

# Implementation plan for Information Security Management System framework in accordance with **ISO 27001** and **NIS2** using nVision

---



|                                                                 |    |
|-----------------------------------------------------------------|----|
| 1. Identification and inventory of assets (A.5.9, A.8.20).....  | 6  |
| 1.1 Device Inventory .....                                      | 8  |
| 1.1.1 Network scanning.....                                     | 8  |
| 1.1.2 Agent installation .....                                  | 9  |
| 1.1.3 Creating departments.....                                 | 10 |
| 1.1.4 Assigning departments to devices .....                    | 11 |
| 1.1.5 Automatic asset creation from Agent.....                  | 13 |
| 1.1.6 Creating the <i>network device</i> asset type .....       | 14 |
| 1.1.7 Identification of critical devices .....                  | 15 |
| 1.2 Inventory of software and web applications .....            | 19 |
| 1.2.1 The software scanning process .....                       | 20 |
| 1.2.2 Inventorying additional systems .....                     | 21 |
| 1.2.3 Assigning systems to departments .....                    | 22 |
| 1.3 Primary and supporting assets.....                          | 23 |
| 1.3.1 Introducing information assets .....                      | 23 |
| 1.3.2 Adding a relation.....                                    | 25 |
| 1.3.3 Assigning supporting assets.....                          | 25 |
| 1.4 Users .....                                                 | 26 |
| 1.5 Grouping assets .....                                       | 28 |
| 1.5.1 Creating the <i>Device Group</i> type .....               | 28 |
| 1.5.2 Adding devices of a given type to a group .....           | 33 |
| 1.6 Optimizing the inventory process .....                      | 34 |
| 1.6.1 Exporting data on user activity .....                     | 34 |
| 1.5.3 Creating audit snapshots on recurring basis.....          | 34 |
| 1.6.2 Creating an alert for additional assets .....             | 36 |
| 1.7 Summary .....                                               | 37 |
| 2. Definition of responsibility for assets (A.5.9, A.5.2) ..... | 38 |
| 2.1 Assigning business owners.....                              | 38 |
| 2.1.1 Creating a group for business owners .....                | 39 |
| 2.1.2 Assigning business owners to network devices .....        | 41 |
| 2.1.3 Assigning business owners to device groups .....          | 43 |

|       |                                                                        |    |
|-------|------------------------------------------------------------------------|----|
| 2.1.4 | Assigning business owners to systems .....                             | 43 |
| 2.2   | Announcement to business owners .....                                  | 43 |
| 2.2.1 | Exporting the list of assets of business owners .....                  | 44 |
| 2.2.2 | Announcement template and sending.....                                 | 45 |
| 2.3   | Assigning responsible people to assets.....                            | 48 |
| 2.4   | Verification of asset status by users .....                            | 51 |
| 2.4.1 | Preparing the announcement to users .....                              | 52 |
| 2.4.2 | Ticket automation .....                                                | 53 |
| 2.4.3 | Sending the announcement.....                                          | 55 |
| 2.5   | Managing change in the scope of responsibility and permissions.....    | 56 |
| 2.5.1 | Restricting access in the event of suspended cooperation .....         | 56 |
| 2.5.2 | Applying blocks to the accounts of deactivated users .....             | 57 |
| 2.5.3 | Disabling the account.....                                             | 61 |
| 3.    | Risk analysis for assets .....                                         | 62 |
| 3.1   | Introduction to threats and security controls in nVision .....         | 62 |
| 3.1.1 | Threats and security controls – creating asset types .....             | 63 |
| 3.1.2 | Importing threats and security controls.....                           | 65 |
| 3.1.3 | Creating relations .....                                               | 66 |
| 3.2   | Linking threats and security controls to assets (6.1.2, A.8.8) .....   | 67 |
| 3.3   | Conducting and digitizing the risk assessment (6.1.2) .....            | 69 |
| 3.3.1 | Estimating the risk level .....                                        | 69 |
| 3.3.2 | Adding a global field .....                                            | 71 |
| 4.    | Selection and implementation of security controls (6.1.3) .....        | 72 |
| 4.1   | Implementation of appropriate security controls.....                   | 72 |
| 4.2   | Testing security controls .....                                        | 74 |
| 4.2.1 | One-off tests .....                                                    | 75 |
| 4.2.2 | Recurring notifications .....                                          | 76 |
| 4.3   | Vulnerabilities – identification and response to their occurrence..... | 80 |
| 4.3.1 | Asset reports .....                                                    | 80 |
| 4.3.2 | Obligations of the business owners of systems.....                     | 82 |
| 5.    | Submission Forms.....                                                  | 84 |
| 5.1   | Incident submission and assessment form .....                          | 85 |

|       |                                                                             |     |
|-------|-----------------------------------------------------------------------------|-----|
| 5.2   | Exception submission form .....                                             | 87  |
| 5.3   | Access granting form.....                                                   | 87  |
| 5.4   | Corrective action card form (post-audit) .....                              | 88  |
| 5.5   | Security control implementation form (resulting from risk assessment) ..... | 88  |
| 5.6   | Continuity plan performance/testing confirmation form .....                 | 89  |
| 5.7   | Onboarding form .....                                                       | 89  |
| 5.8   | Offboarding form.....                                                       | 90  |
| 6.    | Register of granted access.....                                             | 92  |
| 7.    | Maintenance tasks – reminders and announcements.....                        | 96  |
| 7.1   | Security awareness and good practices .....                                 | 98  |
| 7.2   | Password security .....                                                     | 98  |
| 8.    | Supporting the audit.....                                                   | 99  |
| 8.1.1 | Filtering assets in the list .....                                          | 99  |
| 8.1.2 | Exporting data from the reports view .....                                  | 100 |
| 9.    | Conclusion.....                                                             | 101 |

An **information security management system (ISMS)** is an organized set of activities aimed at bringing order to and strengthening information security within an organization. This document provides a set of guidelines that will help you use nVision to build a solid foundation for an ISMS that meets the requirements of the ISO 27001 standard.

### **Purpose:**

- to ensure the organization's resilience,
- to reduce the risk of incidents,
- to meet formal regulatory requirements.

This document also considers the requirements of the NIS2 Directive (and its transposition into the applicable national implementing legislation) regarding risk management, security of networks and information systems and operational obligations concerning inventory, asset classification, monitoring and configuration documentation.

### **Main implementation stages:**

1. Identification and inventory of assets.
2. Definition of responsibility for assets.
3. Risk analysis for assets.
4. Selection of security controls appropriate to the risk level.
5. Development of operational processes that support risk management.

# 1. Identification and inventory of assets (A.5.9, A.8.20)<sup>1</sup>

An **asset** is anything of value to the organization (per ISO/IEC 27000). We describe assets using the following parameters:

- owner,
- location,
- information about related systems,
- data sensitivity level,
- supplier.

The first stage of the process is gathering knowledge about assets (identification) and mapping them in nVision. At this stage, you determine what you want to protect by answering the following questions:

- what information does the organization process?
- who is responsible for it?
- what are the dependencies between the processes and services and the inventoried assets?
- which elements are critical to the services and processes provided?

With this knowledge, you will determine the risk level, identify possible threats and create appropriate protective procedures in the later stages.

At this stage, you will build a knowledge base about your infrastructure. Based on this, you will:

- assign responsibility for assets,
- establish the level of restrictions for specific categories of hardware,
- define the rules for granting permissions and access,
- increase control over the addition and removal of assets.

To take full advantage of the module's capabilities, ensure that the nVision Agent is installed on every computer within your organization.

---

<sup>1</sup> This requirement also corresponds to the obligations set out in Article 21(2)(a) and (e) of the NIS2 Directive, together with applicable national cybersecurity legislation, which require organizations to maintain an inventory of and exercise oversight over network assets, equipment and services affecting the security of critical infrastructure.

The nVision Agent is a small program installed on computers that sends detailed data about the following to the nVision server:

- hardware and technical parameters of connected devices (disk usage, CPU usage, memory usage, connected external storage sources),
- users and their activity (working time, applications used, websites visited, network traffic generated, cost and number of pages printed),
- software and configuration (installed applications, changes to the hardware and software configuration of devices, applications launched),
- system operational data (data transmission, application monitoring, application blocking, Windows event log).

During the inventory process, you will encounter two basic concepts:

**device** – any type of physical hardware connected to the network; a device is discoverable and can be monitored to collect information about its performance and other parameters;

**asset** – can be anything you need to inventory: all kinds of hardware or related documentation (e.g. licenses), but also software, web applications, and even processes.

These concepts correspond to two tabs in nVision, and therefore to two separate views. Devices belong to the Network module and they are usually discovered rather than added. Once discovered, they are mapped to assets.

Assets, in turn, belong to the Inventory module. You can add, remove and modify them, group them into types, assign departments or users to them, and even create relations between them. It is this asset view that you will use as the foundation of your information security system.



Implementing the requirements of ISO 27001 and NIS2, together with the applicable national implementing legislation, introduces a category of assets comprising the concepts of devices and assets, which are used in nVision.

## 1.1 Device Inventory

To ensure compliance with ISO 27001, you must have an **accurate, up-to-date and complete list of assets**, including:

- computers,
- network devices,
- servers,
- virtual environments,
- peripheral hardware.

**Without an asset inventory, you cannot demonstrate compliance with the standard's fundamental requirement.**

The inventory will also enable you to assess risk and plan security controls.

Computers and network devices are information-processing assets, and as such are relevant to information security. Every computer stores and processes data and provides access to information. Every network device controls the flow of information and secures its transmission, which is a key element of availability. This is why you need tools that will allow you to oversee the configuration of assets and any changes to them.

The inventory also ensures accountability by making it possible to assign devices to their owners who are responsible for the associated risks. By defining the level of permissions and the scope of device use, it also makes it possible to identify violations and incidents.

### 1.1.1 Network scanning

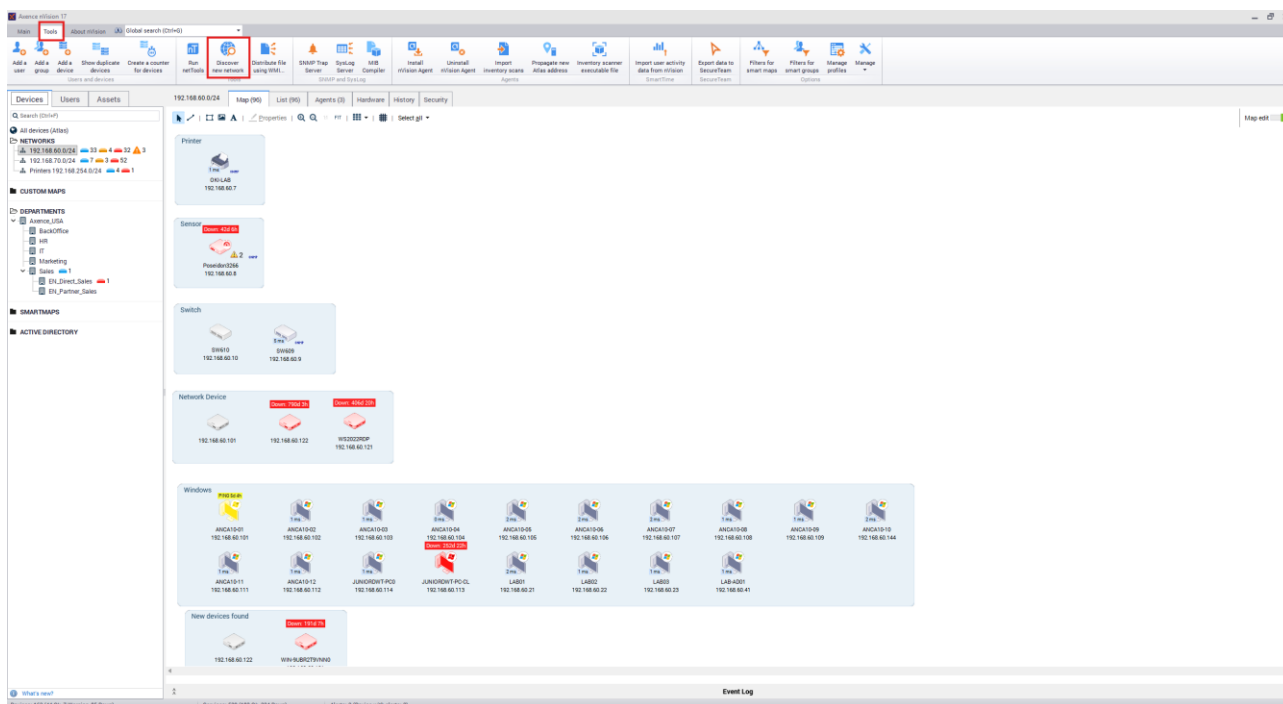
Network scanning enables the automatic discovery of network infrastructure elements, which allows you to:

- define the devices operating within a given network, such as computers, printers, routers, switches and servers,
- identify the services running on the devices and, consequently, determine the functions of a given device and the traffic it generates,
- identify dependencies between network elements,
- determine which ports are active,
- generate network maps.

From a security management perspective, the benefits are considerable:

- a complete list of active infrastructure elements,
- knowledge of shadow IT (devices connected without the administrators' knowledge)<sup>2</sup>,
- infrastructure documentation,
- dependency analysis and identification of critical points,
- insight into the operating parameters of devices.

To perform network scanning, use the **Discover new network** option on the **Tools** tab of the nVision console.



More information about network scanning can be found [here](#).

## 1.1.2 Agent installation

The nVision Agent provides the following for inventorying network elements:

- the device's hardware parameters (CPU, RAM, disk),
- information about connected devices (USB, other peripherals),
- data on the device's status and communication (transmission, availability),
- information about the logged-in user,

<sup>2</sup> Article 21(2)(d) and (h) of NIS2, together with applicable national cybersecurity legislation, require organizations to be able to detect unauthorized devices and services to ensure supply chain integrity and protect infrastructure from uncontrolled assets.

- continuous visibility of the hardware in the system.

You can install the nVision Agent in three ways:

- through Active Directory, using the MSI installer,
- remotely, using the management console of your antivirus software,
- manually.

More information about installing and running the Agent can be found [here](#).

### 1.1.3 Creating departments

Departments allow you to create the organizational structure in nVision that reflects the division of your organization into functional organizational units (e.g. marketing, sales, HR, etc.). They are particularly useful in large organizations. They may differ in terms of:

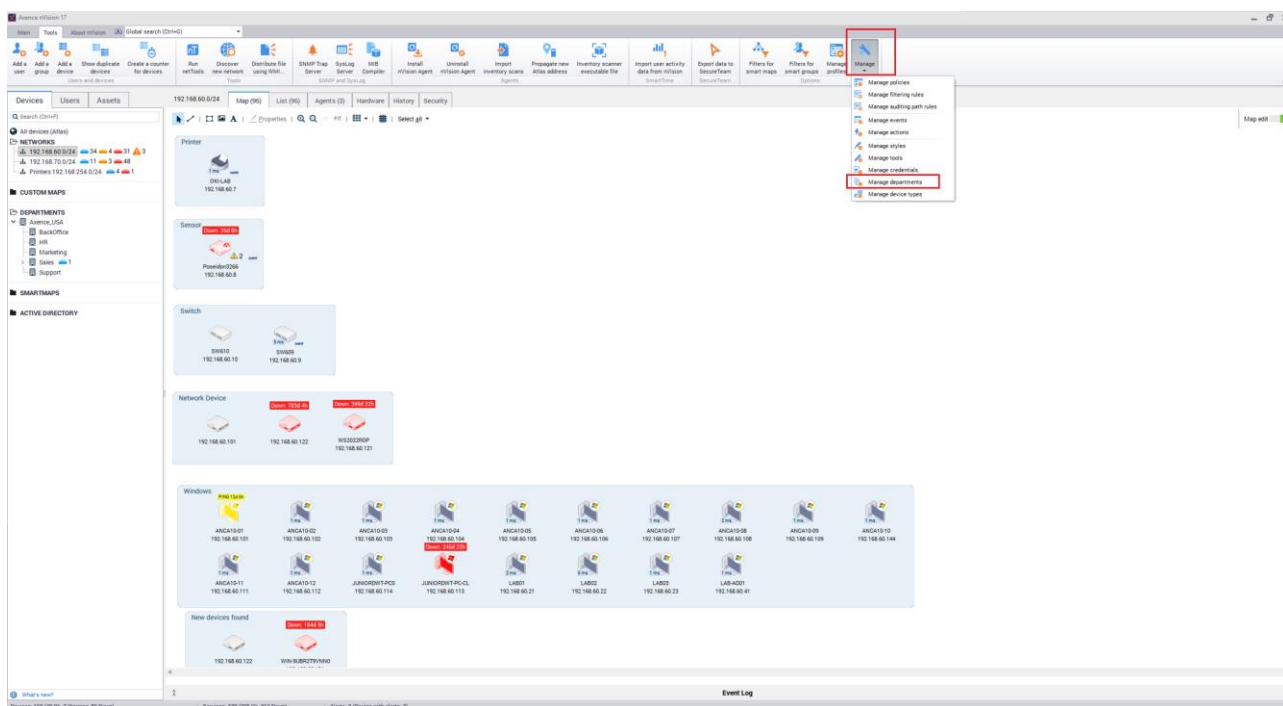
- assigned assets (e.g. HR department computers, management laptops, printers in the administration department),
- the web and desktop applications used (e.g. the CRM in the sales department – Salesforce, HubSpot or other),
- system permissions (e.g. IT has administrative permissions to the infrastructure, accounting has access to the financial system),
- identified threats (e.g. sales: loss of customer data, HR: leak of personal data),
- implemented security controls (e.g. disk encryption on HR laptops, MFA in financial systems).

If your organization does not have an extensive structure, treat this step as optional: the asset inventory will be considered from the perspective of the entire organization. Otherwise, defining departments is important, because it sets the context in which you determine risks, priorities and the rules for using assets.

Creating departments allows you to:

- more easily assign responsibility for assets,
- determine where data is processed,
- adapt security controls to the context of a given location,
- differentiate information and access policies,
- limit the scope of a potential incident,
- quickly identify where a problem has occurred.

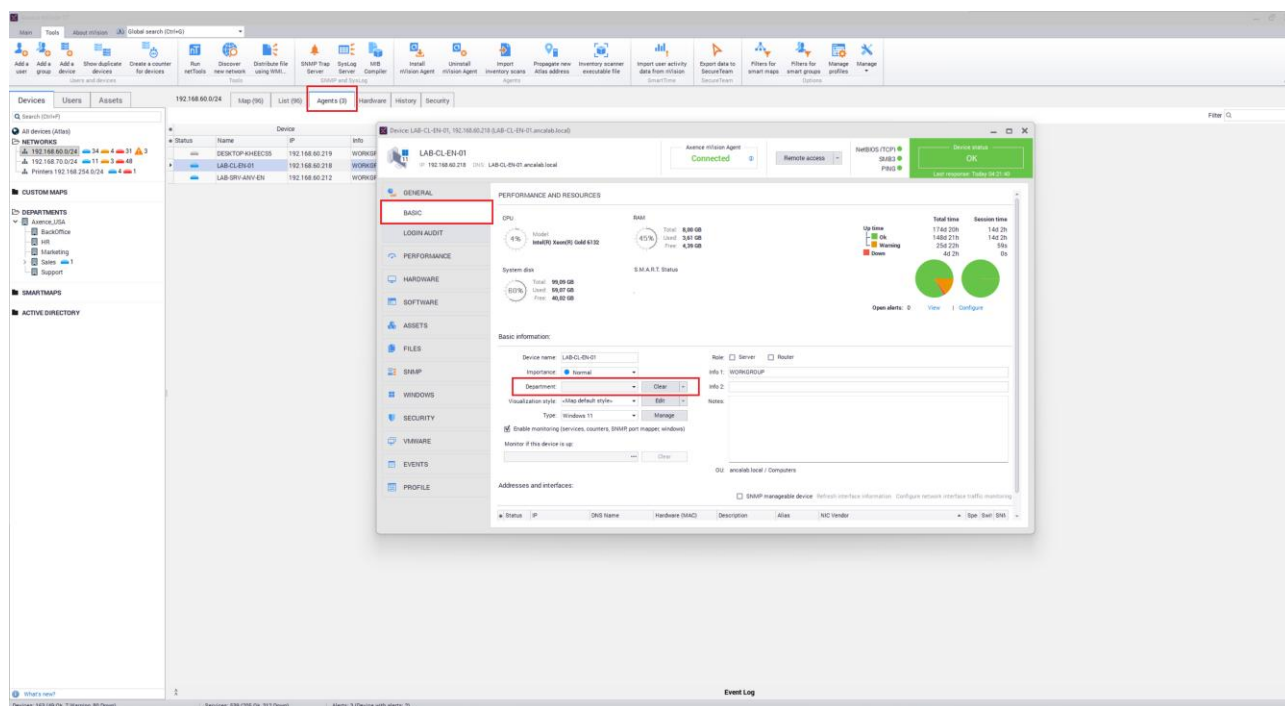
You can add departments and arrange them into a hierarchy using the **Manage departments** option, which can be found under the **Manage** button on the **Tools** tab:



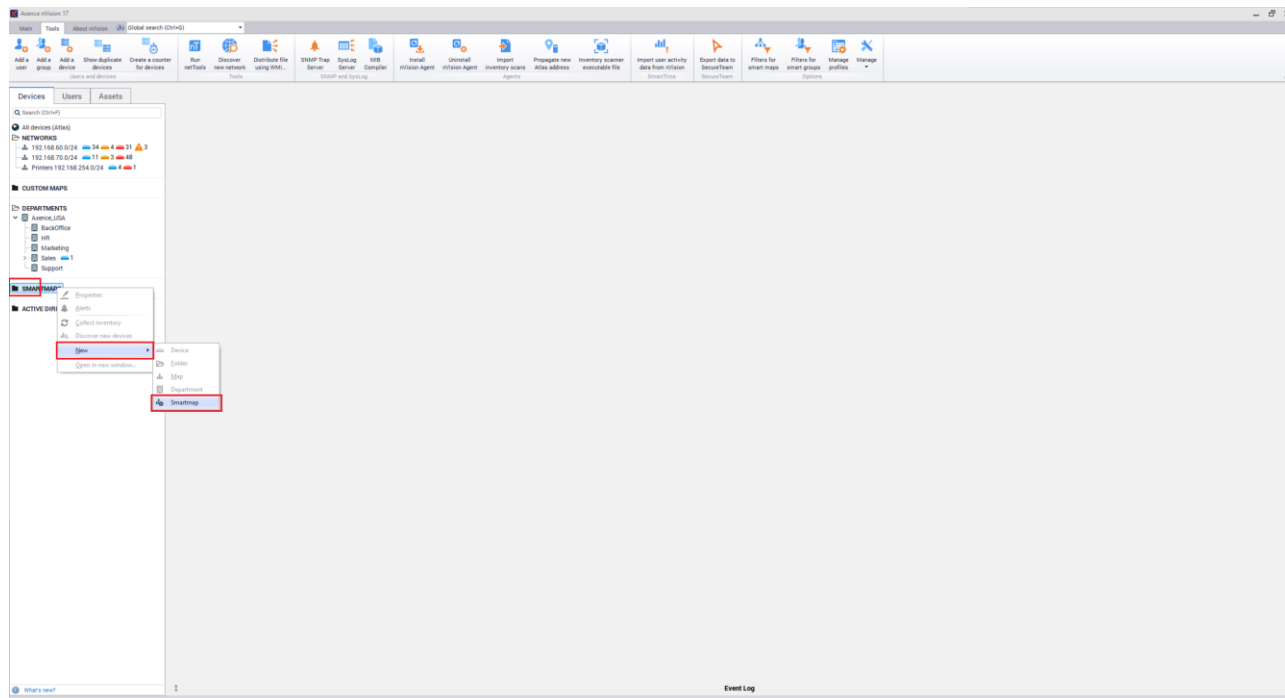
This allows you to create a representation of your actual organizational units in nVision. You can see the example in the screenshot above. The departments are separated out, and some of them have already been linked to devices (the blue and red icons next to marketing and sales). More information about departments can be found [here](#).

### 1.1.4 Assigning departments to devices

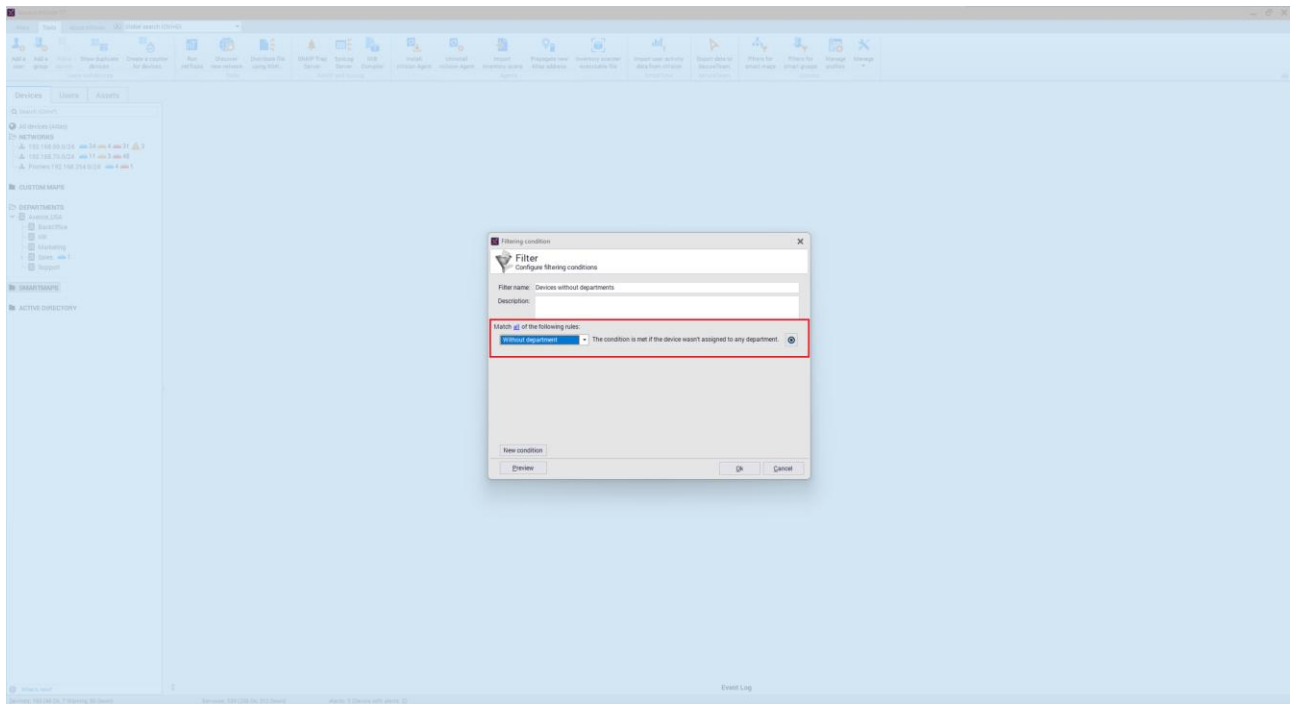
Thanks to network scanning and the installation of Agents, you can see a list of all the devices operating in your network. At this stage, you can link them to departments by assigning a department to an individual device. This step is essential to take full advantage of the possibilities provided by structuring. You can assign departments to devices in the **Basic** section of the specific device's window:



Once you have determined the department membership of all detected devices, you can ensure you will quickly learn about the detection of new ones in the future. To do this, create a SmartMap with an appropriate filter. Right-click **SMARTMAPS** and select **New > SmartMap**:



Select the appropriate filter and save everything:

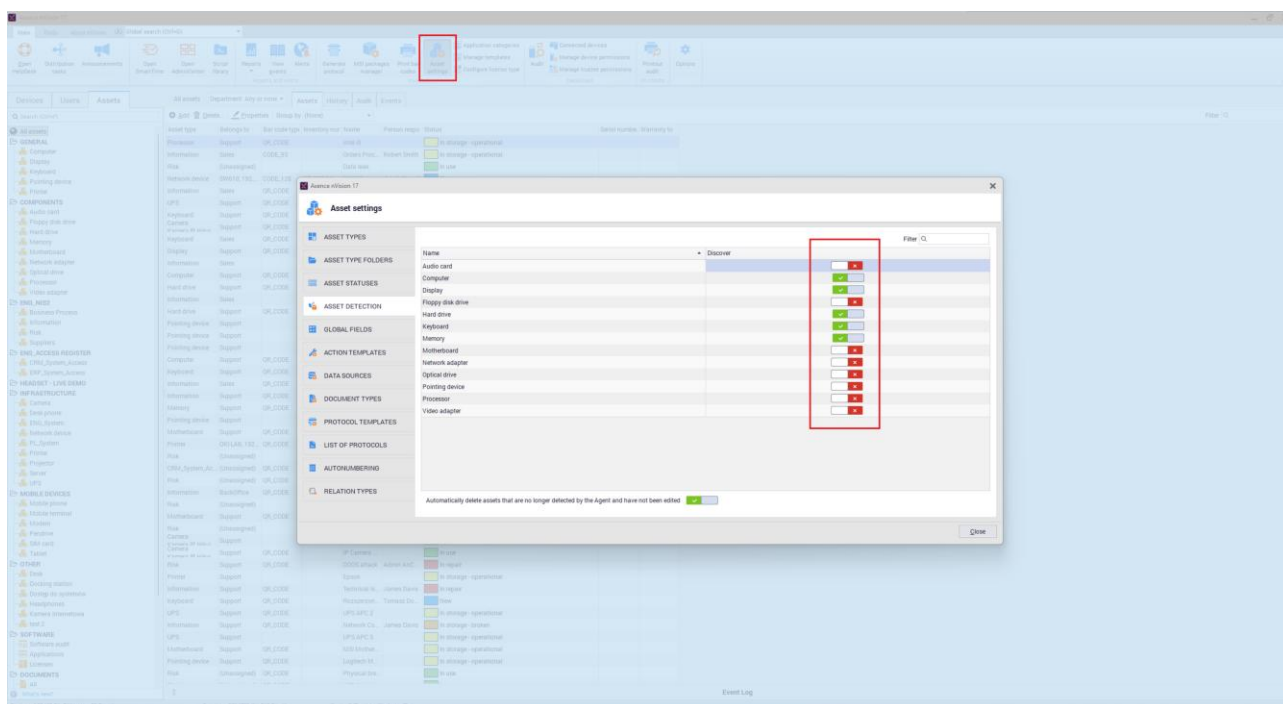


All the devices on this map are unidentified and not linked to a department, so they are potentially part of *shadow IT*.

### 1.1.5 Automatic asset creation from Agent

Installing the Agent enables the automatic detection of assets. This is important because you conduct the inventory and risk assessment at the asset level, not the device level. This is why all devices relevant to these processes must be mapped to assets.

You can automate this process for computers and servers with the Agent installed. In the **Asset settings** section, on the **Asset detection** tab, select the assets to be detected automatically. For the purposes of an ISO-oriented inventory, focus on the most relevant **Computer** type units and their key components.

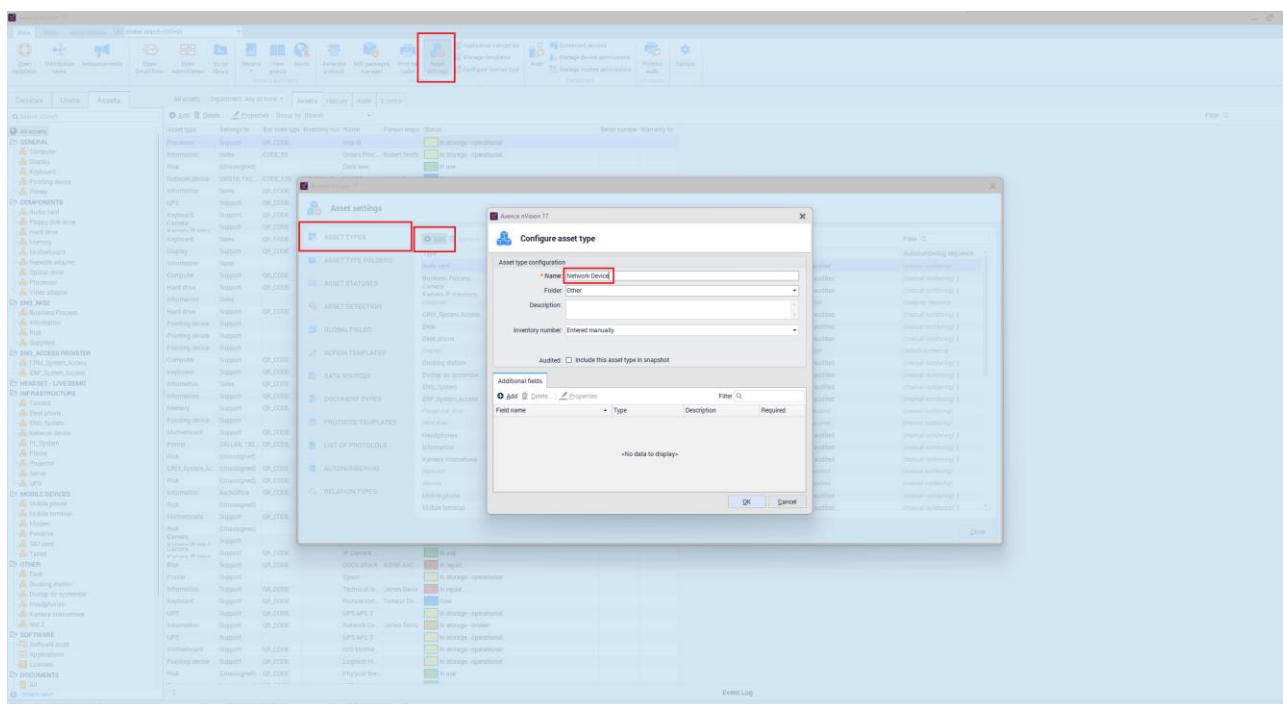


Regardless of how you introduce an asset into the system, it will be automatically assigned to a specific department based on information from the network maps and the device data.

Assets belong to the Inventory module, which provides key mechanisms for the identification, recording and control of assets. You can read more about assets and their settings [here](#).

### 1.1.6 Creating the *network device* asset type

A separate asset type for network devices will be useful for the following steps. These assets will be needed for the risk assessment to be performed later. You can create it using the **Add** option on the **Asset types** tab in the **Asset settings** section:



The type's inventory number should be generated **automatically** from the **default numbering** sequence. On the **Additional fields** tab, add the following optional fields: warranty (date), model (text), manufacturer (text), type (text). On the **Alert rules** tab, add a rule for the **warranty** field. You can learn more about asset types [here](#).

### 1.1.7 Identification of critical devices

**At this stage, you have already identified all computer-type assets that are active in your network.**

A very important part of the asset inventory process is marking critical devices. It is essential for carrying out a proper risk assessment and for implementing appropriate security controls, which in turn has an enormous impact on the operational continuity of devices and on the security and availability of data.

Classifying assets and identifying critical assets is also a requirement of NIS2 (Article 21(2)(k)), which mandates the implementation of measures to ensure operational continuity and protect systems of the highest operational importance.

This stage is most important when you have a very large number of devices without the Agent installed and cannot automate asset creation. In such a situation, it will be very important to analyze which devices operate in the network and their importance to service delivery and information security.

You can identify critical devices using a list of categories of functions critical to network and service security (the Act of 5 July 2018 on the National Cybersecurity System, Annex 3<sup>3</sup>).

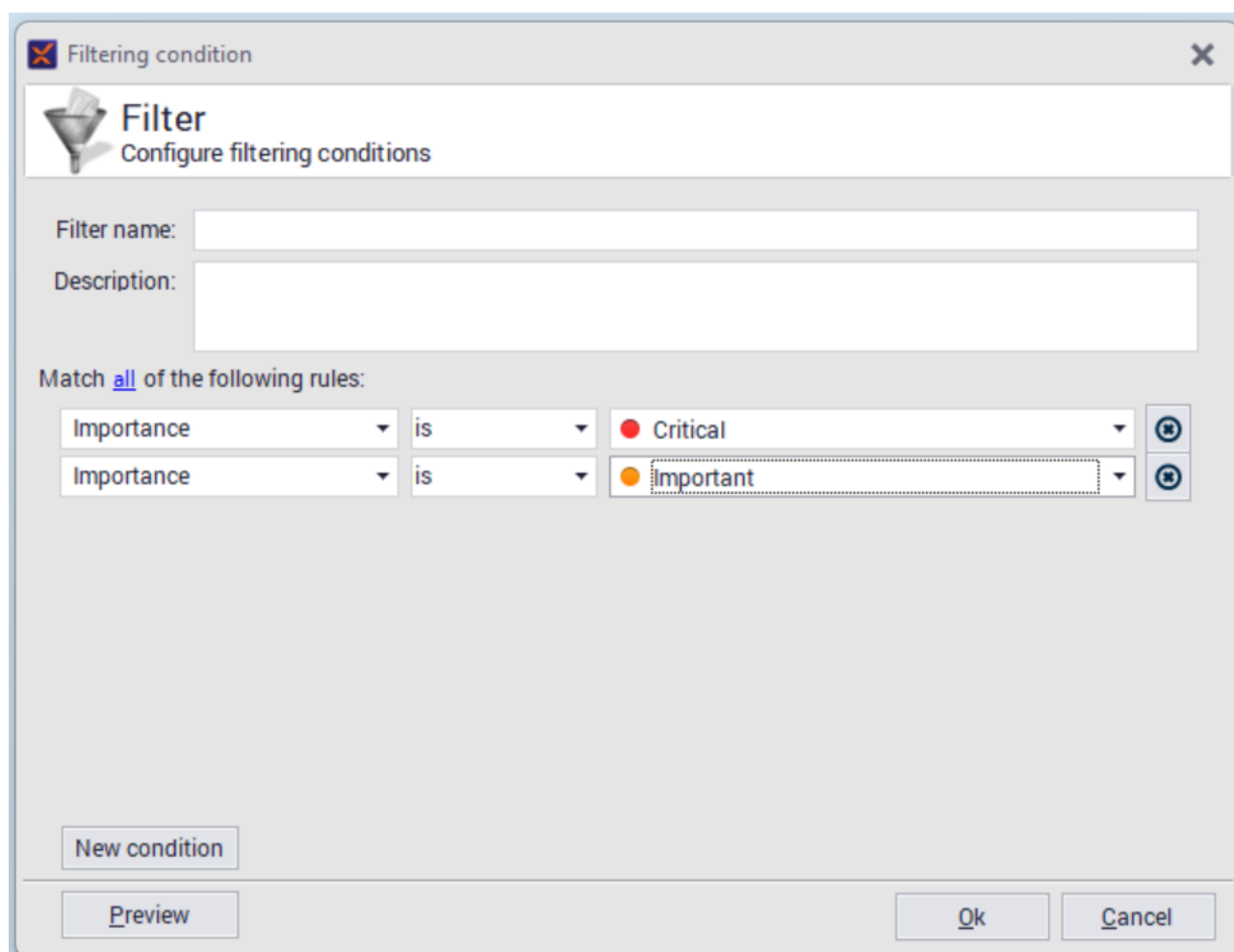
Mark the identified critical/important devices with the appropriate status in the device properties - double-click the selected device on the list and select the appropriate importance level from the list:

The screenshot shows the Axence nVision Agent interface for a device named LAB-SRV-ANV-EN. The interface includes a sidebar with navigation options like GENERAL, BASIC, LOGIN AUDIT, PERFORMANCE, HARDWARE, SOFTWARE, ASSETS, FILES, SNMP, WINDOWS, SECURITY, VMWARE, EVENTS, and PROFILE. The main area displays performance metrics (CPU, RAM, System disk) and basic information. In the 'Basic information' section, the 'Importance' dropdown menu is highlighted with a red box, showing options: Normal (selected), Critical, and Important. Other fields include Device name, Department, Visualization style, Type, and a checkbox for 'Enable monitoring'. Below this is a table for 'Addresses and interfaces'.

| Status | IP             | DNS Name              | Hardware (MAC) | Description           | Alias | NIC Vendor         | Speed  | Switch => Interface  | SNMP                     |
|--------|----------------|-----------------------|----------------|-----------------------|-------|--------------------|--------|----------------------|--------------------------|
| ●      | 192.168.60.212 | LAB-SRV-ANV-EN.anc... | 00155D9EB11A   | Microsoft Hyper-V ... |       | Microsoft Corpo... | 1 Gbps | SW609, 192.168.60... | <input type="checkbox"/> |
| ●      | 192.168.60.212 | LAB-SRV-ANV-EN        | 00155D9EB11A   | Microsoft Hyper-V ... |       | Microsoft Corpo... | 1 Gbps | SW609, 192.168.60... | <input type="checkbox"/> |

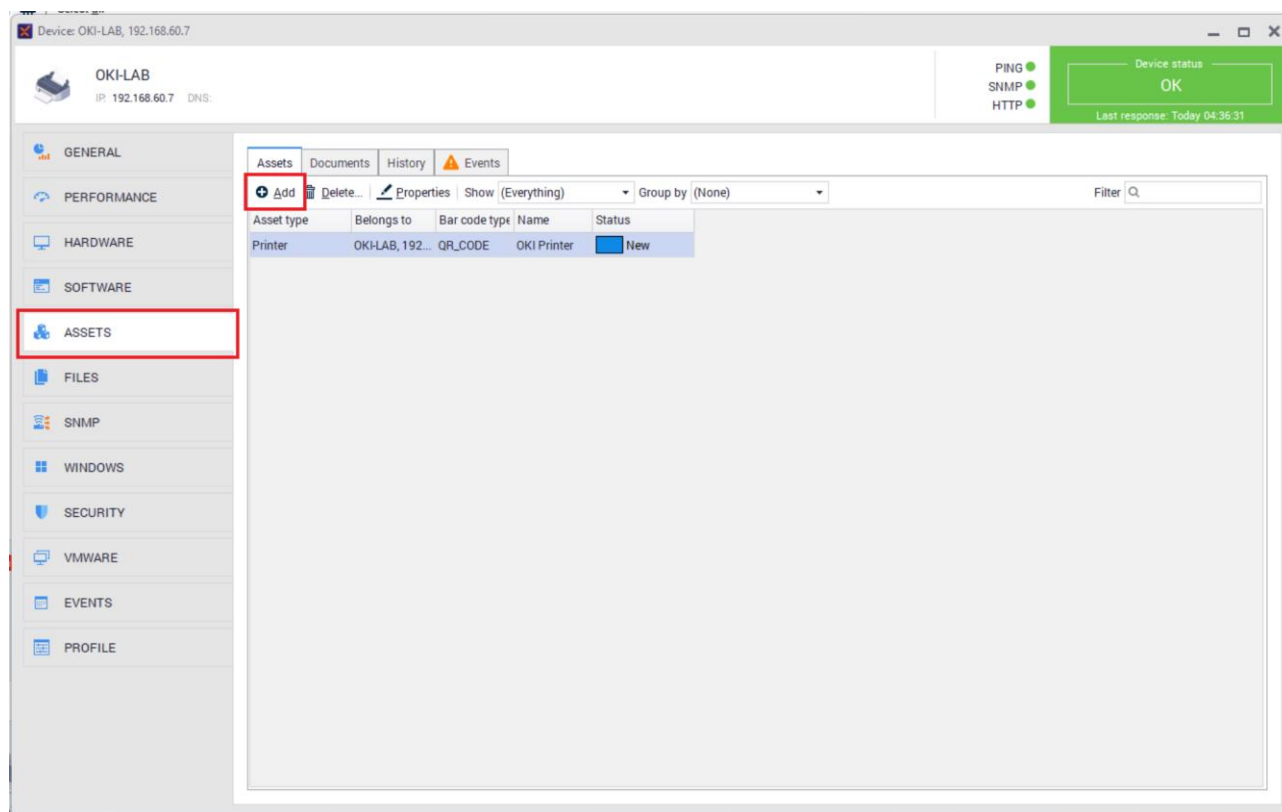
To quickly find important devices, create a SmartMap with the appropriate filter selected:

<sup>3</sup> Journal of Laws 2018 item 1560



The image shows a 'Filtering condition' dialog box. At the top, there's a title bar with a close button. Below it, a section titled 'Filter' with a funnel icon and the text 'Configure filtering conditions'. There are two text input fields: 'Filter name:' and 'Description:'. Below these, a label says 'Match all of the following rules:'. There are two rows of conditions. Each row has a dropdown menu for the field name (both set to 'Importance'), a dropdown for the operator (both set to 'is'), and a dropdown for the value. The first row's value is 'Critical' with a red circle icon. The second row's value is 'Important' with an orange circle icon. To the right of each value dropdown is a button with a plus sign. At the bottom left is a 'New condition' button. At the bottom right are 'Preview', 'Ok', and 'Cancel' buttons.

