nVision
axence®

User Manual:

# How to Organize Remote Work with Axence nVision®?

# Table of Content

# Introduction

Welcome to the User Manual for organizing remote work with Axence nVision®! In today's rapidly evolving digital landscape, remote work has become an integral part of many organizations, offering flexibility and efficiency. However, to make the most of remote work arrangements, it is crucial to implement robust security measures to safeguard your data and devices. With Axence nVision®, you have a powerful tool at your disposal. This guide aims to familiarize you with the various settings and features offered by Axence nVision® that can enhance the safety of your remote work setup. We will delve into the various functionalities provided by Axence nVision® and illustrate how they can be effectively leveraged to organize remote work seamlessly.

**- The Axence Team**

# INVENTORY

## 1. Hardware configuration changes

### I. Always up-to-date information about the hardware

Having always up-to-date information about the hardware is important for several reasons. First and foremost, it ensures smooth functioning of devices, minimizes technical issues, enables efficient troubleshooting, and facilitates timely maintenance. Up-to-date hardware information also contributes to data security by incorporating the latest patches and fixes for vulnerabilities. Additionally, it allows organizations to allocate assets effectively and make informed decisions about hardware upgrades or replacements.

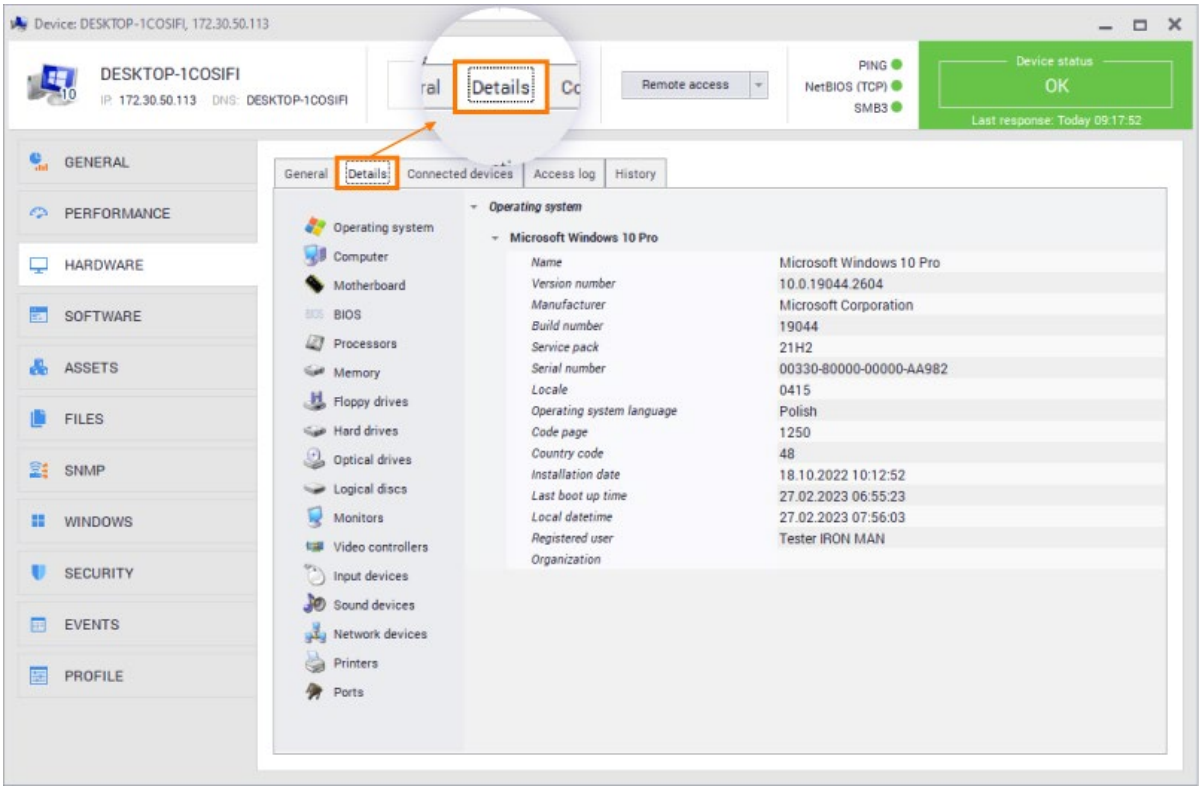
**Hardware Information Scanning:** Scanning for hardware information is always enabled in nVision. In the Device information window, when you go to the Hardware tab, you can see the current hardware configuration of the device.

