ivanti

File Director OneDrive for Business Connector

WHITE PAPER

Contents

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as “Ivanti”), and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.Ivanti.com.

Purpose of this Document

This document demonstrates how Ivanti® File Director can be configured to use OneDrive accounts as the storage location for users' home map points. File Director can then utilize the 1TB of storage, included free of charge, with each Office 365 for Business license.

Once configured, users can update files on map points using File Director and OneDrive clients. All changes are synchronized with the File Director server so the files are up-to-date, regardless of the client used to edit or view them.

We will use a small case study to illustrate the power of the File Director OneDrive for Business connector. This will demonstrate how the complex task of migrating to Microsoft Windows 10 can be simplified and keep end-user disruption to a minimum.

It should be noted that this document will not include details on the initial installation or configuration of Ivanti File Director.

Assumptions

Throughout this document, is it is assumed that Ivanti File Director version 4.3 or later is installed and configured, and that the new Microsoft Azure AD portal is being used.

Prerequisites

- Your perimeter firewall must allow communication to <instance name> - my.sharepoint.com on port 443 and Microsoft-supplied URLs detailed in this article.
- You are an Office 365 administrator.
- Your public domain is associated with your Azure AD instance.
- Password replication is set up on your local AD.

  Note: *Federated AD access is not supported. The local username UPN must match the one used to sign into Azure. Users' on-premises AD passwords must be in sync with Azure AD.*

- Users have an Office 365 license assigned to them from the Office 365 Admin Center.
- Users have OneDrive storage provisioned.

For further information about how to pre-provision OneDrive for Business for your users, see: https://technet.microsoft.com/en-us/library/dn800987.aspx

For further reading about integrating applications with Azure AD, see the following Microsoft documentation.

The Challenges of Office 365

It’s no secret that migrating from on-premises file servers to storage hosted by Microsoft in its public cloud has compelling benefits. Not only does it allow continued access to the ubiquitous Office programs such as Word, Outlook, and Excel, it provides document synchronization with the 1TB of free storage via OneDrive. This functionality provides benefits to the IT organization that include:

- Anytime, anywhere access to documents.
- No need for a Virtual Private Network (VPN) connection to be established.
- Reduction in storage and infrastructure costs.

Organizations are realizing these benefits and are migrating at an increasing rate—leading to a 43-percent year-on-year increase in Office 365 adoption from June 2016 to June 2017. However, and as with any transition of this scale, a migration to Office 365 can introduce roadblocks, namely:

- No centralized reporting or control over which file types, size, or age are synchronized.
- OneDrive lacks the necessary synchronization and reporting controls for scenarios such as an Operating System migration, break/fix, or hardware refresh.
- End users are required to change their established working behaviors. For example, they must now change the location where they save and open their files.

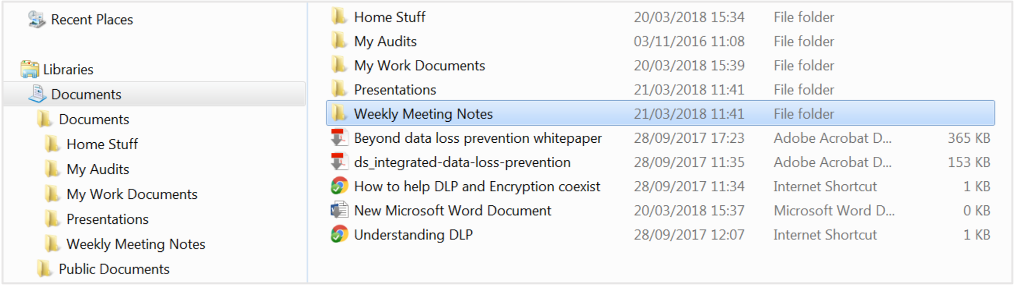
Using cloud storage should not impact a great user experience or remove existing enterprise control

Remove One Drive roadblocks for IT and End Users

The availability of all those Terabytes of new storage poses a challenge for IT because it now has an area of storage that it cannot control and manage. How does IT audit and control the type of data stored in OneDrive? How does IT determine which files are stored on-premises and which can be synced to the cloud?

But I have always saved my files there…

OneDrive requires that a user must now save their files into a different location than they’re accustomed to. Not only can this result in increased Service Desk calls but also in costly and time-consuming retraining of users. For example, a user may have structured their “My Documents” folder similarly to this:

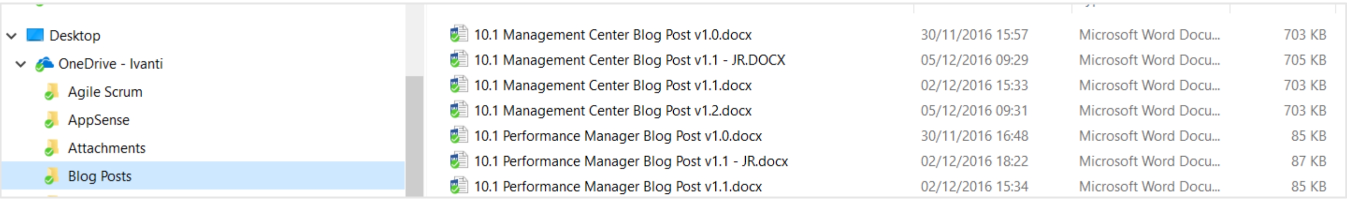


Recent Places

Libraries
- Documents
  - Documents
    - Home Stuff
    - My Audits
    - My Work Documents
    - Presentations
    - Weekly Meeting Notes
  - Public Documents

Home Stuff	20/03/2018 15:34	File folder	
My Audits	03/11/2016 11:08	File folder	
My Work Documents	20/03/2018 15:39	File folder	
Presentations	21/03/2018 11:41	File folder	
Weekly Meeting Notes	21/03/2018 11:41	File folder	
Beyond data loss prevention whitepaper	28/09/2017 17:23	Adobe Acrobat D...	365 KB
ds_integrated-data-loss-prevention	28/09/2017 11:35	Adobe Acrobat D...	153 KB
How to help DLP and Encryption coexist	28/09/2017 11:34	Internet Shortcut	1 KB
New Microsoft Word Document	20/03/2018 15:37	Microsoft Word D...	0 KB
Understanding DLP	28/09/2017 12:07	Internet Shortcut	1 KB

However, for IT to make use of the OneDrive storage for that user, it’s the user that must change the location where they save their files:

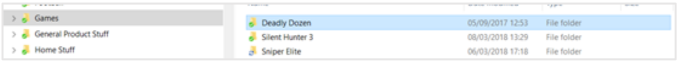


Desktop
OneDrive - Ivanti
Agile Scrum
AppSense
Attachments
Blog Posts

10.1 Management Center Blog Post v1.0.docx	30/11/2016 15:57	Microsoft Word Docu...	703 KB
10.1 Management Center Blog Post v1.1 - JR.DOCX	05/12/2016 09:29	Microsoft Word Docu...	705 KB
10.1 Management Center Blog Post v1.1.docx	02/12/2016 15:33	Microsoft Word Docu...	703 KB
10.1 Management Center Blog Post v1.2.docx	05/12/2016 09:31	Microsoft Word Docu...	703 KB
10.1 Performance Manager Blog Post v1.0.docx	30/11/2016 16:48	Microsoft Word Docu...	85 KB
10.1 Performance Manager Blog Post v1.1 - JR.docx	02/12/2016 18:22	Microsoft Word Docu...	87 KB
10.1 Performance Manager Blog Post v1.1.docx	02/12/2016 15:34	Microsoft Word Docu...	85 KB

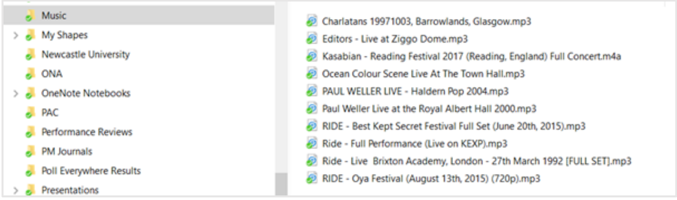
How do we control what is being uploaded?

Once users have adapted to the new way of working, they are then free to upload—almost without exception—files of any type, size, or age into their OneDrive storage. IT has no way of controlling or auditing this.



Games
General Product Stuff
Home Stuff

Deadly Dozen	05/09/2017 12:53	File folder
Silent Hunter 3	08/03/2018 13:29	File folder
Sniper Elite	06/03/2018 17:18	File folder



Music
My Shapes
Newcastle University
ONA
OneNote Notebooks
PAC
Performance Reviews
PM Journals
Poll Everywhere Results
Presentations

Charlatans 19971003, Barrowlands, Glasgow.mp3
Editors - Live at Ziggo Dome.mp3
Kasabian - Reading Festival 2017 (Reading, England) Full Concert.m4a
Ocean Colour Scene Live At The Town Hall.mp3
PAUL WELLER LIVE - Haldern Pop 2004.mp3
Paul Weller Live at the Royal Albert Hall 2000.mp3
RIDE - Best Kept Secret Festival Full Set (June 20th, 2015).mp3
Ride - Full Performance (Live on KEXP).mp3
Ride - Live Brixton Academy, London - 27th March 1992 [FULL SET].mp3
RIDE - Oya Festival (August 13th, 2015) (720p).mp3

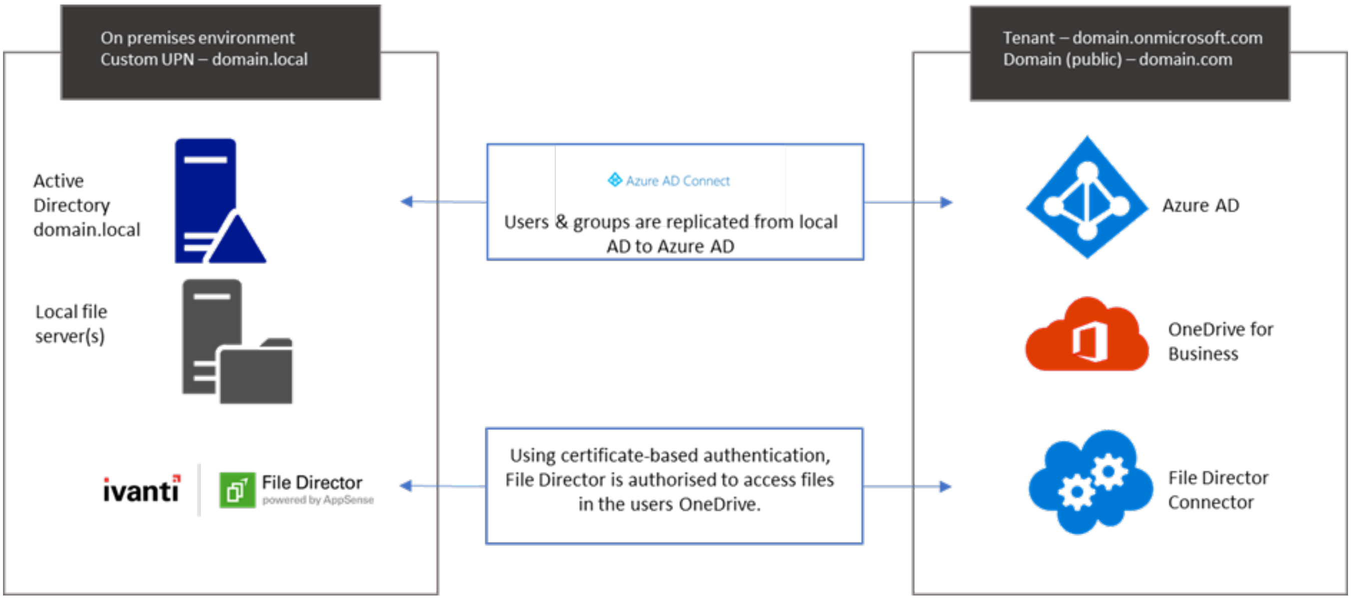
File Director’s OneDrive Connector allows IT to capture, control, and audit users’ usage of the Office 365 1TB of free OneDrive storage. Couple this with the granular sync engine and In-Location Sync feature and a user’s files can be mapped to OneDrive, all without impacting the user and their everyday working experience.

Setting Up the File Director OneDrive Connector

The OneDrive connector is easily configured via the Azure AD portal and the File Director web admin console. The following steps provide a walk-through to enable you to configure and start using the connector.

This video from the Ivanti YouTube channel also shows the steps required to set up the OneDrive connector.

