ivanti

Ivanti File Director Deployment Whitepaper

Document Purpose

This Document provides guidance on Ivanti® File Director deployment and configuration best practices. File Director is a powerful User Data Management Tool that can be deployed to fully utilize both local and cloud storage within the secure parameters of a granular sync and auditing policy engine.

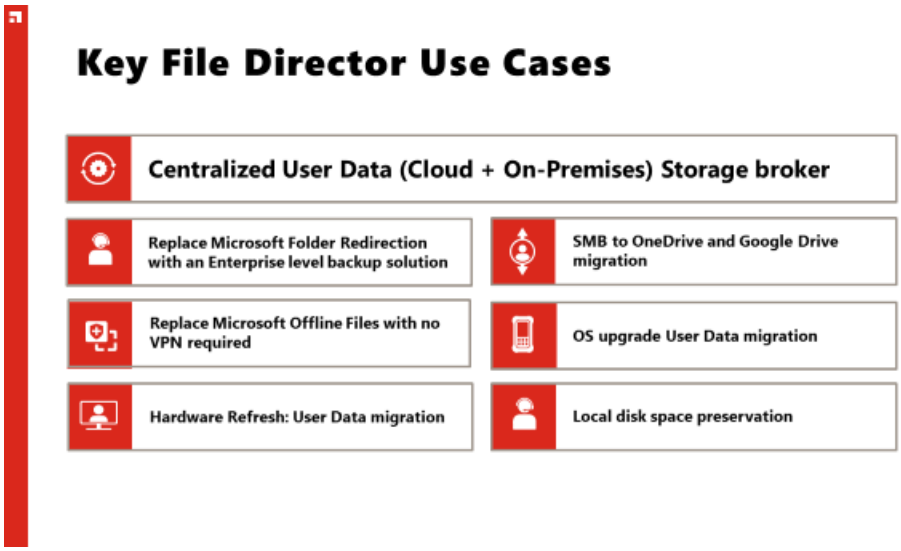
File Director has been successfully deployed by several Enterprises to deliver upon a variety of wide-ranging Use cases all with the shared goal of improving the End user Data access experience. The recommendations provided within this document have been founded based upon real world Data and feedback from our Customers and technical field staff.

Please note this Document should be used in conjunction with the official Product help Documentation. This is not a replacement for the Installation and Upgrade Guide and will focus on best practices rather than a step by step installation workflow.

Assumptions

It is assumed that you previously have or are in the process of consulting the Official Ivanti® File Director Documentation on Installation and Upgrades and Policy Configuration.

Why File Director?



More and more Desktop IT organizations are thinking strategically about Data management and baking it into key Desktop projects like Windows 10 migrations and physical-to virtual initiatives instead of treating it as an afterthought. It's more than just a user convenience. Our customers are seeing measurable gains through better user productivity, ease of management, and compliance.

Much of what we accomplish with every release is focused on enabling better user Data management for the primary desktops where users spend the bulk of their time. This is a direct result of our extensive collaboration with organizations that are tackling user data challenges at enterprise scale. We also put significant effort into improving the user experience across all of our platforms including Mac, IOS, Android and Web.

The purpose if this Document is to help you extract maximum value from your File Director investment by means of best practice deployment and configuration. Prior to embarking on this journey, you should define the problems you intend the product to solve and use cases you anticipate it to deliver on.

Total sync control

File Director's granular sync mechanism allows users' files to by synced to OneDrive for Business storage and to every endpoint—either in the background, on-demand, or in real time. IT can control which files sync by type, age, size, and path to ensure only relevant content is uploaded to the cloud.

These elective-sync methods allow users access to files as needed, without incurring costly storage or bandwidth penalties associated with limited local disk resources or slow network links. File Director's efficient delta sync mechanism ensures large files, including in-use Outlook PST files, can be synced from endpoints, sending only relevant changes. This reduces network traffic and sync time significantly and provides endpoint coverage of users' data requirements.

In-location sync

In-location sync ensures users' files are synced to OneDrive for Business storage without moving the original files. Files within a user's existing profile are synced automatically from their current location, for example,

from the Desktop, Documents, Pictures, or Downloads folders, to the cloud, therefore eliminating data sprawl and enabling centralized back-up of user data.

Users continue to save their files locally on their endpoint, in the usual folders, without having to move or copy them to a specific folder for them to be synced. This eliminates the need for user re-training, as all file-sync and migration actions are imperceptible to the user, and it ensures a native user experience.

Replace offline Files

With typical mapped drives, when users go offline, their files become inaccessible unless a VPN network is used. This can lead to user dissatisfaction, loss of productivity, or additional complexity associated with VPN connections and support. File Director's Mapped Drive Emulation enables users to view and access files on mapped drives, even when offline. All content is searchable and files that have been accessed prior to going offline remain accessible for viewing and editing. Any files that are edited offline are then synced automatically to OneDrive for Business storage as soon as a network connection becomes available.

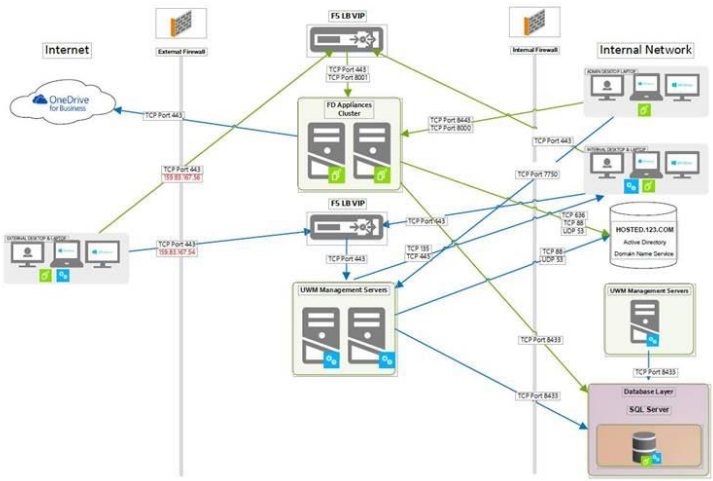
Customer Story – Unlock Cloud storage on RDSH

Customer: UK University
Users: 30000 (12-15000 Concurrent)
Clients: Server 2016 RDSH Pool - Windows 7 Physical Desktops – IOS Mobiles.
Home Drive Storage: Local SMB
Average Profile Size: 10gb

File Director Deployment Goals:

- Unlock the 1TB of free OneDrive storage for each of our Users. We require files delivered on demand as we do not have the local disk space on our terminal Servers to host up to 1TB Per User.
- We do not want to disrupt the normal workflow of our users in any way. File Director should be invisible and undisruptive.

