ivanti | File Director

# Windows Client Advanced Configuration Guide

Version 2018.3 SP1

**Copyright Notice**

# Contents

# Windows Client Advanced Configuration

*Windows Client Advanced Configuration* explains how to install and configure the File Director Windows client. You can configure a Windows Installer package (MSI file) to roll out File Director quickly to multiple users with preconfigured settings applied. You can also use Group Policy ADMX files with a combination of registry settings to apply a base configuration to Windows endpoints. Advanced settings for Single Sign-On, In-location Sync, Sync Controls, and Bandwidth Throttling can also be set up quickly in the same way.

# MSI File

You can configure an MSI file to roll out File Director quickly to multiple users with preconfigured settings applied.

By creating a batch file, you can add a series of commands to set attributes for your File Director deployment, making installation quick and easy for your users. When you roll File Director out to your users, they can run the batch file after installation to apply the default settings you want them to use.

The format for the command line is:

```
MSIEXEC/I DataNow{32/64}.msi {options}
```

Specify the version of windows and replace `{options}` with one or more of the following attribute settings, multiple commands should be separated with a space:

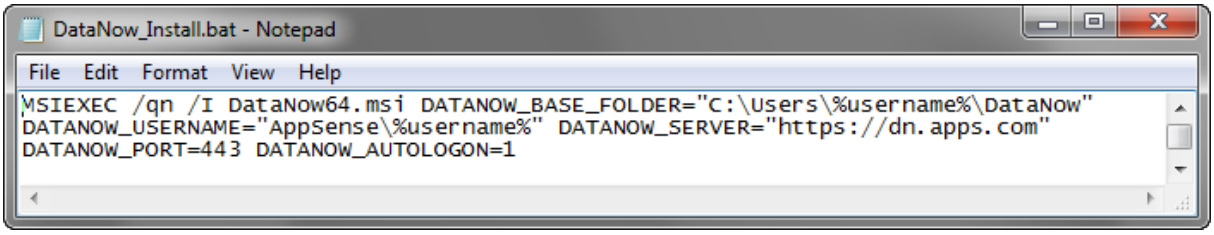
| Command | Details |
|---|---|
| `DATANOW_USERNAME="{username}"` | Replace {username} with a username or use environment variables to apply to a range of users. |
| `DATANOW_SERVER="{servername}"` | Replace {servername} with the server you want users to connect to as a string in quotes. |
| `DATANOW_PORT="{port}"` | Replace {port} with the decimal number of the port on which clients connect to the appliance. |
| `DATANOW_BASE_FOLDER="{local folder}"` | Replace {local folder} with the path of the local File Director folder. |
| `DATANOW_AUTOLOGIN="{1/0}"` | Specify whether to automatically log users in to the File Director server when they start Windows. |

Once created, you can save the batch file with the File Director MSI and email the location to the users to whom you want to roll File Director. They can then install File Director with the MSI and configure the default settings with the batch file.

## Example

The batch file below, opened in Notepad, is for a 64-bit Windows installation and applies the following settings on users' machines:

- Base folder is C:\Users\%UserName%\DataNow
- Server to dn.apps.com
- Port as 443
- Users will automatically log on to the File Director server when they start Windows




To hide the commands when the running the file, start the batch file with @echo off.

# Group Policy ADMX

You can use Group Policy ADMX files with a combination of registry settings (engineering keys) to apply a base configuration to Windows endpoints. Advanced settings for Single Sign-On, In-location Sync, Sync Controls, Bandwidth Throttling, File Locking, and Conflict Resolution can also be set up quickly in the same way.

File Director group policies are provided in the File Director GroupPolicy zip file, which customers can download from the support web site. The zip file contains DataNow.admx and the en-US folder containing DataNow.adml language file.

The File Director Group Policy ADMX file can be used with both Local and the Domain-based Group Policy. Save the ADMX file and the language folder to **%systemroot%\PolicyDefinitions** to make the policies editable through Administrative Templates in either the Group Policy Object Editor or the Group Policy Management Console.

For further details about editing local and domain-based GPOs with ADMX files, see

When you use the ADMX template to configure settings via a GPO, the registry values are written into the Policies section in HKCU and HKLM.

Registry settings are evaluated in the following order, with highest priority applied:

1. HKCU Policy (HKCU\Software\Policies\AppSense\DataNow)
2. HKLM Policy (HKLM\Software\Policies\AppSense\DataNow)
3. HKCU (HKCU\Software\AppSense\DataNow)
4. HKLM (HKLM\Software\AppSense\DataNow)

For more information on configuring the settings for the base configuration and advanced settings, see the relevant topics.

# Base Configuration

During installation, users require a valid username, password, and the File Director server name. The installation wizard walks through the steps required to successfully connect to a File Director server. Many administrators may want to automate this, or roll the required settings into any base image.

