



IP-Scan

Inventory of IP Systems

TITLE	IP-Scan
AUTHOR	Docusnap Consulting
DATE	11/28/2023
VERSION	4.0 valid from November 28, 2023

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.

TABLE OF CONTENTS

1.	Introduction	4
2.	Prerequisites	5
2.1	Risks and Difficulties	5
3.	IP-Scan	6
3.1	IP-Scan Wizard	6
3.2	Analysis and Result	7
3.3	MAC Filters for IP Systems	7
4.	Optional: IP-Scan Analysis Tool	9
4.1	Purpose of Use	9
4.2	Application of the Test Program	10
4.2.1	Scan	10
4.2.2	Analyze	10
4.2.3	Help	10
4.3	Transfer to Docusnap	11
4.3.1	Analysing results	11
4.3.2	Adaptation of the Docusnap IP Scan Configuration	11
5.	Application Cases and Practical Examples	13
5.1	Initial Inventory	13
5.2	Increase data quality	13
5.3	Detect Security Vulnerabilities	14

1. Introduction

The IP-Scan in Docusnap gives you the possibility to search your network or that of a customer extensively for active systems. All you need for this initial overview, or to check for a complete inventory, are the relevant IP address ranges. No login information or community strings are used for the IP Scan. This way you can quickly and easily inventory a new network and get an overview.

In your own network, you can use this method to capture active components that you have not yet captured with a more detailed scan. Reasons for this could be, for example, that the system is not known, or the necessary logon information is missing.

This HowTo describes the use of the IP Scan and is divided into the following chapters:

- [Chapter 1](#) explains the necessity and installation of the NPCAP driver.
- [Chapter 2](#) describes the actual IP Scan.
- [Chapter 3](#) shows how to test NMAP parameters and then transfer them to Docusnap.
- In [Chapter 4](#), use cases and practical examples are listed

Docusnap distinguishes between a normal and an extended IP Scan. Both IP Scans are based on **NMAP (Network Mapper)**. The normal IP Scan uses functions like SYN-ACK, ARP-Request, ICMP requests and name resolution. Responding systems are captured with rudimentary network information.

By using special NMAP parameters, the extended IP Scan can detect additional information such as the operating system.

Prerequisite for the extended IP Scan is the installation of the **NPCAP driver** on the inventorying system.

2. Prerequisites

In the first step, a successful IP scan only requires the IP address ranges to be inventoried to be known.

As already mentioned, a distinction is made between the simple and the extended IP scan. The NPCAP driver is required for the extended IP scan. The NPCAP driver is required on the system from which the IP scan is performed. This can be the Docusnap Server, Docusnap Client and the Docusnap Discovery systems.

The installation of the NPCAP driver is offered to you in the course of the Docusnap installation and is active by default.

You can perform a subsequent installation using the setup provided:

- %ProgramFiles%\Docusnap 13\MSI\npcap-oem.exe
- %ProgramFiles%\Docusnap Discovery\MSI\npcap-oem.exe

2.1 Risks and Difficulties

Prerequisite for the installation of the NPCAP driver are local administrator rights.

When installing the NPCAP driver, please note that it interferes with the network area. Especially with systems such as a domain controller, Exchange server or similar, an installation should not be carried out lightly.

Also note that installing the NPCAP driver may be in competition with similar network drivers. This may also affect other versions of the NPCAP driver. For example, a Wireshark or PRTG installation will also install a NPCAP, or former WINPCAP, driver. Since it is possible that Wireshark or PRTG has different installation options, both Wireshark and Docusnap may produce incorrect results.

You can find further information on the requirements and problems with e.g. firewalls and monitoring in our [White Paper Docusnap Inventory](#) in the IP Scan chapter.

3. IP-Scan

3.1 IP-Scan Wizard

The IP-Scan is a standalone inventory wizard in Docusnap. A distinction is made between the **Simple IP-Scan** and the **Advanced IP-Scan**. The selection can be made during the wizard using a checkbox.

