



File Director

# Install and Configure Guide

Version 2018.3 SP1

## Copyright Notice

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](http://www.ivanti.com).

Copyright © 2019, Ivanti. All rights reserved.

Ivanti and its logos are registered trademarks or trademarks of Ivanti, Inc. and its affiliates in the United States and/or other countries. Other brands and names may be claimed as the property of others.

Protected by patents, see <https://www.ivanti.com/patents>.

# Contents

<b>Install and Configure Guide</b> .....	<b>1</b>
<b>The File Director appliance</b> .....	<b>5</b>
<b>Appliance prerequisites</b> .....	<b>6</b>
The appliance in an enterprise network .....	6
Supported operating systems and technologies .....	7
LDAP Directory Service .....	7
DNS Settings .....	7
Checklist of Required Information .....	7
<b>Install and start the File Director appliance</b> .....	<b>9</b>
Start the appliance and change your password .....	10
<b>Appliance Network Identity</b> .....	<b>12</b>
Configure the Appliance Network Identity .....	12
<b>Configure the File Director Appliance</b> .....	<b>13</b>
Connect to the Admin Console .....	13
Licensing .....	14
Enable HTTP access .....	15
Configure DNS for file server location .....	16
Configure the Active Directory Connection .....	17
Create File Director Admin users .....	18
Check the Appliance Status .....	19
Reboot the Appliance .....	20
<b>Configure Certificates for the File Director Appliance</b> .....	<b>21</b>
Upload an Existing PKCS #12 / PFX Certificate .....	21
Request and apply a certificate using the File Director appliance .....	21
Back Up a PKCS #12 / PFX certificate .....	29
<b>File Director Version</b> .....	<b>31</b>
<b>Backup and Restore</b> .....	<b>32</b>
Backup an Appliance Configuration .....	32
Restore an Appliance Configuration .....	33
<b>Apply a File Director Patch</b> .....	<b>34</b>
<b>Map Point Configuration</b> .....	<b>35</b>
<b>Clustering</b> .....	<b>37</b>
Set up the Initial Cluster Node .....	37
Configure Additional Cluster Nodes .....	39
Manage a Cluster in the Admin Console .....	40
Apply a Patch to a Cluster .....	43
<b>Kerberos Authentication</b> .....	<b>46</b>
Prerequisites for Kerberos Authentication .....	46
Configure Kerberos in the File Director Admin Console .....	47
Kerberos Constrained Delegation .....	50
<b>Advanced Configuration</b> .....	<b>56</b>
DSCP QoS Configuration .....	56

---

HTTP Access .....	56
TLS 1.0 .....	57
NTP .....	57
Load Balancer Status .....	58
SMB Storage Authentication .....	58
SMTP Configuration .....	59
Syslog Server .....	59
<b>Policy .....</b>	<b>61</b>
Global Policy .....	61
Mobile Policy .....	63
Map Point Policy .....	65
Users and Devices Policy .....	67
<b>Auditing .....</b>	<b>70</b>
Configure a Remote Syslog Server in File Director .....	70
Set up a Remote Syslog Server .....	70
Report Logs .....	72
<b>Link Based Sharing .....</b>	<b>73</b>
Preparation .....	73
Admin Console .....	73
Set Up the SMTP Server .....	74
Create Staging Map Points .....	74
Enable Link Based Sharing on Map Points .....	75
Set the Automatic Expiration for Link Based Sharing .....	77
<b>File Director SMB3 Encryption .....</b>	<b>78</b>
About File Director SMB3 Encryption .....	78
<b>Roll Out File Director .....</b>	<b>79</b>
Install Trusted Certificates on Client Devices .....	79
Install Root Certificates on Windows .....	80
Install Root Certificates on Mac .....	81
Install Root Certificates on iOS .....	81
<b>File Director SAN Certificates .....</b>	<b>83</b>
DNS and SAN Certificates .....	83
General Certificate .....	84
SAN Certificates in the File Director Appliance .....	89
<b>File Director Command Line Interface .....</b>	<b>91</b>
Access the CLI using the Virtual Terminal .....	91
Access the CLI using Secure Shell .....	92
Commands .....	92
<b>OneDrive connector for home map points .....</b>	<b>94</b>
Prerequisites .....	94
Step 1 - Create your Azure AD application and grant permission to access OneDrive storage .....	95
Step 2 - Configuring File Director .....	102

## The File Director appliance

The File Director virtual appliance is a data broker that forms a connection from your existing file store, through the enterprise firewall, to File Director clients on end-user workstations and mobile devices. After configuration, the broker allows the File Director client application to make encrypted connections over public networks or the Internet to files inside the organization.

The appliance connects to an Active Directory using Lightweight Directory Access Protocol (LDAP) and reads the location of home folders for all users. When a user connects a File Director client to the appliance, it provides a channel to securely synchronize the user's network home folder to their device.

The appliance is simple to configure and can easily be backed up, so it can be recreated quickly. Configure map points and define related policies, using the appliance to manage behavior for specific organizational units, users, and groups of users.

# Appliance prerequisites

## The appliance in an enterprise network

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).

## External firewall requirements

For the external firewall, configure the following IP ports:

**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

For the internal firewall, configure the following IP ports:

- **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 are 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.

## Supported operating systems and technologies

For details of supported operating systems see the [Maintained Platforms Matrix](#) on ivanti.com.

### LDAP Directory Service

The appliance needs read-only access to a Microsoft Active Directory (AD) service through a read-only user account.

You can change the home folder field that the appliance uses in the AD records. By default, it uses homeDirectory. If you want to use the RDP or Terminal Services home folder, you can specify CtxWfHomeDir instead. The home folder feature can be disabled if required.

### DNS Settings

File Director requires internal DNS settings and a public DNS record.

To synchronize user home folders, the appliance needs to correctly resolve the address of the file servers where the folders are stored. The appliance uses DNS resolution to locate the correct file server. The appliance DNS settings must specify the DNS servers within the Active Directory and, in order to resolve the short-form file-server addresses used in user AD records, the domain names it should search.

To access the File Director service on the Internet, you must set up a public DNS record using the File Director server name. You can then use this public DNS name to generate the Certificate Signing Request (CSR) and apply for a publicly trusted SSL certificate.

A Reverse DNS (PTR) record is required in DNS for each file server that will be accessed by File Director. This can be validated from a Windows endpoint by typing **ping -a 10.0.0.1** (where 10.0.0.1 is the file server IP v4 address). If reverse DNS is properly configured, it should return the FQDN, for example, server.mycompany.com. If it returns just the IP address, or the single-label host name, for example, server, then it is likely that reverse DNS is not configured correctly.



Any changes to DNS configuration may require a reboot of the File Director appliance to expedite the changes to its DNS cache.

### Checklist of Required Information

To complete the installation and configuration of the File Director appliance you need the following information.

Hypervisor	Details
Hypervisor	Hyper-V or VMware ESX

File Director Network	Details
File Director Appliance Name	<appliance name>
Appliance IP address	<IP address>
Subnet mask	<IP mask>
Gateway	<gateway IP>

DNS	Details
DNS servers	<IP addresses>
DNS search domains	<domain names>

Active Directory	Details
Domain controllers	<IP addresses>
LDAP port	<port number> (default 389)
LDAP bind account	<userID@domain.com>
LDAP bind password	<password>



# Install and start the File Director appliance

1. Log into [Ivanti Support](#) and download the required File Director appliance software.  
Appliance software is available for ESXi VMWARE 5.5 onward and Hyper-V 2012 R2.
2. Extract the appliance image files and template.
3. In the hypervisor or virtual machine manager, import the template.
4. The template creates the required appliance environment.
5. Start the appliance.

## Examples:

### Install the appliance on Microsoft Hyper-V

1. Log in to a Windows Server desktop.
2. Download and extract the File Director Hyper-V zip file to a suitable storage location. Hyper-V uses the virtual hard disks from the location you choose.
3. Start Microsoft Hyper-V Manager.
4. Select the Import Virtual Machine action.



If you are using System Center, select **New Virtual Machine** to import the template.

---

5. Browse to the folder that you extracted. The Import Virtual Machine wizard requires the folder that contains the config.xml file.
6. Select the option to copy the virtual machine and create a new unique ID.
7. Click **Import**.

### Install the appliance on ESX using vSphere client

When deploying to ESX, the OVT template defaults networking to "Host Only" and must be manually assigned the correct network before using the appliance.

1. Download and extract the File Director ESX zip on your local machine.
2. Start the VMware vSphere Client and log in to the host of vCenter Server.
3. From the menu, select **File > Deploy OVF Template** and follow the wizard.

## Start the appliance and change your password

During deployment, connectivity can be lost when the appliance is migrated to another node, for example following a reboot. Network configurations will not be applied because dynamic MAC addresses assigned in Hyper-V are lost when the node is moved.

To solve this issue, configure a static MAC address in Hyper-V prior to booting the appliance for the first time.

For further information, see [Microsoft KB 976724](#).

1. Start or power on the virtual machine and wait for the appliance to boot.
2. If required, change the input locale. Press **F9** to cycle through the available options. This sets the character mapping for your keyboard.



The default locale for keyboard mapping is US English. If you set a password which contains characters with different mapping in your locale, it could affect your login. For example, if your password is set to P@ssword through the console using a UK English keyboard, it will be recorded as P"ssword. Therefore, if you log in from the web client or an SSH client which supports character translation, the wrong password will be supplied and login will fail.

3. Press **F2**.

The password prompt displays.

4. Enter the default password: *Ivanti*

The Main Menu displays.

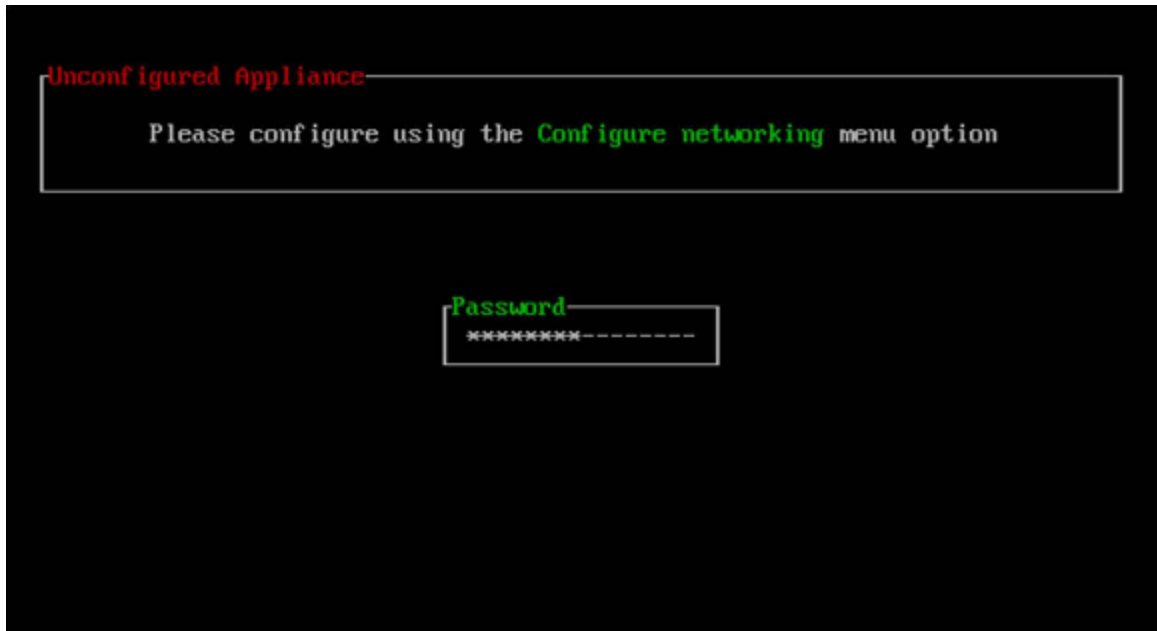


The password must be changed before networking can be configured.

**Do not forget the appliance password. It cannot be recovered or reset.**

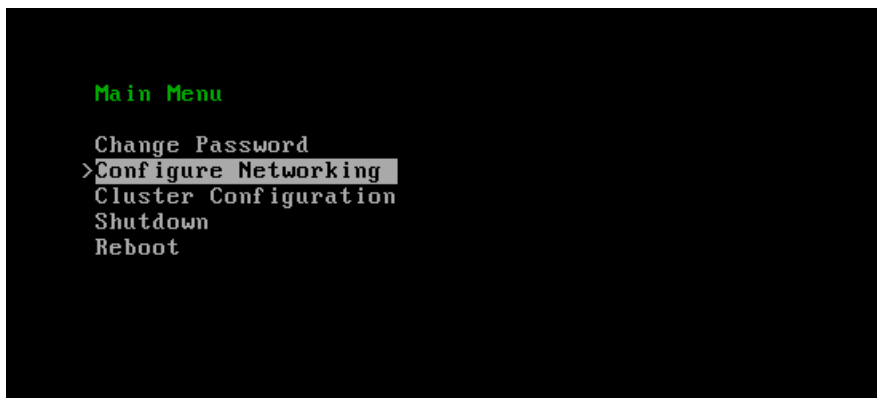
5. Select **Change Password** and press **Enter**.

The password prompt displays.



6. Type the default password, *Ivanti*, and press **Enter**.
7. Type the new password and press **Enter**.
8. Type the new password again to verify it and press **Enter**.

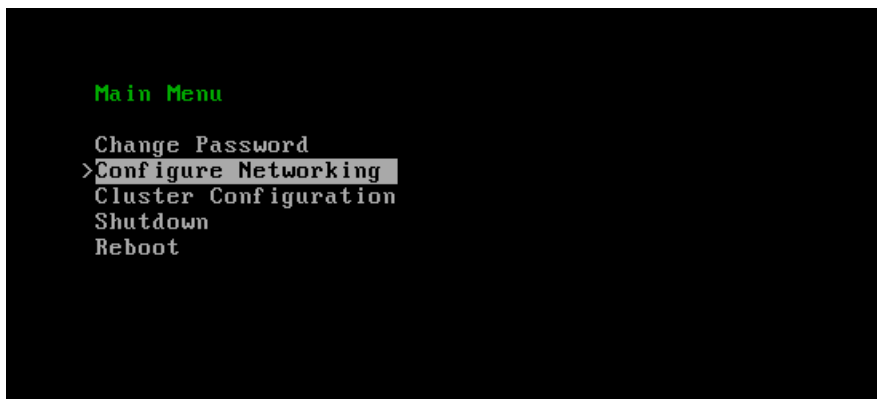
The Main Menu displays with the Configure networking option now available.



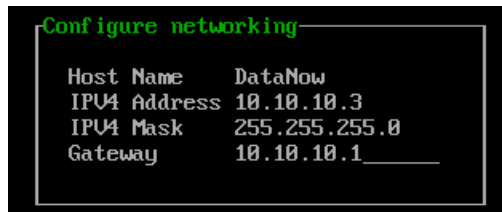
# Appliance Network Identity

## Configure the Appliance Network Identity

1. After the appliance has booted, click in the console and press **F2**.  
The Password prompt displays.
2. Type the password and press **Enter**.  
The main menu displays.
3. Use the arrow keys to select **Configure Networking** and press **Enter**.



The Configure networking box displays.



4. Enter a host name. When you set a host name, the appliance uses it to generate a temporary self-signed SSL certificate.
5. Enter an IP address, subnet mask and a default gateway. The default gateway is the IP address of the internal gateway to services that include, for example, the DNS server, the Active Directory service, the email server and the file store.
6. Press **F10** to save the network settings.
7. From the main menu, select Reboot and press **Enter**.

The server reboots then displays the host name and IP address.

# Configure the File Director Appliance

The following processes should be completed in order:

1. [Connect to the Admin Console](#)
2. [Upload a License File](#)
3. [Enable HTTP access](#)
4. [Configure DNS for file server location](#)
5. [Configure the Active Directory Connection](#)
6. [Create File Director Admin users](#)
7. [Check the Appliance Status](#)
8. [Reboot the Appliance](#)
9. [Configure Certificates for the File Director Appliance](#)

## Connect to the Admin Console

By default, the File Director Admin Console listens for secure socket layer (SSL) connections on TCP port 8443.

Initially you can use the unqualified server name or IP address. If you want to use the server name, you can add the server to your enterprise DNS or add the IP address and server name to the *hosts* file on your local computer.

1. In a web browser, connect to the File Director Admin Console by typing `https://<server>:8443` in the address bar, where *<server>* represents the fully qualified domain name (FQDN) of the File Director appliance, for example *filedirector.ivanti.com*. Press **Enter**.



When you configure the appliance network settings, a temporary, self-signed, SSL certificate is generated that uses the unqualified server name specified. Your web browser will indicate that there is a problem with the website's security certificate because it is self-signed and not issued by a trusted certification authority (CA). You can trust this temporary certificate initially and continue to the website.

Replace this certificate with a trusted certificate containing the server's fully qualified name.

---

The browser connects to the File Director Admin Console and displays the login screen.

2. Log in to the console:

- Username: appliance
- Password: The password you configured when you started the appliance.



By default MS Internet Explorer 9 connects in compatibility mode for intranet sites, that is, sites that do not use the FQDN. You must view the Admin Console with IE9 compatibility view disabled. Press **F12** to change the Browser Mode.

---

## Licensing

Before you can set up and configure your appliance, you must upload a valid license file. License files are provided by Ivanti - if you have not received yours, contact our support team. Until the license has been uploaded, the Configuration and Policy tabs are not accessible. When you view your license details, the license status is License Expired.

### Upload a License File

1. Select **Home > License**. If this is the first time you have accessed the appliance or your current license is not valid, the License Status shows License Expired.

2. Click **Choose file**, navigate to your license file and click **Upload License File**.

**Upload a new License file (provided by Ivanti)**

**Choose file** No file chosen

**Upload License File**

If your license is valid, the license status is updated and details about your license are displayed.

**License Status:**  
**License Installed**

**AppS QA**

Licensee Name:	AppS QA
License ID:	9323e6ea-b390-4ae5-aece-eefa0de5a663
License Type:	Subscription
Expires:	Sun Dec 31 2017 14:00:00 GMT+0000 (GMT Standard Time)
Date Issued:	Wed Feb 01 2017 14:00:00 GMT+0000 (GMT Standard Time)

**Features Included:**

DataNow Enterprise (F5E79D27-B94C-4DF1-996B-58DE8FCAFF74)	Flex, 50 Users versions: 4.**.* - 4.**.*
--	--

Once installed, you can access all areas of the appliance enabling you to configure File Director.

## Enable HTTP access

Select **Configuration > Advanced**.

▼ HTTP Access

**Enable access over HTTP**

**This should only be used in a load balanced environment or with an SSL offload appliance.**

Update

In the HTTP Access area of the Advanced options, configure the required setting and click **Update** to apply.

This option should only be used to enable connection by HTTP in a load balanced environment or with an SSL offload appliance.

## Configure DNS for file server location

To synchronize user home folders the appliance needs to correctly address the file servers where the folders are stored. The appliance uses DNS to resolve the file server IP address.

The appliance DNS settings must specify the DNS servers within the Active Directory (AD) and the domain names it should search in order to resolve the short-form file-server addresses used in user AD records.

1. Select **Configuration > DNS** and click **Edit**.
2. Complete the following DNS Settings:
  - DNS Server IP address.
  - DNS Search Domain.
3. To add further DNS server details, use the + buttons.