## Setup

The table below contains the recommended minimum items an administrator should configure to enable a user to successfully logon to a File Director service.

| Values | Description |
|---|---|
| Value Name: **DataNowBaseFolder** Value Type: **REG_SZ** | The location under which all File Director map points appear for the user. If using In-location Sync, the option must still be specified but this path is only used to contain shared map points. The full path is required, for example. %USERPROFILE%\DataNow<br><br>If you apply these settings using Environment Manager, you must double-escape any environment variables - for example, %%USERPROFILE%%. |
| Value Name: **DataNowServer** Value Type: **REG_SZ** | The URL of the server including the protocol. For example, https://dn.domain.com. DataNowPort must be appropriate for the protocol. |
| Value Name: **DataNowPort** Value Type: **REG_DWORD** Default Value: **443** Minimum Value: **1** Maximum Value: **99999** | The port used for communication with the server. This must match the scheme used in the server address. For example, for HTTPS, port 443.NoteDataNowPort must be appropriate for the protocol as defined inDataNowServer. |
| Value Name: **Username** Value Type: **REG_SZ** | Set the username for users. This can be in one of three formats:<br>• UPN – user@mydomain.com<br>• DNS Name – mydomain.com\user<br>• DNS Short Name – MYD\user<br>You can use environment variables to set the username for all users according to their login credentials:<br>• UPN – %USERNAME%@%USERDNSDOMAIN%<br>• DNS Name – %USERDNSDOMAIN%\%USERNAME%<br>• DNS Short Name – %USERDOMAIN%\%USERNAME% |

| Values | Description |
| --- | --- |
| | In the case where **EnableSSO** is going to be used, the username format must be UPN. Commonly defined using environment variables under HKLM, i.e. %USERNAME%@%USERDNSDOMAIN% |

# User and Profile Options

Other basic configuration items available to administrators enable changes to the File Director file overlays and tray notifications.

| Values | Description |
| --- | --- |
| Value Name: **DataNowOverlayMask** Value Type: **REG_DWORD** | The overlays that are displayed on endpoints. You can enable or disable the following file overlay icons that users can see in Explorer:<br>• **Pending** - The file is not in sync and requires synchronization<br>• **Synchronized** - The file is in sync (up-to-date)<br>• **Synchronizing** - The file is being synchronized<br>• **User action** - User action is required<br>• **Base folder** - The 'File Director' icon will be overlaid on the base folder<br>• **Home folder** - The 'home' icon will be overlaid on the home map-point folder<br>• **ReadOnly folder** - The 'read only' icon will be overlaid on a read-only folder<br>• **Shared folder** - The 'shared' icon will be overlaid on a non read-only, non-home online map-point folder<br>• **Offline folder** - The 'offline' icon will be overlaid on an offline map-point folder<br>The values chosen for this setting have no effect on the installation and registration of the overlays with Windows Explorer.<br>The default value enables the following: Home, ReadOnly, Shared and Offline folder overlays plus Pending, Synchronized, Synchronizing and User Action file |

| Values | Description |
| --- | --- |
| Value Name:<br>**DataNowShowStatusUpdates**<br>Value Type: **REG_DWORD** | Balloon notifications appear in the system tray and typically show error messages. Only unrecoverable errors are shown in this way, such as attempting to sync a file to a map point that no longer exists or has been made read only by the administrator. No value or any non-zero value enables notifications, a value of 0 (zero) disables notifications. |

# Single Sign-On

File Director can be configured to automatically log users into File Director using their Windows credentials. The Windows logon must be to the same domain to which the File Director Appliance is connected.

If a Windows domain password is modified locally while File Director Single Sign-On is enabled, the new password is used for subsequent File Director logins.

## NTLM

Once SSO has succeeded, credentials are stored in the Windows Credential Store and AutoLogon is enabled. The File Director client will then automatically handle File Director session expiry and will only prompt for a password in the event of a background logon failure, if the password expires, or if the user changes their password using another device. If the user changes their password using the same Windows endpoint, the SSO credentials are automatically updated.

## Kerberos

Endpoints must have access to the Kerberos Ticket Granting server within Active Directory (AD) to locate the key information associated with the user account and allow a token to be returned to the client system, allowing access the File Director server. In order to use Kerberos authentication from the Windows endpoint, the environmental prerequisites for Kerberos Authentication must be met.

For more information, see Kerberos authentication.

## Setup

| Values | Description |
|---|---|
| Value Name: **EnableSSO**<br>Value Type: **REG_ DWORD** | Automatically logs users in to File Director when they successfully log in to Windows.<br>To disable SSO **EnableSSO** set to **0**<br>To enable SSO using NTLM **EnableSSO** set to **1**<br>To enable SSO using Kerberos **EnableSSO** set to **2**<br>For Kerberos, the environment prerequisites must be met. |

# Bandwidth Throttling

File Director can support customers in scenarios where network speed or quality may result in a lower quality of service for users. Bandwidth Throttling routinely and passively measures the available upload bandwidth between the File Director Windows client and map point storage. No additional bandwidth is consumed as a result of these measurements.

File Director administrators can apply settings for Windows clients to consume a percentage of the total bandwidth available. The following settings can be defined in **HKLM/Software/AppSense/DataNow** for all appropriate endpoints.