The IP-Scan Wizard can be found here:

- Discovery – All Wizards – IP Scan
- Inventar – All Wizards – IP Scan
- Alle Aufträge – All Wizards – IP Scan

IP Scan

The IP Scan checks the addresses using ICMP requests. If the requested system responds, it is recorded as an IP system and stored in the database with additional information (scan date, IP address and subnet mask). In addition, the IP Scan attempts to resolve the associated DNS name. If this is successful, the system is registered with the DNS name.

Advanced IP Scan

With the help of the extended mode, MAC vendor, information on the operating system, operating time and the last system start are also recorded. The accuracy of the information collected is expressed as a percentage. This is because NMAP cannot always determine the operating system etc. one hundred percent. NMAP estimates this information based on the response to requests sent.

If the Extended IP Scan is activated, Docusnap searches for the required NPCAP driver. If this is not available, the extended IP Scan cannot be used.

If you want to specify several networks for inventory it is recommended to use the CSV import. You can call this up by choosing **Load list**. In the following figure the structure of the CSV file is described.

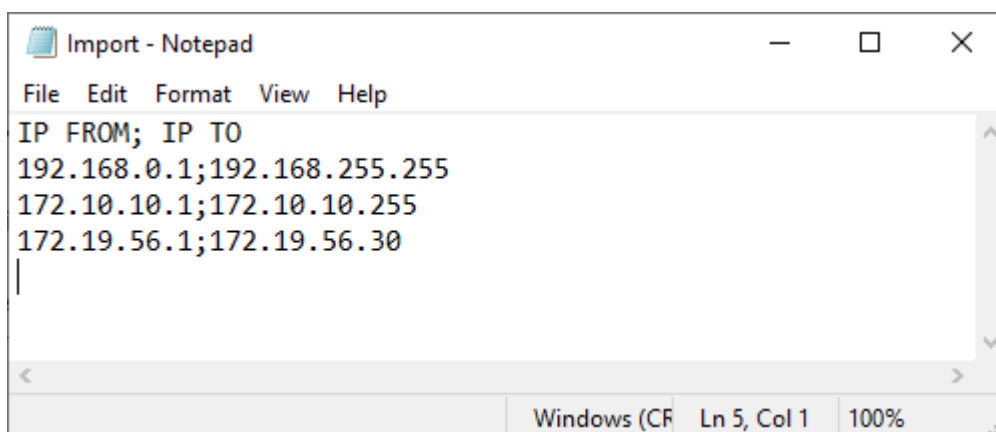


Fig. 1 - IP Ranges - CSV Import

The maximum size of a network segment is limited to Class B (192.168.1.1 - 192.168.255.255).

3.2 Analysis and Result

You can find the results of your IP Scan in the Docusnap data tree under

- **Company - Infrastructure - Domain - IP Systems.**

Overview of the information that can be captured:

- **Name:** Name of the system. If a DNS entry exists, this DNS entry will be used as the name, otherwise the IP address.
- **Scan Date:** Time at which the system was last captured by IP Scan
- **IP Address:** IP address of the system
- **Subnet Mask:** Subnet mask of the system
- **MAC Address:** MAC address of the system. **Note: The MAC address is only available if the inventoried IP system is on the same network as the inventorying part (Docusnap Server, Client, Discovery Service)**
- **MAC Vendor:** Vendor - Based on the MAC address entered
- **Operating System:** Information on the operating system used
- **Vendor:** Vendor of the operating system
- **Version:** Version number of the operating system
- **System Family:** Family, e.g. Windows or Linux
- **Operating Time:** Time in hours
- **Last Boot Start:** Date on which the system was last booted
- **Accuracy:** Indication of the accuracy of the extended information in percent

With the help of advanced information such as the MAC vendor and information on the operating system, a general overview of the network can be obtained. The systems can then be assigned to an assistant for further inventory.

IP systems are considered in reports as well as in the network and Topology Plan.

3.3 MAC Filters for IP Systems

Some systems can only be captured via IP Scan because no other standard interface, e.g. SNMP, is supported. A MAC filter is available so that these systems can be displayed in the Topology Plan as telephones, for example. This makes it easier for you to distinguish the IP systems in the Topology Plan.