Then, for each of the devices filtered on the list, use the **Add** option:



From a risk assessment perspective, it is best to first inventory the critical and important devices, given their impact on the services provided by the organization. Mark the remaining devices with a low importance status. For these devices, you can analyze risk on a group basis, taking into account the various types of devices.

An example categorization might look like this:

|           | Description                                                                                                                                                                                                                                                                                                                                                          | Requirements                                                                                                                                                          | Examples                                                                                                                        |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| critical  | <ul style="list-style-type: none"> <li>their unavailability causes <b>downtime of key services or of the entire organization</b></li> <li>their failure has a <b>high impact on the confidentiality, integrity or availability of information</b></li> <li>they are <b>central points of the infrastructure (core)</b> or single points of failure (SPOF)</li> </ul> | <ul style="list-style-type: none"> <li>individual risk assessment</li> <li>strict control and monitoring</li> <li>assigned owner</li> </ul>                           | firewalls / UTM, edge routers, core switches, servers (AD, ERP, databases, backup, hypervisor), storage / SAN, WiFi controllers |
| important | <ul style="list-style-type: none"> <li>they support day-to-day operations</li> <li>their unavailability causes <b>local or limited disruptions</b></li> <li>they affect information security, but are <b>not critical to the continuity of the entire organization</b></li> </ul>                                                                                    | <ul style="list-style-type: none"> <li>risk assessment (individual or group)</li> <li>standard security controls</li> <li>access and configuration control</li> </ul> | access points (AP), managed switches (edge), network printers, IP cameras                                                       |
| low       | <ul style="list-style-type: none"> <li>they have a <b>minimal or negligible impact on operational continuity and information security</b></li> <li>they do not process data or have <b>limited access to systems</b></li> <li>their compromise does not cause a significant incident</li> </ul>                                                                      | <ul style="list-style-type: none"> <li>simplified, group risk assessment</li> <li>basic security controls (e.g. network segmentation)</li> </ul>                      | hubs, simple IoT devices (e.g. sensors, minor devices), other peripheral devices with an IP of low importance                   |

## 1.2 Inventory of software and web applications

The inventory of software and applications concerns assets that directly process, store or make information available. Without a record of these assets, there is a lack of control over the environment, gaps and risk.

If programs and applications are not inventoried, you cannot:

- properly manage access and responsibility (assigning an owner, securing entry points),
- define security requirements,
- identify vulnerabilities or define threat models,
- assess risk,
- carry out security tests,
- oversee changes and deployments.

Consequently, you cannot protect the data processed by the system or ensure the operational continuity of that system.

The inventory of applications will enable you to detect one of the greatest security threats, i.e. unauthorized software (shadow IT):

- private programs,
- illegal licenses,
- self-hosted web applications.

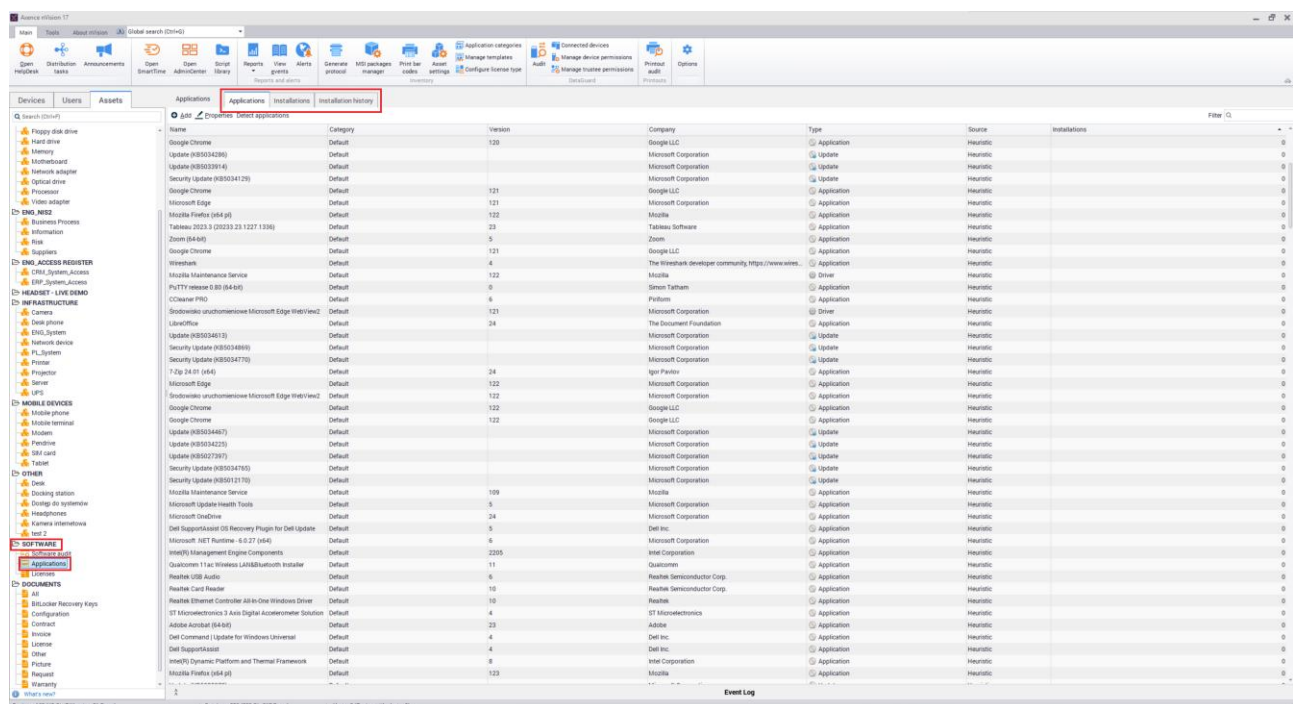
The absence of a software record creates the following risks:

- legal (pirated or non-compliant licenses),
- financial (penalties, over-licensing),
- operational (obsolete, unsecured versions).

## 1.2.1 The software scanning process

The nVision Agent runs as a permanent system service on the monitored device. It uses the Windows registry and the file system, which gives it full access to system information, installed programs and updates. It collects data on registry entries and files (including executable ones) stored on the device, as well as the detailed configuration of the system.

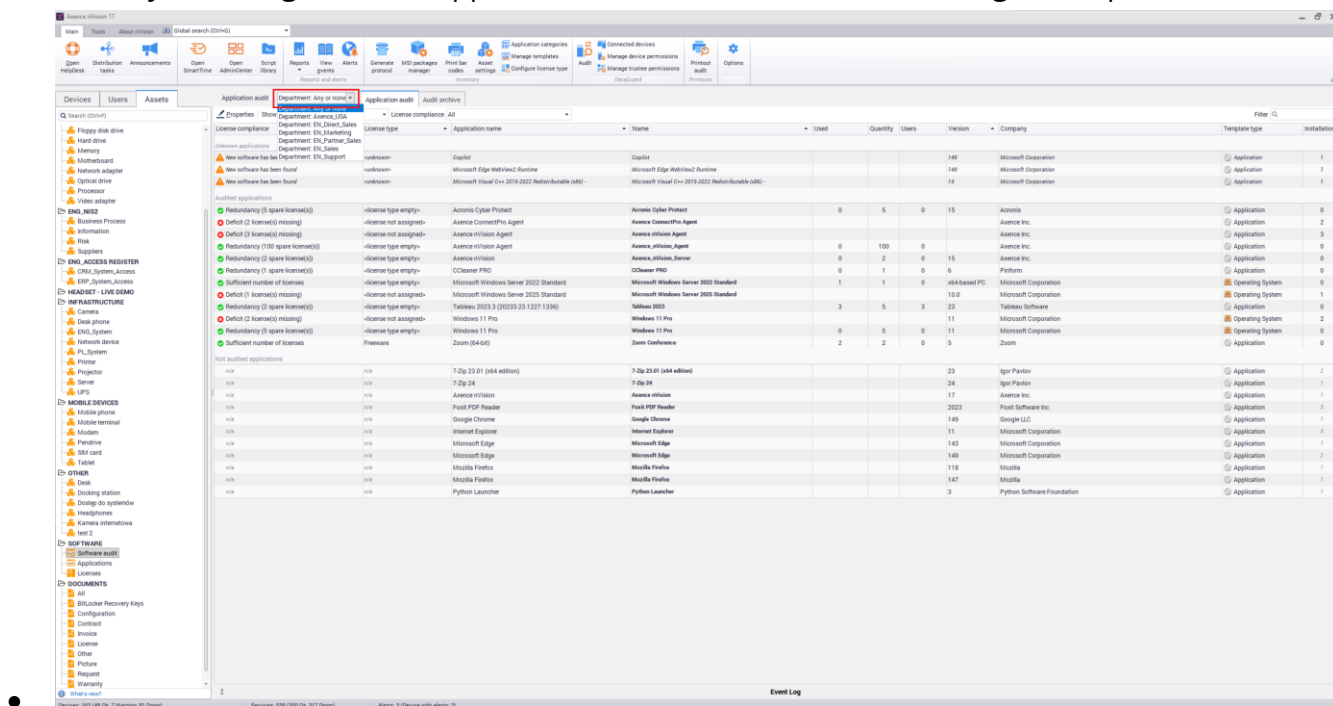
You can find the software information collected by the Agent on the **Assets** tab, in the **Software** section. Details on this section can be found here. The list of applications (and installations) themselves can be displayed in the **Applications** subsection:



| Name                                                    | Version | Company                                               | Type        | Source    | Installations |
|---------------------------------------------------------|---------|-------------------------------------------------------|-------------|-----------|---------------|
| Google Chrome                                           | 128     | Google LLC                                            | Application | Heuristic | 0             |
| Update (KB5034286)                                      | Default | Microsoft Corporation                                 | Update      | Heuristic | 0             |
| Update (KB5032914)                                      | Default | Microsoft Corporation                                 | Update      | Heuristic | 0             |
| Security Update (KB5034129)                             | Default | Microsoft Corporation                                 | Update      | Heuristic | 0             |
| Google Chrome                                           | 121     | Google LLC                                            | Application | Heuristic | 0             |
| Microsoft Edge                                          | 121     | Microsoft Corporation                                 | Application | Heuristic | 0             |
| Mozilla Firefox (64 bit)                                | 122     | Mozilla                                               | Application | Heuristic | 0             |
| Tableau 2023.3 (2023.2.1 127.1398)                      | 23      | Tableau Software                                      | Application | Heuristic | 0             |
| Zoom (64-bit)                                           | 5       | Zoom                                                  | Application | Heuristic | 0             |
| Google Chrome                                           | 121     | Google LLC                                            | Application | Heuristic | 0             |
| WinRAR                                                  | 4       | The WinRAR developer community https://www.winrar.com | Application | Heuristic | 0             |
| Microsoft Maintenance Service                           | 122     | Mozilla                                               | Driver      | Heuristic | 0             |
| PyTTY (version 0.8) (64-bit)                            | 8       | Simon Tatham                                          | Application | Heuristic | 0             |
| CCleaner PRO                                            | 6       | Piriform                                              | Application | Heuristic | 0             |
| Sonylink unauthenticated Microsoft Edge (Win)           | 121     | Microsoft Corporation                                 | Driver      | Heuristic | 0             |
| Update (KB5034611)                                      | 34      | The Document Foundation                               | Application | Heuristic | 0             |
| Security Update (KB5034888)                             | Default | Microsoft Corporation                                 | Update      | Heuristic | 0             |
| Security Update (KB5034770)                             | Default | Microsoft Corporation                                 | Update      | Heuristic | 0             |
| 7 Zip (64 bit) (64)                                     | 34      | Igor Pavlov                                           | Application | Heuristic | 0             |
| Microsoft Edge                                          | 122     | Microsoft Corporation                                 | Application | Heuristic | 0             |
| Sonylink unauthenticated Microsoft Edge (Win)           | 122     | Microsoft Corporation                                 | Application | Heuristic | 0             |
| Google Chrome                                           | 122     | Google LLC                                            | Application | Heuristic | 0             |
| Update (KB5034487)                                      | Default | Google LLC                                            | Update      | Heuristic | 0             |
| Update (KB5034423)                                      | Default | Microsoft Corporation                                 | Update      | Heuristic | 0             |
| Update (KB5027297)                                      | Default | Microsoft Corporation                                 | Update      | Heuristic | 0             |
| Security Update (KB5034160)                             | Default | Microsoft Corporation                                 | Update      | Heuristic | 0             |
| Security Update (KB5031270)                             | Default | Microsoft Corporation                                 | Update      | Heuristic | 0             |
| Microsoft Maintenance Service                           | 109     | Mozilla                                               | Application | Heuristic | 0             |
| Microsoft Update Health Tools                           | 5       | Microsoft Corporation                                 | Application | Heuristic | 0             |
| Microsoft OneDrive                                      | 34      | Microsoft Corporation                                 | Application | Heuristic | 0             |
| Del SupportAssistant (5 Recovery Plugin for Dell Update | 5       | Dell Inc.                                             | Application | Heuristic | 0             |
| Microsoft .NET Runtime - 6.0.27 (x64)                   | 6       | Microsoft Corporation                                 | Application | Heuristic | 0             |
| Intel(R) Management Engine Components                   | 2205    | Intel Corporation                                     | Application | Heuristic | 0             |
| Qualcomm 11ac Wireless LAN/Bluetooth installer          | 11      | Qualcomm                                              | Application | Heuristic | 0             |
| Realtek USB Audio                                       | 4       | Realtek Semiconductor Corp.                           | Application | Heuristic | 0             |
| Realtek Card Reader                                     | 10      | Realtek Semiconductor Corp.                           | Application | Heuristic | 0             |
| Realtek Ethernet Controller All-in-One Windows Driver   | 10      | Realtek                                               | Application | Heuristic | 0             |
| ST Microelectronics 3 Axis Digital Accelerometer        | 4       | ST Microelectronics                                   | Application | Heuristic | 0             |
| AdiTech (64-bit)                                        | 23      | AdiTech                                               | Application | Heuristic | 0             |
| Dell Command   Update for Windows Universal             | 4       | Dell Inc.                                             | Application | Heuristic | 0             |
| Del SupportAssistant                                    | 4       | Dell Inc.                                             | Application | Heuristic | 0             |
| Intel(R) Dynamic Platform and Thermal Framework         | 8       | Intel Corporation                                     | Application | Heuristic | 0             |
| Mozilla Firefox (64 bit)                                | 123     | Mozilla                                               | Application | Heuristic | 0             |

However, it will be simpler to use the **Software audit** subsection, which:

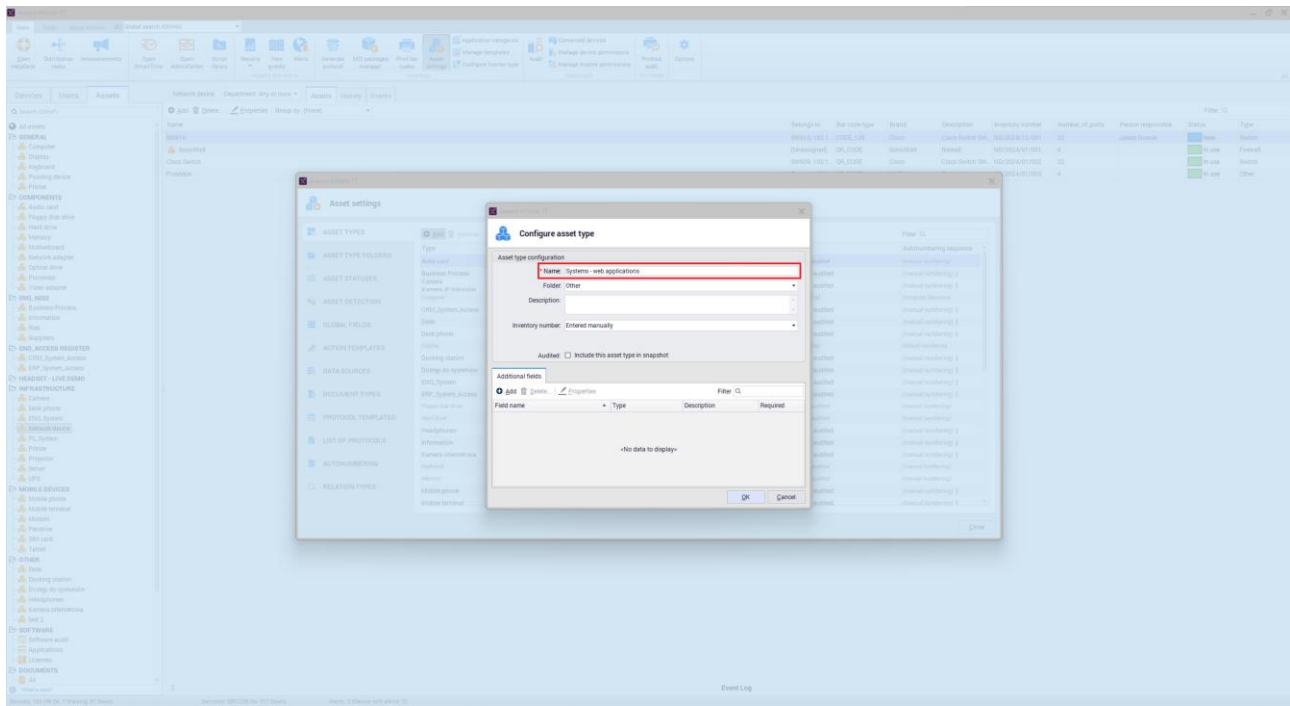
- contains a list of applications installed on devices with the Agent,
- divides applications into **unknown**, **audited** and **non-audited** (set in the installation properties, in the **Applications** subsection),
- allows you to single out the applications installed on the devices in a given department.



The inventory of locally installed assets is important because the strategy for updating and patching vulnerabilities can be complicated in their case. In contrast, for web applications, responsibility for updates lies with the supplier.

## 1.2.2 Inventorying additional systems

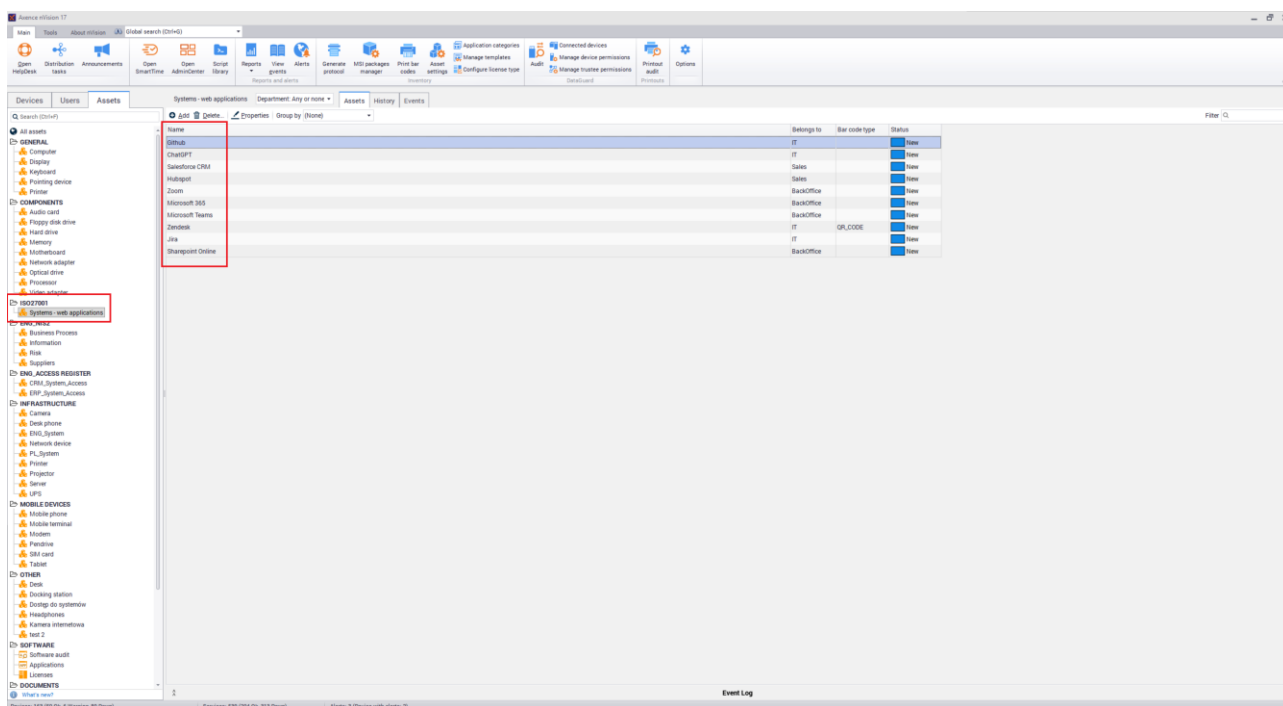
The Agent can detect software installed on a computer. However, it will not provide data on web applications or cloud services. You must enter such applications into nVision manually because, even though they are undetectable, they should be identified and inventoried. Adding a new asset type, **Systems – web applications**, will help you with this:



This asset type is most often inventoried by IT department personnel, who are able to identify the largest number of systems used in the organization. Business owners of assets can also handle this process. They can be engaged by means of announcements sent out (for more information, see section [2.2.2](#)).

### 1.2.3 Assigning systems to departments

Once all the systems are in the nVision assets, assign each to a specific organizational unit (i.e. to a specific department). This will make it easier for you to later assign business owners by means of the appropriate relation. Most often, the business owner of the systems of a given department is the supervisor of that department (or a person designated by them). To assign such a person to all the systems of a given department, filter the systems by the selected department (e.g. **Marketing**) and add the appropriate relation.



Of course, some systems are used across the entire organization, but there is one business owner (the person managing a given system who defines the system's membership in a unit. Assigning a business owner to assets will be discussed in **section 2.1**.

Collecting assets in nVision minimizes the risk that the inventory will fail to account for something that is actually in use.

## 1.3 Primary and supporting assets

In the context of ISO 27001 and risk assessment, it will be useful to divide assets into:

- **primary (information)** assets – information and business processes,
- **supporting** assets – everything that enables them to function.

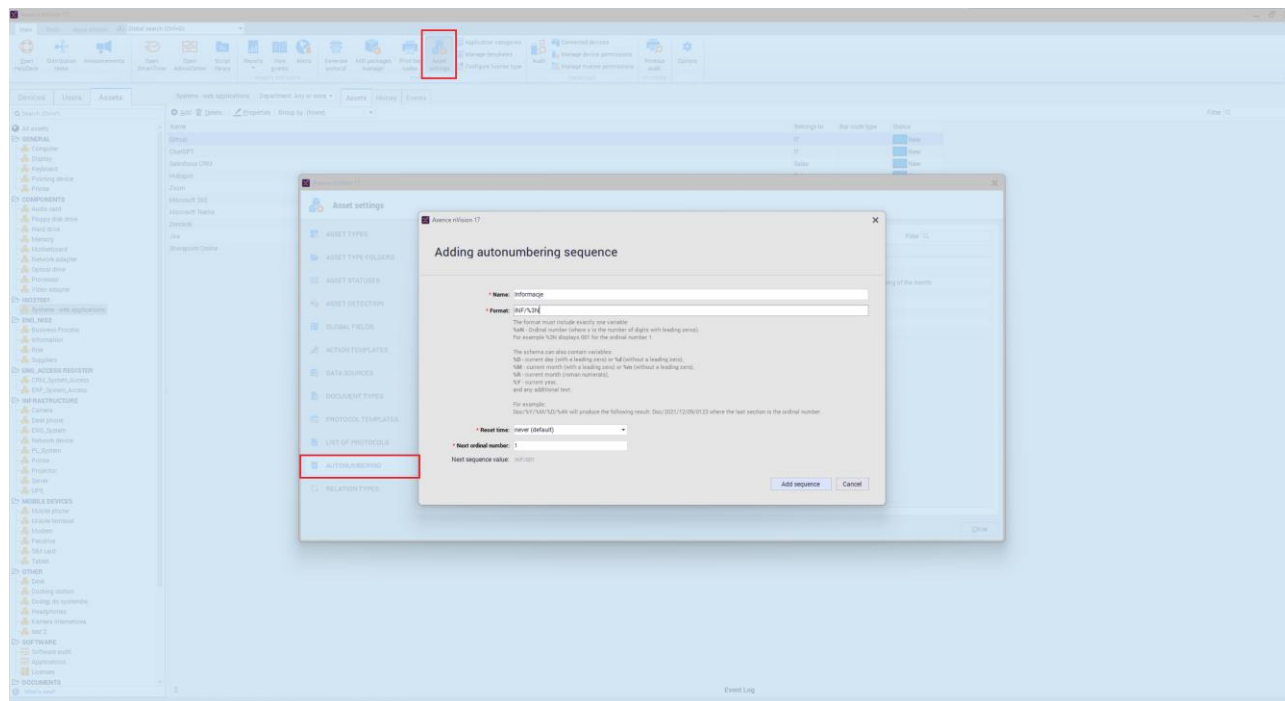
The assets inventoried so far are classified as supporting assets, which process, store, transmit or otherwise support information assets.

You need to supplement the asset register with information assets and then link them to the appropriate supporting assets (individual or groups) through relations.

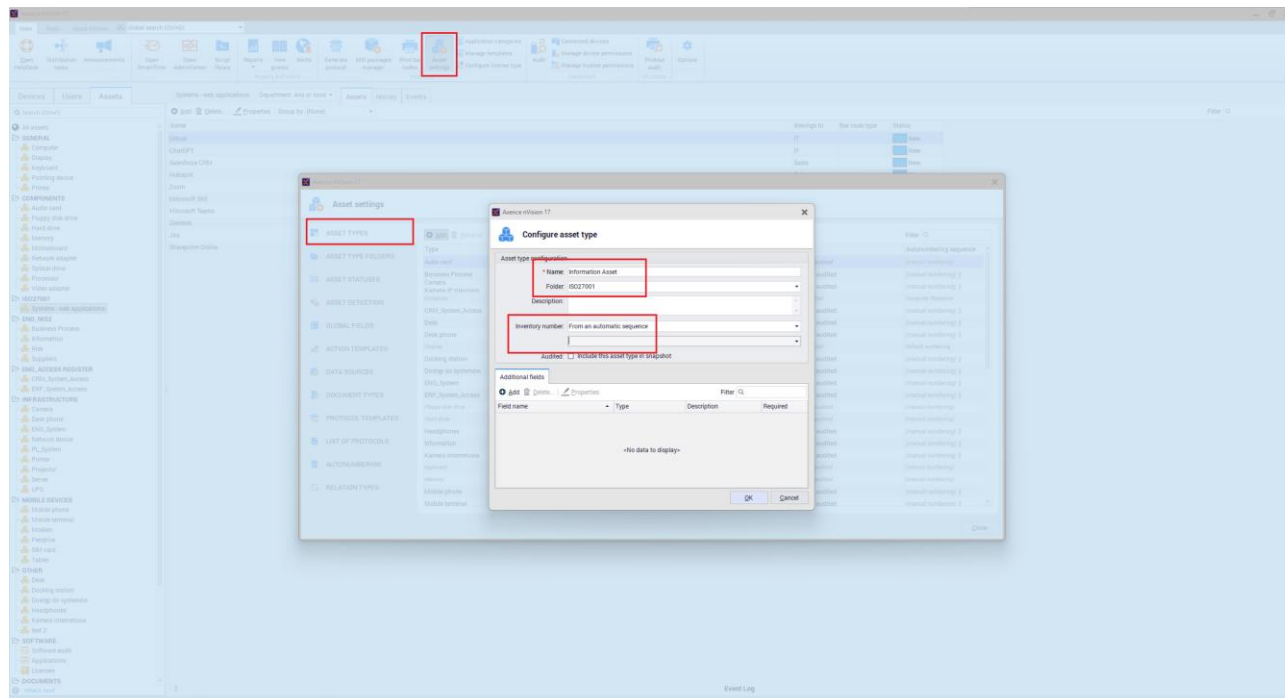
### 1.3.1 Introducing information assets

Add a new asset type: **information assets**. You can do this in the **Asset settings** section.

Start by creating an asset autonumbering sequence, which will simplify assigning the inventory numbers. Go to the **Autonumbering** tab and add a new sequence:



Then, on the **Asset types** tab, add the **Information assets** type with an inventory number created automatically from the **Information** sequence:



To learn more about autonumbering, see the [documentation](#).

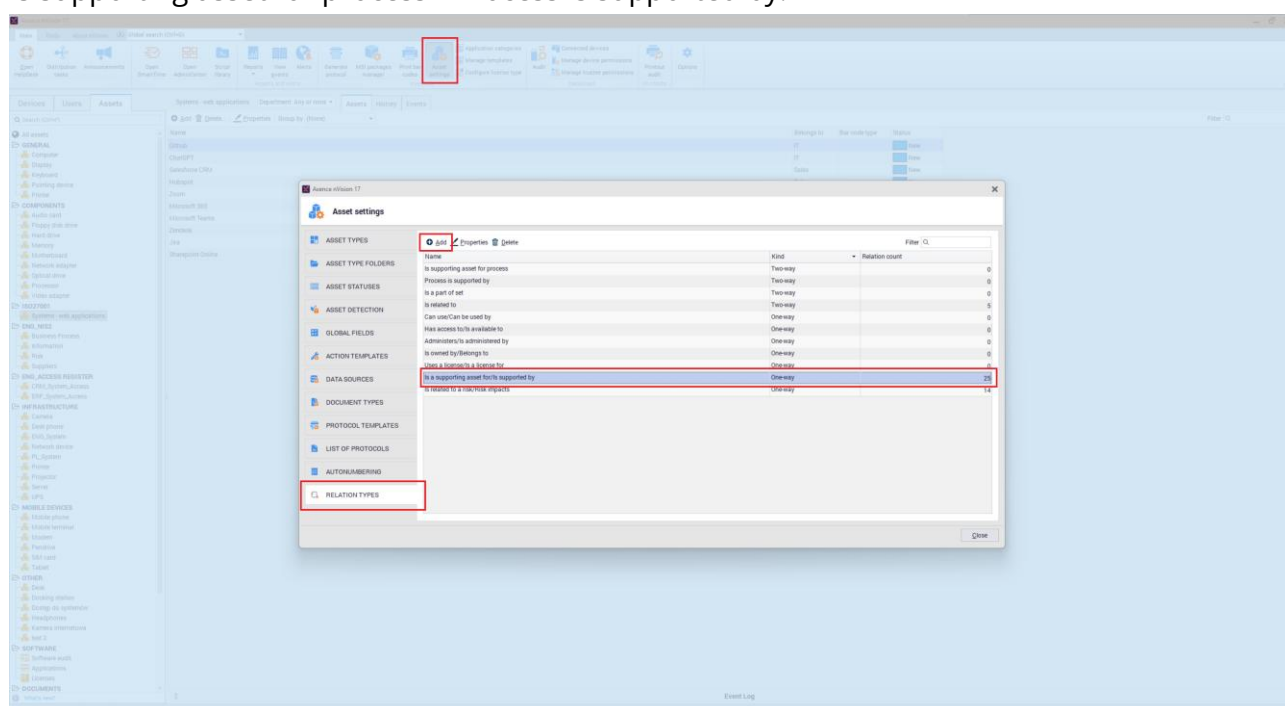
Create a list of information assets in the form of a CSV file and import it into nVision. You can find an example of information assets in a CSV file on the **Legal regulations** page, accessible

from the main navigation ribbon in nVision. During the import, follow the instructions in the [documentation](#).

### 1.3.2 Adding a relation

To link information assets with supporting ones, you need a new one-directional relation type: **Is a supporting asset for / Is supported by**. You can differentiate between supporting information and supporting a process by creating the following, in **Asset settings** on the **Relation types** tab:

- Is supporting asset for information / Information is supported by,
- Is supporting asset for process / Process is supported by.



### 1.3.3 Assigning supporting assets

Assign each of the imported information assets to selected supporting assets (either to individual assets or to the whole groups of assets).

For example, among the information assets, you can find **Product presentations**:

| Name                              | Settings   | Bar code type | Person responsible | Status     | Accessibility | Confidentiality | Integrity | Information    |
|-----------------------------------|------------|---------------|--------------------|------------|---------------|-----------------|-----------|----------------|
| Sales Procedures                  | Sales      | QR_CODE       | Robert Smith       | in storage | 1             | 2               | 1         | Internal info. |
| Orders Procedures                 | Sales      | CODE_93       | Robert Smith       | in storage | 1             | 2               | 1         | Internal info. |
| Suppliers Information             | Sales      |               | Mary Smith         | in storage | 1             | 2               | 1         | Confidential   |
| Employees Contracts               | Sales      |               | Mary Smith         | in storage | 1             | 2               | 1         | Confidential   |
| Customer Agreements               | Sales      | QR_CODE       | Mary Smith         | in storage | 1             | 2               | 1         | Confidential   |
| Source Code                       | IT         | QR_CODE       | James Davis        | in repair  | 4             | 4               | 4         | Critical info. |
| Marketing Strategy                | BackOffice | QR_CODE       | Mary Smith         | in storage | 1             | 2               | 1         | Confidential   |
| Technical Issues Information      | IT         | QR_CODE       | James Davis        | in repair  | 3             | 4               | 3         | Critical info. |
| Network Configuration Information | IT         | QR_CODE       | James Davis        | in storage | 1             | 2               | 1         | Confidential   |
| Brochure in PDF                   | BackOffice | QR_CODE       | Mary Smith         | in use     | 1             | 1               | 1         | Regular info.  |
| Customer information              | Sales      | QR_CODE       | Robert Smith       | in storage | 1             | 2               | 1         | Confidential   |
| Product information               | Sales      | QR_CODE       | Robert Smith       | in storage | 1             | 2               | 1         | Confidential   |
| Product presentation              | BackOffice | QR_CODE       | Mary Smith         | in use     | 1             | 1               | 1         | Regular info.  |

As information (as opposed to a process), they are supported by the **Laptop 1** asset:

| RELATIONS WITH OTHER ASSETS, USERS, LICENSES AND GROUPS |
|---------------------------------------------------------|
| is supported by                                         |
| 2nd computer (James)                                    |
| PALAB-CL02                                              |
| HP computer                                             |
| PALAB-CL01                                              |
| PALAB-CL03                                              |
| 2nd computer                                            |
| 3rd computer                                            |
| HP computer 2                                           |
| LAB-DRIVEN                                              |
| LAB-CL04                                                |
| DESKTOP4HECCS                                           |

## 1.4 Users

In the inventory process, you must determine:

- the business owners of the individual assets,

- the end users of the systems and assets,
- the technical administrators.

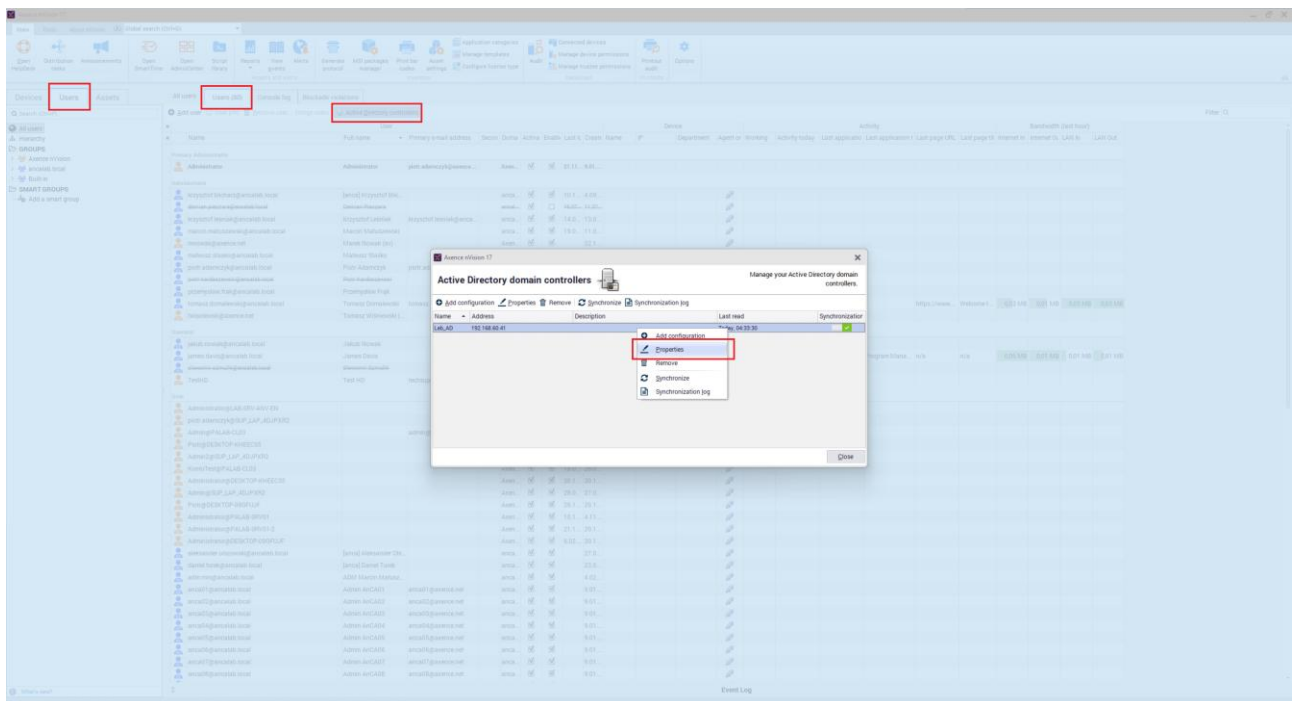
Later stages include:

- restricting access to assets (the elimination of shadow access – accidental, historical or unnecessary access),
- recording user actions (used in the event of incidents),
- managing the user lifecycle (onboarding / offboarding).

This is why it is worth ensuring that users are entered into the system as early as the inventory stage.

If the organization does not have a domain, it can use local accounts. Local system accounts are created on each computer and detected by the installed Agent, which sends the data to nVision. nVision automatically creates accounts for new users based on this data. These accounts contain essential information – the user's login appears as the name, and everything else must be filled in manually.

If you have an organizational domain, it is best to use domain accounts and direct synchronization of users between Active Directory and the nVision database. You can do this using the [ **Active Directory controllers** ] button and by adding a new configuration based on template data:



In the configuration, you can indicate the specific organizational units (OUs) to be synchronized. You can read more about this [here](#).

## 1.5 Grouping assets

You can describe every device as an asset of a specific type. Assets of the same type can be further divided into smaller groups based on various criteria – functional, organizational unit or user criteria.

You can link devices to departments, thereby creating a representation of the actual structure of the monitored group of devices in nVision. However, the division into departments is based solely on the organizational unit criteria, whereas, in practice, there may be more possible divisions, and they may require taking two or more criteria into account simultaneously.

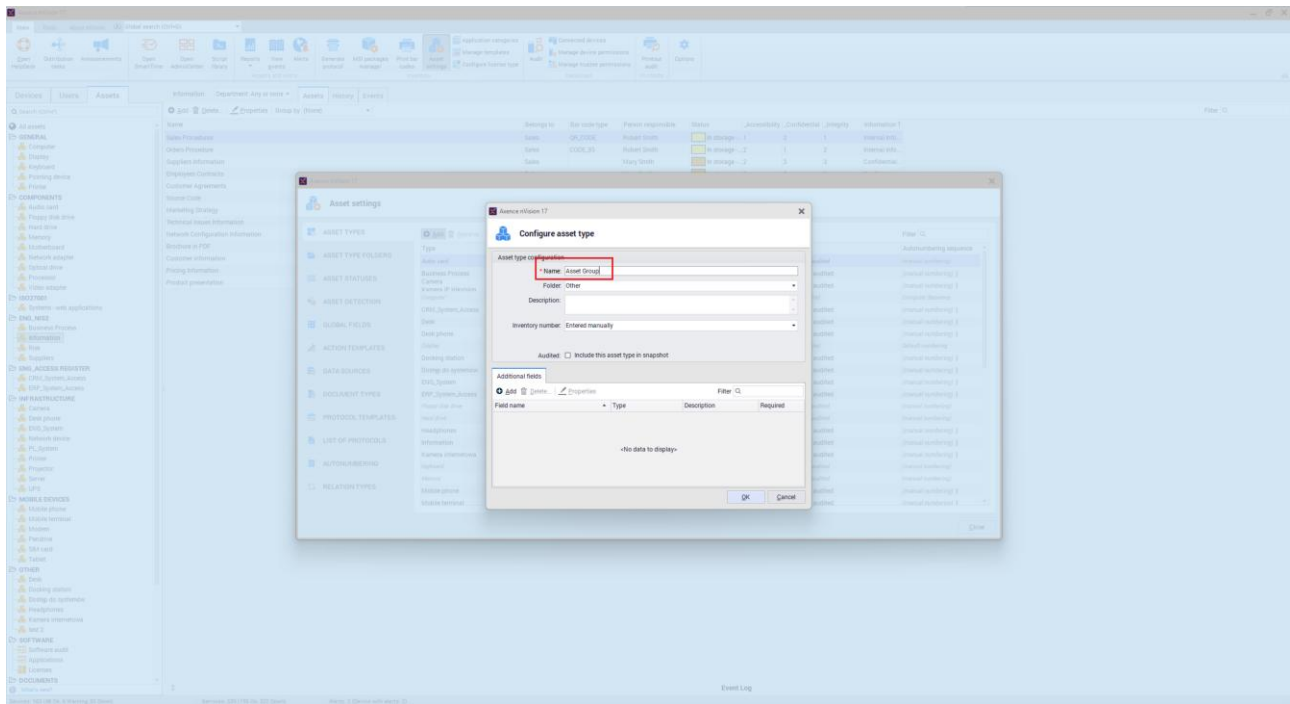
Such grouping will allow you to:

- arrange assets logically,
- identify critical assets more quickly,
- determine action priorities more easily,
- assign business owners.

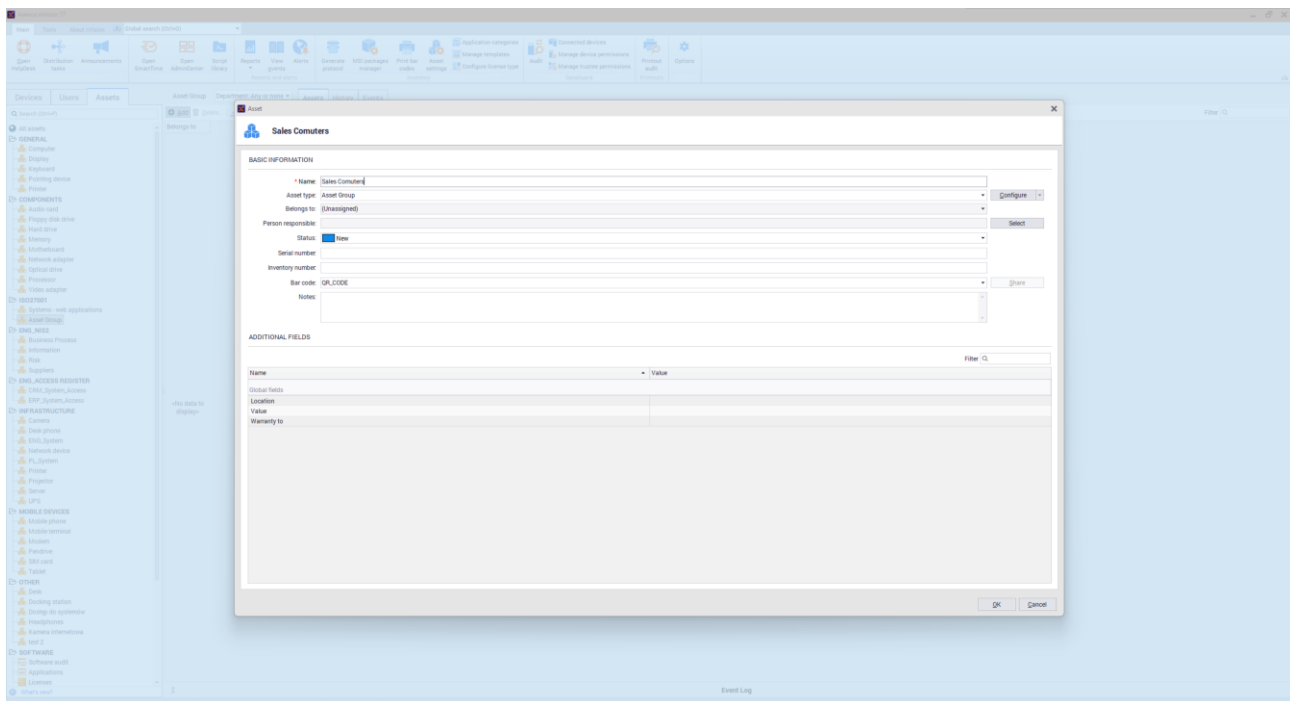
Above all, it will make it easy to assign threats and security controls. For many devices, the list of threats and security controls will be the same due to their specific nature or their assignment to a department. Groups simplify operating on these lists, saving you work.