These keys only affect uploads.

| Values | Description |
|---|---|
| Value Name: **AutoThrottlePercentage**<br>Value Type: **REG_DWORD**<br>Value Data: **Decimal Value** 0 to 100<br>Default Value: 100 | The percentage of the estimated pipe that File Director is permitted to use:<br>• 100 – Turns off throttling<br>• 1-99 – The percentage of available estimated upload bandwidth is used<br>• Value not present – 100 percent of estimated available bandwidth is used<br>This setting is only available for HKLM. |
| Value Name: **AutoThrottleMinimumKBps**<br>Value Type: **REG_DWORD**<br>Value Data: **Decimal Value** (in kbps)<br>Default Value: 30 | The minimum limit in Kb/s below which the File Director connection is not throttled.<br>File Director runs a passive test on its own upload speed, and once it's collected enough data will throttle its connection to use a percentage of that upload pipe. This setting applies a minimum working connection speed beyond which, File Director will not throttle.<br>In certain network conditions the test may not be reliable. For example, uploading very large numbers of tiny files can skew the result causing underestimation of available bandwidth or where there is an excellent connection to the network but very poor connection to the DN server. This can cause us to falsely underestimate the size of the upload pipe.<br>This setting is only available for HKLM. |
| Value Name: **AutoThrottleRetestInterval** | How often File Director retests the amount of available bandwidth. Enter a value in milliseconds. Performing this test briefly removes the throttle. If a value is not present a period of 1 hour |

| Values | Description |
| --- | --- |
| Value Type: **REG_DWORD**<br><br>Value Data: **Decimal Value** (interval in ms)<br><br>Default Value: 3600000 | (3600000ms) is applied.<br><br>File Director needs to perform this retest as network conditions may change on the end point. For example, the user may be roaming across different wireless networks and a throttle value which seemed appropriate at a particular time of the day may be inappropriate at another.<br><br>This setting is only available for HKLM. |

# In-Location Sync

In-location Sync (ILS) allow folders within the user's profile to be mapped directly into File Director without the need for complex redirection or asking users to change their behaviors. The private map point does not have to be the default "home" map point - using the **PrivateMapPoint** engineering key, administrators can select any private map point in the map point listing but only one map point can be used for ILS.

ILS is an alternative to folder redirection and should not be used in conjunction with it.

Use the **InLocationSyncFolders** engineering key to configure a set of folders for ILS. This REG_MULTI_SZ key provides administrators with a single key to define all of the folders inside the user's profile which are to be managed by File Director.

At log on, File Director automatically creates the folder mappings as defined by the **InLocationSyncFolders** engineering key. The mapping creates the folder inside the private map point and synchronizes data directly from the user profile. When configured for ILS, the private map point will no longer be visible in the map point listings, as essentially the local locations are File Director folders. The user must log out and back into File Director for the settings to take effect.

It is possible to use InLocationSyncFolders to set an entire user profile - the user profile root folder - to be managed by File Director. This means, for example, that - regardless of a user's folder customization - any data under their profile is captured for backup or migration.

If you set the total user profile as a managed location. using other map points (Mapped Drives) is not supported.
The File Director folder is part of the user profile. Before you make the base user profile folder a managed location, you must first move the File Director folder out of the user profile. If you do not, you will get an error message when you log into the client.

You can set the user profile as a mapped location using environment variables or an absolute path. See the table below for examples. When you set a user profile as a managed location, some folders in the profile are ignored by File Director by default.

This is to save bandwidth and storage because the folders contain non-user data. You can add or override profile folders to ignore using the standard File Director exclusions and exclusion override functionality. For more information about default exclusions and exclusion overrides, see Exclusions and Electives.

| Values | Description |
|---|---|
| Value Name: **PrivateMapPoint** | This map point is the only one that may have In-Location Sync folders |

| Values | Description |
|---|---|
| Value Type: **REG_SZ** | mapped into it. If not operating In-location Sync mode, the private map point displays with the home overlay when viewed in the File Director folder. Enter the name of the private map point preceded by a forward slash.<br><br>If no value is present, /home is used as the private map point |
| Value Name: **InLocationSyncFolders**<br><br>Value Type: **REG_MULTI_SZ** | This key maps the local folders to the destinations inside the private map point. For example, a user's My Documents or Desktop can be mapped so all files in these locations are automatically synced with File Director. Local locations can be paths or Microsoft CSIDL locations.<br><br>Multiple locations can be defined in the key, with each mapping on a separate line. Each mapping takes the format of destination, source (separated by a comma).<br><br>Examples include:<br><br>• /My Documents,CSIDL_MYDOCUMENTS<br>• /My Documents,%USERPROFILE%\Documents<br>• /Desktop,CSIDL_DESKTOP,HIDE_OVERLAYS<br><br>In last example above uses the HIDE_OVERLAYS flag so that the File Director overlays do not appear on desktop icons.<br><br>The destination can also include variables:<br><br>• /Backup/%computername%/%username%/Documents,CSIDL_MYDOCUMENTS<br>• /Backup/%/Backup/%username%/Download,%userprofile%\Downloads<br><br>The following examples set an entire user profile as a managed location:<br><br>• /Profile, %UserProfile%<br>• /Profile, CSIDL_PROFILE<br><br>If the list is incorrectly defined, the File Director client will not login and an error message will be logged locally. |

If you experience errors during configuration, see In-Location Sync Errors for more information.

