TIBCO Statistica™

Document Management System Admin Guide

Software Release 13.4

May 2018

Two-Second Advantage®

Important Information

Contents

TIBCO Documentation and Support Services

Documentation for this and other TIBCO products is available on the TIBCO Documentation site. This site is updated more frequently than any documentation that might be included with the product. To ensure that you are accessing the latest available help topics, visit:
https://docs.tibco.com

How to Contact TIBCO Support

For comments or problems with this manual or the software it addresses, contact TIBCO Support:

- For an overview of TIBCO Support, and information about getting started with TIBCO Support, visit this site:
  http://www.tibco.com/services/support
- If you already have a valid maintenance or support contract, visit this site:
  https://support.tibco.com
  Entry to this site requires a user name and password. If you do not have a user name, you can request one.

How to Join TIBCO Community

TIBCOmmunity is an online destination for TIBCO customers, partners, and resident experts. It is a place to share and access the collective experience of the TIBCO community.

TIBCOmmunity offers forums, blogs, and access to a variety of resources. To register, go to the following web address:

https://www.tibcommunity.com

TIBCO Community is an online destination for TIBCO customers, partners, and resident experts. It is a place to share and access the collective experience of the TIBCO community.

TIBCO Community offers forums, blogs, and access to a variety of resources. To register, go to the following web address:
https://community.tibco.com

Introduction

General Overview

The Statistica Document Management System (SDMS) is a complete, highly scalable database solution package for managing electronic documents. SDMS enables you to quickly, efficiently, and securely manage documents of any type [e.g., find them, access them, search for content, review, organize, edit (with trail logging and versioning), approve, etc.]. It is specifically designed to ensure compliance with FDA 21 CFR Part 11 regulations and ISO

9000, 9001, 14001 documentation requirements.

SDMS is extremely transparent and easy to use. Its key features include:

- Flexible, customizable (optionally Browser/Web-enabled) user interface
- Electronic Signatures
- Comprehensive Auditing Trails, Approvals
- Optimized Searches
- Security
- Satisfies the FDA 21 CFR Part 11 Requirements
- Satisfies ISO 9000 (9001, 14001) Documentation Requirements
- Unlimited scalability (from desktop or network Client-Server versions to the ultimate size, Web-based worldwide systems)
- Open Architecture and Compatibility with Industry Standards

Compliance

FDA. The general requirements put forth in the Code of Federal Regulations (CFR) Title 21 Part 11 specify what a business needs to do in order to maintain electronic records acceptable for submission to the FDA (Food and Drug Administration).

ISO. Similar guidelines for manufacturing in general (often collectively known as ISO 9000 standards) have been published by the International Organization for Standardization (e.g., see ISO 9001 4.5: Document and data control; also ISO 14001, Ch. 4.5.5.).

Compatibility

Integration with Statistica products. The Statistica Document Management System provides seamless integration with Statistica PROCEED (for building predictive models and Web SEWSS/SEWSS (for process analysis and quality control/improvement). Directing your files (e.g., projects, profiles, monitors or configurations) to the secure repository of the Statistica Document Management System is as easy as simply saving a file. When your authentication is based on your initial log on into the system, no entry of additional passwords is necessary.

Stand-alone, highly compatible application. SDMS can be used as a stand-alone system. Additionally, because of its COM and SOAP-based architecture, it can be called from other applications, integrated into existing systems or expanded by adding custom functionality.

Compatibility with other standards. Please also inquire about the compatibility of Statistica Document Management System with the Open Document Management API (ODMA) standard and the interfaces and support for the Web-based Distributed Authoring and Versioning (WebDAV) standard.

How the Statistica Document Management System Works

To satisfy the diverse functionality and security requirements of various types of users, SDMS implements a set of options to manage documents in a flexible and secure database.

1. Statistica Document Management System enables you to save documents to a secure repository database. With its self-explanatory user interface, you can easily perform all document management operations [from any computer connected to the network or (optionally) via the Internet].

2. Most document types can be maintained both in a) the archival, review-only (non-editable) PDF format, featuring the appropriate electronic signatures, and also b) in the respective editable (source) format allowing the user with the appropriate access privileges to create new, modified versions. None of the edits or changes, however, will ever overwrite either the archival review-only or the source files of the previous version; they will only add new files to the repository.

3. Strict security via electronic signatures (compliant with 21 CFR Part 11 requirements) is enforced, and different groups of users can be authorized to create, edit, or review documents in different parts of the archive.

4. Documents in the document archive cannot be deleted by end users, other than using a designated process accessible only to the administrator with the top level access privileges. Every time a document is edited, a new version is created and logged with annotations (metadata) to identify the time and the author of the modifications and other information (either optional or required by the local configuration).

5. Approval trail requirements can be established so that documents must be reviewed, approved, and signed (via electronic signatures) by designated supervisors before they can be placed in designated parts of the repository.

6. A complete auditing trail of all document edits is automatically created (e.g., who made the changes and when the changes were made) and can be retrieved for submission to regulatory bodies or agencies.

Ensuring Security and Compliance

Statistica Document Management System is designed to deliver not only a flexible, high-performance system to manage your documents in a way that will increase your productivity by facilitating access to and management of crucial information, but also to ensure security and compliance with the requirements of regulatory agencies (e.g., FDA 21 CFR Part 11, ISO 9000).

Security, Electronic Signatures

1. By default, the SDMS requires valid passwords to contain more than 6 letters, and it does not allow for passwords of a **common** type (e.g., "111111" is not allowed). Furthermore, the password requirements are completely configurable. For example, you can require that all passwords contain a minimum of two numbers, two lower case letters, and two uppercase letters. Note that for Integrated Windows accounts password

2. For SDMS local accounts (i.e., non Integrated Windows accounts), passwords can be configured (by the administrator) to expire so that users are forced to change passwords

3. The system applies automatic user-lockout and e-mail notification (e-mail notification will not be in the first release, Version 1.0) of the administrator(s) when a certain number of attempts is made to log into the system with the wrong password. This event

4. Statistica Document Management System offers groupware functionality, supports workgroups, and enables you to define users and groups of users with specific privileges (i.e., the permission to create documents, edit documents, review documents, approve documents, etc.).

Version Control and Audit Trails

1. In SDMS, "everything" is documented and traceable, which means, for example, that documents are never deleted. When a document is edited, a new version of that document is created and properly authenticated. Authorized and authenticated users may be required to explicitly "check out" the respective documents from the repository and check new versions into the repository with notes and documentation regarding the nature and purpose of the edits. Additionally, authorized users can apply electronic signatures using the SDMS approval functionality.

2. The program can be configured to perform configuration-specific verification and documentation maintenance operations whenever a document is checked in. For example, you may require users to complete a check list or a custom form that states the purpose of the edits or gives a brief summary of editing activities. The system is fully programmable during installation, or any time thereafter, so that custom reporting, annotation, signatures, or other requirements associated with the creation or editing of documents can be enforced.

3. Summary options are available to enable authorized users to review the complete audit trail for requested documents.

4. Various options are available to perform simple or complex searches of the documents (current and previous versions) managed by SDMS.

Recommended (and FDA Approved) Archival Document Types

One of the unique strengths of the Statistica Document Management System is its ability to store and exchange information in various file formats including your proprietary formats. This enables SDMS to share information internally in ways that are most convenient for your specific organization and externally with practically all industry standard applications or protocols for information exchange.

Most importantly, the program allows you to store renditions of a document (e.g., in PDF or XPORT formats). With this feature, you can store an XPORT rendition of a Statistica Spreadsheet with the spreadsheet file (.sta). These formats (PDF and XPORT) are recommended in the FDA "Guidance for Industry: Providing Regulatory Submissions in Electronic Format - General Considerations."

Open Architecture System

Just as the entire Statistica system, SDMS is completely programmable, and all of its functionality is accessible to other applications. The system can be customized to accommodate highly domain-specific tasks and can also provide seamless integration into existing systems for data and document management.

SDMS can be easily accessed and customized from a variety of development environments including COM, .NET, VB, VBA, and any other platform (not limited to Windows) that allows or supports intranet/internet communication using SOAP protocol.

System Security Overview

SDMS is a secure system for controlling access to document content. This section provides an overview of the system's built in security features.

User account types. Access to the system is allowed for authenticated users only. SDMS user accounts can be native or integrated. A native SDMS account is one that exists in the SDMS system only (i.e., it is independent of the Windows user account). SDMS maintains the user name and password of this type of account. An integrated SDMS account is one that is associated with a Windows user account and uses the Windows user name (in the form domain \ user) and password to log in to the system.