### 1.5.1 Creating the *Device Group* type

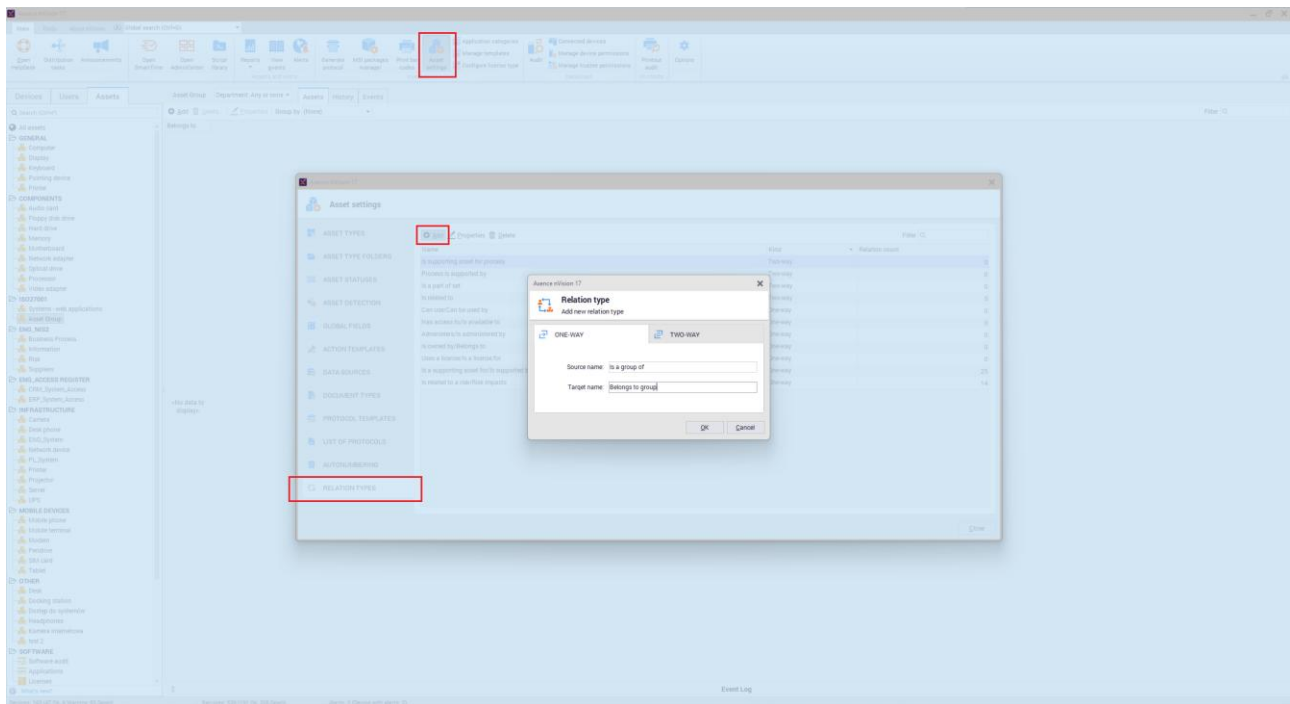
To group assets, you need a new asset type. You can configure it very simply. Just add a new type with an appropriate name and manually assign an inventory number:



Once you have created this asset type, you can add the necessary groups (e.g. *Sales computers* or *Sales network devices*):

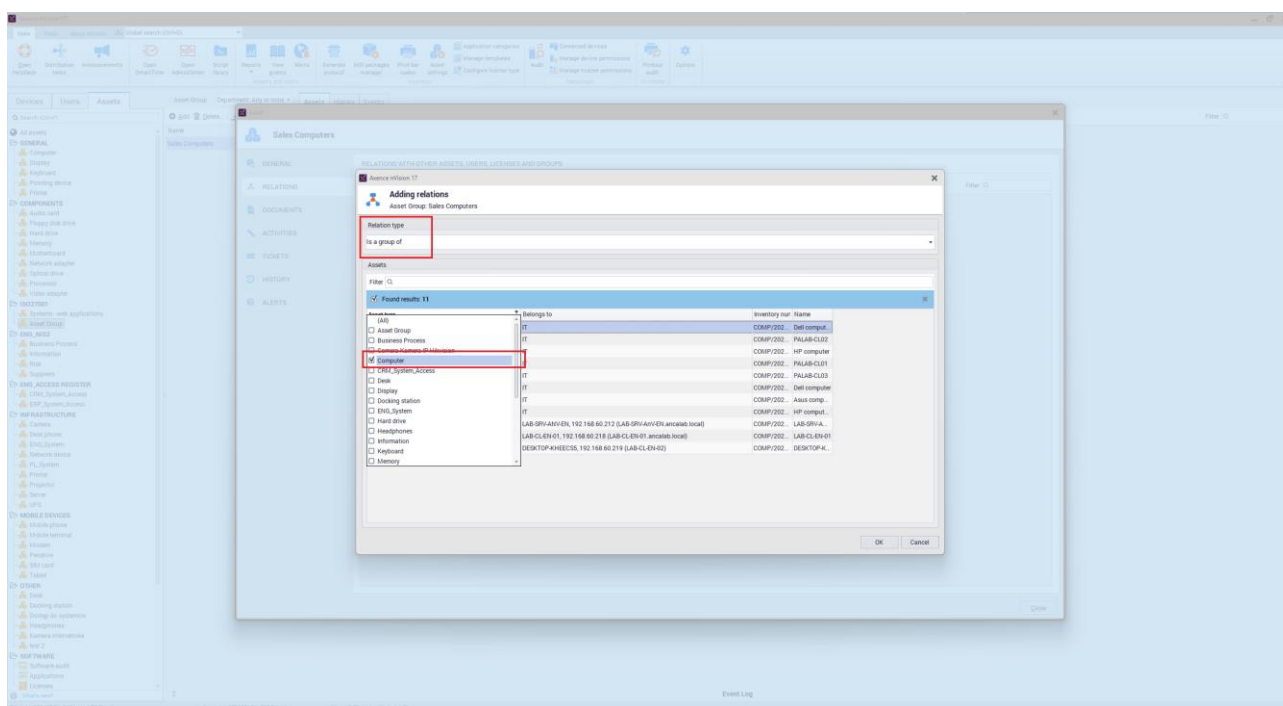
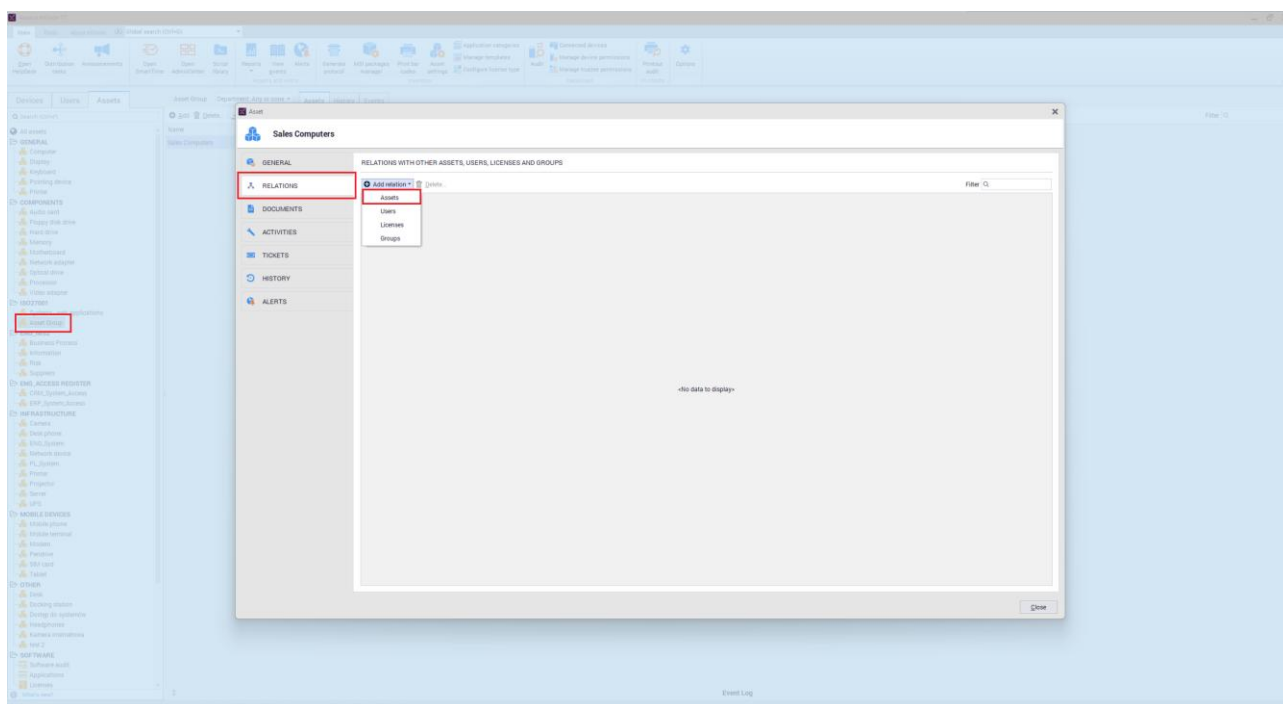


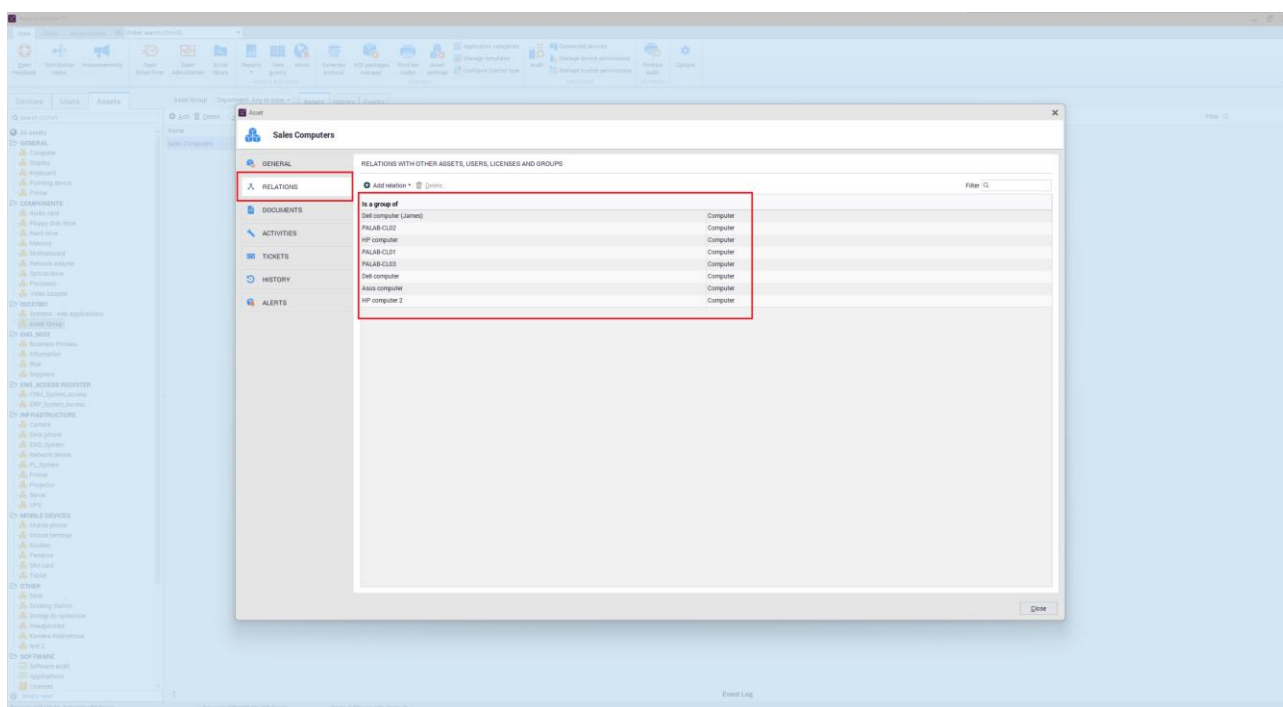
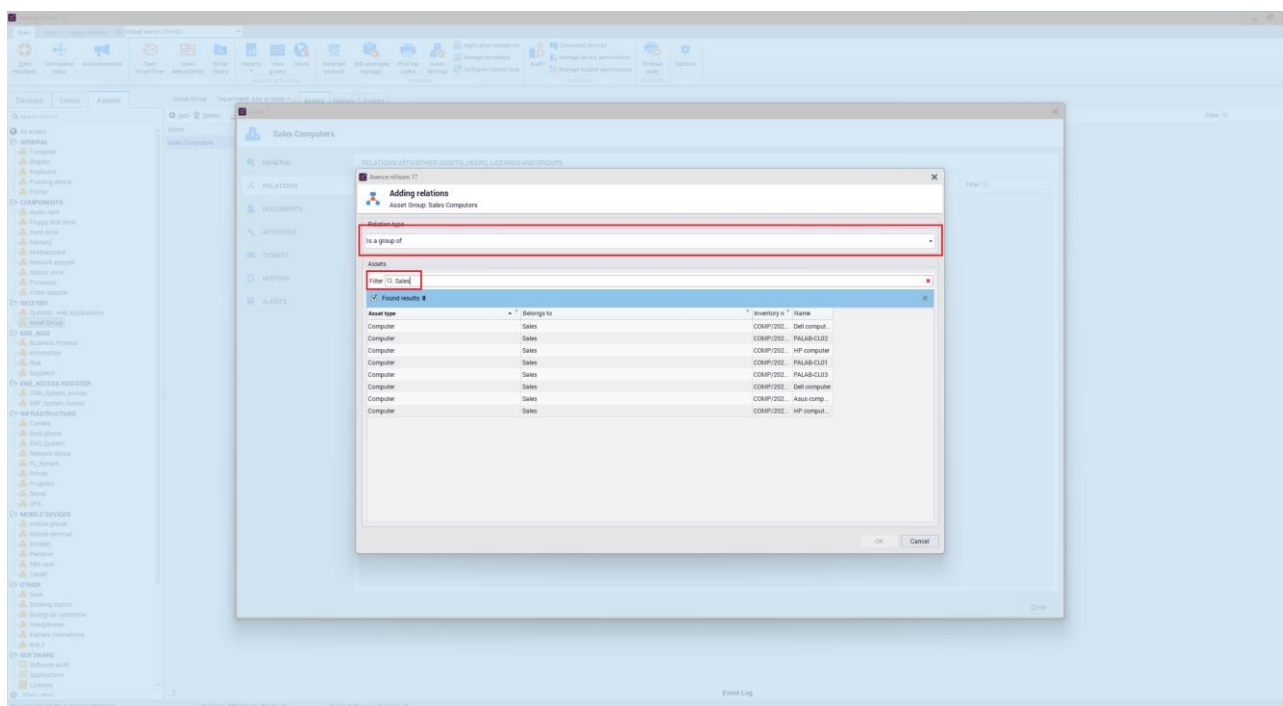
In each group, configure a relation with the **assets**. You will need a new **one-directional relation type**, which you can add in the **Asset settings** section – the **Is a group for / Belongs to group**.



Assign a one-directional relation to a single asset, linking it with another one. The same relation, but in the opposite direction, is automatically created on that assigned asset.

You can therefore use the type you created and set the relation in the group to **Is a group for**. You can select the assets for the relation using a filter (you can search for an asset either by asset type or by the name of the department to which the assets are assigned).



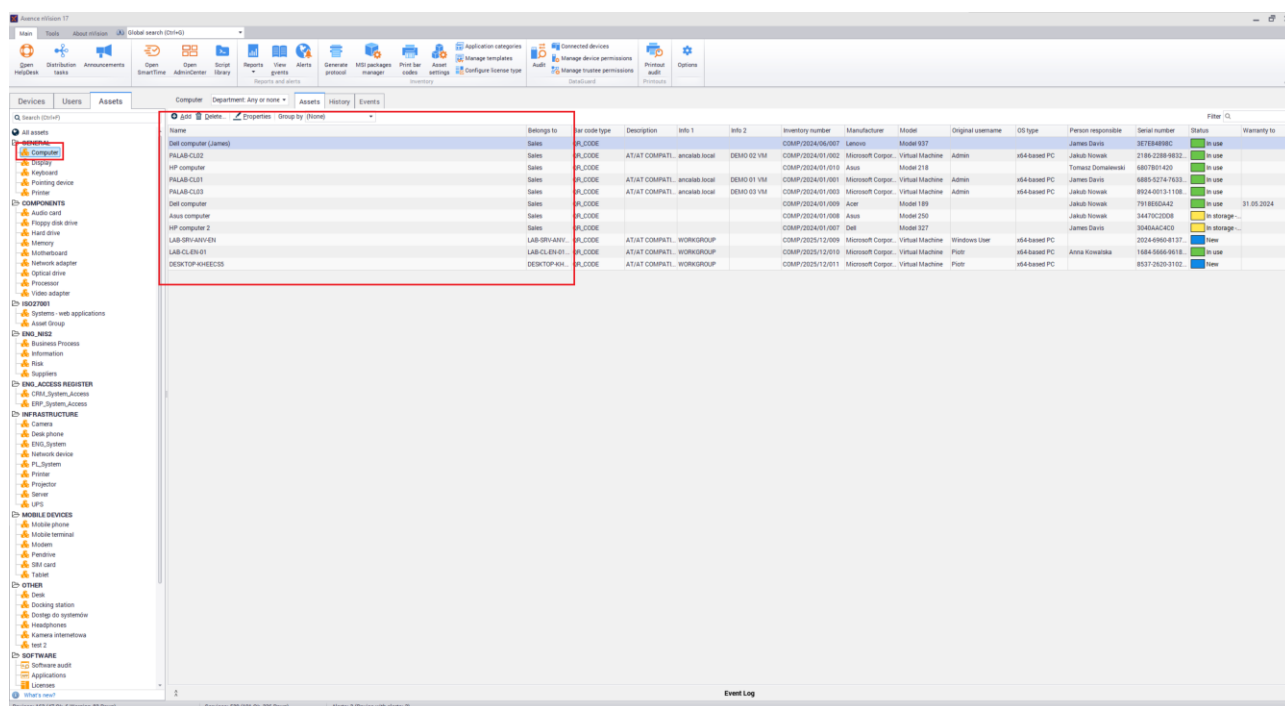


Once you confirm the relation, it will automatically appear in the properties of each of the assets added here – every computer will have the **Is a group of/Belongs to group** relation.

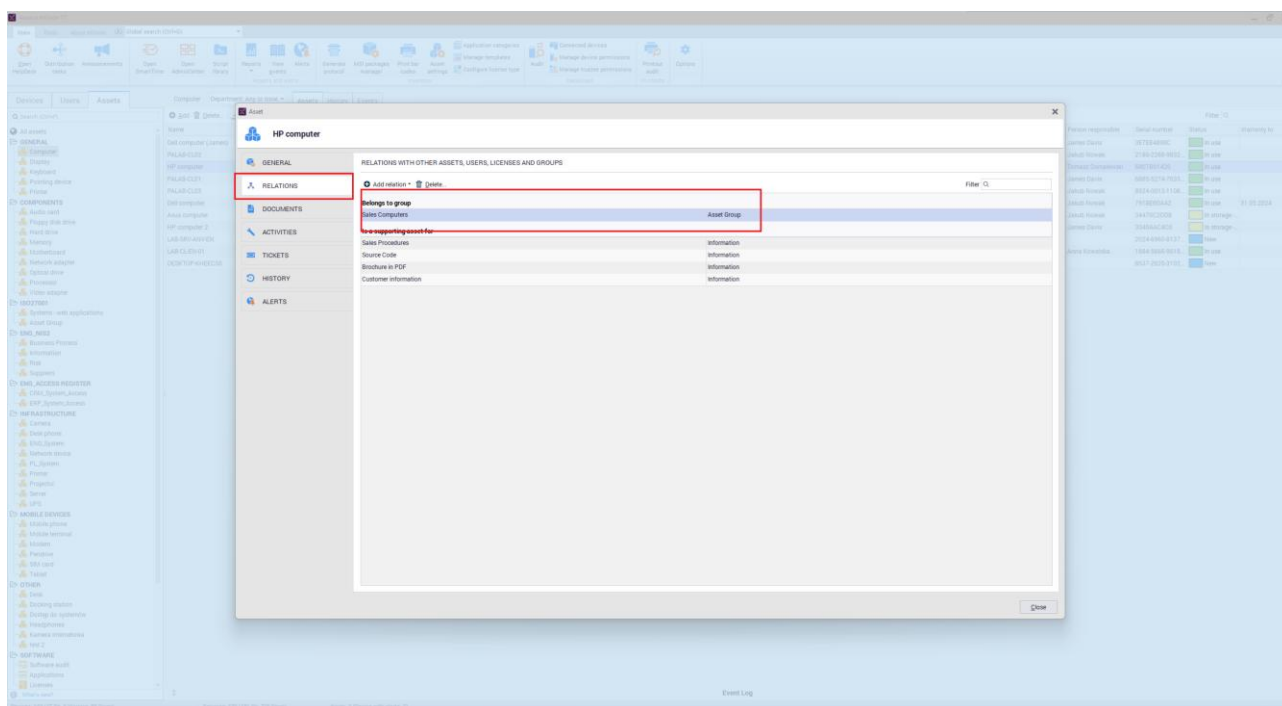
This is an exceptionally useful solution, especially for a large number of devices. With it, you can easily assign threats and security controls to a whole group instead of doing so individually for each device.

## 1.5.2 Adding devices of a given type to a group

Now you can add the devices represented by assets to the group you created. In this example, add the assets with the **Computer** asset type that belong to the sales department to the **Sales computers** group. The **Is a group of/Belongs to group** relation should already be set in the properties of each asset of this type and for this department. The exception is assets added after the relation was defined in the group's properties – you can update the group from their side as well, by setting the relation:



| Name                   | Serial number | Inventory number              | Manufacturer | Model            | Original username | OS type         | Person responsible | Serial number  | Status        | Warranty to |
|------------------------|---------------|-------------------------------|--------------|------------------|-------------------|-----------------|--------------------|----------------|---------------|-------------|
| Sales computer (Lemex) | PL-0000       | COMP/2024/01/001              | Lemex        | Model 107        | Admin             | x64-based PC    | James Davis        | 3678494962     | In use        |             |
| PALAB-CL02             | PL-0000       | AT/AT COMPATL_ assuacal local | DEKMO 02 198 | COMP/2024/01/002 | Microsoft Corp... | Virtual Machine | James Davis        | 2184-2289-9832 | In use        |             |
| vPC computer           | PL-0000       | COMP/2024/01/010              | Asus         | Model 218        | Admin             | x64-based PC    | Tomasz Domanski    | 6807801420     | In use        |             |
| PALAB-CL01             | PL-0000       | AT/AT COMPATL_ assuacal local | DEKMO 01 198 | COMP/2024/01/001 | Microsoft Corp... | Virtual Machine | James Davis        | 6885-0274-7833 | In use        |             |
| Sales computer         | PL-0000       | AT/AT COMPATL_ assuacal local | DEKMO 03 198 | COMP/2024/01/003 | Microsoft Corp... | Virtual Machine | James Davis        | 8024-0013-1108 | In use        |             |
| Asus computer          | PL-0000       | COMP/2024/01/008              | Asus         | Model 199        | Admin             | x64-based PC    | James Davis        | 791-8802342    | In use        | 31.05.2024  |
| HP computer 2          | PL-0000       | COMP/2024/01/007              | Dell         | Model 327        | Admin             | x64-based PC    | James Davis        | 34470C2008     | In storage... |             |
| LAB-SH-ADV-EN          | PL-0000       | AT/AT COMPATL_ WORKGROUP      | DEKMO 01 198 | COMP/2025/12/009 | Microsoft Corp... | Virtual Machine | James Davis        | 35404AC4C0     | In storage... |             |
| LAB-CL-EN-01           | PL-0000       | AT/AT COMPATL_ WORKGROUP      | DEKMO 01 198 | COMP/2025/12/010 | Microsoft Corp... | Virtual Machine | James Davis        | 2024-0803-0137 | In use        |             |
| DESKTOP-KH0ECIS        | PL-0000       | AT/AT COMPATL_ WORKGROUP      | DEKMO 01 198 | COMP/2025/12/011 | Microsoft Corp... | Virtual Machine | James Davis        | 1884-0566-9618 | In use        |             |



## 1.6 Optimizing the inventory process

The inventory is a complex process that binds assets and users into a structure, and it is also a continuous process. However, you can streamline this process by using the mechanisms offered by nVision.

### 1.6.1 Exporting data on user activity

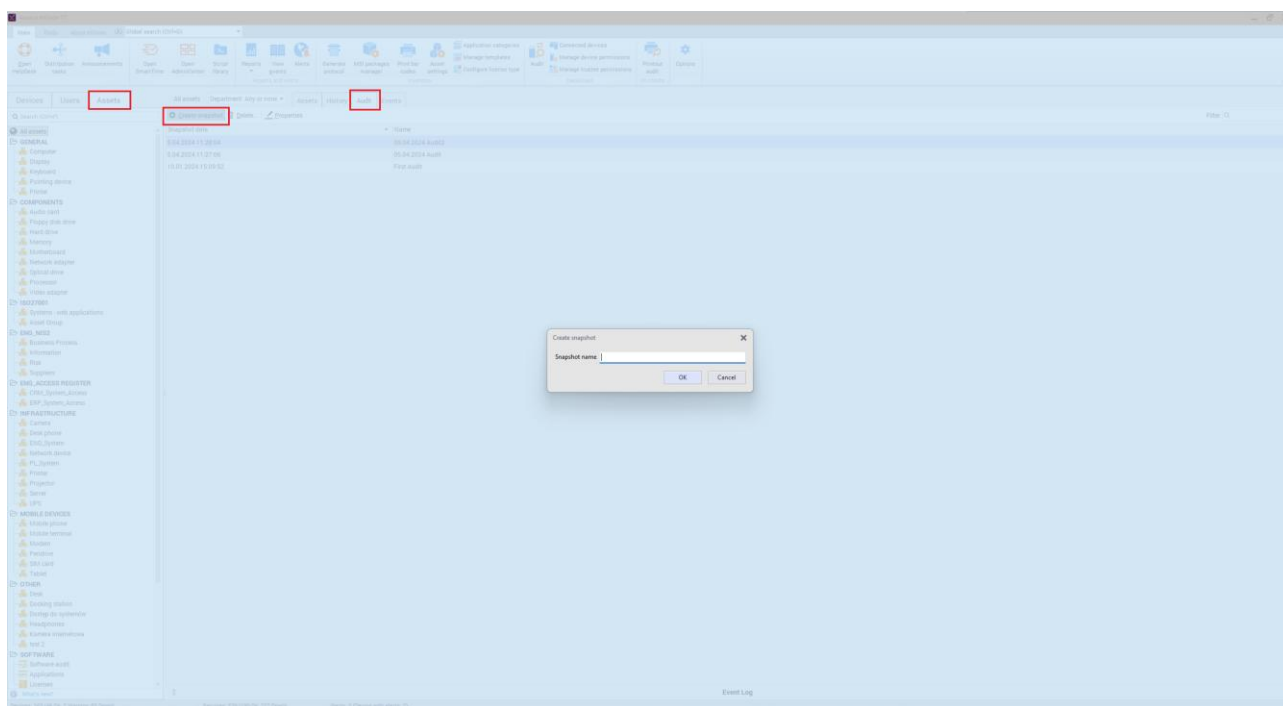
The nVision reporting system contains an entire module dedicated to user activity. You can find a detailed discussion of the reports gathered there **here**. Using these reports will allow you to export data on which applications are used by the users and which websites are visited by them within a given time period. By comparing this list with the list of previously inventoried assets, you can ensure that only inventoried assets are being used.

After anonymization, data exported from nVision can be analyzed with the use of GenAI solutions, if this is permissible under the organization's security policy. Such tools will definitely speed up the process of identifying the systems used in the organization.

### 1.5.3 Creating audit snapshots on recurring basis<sup>4</sup>

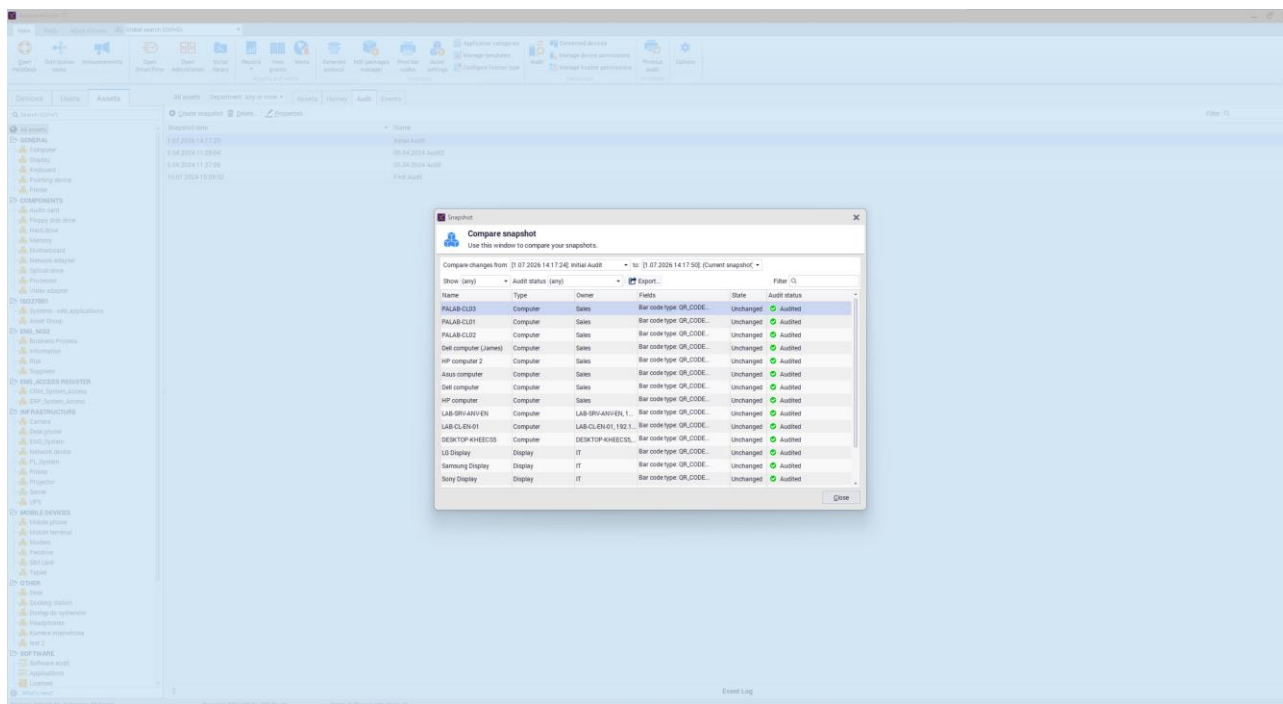
On the **Assets** tab, use the **Audit** option available after selecting all assets:

<sup>4</sup> Regular verification of the status of assets and comparison of changes complies with NIS2 (Article 21(2)(g)), together with applicable national cybersecurity legislation, which requires the assessment of the effectiveness of implemented security measures.



In this way, you can create a snapshot that archives the state of the assets at a given moment. The snapshot covers assets whose type has been defined as audited.

Create such a record of the state after completing the inventory, and then repeat it on a recurring basis (e.g. once a month). Comparing snapshots will make it easy to see what has changed on the asset list:

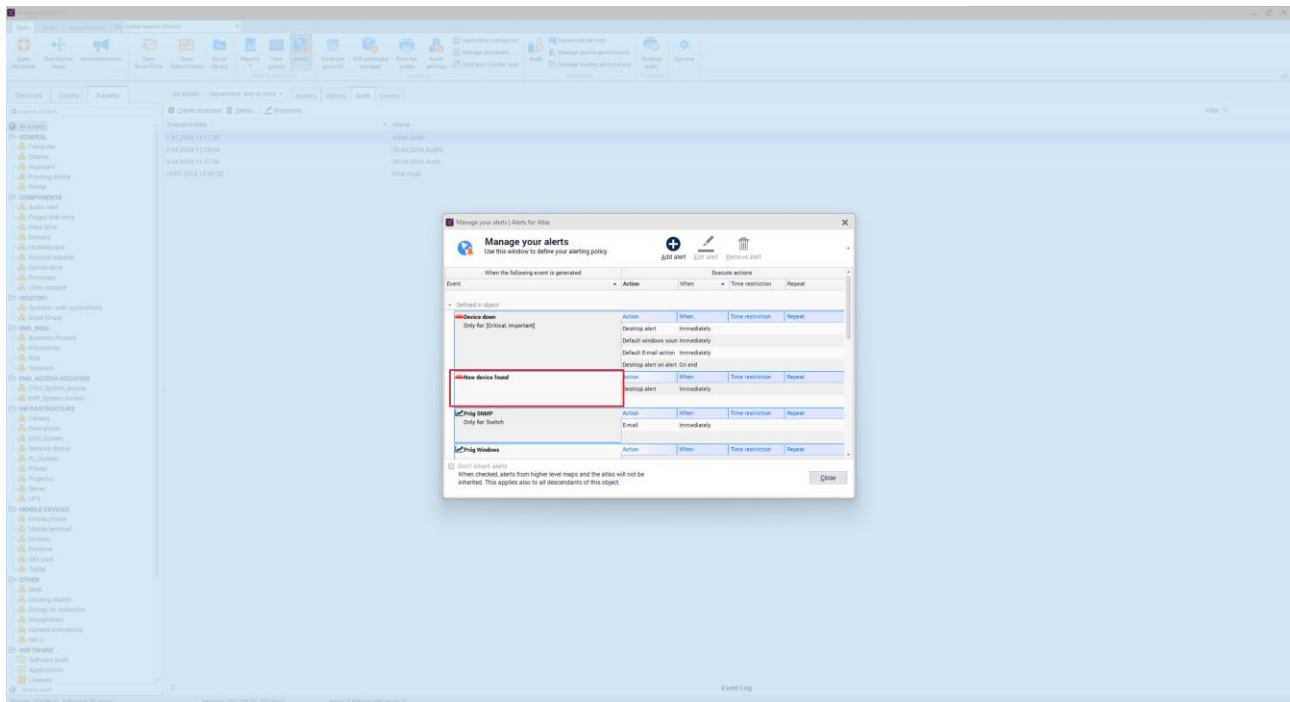


You can compare archived snapshots, and you can also compare a snapshot from the archive with the current state. You can read more about asset auditing [here](#).

## 1.6.2 Creating an alert for additional assets

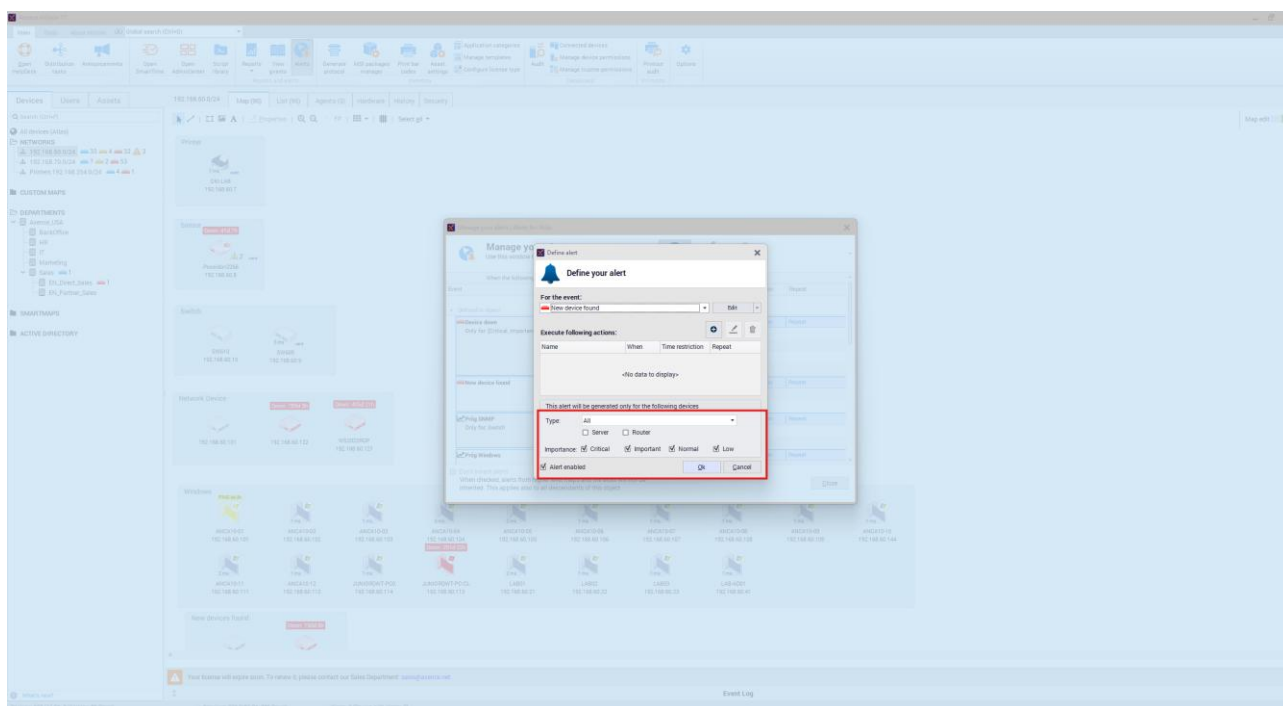
With nVision, you also have the ability to easily detect new devices and software<sup>5</sup>, which translates directly into better detection of so-called shadow IT.

At the Atlas level, several default alerts are set up, including the **New device** alert:



This alert will operate globally, meaning you will receive a notification for every new device. You can disable it for specific device types or devices with a specific importance status.

<sup>5</sup> Article 21(2)(b), (c), and (i) of NIS2, together with applicable national cybersecurity legislation, requires the implementation of continuous monitoring and vulnerability management, as well as mechanisms for rapidly detecting changes to infrastructure, including new devices, unauthorized services and configuration changes.



In addition to alerts at the Atlas level, you can also create alerts at the map level (including on SmartMaps – for example, the previously created map of unassigned devices). More information about alerts can be found [here](#).

## 1.7 Summary

ISO 27001 (and related ISO 27002) requires the organization to maintain an **up-to-date inventory of information assets**. This inventory includes, among other things, hardware, systems, applications, databases, IT services, processes and employees.

This is directly connected with:

- the management of assets (**A.5**),
- the inventory of assets, the assignment of owners and the classification and handling of sensitive data (**A.5.9–A.5.12**),
- the **risk assessment** process.

In turn, NIS2 (Article 21(2)(d) and (e)) requires oversight of all systems in use, including SaaS, web applications and external services, which likewise requires their full inventory and the assignment of owners.

Without knowing what you have to protect, it is impossible to assess risk or plan security controls.

**The inventory of hardware and systems allows you to:**

- **identify** assets and assess their value and vulnerabilities,
- perform a reliable **risk assessment** and to plan effective, proportionate **security controls** in accordance with **ISO 27001**,
- obtain a complete **picture** of assets and their **relations**,
- **identify threats** in all areas required by NIS2 and the applicable national implementing legislation,
- perform a multi-faceted **risk assessment** that forms the basis for implementing appropriate, proportionate and mandatory **cybersecurity measures**.

## 2. Definition of responsibility for assets (A.5.9, A.5.2)

ISO 27001 requires that all assets have a defined owner, understood as **the person responsible for the value, risk and decisions concerning a given asset**.

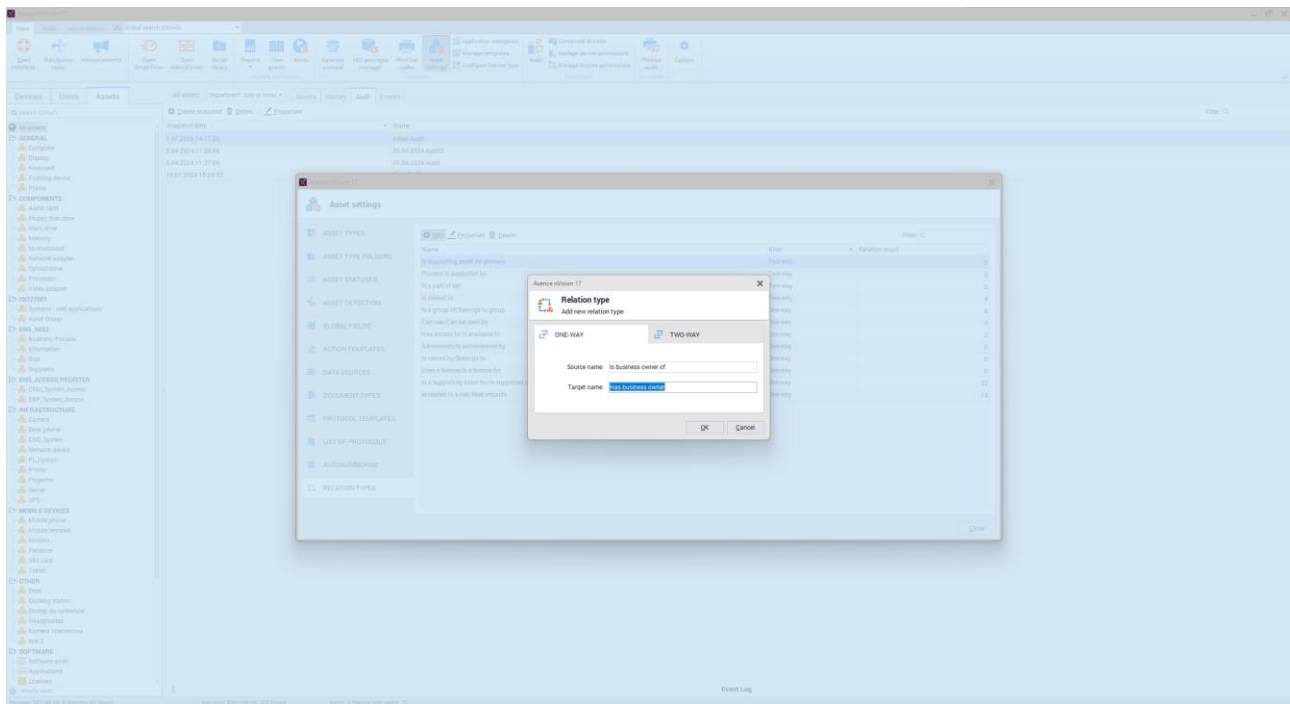
The NIS2 Directive (Articles 20 and 21) and the applicable national implementing legislation extend the responsibility of asset owners and management, requiring clear allocation of responsibility for maintaining the security of systems and operational continuity. Inventorying assets is a key element of building a security management system. At the same time, it is the starting point for assigning the responsibility.

