Caseware SmartSync Server

Getting Started Guide

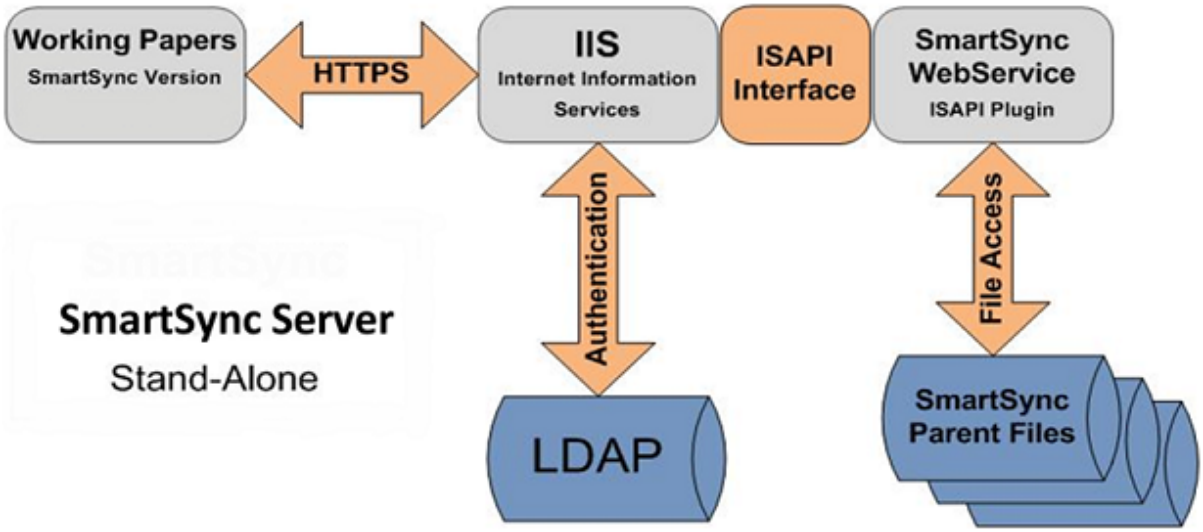
caseware

Caseware International Inc.
1100–351 King St East, Toronto, ON, M5A 0L6, Canada
T: +1 416-867-9504 | F: +1 416-867-1906 | E: info@caseware.com

Contents

Introduction

SmartSync Server is an add-on for Microsoft Internet Information Server (IIS). If you have a Windows server, you already have IIS available.



ISAPI Server component

Most organizations will not require any additional hardware to implement SmartSync Server. Simply install SmartSync Server as an add-on to your current web server to get started.

SmartSync file traffic

After installing SmartSync Server, all SmartSync traffic within your organization transmits through it. By utilizing the latest web services technology, SmartSync synchronizes your files from anywhere with an Internet connection.

Pass-through authentication

SmartSync Server authenticates users by leveraging your existing Windows Active Directory system; you don't require additional passwords or credentials. If a user can log onto their computer, then they can access SmartSync Server.

SSL/HTTPS support

To ensure confidentiality, SmartSync Server supports SSL and HTTPS encryption. All file updates synchronized through SmartSync Server are encrypted during transmission, so your client information stays safe even when you're working off-site.

Using multiple SmartSync Servers

You can employ multiple SmartSync Servers by installing multiple instances on a single IIS server or by using a load balancer to switch between multiple servers.

Binding multiple SmartSync Servers to an IIS server

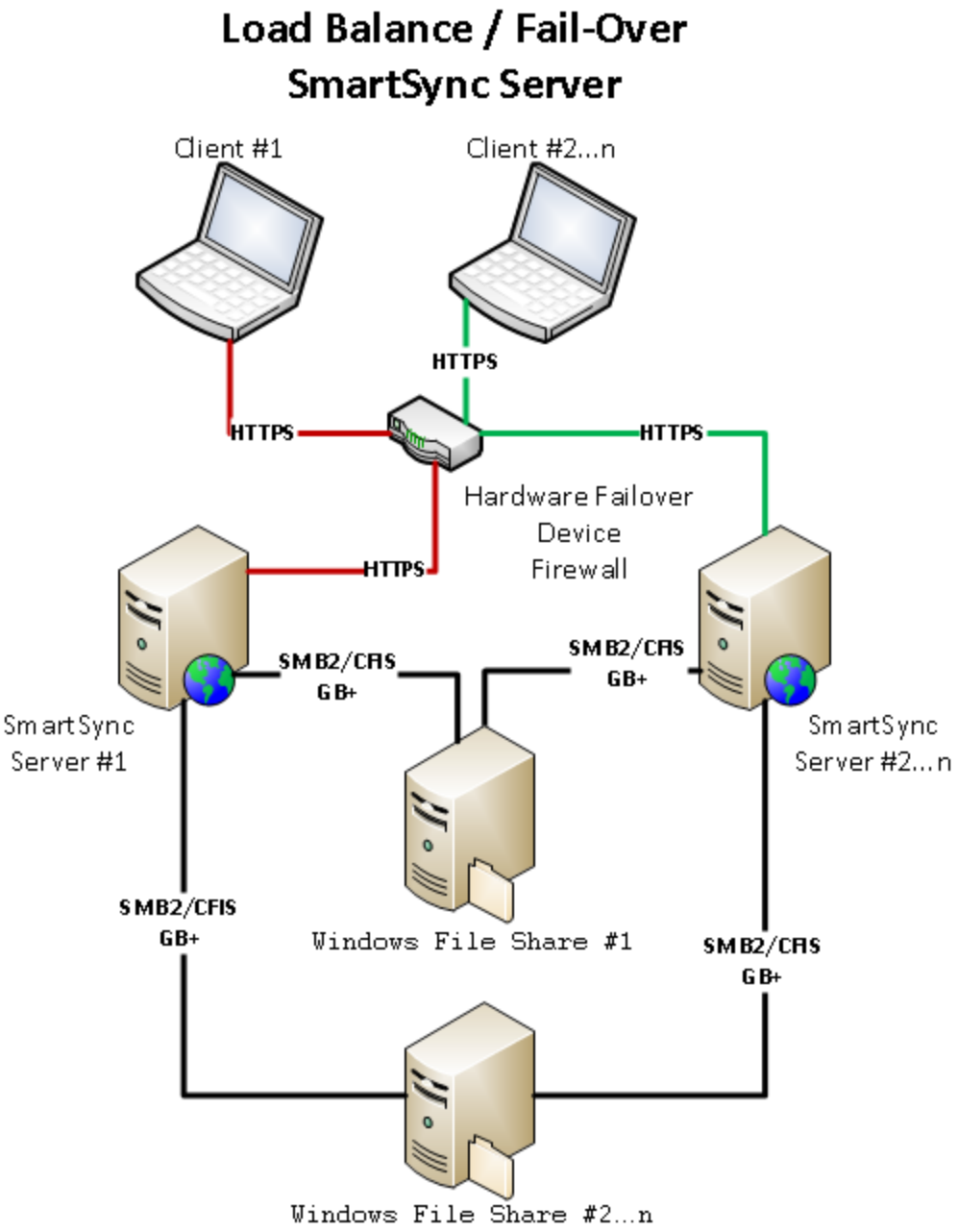
To run multiple SmartSync Servers on a single IIS server, each SmartSync Server needs to be set up in its own folder using the manual installation method. The handler mappings setup points to the alternate folder so that a different SmartSync Server is referenced. This involves adding a separate application pool to use for the extra server. A separate binding also needs to be set up for each extra SmartSync server.

Load balancing multiple SmartSync Servers

Multiple SmartSync Servers can be configured together for high availability using a load balancer. This type of scenario requires that the load balancer is able to direct traffic using "sticky" sessions so that the same SmartSync Server is used to answer the requests for any given client unless a failover scenario occurs.

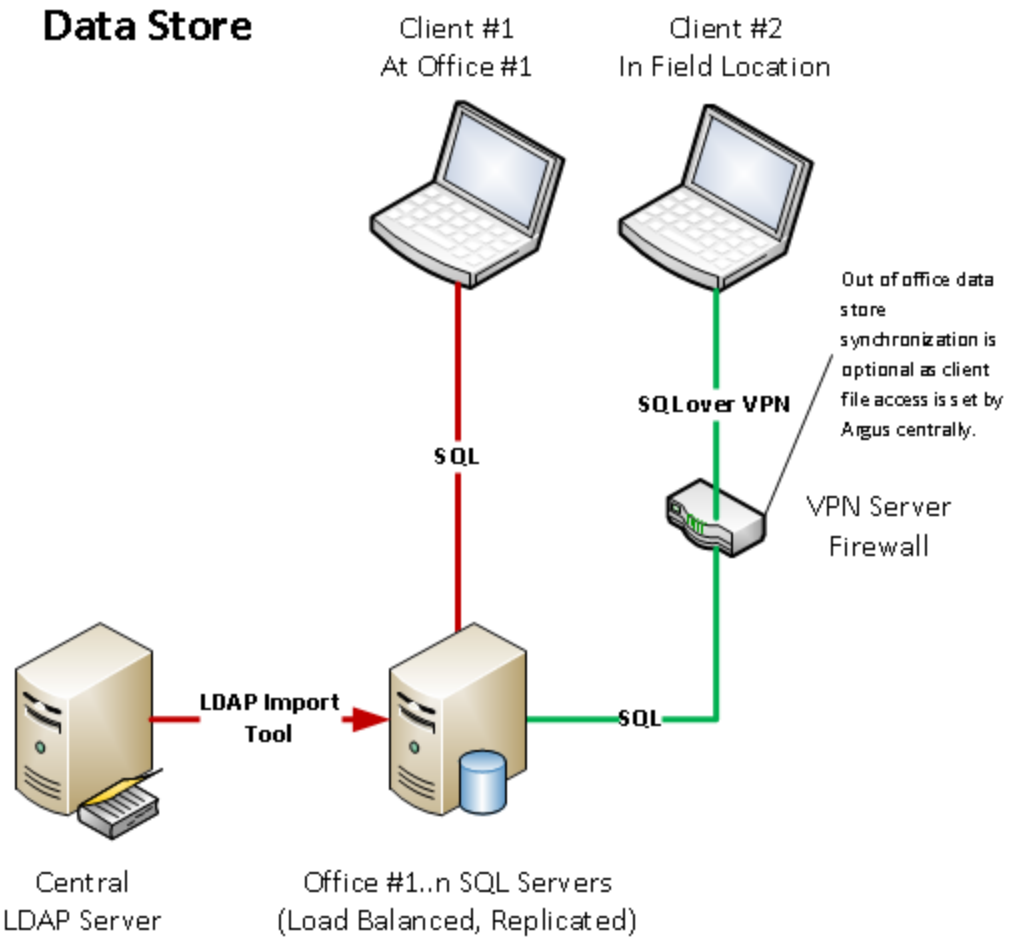
Note: This type of complex network topology should generally be undertaken with the assistance of Caseware Technical Support.

The diagram below illustrates a SmartSync Server setup where two SmartSync Servers are being used to load balance requests as staff (Client 1 and Client 2) work on files stored on multiple Windows File Share appliances. Requests from Client 1 are directed to SmartSync Server 1 through the load balancer along the red line and requests from Client 2 are directed to SmartSync Server 2 through the load balancer along the green line. Windows File Share storage devices are available to both SmartSync Servers. In the event of a failover, the client whose SmartSync Server is no longer available would have their requests redirected to the available SmartSync Server by the load balancer. The same copy of the client file on the same Windows File Share would be accessed by the new SmartSync Server. This requires that the load balanced topology be created with the file storage component external to the SmartSync Server so that it remains available.



Data store load balancing

Locate a data store server in each office location with users in that office set up to synchronize with that local SQL server. The data stored in the branch offices need to be populated using the central data store in the data center. These data store servers would be one-way replicated from the data center data store using SQL replication.



System requirements

To run Caseware SmartSync Server, you must meet or exceed the following system requirements:

IIS web server

Hardware

- 1 GHz 64-bit (x64) processor; 2 GHz recommended for improved performance
- 2 GB of RAM; 8 GB recommended for improved performance, with an additional 1 GB for every 100 users and 5000 files
- Solid-state drive (SSD) recommended for optimal performance
- Minimum 10 GB hard disk space, 40 GB or more recommended for improved performance

Note: These are the approximate disk space requirements for the system partition. Itanium-based operating systems will vary from these estimates. Additional disk space may be required if you install the system over a network.

File server/networks

Operating systems

- Microsoft Windows Server 2019 (with IIS 10)
- Microsoft Windows Server 2016 (with IIS 10)
- Microsoft Windows Server 2012 R2 (with IIS 8.5)
- Microsoft Windows Server 2012 (with IIS 8)
- Failover server and regular backups recommended for High Availability (HA)

Additional components

- A licensed copy of Caseware Working Papers with SmartSync must be installed on the same server as the SmartSync service
- Internet browser that supports TLS 1.2 or later (see Disabling access to Caseware Cloud for older and unsupported browsers for more information)

Firewall rules

- SmartSync Server: Port 443 for HTTPS access
- Workstations: Port 443 for HTTPS access to the IIS web server where SmartSync Server is installed
- For parent client files stored on a separate server, ports 135 and 139 are required for communication between the two servers

Accounts and permissions

Service account selection

SmartSync Server installs a Windows Service called *CasewareFileService* to the server to process requests such as Sync log flushing and converting client files to the server installed version of Working Papers SmartSync. It is recommended that one of the following service accounts be used to manage the SmartSync File Service:

- **Local Service**

  Use this setting when setting up the SmartSync File Service on the same server as the SmartSync server and the copy of SmartSync. The client files must be stored on the same server. Local service is recommended when no network resources will be used by SmartSync Server.

- **Network Service**

  Use this setting when the SmartSync File Service and the copy of SmartSync are on different servers than the IIS web server with SmartSync Server or when accessing client files through a UNC. Network Service is recommended when the service requires domain authentication abilities

Note: A user account must have permission to **Log on as a service** on your server to manage the **SmartSync File Service** and is not recommended

File level permissions

We recommend the use of an NTFS volume to set up the top level parent directory (root folder hosting the SmartSync parent files).

If using the Network Service account for the Caseware Application Pool and the File Service, the following permissions should be applied to the top level directory:

- SYSTEM - Full Control
- NETWORK SERVICE - Full Control
- Domain Admins - Full Control
- Administrators - Full Control

If using the Local Service or a specific user account for the Caseware Application Pool and the File Service, that account should be given rights to the server with log on as a service in the **Local Security Policy**.

Note: Do not use 'Creator Owner' to attach specific NTFS permissions to the top level or to any directories under it. This will cause permissions errors when users attempt to access files via SmartSync.

