



Inventory - Software and File Search

*Software and file search for Linux, Mac and Windows
Inventory*

TITLE	Inventory - Software and File Search
AUTHOR	Docusnap Consulting
DATE	12/12/2023
VERSION	1.1 valid from 9/27/2022

This document contains proprietary information and may not be reproduced in any form or parts whatsoever, nor may be used by or its contents divulged to third parties without written permission of Docusnap GmbH. All rights reserved.

CONTENTS

1.	Introduction	4
2.	Set up Software and File search	5
2.1	Software search Windows	6
2.2	File search	6
3.	Perform Software and File Search	8
4.	Analysis	10
4.1	Software Search	10
4.2	File search	10

1. Introduction

The software and file search in Docusnap is used to search for specific files on the file system of Linux, Mac, and Windows systems. Here, file names are defined, which Docusnap then searches during the inventory on the file system.

The files found are made available for evaluation in Docusnap in different ways depending on the categorization (file search Linux, Mac and Windows or software search Windows).

The software search here refers to applications that have been "installed" on the target system without registration. If the defined files are found, a corresponding entry is created in the list of installed software products on the system. Thereupon this software can be analyzed also in the range of the license management.

The file search designates here any files, which you would like to search, for example due to a safety gap (log4j). The files are then also listed with the path in which they were found. A new object within the summary and a new predefined Docusnap Connect package provide the possibility for cross-system analysis.

At the current time (September 2022) it is not possible to perform a file search using the script variants for Linux and Mac.

A detailed description of how to use the software and file search when using the script variant for Windows can be found in the [HowTo: Inventory - Docusnap Script for Windows](#).

2. Set up Software and File search

Software and file search is set up and managed in Docusnap **Administration - Inventory**. The first step is to assign a **name** and select the **category**:

- File Search Linux
- File Search Mac
- File search Windows
- Software search Windows

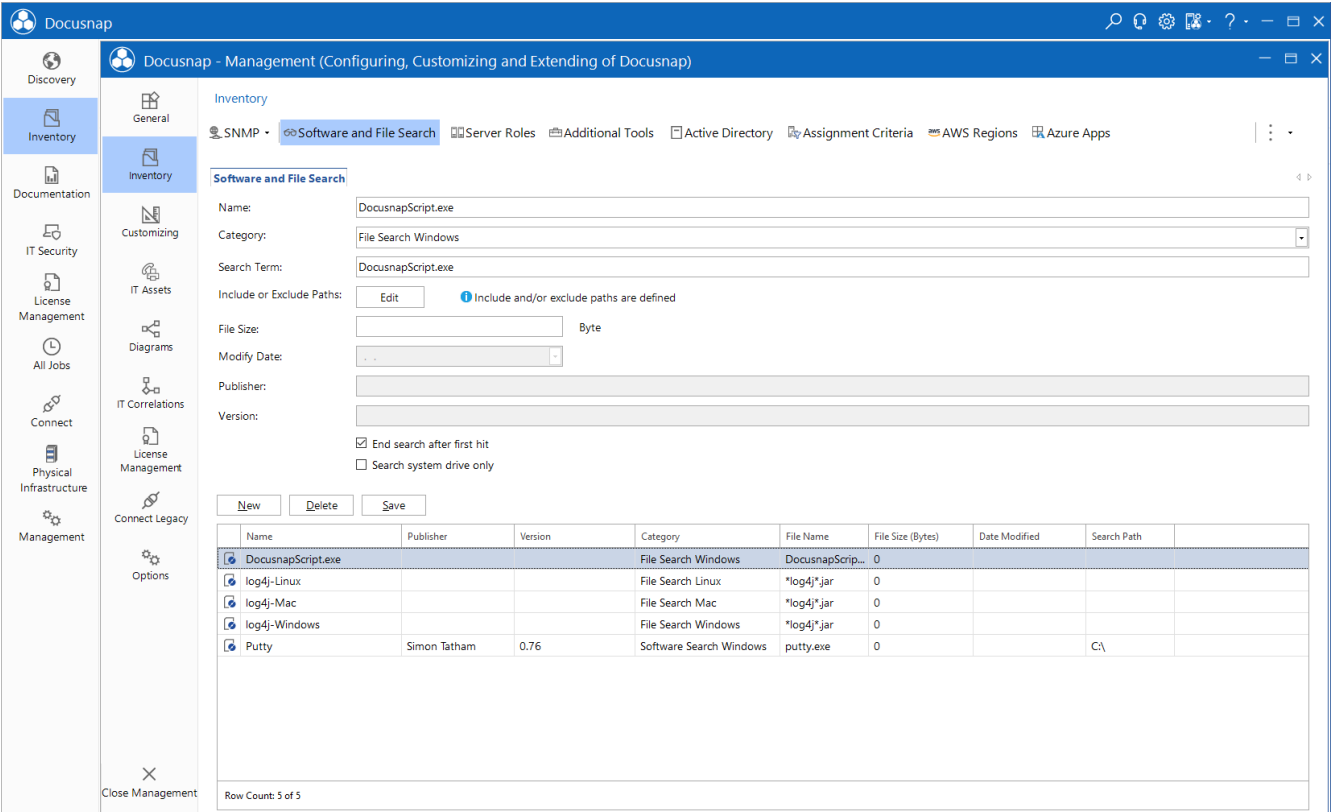
In the next step you define the search term or file name. Here you can enter the actual file name. Placeholders can also be used to make the search more flexible (e.g., Docusnap*.exe). A ? replaces one character, the * replaces several characters.

