System Security

www.therefore.net

Therefore™

PEOPLE PROCESS INFORMATION

VERSION: 2012 - 01

Contact: *documentation@therefore.net*

Table of Contents

1. **Introduction** 5

2. **Web Security** 5

2.1 Microsoft® IIS 5

2.1.1 Web.Config 6

2.1.2 Therefore™ Web Application 7

2.2 Https 10

2.2.1 XML Web Service 11

2.2.2 MFP Manager Service 12

2.2.3 Disable SSL v2.0 12

2.2.4 Microsoft® IIS 14

3. **Prohibited Extensions** 17

4. **Minimum Privileges** 17

4.1 Minimum Privileges for Therefore™ Server Service 17

4.1.1 Database Server 18

4.1.2 Windows® Active Directory® 18

4.1.3 LDAP 18

4.1.4 Therefore Server Machine 19

4.1.5 Storage folders 19

4.2 Minimum Privileges for other Therefore™ Services 19

4.2.1 Therefore™ Web Service 19

4.2.2 Therefore™ XML Web Service 19

4.2.3 Therefore™ Content Connector Service 20

4.2.4 Therefore™ Conversion Service 20

4.2.5 Therefore™ MFP Manager Service 20

4.2.6 Therefore™ Services for Connector to Microsoft® Exchange Server 20

4.2.7 Therefore™ Full-text Service 20

4.3 Minimum User Privileges 20

4.3.1 Therefore™ Object 20

4.3.2 Therefore™ Server Object 20

4.3.3 Categories Object 21

4.3.4 Keyword Dictionary Object 22

4.3.5 Data Types Object 22

4.3.6 Cross Category Template Object 22

4.3.7 Users and Groups Object 22
4.3.8 Capture Client Profiles Object 22
4.3.9 Document Loader Object 22
4.3.10 Workflow Object 23
4.3.11 Device Object 23
4.3.12 Storage Policy Object 23
4.3.13 Retenion Policy Object 23
5. Storage of Therefore™ Documents 23
5.1 Managing External Audit Permissions 23
5.2 Digital Signatures 24
5.3 Composite Files 25
5.4 Saving to Therefore™ 26
5.5 Document History 28
5.6 Document Retention 29
5.7 Audit Trail 30

1. Introduction

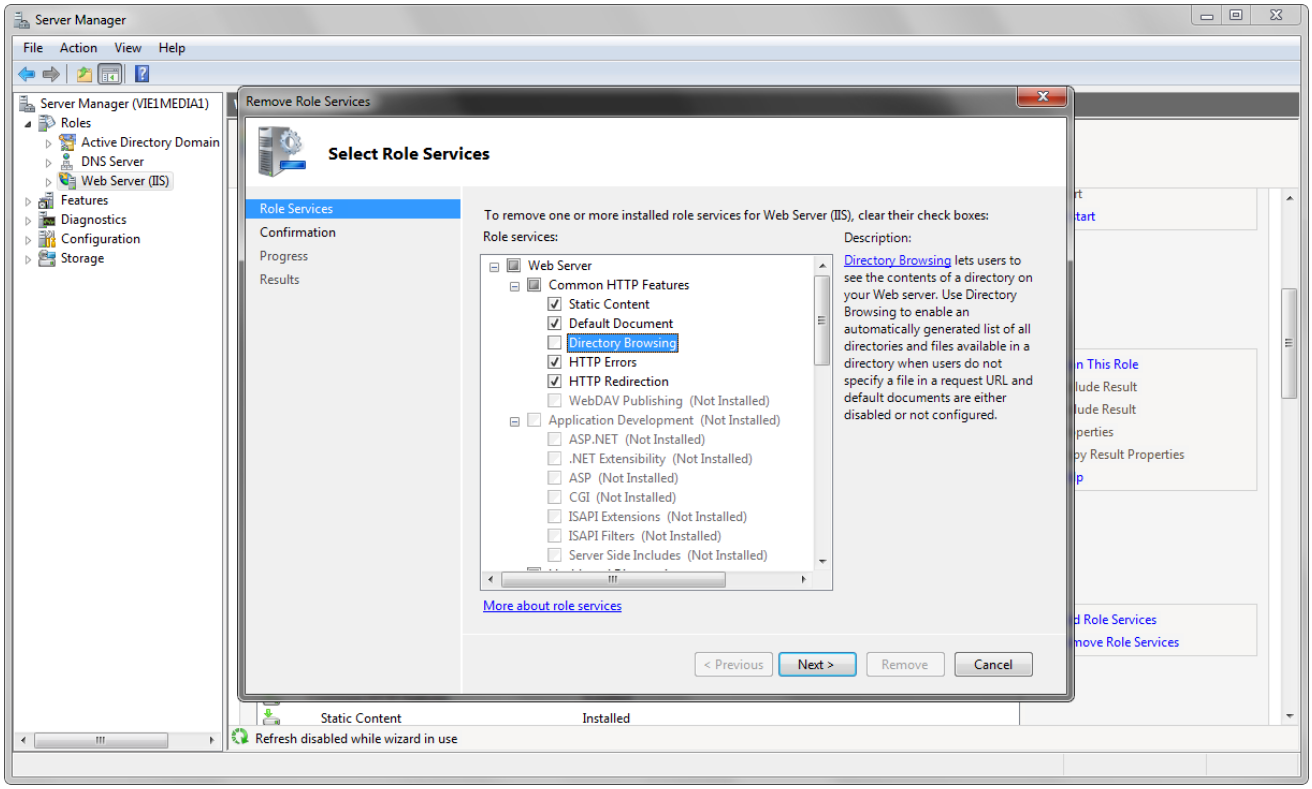
The purpose of this document is primarily to help people ensure that their Therefore™ system is as secure as possible. In addition we have also provided some general information on security in Therefore™.

2. Web Security

2.1 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.