Procedure:

- Identify the lowest common denominator at the MAC address. For two IP telephones, each with one MAC address **00-1A-E8-EC-CA-70** and **00-1A-E8-EC-E9-DC**, the lowest common denominator would be **00-1A-E8-** (= Vendor).
- Switch to Docusnap **Administration - Inventory** tab - **MAC filter**
- Put the MAC address there - **00-1A-E8-**
- Supported wildcard characters are ***** to specify multiple arbitrary characters and **?** to specify exactly one arbitrary character.

MAC addresses of the Ignore and Virtual type are no longer displayed in the Topology Plan.

Further information about the MAC Filter can be found in the Docusnap manual in the MAC Filter section. (F1 key in the corresponding area within the Docusnap Administration) or in the [HowTo Inventory and Analysis of SNMP](#) in the Docusnap Knowledge Base.

4. Optional: IP-Scan Analysis Tool

The IP Scan Analysis Tool is available on request from Docusnap Support.

4.1 Purpose of Use

Every network is different. Thus, it can happen that the IP Scan does not deliver any results in rare cases. This can be caused by the virus scanner, the configuration of the firewall or a proxy. Various network components can affect the results of the IP Scan. The Docusnap IP Scan uses parameters in the standard which successfully inventory data for a large part of the networks. To get the best results with the IP Scan in your network, you can use the IP Scan Analysis Tool to find out the NMAP parameters that are right for you. You can then pass them to Docusnap.

The IP Scan Analysis Tool is a standalone application. No Docusnap installation is required. Prerequisite is the installation of the NPAC driver.

For the best possible analysis, you should run the IP Scan Analysis Tool on the same system as the Docusnap IP Scan is running on, e.g. Docusnap Server or Docusnap Discovery Service.

Standard parameters of the Docusnap IP Scan, Docusnap version 10.0.1472.2:

```
-F -T3 -O --osscan-guess --script smb-os-discovery.nse
```

4.2 Application of the Test Program

If you start the IP Scan Analysis Tool with a double-click, a new window opens. Within this GUI, you can perform an IP Scan, influence parameters, and then analyse the results.

The Analysis Tool is divided into three areas. **Scan**, **Analyze** and **Help**.

4.2.1 Scan

Within the **Scan** area it is possible to adjust the parameters according to your network. You can also use presets to do this. The presets differ in the parameters used. The following presets are available:

- PingScan: Parameter -PE - Ping. (echo reply expected)
- Nmap PingScan: Parameter -sP - simple IP Scan in Docusnap
- Docusnap Version: Uses NMAP parameters of the respective Docusnap version

You can adjust the parameters to be used under **Parameter Section**. Parameters can be selected using the checkboxes or added by entering text into the text box **Parameter**. A detailed overview of all available NMAP parameters can be found at <https://nmap.org/>.

In the following example the scan is performed with the preset of the last Docusnap version. The parameters are set automatically with a click on the respective preset. The **Start Scan** button starts the scan with the specified parameters.

The parameters used and the path of the log file can be found in the respective text boxes. Logfiles are saved in an automatically created folder on your desktop. In the logging, you see information about the status of the scan.

Example:

To accelerate the execution of the IP Scan, the speed is increased and the measures for operating system detection are minimized.

Note that increasing the speed can affect the quality of the results.

4.2.2 Analyze

In the **Analyze** area you can evaluate the results of your last or previous scans. More detailed information on analysis can be found in the following chapter [Analysing Results](#)

4.2.3 Help

Within the **Help** tab you will find more information about **timing settings** and **analysis**.

4.3 Transfer to Docusnap

4.3.1 Analysing results

You can then evaluate the results of your scans in the Analyze area. By default, the IP Scan Analysis Tool opens the last scan performed. If you want to evaluate a certain scan, you can load the desired .xml file into the analysis window via **File Selection**.

A distinction is made between **Simple Analyze** and **Analyze with ProxyCleanup**.

In the **Simple Analyze**, only the results from the scan are evaluated. Incorrectly detected hosts, e.g. triggered by a transparent proxy, are not filtered.