The search path specification differs depending on which category is selected - more information in the following sections.

The remaining fields are optional:

- File size (specification in bytes)
- modification date
- Manufacturer
- Version

Entries can be removed again with the help of the Delete button. An entry can also be deleted if it has already been used. If an order was created for an inventory in which the file search is used, the order can still be executed if the associated definition of the software and file search as been deleted. However, when the job is processed, the deleted definition is no longer available and as soon as the processing is completed, this definition is no longer considered in the inventory.



Software and File Search

Name: DocusnapScript.exe

Category: File Search Windows

Search Term: DocusnapScript.exe

Include or Exclude Paths: Include and/or exclude paths are defined

File Size: Byte

Modify Date:

Publisher:

Version:

☒ End search after first hit

☐ Search system drive only

Name	Publisher	Version	Category	File Name	File Size (Bytes)	Date Modified	Search Path
DocusnapScript.exe			File Search Windows	DocusnapScript...	0		
log4j-Linux			File Search Linux	*log4j*.jar	0		
log4j-Mac			File Search Mac	*log4j*.jar	0		
log4j-Windows			File Search Windows	*log4j*.jar	0		
Putty	Simon Tatham	0.76	Software Search Windows	putty.exe	0		C:\

Row Count: 5 of 5

Figure 1 - Manage Software and File Search

2.1 Software search Windows

A search path for the Windows software search is optional. If no search path is specified, all local drives are searched.

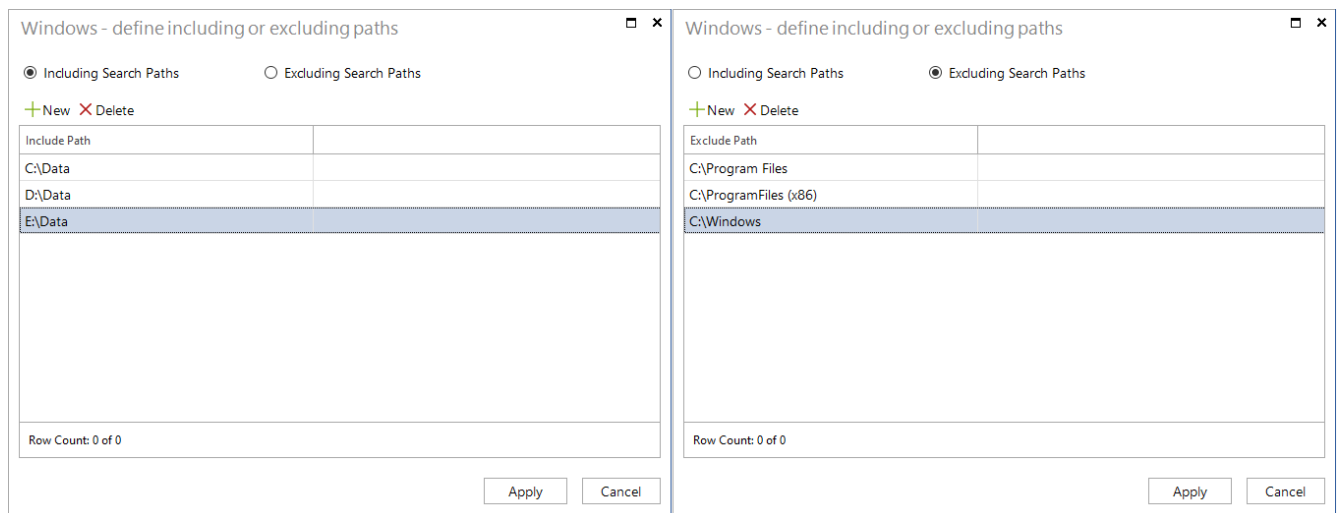
Specifying a search path can contribute significantly to the execution time. The Windows software search can significantly increase scan times and requires a noticeably higher workload on the systems involved. Among other things, how many software searches are activated per scan is also relevant with regard to the scan times as well as the workload.