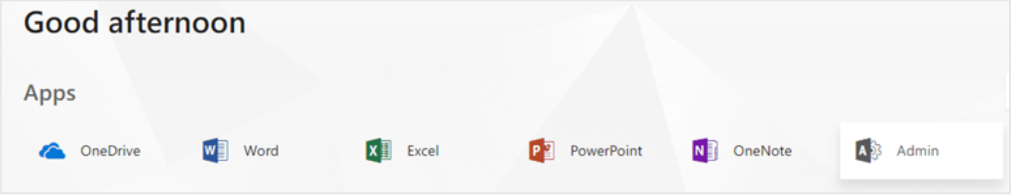
Overview


On premises environment
Custom UPN – domain.local
Active Directory domain.local
Local file server(s)
ivanti
File Director
powered by AppSense
Azure AD Connect
Users & groups are replicated from local AD to Azure AD
Using certificate-based authentication, File Director is authorised to access files in the users OneDrive.
Tenant – domain.onmicrosoft.com
Domain (public) – domain.com
Azure AD
OneDrive for Business
File Director Connector

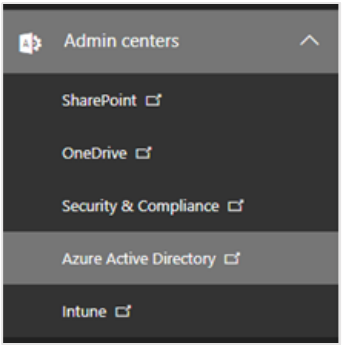
Note: *Ensure that all of the required pre-requisites are in place before continuing.*

Azure portal configuration

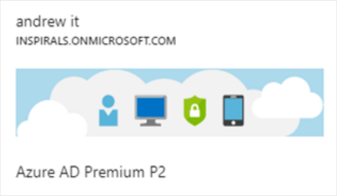
1. Log into Office 365 as an Administrator and open the Admin Center.



2. From the Admin Center menu on the left, open Azure Active Directory (AD).

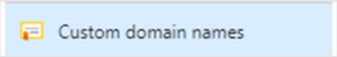


3. Select the tile for your Azure AD.

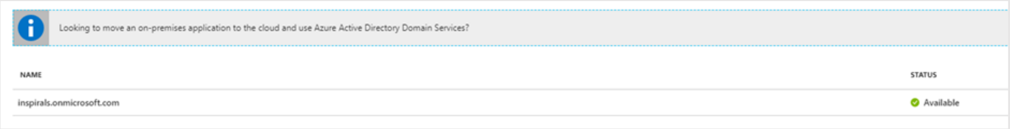


Note: *Where this tile is displayed can vary depending upon any customization you may have made to your Azure AD dashboard.*

4. We will need the domain name for your Azure AD. This is obtained by opening the Custom Domain Names option within the Manage menu.



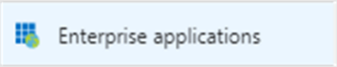
Copy the name of the domain to a text editor; we will need this when we come to configure the connector within the File Director Admin console.



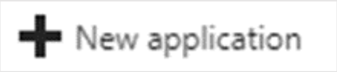
Looking to move an on-premises application to the cloud and use Azure Active Directory Domain Services?

NAME	STATUS
inspirals.onmicrosoft.com	✓ Available

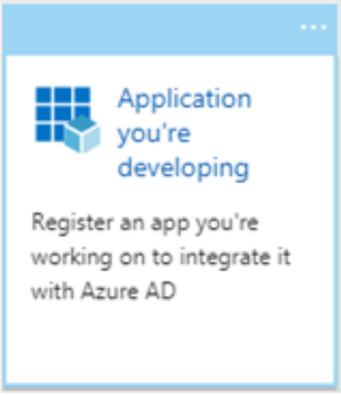
5. Now that we have the domain details from Azure, we need to add File Director as an application within Azure AD. To do this, select Enterprise Applications. This can be found again within the Manage menu.



Next, we will add a new application.



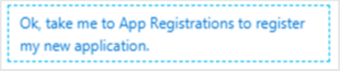
And then we need to add an Application you’re developing.



Application you're developing

Register an app you're working on to integrate it with Azure AD

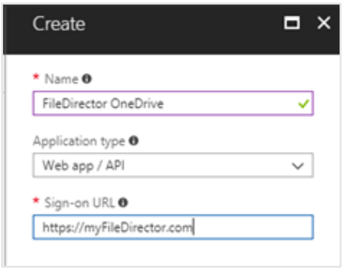
We now need to register the application.



Ok, take me to App Registrations to register my new application.

Then, from within the App registrations blade

we can then add the details of our application within the Create blade.



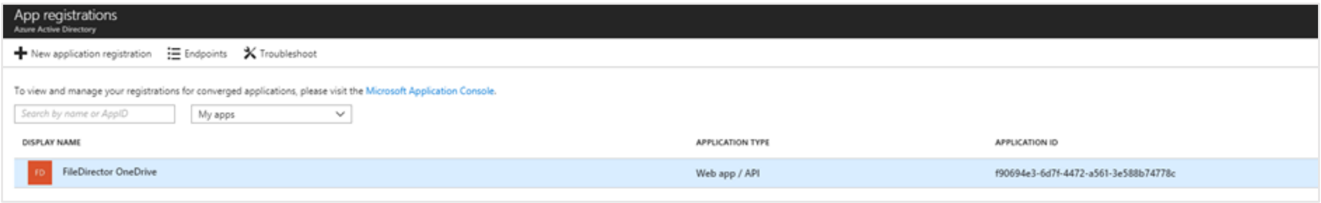
Create

* Name: FileDirector OneDrive

Application type: Web app / API

* Sign-on URL: https://myFileDirector.com

Once you have added the details, click Create and File Director will now be added to the list of registered Azure applications.

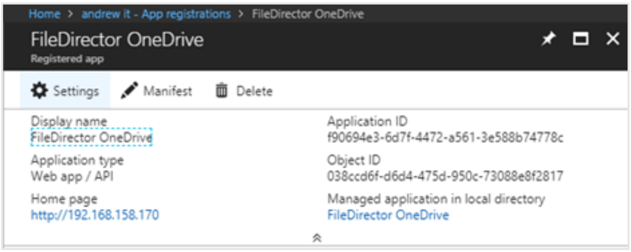


App registrations
Azure Active Directory

To view and manage your registrations for converged applications, please visit the Microsoft Application Console.

DISPLAY NAME	APPLICATION TYPE	APPLICATION ID
FD FileDirector OneDrive	Web app / API	f90694e3-6d7f-4472-a561-3e588b74778c

6. We now need to configure the permissions for the appliance. This will determine what the File Director application can do and what it can access. Select Settings from the App Registration blade for your application.



Home > andrew it - App registrations > FileDirector OneDrive

FileDirector OneDrive

Registered app

Display name
FileDirector OneDrive

Application type
Web app / API

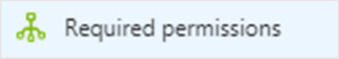
Home page
http://192.168.158.170

Application ID
f90694e3-6d7f-4472-a561-3e588b74778c

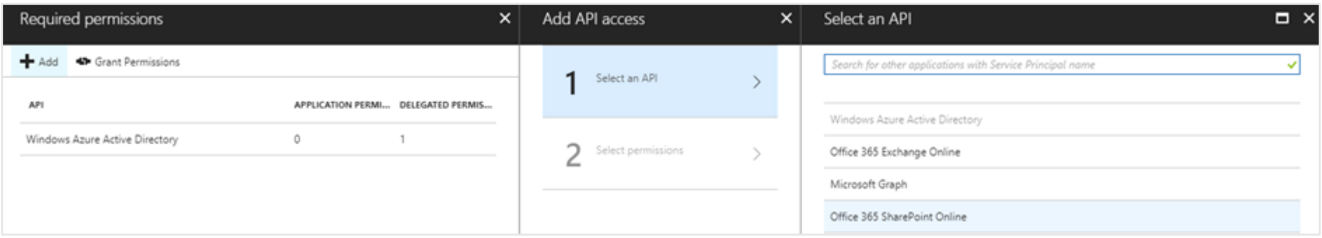
Object ID
038ccd6f-d6d4-475d-950c-73088e8f2817

Managed application in local directory
FileDirector OneDrive

Then, from within the API Access menu, we are going to add the required permissions.



We now need to add permissions for the Office 365 SharePoint Online API.



Required permissions

API	APPLICATION PERMI...	DELEGATED PERMIS...
Windows Azure Active Directory	0	1

Add API access

1 Select an API

2 Select permissions

Select an API

Search for other applications with Service Principal name

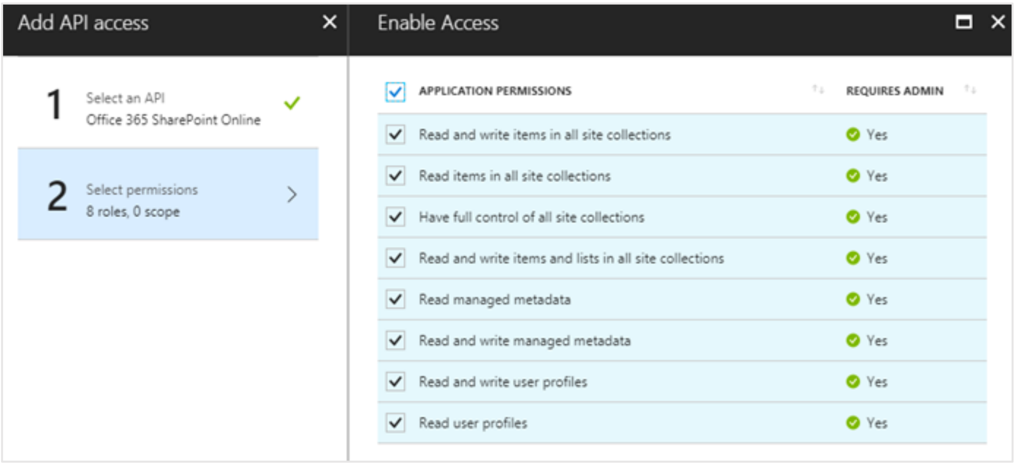
Windows Azure Active Directory

Office 365 Exchange Online

Microsoft Graph

Office 365 SharePoint Online

We need to add the Application Permissions. This can be done by selecting each item individually or by multi selecting via the tick box to the left of Application Permissions.



Add API access

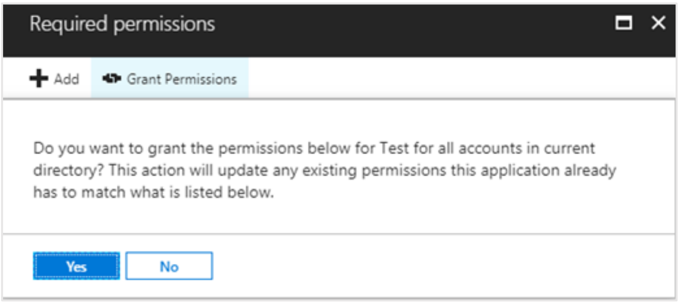
1 Select an API
Office 365 SharePoint Online ✓

2 Select permissions
8 roles, 0 scope

Enable Access

☑ APPLICATION PERMISSIONS	REQUIRES ADMIN
☑ Read and write items in all site collections	✓ Yes
☑ Read items in all site collections	✓ Yes
☑ Have full control of all site collections	✓ Yes
☑ Read and write items and lists in all site collections	✓ Yes
☑ Read managed metadata	✓ Yes
☑ Read and write managed metadata	✓ Yes
☑ Read and write user profiles	✓ Yes
☑ Read user profiles	✓ Yes

Once you have added the permissions, click Select and then click Done. The last step is to grant the permissions that have just been enabled.



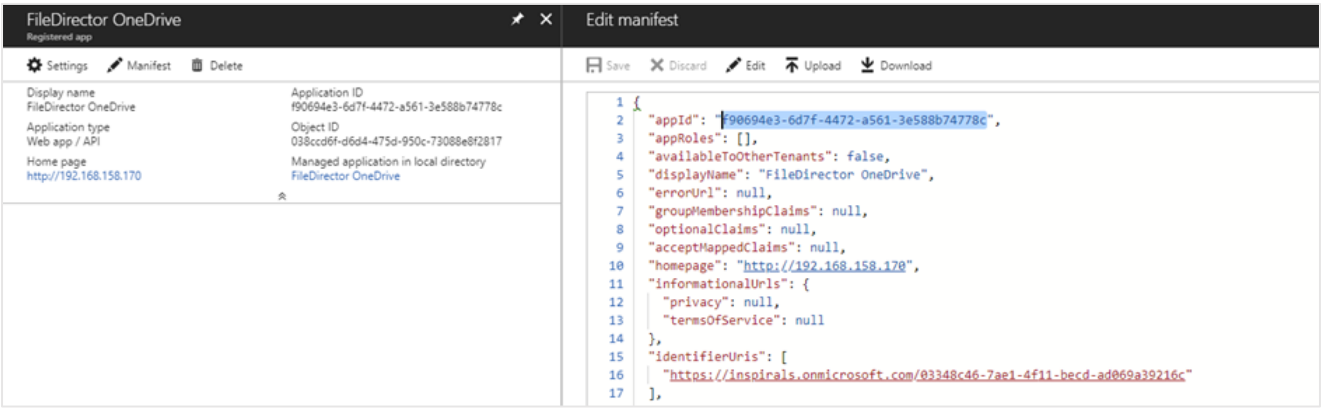
Do you want to grant the permissions below for Test for all accounts in current directory? This action will update any existing permissions this application already has to match what is listed below.