### 2.1 Assigning business owners

The division of responsibility for the elements of the information security management system depends on the management of a given organization. Usually, however, it is assumed that asset owners are responsible (or jointly responsible) for:

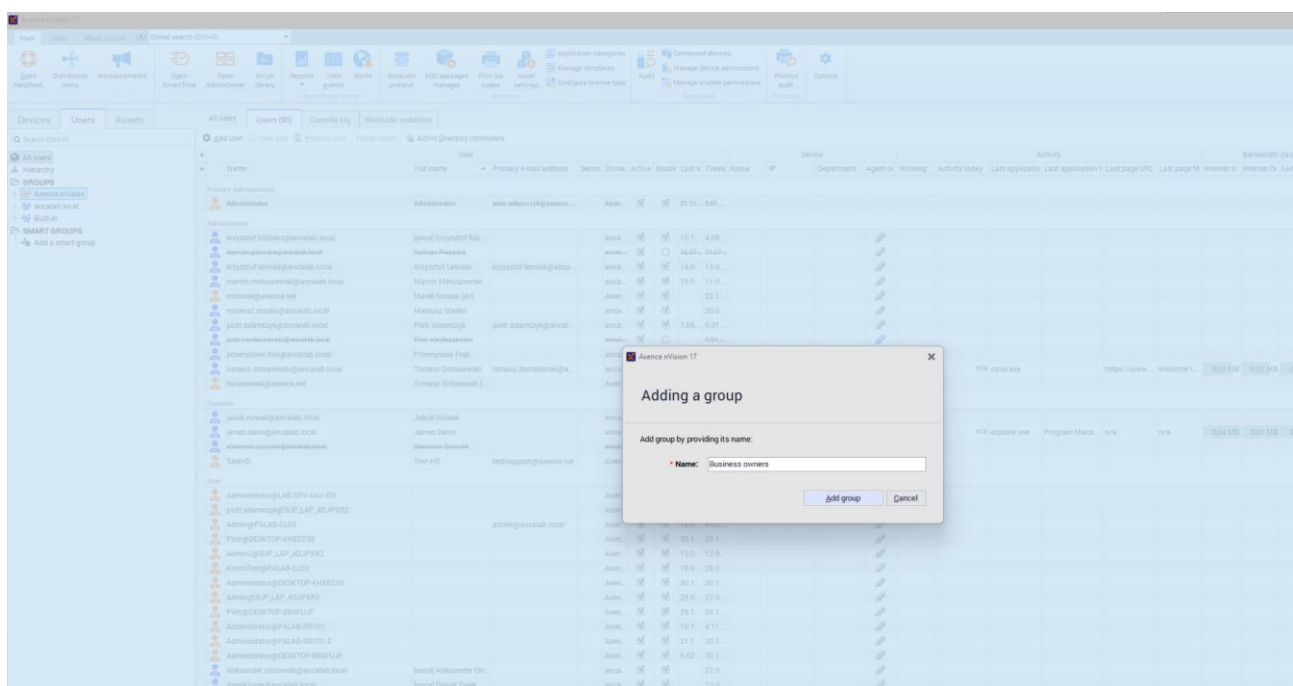
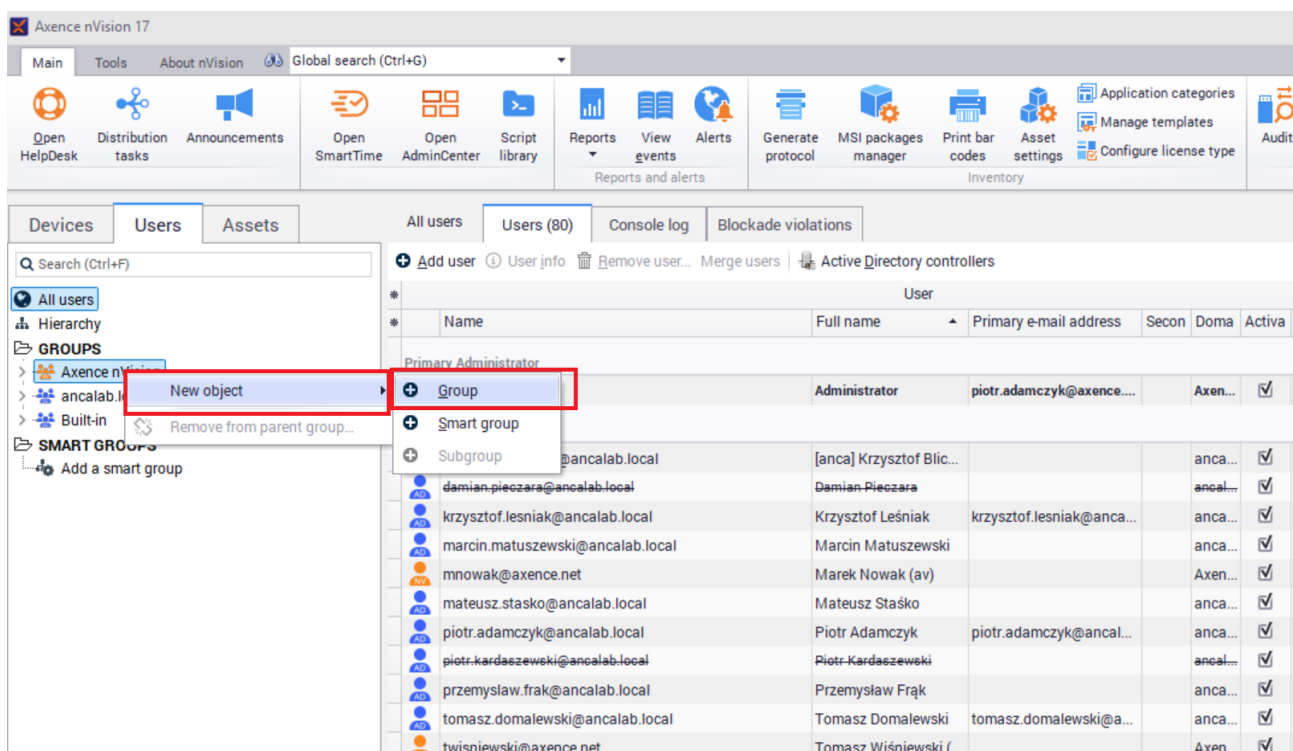
- the classification of information,
- the identification of threats,
- the acceptance of risks,
- decisions regarding security controls,
- determining the level of access and protection,
- controlling modifications.

Therefore, after entering all the assets into nVision, assign owners to them. To do this, define another relation type, **Is business owner of / Has business owner**, in the **Asset properties**, in the **Relation types** section:



## 2.1.1 Creating a group for business owners

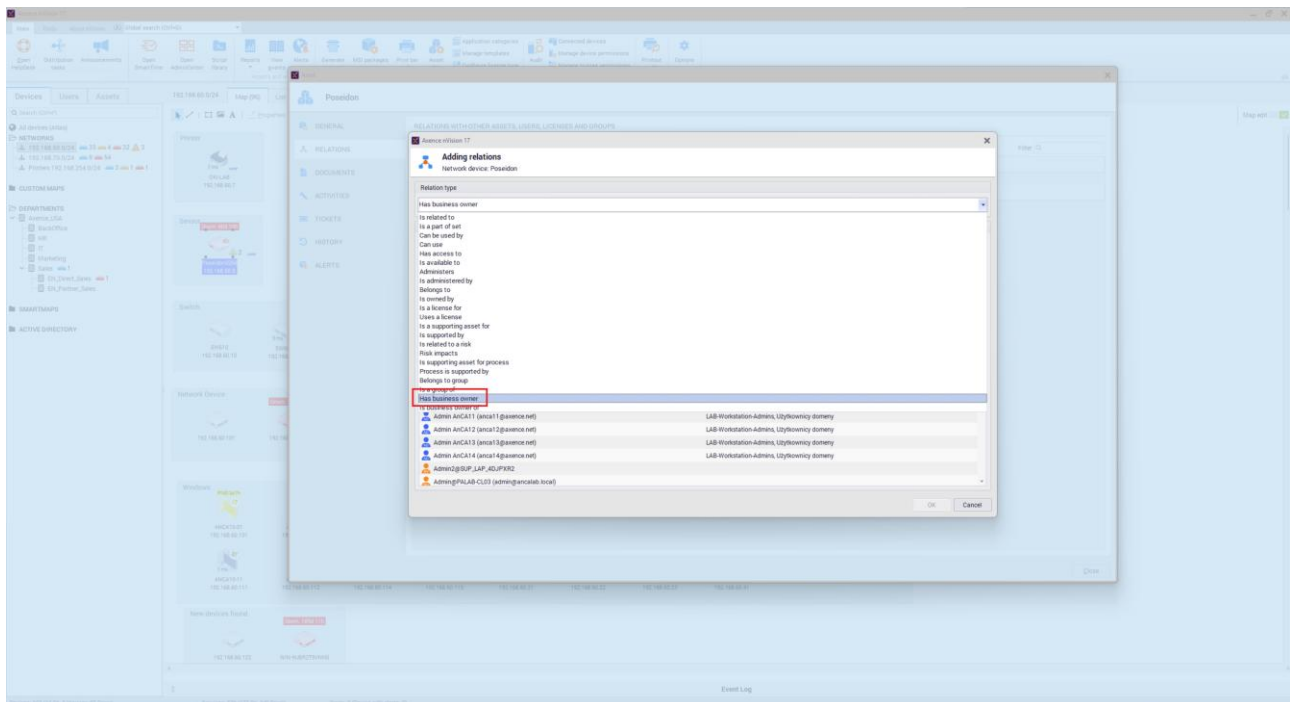
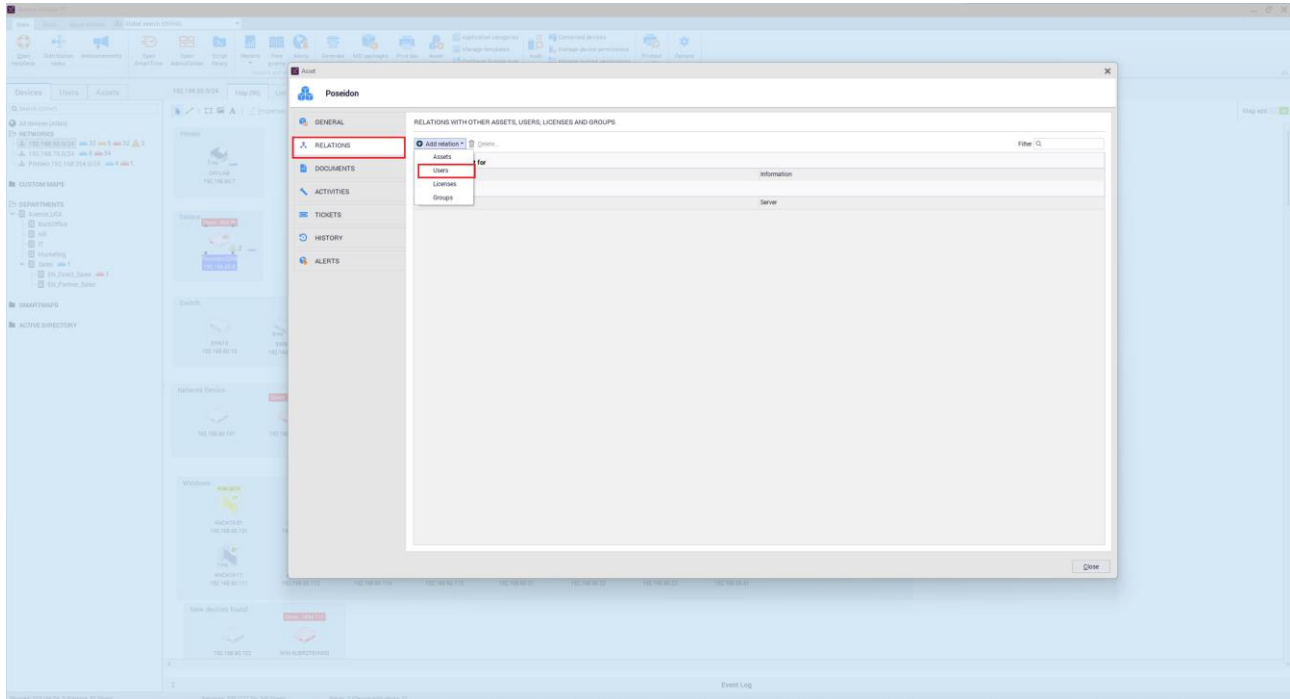
By creating this group, you will have an easy-to-update list of business owners that will be useful, among other things, for efficiently managing the sending of announcements at later stages (e.g. to inform business owners of the need to verify the assets they are responsible for). An ordinary group will suffice; you do not need a smart group:

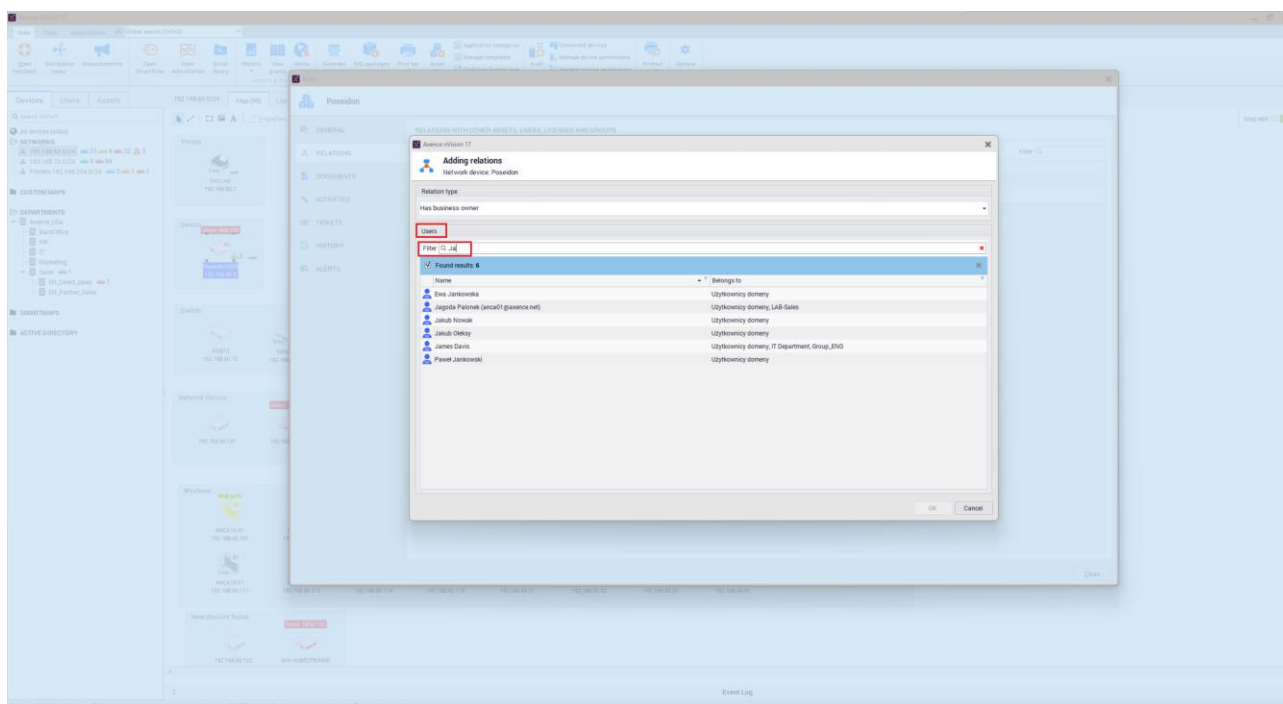


Keep this group up to date, by adding all users marked as business owners in the following steps. More information about groups can be found [here](#).

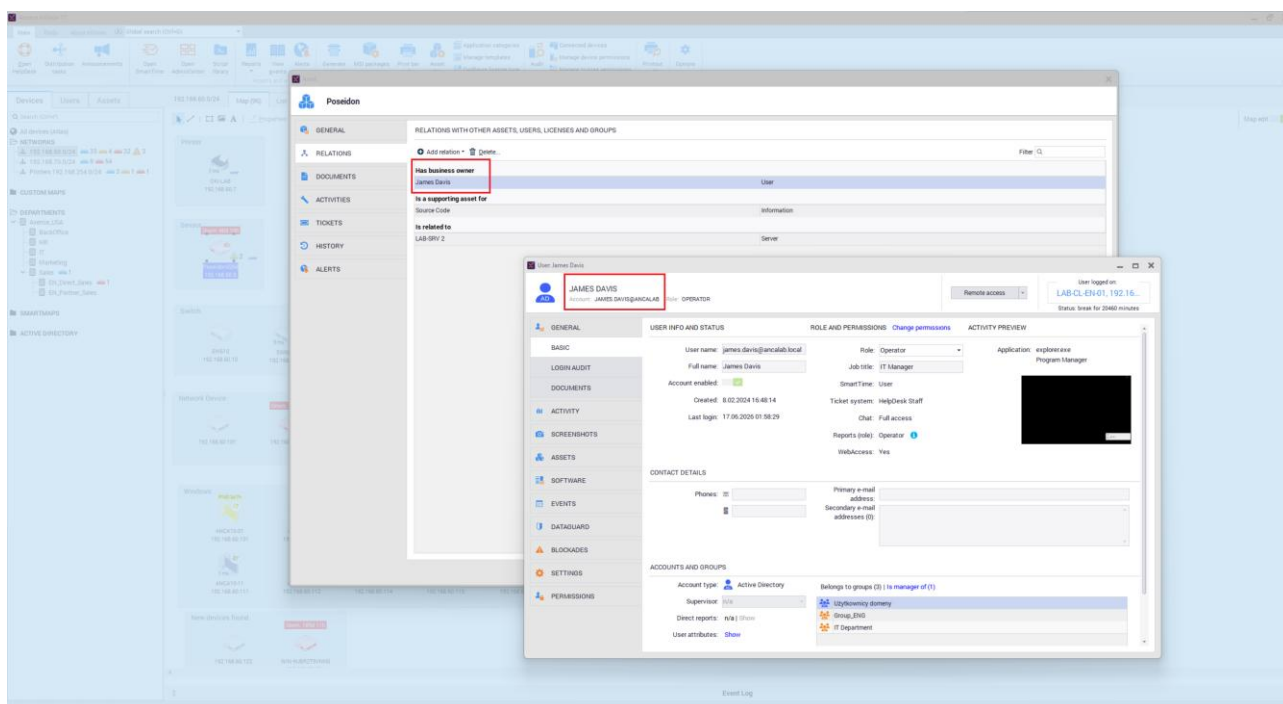
## 2.1.2 Assigning business owners to network devices

For network devices, indicate the business owners responsible for the configuration and security of critical devices. Select those with **important** or **critical** status (you can use the SmartMap created earlier) and assign an owner in the linked asset:





After confirming the selection of an owner, you can check that the relation has automatically appeared in the window with their information:

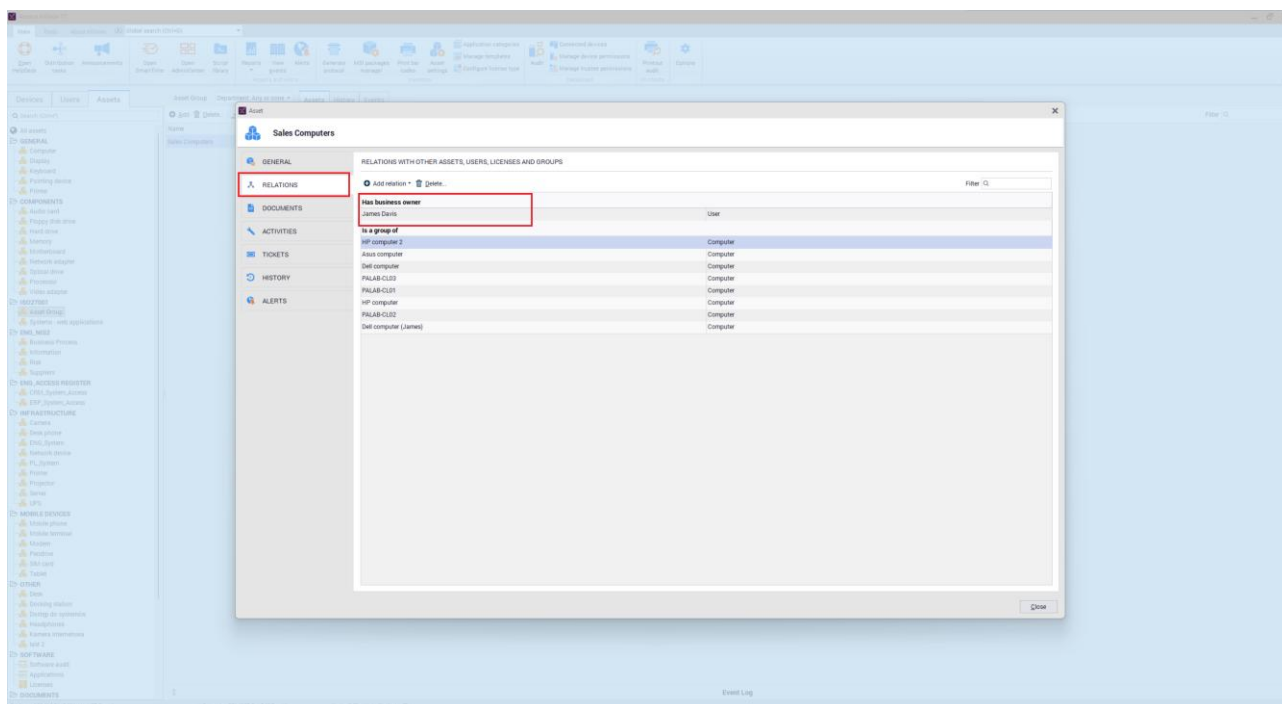


Assign an owner to the remaining network devices in the same way, that is, update each device separately. In such a situation, a SmartMap complementary to the one with important and

critical devices will come in handy. You can also create a device group and assign an owner to the entire group rather than to a specific device.

### 2.1.3 Assigning business owners to device groups

Device groups can also have their own business owners. Thanks to this, you do not have to assign them to each device separately:



However, remember that assigning a business owner to a group **does not propagate** to the devices: a business owner assigned to a group will not be directly linked to a device and will not be visible from the device level. If you need to display the business owner on specific devices, add them via a separate relation with the device.

### 2.1.4 Assigning business owners to systems

Assign business owners to systems (web applications) in the same way. You can do this separately for individual systems, or you can group these assets and give the group an owner.

## 2.2 Announcement to business owners

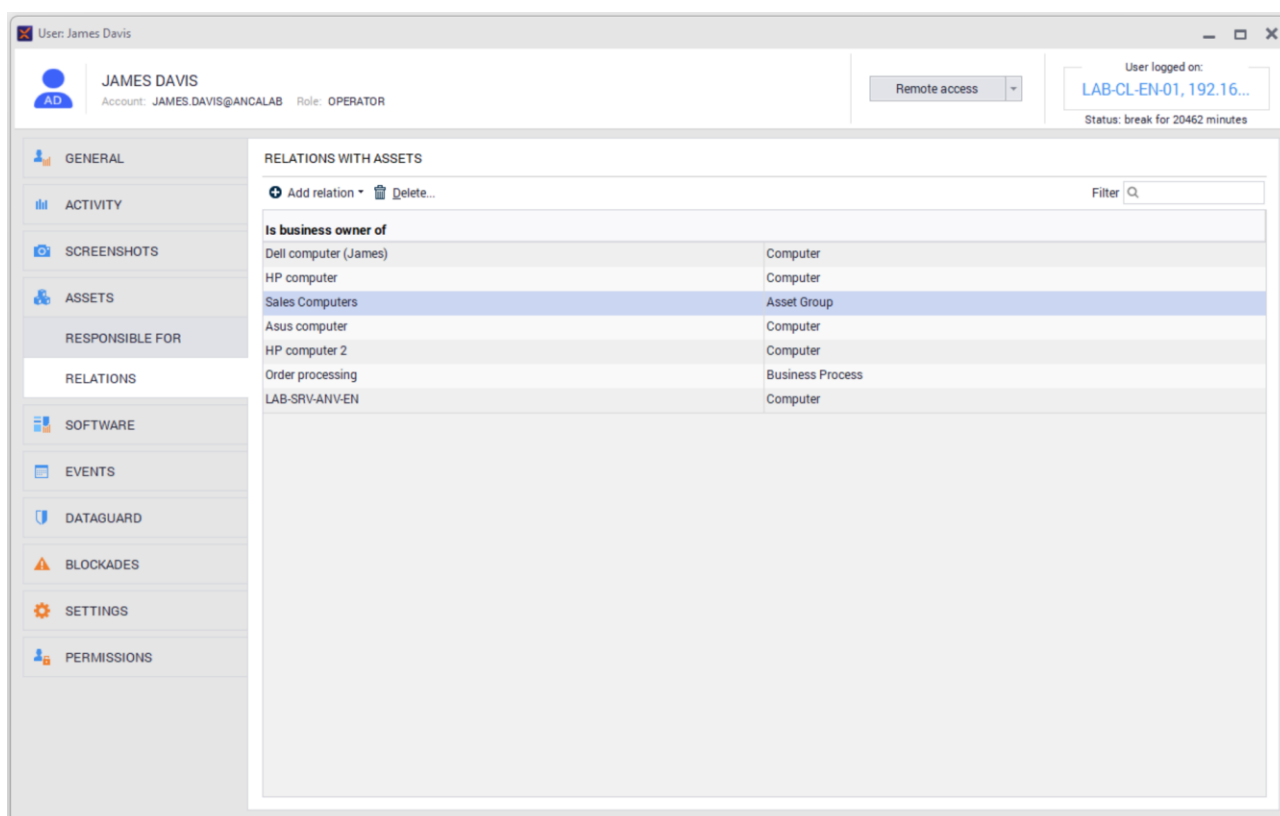
The IT department plays a key role in adapting the organization to ISO 27001, but it may have incomplete knowledge of all the assets used in the individual organizational units. This is why the inventory of assets, systems, threats and security controls is also the responsibility of the business owners of the assets in the individual organizational units. They can supplement the information entered by the IT department. They should only do this after the IT department has

completed the initial inventory stage. Therefore, you need an efficient way to notify them that they need to participate in the inventory process.

For this purpose, you can use nVision, and more specifically the **Announcements** option in the HelpDesk module.

## 2.2.1 Exporting the list of assets of business owners

Start by preparing a list of the assets assigned to a specific business owner. On the **Users** tab, open the **Business owners** group. For each user, select all occurrences of the **Is business owner of** relation in the **Assets > Relations** section.



The screenshot shows the nVision interface for user JAMES DAVIS. The sidebar on the left contains navigation options: GENERAL, ACTIVITY, SCREENSHOTS, ASSETS, RESPONSIBLE FOR, RELATIONS, SOFTWARE, EVENTS, DATAGUARD, BLOCKADES, SETTINGS, and PERMISSIONS. The main area displays the 'RELATIONS WITH ASSETS' section. At the top, there are buttons for 'Add relation' and 'Delete...'. Below this is a table with the following data:

| Is business owner of  | Asset            |
|-----------------------|------------------|
| Dell computer (James) | Computer         |
| HP computer           | Computer         |
| Sales Computers       | Asset Group      |
| Asus computer         | Computer         |
| HP computer 2         | Computer         |
| Order processing      | Business Process |
| LAB-SRV-ANV-EN        | Computer         |

Right-click and select the **Export** option, then save the list in a convenient location in .xlsx format.

In this way, you will prepare a file for each business owner with a list of their assigned assets. Exporting to.xlsx format allows for convenient viewing of the data and its further processing.

Create a folder (e.g. **ISO asset verification**) in a central location (OneDrive, SharePoint or a network share) to store the exported lists. Share the prepared files with the business owners (making sure to grant the correct access permissions).

Inform the business owners that they need to review the list of assets assigned to them. The simplest way to do this is to use the **Announcements** function in the HelpDesk module.

## 2.2.2 Announcement template and sending<sup>6</sup>

Include a request in the announcement to verify one's own asset holdings and to report any discrepancies between the actual state and the provided asset list to the given e-mail address. Give the message an appropriate title.

### Example announcement:

**Subject:** Verification of assets assigned to the business owner

**Content:** Dear Sir or Madam,

as part of the asset inventory and information security management process, please review the list of **assets assigned** to you as the business owner.

The list is available at: [LINK TO LOCATION].

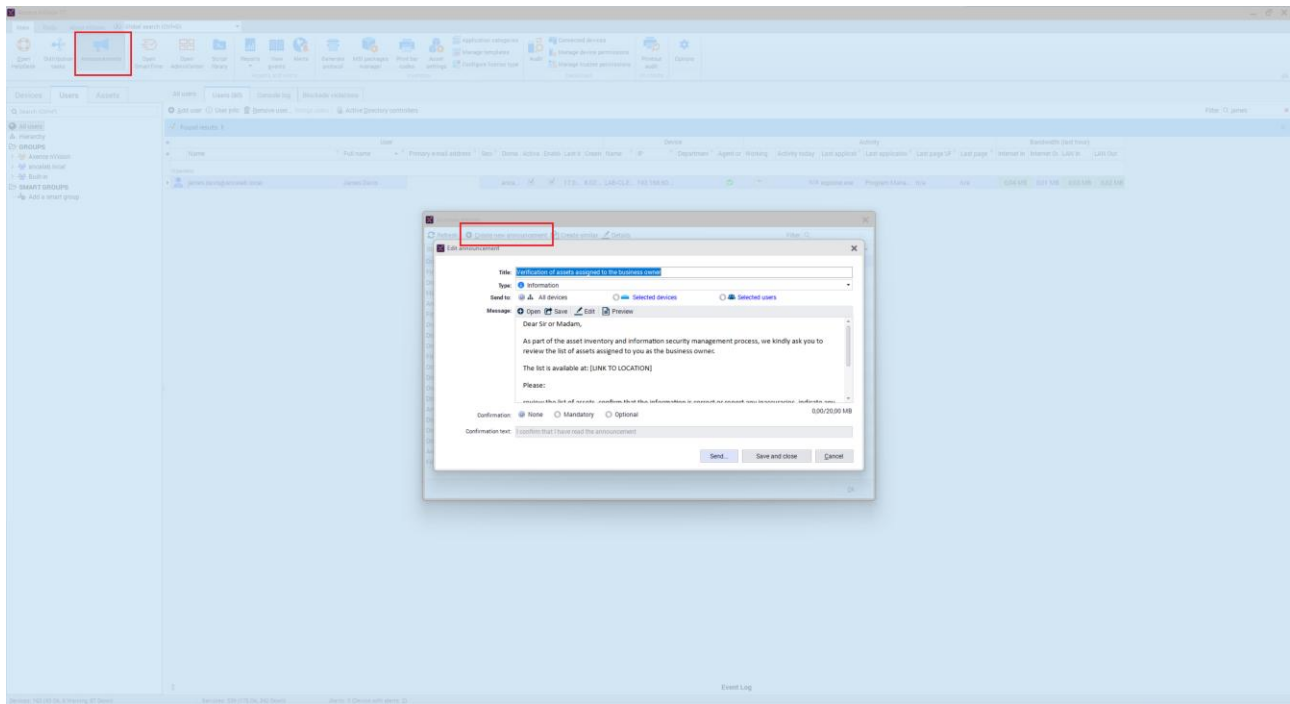
We ask that you:

- review the list of assets,
- confirm their correctness or report any inaccuracies,
- indicate any additional assets or systems that should be taken into account.

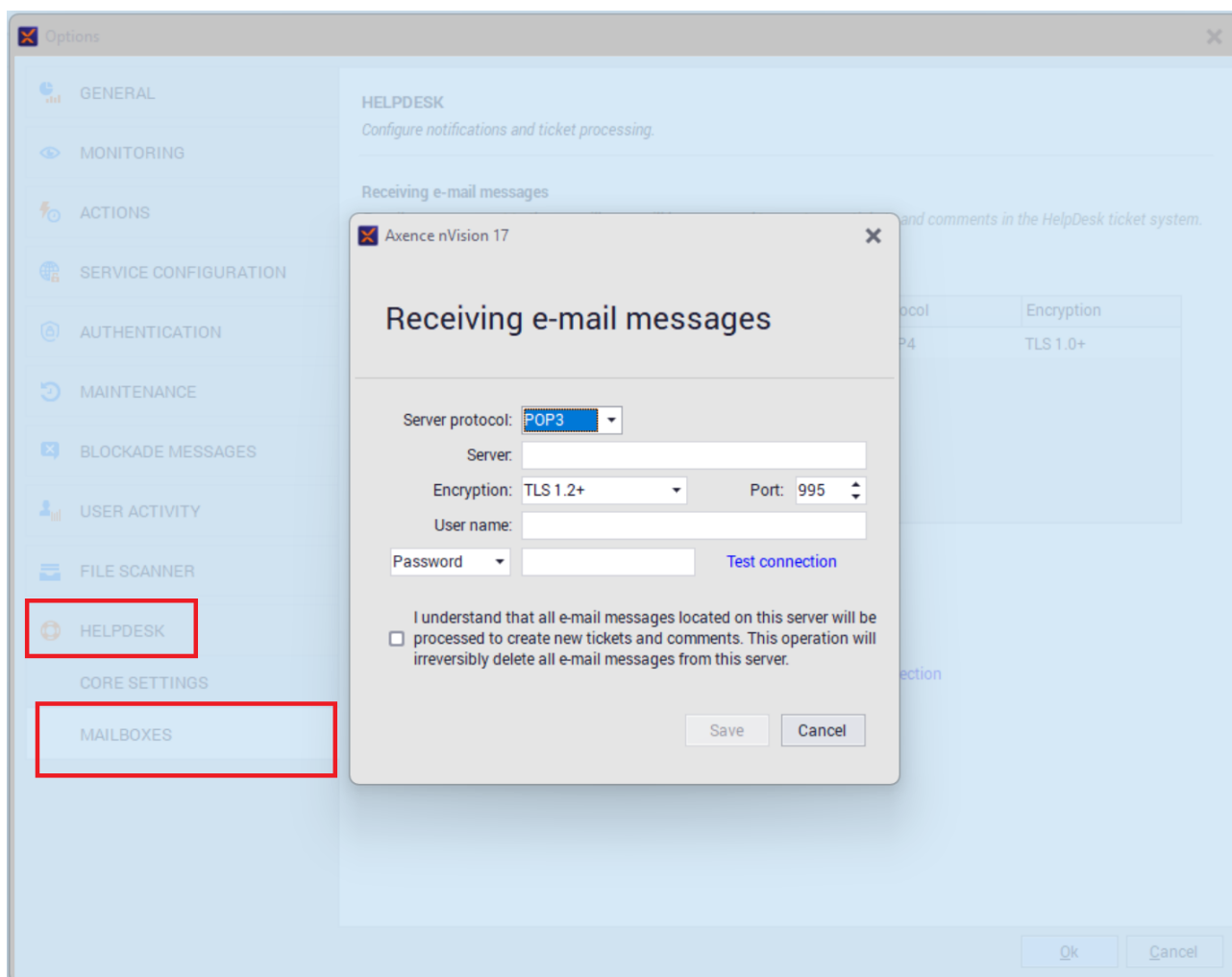
If you have any comments, please send them to: [E-MAIL ADDRESS].

Deadline: [DATE]

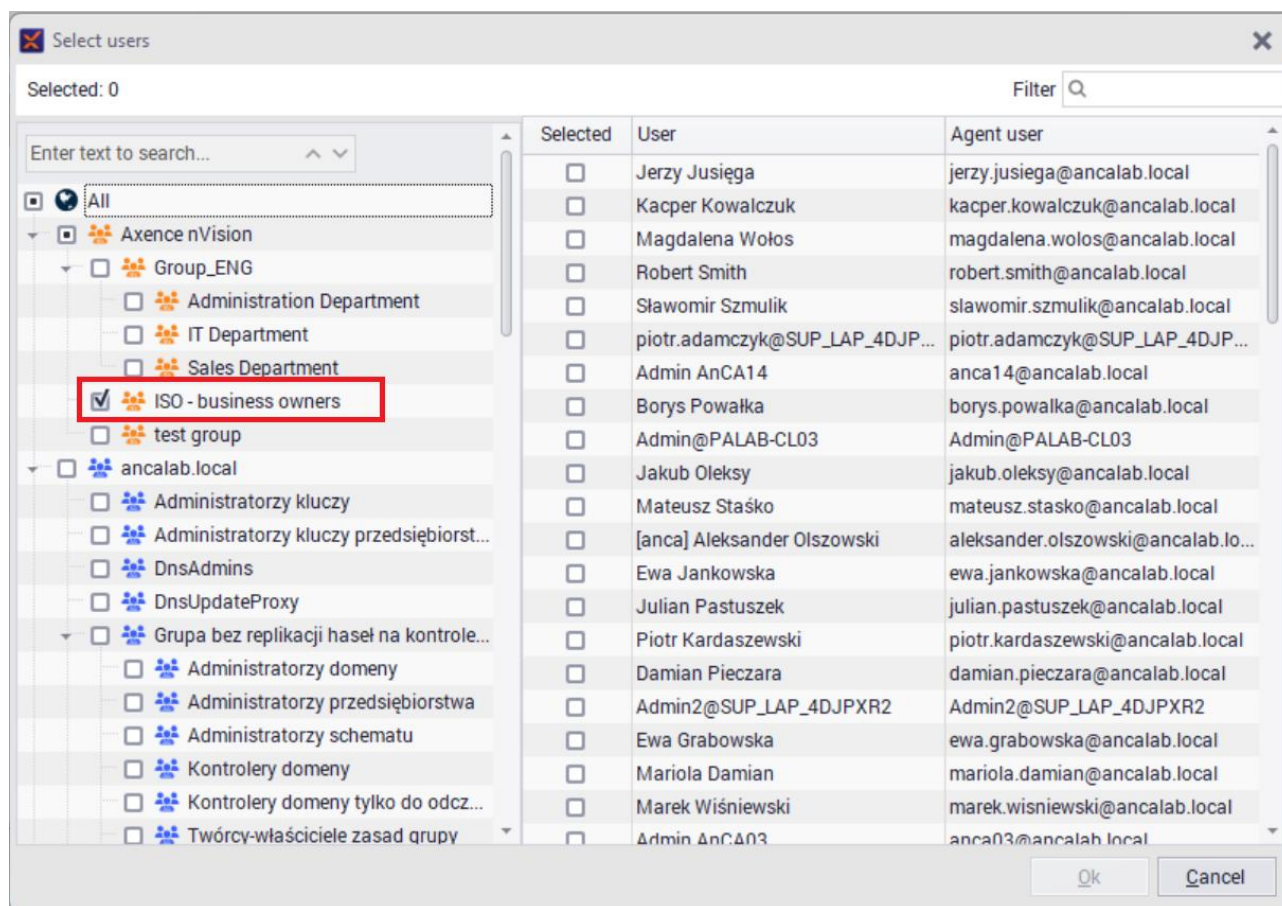
<sup>6</sup> Article 21(2)(j) of NIS2, together with applicable national cybersecurity legislation, requires the implementation of security-related communication processes, including informing personnel of their system security obligations and the need to ensure that asset data is kept up to date.



Add the address from which tickets and comments are generated in the **Options** section, on the **HelpDesk > Mailboxes** tab. Enter the details in accordance with your mail provider's data. If you want to receive e-mail notifications about changes to tickets, also configure the **Sending e-mail messages** section. You can read more about e-mail settings [here](#).



Select sending to selected users and indicate all users from the business owners group as recipients:



Confirm your selection by clicking the [ **Ok** ] button. **Do not send the message; only save and close it.** In this way, you will create a draft that you can send multiple times (the **Create similar** option is hidden under the right mouse button).

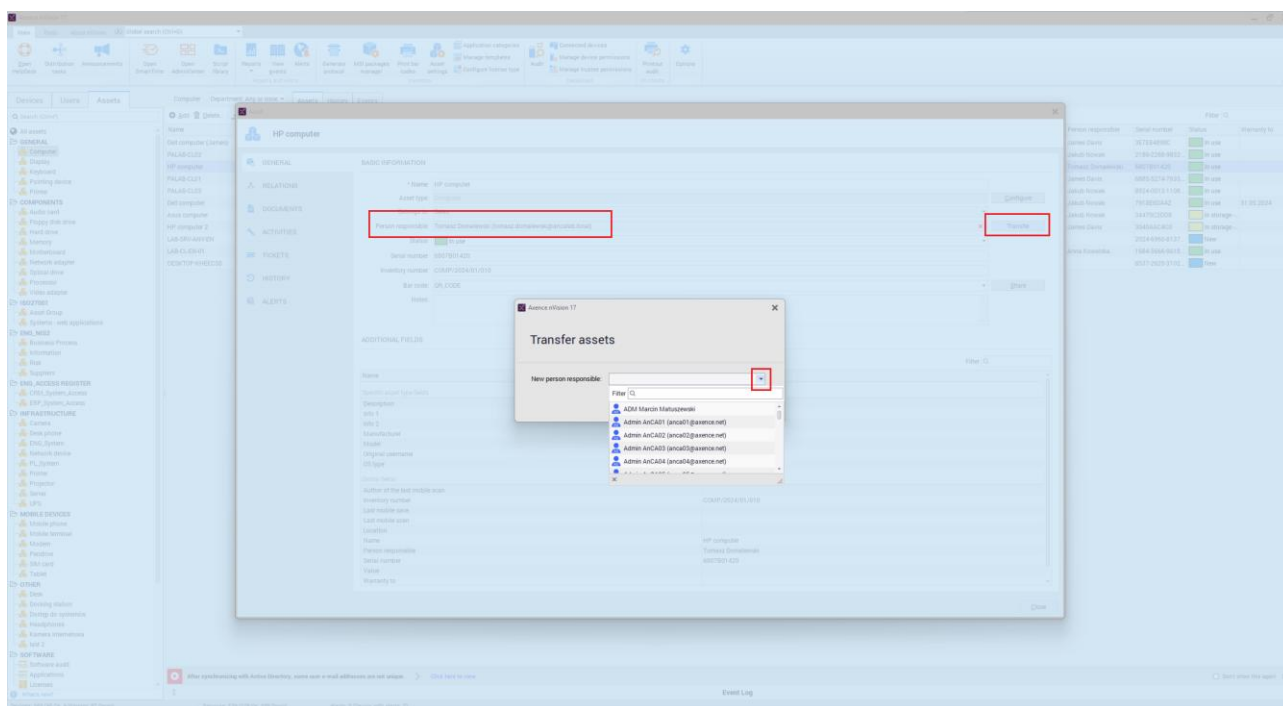
More information on creating announcements can be found [here](#).

## 2.3 Assigning responsible people to assets

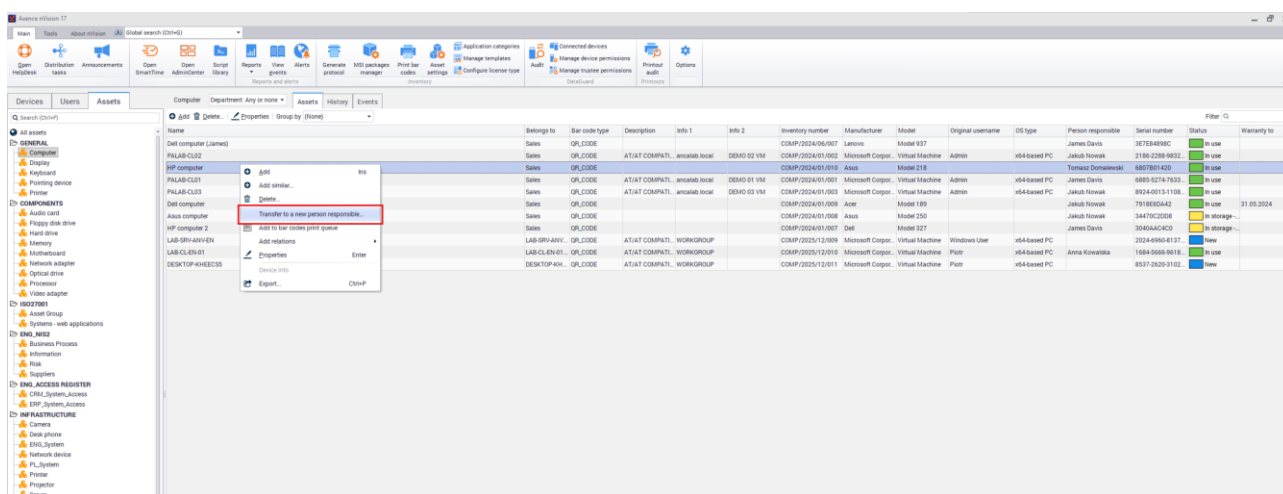
ISO 27001 states that the owner of an asset is responsible for defining permissions and access rules. However, it also points to the existence of actual users, i.e. individuals who use the asset. A similar mechanism occurs in NIS2 and the applicable national implementing legislation.