# Mapped Drive

This feature extends In-Location Sync functionality enabling all File Director shared map points to be mapped drives. Administrators can map any File Director shared map point in Windows Explorer to user's native mapped drives. This includes the Home map point, if it has not already been mapped by In-Location Sync.

Mapped Drive functionality is not supported when you have set the entire user profile as a managed location.

| Values | Description |
|---|---|
| Value Name:<br>**MappedDrives**<br>Value Type:<br>**REG_MULTI_SZ** | This key maps shared map points to mapped network drives. Multiple mapped drives can be defined in the key. The drive and the map point must be separated by a comma and each drive must be on its own row. There must not be a space following the comma otherwise the space will be added to the map point name.<br>For example:<br>T,Company Documents<br>Z,Team Shares<br>This example maps the Company Documents shared map point to the T drive and the Team Shares shared map point to the Z drive.<br>User home/map points can be mapped using the format above. |

# File Sync Controls

File Director keeps all files in sync, regardless of age, type, or size. The sync happens when a user logs in or interacts with files in both automatic or manual modes, based on server policy.

You may want to tailor what gets synced, saving network bandwidth and storage.

You can customize file syncing in File Director using a series of engineering keys. Set the engineering keys at the following locations:

- HKCU\Software\Policies\AppSense\DataNow
- HKLM\Software\Policies\AppSense\DataNow
- HKCU\Software\Appsense\DataNow
- HKLM\Software\Appsense\DataNow

HKCU settings take precedence over HKLM settings.

## Excluding and electing files

You can use file sync controls to exclude files and file types from being uploaded and downloaded. For example, temporary files are automatically excluded from synchronization and are not uploaded.

You can also define electives. Files for which an elective applies are visible to users but must be synchronized individually using the option from the File Director context menu or by double-clicking the required file. Electives are a way to avoid heavy network traffic. A good example is to make files over a certain size elective, and so not automatically synchronized.

When enabled, exclusions and electives are enforced across all map points regardless of map point sync policy. Changes are applied when the user logs into File Director.
For more information, see Exclusions and Electives.

## File prioritization

Unlike other sync technologies, File Director is aware of user interaction and delivers needed content first.  As soon as files are identified, syncing starts and files are queued for upload and download. While syncing is in progress, File Director dynamically prioritizes the files according to the following criteria:

- Activity origin - For example, a double-click by a user indicates that a file is likely to be more important than a file that is simply found during onboarding.
- Previous run status - For example, if a file was previously downloading and then paused, it will jump the queue when downloading is resumed.
- Low priority status - You can designate files as low priority for syncing using an engineering key that uses the same language as exclusions and electives
- Last modified time - Files with the most recent modified time are given priority, as they are most likely to be files that users want or need.

For more information on configuring low priority files, see File Prioritization.

### Delta uploads and downloads

Depending on file size, syncing can consume a lot of bandwidth, so File Director supports delta uploads and downloads, in which only the altered portion of a file is synced. However, a delta upload can be expensive in terms of CPU usage. Using file sync controls, you can set a size threshold after which a file is eligible for delta uploads.

For more information, see Delta Sync Options.

### Using Engineering keys to control syncing

Some types of files, such as database type files, present a problem for syncing because these files are often large and remain open or locked. Further writes to the files can occur while syncing is taking place. To resolve the issue for these file types, File Director supports the Windows Volume Shadow Copy service, which creates read-only point-in-time snapshots of volumes, even when they are in use. Shadow Copy syncing of these file types takes place at regular intervals - the default is 24 hours. You can alter the interval using an engineering key.

You can also use engineering keys to set whether:

- Users have the ability to apply their own sync preferences at folder level. See Endpoint Sync Policy
- File Director client will still report stats such as user cache size and file count via the usual server interface. See Endpoint Sync Control.

### Cache cleanup

File Director provides an automatic cache cleanup function configurable to your requirements. This can help simplify maintenance and reduce endpoint hard disk usage.

The cache cleanup will apply only to files that have been synced, where the user is online, and where no uploads are pending. As an administrator, you determine the grace period, this is the length of time unused files may remain in the cache before being removed. When the grace period expires the cached files are removed from the local cache. Rules can be specified to exclude specific file types from the cleanup. See Cache Cleanup.

## Exclusions and Electives

Set exclusions in the following locations:

- HKCU\Software\Policies\AppSense\DataNow\FilePolicy\Exclusions
- HKCU\Software\Policies\AppSense\DataNow\FilePolicy\ExclusionOverrides
- HKLM\Software\Policies\Appsense\DataNow\DeltaPolicy\Exclusions
- HKLM\Software\Policies\Appsense\DataNow\DeltaPolicy\ExclusionOverrides

Set electives in the following locations:

- HKCU\Software\Policies\AppSense\DataNow\FilePolicy\Electives
- HKCU\Software\Policies\AppSense\DataNow\FilePolicy\ElectiveOverrides
- HKLM\Software\Policies\Appsense\DataNow\DeltaPolicy\Electives
- HKLM\Software\Policies\Appsense\DataNow\DeltaPolicy\ElectiveOverrides

HKCU settings take precedence over HKLM settings.

