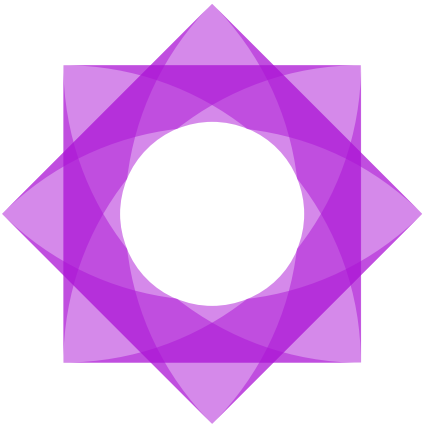


Lasernet 10.

Lasernet Config Server and Deployment 10

Torben Pedersen, Sunil Panchal, Adam McStravick, Haveela Anil
Revision 9
2024-01-13

Formpipe.

Contents.

1 Introduction. 4
1.1 Who Should Use This Guide? 4
2 Terms of Use. 5
3 Overview. 6
3.1 Running Service for Lasernet Config Server 6
3.2 Lasernet Config 10 7
3.2.1 Log file 7
3.2.2 Server setting file 7
3.3 Lasernet Application Process 14
3.4 Lasernet Config Server 15
3.4.1 Disabling Internet Explorer Enhanced Security Configuration 17
3.4.2 Group policy to "disable" OCSP checking 17
4 Lasernet Config Server: Getting Started. 18
4.1 Login Page 18
4.1.1 Reset the Admin Password 18
4.2 Home 21
5 Workflow. 22
5.1 Lasernet Server License Manager 22
5.2 Servers 24
5.2.1 List of Servers 24
5.2.2 Add Server 24
5.2.3 Remove Server 25
5.2.4 Insights 26
5.3 Configurations 29
5.3.1 New Configuration 29
5.3.2 Import Configuration 31
5.3.3 Open Configuration 32
5.3.4 List of Configurations 33
5.4 Deploy 34
5.4.1 History: Configuration Revisions 34
5.4.2 Commit 36
5.4.3 Revert 39
5.4.4 Deploy to Server 40
5.4.5 Open Old Revision of Configuration 50
5.4.6 Patch 52
5.4.7 Add Multiple Server Instances in Lasernet Config Server 53
5.4.8 Add Multiple Server Instances in Lasernet Developer 54
5.5 Users and Groups 56
5.5.1 Add User 56
5.5.2 Edit User 57
5.5.3 Add Group 58

5.5.4 Edit Groups....58
5.6 Security Roles....60
5.6.1 Developer....60
5.6.2 Monitor....69
5.6.3 Client....69
5.6.4 Printer Service....72
5.7 Migration to Microsoft SQL Server....73
5.8 Multi-users....75

1 Introduction.

1.1 Who Should Use This Guide?

This guide is intended to provide users with an overview of Lasernet server configuration and deployment.

2 Terms of Use.

No part of this publication may be reproduced, transmitted, transcribed, or translated into any language in any form by any means without the prior written permission of Formpipe Software. The information in this manual is subject to change without notice. Any company names or data is fictive unless otherwise stated.

Formpipe Software shall not be liable for any loss or damage whatsoever arising from the use of this manual and the information contained therein (including errors or omissions).

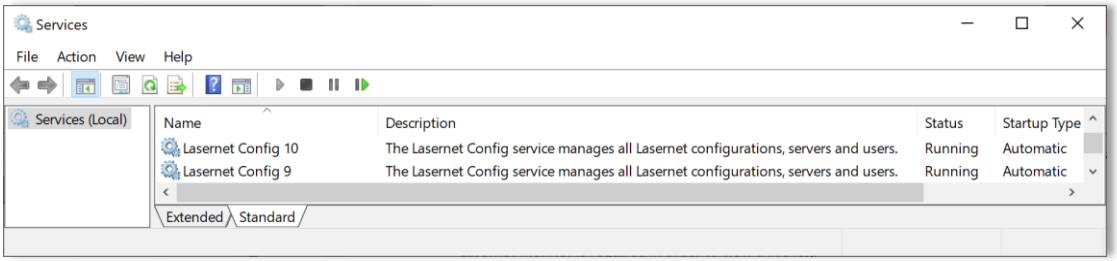
Trademarks of other companies mentioned in this document appear for identification purposes only and are the property of their respective companies.

© 2023 Formpipe Software.

3 Overview.

3.1 Running Service for Lasernet Config Server

A single service named Lasernet Config 10 is installed by the Lasernet Server 10 installer and must be running for the Lasernet Config Server.



Note: The Lasernet Config 9 service can run on the same server at the same time.

3.2 Lasernet Config 10

This service manages all Lasernet configurations and act as a relay proxy between

- Lasernet Developer
- Lasernet Client app
- Lasernet Web Client
- Lasernet OCR
- Lasernet Meta

and the Lasernet Service(s).

3.2.1 Log file

The log file(s) for the config server are located in:

C:\ProgramData\Formpipe Software\Lasernet 10\Config\Default\Config.lnlog

The config.lnlog contains status information about:

- Database connections
- Deployments
- Expiring of tokens
- Migrations
- Start and stop of config service
- Transactions between client apps and server

3.2.2 Server setting file

The settings for the Lasernet Config server are located in:

C:\ProgramData\Formpipe Software\Lasernet 10\Config\Default\ServerSettings.json

and the config service settings are grouped in to:

- Authentication
- Bindings
- Port
- Servers

3.2.2.1 Authentication

Type of authentication can be configured to either Lasernet local or external users (OpenID Connect), like Microsoft Entra ID. In order to configure Lasernet for Microsoft Entra ID authentication please read the “Lasernet Configuring Microsoft Entra ID Authentication” guide.

```
{
    "Service": {
        "Authentication": {
            "Providers": {
                "Default": {
                    "ClientId": "<Application (client) ID>",
```

```
                    "Name": "<Tenant name 1>",
                    "OIDCMetadataEndpoint": "<OpenID Connect metadata document URI>"
                },
                "Backup": {
                    "ClientId": "<Application (client) ID>",
                    "Name": "<Tenant name 2>",
                    "OIDCMetadataEndpoint": "<OpenID Connect metadata document URI>"
                }
            },
            "Type": "Local"
        }
}
```

The Authentication object contains the following properties:

Property	Type	Description
Type	String	Tells Lasernet whether to use local or external users (OpenID Connect). Can be set to either 'Local' or 'External'.
Providers	String	Contains a list of named authentication provider objects. When external configuration is used you must add at least one provider. One of the providers must be named "Default" and will be used if the user doesn't specify a provider when logging in.

The format of a Provider object is as follows:

Property	Description
ClientID	Contains the Application (Client) ID identifying the App registration in Microsoft Entra ID.
OIDCMetadataEndpoint	Contains the URI of the OpenID Connect Metadata document for the Microsoft Entra ID tenant. The OpenID Connect Metadata document provides Lasernet with the information required to validate the JWT tokens issued by Microsoft Entra ID.

It is possible to configure several different providers. In order to authenticate using a different provider, the user has to specify the name of the configured provider when attempting to log in.

3.2.2.2 Bindings

It is possible to configure several hostnames to bind with a local server certificate and obtain a secured connection via the IP address, the local host name or a DNS name.

```
{
    "Service": {
        "Bindings": [
            {
                "Hostname": "<IP address>"
            },
            {
                "Hostname": "localhost"
            },
            {
                "Hostname": "<local server name>"
            },
            {
                "Hostname": "<dns name>"
```

```
                "Thumbprint": "<thumbprint>"
                "PFX": "<path+filename>"
                "Password": "<password>"
            }
        ],
    }
}
```

If no bindings are configured Lasernet will auto-generate self-signed certificates for 'localhost', '<machine name>' and (if applicable) '<machine name>.<active directory domain name>'.

Lasernet can use certificates installed in the Windows certificate store (under Computer certificates) or certificates stored on disk as PFXs.

The Bindings object is an array of Bindings with the following format:

Property	Type	Description
Hostname	String	(Required) The hostname for which to bind a certificate
Thumbprint	String	(Optional) This will force Lasernet to use the certificate with the specified thumbprint in the Windows Certificate store.
PFX	String	(Optional) A path and filename to the certificate (including private key) stored in PFX format.
Password	String	(Required when using PFX) Specifies the password for the PFX file.

If only Hostname is specified, Lasernet will attempt to find a suitable certificate for the specified hostname in the Windows Certificate store. If no suitable certificate is found, Lasernet will generate a self-signed certificate for this hostname.

3.2.2.3 Port

The port number to run the config server. The default port number is 33443, but can be configured to any port number, which is not in conflict with other services running on the Windows server.

```
{
    "Service": {
        "Port": <port number>,
    }
}
```

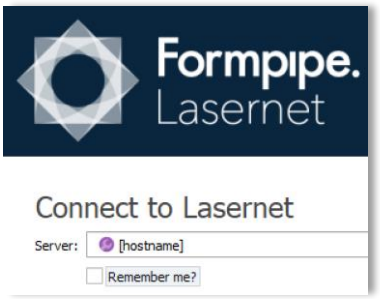
The Port object contains the following property:

Property	Type	Description
Port	String	Tells Lasernet which port number to run the Lasernet Config server at.

To connect to the Lasernet Config web site, from a browser, using default port number 33443, use this URL:

https://[hostname]:33443/lasernet/config

To connect to the Lasernet Config web site, from a Lasernet app, using default port number 33443, use this URL:



To connect to the Lasernet Config web site, from a browser, using port number 443, use this URL:

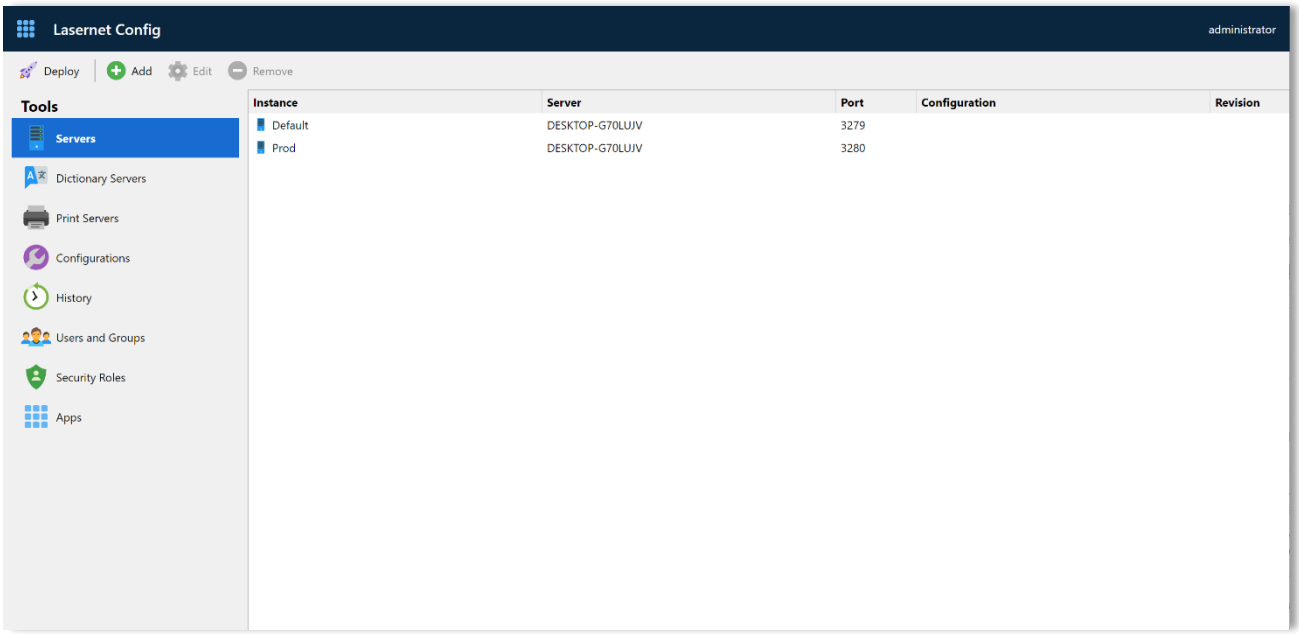
https://[hostname]/lasernet/config

To connect to the Lasernet Config web site, from a Lasernet app, using default port number 443, use this URL:

3.2.2.4 Servers

The list of server instances, including port number can either be maintained from the Lasernet Config web site or from the Servers object.

Note: The Servers object can be excluded if you would like to maintain these settings from the Lasernet Config web site:



If a Servers object exist, the server settings on the web site are in read-only mode.

```
{
    "Service": {
        "Servers": {
            "<InstanceName1>": {
                "ClientSecret": "<ClientSecret>",
                "Insights": {
                    "Performance": <Boolean>,
                    "Transactions": <Boolean>
                },
                "Port": <PortNumber>,
                "Server": "<Hostname>"
            },
            "<InstanceName2>": {
                "ClientSecret": "<ClientSecret>",
                "Insights": {
                    "Performance": <Boolean>,
                    "Transactions": <Boolean>
                },
                "Port": <PortNumber>,
                "Server": "<Hostname>"
            }
        },
        "DictionaryServers": {
            "Dictionary": {
                "Server": "<Hostname>",
                "Port": <PortNumber>
            }
        }
    }
```

```
}
```

To mitigate a “server-side request forgery” the security level is increased by optionally maintaining the server list in the ServerSettings.json configuration file.

The Servers object is an array of server instances with the following format:

Property	Type	Description
Instance name	String	(Required) The name for each instance can be found and copied from the Lasernet Server License Manager. This was created when the instance was added to the server.
Client secret	String	(Required) The client secret for each instance can be found and copied from the Lasernet Server License Manager. The client secret was created when the instance was added to the server
Insights	String	(Optional) A Boolean, set to false (default) or true, to activate counters for Performance or Transactions on the Lasernet Server. The counters can be viewed in the Lasernet Monitor.
Port	Number	(Required) The port number for each instance can be found and copied from the Lasernet Server License Manager. The port number was created when the instance was added to the server
Server	String	(Required) The name of a Lasernet Server to run one or several instances. An active connection between the Lasernet Config Server and to the Lasernet Server instance is required to deploy a configuration.

3.2.2.5 Dictionary Servers

The Dictionary Servers object is optionally used by the OCR Engine, which is a part of the Lasernet Input Management solution.

The list of Dictionary server instances, including port number can either be maintained from the Lasernet Config web site or from the DictionaryServers object:

Property	Type	Description
Instance name	String	(Required) The name for each instance can be found and copied from the Lasernet Server License Manager. This was created when the Dictionary instance was added to the server.
Port	Number	(Required) The port number for each instance can be found and copied from the Lasernet Server License Manager. The port number was created when the Dictionary instance was added to the server. It is recommended to use the same port number as configured for the Lasernet Config server (default 33443)
Server	String	(Required) The name of a Lasernet Server to run one or several Dictionary instances. An active connection between the Lasernet Config Server and to the Lasernet Server instance is required to connect to the Dictionary Server database.

3.2.2.6 Example of a server setting file

In the following you can find an example where we have configured the Lasernet Config server and Lasernet Services with the following parameters

Property	Description
Authentication	End-users are using external authentication and can log in with their Microsoft Entra ID user login added to the listed provided from the Lasernet applications.
Bindings	End-users can access the Lasernet Config server via a secured connection via the listed IP address and hostnames.
Port	Lasernet Config server is configured to communicate on port number 443.
Servers	Lasernet server instances, named Default and Prod, are configured to communicate on port number 3279 and 3280. Lasernet Dictionary server instance is configured to communicate on port number 443.


```
{
    "Service": {
        "Authentication": {
            "Providers": {
                "Default": {
                    "ClientId": "999ee99f-9fc9-9a99-ad99-99999fd099e9",
                    "Name": "Formpipe Software AB tenant",
                    "OIDCMetadataEndpoint": "https://login.microsoftonline.com/9999be9c-
9c99-99bb-a6de-c999db099a99/v2.0/.well-known/openid-configuration"
                }
            },
            "Type": "External"
        },
        "Bindings": [
            {
                "Hostname": "192.168.99.1"
            },
            {
                "Hostname": "localhost"
            },
            {
                "Hostname": "ln-win2019-test"
            },
            {
                "Hostname": "ln-win2019-test.northeurope.cloudapp.azure.com"
            }
        ],
        "Port": 443,
        "Servers": {
            "Default": {
                "ClientSecret": "9CAZTx9+svqBq9YvMOWzX/9QBRu999zLAJthBh1US99=",
                "Insights": {
                    "Performance": true,
                    "Transactions": false
                },
                "Port": 3279,
                "Server": "ln-win2019-test"
            },
            "Prod": {
```

```
                "ClientSecret": "Ix+XAKvNNJ99CRyK99gc9SWO0FFq9Rts9N9gbr9OwcY=",
                "Insights": {
                    "Performance": false,
                    "Transactions": false
                },
                "Port": 3280,
                "Server": "ln-win2019-test"
            },
            "DictionaryServers": {
                "Dictionary": {
                    "Port": 443,
                    "Server": "ln-win2019-test"
                }
            }
        }
    }
}
```


3.3 Lasernet Application Process

This chapter gives an overview of the Lasernet application process as well as information on how to manage, configure and run it.

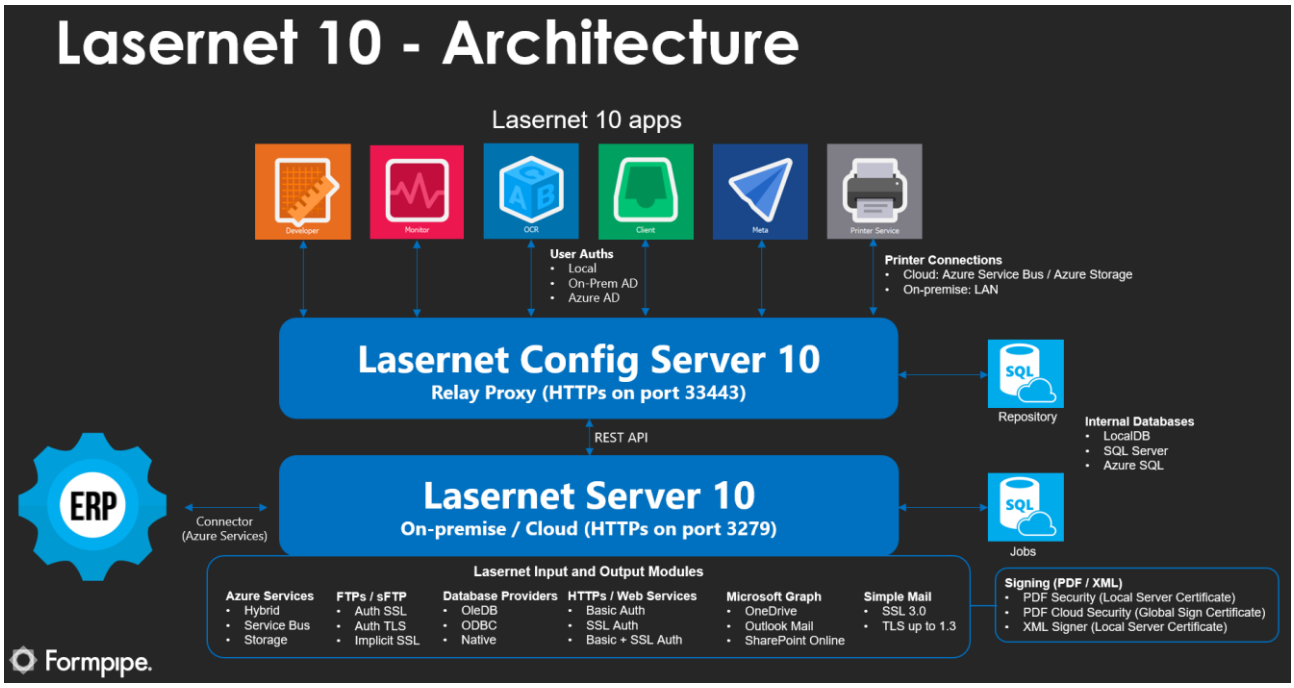
Lasernet Developer 10: one (single client) or several computers (multiple clients) to create and build a configuration.

Lasernet Config Server 10: a single server to store configurations, server settings, revisions, history, users and groups and security roles. Access to a Microsoft SQL Server is required.

Lasernet Server 10: one (single) server to run the production service instance or several servers to setup an enterprise environment for the development, staging and backup servers. Access to a Microsoft SQL Server is required.

The applications and service can be installed on a single computer, but multi-server environment is recommended.

Note: Lasernet is pre-installed by default with a Microsoft SQL Server 2017 LocalDB. Migrating to Microsoft SQL Server is recommended for enterprise users backing up servers.

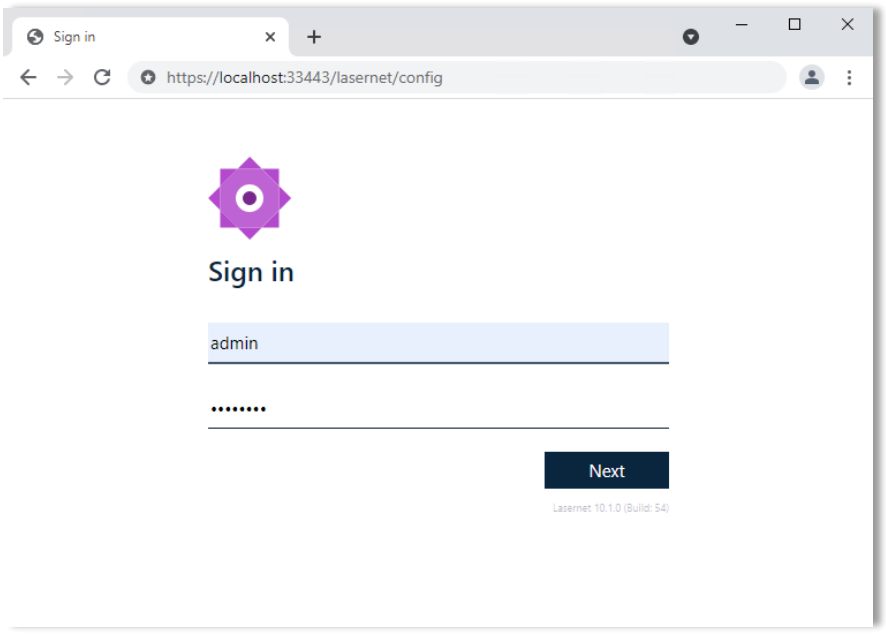


The listed port numbers are default values and can be changed in:

C:\ProgramData\Formpipe Software\Lasernet 10\Config\Default\ServerSettings.json

An open connection between the listed applications and services is required.

3.4 Lasernet Config Server



To access the Lasernet Config Server use the following URL:
https://[servername]:33443/lasernet/config

3.4.1 Disabling Internet Explorer Enhanced Security Configuration

On some computers you may need to disable the IE Enhanced Security Configuration in the Server Manager → Local Settings.

More information can be found here:
https://support.microsoft.com/en-au/help/815141/internet-explorer-enhanced-security-configuration-changes-the-browsing

Supported browsers are: Microsoft Edge, Google Chrome, Mozilla Firefox

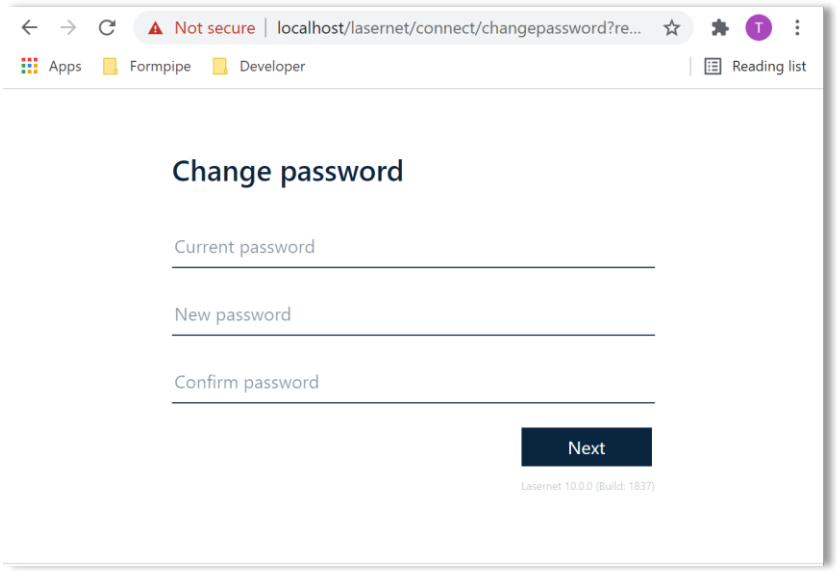
3.4.2 Group policy to "disable" OCSP checking

On some computers, not connected to the Internet, you may need to change the OCSP request timeout in the Server Manager → Local Group Policy Editor → Local Computer Policy → Computer Configuration → Windows Settings → Security Settings → Public Key Policies

- Object Type: Certificate Path Validation Settings
- Tab: Network Retrieval
- Define these policy settings: Active
- Default URL retrieval timeout: 1 second (Default: 15 seconds)
- Default path validation cumulative retrieval timeout: 1 second (Default: 20 seconds)

4 Lasernet Config Server: Getting Started.

4.1 Login Page



When logging in for the first time, create a new password for the admin user:

User: admin

Current password: [leave empty]

New password: [choose a password]

Confirm password: [choose a password]

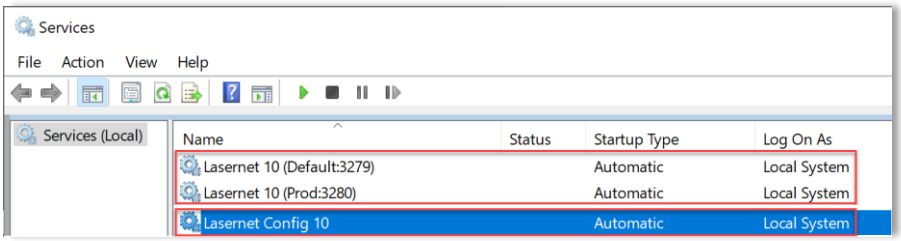
You can now set a password for the admin account. The password must be changed when you log in to the config website for the first time.

4.1.1 Reset the Admin Password

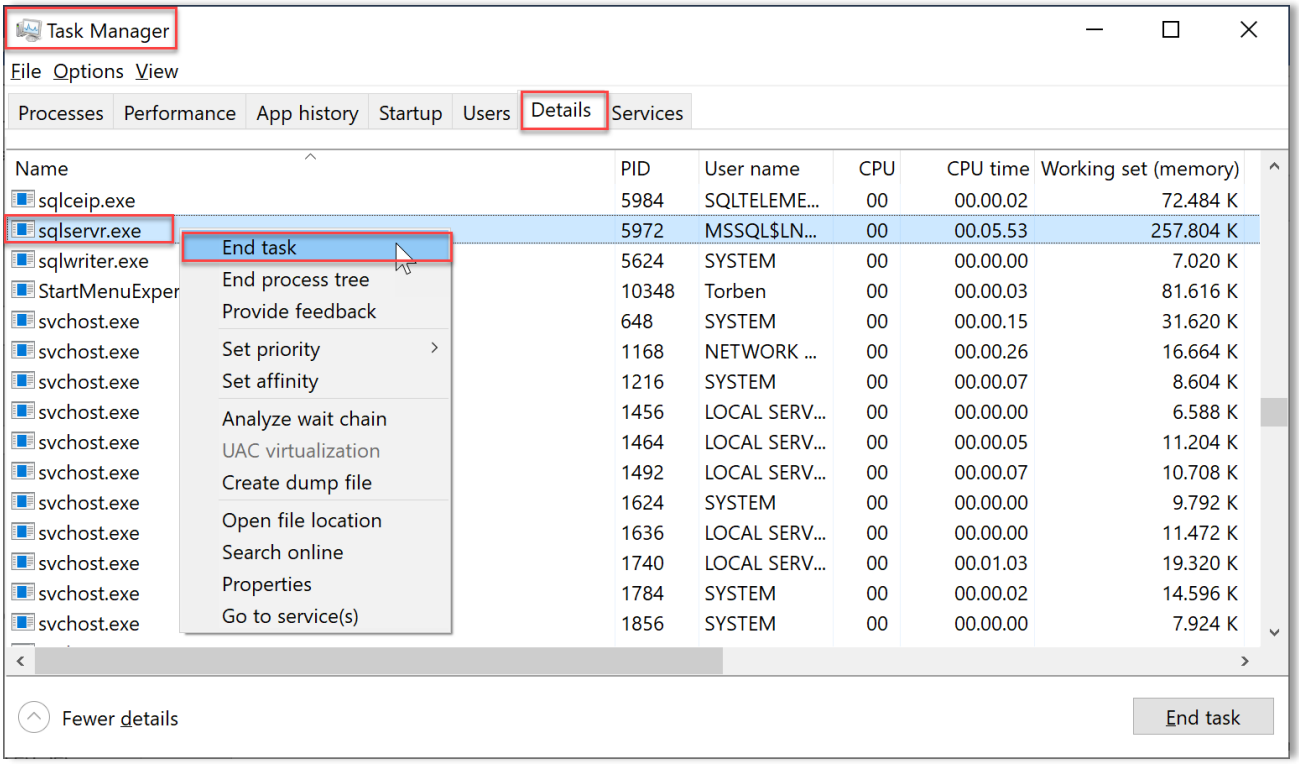
If you forgot the password, you can always reset it. It requires that you have admin rights on the server, where the Lasernet Config Server is installed

You must run the following steps:

1. Run Services and stop your Lasernet Config 10 and Lasernet 10 Service(s).

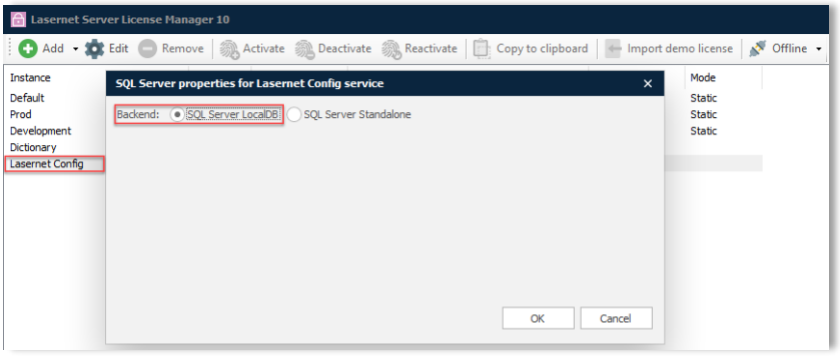


2. Run the Task Manager and click the Details tab.



3. Select the sqlservr.exe, right click and select End task to kill the process. Continue this process for any sqlserver.exe running on the server.