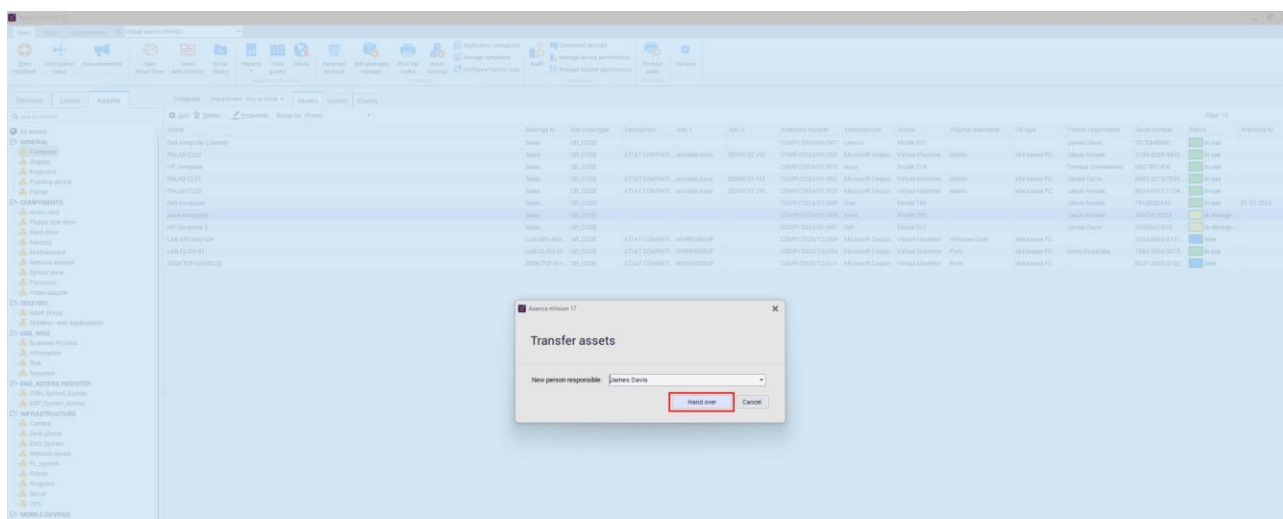
It is important to determine the user because they are responsible for using the asset properly. At the system level, you can determine the user by handing the asset over to them. By indicating the actual user, you can properly manage permissions and risk, as well as keep the asset register up to date.

Select the actual user from the drop-down list and set them in the **Responsible person** field in the asset property window:

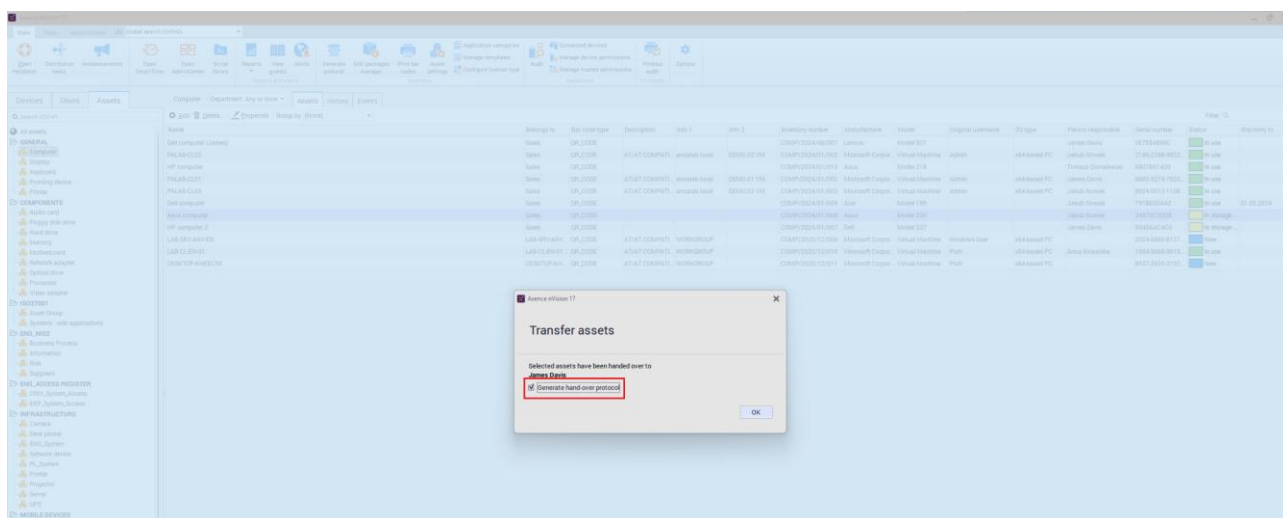


You can also right-click the asset and select the option to hand it over to the responsible person:

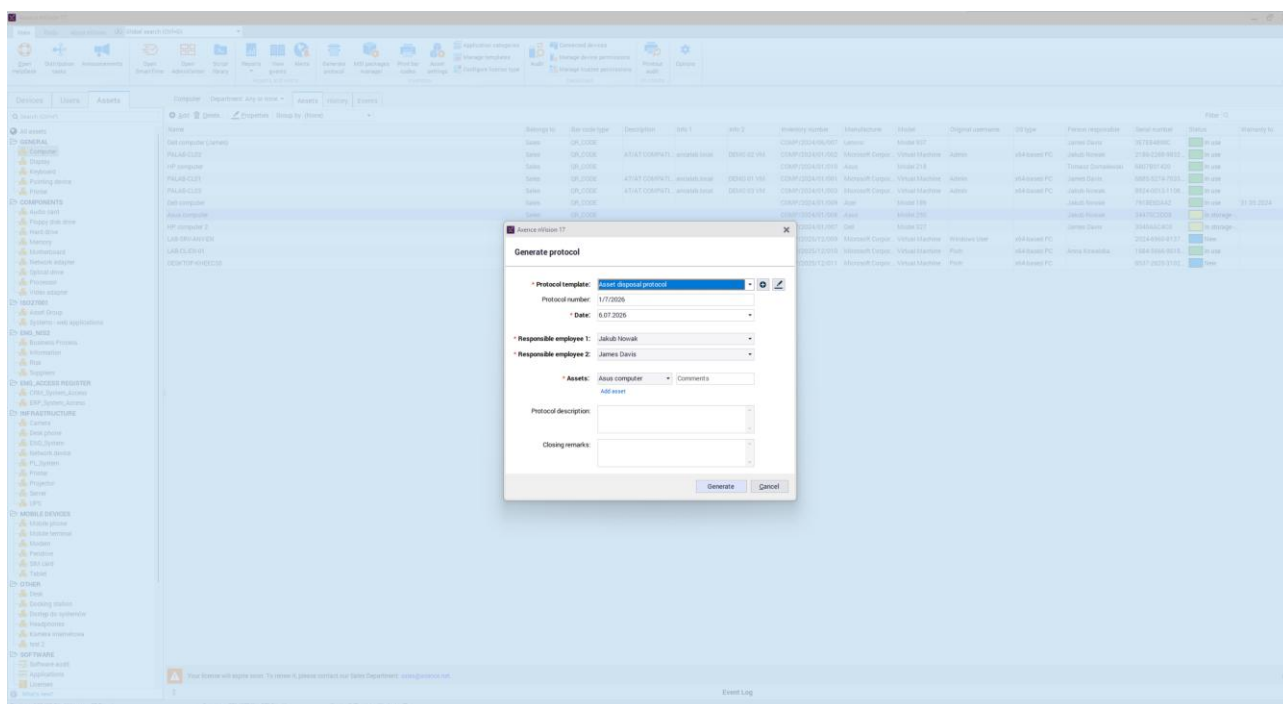




After clicking [ **Hand over** ], you can decide to generate a handover protocol:



If not, do not select the option and click [ **Ok** ]. If so, select the option and confirm the data for the protocol:



Save the created protocol to your computer (you can print it and give it to the new user of the asset to sign). In the system, you will find it in the asset setting window on the **Protocols** tab, where you can also generate a new protocol

You can read more about protocols [here](#).

## 2.4 Verification of asset status by users

The HelpDesk and Inventory modules are integrated with each other. Thanks to this integration, each active nVision user can log in to the HelpDesk panel (or go through the link from the nVision Agent level) and review the list of assets they use (for now, the list includes only assets based on physical devices):

| HelpDesk                             |                |              |               |             |              |              |            |         |  |
|--------------------------------------|----------------|--------------|---------------|-------------|--------------|--------------|------------|---------|--|
| Enter a search phrase or a ticket ID |                |              |               |             |              |              |            |         |  |
| Advanced                             |                |              |               |             |              |              |            |         |  |
| MY ASSETS (19)                       |                |              |               |             |              |              |            |         |  |
| Enter the asset name or number       |                |              |               |             |              |              |            |         |  |
| Export (19)                          |                |              |               |             |              |              |            |         |  |
| NAME                                 | ASSET TYPE     | PERSON RE... | TICKET COU... | STATUS      | SERIAL NO... | INVENTORY... | DEPARTMENT | ACTIONS |  |
| Access for james                     | CRM_Syste...   | james Davis  | 0             | In use      | -            | -            | Sales      |         |  |
| Axus computer                        | Computer       | james Davis  | 0             | In stora... | 34470C2D08   | COMP2024...  | Sales      |         |  |
| Business customer service            | Business Pr... | james Davis  | 0             | In use      | -            | -            | Axence_USA |         |  |
| Complaint handling                   | Business Pr... | james Davis  | 0             | In use      | -            | -            | Axence_USA |         |  |
| Credit Management                    | Business Pr... | james Davis  | 0             | In use      | -            | -            | Axence_USA |         |  |
| Credit risk management               | Business Pr... | james Davis  | 0             | In use      | -            | -            | Axence_USA |         |  |
| Customer contact                     | Business Pr... | james Davis  | 0             | In use      | -            | -            | Axence_USA |         |  |
| Dell computer (james)                | Computer       | james Davis  | 0             | In use      | 3E7E489BC    | COMP2024...  | Sales      |         |  |
| Electronic Banking                   | Business Pr... | james Davis  | 0             | In use      | -            | -            | Axence_USA |         |  |
| Employee education                   | Business Pr... | james Davis  | 0             | In use      | -            | -            | Axence_USA |         |  |

Therefore, if you send users an announcement asking them to verify the status of the assets assigned to them, they will actually be able to do so. Sending such announcements on a

recurring basis is good practice and will allow you to continuously collect information about any inventory inconsistencies.

A convenient way to manage this process is to use the **Announcements** option in the HelpDesk module.

### 2.4.1 Preparing the announcement to users

Include a request in the announcement to verify one's own asset holdings and report any inaccuracies to the given e-mail address. Give the message an appropriate title.

#### Example announcement:

**Subject:** Verification of assets assigned to users

---

**Content:** Hello,

We ask that you verify the list of assets assigned to you in the HelpDesk system. You will find the list of assets you are responsible for on the **My assets** tab after logging in to the HelpDesk panel. Make sure that the devices and other assets shown there match the actual state.

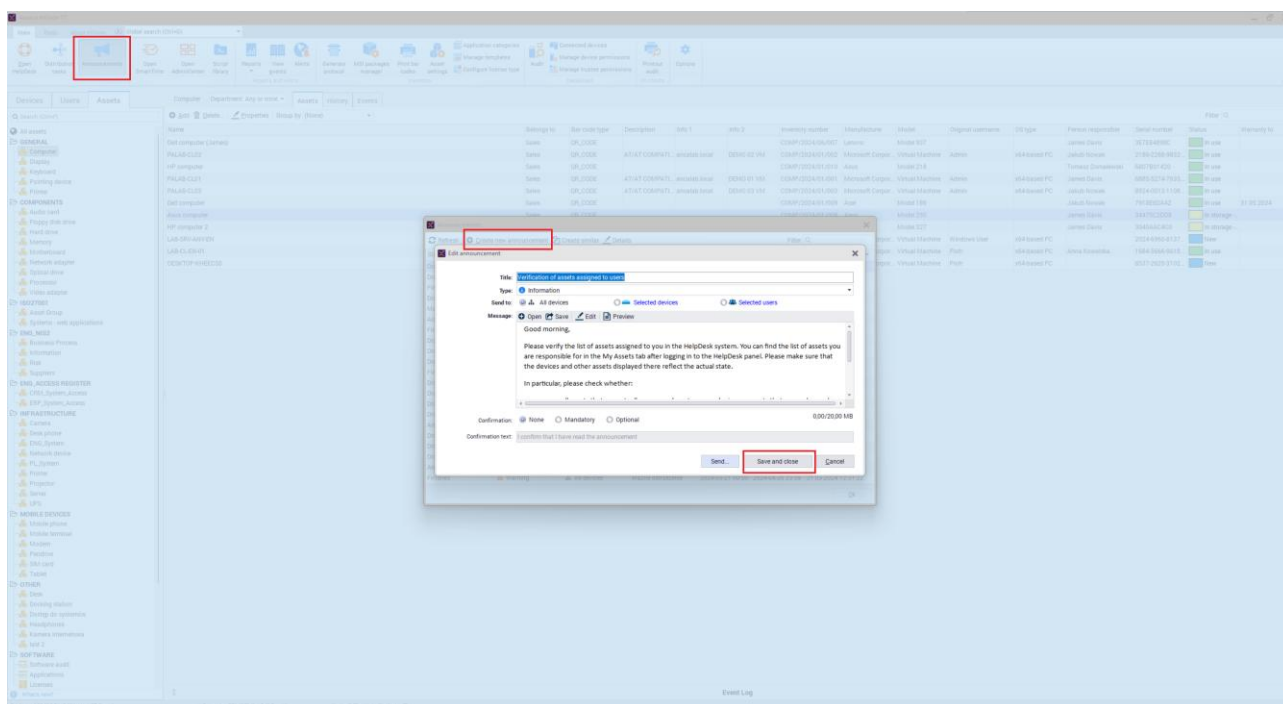
In particular, check whether:

- you see all the assets you actually use,
- you do not see any devices or assets that you no longer have or that should not be assigned to you
- check if asset data is correct.

If everything is in order, you do not need to take any additional action. If you notice any discrepancies, please report them to: **[E-MAIL ADDRESS]** or via a ticket in HelpDesk.

Verification deadline: **[DATE]**

Thank you.



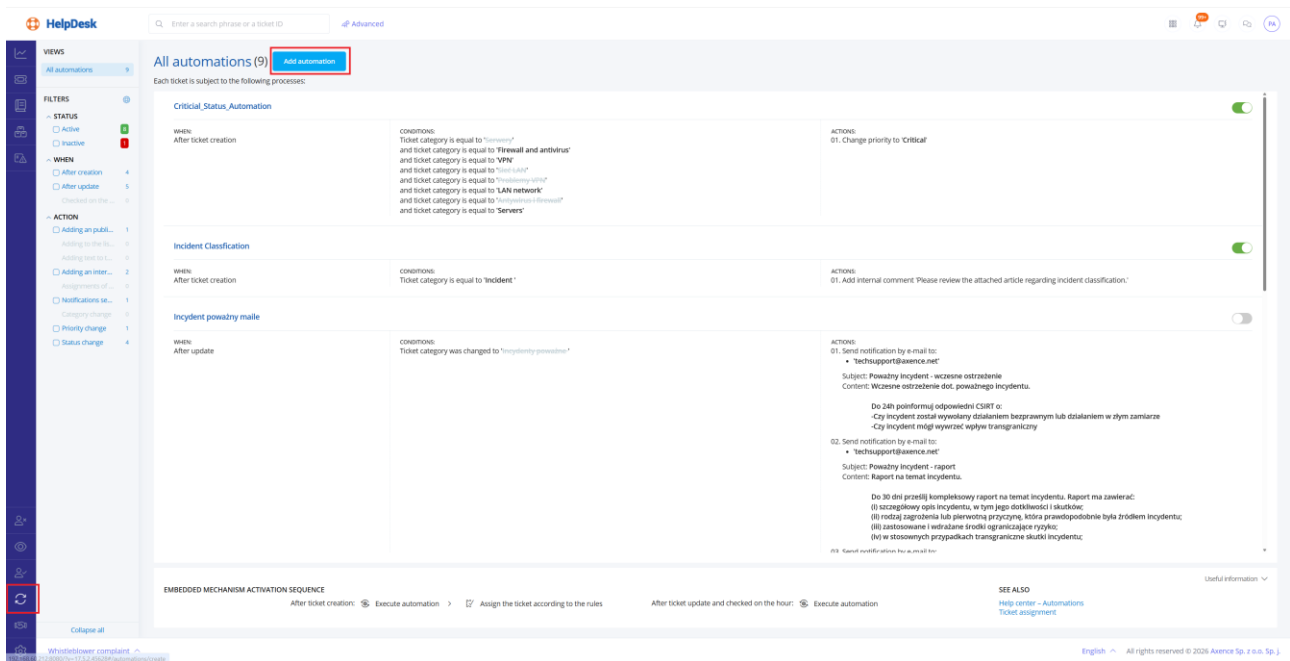
You can configure the e-mail address on the **HelpDesk > Mailboxes** tab (you can find more information on this topic in section [2.2.2](#)).

Select **Sending to all users**. Save and close the message. You will send the prepared draft after setting up the automation in the HelpDesk panel.

## 2.4.2 Ticket automation

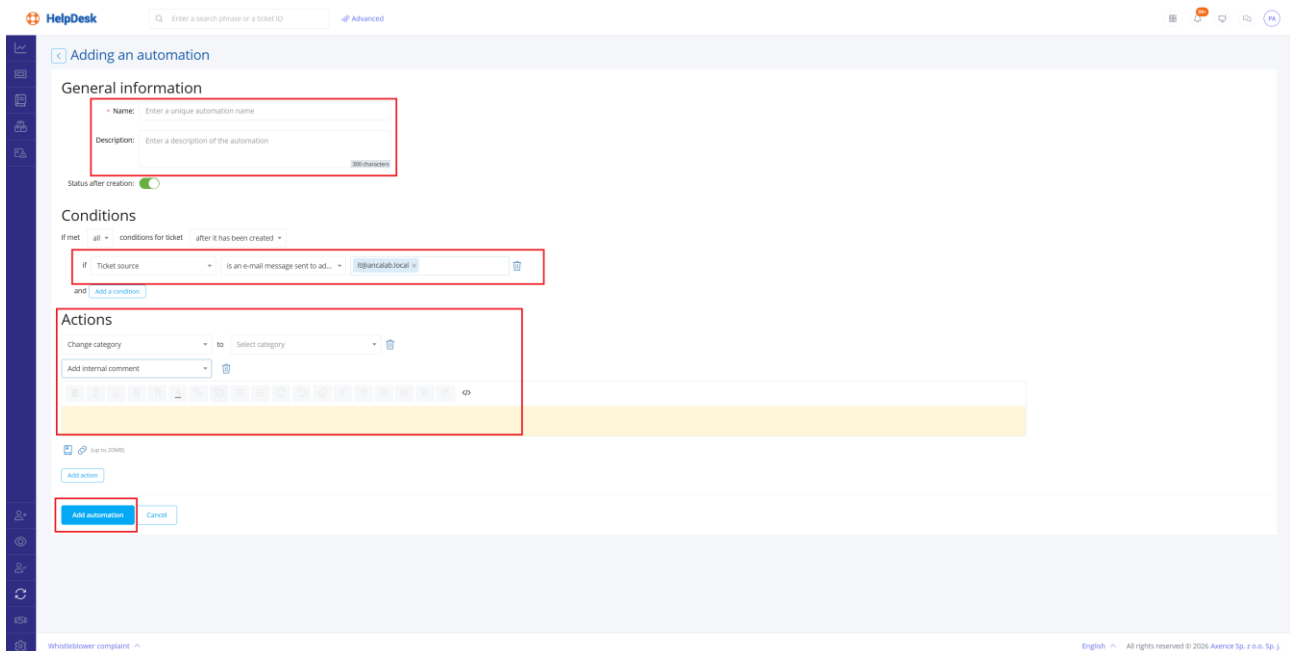
Create a separate ticket category. In the **Settings** tab, add a new category: **Asset discrepancies**. You can assign it a specific submission form to be used later when creating a direct ticket. You can read more about categories [here](#).

Go to the **Automations** tab and add a new one.



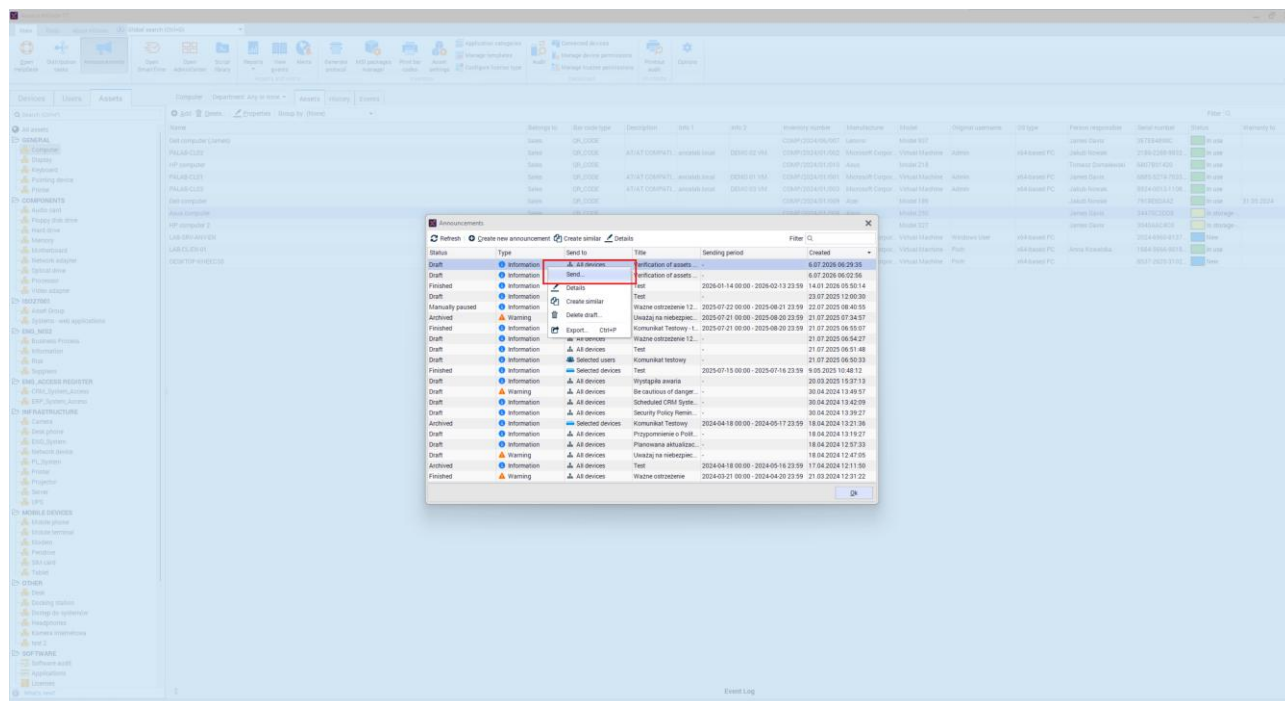
Set the condition to **The ticket source is an e-mail message sent to the address** and enter the address provided in the announcement.

For the action, add a change of the ticket category to the previously created **Asset discrepancies**. You can also add an internal comment about the actual source of the ticket.

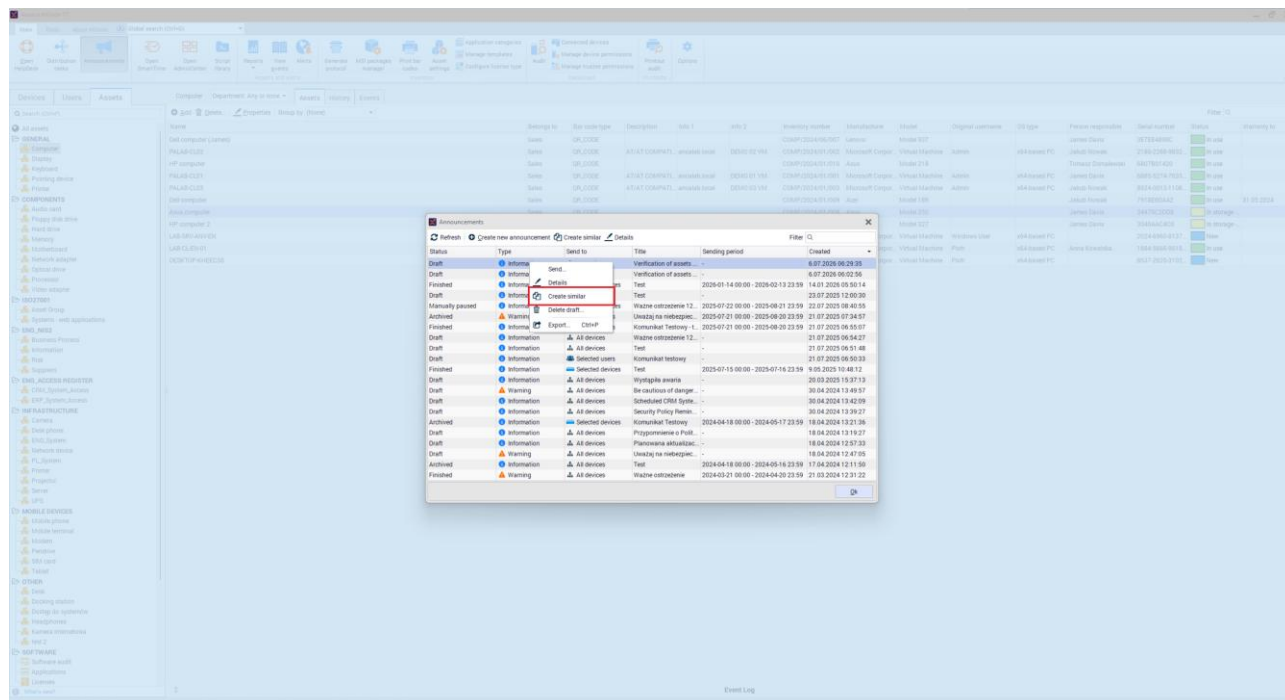


## 2.4.3 Sending the announcement

Once you have prepared the automation, you can send the announcement.



When resending, you do not have to create a new draft from scratch. You can use the **Create similar** option.



## 2.5 Managing change in the scope of responsibility and permissions

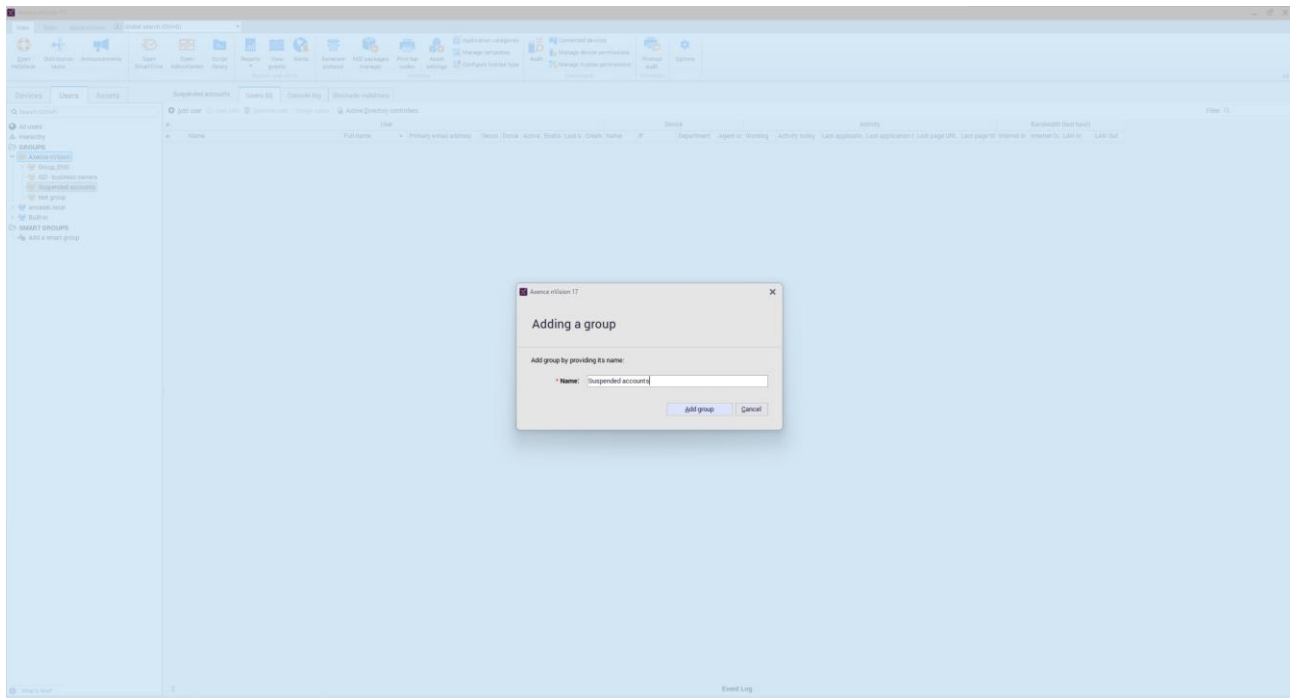
A very important aspect from the ISO perspective is changes in the scope of responsibility and permissions, especially those related to termination of cooperation, because they:

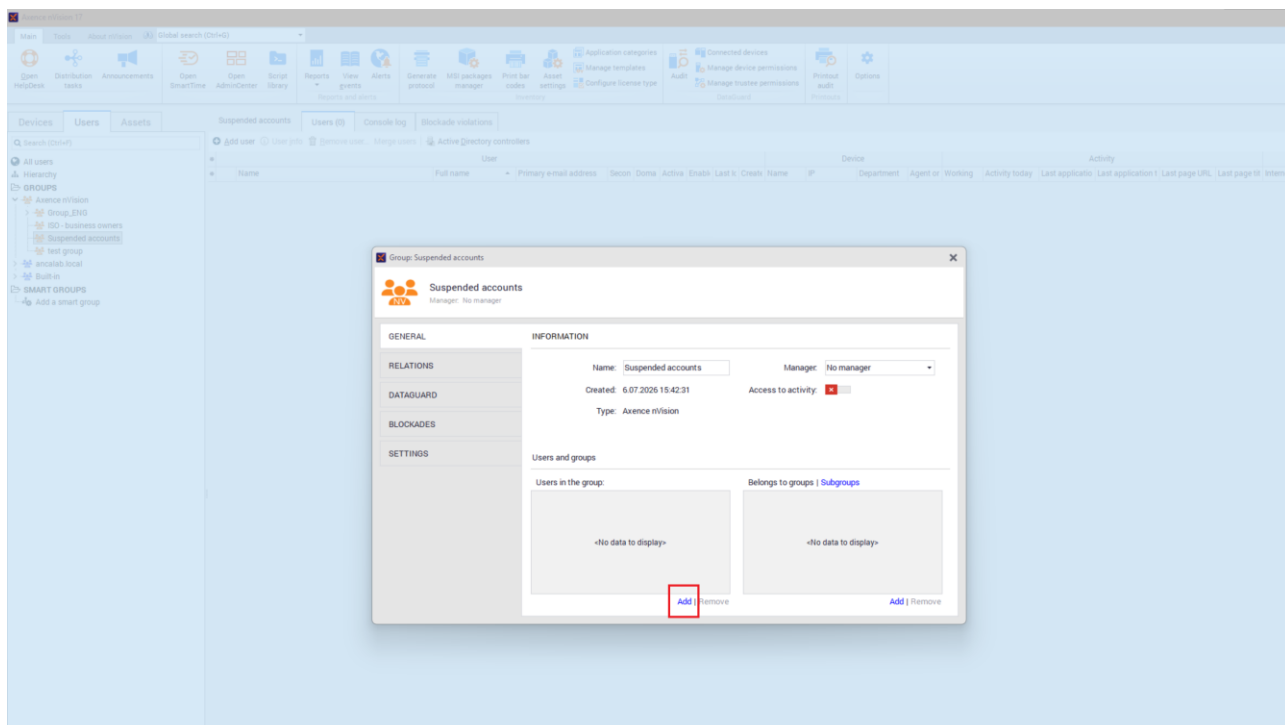
- reduce the risk of unauthorized access,
- prevent abuse and security incidents,
- ensure compliance with regulations (e.g. GDPR) and the ability to audit actions,
- protect the organization's systems, data, and intellectual property

The NIS2 Directive (Article 21(2)(f) and (h)) and the applicable national implementing legislation likewise require the appropriate access control measures, identity management and immediate withdrawal of permissions from users who should not have access to systems.

### 2.5.1 Restricting access in the event of suspended cooperation

When cooperation ends, whether with an employee or a contractor, ensure that their access to all systems is withdrawn. You can make this process easier for yourself by creating a separate group of users to which you can add successive people.



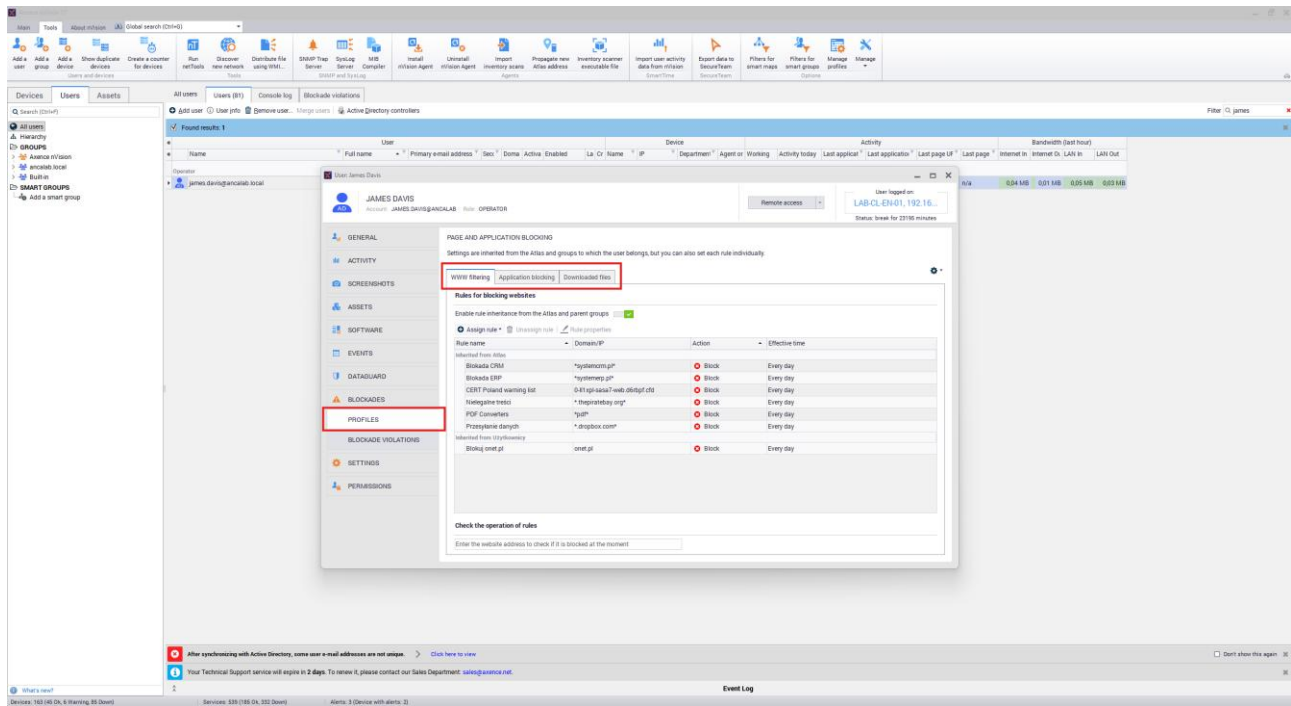


After creating such a group and assigning users to it, you can select the appropriate rules for blocking access to selected applications and websites.

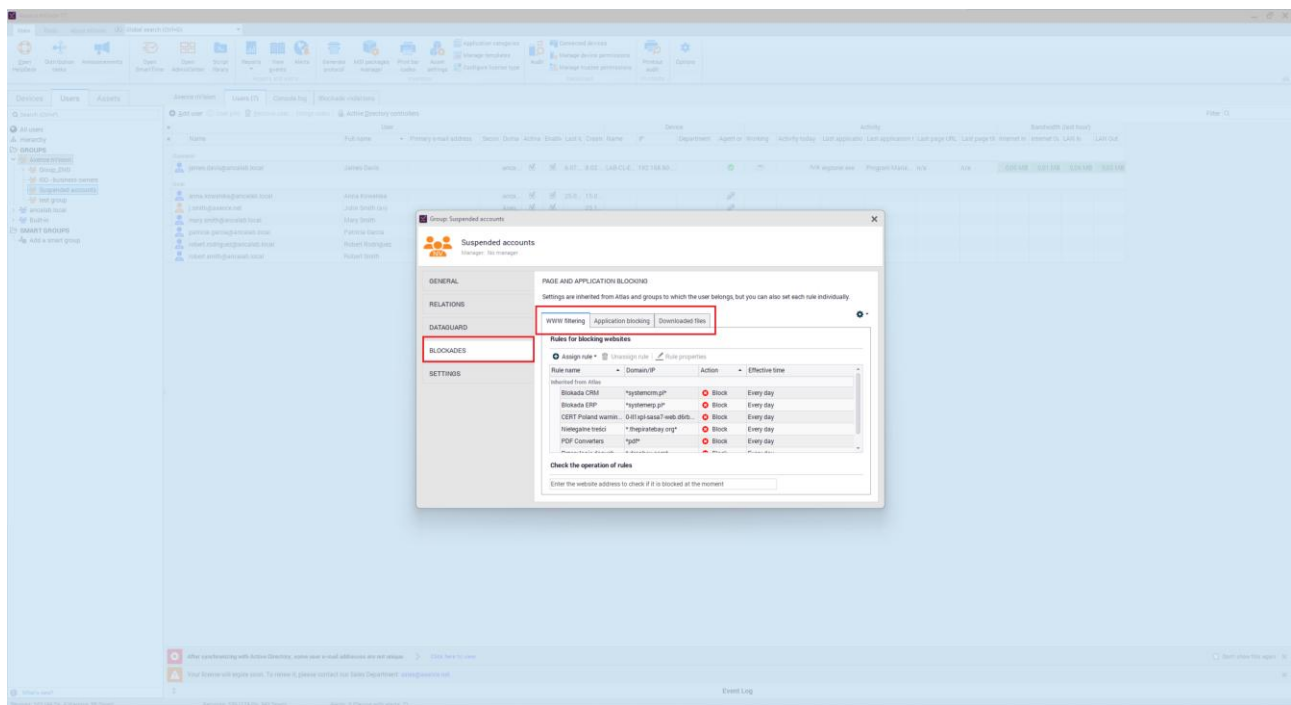
## 2.5.2 Applying blocks to the accounts of deactivated users

Sometimes, it may be necessary to quickly cut users off from all web systems, applications, and even prevent them from downloading files. The Users module can help with this by applying blockades.

Blockades can be created for a specific user, in the **Details** window:

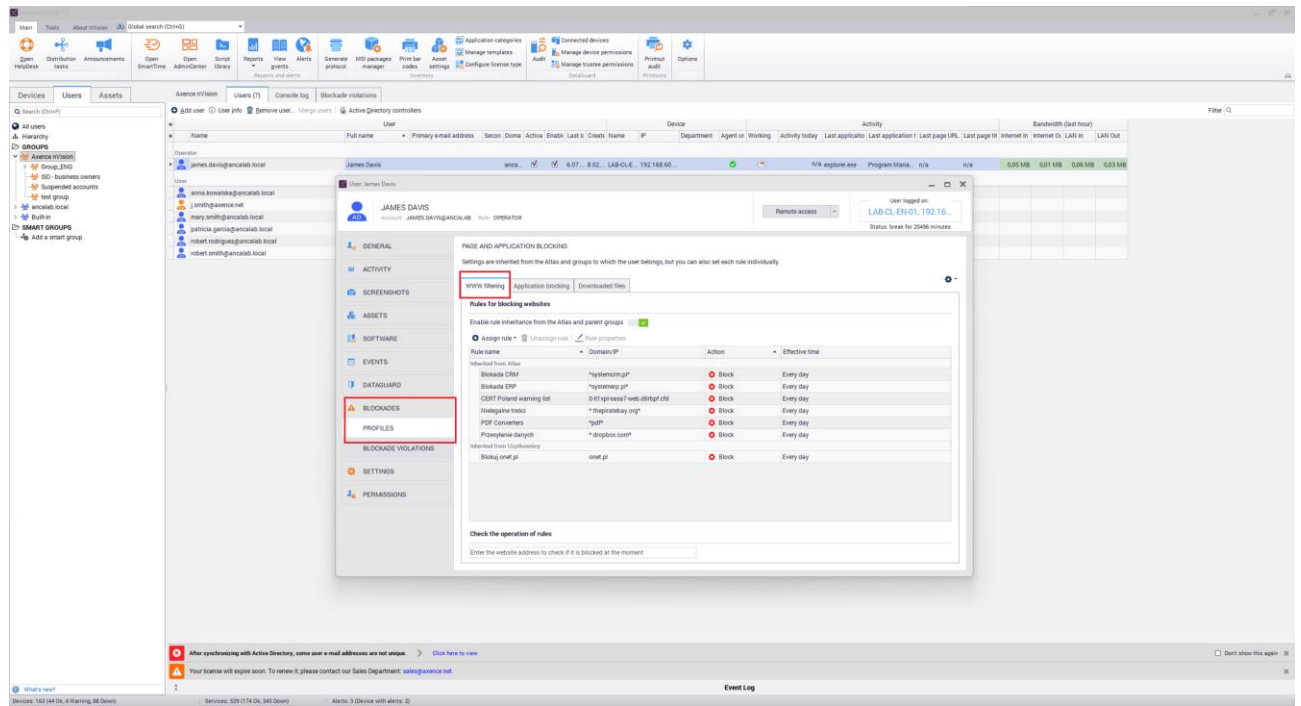


You can also block actions at the group or Atlas level. This is precisely why a group of suspended users is needed.