Setting up the user account for SmartSync Server

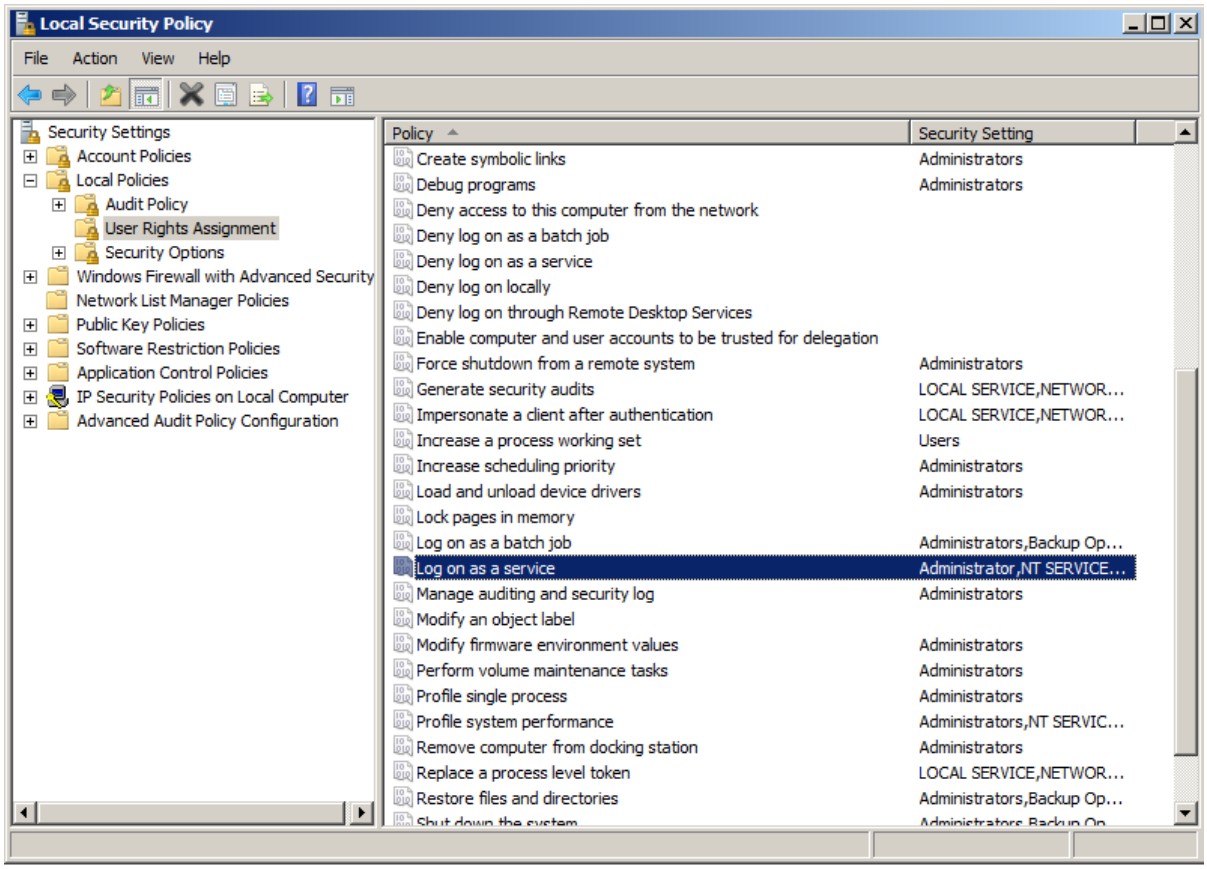
To operate the SmartSync File Service, follow these steps to assign the required service properties to the desired account.

Prerequisites:

- Administrator credentials

Procedure

1. Open **Local Security Policy** from Administrative tools or using the search on the Windows task bar..
2. Select **Local Policies | User Rights Assignment** in the left navigation pane.
3. Scroll down in the right pane and select **Log on as a service** from the list.



4. Right-click **Log on as a service | Properties**.
5. Click **Add User or Group**.
6. Use the dialog to add a user or service account to this right.
7. Click **OK** and close the Local Security Policy dialog.

Results

The rights and credentials are ready. Provide these credentials during the manual SmartSync Server Installation to operate the SmartSync File Service.

Installing the IIS web server on Windows Server

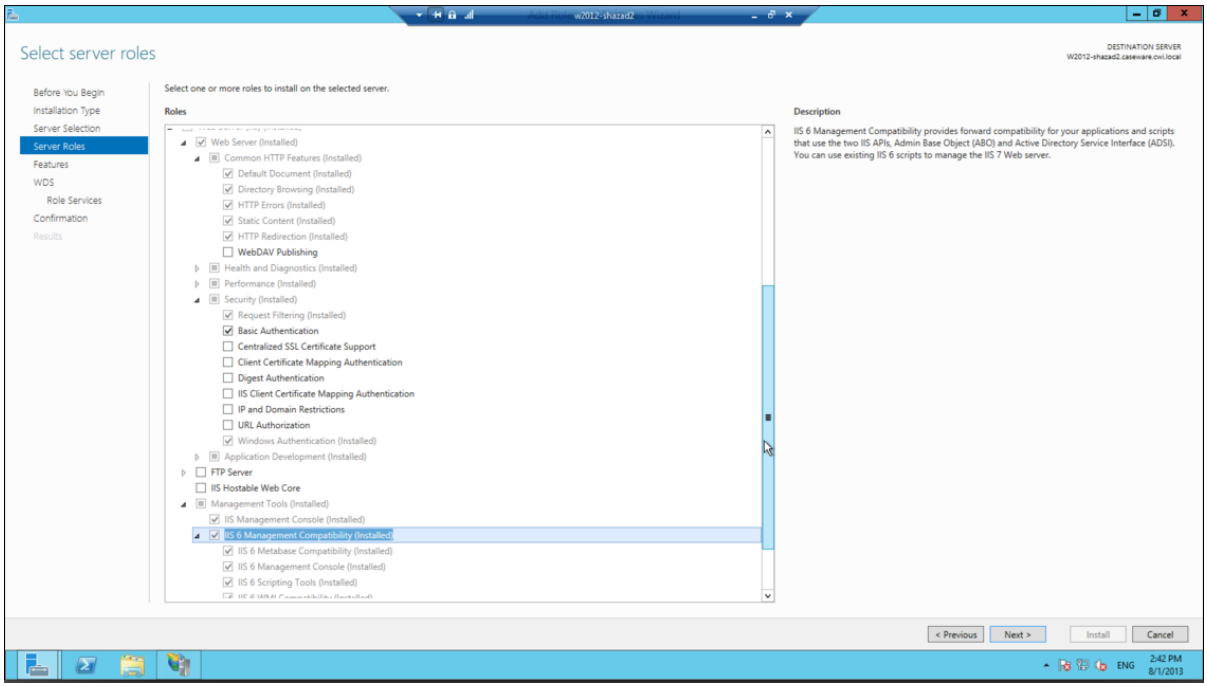
This section provides instructions for installing the IIS web server on Windows Server.

Prerequisites:

- Administrator credentials.
- .Net Framework 4.5

Procedure

1. Open **Server Manager**.
2. Under Manage menu, select **Add Roles and Features**.
3. Select **Role-based Installation** or **Feature-based Installation**.
4. Select the local server from the list and click **Next**.
5. Select Web Server (IIS) and click **Next**.
6. Click **Next** on the **Select Features** screen and on the screen after it.
7. Follow the on-screen instructions to add all of the IIS roles listed in IIS Options for SmartSync Server and click **Next**.



8. Click **Install**.
9. Click **Close** to exit the wizard.

Results

The IIS web server is set up and ready for the SmartSync Server Installation.

Installation

SmartSync Server Installation Wizard

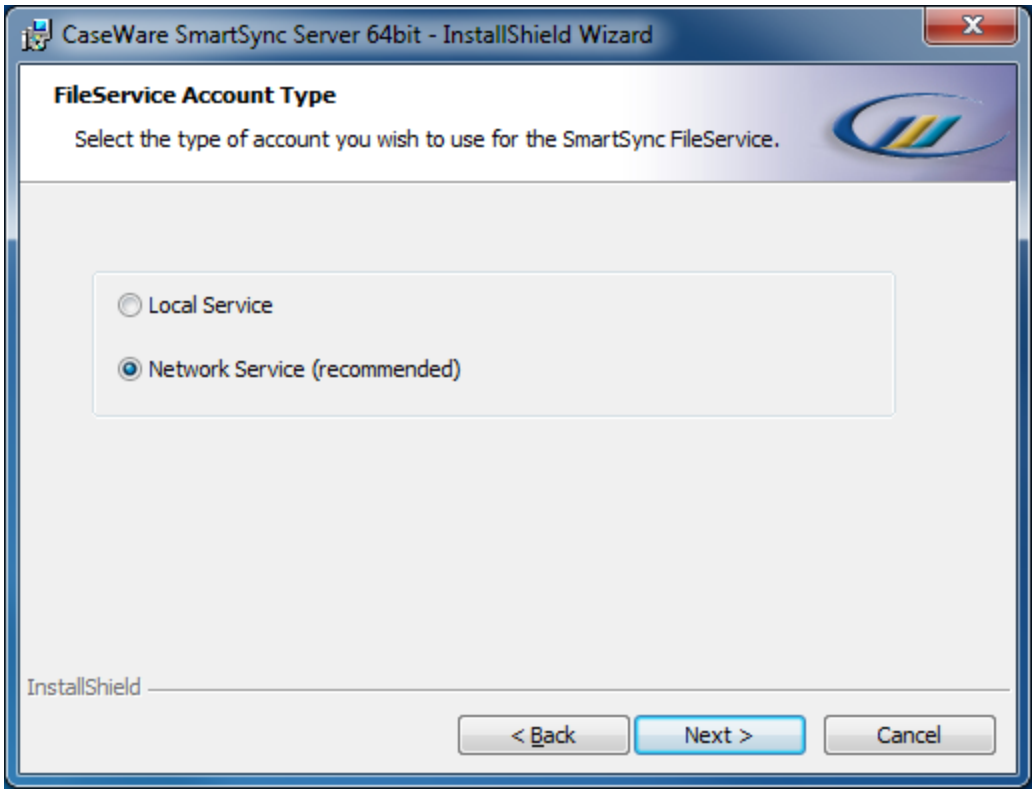
The following procedure walks you through the process of installing SmartSync Server or upgrading your version of SmartSync Server using the **Installation Wizard**. Firms using a **named user account** to run the SmartSync FileService must perform a manual installation

Prerequisites:

- Complete the procedures for the topics listed under **Configuring Your Windows Server**.

Procedure

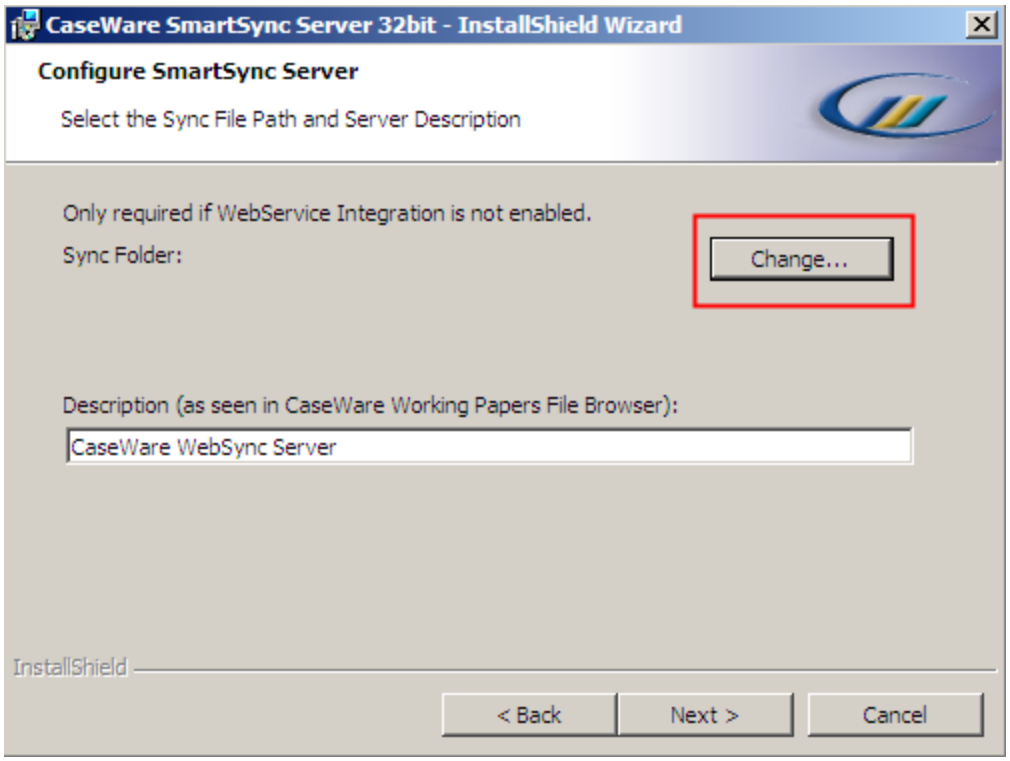
1. Download the SmartSync Server installer.
2. Double-click the **Setup** file.
3. (If applicable) Click **Yes** or **Continue** on the User Account Control dialog.
4. Click **Next** on the Caseware installer **Welcome** screen.
5. Accept the license agreement and click **Next**.
6. Click **Change** to modify the **Request Folder** path. Click **Next**.
7. Select to run the **SmartSync FileService** as a **Local Service** or **Network Service**. Click **Next**.



8. Click **Change** to navigate to the **Sync File Path** where the SmartSync top-level parent files will be stored on this server. Also known as the **Publish Folder**.

   Note: For network shares, use a UNC Path. Example: \\SERVER01\Shared_Sync_Folder

9. Type a **Description** for the server. This will display on the Servers tab in Working Papers. Click **Next**.



10. Click **Install**.
11. (If required) Microsoft .Net 4.0 Framework is installed. Accept the license agreement and click **Install**. Click **Finish** once the .Net installation is complete.

    Note: Microsoft Server 2012 requires .Net 4.5 Framework to be installed.
12. (If required) Microsoft C++ 10.0 is installed. Accept the license agreement and click **Install**. Click **Finish** once the C++ installation is complete.
13. Click **Finish**.

Results

SmartSync Server is installed.

Notes:

- If the **Publish Folder** is local to the server where SmartSync Server is installed, do not share it.
- If the **Publish Folder** is on a mapped drive or a network share, the folder must be shared.
- The network service or user account that runs the file service requires full *Read* and *Write* access to **three (3) folders:** the location of the parent file (Publish Folder), *"C:\CWRequests"*, and *"C:\Program Files\Caseware SmartSync Server"*.
- The IIS application pool account called CasewareAppPool requires full *Read* and *Write* access to the location of the parent file (Publish Folder).

SmartSync Server manual installation

Install or upgrade SmartSync Server using a manual installation. This is required if running the **SmartSync FileService** under a **named user account**. This process installs the same components in the same sequence as the Wizard Installation but with less detail.

Prerequisites:

- Complete the procedures for the topics listed under **Configuring Your Windows Server**.

Procedure

1. Open an **Administrator Command Prompt** on your server.
2. (If applicable) Remove the **SmartSync FileService** added by a previous SmartSync Server 2014 installation:
    a. Enter the following command: **SC delete "FileService"**.
    b. Navigate to the installation folder (example: *C:\Program Files\Caseware SmartSync Server*) and delete **FileService. exe** and **FileService.exe.config**.
3. In the **Administrator Command Prompt** enter the following command:

    setupxxbit.exe /S /V "/qb ACCOUNTTYPE=2 IS_NET_API_LOGON_ USERNAME=domain\username IS_NET_API_LOGON_PASSWORD=password CWREQUESTS=C:\CWRequests CW_SYNC_FILEPATH=C:\SyncFiles".