2.1.1 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 and Therefore™ Mobile 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:

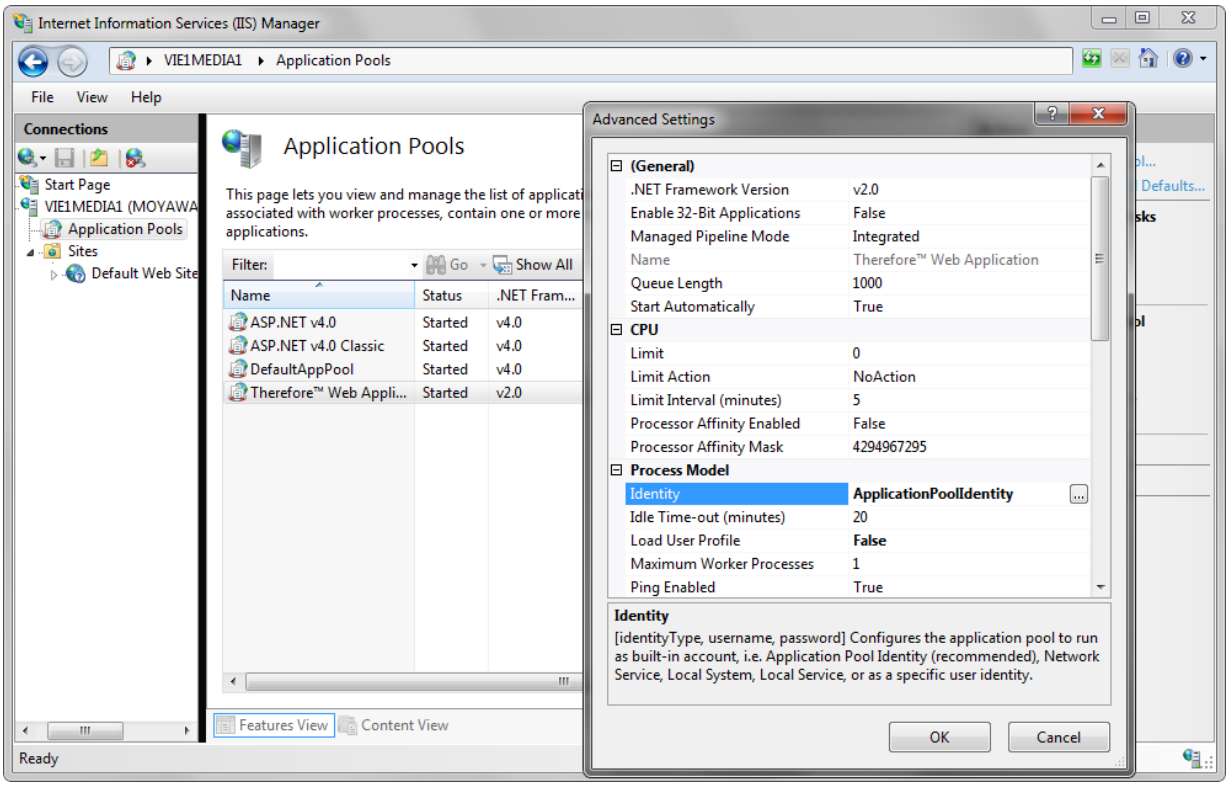
```
<system.web>

...
...

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

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

2.1.2 Therefore™ Web Application

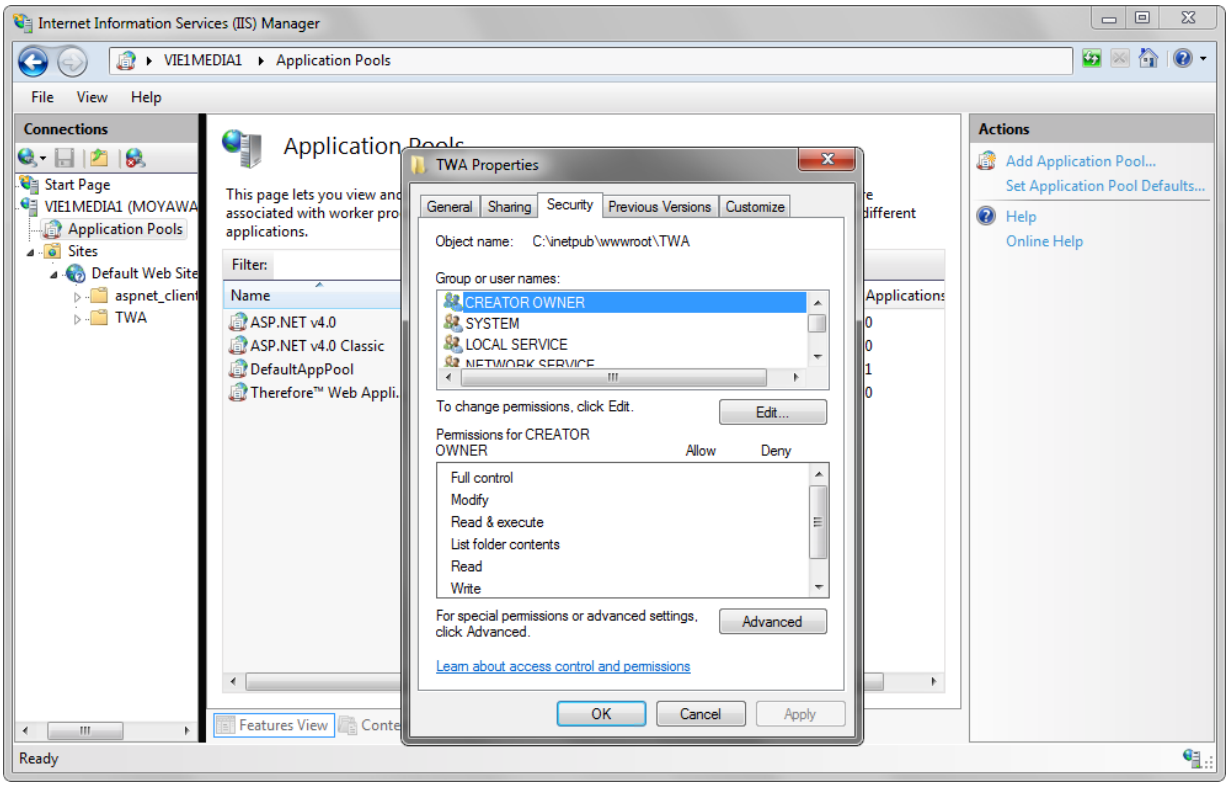
To ensure that the Therefore™ Web Access application has minimum required permissions on the server run the **Best Practices Analyzer for IIS** which is included in Windows® Server 2008 R2. The BPA will then report "Application pools should be set to run as application pool identities".

To solve this issue the following can be done:

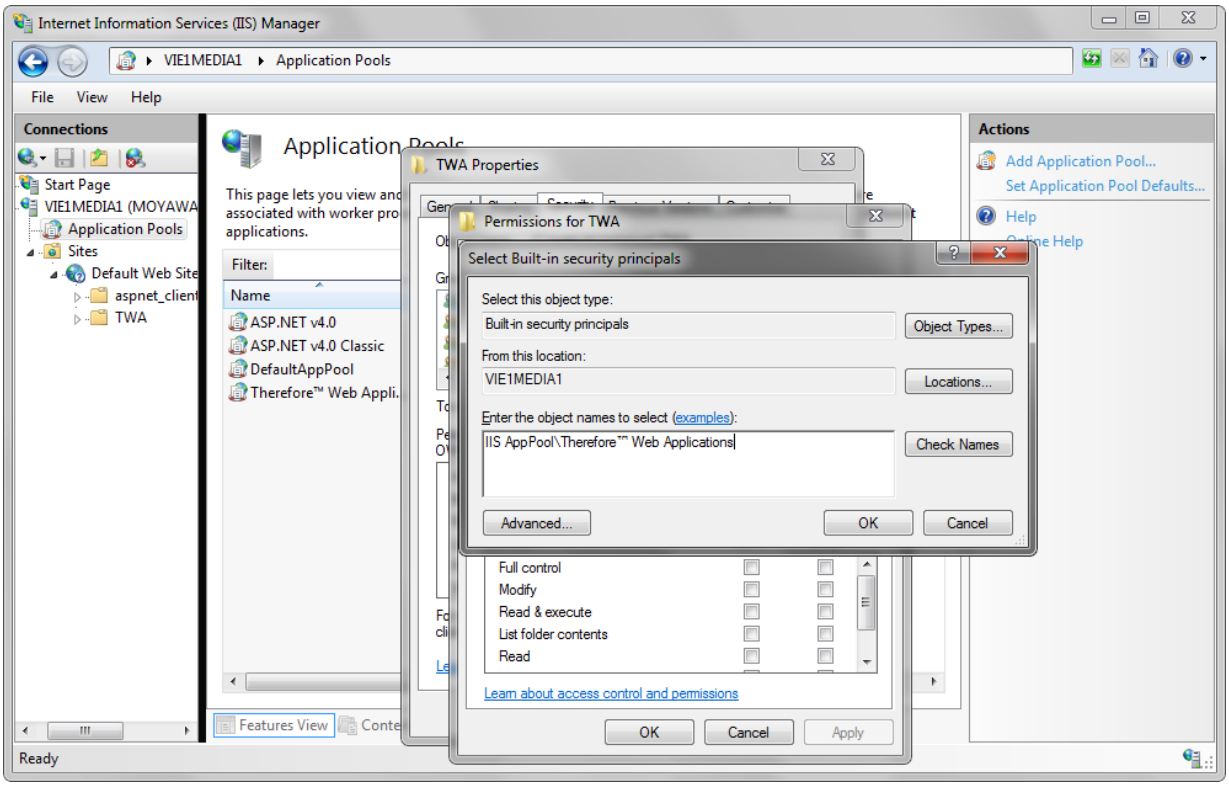
1. Go to **Internet Information Services (IIS) Manager** under **Application Pools** right click on the **Therefore™ Web Application** and choose **Advanced Settings...** Set the application pool's identity to **ApplicationPoolIdentity.**



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™ Web Applications** and in this case the user would be "**IIS AppPool\Therefore™ Web Applications**" (the pool user is located on the server itself, so you have to set the Location to <servername>).



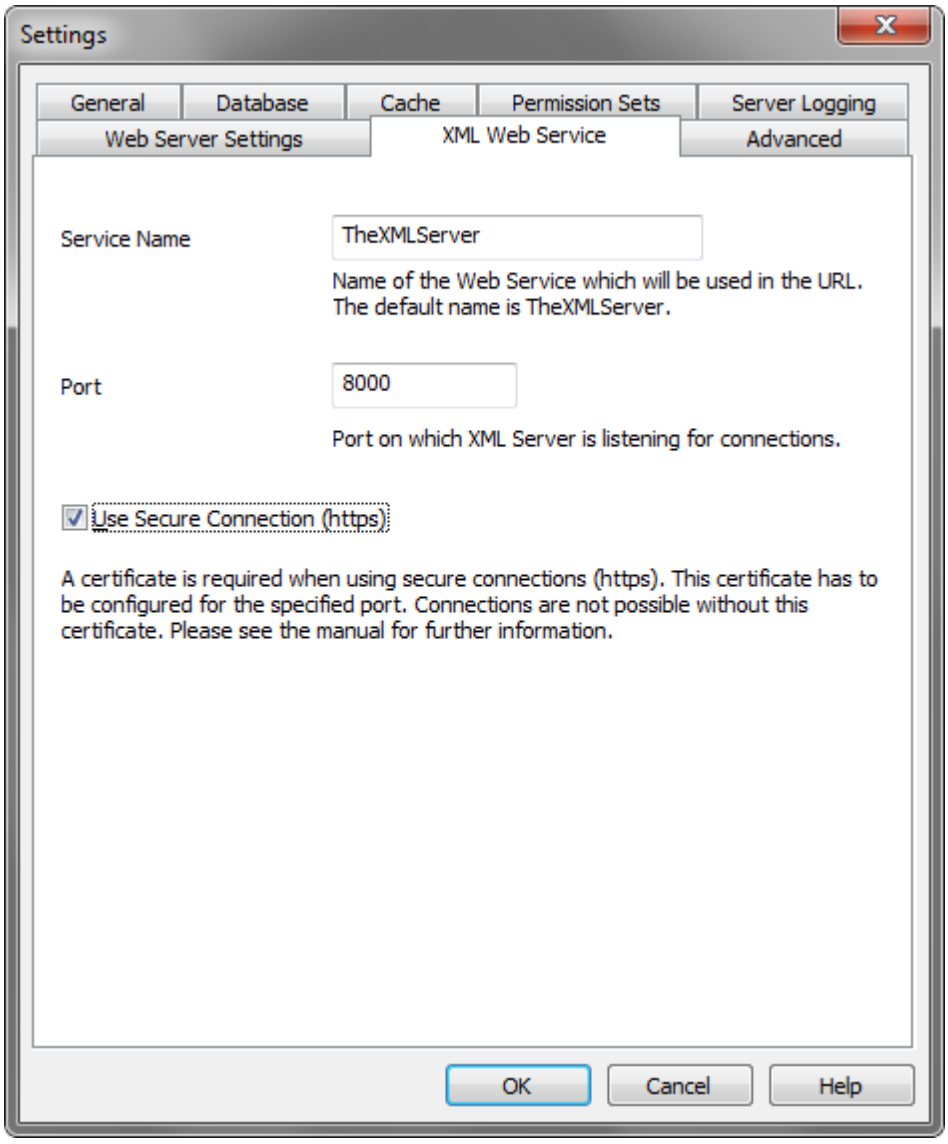
4. Grant the user Read & Write permissions only.
5. Add the **IIS AppPool\Therefore™ Web Applications** user to the Distributed COM Users group. If you get an access denied in event log, please see the Therefore™ Installation Guide for information on DCOM configuration.
6. Restart Therefore™ services.
7. Restart Microsoft® IIS.

2.2 Https

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

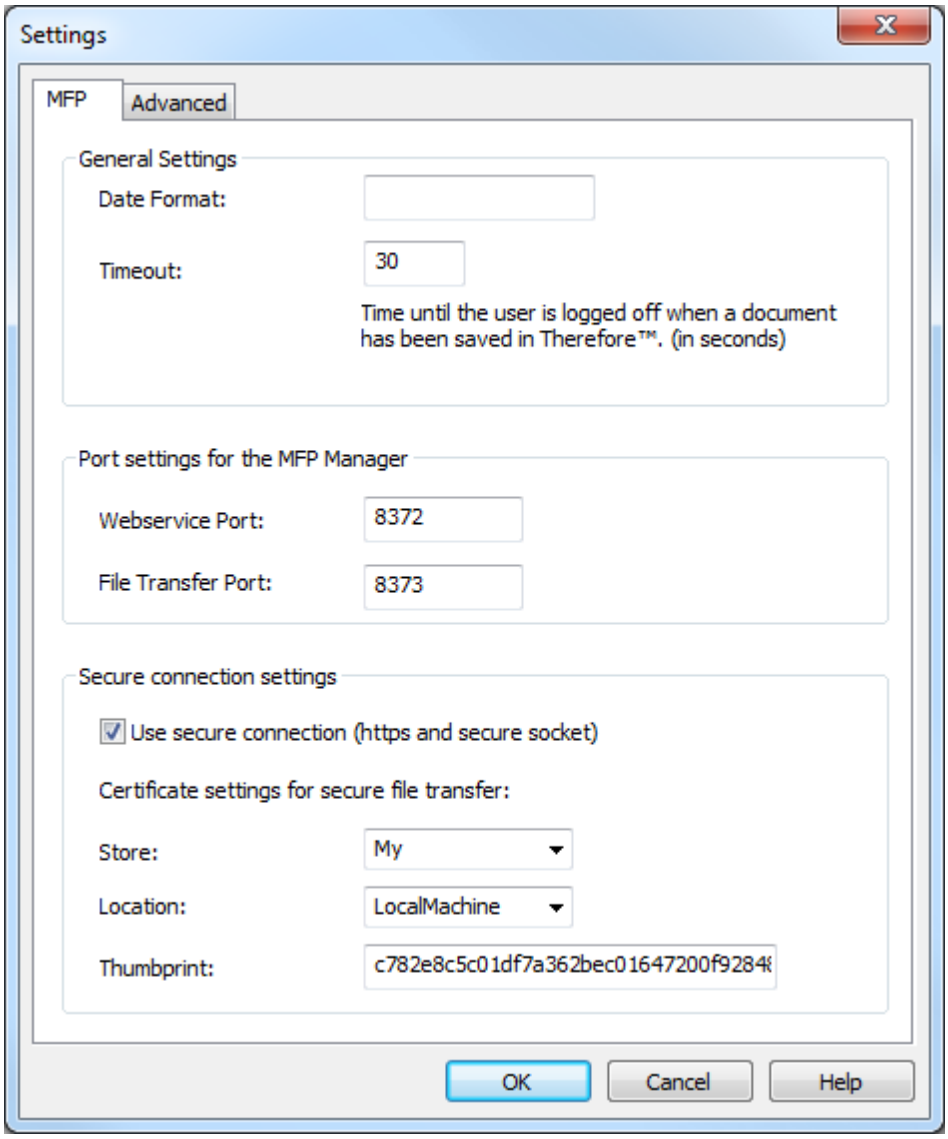
2.2.1 XML Web Service

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 configure SSL certificates, please see the Administration manual.



2.2.2 MFP Manager Service

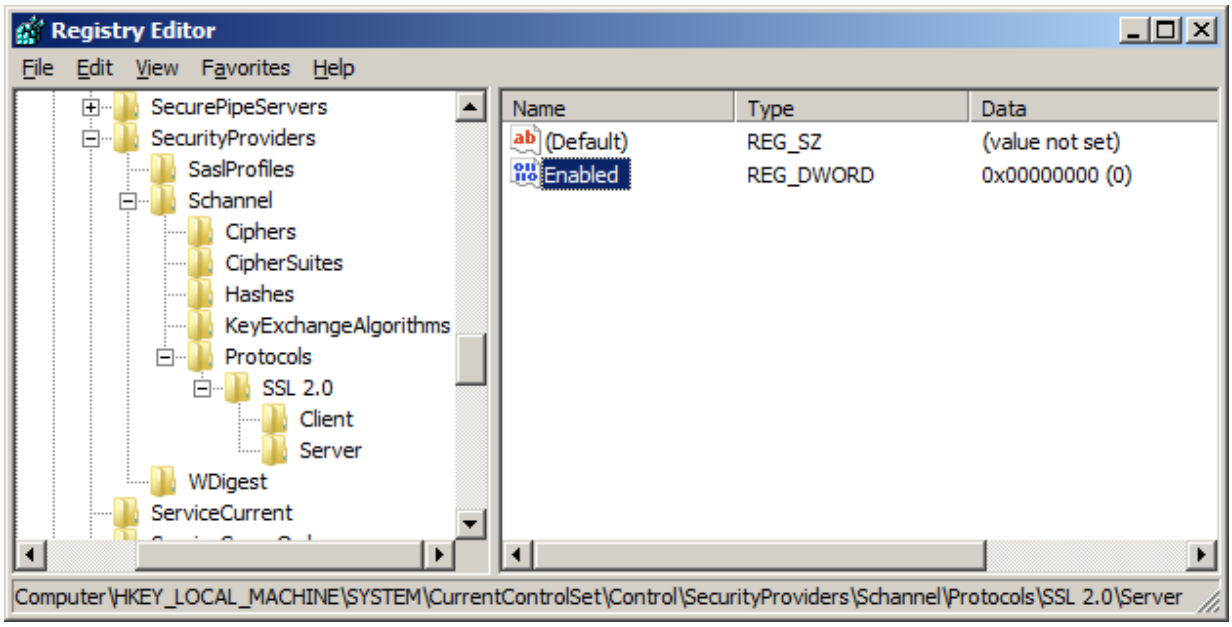