Integrated accounts. This is the recommended type of account. In most cases, users can be authenticated to SDMS with pass-through authentication (i.e., using their current Windows login for authentication) without having to type in their user name and password again. Thus logging in to the workstation is sufficient to log in to SDMS as well. In some cases, for example if you are logged in to the workstation as one user and logging in to SDMS as another or if you are accessing the SDMS SOAP Server through a firewall, you may have to provide your user name and password. In that case, the SDMS system attempts to log you in to the domain or local machine on the server. The provided credentials must therefore correspond to an active Windows domain user account or local account on the server. Some of the security features of this type of account are:

- SDMS does not store passwords
- When not using pass-through authentication, SDMS will disable the SDMS account (not the Windows account) after a configurable number of failed login attempts with an incorrect password. This event is logged in the system as well as the Windows Event Log.
- Pass through authentication to the SDMS SOAP Server is implemented using IIS Integrated Windows Authentication. It supports, among others, the NTLM and Digest authentication methods which do not transmit passwords over the network.

Native Accounts. Native accounts are maintained by SDMS independent of Windows user accounts. The security features of these accounts include:

- The password itself is not stored in the database and so cannot be compromised. Instead an irreversible cryptographic hash (with salt) of the password is stored. This is a standard and secure technique to protect password security.
- Configurable password security requirements exist to enforce minimum password complexity.
- Passwords expire and require changing after a configurable number of days.
- After a configurable number of failed log in attempts with an incorrect password, the SDMS user account is disabled.
- When an administrator resets a password, it is marked as expired so that the user is forced to change it on his or her next login. Therefore, the administrator does not know the individual user's password.
- User accounts can be disabled at any time or have their passwords marked as expired at any time.

Other security features

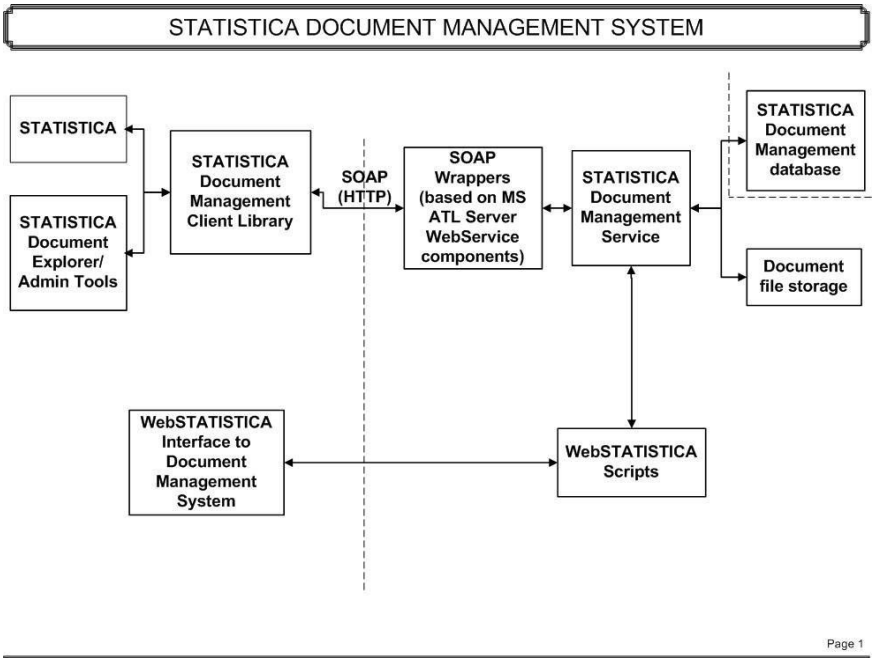
- Supports Secure Sockets Layer (SSL) over HTTP (HTTPS) for communicating with the SOAP Server. When enabled, this means all information and document content sent to or from the remote SDMS SOAP Server is encrypted.
- The database connection string is stored in encrypted form in the system configuration file. Thus the database password is protected. This configuration file (SDMSOpts.xml in the SDMS installation directory on the server) can also be access controlled via standard Windows file security.
- A user's SDMS session will time out after a configurable period of time.

- The actual document content is stored on the server's file system. It can therefore be protected via standard Windows File Security and could also be encrypted using Windows Encrypting File System (EFS). When using EFS on the SDMS Repository, only the user that the SDMS service runs as must be able to decrypt the files (not the individual SDMS users). (It is recommended that administrators understand Windows Encrypting File System and strategies for document recovery before using this.)
- As per 21 CFR Part 11 requirements, executing an Approval (an electronic signature) requires the user to enter his user name and password at the time of the Approval.

Architecture

Overview

SDMS is comprised of several components: a database (SQL server or Oracle), an SDMS Windows Service Process, a Microsoft Management Console (MMC) Snap-In Server Administration tool, and the SDMS Explorer (client application). The SDMS Server Administration tool is used to control the system settings (e.g., security, indexing, and document storage locations); define users, groups, and approval levels; and manage user sessions. The SDMS Explorer (client application) provides the tools for users and groups to store, retrieve, approve and search for documents in a secure, easy-to-manage environment. Both of these applications communicate with the SDMS service (which actually controls the document management environment) via SOAP (HTTP). SDMS is integrated with Statistica Enterprise-wide SPC System, WebStatistica, and PROCEED to provide users with easy access to the files stored in the SDMS database.



SDMS Database

SDMS can be used in conjunction with either a SQL Server 7+ (or MSDE) or Oracle 8+ database. Upon initial installation, the database will be filled with the necessary tables for document storage and management.

SDMS Service

The SDMS Service is the central application for SDMS. It is a Windows service (requiring Windows 2000 operating system or above). Both the client and administrator applications interface with this system through SOAP (HTTP) application.

SDMS Explorer (Client Application)

The SDMS Explorer provides end-user access to the documents stored within the SDMS database. This interface allows the user to view the overall organization schemata in a folder tree (left pane of the SDMS Explorer) and the documents stored within a selected folder in a document view (right pane of the SDMS Explorer). The system requires users to log on with a user name and password. This identifies the user to the system and enables all functions regarding documents to be controlled and tracked. To simplify management of users with similar permissions, users can be assigned to groups. These groups can be assigned permissions to documents and folders.

The main tools of the client application are its document storage interface, search facilities, and permissions.

Document Storage Interface (check in, check out, get latest, document history, etc.). The document storage interface provides the means for users (with appropriate permissions) to create subfolders for document storage, add documents to the SDMS database, check out documents (for editing purposes), and check in documents (with supporting metadata). It also enables users to retrieve the latest version of a document for reading, approve documents, review document and approval histories, and store document renditions.

Search Facilities. SDMS uses Microsoft Indexing Service for indexing document content. Within the client application, users can conduct basic or advanced searches for specific words or phrases. Additionally, they can search for system properties (i.e., checked in, status, file size) and custom properties (i.e., custom-defined document metadata including author, department, expiration date, etc.).

Permissions. Access to documents and folders within the system are monitored by permissions that are assigned at either the folder or document level. Permissions can either be expressly allowed or expressly denied, and they can be assigned at the user or group level. A set of standard permissions (i.e., read, write, delete, list folder contents, set permissions, and approval type permissions) is defined for each SDMS installation.

SDMS Server Administration Tool

The SDMS Server Administration Tool is an MMC Snap-in used to configure the SDMS

service. The main sub-components of the system are user and group management, system settings and approvals.

User management. SDMS supports both native and integrated user accounts. Native accounts keep the user names and (encrypted) passwords in the database, and authentication is performed against this user name and password. Integrated accounts require that the user name/password must be a valid user account on the machine where the SDMS is running. Integrated accounts can support both local machine accounts and domain accounts; however, the user must be a member of a specially-created local machine group, SWS_SDMS_USERS. Only members of this group will be able to login to SDMS.

Every user, both integrated and native, will get a record in the Users table with a unique UserID. That UserID is always associated with this user and will never change. The UserID is used to determine if this user has permissions to perform various operations on documents. It is also used to track the user in the audit and logging operations.

Group management. Groups in SDMS are logical collections of users. Groups are especially useful in that permissions can be assigned to certain groups. Folder and document access can also be controlled at the group level. The Document Administrators and System Administrators groups are predefined within the SDMS system. Members of the System Administrators group are able to administer the system using the Server Administration Tool. They can perform such actions as creating user accounts, defining groups, configuring system settings, and defining Approval types. Members of the Document Administrators group are given full access to document content. In addition, they can create and modify document properties and profiles

System settings. A variety of system settings can be controlled from with the SDMS Server Administration tool. There are seven categories: Database, Files and Directories, Indexing Service, Intervals and Timeouts, Loggings, Security, and Miscellaneous.