Notes:

- If you encounter errors or if the process halts during installation, contact Caseware Support before attempting the installation again . You will need to provide the installation log file to the support team. The log file (*MSIxxxxx.log*) is located in the *%temp%* folder on the server. Ensure this is the correct log file by verifying the date/time stamp of the file.
- The network service or user account that runs the file service requires full *Read* and *Write* access to **three (3) folders:** the location of the parent file (Publish Folder), *"C:\CWRequests"*, and *"C:\Program Files\Caseware SmartSync Server"*.
- The IIS application pool account called CasewareAppPool requires full *Read* and *Write* access to the location of the parent file (Publish Folder).

Windows post-installation configuration

Active Directory authentication

To use Windows Active Directory authentication to authorize connections from Working Papers, SmartSync Server must be installed on a the server that is part of the Active Directory domain and the authentication for the SmartSync site must be configured for Windows authentication.

Adding the server to the domain

To confirm that the server is part of the same Active Directory, enable Working Papers to pass through the Active Directory credentials to the SmartSync Server. See Join a computer to a domain for more information.

Configuring Windows authentication for SmartSync Server

Configure Active Directory Authorization on IIS for SmartSync Server using the following procedure.

Prerequisites:

- Complete the IIS server configuration and the SmartSync Server installation.

Procedure

1. Open **Administrative Tools | IIS Manager**.
2. In the **Connections** pane, click **computer name | Sites | Default Web Site**.
3. Click on **SmartSync**.
4. Double-click the **Authentication** icon in the center pane.
5. In the **Authentication** pane, ensure that all entries are disabled except **Windows Authentication**. To enable or disable an entry, select the entry and click **Enable** or **Disable** on the **Actions** pane.
6. Click the computer name in the **Connections** pane and on the **Actions** pane, click **Restart**.

Results

SmartSync Server is configured to use Active Directory authentication.

Note: During Kerberos authentication, the security ticket includes all security groups which the user is a member of and encodes this in the Authorization header. If the user is a member of many

security groups, the Authorization header can exceed the size limit. This can result in failed authentication or slow response times. For more information, see Kerberos authentication and network authentication issues.

Anonymous authentication

Anonymous authentication can be used in situations where the IIS server hosting SmartSync Server is only available from an internal network. Users who are obtaining authorization for their requests under this model do not need to pass their Active Directory credentials with their requests. Anonymous authentication uses less bandwidth when communicating with SmartSync Server.

Anonymous authentication is less secure than Windows authentication. It is only recommended used when access to the server is limited to a closed network. Users accessing the SmartSync Server must be on the same network as the server. The connection can consist of a physical connection, a wireless connection, or a VPN connection to the local area network. Because Windows authentication is not being used, the server does not need to be joined to the domain.

To set up anonymous authentication, follow the **Configuring Windows authentication for SmartSync Server** procedure. For step 5, ensure that all entries are disabled except **Anonymous Authentication**.

Using a non-default web site

You can run SmartSync Server on a non-default web site after installing it to the default web site. Use the following procedure to set up additional SmartSync Server instances that are accessed under a different URL and use different folders to store files.

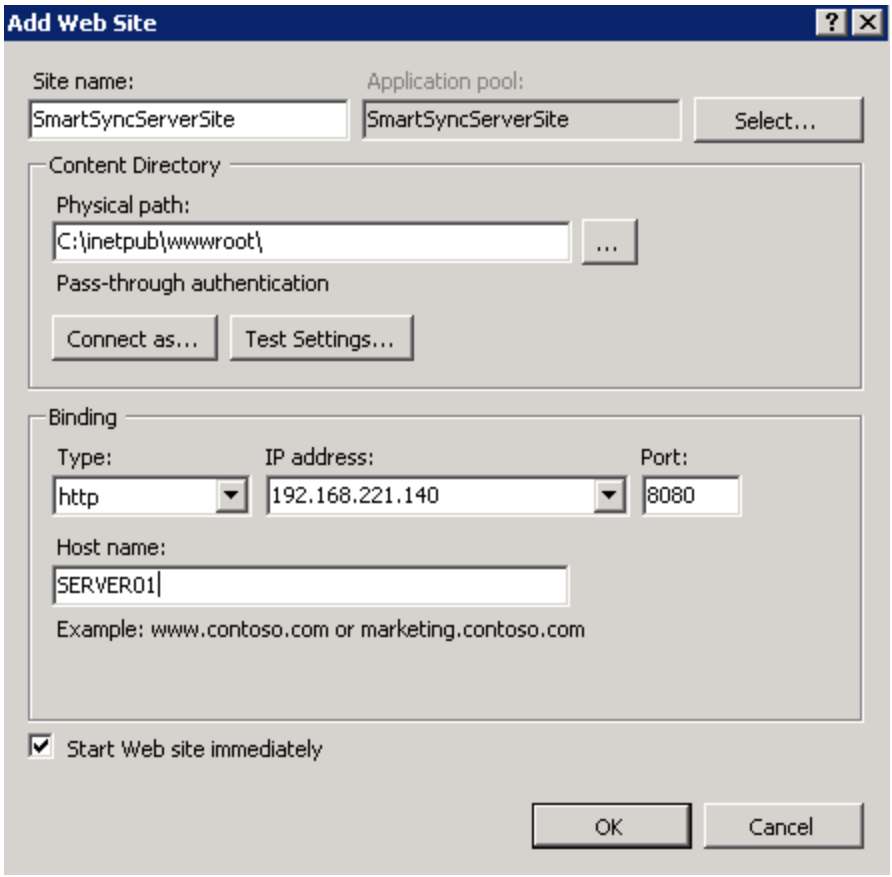
Prerequisites:

- Complete the IIS server configuration and the SmartSync Server installation.

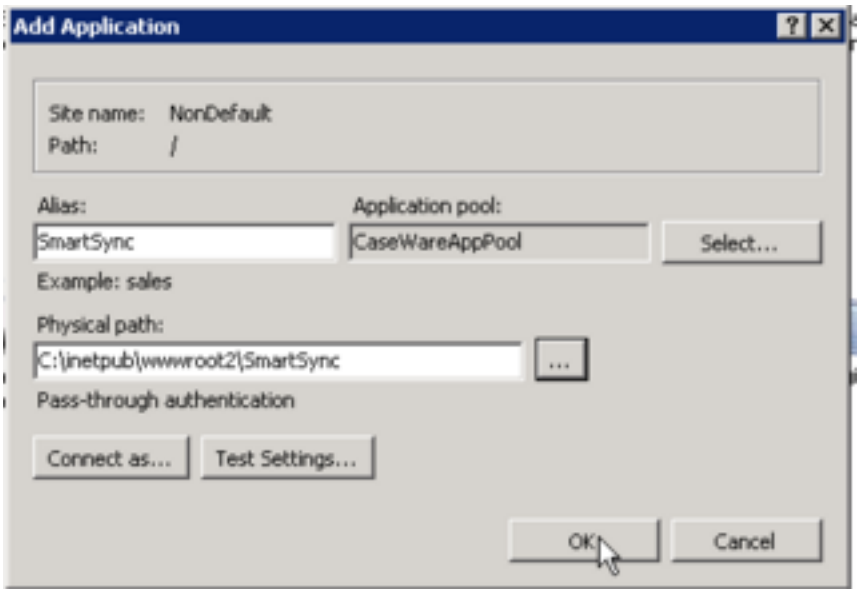
Procedure

1. Open **Administrative Tools | IIS Manager**.
2. In the **Connections** pane, click **computer name | Sites**.
3. On the **Actions** pane, click **Add Web Site**.
4. Complete the following fields:
    - **Site name**
    - **Physical path** (Location for the site folder. Click ... to browse for, and create, a folder.)

- **Type**, **IP address** and **Port**.
- **Host name** (Type in the name of the server.)

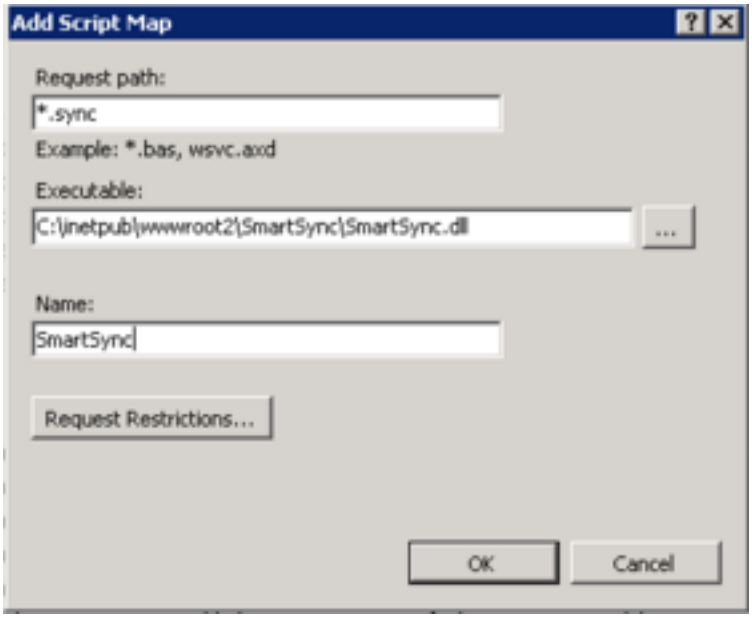


5. *If applicable*: Create a new folder (e.g. SmartSync1) and copy all of the files from **inetpub\webroot\SmartSync** except **web.config** into it.
6. On the **Connections** pane, right-click on the new site and click **Add Application**. We recommend creating a new **Application pool** for the non-default site. If you are running the non-default site parallel to the default site, the new Application pool should be identical to **CasewareAppPool**.



Click **OK** to add the SmartSync application.

7. Select the new application and double click on the **Handler Mapping** icon in the center pane.
8. On the **Actions** pane, click **Add Script Map**.
9. Type the following (items in bold will vary):
    - Request path: **.sync*
    - Executable: *C:\inetpub\wwwroot***new web site folder***\SmartSync.dll*
    - Name: **user defined**



10. Click **Request Restrictions** and clear **Invoke handler only if request is mapped to**. Click **OK**.

11. Click **OK** to close **Add Script Map**. On the confirmation message, click **Yes**.
12. Select the new application and double click on the **Request Filtering** icon in the center pane.
13. On the **Actions** pane, click **Deny File Name Extension**.
14. Enter **.dll** in the Deny File Name Extension dialog.
15. Select the new application and double click on the **Configuration Editor** icon in the center pane.
16. Add a key named *Files* with the value set to the location of the SmartSync **Files** folder (e.g. C:\Sync Files Folder\). This is the SmartSync folder specified during the SSS installation.

Results

The non-default web site has been initialized. The following procedures in this section and under SmartSync Server Post-Installation Configuration also need to be applied to the non-default web site for the set up to be complete.

Notes:

- To upgrade a non-default website, you must first upgrade the default website, then copy over the upgraded **smartsync.dll** file to the non-default website.
- Remove the handler mapping and the original application from the default web site when transferring the SmartSync server to a new site and not setting up an additional server.
- Each separate site can be run by a different account.

Changing the default application pool

Changing the default application pool for SmartSync Server is required if the domain user's account does not have access to the files location because SmartSync Server resides on a different domain or because it specifically denies rights to Domain Users.

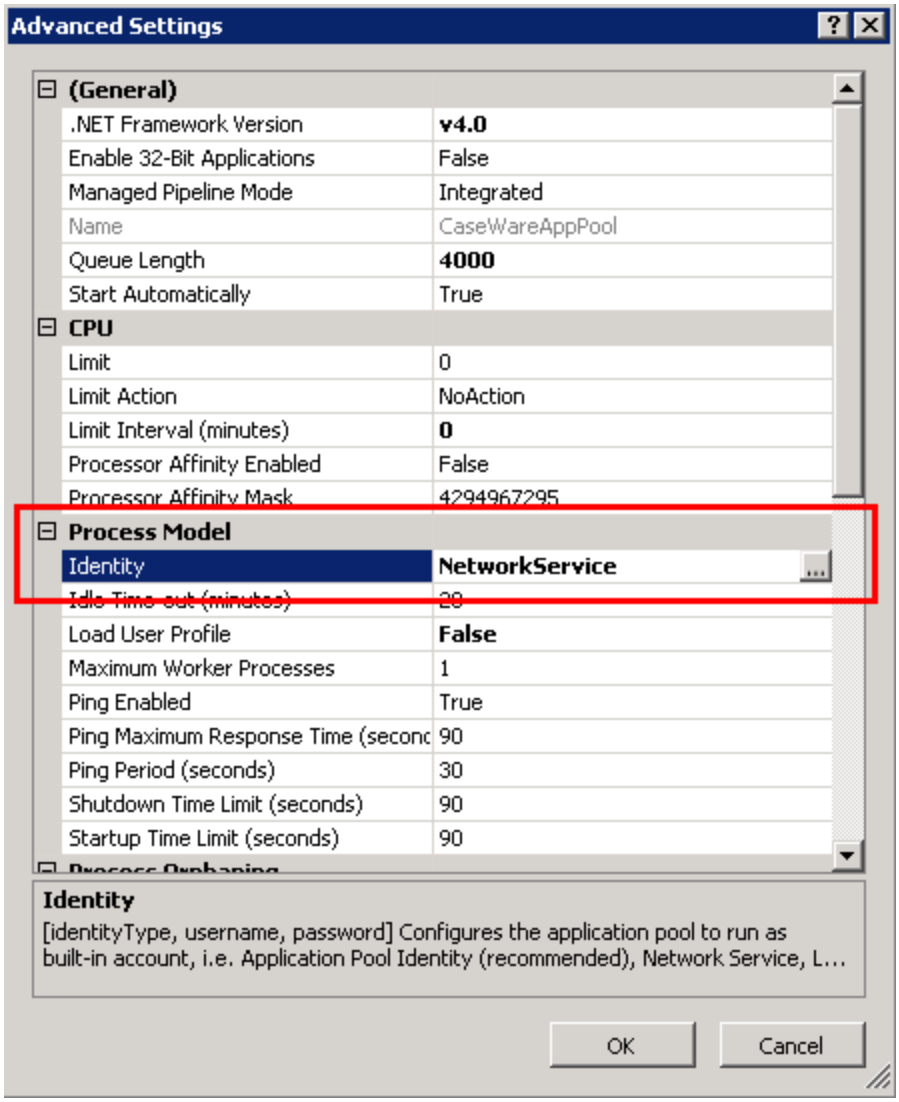
Prerequisites:

- Complete the IIS server configuration and the SmartSync Server installation.
- Credentials with rights to modify these settings.

Procedure

1. Open **Administrative Tools | IIS Manager**.
2. In the **Connections** pane, double-click **computer name | Application Pools**.
3. Right-click on **CasewareAppPool** and select **Advanced Settings**.