You define electives and exclusions using expressions.

## Default Values

File Director includes a default exclusion expression that prevents temporary, partial, and other files that are unlikely to be required from being synchronized.

| Exclusion | Description |
|---|---|
| `.*\.tmp` | All files ending with .tmp |
| `.*\.partial` | IE temp download files |
| `.*\.crdownload` | Chrome temp download files |
| `*\.part` | Firefox temp download files |
| `.*\.download` | Safari temp download files |
| `~\$.*` | All office backup files starting with ~$ |
| `[0-9A-F]{8,8}` | Excel temp files |
| `.*~` | Files ending in a tilde ~ |
| `$Recycle.Bin` | The Recycle bin |

## Default Exclusions for User Profile Folders

If you use In-Location Sync to select an entire user profile to be managed by File Director, the following locations in the profile are ignored by default to save bandwidth and storage:

- The App Data directory
- NTUSER.DAT* files, for example ntuser.dat.LOG1 or ntuser.ini
- OneDrive
- Junctions, for example Links, Favorites, or Printer Shortcuts

You can add additional locations in a user profile to ignore using the standard exclusions language. For example, if installed, you may want to exclude the Dropbox folder.

Default exclusions are always applied unless they are explicitly overridden by an ExclusionsOverride entry in the registry. For more information, see Exclusion and Elective Overrides.

## Variables

When an expression is evaluated by the File Director client, the following variables are initialized with information relating to the file being processed:

| Variable | Description |
|---|---|
| Size | The size of the file. |
| Age | The period between now and the date the file was last modified in days, months or years (d, m or y). |
| Path | The full path of the local file including drive and parent directories. |
| Name | The name of the file. For example, file.docx. |
| Ext | The extension of the file. For example, docx. |
| Type | The type of file. This can be file or directory. |
| InSync | True if the file has previously been synchronized because it had a different name or its size or age meant it was previously not excluded. |

Files can be excluded on the basis of:

- **Type** - The exclusion is applied against the filename extension and not using any metadata inspection to determine the file type. One file type exclusion can be set for each key.
- **Size** - Files over a defined maximum limit are excluded from synchronization. Customers can define maximum size of any file to be synced. The file size limit is set in MB one size limit exclusion per key can be set.
- **Age** - Files older than a defined maximum age are excluded from synchronization. The maximum age is taken from the Last Modified date. One age restriction exclusion per key can be set.

Environment variables are supported in exclusion expressions when used with the `BENEATH` keyword. You can also use an absolute path. For example, the following expression uses the `BENEATH` keyword to exclude both the Favorites and the Links folder when a user's profile is set as a managed location:

```
BENEATH == "%USERPROFILE%\Favorites" OR BENEATH == "%USERPROFILE%\Links"
```

There are no user-definable variables in the expressions. If the client encounters a syntax error in an expression, a message is logged in the Windows event log and the default values are applied.
You can apply multiple exclusions in a single expression, for example see the expression in the last row of the table.

### Examples

| Example | Description |
|---|---|
| `Ext In [doc docx]` | The file's extension is doc or docx. |
| `Age > 5Y` | The file was created over 5 years ago |
| `Size >= 2Gb` | The size of the file is greater than or equal to 2Gb. |
| `Name = /.*~/` | The name of the file matches the regular expression ".*~" i.e. the filename ends in a tilde. |
| `Path = /\$Recycle.Bin$/` | The path of the file matches the regular expression "\$Recycle.Bin$", i.e. the path ends with the string "$Recycle.Bin". |
| `((Age > 5Y) OR (size > 2Gb)) AND (Ext NotIn [doc docx])` | Files older than five years, or bigger than 2Gb but not Word documents. |

## Exclusion and Elective Overrides

To override an exclusion, create an Override entry in one of the following locations:

- HKCU\Software\Policies\AppSense\DataNow\FilePolicy\ExclusionOverrides
- HKLM\Software\Policies\Appsense\DataNow\DeltaPolicy\ExclusionOverrides

To override an exclusion, create an Override entry in one of the following locations:

- HKCU\Software\Polices\AppSense\DataNow\FilePolicy\ElectiveOverrides
- HKLM\Software\Policies\Appsense\DataNow\DeltaPolicy\ElectiveOverrides

Overrides use the same language as exclusions. For example, if a user wants remove the exclusion of TMP files, they can define an Override value as follows:

```
HKCU\Software\Policies\AppSense\DataNow\FilePolicy\ExclusionOverrides]
"Allow tmp files"="Ext In [tmp]"
```

This turns off the default exclusion of TMP files, but all other default exclusions remain in place.