- Database settings control the format SDMS uses when querying the SDMS database to retrieve documents and other stored information.
- Files and Directories settings are used to control the location and security of stored documents on the SDMS server.
- Index Service settings are related to the Microsoft Indexing Service used for indexing SDMS content.
- Intervals and Timeouts settings are used to control time related operations and files such as user sessions and temp files.
- Logging settings are used to configure the location and contents of the SDMS log file.
- Security settings are used to control the size and content of SDMS (native user) passwords.
- The Misc settings group is used in managing integrated Windows users.

Approvals. By default, three approval types are defined for the SDMS application: Read and Understood, Approved for internal distribution, and Approved for publication. These default approval types can be deleted or renamed as needed during initial setup. (They can be deleted until they are actually used.) For permissions purposes, approval types are associated with approval levels (level 1–level 5), and any number of additional approval types can be created using the SDMS Server Administration tool. The approval level permissions support allowing or denying individual users or groups the ability to execute none, some, or all approval types.

Approvals are given to a document when it meets specific criteria established by the company and require user authentication and permission before they can be granted.

Installation

Requirements

1. The installation of the Statistica Document Management System (SDMS) entails two parts: server installation and workstation installations on each of the client computers.
2. The installation of the server component of SDMS requires Windows 2000 or Windows XP Professional or higher. Server installation also requires Internet Information Services (IIS) and Indexing Service. These system components should be installed before beginning the server installation.
3. Installation of the workstation client supports Windows 9X, ME, NT, 2000, XP Home and XP Professional or higher.
4. Installation on both server and client requires Internet Explorer 5.5 or higher.

Server Installation (optionally with client):

1. Ensure no other applications are running.
2. Double-click on **Setup.exe** to begin the server installation process.
3. The Welcome dialog box will appear. Click the **Next** Button.
4. In the Setup Type dialog, you will be prompted to select the installation type.
    a. If you want to be able to run SDMS Explorer on the server, select the **Install both SDMS server and client option** button and click **Next**.
    b. If you do not want to run SDMS Explorer on the server, select the **Install SDMS** server option button and click **Next.**

5. In the **License Agreement** dialog box, select **I agree to the terms of the license agreement** and click **Next** to agree with the licensing terms and proceed with the installation.

6. In the Setup Type dialog, select **Complete installation** and click **Next**.

7. When you are asked to register your license with Statistica, fill in the requested information and click **Next**.

8. The registration information can be automatically sent to Statistica by email or manually sent to Statistica after the installation. The installation will be set to expire 14 days after installation and this registration information is required to receive your full and complete licensing for the entire timeframe for your licensing period.

    a. If you want to send the registration information immediately through email, select the first option to automatically email and click **Next**. You may be prompted by your email client that an application is trying to send email. Acknowledge and the email will be sent. If an email client is not available on the server, the second option is recommended.

    b. If you wish to send the registration information manually, select the second option for all other methods and click **Next**.

    c. You will then be prompted for a location to save the registration information. Select the location and click **Next**.

9. In the Database Install Type dialog, select whether you would like to create a new SDMS database or use an existing database.

10. In the Database Management System Selection dialog, you will be presented with a dialog prompting for Database selection. Select the Database Management System of your choice.

SQL Server or SQL Server/MSDE:

In the Data Link Properties dialog, on the Connection tab, enter or select the server name where the SQL Server Database is located, enter the information required to gain access to the server, and select the database on the server where the SDMS schema will be applied. If a specific DB user name is specified, be sure to check the **Allow saving** password box.

Click **Test Connection** to ensure that the connection information is correct.

If the test connection is successful, click **OK** to apply the connection information. If the test is unsuccessful, verify that the connection information is correct and try again.

ORACLE:

In the Data Link Properties dialog, on the Connection tab, enter the name of the server where the Oracle Database is located and enter the information required to gain access to the database. Click Test Connection to ensure that the connection information is correct.

If the test connection is successful, click OK to apply the connection information. If the test is unsuccessful, verify that the connection information is correct and try again.

If installing to a new database, the database tables and views will be created at this time.

1. In the Ready to install program dialog, click Install to process the installation of the files and other required system updates. A progress bar will be shown advising on the status of the installation process. Note the installation of MSDE (if selected previously) will take more than 7 minutes.

2. Once the installation is complete, you will be prompted to finish the installation. Click the Finish button to complete. When necessary, the installation process may require a reboot of the operating system (i.e., for installing XML Parser). The reboot (if prompted) is required before you can use SDMS.

Note that a default account is setup within the SDMS. The user name is Admin with a password of 111111.

Client Installation:

Using the Server installation instructions as directed above will result in both a server and client installation on the SDMS Server. To install the client on additional workstations, use the following steps:

3. Browse to the Workstation Installer folder on the server (as installed above) and

4. The Welcome dialog will be displayed. Click the **Next** button.

5. In the Setup Type dialog box, select the **Complete installation** option button and click **Next**.

6. In the Ready to install program dialog box, click **Install** to process the installation of the files and other required system updates. A progress bar will display advising on the status of the installation process.

7. During the installation, system updates may need to be applied. Some updates, such as XML parser, will launch a separate installation routine. Advance through the installation routines for any required updates.

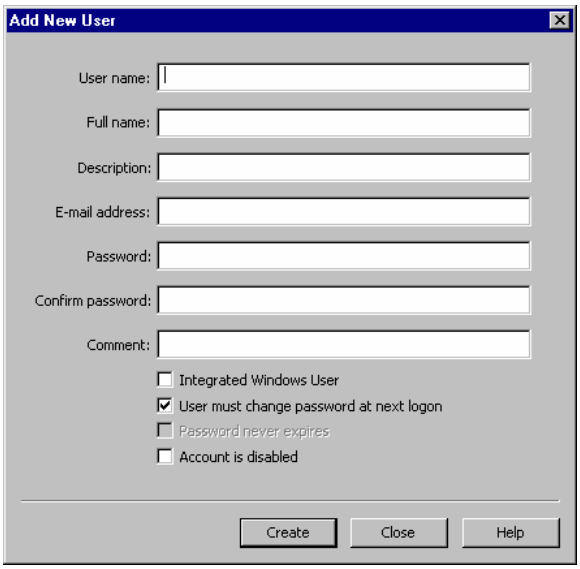
8. After the files have been copied to your computer, click **Finish** to complete the installation. When necessary, the installation process may require a reboot of the operating system (i.e., for installing XML Parser). The reboot (if prompted) is required before you can use SDMS.

Configuration

Defining SDMS Users

Initially, two users are defined for SDMS: System (used internally) and Admin (password 111111). New users are defined using the SDMS Server Administration tool.

Creating a new user (native or integrated). To create a new user, you must log in to the SDMS Server Administration tool as Admin (or as a user in the System Administrators group). From the Action menu (or the Users folder shortcut menu), select **New User** to display the Add New User dialog box. SDMS supports two types of users: integrated Windows users and native (or local) users. Both types of users can be created using this dialog, although Importing Windows Users and Groups, see below, describes the recommended method for importing multiple Windows users at once. The dialog works much like a form. Once you click the **Create** button, the fields are cleared enabling you to create additional users.



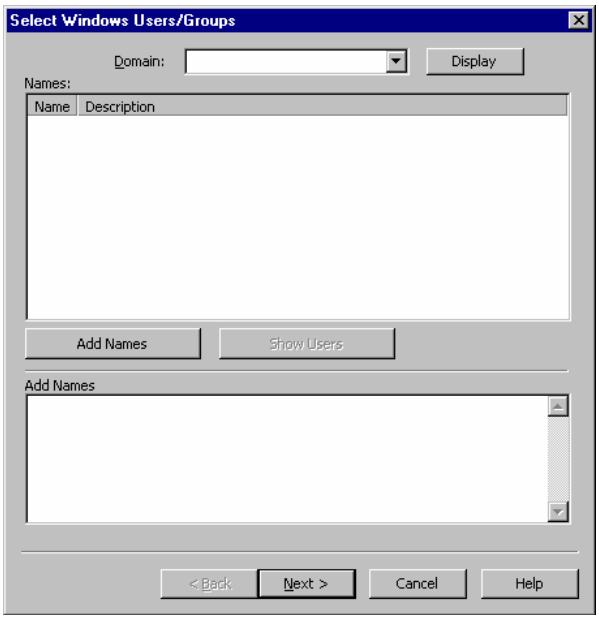
Creating a native user. Enter values for each field shown in the dialog (note that Description and E-mail address are optional), and verify that the **Integrated Windows User check box** is cleared. You can require that the user enter a new password by selecting the User must change password at next logon check box. To select the **Password never expires** checkbox, you must first clear the **User must change password at next logon** checkbox. Once you have specified all the relevant information for the new user, click Create.