Edit

▼ DNS Server IPs

10.0.35.1  
10.0.35.2  
10.0.35.3

▼ DNS Search Domains

qadnroot2.local  
qachild2.qadnroot2.local  
qababy.qachild2.qadnroot2.local

4. Click **Save** to commit your DNS settings.



## Configure the Active Directory Connection

The appliance needs read-only access to a Microsoft Active Directory (AD) service through a read-only user account. The appliance communicates with the Active Directory using Lightweight Directory Access Protocol (LDAP). The LDAP port is configurable - the default is port 389.



To use a name for the directory server you must set the DNS IP address and search domains first.

1. Select **Configuration > Directory Services** and click **Add New AD**.
2. Complete the following Active Directory settings:
  - **Name** - A descriptive name for the server. This is a free text field used to easily identify servers.
  - **Server** - The name or IP address of the LDAP server.
  - **Port** - The port for your AD. The default for LDAP communication is 389.
  - **Home Directory Field** - Select which field to use for active directory. The default setting is homeDirectory but this can be changed to use a different AD attribute or disabled if required. This field corresponds to the active directory Attribute Editor properties. You can use any of the attributes defined in the domain controller and add a value. Changing the attribute in the admin console changes the value read on the DC.
  - **Bind User** - A username with read permissions to the required records. This user account is used by the appliance to synchronize with the directory. Format - username@domain or domain\user.
  - **Bind Password** - The password for the bind user.
  - **Enable SSL** - Adds further encryption between the File Director and LDAP servers. When this option is applied, the port setting is automatically updated to use port 636.

**Active Directory - UKDC1**

**Name:**

**Server:**

**Port:**

**Home Directory Field:**

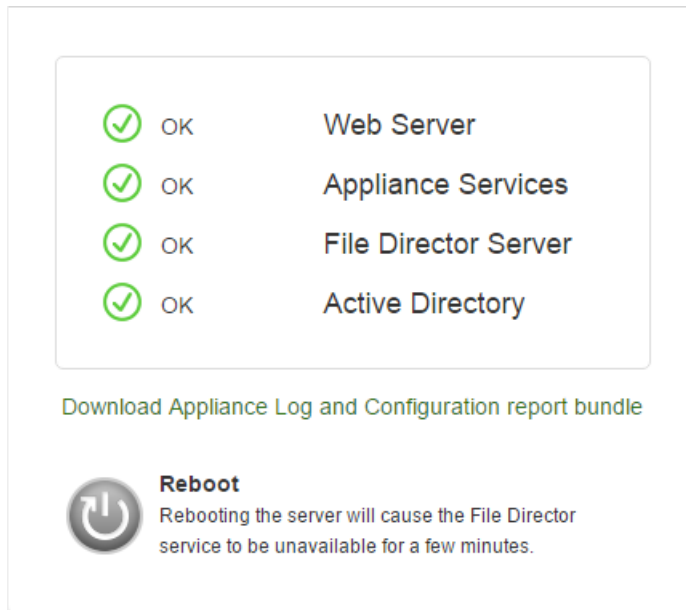
**Bind User:**

**Bind Password:**

**Enable SSL:**

3. Click **Save** to commit your Active Directory settings.
4. Reboot the appliance.

- Following the appliance restart, select **Home > Status** to verify that the WebServer, Appliance Services, File Director Server and Active Directory have been configured.



## Set Home map point source

Select where the Home map point is derived from:

- None
- Active Directory
- OneDrive

For further information about using OneDrive as the home map point, see [OneDrive connector for Home map points](#).

## Create File Director Admin users

After connecting the Active Directory, to continue configuring the appliance, it is recommended that you create a File Director admin user in the console. File Director admin users log in to the console using their domain credentials and can synchronize File Director users with the Active Directory without rebooting the appliance.

This is an optional process for delegated admins because all appliance actions can be performed using the appliance login.

- Select **Configuration > Admin Users** and click **Add User**.

The Admin Users search field is displayed.

- Enter a username or part of the username you want to add.

3. If required, click **Browse** to target a specific domain.
4. Click **Search**.

Any users matching the search criteria are displayed.

**Select User**

Username:   Search In:

Name ▲	User Principal Name
Administrator	Administrator@DNRoot.local
Insight Admin	insightadmin@DNRoot.local
Performance Admin	perfadmin@DNRoot.local
	administrator@DNRoot.local

5. Select a user and click **OK**.

If you are configuring the appliance for the first time, you must log out as the appliance user and log in again as an admin user before continuing.

6. Click **Log out**.
7. Log in as the admin user.

The username format is domain\username. The UPN style login is also supported, for example, username@domain.

If you are configuring the appliance for the first time, you must log out as the appliance user and log in again as an admin user before continuing.

## Check the Appliance Status

Following a reboot, the Status page is automatically displayed. This shows you the areas of the appliance which are configured and those areas requiring attention. Select **Home > Status** to view the Appliance status.

The screenshot shows a status page with a list of services on the left and a notifications section on the right. The services listed are Web Server, Appliance Services, File Director Server, and Active Directory, all with green checkmarks and 'OK' status. Below the list is a link to 'Download Appliance Log and Configuration report bundle'. At the bottom left is a 'Reboot' button with a power icon and a warning message: 'Rebooting the server will cause the File Director service to be unavailable for a few minutes.' The notifications section on the right contains two items: an information icon with the text 'A valid SSL certificate is enrolled for \*.qauk.com. Certificate expires: 27/10/2017' and a warning icon with the text 'No Admin Users specified. Set Admin Users'.

	OK	Web Server
	OK	Appliance Services
	OK	File Director Server
	OK	Active Directory

[Download Appliance Log and Configuration report bundle](#)

**Reboot**  
Rebooting the server will cause the File Director service to be unavailable for a few minutes.

**Notifications:**

- A valid SSL certificate is enrolled for \*.qauk.com. Certificate expires: 27/10/2017
- No Admin Users specified. Set Admin Users

## Reboot the Appliance

When you are configuring the appliance or updating its settings, a reboot is required for the settings to take effect.

To reboot, select **Home** > **Status** and click **Reboot**.

This screenshot is identical to the one above, but the 'Reboot' button and its associated warning message are highlighted with a white background, indicating the next step in the process.

	OK	Web Server
	OK	Appliance Services
	OK	File Director Server
	OK	Active Directory

[Download Appliance Log and Configuration report bundle](#)

**Reboot**  
Rebooting the server will cause the File Director service to be unavailable for a few minutes.

# Configure Certificates for the File Director Appliance

If you have an existing certificate - [Upload an Existing PKCS #12 / PFX Certificate](#)

If you need to request a new certificate from a Certification Authority - [Request and Apply a Certificate Using the Admin Console](#)

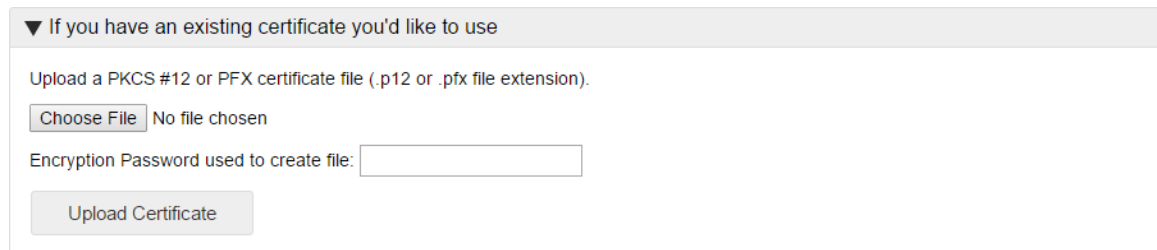
## Upload an Existing PKCS #12 / PFX Certificate

To use an existing certificate for File Director, it must fulfill the following criteria:

- The certificate's CN must match the URL for File Director (unless a wildcard is used)
- The certificate must be valid for the server authority
- The private key must be available to export in PFX/P12
- The certificate must contain the full chain
- The certificate must have a valid date

If your certificate conforms to all of the above, it can be uploaded to the appliance.

1. Select **Configuration** > **SSL Certificate**.
2. In the If you have an existing certificate you'd like to use area, click **Choose File**.



▼ If you have an existing certificate you'd like to use

Upload a PKCS #12 or PFX certificate file (.p12 or .pfx file extension).

No file chosen

Encryption Password used to create file:

3. Browse to the location of your certificate.
4. If the certificate was created with an encryption password, type it into the field provided.
5. Click **Upload Certificate**.

## Request and apply a certificate using the File Director appliance

The File Director Admin Console allows creates a Certificate Signing Request (CSR) for your appliance. Once the CSR is generated, a trusted person within your organization can apply for a public certificate from one of the public Certification Authorities (CA). A trusted person is normally a director or someone publicly acknowledged to represent the organization. The process is split into four sections:

- [Create a CSR from the File Director appliance](#)
- [Request a certificate for your appliance](#)
- [Prepare your certificates](#)
- [Apply a certificate to the appliance](#)

## Create a CSR from the File Director appliance

1. Select **Configuration** > **SSL Certificate**.
2. Expand the **To obtain a certificate from a Certificate Authority** section and complete the following fields:
  - **Host Name** - The fully-qualified domain name of the server where the certificate will be installed. Wildcard domains can be specified with a \* prefix.
  - The host name does not have to match the appliance host name set in the appliance console. However, the host name you provide must match the FQDN on your DNS 'A' records.

For further information about wildcards and SAN attributed certificates, see [File Director SAN Certificates](#).

- **Company/Organization Name** - The name of the organization requesting the certificate.
- **Organizational Unit** - The division within the organization. For example, Engineering or Human Resources, or if applicable, the database administrator name for the organization.
- **City** - The full name of the city where the organization is located. Do not use codes or abbreviations.
- **State/Province** - The full name of the state or province where the organization is located. Do not use abbreviations or codes.
- **Country** - The two digit ISO country code where the organization is located. For example, US, FR.
- **Email** - The email address that will be a point of contact for the certificate request.

3. Click **Create CSR**.

A text box displays the certificate request data.



Every time you use the **Generate New CSR** option, the unique server key is changed, making any previous certificates generated for this appliance invalid.

---

4. Copy the entire text including the lines containing `BEGIN CERTIFICATE REQUEST` and `END CERTIFICATE REQUEST` and save it as a TXT file.

## Using a Private or Enterprise Certification Authority

We recommend that you use a public Certification Authority (CA). However, your organization may use an Enterprise CA and a private CA for proof of concept (PoC) tests.

The following procedure describes generating certificates using Microsoft Enterprise Certificate Authority on Windows Server. Other Enterprise CA solutions are available.

If you are not using a public CA you need to install the root certificate for your private CA on the appliance before installing any chain certificates and the appliance certificate. You also need to provision the root certificate on every client device that uses the File Director client.

### Request a Certificate Using a Microsoft Private CA

1. In a web browser, navigate to: `https://<your CA>/certsrv`
2. Click **Request a Certificate**.
3. Click **Advanced certificate request**.
4. Click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or Submit a renewal request by using a base-64-encoded PKCS #7 file**.
5. Paste the CSR you generated into the Saved Request field.
6. From the Certificate Template list, select **Web Server** and click **Submit**.

**Submit a Certificate Request or Renewal Request**

To submit a saved request to the CA, paste a base-64-encoded C

**Saved Request:**

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
7sP/3Jx5464kmT5AxcY1yjiCkCrU+9GJAzC1SLpj
+z1Gh2jA4F3N7mIMdvOW4Q6Lef7rN8fmq6A4YWZ1
k478S/da0+YaB0h1mJlWfuy8HmO341VVKCiHXVx7
7E3d6Gn1EIik683k09oFE5i+HhjtAb6h3P+FQoM
ZoRFfZvd3XbYDGo=
-----END CERTIFICATE REQUEST-----
```

**Certificate Template:**

Web Server

**Additional Attributes:**

Attributes:

7. Select **Base 64 encoded**, click **Download certificate chain** and save.

8. Once the download is complete, install the certificates and follow the processes detailed in:
  1. [Prepare your certificates](#)
  2. [Apply a certificate to the File Director appliance](#)



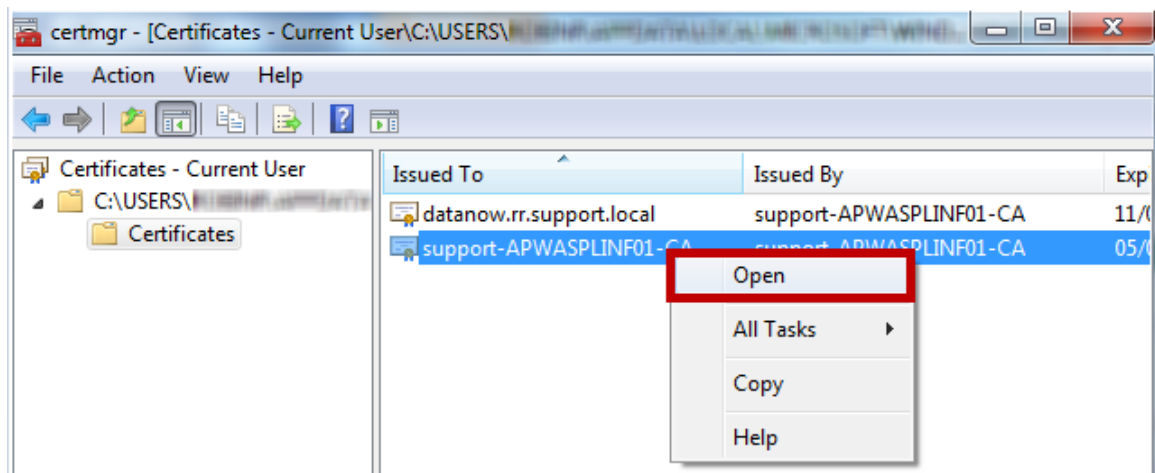
If the private CA is installed with default settings, it may sign the resulting issued certificates with SHA1. This generates browser warnings when accessed by certain browsers. It's recommended to use SHA256 or higher to mitigate this.

## Prepare your certificates

Your certificate will be a web certificate and should include intermediate and root certificates. Once it is installed, you can access your File Director certificate from Certificate Manager. Before you can apply your certificates to the File Director appliance, they must be exported.

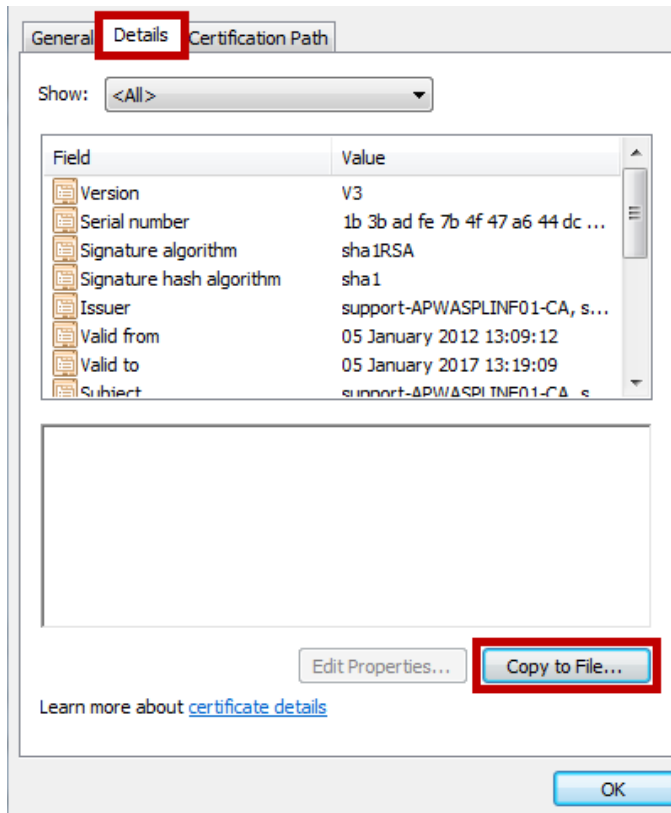
## Export certificates

1. Open Certificate Manager.
2. Right click on the root File Director certificate and select **Open** from the short-cut menu.

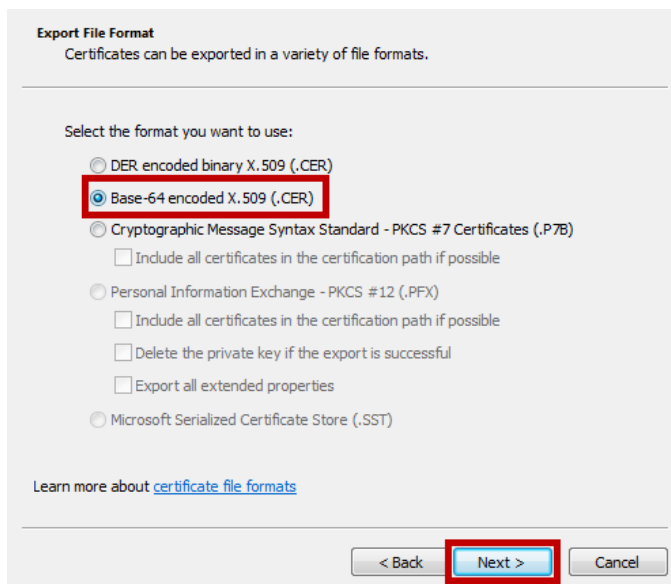




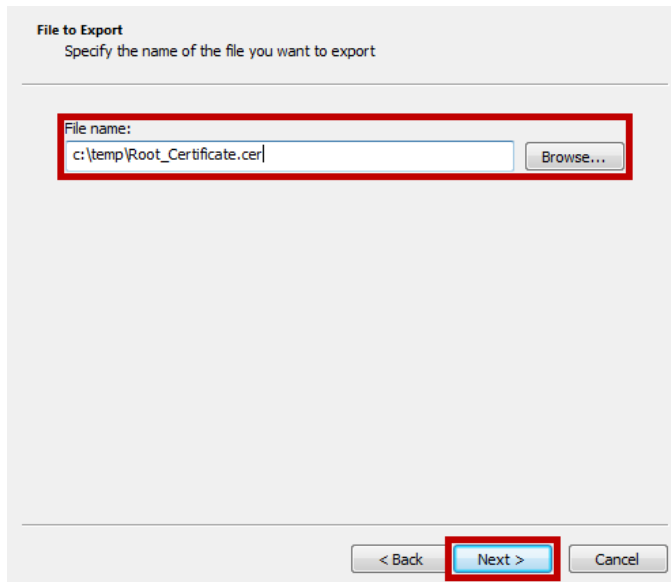
3. Select the **Details** tab and click **Copy to File**.



4. The Certificate Export Wizard opens, click **Next**.
5. Select **Base-64 encoded X.509 (.CER)** and click **Next**.



6. Browse to where you want to save the certificate, give the root certificate a name and click **Next**.



7. Review your settings and click **Finish** to start the export.  
You are notified when the certificate has been successfully exported.
8. Repeat this process for your Standard certificate and any Intermediate certificates.

## Apply a certificate to the appliance

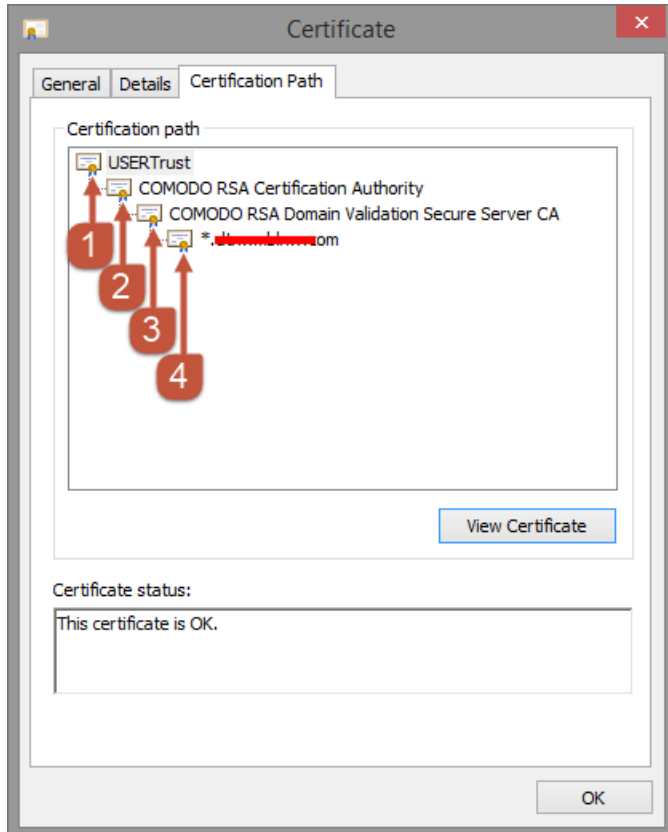
This section describes how to apply a certificate for both Private and Public Certification Authority (CA). Most major public CA root certificates are included in the File Director appliance and in client operating systems for the computers and devices that support the File Director client.



You must have the root certificate from your Private CA. If your CA is a subordinate CA you will require its certificate (intermediate/chain) and any other subordinate CA certificates and the root certificate.

File Director uses 2048-bit RSA certificates in Base64 PEM format, which must be installed in the following in order:

1. Root Certificate
2. Chain 1 Certificate
3. Chain 2 Certificate
4. Server Certificate



Before continuing with this process, we recommend that you take a hypervisor snapshot to back up the pending CSR state prior to any further configuration.

## Apply certificates to File Director

To restart the certificate upload process, click **Reset Certificates**. Any entered data is deleted without removing the pending Certificate Signing Request (CSR).

1. Locate the CER file for the root certificate.
2. Open the certificate in a text editor, such as Notepad.
3. Copy the text including the `BEGIN CERTIFICATE` and `END CERTIFICATE` statements.
4. In the File Director Admin Console, select **Configuration > SSL Certificate**.
5. In the Set New Certificate area of the File Director appliance, paste the certificate details into the text box.

6. Select **Root Certificate** and click **Upload Certificate**.

▼ Set a new Certificate

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC1TCCAb0CAQAwY8xCzAJBgNVBAYTAkdCMRswGQYDVQQIEExJHcmVhdGVyIE1h
bmNoZXN0ZXIxEzARBgNVBAcTCk1hbmNoZXN0ZXIxDDAKBgNVBAoMA0RldjEMMAoG
A1UECwwDRGV2MRyWfAYDVQQDDA10bi53b2ZqZ2ZyY29tMR0wGAYJKoZIhvcNAQkB
DAthcHBAYXBwLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALFP
Y0v2RN0pDuC3XCMJaOcccH0Yjkk/FNADpclCKnNvHL7rSRGYP8SHsO+1/6qTC/bM9
OGKX3RLhBsVOpAnAnBcnNb1viCbJwpNHDrGBp4R860hBjaolCmLz5Kzsu9pLN0Tk
TSxmtH14v633jn/zJhg5gXmxc7JAHC07FODK0451V84EDRptMrBm96OTT7WRP5Xs
u6qnBj3qETZl7pvido7eZ97kd6yTi6hnmEzdLfYdH4aKVjA7Zq33SFE0abRamTzY
PJ+gNuBs1gXSeSIfbLbxe4quFr4GjZdhwkITMJ1JZ80hMSZtOqgSvzhRnaV6d/dK
BDNOwEjnmD5gOQPpM4MCAwEAAsAAAMA0GCSqGSIb3DQEBCwUAA4IBAQA2zZRX3pcG
YSHES8w7UWSB0tsPXK0zHAWGBanF9sxFxSSE7pNt16Ja9EC27236jYKAdT9w/2qp
bRmisaafu1QZjmlqfki7VJmEauKJ+jQav3T6oR/t2KR6RRd+UmeuggpvcvLWI1t8cbk
C7ZyhRNnJW07Qr8uUJILfh9Wzfk1LFbrhnhXZAQFocOYb7E1tKMT8JfZk406tgi
wvvsOKzDnRn/G3sjS2hXiMWT0/5LSFFN6xyjqwE7jKgKKoh9b39/B5zZcHwQQU9R4
```