The Azure AD manifest

Now that we have configured Azure to allow File Director access, we must now update the Azure AD manifest. This uses public key infrastructure to generate a self-signed certificate in the server and upload the public key to Azure as part of the application manifest.

To complete this step, you will require access to the File Director Admin console.

1. Open your Azure AD application and select Manifest from the App Registration blade.



Display name
FileDirector OneDrive

Application type
Web app / API

Home page
http://192.168.158.170

Application ID
f90694e3-6d7f-4472-a561-3e588b74778c

Object ID
038ccd6f-d6d4-475d-950c-73088e8f2817

Managed application in local directory
FileDirector OneDrive

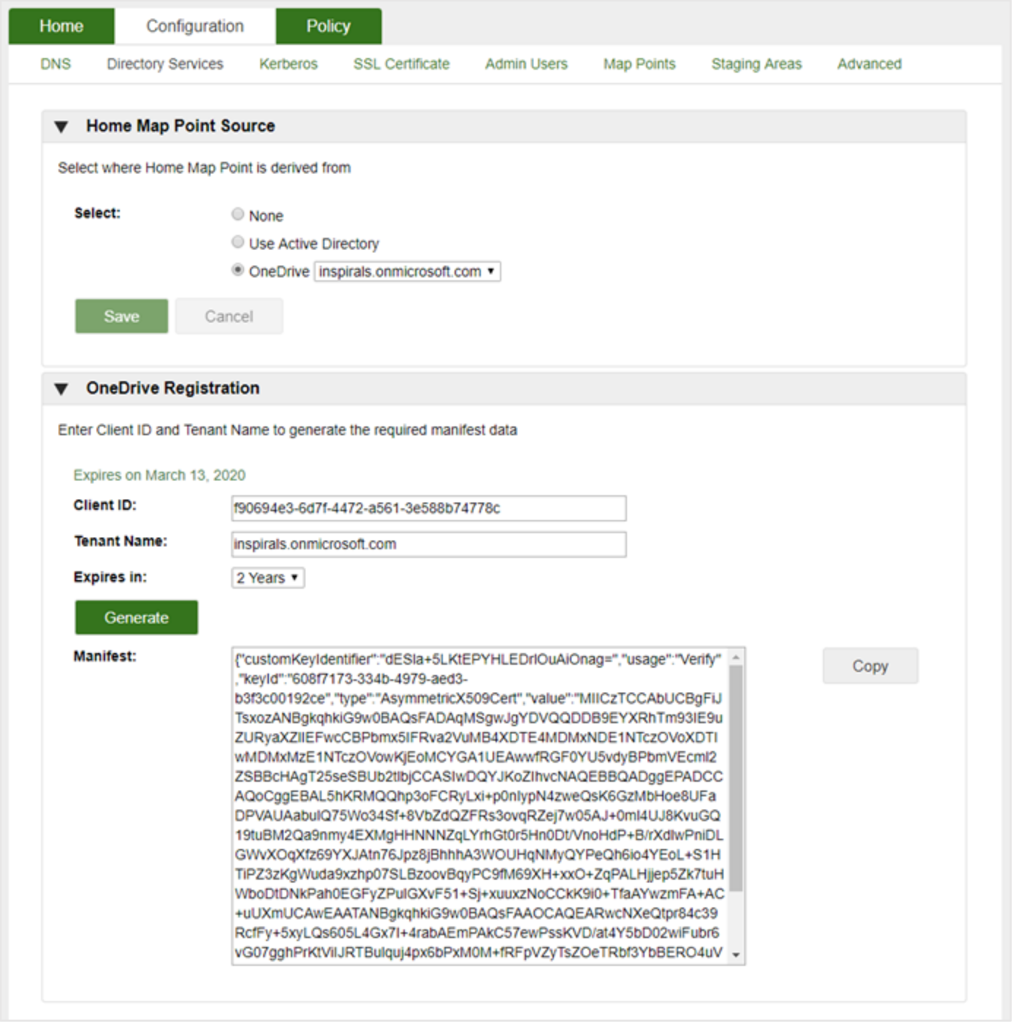
```
{
  "appId": "f90694e3-6d7f-4472-a561-3e588b74778c",
  "appRoles": [],
  "availableToOtherTenants": false,
  "displayName": "FileDirector OneDrive",
  "errorUrl": null,
  "groupMembershipClaims": null,
  "optionalClaims": null,
  "acceptMappedClaims": null,
  "homepage": "http://192.168.158.170",
  "informationalUrls": {
    "privacy": null,
    "termsOfService": null
  },
  "identifierUris": [
    "https://inspirals.onmicrosoft.com/03348c46-7ae1-4f11-becd-ad069a39216c"
  ],
```

Copy the value of the appId class to a text editor. We are going to need this when we come to generate data for the manifest within the File Director Admin console.

2. We now need to generate the key credentials that will be used to allow the File Director appliance to access our Azure AD application. Log in to the File Director Admin console and browse to Configuration > Directory Services. Complete the OneDrive registration.

Attribute	Value
Client ID	Use the appId you copied in the step above.
Tenant Name	This is the domain name you copied from your Azure AD.
Expires in	Select 1 or 2 years.

Once you have completed all the required details, click Generate. This will generate content that we will add to the manifest of our Azure AD application.



▼ Home Map Point Source

Select where Home Map Point is derived from

Select: ○ None ○ Use Active Directory ● OneDrive inspirals.onmicrosoft.com ▾

▼ OneDrive Registration

Enter Client ID and Tenant Name to generate the required manifest data

Expires on March 13, 2020

Client ID: f90694e3-6d7f-4472-a561-3e588b74778c

Tenant Name: inspirals.onmicrosoft.com

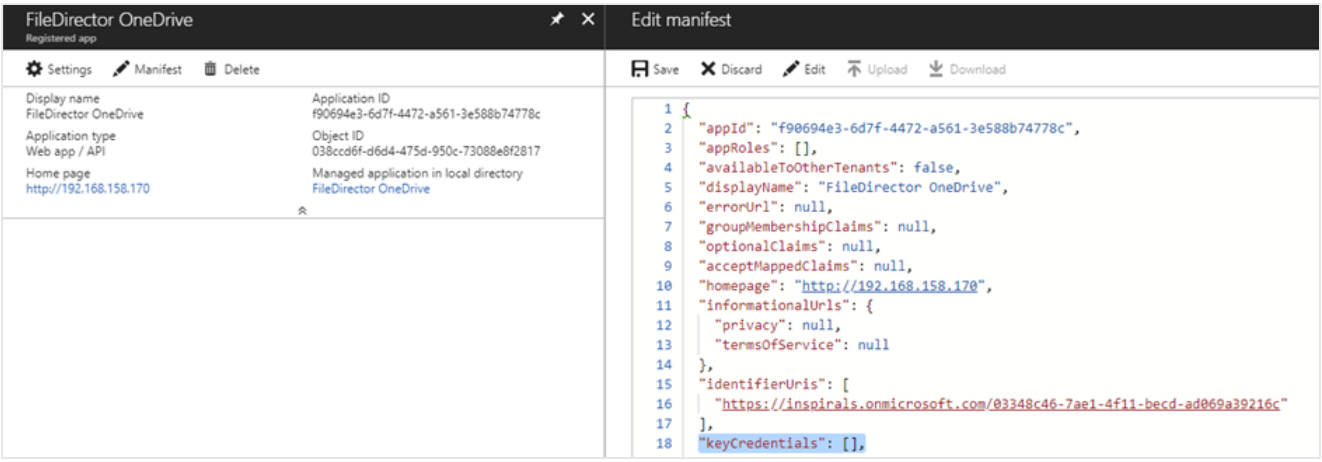
Expires in: 2 Years ▾

Manifest:

```
{"customKeyIdentifier":"dESIa+5LKtEPYHLEDrlOuAiOnag=","usage":"Verify"
,"keyId":"608f7173-334b-4979-aed3-
b3f3c00192ce","type":"AsymmetricX509Cert","value":"MIICzTCCAbUCBgFiJ
TsxozANBgkqhkiG9w0BAQsFADAqMSgwJgYDVQQDDB9EYXRhTm93IE9u
ZURyaXZlIEFwcCBPbmx5IFRva2VuMB4XDTE4MDMxNDE1NTczOVoXDTI
wMDMxMzE1NTczOVowKjEoMCYGA1UEAwwfRGF0YU5vdyBPbmVEcml2
ZSBBcHAgT25seSBUb2tlbjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAL5hKRMQQhp3oFCRyLxi+p0nIypN4zweQsK6GzMbHoe8UFa
DPVAUAabulQ75Wo34Sf+8VbZdQZFRs3ovqRZej7w05AJ+0ml4UJ8KvuGQ
19tuBM2Qa9nmy4EXMgHHNNNZqLYrhGt0r5Hn0Dt/VnoHdP+B/rXdlwPniDL
GWvXOqXfz69YXJAtn76Jpz8jBhhhA3WOUHqNMyQYPeQh6io4YEoL+S1H
TiPZ3zKgWuda9xzhp07SLBzoovBqyPC9fM69XH+xxO+ZqPALHjjep5Zk7tuH
WboDtDNkPah0EGFyZPulGXvF51+Sj+xuuxzNoCCkK9i0+TfaAYwzmFA+AC
+uUXmUCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEARwcNXeQtpr84c39
RcfFy+5xyLQs605L4Gx7I+4rabAEmPAkC57ewPssKVD/at4Y5bD02wiFubr6
vG07gghPrKtVilJRTBulquj4px6bPxM0M+fRFpVZyTsZOeTRbf3YbBERO4uV
```

Use the Copy button to copy the contents of the manifest to the clipboard. If you are not planning on updating the Azure AD application manifest immediately, save this to a text editor.

3. Return to Azure AD and locate the keyCredentials class in the manifest for your application.



Display name
FileDirector OneDrive

Application type
Web app / API

Home page
http://192.168.158.170

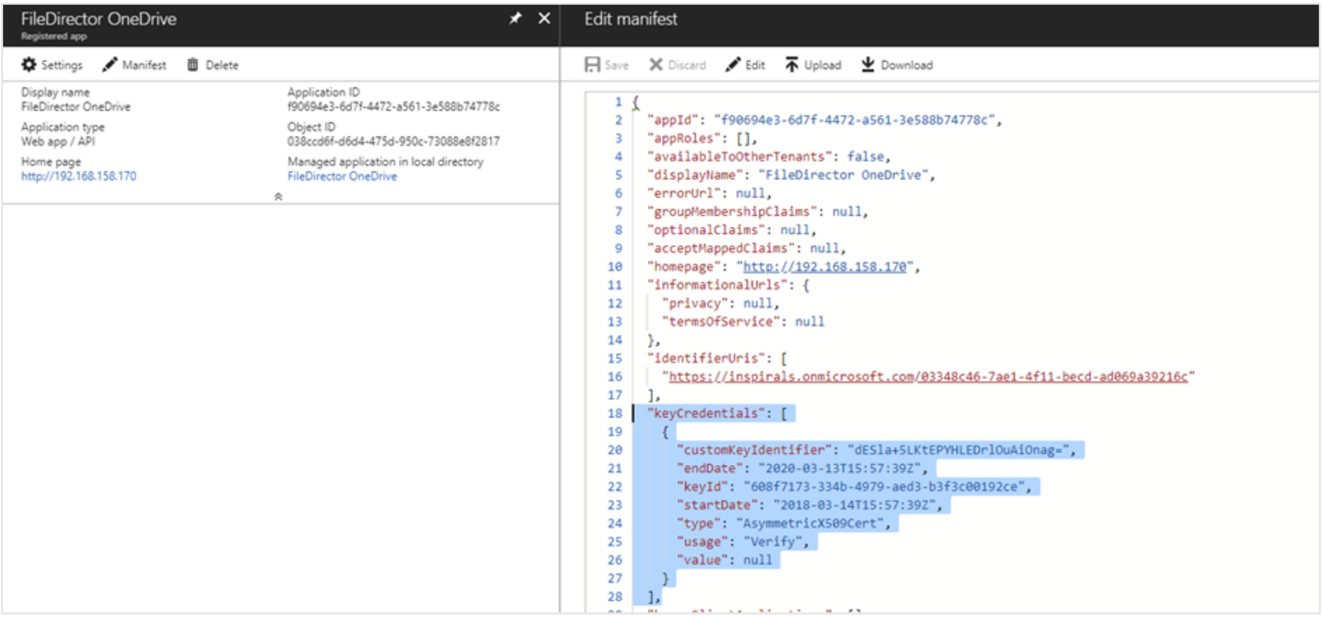
Application ID
f90694e3-6d7f-4472-a561-3e588b74778c

Object ID
038ccd6f-d6d4-475d-950c-73088e8f2817

Managed application in local directory
FileDirector OneDrive

```
{
  "appId": "f90694e3-6d7f-4472-a561-3e588b74778c",
  "appRoles": [],
  "availableToOtherTenants": false,
  "displayName": "FileDirector OneDrive",
  "errorUrl": null,
  "groupMembershipClaims": null,
  "optionalClaims": null,
  "acceptMappedClaims": null,
  "homepage": "http://192.168.158.170",
  "informationalUrls": {
    "privacy": null,
    "termsOfService": null
  },
  "identifierUris": [
    "https://inspirals.onmicrosoft.com/03348c46-7ae1-4f11-becd-ad069a39216c"
  ],
  "keyCredentials": [],
```

We now need to paste the manifest content that we copied from the File Director admin console between the square brackets.