Note: This step is only needed when using SQL Server LocalDB for the Lasernet Config server.

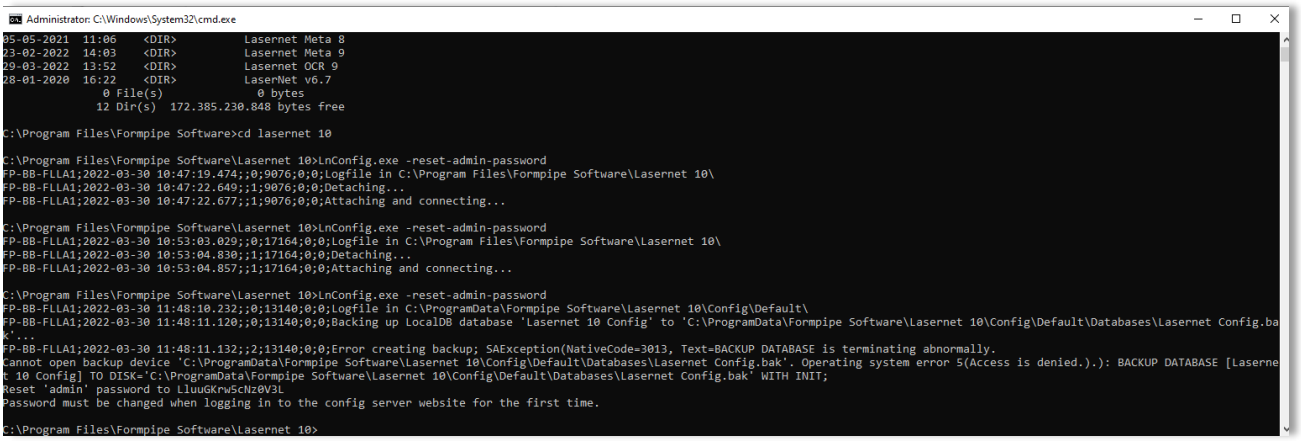


4. Run a Windows command prompt with admin rights

5. Change the directory to Lasernet 10 installations folder
```
cd C:\Program Files\Formpipe Software\Lasernet 10\
```

6. Run *LnConfig.exe* in the command prompt with the following parameter:
```
LnConfig.exe -reset-admin-password
```

Note: This can generate a list of database errors in. In the fact that the database is no longer in use, by the sqlservr.exe process, means that it is now accessible for a password reset.



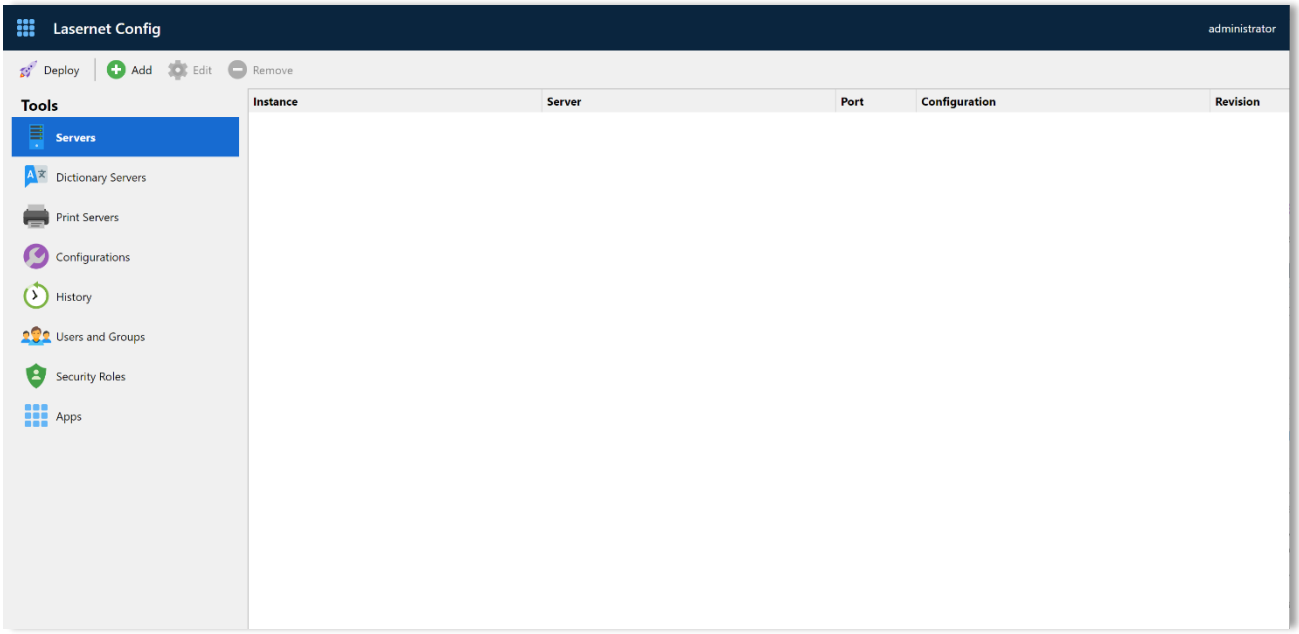
As a result, a new password for the admin account is generated and shown in the console. This password must be changed when logging in to the config server web site next time.

7. Start your Lasernet Config 10 and Lasernet 10 Service(s).

Note: The sqlserver.exe processes will automatically start again when Lasernet Config 10 and Lasernet 10 Service(s) are started.

4.2 Home

The web interface of the Lasernet Config Server has the following sections:

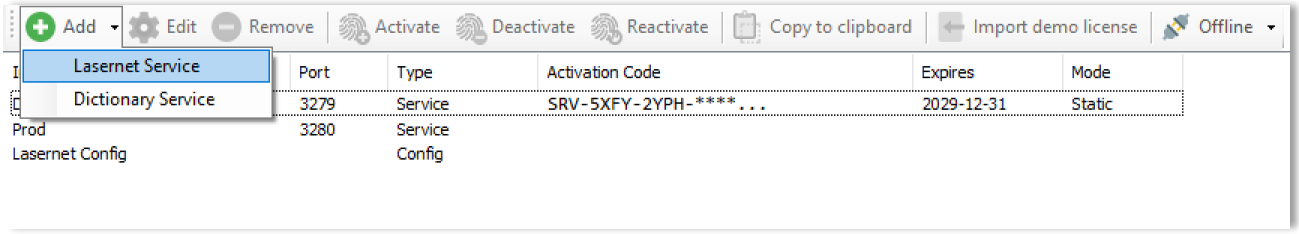


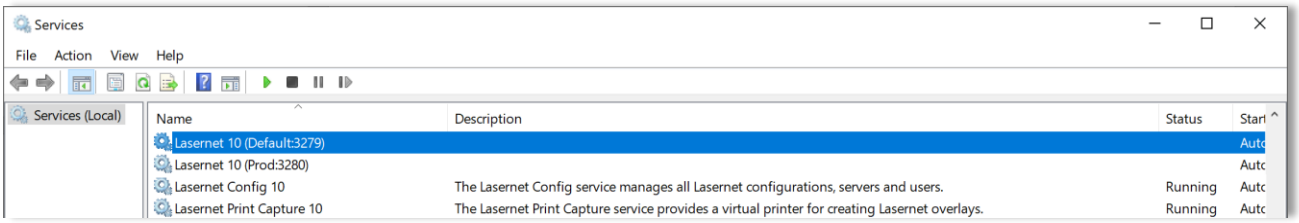
Name	Description
Servers	Manage name of Lasernet instances, servers, port numbers and client secrets.
Dictionary Servers	Manage name of Dictionary Servers, hostname and port number to be used by the OCR Editor and OCR Engine.
Print Servers	Manage name of Windows printer servers and connection strings for printing via cloud or on-premise.
Configurations	Shows all the available configurations.
History	Allows you to view the deployment history.
Users and groups	Allows viewing and editing names of local users and groups.
Security roles	Allows you manage security roles for Lasernet Developer and Client
Apps	Allows you to manage access to web applications and services.

5 Workflow.

5.1 Lasernet Server License Manager

Add and license for your instances running on the Lasernet 10 server via the Lasernet Server License Manager.





We recommend that you install and run your development and production services on different machines. The image above shows all the Lasernet services running on the same server.

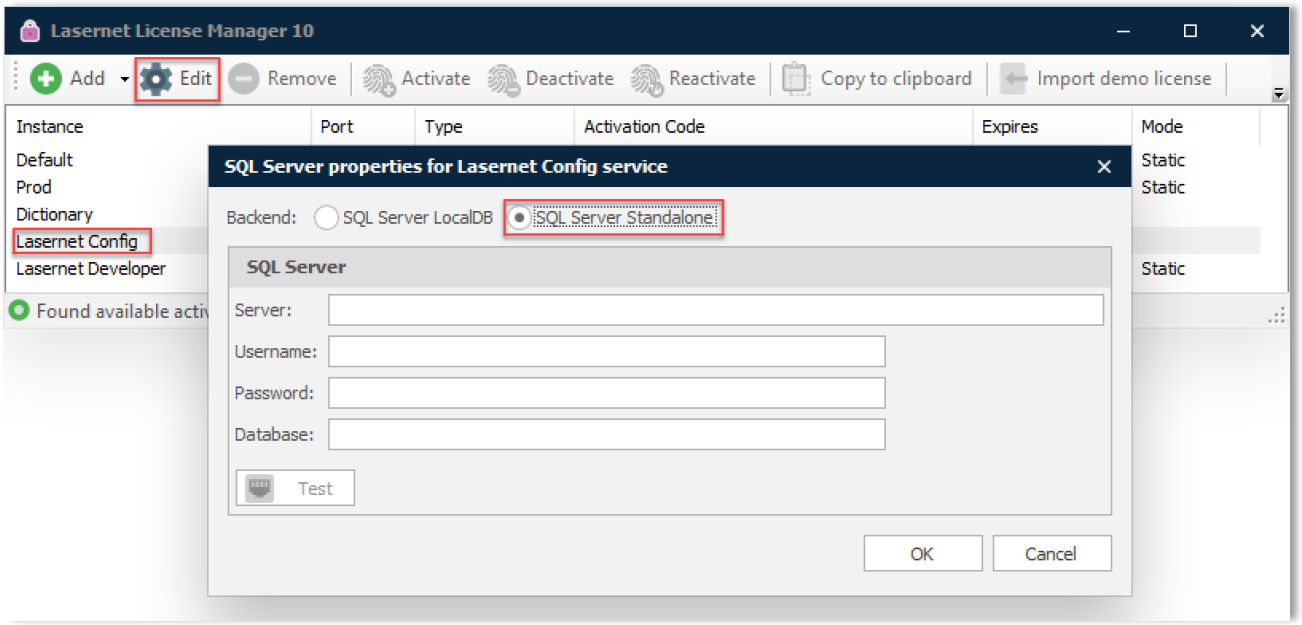
By default, Lasernet Config Server connects to the Microsoft SQL Server 2017 LocalDB database to store configurations, revisions and deployment history log.

The database and repository for the Lasernet Config Server are installed in here:

C:\ProgramData\Formpipe Software\Lasernet 10\Config\Default\Databases

We recommend that enterprise users backup this folder or replace it with a Microsoft SQL Server standalone edition.

You can use the Lasernet Sever License Manager at any time to migrate the Lasernet Configuration data from the Microsoft SQL Server 2017 LocalDB to the Microsoft SQL Server. Select the Lasernet **Config SQL Server** instance, click Edit and SQL Server Standalone with the required connection, authentication and database

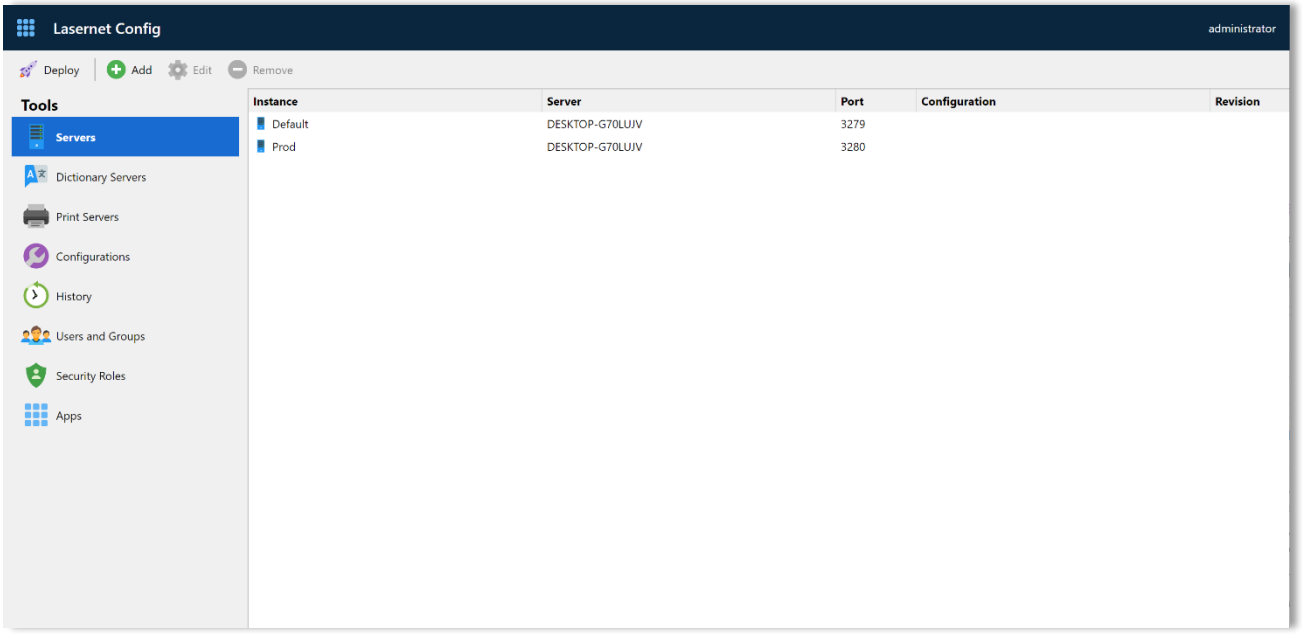


More information about creating a database in Microsoft SQL Server can be found later in this manual.

5.2 Servers

5.2.1 List of Servers

A list of servers added can be accessed via the **Servers** tab.

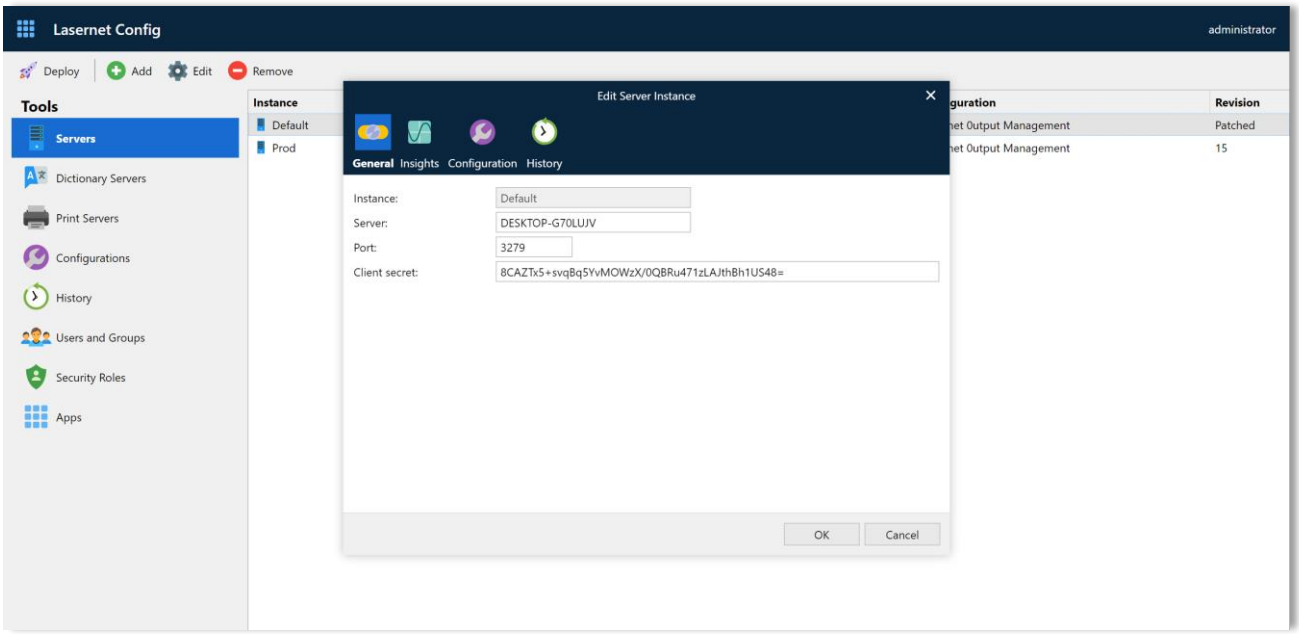


Use the command buttons to manipulate items in the list:

- Click **Add** to add a server
- Select Click **Remove** to remove a server.

5.2.2 Add Server

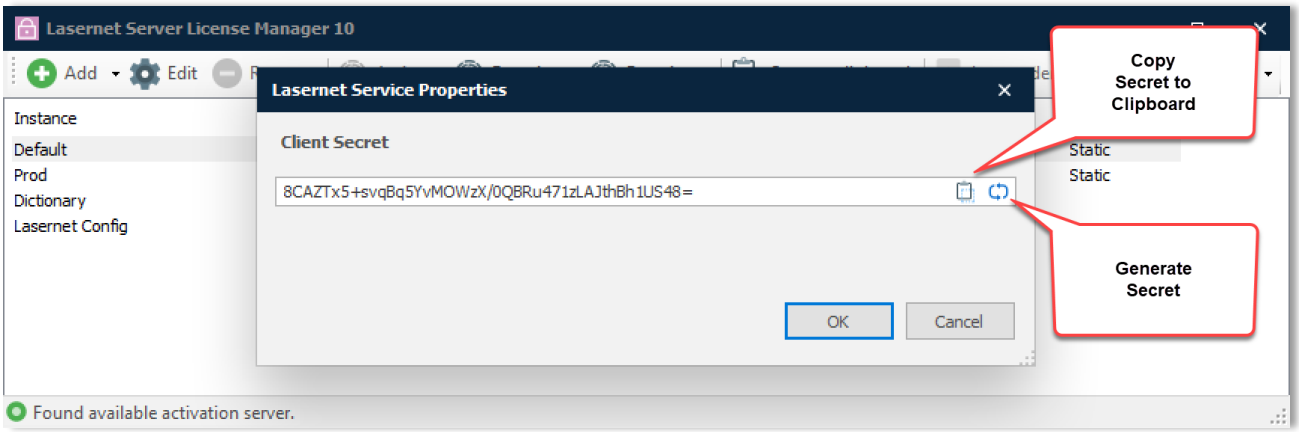
You can add a server to the Lasernet Config Server by clicking the **Add** button on the Servers page. This will display the Edit Server Instance dialog.



When entering data, please note that instance names are unique and cannot be changed; they can be only removed.

The hostname and port number can be changed at any time. Both the host and port must have an active connection to the server when a configuration is deployed or patched.

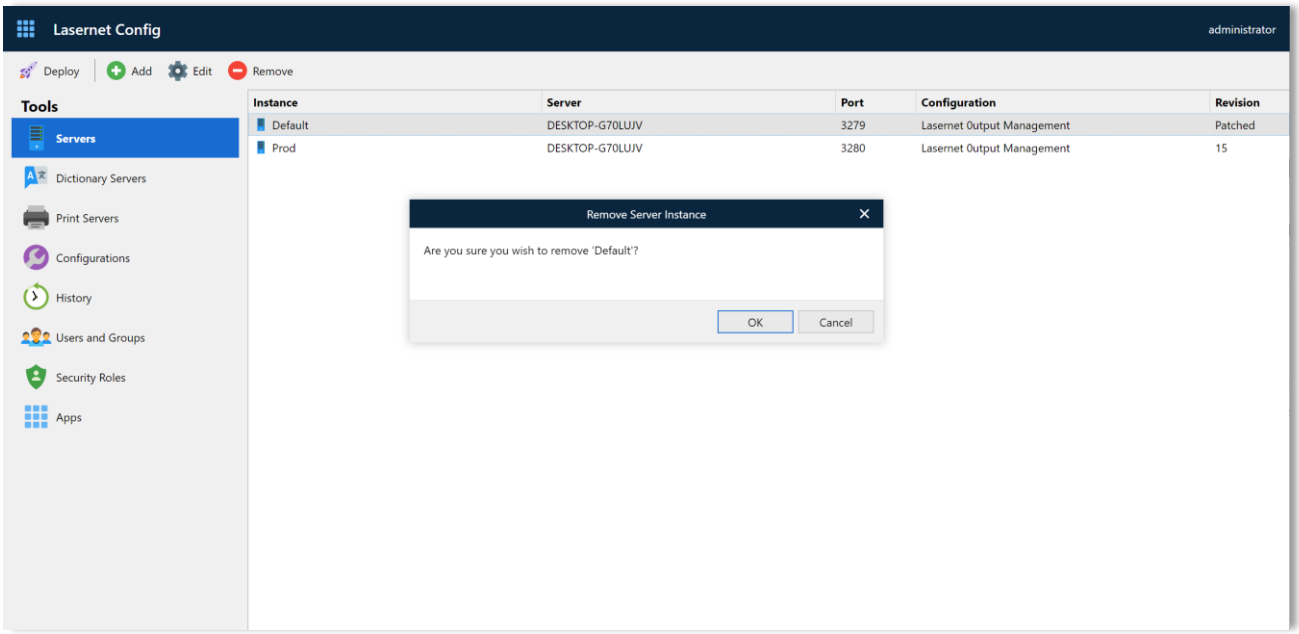
The client secret for each instance can be found and copied from the Lasernet Server License Manager. This was created when the instance was added to the server.



5.2.3 Remove Server

You can remove a server from the Lasernet Config Server by clicking the **Remove** button on the Servers page.

You are prompted to confirm your action before the server is removed.

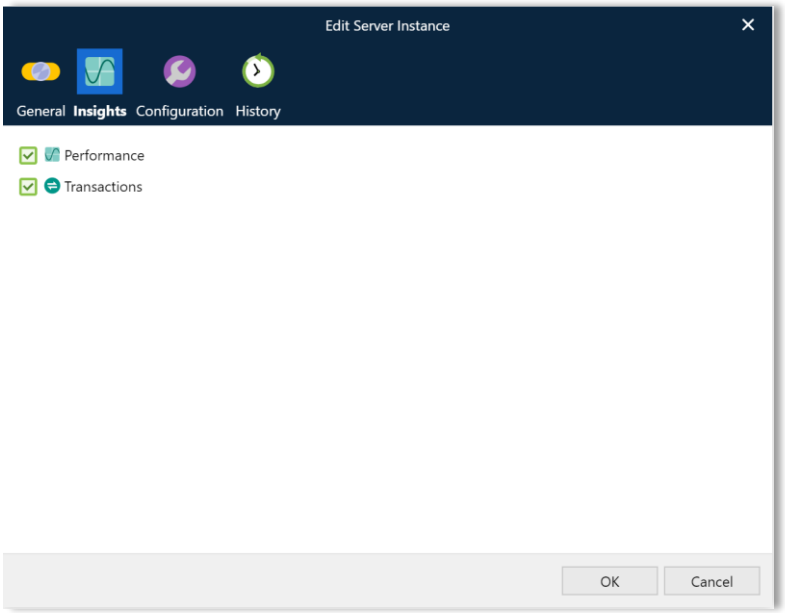


Services installed on the Lasernet Server are not removed after a server instance is removed from the Lasernet Config Server.

Please note that you are not able to deploy or patch to a server instance after removing it.

5.2.4 Insights

For each server instance you can activate the **Performance** and **Transactions** counters.



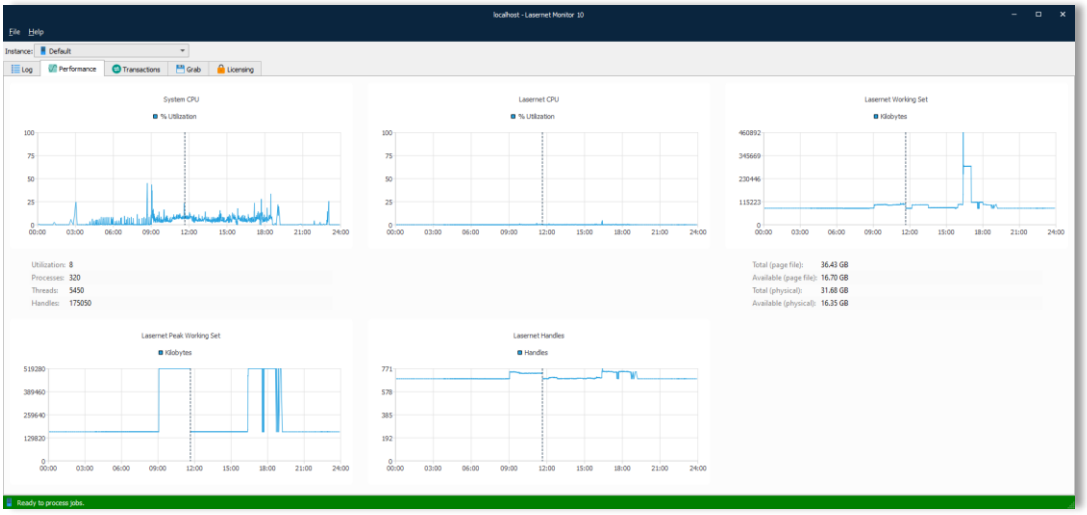
Insights will collect system details for the selected server instance when running jobs through Lasernet. Start the Lasernet Monitor, select the server instance and the **Performance** tab to show system details for the latest 24 hours.

Important: You must manually restart the Lasernet Server Instance, in the Windows Services app, before the selected settings will have impact on the selected Lasernet Server Instance.

5.2.4.1 Performance

Activate **Performance** to show details for:

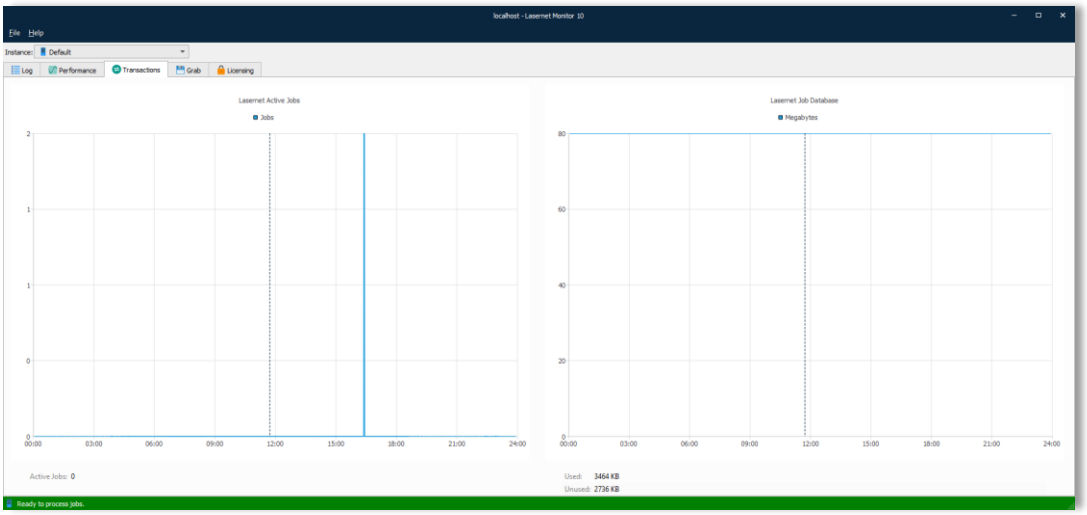
- Lasernet CPU
- System CPU
- Lasernet Workset Set
- Lasernet Memory Load
- Lasernet Handles



5.2.4.2 Transactions

Activate **Transactions** to show details for:

- Lasernet Active Jobs
- Lasernet Job Database (Monitor app only)


localhost - Lasernet Monitor 10
File Help
Instance: Default
Log
Performance
Transactions
Grab
Licensing
Lasernet Active Jobs
Jobs
Lasernet Job Database
Megabytes
Active Jobs: 0
Used: 3464 KB
Unused: 2736 KB
Ready to process jobs.