Certificate Type:

Root Certificate

Chain Certificate/Bundle

Server Certificate

Reset pending root and chain certificates:

A message will confirm that the certificate has been installed.

7. Add your Chain Certificate - select **Chain Certificate/Bundle** and click **Upload Certificate**.

If your chain is a bundle, you must add each chain certificate (e.g. number 3 then number 3) to the text box in reverse order.

In the example below, Chain 2 has been added followed by Chain 1.

▼ Set a new Certificate

```

u6qnBj3qETZl7pvldo7eZS7kd6yTi6hnmEzdLfYdH4aKVjA7Zq33SFE0abRamTzY
PJ+gNuBs1gXsesIfbLbxe4quFr4GjZdhwkITMJ1JZ8OhMSZtOqgSvzhRnaV6d/dK
BDNOwEjnmSgOQFPm4MCAwEAAaAAMA0GCSqGSIB3DQEBCwUAA4IBAQA2z2RX3pcG
YSHES8w7UWSB0tsPXK0zHawGBanF9exFxSSE7pNt16Ja9EC27236jYKAdT9w/2qp
bRmisaafu1QZjmlqfki7VJmEauKJ+jQav3T6oR/t2KR6RRd+Umeugpcv1Wl1t8cbk
C7ZyhRnNjW07Qr8uUJILfh9WzfkLLFbrhnmhXZAQFocOYb7E1tKMT8Jfzk406tgi
wvvsOkZcRn/G3sjS2hXiMWT0/5LSfFN6xyjqwE7jKgKKoh9b39/B5zccHwQU9R4
839A/vuBKkqryEd1DaByqfToapHjHAysh61VoBHNuao8Rjztou4UGs11zP5YhnzQ
k9+Rb/CSstOMF
-----END CERTIFICATE REQUEST-----
-----BEGIN CERTIFICATE REQUEST-----
MIICh1TCCAbOCAQAwY8xCzAJBgNVBAYTAkdCMRswGQYDVQIExJHcmVhdGVyIE1h
bmNoZXNOZXIxZezARBgNVBAcTck1hbmNoZXNOZXIxDDAKBgNVBAoMA0RldjEMMAoG
A1UECwwDRGV2MRyWFAyDVQDDA10b1S3b2ZqZ2YuY29tMR0wGAYJKoZIhvcNAQkE
DAthcHEAYXBwLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALFP
wG...

```

Certificate Type:

Root Certificate

Chain Certificate/Bundle

Server Certificate

A message confirms that the certificate has been installed.

8. Add your Server Certificate - select **Server Certificate** and click **Upload Certificate**.

When all certificates have successfully installed, an information message informs you that the certificate has been enrolled.

9. Reboot the appliance to apply the certificates to the web service.

To test the certificate, close and reopen the browser and connect to the Admin Console using the fully qualified server name specified in the certificate. If the certificates are installed correctly, the browser connects securely without any security warnings.



We recommend that you back up the File Director appliance configuration snapshot.

## Back Up a PKCS #12 / PFX certificate

A PKCS #12 / PFX certificate containing your encrypted SSL certificate and your private keys can be downloaded from your File Director appliance. You can use this when configuring new installations of the appliance without having to repeat the process of configuring an SSL certificate.

1. Click the **Configuration** tab and click **SSL Certificate**.
2. Locate the **To back up the existing SSL certificate chain** area.

▼ To back up the existing SSL certificate chain

Download the current SSL certificate in PKCS #12 (.p12) format.

**IMPORTANT - Please note the encryption password and save in safe location.**

Set Encryption Password:

3. If required, enter an encryption password.

Encryption passwords are optional and add an extra level of security. If you set a password during download, it must be entered to successfully upload your certificate. Passwords are non-recoverable, so it is important that you remember the password or store it in a safe location.

4. Click **Download P12** and save the certificate.

# File Director Version

Check which version of File Director you are running and upload new patches of the software.

Select **Home > Version**.

The left-hand side of the version view shows the version numbers of the components that make up the appliance.

## Components:

Appliance Configuration Services:	release - 4.2.0.1
Appliance Text Console:	release - 4.2.0.1
Appliance Operating System:	release - 20160926
Fission Clustering Services:	release - 2.0.0.112
Patch Server:	release - 1.0.0.13
File Director Server:	release - 4.2.1.5
File Director Web Admin:	release - 4.2.0.24
File Director Web Client:	release - 4.2.0.10
File Director Appliance Plugins:	release - 4.2.1.1

# Backup and Restore

Before applying updates to File Director it is strongly recommended that you;

- Take a snapshot of your virtual machine(s) so you can rollback if required. Refer to your virtualization software supplier for procedure information.
- If you have clustering enabled, take a backup of the File Director database. See [Clustering](#).
- Take a backup of the appliance configuration.

We recommend appliances are forced offline via the maintenance mode flag (or manually via the load balancer) during the upgrade process. This is stop any traffic from the load balancer.

You can back up your appliance configuration information from within the File Director appliance. The whole personality of the appliance and the SSL certificates are backed up to create a snapshot that can be used to configure one or more appliances with the same settings.

The backup and restore does not include the database location because that is a clustered setting. For example, if you are connected to an external database and you perform a backup, it backs up the settings from there. If you restore a snapshot to an appliance pointing to its internal database, the configuration is restored to that. This is a useful mechanism to move from a single appliance a clustered appliance, or to restore a configuration to a spare database, for example.

## Backup an Appliance Configuration

1. Select **Home > Backup & Restore**.
2. In the Backup Appliance Configuration section of the page, enter an Encryption Password in the field provided. This is an optional level of security that requires the same password to be entered when restoring the configuration.
3. If set, it is important that you do not lose or forget an encryption password because they are non-recoverable and the backup will become unusable.
4. In the Backup Appliance Configuration section of the page, click **Download Snapshot**.

▼ Backup Appliance Configuration

Download a snapshot of the current appliance configuration settings.

**IMPORTANT - Please note the encryption password and save in safe location.**

Lost encryption passwords are non-recoverable and will result in an unusable backup configuration file.

Encryption Password:  (optional)

The configuration snapshot is saved to your default download location.



## Restore an Appliance Configuration

1. Select **Home > Backup & Restore**.
2. Click **Browse** and locate the required configuration snapshot.
3. If required, enter the encryption password, defined when the snapshot was created. If you did not set a password, leave the field blank.
4. Click **Restore Settings**.

▼ Restore Appliance Configuration

Restore the appliance configuration settings from a previously generated snapshot file.

No file chosen

Encryption Password:  (optional)

5. Reboot the appliance.

The settings from the snapshot are applied to the appliance.

# Apply a File Director Patch

File Director software can be updated by applying a patch, supplied by Ivanti, which can be uploaded through your appliance. If clustering is enabled and a patch server has been set, patches are applied in the [Cluster tab](#).



Before applying any update to File Director you are advised to take a backup or snapshot of your virtual machine(s), your database, and the appliance configuration. See "Backup and Restore" on page 32

1. Log into Ivanti Support and navigate to the File Director software page.
2. Click the link for the required software.
3. Log in to the File Director Admin Console.
4. Select **Home > Version**.

In the Status section, details of the current patch version are displayed.

5. Click **Choose File** and navigate to a File Director patch file.

The screen updates to list the components that the patch is updating and their version numbers. Click a patch to view further details.

6. Select the required patch and click **Deploy Update** file.

To complete the patch install, the server automatically reboots. Connected devices are unable to communicate with the server for few minutes whilst the reboot completes.

## Note: 2018.3 Patch

Periodically, large patches are issued containing multiple component updates and upgrades to the OS. The 2018.3 patch is an example. Before installing the 2018.3 patch be aware it will require a system reboot several times during the update process. In addition, it is essential you perform recommended backups, as in some circumstances you will need to re-import the appliance snapshot after the update process has completed.

# Map Point Configuration

Map points allow usage policy sets to be targeted to different users based on the server they connect to and their OU membership. You can create Map Points for whole OUs, user groups, and individual users to create a usage policy that meets their requirements while adhering to your security policy.

There are two parts to setting a Map Point:

- **Connection String** - Define the File Director server for the Map Point and set the download policy.
- **Policy** - Define usage policies and platform access for the Map Point.

1. Select **Configuration > Map Points** and click **Add New**. Or click **Edit** to update an existing Map Point.
2. Enter a name for your map point. This can be any value to easily identify the map point.

The name "Home" is reserved for use by Active Directory home drive settings and should not be set as the name of a webdav or SMB map point.

Do not name a Map Point "Share".

3. Enter a connection string.
  - It is recommended that file servers are entered as fully qualified domain names (FQDN), particularly if you are using Kerberos authentication.
  - SMB connection strings must begin with \\ or smb://
  - WebDav connection strings must begin with http:// or https:// To designate a user directory, insert %UserName% into the share path, for example, http://servername.company.com/users/%UserName%). %UserName% is case sensitive.

4. Select the required sync mode:
  - **Manual: Only download files as requested by the user** - Files are downloaded to a user device as they are opened.
  - **Automatic: Download/sync all files for this map point** - All File Director files are downloaded locally when the user logs in to File Director and changed, and new local files are automatically synchronized with the server.

These settings apply to Windows and Mac clients. Mobile devices upload and download on demand rather than sync.



For Windows clients, electives can be applied that prevent certain files being automatically downloaded. For example, certain file types or files above a certain size can be prevented from being automatically downloaded. See [File Sync Controls](#).

▼ **Add New Map Point**
Save Cancel

**Name:**

**Connection String:**

**Sync Mode:**

SMB connection strings must begin with \\

WebDav connection strings must begin with **http://** or **https://**

To designate a user directory, insert %UserName% into the share path  
(examples: \\servername\users\%UserName% or http://servername.company.com/users/%UserName%).

5. Click **Save**.
6. To set a policy for the map point, click the **Set policy for this map point**.

▼ **Temp Area**
Set policy for this map point
Edit Delete

**Name:** Temp Area

**Connection String:** \\Map Points\Temp Area

**Sync Mode:** Manual: Only download files as requested by the user.

# Clustering

File Director supports clustered infrastructures and failover processing and is fully scalable to meet the varying demands of organizations.

If an appliance is taken offline, the File Director service is maintained by having users log on in the background to an alternate appliance in the cluster, according to the current network load balancing method. Although users are momentarily disconnected, they are automatically returned to the service without losing their session state. Any transactions that have not been committed to the database are rolled back.

When setting up the load balancer, ensure that session persistence is setup for the File Director cluster. It is recommended that the cookie insert method is used.

## Set up the Initial Cluster Node

### Prerequisites

Before configuring clustering:

- Ensure all appliances that will be in your cluster are of the same version.
- Create a new blank database in the default SQL instance (SQL Server 2008, 2008R2, 2012, 2014 and 2016 are supported).
- Create a new SQL account. It is recommended that the SQL Service account has DBO privileges. Note that only local SQL accounts are supported, domain-based accounts are not supported.
- Configure the switching environment to allow Broadcast traffic.
- Ensure all cluster nodes that are to share common settings are available on the same network to allow low frequency broadcast discovery between the cluster peers.
- Take a backup of the current appliance configuration.

## Enable Clustering on the First File Director Appliance

1. Boot up the appliance for the first cluster node.
2. Press **F2** and logon.
3. Select **Cluster Configuration** and press **Enter**.
4. Enter a cluster name.
5. Enter a port number. The default port is 49152 but you can use any port from 49152 to 65535.
6. Press **F10** to save the cluster configuration.

### Disable Clustering

To disable clustering, follow the process above and at step 4 leave the cluster name field blank.

## Configure an External Microsoft SQL Database

1. Log on to the Admin Console for the first cluster node.
2. Select **Cluster > Database**.
3. Select **Microsoft SQL Server**.

**▼ Database Settings**

*i* Clustering is enabled - all clustered appliances are currently using the database configured below.

**Database Type:**     Local Database  
 Microsoft SQL Server

**Host:**                   

**Instance Name:**         (optional)

**Database Port:**       

**Database User:**       

**Database Password:**   

**Database Name:**

4. Complete the following fields to configure your database:
  - **Database Host:** DNS name or IP Address of the SQL server
  - **Database Port:** 1433
  - **Database User:** SQL account created during initial SQL setup.
  - **Database Password:** Password set for the SQL account created during initial SQL setup.
  - **Database Name:** Name of the blank database created during initial SQL setup
5. Click **Save** to configure the database. A message confirms the setup has been successful.
6. Restore the backup of the appliance configuration you took prior to configuring clustering.
7. Select **Home > Status** to ensure that appliance is fully set up.

## Configure the Appliance on the Initial Cluster Node

The following appliance settings from the initial cluster node are shared between appliances in the cluster:

- DNS server settings
- Certificate settings
- Database configuration settings
- NTP server settings
- Web client enabled state

- DSCP setting
- Toggle Web Client setting
- HTTP Access setting
- Syslog settings
- Kerberos settings
- License details

It is recommend that once you have enabled clustering and set up the database on the first node, you configure the appliance settings or restore a backup with the required settings configured. When further nodes are added to the cluster, the appliance settings are automatically applied.



Application settings, such as Map Points, are not automatically moved to the SQL server when database settings are updated. A backup of the required settings must be restored to seed these settings in the database when switching from a configured local setup to a clustered one.

## Check the Load Balancer Status

1. Select **Configuration > Advanced**.
2. Locate the Load Balancer Status section.

▼ Load Balancer Status

Status URL: <http://dn-fig-01.qauk.com:8001/status>

**Enable maintenance mode**

When this setting is enabled the server is temporarily removed from the load balancer pool. This setting has no effect unless the load balancer environment is configured to monitor the status URL.

3. Click the Status URL link to check the health status of a server in a load balanced environment. A status page is displayed showing one of the following:
  - Success - The server is functioning correctly within the load balancer pool.
  - Failure - The server is either offline or is not functioning correctly within the load balancer pool.

## Configure Additional Cluster Nodes

Once you have successfully configured the initial cluster node, configure all the nodes you want to be part of the cluster.

1. Boot up the appliance for the node you are adding to the cluster.
2. Log in to the Admin Console for that node and [Upload a License File](#).

3. On the appliance text console, press **F2** and logon.
4. Select **Cluster Configuration** and press **Enter**.
5. Enter the name of the cluster. This must be the name you entered when setting up the initial cluster node.
6. If you are not using the standard port number (49152), enter the port number you are using for your cluster.
7. Press **F10** to save the cluster configuration.
8. If you have already performed configuration via other nodes of the cluster, the settings are automatically updated to any new nodes in the cluster and thereafter should automatically remain synchronized through updates when any setting changes.

To confirm clustering is operating correctly, logon to the web admin for the node and make a simple change, such as changing the DNS settings. When you log into another node in the cluster, the same change should be apparent.

9. Repeat this process for every new node that you add to the cluster.

## Manage a Cluster in the Admin Console

If clustering is enabled on the appliance, you can check the status of the nodes in your cluster, apply a patch to your cluster, update, and shutdown nodes.

### Patch Server

By nominating one of the nodes in a cluster as the Patch Server, you can apply patches to all nodes in the cluster. Any active node in a cluster can be used as the patch server.