Creating an integrated Windows user. Note that SDMS cannot be used to create windows users. This option simply enables you to create an SDMS account for an integrated Windows user. Integrated Windows users can also be imported into SDMS (see Importing Windows users and groups, below).

To create an SDMS user account for an integrated Windows user, enter the domain name \ user name for the Windows user in the User name field, then select the **Integrated Windows User** check box. No other fields are required. Click the **Create** button to add the user to SDMS and clear the fields in this dialog.

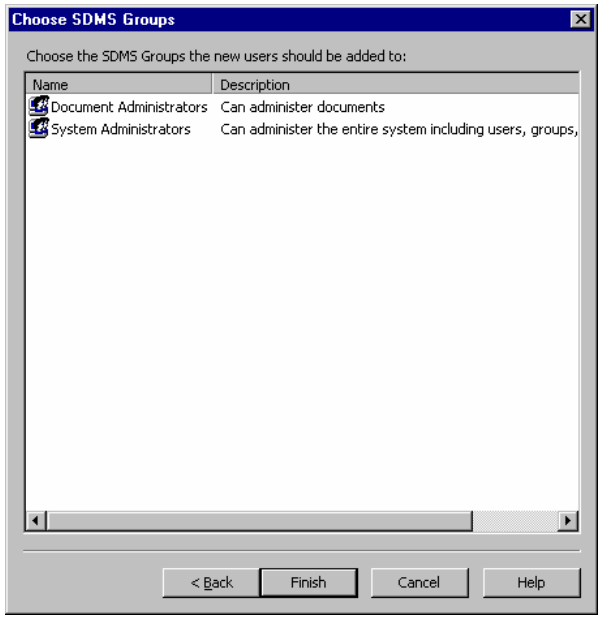
Note that users are assigned permissions to specific folders or documents using the SDMS Client application. All Windows user accounts must be members of the local machine group SWS_SDMS_USERS before they can be added or imported into SDMS.

Importing Windows users and groups. Select Import Windows Users from the Action menu when the Users folder has been selected, or right-click the Users folder and select Import Windows Users from the shortcut menu to display the Select Windows Users/Groups dialog. Use the options on this dialog to create (import) integrated Windows accounts.



Note that while you cannot import a Windows group as an SDMS group (all SDMS groups are defined locally) you can import Windows users by selecting Windows groups. All the users in the selected group will be imported as SDMS users.

First select (or enter) a domain name, then click Display to show a list of available Windows groups. You can display user names by clicking the Show Users button. Select the desired groups and users, and then click the Add Names button. Once you have finished selecting users and groups, click the Next button to display the Choose SDMS Groups dialog.



By default, two groups are defined within SDMS: Document Administrators and System Administrators. Additional groups can also be defined (see documentation, below). Select the groups to which the imported users should be assigned, then click Finish to display the Confirm Selections dialog. You can use that dialog to confirm users and their group assignments. When you click OK on that dialog, all the selected users will be added to SDMS.

Remember, Windows user accounts must be members of the local machine group

SWS_SDMS_USERS before they can be added or imported into SDMS.

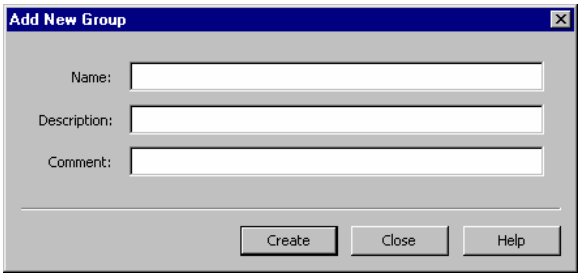
Defining SDMS Groups

Groups are collections of users and are defined locally. There are two special groups given fixed group ID's: Document Administrators and System Administrators. Document Administrators can perform all administration regarding documents and folders, and System Administrators can manage users and groups.

Document Administrators. Users in the Document Administrators group are able to perform any operation on a document or folder, regardless of any explicit permissions. In addition, they can create and modify document profiles and properties.

System Administrators. If a user belongs to the System Administrators group, then this user can perform system administrator functions such as adding new users, changing passwords, adding groups, setting group memberships, etc. Of course, the System Administrator can assign users to groups, so they can make anyone a member of the Document Administrators group.

Creating new SDMS groups. To create a new group, you must log in to the SDMS Server Administration tool as Admin (or as a user in the System Administrators group). Select the Groups folder in the tree view and then select New Group from the Action menu or the Groups folder shortcut menu to display the Add New Group dialog.



For each group you want to create, enter a Name, Description, and Comment. The dialog works much like a form. Once you click the Create button, the fields are cleared, and you can create additional groups. Note that groups are assigned permissions to specific folders or documents using the SDMS Explorer.

Integrated Log In

In accordance with FDA regulation 21 CFR Part 11, SDMS requires users to log on with a user name and password. This identifies the user to the system and enables all functions regarding documents to be controlled and tracked. An option for integrated log in is provided on the SDMS Login dialog. When this option is selected the application will attempt to log in using the credentials of the currently logged in Windows user. If that log in fails (e.g., the integrated Windows user for that machine has not been imported into SDMS), then the SDMS Login dialog will be displayed

Document Security

Document permissions are used to ensure that the current user is allowed to perform the desired operation on the specific document. Every document has a set of effective permissions for each user. These permissions can be explicitly applied at the document level or recursively inherited from parent folders. Permissions can either be expressly granted or expressly denied, and they can be at the user or group level.

Within SDMS Explorer, they are assigned at either the folder level (Folder Settings - Security tab) or the document level (Document Settings - Security tab). The set of available permissions is described here.

Read. Users with read permissions on a document can read and download documents but are unable to modify them. Read permission on a folder is required to move a document out of the folder.

Write. Users with write permissions on a document have Check Out and Check In abilities as well as the ability to change document properties via the Document Properties dialog. Write permission on a folder allows moving a document into a folder and adding new documents to the folder.

Delete. Users with delete permissions are able to delete documents and folders.

List Folder Contents. Users with this permission can view the contents of a folder including its documents and its child folders. If this permission is denied for a folder, the user will be unable to expand the folder in the folder tree and unable to see the documents in the folder.

Set Permissions. Users with this permission can allow or deny permissions for groups and users at either the folder or document level.

Read and Understood Approve. Users with this permission are able to approve a document indicating that they have read and understood its content. This is the **Group 1 Approve** permission. By default it is associated with the **Read and Understood** Approval Type. If this approval type is changed, the displayed name of the permission will change in the permissions dialog.

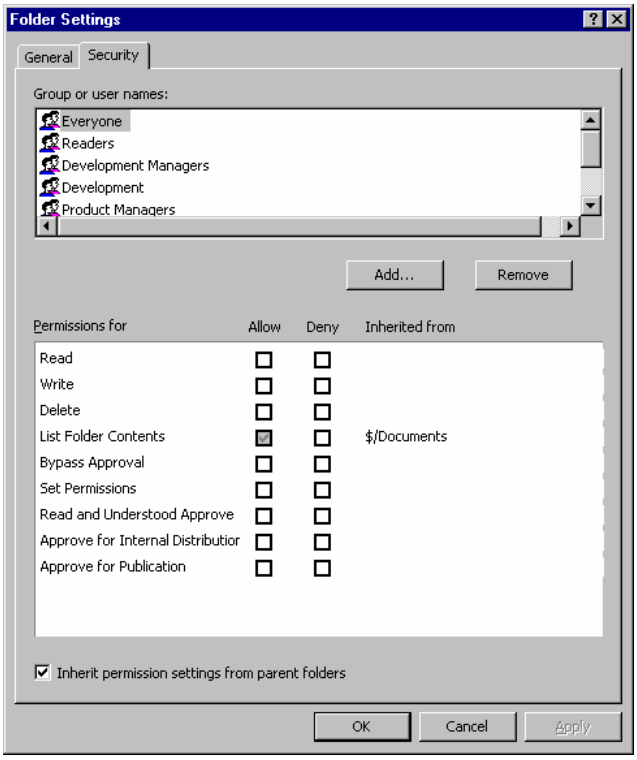
Approve for Internal Distribution. Users with this permission are able to approve a document for internal (company) distribution. This is the **Group 2 Approve** permission. By default, it is associated with the **Approved for Internal Distribution** Approval Type. If this approval type is changed, the displayed name of the permission will change in the permissions dialog.