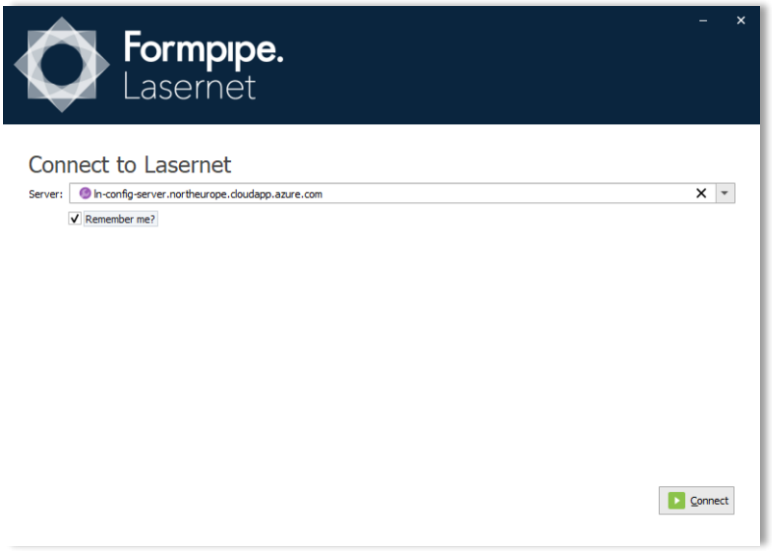
5.3 Configurations

5.3.1 New Configuration

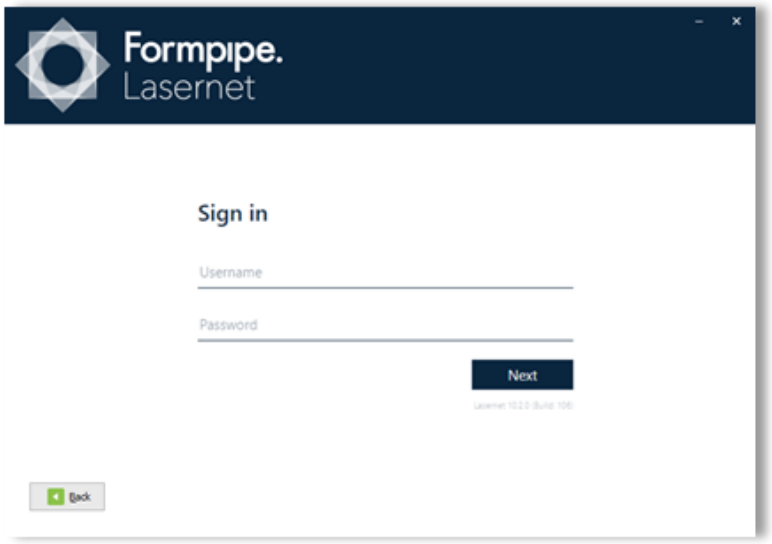
To create a new configuration, follow the steps listed below:

1. Launch the Lasernet Developer.

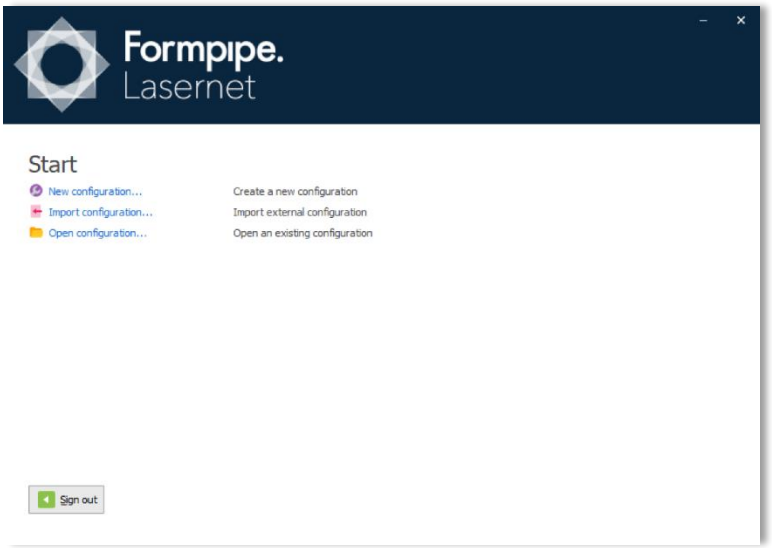
2. Enter your credentials and then click **Connect**.



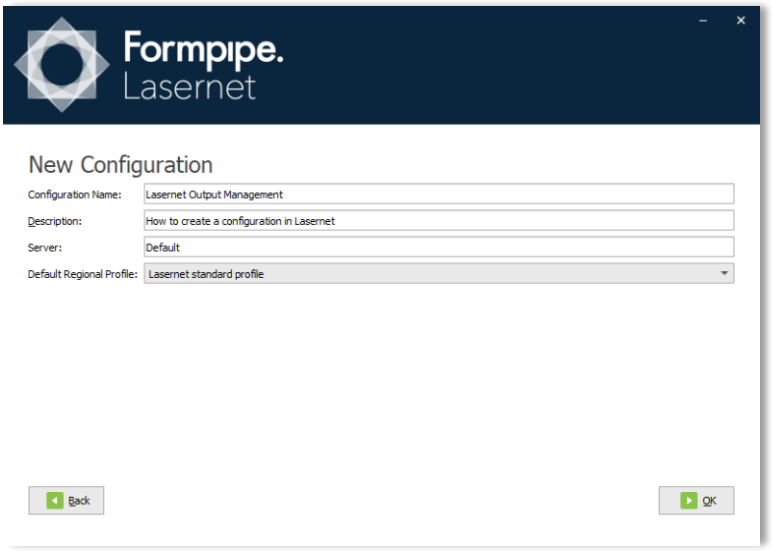
3. Enter your credentials and then click **Connect**.



4. On the **Start** screen, click **New configuration…**.



5. On the **New Configuration** screen, enter the required data and then click **OK**.



As a result, a new configuration is deployed to the Lasernet Config Server as ‘revision 1’.

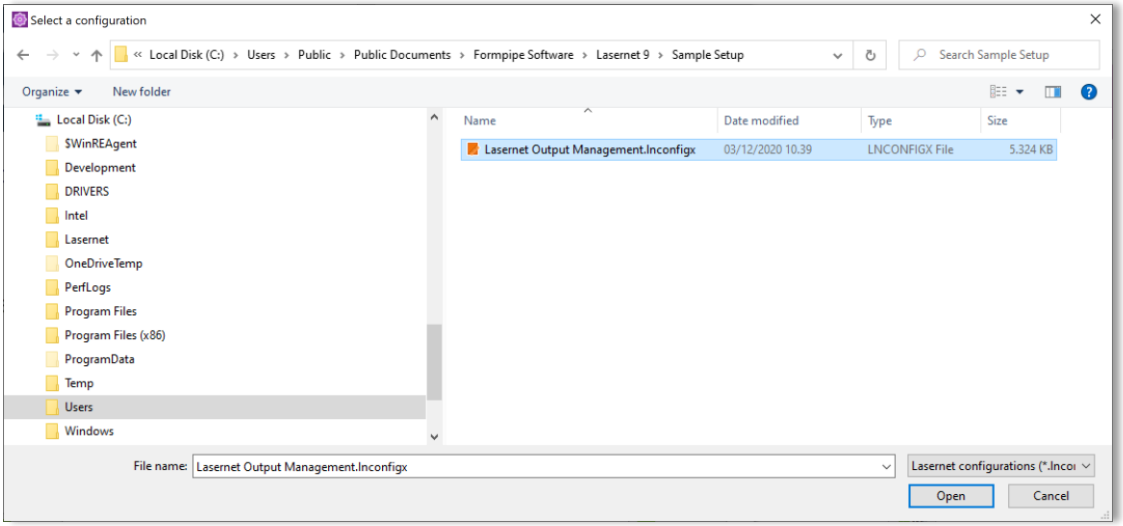
A checked-out copy of the configuration is stored for your Windows user on the local computer at this location:

C:\Users\[WindowsUser]\AppData\Local\Formpipe Software\Lasernet 10\Developer\Configurations

Important: Uncommitted objects are stored in this location. If you do not have access to this folder, they will not be committed.

5.3.2 Import Configuration

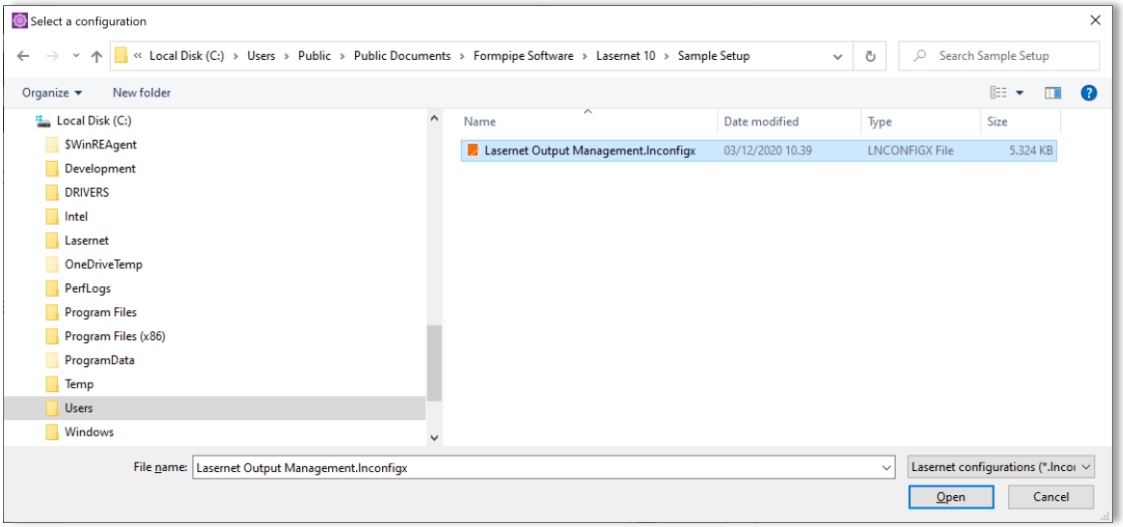
You can import an external configuration (*lasernet.lnconfig*) from a file, if coming from an older version of Lasernet.



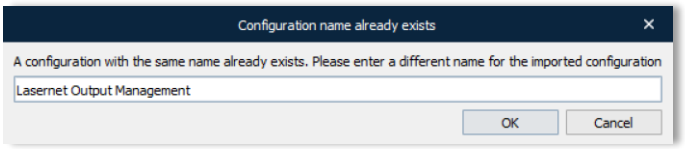
In addition, you can also import configurations exported from Lasernet 10 (*[name].lnconfigx*).

The Lasernet 10 installer includes a sample setup which can be imported from here:

C:\Users\Public\Documents\Formpipe Software\Lasernet 10\Sample Setup\Lasernet Output Management.lnconfigx



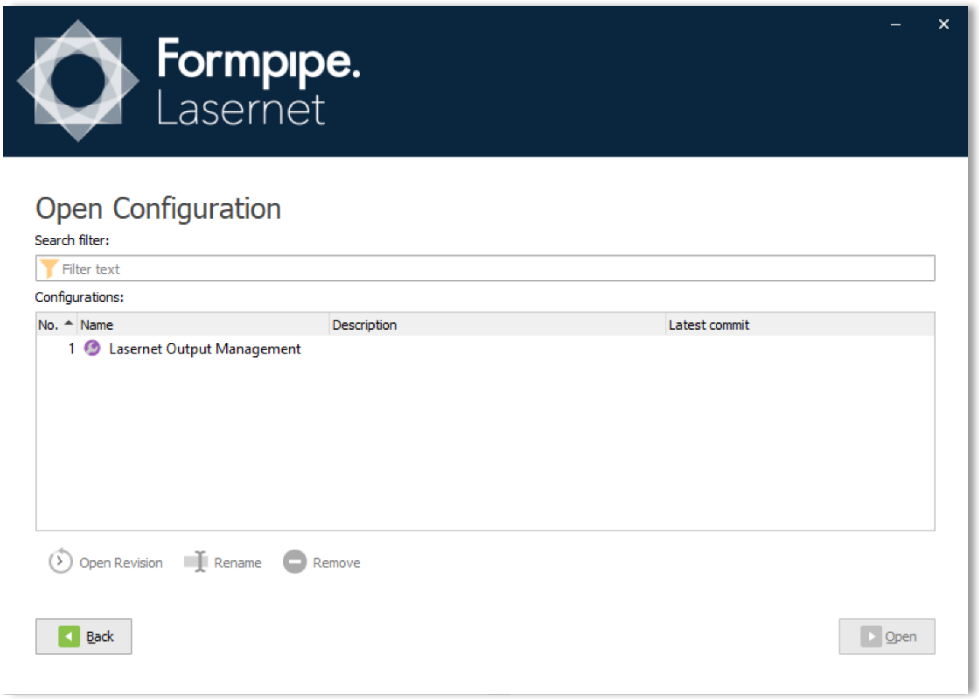
Lasernet Developer prevents you from importing a configuration with the same name to the Lasernet Config Server. You will be prompted to rename the imported configuration if the name already exists.



You cannot use the Export Configuration from the Lasernet Developer to export a full configuration from one computer and import it to another, replacing the configuration completely. Instead, the Exported Configuration can only be actioned from start page of the Developer, opening the exported configuration as a whole. If you remove a configuration before you open the exported configuration, your revision history will be lost.

Instead, you must use the Export and Import Objects functionality and select individual objects from the configurations as in previous versions of Lasernet. This is to ensure that the revision and history log will be updated successfully.

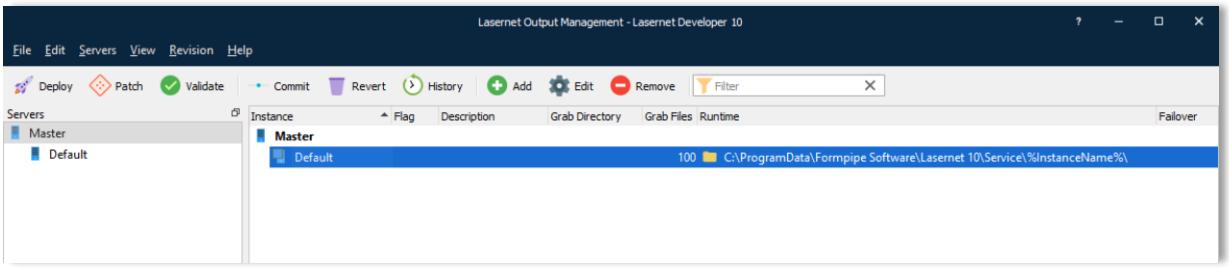
5.3.3 Open Configuration



You can open, rename or remove an existing revision of a configuration stored on the Lasernet Config Server.

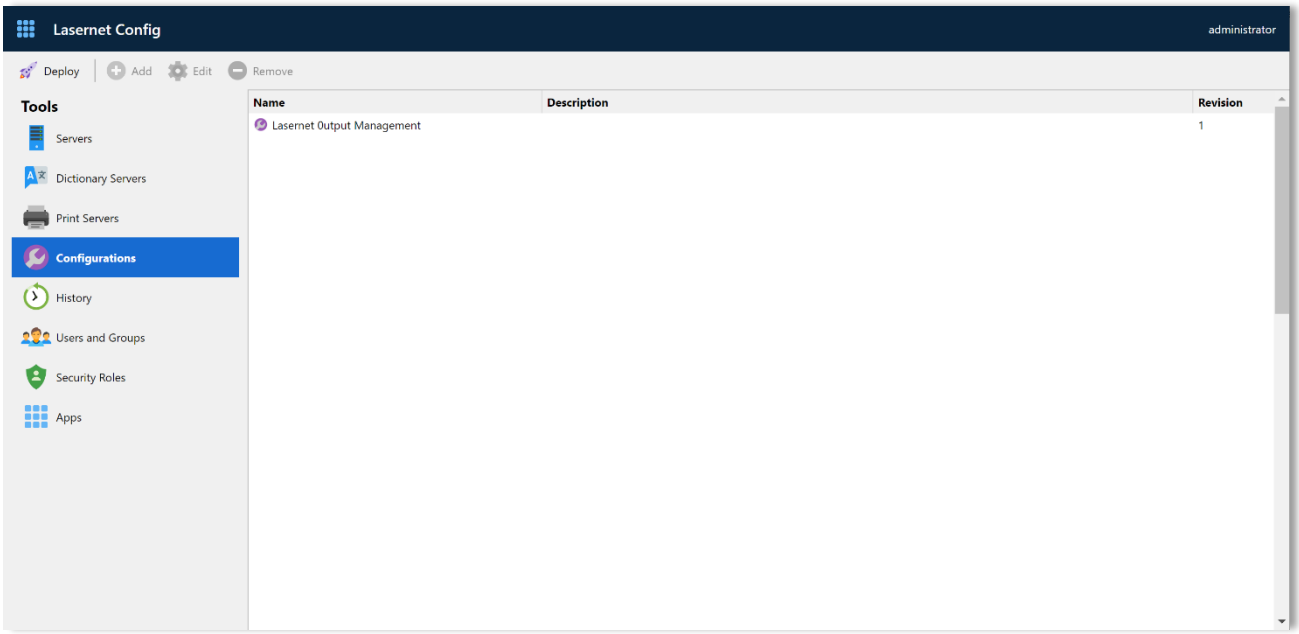
A configuration cannot be opened more than once at the same time by the same Windows user on the same computer.

A configuration opens in the Lasernet Developer application.



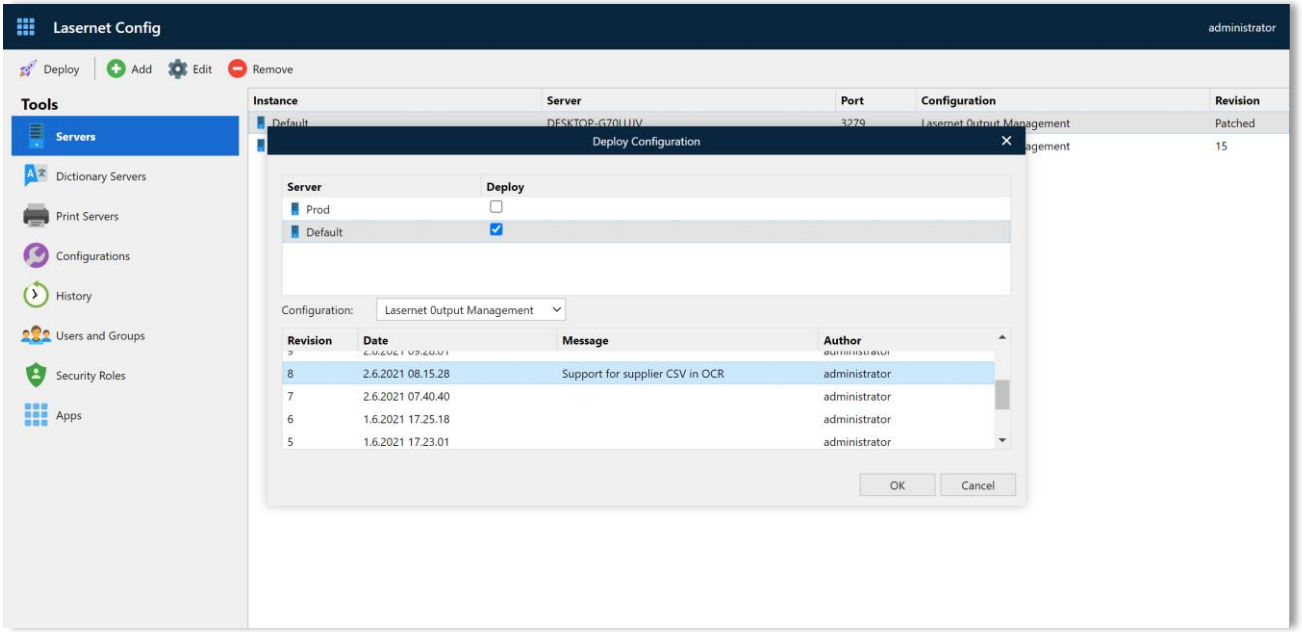
5.3.4 List of Configurations

After you have created your first configuration it is stored in the Lasernet Config Server and figures in the **Configurations** tab.



5.4 Deploy

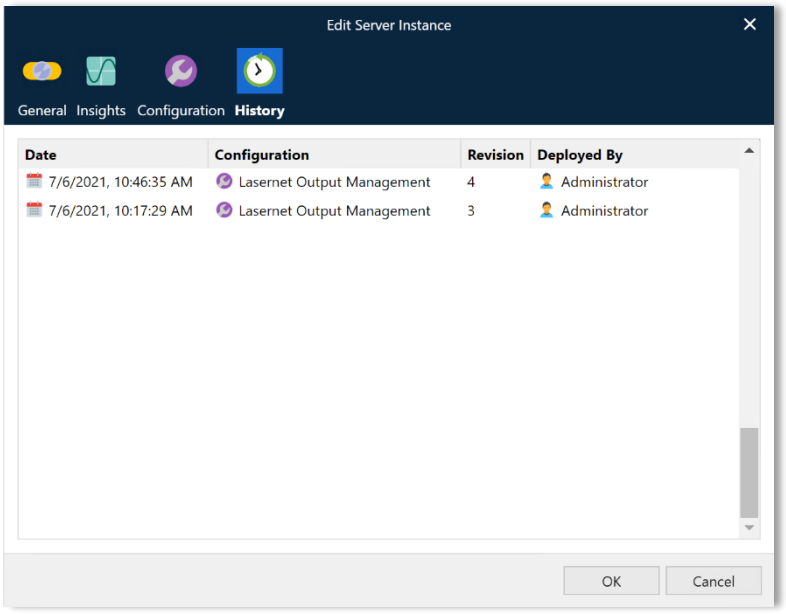
To view or deploy existing revisions of a configuration, start the Lasernet Config Server, and click the Deploy button in the tool bar.



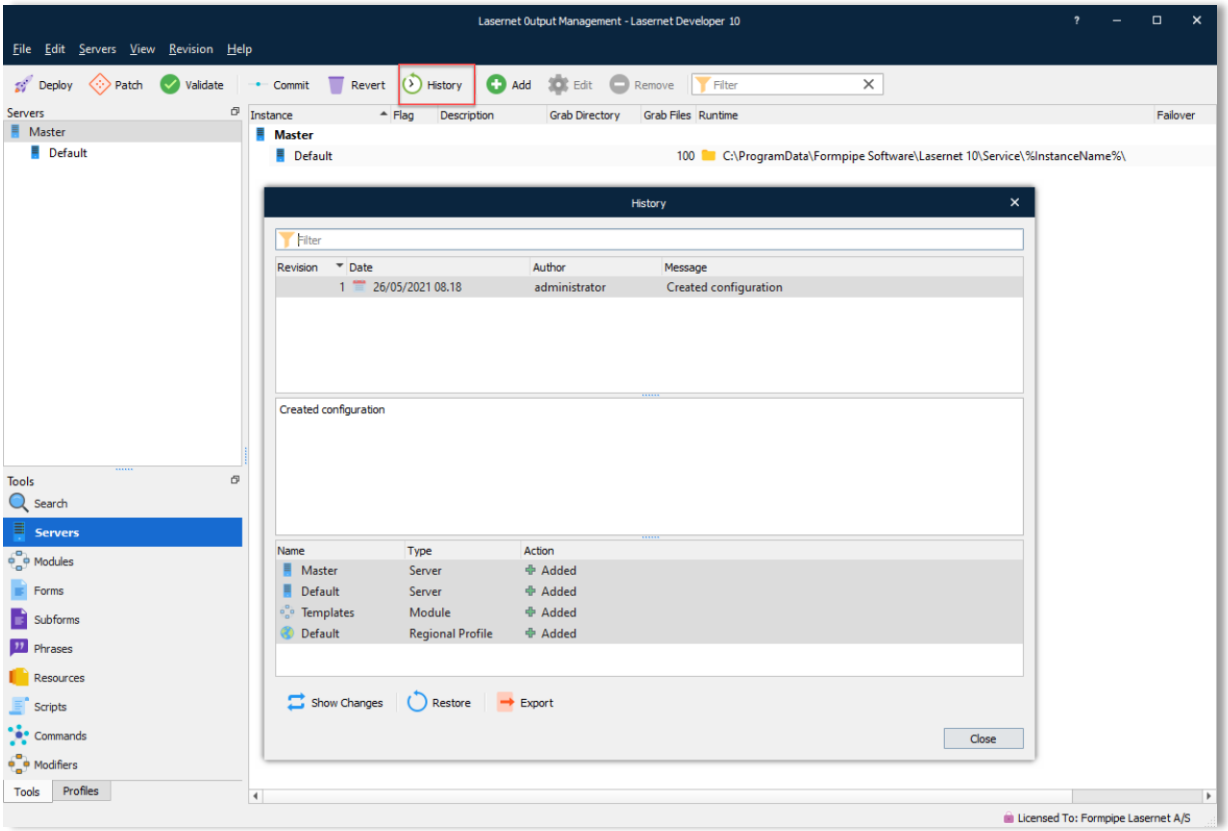
In the **Deploy Configuration** dialog you view and select any revision of a configuration you would like to deploy to any instance of a server available in the dropdown list.

5.4.1 History: Configuration Revisions

In the Lasernet Config Server you view the history of any revision deployed to any server instance. Select the server instance name and click the **Edit** button. In the Edit Server Instance dialog select the **History** tab.

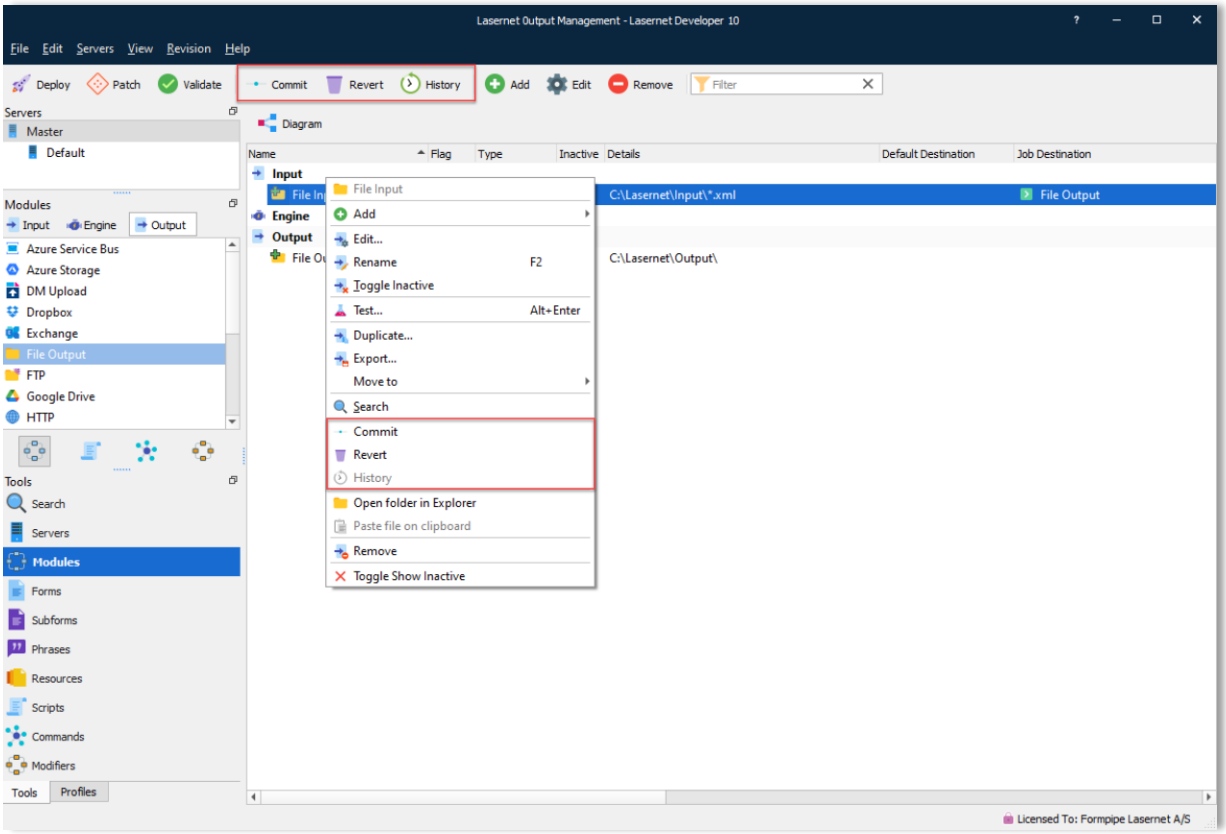


In the Lasernet Developer, you can also view and select any revision of a configuration by clicking the **History** button.



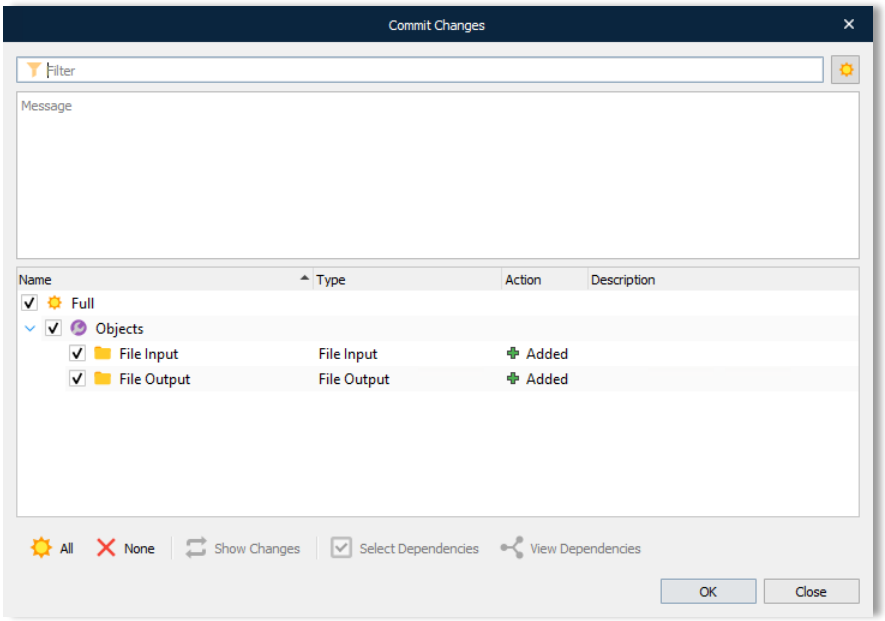
When you make any changes to a configuration, the changes are stored locally. To push those changes to the Lasernet Config Server, you have to **commit** them.

If you are not satisfied with the changes, you can **revert** them before committing or **restore** them after a commit.