Architectural Design



File Director Deployment Strategy

Onboarding (The term used to describe the initial Upload and or Download of the Profile Data)

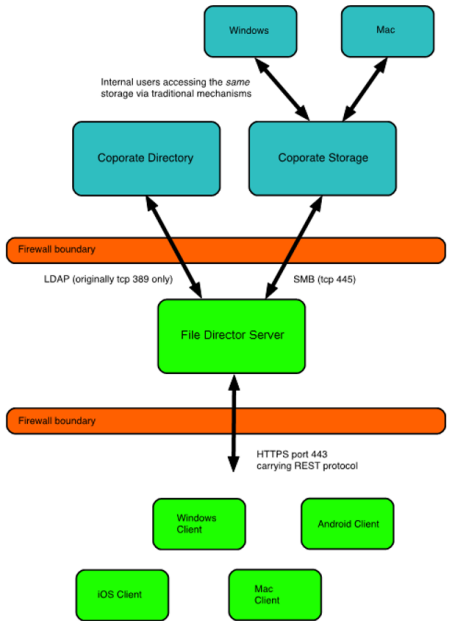
- 2 Appliances (ESXi) clustered sat behind a Citrix Netscaler
- Installed the client on a pool of 2016 RDSH Servers with up to 1000 concurrent Users. Using Splunk they monitored the Syslog Data to track the health of the appliance during the On-boarding of these users.
- Configured the Home Map Point to Sync Automatically at Logon. Enabled access to this Map Point on both Windows and IOS Devices.
- Configured a shared Map Point (Research Drive) to sync on demand. Restricted access to Windows clients only.
- Cache Management configured to clean up the local copy of the Users Cache at Logoff.
- In-Location-Sync for Documents, Downloads and Desktop to ensure sync occurs from the native location without user intervention
- Kerberos Single Sign On enabled.
- File Type Exclusions for .msi files. 2gb File Size exclusion with an override set for .xls files.

File Director Architecture Overview

On Premises storage

Access to Data is provided by client software which is available for Windows, Mac, iPad, iPhone, Android, or via browser.

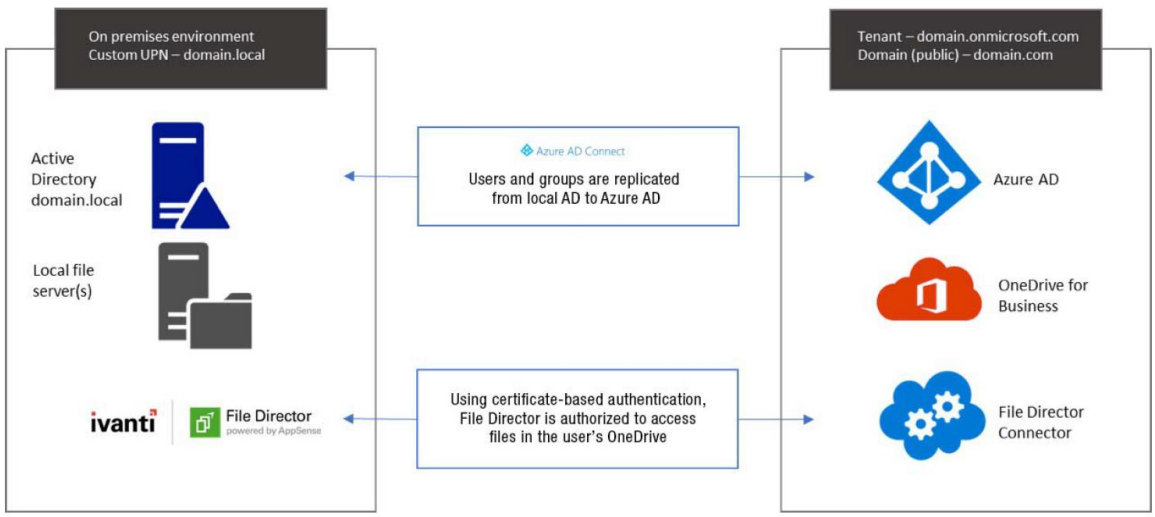
Connectivity is facilitated via a virtual appliance which sits in the perimeter of the customer's network and acts as a broker between the File Director clients and the customer's storage.



