Configuring client and server authentication

This is where you choose the authentication methods and user accounts that are used when the FotoWare server tries to reach other FotoWare servers in the network. These settings are configured on the **Server settings** tab in the Operations Center.

### Client authentication

Here you set the method of authentication to use for communications between FotoWare applications. When connecting to an index, for example, a FotoStation user may be asked to authenticate with a user name and password. The same is true when an Index Manager Union server connects to member indexes on other servers, for example. The Client Authentication setting controls whether the clients are authenticated in the server's local user registry, through Active Directory or using any SAML-compliant Identity Provider. If you choose AD authentication, naturally the server must first be a member of the domain. For details on SAML authentication, see the SAML paragraph below.
Server access keys are used for incoming connections from other FotoWare server products on the network to this server's Operations Center - without having to resort to using actual user accounts. Another benefit of using access keys rather than user accounts is that an access key can be easily revoked to invalidate it as required. One access key should be created per server.

**Example:**
Say you have an Index Manager Server that you need to accept incoming connections from Color Factory running on another server on the network.

On the Index Manager server, click on Add to create an access key pair and copy the Account ID and Access Key to the clipboard (and store them safely in a secure document). Once you close the dialog you will not be able to retrieve the keys again.

Now, on the Color Factory server, add these account credentials to the Server Authentication settings in the Operations Center, so that when connecting to the Index Manager server (hostname IMSERVER in the example screenshot below), Color Factory will pass these credentials.
SAML Authentication

The Operations Center can be configured to authenticate clients and servers using a SAML Identity Provider (IdP).

First choose **SAML 2.0** as the client authentication method and click on the **Settings** link to set up the connection to the IdP.

Paste in the certificate endpoint url in the corresponding fields as seen in the above screenshot. They are both obtained from the Identity Provider (IdP) configuration interface, although where you find them may vary from one IdP to another.

Next, set up group name mappings, mapping the **SAML group name** with a corresponding **Group name** stored in the Operations Center. This is the group name value the Operations Center will return when a client requests to know which group a user is a member of.

Finally, in the **Property Mapping** section, set the attribute that the IdP sends containing group membership data and the format of the values from the drop down field (Single/Multi).

**Note:** The **Username**, **First name**, and **Last name** fields are **NOT** currently in use.

**FotoStation TIP:** To upload configurations from FotoStation to an Index Manager server, the user who updates the configuration must be a member of the **FotoWare Administrators** group. Hence you should take care to set up a mapping between a SAML Group name and a corresponding Operations Center group named precisely **FotoWare Administrators**, to facilitate configuration updates for these users.

---

Server authentication

Here you can set the user name and password that this FotoWare server should use when setting up **outgoing connections** to other FotoWare servers on the network. You add a new entry in the list by clicking the **Add** button, after
which you type in the host name of the server you want to connect to and optionally the port number, and which user account you wish to use when connecting to that server. You can also specify that you want to authenticate using a domain account by typing domain\username in the Username field.

We recommend creating access keys (see above) on the server that receives the incoming connections and then adding the credentials obtained to the server that sets up the connection.

Note: When using the file browser in any of the server interfaces you will notice that when connecting to a server for which no authentication credentials have been defined, you will be given the opportunity to manually enter a user name and password. This information will be stored in this list in the Operations Center and used for future connections to that server.