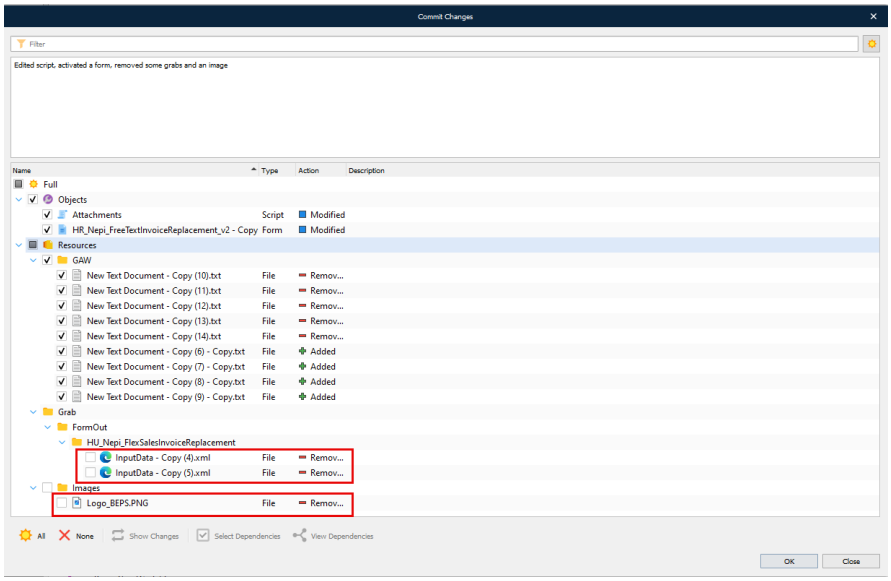
5.4.2 Commit

To push any new changes (additions, edits, deletions) to the configuration server since the last revision, click **Commit**.



Click **OK** to confirm your action. The changes will then be sent to the configuration server and a progress window will appear.

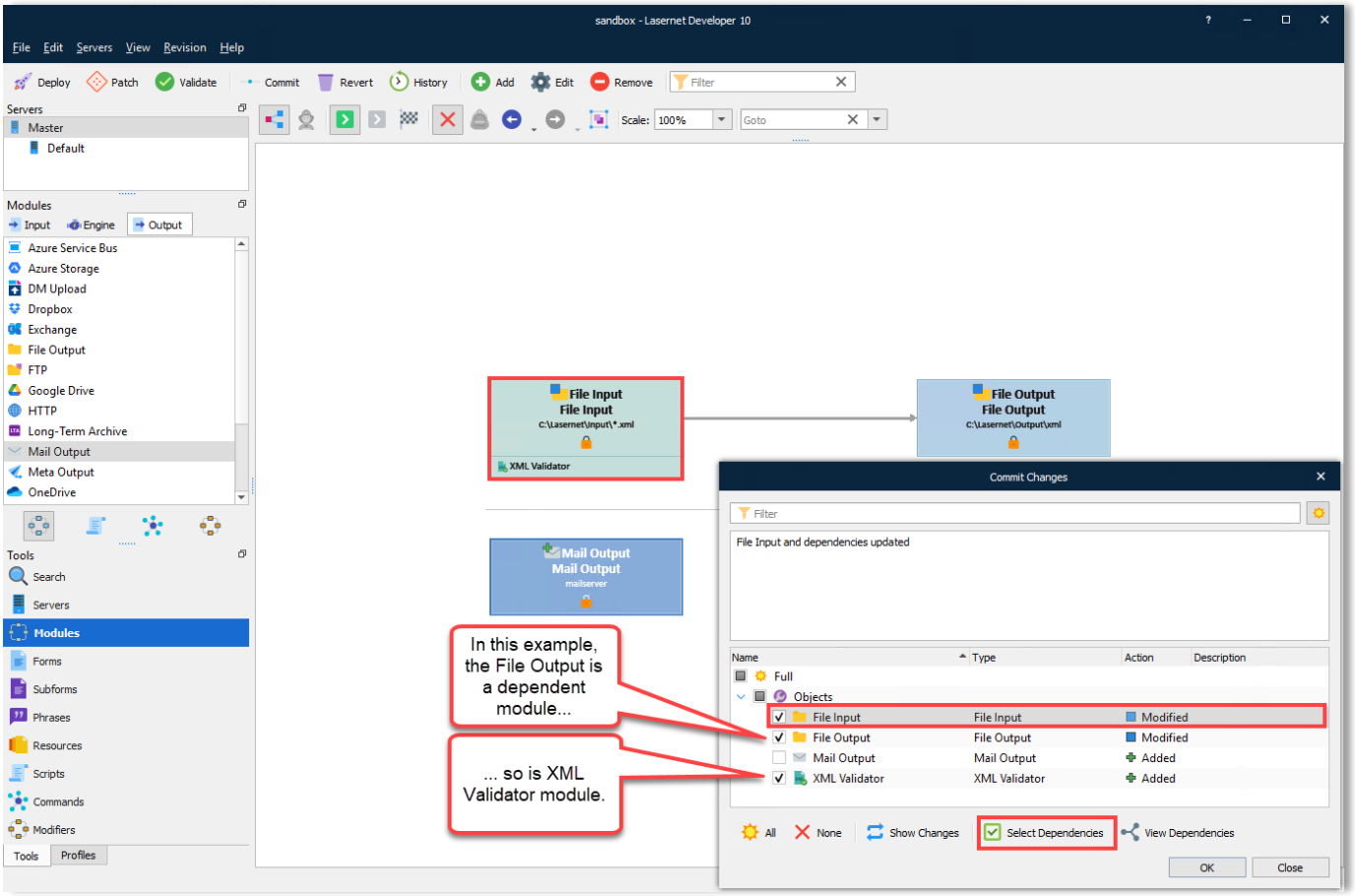
Note: When committing changes to the **Resources** folder, including when removing or adding files to **Grabs**, **Overlays**, and **Images**, ensure that these items are selected in the commit tree. If you fail to do so, they will not be committed.



Once complete, click **Close**.

5.4.2.1 Dependency Walker

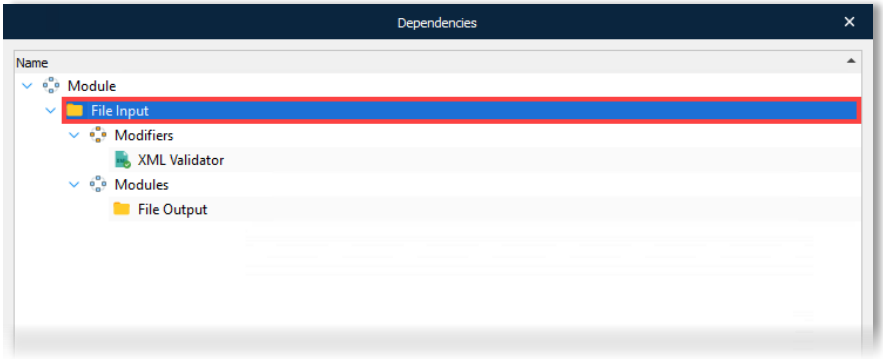
Select Dependencies – Automatically selects all other objects, related to the selected object, that have not yet been committed.



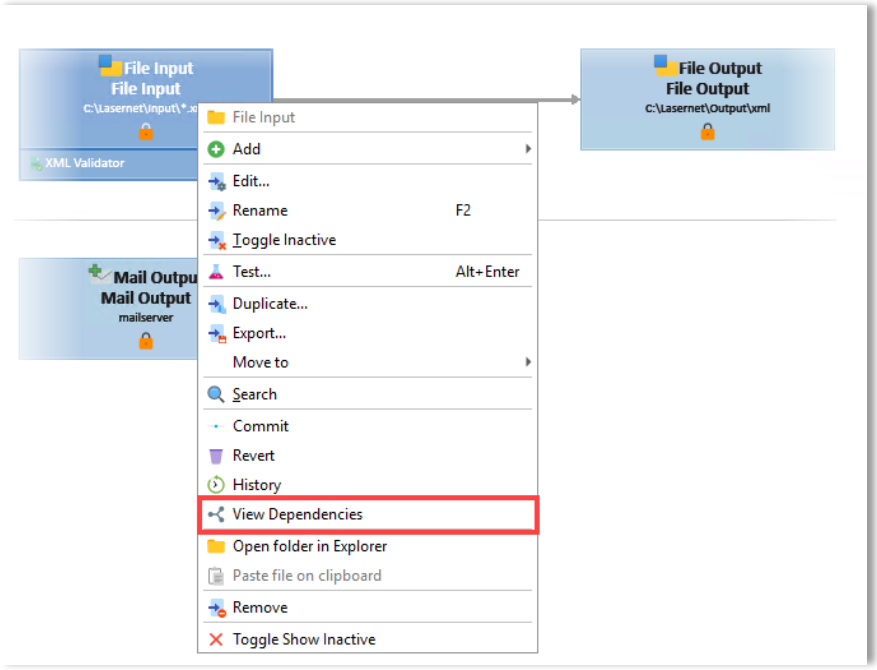
Note: Lasernet will not show:

- More than one level of dependencies
- References used by script functions
- References from JobInfo Substitution
- DataType profiles used from Web Server input
- Database Connections added to SharePoint module

View Dependencies – Displays all dependencies to the selected object.

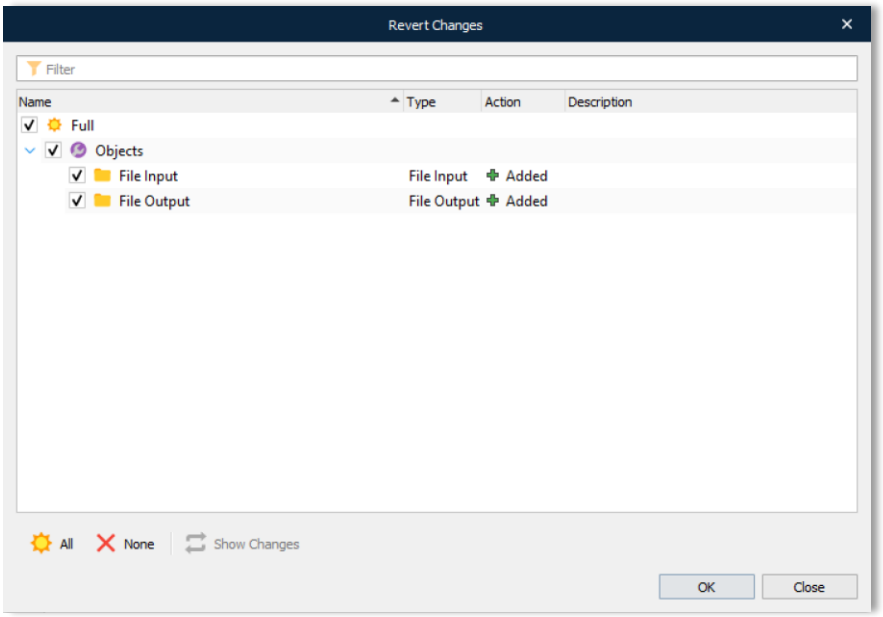


Note: You can also select **View Dependencies** by right-clicking a module or form.



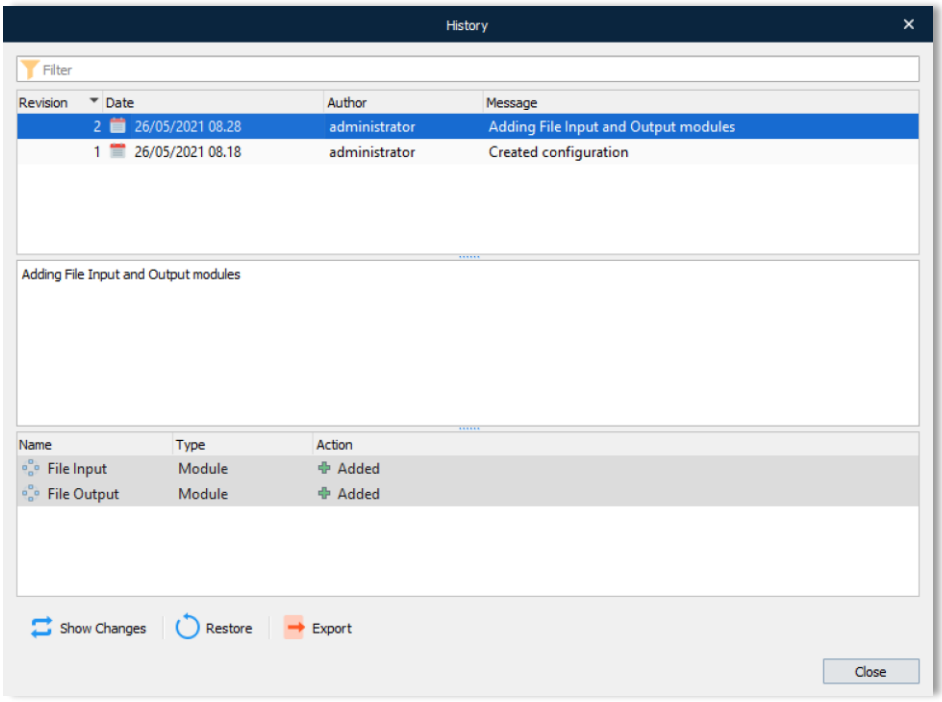
5.4.3 Revert

Click **Revert** to revert changes for selected objects since the last commit.



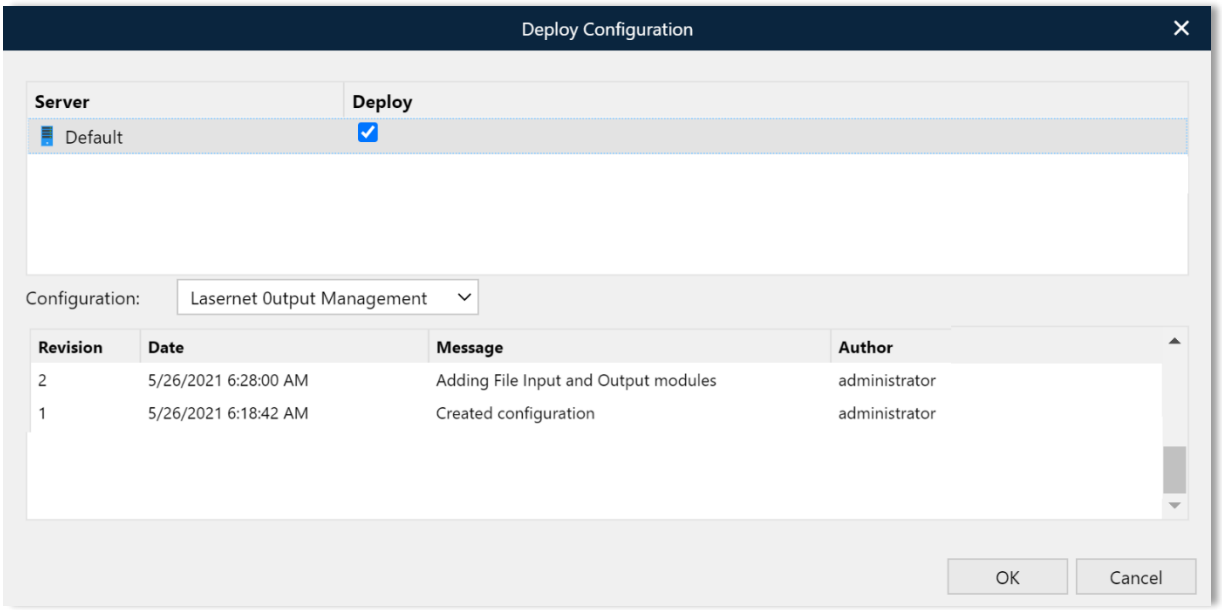
5.4.3.1 History

To view all of the commit changes as well as user information for past revisions, click **History**.



5.4.4 Deploy to Server

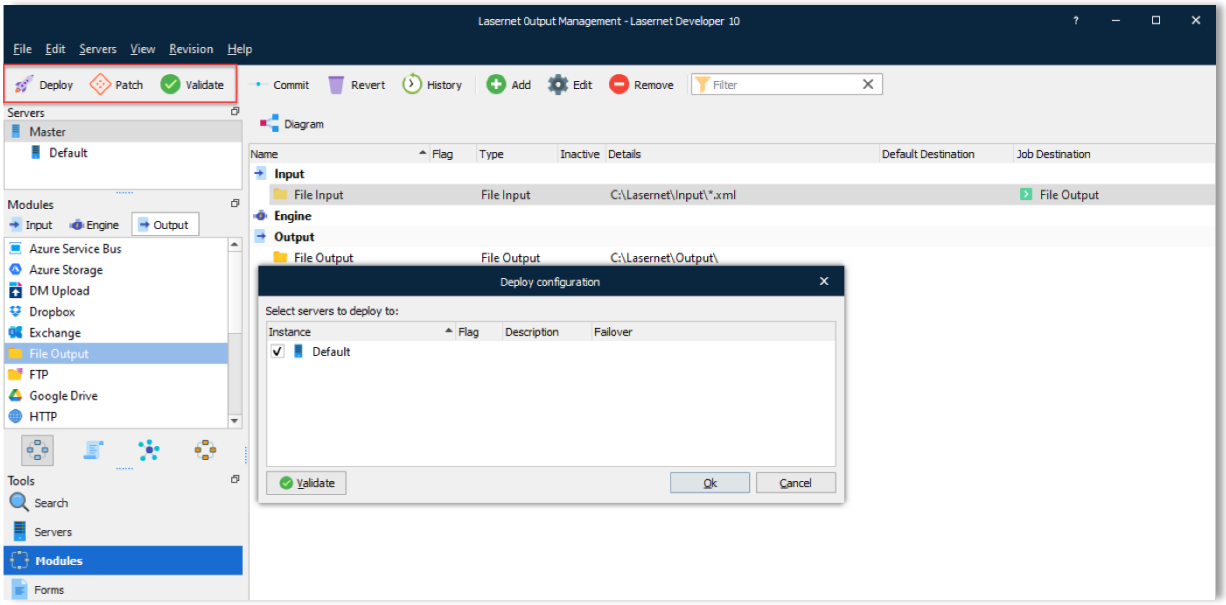
Once the changes made within a revision are accepted and approved, the revision can then be deployed to one or more servers. To do this, navigate to the Lasernet Config Server and click the **Deploy** button for the revision you want to deploy to the server.



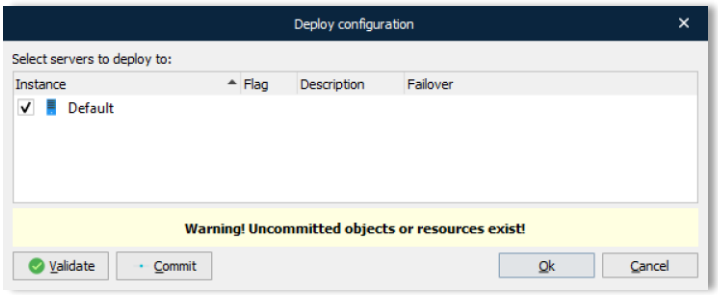
5.4.4.1 Deploy in Lasernet Developer

You can also activate the **Deploy** button in the Lasernet Developer application to deploy changes to a server.

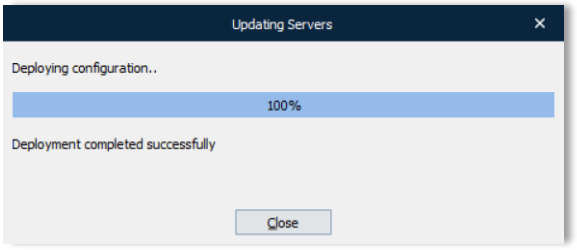
Notes: Only committed objects can be deployed.



If you try to deploy objects or resources from the configuration you have not committed, you will see a warning message in the **Deploy configuration** dialog. You can click the **Commit** button at this point to commit the selected object(s) or click **Ok** to deploy a configuration without the uncommitted objects.



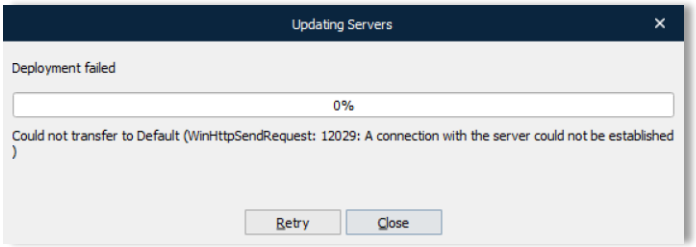
Click **OK** to confirm. The deployment will then start with a progress dialog.



Once completed, click **Close**.

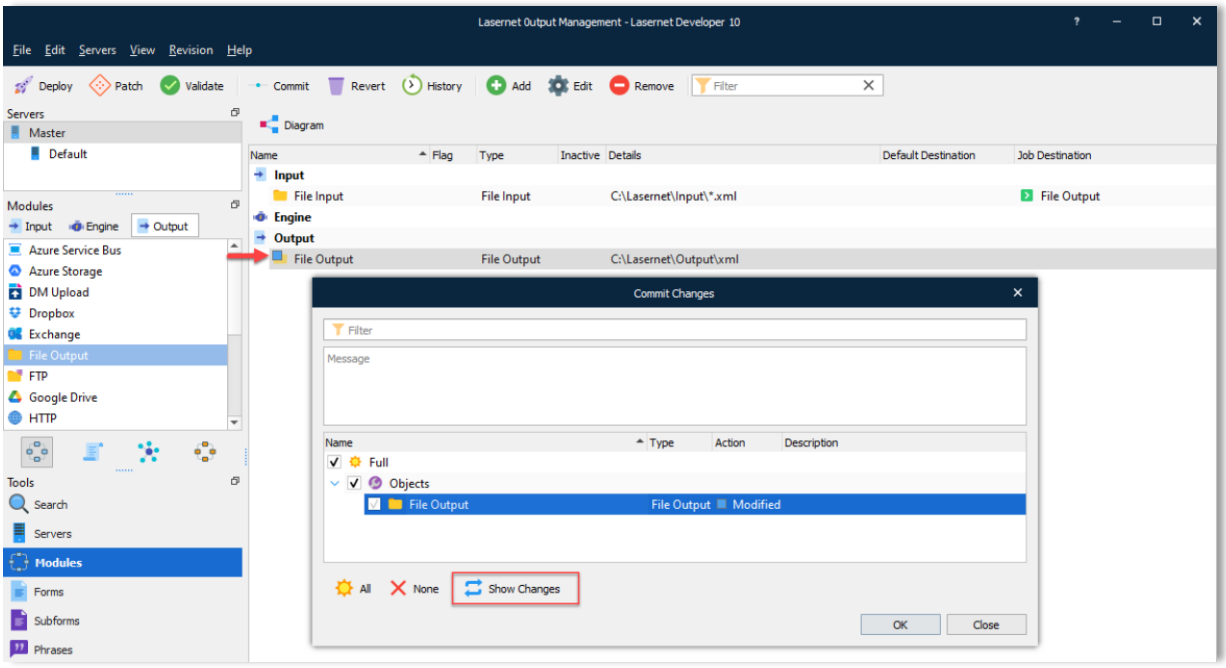
Note: Before deploying, ensure there is an active connection between the Lasernet Developer, Lasernet Config Server and the Lasernet Service is running.

If the selected server Instance is not committed or stopped, or the Lasernet Config 10 service or connections are not running, the transfer process will fail.

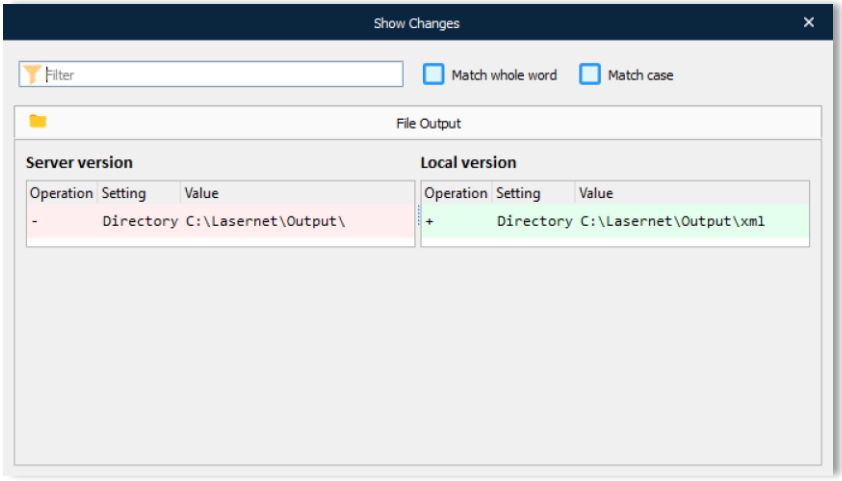


5.4.4.2 History: View Changes

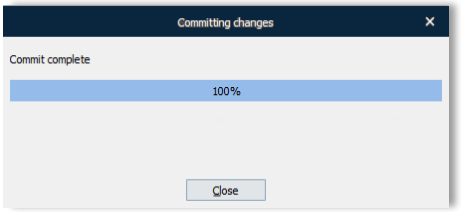
It is possible to view changes while committing them. To do this, click the **Show Changes** button.



Changes are shown in a separate dialog.



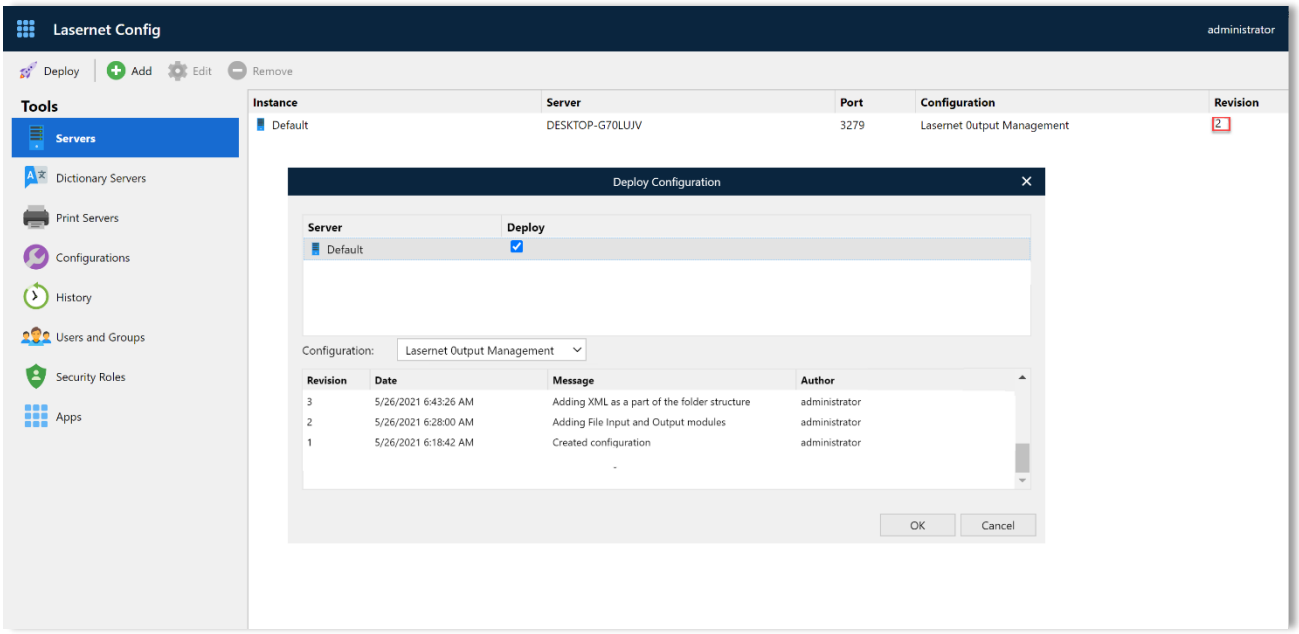
Confirm the commit by clicking **OK.** The progress dialog will then appear.



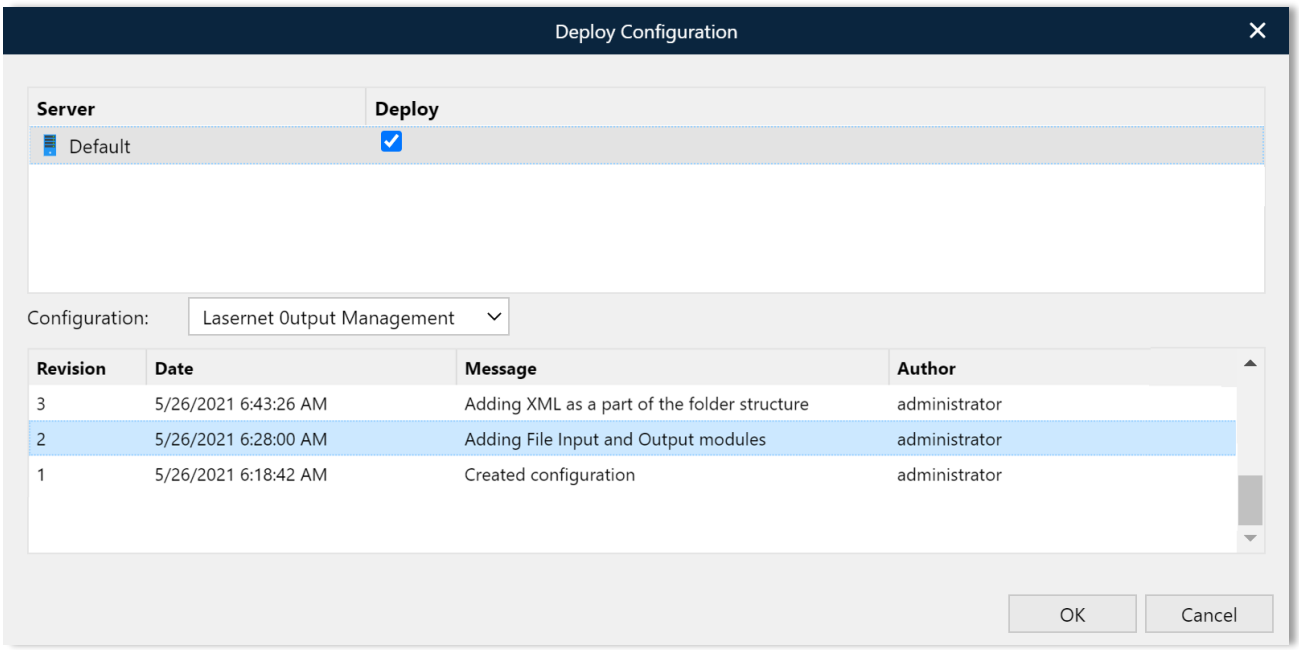
Once completed, click **Close**.

5.4.4.3 Deploy in Lasernet Config Server

In the Lasernet Config Server, select the Configuration that contains changes you want to deploy.



Select the newest revision to deploy the latest committed objects to the server and click OK.