In a **Cleanup Analyze**, the detected hosts are then filtered in the same way as in Docusnap. This tries to filter out hosts that were wrongly recognized as positive. In networks with a transparent proxy, it may happen that the proxy responds to every request of the IP Scan. Thus, all addresses are recognized as positive. The Cleanup function is used to filter out incorrectly detected systems. You can then see the results of your scan in the analysis window and export them to a CSV file, for example.

If the results of the scan correspond to the systems of your network, you can then pass the parameters you set to Docusnap.

4.3.2 Adaptation of the Docusnap IP Scan Configuration

The NMAP parameters for the IP Scan are performed in **DocusnapSettings.xml**. Please note that this adjustment must be carried out on every system. If, for example, you have several Docusnap Discovery Services in use, the DocusnapSettings.xml must be adapted on the respective system.

If no parameters are set, the Docusnap IP Scan automatically uses the parameters of the respective Docusnap version.

By default, DocusnapSettings.xml is located on the Docusnap or Docusnap Discovery Service host system in the following directory:

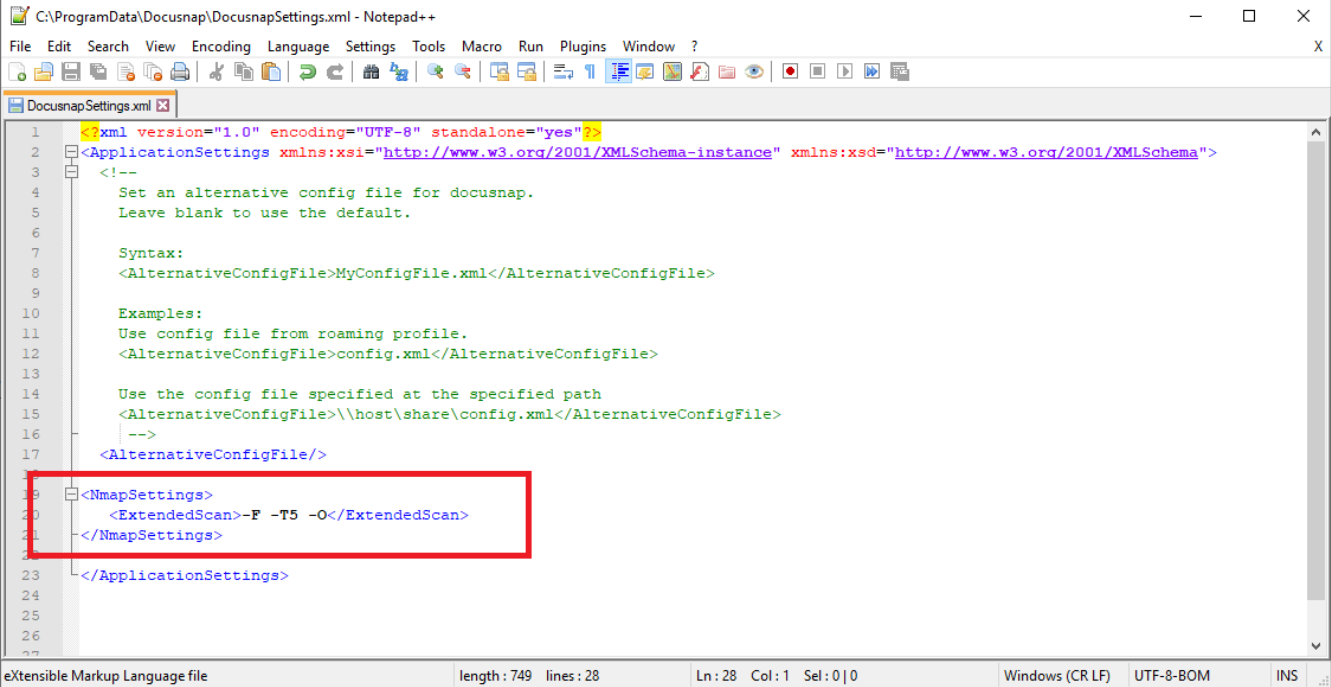
C:\ProgramData\Docusnap\DocusnapSettings.xml

You can edit DocusnapSettings.xml with a text editor, such as Notepad.

Within the **<ApplicationSettings>** tags the new tags are inserted. Between the **<ExtendedScan>** tags you can then store your parameters.