Display name
FileDirector OneDrive

Application type
Web app / API

Home page
http://192.168.158.170

Application ID
f90694e3-6d7f-4472-a561-3e588b74778c

Object ID
038ccd6f-d6d4-475d-950c-73088e8f2817

Managed application in local directory
FileDirector OneDrive

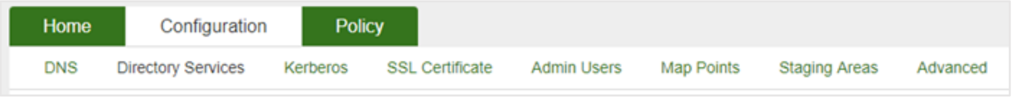
```
{
  "appId": "f90694e3-6d7f-4472-a561-3e588b74778c",
  "appRoles": [],
  "availableToOtherTenants": false,
  "displayName": "FileDirector OneDrive",
  "errorUrl": null,
  "groupMembershipClaims": null,
  "optionalClaims": null,
  "acceptMappedClaims": null,
  "homepage": "http://192.168.158.170",
  "informationalUrls": {
    "privacy": null,
    "termsOfService": null
  },
  "identifierUris": [
    "https://inspirals.onmicrosoft.com/03348c46-7ae1-4f11-becd-ad069a39216c"
  ],
  "keyCredentials": [
    {
      "customKeyIdentifier": "dESla+5LKtEPYHLEDrlOuAiOnag=",
      "endDate": "2020-03-13T15:57:39Z",
      "keyId": "608f7173-334b-4979-aed3-b3f3c00192ce",
      "startDate": "2018-03-14T15:57:39Z",
      "type": "AsymmetricX509Cert",
      "usage": "Verify",
      "value": null
    }
  ],
```

Finally, save your changes.

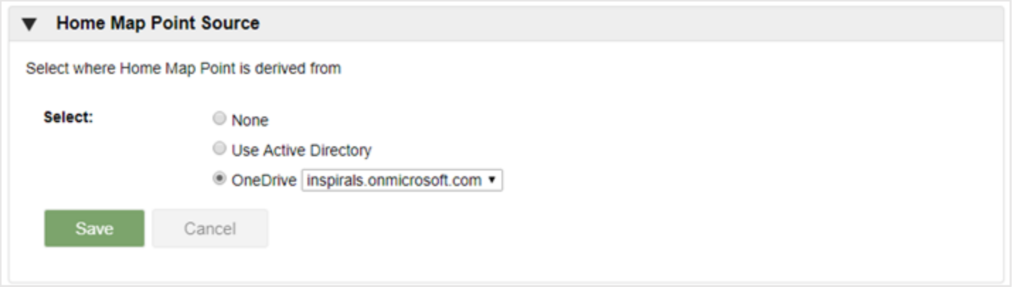
We have now completed the steps required to set up and configure our Azure AD application. Next, we need to configure File Director to use the user's OneDrive storage as their Home map point source.

File Director configuration

1. Log into the File Director admin console and browse to Configuration > Directory Services.



2. From within the Home Map Point Source section, select OneDrive. You will notice the tenant name is populated automatically with the information you entered when configuring the Azure AD application manifest.

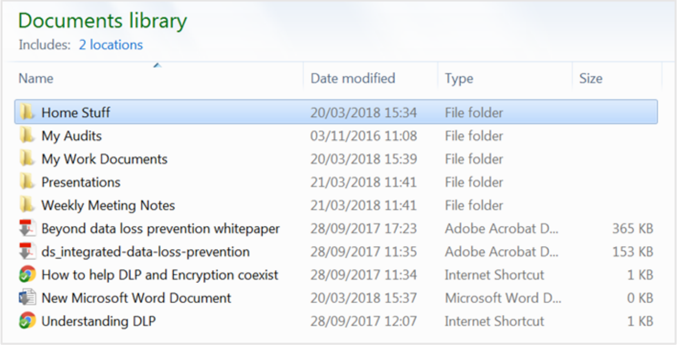


▼ Home Map Point Source

Select where Home Map Point is derived from

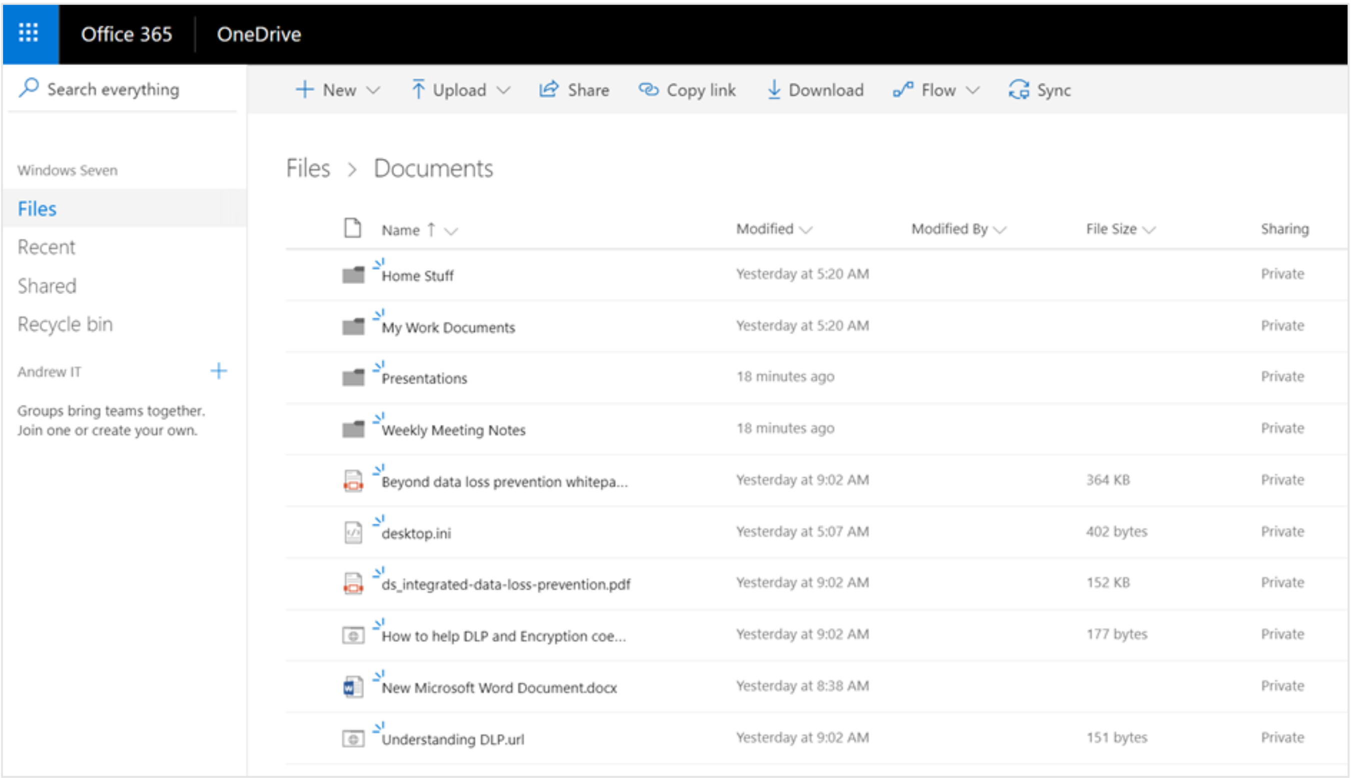
Select:
○ None
○ Use Active Directory
● OneDrive inspirals.onmicrosoft.com ▾

That's it! When users access their Home Folder, they will now be using the free 1TB of OneDrive storage without impacting their experience. Plus, they also have easy access to their files, allowing them to work on them from anywhere at any time irrespective of the Operating System or version of Windows on their endpoints.



Documents library
Includes: 2 locations

Name	Date modified	Type	Size
Home Stuff	20/03/2018 15:34	File folder	
My Audits	03/11/2016 11:08	File folder	
My Work Documents	20/03/2018 15:39	File folder	
Presentations	21/03/2018 11:41	File folder	
Weekly Meeting Notes	21/03/2018 11:41	File folder	
Beyond data loss prevention whitepaper	28/09/2017 17:23	Adobe Acrobat D...	365 KB
ds_integrated-data-loss-prevention	28/09/2017 11:35	Adobe Acrobat D...	153 KB
How to help DLP and Encryption coexist	28/09/2017 11:34	Internet Shortcut	1 KB
New Microsoft Word Document	20/03/2018 15:37	Microsoft Word D...	0 KB
Understanding DLP	28/09/2017 12:07	Internet Shortcut	1 KB



Name ↑	Modified	Modified By	File Size	Sharing
Home Stuff	Yesterday at 5:20 AM			Private
My Work Documents	Yesterday at 5:20 AM			Private
Presentations	18 minutes ago			Private
Weekly Meeting Notes	18 minutes ago			Private
Beyond data loss prevention whitepa...	Yesterday at 9:02 AM		364 KB	Private
desktop.ini	Yesterday at 5:07 AM		402 bytes	Private
ds_integrated-data-loss-prevention.pdf	Yesterday at 9:02 AM		152 KB	Private
How to help DLP and Encryption coe...	Yesterday at 9:02 AM		177 bytes	Private
New Microsoft Word Document.docx	Yesterday at 8:38 AM			Private
Understanding DLP.url	Yesterday at 9:02 AM		151 bytes	Private

This is great from the user's perspective since they can continue working in a familiar way with their Desktop/Document folders. Inevitably, there will be some content that the administrator will not want to sync back to the server—a user's music or film library for example. In addition, some other file types, like in-use database files, just don't support being replicated by any file-level sync product.

Optimizing the File Director Configuration

So now that we have the File Director OneDrive connector configured and providing users with seamless access to cloud-based storage, how do we ensure that IT retains control over what is being stored? Because the OneDrive storage is provided to users, IT admins lack the controls they need to view and manage OneDrive storage and its content.

Exclusions

Exclusions allow an administrator to define a policy as to what files are synchronized. File Director's advanced bi-directional, client-side conditional exclusions are based on regular expressions, with criteria that can be evaluated by type, age, size, and path. We can build exclusion expressions based upon combinations of the following:

- File and folder paths
- File extension(s)
- File age
- File size

In addition to these conditions, File Director excludes certain temporary files from syncing. These are:

- Files with an extension of tmp, lnk, partial, crdownload, part, and download
- Microsoft Office backup files starting with ~$
- Microsoft Excel temporary files
- Open Office temporary files
- The Windows Recycle bin

So, what does this mean in practice? How, as an IT administrator, can you apply exclusions to prevent items such as a user's iTunes library being synchronized, while ensuring that important files such as Word and Excel documents are synchronized? To demonstrate this, we will use an Ivanti Environment Manager configuration to define the exclusions that will then be applied to an endpoint's registry.