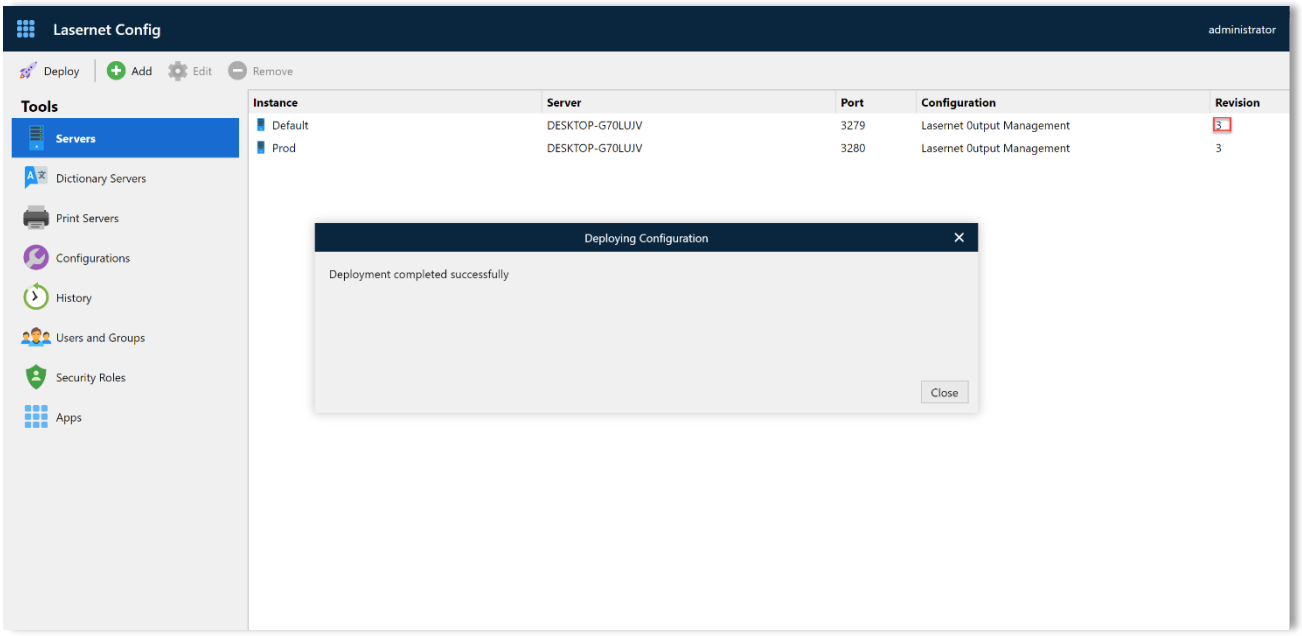


To deploy another revision select any of the revisions in the Deploy Configuration dialog and click OK.

The **Deploy** tool in the Lasernet Config Server work similarly to the one in the Lasernet Developer application. The only difference is that you can deploy old revisions from the Lasernet Config Server,

whereas you can only deploy the newest revision from Lasernet Developer. You can, however, open an old revision in the Lasernet Developer for viewing and exporting purposes.

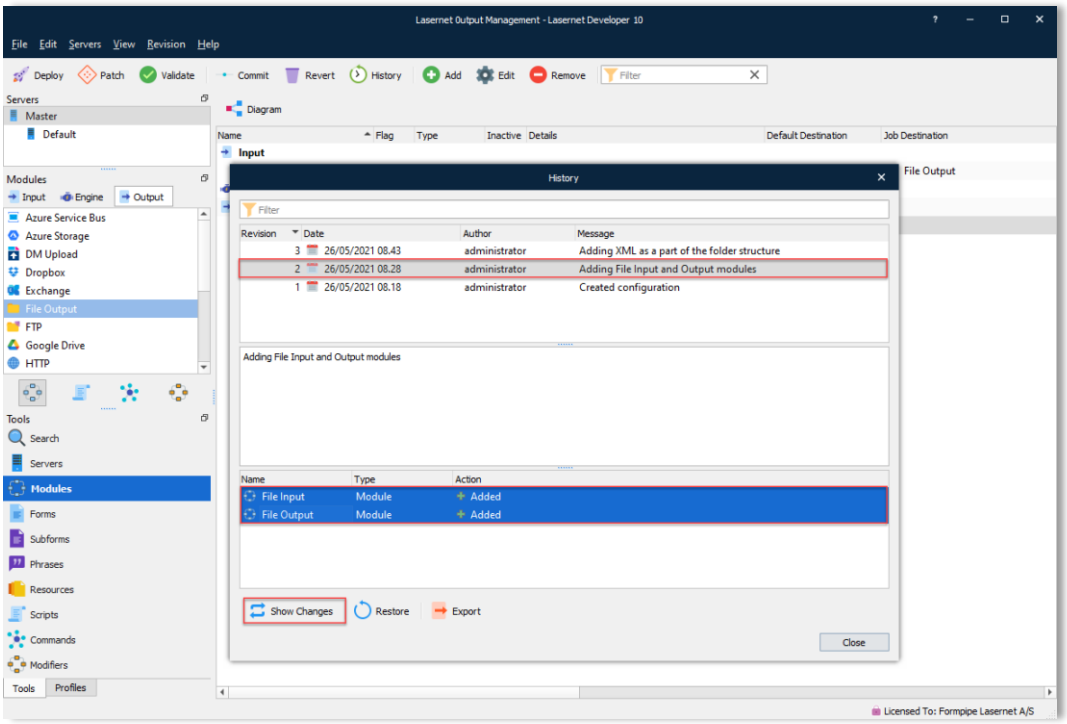
Once the deployment has completed successfully the dialog will report about this.



The example shows that **Revision 3** of the **Lasernet Output Management** configuration is now active for the server instance named **Default**.

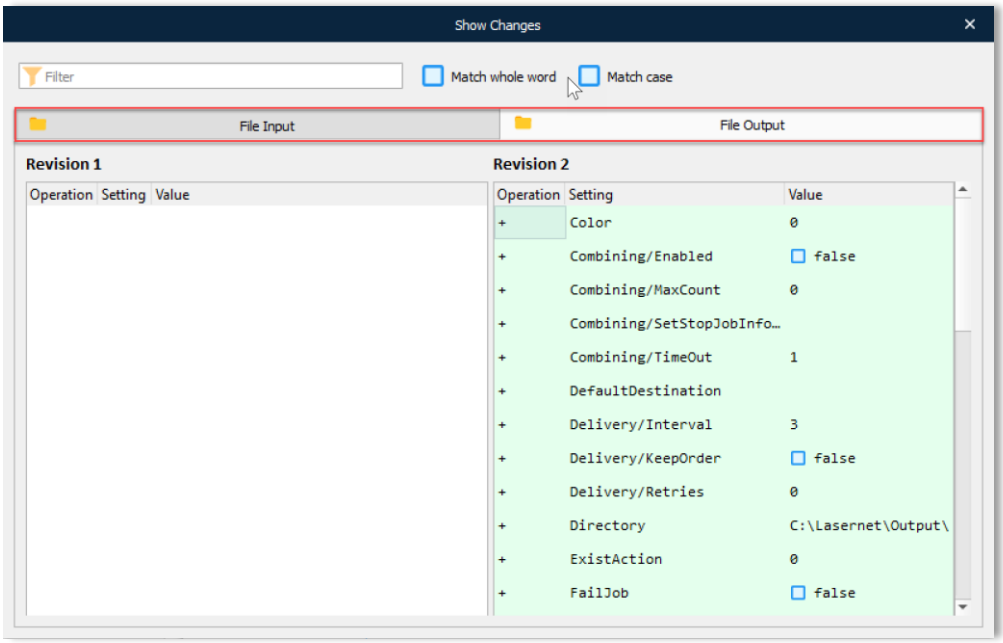
5.4.4.4 History: Show Changes and Restore

In the Lasernet Developer application, click the **History** button to view a list of changes made to a configuration.

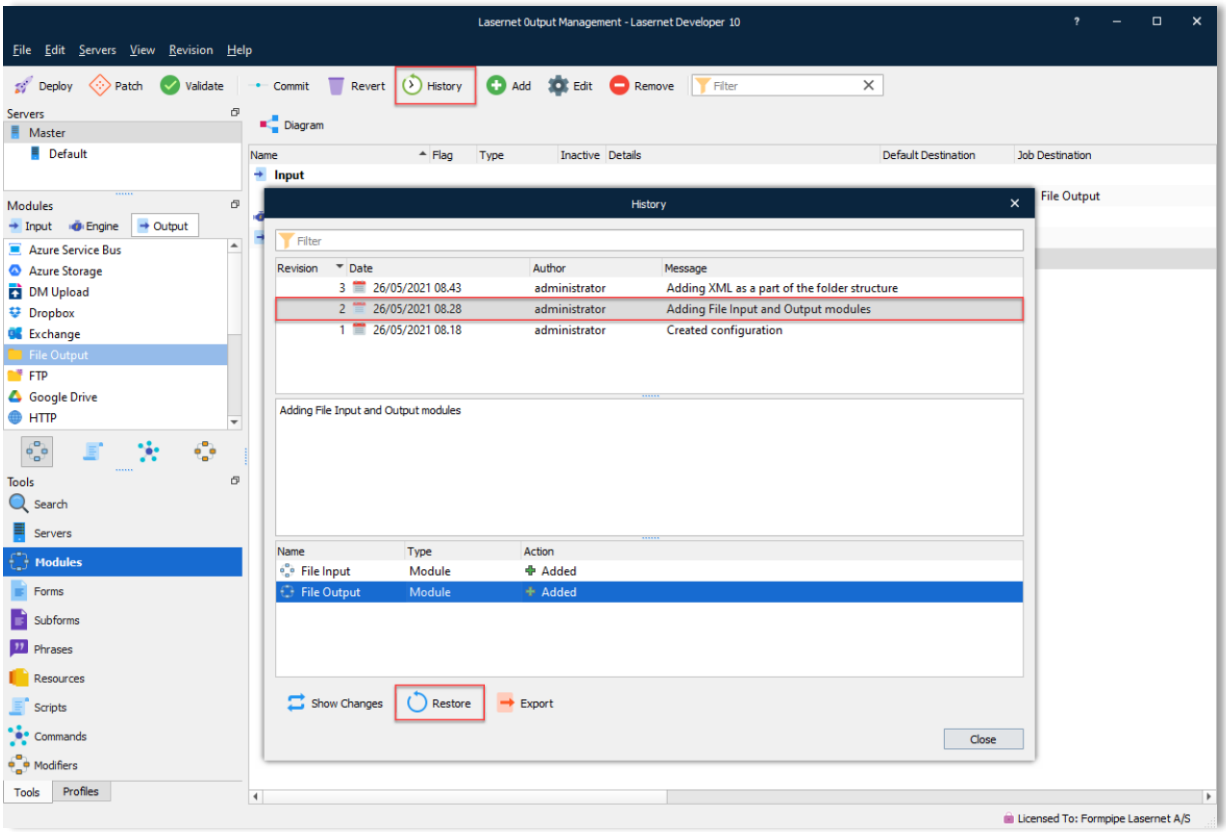


You can select up to 10 objects at a time to compare across revisions.

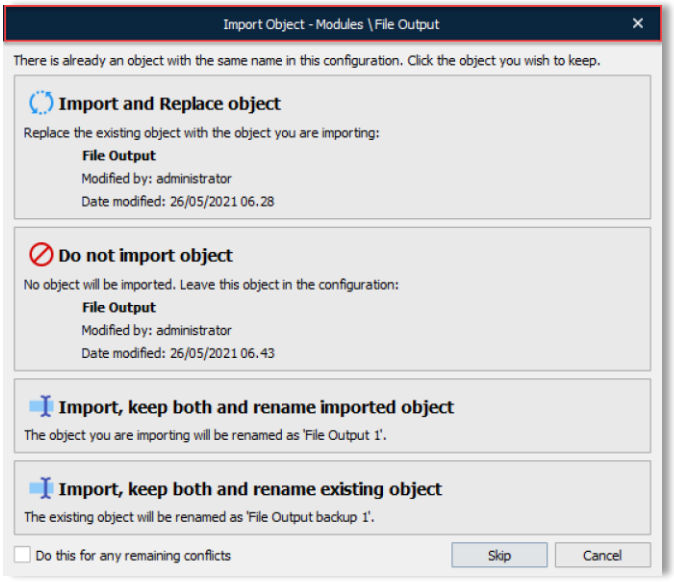
The example below shows two objects with all the settings added at the same time. To view changes separately, select the object tabs.



In the **History** dialog, click the **Restore** button to restore the selected object from an old revision and import it to the newest revision.



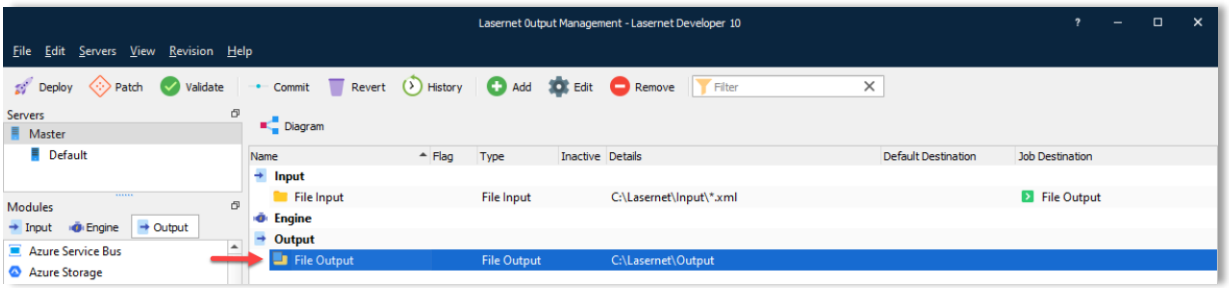
From the **Import Object** dialog (also accessible via the toolbar: **File** > **Import Objects**), select the required action.



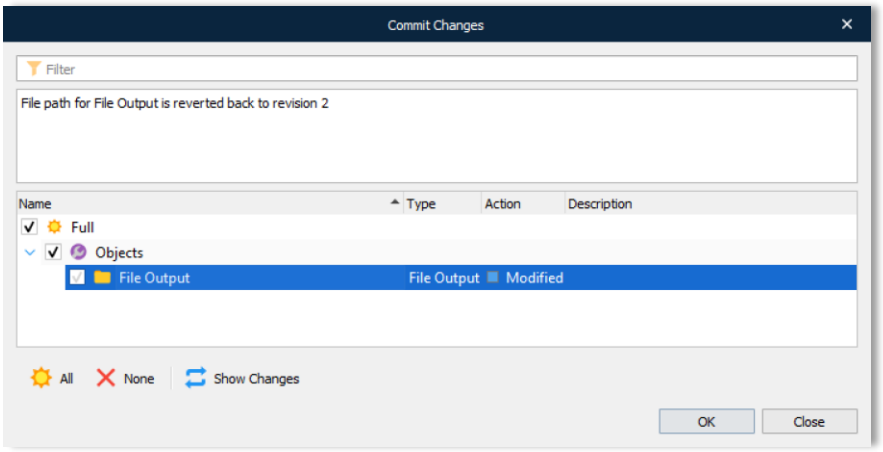
Action	Description

Import and replace object	Replaces the existing object with the one being imported.
Do not import object	No object imported. All the objects stay the same.
Import, keep both and rename imported object	Keeps the existing object without renaming it, imports the new object and renames it.
Import, keep both and rename existing object	Keeps the existing object, renames it, and imports the new object without renaming it.

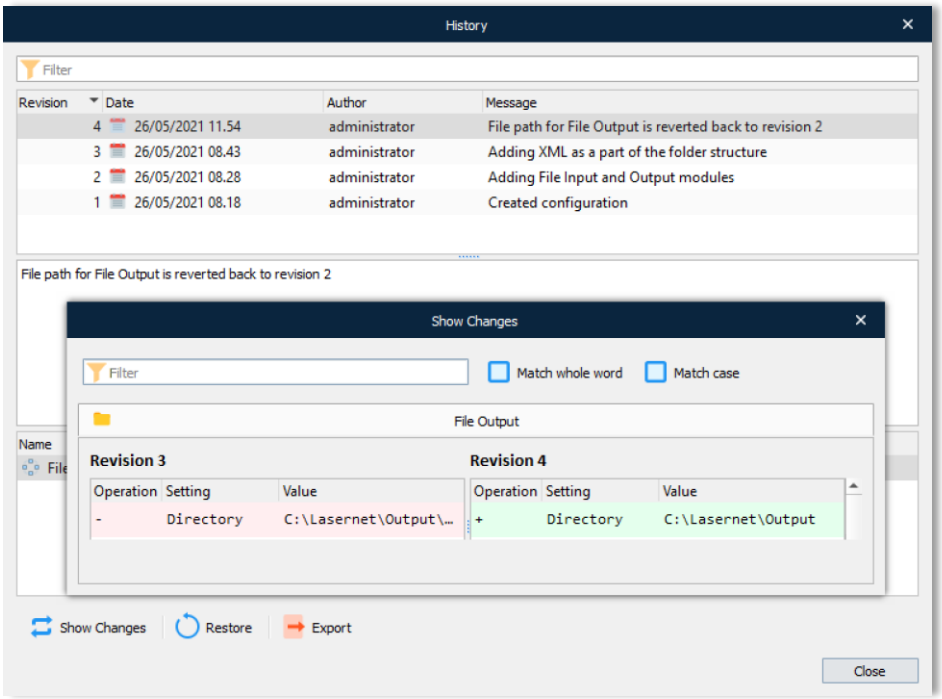
If the old revision of the imported object has the same hash as the new one, the object will not be registered as modified.



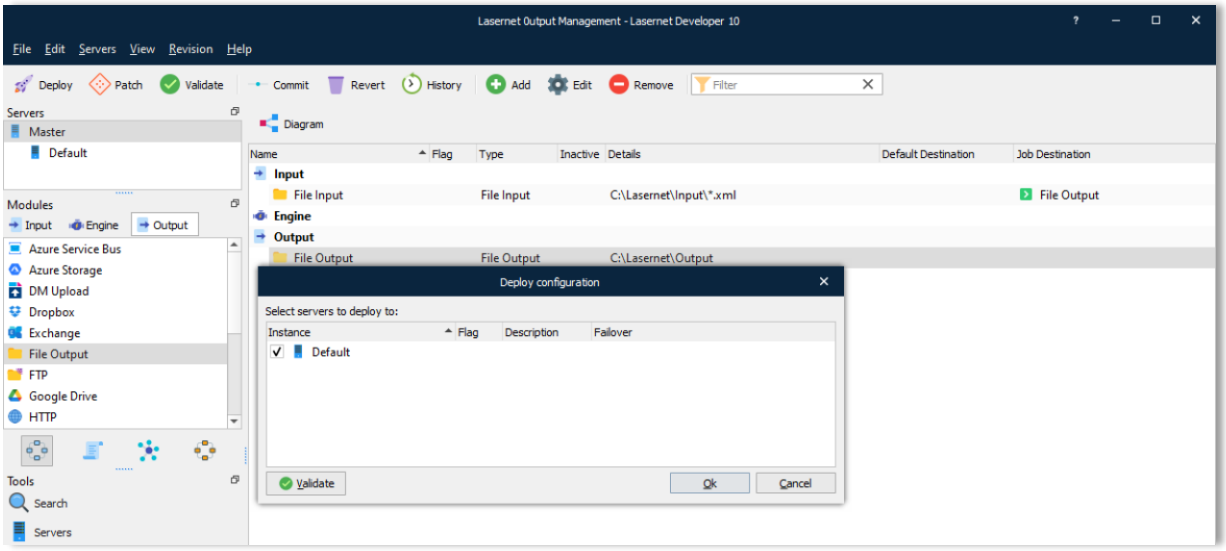
If the imported object differs from the one in the latest revision, it is defined as modified and must be committed before the revision is updated.



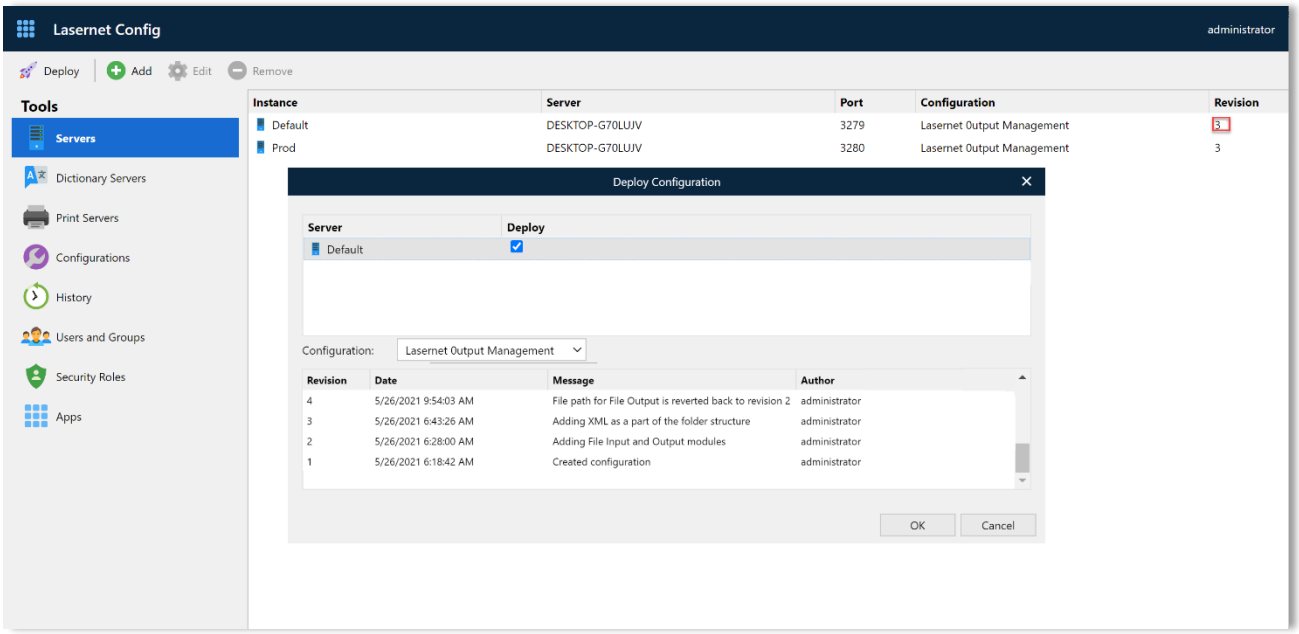
To validate that the restored object contains a modified property, click **Show Changes**.



After committing, the configuration is deployed as a new revision.



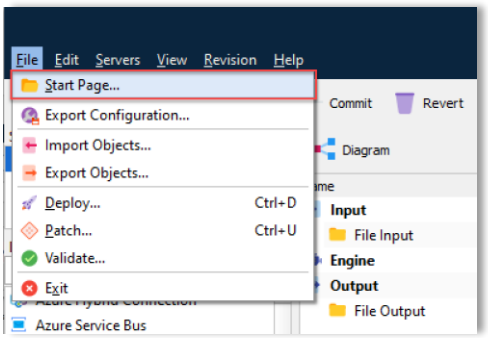
The example below shows that **Revision 4,** which includes the restored object, is active.



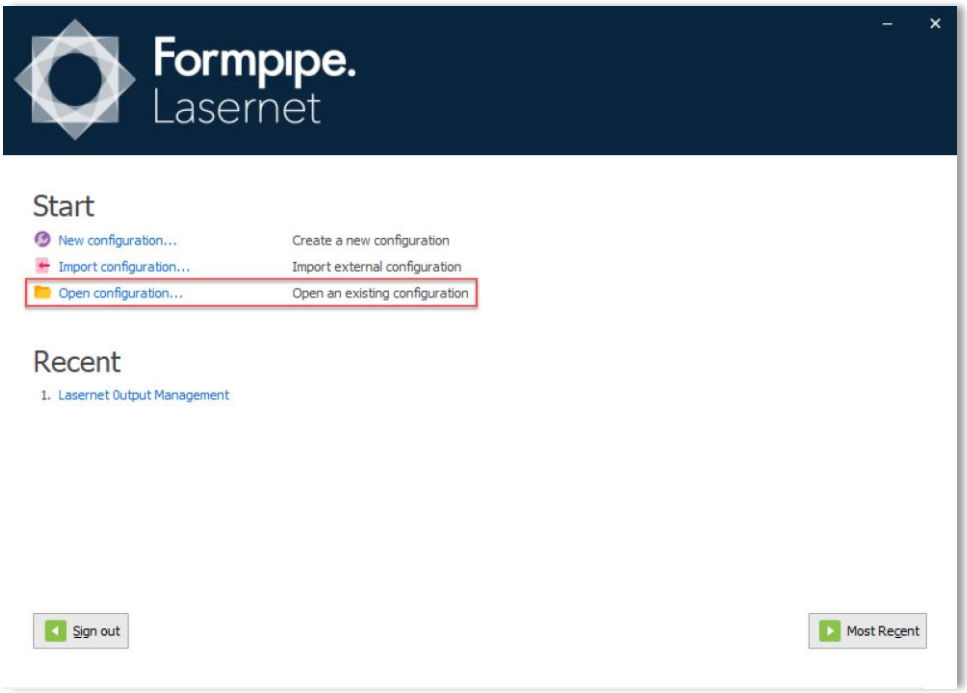
5.4.5 Open Old Revision of Configuration

To open an old revision of a configuration, follow the steps listed below:

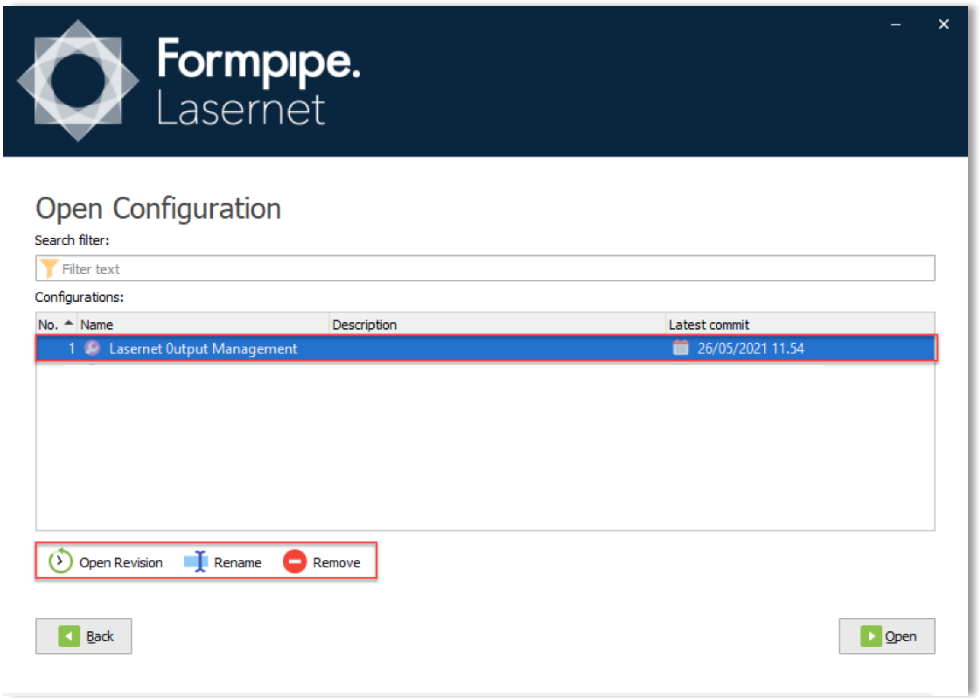
1. In Lasernet Developer, click **Start Page…** on the **File** menu.



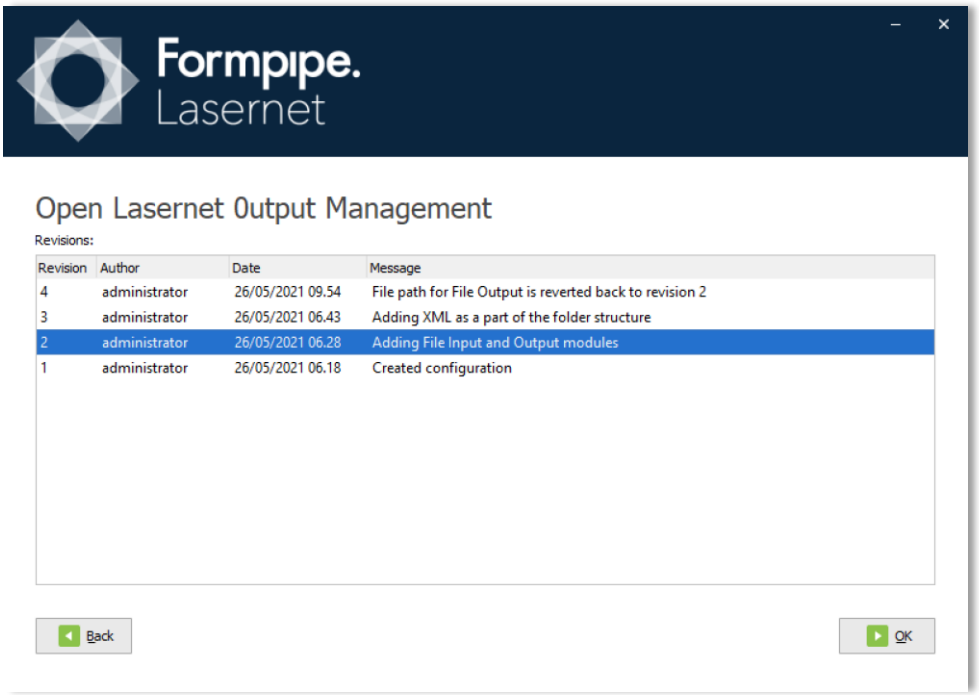
2. In the dialog displayed, click **Open configuration…**.