To make a node the patch server, log into the web admin console for a node that is not currently the patch server, select **Cluster > Status** and click **Promote to Patch Server**. The current node is now identified as the patch server.

Cluster Status	Host	IP Address	Action
 Active v4.0.0.54	dn-play-01 (this) (Patch Server)	10.0.32.211	Reboot



## Status

[Status](#)   [Update](#)   [Database](#)






---

**Status**

Cluster details **dn-play:55555**

DataNow Server Version **4.0.0.56**

Current Patch Server **dn-play-01 (10.0.32.211)**



Cluster Status	Host	IP Address	Action
 Active v4.0.0.56	dn-play-05 <i>(this)</i>	10.0.32.215	<input type="button" value="Reboot"/>
 Active v4.0.0.56	dn-play-01 <i>(Patch Server)</i>	10.0.32.211	<input type="button" value="Reboot"/> <input type="button" value="Shutdown"/>
 Active v4.0.0.56	dn-play-04	10.0.32.214	<input type="button" value="Reboot"/> <input type="button" value="Shutdown"/>
 Active v4.0.0.56	dn-play-03	10.0.32.213	<input type="button" value="Reboot"/> <input type="button" value="Shutdown"/>
 Active v4.0.0.56	dn-play-02	10.0.32.212	<input type="button" value="Reboot"/> <input type="button" value="Shutdown"/>


The status shows the name of the cluster, the File Director server version, and which node in the cluster is currently the patch server.

If a patch server has not been set, these details are not displayed.

## Cluster Status

The state of each node in the cluster is denoted by the icon displayed in the Cluster Status column.

Icon	Meaning
	<p><b>Active</b> The node is online and using the correct File Director server version, determined for the cluster by the version applied to the patch server.</p>
	<p><b>Warning</b> This can signify one of the following states:</p> <p>A patch server has not been set. Set one of the nodes as the patch server.</p> <ul style="list-style-type: none"> <li>The node's File Director server version is different to that of the patch server. Reapply the current patch to the cluster. This updates only those nodes that are not at the File Director server version applied to the patch server. Nodes already at the correct version are unaffected by the update.</li> <li>The node requires a reboot. Click the Reboot button for the node.</li> </ul>

Icon	Meaning
	<ul style="list-style-type: none"><li>• Component information cannot be retrieved.</li></ul>
	<b>Inactive</b> The node is offline.

## Host

Displays the name of each node in the cluster, identifies which node is the patch server, and which node you are currently accessing through the web admin console. Click on a name to see details of the current component versions of that node and its patching history. The name of the current node and the patch server are annotated appropriately.

## IP Address

The IP address of each node in the cluster.

## Action

In the web admin console for any node in the cluster, use the buttons in the Actions column to reboot or shutdown any other node in the cluster. If a node is inactive, it can be removed from the list using the corresponding button. If a removed node restarts, it will automatically re-display in the list.

## Update

**Status**

Cluster details **Fig:49152**

File Director Server Version **4.2.1.5**

Current Patch Server **dn-fig-01 (10.0.35.80)**

**Upload Patch**

No file chosen

---

**Updates** - select an update to deploy or show details

Name	File Director Server Version
DataNow 4.1.0.77	4.1.0.152
DataNow 4.1.0.79	4.1.0.166
DataNow 4.1.0.80	4.1.0.166
Security Update 5	Unknown
DataNow 4.1.1.89	4.1.0.179
DataNow 4.1.2.120	4.1.2.29
DataNow 4.1.2.123	4.1.2.29
DataNow 4.2.0.20	4.2.0.64
File Director 4.2.0.24	4.2.0.71

The Update screen displays cluster name, File Director Server Version and which node is the current patch server. All patches that have previously been uploaded are listed in the Updates area.

## Apply a Patch to a Cluster

This process explains how to apply a patch to all nodes in a cluster. To apply a patch when clustering has not been enabled, see [Apply a File Director Patch](#).



Before applying any update to File Director you are advised to take a backup or snapshot of your virtual machine(s), your database, and the appliance configuration. See "Backup and Restore" on page 32

We recommend appliances are forced offline via the maintenance mode flag (or manually via the load balancer) and brought back online following the patching process. This is stop any traffic from the load balancer.

You can apply a patch to a cluster using any nodes as long as one of the nodes in the cluster is the patch server. To make the current node the patch server, select **Cluster > Status** and click **Promote to Patch Server**.

Log in to the web admin console on any node in the cluster.

1. Select **Cluster > Update**.
2. In the Status section, details of the current patch version are displayed.
3. Click **Choose File** and navigate to a File Director patch file.
4. Click **Upload**.

The patch is displayed in the Updates section of the screen along with all patches that have been previously uploaded.

Select a patch and click **Delete** to remove it from the list and from the patch server.

5. Select the row in the table of the required patch and click **Deploy Update**.  
To see the components and release notes for a patch, click the patch name.

### **Note: 2018.3 Patch**

Periodically, large patches are issued containing multiple component updates and upgrades to the OS. The 2018.3 patch is an example. Before installing the 2018.3 patch be aware it will require a system reboot several times during the update process. In addition, it is essential you perform recommended backups, as in some circumstances you will need to re-import the appliance snapshot after the update process has completed. For further information on installing the 2018.3 patch, see <https://community.ivanti.com/docs/DOC-70692>

### **Applying Updates - Additional Information**

- Updates are applied in parallel to all components across the cluster that are not the same version as the patch.
- Nodes may require a reboot following an update - follow the instructions displayed.
- Nodes that are offline are not updated and display with a warning icon in the Status screen. Reapply the patch when the node is online to update its components. This does not affect any nodes that have already been updated.
- The progress of the update is displayed and you are informed when the update is complete.
- Depending upon the File Director version you are upgrading from, you may be required to restore your appliance configuration from the pre-upgrade backup. See "Backup and Restore" on page 32.
- Disable maintenance mode on each appliance and test client connections to File Director.

## **Maintenance Mode**

Maintenance mode status is recommended for appliances before starting the patching process as a database schema upgrade may be required. This is performed by the first node to be upgraded. From this point on, all older nodes are blocked from communicating with the database, which causes their health monitors to fail and be marked as offline by the load balancer. Client device session tokens (logon states) are held in appliance memory. When the cluster is patched, these are lost, which means that the clients need to reauthenticate on their next connection with the appliance (generally within 30 seconds unless notification checks are disabled). Because all this traffic will be directed at the first single updated appliance that shows as online to the load balancer, the resultant traffic could saturate this appliance and result in an unbalanced configuration.

# Kerberos Authentication

## Prerequisites for Kerberos Authentication

---



These prerequisites are only required for configuring Windows Client Kerberos SSO.

---

In order to use Kerberos authentication against the File Director appliance, Active Directory needs to be configured with a user that allows:

- A. The Kerberos keytab to be acquired from a user account so the server can trust the authorized user to access it.
- B. Preauthentication checks.
- C. Kerberos Ticket Granting services, which are part of Active Directory, to determine the 'service principal' used to access the File Director appliance and obtain a ticket to establish an authorized connection to the File Director appliance.
- D. The re-use of service tickets sent to the platform so that the service can access data upon the user's behalf (Kerberos Unconstrained Delegation). This is required if setting up Kerberos on the client.

To perform the setup, complete the following steps:

1. Create a user account in Active Directory for this purpose and set a password to be used by the appliance to perform actions A and B. It is recommended that this account is not an admin account.



To ensure the correct default domain is used, the username for this account must include the relevant realm name. The required format is `username@REALM`, for example, `bsmith@FILEDIRECTOR.LOCAL`. The realm must be entered in uppercase.

---

2. Set the account so that the password cannot be changed and never expires. This is recommended because it removes the need to reconfigure the platform to use new credentials.
3. Ensure DNS references the File Director server and always use the full DNS name to access the File Director server in the future.

DNS should be an A record that points to either the File Director appliance or, in the case of a clustered environment, the NLB VIP. A CNAME record can be used by clients as the server address, but the SPN must be registered against the A record.

4. Take the DNS name and use the `setspn` tool from a domain controller to add HTTP Kerberos service principals that match the DNS name to the user account.

For example, if the user account is called 'fdpreauth' and the DNS name that will be used to access the user account is 'fd.mycompany.com', issue the following `setspn` commands on a domain controller and ensure they run error free:

```
setspn -S http/fd.mycompany.com fdpreauth
```

---



If the client endpoints point to a DNS CNAME address that references an A record, the SPN needs to be registered against the A record rather than the CNAME.

---

Following step 4, a new **Delegation** tab appears in Active Directory Users and Computers associated with the user account. This tab is used to allow the Kerberos Ticket Granting server in AD to locate the key information associated with the user account and allow a token to be returned to the client system to access the File Director appliance.

5. Select the **Delegation** tab for the preauthenticated user and select **Trust this user for delegation to any service (Kerberos only)**. The File Director appliance has authorization to use the Kerberos ticket forwarded to it by the File Director client or web browser so that it can reuse the user identity to access file service resources.
- 



The process describes how to configure File Director for Kerberos Unconstrained Delegation. If you are using Credential Guard on a Windows 10 client, you need to configure [Kerberos Constrained Delegation](#).

---

## Configure Kerberos in the File Director Admin Console

This process describes how to configure the File Director Admin console for Kerberos authentication.

## Kerberos Realm

1. In the File Director Web Admin console, select **Configuration > Kerberos**.
2. Click **Add Realm**.

The Add/Edit Kerberos Realm dialog displays.

### Add/Edit Kerberos Realm

Update the domain and Key Distribution Centre (KDC) for this Kerberos realm.  
The KDC should be specified using its Fully Qualified Domain Name.  
The backup KDC is optional.

<b>Domain:</b>	<input type="text" value="dnroot2.local"/>
<b>PRIMARY KDC:</b>	<input type="text" value="dnroot2dc1.dnroot2.local"/>
<b>BACKUP KDC:</b>	<input type="text" value=""/>

3. In the **Domain** field, enter the default domain name.
4. Enter the fully qualified domain name of the domain Key Distribution Center (**Primary KDC**). This is usually the same DNS as the Active Directory controller.

If you are unsure of the KDC name, use `nslookup _kerberos._tcp.<domainFQDN>` from a domain-joined client to get the IP of the KDC. The use `ping -a <ip address>` to get the name of the KDC.

Optionally, enter the domain name of your **Backup KDC**.

In the event that your primary server is offline, the appliance will automatically use the backup for Kerberos authentication.



- Click **OK**.

Details of the realm are added to the Kerberos section of the screen. The name of the realm is automatically added. Realm names are case sensitive and are usually the same as the domain name in upper-case letters.

**▼ Kerberos Realms**

To use a Kerberos connection to the SMB storage or to use Kerberos SSO, enter details of your Kerberos realm(s).

Name ▲ <sub>1</sub>	KDC	Default Domain
DNROOT2.LOCAL	dnroot2dc1.dnroot2.local	dnroot2.local

- Repeat steps **2** to **6** for all relevant realms. This ensures successful authentication to all shares added as map points.
- Click **Save**.

## Kerberos Token Size

Set the maximum token size for users in your environment. The default value is 12k and this can be increased up to 64k to accommodate users with large tokens.



Setting the token size too large can have a effect on performance. For more information about checking the size of tokens, see [blogs.technet.microsoft.com/askds/2007/11/02/whats-in-a-token/](https://blogs.technet.microsoft.com/askds/2007/11/02/whats-in-a-token/).

**▼ Kerberos Token Size**

If using Kerberos SSO and your users have large Kerberos Tokens, set the maximum Kerberos Token size to accommodate the appropriate token size for your environment.

**Maximum Token Size:**

## Kerberos Preauthentication

This setting is required when configuring encryption for Kerberos from the client. A preauthentication user is not required for username and password authentication.

Select **Configuration > Kerberos**.

In the **Kerberos Preauthentication** section, enter the username and password for the preauthentication user. The username can be entered as *username* or *username@REALM*. Where the realm is used, it must be in upper case - for example, *bsmith@FILEDIRECTOR.LOCAL*. This is the preferred format where multiple domains are configured.



Only one preauthentication user can be added. See the [prerequisites](#) for details about setting up this user.

▼ Kerberos Preauthentication

Credentials for the user account that enables the Kerberos keytab to be acquired, allowing authorised users access to the File Director server.

**Preauth User:**

**Preauth Password:**

## Kerberos Constrained Delegation

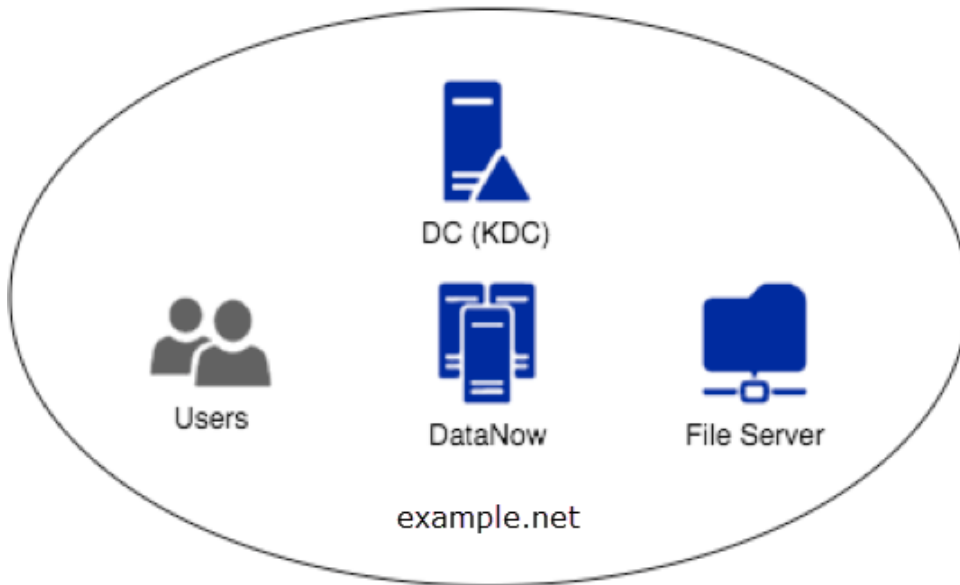
Credential Guard was introduced in Windows 10 Enterprise and uses virtualization-based security to isolate NTLM password hashes, Kerberos Ticket Granting Tickets, and credentials stored by applications as domain credentials - all so that only privileged system software can access them. File Director supports cross-realm Kerberos constrained delegation, where users/endpoints are in different domains to the storage and preauthentication account.

If Credential Guard is enabled on a Windows 10 client, users' ticket granting ticket is not forwarded to the File Director server and the File Director server fails to authenticate the user. Enabling Kerberos Constrained Delegation allows the File Director server to create a ticket on behalf of the user. Preauthentication accounts must use constrained delegation with any protocol, to enable Windows server support for MS-S4U.

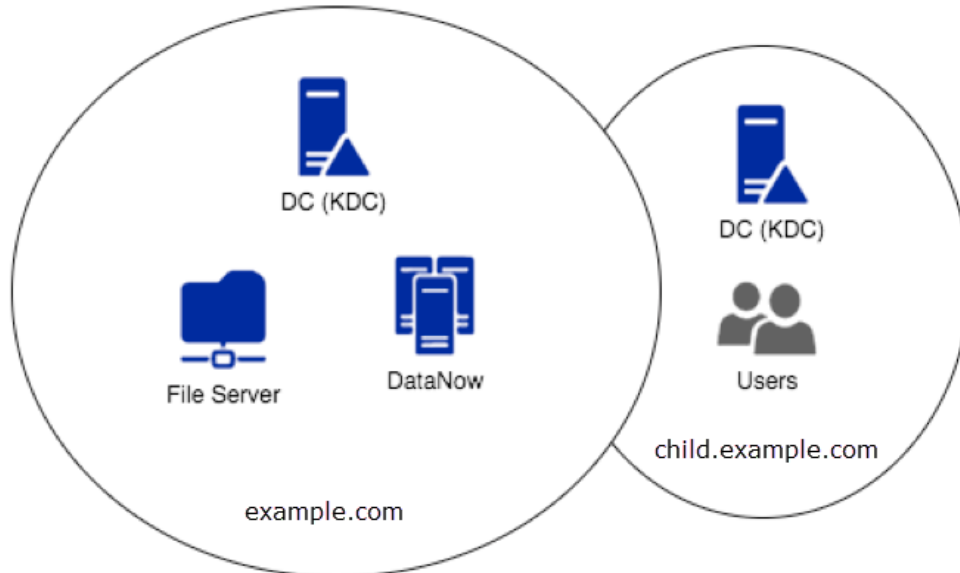
## Environments

Kerberos Constrained Delegation has been tested in the following environments:

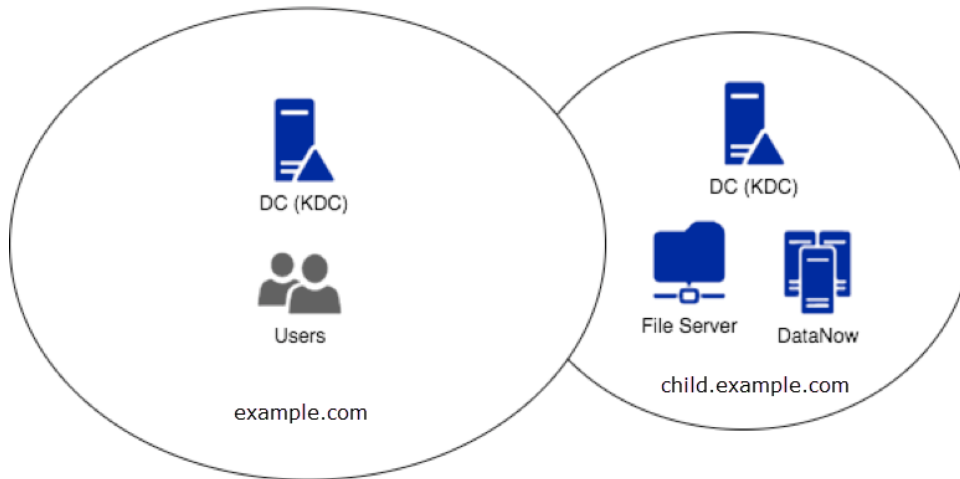
**Users, endpoints and preauthentication account and storage in the same domain**



**Users and endpoints in example.com, file servers and preauthentication in trusted child domain child.example.com**

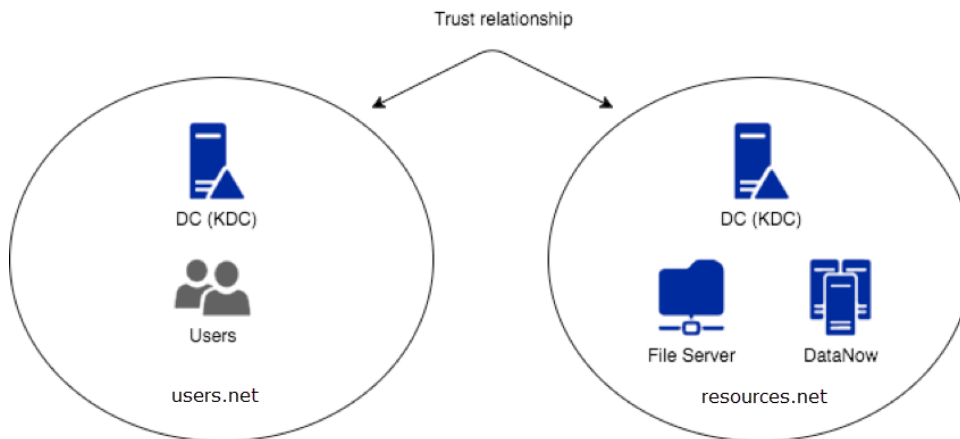


## File servers and preauthentication example.com with users and endpoints in trusted child domain child.example.com



## Users and endpoints in forest users.net with file servers and preauthentication account in forest resources.net

For the configuration below, Active Directory must be setup in a 2-way transitive forest trust to allow Kerberos tickets to be utilized across realms.