Https for the MFP Manager Service can be configured in the Solution Designer under the Therefore™ MFP Application Settings. For information on creating self-signed certificates and configure SSL certificates, please see the Administration manual.



2.2.3 Disable SSL v2.0

By default SSL v2.0 is enabled on every server system. However, since this version has been hacked and hence non-secure, please do the following on the servers where Microsoft® IIS, Therefore™ XML Web Service and Therefore™ MFP Manager Service are running.

1. Click **Start**, click **Run**, type **regedit**, and then click **OK**.
2. Locate the following registry key/folder: HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0
3. Right-click on the SSL 2.0 folder and select New and then click Key. Name the new folder Server.
4. Inside the Server folder, click the **Edit** menu, select **New**, and click DWORD (32-bit) Value. (Also possible via right-click)
5. Enter Enabled as the name and hit Enter.
6. Ensure that it shows 0x00000000 (0) under the Data column (it should be by default). If it doesn't, right-click and select Modify and enter 0 as the Value data.

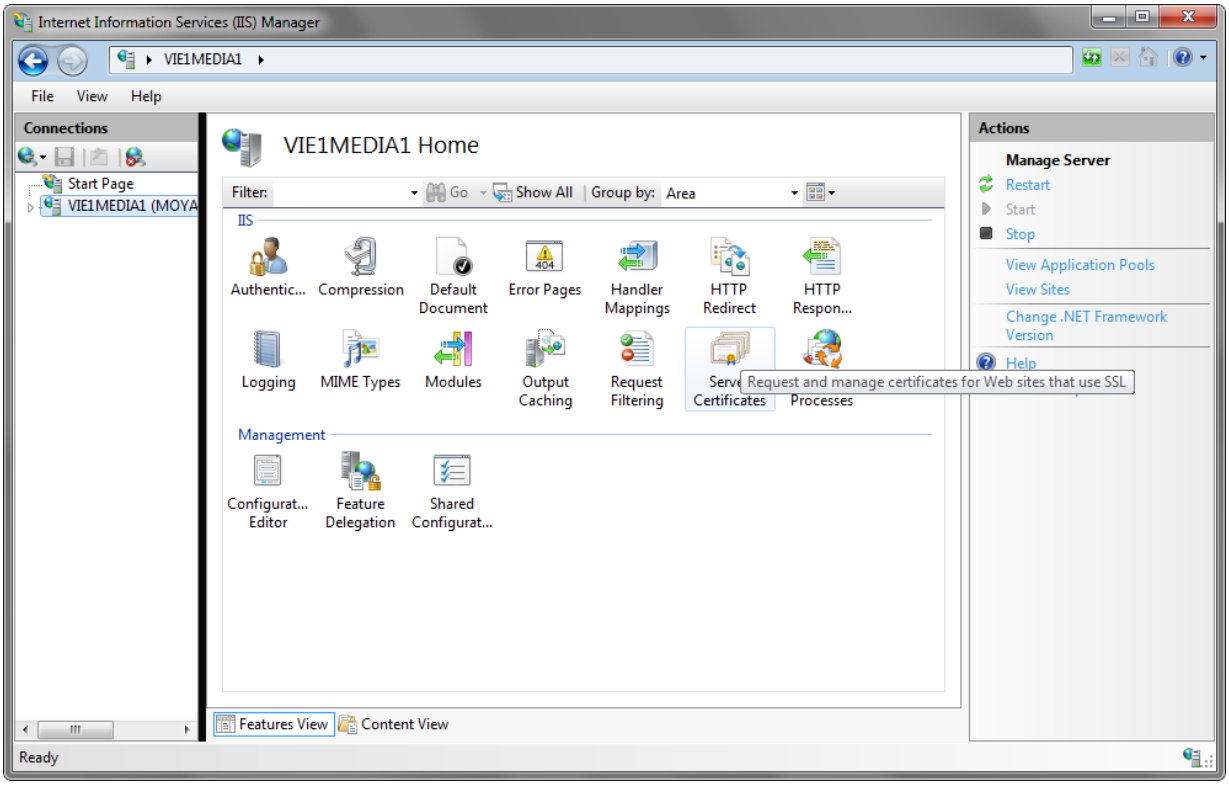


7. Restart the computer.

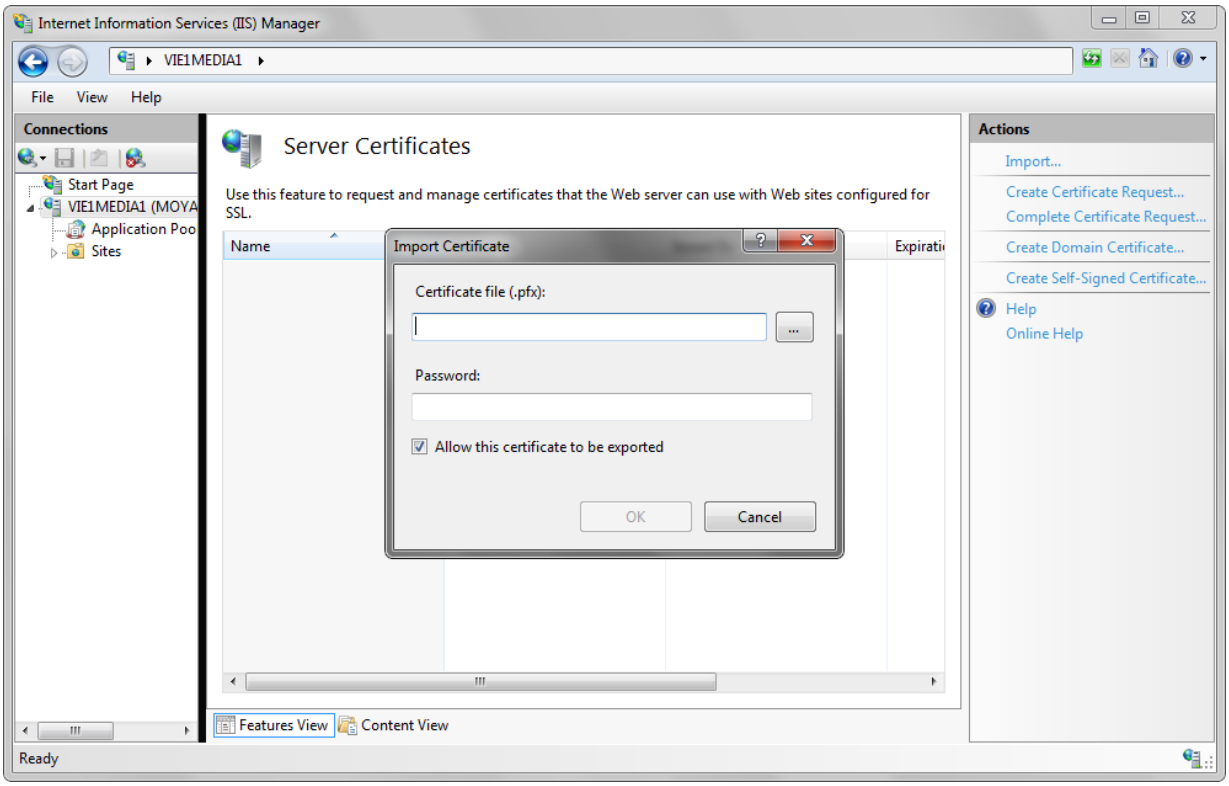
2.2.4 Microsoft® IIS

You can configure https for Microsoft® IIS as follows:

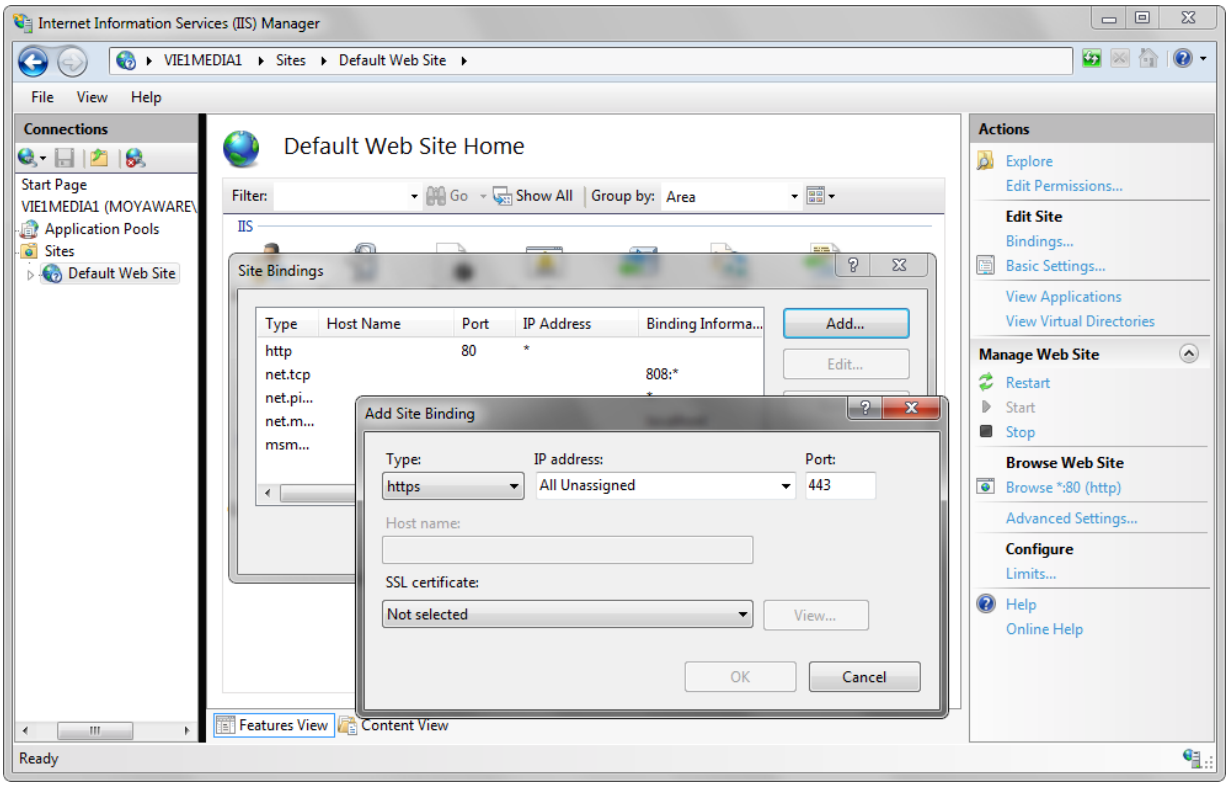
1. Go to **Internet Information Services (IIS) Manager.** Under the server Home, open **Server Certificates.**



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.

3. Prohibited Extensions

To prevent users from saving potentially dangerous files to the system we recommend the following extensions, in addition to dll and exe, to be prohibited in the Solution Designer advanced settings: aspx; asp; ascx; Master; master; htm; html; js; browser; ashx; asmx; bat; cmd; class; jse; lnk; msi; reg; shtm; shtml; soap; url; vb; vbe; vbs.

4. Minimum Privileges

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

4.1 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.

4.1.1 Database Server