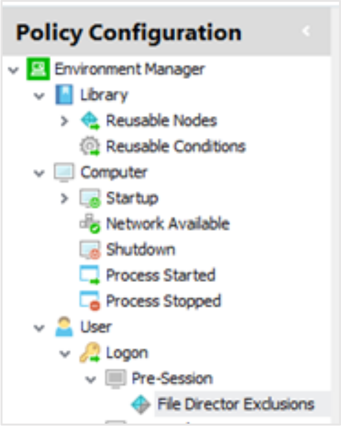
The configuration we will apply will set the following exclusions:

- Only synchronize files that are younger than one year
- Are under 500MB
- Are not .mp3, .mp4, or .avi files

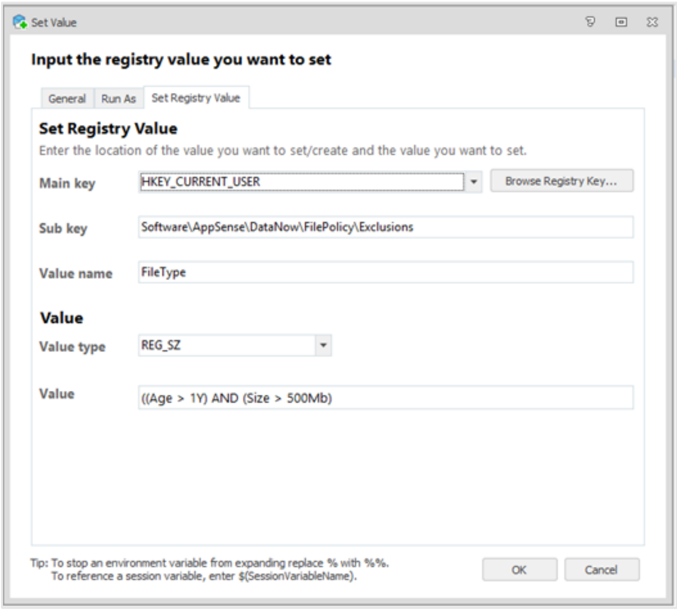
First, let's deal with the age and size of the files.

Note: *It is assumed that you have experience using Environment Manager to create and manage configuration*

We need to modify the relevant policy node. In this example we have a ‘File Director Exclusions’ node as part of the User > Logon > Pre-session trigger, under which we have a node of ‘File Director Exclusions’. We need to create our exclusions entry here.



Under here we need to create a set registry value action to set our exclusions.



Input the registry value you want to set

Set Registry Value

Enter the location of the value you want to set/create and the value you want to set.

Main key: HKEY_CURRENT_USER

Sub key: Software\AppSense\DataNow\FilePolicy\Exclusions

Value name: FileType

Value

Value type: REG_SZ

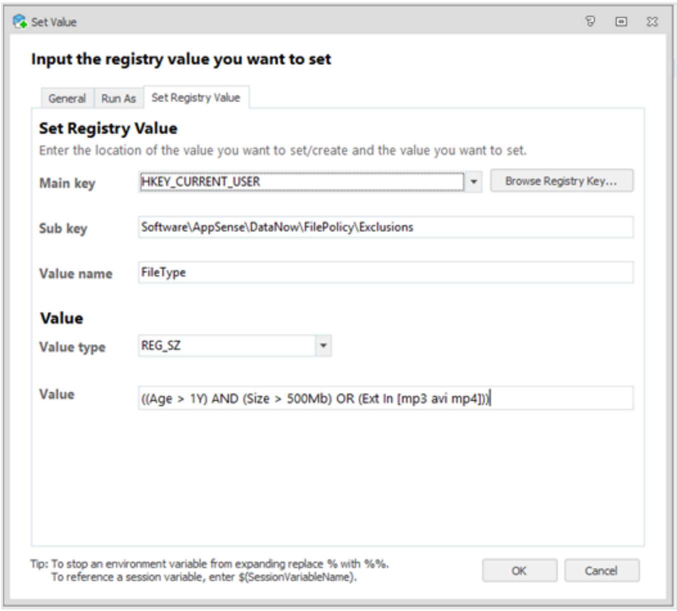
Value: ((Age > 1Y) AND (Size > 500Mb)

Tip: To stop an environment variable from expanding replace % with %%.
To reference a session variable, enter $(SessionVariableName).

This will place a bidirectional synchronization exclusion on files that match both aspects of the criteria. For example, a file that is over one year in age and is 600MB in size will be excluded, whereas a file that is over one year in age and is 450MB in size will be included. We could of course have used an OR statement if we wanted to block either criteria.

((Age > 1Y) OR (Size > 500MB))

So, this is great. We are now preventing files based upon their age and size being synchronized. But what if a user has an .avi file that is less than a year old and 750MB in size? In this example, it will also be synchronized. To prevent this, we need to add an exclusion that prevents .mp3, .mp4, and .avi file types from being synchronized.



Input the registry value you want to set

Set Registry Value

Enter the location of the value you want to set/create and the value you want to set.

Main key: HKEY_CURRENT_USER

Sub key: Software\AppSense\DataNow\FilePolicy\Exclusions

Value name: FileType

Value

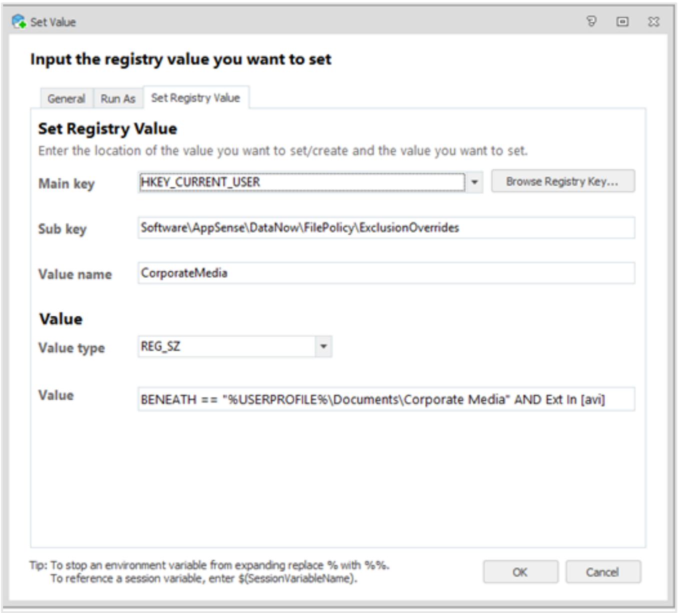
Value type: REG_SZ

Value: ((Age > 1Y) AND (Size > 500Mb) OR (Ext In [mp3 avi mp4]))

Tip: To stop an environment variable from expanding replace % with %%.
To reference a session variable, enter $(SessionVariableName).

We now have in place exclusions that will prevent files from being synchronized based upon their age, size, and type. Great. But what if a user has .avi files that they require for their job role—a presentation or marketing video, for example? In this scenario, we can make use of File Director's Exclusion override capability to include .avi files that are saved in a known location to be synchronized.

Again, we are going to deploy a registry key to an endpoint via our Environment Manager configuration. This time we will use a separate node named 'File Director Overrides' and add a set registry value action.



Input the registry value you want to set

Set Registry Value

Enter the location of the value you want to set/create and the value you want to set.

Main key: HKEY_CURRENT_USER

Sub key: Software\AppSense\DataNow\FilePolicy\ExclusionOverrides

Value name: CorporateMedia

Value

Value type: REG_SZ

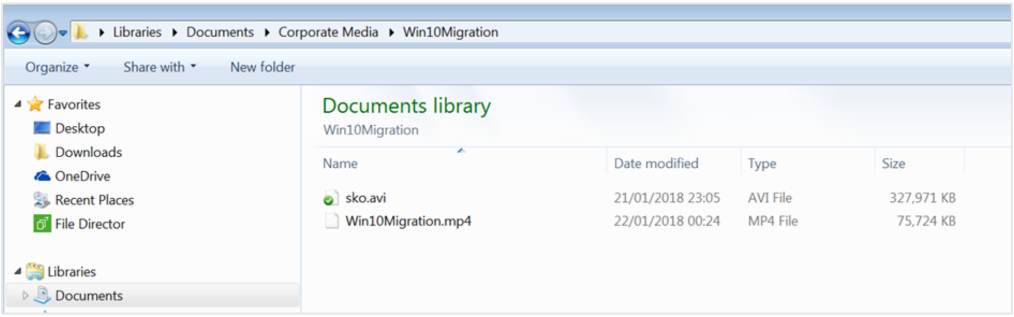
Value: BENEATH == "%USERPROFILE%\Documents\Corporate Media" AND Ext In [avi]

Tip: To stop an environment variable from expanding replace % with %%.
To reference a session variable, enter $(SessionVariableName).

We now have the following rules in place that:

- Are preventing files older than a year and are greater than 500MB in size from being synchronized to OneDrive.
- Prevent all .mp3, .mp4, and .avi file types from being synchronized unless they are in the ‘Corporate Media’ folder.

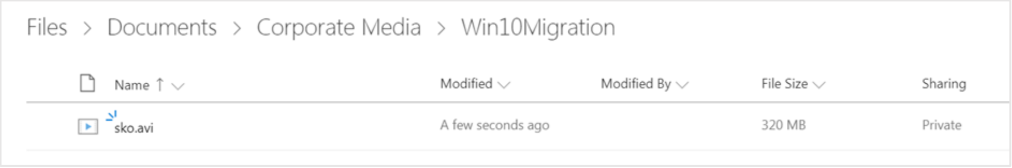
If we look on the endpoint we can now see that there is an .avi file and a .mp4 file stored in the user’s ‘Corporate Media’ folder. However, only the ‘sko.avi’ file has been synchronized with OneDrive (indicated by the green tick overlay).



Documents library
Win10Migration

Name	Date modified	Type	Size
sko.avi	21/01/2018 23:05	AVI File	327,971 KB
Win10Migration.mp4	22/01/2018 00:24	MP4 File	75,724 KB

And if we look via the OneDrive portal:



Name ↑	Modified	Modified By	File Size	Sharing
sko.avi	A few seconds ago		320 MB	Private

Electives

We are now controlling what files are being synchronized from the endpoint to OneDrive storage, so let’s change our focus to the onboarding of a new user; a Windows 10 and hardware refresh situation, for example.

Let’s set the scene.

Our company—let’s name it Acme Tech—is embarking on a Windows 10 operating system rollout, and at the same time, is providing new laptops to its users. The company wants to approach this in the following way:

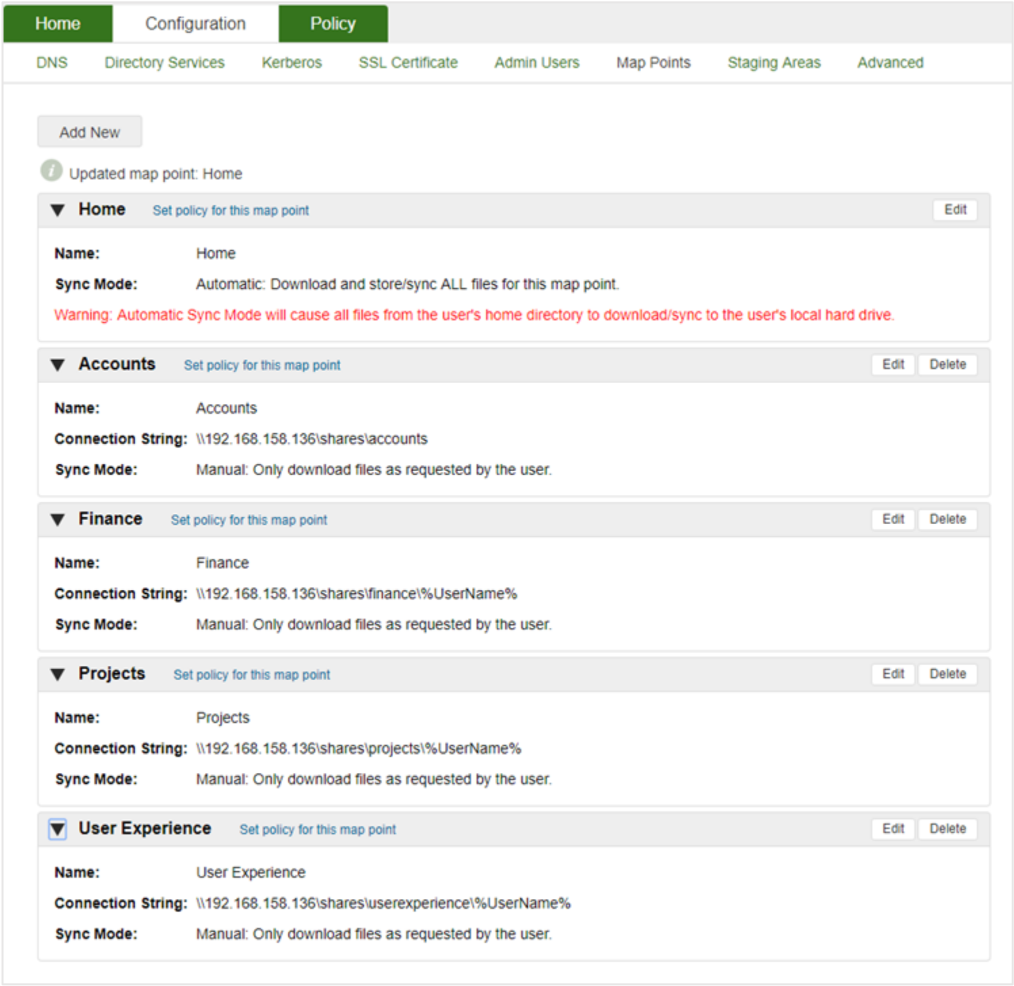
- Synchronize all relevant user files (it doesn’t want .mp3 files, etc.) to OneDrive for Business, without its end users being aware.
- Receive the user’s current laptop back from them and replace it with a new machine running Windows 10.
- Have its end users not be impacted by the migration and have all their files and folders be in the same place on their new laptop as they were on their previous device.