The software search is terminated as soon as a file with the corresponding file name has been found.

2.2 File search

For the file search, you can define both inclusive and exclusive search paths. For each path, a separate entry must be created using the New button.

If no paths are specified, all local drives are searched here as well.



Windows - define including or excluding paths	
<input checked="" type="radio"/> Including Search Paths <input type="radio"/> Excluding Search Paths	
+ New -X Delete	
Include Path	
C:\Data	
D:\Data	
E:\Data	
Row Count: 0 of 0	
Apply	Cancel

Windows - define including or excluding paths	
<input type="radio"/> Including Search Paths <input checked="" type="radio"/> Excluding Search Paths	
+ New -X Delete	
Exclude Path	
C:\Program Files	
C:\Program Files (x86)	
C:\Windows	
Row Count: 0 of 0	
Apply	Cancel

Figure 2 - Including and Excluding Paths

In the Windows file search, in comparison with the Linux and Mac file search, there is an additional option **End search after first hit**.

If this option is enabled, Docusnap will stop searching for the specified file as soon as it is found for the first time.

So, for example, if you are concerned with identifying the possibly affected systems in the event of a threat, it would be sufficient to stop the search after the first find.

However, if you would like to obtain detailed information about the searched file on the respective system, perform the file search without the mentioned option. Docusnap will then list all paths found for the file.

It is also true for the Windows file search that the search can significantly increase the scan times and a higher load is generated on the systems involved.

3. Perform Software and File Search

In order for the software and file search to be performed in the course of the inventory, you must activate it in the options.

To do this, open the Options (title bar - cogwheel) - Inventory:

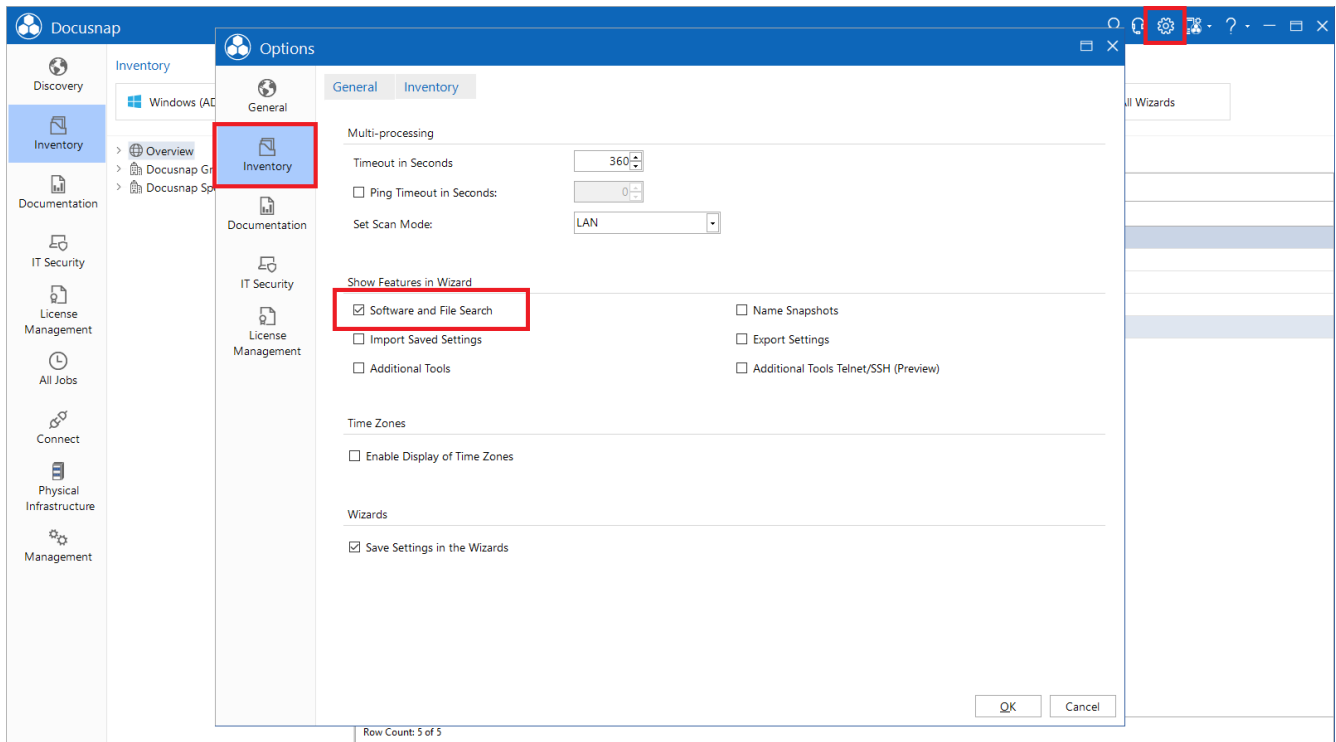
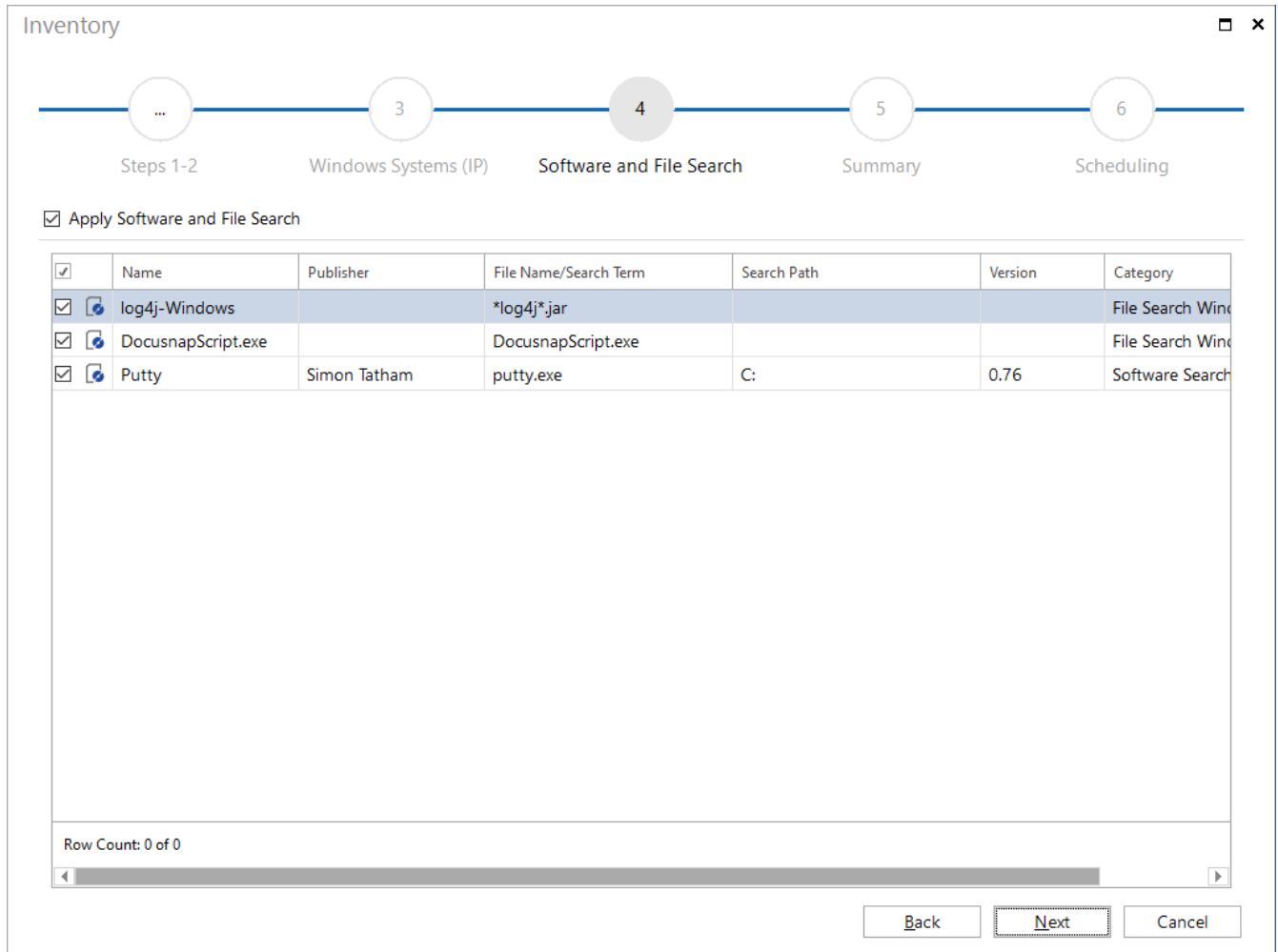


Figure 3 - Activate Software and File Search

Then you can select the software or files to search for in the corresponding wizards (Linux, Mac, Windows AD & IP):