Server Level:
To achieve the minimum required permissions it is necessary to manually create the Therefore™ database before installing Therefore™. (Typically with 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, CONTROL 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.

4.1.2 Windows® Active Directory®

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


This only applies to Scenario 1.

4.1.3 LDAP

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


This only applies to Scenario 1.

4.1.4 Therefore Server Machine

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

MachineKeys folder
Windows Server® 2003:
C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys

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 accesSts to these folders.

4.1.5 Storage folders

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

4.2 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:

4.2.1 Therefore™ Web Service

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

4.2.2 Therefore™ XML Web Service

The account for Therefore™ XML Web service requires access to the Therefore™ server machine (DCOM level).

4.2.3 Therefore™ Content Connector Service

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

4.2.4 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.

4.2.5 Therefore™ MFP Manager Service

The account for Therefore™ MFP Manager Service requires access to the Therefore™ server machine (DCOM level).

4.2.6 Therefore™ Services for Connector to Microsoft® Exchange Server

The account for Therefore™ services for the Connector to Microsoft® Exchange Server: please see the documentation for the Therefore™ connector for Microsoft® Exchange Server.

4.2.7 Therefore™ Full-text Service

The account for the Therefore™ Full-text service must be run with the Local System account.

4.3 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.

4.3.1 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.

4.3.2 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