It is also vital that, during the onboarding process, the network is not impeded by the increase in bandwidth consumption.

File Director has two synchronization policies—‘automatic’ and ‘manual’—which administrators can apply to map points. These are defined as:

- **Automatic** – All content not matching an exclusion filter is synced between the map point and the local File Director cache on the endpoint.
- **Manual** – All locally created content syncs to the server and is ‘in-sync’ from that point forward. Server-side content is represented locally by a ‘ghost’ file that doesn’t consume any local disk space but allows the user to see and interact with the file in the same location. This is only downloaded to the user cache on the first access by the user or the application, i.e. when the user double-clicks to open the file.

Acme Tech has its map points configured in the following way, meaning that the end user’s Home map point will start to synchronize files from OneDrive to the endpoint automatically.



Updated map point: Home

Home

Name: Home
Sync Mode: Automatic: Download and store/sync ALL files for this map point.
Warning: Automatic Sync Mode will cause all files from the user's home directory to download/sync to the user's local hard drive.

Accounts

Name: Accounts
Connection String: \\192.168.158.136\shares\accounts
Sync Mode: Manual: Only download files as requested by the user.

Finance

Name: Finance
Connection String: \\192.168.158.136\shares\finance\%UserName%
Sync Mode: Manual: Only download files as requested by the user.

Projects

Name: Projects
Connection String: \\192.168.158.136\shares\projects\%UserName%
Sync Mode: Manual: Only download files as requested by the user.

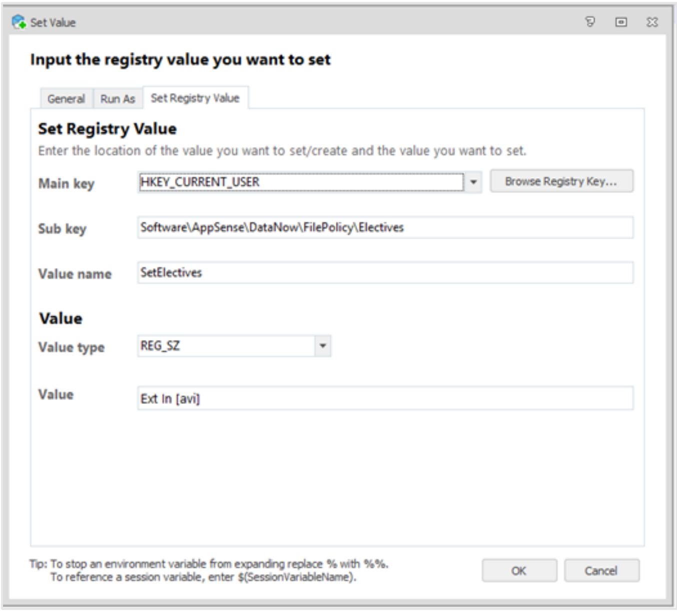
User Experience

Name: User Experience
Connection String: \\192.168.158.136\shares\userexperience\%UserName%
Sync Mode: Manual: Only download files as requested by the user.

We want to make sure we don’t impact bandwidth consumption during the onboarding of users. So, we’re going to make file types that the user isn’t expected to use frequently download-on-demand. In a similar way to how we can exclude files based upon criteria from being synchronized, we can make use of another File Director feature known as Electives to help with our migration. Electives are synonymous with “Automatic” map points. They are defined in a way similar to exclusions and it is possible to apply the same level of granularity.

For this example, we will apply an elective to not download .avi files automatically. All other files will be downloaded once the user logs in.

Within our Environment Manager configuration, we need to create a new node named “File Director Electives” beneath the Pre-Session trigger, and, as we have done earlier, add a set registry value action.



Set Value

Input the registry value you want to set

Set Registry Value

Enter the location of the value you want to set/create and the value you want to set.

Main key: HKEY_CURRENT_USER

Sub key: Software\AppSense\DataNow\FilePolicy\Electives

Value name: SetElectives

Value

Value type: REG_SZ

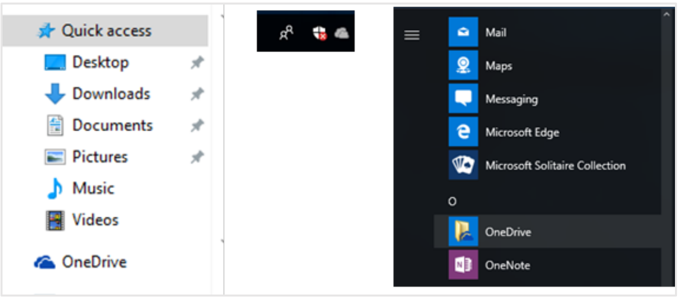
Value: Ext In [avi]

Tip: To stop an environment variable from expanding replace % with %%.
To reference a session variable, enter $(SessionVariableName).

We now have an Elective in place that will control the way that .avi files are downloaded from OneDrive storage to our endpoints.

Built-in OneDrive Shortcuts

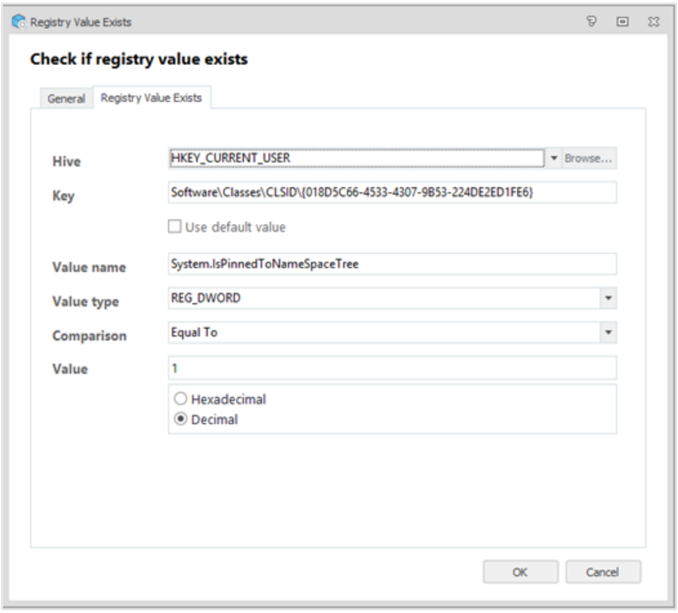
We now have File Director and Environment Manager configured to allow controlled access to OneDrive storage. However, there are still visual references to OneDrive in areas such as the Windows Start Menu and Explorer. If we leave these in place we run the risk of users trying to use OneDrive through the default shortcuts, which could in turn result in user confusion and expensive Service Desk calls.



Windows Explorer

We can address OneDrive being pinned in Explorer by using our Environment Manager configuration. First, we will check if the current user has the OneDrive icon pinned in their explorer view, and if so, modify the registry to unpin it.

To do this, open the Environment Manager configuration and under the Pre-Desktop trigger create a new node named “Remove OneDrive References.” Then beneath this we need to check for a registry value being in place.



Check if registry value exists

Hive: HKEY_CURRENT_USER

Key: Software\Classes\CLSID\{018D5C66-4533-4307-9B53-224DE2ED1FE6}

□ Use default value

Value name: System.IsPinnedToNameSpaceTree

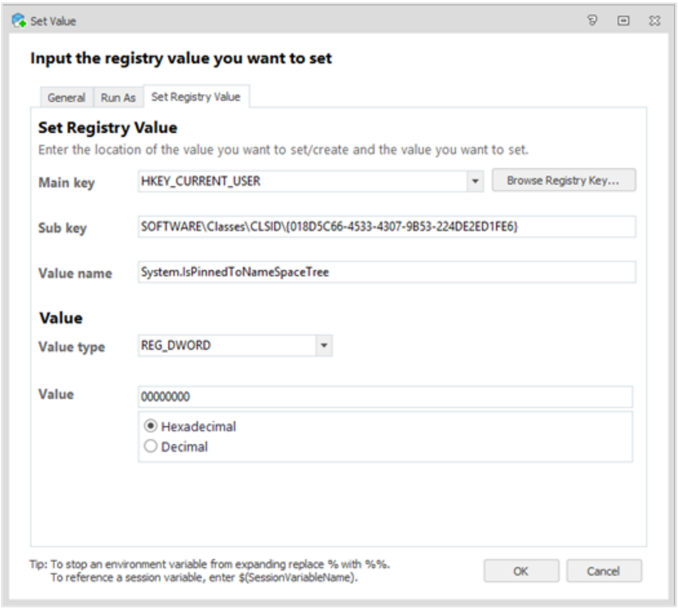
Value type: REG_DWORD

Comparison: Equal To

Value: 1

○ Hexadecimal
● Decimal

If this registry value is equal to ‘1’, we need to set it to ‘0’ using a set registry value action.



Input the registry value you want to set

Set Registry Value

Enter the location of the value you want to set/create and the value you want to set.

Main key: HKEY_CURRENT_USER

Sub key: SOFTWARE\Classes\CLSID\{018D5C66-4533-4307-9B53-224DE2ED1FE6}

Value name: System.IsPinnedToNameSpaceTree

Value

Value type: REG_DWORD

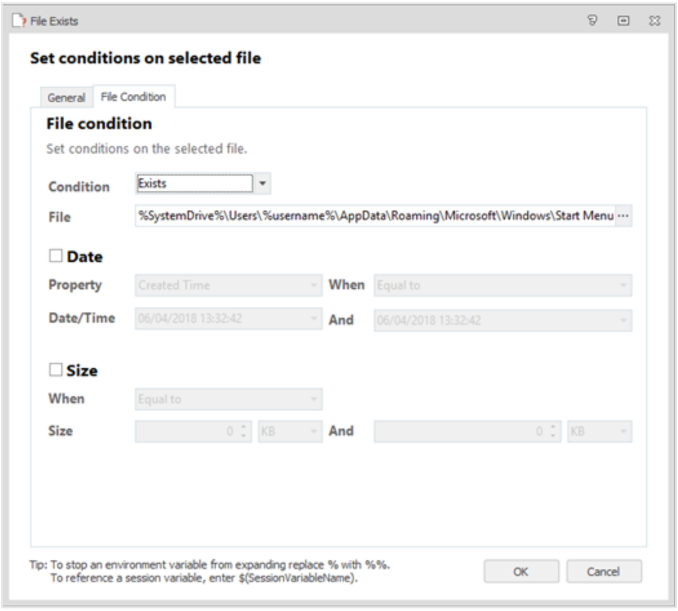
Value: 00000000

● Hexadecimal
○ Decimal

Tip: To stop an environment variable from expanding replace % with %%.
To reference a session variable, enter $(SessionVariableName).

The Start Menu

OneDrive has an item included as standard within the Windows 10 Start Menu, so we need to make sure this is removed. This time we will check if a shortcut file exists within the current user's AppData.



Set conditions on selected file

File condition

Set conditions on the selected file.

Condition: Exists

File: %SystemDrive%\Users\%username%\AppData\Roaming\Microsoft\Windows\Start Menu

□ Date

Property: Created Time   When: Equal to

Date/Time: 06/04/2018 13:32:42   And: 06/04/2018 13:32:42

□ Size

When: Equal to

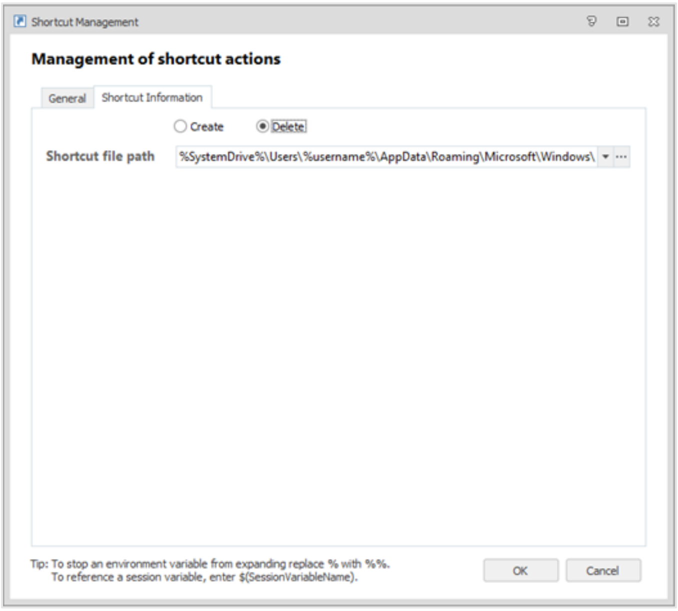
Size: 0 KB   And: 0 KB

Tip: To stop an environment variable from expanding replace % with %%.
To reference a session variable, enter $(SessionVariableName).

