookies httpOnlyCookies="true" requireSSL="false" /><!--
requireSSL: SET TO TRUE ONLY IN CASE OF SECURE CONNECTION (HTTPS) - SECURE COOKIE FLAG-->
    <authentication>
      <forms requireSSL="false" /><!--
requireSSL: SET TO TRUE ONLY IN CASE OF SECURE CONNECTION (HTTPS) - SECURE COOKIE FLAG-->
    </authentication>
```

Should be changed to:

```
  <system.web>
    <httpCookies httpOnlyCookies="true" requireSSL="true" /><!--
requireSSL: SET TO TRUE ONLY IN CASE OF SECURE CONNECTION (HTTPS) - SECURE COOKIE FLAG-->
    <authentication>
      <forms requireSSL="true" /><!--
requireSSL: SET TO TRUE ONLY IN CASE OF SECURE CONNECTION (HTTPS) - SECURE COOKIE FLAG-->
    </authentication>
```

5.3 Encrypt Links

The case, document, workflow instance and task numbers can be encrypted in links used for Therefore™ web applications by setting the Encrypt Link setting in the Advanced settings in the Therefore™ Solution Designer to true.

6. Virus Scanning

6.1 Standard Anti-Virus Configuration

It is recommended to install anti-virus software on the Therefore™ Server to protect the system against malware being stored in Therefore™. In a default configuration, the anti-virus software checks all files saved in the storage device to protect the system against malware.

- Ensure configuration of the anti-virus software to scan inside .zip and .thex files in on-access scans in order to protect the system effectively.
- Virus scanning can be turned off for Therefore™ end media.
- Depending on the preferences of the administrator, it is optional to disable scanning of the Therefore™ Cache folder when scanning has been turned off for document retrieve.

6.2 Enhanced Anti-Virus Configuration

The Therefore™ Server can also be configured to scan all incoming and/or outgoing documents by explicitly calling the installed anti-virus software. This configuration enables greater efficiency in scanning process and avoids unnecessary scans while saving or retrieving documents.

Requirements:
The enhanced configuration is only possible under the following conditions:

- The operating system is Windows 2016 (or later).
- The anti-virus software is AMSI compatible (e.g. Windows Defender, McAfee or ESET).

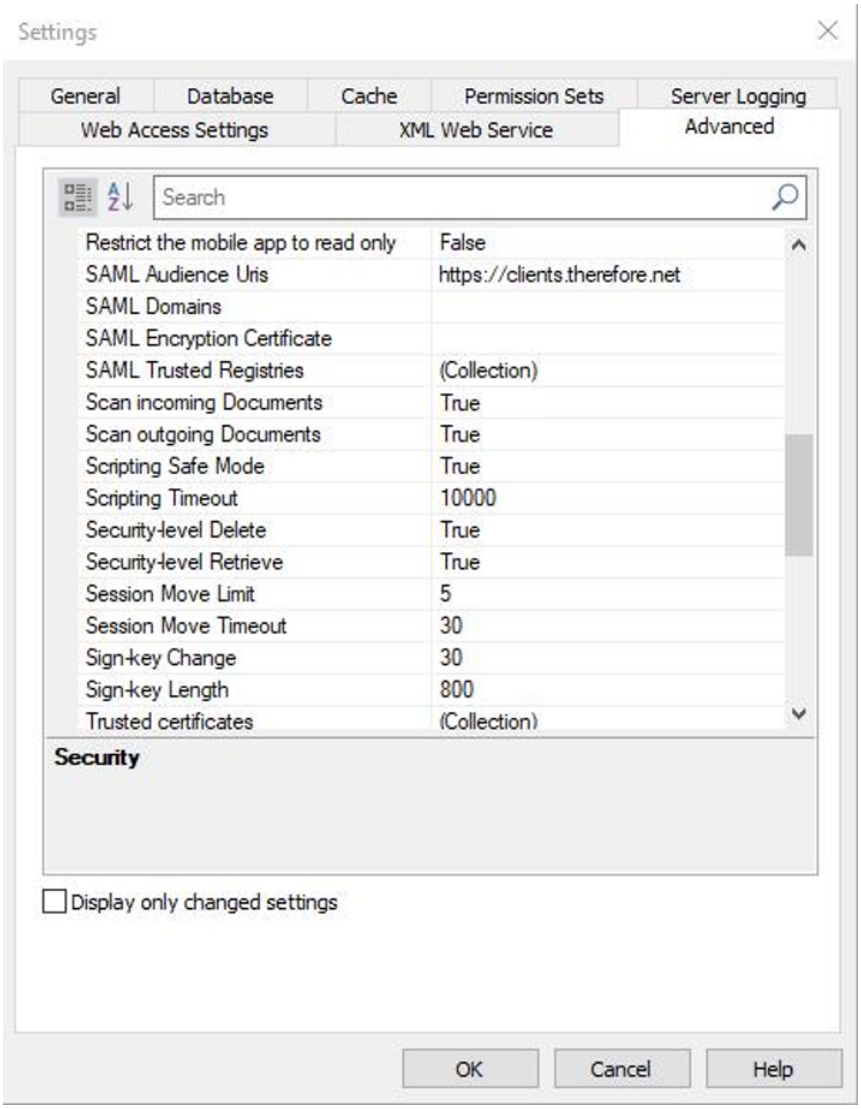
Without these requirements, the standard configuration explained above has to be used.

6.2.1 Enabling explicit scanning in Therefore™

To allow virus scanning for documents within the Therefore™ system, follow these basic steps:

1. Open the Therefore™ Solution Designer, right-click on the Therefore™ logo node and select the Settings option.

2. Under the Advanced tab, expand the Security section and find the two settings, 'Scan incoming documents' and 'Scan outgoing documents' and set these as 'True'.



Purpose of each Anti-virus scan setting:

- Scan incoming Documents: Scan documents for malware when saving documents to the Therefore™ Server. This setting will only have an effect when the Therefore™ Server Service is running on Windows Server 2016 or newer.
- Scan outgoing Documents: Scan documents for malware when retrieved by a Therefore™ client. This setting will only have an effect when the Therefore™ Server Service is running on Windows Server 2016 or newer.

6.2.2 Defining exceptions for Anti-Virus Software

With the above configuration, the Therefore™ Server will scan all incoming and outgoing documents by explicitly calling the anti-virus software. Thus, it is no longer required to let the anti-virus software scan files on storage used by Therefore™. The following exceptions should be configured in the anti-virus software to avoid unnecessary scans:

- Locations: Buffer, Cache, end media and transfer folder (if configured).
- Applications: TheServer, TheXMLServer, TheConversionServer.

Notable Error messages will appear under the 'Event log' (on the server), which can be found by searching for the event ID '221'. Depending on the virus scanner used, an error may also be found in the virus scanner's scan log.