4. Under **Process Model**, select the **Identity** field and click ....



5. Select **Custom Account** and click **Set**.
6. Specify an Administrator account and password.
7. Click **OK**.
8. Restart the IIS server.

Results

The SmartSync Server default app pool has been modified.

Configuring bindings and SSL

The installation wizard sets up a binding on port 443 for the SmartSync Server. Manual installation requires that you use the procedures below to provide an SSL certificate to bind at the site level on

IIS.

Note: If limiting SmartSync Server access to users connecting from within the internal network and externally using VPN, adding SSL may not be desired as SSL adds another encryption layer, requiring additional bandwidth.

Importing or creating a certificate

The certificate must be available before beginning the procedure.

1. Open **Administrative Tools | IIS Manager**.
2. In the **Connections** pane, click **computer name**.
3. Double-click on **Server Certificates** icon in the center pane.
4. On the **Actions** pane, click **Import** to import an existing certificate or click to create a new certificate of the specified type.

Creating a new binding

1. On the **Connections** pane, select **Default Web Sites**.
2. On the **Actions** pane, click **Bindings** to assign the certificate to the server.
3. Click **Add** to create an HTTPS connection.
4. In the Add Site Binding dialog, select the **Type** as **https** and the **SSL certificate** as the imported or created certificate from step 4 in the Importing/Creating a Certificate procedure above.
5. Click **OK**.
6. Click **Close**.
7. Restart the IIS service.

Results

The IIS web server bindings for SmartSync Server have been configured.

Notes:

- Enabling HTTPS uses TLS 1.0 by default. To ensure no other encryption protocols are used, follow the instructions on Microsoft's support page.

Configuring the firewall

The server firewall must be configured to permit traffic for SmartSync server.

Prerequisites:

- Credentials with rights to modify these settings.
- Ensure the following procedure is in compliance with the firm IT firewall policies.

Procedure

1. Open **Administrative Tools | Windows Firewall with Advanced Security**.
2. Click **Inbound Rules**.
3. On the **Actions** pane, click **New Rule**.
4. Open port 443 for HTTPS access.
5. (If applicable) Repeat step 3 to open ports 135 and 139 if top-level parent client files are stored on a separate server.
6. Client workstations require an HTTPS (port 443) connection to the IIS web server where SmartSync Server is installed.

Results

The firewall is configured to allow connections to SmartSync Server.

Storing parent files on a separate server

If you intend to store your firm's parent files on a separate server from the SmartSync Server, you'll need to create a top-level parent folder with specific share settings.

Prerequisites:

- You must sign in to the server with Administrator credentials.
- In Windows Firewall, ensure that the **File** and **Print Share** ports accept inbound and outbound traffic. For more information, see SMB: File and printer sharing ports should be open.

To create a top-level parent folder (file share):

1. Launch **Server Manager**.
2. On the menu, click **File and Storage Services | Shares**.
3. In the filter drop-down, select **Tasks**. Click **To create a file share, start the New Share Wizard**.
4. In the New Share Wizard, select the applicable profile for the share. Click **Next**.
5. Select the server and volume for the share, then click **Next**.
6. Enter a name and optional description for the share, then click **Next**.
7. Select any applicable options for the share. We suggest disabling **Allow caching of share**. Click **Next**.

8. Specify the permissions for the share. We suggest removing the **Owner Creator** account and any other user accounts or groups, then adding the **Caseware App Pool** (IIS), **Caseware File Services** (Windows Services) and **Network Services** accounts with full permissions. Click **Next**.
9. Review the settings for your share, then click **Create**.

The top-level parent folder is created. Parent files that are stored in this folder will be shared with the SmartSync Server. Click **Close**.

Alternatively, you can share an existing top-level parent folder using Windows Explorer.

To share a top-level parent folder using Windows Explorer:

1. Right-click the top-level parent folder and select **Properties**.
2. Click the **Sharing** tab, then click **Advanced Sharing...**.
3. Select **Share this folder**. Enter a name for the share.
4. Click **Permissions**. In the dialog, specify the permissions for the share as required. We suggest removing the **Owner Creator** account and any other user accounts or groups, then adding the **Caseware App Pool** (IIS), **Caseware File Services** (Windows Services) and **Network Services** accounts with full permissions. Click **OK**.
5. Click **Caching**. In the dialog, select the applicable caching setting. We suggest selecting **No files or programs from the shared folder are available offline**. Click **OK**.
6. Click **OK** to share the folder.

The top-level parent folder and its contents are shared with the SmartSync Server.

SmartSync Server post-installation configuration

Configuring publish folders for client files

Complete the SmartSync Server setup by configuring the publish folders. These folders will contain the published client files and the top-level parent files. All paths to the folders are specified in the IIS configuration.

The Wizard Installation creates the publish folder and the Smartsync path. Modify the path and add additional folders to specify locations, such as the SmartSync top-level parent files publish folder.

With the Manual Installation, publish folders must be created and configured.

Authentication for the publish folders

Modify the publish folder security settings to allow **MACHINENAME\IUSR_MACHINENAME** to have *Read and List folder contents* rights. If the installation is not using Windows authentication, the account will also require *Write and Modify* permissions. The publish folder created by the Wizard Installation has this authentication set.

All users that will be publishing or replacing parent files require the *Write and Modify* permissions for this folder.

Note: Operating the SmartSync File Service using a named user requires the rights described above.

Modifying the parent file and publish file location

Modify the location where SmartSync Server stores top-level parent files or where the files are published.

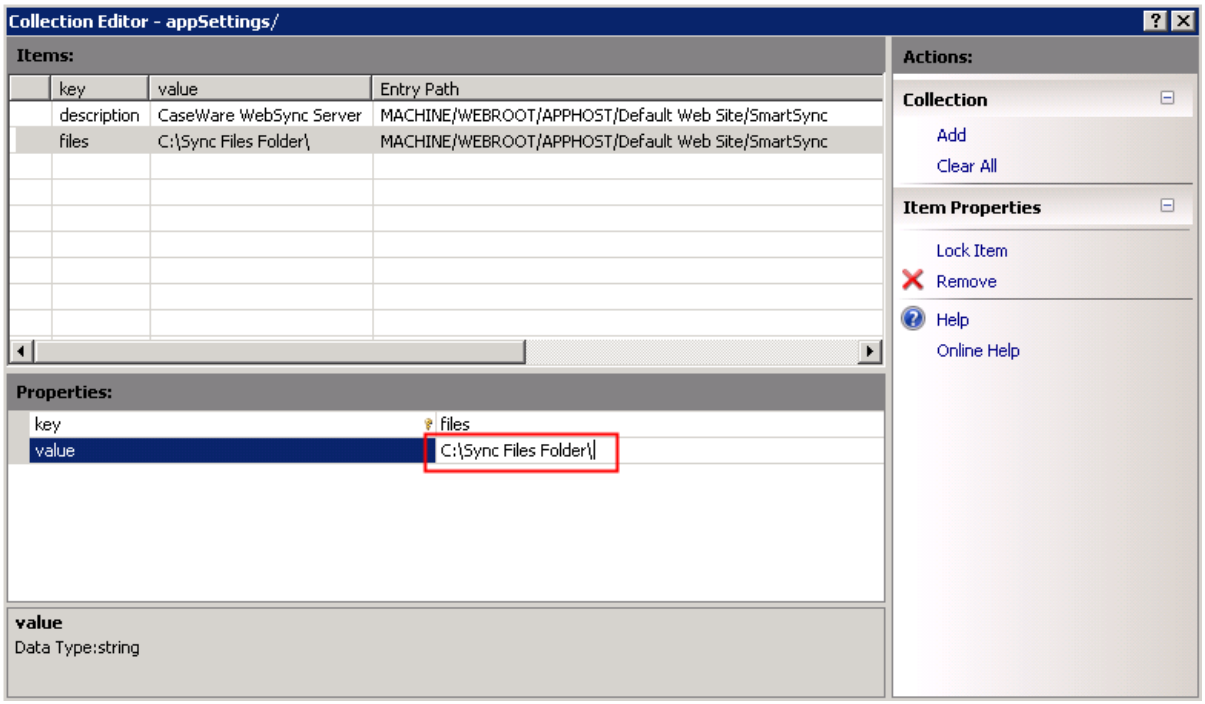
Prerequisites:

- Credentials with rights to modify the IIS configuration.

Procedure

1. Open **Administrative Tools | IIS Manager**.
2. On the **Connections** pane, select the **SmartSync** entry.
3. Double-click the **Configuration Editor** icon in the center pane.
4. Select **(Collection)** and click  .
5. In the **Items** pane, select the item to modify. Example: Select **files** to modify the top-level parent location or **publish** to modify the publish file location.
6. In the **Properties** pane, modify the **value**.

   Tip: For the **publish** key, add multiple folders and labels separated by a semi-colon (;). Example: *C:\Sync Files Folder\2010"2010 Files";C:\Sync Files Folder\2011"2011 Files"*.



7. Click **X** to close the **Collection Editor**.

Results

The SmartSync Server file location has been modified.

Notes:

- Modifying the top-level parent location (**files** key) to a central folder containing all parent files automatically uploads files to SmartSync Server.

Preventing request file generation

Add a flag to the Configuration Editor to disable users from generating a request file.

Prerequisites:

Rights to modify the IIS configuration.

Procedure

1. Open **Administrative Tools | IIS Manager**.
2. In the **Connections** pane, select the **SmartSync** entry.
3. Double-click the **Configuration Editor** icon in the center pane.
4. On the **Configuration Editor**, select **(Collection)** and click **...**.
5. On the **Actions** pane, click **Add**.

6. In the **key** field, type **GenerateRequestFile**.
7. In the **value** field, type **0**.

Results

Request files will not be generated by the server for any file, including conversion and flush requests, even if explicitly requested by the user.

Filtering files

Specify the files visible to users with a filter key.

Prerequisites:

- Enable Working Papers protection on the client files.

Procedure

1. Open **Administrative Tools | IIS Manager**.
2. In the **Connections** pane, select the **SmartSync** entry.
3. Double-click the **Configuration Editor** icon in the center pane.
4. On the **Configuration Editor**, select **(Collection)** and click  .
5. On the **Actions** pane, click **Add**.
6. Enter **filter** as the name of the new key.
7. Enter one of the following values:
    - **Server** - ensures that the file listing only shows files accessible to the authenticated user.
    - **Client** - ensures that the server shows files accessible to the current Windows user.

      Tip: Use **Server** or **Client** only if Windows authentication is disabled on SmartSync Server and if Caseware protection is using LDAP (Active Directory).
    - **Any** - does not limit the files that are visible on the client side and enables the *Specific User* and *Any User* filters in Working Papers to function.
    - **None** - all files are displayed for all users.

Results

The list of files displayed to users is filtered, based on the server setup.

Notes:

- The Working Papers interface used to open files from the server displays an icon that can be used to filter the list of files.

- Apply different filters to **different site accounts** to filter the available file list for certain users.

Adding publish folders

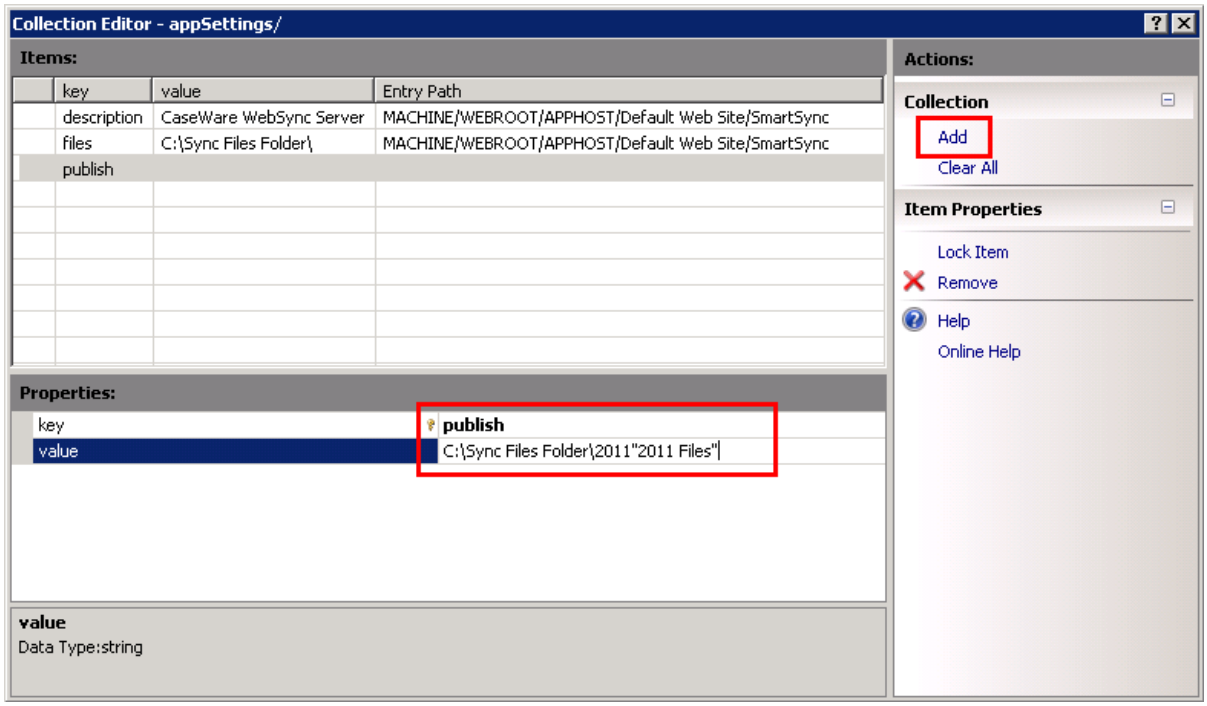
Create subfolders in the SmartSync top-level parent folder to provide additional save locations when uploading new parent files using **Publish to Server**.

Prerequisites:

- Rights to modify the IIS configuration.

Procedure

1. Open **Administrative Tools | IIS Manager**.
2. In the **Connections** pane, select the **SmartSync** entry.
3. Double-click the **Configuration Editor** icon in the center pane.
4. Select **(Collection)** and click ....
5. In the **Actions** pane, click **Add**.
6. In the **Properties** pane, in the **key** field, enter **publish**.
7. In the **Properties** pane, in the **value** field, enter a valid location. Example: *C:\Sync Files Folder\2011*.



8. (Optional) After the path, enter a label in between quotation marks to be used in Working Papers. Example: *C:\Sync Files Folder\2011"2011 Files"*.
9. (Optional) Add multiple folders, and labels, in the **value** field separated by a semi-colon (;). Example: *C:\Sync Files Folder\2010"2010 Files";C:\Sync Files Folder\2011"2011 Files"*.

Results

Publishing a SmartSync file stores it in the specified location on the server.

Notes:

- The path of the **publish** key overrides the path of the **files** key. To create subfolders while using the **publish** key enter the following path: *C:\files key path\subfolder name*.