The full file path we are checking for is as follows:

%SystemDrive%\Users\%username%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\OneDrive.lnk

If this file is found, then we need to use a shortcut management action to delete it.



Management of shortcut actions

○ Create   ● Delete

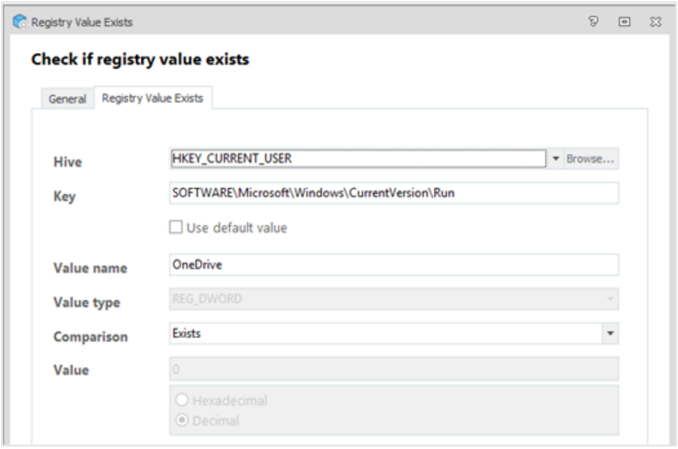
Shortcut file path: %SystemDrive%\Users\%username%\AppData\Roaming\Microsoft\Windows\

Tip: To stop an environment variable from expanding replace % with %%.
To reference a session variable, enter $(SessionVariableName).

Stop OneDrive from Starting

The final change we need to make is to the behavior of the OneDrive client when the user signs into Windows. By default, this is set to start automatically and will show a grey cloud icon in the system tray that is likely to be confusing to the end user.

Again, we are going to check for a registry key being in place.



Registry Value Exists

Check if registry value exists

Hive: HKEY_CURRENT_USER

Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Run

□ Use default value

Value name: OneDrive

Value type: REG_DWORD

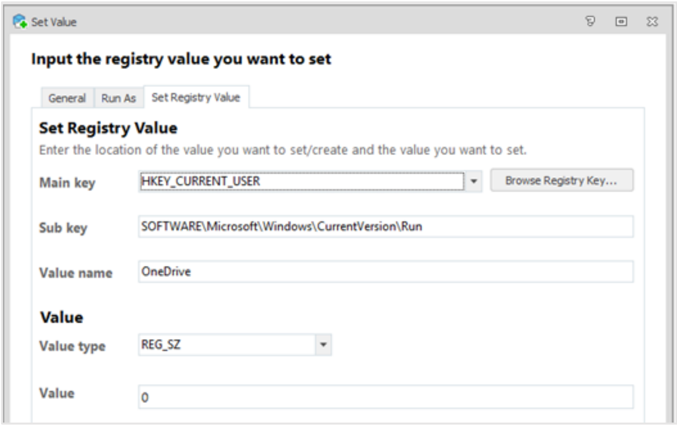
Comparison: Exists

Value: 0

○ Hexadecimal

● Decimal

If this registry key is found, we then need to stop OneDrive from starting automatically when the user logs on. We will do this by setting the value of a key.



Set Value

Input the registry value you want to set

Set Registry Value

Enter the location of the value you want to set/create and the value you want to set.

Main key: HKEY_CURRENT_USER

Sub key: SOFTWARE\Microsoft\Windows\CurrentVersion\Run

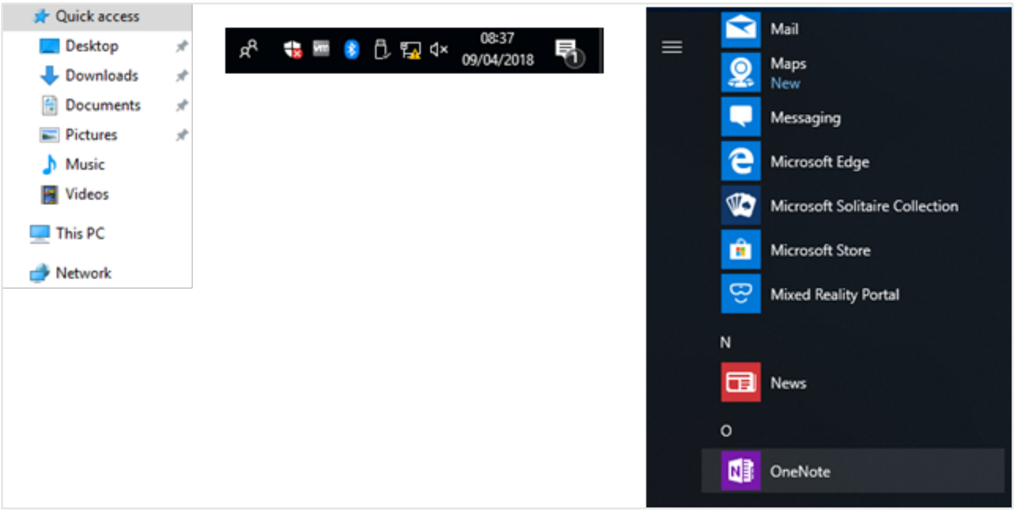
Value name: OneDrive

Value

Value type: REG_SZ

Value: 0

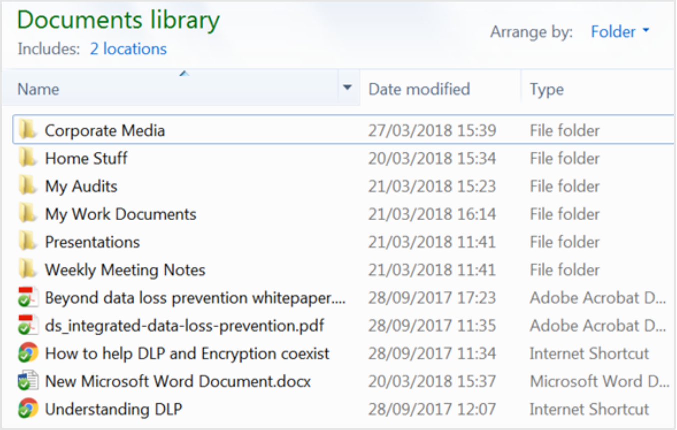
When combined, these steps remove the user-facing references to OneDrive from the operating system. This helps remove user confusion and ensures that the migration to OneDrive storage is seamless.



Bringing It All Together

So, we are now ready to migrate the user from their existing laptop to their new Windows 10 laptop.

As an example, we will use the following user who is currently working on a Windows 7 endpoint. As you can see, they have many folders containing a mix of files, some of which we want to migrate and others—.mp3's for example—that we don't.

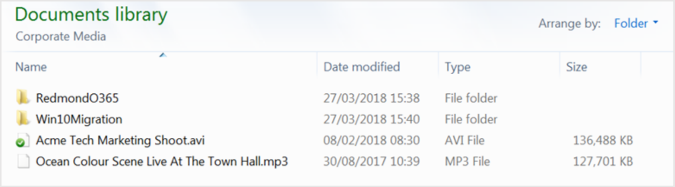


Documents library

Includes: 2 locations

Arrange by: Folder

Name	Date modified	Type
Corporate Media	27/03/2018 15:39	File folder
Home Stuff	20/03/2018 15:34	File folder
My Audits	21/03/2018 15:23	File folder
My Work Documents	21/03/2018 16:14	File folder
Presentations	21/03/2018 11:41	File folder
Weekly Meeting Notes	21/03/2018 11:41	File folder
Beyond data loss prevention whitepaper....	28/09/2017 17:23	Adobe Acrobat D...
ds_integrated-data-loss-prevention.pdf	28/09/2017 11:35	Adobe Acrobat D...
How to help DLP and Encryption coexist	28/09/2017 11:34	Internet Shortcut
New Microsoft Word Document.docx	20/03/2018 15:37	Microsoft Word D...
Understanding DLP	28/09/2017 12:07	Internet Shortcut