Hardware and software inventory can also be performed without installing Agents. To do this, use the nVision **Inventory Scanner.**

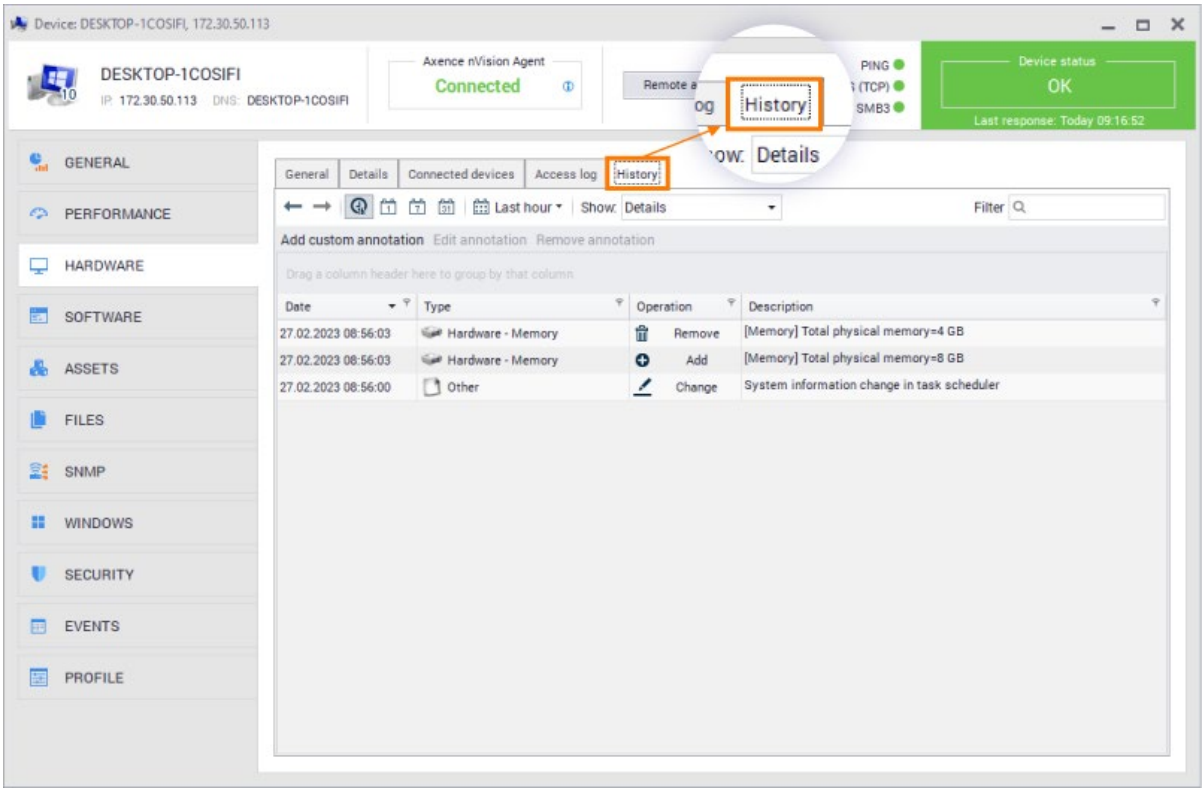
The hardware information scan collects a significant amount of data, and is therefore divided into different tabs in nVision:

1. **General:** The General view collects the most relevant information about the hardware associated with a particular device. In particular, there is some selected information about the computer, processor, memory, operating system, display and others. To maintain consistency with the data from Agents, it is not possible to manually fill in missing data.