4.3.3 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.

Permission	Explanation
Access category/ folder	When allowed, the category/folder can be opened.
Execute search	When allowed, a search on the category can be executed. Note: You must refresh the Therefore™ Navigator's tree view (view menu), or exit and restart the Navigator application for this change to take effect.
View document in hit list	When allowed, documents will be displayed in the hit-list. If the Open permission is denied then users can view index data in the hit-list, but not the document itself.
Open document	When allowed, documents can be opened for viewing.
Print document	When allowed, documents can be printed.
Export/send document	When allowed, documents can be e-mailed or exported to disk.
View document history	When allowed, the documents's history can be viewed (this includes who has checked out and modified the document).
View annotations	When allowed, annotations applied to the document can be viewed.
Hide annotations	When allowed, annotations can be hidden. (i.e. sections of hidden text can be viewed by deactivating annotations).
Add annotations	When allowed, annotations can be added (only TIFF files).
Delete annotations	When allowed, annotations can be deleted.
Update index data	When allowed, the index data can be changed.
Edit document	When allowed, the document can be edited.
Add document pages	When allowed, pages can be added to a document.
Retention Policy	When allowed, users can enable or disable the retention policy for a document.
Manage document links	When allowed the user can create and delete manual links between documents.
Delete document pages	When allowed the user can delete pages in a document.
Delete document	When allowed the user can delete a document (this will be placed in the re-cycle bin and can be restored).

Permission	Explanation
Add documents	When allowed a user can save documents to Therefore™.
Search administrator	When allowed, global searches can be added or deleted.