Inventory

Steps 1-2 Windows Systems (IP) **Software and File Search** Summary Scheduling

☒ Apply Software and File Search

<input checked="" type="checkbox"/>	Name	Publisher	File Name/Search Term	Search Path	Version	Category
<input checked="" type="checkbox"/>	log4j-Windows		*log4j*.jar			File Search Windows
<input checked="" type="checkbox"/>	DocusnapScript.exe		DocusnapScript.exe			File Search Windows
<input checked="" type="checkbox"/>	Putty	Simon Tatham	putty.exe	C:	0.76	Software Search

Row Count: 0 of 0

Back Next Cancel

Figure 4 - Using the Software and File Search (Windows IP)

4. Analysis

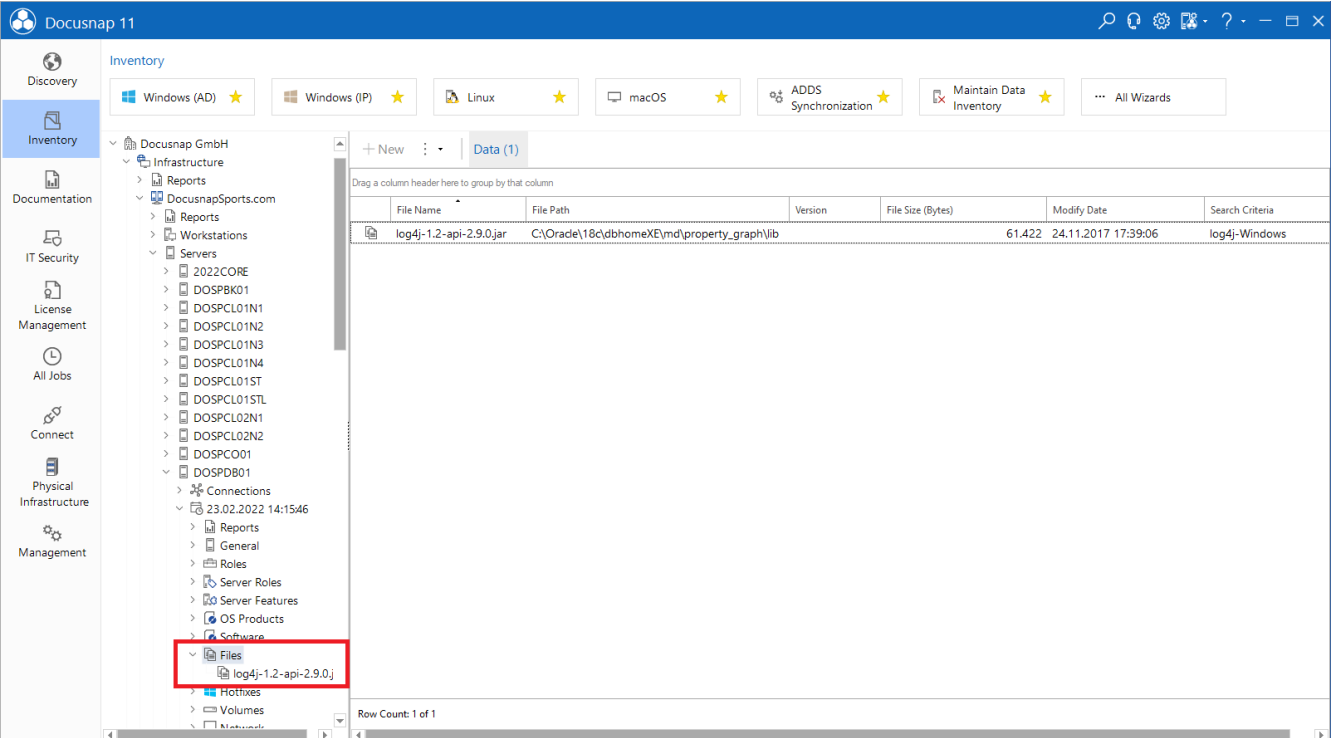
4.1 Software Search

If the defined files are found during the software search, corresponding entries are generated for these in the software list of the system. Thus, this software is listed also in all remaining evaluations of installed software products. This means for example:

- Directly below the system in the list of installed software
- Summary - Software (Company - Infrastructure - Domain - Summary)
- Software reports (Company - Infrastructure - Domain - Reports - Infrastructure SW)

4.2 File search

Also, with the file search the first analysis possibility is directly below the system. In the node Files the found files are listed. In addition to the file name, the file path, version, file size, modification date and the search criterion are also displayed.