  Example: The path of **files** key is *C:\Sync Files Folder*. To create subfolders *Sub1*, *Sub2*, *Sub3*, the **publish** key value should be defined as *C:\Sync Files Folder\Sub1;C:\Sync Files Folder\Sub2;C:\Sync Files Folder\Sub3*.
- Two types of paths can be specified for the **files** key or the **publish** key.
  - For files on the same server as the IIS service, use the absolute path. Example: *C:\SyncFiles*.
  - For files on a different server than the IIS service, use a UNC path. Example: *\\server\path*.

  Entering a path in a format other than these two types will prevent the SmartSync Server from accessing top-level parent files.

Adding publish folders using metadata

Publish folders and labels, defined in a **publish** value key, can use Working Papers metadata to create dynamic folder names. By using metadata, each folder level can adhere to a data category, such as locales, client identifiers, or date/time.

Metadata fields in **publish** value keys must have the following syntax:
\\servername\foldername\%ServerMetaDataFolder%"%ServerMetaDataLabel"\%%ClientMetaDataFolder%%"ClientMetaDataLabel"

Example:

- A key value of *\\SERVER1\FILES\%CompanyCity%"%ClientNumber%"*, with the client file:
  - **Company City** - Springfield
  - **Client Number** - 1010

creates the folder *\\SERVER1\FILES\Springfield* on the server and labels the client files as *1010*.

- A key value of *\\SERVER2\FILES\%YearEndYear%\%YearEndMon%\%%ClientName%%*, with the client file:
    - **Year End Year** - 2014
    - **Year End Month** - December
    - **Client Name** - ABC Limited

  creates the folder *\\SERVER2\FILES\2014\Dec* on the server. Opening a sync copy on a workstation creates the folder *ABC Limited* in their default sync path.

Notes:

- If the server is unable to resolve a meta-field, it is removed from the path and all subsequent folders in the path are moved up one folder.
- For client side substitutions, each meta-field must be resolved in order for files to be published.
- Meta-fields with date types can be formatted by appending a suffix to the field name:

Suffix	Formatting	Example
Year	Numeric Year	2011
Month	Full month name	October
Mon	Three letter abbreviation for month	Oct
Day	Numeric day of the month	21
Date	Date with format DD/MM/YYYY	21/10/2011
Time	Time with format HH:MM:SS	17:30:15 – [UTC]

Adding publish folders using a configuration file

A configuration file can be used instead of the **Collection Editor** to define **publish** value keys, simplifying the process of creating and maintaining complex keys.

Create a file named **publish.xml** in your SmartSync Server folder. Example: *C:\inetpub\wwwroot\SmartSync*. The configuration file will override collections created in the **Collection Editor**.

Defining publish folders and custom fields

The configuration file must use the following syntax:

- <settings>
  - <directory>
    - <label>%%ClientName%%</label>
    - <location>\\SERVER2\FILES\%YearEnd%</location>
  - </directory>
  - <field>
    - <label>Color</label>
    - <name>Color</name>
    - <type>string</type>
    - <default>None</default>
    - <minimum></minimum>
    - <maximum></maximum>
    - <list>
      - <item>
        - <label>Blue</label>
        - <value>Blue</value>
      - </item>
      - <item>
        - <label>Green</label>
        - <value>Green</value>
      - </item>
    - </list>
  - </field>
- </settings>

Configuration file syntax values

SmartSync Server supports using a configuration file to define **publish** value keys, simplifying the process of creating and maintaining complex keys.

Available tags

Tag	Metadata	Description
<settings>	N	Configuration file settings opening tag.
<directory>	N	Publish folder settings opening tag.

Tag	Metadata	Description
<label> </label>	Y	Publish folder label tag.
<location> </location>	Y	Publish folder location tag.
</directory>	N	Publish folder settings closing tag.
...	-	Replace the ... with another <directory></directory> element for additional publish folders.
<field>	N	Tag opening the custom field settings opening tag.
<label> </label>	Y	Custom field description tag.
<name> </name>	N	Field name tag.
<type> </type>	N	Field type tag. Example: string, date, integer, decimal, or boolean.
<default> </default>	N	Field default value tag.
<minimum> </minimum>	Y	Minimum integer range value tag.
<maximum> </maximum>	Y	Maximum integer range value tag.
<list>	N	List settings opening tag.
<item>	N	Item settings opening tag. Encapsulate values in the drop-down list.
<label> </label>	Y	List description opening tag.
<value> </value>	Y	Field values tag. These values are in addition to the default value specified in <default></default>
</item>	N	Item settings closing tag.
</list>	N	List settings closing tag.

Tag	Metadata	Description
</field>	N	Custom field settings closing tag.
...	-	Replace the ... with another <field></field> element for additional custom fields.
</settings>	N	Configuration file settings closing tag.

Notes:

- You can add custom metadata in the publishing path. These custom fields enable you to define directory names specific to your firm. Furthermore, custom fields can be defined to present Working Papers users with a drop-down list of options if displayed on the client side. These options are defined as items in the <list> element
- Label tags accept a ‘language' attribute for localized descriptions of publish folders or fields. For each element, multiple label tags can be added – each with a different language attribute designating the language of the label. Example:
    - <label>Default language label</label>
    - <label language="en">Generic English label</label>
    - <label language="en-US">English (US) label</label>
    - <label language="fr">Generic French label</label>

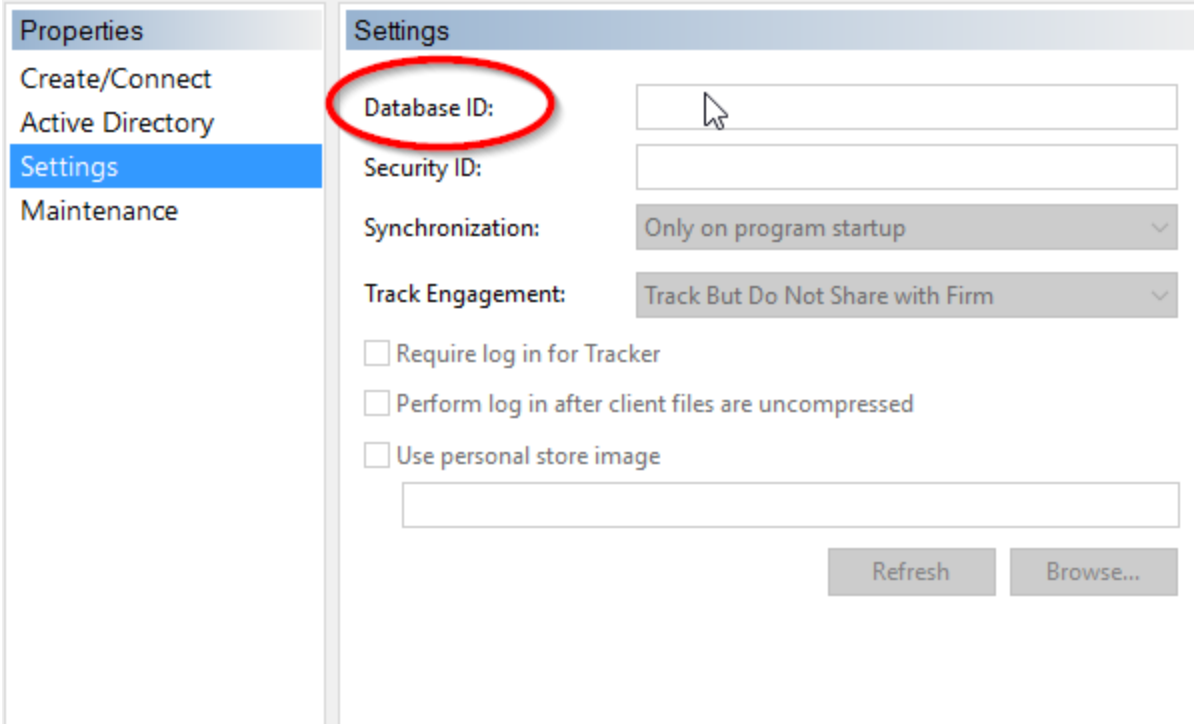
Updating SmartSync Server with data store changes

Update SmartSync Server to ensure file access changes from data store are automatically reflected in Working Papers. Users can then *immediately* see any recently assigned files on the SmartSync Server file open list and, conversely, won't see any files that have been unassigned from them.

Prerequisites:

- A supported version of Working Papers is required for this configuration to work.
- Working Papers must have access to the shared data store location for file access changes to update.
- SmartSync Server filter configuration must be set to either "server" or "Client" (see **Filtering Files**).
- **Active Directory** must be enabled on the user's machine and in their data store.

- You'll also need the **database ID** from your data store. This value can be found under **Settings**.



IMPORTANT: If you have multiple data stores (for example, across several offices), the database ID for each data store must be the same.

Procedure

1. Open **Administrative Tools | IIS Manager**.
2. In the **Connections** pane, select the **SmarSync** entry.
3. Double-click the **Configuration Editor** icon in the center pane.
4. Select **(Collection)** and click ....
5. In the **Actions** pane, click **Add**.
6. In the **Properties** pane, in the **key** field, enter **databaseid**.
7. In the **Properties** pane, in the **value** field, enter the database ID from your data store.

Distributing settings with a CWC file

Distribute data store, Cloud, and SmartSync Server settings to users without administrator rights with .cwc files. This allows the users to connect to a data store, or to apply registry settings for use with Cloud and SmartSync Server.

The following entries relate to server details each Working Papers user requires to connect to their parent location on SmartSync Server:

Important Note: The order of the entry set is important. Do not specify the SmartSync Server entry set before the data store entry set.

CWC entry	Description
[SmartSyncServer]	Specify where SmartSync Server entries begin.
DeleteServerInfo	Deletes the SmartSync Server registry hive "HKEY_CURRENT_USER\Software\CasewareInternational\Working Papers\20xx.00\SyncServer".
NoSmartSyncServerChange=1	Set to the value 1 to disable users from adding or deleting servers in the File Open dialog (Server tab).
AddServer={GUID}|Server_machine_name|Server_label	Adds a SmartSyncServer registry hive. This entry replicates the Add Server command from the File Open dialog (Server tab). Multiple AddServer entries can be specified. Specify the value of this entry in the following way (delimited by the pipe character "|"): AddServer=Server_machine_name|Server_label AddServer={GUID}|Server_machine_name|Server_label Where: • **Server_machine_name** - a network name or IP address for the server. • **Server_label** - the SmartSync Server label appearing in Working Papers. • **{GUID}** - the Globally Unique Identifier (GUID) for your server. If you are specifying this option, place it at the beginning of your pipe delimited list and ensure to use curly braces around the GUID value.

Upgrade a self-hosted SmartSync Server

To perform an in-place upgrade of a self-hosted SmartSync Server, administrators can complete the following process using the default website (with the default port 80 or port 443).

Notes:

- To upgrade to a non-default website, contact Caseware Support.
- Self-hosted SmartSync Servers often incur issues when used with Distributed File Systems (DFS). Due to this, we do not recommend the use of DFS with self-hosted SmartSync Servers. For more information, see Sync issues on self-hosted SmartSync Servers.

To upgrade a self-hosted SmartSync Server:

1. Log into MyCaseware.
2. Select **Software Downloads**.
3. Locate the latest version of SmartSync Server and click **Download**.
4. Navigate to the folder where the installation file was downloaded, then drag the installation file onto your desktop.
5. Before performing the installation, ensure that all other users close any synchronization file copies.
6. Right-click the installation file and click **Properties**. On the General tab, select **Unblock**. Click **OK**.
7. Right-click the installation file again and click **Run as administrator**.
8. The InstallShield Wizard displays. On the Welcome screen, click **Next**.
9. Accept the terms and click **Next**.
10. On the FileService Account Type screen, select **Network Service (recommended)** if the service and files are stored separately from IIS. This option requires domain authentication permissions. Click **Next**.

    Note: If you are using a domain user account instead of the default Network Service, you must change the Caseware App Pool (IIS) and the Caseware File Service (Windows Services) accounts back to the domain user account after installation.
11. On the Configure SmartSync Server screen, we suggest that you keep the default sync folder location. If your organization has a custom sync folder location, click **Change...**. Navigate to the folder where your parent files are stored and click **Select Folder**. Click **Next**.

    Note: For files that are stored in a shared folder rather than locally on the SmartSync Server, you must select the path to a UNC folder (for example, \\SERVER01\Shared_folder).
12. Click **Install** to begin the installation. Note that you may need to restart your computer.

SmartSync Server is updated on your computer. To verify the version of SmartSync Server you've installed, launch the Windows Control Panel and click **Programs | Programs and Features**. Locate SmartSync Server and verify the version under the Version column.

After the update, ensure that you give any applicable users and groups read/write access to:

- C:\Program Files\Caseware SmartSync Server
- C:\CWRequests
- C:\Sync File Folder

Additionally, if you store your files in a custom sync folder (such as a shared folder on a network) and you did not change the default path during installation, you will need to update the file path manually.

If you selected the Network Service (recommended) option, you must provide the following permissions to the root folder where your SmartSync parent files are hosted:

- System: Full control
- Network Services: Full control
- Domain Admin: Full control
- Administrators: Full control

If you are using a Domain User account for the Caseware App Pool and the Caseware File Service, you require the following permissions:

- Full permissions for the file share where your Working Papers files reside
- Full permissions for C:\Program Files\SmartSync

SmartSync Server services

The about.sync page

The SmartSync Server status page is available through you browser at **https://<serveraddress>/smartsync/about.sync** where **<serveraddress>** is the address of your SmartSync server. This page also lists the installed version number. The following table describes the information available on this page.

Section	Description
Total uptime	Total uptime is the amount of time the server process has been running without a restart.
Active threads	Active threads are the number of thread pool threads actively in use - this will always be at least 1 (for the about.sync request). If this number stays consistently high (especially if it is near 8 times the number of processors on the host), that

Section	Description
	could indicate a deadlock, which might require a service restart.
Tracked files	Tracked files is the total number of files being tracked. Using reset.sync will reset this to 0 and will count back up as the scan retrieves the files
Sessions - Connected	Sessions are the number of active SmartSync connections - there are usually 2 per user (one for SmartSync events and one for user tracking).
Sessions - Waiting	Waiting sessions are those in a push-wait state, ready to be woken when new data becomes available.
Requests - Maximum waiting / Currently waiting	Requests are the raw HTTPS requests. Maximum waiting indicates the maximum number of requests that have waited simultaneously on thread pool slots. Currently waiting indicates the number or threads currently waiting for thread pool slots. If either of these values accumulates, this indicates a lockup in the thread pool handling.
Requests - Processed	Processed is the number of HTTPS requests that have been serviced since the server process started with the average indicating the rate.
Requests - Failed	Failed indicates HTTPS requests that did not complete. This could either be due to connection loss or specific failure cases. There will likely be a few of these because of the connection type detection system which abandons obsolete requests. Unless this value becomes a very large in comparison with requests processed, it can be safely ignored.
Requests - Response time	Response time is the overall average response time for HTTPS requests.

The reset.sync page

Occasionally, SmartSync server can experience issues while scanning the file system that result in errors in the file listings. If this occurs, use the server reset command. The SmartSync Server reset page is available through you browser at **https://<serveraddress>/smartsync/reset.sync** where **<serveraddress>** is the address of your SmartSync server.