# File Prioritization

Using the same expression mechanism as exclusions and electives, you can use the LowPriorityFileTypes key to configure files that will be treated as low priority for syncing. You can also configure an expiry date for the low prioritization, in terms of how old the file is. For example, if you configure a low priority for filesthis means that recent large ISO and MP3 files are given a low upload or download priority. However, once files older than 12 days are being processed for syncing, the ISO and MP3 files are synced in terms of age order, like any files.

| Values | Description |
|---|---|
| Value Name:<br>**LowPriorityFileTypes**<br>Value Type:<br>**REG_EXPAND_SZ** | Defines the files to be treated as low priority for syncing. Set the value using an expression with the same variables and values as for exclusions and electives. If an expression is present, the expression is used to determine which files to treat as lower priority. If no expression is present, no files are regarded as low priority. |

# PST Synchronization

Endpoints can now synchronize file formats in the user's profile, including the large database format of PST.

File Director is a sync technology; if you use the same file in multiple locations, conflicts can occur.

| Values | Description |
|---|---|
| Value Name:<br>**ShadowSyncPeriod**<br>Value Name:<br>**REG_DWORD** | By default, File Director synchronizes PST files every 24 hours. Using ShadowSyncPeriod admins can change the frequency in which PST files are synchronized from the endpoint. Set the ShadowSyncPeriod to an integer in seconds, to define the period. If set to zero or if a value is not present, the default of 86400 seconds (24 hours) is used. |
| Value Name:<br>**ShadowSyncChangeThreshold**<br>Value Type:<br>**REG_DWORD** | This setting allows for files with a large amount of change to be synchronised early. The setting specifies the number of megabytes change in a file that will trigger an upload ahead of the regular ShadowSyncPeriod. By default this feature is turned off (a value of 0). If turned on, we recommend a minimum threshold of 100Mb is used. |

# PST Smart Linking

When opening Outlook for the first time on a new endpoint, File Director will download the PST file(s) if they are not held locally. The end user may experience delays at logon whilst the file is being downloaded. File Director performs a background task to unlink any remote Outlook Data Files (PST) before Outlook is opened on a new endpoint for the first time. This occurs before the desktop has been loaded, ensuring that the end user experience is not affected whilst potentially large PST files are download. Once PST files are downloaded, File Director then performs a relink in the background, ensuring a smooth onboarding process for the end user throughout.

By default PST unlinking and relinking in File Director is enabled.

| Values | Description |
|---|---|
| Value Name:<br>**PstUnlinkingEnabled**<br>Value Name:<br>**REG_DWORD**<br>Default Value: **1** | To disable PST unlinking and relinking background tasks, set the value of this key to 0.<br>The key is stored in: HKLM\Software\AppSense\DataNow\ |

# Endpoint Sync Policy

Set whether users have the ability to apply their own sync preferences at folder level.

| Values | Description |
|---|---|
| Value Name:<br>**ForceManualMode**<br>Value Type: **REG_DWORD** | Set all folders to manual mode. This hides the sync/unsync File Director menu. A non-zero value applies manual mode to all folders. No value or a value of 0 uses the preferences set by the admin or user. |

# Endpoint Sync Control

If this is switched on, the File Director client will still report statistics such as user cache size and file count via the usual server interface. This allows administrators to produce reports on the statistics so that staggered on-boarding decisions can be made for particular groups of users based on what is known about their local caches.

| Values | Description |
|---|---|
| Value Name:<br>**AdminPause** | Permits administrator, via group policy or Environment Manager, to specify that an end point should not sync any data. To enable admin pause, set to1. To unpause the endpoint, either set to 0 or remove the entry. The |

| Values | Description |
|---|---|
| Value Type: **REG_DWORD** | AdminPause value is written in HKCU\Software\AppSense\DataNow.Note |

# Delta Sync Options

| Values | Description |
|---|---|
| Value Name: **DownloadFileSizeDeltaThreshold**<br>Value Type: **REG_DWORD**<br>Default Value: **4096**<br>Minimum Value: **4096**<br>Maximum Value: **4294967296 (4Gb)** | The size, in bytes, that a file must be larger than for File Director to attempt a delta download. |
| Value Name: **UploadFileSizeDeltaThreshold**<br>Value Type: **REG_DWORD**<br>Default Value: **4096**<br>Minimum Value: **4096**<br>Maximum Value: **4294967296 (4Gb)** | The size, in bytes, that a file must be larger than for File Director to attempt a delta upload. If a value is not present, the default value is used. |

# Sync Status

Shows the status of File Director endpoints in terms or sync activity. The value is automatically updated and can be used in applications, such as Environment Manager, to create actions and conditions that are dependent on the sync status of endpoints.

| Values | Description |
|---|---|
| Value Name:<br>**DataNowSyncStatus**<br>Value Type:<br>**REG_DWORD** | The DataNowSyncStatus value is stored in HKCU\Software\AppSense\DataNow and can show one of the following values:<br>• 0 = IDLE - The endpoint is in currently in sync. This is the ideal state for an upgrade, refresh or OS update.<br>• 1 = SYNCING - There is some sync activity currently occurring on the endpoint such as uploading, downloading and listing. This activity makes it unsuitable for an upgrade.<br>• 2 = PAUSED - There is currently no sync activity on the endpoint and its state is remains unknown until the endpoint is taken off pause. |

| Values | Description |
|---|---|
| | • 3 = OFFLINE - The endpoint is offline and until it contacts the server, its state remains unknown. |

## Cache Cleanup

When enabled, a grace period is specified to determine how long unused files can remain in the cache before being considered for deletion. At a system level, File Director monitors for file closes and uses the period of no closes as the period of inactivity. Certain third party applications such as Explorer.exe for example, will continuously open and close cached files without user action. For this reason, processes performed by specified applications are excluded from cache cleanup altogether. Additional application processes can be added to the exclusion blacklist.