Approve for Publication. Users with this permission are able to approve a document for publication (i.e., external distribution). This is the **Group 3 Approve** permission. By default, it is associated with the **Approved for Publication** Approval Type. If this approval type is changed, the displayed name of the permission will change in the permissions dialog.

By default, there are no Approval Types associated with the **Group 4 Approve** and **Group 5 Approve** permissions; therefore, these do not show up in the permissions dialog. If new Approval Types are added and configured to use these permissions, they will be displayed.

Assigning Permissions

An SDMS Administrator can assign permissions to folders (or individual documents) within the SDMS Explorer. To assign permissions at the folder level, right-click a folder in the folder tree, and select **Settings**. Permissions are assigned on the Security tab of the Folder Settings dialog. Note that settings on the Document Settings – Security tab are identical to the settings described here.



Group or user names. This list box displays the group names and user names that have either explicit or inherited permissions settings on this SDMS document or folder. Select a **Group** or **User** name in the top pane of the dialog to view or change the permissions in the bottom pane of the dialog. To view permissions for a specific Group or User, click the **Group** or **User** name. Permissions for the selected Group or User will be displayed in the second list box as well as whether the permissions have been inherited from a specific Group or folder.

Permissions for. A variety of tasks can be performed by users in SDMS. These include reading and writing to documents, deleting folders and documents, listing (and viewing) folder contents, setting permissions for users and groups, bypassing the approval process and granting approval types to documents. Available permissions are listed in this box.

Allow/Deny. Select a check box adjacent to the specific permission to Allow or Deny that permission for the selected User or Group. A selected, grayed box indicates that the specific permission has been inherited either from a Group or folder. Grayed out permissions cannot be changed for the selected group or user name, but a User with appropriate permissions can go to the folder or group in which the permissions originated and change permissions.

Inherited from. Permission settings can be inherited from a group or folder. In that case, this column displays the source of the permission setting. If a user name is selected in the Group or user Names list box, then the Inherited From column may show a group name or a folder name (preceded by "$"). If a group name is selected, a folder name may be displayed. If a Group name is displayed in the Inherited From column, the user can select that group name in the Group or user Names list box to determine from which folder the permission setting is inherited. If a folder name is displayed, the user could go to that folder's permissions dialog and modify the setting as desired. Thus the Inherited From column allows you to trace the ancestry of inherited permissions. If nothing is displayed in the Inherited From column, then the permission setting is on the current document or folder and can be changed.

Add. Click the Add button to display the Groups and Users dialog, where you can add new groups or users.

Remove. To remove a Group or User from this folder, select the group or user name and click the Remove button. A Group or User displayed here due to permissions inherited from a parent folder cannot be removed from the list. In that case, any explicit permissions settings on the current document or folder are removed, but the user or group name will not be removed from the list.

Inherit permission settings from parent folders. By default, all documents and folders inherit permissions settings from their parent folders. Clear this check box to break this inheritance chain and define new permissions for the selected document or folder (and its children) regardless of the parent folder's settings.

Permission checking implementation. In order to effectively assign permissions, it is important to understand how SDMS implements permission checking. Whenever an action is attempted on a document or folder, the system uses the following process to determine whether to allow or deny the action.

First, the system determines if there is an Allow or Deny setting for this user on this document (folder). If so, that setting is used. If not, the system determines if there are any settings for any of this user's groups on this document (folder). Deny takes precedence over Allow, so if any of the user's groups has a Deny setting, the action is not allowed. Otherwise if an Allow setting is present for any of the user's groups, the action is allowed. Note that explicit user level settings take precedence over the user's group level settings. This means that if a group has a Deny but the user has an Allow, the action is allowed. If settings are not found for the user or any of his groups and if the document or folder does not inherit permissions from its parent folder, then checking stops and the action is denied. If it does inherit permissions, the checking continues up the chain of parent folders.

The permissions on the parent folder are checked in the same way. If a setting exists for this user on this folder, that setting is used. If not, the system determines if any of the user's groups has a setting on this folder and if so it is used with any Deny taking precedence. Checking continues up the folder tree until a setting is found, a folder that does not inherit permissions settings is encountered, or the root folder is reached. If no setting is found, the action is denied.

Note that permission checking proceeds up the folder tree not down to ensure that the nearest setting is always used. An Allow on the immediate parent folder would override a Deny on a grandparent folder.

Password Security

For native SDMS user accounts, as opposed to Integrated Windows user accounts, password security (i.e., password size and content, number of allowed failed login attempts) is controlled via the SDMS Server Administration tool. For integrated users, password security is controlled by the operating system. A System Administrator can modify security system settings as needed. The following settings are available:

Incorrect Password Disable Interval. Use this system setting to specify the minimum amount of time (in minutes) during which consecutive failed logins due to an incorrect password will cause a user's account to be disabled. For example, if this is set to 60 minutes, then a user's account will be disabled after N consecutive incorrect passwords within any 60 minute interval. The number (N) of consecutive incorrect passwords which can be attempted is set via the Max Incorrect Password Login Attempts system setting.

Max Incorrect Password Login Attempts. Use this system setting to specify the number (N) of consecutive failed logins due to incorrect passwords which can be attempted in a given interval before the user's account will be disabled. For example, when this is set to 4 and a user attempts to log in with an incorrect password more than four times in the given time period, his/her account will be disabled. Use the Incorrect Password Disable Interval system setting to specify the minimum amount of time (in minutes) during which consecutive failed logins due to an incorrect password will cause a user's account to be disabled. Note that for integrated users, only the SDMS user account (i.e., not the operating system user account) will be disabled.

Min Password Digits. Use this system setting to specify the minimum number of unique digits to require for native user passwords. For example, if this is set to 2, then native users are required to have two unique numbers in their password.

Min Password Length. Use this system setting to specify the minimum password length for native users. For example, if this is set to 8, then native users are required to have at least 8 characters in their password.

Min Password Letters. Use this system setting to specify the minimum number of unique letters to require for native user passwords. For example, if this is set to 2, then native users are required to have two unique letters in their password.

Min Password Lower Case. Use this system setting to specify the minimum number of unique, lower case letters to require for native user passwords. For example, if this is set to 2, then native users are required to have two unique, lower case letters in their password.

Min Password Non-Alphanumeric. Use this system setting to specify the minimum number of unique, non-alphanumeric characters (e.g., |, $, %, etc.) to require for native user passwords. For example, if this is set to 2, then native users are required to have two unique, non-alphanumeric characters in their password.

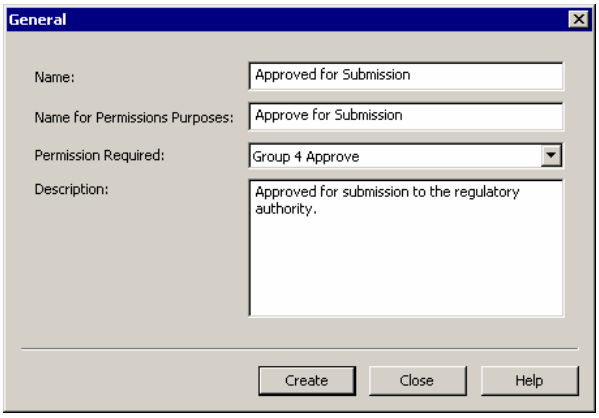
Min Password Upper Case. Use this system setting to specify the minimum number of unique, upper case letters to require for native user passwords. For example, if this is set to 2, then native users are required to have two unique, upper case letters in their password.

Password Age. Use this system setting to specify the number of days before a native user's password will expire.

Approval Types

Approval types can be added or edited in the Server Administration tool. The available approval types will be displayed to users when they attempt to approve a document in the SDMS Explorer client application. The system supports up to five levels of permissions for approvals so that users can be allowed or denied the ability to grant different approval types.

To add a new approval type, select **Document Approval Types** in the Server Administration tree view. From either the Action menu or the shortcut menu, select **New Approval Type**. The New Approval Type dialog box will be displayed.