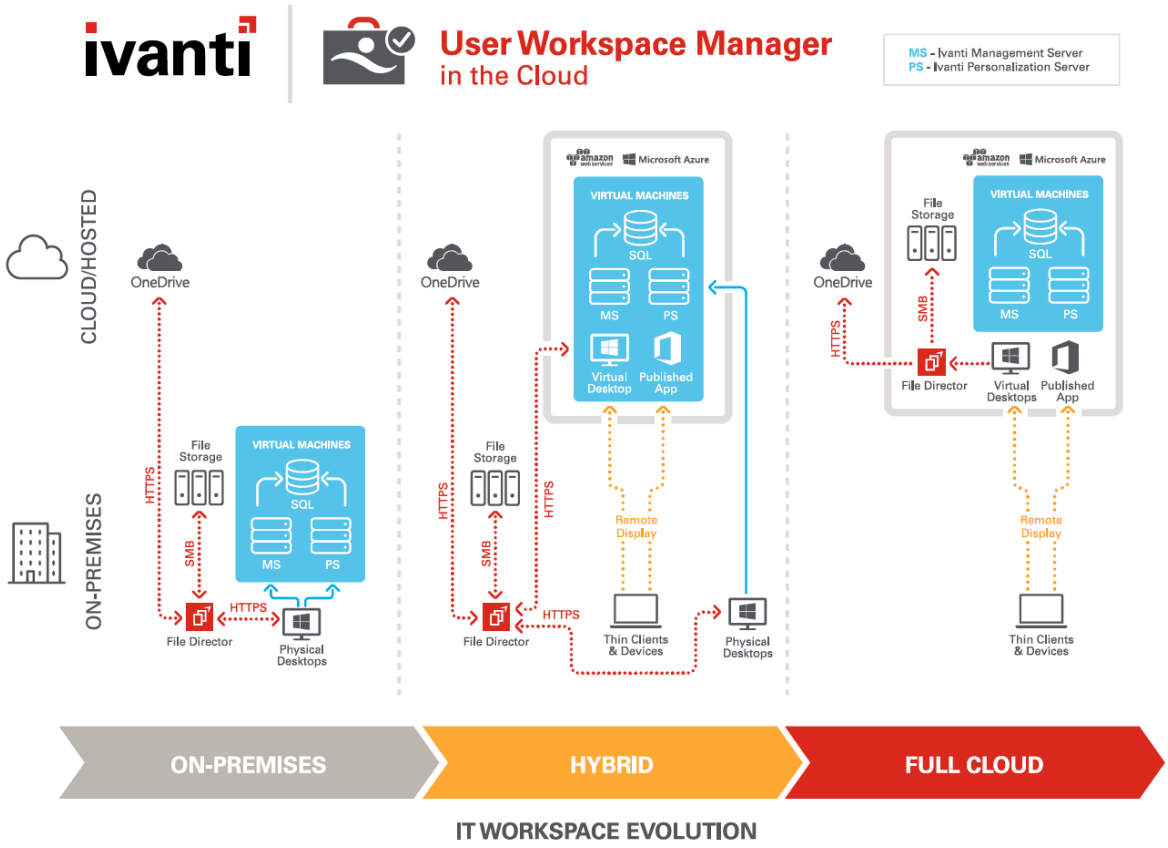
All WAN traffic to and from the appliance occurs over SSL (HTTPS).
The Appliance accesses internal resources using the following ports:

TCP 443	Clients accessing File Director Appliance
TCP 80	Clients accessing File Director Appliance (optional)
TCP 389	LDAP to Active Directory Server
TCP 636	LDAPS to Active Directory Server
TCP 445	SMB/CIFS (File Server/Storage)
UDP 53	DNS
TCP 8443	Appliance Web Administration

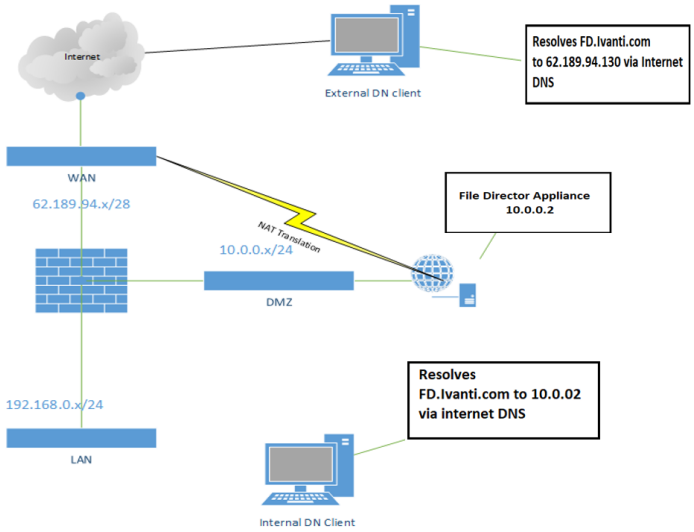
Cloud storage



HYBRID STORAGE

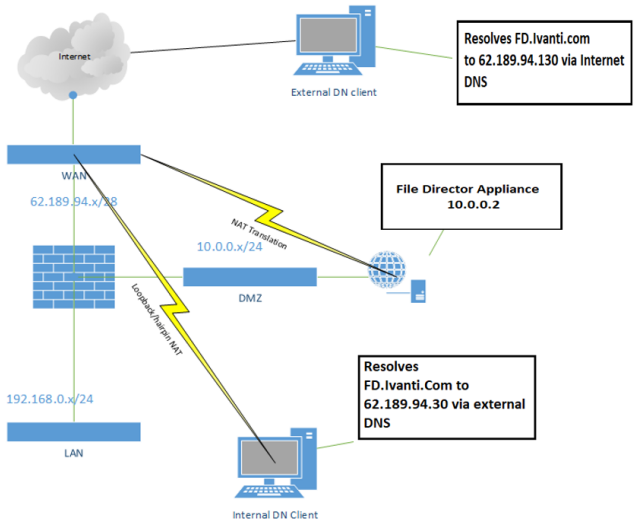


Topology Example 1 – Split DNS and NAT



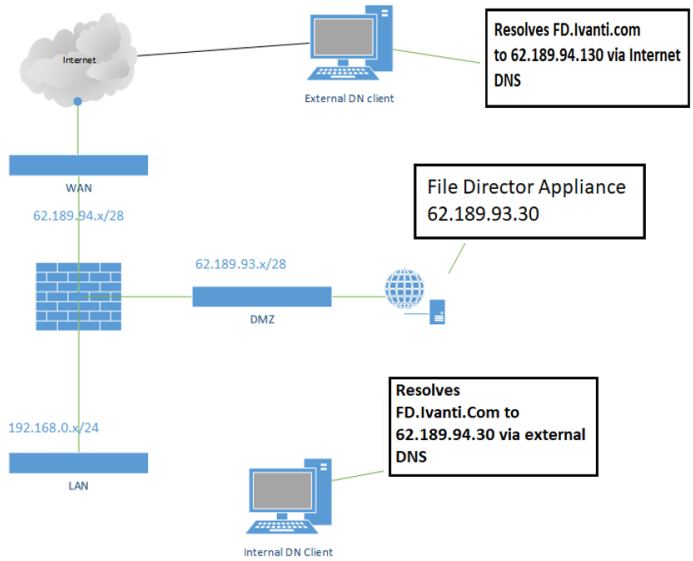
- Same DNS namespace internally and externally – eg ivanti.com
- Appliance has a private IP address in a different subnet to the LAN
- IP address will be different for the CN of the appliance when resolved internally vs externally