## Installing Credential Guard to support Kerberos Constrained Delegation

### Pre-requisites

- Microsoft require that the domain/forest functional level be at least 2003 in order to support Protocol Transition.

- If the users and resources are in different forests, there must be a 2-way transitive forest trust configured. The Forests should be configured to support Kerberos constrained delegation/protocol transition. This may require the deployment of a Forest search order policy if not already present - see [Configure Kerberos Forest Search Order \(KFSO\)](#).
- If the users and resources are in different domains, there must be a 2-way transitive trust relationship established.
- The maximum Kerberos token size must be ascertained and configured in the admin console. For more information, see [blogs.technet.microsoft.com/askds/2007/11/02/whats-in-a-token/](https://blogs.technet.microsoft.com/askds/2007/11/02/whats-in-a-token/)



base64 encoding adds around a third extra overhead to the actual size of the token - be sure to allow for this when configuring the maximum size.

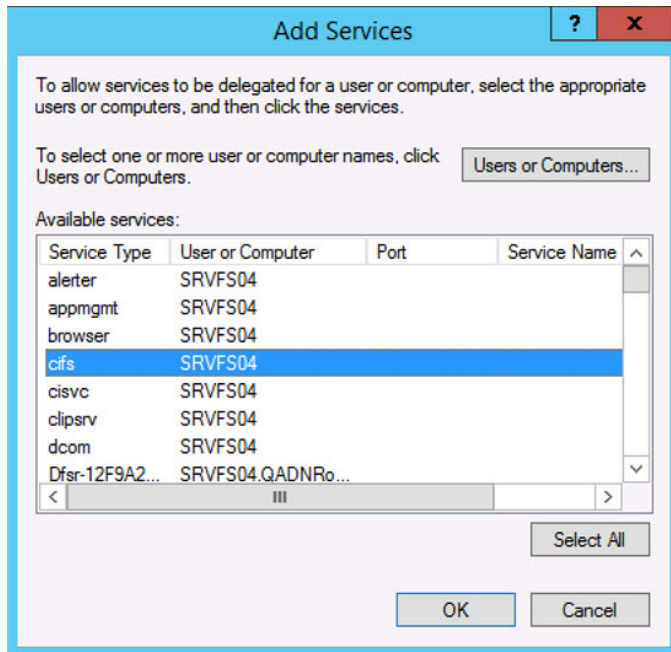
---

- Clock accuracy must be ensured on endpoints, appliances (see admin guide for configuring NTP), File servers and domain controllers
- the SPN (Service Principal Name) used by File Director clients must point to a DNS A record, not a CNAME
- Kerberos AES128 encryption must be allowed in KDC policy (as per default)
- Endpoints must have connectivity to a domain controller as well as the File Director appliance to acquire a service ticket
- File Director server version must be 4.2+

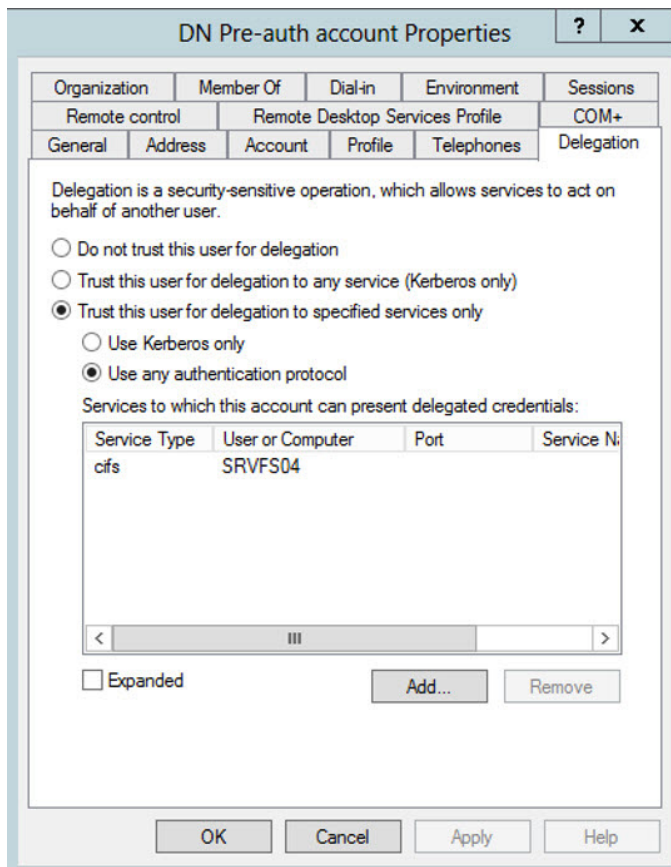
## Configuring Kerberos Constrained Delegation for File Director Preauthentication Account

1. Locate your preauthentication account in Active Directory Users and Computers.
2. From the preauthentication account properties, select the **Delegation** tab.
3. Select **Trust this user for delegation to the specified services only** to enable the associated options.
4. Select **Use any authentication protocol**.
5. Click **Add** to select the resources you wish to access using Kerberos constrained delegation
6. Click **Users or Computers** button to allow you to search AD.
7. Select the computer account for the file server you want to access. If you have multiple file servers, select all of them.

- In the Service Type field for the server, select **cifs**.



9. Click **OK**.



10. Click **Apply**,

Your File Director preauthentication account is setup for Kerberos Constrained Delegation to access the selected servers.

# Advanced Configuration

The advanced options are used to set DSCP QoS options and to create and restore configuration backups. Select **Configuration** > **Advanced** to access the Advance options.

## In this section:

### DSCP QoS Configuration

▼ DSCP QoS Configuration

Stays the same (link layer and routing protocol keep alive)

Stays the same (used for IP routing protocols)

Express Forwarding (EF)

Class 4

Class 3

Class 2

Class 1

Best effort (QoS disabled)

This setting is only required if your organization uses Differentiated Services Code Point (DSCP) settings to help manage its network traffic.

The setting must be applied to in accordance with your organization's networking requirements. Your network team will be able to advise which setting to apply.

In the DSCP QoS Configuration area of the Advanced options, select the required configuration and click **Update**.

### HTTP Access

▼ HTTP Access

**Enable access over HTTP**

**This should only be used in a load balanced environment or with an SSL offload appliance.**

In the HTTP Access area of the Advanced options, configure the required setting and click **Update** to apply.



This option should only be used to enable connection by HTTP in a load balanced environment or with an SSL offload appliance.

## TLS 1.0

▼ TLS 1.0 (for legacy clients)

**Enable TLS 1.0**

To comply with PCI compliance, TLS1.0 is not enabled by default. Enabling TLS1.0 allows legacy clients that do not support TLS1.1 or TLS1.2 to connect to File Director.

Note: enabling TLS1.0 does not disable TLS1.1 or TLS1.2 access

Update

PCI compliance requires SSL v3/TLS 1.0 to be disabled in File Director. Configuring endpoints to default to a secure protocol (TLS 1.1 or TLS 1.2) requires the implementation of registry settings and potentially an update. Customers that are unable to implement this change can now toggle TLS 1.0 on in File Director 4.2.



For more information, see this Microsoft support article [3140245](https://support.microsoft.com/3140245).

Select **Configuration > Advanced** and apply the **Enable TLS 1.0** option as required.

When enabled, this is done across the whole cluster.

Ivanti recommends turning off TLS 1.0 support as soon as all legacy endpoints in the environment are updated or replaced.

## NTP

▼ NTP

Configure upto three NTP servers

Click 'Reset' to use the default settings

0.pool.ntp.org

1.pool.ntp.org

2.pool.ntp.org

Update Reset

Add the server addresses or FQDNs of the NTP servers you want to use. File Director is configured with the addresses of three default NTP servers. If you use your own NTP servers, replace the default addresses with the addresses of your own. You can use a maximum of three NTP servers and a minimum of one.

## Load Balancer Status

▼ Load Balancer Status

Status URL: <http://dn-fig-01.qauk.com:8001/status>

**Enable maintenance mode**

When this setting is enabled the server is temporarily removed from the load balancer pool. This setting has no effect unless the load balancer environment is configured to monitor the status URL.

Click the Status URL link to check the health status of a server in a load balanced environment. A status page is displayed showing one of the following:

- **Success** - The server is functioning correctly within the load balancer pool.
- **Failure** - The server is either offline or is not functioning correctly within the load balancer pool.

## Enable Maintenance Mode

Select **Enable Maintenance Mode** to temporarily take the server offline. The server is no longer available in the load balancer pool and cannot be communicated with. This allows any necessary maintenance and configuration tasks to be completed. Whilst the server is in Maintenance Mode, the status of the server shows as 'failure'.

De-select **Enable Maintenance Mode** to make the server available in the load balancer pool once again.

## SMB Storage Authentication

▼ SMB Storage Authentication

Specify the authentication method used by the DataNow appliance to connect to the SMB storage.

**Method:**

NTLM  
 Kerberos

Set the authentication method used by the File Director appliance to connect to the SMB Storage - NTLM or Kerberos.

If you select **Kerberos**, you must configure the Realm and Key Distribution Center (KDC) settings in the Kerberos page.

## SMTP Configuration

▼ SMTP Configuration

<b>SMTP Server Hostname/IP:</b>	<input type="text" value="smtp.demolab.com"/>
<b>SMTP Server Port:</b>	<input type="text" value="25"/>
<b>Encryption Type:</b>	<input type="radio"/> TLS <input checked="" type="radio"/> SSL <input type="radio"/> None
<b>From Address:</b>	<input type="text" value="administrator@demolab.com"/>
<b>Send test email to:</b>	<input type="text"/>
<b>Requires Authentication:</b>	<input checked="" type="checkbox"/>
<b>Username:</b>	<input type="text" value="administrator@demolab.com"/>
<b>Password:</b>	<input type="password" value="••••••••"/>

Set up SMTP to use the required account for initiating Link Based Sharing emails.

The server URL, provided in the client's request, is used to create the link included in emails to users. The File Director server URL configured for your company's appliances must be accessible externally.

1. Select **Configuration > Advanced**.
2. In the SMTP Configuration section, enter the details of the SMTP server and email address:
  - Hostname or IP address of the SMTP server
  - SMTP server port number
  - Encryption type to use when sending emails
  - The email address to send emails from
  - Email address to receive test email
  - Indicate if authentication is required and, if so, provide the username and password
4. Click **Update**.

## Syslog Server

▼ Syslog Server



File Director uses Transmission Control Protocol (TCP) to output syslog rather than User Datagram Protocol (UDP).

---

1. Select **Configuration** > **Advanced** and scroll down to the Syslog Server section of the screen.
2. Enter the IP address of the remote syslog server and click **Update**.

# Policy

Configure a range of settings to determine how File Director is used in your organization and by whom. There are four categories of policy rules in File Director. Select **Policy** and the required category:

- [Global Policy](#) - Set restrictions on platform, IP address, timeout and login attempts that apply to all your users.
- [Mobile Policy](#) - Configure a range of settings to dictate how File Director behaves on mobile devices.
- [Map Point Access Policy](#) - Define policy settings unique to each map point allowing different sets of rules to match the requirements of different users and groups of users.
- [Users and Devices Policy](#) - Verify new users and devices and manage their access. Users and devices can be remote wiped and unlocked if required.


## Global Policy






Set restrictions on platform, IP address, timeout and login attempts that apply to all your users.

In the admin console, select **Policy** > **Global** and click **Edit**. When all required changes have been made, click **Save**.

## Client Access

▼ Client Access



<input checked="" type="checkbox"/>		Enable Windows client access
<input checked="" type="checkbox"/>		Enable Mac client access
<input checked="" type="checkbox"/>		Enable iOS client access
<input checked="" type="checkbox"/>		Enable Android client access
<input checked="" type="checkbox"/>		Enable Web client access

The Global options above will prevent **all logins** from that platform. This cannot be overridden at the map point level.  
To restrict platform access for some map points but not others, set policy at the [Map Point Policy](#) level instead.

Specify which platforms can log on to File Director on your server. Set the policy for each platform to **On** or **Off** as required.


Platform restrictions can also be set for individually for each Map Point. Global restrictions take precedence over those set at Map Point level - if you disable a platform at the global level, it is disabled for all users regardless of the setting on their Map Point.

The table below illustrates this behavior.

Platform	Global	Map Point	Effect
Windows	On	On	Users for that Map Point can access the File Director server through Windows.
Mac	On	Off	Users for that Map Point cannot access your server on a Mac as the Global setting is overridden.
iOS	Off	Off	Users cannot access your server on an iOS device regardless of their Map Point.
Android	Off	On	Users cannot access your server on an Android device regardless of their Map Point as the Map Point setting is overridden.

## IP Address Login Restrictions

▼ IP Address Login Restrictions



Allow logins to File Director from the following IP ranges ONLY:

222.12.144.220-255


Enter each IP range on a separate line in IPv4 format.  
 Use a dash character "-" to specify a range of values, for example: 222.12.144.220-255 or 12.144.33-35.0-128  
 Use an asterisk character "\*" to specify a wildcard (all values 0-255) such as: 12.45.\*.\* or 192.77.196.\*

Specify which IP addresses can access your File Director server using the following formats:

- Enter each IP address on a separate line in IPv4 format.
- Specify a range of values using a dash. For example, 222.12.144.220-255.
- Use an asterisk to specify denote a wildcard - any value between 0 and 255. For example, 222.12.144.\*

## Failed Login Attempts

▼ Failed Login Attempts



Policy has been successfully updated.

ON

Lockout user for **15 minutes** after **5** consecutive failed login attempts  
 (Locked out users can also be manually "unlocked" in the [Users & Devices](#) section.)

ON

Wipe all locally stored files after **10** consecutive failed login attempts.

Set the number of consecutive failed login attempts before a user is locked out for the specified time period.

You can also specify the number of consecutive failed login attempts before locally stored data is wiped from the desktop or device.




If an account is wiped in this way, the user is put on the Remote Wipe list for the web platform which prevents the user from all web login attempts.

It is therefore recommended that you do not set the failed login attempts before wiping data at a very low figure (less than five).

This policy works differently for mobile devices where the PIN check occurs on the local device, not the server. There is no lockout for PIN attempts but if the Remote Wipe setting does apply - if the number of PIN attempts exceeds the Remote Wipe Failed Login Attempts number, the local device is wiped of all data and stored login credentials, including the PIN.

## Sharing

▼ Sharing



Policy has been successfully updated.

Shares will automatically expire after **30** days

ON (Note: this policy applies to newly created shares and will not retroactively change the expiration date of existing shares.)

Set the length of time, in days, that files are available to recipients when shared by a link. If you do not require a time limit for a share, set to **Off**.

When updating this setting, changes only apply to newly created shares - existing shares adhere to the setting which was applied when the share was created.



The figure set here is also the number of days a share is extended by when an expiry date is extended.


## Mobile Policy

Configure a range of settings to dictate how File Director behaves on mobile devices.

In the admin console, select **Policy** > **Mobile** and click **Edit**. When all required changes have been made, click **Save**.

## Client Security

▼ Client Security



ON Store the user's encrypted password in the mobile device keychain.  
If enabled, user may use a PIN for authentication instead of a password.  
If disabled, the user must enter their password each time they launch the File Director app.

Users **must** enter a PIN each time the File Director app launches or returns to the foreground

ON User must re-enter their password after **30 minutes** of inactivity

The following security policies are available:


- Set whether user's encrypted passwords is stored in the mobile device keychain.
  - **On** - Users can use a PIN for authentication instead of a password.
  - **Off** - Users must enter their password each time they launch the File Director app.

If this policy is enabled, a further option is available - **Require PIN authentication check every time File Director app launches to the foreground**. If this policy is applied, users must enter their PIN each time the File Director app launches or returns to the foreground.

- Set whether users must enter their password after a defined period of inactivity. This can be in minutes, days.

## Data Security

▼ Data Security



ON Wipe downloaded files as soon as they are not being actively viewed.

ON Allow downloaded files to be opened by other apps.  
(Files opened in other apps could be printed or saved in non-encrypted format.)

ON Allow copy/pasting from the File Director app to other apps.

ON Allow file uploads, including 'open in' from other apps into File Director.

Set the File Director behavior for downloaded files using the buttons to configure the following:

- **Wipe downloaded files** - Only stores files whilst they are in the foreground on a device. When the file is no longer in the foreground, the local copy is deleted from the device or endpoint.
- **Allow downloaded files to be opened by other apps** - Files downloaded from the File Director app can be opened in other apps. This can potentially compromise security as files opened in other apps may be able to be printed or saved in a non-encrypted format.
- **Allow copy/pasting from the File Director app to other apps** - Protect your organization's sensitive information by disabling copy and paste from File Director apps.



- **Allow file uploads** - Select whether users can upload files from their mobile devices to your File Director server. When this option is set to On, it enables and disables the 'Open in' feature from other apps to File Director. If this option is turned off, all downloaded files are read-only and users cannot upload files to your File Director server.

## Map Point Policy

Create and maintain policies, platform and file sharing options for map points. A policy can be created to define permissions for users connected to the map point. Further policies can be defined to set different permissions for individual users, Organizational Units (OU) and User Groups.

In the example below, one policy has been created for Admin Users and one for all other users. Admin Users can only connect to the server on verified devices whilst for all other users connected to the map point, all data is read-only. These policies apply concurrently on the map point.

The screenshot displays two overlapping configuration windows for a map point. The top window is for 'All Users' and the bottom window is for 'Admin Users'. Both windows show a 'Policies for' section with toggle switches and a 'Platform Access' section with checkboxes and icons.

**Home** Change connection string for this map point Save Cancel

**All Users**

Organizational Units: Add

Admin Users

**Policies for All Users :**

ON Force read-only (files may not be modified).

OFF Only allow VERIFIED devices to connect.

**Platform Access:**

**Home** Change connection string for this map point Save Cancel

All Users

Organizational Units: Add

Admin Users

User Groups: Add

No User Group policies have been set.

**Policies for Admin Users :**

OFF Force read-only (files may not be modified).

ON Only allow VERIFIED devices to connect.

**Platform Access:**

ON Allow Windows Access

ON Allow Mac Access

## Edit Map Point Access

1. Select **Policy > Map Point Access**.



Map Point Access policy settings can also be accessed directly from the link in the corresponding map point connection string configuration - **Configuration > Map Points**.

2. Click **Edit**.
3. Click **Add** to create the policy you want to define:
  - **Organizational Units** - Find the OU you want to add and click **Select**.
  - **User Groups** - Find a user group and click **Select**.
  - **Individual Users** - Find a user and click Add by the users you want to set a policy for.
4. Select an OU, User Group, Individual user or select **All Users** to apply settings to everyone who uses that map point.

5. Configure the required settings:
  - **Force read-only** - Users cannot modify or upload File Director files.
  - **Only allow VERIFIED devices to connect** - Only those devices which have been approved by the administrator can connect to the File Director server.
  - **Platform Access** - Set which devices users can use to for this Map Point. Platform Access can also be set globally which can conflict the Map Point policy settings as show by the examples in the table below.