NMAP parameter tags for DocusnapSettings.xml:

```
<NmapSettings>
  <ExtendedScan></ExtendedScan>
</NmapSettings>
```



```
1 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2 <ApplicationSettings xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
3   <!--
4     Set an alternative config file for docusnap.
5     Leave blank to use the default.
6
7     Syntax:
8     <AlternativeConfigFile>MyConfigFile.xml</AlternativeConfigFile>
9
10    Examples:
11    Use config file from roaming profile.
12    <AlternativeConfigFile>config.xml</AlternativeConfigFile>
13
14    Use the config file specified at the specified path
15    <AlternativeConfigFile>\\host\share\config.xml</AlternativeConfigFile>
16    -->
17   <AlternativeConfigFile/>
18
19   <NmapSettings>
20     <ExtendedScan>-F -T5 -O</ExtendedScan>
21   </NmapSettings>
22
23 </ApplicationSettings>
```

Fig. 2 - NMAP Parameters in Docusnap - DocusanpSettings.xml

5. Application Cases and Practical Examples

5.1 Initial Inventory

A complete and detailed inventory of a network environment is only possible with sufficiently privileged users. Often the person taking the inventory has neither root access to Linux systems nor administrative access to Windows systems for a new customer. Nevertheless, the network needs a first overview.

The advanced IP Scan allows you to analyze the desired networks without the need for administrative rights. You can find out how many systems are available. With the help of the operating system information it is then possible to subdivide the data into corresponding categories.

- ➔ Number of Windows systems
- ➔ Number of Linux systems
- ➔ Number of possible SNMP systems
- ➔ Etc.

5.2 Increase data quality

A prerequisite for high-quality documentation is good data quality in Docusnap. Since there is often no overview of the existing systems, it is not possible to check the inventoried systems against each other. With the help of the IP Scan it is possible for you to create an overview with unknown systems and to capture them specifically.

Initial situation:

All the company's printers are in the XYZ network. This network is already regularly inventoried via SNMP. To make sure that all systems within the network are really captured, the IP Scan is also used regularly.

In this case, if devices are not yet included in Docusnap, they will now be added to the IP systems.

You should then check the IP systems that have been captured regarding the SNMP interface.

If these systems are recorded as SNMP systems in the future, the entry below the IP systems will be moved. However, a downgrade is not possible - e.g. SNMP to IP system.

5.3 Detect Security Vulnerabilities

Bring your own device, old network components and Internet of Things. These systems are often associated with security vulnerabilities. The following describes how you can detect, document, and react to security vulnerabilities using the Docusnap IP Scan.

Detect old network components:

In a growing network, more and more old systems may become available over time. Depending on the function, this can result in a security gap. If these systems do not support at least the SNMP protocol as an interface, it will be difficult to record, document and react accordingly.

The IP Scan allows you to perform a regular scan of your network. If, for example, an old switch is still in use, it is detected by the IP Scan. This will prevent your network from failing due to outdated hardware, for example.

Bring your own Device / Internet of Things

The statement "Every new refrigerator has an IP address" does not quite correspond to reality but hits the nail on the head. Various systems are connected to the networks of a company. From workstations, servers, private mobile phones to everyday systems, everything is included. Due to the security of the network, these are often divided into different areas. Security gaps can occur if the coffee machine is suddenly available in the same VLAN as the switches.

To detect such a misconfiguration, the IP Scan is a good choice. Since all active systems are captured on the network, you can also find the everyday systems and other devices and check their network configuration.

LIST OF FIGURES

FIG. 1 - IP RANGES - CSV IMPORT.....	6
FIG. 2 - NMAP PARAMETERS IN DOCUSNAP - DOCUSANPSETTINGS.XML	12

VERSION HISTORY

Date	Description
October 7, 2019	Version 1.0 - Description of the IP Scan
April 22, 2020	Version 2.0 - Revision of the HowTo for Docusnap 11
August 01, 2022	Version 2.1 – Extension by the missing MAC addresses from other networks
January 10., 2023	Version 3.0 – Revision of the HowTo for Docusnap 12
November 28, 2023	Version 4.0 – Revision of the HowTo for Docusnap 13