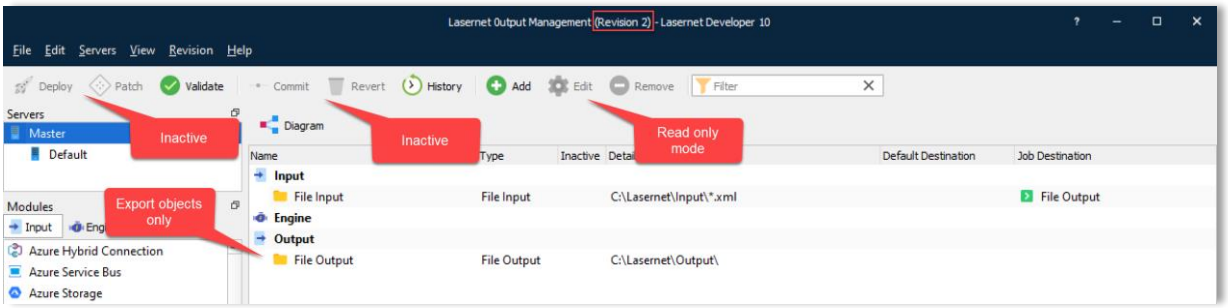
3. On the **Open Configuration** screen, you can rename or remove a configuration from the Lasernet Config Server, or you can click **Open Revision** to open any revision of the selected configuration.



If you have restricted user rights in the Lasernet Developer application you can still open an old revision of a configuration, however most objects will be in read-only mode.



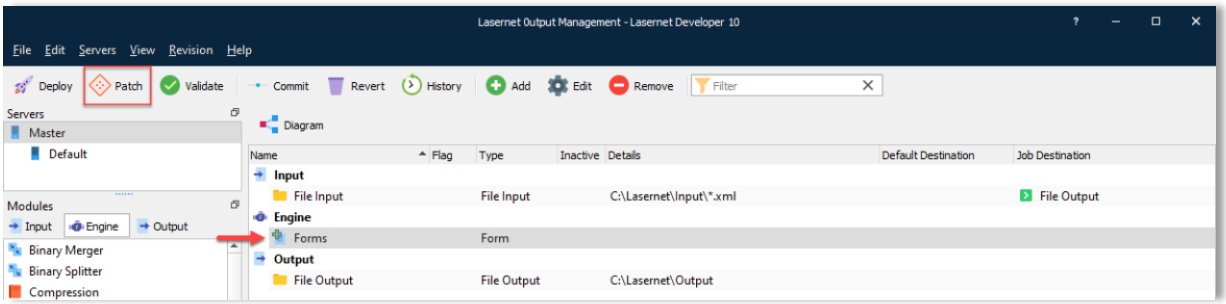
You can validate and view the history. Objects can also be exported and imported to the latest revision of another configuration.



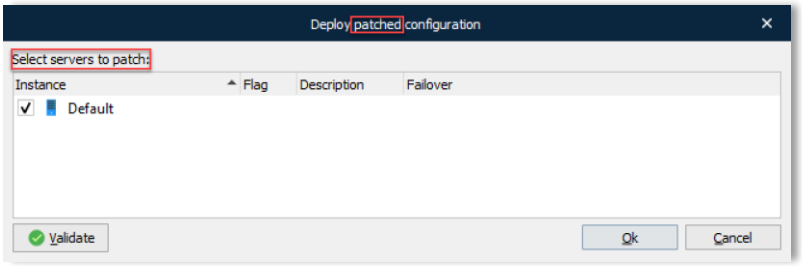
5.4.6 Patch

Patch server is a way to verify your configuration on your server with added or modified objects in the configuration without being forced to a commit and create a new revision.

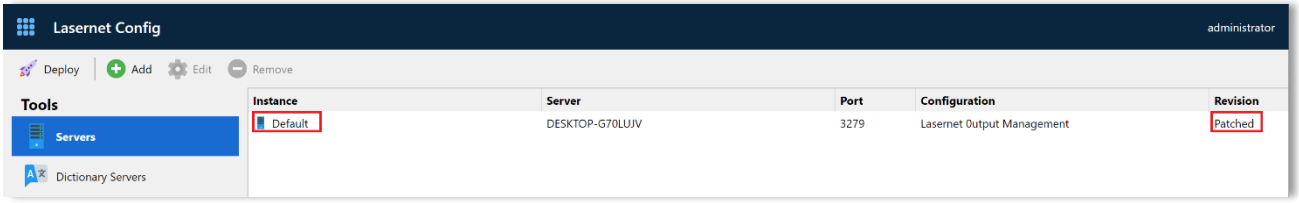
All objects in the configuration are then transferred to the selected server, and non-committed objects are merged to the latest revision.



You can have multiple users patching the same server. Non-committed objects are then merged to a single patch.



On the web interface of the Lasernet Config Server, go to the **Deployment** section and click the required instance to view the patched object(s) list.



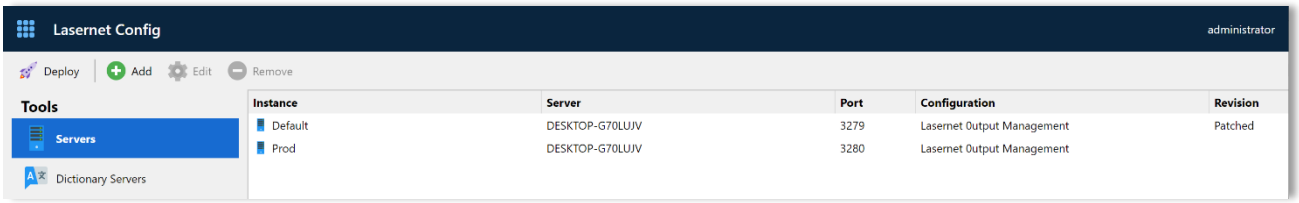
The patch ID is an internal identifier that varies from user to user. The same user has the same ID.

The server runs in patch mode until a user creates a new commit/revision. Active patches for any user are then cleared. They must be either committed (including their objects), or a new patch with uncommitted objects will be created.

Important: Patch mode must be used carefully in a multi-user environment. The functionality is only recommended for testing purposes and advanced users.

5.4.7 Add Multiple Server Instances in Lasernet Config Server

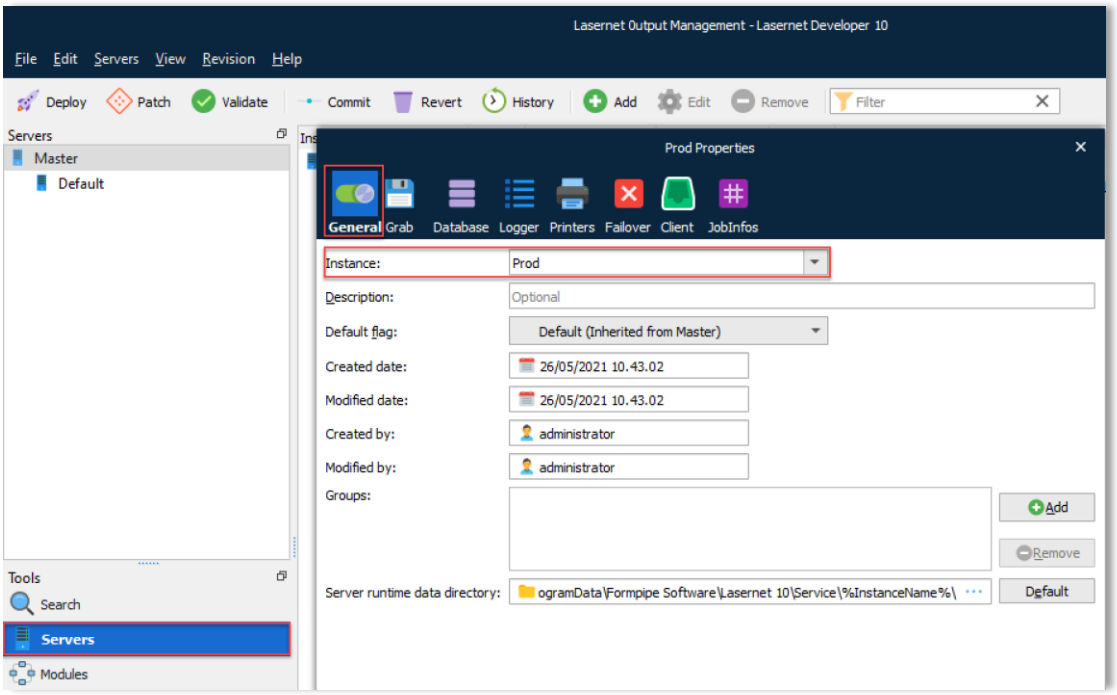
Add another server instance to the Lasernet Config Server. In this example, an instance to run the production environment is added.

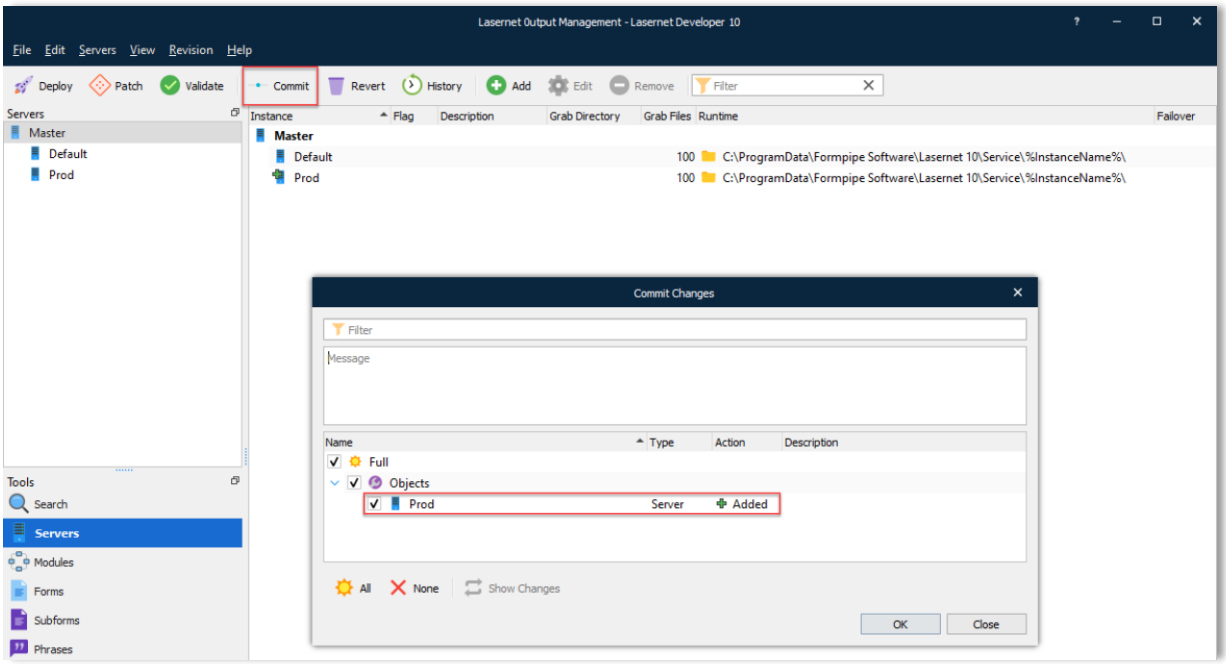


5.4.8 Add Multiple Server Instances in Lasernet Developer

Log in to Lasernet Developer and open the configuration again to obtain a list of servers recently added to the Lasernet Config Server.

In the Lasernet Developer, add a new server instance to your configuration and commit your changes.

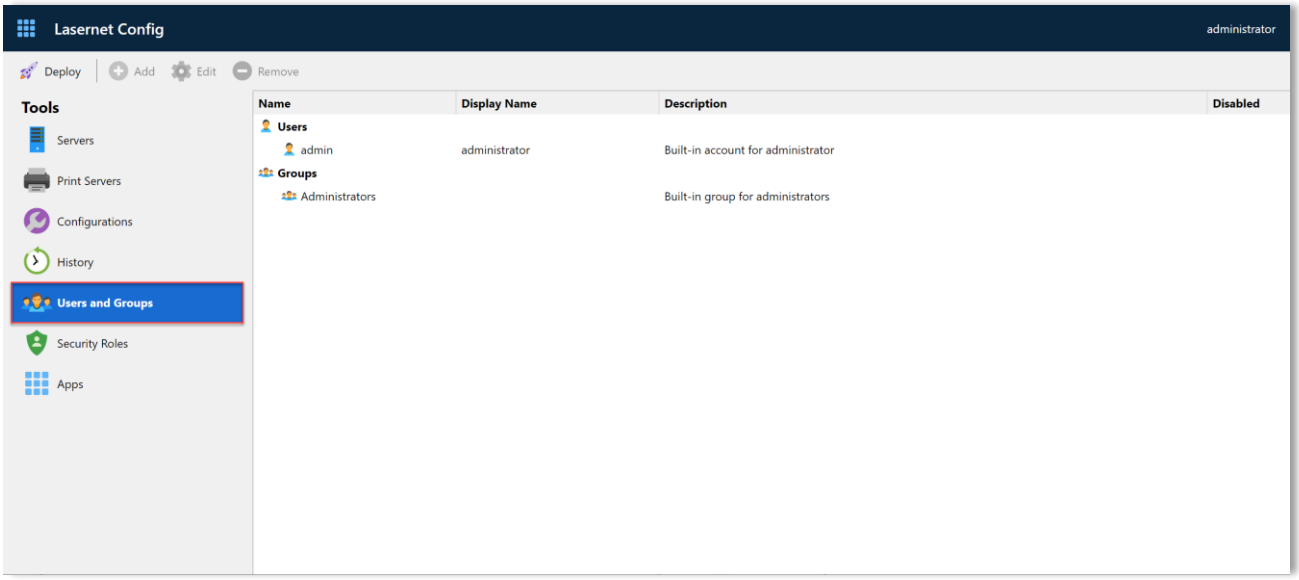




You are now able to deploy your configuration to your new server instance.

5.5 Users and Groups

Select the User and Groups tab to view and edit local Lasernet users.



Lasernet has as a default admin user and a group of administrators that cannot be removed. The security role cannot be changed for this user and this group.

New users can be added to the administrator group and will obtain the same privileges.

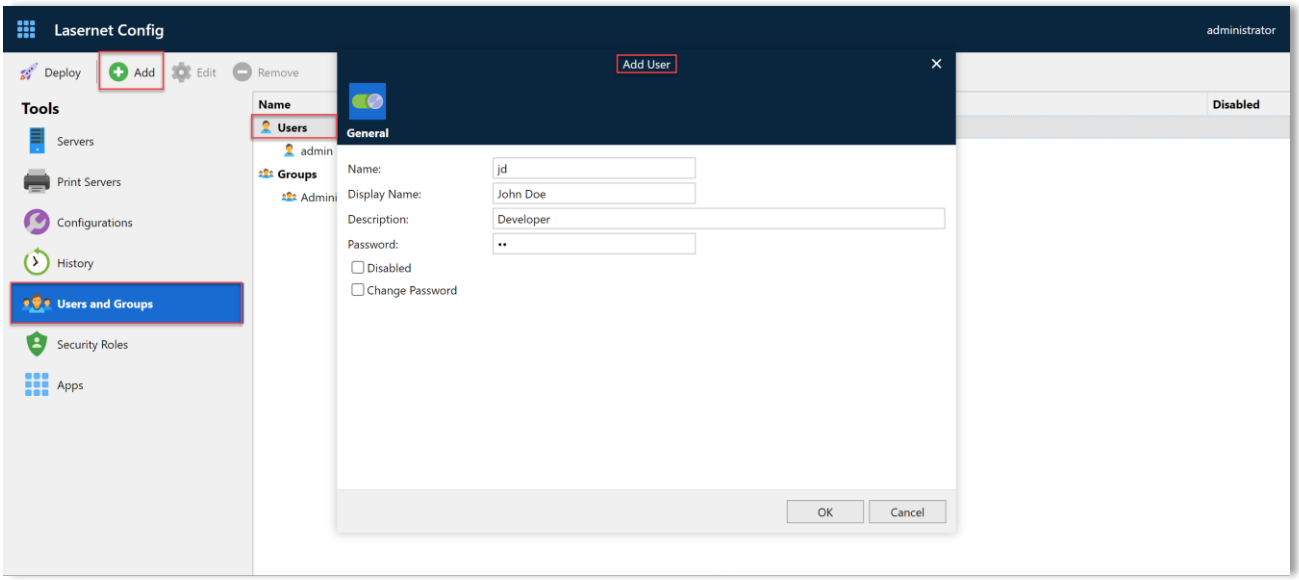
Important: Users and groups added to a configuration in an older version of Lasernet are not migrated to the Lasernet Config Server 10 and must be added manually.

5.5.1 Add User

To add a user, select the **Users** section and click **Add**. Afterwards, fill in the fields with the required data and click the **OK** button.

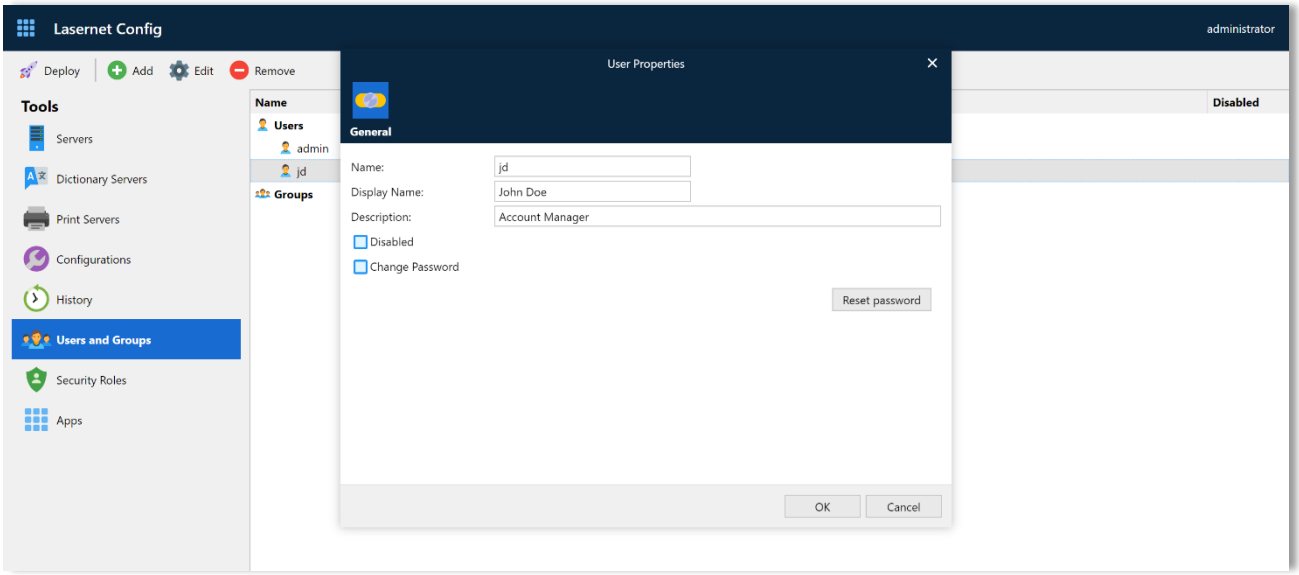
Selecting the **Disabled** check box allows you to disable the user record (the admin record cannot be disabled).

You can force the user to change the password at next login, supported by the Lasernet Config Server and Lasernet Developer only, by selecting the **Change password** check box.

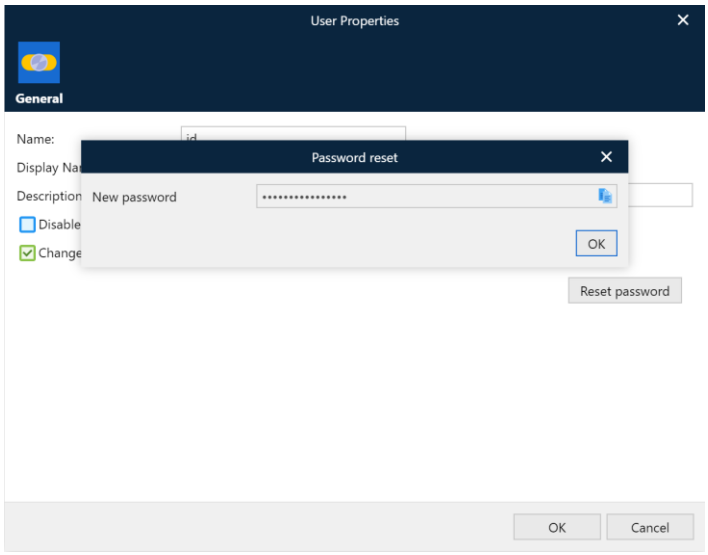


5.5.2 Edit User

To edit a user, click a name of the added user(s). You can now edit the name of the user, disable the account, force the user to change password at the next login or reset the password.

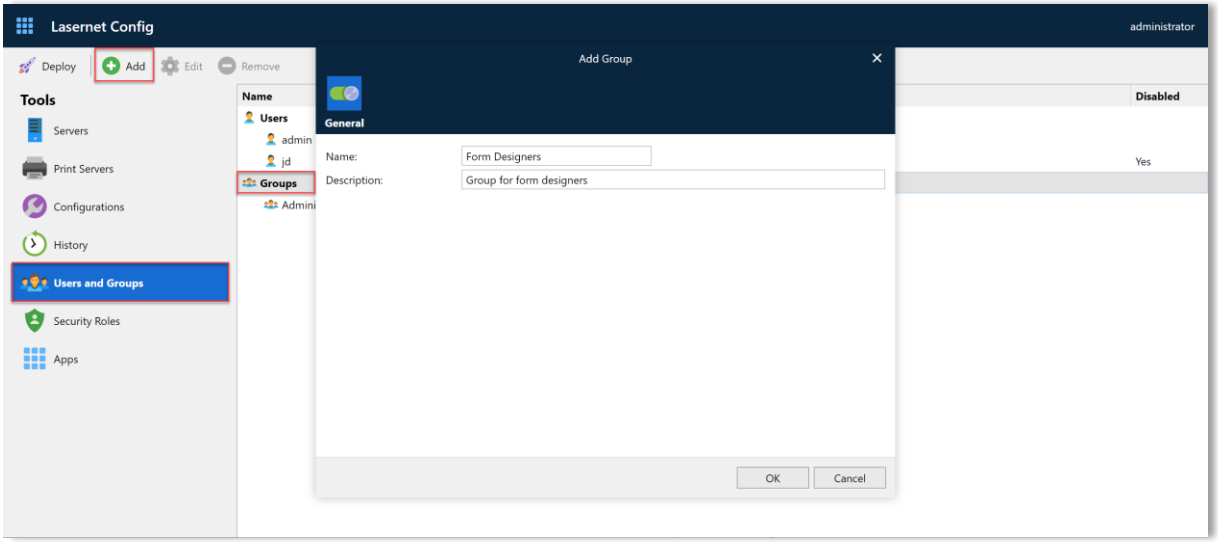


Click Reset password button to create a new temporary password for the user, who as default will be asked to change the password next time the user signs in. Click the copy to clipboard button to get the password in clear text.



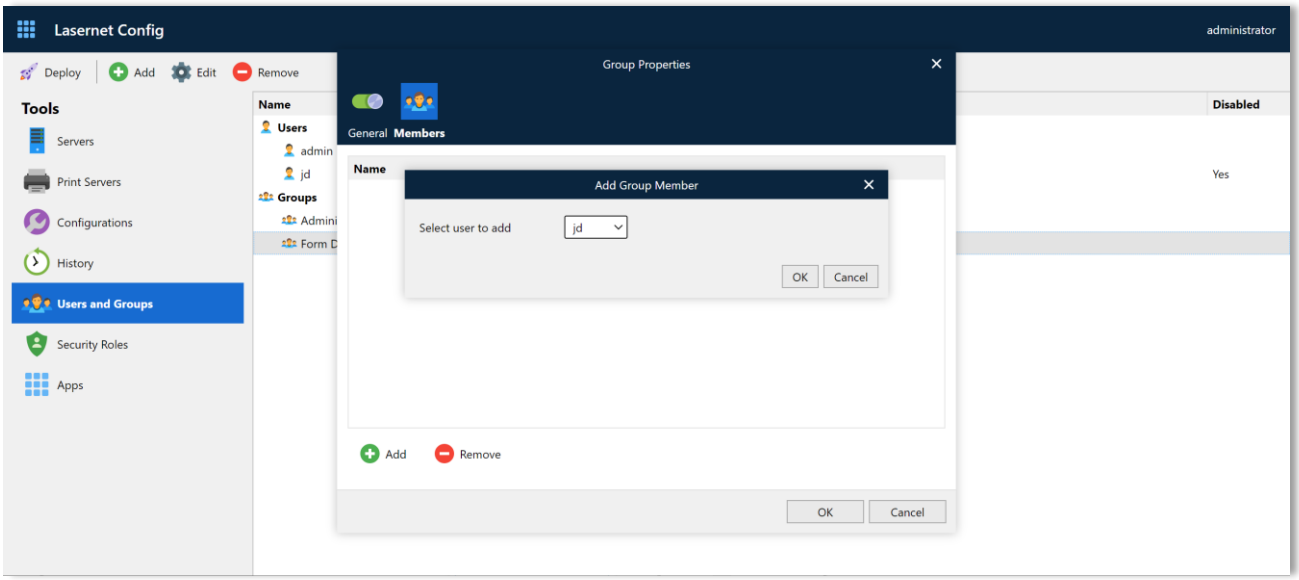
5.5.3 Add Group

To add a group, select the **Groups** section and click **Add**. Afterwards, fill in the fields with the required data and click the **OK** button.

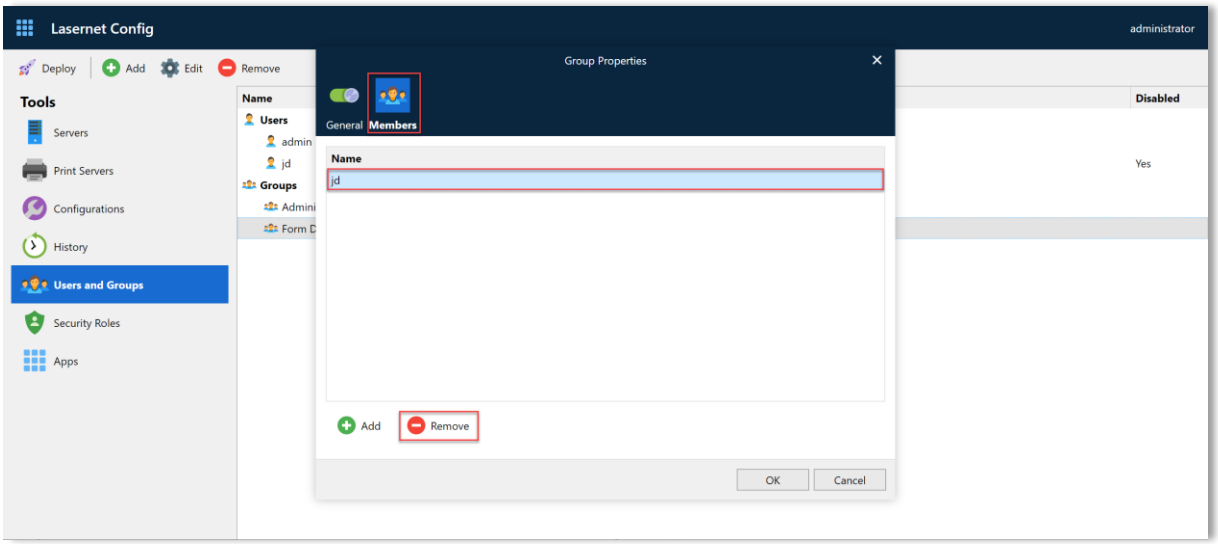


5.5.4 Edit Groups

To edit a group, click a name of the added group. You can now add group members.

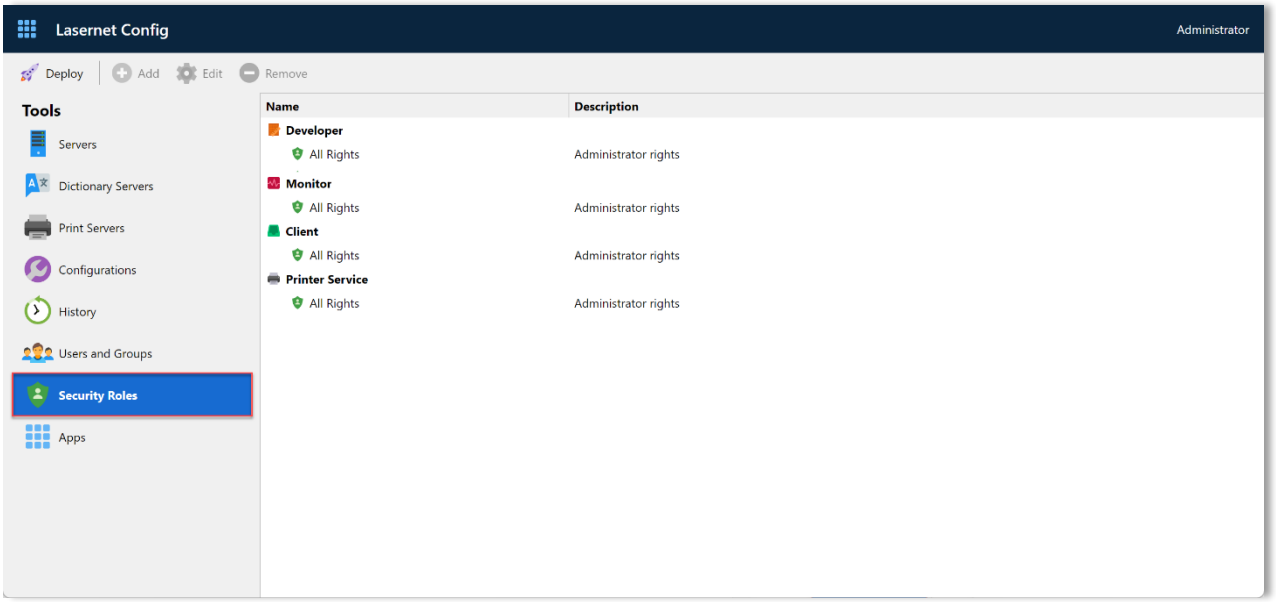


You can also remove group members, if required.