Category/folder administrator	When allowed, folders can be added/deleted and categories can be moved between folders.
Category Operator	When allowed, the user can perform operator tasks e.g. retention processing.
Set permissions	When allowed, the security settings in this list can be modified.

4.3.4 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.

4.3.5 Data Types Object

For a user to simple use a data type 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.

4.3.6 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.

4.3.7 Users and Groups Object

No permissions are required here for a general user.

4.3.8 Capture Client Profiles Object

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

4.3.9 Document Loader Object

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

4.3.10 Workflow Object

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

4.3.11 Device Object

General users need no permissions here.

4.3.12 Storage Policy Object

General users need no permissions here.

4.3.13 Retenion Policy Object

General users need no permissions here.

5. Storage of Therefore™ Documents

5.1 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.

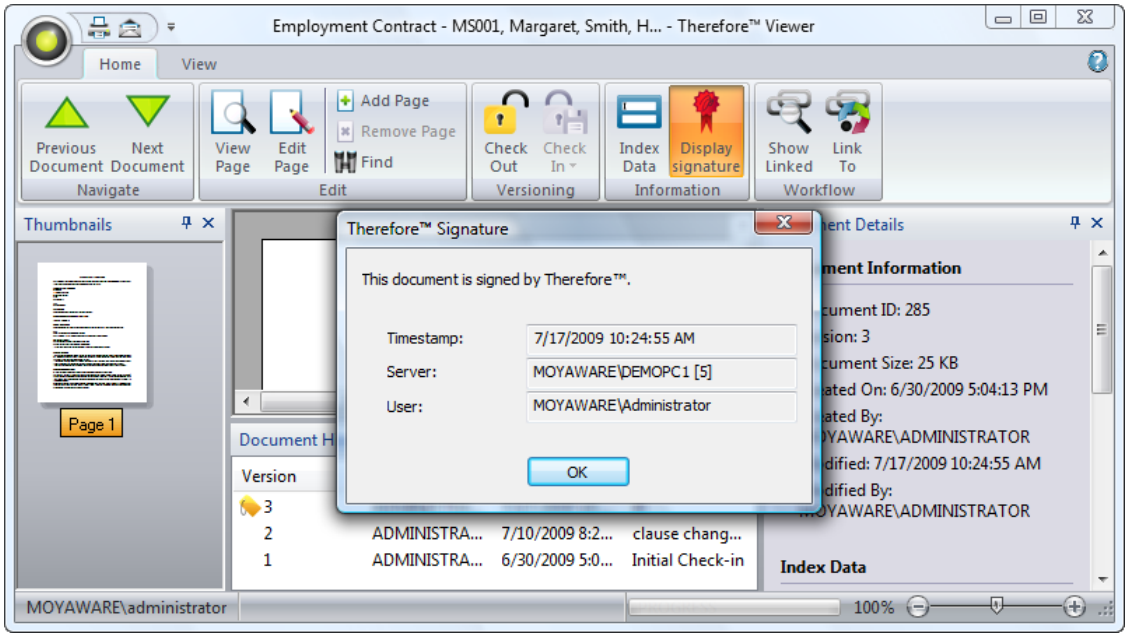
Mobile Access (Z3)
An auditor is provided with a Therefore™ Client software and permission to take the required documents offline. The required documents are taken offline and user permissions allow the auditor to view these documents.

5.2 Digital Signatures

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.

- All pages of the document (tiff, pdf, word, …)
- Timestamp
- Name of the Therefore™ Server
- ID of the used key
- Username who triggered the archive operation
- Document number

The signature is stored within ".thex" document files 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. On retrieval of a document the server re-computes the SHA 256 Hash and then verifies the signature. Only documents with valid signatures are sent to the client; however, administrators can be given rights to bypass this check in order to analyse invalid 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 new document version with 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. Therefore™ also provides this possibility when saving documents to Therefore™ using the Therefore™ Capture Client.