Topology Example 2 – Single DNS and Loopback NAT



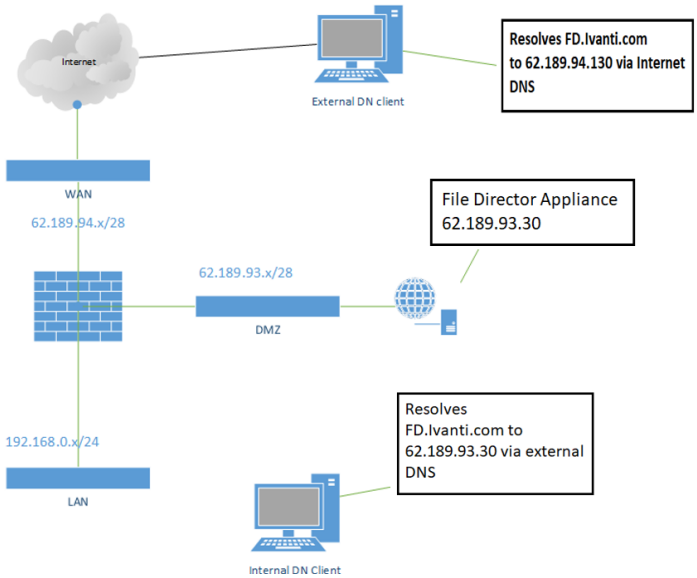
- All clients internal and external use the same external DNS.
- Internal clients traverse external interface of firewall to reach DMZ (hairpin or loopback NAT)
- Common configuration when customer has different internal and external namespaces (eg ivanti.com vs ivanti.local)

Topology Example 3 – Internet Routed DMZ



- Appliance assigned a public IP which is part of an internet routed IP block assigned to the firewall DMZ interface
- May comprise single DNS or split DNS configurations
- Internal and external traffic routed to DMZ interface

Topology Example 4 – Reverse Proxy and DNS conditional forwarder



- Allows one or more external IP addresses to service multiple internal HTTPS resources
- May use internal or external IP addresses and any combination of DNS configurations.
- May be common in small businesses where IP space is finite, or secure organisations where reverse proxy is required for compliance

Appliance

We recommend that you install the File Director appliance on a hypervisor or virtual machine server in the enterprise demilitarized zone (DMZ). From there the appliance does the following:

- Provides secure communications using Secure Socket Layer (SSL) encryption.
- Uses your existing Lightweight Directory Access Protocol (LDAP) to communicate with the Active Directory and configure users, groups, and home folders.
- Looks up the location of the file servers using a Domain Name System (DNS) server.
- Connects to existing file storage using Server Message Block (SMB) protocol (also known as Common Internet File System, CIFS).

What is the difference between the File Director Appliance and the File Director Server?

- The File Director Appliance is the virtual appliance and Linux operating system that hosts the File Director server. This is managed via the console / hypervisor and SSH where 'support mode' is activated.
- The File Director Server is the File Director application that resides on the appliance and services the File Director Clients. This is managed via the Admin console, which is accessed through a web browser (IE9 and above) on TCP / SSL port 8443

System Requirements and Prerequisites:

The Appliance can be deployed to the following Hypervisors via the corresponding media:

VMWare ESX Version 4.1 or Later

Microsoft Windows Server Hyper-V 2012 R2 / 2016

- Each Virtual Appliance requires a Minimum of 4GB RAM and 4 Processor Cores
- A Single Static IP Address and A Record (Resolvable Internally and Externally in DNS) are required.
- A Read-Only Low Privilege Active Directory account is required for LDAP bind.
- SQL Authentication Account for High Availability Clustering.
- A Valid File Director License File is required to configure the Appliance

External firewall requirements

TCP 443 - Clients connect to the File Director appliance on SSL on port 443 so that they can synchronize files. It is recommended that you make this the only external port mapped to the appliance.

Internal firewall requirements

TCP 25 - For SMTP to the internal email system

TCP 389 - Active Directory service LDAP on TCP 389

TCP 445 - File store SMB/CIFS on TCP 445

TCP 443 - For internal client connections

TCP 8443 - The web administration interface is available over SSL on http port 8443

TCP 80 - May be required if connecting to internal non-SSL WebDAV resources

UDP 53 - Domain Name System (DNS) on UDP 53

Additional Ports

The following ports can be enabled if required:

TCP 8000 - Open this port if you require the Ivanti Support service.

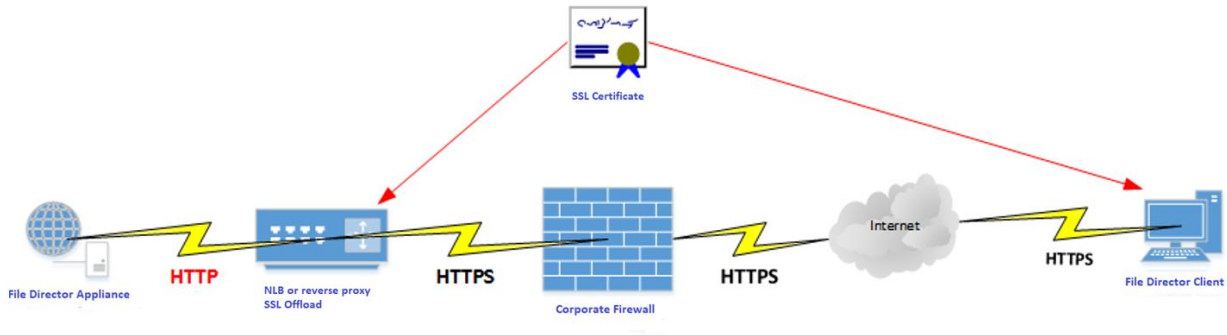
TCP 8001 - Open this port if you require the Network Load Balancing health check.

TCP/UDP 88 - If the File Director server is secured in a DMZ, you must open port 88 on the firewall for Kerberos Authentication to work.