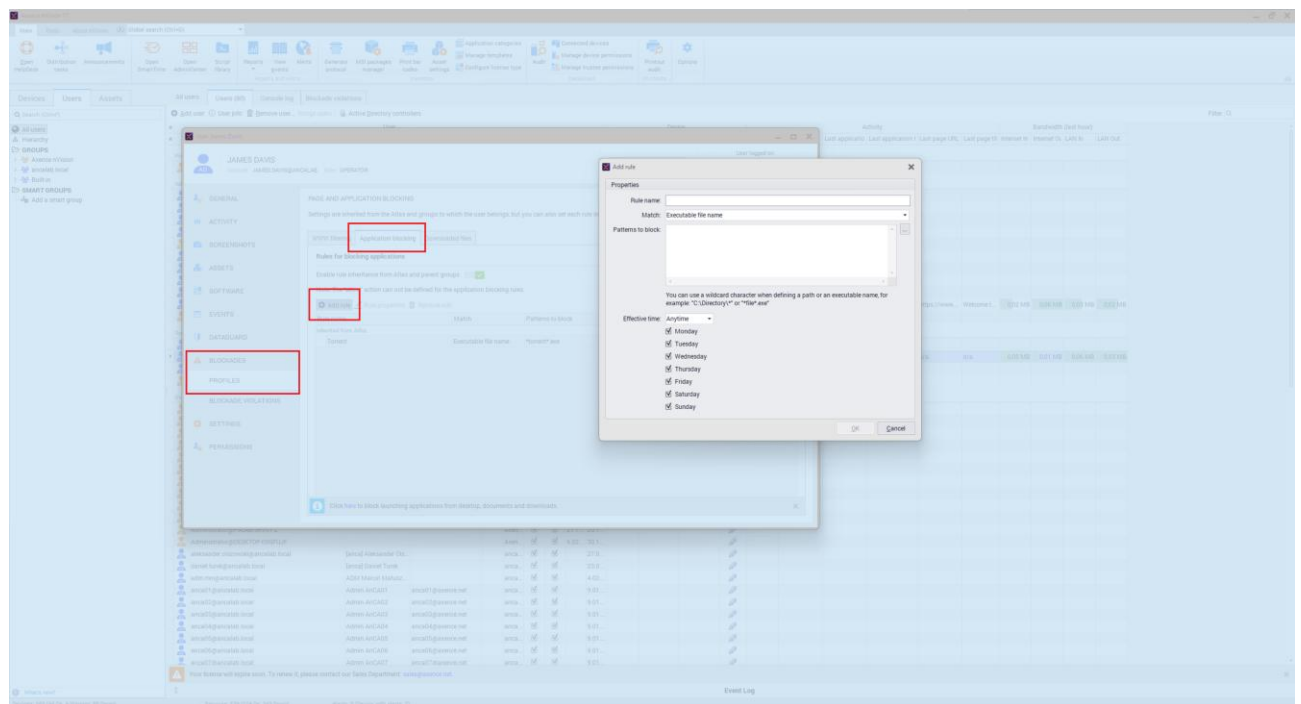


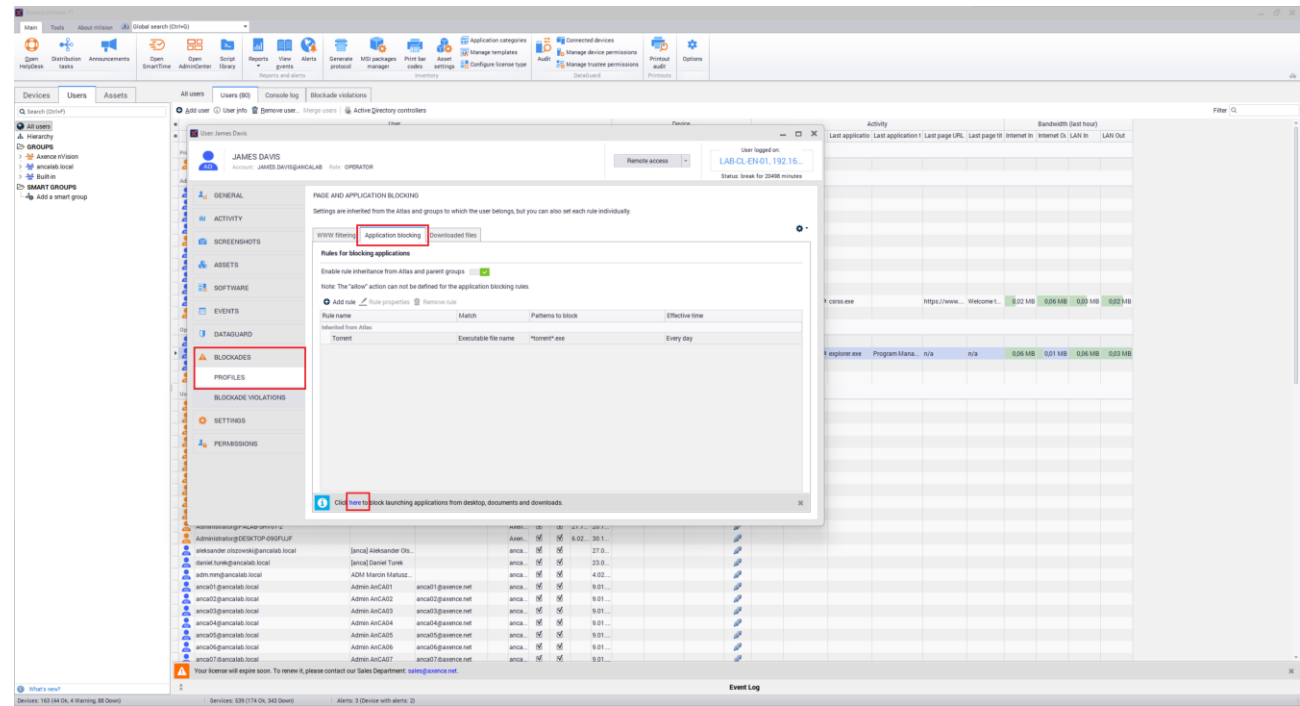
You can block:

- access to websites - selected ones or all of them (you can read more about blocking [here](#))

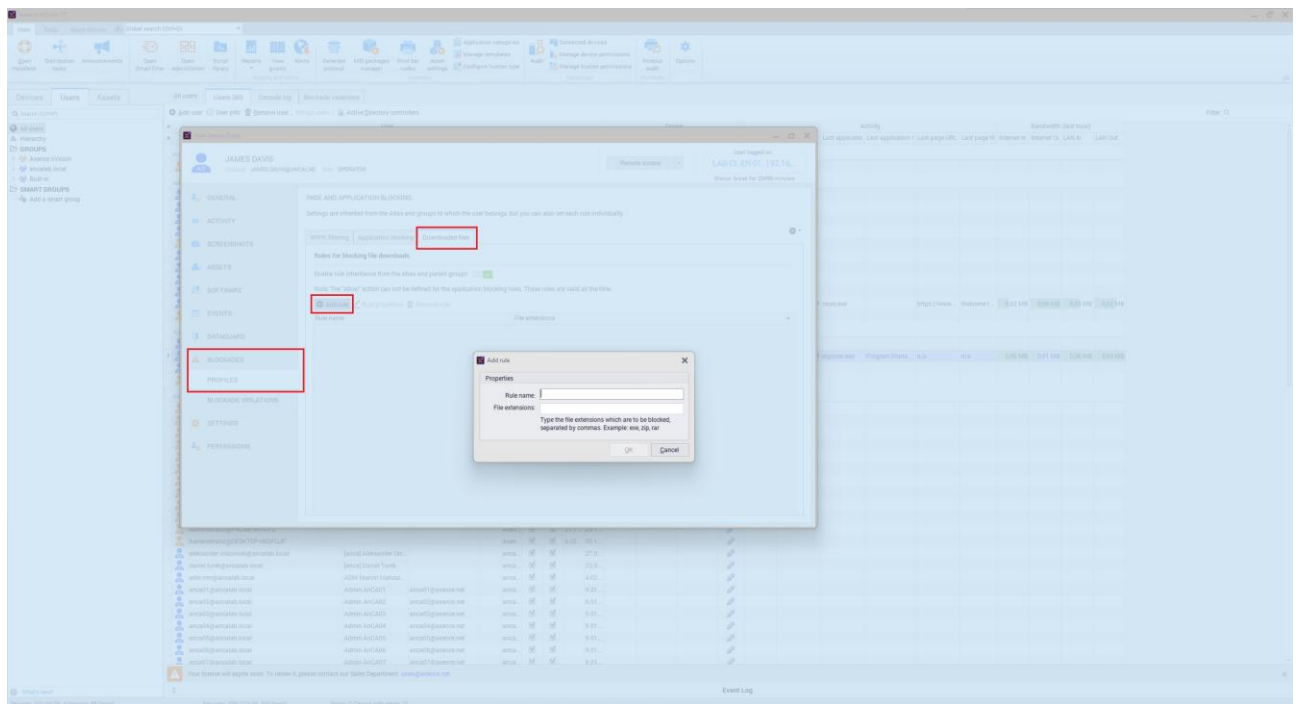


- the ability to launch applications - you can read more about it [here](#)),



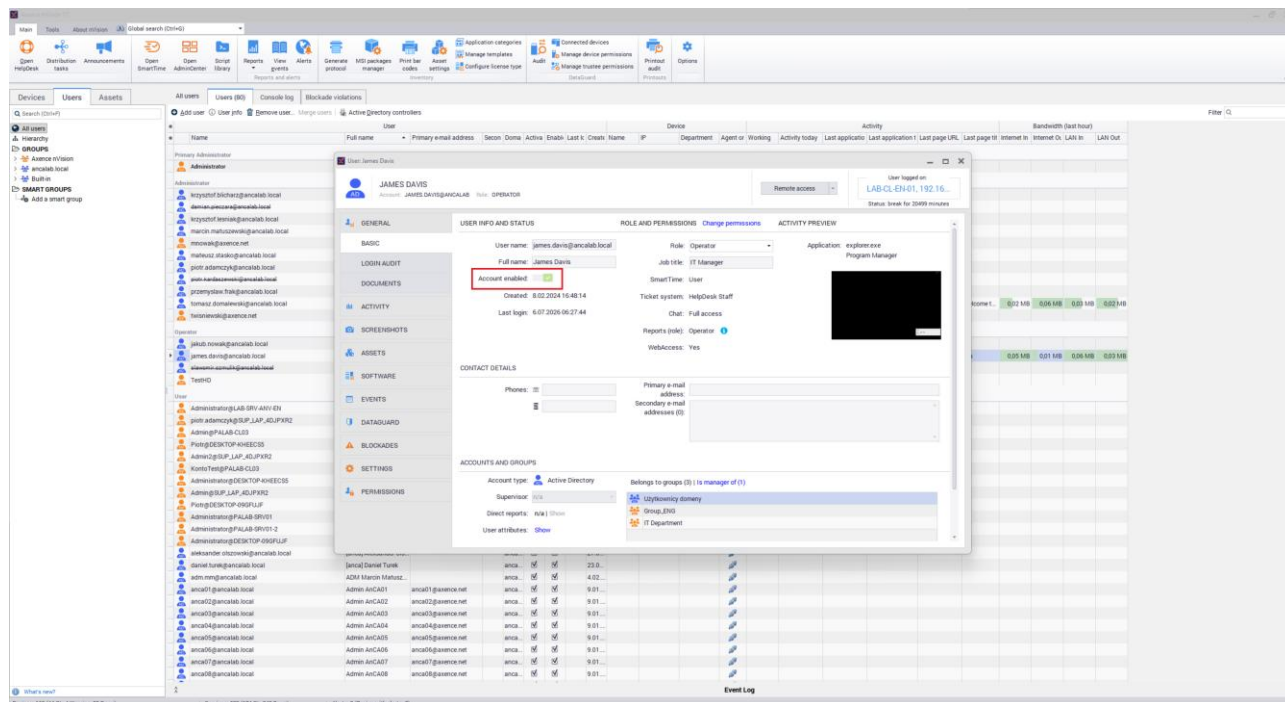


- the ability to download files



## 2.5.3 Disabling the account

Once access has been withdrawn and the user has returned the company hardware, disable the account:

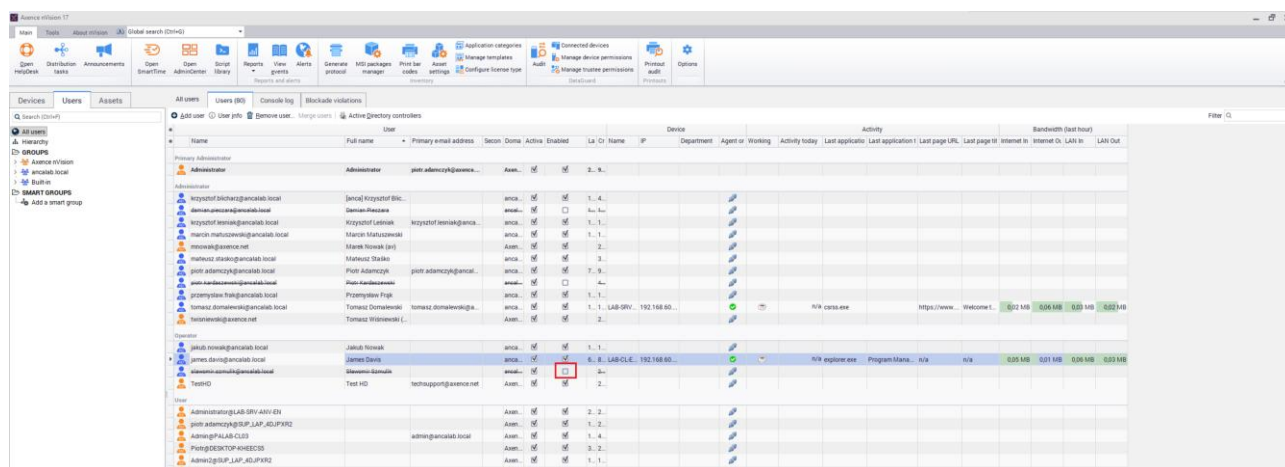


Disabling the account means that the user will lose the ability to:

- log in to the nVision console,
- use the Agent.

A message displayed after flipping the switch will remind you of this.

When you disable the account, the user's view on the list changes:



The data will be displayed in a different color and the checkbox indicating the account status will be empty. This checkbox provides an alternative, quicker way to enable or disable the account.

## 3. Risk analysis for assets

Once the inventory is complete, you have a complete, structured knowledge base about the organization's assets. You already know what to protect and from what. Now, you need to carry out a risk assessment that complies with ISO 27001, NIS2 and the applicable national implementing legislation requirements.

Both standards require you to make security decisions based on a documented analysis. According to ISO 27001, the risk assessment must be reliable and repeatable and focus on protecting the confidentiality, integrity and availability of information. NIS2 and the applicable national implementing legislation extend this perspective with the need to consider all types of threats, including environmental and operational ones, as well as those resulting from supplier dependencies.

Risk, within the meaning of **ISO 27001**, is a **combination of the likelihood of a threat occurring and the consequences** that the materialization of the threat may have for the confidentiality, integrity or availability of information. NIS2 broadens the context: from threats to confidentiality, integrity or availability to all threats that may affect **networks, information systems and the continuity of essential services**, in line with the all-hazards approach (the full spectrum of threats, considering the entire environment in which the organization operates). The same applies under the applicable national implementing legislation.

Your risk analysis will be based on a process key to adapting the organization to the requirements: the systematic identification of threats and existing security controls for each asset. This step will allow you to identify the risks associated with particular systems, devices or information and determine which protective mechanisms are already in place and where gaps exist.

**Remember that the examples we cite are not exhaustive.** Every organization is unique and embedded in its own context. Familiarize yourself with the examples and proposals we provide and then use them as a basis for the development of your own solutions.

### 3.1 Introduction to threats and security controls in nVision

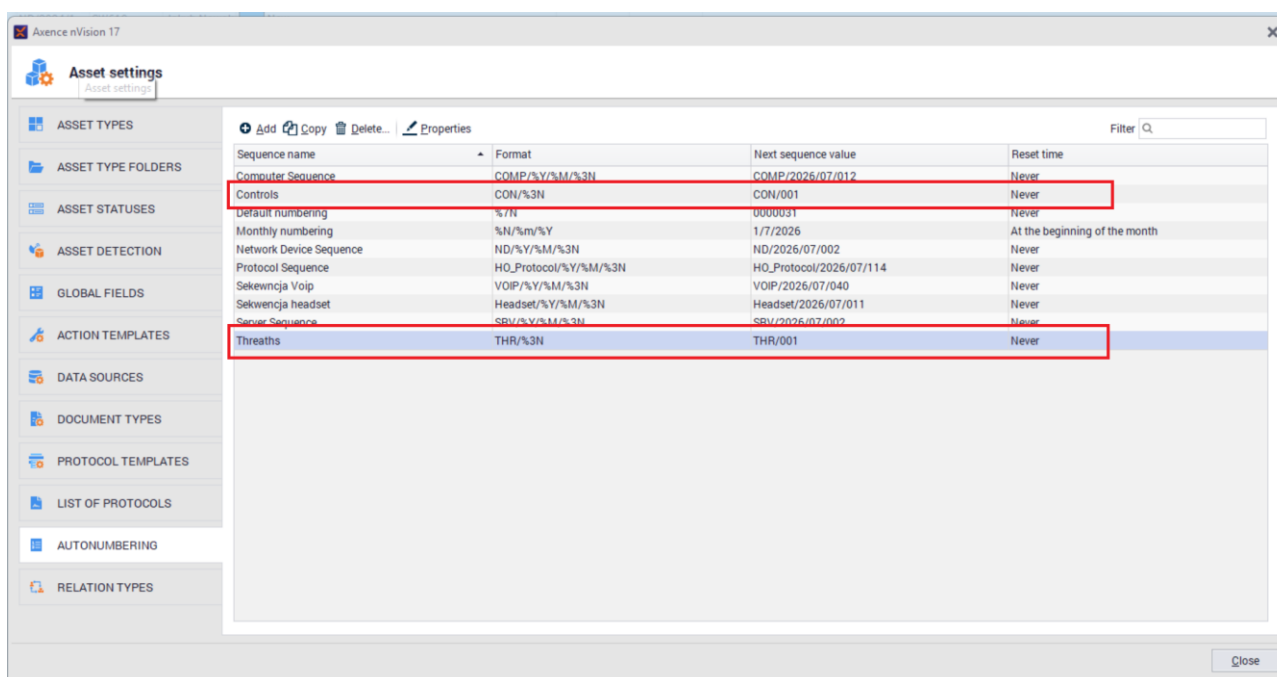
A **threat** is **any potential event** that may **exploit a vulnerability in an asset**, compromising its **confidentiality, integrity or availability**. A security control, in turn, is a **technical, procedural or organizational measure** that reduces risk to an acceptable level<sup>7</sup>.

<sup>7</sup> This is a perspective based on ISO 27001. NIS2 broadens the scope of threats to include nearly the entire environment surrounding of the organization, while narrowing the concept of security to cybersecurity risk management measures.

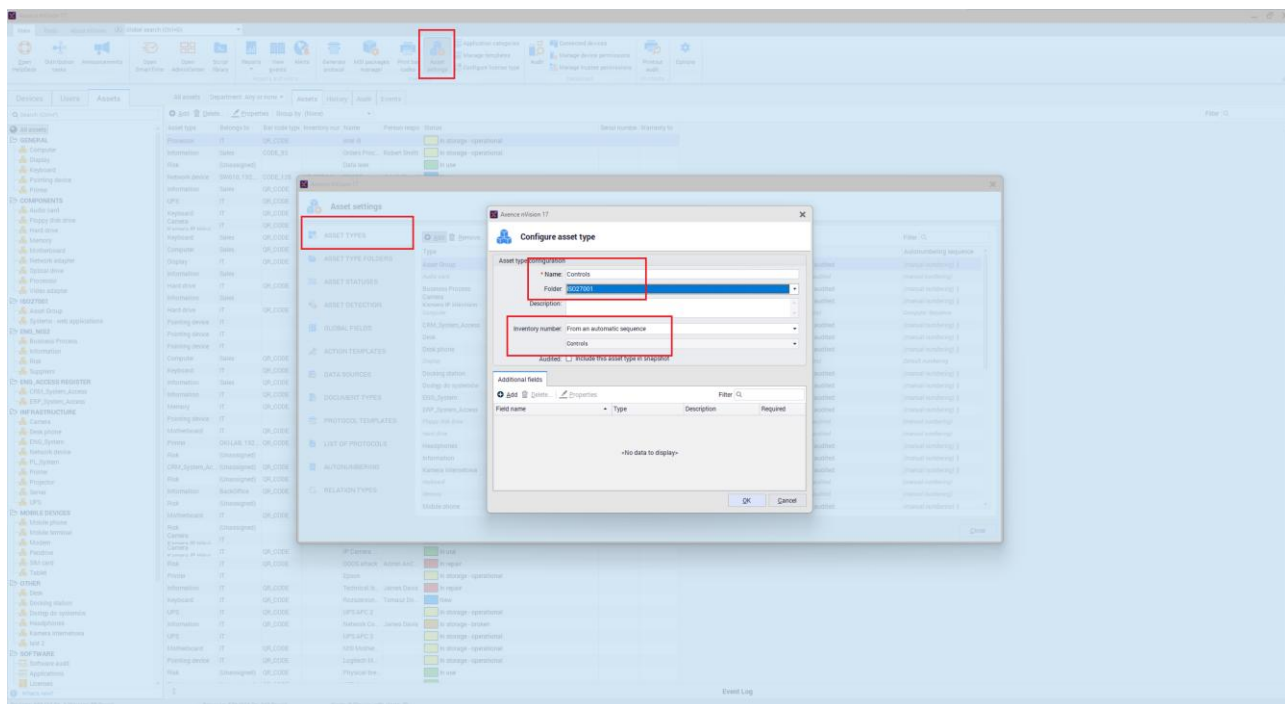
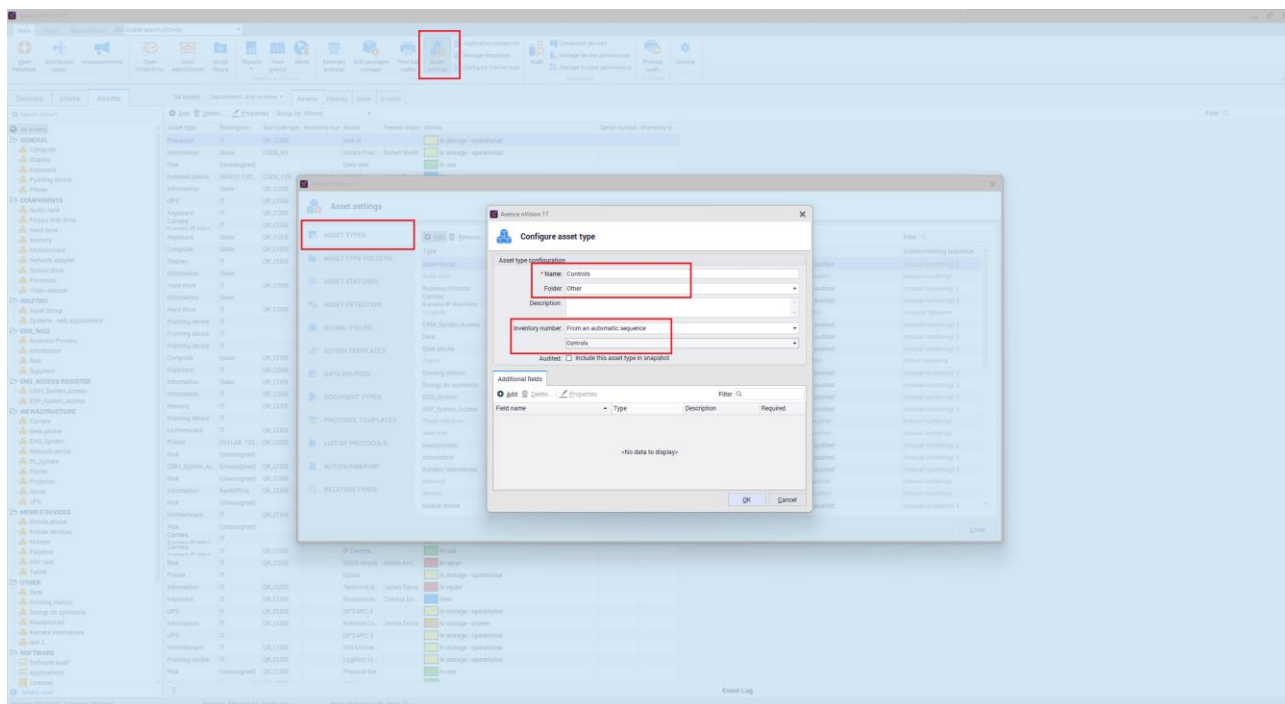
Assigning threats and security controls to inventoried assets forms the basis for the subsequent risk assessment, so you need tools that will make this assignment possible, such as asset types and relations.

### 3.1.1 Threats and security controls – creating asset types

You can create the asset types in the **Asset settings** window. As [with information assets](#), start by adding an [autonumbering sequence](#):



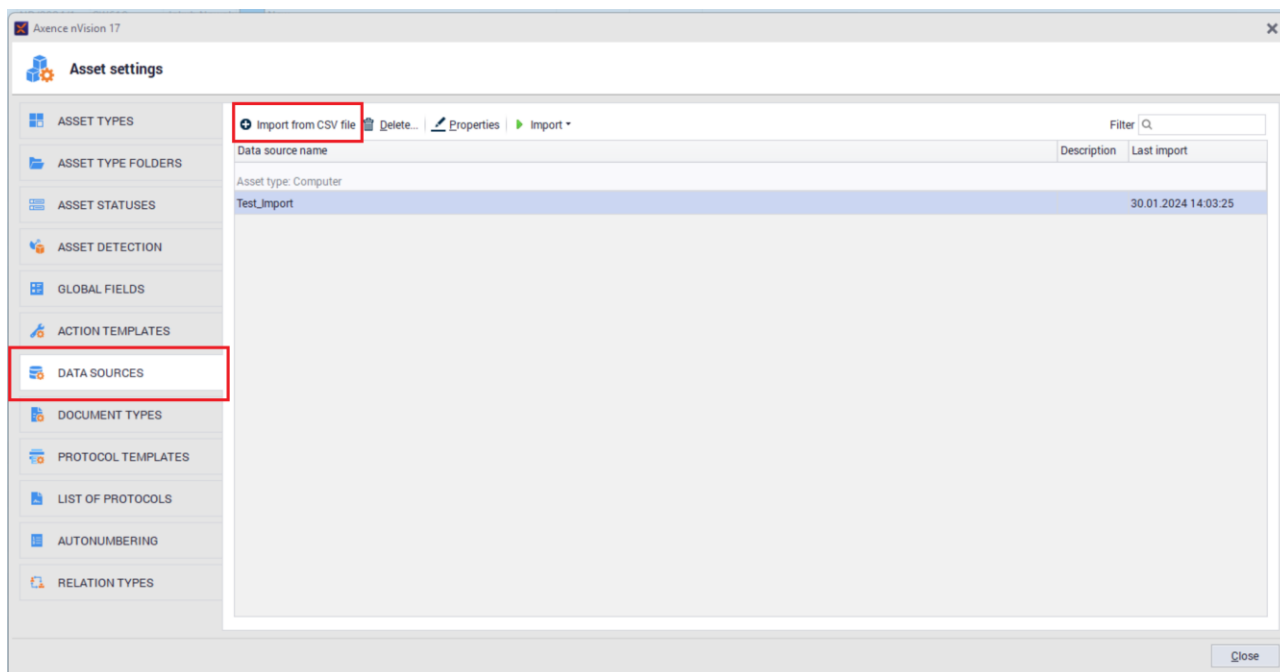
Then move to the **Asset types** tab, where you can add a type for security controls and one for threats. For both types, set the inventory number to autonumbering and select the appropriate sequence. The folder can be any one you like, but it will be convenient to keep all the asset types related to the implementation of the standards in one place.



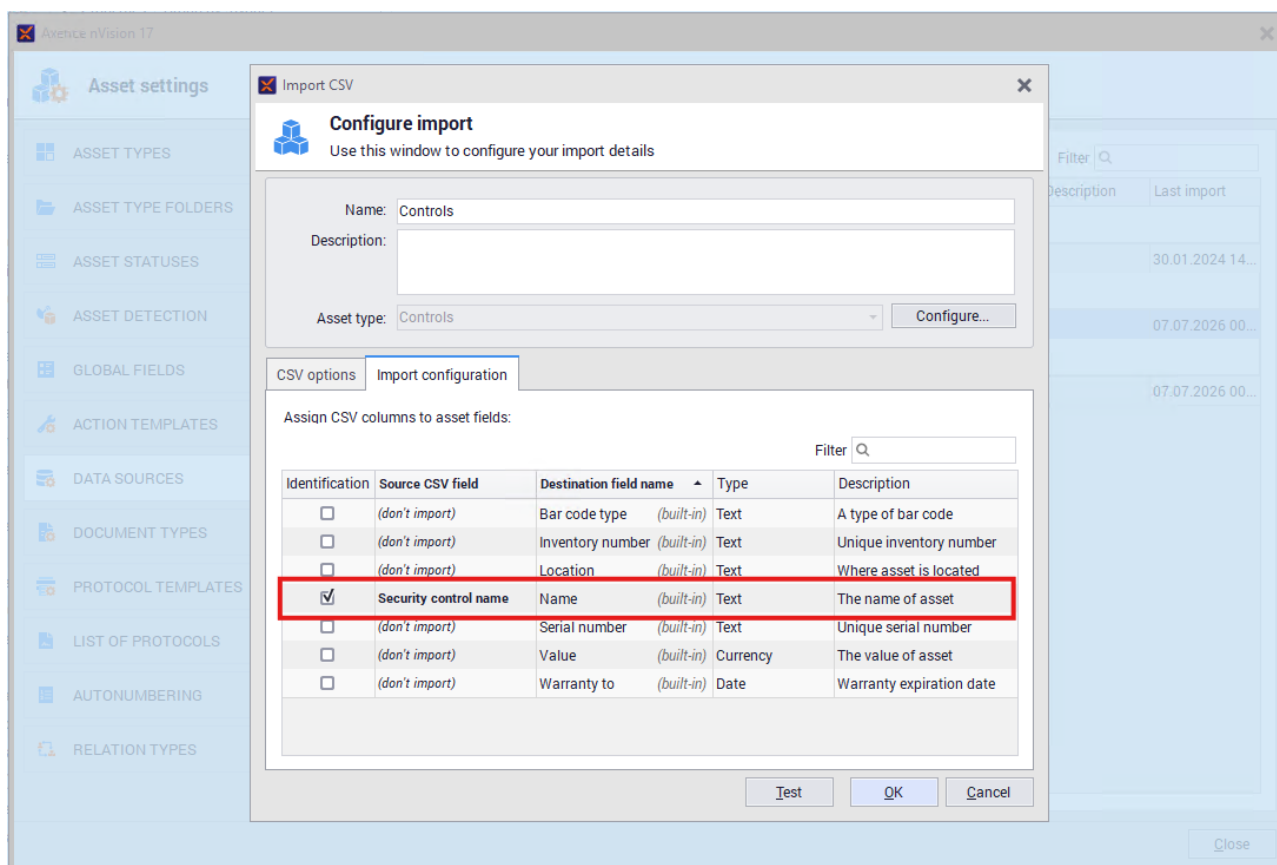
### 3.1.2 Importing threats and security controls

Access to the nVision system also means access to regularly updated CSV files containing lists of threats and security controls. You can find these CSV files on the **Legal regulations** page, accessible from the main navigation ribbon in nVision.

In **Asset settings** on the **Data sources** tab, an option to import from a CSV file is available. Use it, following the instructions in the [documentation](#).



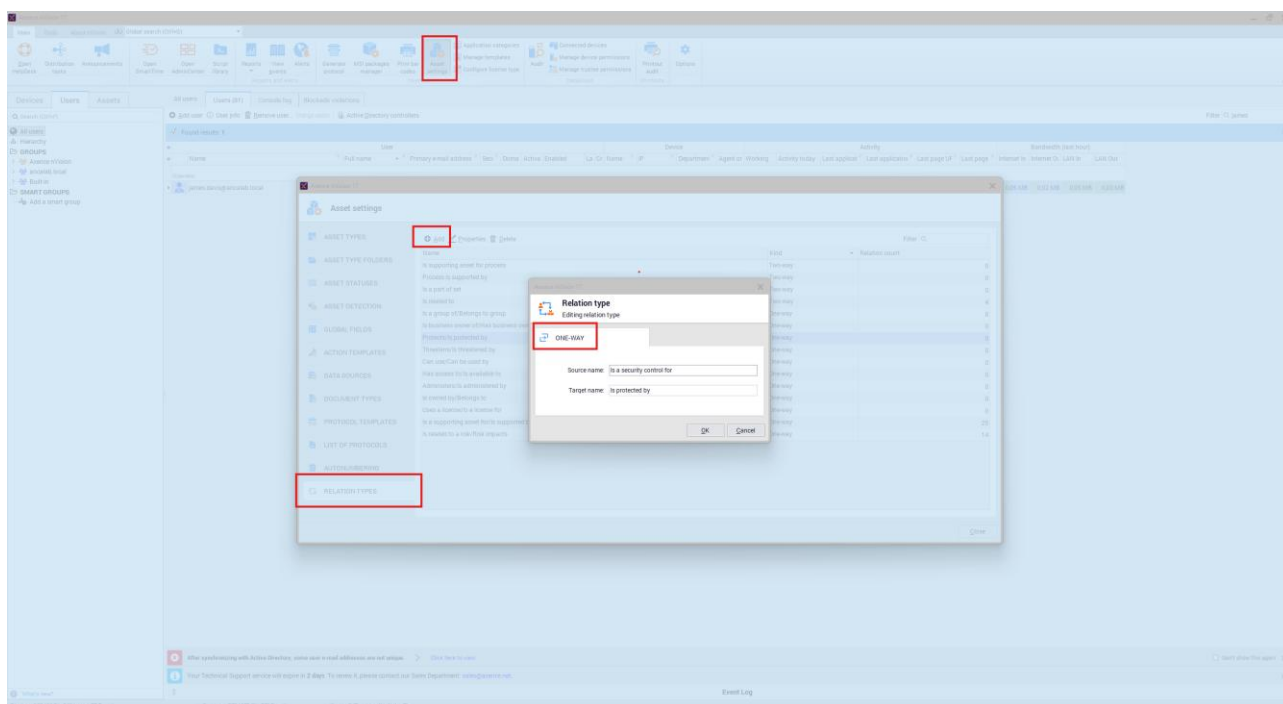
During the import process, select the asset name as the identifying field (unique for each asset). Remember to map the name of the threat/security control to the **Asset Name** field.



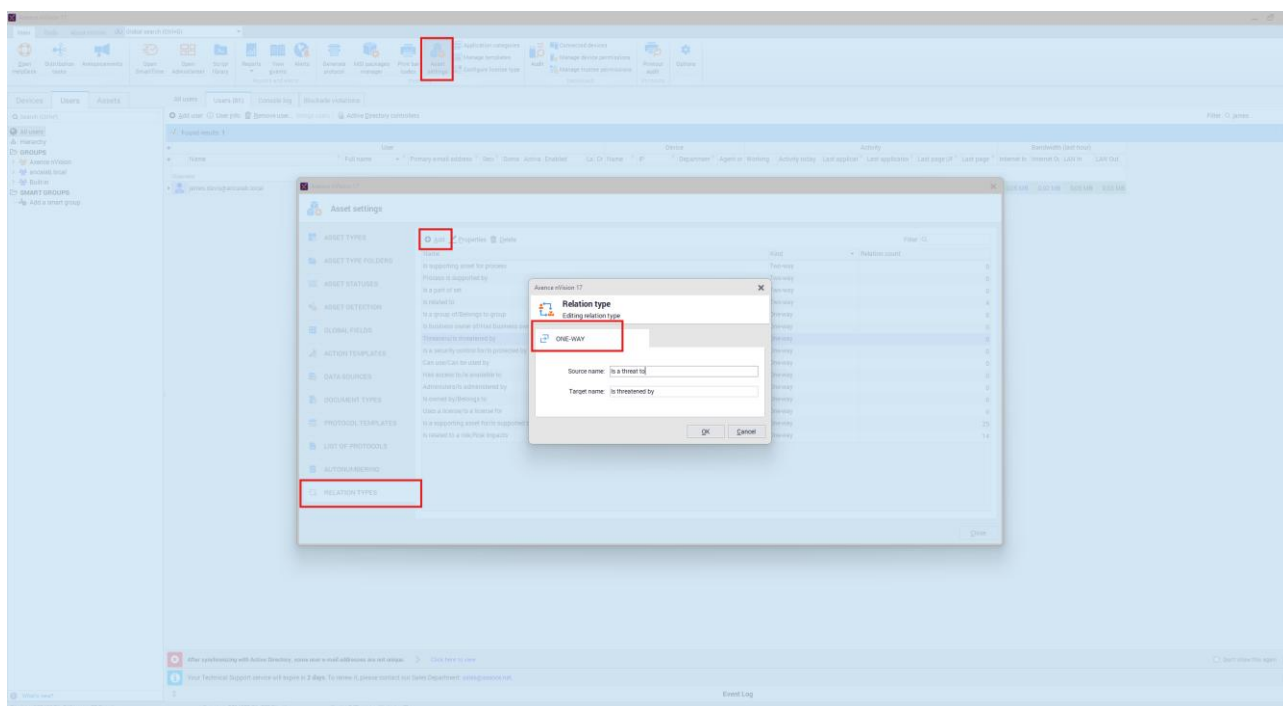
### 3.1.3 Creating relations

To link assets with threats and security controls, you need additional relation types. On the **Relation types** tab in **Asset settings**, add two one-directional relations:

- **Is a security control for / Is protected by:**



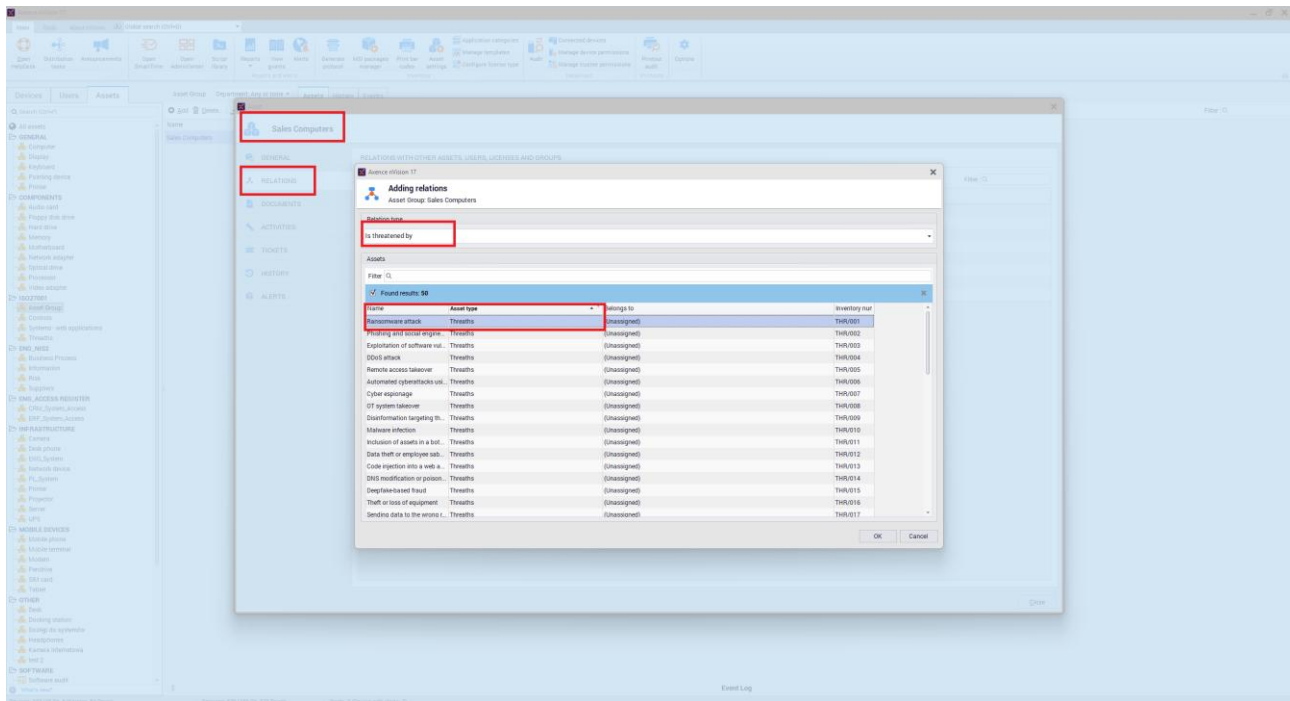
- Is a threat to / Is threatened by:



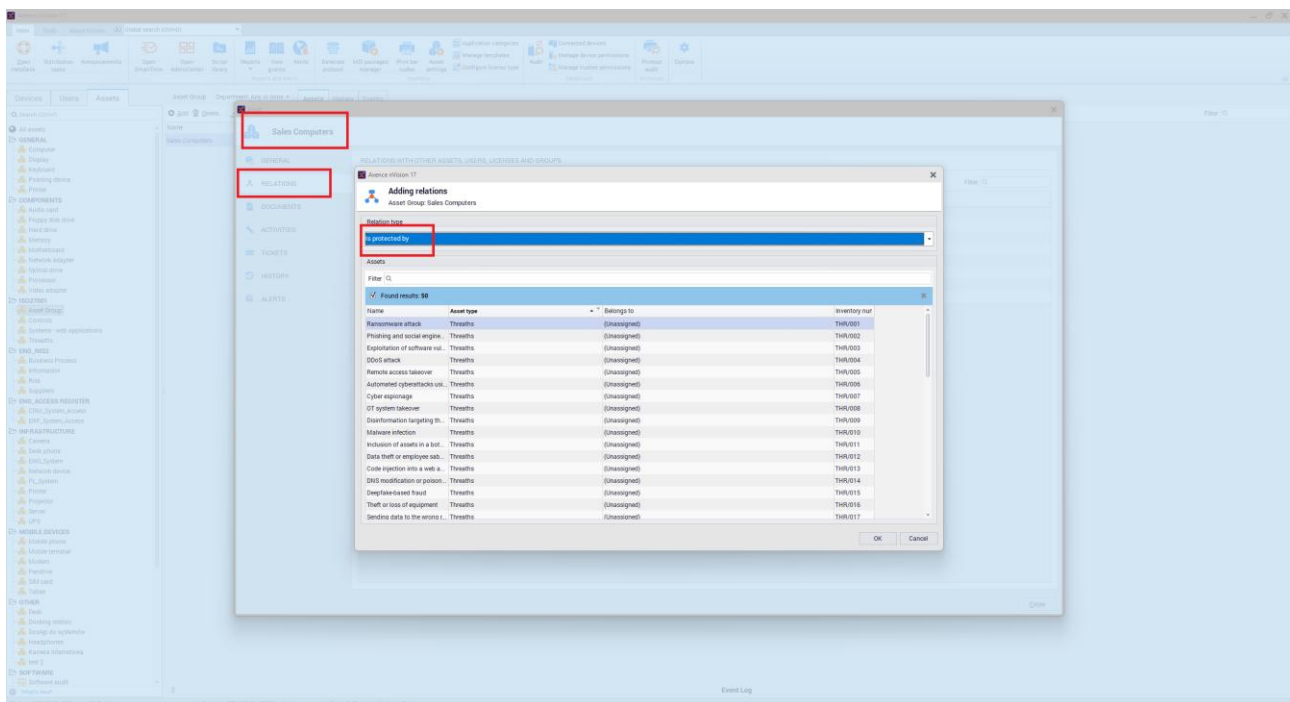
## 3.2 Linking threats and security controls to assets (6.1.2, A.8.8)

Assign each of the imported information threats and security controls to selected assets. Usually, you will assign them to a whole group of assets.