Personal folder files (.pst files) are excluded from the cache cleanup due to their typical size. Further file types can be added to the list of exclusions such as .pdf for example.

File Directorchecks any file identified for removal to ensure the client is online, the file exists locally and on the server, and that the file is in sync with no uploads pending. If the criteria are met, then the file will be marked for removal from the cache. If the file cannot be removed immediately from the cache, it will be removed at the next earliest opportunity, for example, when the file has uploaded to the server.

All files removed from the cache are audited and recorded in event logs.

| Values | Description |
|---|---|
| Value Name:<br>**CacheCleanupEnabled**<br>Value Type: **REG_DWORD**<br>Default Value: **0** | The cache cleanup function is enabled / disabled via the CacheCleanupEnabled key. By default, cache cleanup is disabled.<br>The key is stored in HKLM\SOFTWARE\AppSense\DataNow and can show one of the following values:<br>• 0 = DISABLED - The cache cleanup function is disabled.<br>• 1 = ENABLED - The cache cleanup function is enabled. |
| Value Name:<br>**CacheCleanupGracePeriod**<br>Value Type: **REG_DWORD**<br>Default Value: **300 (5m)** | The grace period is specified via the CacheCleanupGracePeriod key. The value entered is measured in seconds. The default value is 300 seconds.<br>The key is stored in HKLM\SOFTWARE\AppSense\DataNow |
| Value Name:<br>**CacheCleanupBlacklist**<br>Value Type: **REG_MULTI_SZ** | File closes that have been triggered by certain web browser applications are excluded from the grace period. By default the list includes: explorer.exe, mspeng.exe, svchost.exe, runtimebroker.exe, searchprotocolhost.exe |

| Values | Description |
|---|---|
| Default Value: **explorer.exe, mspeng.exe, svchost.exe, runtimebroker.exe, searchprotocolhost.exe** | Process exclusions are added via the CacheCleanupBlacklist key.<br>The key is stored in HKLM\SOFTWARE\AppSense\DataNow |
| Value Name:<br>**CacheCleanupExcludedFileTypes**<br>Value Type: **REG_MULTI_SZ**<br>Default Value: **pst** | File types can be excluded from the cache cleanup process. By default .pst files are excluded so will not be selected for removal.<br>File types are excluded from the cache cleanup function via the CacheCleanupExcludedFileTypes key.<br>The key is stored in HKLM\SOFTWARE\AppSense\DataNow |

Enabling/disabling cache cleanup and /or setting the grace period will require a File Director logoff/logon or service restart.
To prevent Access Denied errors or files being removed before applications are fully initialized, it is recommended that 10 seconds is the minimum grace period value.

# File Locking

File Director provides offline access to content by keeping local copies (caches) on the endpoint, which File Director tracks and keeps in sync with the back end storage. Some users are used to working corroboratively on shared resources where desktop applications honor read-write or read-only access depending on who accesses the content first. Such local cached access requires changes to workflows and behaviors.

The File Director locking feature provides the benefits of local cached content whilst providing the native file locking experience that users may be used to when accessing content directly over SMB. The file locking feature maintains a lock on back end storage for files open on the endpoint whilst keeping the endpoint cache in sync. This file lock is not only part of the

Native SMB locking is driven by the application, with most not requesting to maintain a lock. File Director uses a whitelist approach to define which application requests to maintain a lock through File Director.

File Director file locking is not enabled by default and is activated on the Windows endpoint.

For this setting to function correctly, clients must be connected to a server that supports file locking.

| Values | Description |
|---|---|
| Value Name: **ServerLockingEnabled**<br>Value Type: REG_ **DWORD** | A non-zero value activates file locking. Activated windows clients synchronously contact the File Director server to obtain a lock where the application supports it.<br>When activated the default applications that request to maintain a lock are:<br>• Microsoft Excel (EXCEL.EXE)<br>• Microsoft Access (MSACCESS.EXE)<br>• Microsoft Publisher (MSPUB.EXE)<br>• Microsoft OneNote (ONENOTE.EXE)<br>• Microsoft PowerPoint (POWERPNT.EXE)<br>• Microsoft Visio (VISIO.EXE)<br>• Microsoft Project (WINPROJ.EXE)<br>• Microsoft Word (WINWORD.EXE)<br>• Microsoft Office InfoPath (INFOPATH.EXE)<br>• Microsoft Organization Chart (ORGCHART.EXE)<br>  All File Director Windows endpoints must be activated to provide a consistent experience across the entire estate. |

# Conflict Resolution

File Director conflict resolution allows administrators to configure the format of file and folder names, following a conflict during syncing. For example, by appending a file name with an incrementing number or the date and time. Multiple flags can be used at the same time and different flags can be applied to specific users and groups or company-wide.