In the Name field, enter the text you want users to see when they are executing an approval. Once a user has been authenticated to the system, (s)he can select from a list off approval types (such as **Approved for Submission**). The Name for Permission Purposes is the text that will be displayed on the Security tab of the Document/Folder Settings dialog for the purpose of assigning permissions. Use the **Permission Required** drop-down list box to assign a level of permission required for users to grant this approval type.

Properties and Profiles

Each document in the system is associated with a collection of properties known as a profile. Properties are document metadata that are entered by users when they add or check in a document. There are several types of properties, and they can be optional or required. The system supports sophisticated searching for documents based on property values.

Profiles are collections of properties. The system allows administrators to create any number of properties and profiles and assign any number of properties to each profile. Each folder in the system has a default profile associated with it. The profile can be assigned explicitly or inherited from the parent folder, and it can be viewed or assigned on the Folder Settings dialog in the SDMS Explorer. By default, new documents added to the system will have their parent folder's default profile assigned to them. However, the user adding or checking in the document can change the profile associated with the document.

Property types. The system supports these property types.

- **Text.** A text property for properties such as **Author, Department**, etc.
- **Long Text**. A text property for larger, free form text values such as a **Description** property.
- **List.** A list property has a list of potential values associated with it. During check in, the user is able to select one of the pre-assigned list values. Optionally, the list property can enable users to enter custom values that are not in the list of pre-assigned values.

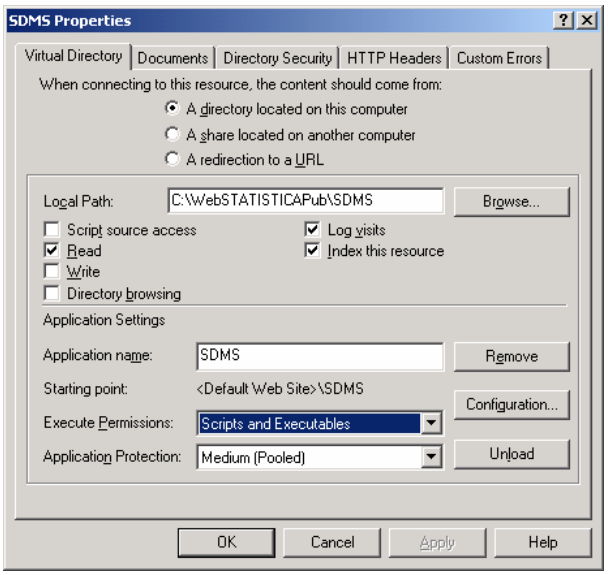
- **MultiList.** A multilist is similar to a list property; however, users are able to select more than one of the pre-assigned list values. MultiList properties can also be configured to enable users to enter custom values that are not in the list of pre-assigned values
- **Integer.** A numeric property with no fractional part.
- **Double.** A real number with decimal/fractional part.
- **Date.** A date and time property.
- **Boolean.** A true/false property.

Properties and profiles are edited and created in the SDMS Explorer. From the Tools menu, select Profile and Property Management.

IIS Configuration

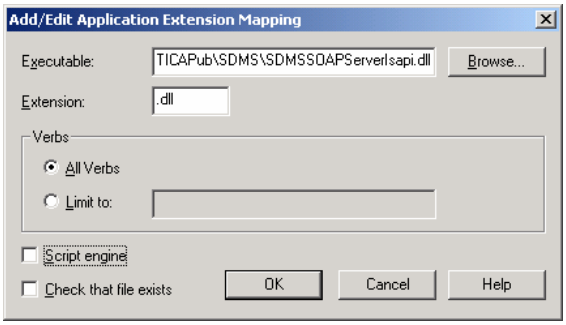
In most cases, the installer configures Microsoft Internet Information Services (IIS) for use with SDMS. This section describes the IIS configuration if customization is required. Some familiarity with administering IIS is assumed. Other than what is described here, the default IIS settings for a new virtual directory are acceptable.

The SDMS Server installation creates a virtual directory called SDMS under the Default Web Site on the server. At a minimum this Virtual Directory must grant Read access. It also installs an ISAPI extension dll, SDMSSOAPServerIsapi.dll. By default it is under C:\WebStatisticaPub\SDMS. This must be configured as a Web Application under IIS, as depicted below:

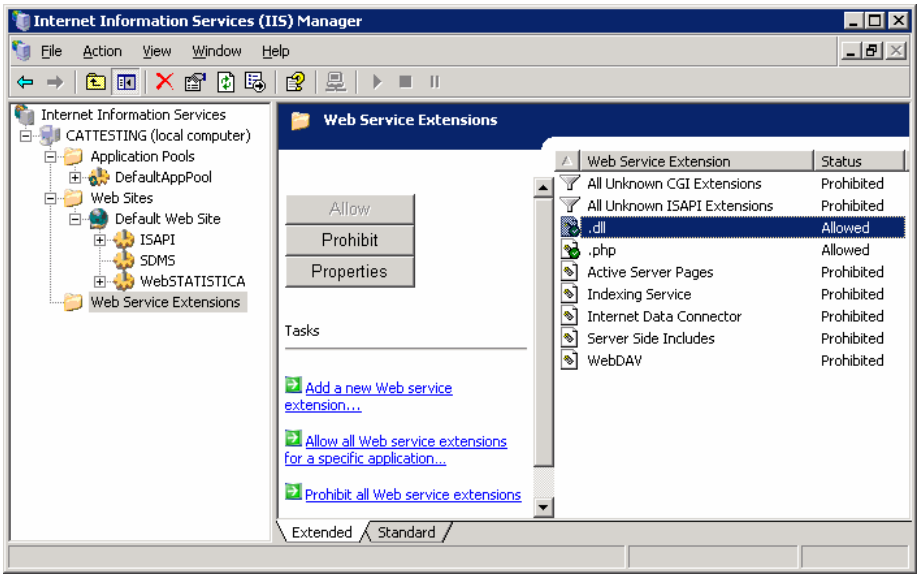


Scripts and Executables must be selected in the Execute Permissions list box. The Application Protection option can be any available setting; by default, it is Medium (Pooled).

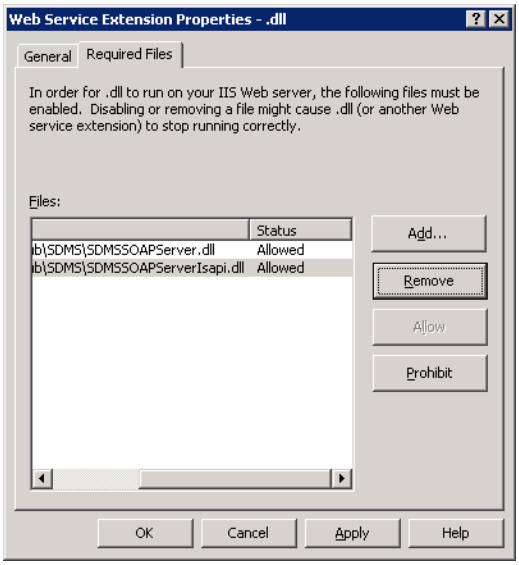
Click the **Configuration** button to display the Add/Edit Application Extension Mapping dialog box and create an extension mapping for the .dll extension.



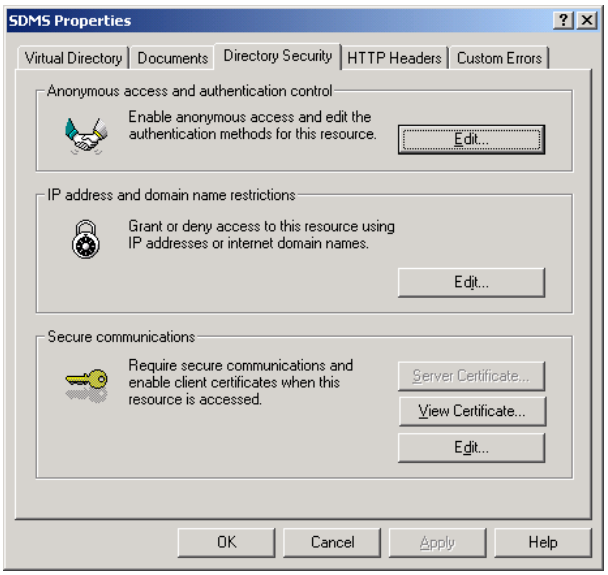
As illustrated above, the .dll extension must be mapped to the SDMSSOAPServerIsapi.dll file. On Windows Server 2003, the Web Service Extensions must be configured as well. The .dll extension must be allowed as shown below:



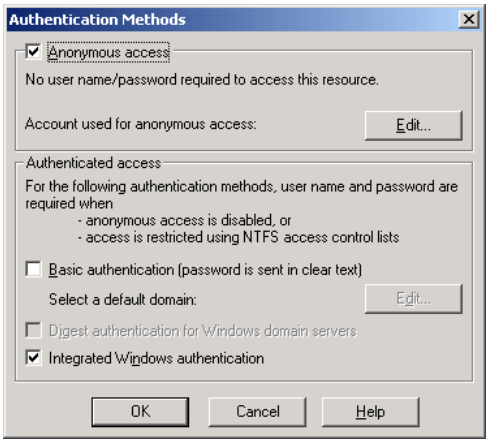
Also, the SDMS Web Service dlls must be added. To do this, select **Properties** in the IIS Manager to display the Web Service Extension Properties dialog box:



As shown above, the files SDMSSOAPServer.dll and SDMSSOAPServerISAPI.dll must the **Allowed status.** By default, these files are installed to C:\WebStatisticaPub\SDMS. Finally, the directory security must be set from the SDMS Virtual Directory Properties dialog.