For example, you have a **data-encrypting software attack** (ransomware) among the threats, which you will assign to the **Sales computers** group:

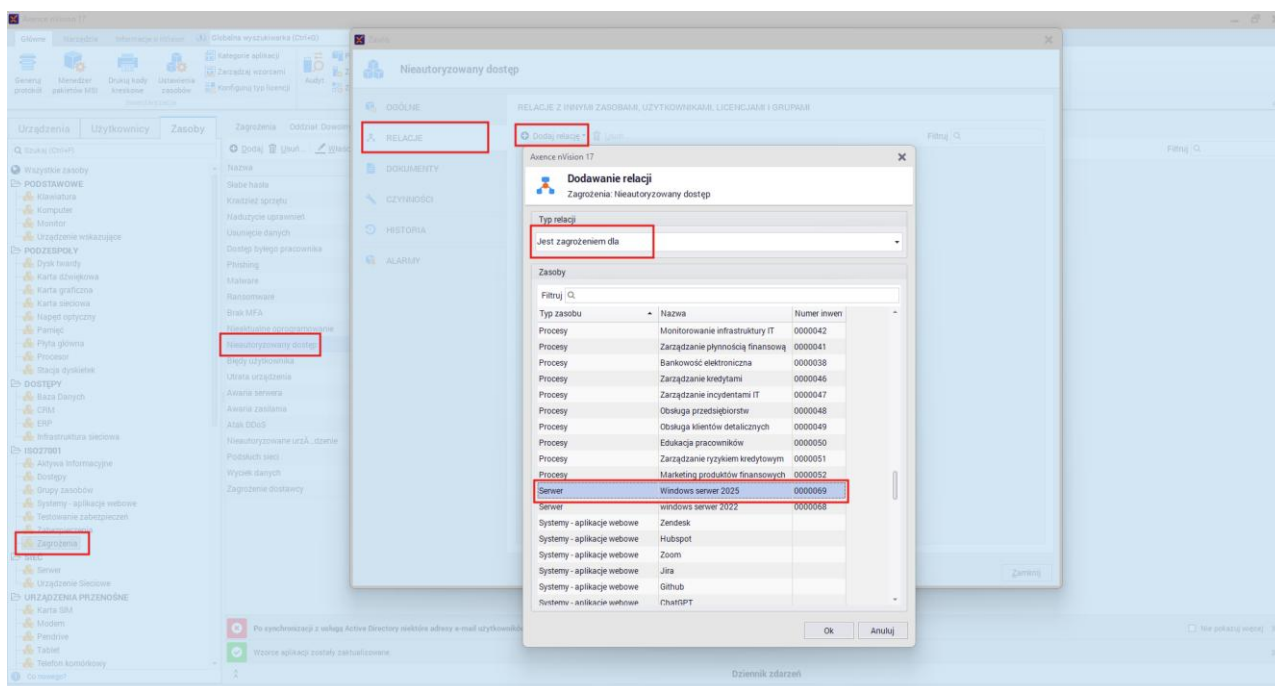


Add security controls to the same group:



In particular cases, you can also add threats or security controls at the level of individual assets.

For example, a threat to an individual server may be a physical intrusion by an unauthorized person into a protected zone:



The security controls and threats will be visible on the **Relations** tab of a given asset or group of assets – and vice versa, the asset will be visible on the **Relations** tab of a given threat or security control.

### 3.3 Conducting and digitizing the risk assessment (6.1.2)

To assess the risk level, use the ENISA risk matrix. It provides a consistent, practical and regulatorily accepted method of estimating the impact and likelihood of threats.

This matrix provides an organized way to estimate risk based on threat scenarios. It is based on two axes: likelihood (how frequent / how realistic is the occurrence of the threat?) and impact (what consequences will the occurrence of the threat have?). The risk level is calculated at the intersection of these axes using the following formula:

$$\text{risk} = \text{likelihood} \times \text{impact}$$

#### 3.3.1 Estimating the risk level

Analyze the risk scenarios for successive assets or groups of assets, using the formula **If threat X affects asset Y, then consequence Z will occur**. Assess:

- the **impact** of the materialized risk (in accordance with the National Cybersecurity System, many factors must be considered, e.g. the possible harm to users of the services),
- the **likelihood** of the event occurring,

taking into account the threats and security controls assigned to them (by means of the previously defined relations).

|            |                    | Impact     |             |                                     |                                |                 |
|------------|--------------------|------------|-------------|-------------------------------------|--------------------------------|-----------------|
|            |                    | 1          | 2           | 3                                   | 4                              | 5               |
|            |                    | negligible | short-lived | significant hindrance to operations | serious disruption of services | critical impact |
| Likelihood | 5<br>very likely   | 5          | 10          | 15                                  | 20                             | 25              |
|            | 4<br>likely        | 4          | 8           | 12                                  | 16                             | 20              |
|            | 3<br>possible      | 3          | 6           | 9                                   | 12                             | 15              |
|            | 2<br>unlikely      | 2          | 4           | 6                                   | 8                              | 10              |
|            | 1<br>very unlikely | 1          | 2           | 3                                   | 4                              | 5               |

You still need to determine how to interpret the results, as the interpretation depends on the arrangements within the organization. For example:

| Risk         | Interpretation (defined by organization) |
|--------------|------------------------------------------|
| <b>16-25</b> | unacceptable risk                        |
| <b>11-15</b> | action required                          |
| <b>6-10</b>  | monitoring required                      |
| <b>1-5</b>   | acceptable risk                          |

Single out and estimate the risk for each asset / group of assets, taking into account the possible scenarios. Since you will be determining a generalized risk level for a specific asset in the next step, it will be helpful to briefly describe the scenario cases in the **Notes** field in the asset window:

**HP computer**

**GENERAL**

**BASIC INFORMATION**

\* Name: HP computer

Asset type: Computer Configure

Belongs to: Sales

Person responsible: Tomasz Domalewski (tomasz.domalewski@ancalab.local) Transfer

Status: In use

Serial number: 6807B01420

Inventory number: COMP/2024/01/010

Bar code: QR\_CODE Share

Notes:

**ADDITIONAL FIELDS**

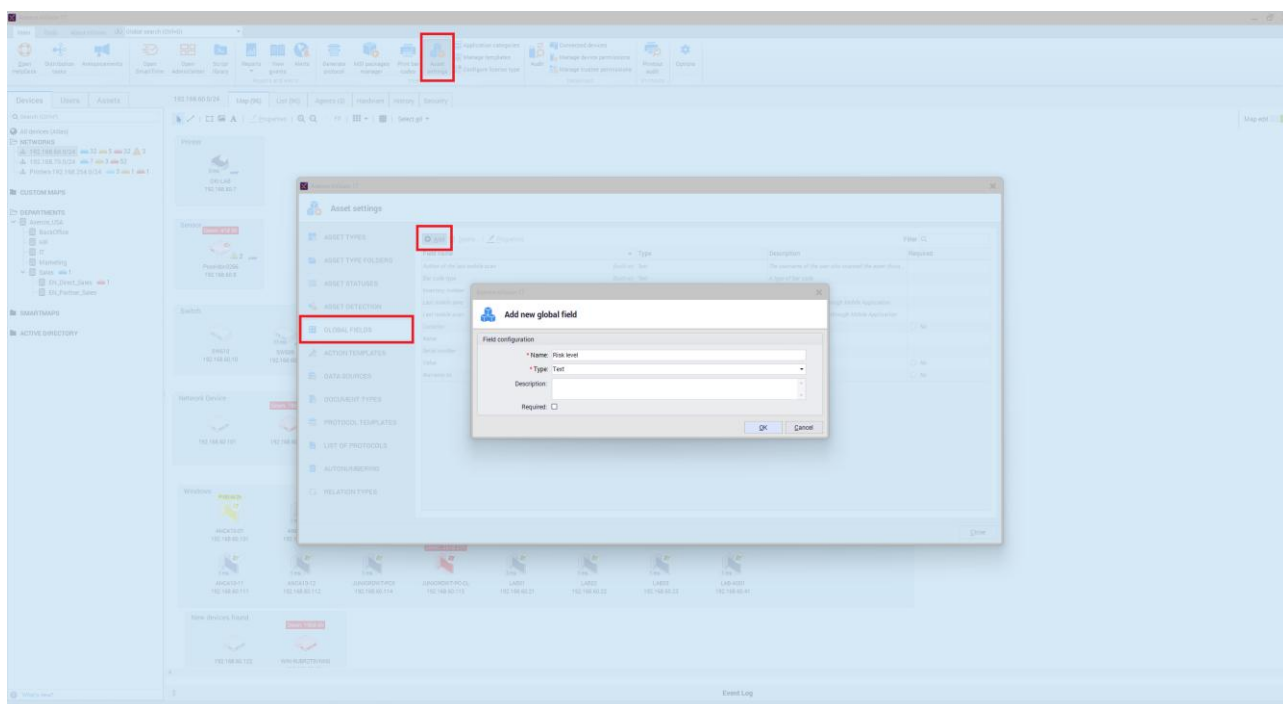
| Name                           | Value             |
|--------------------------------|-------------------|
| Specific asset type fields     |                   |
| Description                    |                   |
| Info 1                         |                   |
| Info 2                         |                   |
| Manufacturer                   | Asus              |
| Model                          | Model 218         |
| Original username              |                   |
| OS type                        |                   |
| Global fields                  |                   |
| Author of the last mobile scan |                   |
| Inventory number               | COMP/2024/01/010  |
| Last mobile save               |                   |
| Last mobile scan               |                   |
| Location                       |                   |
| Name                           | HP computer       |
| Person responsible             | Tomasz Domalewski |
| Serial number                  | 6807B01420        |

Close

This will allow you to return to the analysis stage at any time, whether to verify its correctness or to carry out the process again.

### 3.3.2 Adding a global field

Based on the analyzed scenarios and the risks calculated for them, you can assign a general risk level to each asset (low, medium, high or others, in accordance with the arrangements within the organization). Save this value in the **Risk level** field, which you will add as a global field.



The global field will appear in all asset types. Besides allowing you to record the general risk for an asset, it will also enable you to filter the asset list by this field. You can find more information about adding global fields [here](#).

## 4. Selection and implementation of security controls (6.1.3)

Selection of security controls means selecting **appropriate security measures** that reduce this risk to an **acceptable level based on** the identified **threats** and **vulnerabilities**, as well as the risk assessment carried out.

### 4.1 Implementation of appropriate security controls

After selecting the security controls, you can proceed to their implementation by:

- describing them (this is how policies and procedures are created),
- actual application,
- monitoring,
- improving.

In the context of ISO 27001 (and likewise the applicable national implementing legislation), applying and monitoring the implementation of security measures with respect to assets is key. Therefore, you need a way to reflect and confirm the actual use of a security control in nVision. For this, you can use the HelpDesk module.

First, create a form that will allow you to link assets to a ticket:

Save it, and then create the **Security control implementations** category based on this form. You may consider allowing only a specific group of users to create tickets in this category.

Based on the results of the previously conducted risk assessment, for each asset (or group of assets):

- identify the missing security controls (if necessary),
- for each of these security controls, create a new ticket in the **Security control implementations** category,
- if you wish, assign an asset (or group of assets) to it,
- document the security control implementation process using comments on the ticket (from the perspective of ISO 27001, performing a given task and retaining proof of its completion are both essential),
- add the implemented security control to the list of all assets,
- using a relation, assign the security control to the asset (or group of assets) from the ticket.

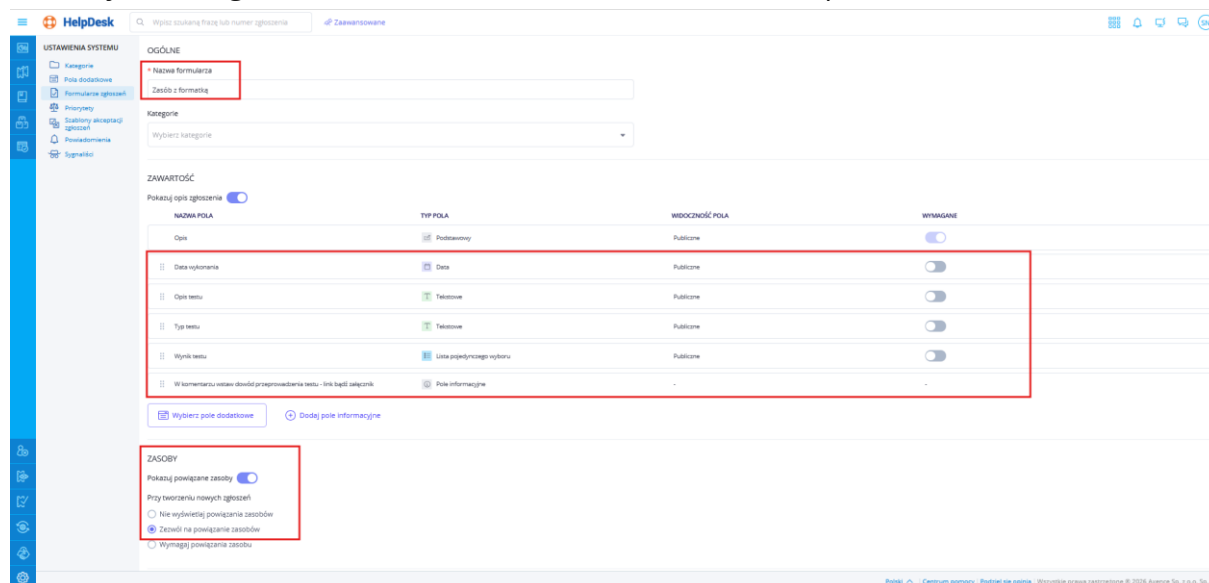
## 4.2 Testing security controls

Testing the implemented security controls involves checking whether the existing and newly implemented security controls are functioning properly. Tests close the risk loop by confirming the effectiveness of the security controls or revealing gaps in them.

A very important element here is the proper documentation of the tests carried out – this is a requirement of both ISO 27001 and NIS2, as well as the applicable national implementing legislation. Particular emphasis should be placed on the scope of the test, the date it was carried out (and any frequency), the results, any non-conformities and corrective actions.

The requirement to document security control tests can be fulfilled in a manner similar to the security control implementation process itself, i.e. by using tickets in the HelpDesk module.

Start by creating a new form (additional fields will be required, so add them beforehand):



**HelpDesk** Wpisz szukany frazę lub numer zgłoszenia Zaloguj się

**USTAWIENIA SYSTEMU**

- Kategorie
- Pola dodatkowe
- Formularze zgłoszeń
- Pracownicy
- Systemy obsługi zgłoszeń
- Powiadomienia
- Logowanie

**OGÓLNE**

Nazwa formularza:

Kategorie:

**ZAWARTOŚĆ**

Pokaż opis zgłoszenia ☐

| NAZWA POLA                                                            | TYP POLA                                                      | WIDOCZNOŚĆ POLA | WYMAGANE                            |
|-----------------------------------------------------------------------|---------------------------------------------------------------|-----------------|-------------------------------------|
| Opis                                                                  | <input checked="" type="checkbox"/> Podstawowy                | Publiczne       | <input checked="" type="checkbox"/> |
| Data wykonania                                                        | <input checked="" type="checkbox"/> Data                      | Publiczne       | <input checked="" type="checkbox"/> |
| Opis testu                                                            | <input checked="" type="checkbox"/> Tekstowe                  | Publiczne       | <input checked="" type="checkbox"/> |
| Typ testu                                                             | <input checked="" type="checkbox"/> Tekstowe                  | Publiczne       | <input checked="" type="checkbox"/> |
| Wynik testu                                                           | <input checked="" type="checkbox"/> Lista poprzedniego wyniku | Publiczne       | <input checked="" type="checkbox"/> |
| W komentarzu zostaw dowód przeprowadzenia testu - link bądź załącznik | <input checked="" type="checkbox"/> Pole informacyjne         | -               | -                                   |

[Wybierz pole dodatkowe](#) [Dodaj pole informacyjne](#)

**ZASOBY**

Pokaż powiązane zasoby ☒

Przy tworzeniu nowych zgłoszeń

☐ Nie wyświetlaj powiązania zasobów

☒ Zezwól na powiązanie zasobów

☐ Wymuś powiązanie zasobów

Publicznie Centrum pomocy Podziel się opinią Wyciekła prawa zastrzeżenie © 2024 Axence Sp. z o.o. Sp. z o.o.

These additional fields will be used to record the course and results of the security control test:

- the date the test was performed,
- the type of test,
- the test result (success / failure),
- a description of the test,
- an informational field to recommend attaching proof (an attachment / link) in a comment.

Then create another ticket category: **Security control testing**. This category will be based on the added form.

## 4.2.1 One-off tests

For one-off tests (as opposed to recurring ones), create a new ticket in the **Security control testing** category for each one:

If you wish, assign an asset (or group of assets) to the ticket. This will give each asset its own security control testing history. Assign a person responsible for documenting the security control testing process using additional fields and comments (from the perspective of ISO 27001, performing a given task and retaining proof of its completion are both essential).

It is worth informing the people who deal with security control testing that tasks concerning security control tests have been added. Inform them of the need to perform a given task and the timeframe for doing so using the [announcement mechanism in nVision](#).

### Example announcement:

**Subject:** Backup test – action required

**Content:** We would like to inform you that, in accordance with the applicable security procedures, a backup test of the assigned system must be performed.

A task concerning the performance of this test has been assigned to you in the HelpDesk system.

 **Deadline:** 3 days from receiving this announcement. After performing the test, complete the ticket in the required form and add appropriate proof of completion.

 Please confirm that you have read this announcement. In case of questions or problems, please contact the system administrator.

## 4.2.2 Recurring notifications

For tests performed on a recurring basis, it is worth ensuring a notification system that will make it possible to automatically create tickets in the **Security control testing** category, which the Administrator will then assign to the appropriate testing personnel.

First, create a new asset type: **[Reminders] Security control testing**. The additional fields you need are:

- **reminder time** – the date of the next reminder
- **interval** – how often the reminder is to be set

Axence nVision 17

### Configure asset type

Asset type configuration

\* Name: [Reminders] Security controls testing

Folder: SO27001

Description:

Inventory number: Entered manually

Audited: ☐ Include this asset type in snapshot

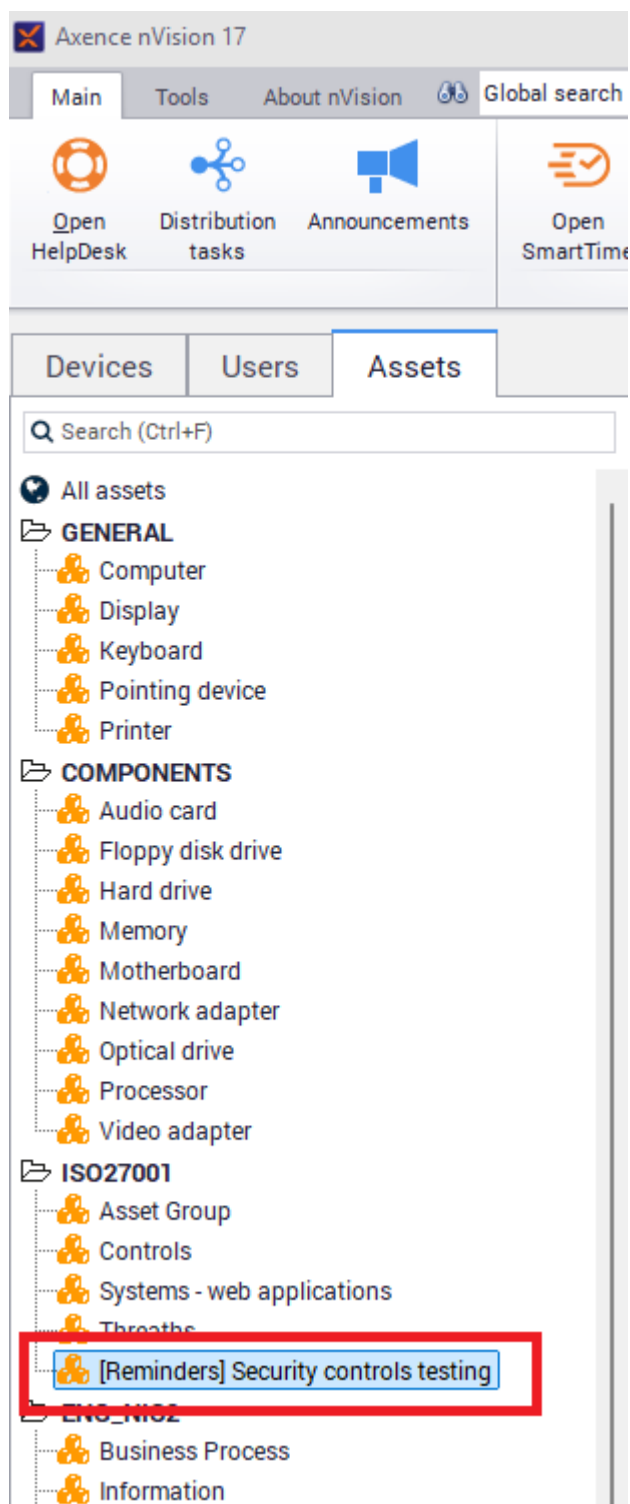
Additional fields

+ Add Delete... Properties Filter

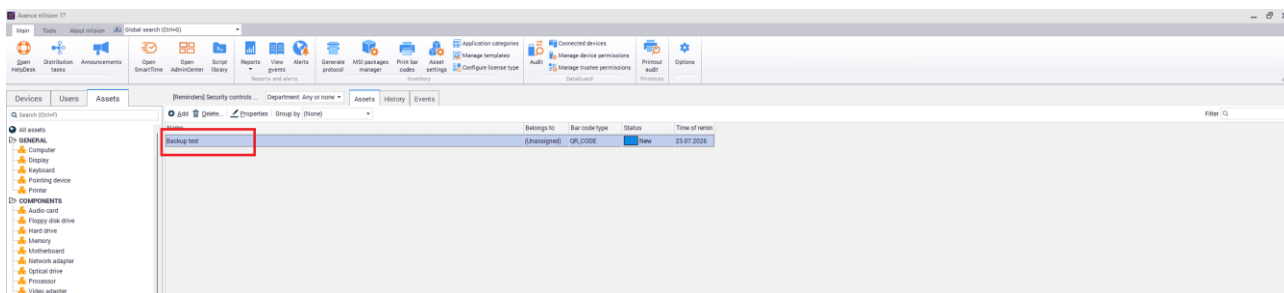
| Field name       | Type          | Description | Required                 |
|------------------|---------------|-------------|--------------------------|
| Interval         | List          |             | <input type="radio"/> No |
| Time of reminder | Date and time |             | <input type="radio"/> No |

OK Cancel

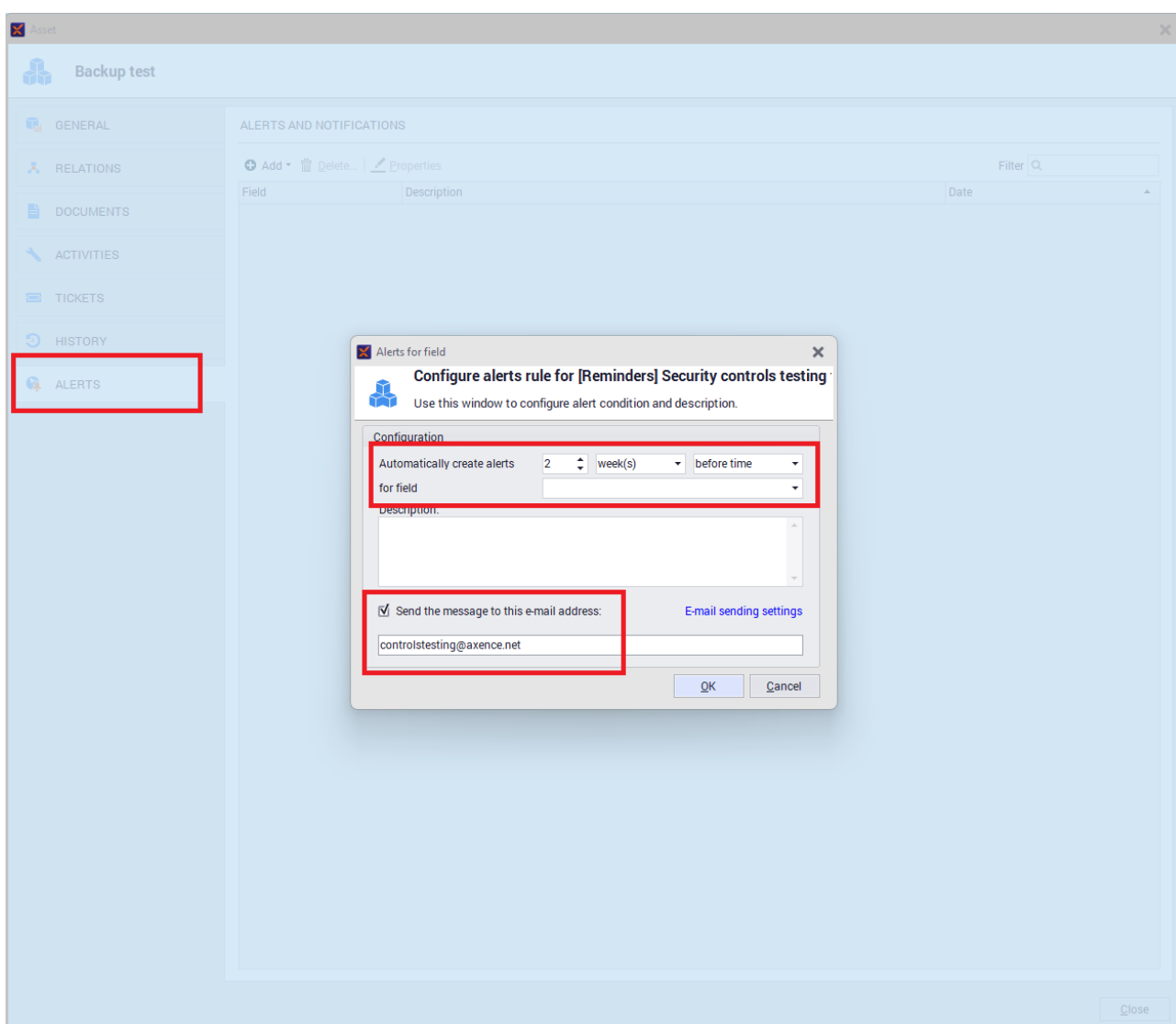
Then identify the security control tests that should be carried out on a recurring basis. For each of these tests, create an auxiliary asset in the ISO 27001 folder:



For example, you can create a **Recurring backup test** asset:



Using the **Add alert for type** option, configure a rule that will send a notification to the indicated e-mail address based on the **Reminder time** field. Set the reminder for the day before the time indicated in the **Reminder time** field.



Following the guidance on [ticket automation](#) in the HelpDesk module, set up automatic creation of a ticket in the **Security control testing** category based on messages received at a special e-mail address (**testowanie.backupu@axence.net** may serve as an example).

After receiving the notification, the Administrator will set a new **Reminder time** using the information in the **Interval** alert field.

## 4.3 Vulnerabilities – identification and response to their occurrence

The purpose of the vulnerability detection process is:

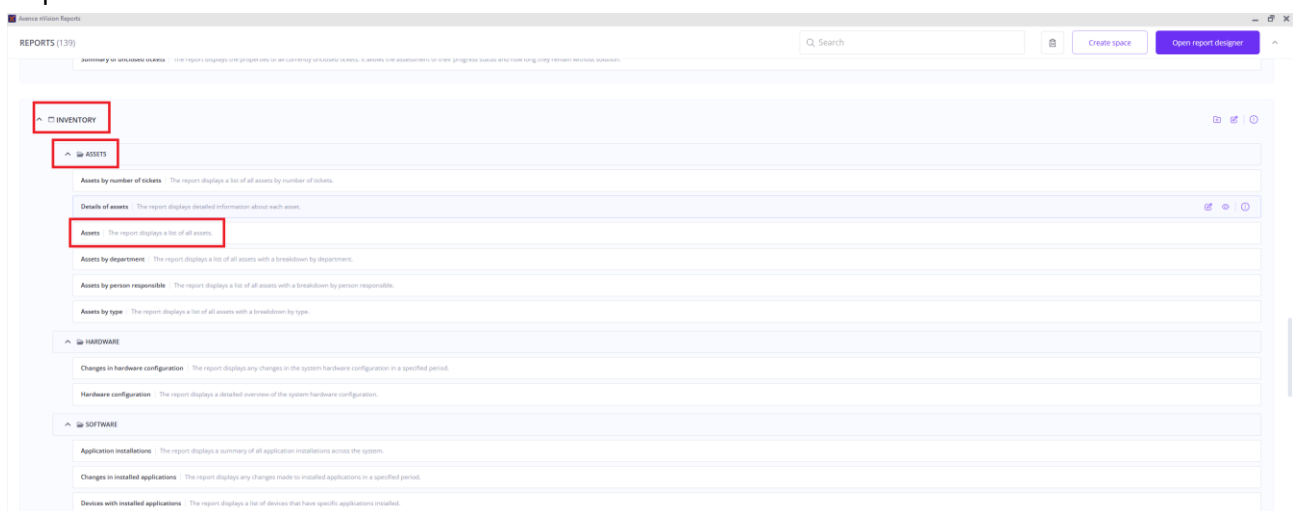
- the identification of technical and organizational weaknesses,
- the assessment of their impact on operational continuity, confidentiality, integrity and availability,
- the selection of appropriate and proportionate security controls.

This is a continuous process, and responsibility for it rests mainly with the IT department whose tasks include, among other things, the systematic verification of installed software.

### 4.3.1 Asset reports

Asset registers are useful for diagnosing vulnerabilities. You can generate them in the **Inventory** section of the **Reports** module:

- report on web applications – in the **Assets** report group, select the report with this exact title, and in the parameters, set the type to **Systems – web applications**; as a result, you will obtain a full list of the applications used in the organization, indicating the department in which the asset is used:



Preview - Axence mVision Reports

1 of 1

axence®

Generation date: 7/7/2026 1:48 AM  
 Type: Systems - web applications  
 Status: All  
 Department: All  
 Person responsible: Everyone

### Assets

| Name              | Type                       | Status | Department | Device | Person responsible | Value | Inventory number | Serial number | Warranty to |
|-------------------|----------------------------|--------|------------|--------|--------------------|-------|------------------|---------------|-------------|
| ChatGPT           | Systems - web applications | New    | IT         |        | - Unassigned -     |       |                  |               |             |
| GitHub            | Systems - web applications | New    | IT         |        | - Unassigned -     |       |                  |               |             |
| Hubspot           | Systems - web applications | New    | Sales      |        | - Unassigned -     |       |                  |               |             |
| Jira              | Systems - web applications | New    | IT         |        | - Unassigned -     |       |                  |               |             |
| Microsoft 365     | Systems - web applications | New    | BackOffice |        | - Unassigned -     |       |                  |               |             |
| Microsoft Teams   | Systems - web applications | New    | BackOffice |        | - Unassigned -     |       |                  |               |             |
| Salesforce CRM    | Systems - web applications | New    | Sales      |        | - Unassigned -     |       |                  |               |             |
| Sharepoint Online | Systems - web applications | New    | BackOffice |        | - Unassigned -     |       |                  |               |             |
| Zendesk           | Systems - web applications | New    | IT         |        | - Unassigned -     |       |                  |               |             |
| Zoom              | Systems - web applications | New    | BackOffice |        | - Unassigned -     |       |                  |               |             |

Report generated by Axence mVision®  
 Page 1 of 1

PREVIEW PARAMETERS

Type: Systems - web applications  
 Status: All  
 Department: All  
 Person responsible: Everyone

RESET SUBMIT

- report on installed software – in the **Software** report group, select the **Application installations** report; you will obtain a full list of the on-premises applications used in the organization:

Axence mVision Reports

REPORTS (139)

Search

Create space Open report designer

Assets by person responsible The report displays a list of all assets with a breakdown by person responsible.

Assets by type The report displays a list of all assets with a breakdown by type.

HARDWARE

Changes in hardware configuration The report displays any changes in the system hardware configuration in a specified period.

Hardware configuration The report displays a detailed overview of the system hardware configuration.

SOFTWARE

Application installations The report displays a summary of all application installations across the system.

Changes in installed applications The report displays any changes made to installed applications in a specified period.

Devices with installed applications The report displays a list of devices that have specific applications installed.

Devices without specific applications The report displays devices that do not have specific applications installed.

Licenses inventory audit The report displays a detailed list of all licenses.

Software on device The report displays a comprehensive list of all software installed on the devices.

Most popular applications The report displays the most frequently installed applications across devices.

Software inventory audit The report displays a detailed list of all installed applications on the system.

User files on device The report displays a list of user-generated files stored on the device.

Preview - Axence Utilization Reports

Generation date: 7/7/2026 1:49 AM  
 Map: All  
 Device type: All  
 Device: All  
 Application type: All  
 Audit status: All  
 Application: All

### Application installations

| Application Name                                             | Version | Company               | Application type | Audit status |
|--------------------------------------------------------------|---------|-----------------------|------------------|--------------|
| 7-Zip 23.01 (x64 edition)                                    | 23      | Igor Pawlov           | Application      | Not audited  |
| Device                                                       |         |                       |                  |              |
| Installation date                                            |         | License serial number |                  |              |
| DESKTOP-KHEECSS 192.168.60.219 (LAB-CL-EN-02)                |         |                       |                  |              |
| 12/29/2025                                                   |         |                       |                  |              |
| LAB-SRV-ANV-EN 192.168.60.212 (LAB-SRV-ANV-EN-arcotab local) |         |                       |                  |              |
| 2/6/2026                                                     |         |                       |                  |              |
| Application Name                                             | Version | Company               | Application type | Audit status |
| 7-Zip 24                                                     | 24      | Igor Pawlov           | Application      | Not audited  |
| Device                                                       |         |                       |                  |              |
| Installation date                                            |         | License serial number |                  |              |
| LAB-CL-EN-01 192.168.60.218 (LAB-CL-EN-01-arcotab local)     |         |                       |                  |              |
| 1/13/2026                                                    |         |                       |                  |              |
| Application Name                                             | Version | Company               | Application type | Audit status |
| Axence ConnectPro Agent                                      |         | Axence Inc.           | Application      | Audited      |
| Device                                                       |         |                       |                  |              |
| Installation date                                            |         | License serial number |                  |              |
| DESKTOP-KHEECSS 192.168.60.219 (LAB-CL-EN-02)                |         |                       |                  |              |
| 12/30/2025                                                   |         |                       |                  |              |
| LAB-CL-EN-01 192.168.60.218 (LAB-CL-EN-01-arcotab local)     |         |                       |                  |              |
| 12/30/2025                                                   |         |                       |                  |              |

Page 1 of 8

PREVIEW PARAMETERS

Map:   
 Device type:   
 Device:   
 Application type:   
 Audit status:   
 Application:   
 RESET SUBMIT

These lists will be useful during both the diagnosis / monitoring of vulnerabilities and the audit. More information about the available reports (as well as the ability to generate your own) can be found in the [documentation](#).

### 4.3.2 Obligations of the business owners of systems

One of the tasks of the business owners (previously grouped according to the [instructions](#) described in 2.1.1) is to monitor threats directly related to the assets they are responsible for. One simple method is to regularly compare the assets held against the CVE database<sup>8</sup>, or at least against the [CISA KEV catalog](#)<sup>9</sup>, which makes it possible to set the right priorities for patching vulnerabilities. Together with the previously described asset reports, you can feed the downloaded catalog, in accordance with internal policies, **into the AI-based tool permitted in your organization** to analyze existing vulnerabilities. Remember that you must verify documents generated in this way. Regardless of how advanced the technology is, everything concerning threats and vulnerabilities should be assessed by competent people.

#### Example prompt:

<sup>8</sup> The **Common Vulnerabilities and Exposures (CVE) database** is a public database that contains information about known security vulnerabilities in software and hardware.

<sup>9</sup> The **Known Exploited Vulnerabilities (KEV) catalog** is maintained by the **Cybersecurity and Infrastructure Security Agency (CISA)** and contains CVEs that are actively exploited and pose a real threat at any given time.

Compare the CISA KEV catalog against the attached reports on assets and vulnerabilities. Above all, identify and indicate the critical vulnerabilities that require an urgent response. Present the results in a table titled **Vulnerabilities requiring an urgent response**, in which you will include the CVE ID, the name of the vulnerability, the manufacturer, the product, the asset or system affected by the vulnerability, the remediation deadline from the [CISA KEV catalog](#), information about use in ransomware campaigns, if applicable, and also the recommended action priority. Finally, add a short summary of the most important conclusions.

Remember that the result of such an analysis is auxiliary. It is not an unequivocal and complete assessment of all vulnerabilities in the environment. The indicated vulnerabilities and recommendations should be verified by the people responsible for security, systems administration or vulnerability management.

Since vulnerability verification is recurring, you can once again use the [announcement sending option](#) in nVision. Prepare an announcement template about the need to check vulnerabilities and send it to the people in your organization who are responsible for examining vulnerabilities (e.g. IT administrators or security specialists) at appropriate intervals.

#### Example announcement:

**Subject:** Quarterly vulnerability verification – task execution

**Content:** In accordance with the adopted information security management process, please carry out the quarterly vulnerability verification for systems and applications.

#### **Scope to be performed:**

1. **Generation of report of systems and applications** (on-premises and web-based)  
Instructions: "Link" (Knowledge Base / HelpDesk)
2. **Vulnerability analysis:**
  - compare the report against the CISA Known Exploited Vulnerabilities database; the use of AI solutions compliant with the applicable security policy is permitted
3. **Environment verification:**
  - check whether critical vulnerabilities are present in the infrastructure
4. **Further actions:**
  - in the event of a vulnerability detection, take remedial actions or pass the information on to the appropriate people.

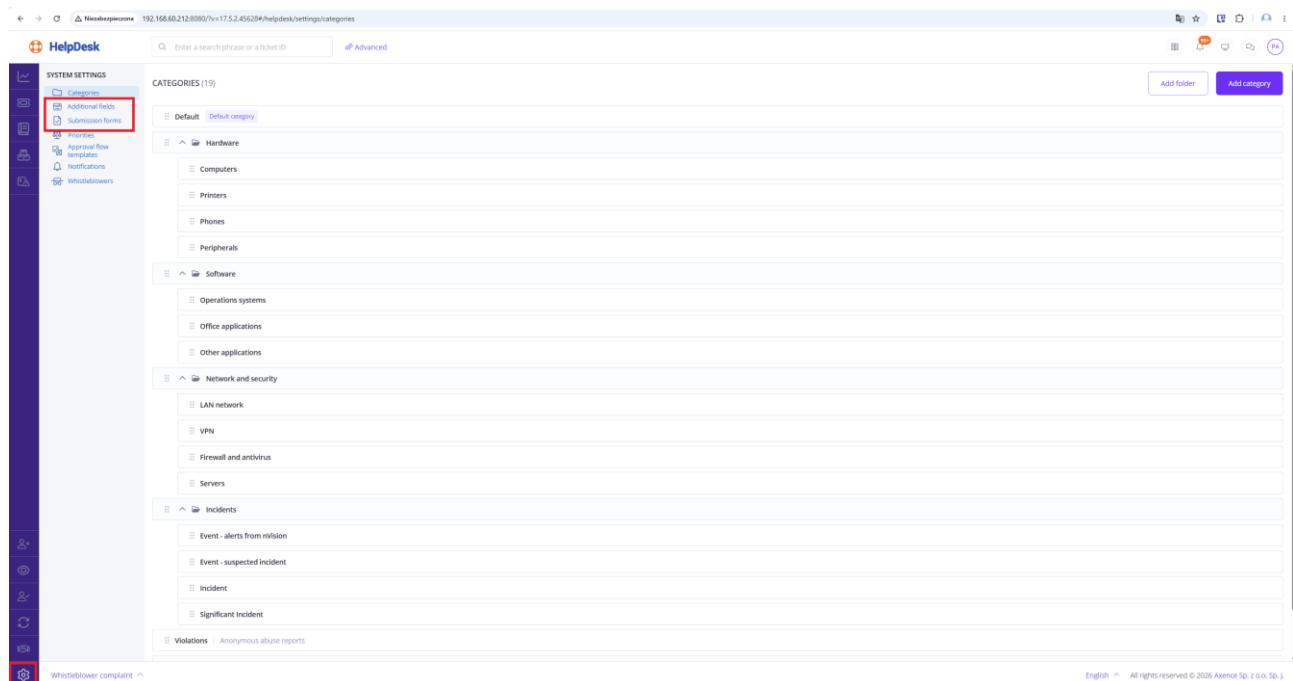
## 5.Submission Forms

Information security requires effective handling of security incidents, as well as onboarding and offboarding processes. In both areas, you can manage access control to assets and mitigate the risk arising from user actions. The timeliness, completeness and clarity of the actions taken are of key importance here, whether you are responding to an event that potentially breaches security or granting, modifying or withdrawing employees' permissions.

In both cases, to preserve the transparency in these processes, facilitate auditing and reduce the risk of errors or unauthorized actions, you will need a way to formally record, verify and track requests. Standardized forms work well for this purpose. They allow you to maintain a consistent approach to process management, streamline day-to-day operations and facilitate the analysis of events and actions within the broader context of the organization's security.

When creating these forms, keep in mind that the only field the user should fill in is the description of the need/situation being reported via the form. The remaining fields should be defined as **internal** and filled in directly by the IT department.

Below, you will find forms that you can transfer into nVision. You can create them using the **Additional fields** and **Submission forms** options in the **Settings** section of the HelpDesk module:



In the form examples attached in this documentation, you may see names of systems, programs or solutions that are not used in your organization. Adapt these examples to your needs by changing or removing field names.