The screenshot shows the Docusnap 11 interface. The left sidebar contains a tree view with nodes like Discovery, Inventory, Documentation, IT Security, License Management, All Jobs, Connect, Physical Infrastructure, and Management. The 'Inventory' node is expanded, showing a list of systems. The 'Files' node under 'log4j-1.2-api-2.9.0.jar' is highlighted with a red box. The main area displays a table with the following data:

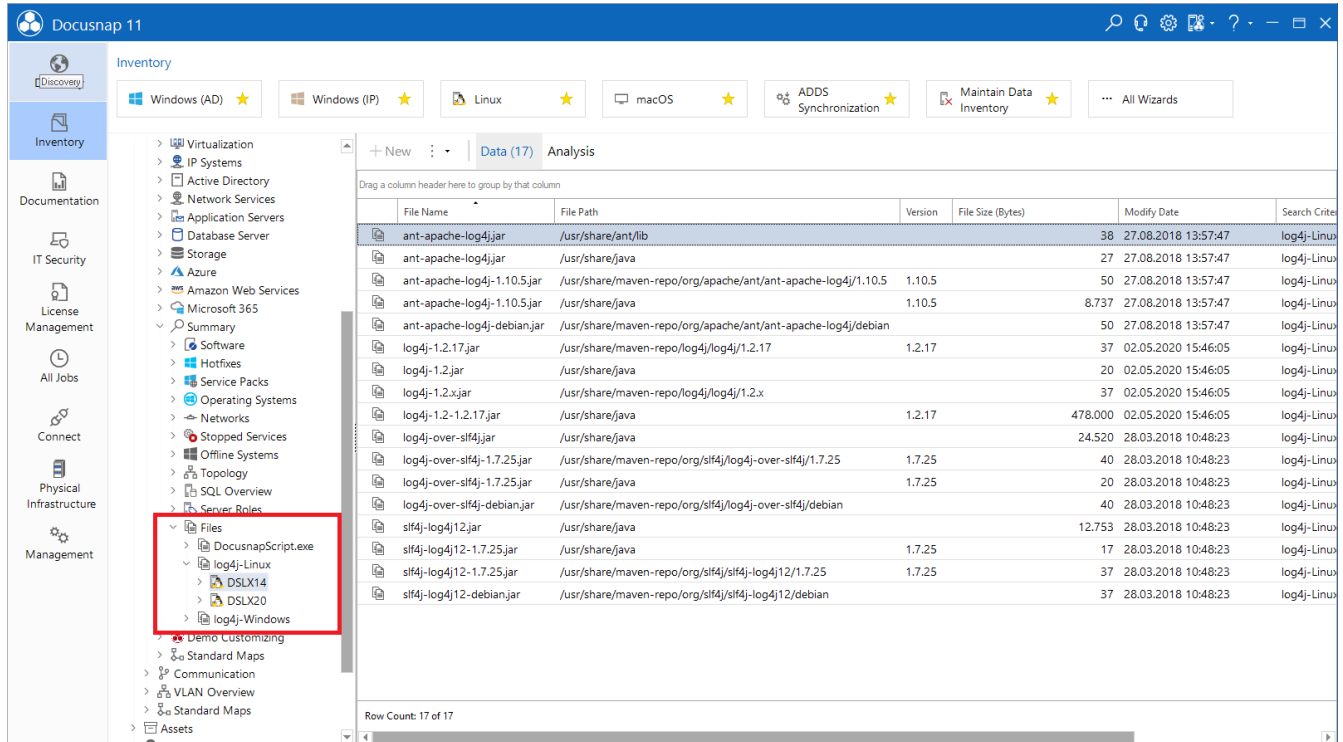
File Name	File Path	Version	File Size (Bytes)	Modify Date	Search Criteria
log4j-1.2-api-2.9.0.jar	C:\Oracle\18c\bin\homeXE\ymd\property_graph\lib		61.422	24.11.2017 17:39:06	log4j-Windows

Row Count: 1 of 1

Figure 5 - File Search - Found File

The next possibility for the file search analysis can be found in the Summary area: Company - Infrastructure - Domain - Summary - Files.

Here, the search terms created in the administration, for which results are available, are displayed first. The next level lists the systems on which the files were found. After that you can view the detailed information of the searched file(s) on the system.



The screenshot shows the Docusnap 11 interface. The left sidebar contains a navigation menu with categories like Inventory, Documentation, IT Security, License Management, All Jobs, Connect, Physical Infrastructure, and Management. The 'Files' folder under 'Summary' is highlighted with a red box. The main area displays a table of search results for 'log4j-Linux'.