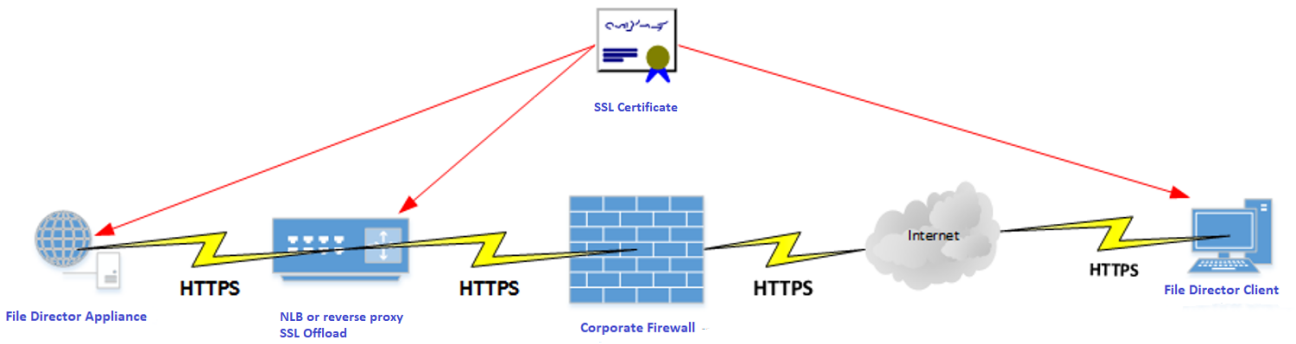
Certificates

SSL Connection:

SSL is the sole communication method for all client access, unless NLB SSL offload is being leveraged to decrease CPU load on the File Director Appliance.



If you are using a reverse proxy with SSL bridging (The SSL channel is maintained from the remote endpoint to the server) the certificate on the proxy listener needs to match the certificate on the server.



SSL Certificates

- File Director has inbuild CSR Generator
- Simplest method for generating the Certificate
- This will only populate Certificate Common Name
- Unable to Populate SAN attributes
- Pre-Existing SSL Certificates can be used
- MUST be supplied in PKCS #12 of PFX Format (.p12 or .pfx file extension)
- To Export PFX or p12 file, you need to have the private key present on the endpoint you are exporting from
- Wildcard Certificates are Supported

Install Trusted Certificates on Client Devices

To use an enterprise certification authority (CA), you need to install the enterprise root SSL certificate on each of the client devices. Network provisioning tools are also available for installing trusted SSL certificates on clients. However, these instructions focus on individual clients.

You only need to add a root certificate to client devices if the enterprise is using a private CA. If you experience difficulties with a certificate issued by a public CA, then review the appliance certificate configuration.

For testing purposes during the evaluation phase of your File Director deployment, to avoid installing the default self-signed certificate on each client device, it is recommended that you request a free time-limited certificate from one of the public CAs.

SMB

File Director – SMB configuration details.

SMB 2.0.2, 2.10

- Signing - HMACSHA256

SMB 3.0.0, 3.0.2

- Large MTU support (up to 1MB transfer buffers)
- Encryption – AES-CCM 128
- Signing - AES-CMAC

Negotiates protocol

- Max Buffer Sizes
- Signing Required
- Sends and receives bytes over the TCP socket (445)

SMB V FD

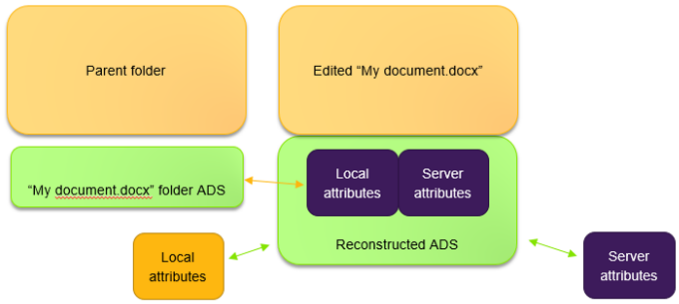
Operation	SMB	File Director	Impact
File/Folder Metadata	Cached	Cached	Improved enumeration of content
File Open	Entire file transferred every time	▪ Local copy is kept ▪ Only Delta is transferred if file changed	End User: ▪ Significant bandwidth savings ▪ Improved user experience through local copy access ▪ Resiliency enables faster sync ▪ Offline access IT Owner: ▪ Resiliency reduces bandwidth usage and speeds migration completion
File Save	Entire file transferred every time	▪ Local copy is kept ▪ Only Delta is transferred	
Network interrupt	Retransfer	▪ Resumable upload ▪ Resumable Download	

Sync Activity

Overview

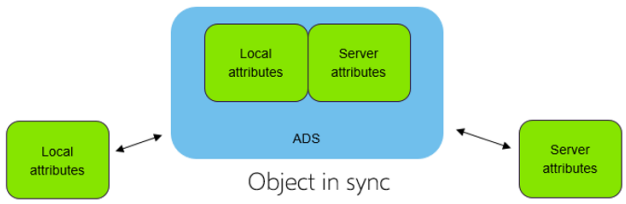
The Windows client uses NTFS Alternate Data Stream files (ADS) stored alongside the real file/folder for:

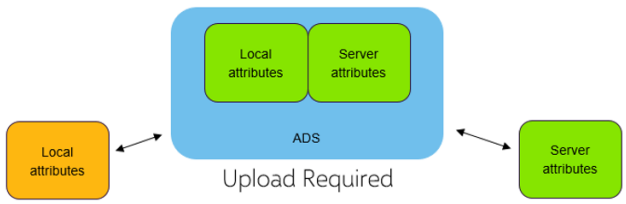
- Automatic downloads
- New files/folders
- Edits
- Moves/Renames
- Deletes
- Any offline file operations
- Conflict detection



Object States

- Filename
- Server Last Modified
- Server Change time
- Server Creation time
- Server Attributes
- Local Last Modified
- Local Change time
- Local Creation time
- Local Attributes
- Conditional API tag
- File size (in bytes)
- Parent GUID
- Folder GUID