5.3 Composite Files

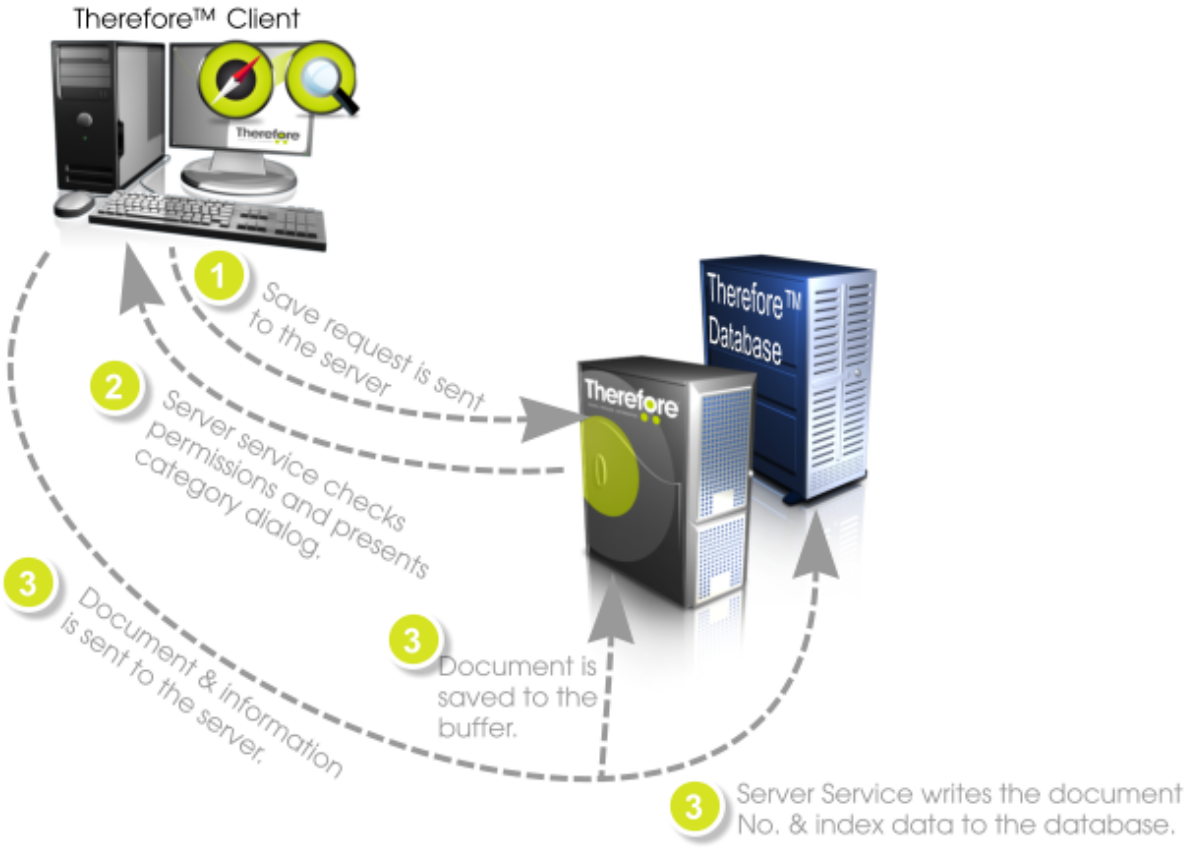
Therefore™ uses a non-proprietary composite file based on the Open Packaging Convention (open XML) and is part of the Office Open XML Standard (Microsoft®, ISO). This is the same format as used by Microsoft® Office (.docx, xlsx, etc.). This allows a single document to consist of multiple single files (e.g. a Microsoft Word document and Microsoft Excel® sheet can make up one Therefore™ composite document). Index information and digital signatures form part of the compound file which carries the extension ".thex". The compound file can be opened using standard unzip software.

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.

5.4 Saving to Therefore™

Documents can be saved to Therefore™ 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.

5.5 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 pages within a document.
4. Editing the index data.

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.

Via the workflow or the API it is possible to edit the index data without creating a new version. But any changes to a document itself will always result in a new document version.

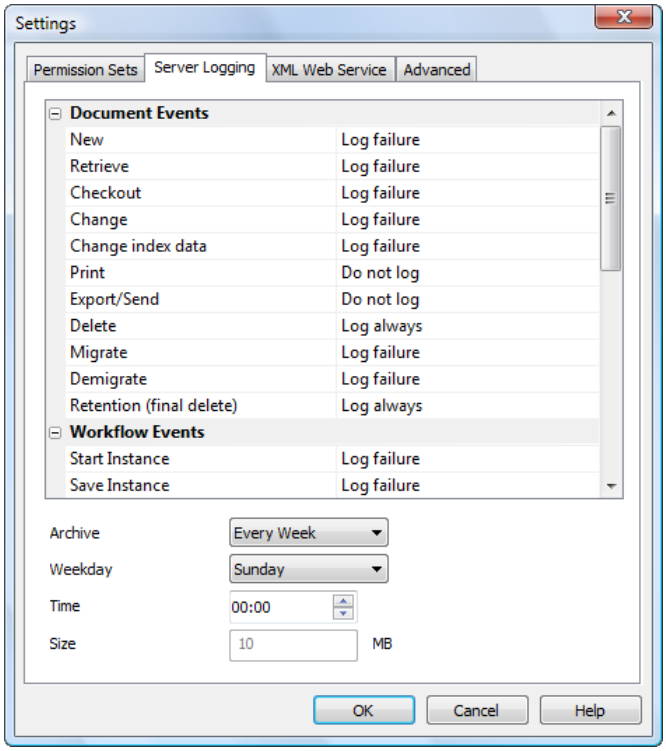
5.6 Document Retention

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.

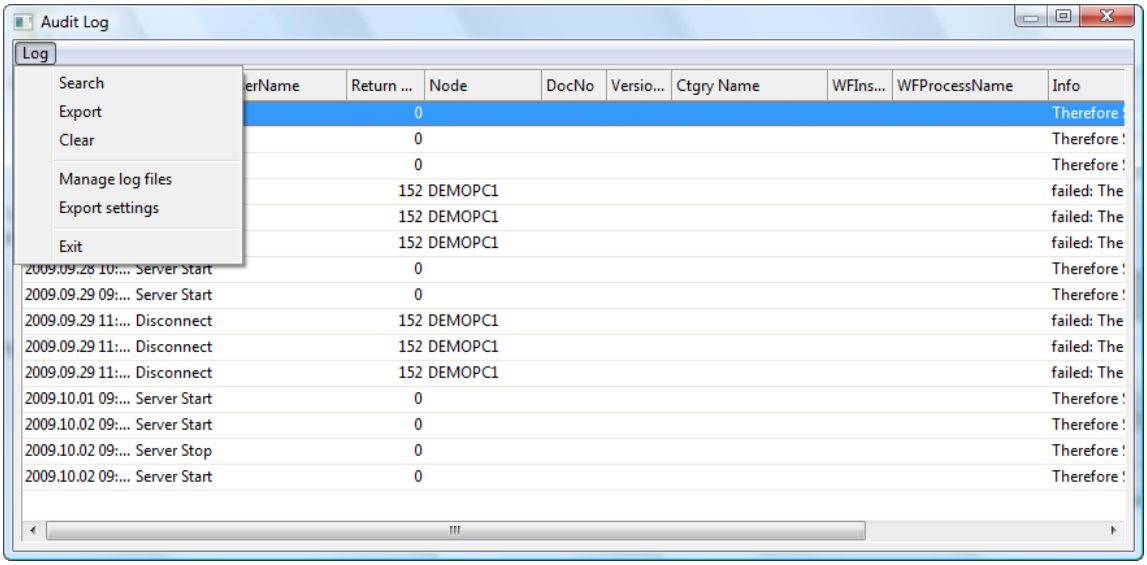
5.7 Audit Trail

The console makes it possible to check what a user has been doing on the Therefore™ system. It is still possible to see some user operations via the Message View but since Therefore™ 2009 R/2 an enhanced audit trail feature has been added. 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.



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



Following is a table detailing the individual events that can be logged.