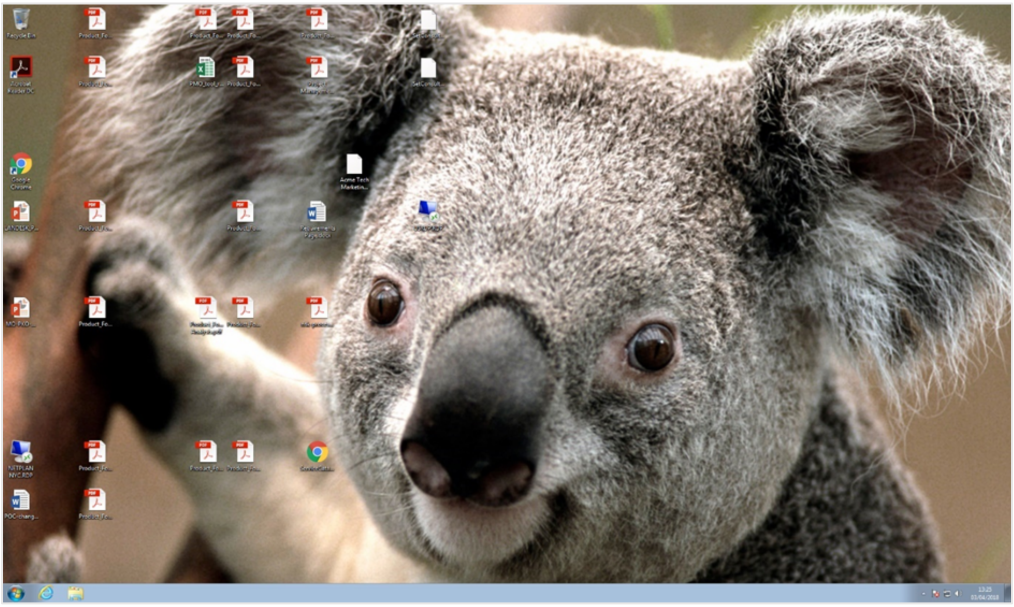
Documents library

Corporate Media

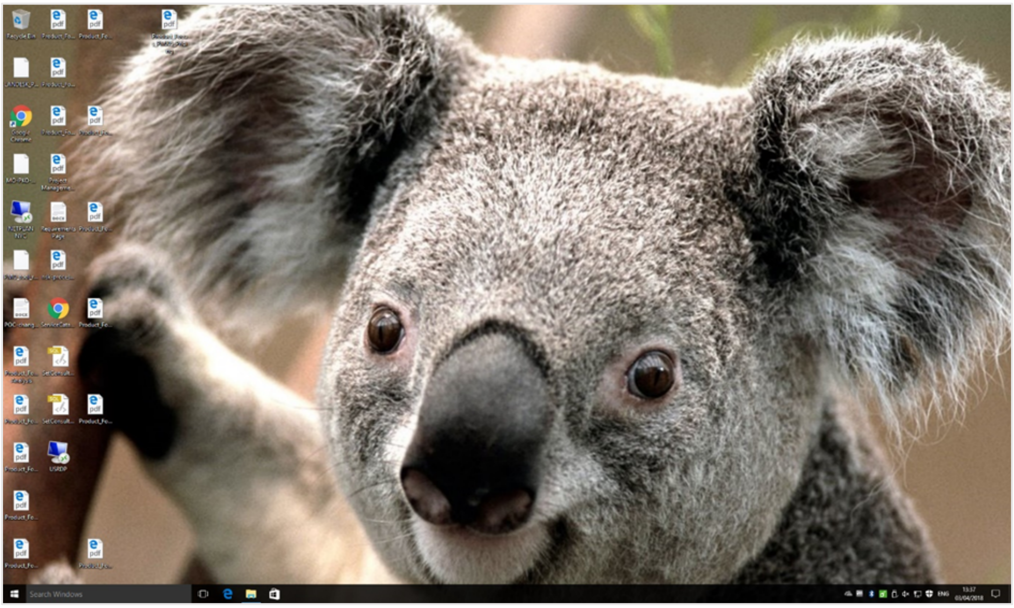
Arrange by: Folder

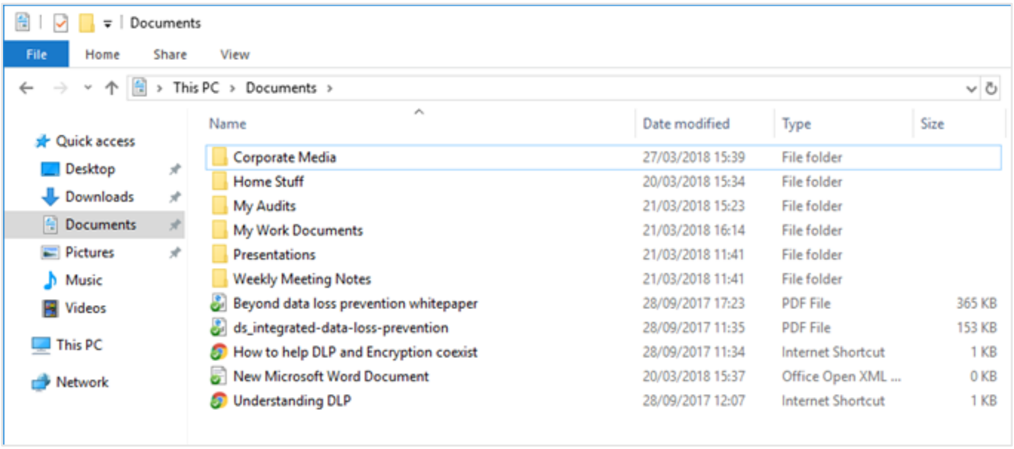
Name	Date modified	Type	Size
RedmondO365	27/03/2018 15:38	File folder	
Win10Migration	27/03/2018 15:40	File folder	
Acme Tech Marketing Shoot.avi	08/02/2018 08:30	AVI File	136,488 KB
Ocean Colour Scene Live At The Town Hall.mp3	30/08/2017 10:39	MP3 File	127,701 KB

The user has also personalized their desktop, so we will capture those modifications using our Environment Manager configuration.

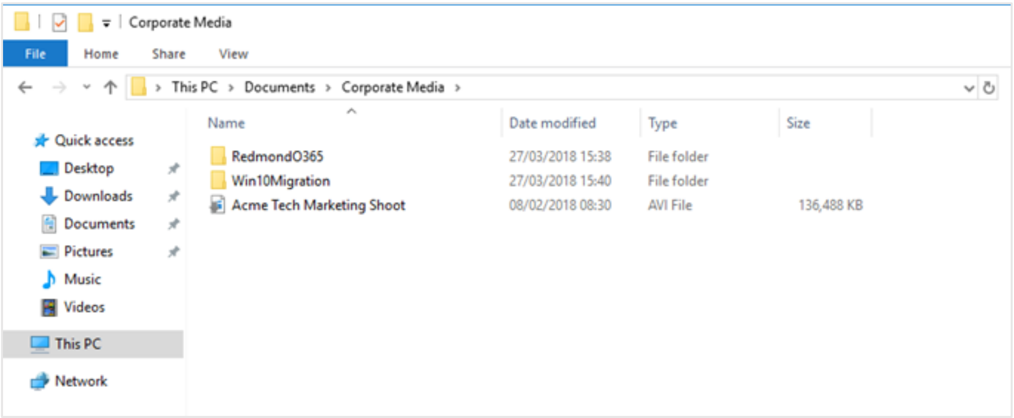


When this user is supplied with their new Windows 10 laptop, they are presented with a familiar look and feel with their files and folders in-place.





Name	Date modified	Type	Size
Corporate Media	27/03/2018 15:39	File folder	
Home Stuff	20/03/2018 15:34	File folder	
My Audits	21/03/2018 15:23	File folder	
My Work Documents	21/03/2018 16:14	File folder	
Presentations	21/03/2018 11:41	File folder	
Weekly Meeting Notes	21/03/2018 11:41	File folder	
Beyond data loss prevention whitepaper	28/09/2017 17:23	PDF File	365 KB
ds_integrated-data-loss-prevention	28/09/2017 11:35	PDF File	153 KB
How to help DLP and Encryption coexist	28/09/2017 11:34	Internet Shortcut	1 KB
New Microsoft Word Document	20/03/2018 15:37	Office Open XML ...	0 KB
Understanding DLP	28/09/2017 12:07	Internet Shortcut	1 KB



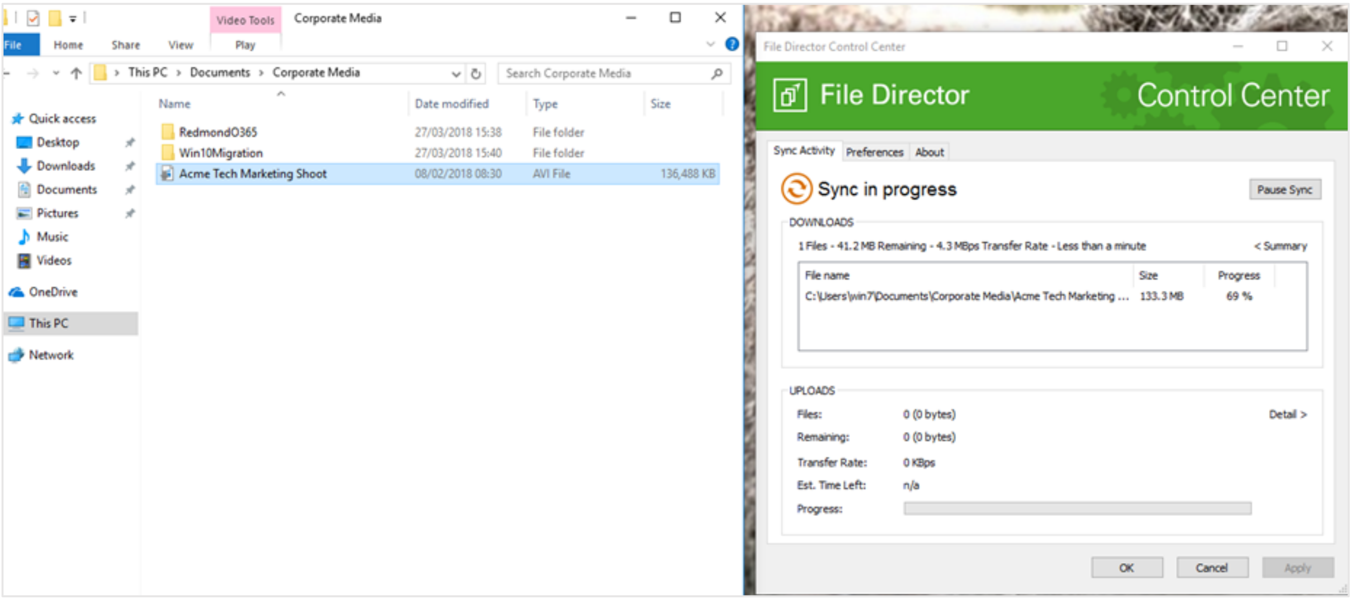
Name	Date modified	Type	Size
RedmondO365	27/03/2018 15:38	File folder	
Win10Migration	27/03/2018 15:40	File folder	
Acme Tech Marketing Shoot	08/02/2018 08:30	AVI File	136,488 KB

Notice that the .mp3 file that was included within the ‘Corporate Media’ folder on the user’s Windows 7 endpoint has not been migrated to their new laptop. Also, the ‘Acme Tech Marketing Shoot’ .avi file has a grey downwards arrow as an overlay. This indicates that the file is making use of another File Director feature, namely Ghost Files.

Additional File Director Features

Ghost Files

As the name suggests, Ghost Files are a representation of the file on the endpoint without the file being in situ on the disk. Only when the user opens the file for the first time is it downloaded to the endpoint, thus helping to keep bandwidth optimized when a user is onboarding.



Name	Date modified	Type	Size
RedmondO365	27/03/2018 15:38	File folder	
Win10Migration	27/03/2018 15:40	File folder	
Acme Tech Marketing Shoot	08/02/2018 08:30	AVI File	136,488 KB

Sync in progress

DOWNLOADS

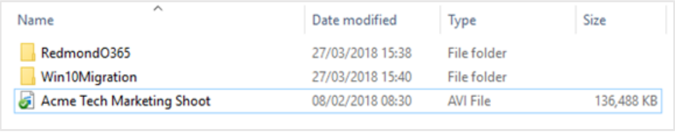
1 Files - 41.2 MB Remaining - 4.3 MBps Transfer Rate - Less than a minute

File name	Size	Progress
C:\Users\win7\Documents\Corporate Media\Acme Tech Marketing ...	133.3 MB	69 %

UPLOADS

Files: 0 (0 bytes)
Remaining: 0 (0 bytes)
Transfer Rate: 0 KBps
Est. Time Left: n/a
Progress:

As can be seen here, once the user opens the file, File Director downloads it to the local disk, making it available to the user.



Name	Date modified	Type	Size
RedmondO365	27/03/2018 15:38	File folder	
Win10Migration	27/03/2018 15:40	File folder	
Acme Tech Marketing Shoot	08/02/2018 08:30	AVI File	136,488 KB

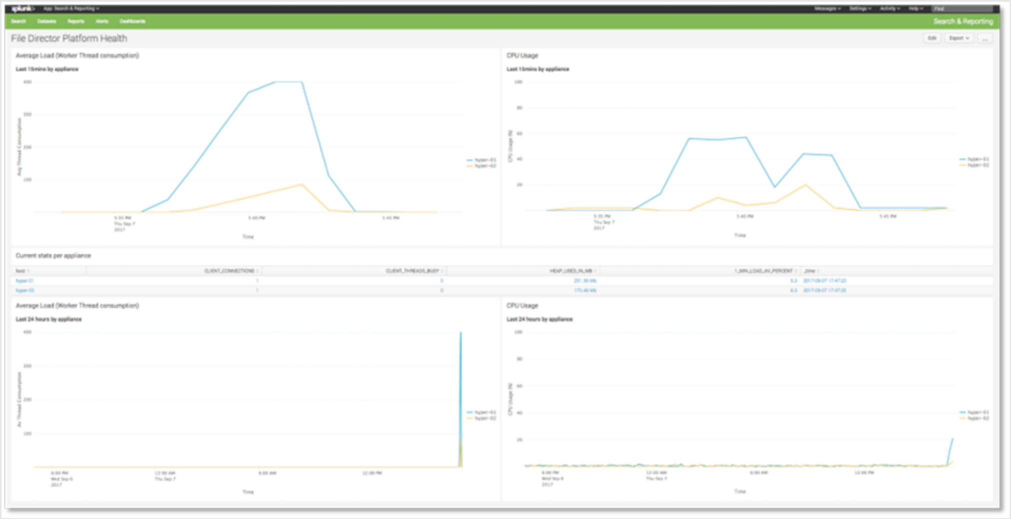
Reporting

During a migration, it is vital that IT teams can monitor their organization’s infrastructure performance. When an OS migration includes user file migration, this visibility becomes even more vital. File Director provides information relating to the appliance’s performance and health, making it possible to monitor and report upon a wide range of metrics, including:

- Number of threads in use
- CPU usage
- Memory usage
- Load average
- OneDrive for Business connector performance statistics

This functionality enables the File Director administrator—via tools such as Splunk and Graylog—to monitor the health of their appliances and clusters, giving IT the required insights to drive operational performance and ensure a high level of end user experience.

Here is an example dashboard using Splunk:



File Director Platform Health

Average Load (Worker Thread consumption)

Last 15mins by appliance

CPU Usage

Last 15mins by appliance

Current stats per appliance

host	CLIENT_CONNECTIONS	CLIENT_THREADS_BUSY	HEAP_USED_IN_MB	1_MIN_LOAD_AV_PERCENT	_time
hyper-01	1	0	251.36 Mb	5.3	2017-09-07 17:47:23
hyper-02	1	0	170.46 Mb	6.3	2017-09-07 17:47:25

Average Load (Worker Thread consumption)

Last 24 hours by appliance

CPU Usage

Last 24 hours by appliance

Details of how to use Splunk to monitor File Director can be found on the Ivanti Community here.

Conclusion

By using a combination of easy-to-configure File Director features along with the use of the OneDrive for Business connector, we have reduced the risk and cost of migrating to Windows 10—while ensuring all files and data settings from a user's former laptop are available instantly on their Windows 10 device. Files and folders follow the user and can be synced selectively with instant access.

Users can work the way they want to, on any device they have on hand, without worrying about data access or loss. IT can capture, control, and audit Office 365 users' 1TB of OneDrive storage.

Easy. Transparent. Simple.

www.ivanti.com ☎ 1 800 982 2130 ✉ sales@ivanti.com