An optional user interface can be displayed to users in the event of a conflict occurring. This allows users to manage conflict resolution themselves.

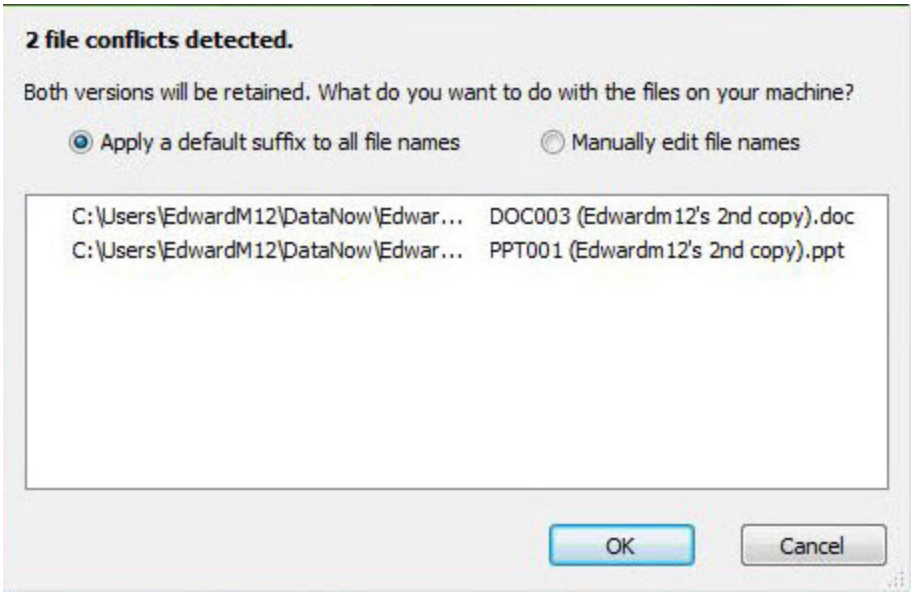
To change the file naming format flag use the key and flags in the table below.

| Values | Description |
|---|---|
| Value Name: **ConflictFileFormat**<br><br>Value Type: **REG_EXPAND_SZ** | The available format flags are:<br>• **%N** - An incrementing permutation number (e.g. 1, 2, etc)<br>• **%k** - Suffix associated with permutation (e.g. nd, th etc)<br>• **%l** - The lower case user name (e.g. john)<br>• **%L** - The capitalized user name (e.g. John)<br>• **%a** - Abbreviated weekday name (e.g. Thu)<br>• **%A** - Full weekday name (e.g. Thursday)<br>• **%b** - Abbreviated month name (e.g. Aug)<br>• **%B** - Full month name (e.g. August)<br>• **%d** - Day of the month, zero-padded (01-31) (e.g. 23)<br>• **%H** - Hour in 24h format (00-23) (e.g. 14)<br>• **%I** - Hour in 12h format (01-12) (e.g. 02)<br>• **%m** - Month as a decimal number (01-12) (e.g. 08)<br>• **%M** - Minute (00-59) (e.g. 55)<br>• **%p** - AM or PM designation (e.g. PM)<br>• **%S** - Second (00-59) (e.g. 02)<br>• **%x** - Date representation (e.g. 08-23-01)<br>• **%X** - Time representation (e.g. 14.55.02)<br>• **%y** - Year, last two digits (00-99) (e.g. 01)<br>• **%Y** - Year (e.g. 2001)<br><br>For example, (%L's %N%k copy) would result in "filename (John's 2nd copy).docx"<br><br>The format must include either %N, %S, %X to make the filename unique enough. |

To enable the conflict resolution dialog for end users, use the key in the table below.

| Values | Description |
|---|---|
| Value Name: **ManualConflictResolution**<br>Value Type: **REG_DWORD** | Permits users to manually control the renaming of files if a conflict is detected with a dialog. A non-zero value enables the dialog allowing users to manage conflict resolution. The default value of zero prevents the dialog displaying and files and folders are renamed according to the flags set for the ConflictFileFormat key. |

When a conflict arises users are presented with the following dialog, allowing them to manage the resolution themselves.



# Diagnostics and Troubleshooting

## Services vs Tray

When troubleshooting an issue, it is common practice to turn off services in turn to see whether a particular service is causing the problem. However, File Director services are responsible for syncing files. It is recommended that you leave the services running and exit the File Director tray by clicking the File Director icon in the system tray and clicking **Exit**. The current work queue will be processed and then syncing will continue once you restart the tray.

## Client Logging

The default location for log files is %programdata%\AppSense\DataNowLogs. This location can be customized; if required, please contact Ivanti Support.

For further information, see this article.

### Turn on Client Logging

To turn on logging in a client, hold down **Shift** and right-click the **File Director** icon in the system tray.

In the context menu, select **Diagnostics** > **Start Logging**.

For advanced logging settings, and a tracedump tool to convert ETL file to text, see this article.

## In-location Sync Errors

If ILS fails to configure, a message displays and an error is registered in the Windows Event Log. There can be numerous causes for this, such as invalid CSIDL specification or a path outside of the profile.