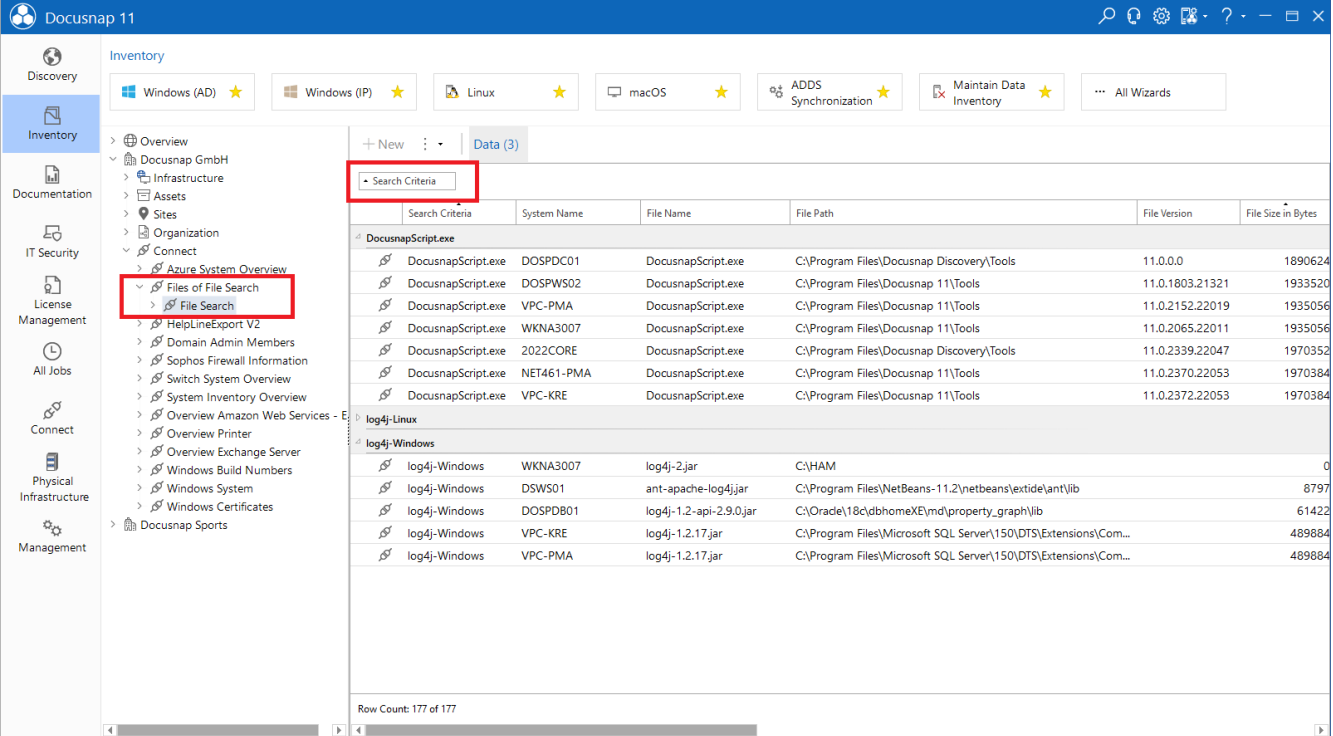
File Name	File Path	Version	File Size (Bytes)	Modify Date	Search Criteria
ant-apache-log4j.jar	/usr/share/ant/lib		38	27.08.2018 13:57:47	log4j-Linux
ant-apache-log4j.jar	/usr/share/java		27	27.08.2018 13:57:47	log4j-Linux
ant-apache-log4j-1.10.5.jar	/usr/share/maven-repo/org/apache/ant/ant-apache-log4j/1.10.5	1.10.5	50	27.08.2018 13:57:47	log4j-Linux
ant-apache-log4j-1.10.5.jar	/usr/share/java	1.10.5	8,737	27.08.2018 13:57:47	log4j-Linux
ant-apache-log4j-debian.jar	/usr/share/maven-repo/org/apache/ant/ant-apache-log4j/debian		50	27.08.2018 13:57:47	log4j-Linux
log4j-1.2.17.jar	/usr/share/maven-repo/log4j/log4j/1.2.17	1.2.17	37	02.05.2020 15:46:05	log4j-Linux
log4j-1.2.jar	/usr/share/java		20	02.05.2020 15:46:05	log4j-Linux
log4j-1.2.x.jar	/usr/share/maven-repo/log4j/log4j/1.2.x		37	02.05.2020 15:46:05	log4j-Linux
log4j-1.2-1.2.17.jar	/usr/share/java	1.2.17	478,000	02.05.2020 15:46:05	log4j-Linux
log4j-over-slf4j.jar	/usr/share/java		24,520	28.03.2018 10:48:23	log4j-Linux
log4j-over-slf4j-1.7.25.jar	/usr/share/maven-repo/org/slf4j/log4j-over-slf4j/1.7.25	1.7.25	40	28.03.2018 10:48:23	log4j-Linux
log4j-over-slf4j-1.7.25.jar	/usr/share/java	1.7.25	20	28.03.2018 10:48:23	log4j-Linux
log4j-over-slf4j-debian.jar	/usr/share/maven-repo/org/slf4j/log4j-over-slf4j/debian		40	28.03.2018 10:48:23	log4j-Linux
slf4j-log4j12.jar	/usr/share/java		12,753	28.03.2018 10:48:23	log4j-Linux
slf4j-log4j12-1.7.25.jar	/usr/share/java	1.7.25	17	28.03.2018 10:48:23	log4j-Linux
slf4j-log4j12-1.7.25.jar	/usr/share/maven-repo/org/slf4j/slf4j-log4j12/1.7.25	1.7.25	37	28.03.2018 10:48:23	log4j-Linux
slf4j-log4j12-debian.jar	/usr/share/maven-repo/org/slf4j/slf4j-log4j12/debian		37	28.03.2018 10:48:23	log4j-Linux