On the Directory Security tab, click the **Edit** button in the Anonymous access and authentication control section to display the Authentication Methods dialog.



On this dialog, you can configure the supported authentication methods. By default, Anonymous and Integrated Windows (NTLM) are allowed. SDMS Integrated Windows Authentication is implemented via IIS. Therefore, to support integrated SDMS login, select one of the authenticated access methods. SDMS supports Basic, Digest, and Integrated Windows (NTLM.)

Anonymous access can be prohibited depending on requirements. If your site will allow SDMS users to access the system from outside the firewall or over the internet, you will most likely need to allow Anonymous access to the Web Server. Alternatively, you could use Digest or Basic authentication methods as these can work through firewalls and proxies (NTLM cannot).

Note that when anonymous access is turned on, anyone can access the SDMS SOAP server, but they must still provide valid SDMS credentials to log in to the SDMS system. Requiring authenticated access simply provides an additional layer of security.

The user accounts that will connect to this Web Server, including the anonymous account if enabled (IUSR_MACHINENAME by default) must have read access to the Web Application files in C:\WebStatisticaPub\SDMS and also read and execute access to the SDMSServicePS.dll file in the SDMS installation directory (C:\Program Files\Statistica\SDMS by default). Normally, giving read and execute permissions to SWS_SDMS_USERS group and IUSR_MACHINENAME is sufficient.

Document Repository

By default, documents in the system are stored in the Document Repository under C:\Program Files\StatSoft\SDMS\Data\Documents. The file structure here is independent of the folder structure in SDMS. Normally, administrators and users would not directly access document content in the repository. Note that no document content is stored in the RDBMS database; rather all document content is stored on the file system. The file names here are of the form documentid (revisionnumber).ext.

Access to the physical document repository should be controlled with standard Windows file security to prevent unauthorized access to document content from outside the SDMS system. Note that setting Windows file security on the Document Repository has nothing to do with SDMS access control from within the system; SDMS manages those permissions from within SDMS. Documents should not be modified directly in the repository, (outside the SDMS system) because SDMS stores a checksum of each document and detects changes to the documents from outside the system. When any such change occurs, SDMS will mark the document as corrupted.

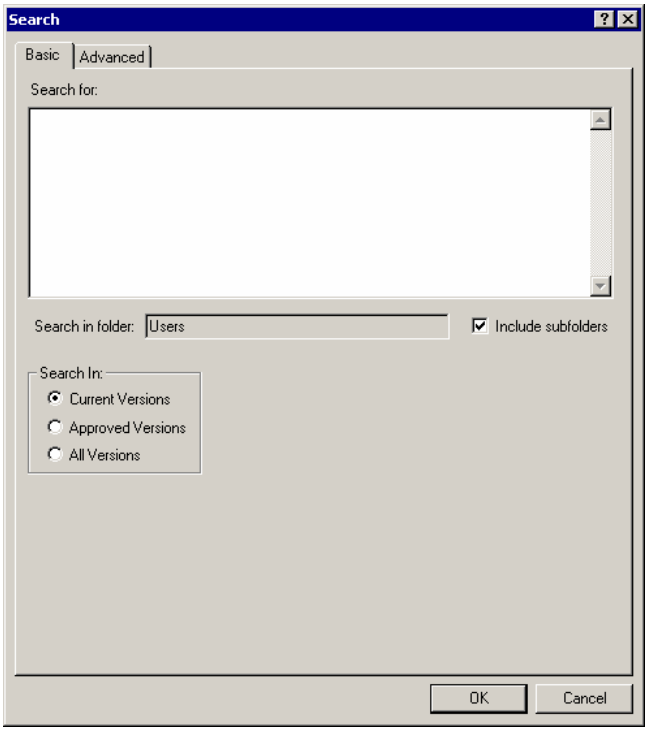
Search; Microsoft Indexing Service Configuration

Search in SDMS is implemented with Microsoft Indexing Service. The SDMS system maintains a mirror of the SDMS folder structure known as the Proxy File Path. By default, it is stored under C:\Program Files\StatSoft\SDMS\Data\ProxyFiles. The actual SDMS folder structure is stored in the RDBMS database. The proxy file path is a mirror of this folder structure containing proxy files that MS Indexing Service indexes for search purposes. This allows searches based on both document content and document property values.

Each document revision in SDMS has a corresponding proxy file. This is an XML file containing information about the real document including its properties for indexing purposes. If this directory becomes corrupted or lost, its content can be deleted; SDMS will re-create it the next time the SDMS service starts.

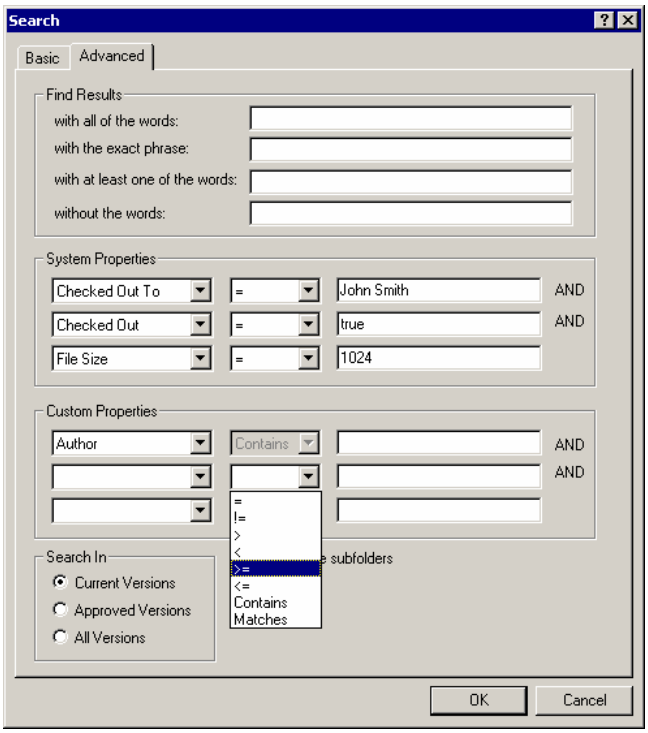
By default, Indexing Service can index several file formats including MS Office documents and common text file types including text files and html files. Additional file types can be indexed if the vendor for that particular file format provides a filter dll. For example, ADOBE provides a freely available filter dll for use with MS Indexing Service to allow filtering of PDF documents. Statistica provides a filter dll for Statistica file types. If you need to search file content for unsupported file types, please inquire with that file type's vendor to determine if they provide a filter dll.

Basic search. Basic searching based on document content, system properties, and custom textual properties is available out-of-the-box. Certain types of advanced property value searches require some additional MSIS configuration (described below). Search is performed from the Search dialog in the SDMS Explorer application. (Select Search from the Folder menu.)