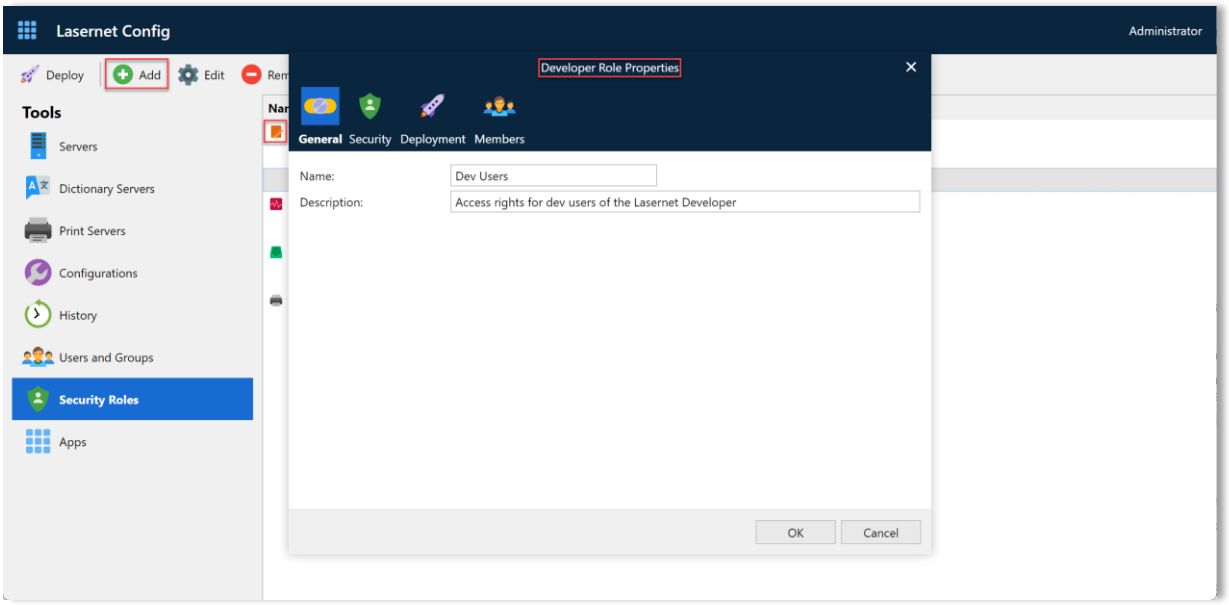
5.6 Security Roles

Select the Security Roles tab to manage access control to Lasernet products and services.



5.6.1 Developer

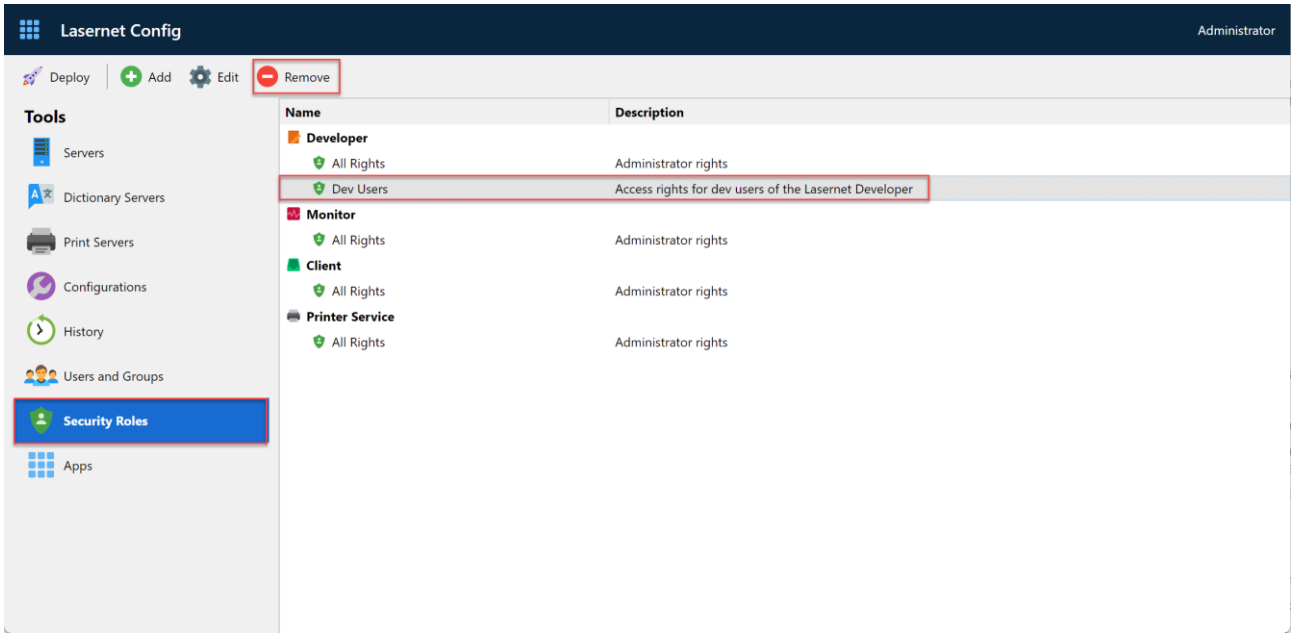
The **Developer** section of the **Security Roles** feature controls user rights in Lasernet Developer and on the Lasernet Config Server website. To add a new developer role, click **Security Roles**, then in the main part of the page click the **Developer** section, then click **Add**.



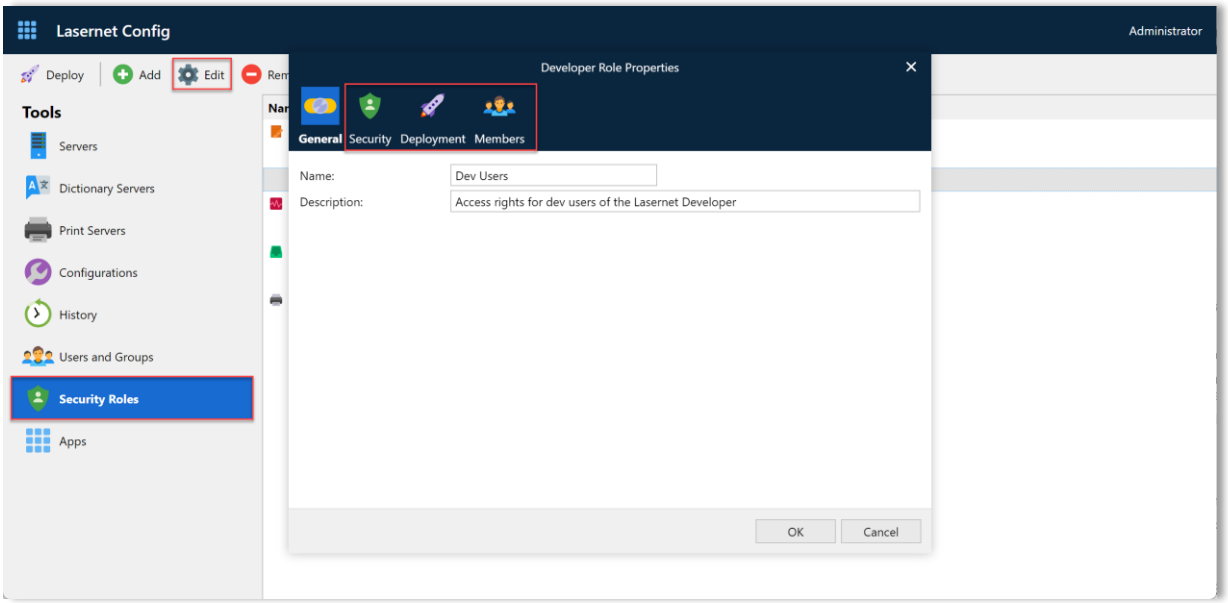
On the page displayed, enter a name and then click **OK**.

Once you are done, a new developer role appears in the list.

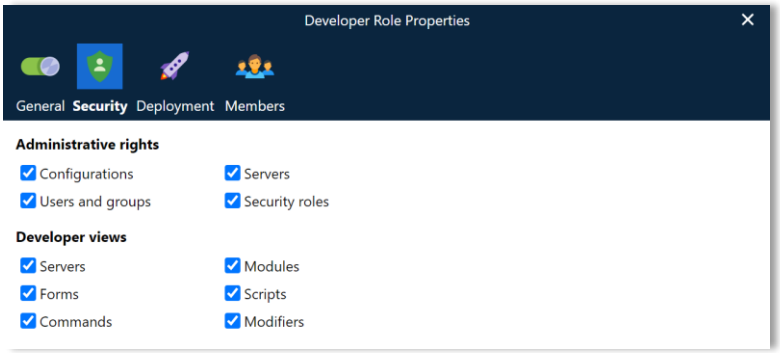
To remove a role, click that role and then click **Remove**.



To edit the role, click that role and then **Edit**.



In the Developer Role Properties window, use the Security and Deployment tabs to configure the selected role's rights to access various administrative tools in the Lasernet Config Server and configuration tools in the Lasernet Developer.



5.6.1.1 Security -> Administrative rights

To manage access rights for the Lasernet Config Server:

- Activate **Configuration** to allow a user to view configuration settings, history and revisions.
- Acitvate **Servers** to allow a user to manage server settings.
- Activate **Users** and groups to allow a user to add, edit and delete users and groups.
- Activate **Security roles** to allow members of a group to manage the security roles for Administrative rights, Developer views, Deployments to specific server instances.
- Deactivate all administrative rights to prevent a user from logging in to the Lasernet Config Server.

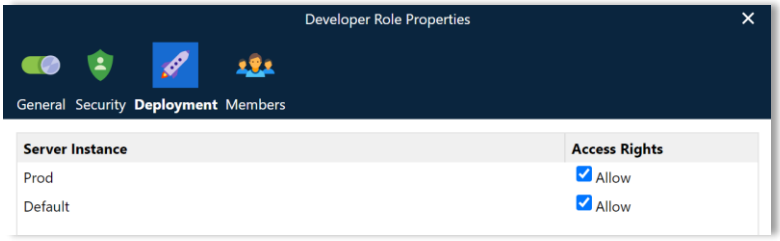
5.6.1.2 Security -> Developer views

To manage access rights for the Lasernet Developer:

- Activate **Server** to allow a user to add, edit and delete server settings.
- Activate **Modules** to allow a user to add, edit and delete module settings.
- Activate **Forms** to allow a user to access the Lasernet Form Editor, SubForms, Phrases, Printer Profiles, Regional Profiles and Barcode Profiles.
- Activate **Scripts** to allow a user to add, edit and delete JavaScripts.
- Activate **Command** to allow a user to add, edit and delete Connections and Command.
- Activate **Modifiers** to allow a user to add, edit and delete Modifiers.

5.6.1.3 Deployment Rights

On the Deployment tab, you can grant configuration deployment rights for each server instance.



5.6.1.4 Members

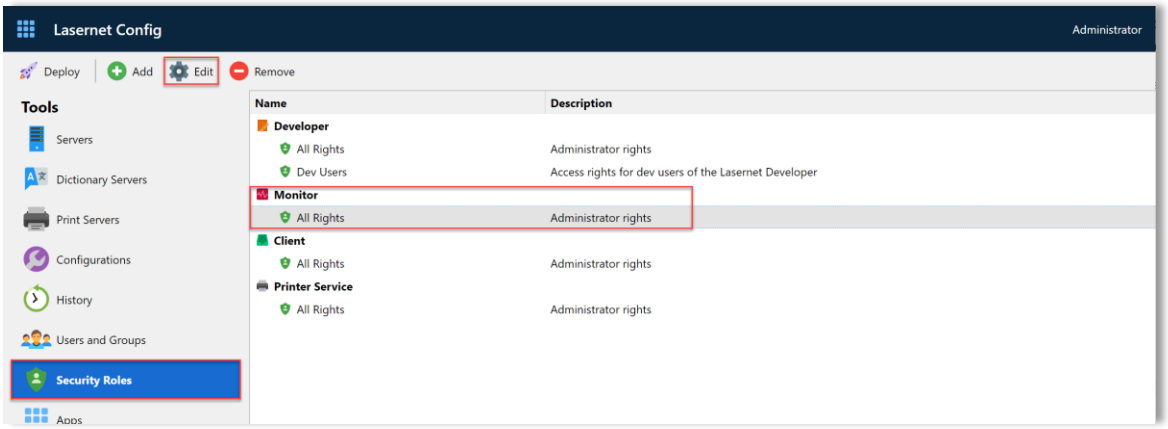
On the Members tab, you can specify which groups are **Members** of the selected security role.

Local Lasernet groups and AD groups can be added as members of a security role.

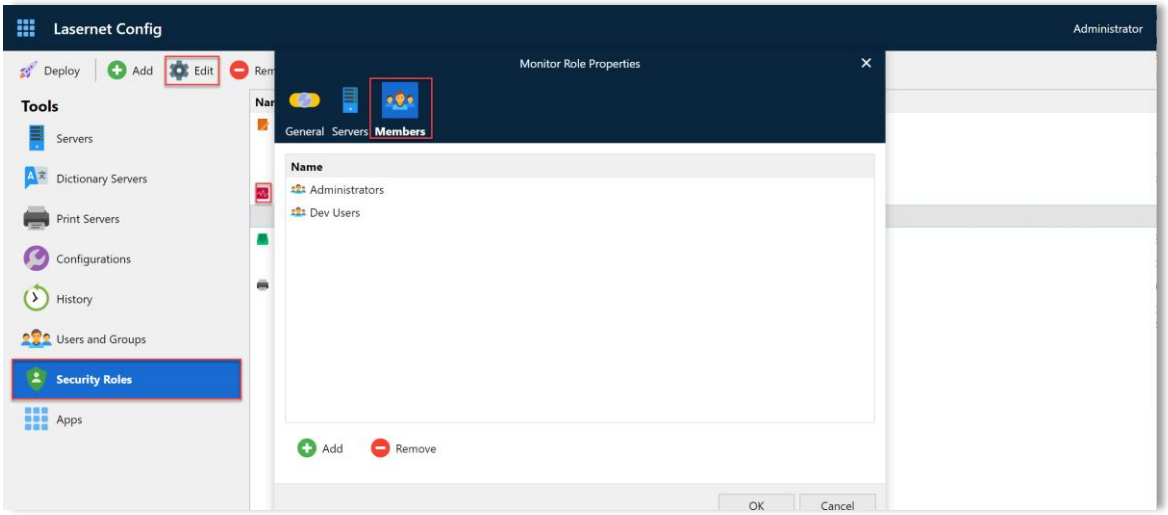
5.6.1.5 Allow a User to Download Grab Files When Using the Lasernet Developer

Permission to download grab files when using Lasernet Developer is not granted by any of the Developer role permissions described above.

To allow a user to download grab files when using the Lasernet Developer, you must ensure that the user's group is a member of the **Monitor -> All rights** role.



When you configure the **Monitor -> All rights** role, include the group that contains the user that you want to grant the access to.

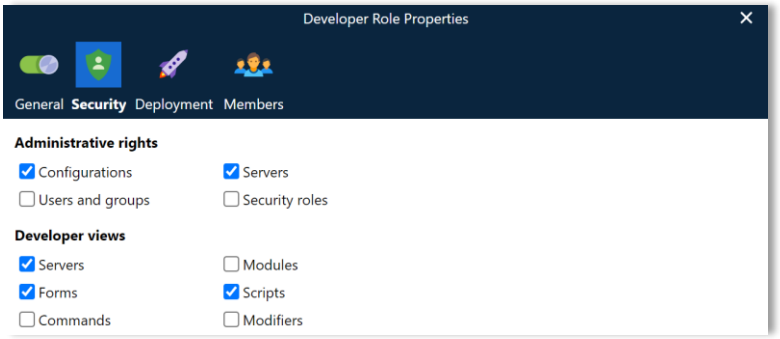


Users that have not been granted this access will be shown an "Access not allowed" error message when activating import grabs functionality from the Lasernet Developer.

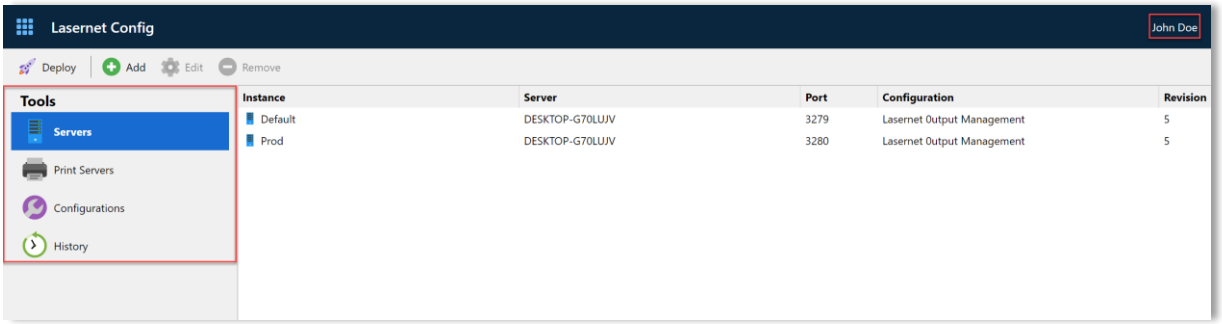
5.6.1.6 Example of Security Roles for a User Logged in to the Lasernet Config Server

This section describes an example security configuration for a role, then shows the effect of that security configuration on the Lasernet Config Server user interface shown to a user who is a member of that role.

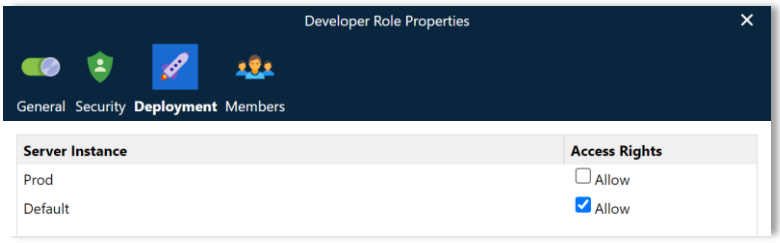
Security: The role's administrative rights are restricted to administrating **Configurations** and **Servers**.



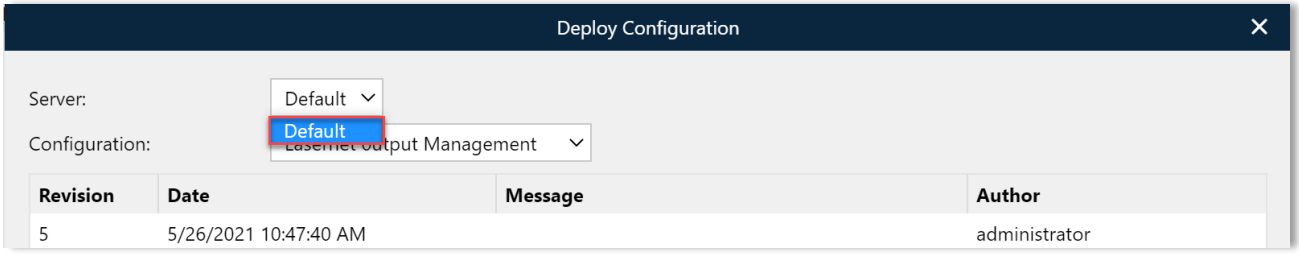
As a result, if a user that has that role logs in to the Lasernet Config Server, they do not have access (in the **Tools** area) to manage **Users and Groups** and **Security Roles**.



Deployment rights: The user's role's deployment rights are restricted to deploying configurations to the Default server instance only.



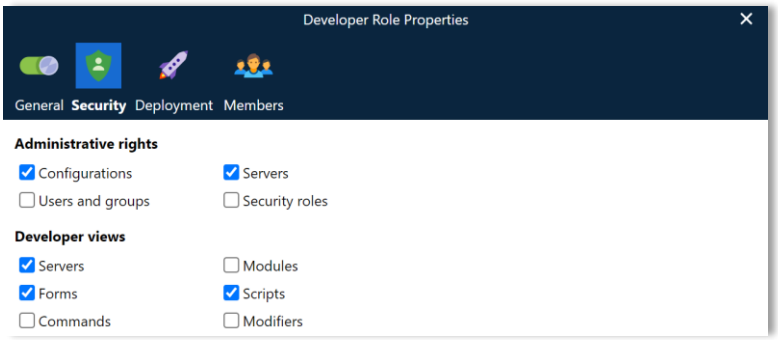
As a result, the list of accessible servers for deployment is now restricted to the Default server only.



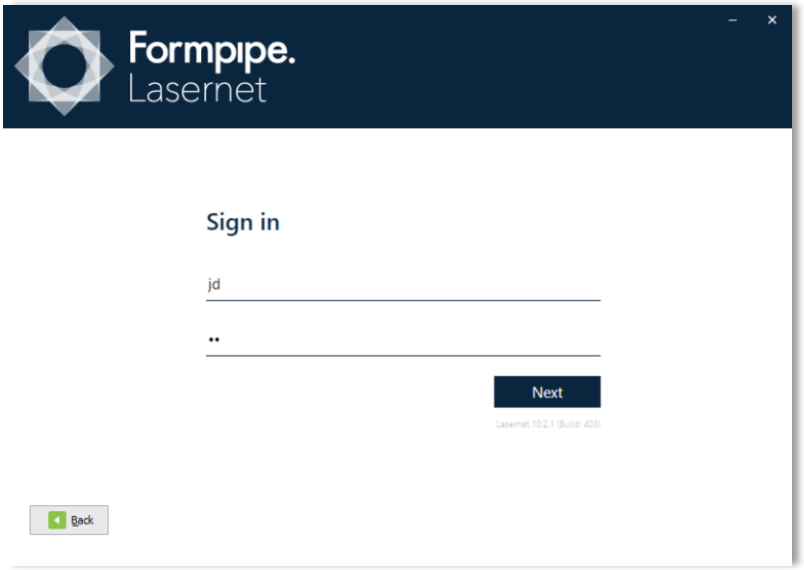
5.6.1.7 Example of Security Roles for a User Logged in to the Lasernet Developer

This section describes an example security configuration for a role, then shows the effect of that security configuration on the Lasernet Developer user interface shown to a user who is a member of that role.

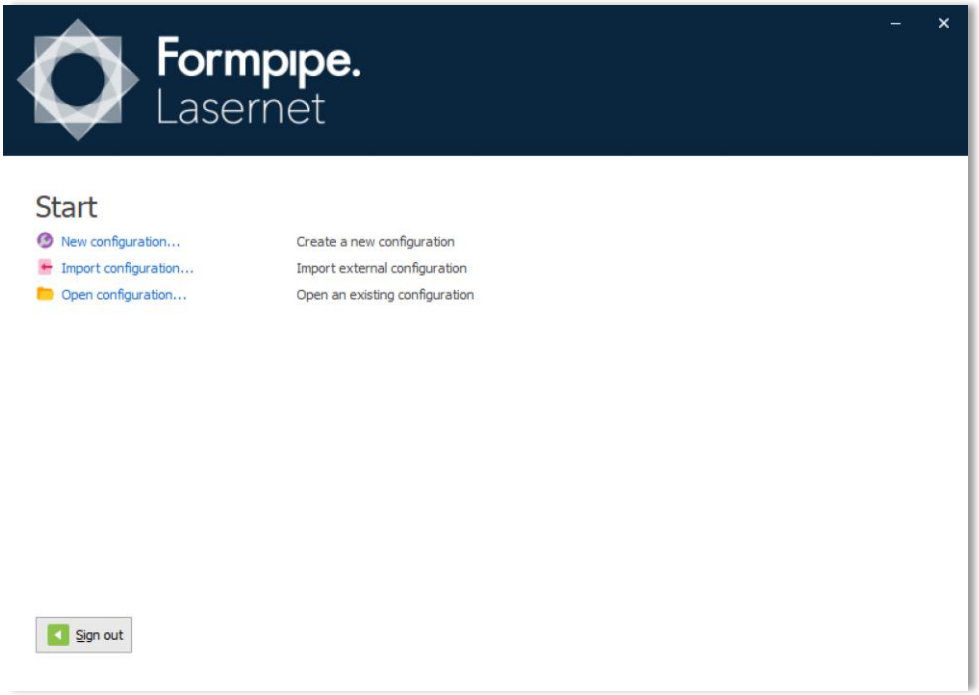
Security: The views that are available to the role in Lasernet Developer do not include the Commands, Modules, or Modifier views, because those check boxes are not selected in the role's security configuration.



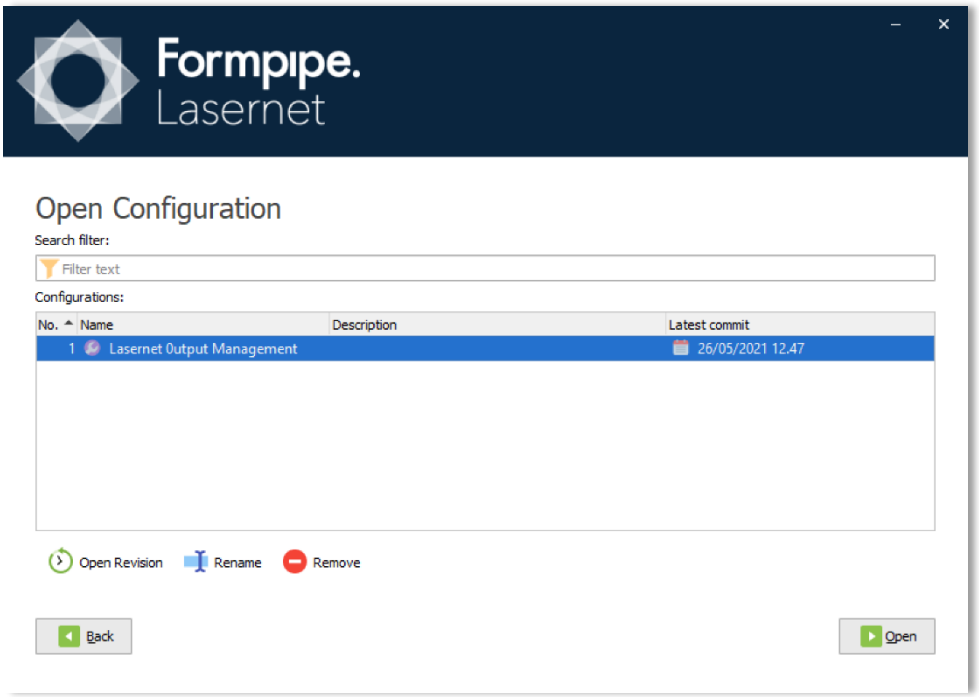
To see the effect of this security configuration, first you must log in to the Lasernet Developer application as a user that is a member of the role that has the restricted rights described above.



When you log in to the Lasernet Developer for the first time, the list of recently used configurations (in the lower part of the window) is empty. This list is stored in the Lasernet Config Server for each user.



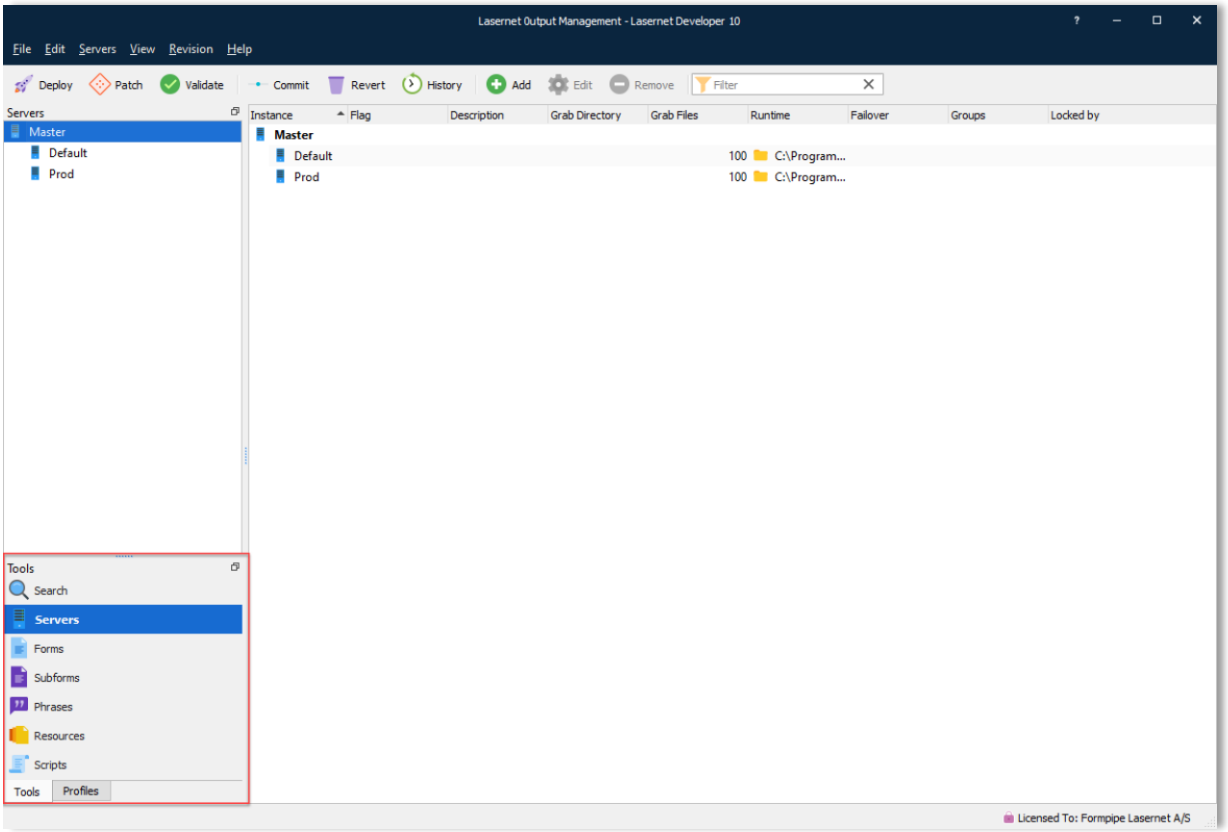
Because there is currently no list of recently used configurations, click **Open configuration** to open an already existing configuration (that is stored in Lasernet Config Server). Find the configuration that you want to use, then click **Open**.