When you open the server reset page, the page should finish loading and then display a blank white page in the browser. You SmartSync Server in IIS will restart and the file scan will reset and rescan for client files. If you are still experiencing errors after attempting a server reset then contact Caseware Technical Support for further assistance.

SmartSync Server FileService

Overview

The SmartSync FileService process monitors the request folder for XML request files. FileService processes the request files by starting up one instance of Working Papers per request in a command-line mode. Once complete, or an error is found, FileService deletes the request file and generates a response file containing the error code and error message in the request folder.

The default request folder is **C:\CWRequests**. A different folder can be specified during installation or with the registry key **HKLM\Software\Caseware International\FileService\XXXX.XX\RequestPath**, where XXXX.XX is the version of SmartSync Server being used. This key can be of type **REG_SZ**, in which case the exact path specified becomes the request path, or of type REG_EXPAND_SZ, in which case any environment variables in the path are expanded first.

Terminating the service

Stopping FileService cancels any unscheduled tasks. Running tasks run to completion. Shutting down the server stops the service and cancels all tasks.

Logging

Most requests and processes are logged to the **GeneralLog.log** file in the request folder.

Statistics

Every 15 minutes the **Statistics.xml** file is updated in the request folder containing the following statistics:

- File service running time (in milliseconds).
- The number of invalid request files processed (for example, a request file containing no operation).
- The number of request files that have been detected but not actually scheduled.
- The number of preempted request files.

Additionally, the following statistics are available for each operation:

- The number of in-progress requests.
- The number of cancelled requests.
- The total number of completed requests.
- The number of requests that failed (where Working Papers returned an error code).
- The number of long-running requests.
- The number of requests made that Working Papers detected as redundant (for example, requesting a conversion of a file that has already been converted).
- The total time taken for all requests.
- The longest time taken by a request.

Task scheduling

FileService only schedules a fixed number of tasks limited by the number of processors on the server. The number of tasks allowed can be modified.

Within the request folder are two subfolders, **High** and **Low**. Requests generated by users in the interface, such as file conversions, go in the **High** folder and the requested task is processed as soon as possible. Requests generated by the system, such as flush requests, go in the **Low** folder and the requested task is usually scheduled for off-peak hours. FileService will preempt any low-priority tasks to process high-priority tasks. Low priority tasks preempted this way will still be processed if they will not prevent other high-priority tasks.

Scheduled low-priority tasks are usually started during a specified time range (by default Tuesday to Friday 12:00am to 6:00am, and from Friday 10:00pm to Monday 6:00am). Once started, the tasks aren't cancelled until the process has finished, regardless of the low-priority scheduled end time.

Tasks that run continuously for a long period of time are moved to the long-running queue to not block other tasks. This queue has a maximum number of long running tasks (by default 4). Adding a long-running task over the maximum number cancels the longest running task to make room of the new one. FileService checks the queue periodically for tasks that exceed the maximum run time and cancels them. Completed long running tasks are removed from the queue and a response file is generated.

Cancelled tasks generate an error message in the system event log as well as the response file.

When the file service is started, it will begin processing all high priority tasks and, if in the low priority time range, low priority tasks.

Response files older than 48 hours are considered stale and deleted by the file service.

Settings

Configure FileService settings in the **FileService.exe.config** file. To add a setting, open FileService.exe.config and add a line to the file between the *<appSettings>* tag and the *</appSettings>* tag with the following syntax **<add key="setting" value="value" />** where **"setting"** refers to the *Setting Name* in the following table and **"value"** is the value that you are setting it to.

For a list of values available for FileService, see SmartSync FileService Settings.

Flushing

The flushing process flushes the sync log of any outstanding sync changes and commits them to the parent file. If a file is not flushed, the outstanding sync changes remain in the sync folder.

The flushing process is performed in two different ways:

- Automatically by the Caseware File Service on the Smartsync Server
- Manually by opening and closing the parent file directly (not recommended if you are using SmartSync Server)

The automatic flushing process managed by the Caseware File Service runs at a scheduled time daily. The default flush time is 0:00, midnight, local time.

Caseware File Service is a Windows Service account that monitors the **CWRequest** folder on the SmartSync Server. It logs all flushing activities to the **GeneralLog** file within the CWRequests folder. If a file does not seem to be flushing, you can reference the GeneralLog file to verify the flush status. Successful flushes report the message "finished with exit code 0" in the log; any other exit code number represents a failed flush.

For example, a successful flush of the file "Sample One Holdings" displays as follows:

- 2021-05-14 11:34:48Z MNP47CWSS1 [1772:34]: FileServiceTask.OnStart: Request file C:\CWRequests\Low\BHF2N4VURQ5KDCPVQR3Y2WOVXU.request (file name = \\Fileserver1\cwdata$\Sample One Holdings.ac) **finished with exit code 0**

Troubleshooting

Configuring IIS maximum content length

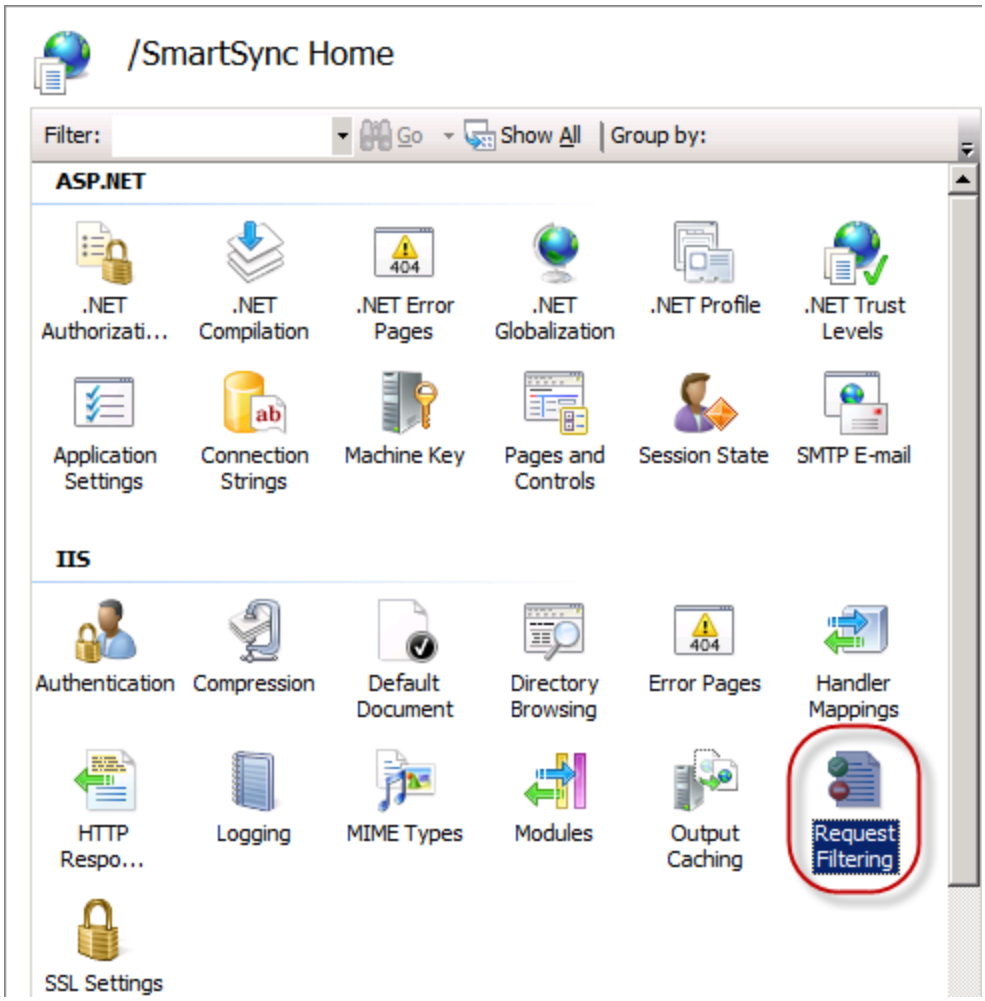
The default IIS configuration does not process requests over 30MB to avoid Denial-of-Service attacks. When a Working Papers client sends data to the SmartSync Server, the data packets are automatically divided into a series of smaller packets, to stay under this limit.

The threshold for dividing a request is 1 MB with requests divided in the range of 128 KB to 28 MB. If IIS is configured with a maximum allowed content length less than 30 MB, these requests can result in HTTPS status codes in the 400 range (specifically, 400, 403, 404). If the IIS limit is lowered to less than 1 MB, communication with the server would encounter issues.

Procedure

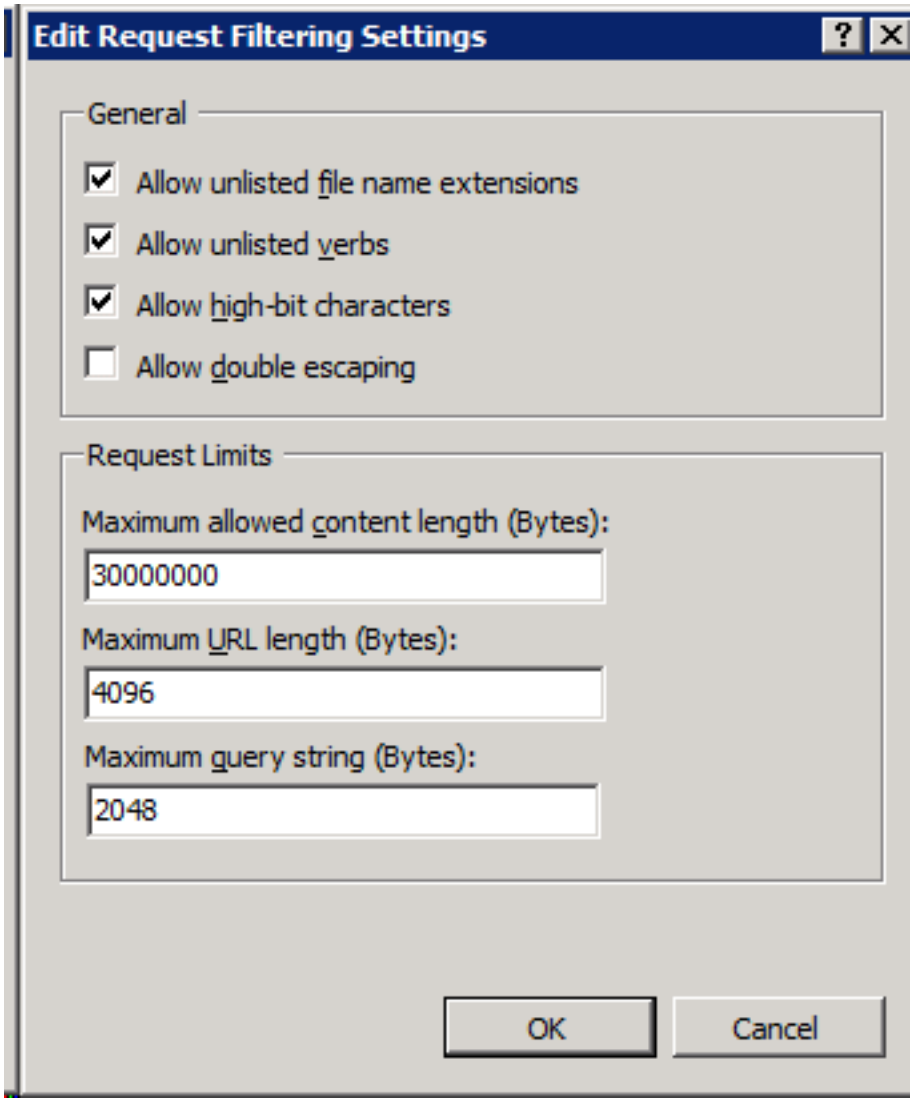
To verify or configure the maximum allowed content length on IIS:

1. Open the **Server Manager**.
2. In the right navigation pane click on **Roles | Web Server (IIS) | Internet Information Server**.
3. In the **Connections** pane, click on the **SmartSync** entry.
4. Double-click **Request Filtering**.



5. Click the **Edit Feature Settings** under the Actions pane on the right.

6. Ensure the **Maximum allowed content length (Bytes)** is at least 30,000,000 (thirty million).



Errors while scanning the file system

Occasionally, SmartSync server can experience issues while scanning the file system that result in errors in the file listings. If this occurs, use the server reset command. The SmartSync Server reset page is available through you browser at **https://<serveraddress>/smartsync/reset.sync** where **<serveraddress>** is the address of your SmartSync server.

When you open the server reset page, the page should finish loading and then display a blank white page in the browser. You SmartSync Server in IIS will restart and the file scan will reset and rescan for client files. If you are still experiencing errors after attempting a server reset then contact Caseware Technical Support for further assistance.

Application pool crashes with Error 5011

This error is caused by the use of long file paths where the path and the file name together are greater than 260 characters. SmartSync Server requires that file paths are less than 260 characters. This includes any file managed by the SmartSync Server and includes files in the sync folder, such as the Sync Log.

SmartSync Server file list not refreshing

SmartSync Server caches its file listing for the lifetime of the server process. The server tracks any changes to the scanned folders while it is active and integrates changes into the file listing displayed in Working Papers. If the service has stopped or the server is rebooted, it needs to rebuild the index. This is required because changes may have occurred since the last time the server was running and checked the folders.

If the list of files on the SmartSync Server displays unchanged for over 24 hours in Working Papers, regardless of changes, contact Caseware Support

Published files don't appear on SmartSync Server page

If published files don't display on the **File | Open | SmartSync Server** page, attempt the process with locally stored files. If the local files display, there may be an issue with the drive storing the published files.

SmartSync Server and SmartSync version compatibility

It is recommended that both SmartSync Server and Working Papers with SmartSync always run the same version. The SmartSync Server version must be equal or later than the Working Papers with SmartSync version. However, once a parent file has been accessed by the later Working Papers version, it will no longer operate with previous version.

Duplicate parent files on server

If files are duplicated on the server, ensure the **Publish File** location in the Configuration Editor is referencing a UNC path and not an absolute path. For information on modifying the publish file location, see **Modifying the Parent File and Publish File Location**.

Example: *\\SERVER01\Share\File Path*.

Kerberos authentication and network authentication issues

Windows authentication is the recommended setup for SmartSync Server. The following authentication issues can occur when using IIS Windows Integrated Authentication for SmartSync Server:

Kerberos authentication fails or is very slow

In Kerberos authentication, each request to the server gets authenticated. The Authorization header carries all group memberships of the user and can exceed the accepted size. To resolve this issue, complete the procedures below.

Adjusting authorization header size

Adjust the MaxRequestBytes and MaxFieldLength parameters to increase the accepted header size.

1. Open the **Registry Editor** on the server where SmartSync Server is installed.
2. Find *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters*
3. Create the following DWORD values:
    a. **aMaxFieldLength**
    b. **MaxRequestBytes**
4. Enter a value above *16384* to increase the header size.

Session-based Kerberos authentication

To switch to session based Kerberos authentication:

1. Open the command prompt on the server where SmartSync Server is installed.
2. Enter the following commands:
    - cd %SystemRoot%\System32\inetsrv
    - appcmd set config /section:windowsAuthentication /authPersistNonNTLM:true
3. Restart IIS service for your changes to take effect.