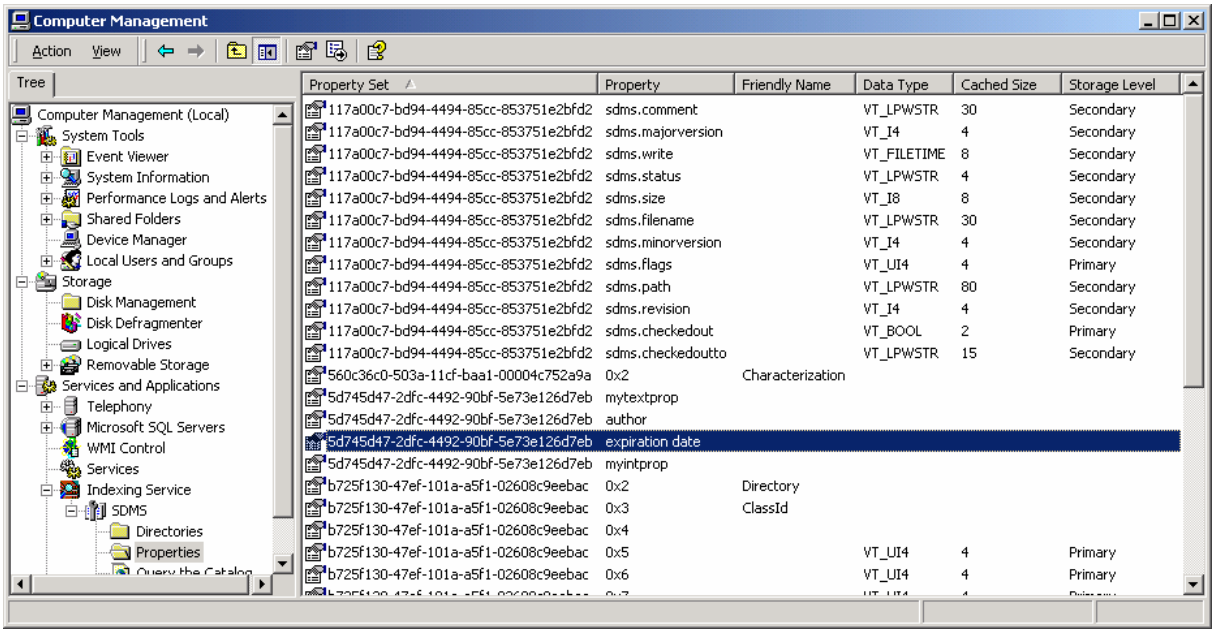
In the Search for edit box, you can type simple words or phrases and then search for documents containing those words or phrases. Use quotes for phrase matching. Advanced users can type more complex queries here using Microsoft's Query Language, Dialect 2. The full syntax of this language is documented by Microsoft on MSDN. (An internet search on **indexing service query language** will provide a starting point.)

Advanced search; property value searches. SDMS supports several options for property value searching. You can search for documents where some site-defined custom property Contains some value, Matches some regular expression, and/or passes some logical test with operators including >, <, >=, <=, and !=. These are all available on the **Advanced** tab of the Search dialog box in SDMS Explorer:



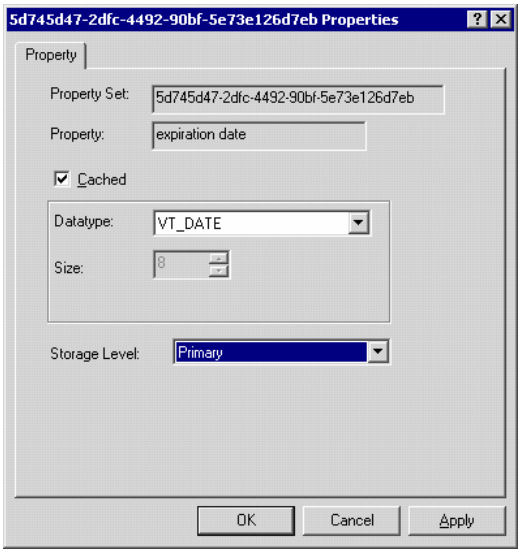
By default, MS Indexing Service does not cache property values. This means that for the Custom Properties, the only type of property value search available is a textual contains search, such as **Author Contains Smith**. In order to use regular expression or logical tests in property value searches, MSIS must be configured to cache the property. Notice in the above screen shot that the Custom Property Author allows only a **Contains** based search; the combo box for choosing a search operator is disabled. This is because the Author property is not cached by MSIS. Non-text type properties such as dates and numeric properties are not displayed here because they cannot be searched for unless they are cached.

Caching custom properties. Suppose you have a custom date property named Expiration Date and you want to be able to search for documents based on values of this property. First, check in at least one document containing a value for this property. At this time, the Expiration Date property will NOT be displayed on the **Advanced** tab of the SDMS Search dialog in SDMS Explorer because it is not cached yet. Open the **Computer Management Snap In** on the server:



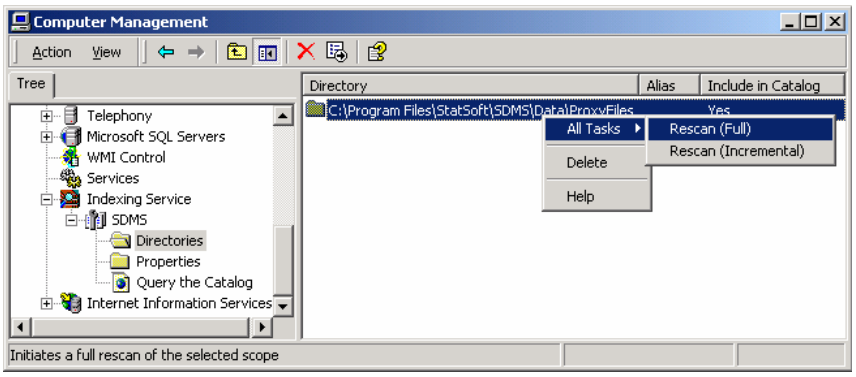
After Indexing Service has finished indexing this document, note that the expiration date property shows up in the Properties folder of the SDMS Catalog under the Indexing Service management branch. (You might need to right-click **Properties - All Tasks - Refresh List**.)

In the Computer Management Snap In, right-click the expiration date and select **Properties** to display this dialog:

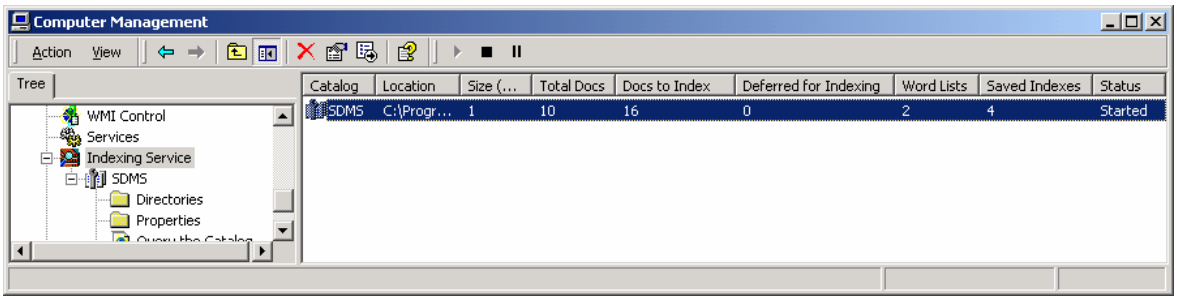


Select the **Cached** check box, and set the **Datatype** to **VT_DATE**. **MSIS** has two storage levels: primary and secondary. MSIS will keep as much of the information from primary and secondary caches in memory as possible to provide fast access. The primary cache has precedence for memory usage over the secondary cache, so typically the primary cache contains only a few, important, value-type properties. This means the values in the primary cache are usually memory-resident, and those in the secondary cache are memory-resident if there is enough storage available.

After you click **OK**, MSIS warns you that you must restart **Indexing Service** and initiate a full rescan to cache the property values for already filtered documents. To restart the Indexing Service, right-click **Indexing Service** in the tree, and select **Stop**. Then, right-click **Indexing Service**, and select **Start**. To initiate a rescan, select the Directories folder under SDMS, right-click the **Proxy File Directory**, and choose **Rescan(Full)**:



You can monitor the progress on the Computer Management dialog.



When the Docs to Index column is zero, the rescan is finished. This may take a while if the repository is large. Now restart the SDMS Explorer client application and select **Search** from the Folder menu to display the Search dialog box. Expiration Date should now be included in the list of Custom Properties on the Advanced tab.

As indicated by Microsoft's documentation for property value queries, date time values should be of the form yyyy/mm/dd hh:mm:ss or yyyy-mm-dd hh:mm:ss. Your date value queries should now work as expected.

Other SDMS property types can be cached in MSIS as the following types:

SDMS Property Type	MSIS Datatype	Notes
Text,LongText,List,Multilist	VT_LPWSTR	
Boolean	VT_BOOL	Usetortrue,forfalseforvaluequeries
Integer	VT_I4	
Double	VT_R8	
Date	VT_DATE	yyyy/mm/ddhh:mm:ssoryyyy-mm-ddhh:mm:ss