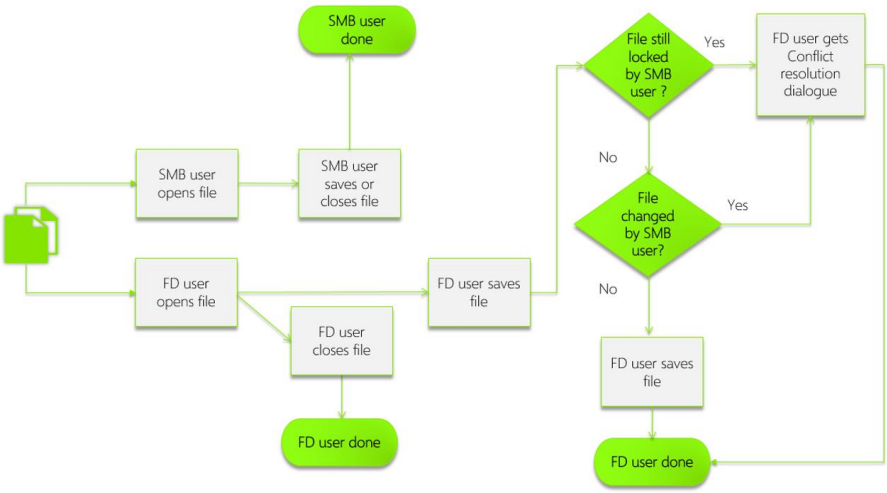
The windows client users a 4 way comparison between current/stored local last modified time and current/stored server last modified time to decide if an item needs to be uploaded/downloaded/left alone or is in conflict.

Conflicts

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.

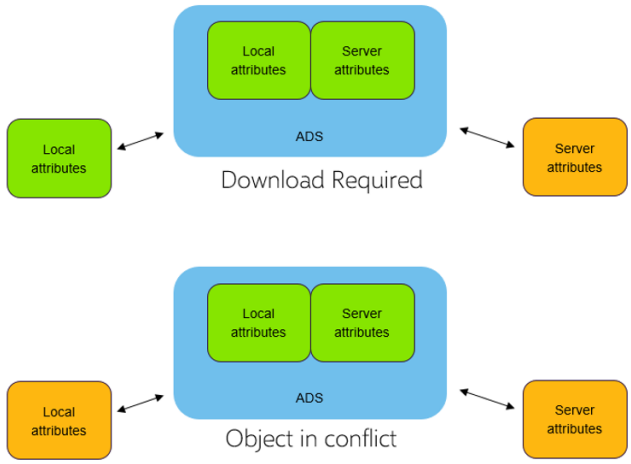
Locking workflow



Conflict Resolution:

Resolved in 1 of 3 ways:

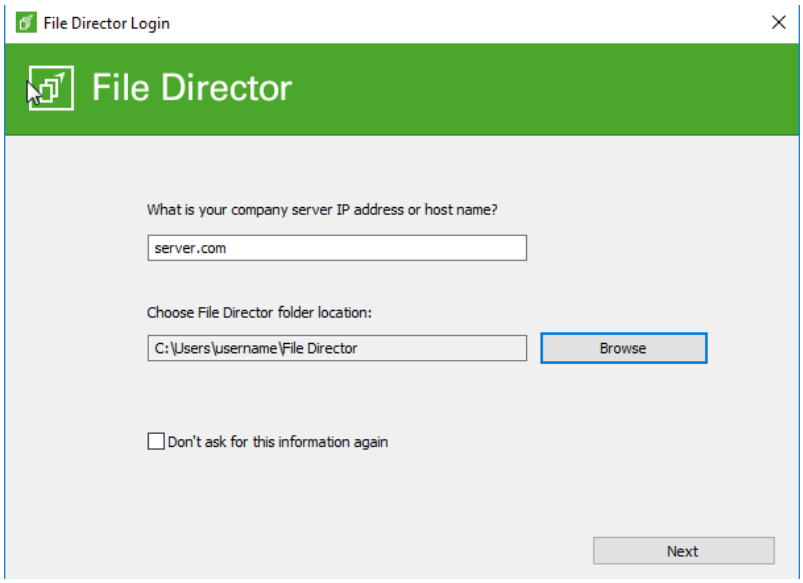
- Default file duplication of filename (1).doc
- Admin defined duplication of filename+format.doc
- User interaction with conflict resolution dialog (with admin defined format)

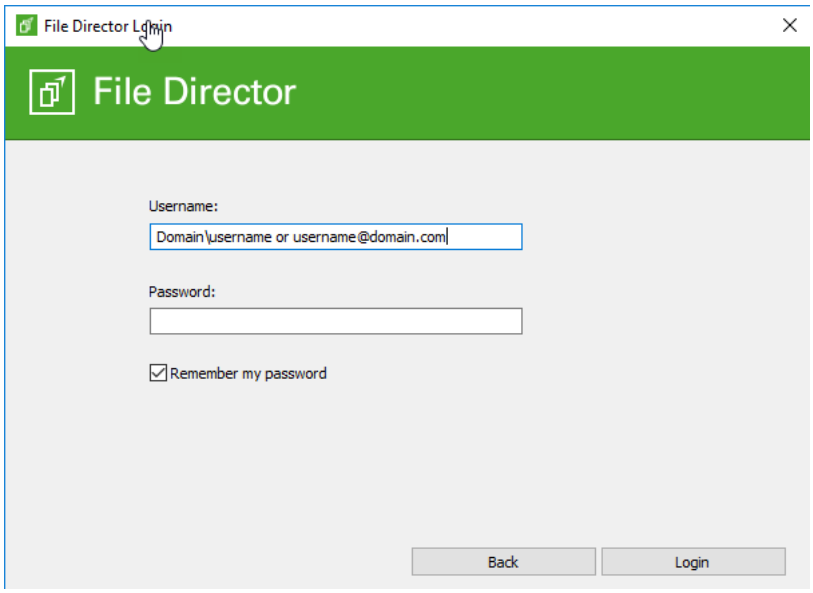


Windows Agent Configurations

Agent Settings

During the initial launch of the agent on a Windows system, users will need to provide information for configuring the connection to the File Director Appliance as seen in the following screenshots.





All local agent settings are managed in the system registry. The required information as seen above can be prepopulated with the required information by setting the following registry values prior to first launch.