Note: The authPersistNonNTLM property controls the re-authorization requirement of Kerberos authentication. Setting this value to true will prevent Kerberos from authenticating every request to SmartSync Server.

Fallback to NTLM Kerberos (session-based) authentication

To configure NTLM authentication on IIS as fallback:

1. Open the Server Manager.
2. In the right navigation pane click on **Roles | Web Server (IIS) | Internet Information Server**.
3. In the **Connections** pane, click on the SmartSync entry.
4. Double-click **Authentication**.
5. Select **Windows Authentication**.
6. On the right pane, click **Providers**. If Provides is not available edit the file applicationHost.config.
7. Promote **Negotiate** above **NTLM:**
    a. Select **NTLM** from the list of **Enabled Providers**.
    b. Click **Move Down** until NTLM appears above **Negotiate** in the list.

Editing applicationHost.config

1. With Administrator credentials, open **C:\Windows\System32\inetsrv\config\applicationHost.config** with a text editor.
2. Search for <windowsAuthentication enabled="true" useKernelMode="true" />.
3. Add the following 4 entries between the bold text:

    <windowsAuthentication enabled="true" useKernelMode="true" />
    <providers>
    <add value="NTLM" />
    </providers>
    </windowsAuthentication>
    </authentication>
4. Save and close the file.
5. Restart IIS service for your changes to take effect.

Specifying a mapped network drive or UNC path (for example, \\network\path\) as the location for the top-level parent blocks user access to network resources

Users logged on with IIS Windows authentication cannot access network resources (UNC) while maintaining the user identity. Example: The current user is authorized for HTTPS communication, but file access to the network is done through the default the NetworkService account, under which the SmartSync web application is running.

Resolve this issue by providing an *Impersonation fallback* to enable switching to NTLM (session based) authentication. To resolve this issue, complete the following procedures:

Fallback to NTLM (session-based) authentication

To configure NTLM authentication on IIS as fallback:

1. Open the Server Manager.
2. In the right navigation pane click on **Roles | Web Server (IIS) | Internet Information Server**.
3. In the **Connections** pane, click on the SmartSync entry.
4. Double-click **Authentication**.
5. Select **Windows Authentication**.
6. On the right pane, click **Providers**. If Provides is not available edit the file applicationHost.config.
7. Promote **NTLM** above **Negotiate:**
    a. Select **NTLM** from the list of **Enabled Providers**.
    b. Click **Move Up** until NTLM appears above Negotiate in the list.

Editing applicationHost.config

1. With Administrator credentials, open **C:\Windows\System32\inetsrv\config\applicationHost.config** with a text editor.
2. Search for <windowsAuthentication enabled="true" useKernelMode="true" />.
3. Add the following 4 entries between the bold text:

    <windowsAuthentication enabled="true" useKernelMode="true" />
    <providers>
    <add value="NTLM" />
    </providers>
    </windowsAuthentication>
    </authentication>
4. Save and close the file.
5. Restart IIS service for your changes to take effect.

Sync issues on self-hosted SmartSync Servers

If your organization is using a Distributed File System (DFS) with a self-hosted SmartSync Server, you may encounter sync issues such as sync conflicts, missing sync events and/or file duplication in the SmartSync Server file list. Due to this, we do not recommend the use of DFS with self-hosted SmartSync Servers.

Best practices for crashes and performance issues

Proceed with the following instructions if your organization's SmartSync Server experiences any of these behaviors:

- The response time in **about.sync** (https://<serveraddress>/smartsync/about.sync) exceeds 1000ms for more than an hour.
- Users encounter errors 403, 404, 503, 584, or a "No file available" message when attempting to connect to the server.
- The W3WP.exe process for the Caseware Application Pool remains at approximately 80% memory or CPU usage for more than 20 minutes.
- The file server remains at approximately 80% disk or CPU usage alongside the W3WP.exe process.

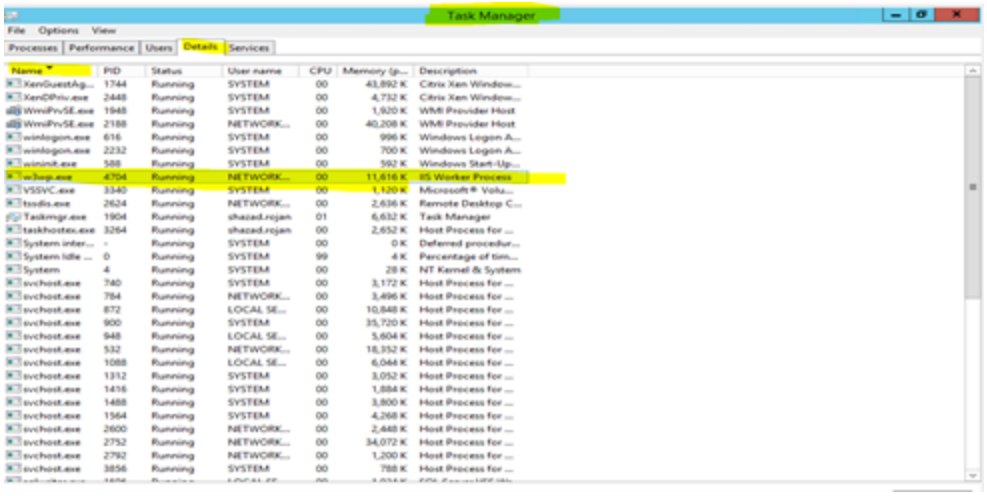
Note: The following instructions are intended for the IT Administrator who manages your organization's IIS/SmartSync Server.

Create dump files

If your organization's SmartSync Server is crashing or experiencing performance issues, you will need to create dump files for the Caseware account's W3WP.exe process on the web server hosting the SmartSync Server. The dump files must be collected while the server is still experiencing issues.

To create dump files:

1. Launch the Windows Task Manager (**Ctrl+Alt+Delete | Task Manager**).
2. Click the **Details** tab.
3. Click the **Name** column to sort by the process name.
4. Locate the **w3wp.exe** process that is associated with the SmartSync Account.



5. Right-click the process, then click **Create dump file**.

6. Wait five seconds, then repeat the process to create another dump file. Repeat this process until you have at least three dump files.

The dump files are created and saved in **C:\users\user.name\AppData\Local\Temp\w3wp.DMP**.

Capture Process Monitor logs

If your organization's SmartSync Server is experiencing performance issues, we suggest capturing Process Monitor logs. You can download the necessary tool to capture these logs from Microsoft's website.

To capture Process Monitor logs:

1. On the SmartSync Server, right-click the **Procmon** tool and click **Run as administrator**.
2. On the toolbar, click **Filter**. The Process Monitor Filter dialog displays.
3. Using the dialog options, create the following filter: **Process Name is w3wp.exe**. Click **Add**, then **OK**.
4. Allow the tool to run for approximately 10 minutes.
5. On the toolbar, click **Save**. Save the Logfile.PML file.

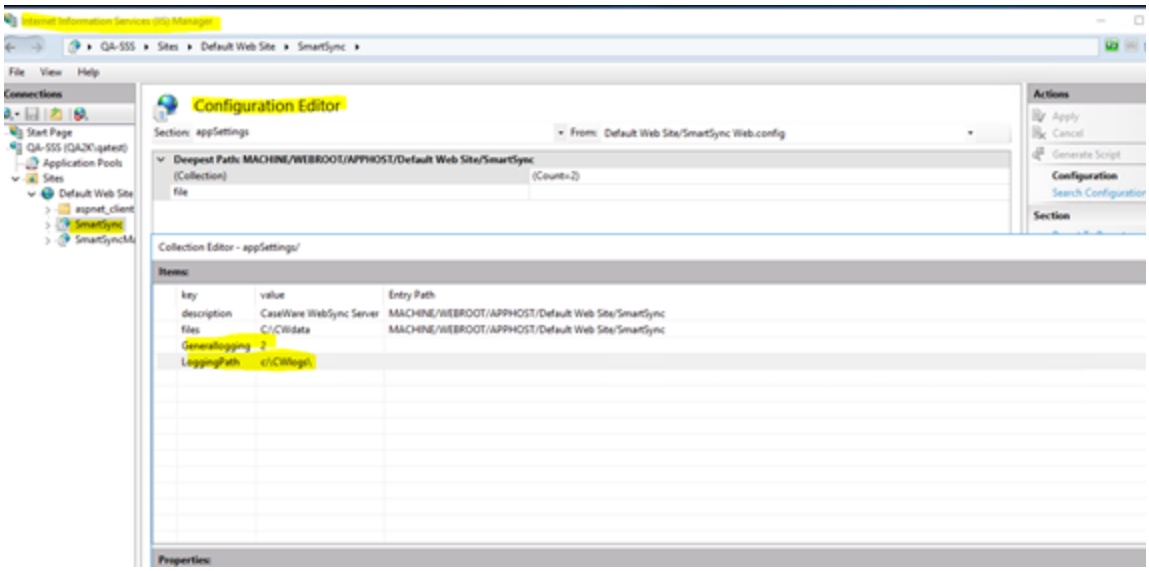
The Process Monitor log is captured. Compress the log as a .ZIP file, then send it to Caseware Support.

Create IIS logs

If your users are encountering error 403, 404, 503, 584, or a "No file available" message, we suggest creating IIS logs from the SmartSync website. These logs are also helpful if **about.sync** is not displaying tracked files.

To create IIS logs:

1. Launch IIS Manager.
2. Navigate to the Smartsync website.
3. Open the **Configuration Editor**.
4. Add the following entries on the IIS for SmartSync:



Key	Value	Entry Path
GeneralLogging	2	MACHINE/WEBROOT/Default Web Site/SmartSync
LoggingPath	C:\cwlog\log.txt or any writable path	MACHINE/WEBROOT/Default Web Site/SmartSync

Note: Changing these configuration settings (i.e. Web.config) will reset the SmartSync Server.

What's next?

After creating the logs, attempt the following:

- Stop IIS and then start it again (or perform an IIS reset from the command line). If the issue is still not resolved, reboot the File Server or the host where the Network Share is located. After a server reboot, ensure that IIS is running and the Smartsync Website is active and running.
- Monitor the SmartSync website using **about.sync** (https://<serveraddress>/smartsync/about.sync).

- Examine the **tracked files** to ensure that the file count is increasing to match the total on the Network Share.
- Examine the **response time** to ensure that the time is dropping below 1000ms.

Anti-virus exclusions

Real-time scans by anti-virus software can lock Caseware files, causing reduced performance or preventing the application from functioning. We suggest adding Caseware file extensions and executables to your anti-virus software's exclusions list to ensure that they operate as intended. Exclusions must be added to each computer hosting Caseware applications or files, including File Share hosts, IIS and client machines.

Note: Updates to your anti-virus software (e.g. Windows Defender) may clear your anti-virus exclusions list. Check the exclusions list after an update to ensure that it still includes the file extensions and executables.

Appendix

IIS options for SmartSync Server

The following options should be selected in the **Add Role Services** section of the Server Manager console on your Windows Server:

Web server (IIS)

- Common HTTPS Features
    - Static Content
    - Default Document
    - Directory Browsing
    - HTTPS Errors
- Application Development
    - ASP .Net
    - .Net Extensibility
    - ISAPI Extensions
    - ISAPI Filters
- Security
    - Basic Authentication
    - Windows Authentication
    - Request Filtering
    - URL Authorization
- Management Tools
    - IIS Management Console
    - IIS Management Scripts and Tools
    - Management Service
    - IIS 6 Management Compatibility
        - IIS 6 Metabase Compatibility
        - IIS 6 WMI Compatibility
        - IIS 6 Scripting Tools
        - IIS 6 Management Console

Storing parent files

Storing parent files on the same drive hosting the SmartSync Server application is the suggested practice for optimal performance and reliability. In scenarios where this is not possible, you can use a **Windows Network Share** on a different computer or Windows File Share drive if the following requirements are met:

1. The file locking semantics must match those documented here.
2. File monitoring at the file system level must perform as documented here.

Testing a network share for use with SmartSync Server

When using a network share of any type, Caseware recommends extensive testing before deployment, including completion of the following:

1. Run the SyncStress test between the system hosting SSS and the network share.
2. Publish files with the expected configuration used in production, including (if applicable) the use of metadata.
3. Create new Sync copies.
4. Synchronize changes by multiple concurrent users.

IIS Logging configurations

IIS Logging enables you to track activity and potential issues through a log of server events. When configuring IIS Logging for your server, we recommend setting the logs to flush after they've reached a specified entry count. Flushing the logs prevents them from becoming too large in size.

To configure flush settings for IIS Logging, see the Microsoft help topic: How to configure flushing a W3C log by entry count.

Managing SmartSync Server files in Tracker

SmartSync Server includes an IIS application called **SmartSyncManage**. With this application, authorized users can manage the parent files stored on SmartSync Server through Tracker.

Authorized users can execute the following Tracker commands:

- Abandon child copy
- Abandon all child copies
- Clear synchronization information

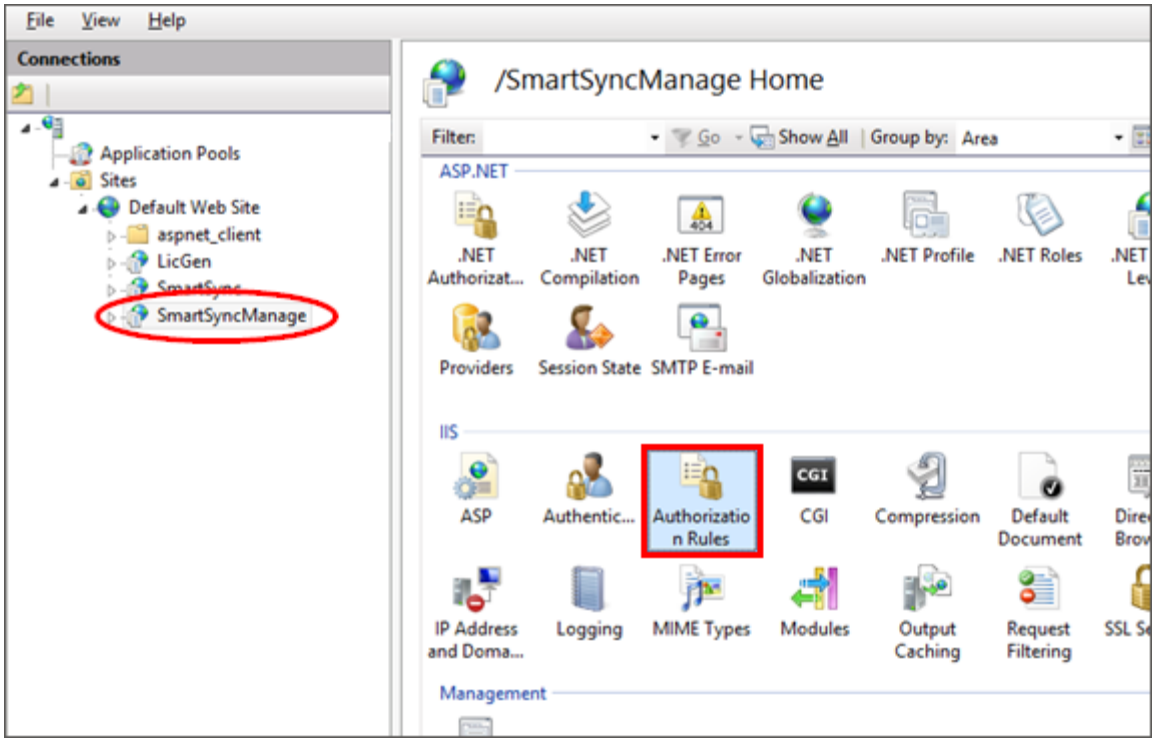
- SmartSync repair
- Delete parent file

Notes:

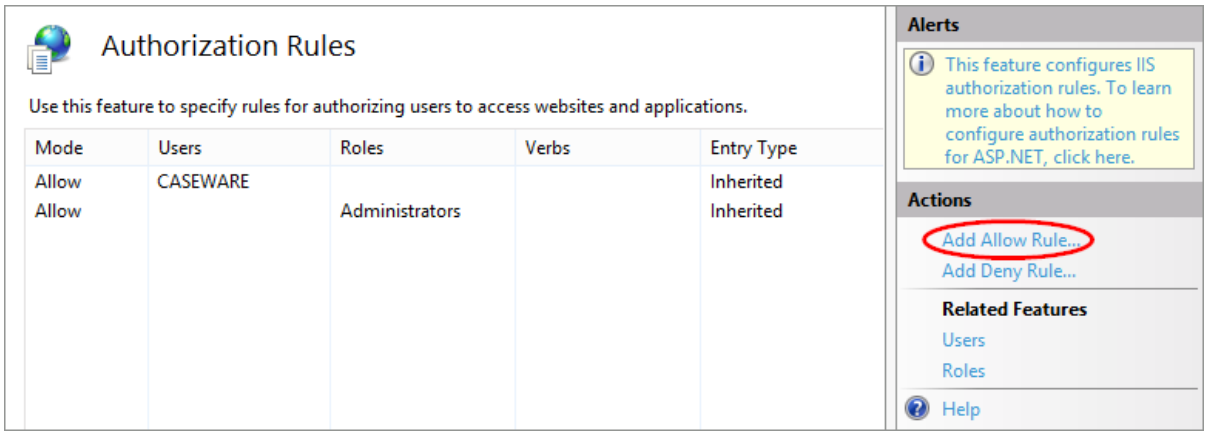
- You must add the **URL Authorization** IIS option before you can access **Authorization Rules**.
- Existing users in the SmartSync application are automatically copied to SmartSyncManage with identical authorization.

To authorize additional users:

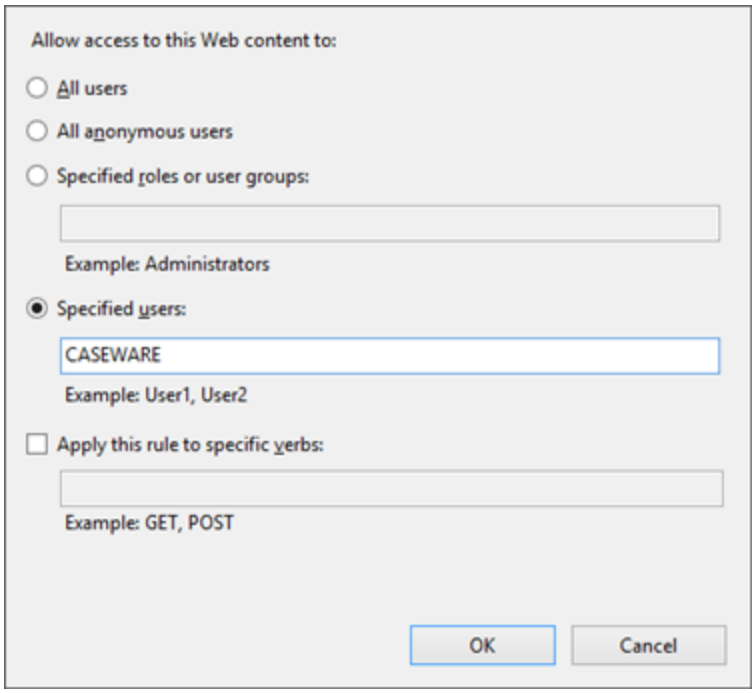
1. Launch **Internet Information Services (IIS)** on the server machine.
2. In the Connections pane, locate and open **SmartSyncManage**. In the IIS group, click **Authorization Rules**.



3. The Authorization Rules pane displays any existing authorized users. In the Actions pane, click **Add Allow Rule**.



4. In the dialog, select the appropriate option for your requirements. For **Specified roles or user groups** and **Specified users**, enter the applicable role, group, or user into the field. Click **OK**.



The designated users are authorized to manage parent files in Tracker.

Manual installation syntax values

SmartSync Server supports manual installations where monitoring and manual input during the installation process are not required. Silent installations are executed from the **Run command** or from a **Command Prompt** window.

Command	Description
setup64bit.exe	The SmartSync Server installer.

Available switches

Switch	Description
/S	Required switch requesting a silent installation.
/V	Required switch requesting arguments be passed to the MSIExec engine.
"	Use the double quotation character (**"**).
/qb	Required switch requesting minimal messages and a progress bar. Only basic messages, such as "Restart required", will display.

Available properties

Set certain properties from the command-line after the switch.

Property	Description
ACCOUNTTYPE=	Required variable specifying the type of account used: • 0 - network service. • 1 - local service. • 2 - named user.
IS_NET_API_LOGON_USERNAME=	(Required if ACCOUNTTYPE=2) The user name for the named user: • **username** - local user. • **domain\username** - local account.
IS_NET_API_LOGON_PASSWORD=	(Required if ACCOUNTTYPE=2) The password of the named user.
CWREQUESTS=	Required variable specifying the folder used by the SmartSync FileService.
CW_SYNC_FILEPATH=C:\SyncFiles	Required variable specifying the folder where SmartSync files are stored. Use a UNC file path if the files are stored on a different server than the server running SmartSync FileService.

SmartSync FileService settings

Available FileService settings

Setting Name	Description	Default Value	Optional Value
threadcount	The number of threads the file service will use to schedule tasks.	Number of processors detected on the server	Between 2 - 32
tasktimeout	The number of milliseconds before a task is considered a long running task	7200000ms (2 hours)	Between 5 minutes and 7 days (in milliseconds)
longrunningtimeout	The number of milliseconds before a long running task is killed. **Note:** Value must be least twice the **tasktimeout** value.	86400000ms (24 hours)	Between 10 minutes and 14 days (in milliseconds)
maxlongrunningtasks	The maximum number of long running tasks that can be run simultaneously.	4 tasks	Between 2 and 32
statisticsupdatefrequency	The number of milliseconds before the statistics are written to **Statistics.xml**.	900000ms (15 minutes)	Between 1 minute and 1 hour (in milliseconds)
filewatchertimeout	The number of milliseconds before resetting the folder monitor.	86400000ms (24 hours)	Between 1 hour and 7 days (in milliseconds)
cleanupinterval	The number of milliseconds before checking for stale response files.	86400000ms (24 hours)	Between 1 hour and 7 days (in milliseconds)
responsefilelifetime	How old a response file can be before it is deleted by the file	86400000ms (24 hours)	Between 1 hour and 7 day

Setting Name	Description	Default Value	Optional Value
	service.		(in milliseconds)
backupstatistics	Whether or not to back up the **Statistics.xml** file.	false - not backed up	true or false
statisticsstylesheet	The location of a style sheet to format the statistics XML file.	Not set	Path to a style sheet, which may contain environment variables.
maxlogfilesize	The approximate maximum log file size in bytes before the log file is backed up and truncated back to zero.	10485760 bytes (10MB)	Between 1 MB and 100 MB (in bytes)
lowpriorityinterval	The number of milliseconds before checking for low priority requests.	60000ms (1 minute)	Between 1 second and 1 hour (in milliseconds)
lowpriorityflushschedule	The time ranges during which low priority items will be scheduled. If the specified time ranges contain any overlapping values, the ranges are merged into one continuous range. **Note:** Flush requests can be scheduled at any time, however, a flush request will not be processed if the file to flush is being accessed by a user. By default, flush requests run at midnight to minimize the impact to the file	Tu - Fr 0:00 - 6:00, Fr 22:00 - Mo 6:00	See Notes.

Setting Name	Description	Default Value	Optional Value
	service.		
lowprioritytypeprocesstype	When to process low priority items. **Note:** This value is case-sensitive.	TimeRange	None, Continuous, or TimeRange. See Notes.
flushthreshold	The threshold at which to flush a SmartSync Server file.	11612 bytes	Any value greater than 11612.

Notes:

- The *lowpriorityflushschedule* accepts the following values:
  - **<day>** - is the first two letters of a day of the week in English.
  - **<time>** - is the time in a 24-hour time of the form hh:mm.
- The *lowpriorityflushschedule* accepts the following syntax:
  - **<day> <time> - <time>** - schedules tasks every week on the specified <day> between the specified <time> - <time>. If the first time is greater than the second time, then the end time will be on the following day.

    Example: Fr 17:00 - 23:00 means that low priority items will be scheduled every Friday starting at 5:00pm, and stop being scheduled at 11:00pm.

    Example: Tu 23:00 - 06:00 means that low priority items will be scheduled every Tuesday starting at 11:00pm, and stop being scheduled on Wednesday at 6:00am.
  - **<day> - <day> <time> - <time>** - schedules tasks every day from the first <day> to the second <day> between the first <time> and the second <time>. If the first time is greater than the second time, then the end time will be on the following day. If both days are the same, the same time rules apply.

    Example: Tu - Th 9:00 - 17:00 means that low priority items will be scheduled every Tuesday to Thursday starting at 9:00am, and stop being scheduled the same day at 5:00pm.

    Example: Mo - Fr 22:00 - 7:00 means that low priority items will be scheduled every Monday to Friday at 10:00pm and stop being scheduled the following morning at 7:00am.

- **<day> <time> - <day> <time>** - schedules tasks every week from the first <day> and first <time> to the second <day> and second <time>. If both days are the same, and the first time is greater than the second time, then the end time will be on the same day of the following week. This may cause the low priority schedule to constantly run.

  Example: Fr 22:00 - Mo 6:00 means that low priority tasks are scheduled every Friday starting at 10:00pm, and stop being scheduled the following Monday at 6:00am.

- If the specified time ranges contain any overlapping values, the ranges are merged into one continuous range
- The *lowpriorityprocesstype* values are:
  - **None** - low priority items are never processed.
  - **Continuous** - low priority items are scheduled as they come in.
  - **TimeRange** - low priority items are scheduled only during the *lowpriorityflushschedule* time range.

Metadata fields

List of Working Papers metadata fields that can be used as variables in Working Papers. For example, when adding publish keys in SmartSync Server.

Name	Type	Description	Notes
FileVersion	Number	File internal version number	Example: 8.79 = 2014.00.091
UserFriendlyFileVersion	Text	Working Papers version number	Example: 2014.00
FileId	Text	File Identifier	Hexadecimal GUID Format
ClientId	Text	Client Identifier	Hexadecimal GUID Format
ClientName	Text	Operating Name	-
ClientNumber	Text	Client Number	-
EngagementType	Text	Engagement Type	-
Progress	Text	Progress	-
Status	Text	Status	-

Name	Type	Description	Notes
AssignedTo	Text	Assigned To	-
YearEnd	Date	Year End Date	-
Due	Date	Due Date	-
CreatedBy	Text	Created By	-
LastAccessedBy	Text	Last Accessed By	-
Created	Date	Created On	-
LastAccessed	Date	Last Accessed On	-
IntegrationFlags	Number	Integration Flags	-
ProjectId	Text	Project Identifier	Hexadecimal GUID Format
IntegratedClientNumber	Text	Cloud Entity Number	-
IntegratedClientName	Text	Cloud Entity Name	-
ProjectNumber	Text	Project Number	-
ProjectDescription	Text	Engagement Name	-
InChargeNumber	Text	In Charge Number	-
TeamLeaderNumber	Text	Team Leader Number	-
StartDate	Date	Start Date	-
CompletionDate	Date	Completion Date	-
BudgetedHours	Number	Budgeted Hours	-
BudgetedAmount	Number	Budgeted Amount	-
ContractAmount	Text	Contract Amount	-
LockdownStatus	Text	Lockdown Status	-
LockdownJurisdiction	Text	Lockdown Jurisdiction	-

Name	Type	Description	Notes
LockdownClass	Text	Lockdown Type	-
DocumentCompletionDate	Date	Document Completion Date	-
LockdownDate	Date	Lockdown Date	-
CleanedUp	Yes or No	Cleaned Up	-
YearEndClosePerformed	Yes or No	Year End Close Performed	-
CompanyAddress1	Text	Address (Line 1)	-
CompanyAddress2	Text	Address (Line 2)	-
CompanyCity	Text	City	-
CompanyState	Text	State/Province	-
CompanyCountry	Text	Country	-
CompanyZipCode	Text	Zip/Postal Code	-
CompanyHomePage	Text	Home Page	-
CompanyPhoneNumber	Text	Phone Number	-
CompanyFax	Text	Fax	-
Contact1Title	Text	Contact 1 Title	-
Contact1FirstName	Text	Contact 1 First Name	-
Contact1LastName	Text	Contact 1 Last Name	-
Contact1Designation	Text	Contact 1 Designation	-
Contact1Position	Text	Contact 1 Position	-
Contact1PhoneNumber	Text	Contact 1 Phone	-

Name	Type	Description	Notes
		Number	
Contact1Fax	Text	Contact 1 Fax	-
Contact1CellPhone	Text	Contact 1 Cell Number	-
Contact1HomePhone	Text	Contact 1 Home Number	-
Contact1Email	Text	Contact 1 Email	-
Contact2Title	Text	Contact 2 Title	-
Contact2FirstName	Text	Contact 2 First Name	-
Contact2LastName	Text	Contact 2 Last Name	-
Contact2Designation	Text	Contact 2 Designation	-
Contact2Position	Text	Contact 2 Position	-
Contact2PhoneNumber	Text	Contact 2 Phone Number	-
Contact2Fax	Text	Contact 2 Fax	-
Contact2CellPhone	Text	Contact 2 Cell Number	-
Contact2HomePhone	Text	Contact 2 Home Number	-
Contact2Email	Text	Contact 2 Email	-
StandardIndustryCode	Text	Standard Industry Code	-
AcrossIndustryCode	Text	Across Industry	-

Name	Type	Description	Notes
		Code	
BusinessNumber	Text	Business Number	-
TaxJurisdiction	Text	Tax Jurisdiction	-
SynchronizationDisabled	Yes or No	Synchronization Disabled	-
SmartSync	Yes or No	SmartSync File	-
ReviewerCopy	Yes or No	Reviewer Copy	-
TaxEntity	Text	Tax Entity	N/A, Corporation, S Corporation, Partnership, Non-Profit

Caseware International Inc.

351 King St E, Suite 1100
Toronto, ON M5A 2W4, Canada

T +1 416 867 9504

F +1 416 867 1906

E info@caseware.com

caseware