## 5.1 Incident submission and assessment form

It is used for:

- reporting security, technical or organizational incidents that require analysis and action (a publicly visible field, filled in by the user reporting the incident),
- assessing the reported incidents (internal fields, filled in by IT department staff)

The first two fields in table below relate to reporting incidents. The first, an informational one, is a set of guidelines that will make it easier for the user to describe the event. The public part of the form is deliberately simplified. Thanks to this, it retains flexibility, because it does not require the reporting person to fill in many different fields or provide a large amount of information.

| Field name                    | Field type                                                                                               | Field visibility | Options / Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Required |
|-------------------------------|----------------------------------------------------------------------------------------------------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| [INC] Event information field |  Information field    | –                | <p>Inform your Supervisor. Describe in detail:</p> <ul style="list-style-type: none"> <li>• What happened.</li> <li>• Describe how you learned of it.</li> <li>• Indicate where you learned of the event from.</li> <li>• Indicate when you learned of the event.</li> <li>• Specify what information the event concerns, e.g. personal data.</li> <li>• Specify what assets the event concerns, e.g. system, computer hardware.</li> </ul> <p>Attach any materials that may help in assessing the event, e.g. window or screen captures.</p> | –        |
| Description                   |  Basic                | public           | ---                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | No       |
| [INC] Classification          |  Multiple-choice list | internal         | <p>DORA</p> <p>NIS2</p> <p>GDPR</p> <p>ISO-27001</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | No       |

|                                                                     |                                                                                          |          |     |    |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------|----------|-----|----|
| [INC] Concise summary                                               |  Text   | internal | --- | No |
| [INC] Date of occurrence                                            |  Date   | internal | --- | No |
| [INC] Date of detection                                             |  Date   | internal | --- | No |
| [INC] Date of confirmation                                          |  Date   | internal | --- | No |
| [INC] GDPR risk assessment                                          | <input type="radio"/> Boolean (Yes/No)                                                   | internal | --- | No |
| [INC] GDPR risk (Art. 33)                                           | <input type="radio"/> Boolean (Yes/No)                                                   | internal | --- | No |
| [INC] NIS2 risk level                                               |  Text   | internal | --- | No |
| [INC] DORA risk level                                               |  Text   | internal | --- | No |
| [INC] Person with whom the incident was legally consulted           |  Text   | internal | --- | No |
| [INC] To be reported to the supervisory authority                   | <input type="radio"/> Boolean (Yes/No)                                                   | internal | --- | No |
| [INC] Reporting party to the supervisory authority / natural person |  Text | internal | --- | No |
| [INC] To be reported to natural persons                             | <input type="radio"/> Boolean (Yes/No)                                                   | internal | --- | No |
| [INC] Whether other interested parties be informed                  |  Text | internal | --- | No |
| [INC] Cause of the incident                                         |  Text | internal | --- | No |
| [INC] Corrective and remedial measures taken                        |  Text | internal | --- | No |
| [INC] List of attached materials                                    |  Text | internal | --- | No |
| [INC] Additional comments                                           |  Text | internal | --- | No |

## 5.2 Exception submission form

| Field name                                  | Field type                                                                                          | Field visibility | Options / Information                                                                                                        | Required |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------|------------------|------------------------------------------------------------------------------------------------------------------------------|----------|
| Description                                 |  Basic             | public           | ---                                                                                                                          | Yes      |
| [ZW] Policy / procedure being departed from |  Text              | public           | ---                                                                                                                          | No       |
| [ZW] Approving person                       |  Text              | public           | ---                                                                                                                          | No       |
| [ZW] Exception information field            |  Information field | –                | In the ticket description, enter the reason, scope and business or technical justification for the exception being reported. | –        |

## 5.3 Access granting form

| Field name                              | Field type                                                                                             | Field visibility | Options / Information                                                                                                                                                | Required |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| Description                             |  Basic              | public           | ---                                                                                                                                                                  | Yes      |
| [DOS] Name of the system/application    |  Text               | public           | ---                                                                                                                                                                  | Yes      |
| [DOS] Supplier – type                   |  Text               | public           | ---                                                                                                                                                                  | Yes      |
| [DOS] Supplier – name                   |  Text               | public           | ---                                                                                                                                                                  | Yes      |
| [DOS] Type of service                   |  Single-choice list | public           | <ul style="list-style-type: none"> <li>• Cloud</li> <li>• Application on a computer</li> <li>• Application on a server in the local Axence infrastructure</li> </ul> | Yes      |
| [DOS] Type of access (permission level) |  Text               | public           | ---                                                                                                                                                                  | Yes      |
| [DOS] Personal data                     | <input type="radio"/> Boolean (Yes/No)                                                                 | public           | ---                                                                                                                                                                  | Yes      |
| [DOS] Permission grantors               |  Text               | public           | ---                                                                                                                                                                  | Yes      |
| [DOS] Access status                     |  Single-choice list | public           | Active; Removed                                                                                                                                                      | Yes      |

|                                |                                                                                        |        |     |     |
|--------------------------------|----------------------------------------------------------------------------------------|--------|-----|-----|
| [DOS] Date permissions granted |  Date | public | --- | Yes |
| [DOS] Date permissions revoked |  Date | public | --- | No  |

## 5.4 Corrective action card form (post-audit)

| Field name                            | Field type                                                                                             | Field visibility | Options / Information                                                                                              | Required |
|---------------------------------------|--------------------------------------------------------------------------------------------------------|------------------|--------------------------------------------------------------------------------------------------------------------|----------|
| Description                           |  Basic                | public           | ---                                                                                                                | Yes      |
| [KOR] Corrective action               |  Text                 | public           | ---                                                                                                                | Yes      |
| [KOR] Date reported                   |  Date                 | public           | ---                                                                                                                | Yes      |
| [KOR] Reporting person                |  Text                | public           | ---                                                                                                                | Yes      |
| [KOR] Non-conformity                  |  Single-choice list | public           | <ul style="list-style-type: none"> <li>• Non-conformity</li> <li>• Vulnerability</li> <li>• Observation</li> </ul> | Yes      |
| [KOR] Root cause                      |  Text               | public           | ---                                                                                                                | Yes      |
| [KOR] Proposed actions                |  Text               | public           | ---                                                                                                                | Yes      |
| [KOR] Responsible person (department) |  Text               | public           | ---                                                                                                                | Yes      |
| [KOR] Deadline                        |  Date               | public           | ---                                                                                                                | Yes      |

## 5.5 Security control implementation form (resulting from risk assessment)

A ticket in the **Security control implementation** category – discussed in detail [here](#).

## 5.6 Continuity plan performance/testing confirmation form

A ticket in the **Security control testing** category – discussed in detail [here](#).

## 5.7 Onboarding form

| Field name                                   | Field type                                                                                             | Field visibility | Options / Information                                                             | Required |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------|------------------|-----------------------------------------------------------------------------------|----------|
| [ISO/HR] Description                         |  Basic                | public           | ---                                                                               | Yes      |
| [ISO/HR] Start date                          |  Date                 | public           | ---                                                                               | Yes      |
| [ISO/HR] Full name                           |  Text                 | public           | ---                                                                               | Yes      |
| [ISO/HR] Job title                           |  Text                 | public           | ---                                                                               | Yes      |
| [ISO/HR] Supervisor                          |  Text                 | public           | ---                                                                               | Yes      |
| [ISO/HR] DEV team leader                     |  Text               | public           | ---                                                                               | No       |
| [ISO/HR] Office room / permanent workstation |  Text               | public           | ---                                                                               | No       |
| [ISO/HR] Remote work                         |  Single-choice list | public           | <ul style="list-style-type: none"> <li>• Hybrid</li> <li>• 100% remote</li> </ul> | Yes      |
| [ISO/HR] Mobile phone                        | <input type="radio"/> Boolean (Yes/No)                                                                 | public           | ---                                                                               | Yes      |
| [ISO/HR] Mobile number                       |  Text               | public           | ---                                                                               | Yes      |
| [ISO/HR] Group membership                    |  Single-choice list | public           | list of groups in the organization, as needed                                     | Yes      |
| [ISO/HR] Access rights                       |  Text               | public           | ---                                                                               | No       |

## 5.8 Offboarding form

| Field name                                                  | Field type                                                                                             | Field visibility | Options / Information                                                                                                                                                    | Required |
|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| [ISO/HR] Description                                        |  Basic                | public           | ---                                                                                                                                                                      | Yes      |
| [ISO/HR] Full name                                          |  Text                 | public           | ---                                                                                                                                                                      | No       |
| [ISO/HR] Date of termination of cooperation                 |  Text                 | public           | ---                                                                                                                                                                      | No       |
| [ISO/HR] Time of access blocking                            |  Text                 | public           | ---                                                                                                                                                                      | Yes      |
| [ISO/HR] Contractors informed of termination of cooperation | <input type="radio"/> Boolean (Yes/No)                                                                 | public           | ---                                                                                                                                                                      | Yes      |
| [ISO/HR] Employees informed of termination of cooperation   | <input type="radio"/> Boolean (Yes/No)                                                                 | public           | ---                                                                                                                                                                      | Yes      |
| [ISO/HR] Verification of access card return                 |  Single-choice list | public           | <ul style="list-style-type: none"> <li>• Card collected</li> <li>• Card lost (incident reported?)</li> <li>• Card will be collected upon signing the protocol</li> </ul> | Yes      |
| [ISO/HR] Mail forwarding to                                 |  Text               | public           | ---                                                                                                                                                                      | Yes      |
| [ISO/HR] Autoresponder                                      |  Text               | public           | ---                                                                                                                                                                      | No       |
| [ISO/HR] Equipment to be returned                           |  Text               | public           | ---                                                                                                                                                                      | No       |
| [ISO/HR] Access block                                       |  Text               | public           | ---                                                                                                                                                                      | No       |

|                                                            |                                                                                        |          |     |    |
|------------------------------------------------------------|----------------------------------------------------------------------------------------|----------|-----|----|
| [ISO/HR] Phone number forwarding to                        |  Text | public   | --- | No |
| [ISO/HR] Sharing the email mailbox                         |  Text | public   | --- | No |
| [ISO/HR] Sharing files from OneDrive                       |  Text | public   | --- | No |
| [ISO/HR] AD, M365, CRM, ERP, VPN account blocked           | <input type="radio"/> Boolean (Yes/No)                                                 | internal | --- | No |
| [ISO/HR] Equipment collected                               | <input type="radio"/> Boolean (Yes/No)                                                 | internal | --- | No |
| [ISO/HR] Return protocol signed                            | <input type="radio"/> Boolean (Yes/No)                                                 | internal | --- | No |
| [ISO/HR] Status changed in nVision                         | <input type="radio"/> Boolean (Yes/No)                                                 | internal | --- | No |
| [ISO/HR] Data archived: email, OneDrive, computer backup   | <input type="radio"/> Boolean (Yes/No)                                                 | internal | --- | No |
| [ISO/HR] Verification of access to external services       | <input type="radio"/> Boolean (Yes/No)                                                 | internal | --- | No |
| [ISO/HR] Informing employees of termination of cooperation | <input type="radio"/> Boolean (Yes/No)                                                 | internal | --- | No |
| [ISO/HR] Informing contractors of                          | <input type="radio"/> Boolean (Yes/No)                                                 | internal | --- | No |

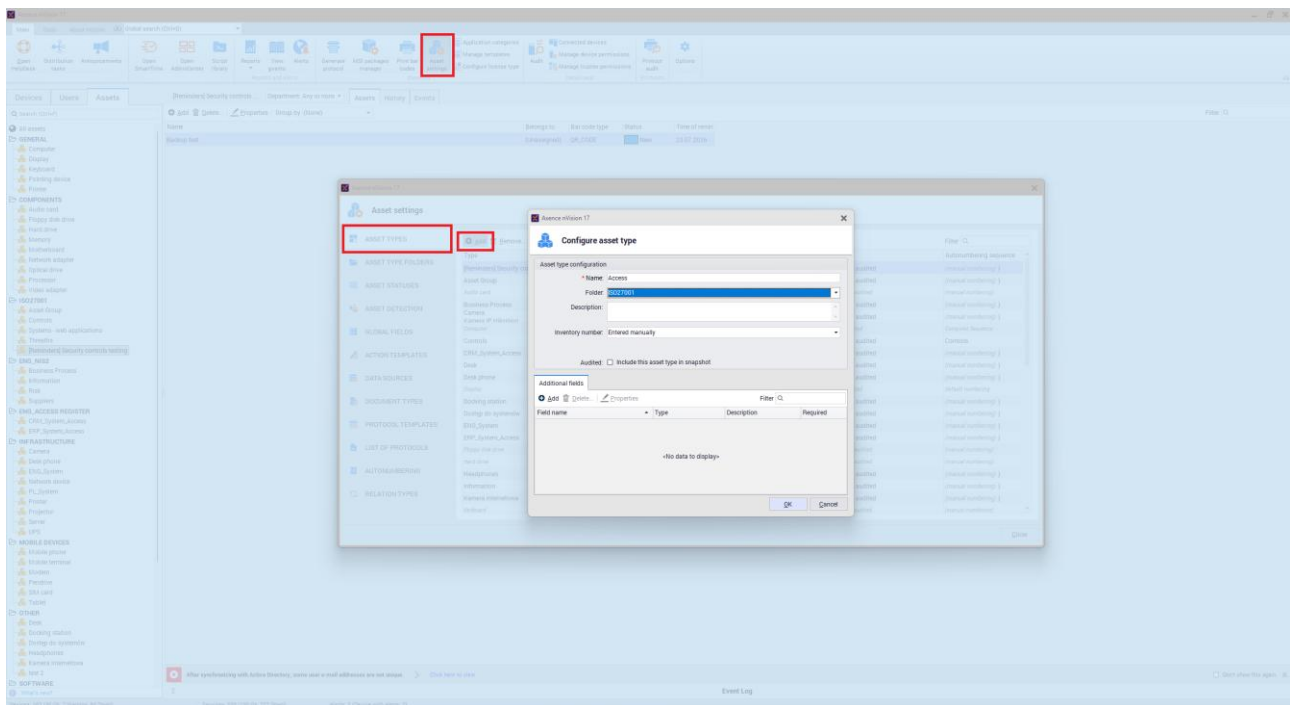
termination of  
cooperation

## 6. Register of granted access

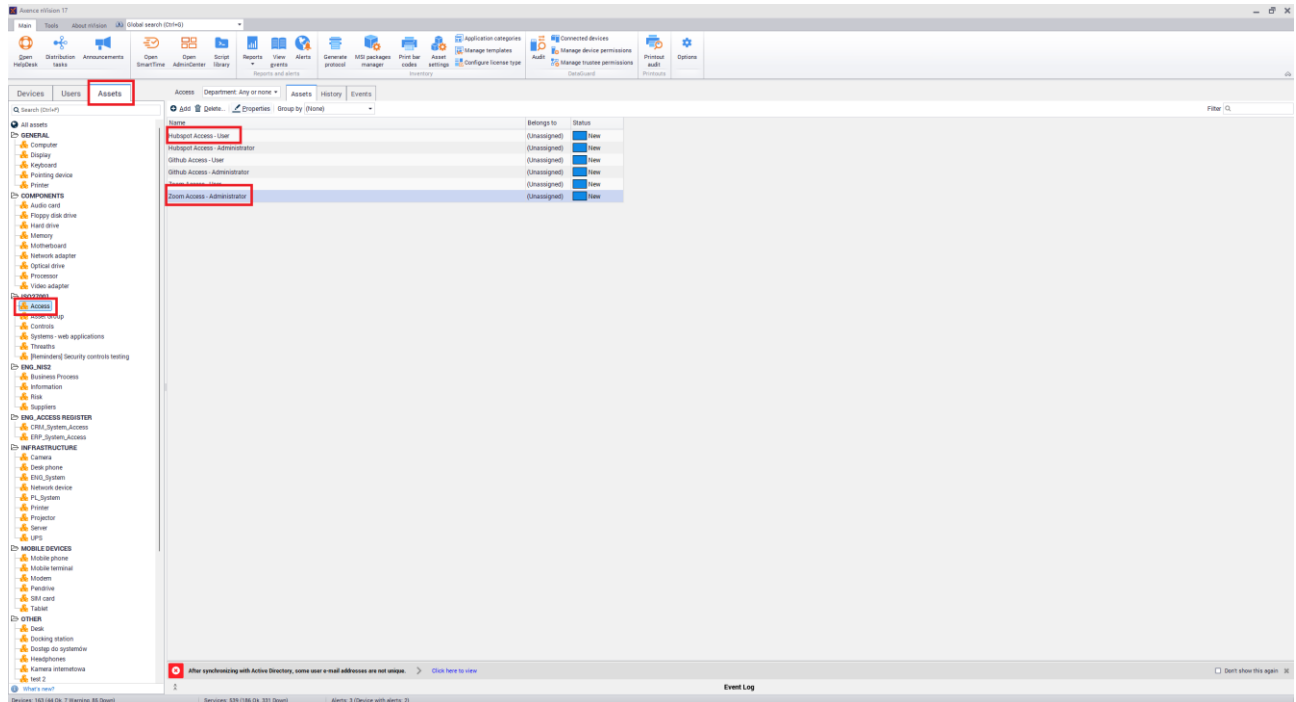
The register of granted access (a record of who has access to which applications) is very important in the context of ISO 27001, because it supports **the management of information security in a controlled and auditable way**.

The nVision system allows you to maintain such a register. In turn:

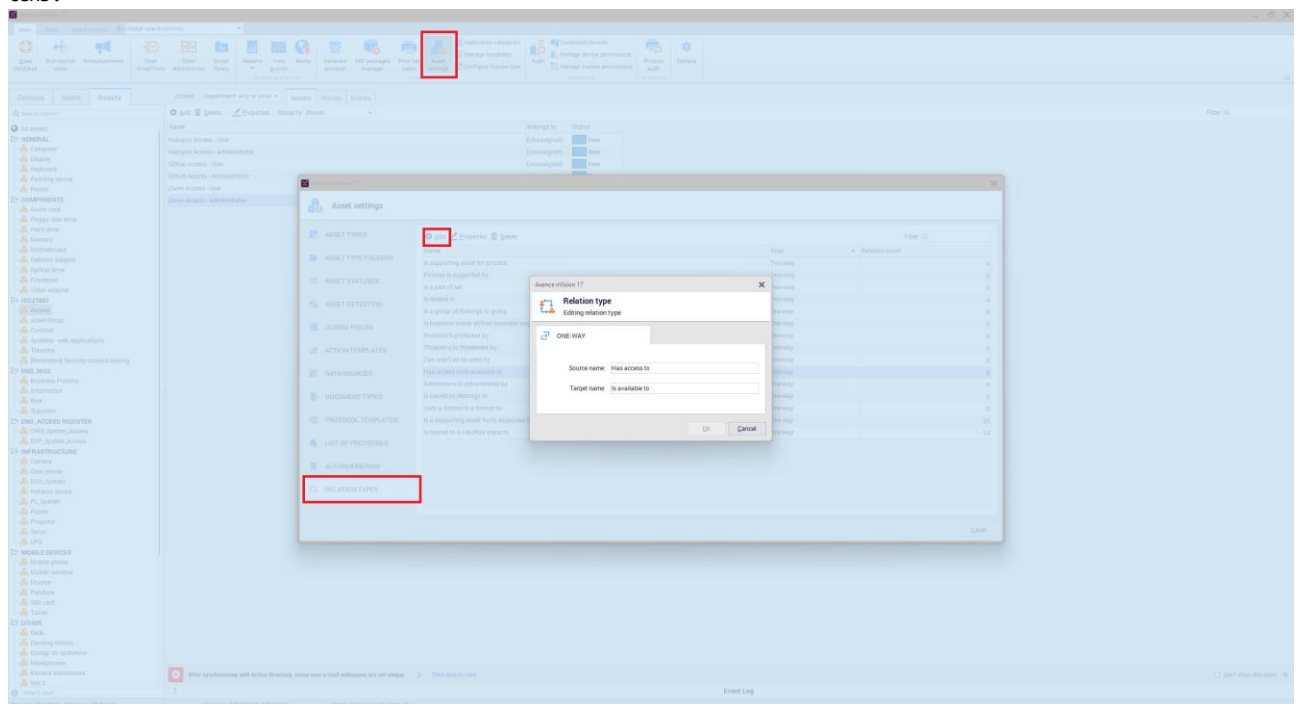
1. Add a new asset type: access. You can do this in the **Asset settings** section, on the **Asset types** tab:



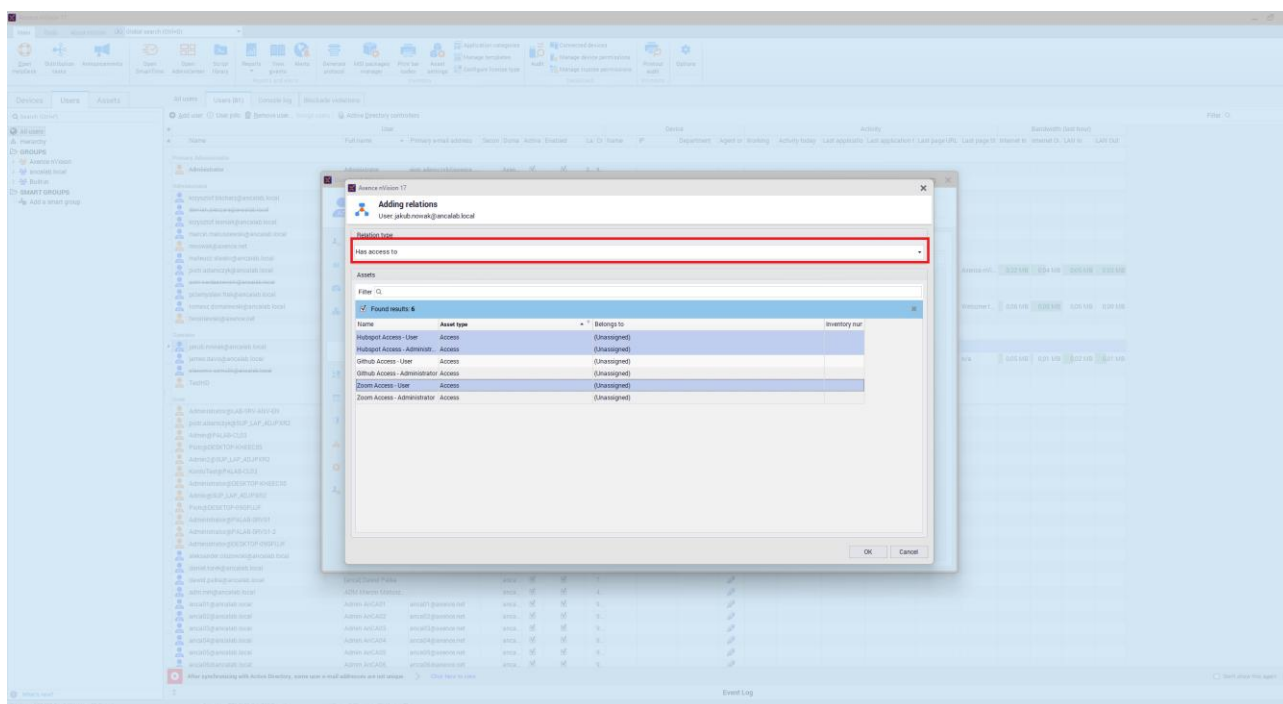
2. Create a pair of access entries for each of the existing assets of the **Systems – web applications** type, one for a regular user and one for an administrator:



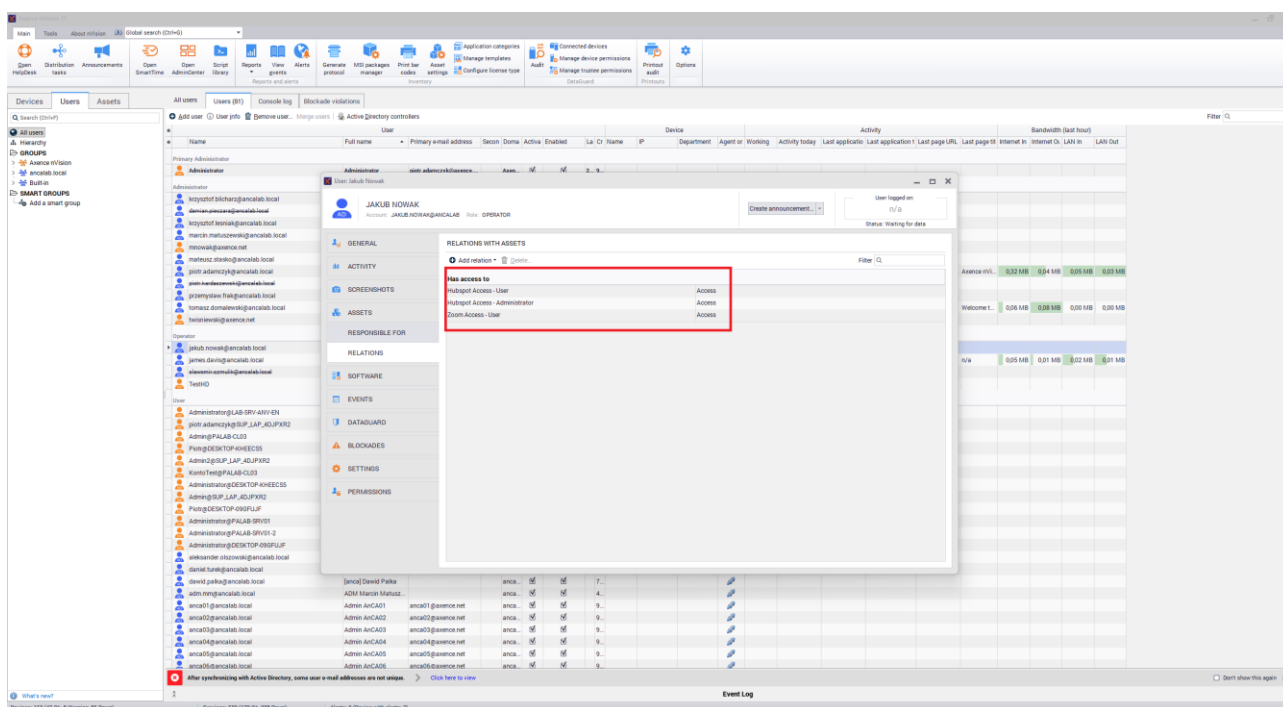
- To assign these access entries to users, you need a new one-directional relation type: **Has access to / Is available to**. You can create it in **Asset settings**, on the **Relation types** tab:



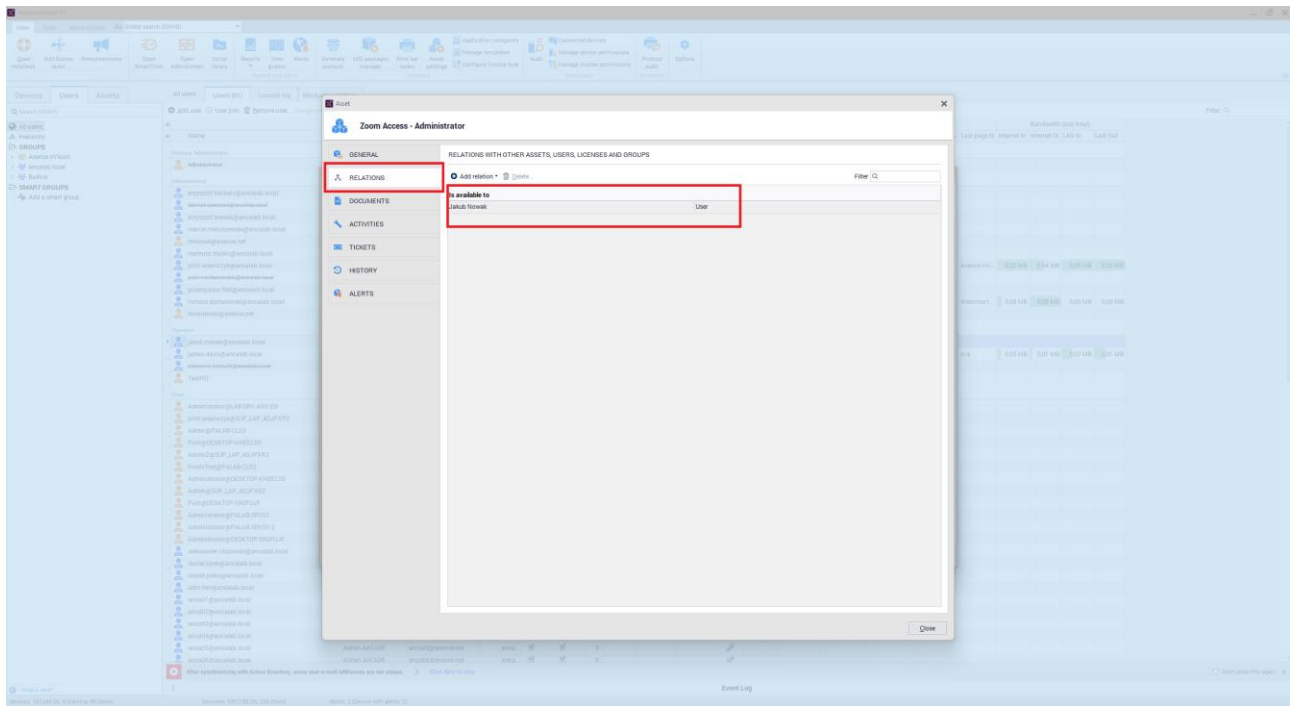
- Now you can link specific access entries to individual users without unduly multiplying assets in the process. This will be useful during onboarding, for example, when granting many access entries to a single user. To do so, just open the user information window and go to the **Assets** tab and there to the **Relations** section, then select the **Has access to** relation type and, while holding down the Ctrl key, click the selected access entries:



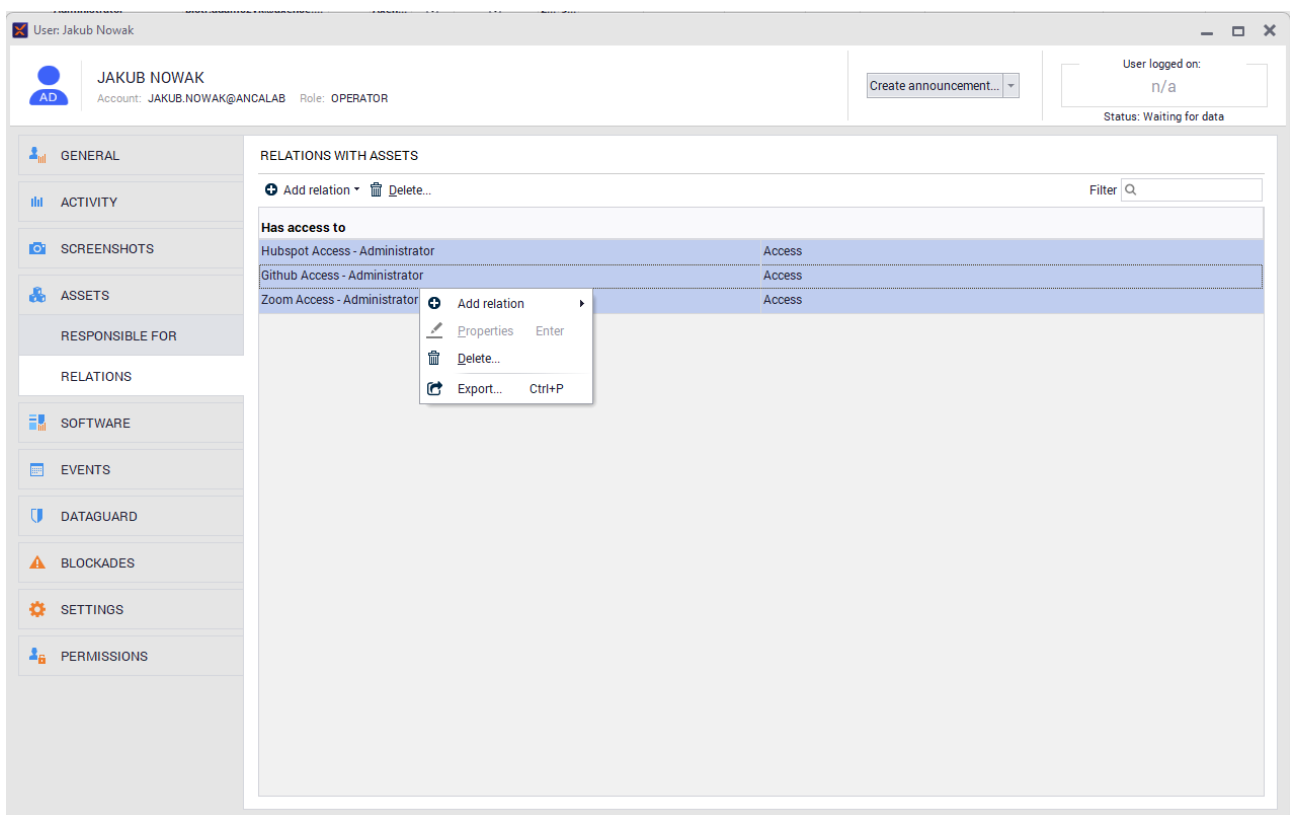
In this way, you can quickly check what access a given user has:



You can also check which users have a relation with a given access entry:



- For each of the access entries, you can download a list of the users who have been granted that access: while holding down the Ctrl key, select the users who have access:



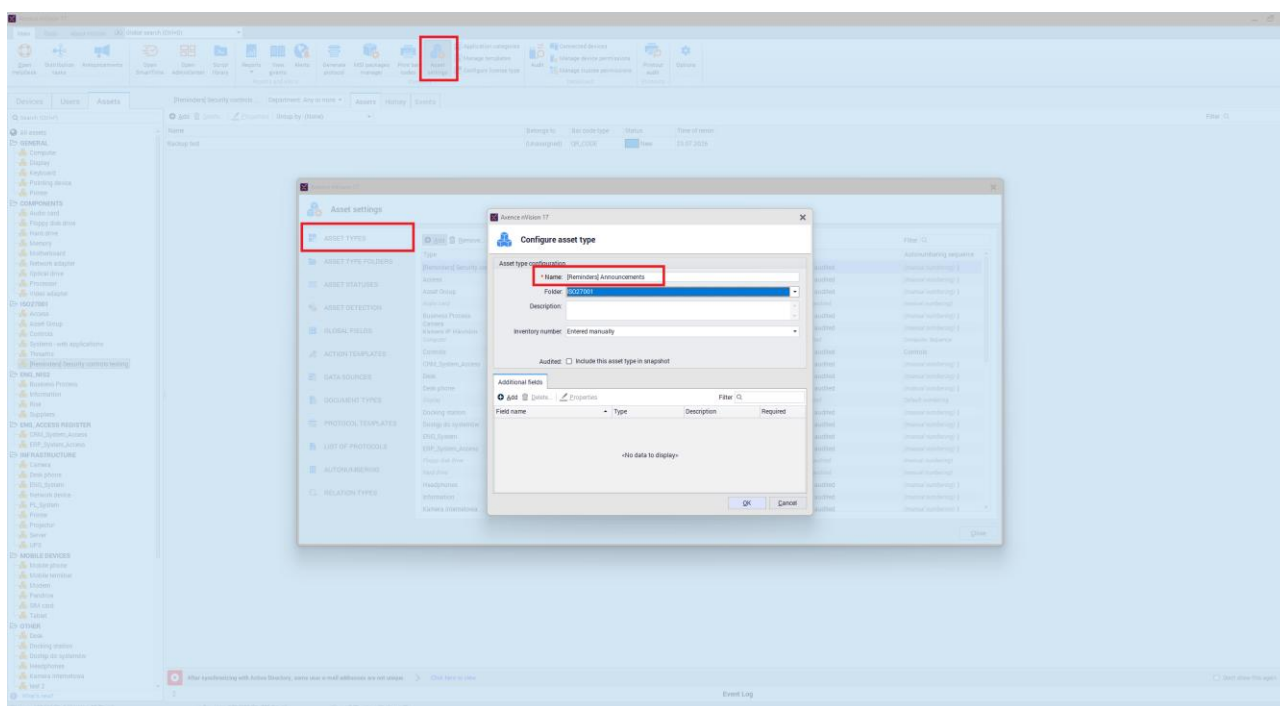
Right-click and select the **Export** option, then save the list in a convenient location in .xlsx format.

## 7. Maintenance tasks – reminders and announcements

Building security in an organization is not a matter of taking a one-off action – it is a process spread out over time. Some activities will be performed once, while others will require repeated execution. One of these activities is sending notifications to system users. You will remind them of the need to confirm the status of assets, the rules for creating and storing passwords or the need to complete training on the SecureTeam platform.

To make this task easier for yourself, use the combined options of asset alerts (the Inventory module) and announcements (the HelpDesk module).

Start by creating an asset type for announcement sending reminders – **[Reminders] Announcements**. You can do this in the **Asset settings** section, on the **Asset types** tab:



Then, add additional fields. For each announcement for which you want to create a reminder, you need two fields: the sending date and the interval. In the examples below, these will be the following fields:

Axence nVision 17

## Configure asset type

Asset type configuration

Configure asset type

\* Name: [Reminders] Announcements

Folder: ISO27001

Description:

Inventory number: Entered manually

Audited: ☐ Include this asset type in snapshot

Additional fields

+ Add

Delete...

Properties

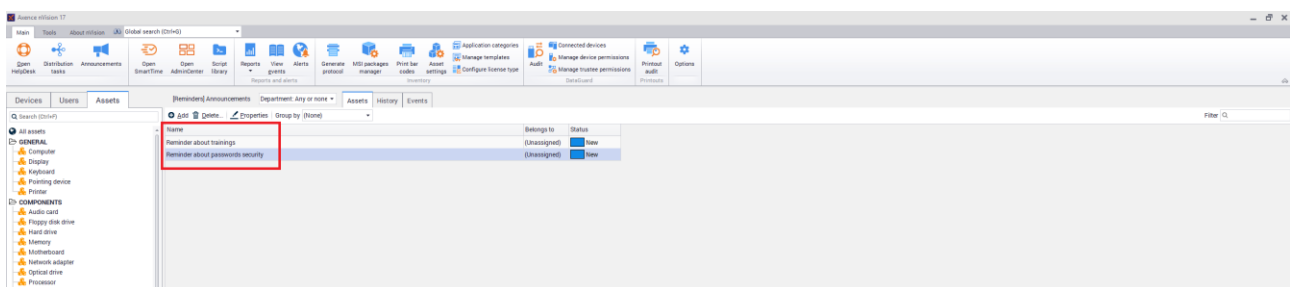
Filter

| Field name            | Type | Description | Required                 |
|-----------------------|------|-------------|--------------------------|
| Interval - passwords  | Text |             | <input type="radio"/> No |
| Interval - trainings  | Text |             | <input type="radio"/> No |
| Send date - passwords | Date |             | <input type="radio"/> No |
| Send date - trainings | Date |             | <input type="radio"/> No |

OK

Cancel

Then, for each of the planned announcements, create a separate asset of the **[Reminders] - Announcements** type:



## 7.1 Security awareness and good practices

Training employees and regularly raising their awareness of cyber threats is one of the basic information security practices. This is important from both the ISO 27001 perspective and the NIS2 requirements and the applicable national implementing legislation, because even the best technical security controls do not eliminate the risk of user errors, phishing or dangerous habits.

For this reason, it is worth regularly informing users about good information security practices – for example, the rules for handling passwords, recognizing phishing, safe use of the internet, data protection and responding to suspicious messages. Such communication should be recurring, so that employees keep their security knowledge up to date.

In nVision, you can prepare recurring announcements that remind users of these good practices and direct them to the relevant materials or internal guidelines. A practical example is the password-security announcement described below.

## 7.2 Password security

Below is an example of a reminder and an announcement concerning the secure creation and storage of passwords.

### Example announcement:

**Subject:** Password security

**Content:** Hello,  
we would like to remind you that passwords must not be saved in text files, spreadsheets, notes, on pieces of paper, in e-mail messages, in messaging apps or in the browser.

Passwords and authentication data should be stored exclusively in a password manager approved by the organization.

Ensure your passwords are unique, strong and not reused across different systems or services.

Link to the password manager: [LINK TO PASSWORD MANAGER].

If you need a VPN to access the password manager from outside the company network, connect to the VPN network before logging in.

In the event of a suspected password disclosure, account takeover or problems with access to the password manager, report the matter to IT / HelpDesk.

## 8.Supporting the audit

You can use the nVision system as a source of data and evidence during an information security audit. Thanks to the ability to filter asset, relation and user lists, as well as export data from lists and reports, you can quickly prepare the statements required by the auditor, e.g. a list of assets, systems, business owners, access, critical assets, or installed software.

### 8.1.1 Filtering assets in the list

The asset view in nVision is one of the basic sources of knowledge about the organization's assets. Here you will find information about inventoried computers, network devices, servers, applications, web systems, information assets and other assets relevant to information security.

You can use the data gathered in the assets during an audit to determine which assets have been identified, how they have been classified and which require special attention due to their assigned risk level. By filtering the asset list, you can narrow the view down to the specific asset categories and prepare statements that match the auditor's needs.

[illegible]

You can export the filtered asset list by right-clicking on the list and selecting the option to export to a **PDF** or **XLS** file. A view prepared in this way is easy to save and hand over to the auditor as proof that an asset register is being kept and that selected security processes are being carried out.

The following elements may prove useful for the purposes of an audit:

| Element                                              | Indicates                                                                                                  |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>Computers</b>                                     | inventoried workstations and user laptops                                                                  |
| <b>Network devices</b>                               | infrastructure elements covered by the register                                                            |
| <b>Servers</b>                                       | key server resources supporting the operation of services and systems                                      |
| <b>On-premises applications (software audit tab)</b> | locally installed software that may require control, updating and vulnerability analysis                   |
| <b>Web applications / web systems</b>                | web systems and services used in the organization, including those not detected automatically by the Agent |
| <b>Information assets</b>                            | information, data or processes that the organization identifies as requiring protection                    |
| <b>Assets with a high or critical risk level</b>     | assets requiring special oversight, monitoring or risk-mitigating actions                                  |
| <b>Threats</b>                                       | identified threats that can be linked to assets or groups of assets as part of the risk analysis           |
| <b>Security controls</b>                             | technical, organizational or procedural measures applied in the organization                               |

Exporting lists of these elements is not mandatory. It is a proposal based on our experience that will make it easier for you to get through the audit procedure. This is not an exhaustive list, but it contains the elements that may interest the auditor the most. You will create these (and other) lists by **filtering** and **exporting assets in nVision**.

### 8.1.2 Exporting data from the reports view

You can also obtain data on assets from the **Reports** module, using the report on assets. This is an alternative way of preparing a list of elements in your infrastructure that is useful during an audit, especially when you need to generate an organized view of the data for a specific asset type.

Preview - Axence nVision Reports

Generation date: 7/7/2026 2:03 AM  
 Type: All  
 Status: All  
 Department: All  
 Person responsible: Everyone

**Assets**

| Name                 | Type                  | Status | Department        | Device | Person responsible | Value | Inventory number | Serial number | Warranty to |
|----------------------|-----------------------|--------|-------------------|--------|--------------------|-------|------------------|---------------|-------------|
| 4 GB (Unknown)       | Memory                | In use | IT                |        | - Unassigned -     |       |                  |               |             |
| 4 GB (Unknown)       | Memory                | In use | IT                |        | - Unassigned -     |       |                  |               |             |
| 4 GB (Unknown)       | Memory                | In use | IT                |        | - Unassigned -     |       |                  |               |             |
| 4 GB (Unknown)       | Memory                | In use | IT                |        | - Unassigned -     |       |                  |               |             |
| 4 GB (Unknown)       | Memory                | New    | - No department - |        | - Unassigned -     |       |                  |               |             |
| 4 GB (Unknown)       | Memory                | New    | - No department - |        | - Unassigned -     |       |                  |               |             |
| 4 GB (Unknown)       | Memory                | New    | - No department - |        | - Unassigned -     |       |                  |               |             |
| 8 GB (Unknown)       | Memory                | New    | IT                |        | - Unassigned -     |       |                  |               |             |
| Access control lists | Controls              | New    | - No department - |        | - Unassigned -     |       | CON/519          |               |             |
| Access for James     | CRM_System_Acces<br>s | In use | Sales             |        | James Davis        |       |                  |               |             |
| Access for Mary      | CRM_System_Acces<br>s | In use | Sales             |        | Mary Smith         |       |                  |               |             |
| Access for Patricia  | CRM_System_Acces<br>s | In use | Sales             |        | Patricia Garcia    |       |                  |               |             |
| Access for peter     | CRM_System_Acces<br>s | New    | - No department - |        | Piotr Adamczyk     |       |                  |               |             |
| Access for Peter     | CRM_System_Acces<br>s | New    | - No department - |        | Piotr Adamczyk     |       |                  |               |             |
| Access for Robert    | CRM_System_Acces<br>s | In use | Sales             |        | Robert Smith       |       |                  |               |             |

Page 1 of 13

PREVIEW PARAMETERS

Type:   
 Status:   
 Department:   
 Person responsible:   
 RESET SUBMIT

In the report, you can display information about the assets gathered in nVision. You can also narrow the scope of the presented data using the available parameters, such as asset type, status, department or responsible person. This allows you to prepare a report covering only a selected category of assets, e.g. computers, network devices, servers, web systems, information assets, threats or security controls.

An important advantage of the reports is the ability to export data to many formats, including, but not limited to, PDF, XLS, and CSV. Exporting to a CSV file allows you to further process the data outside nVision, for example, in a spreadsheet, an external analytical tool or, if the organization's security policy permits it, in solutions that employ AI.

Thanks to this, the reports can be used not only as evidentiary material for the auditor, but also as a source of data for further analysis, comparisons, filtering and preparing additional statements.

More information about the available reports and how to generate them can be found in the [documentation](#).

## 9. Conclusion

The implementation of an information security management system that complies with ISO 27001 and NIS2 requirements, as well as the applicable national implementing legislation is the beginning of a continuous and dynamic process that involves not only the implementation of procedures and policies, but also their regular review, updating and adaptation to the changing technological and legal environment.

Applying the solutions and proposals described in this document will help you bring order to the area of information security in your organization. Thanks to our guidance, you will translate regulatory requirements into concrete, operational steps. It will also be easier for you to identify the elements that need regular verification and updating and ensure proof of compliance (accountability).

Rather than focusing on a specific and limited scope, this document presents a cross-cutting perspective on managing requirements. It approaches the subject holistically. Thanks to this, it can serve as a framework of an information security management system – one that is adaptable and that assumes its elements will change over time.

A key element of our approach is a reliable knowledge base of assets, their owners, relations and threats. This knowledge base forms the foundation for further actions: risk analysis, selection of security controls, monitoring of the environment and responding to incidents.

Cooperation between departments (from IT to the business side) is equally important, as it makes it possible to manage risk more fully and optimally. Thanks to this, all levels of the organization are engaged in building a security culture and conscious management of information.

You too can contribute to shaping the process and its related documentation. If you have comments or thoughts about this document or the issues it raises, send them to us and we will consider them in subsequent versions of the document. We will update this document as the IT landscape, regulatory environment and your needs evolve. Please, send your comments and proposed changes via the form at this [link](#).