HKEY_CURRENT_USER\Software\AppSense\DataNow

REG_SZ "DataNowServer"="https://dn.landesk.com"

REG_SZ "Username"=josh.borges@ivanti.com

NOTE: The base folder is the location where the user's data will be stored locally. The recommendation is to leave the users File Director folder in the default location.

Auto Login Setting
File Director can be configured to auto login after the initial login by configuring the following registry value.

HKEY_CURRENT_USER\Software\AppSense\DataNow

REG_DWORD "DataNowAutoLogon"=00000001

NOTE: If SSO has not been configured the user will be prompted for the password during the first login. After the initial Login to File Director the user's credentials will be stored in the local Microsoft Credential Manager and will be valid until the user's password is changed.

Single Sign On (SSO)

Ivanti File Director supports Single Sign On (SSO). With SSO enabled, File Director will leverage the local credentials to authenticate. This prevents the user from ever getting a prompt for login credentials. If the user is not using domain credentials, the File Director login will fail and the user will be prompted for credentials to login. When a user changes their password, the client will still have access to the files until the domain login token expires. At that point the client will check the local system for the updated credentials.

Configuring SSO:
Configure SSO by adding the follow registry setting to the local machine.

HKEY_LOCAL_MACHINE\Software\AppSense\DataNow

REG_DWORD "SSO"=00000001

Non-SSL Configurations

By default, the Windows agent uses HTTPS over port 443. In order to leverage a Non-SSL connection with the Windows Agent, manual configuration is required. The easiest way to manage this is to set the correct registry values for the server and port to force the connection to HTTP over port 80.

Configuring HTTP connection:
The following registry setting are required for a Non-SSL agent configuration.

HKEY_CURRENT_USER\Software\AppSense\DataNow

REG_DWORD "DataNowPort"=00000050

REG_SZ "DataNowServer"=http://dn.landesk.com

Windows 7

Support for TLS 1.0 has become optional in the File Director. This will cause issues if Windows 7 still exists in the environment. When agents from Windows 7 connect they will get an error. Windows 10 and web connections will work fine. Resolution is to enable TLS 1.0 support in the advance settings in the File Director Administration web portal. See **Certificates with Windows 7**

In Location Sync (ILS)

In Location Sync or ILS is a mechanism to provide an experience similar to folder redirection. The main difference is the data used in ILS is stored in the native locations such as My Documents and Desktop. This makes it easy to give the user a native experience intended by Microsoft. No longer do you need to tell users to save to mapped drives or worry about the problems that come from folder redirection with offline files. ILS is configured by setting the following registry value.

HKEY_CURRENT_USER\Software\AppSense\DataNow

REG_MULTI_SZ InLocationSyncFolders

/My Documents,%USERPROFILE%\Documents

/Desktop,%USERPROFILE%\Desktop

The value needs to be properly formatted to link the folder in the users profile to their file director Map Point. Example as see above is in the format of */folder to sync,Folder location*

The default Map Point used for ILS is the HOME Map Point. See **HOME Map Point** in Appliance configuration section for more information on HOME. If you are going to be using a Map Point other than Home, then the PrivateMapPoint registry value has to be configured in order to enable ILS.

HKEY_CURRENT_USER\Software\AppSense\DataNow

REG_SZ "PrivateMapPoint"=/Map Point Name

NOTE: When ILS is configured, the Map Point will be hidden from the user and will not be visible in the File Director Folder.

Mapped Drives

In addition to ILS, Map Pints can also be configured as Mapped Drives. For example, a user in the HR group might have a team share the is mapped as a U: drive. File Director can mimic this same functionality to present a Map Point to a user as a mapped drive. A Map Point can be configured to be presented as a mapped drive by setting the following registry value.

HKEY_CURRENT_USER\Software\AppSense\DataNow

REG_MULTI_SZ MappedDrives

H,HR

T,IT

The value needs to be properly formatted to set a Map Point as a mapped drive. Example as see above is in the format of *Drive Letter,Map Point Name*

NOTE: When a drive mapping is configured for a Map Point, the Map Point will be hidden and not visible in the File Director Folder. It will only be visible as the mapped drive.

Best practice deployment

Phase 1 – Resource gathering and building your sync policy

- Review the 'Getting Started – Administrators' area of the online File Director documentation. Ensure the Pre-Reqs for the product are in place:

  Licenses / DNS / Active Directory / Certificates

- Download the latest File Director Software. The Mandatory components are a Hypervisor Template (ESXi or Hyper V) and Appliance Patch. Clients for Web, Windows, IOS, Android and macOS are available.

- At least 2 Appliances for redundancy purposes are recommended in production environments. Multiple Appliances have to be clustered which requires an external SQL Database.

- Define your storage source for user's private profile data? The storage a user's data resides upon can be manipulated based upon Active Director User and Group conditions/policies:

  Map Point Policy

  OneDrive Storage Connector

  Google Drive Storage Connector

- Deliver private or shared map point data on-demand or automatically at Logon. Configuring Map Point configuration. Present data to the end users within native profile location or as Mapped Drives.

- Where multiple Appliances are deployed a network load balancer is a requirement. Please follow the best practice guide when configuring your Load Balancer.

- Where SMB storage is being used for private user data, we recommend appliance(s) and storage are as close as possible to ensure the best possible sync experience for the end user. In a multi-geo environment where Appliance(s) sit across various datacenters it is recommended that they sit within independent clusters. This recommendation is based upon a reliance on broadcast traffic being allowed between Appliances for discovery.

- Prior to deployment you should decide upon a Single Sign On method. Both Kerberos and NTLM are available.

- Prior to deployment you should identify files and folders that you wish to exclude from sync. This is to ensure that undesired data is not captured prior to exclusions being applied Exclusion policies are configured in the client registry and can be deployed on scale using Ivanti Environment manager or Group Policy Preferences.

- Download the File Director Performance Monitoring Tool from the Ivanti Marketplace. You will require a Windows server to run the Performance Dashboards on and will later configure Auditing on your Appliance(s) to point to this Server. Splunk is an alternative to the Ivanti Marketplace offering, further details can be found here.