Platform	Global	Map Point	Effect
<b>Windows</b>	On	On	Users for that Map Point can access the File Director server through Windows.
<b>Mac</b>	On	Off	Users for that Map Point cannot access your server on a Mac as the Global setting is overridden.
<b>iOS</b>	Off	Off	Users cannot access your server on an iOS device regardless of their Map Point.
<b>Android</b>	Off	On	Users cannot access your server on an Android device regardless of their Map Point as the Map Point setting is overridden.

- **Link Based Sharing** - Select whether the type of access internal and external users can have - either read-only or collaborative. Link based sharing can also be disabled.

6. Click **Save**.

These settings are applied to the users connected to the File Director server who and match the defined criteria.

## Users and Devices Policy

The Users & Devices page enables you to keep track of your users and their devices. The page shows you the users that have logged on to File Director and displays details of each device on which they have installed File Director. You can see the ID, type and status of all devices and have the option to verify any unverified devices. You can also remote wipe and unlock users and devices if necessary.

## Search for Users and Devices

User/Device Status:  Platform Type:

User Name Matches:

<input type="checkbox"/> User Name	<input type="checkbox"/> Device Info	Type	Status	Client Version	Last Activity
<input type="checkbox"/> Paul1@Root2.local	<input type="checkbox"/> c37b7bd2b9c1406...	iOS	UNVERIFIED	3.5.0	1 hour ago
	<input type="checkbox"/> a246ee63e0d0457...	iOS	VERIFIED	3.5.0	7 hours ago
	<input type="checkbox"/> ebf20dee686c408...	iOS	UNVERIFIED	3.5.0	18 hours ago
	<input type="checkbox"/> c2d36e7f6908489...	iOS	VERIFIED	3.5.0	1 day ago
	<input type="checkbox"/> 3861fc969d37401...	iOS	VERIFIED	3.5.0	3 days ago
	<input type="checkbox"/> 6cd61f83a8cc49b...	iOS	UNVERIFIED	3.5.0	4 days ago

1. Select the **Policy** tab and click **Users & Devices**.
2. Select the required filters and enter your search criteria using the following filters:
  - **User/Device Status** - Display those users or devices at a particular status. For example, you might want to find all users who have been locked out or all unverified devices. Available options are:
    - **All Users and Devices**
    - **Remote Wipe List Devices**
    - **Non-Remote Wipe Devices**
    - **Locked Out Users Only**
    - **Non-Locked Out Users**
    - **Verified Devices Only**
    - **Unverified Devices Only**
  - **Platform Type** - Refine your list of devices by selecting a particular platform. For example, you might only want to view Android devices or Web Client sessions.
  - **User Name Matches** - Perform a search on full or part user names.
3. Click **Show Users/Devices** to update your user/device list using the filter and search settings.

## Manage Users and Devices

1. Select a user(s) and/or device(s) - each user and device has their own checkbox.
2. Click the required action:
  - **Remote Wipe User/Device** - All File Director files are removed from the selected device or, if a user is selected, from all of their devices. This is useful for ensuring sensitive data is not left on a lost or stolen device or on the devices of someone who has left your organization. If a user is logged in at the time of the wipe, their next action on the device automatically returns to the login screen. The current session is invalidated and any login attempts are rejected.
  - **Unlock User/Device** - If a user has had too many unsuccessful login attempts, their account is temporarily locked as defined in the Failed Attempts policy. Once unlocked, the failed login counter is reset.
  - **Verify Device** - Any device that logs in for the first time is considered unverified until an admin manually approves/verifies the device in the File Director appliance. Once verified, a device is added to the verified category and can only be removed following a remote wipe.

The action is performed for the selected devices and/or users.

# Auditing

The File Director appliance supports sending audit and usage data to a single remote syslog server over a TCP connection. The File Director server requires the IP address and port of a remote syslog server. Only IP addresses are supported as DNS can be unreliable.

The syslog message contains JSON encoded data which can be indexed by software, such as Splunk, to provide reporting and analysis. The facility levels in syslog distinguish between usage and audit log data as follows:

Level	Data
local2	audit data
local3	usage data

All messages are sent at the informational severity level.

## Configure a Remote Syslog Server in File Director

1. Select **Configuration** > **Advanced** and scroll down to the Syslog Server section of the screen.
2. Enter the IP address of the remote syslog server and click **Update**.

## Set up a Remote Syslog Server

The syslog server must be configured to listen on a TCP port for it to work with File Director. The following steps instruct you how to do this using either Rsyslog or Splunk.

### Rsyslog

The standard syslog service included in Ubuntu Server is Rsyslog.

1. Create a File Director configuration file in the `/etc/rsyslog.d` folder called `10-dnsyslog.conf`.
2. Add the following lines to `10-dnsyslog.conf` to listen for TCP traffic on port 10514:
 

```
# provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 10514
```
3. To filter out the File Director messages to separate log files you must create a directory `/var/log/datanow` and ensure that the syslog daemon has permission to write to that directory.

4. Add the following lines to 10-dnssyslog.conf to redirect the File Director messages and stop them appearing in the normal syslog files:

```
local2.* /var/log/datanow/audit.log
&~
local3.* /var/log/datanow/usage.log
&~
```

5. Restart the syslog server to pick up changes using the following command:

```
service rsyslog restart
```

## Splunk

For instructions on how to set up Splunk to monitor File Director syslog files, see <https://community.ivanti.com/docs/DOC-43745>

## Troubleshooting

### Check for data arriving on the Syslog server

Check for data arriving on the syslog server either in /var/log/syslog or var/log/datanow/usage.log using the following tail command:

```
tail -f /var/log/datanow/usage.log
```

### Check the server is listening

On the syslog server, use the following command to ensure the server is listening on the port configured:

```
netstat -nlt | grep 10514
```

The response should be:

```
tcp 0 0 0.0.0.0:10514 0.0.0.0:* LISTEN
```

### Check the File Director appliance has connected

On the syslog server, use the following command to ensure the File Director appliance has connected:

```
netstat -nt | grep 10514
```

The response should be:

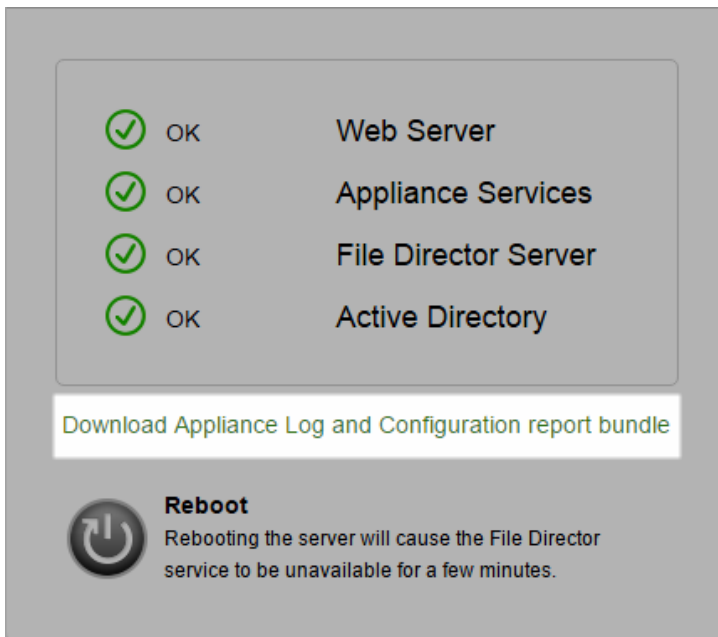
```
cp 0 0 [syslogserver]:10514 [datanow appliance]:42901 ESTABLISHED
```

If support mode is enabled on the File Director server and you have SSH access, then running netstat on the File Director server should show a similar connection as above.

## Report Logs

You can download configuration reports and appliance logs which can be used by Ivanti support to check your installation, performance and to troubleshoot your appliance.

Select **Home** > **Status** and click the download link.



You may be asked for these reports when contacting Ivanti about File Director.



# Link Based Sharing

Link Based Sharing provides File Director users with a fast and efficient way to share content. Once sharing has been configured in the admin console, it can be enabled for the required map points and the type of receivers that are able to access the files can be defined. File Director classifies receivers into two groups:

- **Internal** - Any employee of the organization as defined by membership of the company's Active Directory.
- **External** - Anyone not in the above group.

File Director saves a version of the shared files and automatically creates links which are emailed to listed recipients. For external receivers, File Director automatically enrolls them and sends access details to the shared content.

## Preparation

Sharing files using File Director requires the Server Administrator to create dedicated staging areas for the two types of receivers. These dedicated areas can be on any AD joined file server, NAS, or SAN.

### Steps required for Internal Link Based Sharing

1. Create an Server Message Block (SMB) share. This can be any name you choose.
2. Provide all domain users with modify access.

Users require Modify access to delete expired shares.

### Steps required for External Link Based Sharing

1. Create an SMB share. This can be any name you choose.
2. Provide all domain users with modify access.
3. Create a new domain user with modify access to the external share.

Users require Modify access to contribute to a share.



To prevent users viewing content out of band, you can locate the staging file server in a segregated network to which only the File Director appliance has SMB access.

---

## Admin Console

You must configure SMTP to send the emails containing the links, create new Staging Map Points to hold the shared files, enable sharing on your map points and set the expiration time for the shares before using the Link Based Sharing feature.

## Set Up the SMTP Server

Set up SMTP to use the required account for initiating Link Based Sharing emails.

The server URL, provided in the client's request, is used to create the link included in emails to users. The File Director server URL configured for your company's appliances must be accessible externally.

1. Select **Configuration > Advanced**.
2. In the SMTP Configuration section, enter the details of the SMTP server and email address:
3. address:
  - Hostname or IP address of the SMTP server
  - SMTP server port number
  - Encryption type to use when sending emails
  - The email address to send emails from
  - Email address to receive test email
  - Indicate if authentication is required and, if so, provide the username and password
4. Click **Update**.

▼ SMTP Configuration

SMTP Server Hostname/IP:	<input type="text" value="smtp.demolab.com"/>
SMTP Server Port:	<input type="text" value="25"/>
Encryption Type:	<input type="radio"/> TLS <input checked="" type="radio"/> SSL <input type="radio"/> None
From Address:	<input type="text" value="administrator@demolab.com"/>
Send test email to:	<input type="text"/>
Requires Authentication:	<input checked="" type="checkbox"/>
Username:	<input type="text" value="administrator@demolab.com"/>
Password:	<input type="password" value="....."/>

## Create Staging Map Points

Set up Staging Map Points to enable files to be shared internally and externally. You can only have two staging map points; one internal and one external.

1. Select **Configuration > Staging Areas**.
2. Click **Add New**.

3. Enter details of the Internal Staging Map Point:
  - Name for the staging area
  - Connection string for the staging area
  - Select Internal User Access from the drop-down

The screenshot shows a dialog box titled "Add New Staging Area" with "Save" and "Cancel" buttons. It contains the following fields:

- Name:** Internal
- Connection String:** \\servername\staginginternal
- User Access:** Internal: files shared via this stage can only be accessed by internal users

Below the fields, it states: "Connection strings must begin with \\"

4. Click **Save**.
5. Repeat this process for an External Staging Map Point if you want to enable Link Based Sharing for non-AD users, adding the credentials of the External AD User account you are using to enable the external staging area.

The screenshot shows a dialog box titled "Add New Staging Area" with "Save" and "Cancel" buttons. It contains the following fields:

- Name:** External
- Connection String:** \\servername\stagingexternal
- User Access:** External: files shared via this stage can be accessed by internal and external users
- Ext. AD User(s):** aduser1@yourcompany.com
- Password:** [masked with dots]

Below the fields, it states: "Connection strings must begin with \\"

6. Click **Save**.

## Enable Link Based Sharing on Map Points

Enable Link Based Sharing on your map points by editing your Map Point Access Policy.

1. Select **Policy > Map Point Access**.
2. Click **Edit** for the required map point.
3. Select the users for whom you want to enable Sharing. Sharing can be enabled for All Users associated with the map point or create individual policies for selected OUs, user groups and/or individual users.

Click **Add** for an OU, User Group or Individual User to define a specific policies.

- Open the appropriate Map Point and set the policy for internal and external users.

You can apply the following settings for each type:

- **Disabled** - Link based sharing is not available for users connecting to this map point. If link based sharing is disabled for internal users, it cannot be enabled for external users on the same map point.
- **Read-only** - All shares are read-only for this map point. Users can download files but not upload files to shares.
- **Collaboration** - Users can download and upload files to shares. Internal users can also delete files they upload whilst external users cannot.

In the example below, Link Based Sharing has been disabled for external users and for the map point. Internal users have collaborative access to shares.

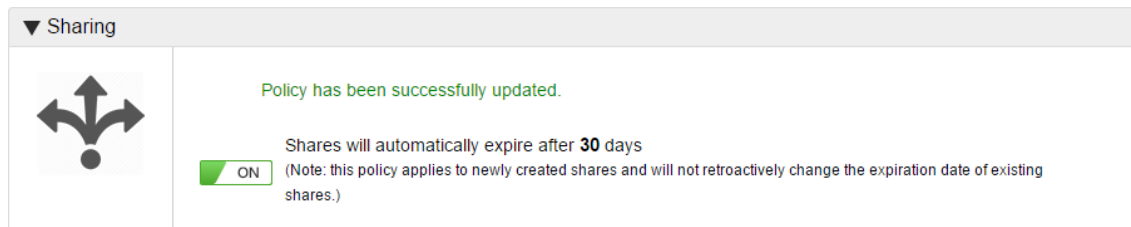
The screenshot shows the 'All Users' configuration page in File Director. The page is titled 'Home' and includes a 'Change connection string for this map point' link and 'Save' and 'Cancel' buttons. The main content is divided into two columns. The left column, under 'All Users', lists three categories: 'Organizational Units' (No OU policies have been set), 'User Groups' (No User Group policies have been set), and 'Individual Users' (No User policies have been set), each with an 'Add' button. The right column, 'Policies for All Users', contains several settings: 'Force read-only (files may not be modified)' (OFF), 'Only allow VERIFIED devices to connect' (OFF), and 'Platform Access' (ON). The 'Platform Access' section includes: 'Allow Windows Access' (ON), 'Allow Mac Access' (ON), 'Allow iOS Access' (ON), 'Allow Android Access' (ON), and 'Allow Web Client Access' (ON). A note states: 'Note: Platform access is also subject to [Global Platform Login Restrictions](#)'. Below this is the 'File Sharing' section, which has three radio buttons: 'Disabled', 'Read-only', and 'Collaboration'. For 'with internal users', the 'Collaboration' radio button is selected. For 'with external users', the 'Disabled' radio button is selected.


- Click **Save** to apply the setting.
- Repeat these steps for any other Map Points where Link Based Sharing is required.

## Set the Automatic Expiration for Link Based Sharing

Set the global expiration for the Link Based Sharing by editing your Global Policy. If a user tries to access a share after it expires, the shared files are removed under the security context of the user's account. If you do not want the Link Based Sharing to have an expiry date, do not enable the Sharing policy.

1. Select **Policy > Global**.
2. Click **Edit**.
3. Set the Sharing policy to **On**.
4. Enter the number of days the shared links will be active for.



 The figure set here is also the number of days by which a share is extended when an expiry date is extended.

5. Click **Save**.

# File Director SMB3 Encryption

## About File Director SMB3 Encryption

File Director supports SMB3.02 encryption for all traffic from File Director servers to back end storage. Support is for SMB3.02 encrypted shares using Windows Server 2012 R2 as the reference platform. Using encrypted SMB3.02 shares requires valid Kerberos configuration items in the File Director server to support authentication. It also requires that map points are specified using a hostname rather than an IP address. It is preferable to use the Fully Qualified Domain Name although using the Shortname will work if valid DNS search domains have been configured.



If the File Director server is secured in a DMZ, port 88 must be open between File Director and Active Directory on the firewall for this to work. This applies to both TCP and UDP protocols.

---

Two modes of authentication are available:

- Username and password authentication on the endpoint with the File Director server switching to Kerberos authentication to communicate securely with the back end SMB3.02 share.
- Using Kerberos from the endpoint right through to the SMB3.02 share utilizing ticket forwarding.

For both authentication modes, reverse IP lookups for file servers and domain controllers must be setup and the clock skew between File Director and must be less than five minutes.



In order for File Director to function correctly, AES-128 encryption must be enabled on the Key Distribution Center (KDC).

---

Once all configuration is complete, enable SMB3.02 protocol on Server 2012 R2 share, otherwise data will not be encrypted in transit.

For further details, see <http://blogs.technet.com/b/filecab/archive/2012/05/03/smb-3-security-enhancements-in-windows-server-2012.aspx>.

# Roll Out File Director

After configuring File Director, all end users specified in the MS Active Directory below the Base DN have access to the website and can synchronize their home folders using the File Director client. Users now need to know how File Director helps them, where to download the client, the address of the File Director appliance and how to use File Director on their devices.

1. Store the client downloads in an accessible location ready for download by users. Consider selecting a location that is accessible from inside and outside the enterprise firewall.
2. If you use Ivanti Application Control software consider elevating user rights for the File Director installer.
3. Communicate the following suggested details to end-users:
  - How and where to download the Windows and Mac clients.
  - How to install the Android clients from the Google Play app store (search for Ivanti).
  - How to install the iOS client for iPhone and iPad from the iTunes app store (search for Ivanti).
  - The server address, username and password to use in the client (their usual username and password from MS Active Directory).
  - How to visit the appliance website using a secure https connection.



The server address for the client and the website address are the same.

---

- Links to the File Director Help Center:
- Your support arrangements in case they encounter difficulties.
- Links to the enterprise acceptable usage policy.
- If you are not using a Public CA, the details of the enterprise SSL certificate and instructions.

## 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. The instructions in this chapter provide information designed to help you install root certificates on Windows, Mac, iOS and Android clients. 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.

## Install Root Certificates on Windows

Web browsers and the File Director Client use the operating system certificate store. So, if you install the certificate in the operating system then both the File Director Client and Internet Explorer automatically trust the server certificate.

This procedure describes one method of installing the root certificate using Internet Explorer and Microsoft Management Console on Windows 7.

1. In Internet Explorer, browse to the File Director Website or File Director Admin Console as follows:
  - Website: `https://<server_address>`
  - Admin Console: `https://<server_address>`
  - The browser displays a security warning.
2. Click **Continue to the website**.
3. In the address bar, right-click the certificate and select **View Certificates**.
4. On the certificate dialog, click the **Details** tab.
5. Click **Copy to file**.
6. In the wizard, select **Base-64 encoded binary X.509 (.CER)**.

The saved file contains the certificate. You can view the file in a text editor to see the certificate.



The certificate must be installed as a trusted certificate for the computer. To do this, run the Microsoft Management Console (MMC) as administrator and add the Certificates snap-in. If MMC is run as a standard user, trusted certificates can only be added at the user account level.

7. Click the Windows Start button.
8. In the search box, begin typing `mmc.exe`, right-click the `mmc.exe` entry in the search results and select Run as Administrator.
9. Select **File > Add/Remove Snap-in**.
10. Select **Certificates** and click **Add**.
11. In the Certificates snap-in dialog, select **Computer account** and complete the wizard.
12. Click **OK**.
13. In the MMC console, expand **Certificates**.
14. Right-click **Trusted Root Certificates** and select **All Tasks > Import**.
15. Follow the Certificate Import Wizard to import the certificate.



After installing the certificate, close and reopen Internet Explorer and load the File Director Website or File Director Admin Console. If the certificate installed correctly and is valid, the security warning no longer displays.