Row Count: 17 of 17

Figure 6 - Summary - File Search

For the file search an additional predefined Docusnap Connect package is available. In this Connect package, the file search results can also be evaluated across domains.

Within the Connect package, the results of all configured file searches are listed. Note the grouping (right click - enable grouping - select field to group by) and filtering options.



The screenshot shows the Docusnap 11 interface. The left sidebar is expanded to 'Inventory', and 'File Search' is selected. The main area displays a table of search results. The table has columns: Search Criteria, System Name, File Name, File Path, File Version, and File Size in Bytes. The results are grouped by file name.

Search Criteria	System Name	File Name	File Path	File Version	File Size in Bytes
DocusnapScript.exe					
DocusnapScript.exe	DOSPC01	DocusnapScript.exe	C:\Program Files\Docusnap Discovery\Tools	11.0.0.0	1890624
DocusnapScript.exe	DOSPWS02	DocusnapScript.exe	C:\Program Files\Docusnap 11\Tools	11.0.1803.21321	1933520
DocusnapScript.exe	VPC-PMA	DocusnapScript.exe	C:\Program Files\Docusnap 11\Tools	11.0.2152.22019	1935056
DocusnapScript.exe	WKNA3007	DocusnapScript.exe	C:\Program Files\Docusnap 11\Tools	11.0.2065.22011	1935056
DocusnapScript.exe	2022CORE	DocusnapScript.exe	C:\Program Files\Docusnap Discovery\Tools	11.0.2339.22047	1970352
DocusnapScript.exe	NET461-PMA	DocusnapScript.exe	C:\Program Files\Docusnap 11\Tools	11.0.2370.22053	1970384
DocusnapScript.exe	VPC-KRE	DocusnapScript.exe	C:\Program Files\Docusnap 11\Tools	11.0.2372.22053	1970384
log4j-Linux					
log4j-Windows					
log4j-Windows	WKNA3007	log4j-2.jar	C:\HAM		0
log4j-Windows	DSWS01	ant-apache-log4j.jar	C:\Program Files\NetBeans-11.2\netbeans\extide\ant\lib		8797
log4j-Windows	DOSPD01	log4j-1.2-api-2.9.0.jar	C:\Oracle\18c\jdkhomeXE\md\property_graph\lib		61422
log4j-Windows	VPC-KRE	log4j-1.2.17.jar	C:\Program Files\Microsoft SQL Server\150\DTSE\Extensions\Com...		489884
log4j-Windows	VPC-PMA	log4j-1.2.17.jar	C:\Program Files\Microsoft SQL Server\150\DTSE\Extensions\Com...		489884

Row Count: 177 of 177

Figure 7 - File Search - Docusnap Connect Package

LIST OF FIGURES

FIGURE 1 - MANAGE SOFTWARE AND FILE SEARCH	6
FIGURE 2 - INCLUDING AND EXCLUDING PATHS	6
FIGURE 3 - ACTIVATE SOFTWARE AND FILE SEARCH	8
FIGURE 4 - USING THE SOFTWARE AND FILE SEARCH (WINDOWS IP)	9
FIGURE 5 - FILE SEARCH - FOUND FILE	10
FIGURE 6 - SUMMARY - FILE SEARCH	11
FIGURE 7 - FILE SEARCH - DOCUSNAP CONNECT PACKAGE	12

Version history

Date	Description
02/24/2022	HowTo created
09/27/2022	Screenshots adjusted