Phase 2 – Building your File Director environment

The number of Appliances you are going to require is largely based upon data throughput rather than number of users. The recommended approach is to build a cluster and onboard users at a steady rate whilst monitoring the health of your Appliances whilst under load.

As you onboard users you can calculate averages in terms of per user data volume and throughput and use this data to plan for further scale. Customer feedback tells us that the Appliance V concurrent user matrix is typically as follows:

Onboarding state – Up to 1000 users Per Appliance

Steady State – Up to 3000 Users Per Appliance

- Build a cluster of Appliances based upon the information above. Key configuration steps are as follows:
- Active Directory / DNS

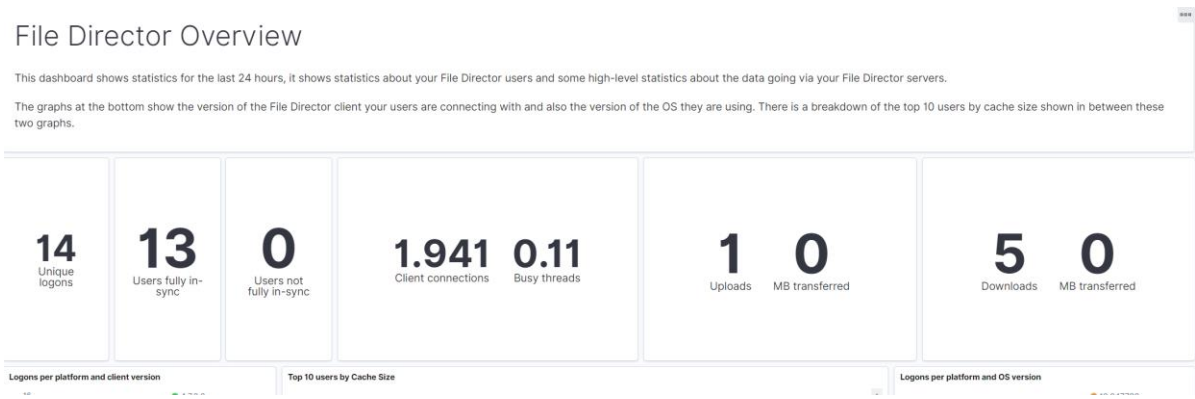
  Licensing

  Certificates

  Appliance Status

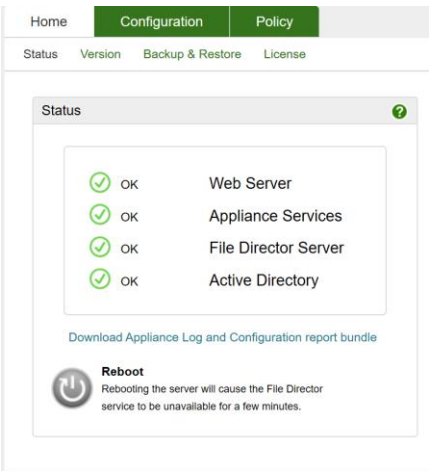
- Configure Auditing on your cluster. This Audit stream should feed in to the File Director Performance Monitoring Tool server you created earlier. Syslog Data from your Appliance(s) will be presented as shown:

Overview Dashboard



Performance Cluster Dashboard

- Configure your Network Load Balancer. Once configured you should be able to hit your Appliance(s) URL via the VIP: http(s)://VIP:443.
- Browse to the Web client via Https://VIP and Login as a test user. You should see the Home Map Point presented. If this fails browse to the Web Client directly via a node hostname or IP to help rule out any issues with the NLB.
- Once your cluster is configured with Auditing enabled and an NLB in place login to the Admin console of all Appliances and review the health status:

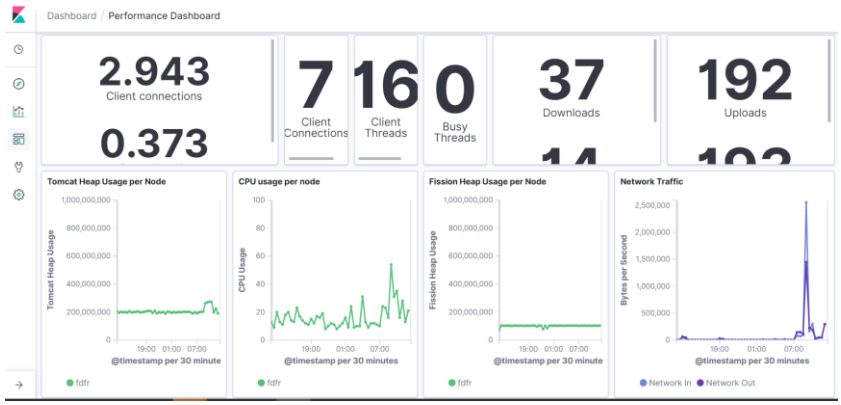


Phase 3 – Client onboarding and health monitoring

We recommend initially onboarding users in cycles of no more than 250. This is to ensure that you can accurately measure the impact on your appliances, storage and bandwidth of onboarding at this scale. You can then use this data to make informed decisions upon increasing this user count and proportionately how much storage + how many Appliances are likely to be required when at full user capacity.

- Install the Windows Client on all devices that form part of the initial onboarding group.
- Configure the clients as per the ‘Windows Agent Configuration’ section of this document. It is possible to run the client in a passive ‘Audit Only’ mode which will allow you to gather data on potential storage requirements without any file sync taking place.
- Once user data sync is active review the Syslog dashboards paying particular interest to the following metrics:

1. Number of busy threads. There are 400 available threads per node is in the example of a 2-node cluster there are 800 available threads for consumption. Should you be nearing this thread capacity you should consider adding further Appliances to ensure continued seamless sync activity.
2. Tomcat Heap usage and CPU usage per-node. Spikes to the maximum threshold are not an issue if they are not for sustained periods of time. Running at maximum CPU and memory proves that the resources available are being fully utilized however should you not see them returned to sustainable levels you should immediately review the number of Appliances available.



3. Response times from OneDrive and Google Drive. File Director actively and passively checks upon the response times for relevant sync operations from cloud storage providers. Should response times regularly be greater than 10 seconds this may indicate that performance/connectivity related issues between your appliances and the cloud storage need to be investigated.