## Install Root Certificates on Mac

Both the web browser and the File Director Client use the operating system certificate store. So, if you install the certificate in the operating system using Safari then the File Director client automatically trusts the certificate.

This procedure describes installing the root certificate on a Mac OS X 10.7.3 using Safari 5.1.3.

1. Launch Safari and browse to the File Director Website or File Director Admin Console as follows:
  - Website: `https://<server_address>`
  - Admin Console: `https://<server_address>`
  - Safari displays a message, "Safari can't verify the identity of the website".
2. Click **Show Certificates**.
3. Select, when using this certificate, **Always Trust**.  
The Secure Sockets Layer (SSL) and X.509 Basic Policy trusts update to Always Trust.
4. Click **Continue**.
5. Provide your password and click **Update Settings**.

Safari adds the root certificate to the certificate store and the browser starts trusting the server.

## Install Root Certificates on iOS

This procedure is based on using the provisioning tool, iPhone Configuration Utility 3.5, on Windows 7 to create or edit a configuration profile containing the certificate and to provision it to an iPad or iPhone. Alternatively, you can email the certificate file to the device and install it. Configuration profiles are XML files that contain device security settings including certificates.



To install the certificate on an iOS device, first install the certificate in the computer operating system - either Windows or Mac.

---

1. In iPhone Configuration Utility, select **Configuration Profiles**.
2. Select an existing profile or click **New** in the toolbar to create one.
3. At the top of the list, click **General** and complete the form.
4. Further down the list, click **Credentials**.
5. If Credentials are not configured, click **Configure**, otherwise, click the plus symbol to add a certificate.

A dialog displays the certificates installed on the computer operating system.

6. Select the required certificate.
7. Plug your iOS device into the computer.
8. In the Devices list, click the device name.
9. Click the **Configuration Profiles** tab.
10. Select the profile you edited, and click **Install**.

The iPhone Configuration Utility installs the configuration and certificates on the device.

# File Director SAN Certificates

This section provides information about configuring a File Director certificate that contains SAN entries.

Subject Alternative Name (SAN) extensions allow a certificate subject to be associated with the service name and domain name components of a DNS Service Resource Record. This enables us to publish multiple DNS names using one SSL web listener.

This allows administrators to use CNAME alias DNS records with an SSL certificate that has a different Common Name set within the subject of the certificate.

This section assumes that you have a functioning File Director appliance with a base DNS, AD, admin user and license configuration applied already.

The configuration is in three parts, DNS, General Certificate and File Director Appliance.

## DNS and SAN Certificates

1. Create DNS entries for your appliance.

mddn1	Host (A)	10.70.22.174
DataNowExternal	Alias (CNAME)	MDDN1.mbd.support.local

2. Check that both records resolve correctly.

```

Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

H:\>ping mddn1

Pinging mddn1.MBD.support.local [10.70.22.174] with 32 bytes of data:
Reply from 10.70.22.174: bytes=32 time<1ms TTL=64
Reply from 10.70.22.174: bytes=32 time<1ms TTL=64
Reply from 10.70.22.174: bytes=32 time<1ms TTL=64
Reply from 10.70.22.174: bytes=32 time<1ms TTL=64

Ping statistics for 10.70.22.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

H:\>ping datanowexternal

Pinging mddn1.MBD.support.local [10.70.22.174] with 32 bytes of data:
Reply from 10.70.22.174: bytes=32 time=1ms TTL=64
Reply from 10.70.22.174: bytes=32 time=1ms TTL=64
Reply from 10.70.22.174: bytes=32 time<1ms TTL=64
Reply from 10.70.22.174: bytes=32 time<1ms TTL=64

Ping statistics for 10.70.22.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

H:\>_

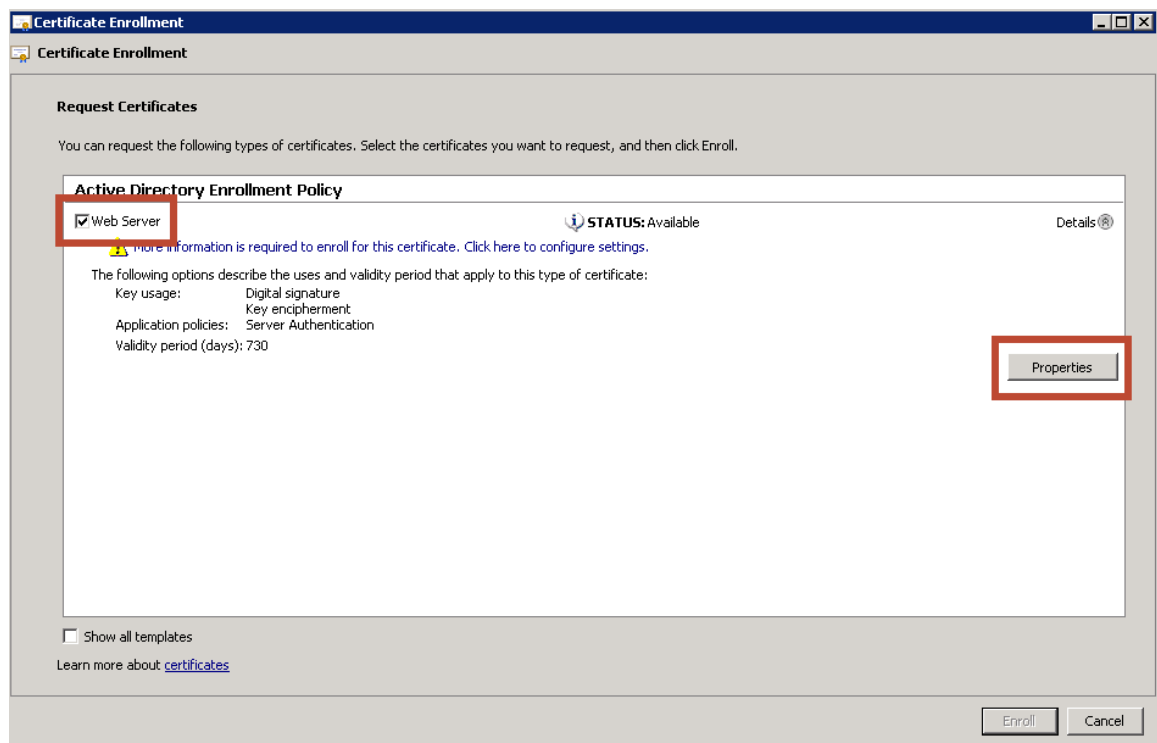
```

## General Certificate

1. Open Microsoft Management Console.
2. Select **Add Certificates** > Computer account > local computer.
3. Click **Finish** and **OK**.
4. Expand Personal and select **Certificates**.
5. Right-click in the center pane and select **Request New Certificate**.

The Certificate Enrollment wizard displays.

6. Click **Next** and **Next** again.
7. Select **Web Server** and click **Properties**.



The Certificate Properties options are displayed.

## 8. Complete the following fields in the Subject name options:

- Common Name
- Organizational Unit
- Organization
- Locality
- State
- Country
- Email

This would be the same information you enter into the File Director appliance when generating a CSR request.

9. In the Alternative name section, select **DNS** from the Type drop down.

## 10. In the Value field, add the Alternative DNS names to be included in the certificate request.

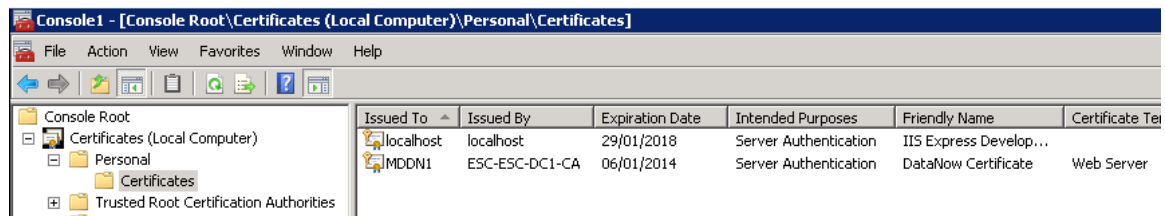
The screenshot shows the 'Certificate Properties' dialog box with the 'Subject' tab selected. The dialog has a title bar with a close button. Below the title bar are tabs for 'Subject', 'General', 'Extensions', 'Private Key', and 'Certification Authority'. The 'Subject' tab is active and contains the following text: 'The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.' Below this is the label 'Subject of certificate' and the description 'The user or computer that is receiving the certificate'. There are two sections: 'Subject name:' and 'Alternative name:'. Each section has a 'Type:' dropdown menu and a 'Value:' text input field. In the 'Subject name' section, the 'Type' is set to 'Organization'. In the 'Alternative name' section, the 'Type' is set to 'DNS'. To the right of each section are 'Add >' and '< Remove' buttons. A list box on the right contains the following entries: 'CN=MDDN1', 'C=GB', 'E=michael.davies@appsense.c', 'L=Warrington', 'S=Cheshire', 'OU=IT', 'DNS', 'MDDN1.mbd.support.local', 'MDDN1', 'DataNowExternal.mbd.support.loc', and 'DataNowExternal'. The 'DataNowExternal' entry is selected. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons. A link 'Learn more about [subject name](#)' is located at the bottom left of the dialog.

11. Select the General tab and enter a Friendly Name and optional Description.
12. Select the Private Key tab and expand the Key Options.
13. Select **Make private key exportable**.



14. Click **Apply** and **OK**.
15. In the Certificate Enrollment dialog, click **Enroll**.
16. When the certificate has successfully enrolled, click **Finish**.

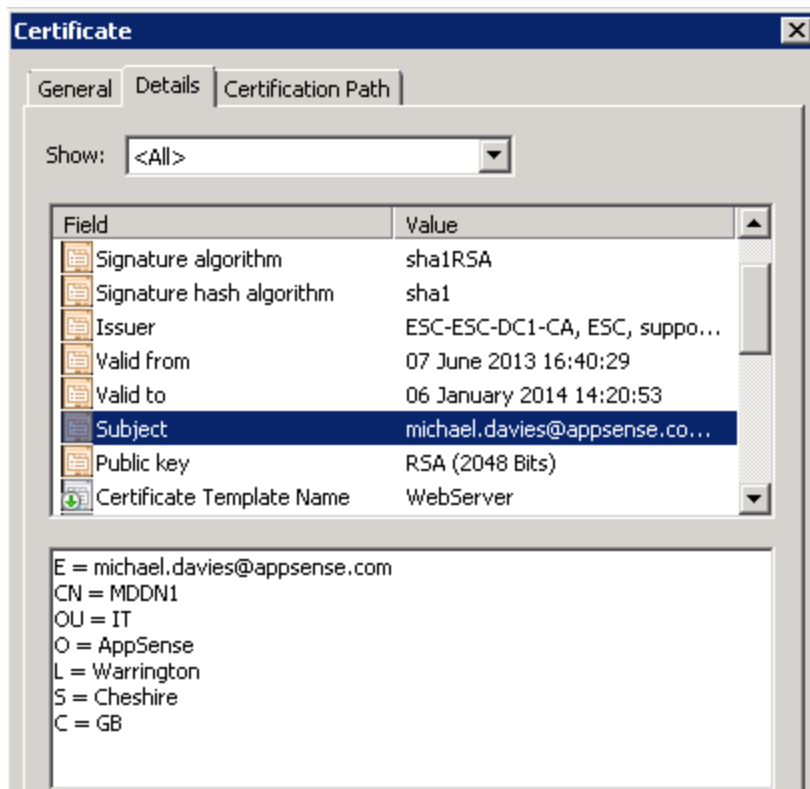
You should see the certificate in the Personal store.



17. Right-click on the new certificate and select **Open**.

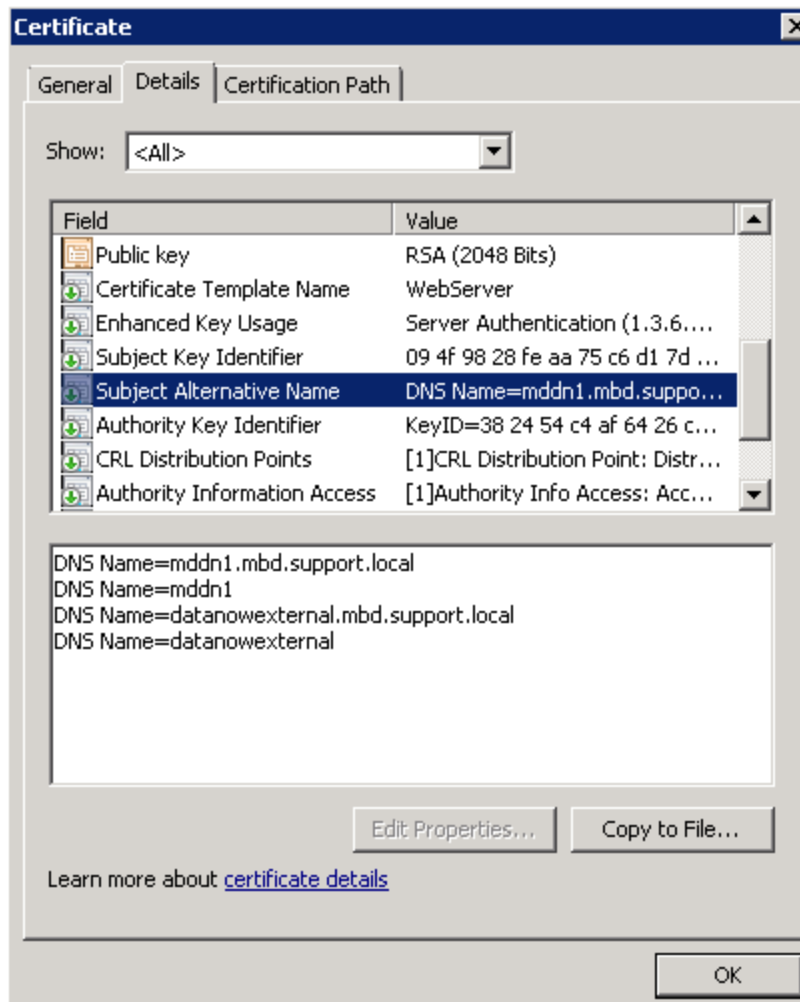
18. Click on the Details tab and select **Subject**.

You will see the subject details for your certificate.



19. Scroll to the **Subject Alternative Name** section.

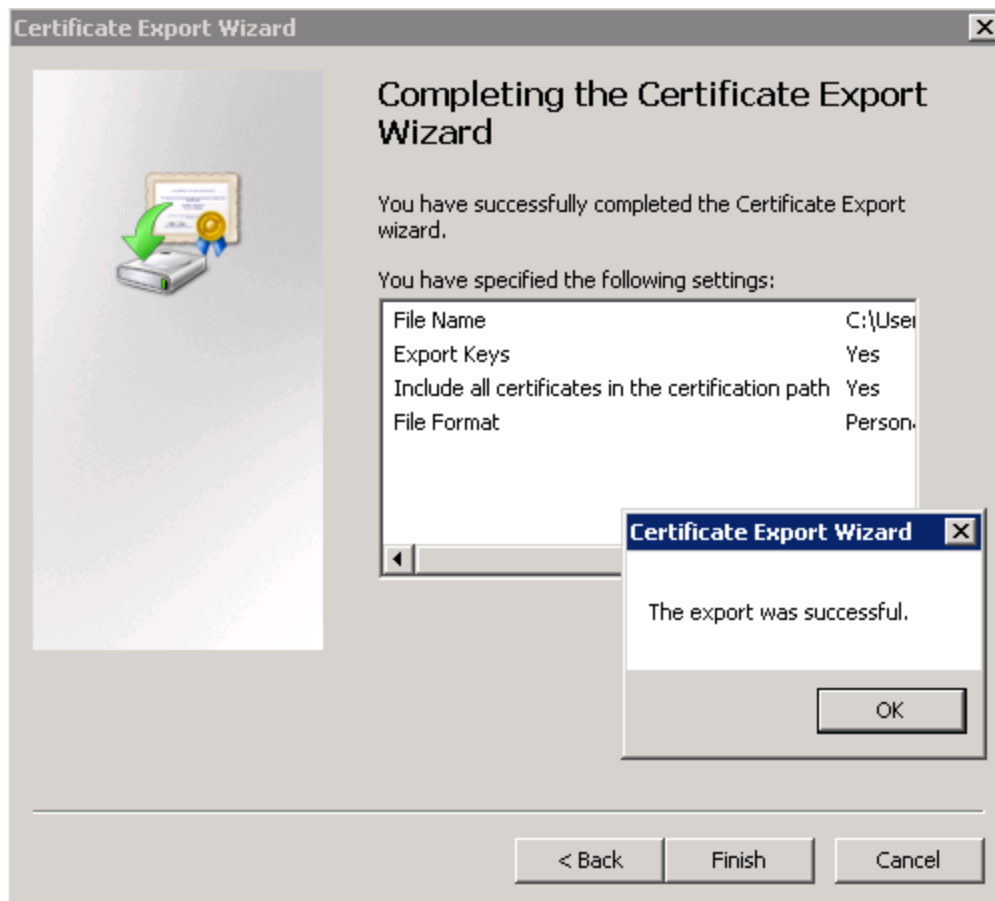
The alternative DNS names you configured should be visible.



20. Click **Copy to File** and then **OK**.
21. Click **Next**.
22. Enable the **Yes, export the private key** option and click **Next**.
23. In the export file format section, select **Include all certificates in the certification path possible** and click **Next**.
24. Type and confirm a password and click **Next**.
25. Save the certificate to a suitable location.



26. Complete the wizard by clicking finish.



## SAN Certificates in the File Director Appliance

1. Open a web browser and connect to your Appliance Admin console.
2. Select **Configuration > SSL Certificate**.

▼ If you have an existing certificate you'd like to use

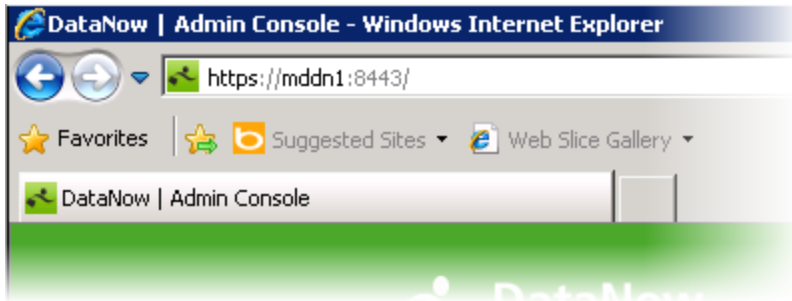
Upload a PKCS #12 or PFX certificate file (.p12 or .pfx file extension).

Encryption Password used to create file:

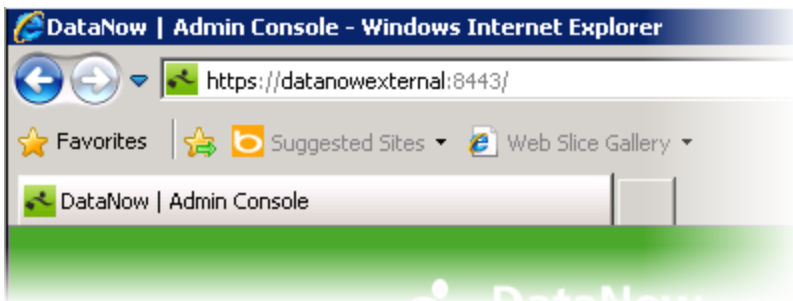
3. Click **Browse** and select the required certificate.
4. If the certificate was created with an encryption password, type it into the field.
5. Click **Upload Certificate** and your certificate should be installed and enrolled for the host name you specified in the Certificate Subject.