Event	Description
New	Logs the creation of a new document.
Retrieve	Logs opening of a document.
Checkout	Logs document checkout.
Change	Logs a new version.
Change index data	Logs when document index data is changed via a workflow dialog.
Print	Logs when a document is printed.
Export/Send	Logs when a document is exported.
Delete	Logs when a document is deleted from the Navigator and sent to recycle bin.
Migrate	Logs when documents are moved from Buffer to storage-
Demigrate	Logs when documents are moved from a storage media back to the Buffer.
Retention (final delete)	Logs when the documents are deleted during the migration process.
Start Instance	Logs the start of a workflow instance.
Save Instance	Logs when a user saves a task.
Finish Task	Logs when a workflow task is completed.
Delegate	Logs when a workflow task is delegated.
Claim	Logs when a workflow task is claimed.
Unclaim	Logs when a workflow task is claimed.
Route	Logs when a workflow instance is routed.
Send Overdue Mail	Logs when an overdue mail is sent.
Finish Instance	Logs when a workflow instance ends.
Server Startup/ Shutdown	Logs when the Therefore Server is started or stopped.

Event	Description
User Connect/ Disconnect	Logs when a user connects to the Server via a Therefore application.
Save Object Definition	Logs the saving of any object in Solution Designer (e.g. Category, Workflow etc.)
Delete Object	Logs the deletion of any object in Solution Designer (e.g. Category, Workflow etc.)
Change Security	Logs when the security of an object is changed.
Change Settings	Logs when Server, Workflow, and storage sett
Run Query	Logs when a search is done in the Navigator.
Mount/Unmount Media	Logs the mounting/unmounting of storage media.
Import/Export Media	Logs the importing/exporting of storage media.
Format/Register Media	Logs the formating/registering of storage media.

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".
HKLM\Software\User\Therefore
AbortExportOnLogFail
AbortPrintONLogFail