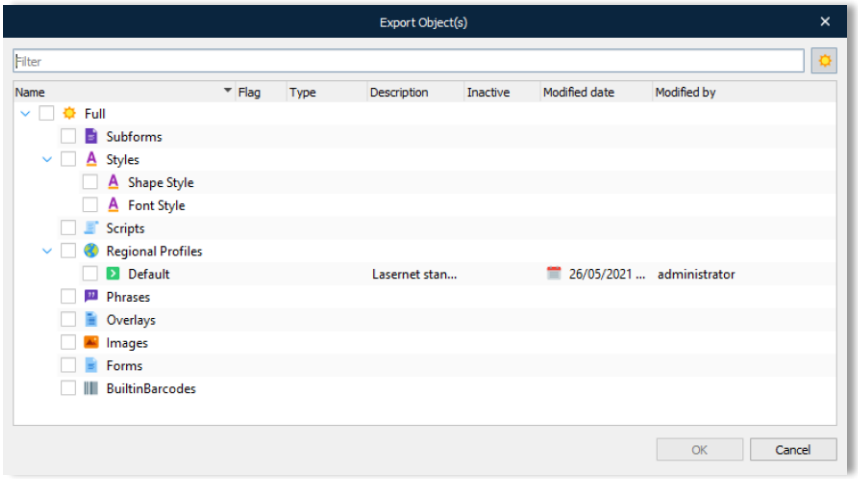
After the Lasernet Developer loads, the Tools and Profiles tabs (see red-outlined area in the image below) enable the current user to add and edit the following object types:

- Form
- Subforms
- Phrases
- Resources
- Printer Profiles
- Regional Profiles
- Barcode Profiles

As a result of the configuration of the user's security role, the **Modules**, **Commands**, and **Modifiers** buttons that can appear in the Tools tab are hidden. Consequently, the user has no access to the functionality in Lasernet Developer that enables users to add, edit, and remove those types of object.



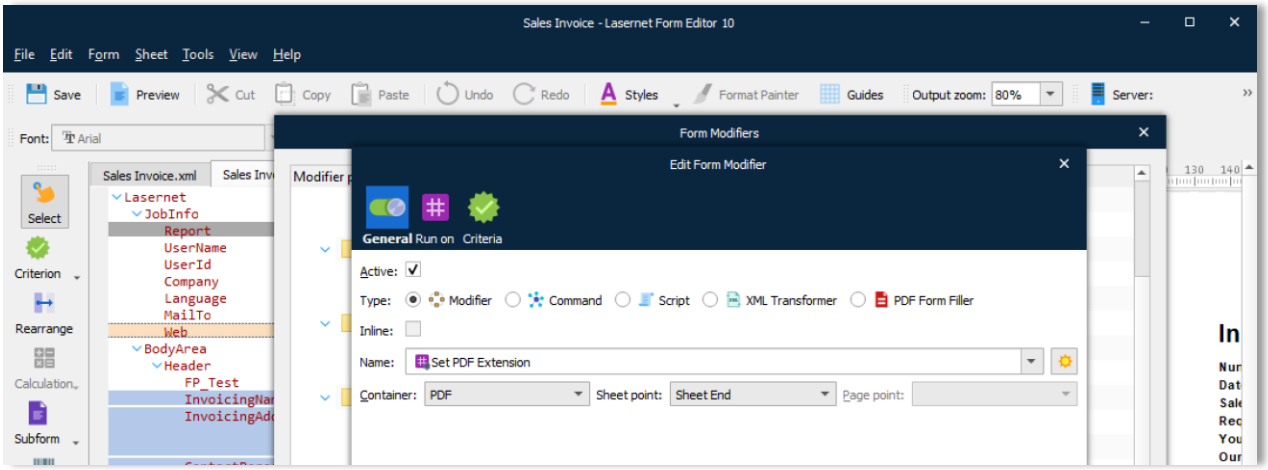
Users with restricted rights for viewing and writing specific object types can only import and export those same object types.



However, users that have restricted rights to add, edit, or delete particular types of object can access and add all object types to the configuration from the following dialogs in the editors:

- Modifier events
- Overlays
- Grab file dialog
- Connections
- Destinations
- Scripts

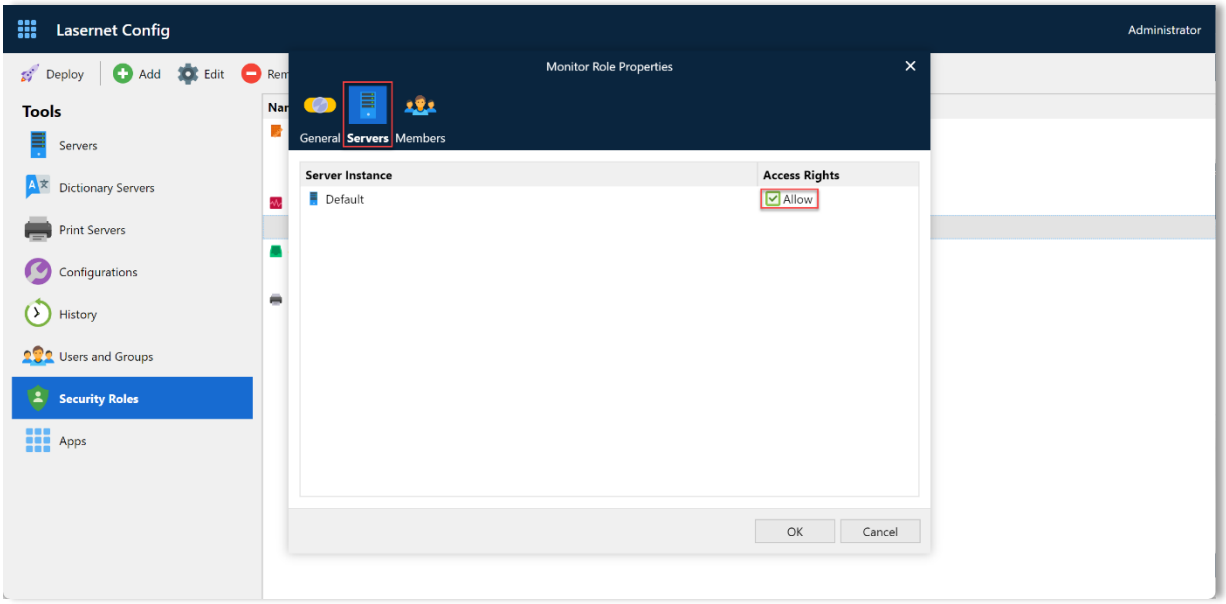
The example screenshot below shows the **Edit Form Modifier** event window in the Lasernet Form Editor. This window can be accessed by all users. Although the logged-in user has restricted rights to the parts of Lasernet Developer that enable users to add, edit, or delete particular types of object, the user can access all object types in this window. But, they cannot edit them.



5.6.2 Monitor

The Monitor security roles relate to the Lasernet Monitor application and define the server instances to which the user has access. Select the **Monitor** section and click **Add** to add a new role.

Click the Servers tab to view and amend the access rights for each instance. Select the **Allow** checkbox to grant access rights to the corresponding instance.

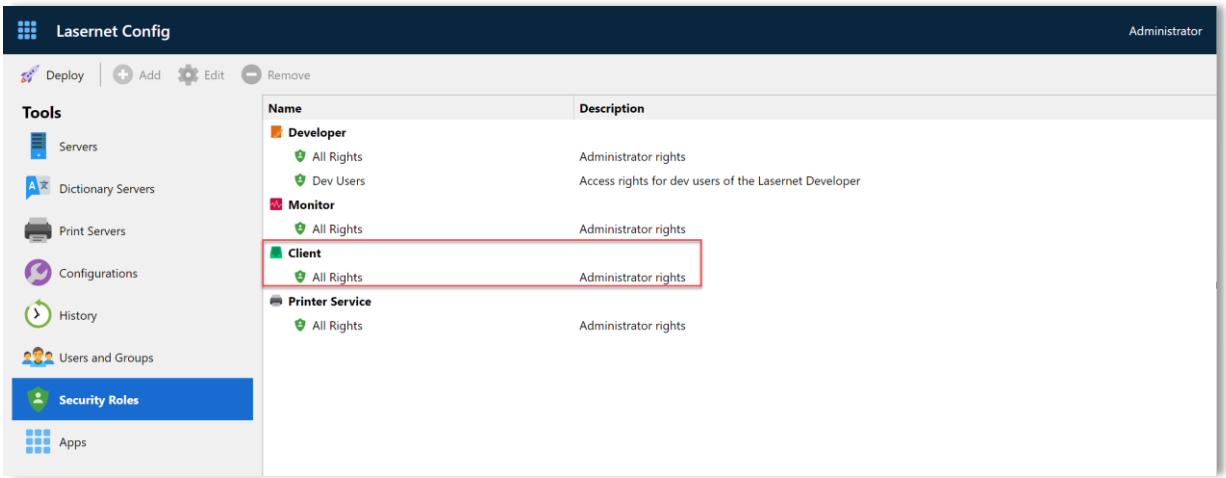


Use the Members tab to add groups to this role.

Important: The ability for a Lasernet Developer user to download grab files is managed by the **Monitor -> All rights** role. For more information, see Allow a User to Download Grab Files When Using the Lasernet Developer on page 63.

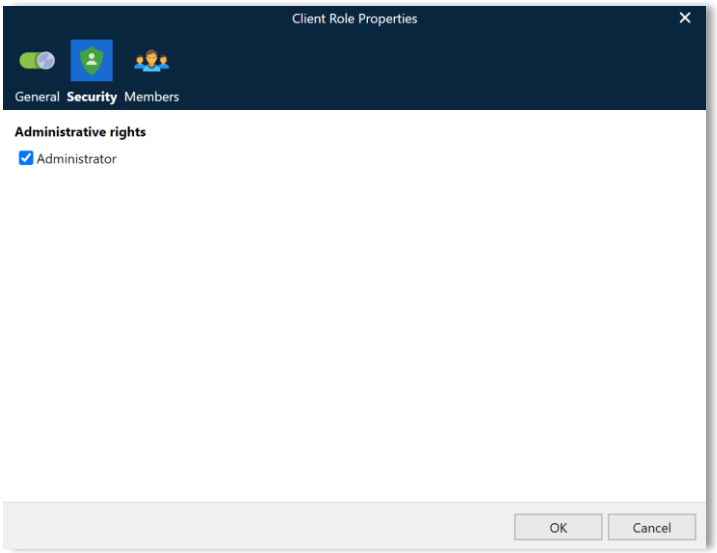
5.6.3 Client

Use the **Client Role Properties** window to add users, groups, or both, to a role that allows users to log in to the Lasernet Client. You can also set access rights to read, write and delete documents / jobs.

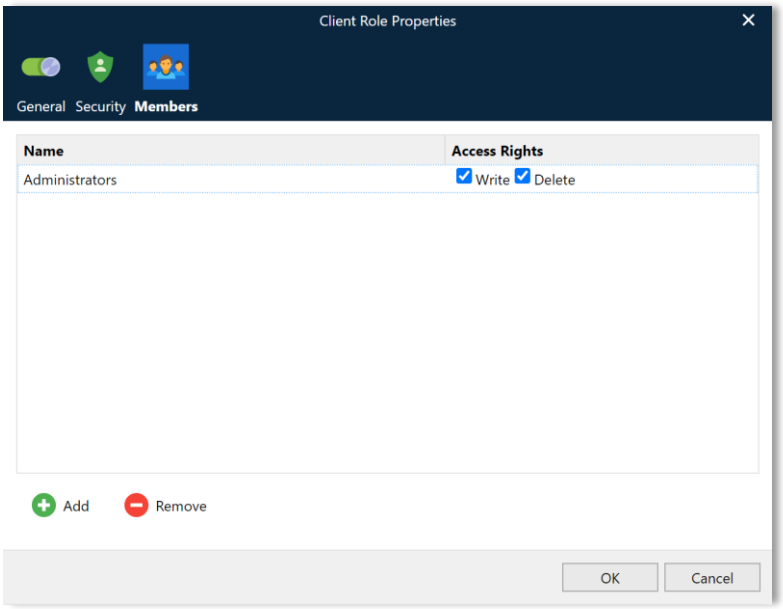


Administrators are members of the **All Rights** role, so they have full access permissions.

On the Security tab of the **Client Role Properties** window, you can specify whether Administrator rights are granted to role members.

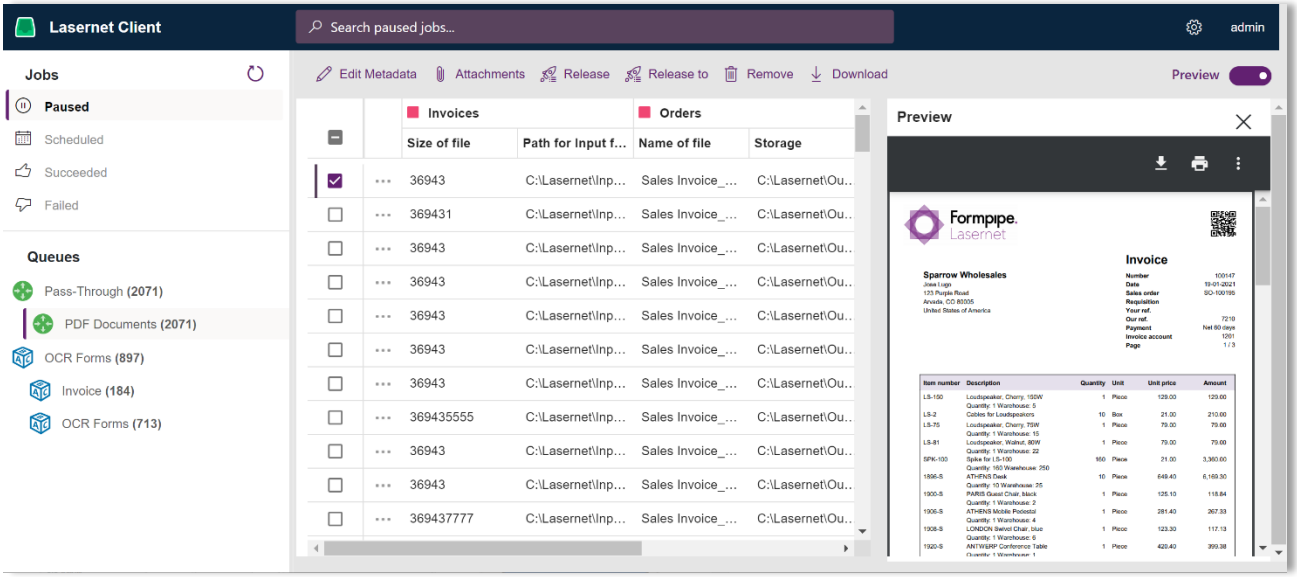


On the Members tab, you can specify which access rights (**Write** and **Delete**) are granted to the local Lasernet users/groups or Active Directory users/groups that are listed on the Members tab.

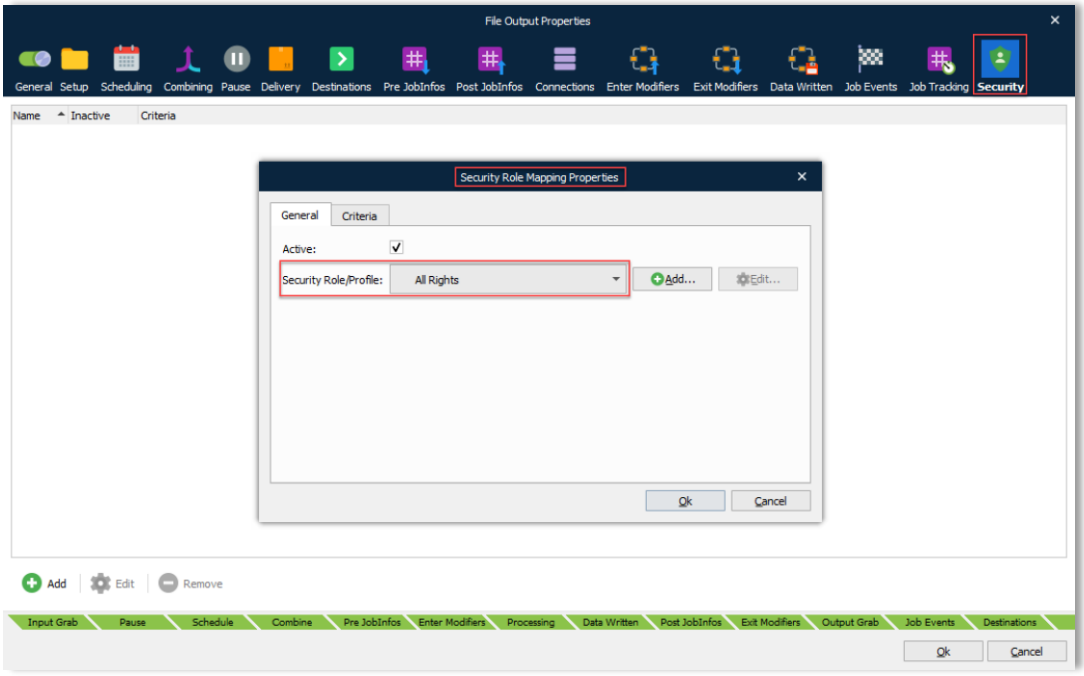


5.6.3.1 Lasernet Client

If you log in to Lasernet Client as admin, you can access all jobs. Whereas if you log in to Lasernet Client as a restricted user with a mapped security role, you will see only specific jobs.



5.6.3.2 Security Roles Mapping in Lasernet Developer



Note: Security Profiles defined in Lasernet 9 or older are not migrated to Lasernet 10 and must be added to the Lasernet Config Server 10 by an Admin user.

The name of a security role added via the modules Security tab in Lasernet Developer will be migrated into Lasernet, retaining the name.

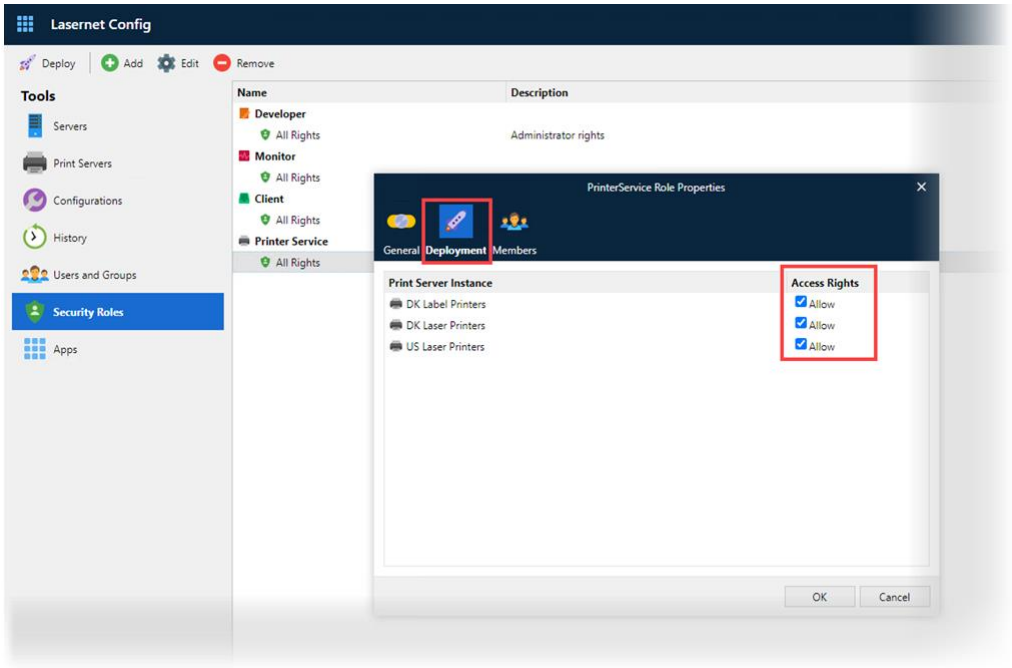
If the security roles added to the Lasernet Config Server 10 use the same names, and the user and groups assigned to the role are the same, they are compatible with older versions after upgrading to Lasernet 10.

New security roles added to the Lasernet Config Server are loaded in the Lasernet Developer every time the **Security Role Mapping Properties** dialog opens; therefore, the configuration does not require reloading.

5.6.4 Printer Service

The Printer Service security roles relate to the Lasernet Printer Service application and specify which Printer Services the user can work with. Select the Printer Service section and click **Add** to add a new developer role.

Click the **Deployment** tab to view and amend the access rights for each Printer Service instance. Select the **Allow** checkbox to grant access rights to the corresponding Printer Service instance.

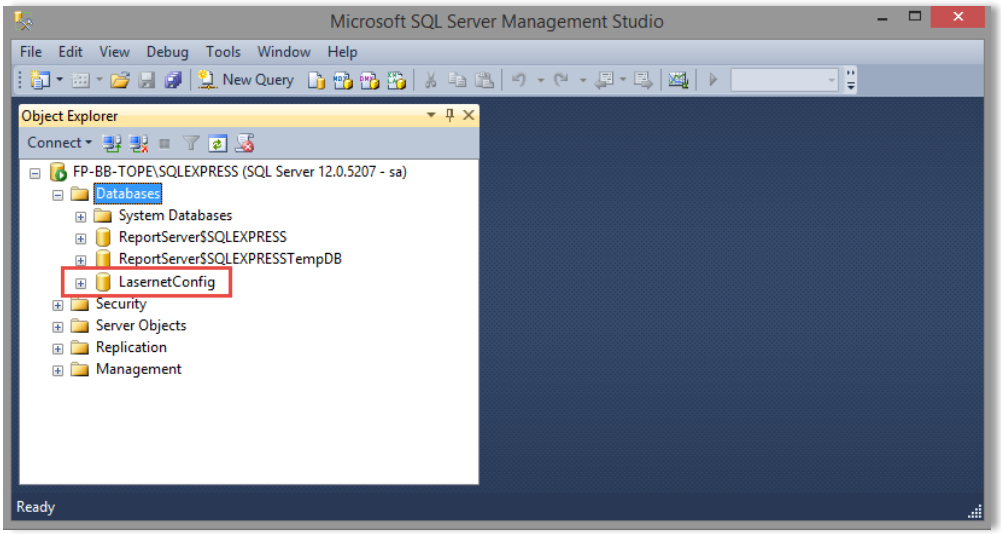


5.7 Migration to Microsoft SQL Server

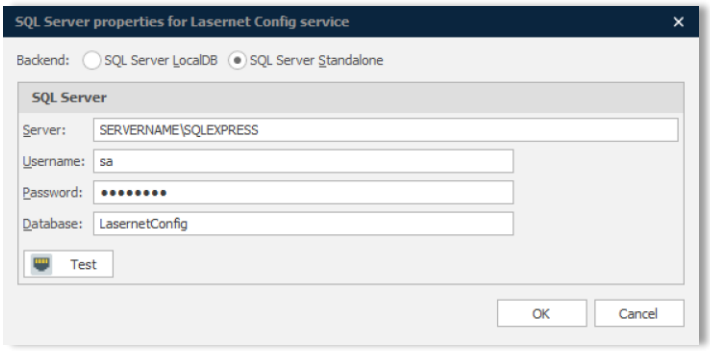
Open Lasernet License Manager to migrate your pre-defined database from Microsoft SQL Server 2017 LocalDB to Microsoft SQL Server. The migration will include:

- Configurations
- Revisions
- Deployment history log
- Users and groups
- Security Roles

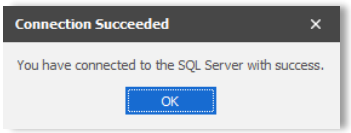
Create a new database with any name in Microsoft SQL Server Management Studio. The database is not added automatically by the migration process. In this example, a database is created in Microsoft SQL Server Express.



Click the **Test** button to validate the connection.



When the **OK** button becomes active, the connection is successfully established. Click the button to start the migration process.



A file with the connection settings is created in the folder.

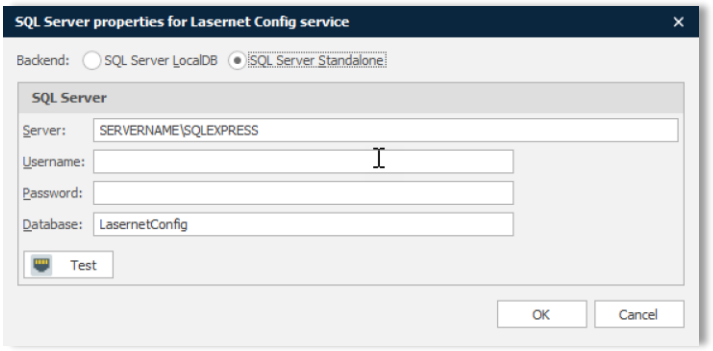
C:\ProgramData\Formpipe Software\Lasernet 10\Config\Default\sqlserver.json

The Lasernet Config Server is now connected to the Microsoft SQL Server. No further actions are needed.

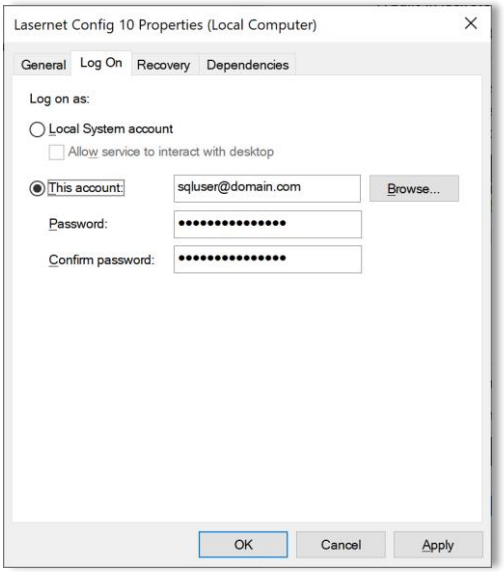
You cannot migrate the opposite way around. If the file **sqlserver.json** is removed, the Lasernet Config Server will connect to the Microsoft SQL Compact 4.0 Server and use the same revision of the database from before the migration.

5.7.1.1 Windows User Authentication

Support for Windows User Authentication in SQL Server is supported by the Lasernet Config Server, by leaving username and password empty in the Lasernet Licenser Manager -> Config SQL Server settings



and authenticate the Lasernet Config 9 Service as the Windows user.



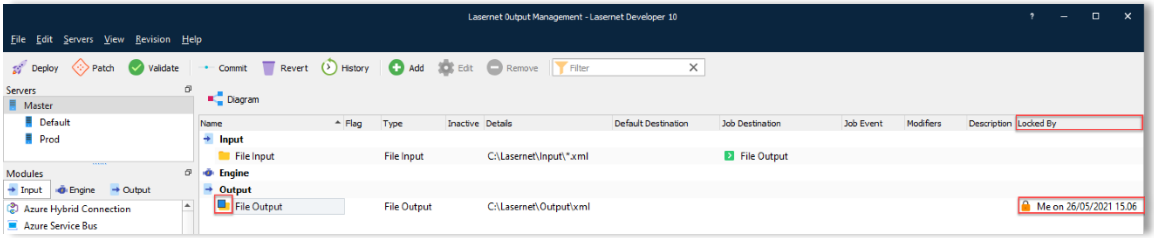
5.8 Multi-users

Multiple users can work with the same configuration from different computers at the same time.

A built-in lock system handles locked and non-committed objects from being edited at the same time.

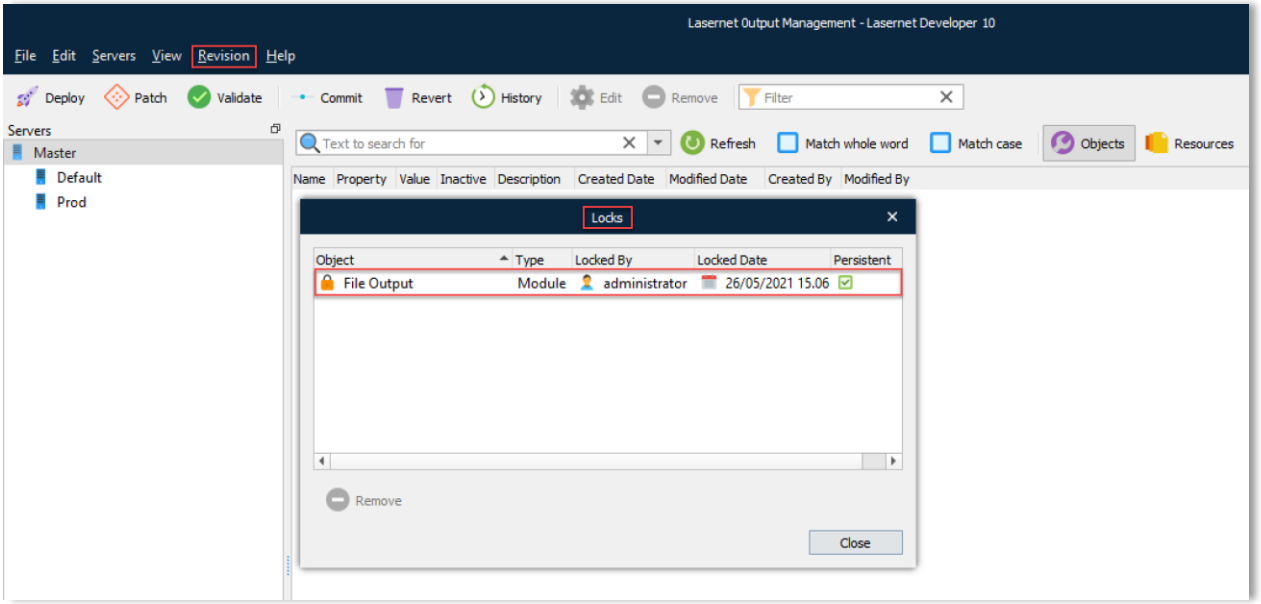
We recommend that you create unique users on the Lasernet Config Server for each user working with the Lasernet Developer, in order to track changes and commits as well as handling object locks in the configuration.

When an object is added, opened or modified, a lock symbol will appear next to it with information about who has locked it and when. Objects are locked by both GUID and name. The name of an added object is locked for any user until it is either commited or reverted.



An object is unlocked when it is commited, or if it is closed without changes. An object is also unlocked if its properties are reverted to the same values as in the previous revision.

A user of the admin group is allowed to remove listed locks for any user from the **Revision → Locks** dialog.



Important: All the modified settings of a non-committed object are immediately lost for a logged in user, or the next time the configuration opens.