You should now be able to use the A and CNAME record to connect to the appliance using SSL.

### A' Record Connection example



### CNAME' Record Connection example



# File Director Command Line Interface

The command line interface (CLI) provides a set of commands for administrators to perform actions using a Virtual Terminal (VT) or Secure Shell (SSH).

CLI is available in File Director version 4.3 and later.



Video: [File Director - Command Line Interface](#)

## Access the CLI using the Virtual Terminal

1. Start your appliance.
2. In the text console, press **Alt+F2**.

The CLI displays.

3. Enter your appliance password.
4. Enter the required command.

```
Welcome to the ivanti platform command line for
advanced configuration and triage capability.

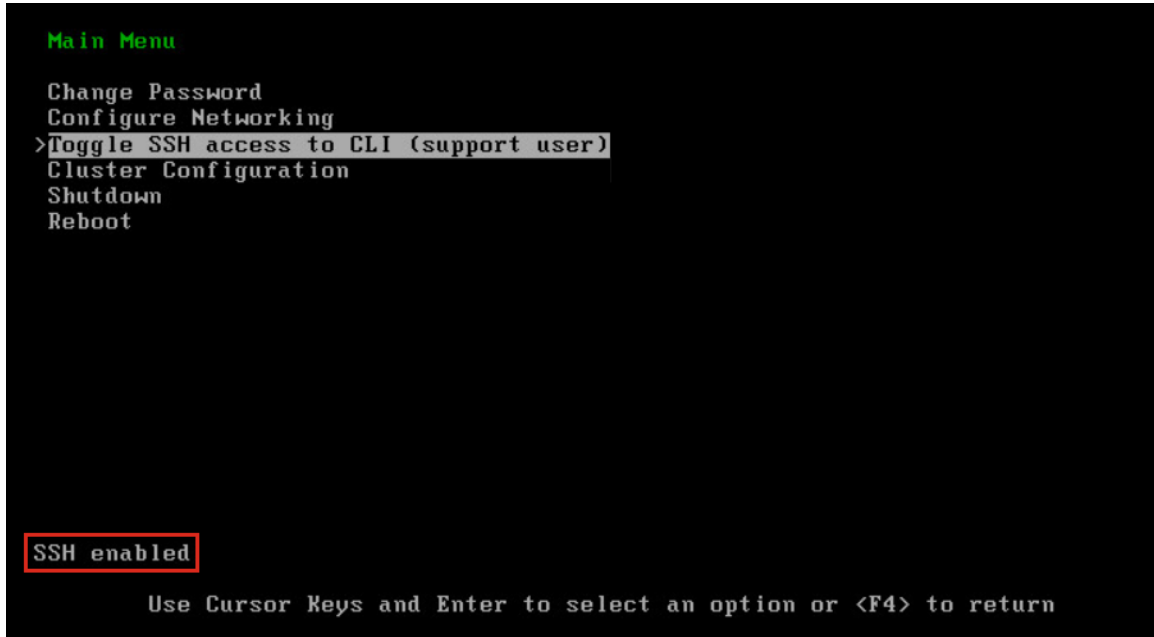
For a list of commands type help or ? followed by return.
[0]>?
[0] filedirector - File Director commands
[0] lookup       - Lookup host
[0] ping         - Test connection through ICMP
[0] restart      - Restart the system
[0] shutdown     - Shutdown the system
[0] logout       - Logout of the command line
[0] help         - Get help about a command
[0] shell        - Switch to shell
[1]>ping dn-play-01
[1] PING dn-play-01 (10.0.32.211): 56 data bytes
[1] 64 bytes from 10.0.32.211: icmp_seq=0 ttl=64 time=0.128 ms
[1] 64 bytes from 10.0.32.211: icmp_seq=1 ttl=64 time=0.048 ms
[1] 64 bytes from 10.0.32.211: icmp_seq=2 ttl=64 time=0.085 ms
[1] 64 bytes from 10.0.32.211: icmp_seq=3 ttl=64 time=0.057 ms
[1] 64 bytes from 10.0.32.211: icmp_seq=4 ttl=64 time=0.104 ms
[1]
[1] --- dn-play-01 ping statistics ---
[1] 5 packets transmitted, 5 packets received, 0.0% packet loss
[1] round-trip min/avg/max/stddev = 0.048/0.084/0.128/0.030 ms
[2]>
```

To exit the CLI and return to the appliance text console, press **Alt+F1**.

## Access the CLI using Secure Shell

1. Start your appliance and go to the main menu.
2. Select **Toggle SSH access to CLI (support user)**.

The screen displays 'SSH Enabled' to confirm that the CLI can be accessed.



```
Main Menu
Change Password
Configure Networking
>Toggle SSH access to CLI (support user)
Cluster Configuration
Shutdown
Reboot

SSH enabled

Use Cursor Keys and Enter to select an option or <F4> to return
```

3. Open the CLI on the required operating system:
  - **Windows** - Windows does not have a built in SSH client but there are many free applications that can be used to access the File Director CLI, for example, PuTTY.
  - **macOS** - To access the File Director CLI on macOS using Terminal, press **command+spacebar** and type **terminal**. When Terminal opens, enter:

```
ssh support@<appliance>
```

Where <appliance> is the hostname or IP address of the File Director appliance.

4. In the CLI, at the **login as:** prompt, enter `support`.
5. Enter your password - this is the same as your appliance password.

For further details, see [Start the appliance and change your password](#).

## Commands

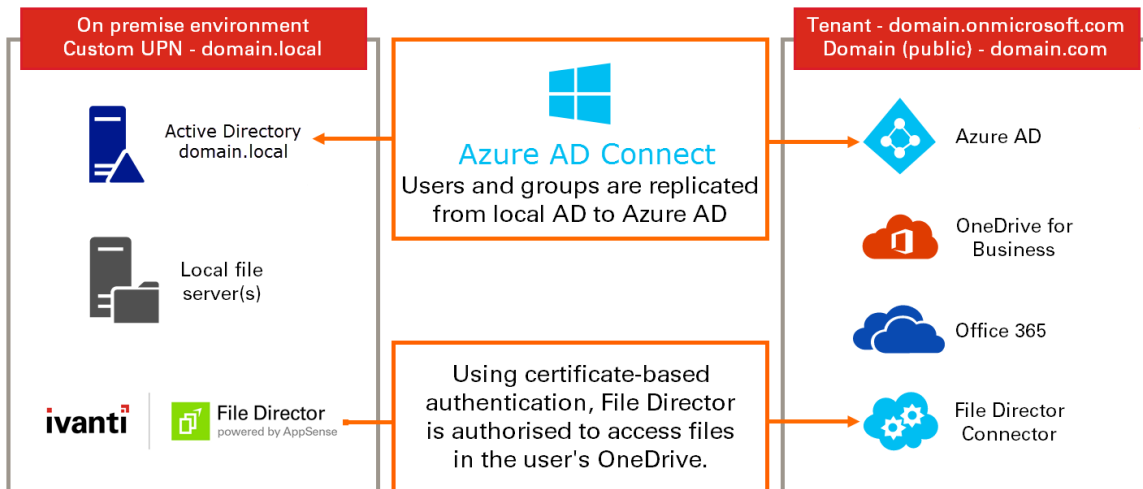
The following commands are available in the File Director CLI:

Command	Parameters	
filedirector	kdc	If you have Kerberos configured, use this command to test the connection to your Active Directory server.
	restart	Restart the File Director application on the current node.
lookup	<hostname>	Forward lookup of hostname. This is compared to the output of the host command from the full shell to validate output. The command returns all IPV4 addresses that the appliance can resolve.
ping	<hostname>	The hostname is resolved and the ping result displayed.
restart	-	Restart your File Director appliance.
shutdown	-	Shutdown your File Director appliance.
logout	-	Log out from the command line.
help or ?	-	<p>Displays the available commands and their descriptions. Prefix a command with ? or help to display the description for that particular command.</p> <p>For example, ? filedirector or help filedirector returns information about what the datanow kdc and datanow restart commands do.</p>

# OneDrive connector for home map points

Configure Azure Active Directory (Azure AD) and the File Director admin console to use OneDrive accounts as the storage location for user's 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.

You can use multiple application IDs when connecting to the SharePoint Online API, so each node in a cluster can have its own application ID, which improves the efficiency of the connector.



## Prerequisites

- Your perimeter firewall must allow communication to <instancename>-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 that Federated AD access is not supported - the local username UPN must match the one used to sign into Azure.
- 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 [Microsoft documentation](#).



Microsoft have published a list of invalid file names and file types for OneDrive. It is available [here](#).

## Step 1 - Create your Azure AD application and grant permission to access OneDrive storage

1. Login to Azure AD Admin Center as Office 365 Administrator.
2. In the sidebar menu click **All Services > App Registrations**.
3. In the **App registrations** dashboard, click **New registration**.

The screenshot shows the Azure Active Directory admin center interface. The top navigation bar is blue and contains the text "Azure Active Directory admin center". Below this, the breadcrumb "Dashboard > App registrations" is visible. The main content area is titled "App registrations" and includes a navigation bar with "New registration", "Endpoints", "Troubleshooting", and "Got feedback?". A blue banner below the navigation bar contains an information icon and the text "Welcome to the new and improved App registrations (now Generally Available). See what's new →". Below this banner, there is a warning icon and the text "Looking to learn how it's changed from App registrations (Legacy)? Learn more" and "Still want to use App registrations (Legacy)? Go back and tell us why". The main content area has two tabs: "All applications" and "Owned applications". Below the tabs is a search bar with the placeholder text "Start typing a name or Application ID to filter these results". At the bottom of the main content area, there is a table header with "DISPLAY NAME" and "AP".

4. Enter an appropriate name for the application, and accept the default supported account types: **Accounts in this organizational directory only**.  
Click **Register** at the bottom of the dialog.



---

[Dashboard](#) > [App registrations](#) > Register an application

## Register an application

---

### \* Name

The user-facing display name for this application (this can be changed later).

### Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Ivanti QA)
- Accounts in any organizational directory
- Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, C

[Help me choose...](#)

### Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Pro optional and it can be changed later, but a value is required for most authentication scenarios.



---

By proceeding, you agree to the [Microsoft Platform Policies](#)

[Register](#)

- An application ID is generated and displayed.

## File Director

<<

[Delete](#)
[Endpoints](#)

- Overview
- Quickstart
- Manage**
- Branding
- Authentication
- Certificates & secrets
- API permissions
- Expose an API
- Owners
- Manifest
- Support + Troubleshooting**
- Troubleshooting
- New support request

Display name : **File Director**

Application (client) ID : **60dafa1c-7132-472c-9ce0-54caa8**


Directory (tenant) ID : a7f39c08-9730-4322-a052-cf701a

Object ID : 7be9ac9f-2f27-48ba-8b73-0e66a9

---

Welcome to the new and improved App registrations. Looking to learn how it's chang


### Call APIs



Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

[View API Permissions](#)

### Sign in users in 5 minutes



Use our SDKs to sign in users and call APIs in a few steps

[View all quickstart guides](#)



You will need to record the application ID as it is required for the next stage in the setup.

## Configure permissions for the appliance

This determines what the application is allowed to do and what it can access.

- Click **API Permissions** > **Add Permission**.

- In the Request API Permissions dialog, click the **APIs my organization uses** tab. Enter *office 365* into the search box to find *Office 365 SharePoint Online*.

Dashboard > App registrations > File Director - API permissions

### File Director - API permissions

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions grant/deny access.

[Add a permission](#)

API / PERMISSIONS NAME	TYPE	DESCRIPTION
▼ Microsoft Graph (1)		
User.Read	Delegated	Sign in a

These are the permissions that this application requests statically. You may also request permissions dynamically through code. [See best practices for requesting permissions](#)

### Grant consent

As an administrator, you can grant consent on behalf of all users in this directory. Granting consent means that end users will not be shown a consent screen when using the application.

[Grant admin consent for Ivanti QA](#)

### Request API permissions

Select an API

[Microsoft APIs](#) **[APIs my organization uses](#)** [My APIs](#)

Apps in your directory that expose APIs are shown below

office 365


NAME	APPLICATION (CLIENT) ID
Office 365 Exchange Online	00000002-0000-00ff-1ce0-000000000000
Office 365 Management APIs	c5393580-f805-4401-95e8-94b7a6ef2fc2
<b>Office 365 SharePoint Online</b>	<b>00000003-0000-00ff-1ce0-000000000000</b>
Office 365 Yammer	00000005-0000-00ff-1ce0-000000000000

- Click **Office 365 SharePoint Online > Application Permissions**.

- In the Request API permissions dialog, select the permissions required then click **Add Permissions** at the bottom of the dialog.

### Request API permissions

[← All APIs](#)

 **SharePoint**  
<https://microsoft.sharepoint-df.com/> [Docs](#) [↗](#)

 SharePoint APIs are available via the Microsoft Graph API. You may want to consider using Microsoft Graph instead.

What type of permissions does your application require?

**Delegated permissions**  
 Your application needs to access the API as the signed-in user.

**Application permissions**  
 Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION	ADMIN CONSENT REQUIRED
▼ Sites (4)	
<input checked="" type="checkbox"/> <b>Sites.FullControl.All</b> Have full control of all site collections ⓘ	Yes
<input checked="" type="checkbox"/> <b>Sites.Manage.All</b> Read and write items and lists in all site collections ⓘ	Yes
<input checked="" type="checkbox"/> <b>Sites.Read.All</b> Read items in all site collections ⓘ	Yes
<input checked="" type="checkbox"/> <b>Sites.ReadWrite.All</b> Read and write items in all site collections ⓘ	Yes
▼ TermStore (2)	
<input checked="" type="checkbox"/> <b>TermStore.Read.All</b> Read managed metadata ⓘ	Yes
<input checked="" type="checkbox"/> <b>TermStore.ReadWrite.All</b> Read and write managed metadata ⓘ	Yes
▼ User (2)	
<input checked="" type="checkbox"/> <b>User.Read.All</b> Read user profiles ⓘ	Yes
<input checked="" type="checkbox"/> <b>User.ReadWrite.All</b> Read and write user profiles ⓘ	Yes

- Having added the permissions, you need to provide Administrator consent for them. In the Grant Consent section, click the button **Grant admin consent for...** In the confirmation dialog displayed, click **Yes**.

Do you want to grant consent for the requested permissions for all accounts in Ivanti QA? This will update any existing admin consent records this application already has to match what is listed below.

grant/deny access.

[+ Add a permission](#)

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
▼ Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	-
▼ SharePoint (8)			
AllSites.FullControl	Delegated	Have full control of all site collections	Yes ⚠ Not granted for Ivanti...
AllSites.Manage	Delegated	Read and write items and lists in all site collections	-
AllSites.Read	Delegated	Read items in all site collections	-
AllSites.Write	Delegated	Read and write items in all site collections	-
MyFiles.Read	Delegated	Read user files	-
MyFiles.Write	Delegated	Read and write user files	-
User.Read.All	Delegated	Read user profiles	Yes ⚠ Not granted for Ivanti...
User.ReadWrite.All	Delegated	Read and write user profiles	Yes ⚠ Not granted for Ivanti...

These are the permissions that this application requests statically. You may also request user consentable permissions dynamically through code. [See best practices for requesting permissions](#)

**Grant consent**

As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end users will not be shown a consent screen when using the application.

[Grant admin consent for Ivanti QA](#)

This action permits access to OneDrive storage for your named application.

- Confirmation of your consent is displayed:

File Director - API permissions

ns

✔ Successfully granted admin consent for the requested permissions.

**API permissions**

Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent process where users are given the opportunity to grant/deny access.

[+ Add a permission](#)

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
▼ Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	- ✔ Granted for Ivanti QA
▼ SharePoint (8)			
AllSites.FullControl	Delegated	Have full control of all site collections	Yes ✔ Granted for Ivanti QA
AllSites.Manage	Delegated	Read and write items and lists in all site collections	- ✔ Granted for Ivanti QA
AllSites.Read	Delegated	Read items in all site collections	- ✔ Granted for Ivanti QA
AllSites.Write	Delegated	Read and write items in all site collections	- ✔ Granted for Ivanti QA
MyFiles.Read	Delegated	Read user files	- ✔ Granted for Ivanti QA
MyFiles.Write	Delegated	Read and write user files	- ✔ Granted for Ivanti QA
User.Read.All	Delegated	Read user profiles	Yes ✔ Granted for Ivanti QA
User.ReadWrite.All	Delegated	Read and write user profiles	Yes ✔ Granted for Ivanti QA

These are the permissions that this application requests statically. You may also request user consentable permissions dynamically through code. [See best practices for requesting permissions](#)

## Step 2 - Configuring File Director

The next step is to go to the File Director console to generate a certificate that can be used to authenticate with OneDrive. Authentication uses public key infrastructure to generate a self-signed certificate in the server and uploads the public key to Azure.

### One Drive Registration

1. In the File Director Web Admin console, select **Configuration > Cloud Connectors**.
2. Enter the **Tenant Name** - this is the domain name you copied from Azure AD in Step 1 - Configure Azure AD.

**OneDrive**

Enter Tenant Name and Application ID(s) to be used by File Director server(s).

**Tenant Name:**

**Application IDs:**

Select an expiry period and then click Generate Key Credential. The Key Credential should then be added to each Application manifest within the Azure AD admin center.

**Expiry period:**

**Key Credential:**



7. In Azure AD, go to App registrations and click **Certificates & secrets** in the sidebar menu then click the **Upload certificate** button.

Dashboard > App registrations > File Director - Certificates & secrets

## File Director - Certificates & secrets

<<

- Overview
- Quickstart

### Manage

- Branding
- Authentication
- Certificates & secrets**
- API permissions
- Expose an API
- Owners
- Manifest

### Support + Troubleshooting

- Troubleshooting
- New support request

Credentials enable applications to identify themselves to the authenticating authority. For a higher level of assurance, we recommend using a certificate (instead of a secret).

## Certificates

Certificates can be used as secrets to prove the application's identity with the authenticating authority.

[Upload certificate](#)

THUMBPRINT	EXPIRES
No certificates have been added for this application.	

## Client secrets

A secret string that the application uses to prove its identity when requesting access to protected resources.

[New client secret](#)

DESCRIPTION	EXPIRES
No client secrets have been created for this application.	

8. Select the .cer file you created earlier, then click **Add**.

Director - Certificates & secrets

temp.cer

Upload certificate

Upload a certificate (public key) with one of the following file types: .cer, .pem, .crt

temp.cer

[Add](#) [Cancel](#)

Upload Completed for temp.cer 14:35  
981 B | "Streaming upload"



## 9. The certificate is now listed in your application.

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

### Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

[Upload certificate](#)

THUMBPRINT	START DATE	EXPIRES
7C5425BD8EEF9813A07DC00155E91CB6	30/04/2019	29/04/2021

Your cloud connector for OneDrive is complete. You can now create a OneDrive home map point and then assign an access policy for users as required. See [Map Point Configuration](#).

When configured, users access their Home folder, and will save to their OneDrive storage - there is no impact on their File Director user experience.

OneDrive will display files that have been saved to the user's File Director home map point. A folder named *\_filedirector\_* is also created in the root of user's OneDrive storage. This folder stores creation times, modified times, and other metadata.



**Video:** [Configure the OneDrive Connector for Home Map Points - Classic Azure portal](#)