2. **Details:** To access full information about the hardware on the monitored computer, go to the Details tab. In the Details view, you can view data by operating system, computer, motherboard, BIOS, processors, memory, floppy drives, hard drives, optical drives, logical discs, monitors, video controllers, input devices, sound devices, network devices, printers, ports.




3. **History:** The History tab provides access to an inventory of all hardware modifications performed on the selected device. In the tab you can view information about the date, type of note, type of action and description.



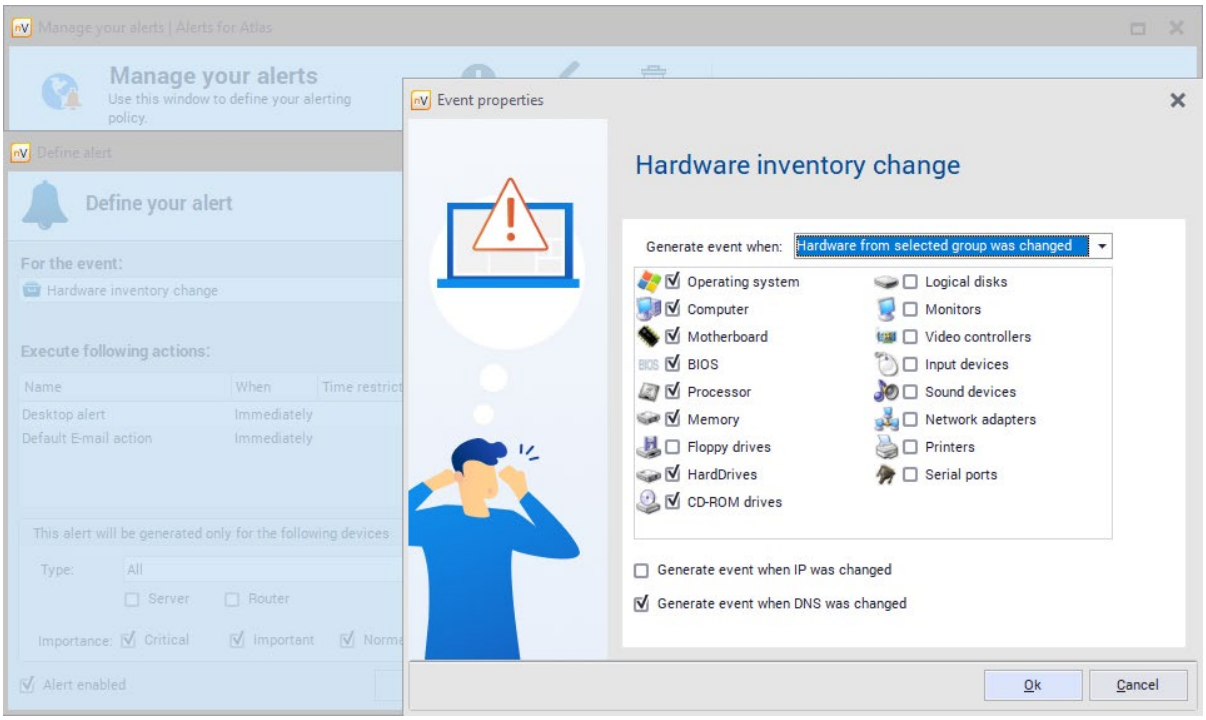
## II. Alerts on any/selected change

Axence nVision® allows you to configure an appropriate alert that will inform the Administrator in a customized way (e.g. e-mail message, Slack message, or desktop alert) about specific events related to hardware configuration changes:

1. **Any Change in Hardware Configuration:** nVision® alerts can be set up to notify the Administrator whenever there is any alteration in the hardware configuration. This comprehensive alert covers all modifications made to the workstation's hardware components.

2. **Selected Changes in Hardware Configuration:** Administrators have the flexibility to specify their preferences regarding hardware configuration changes. They can choose which specific changes they want to be alerted about, based on the components of the workstation. For example, the Administrator can select to receive alerts for changes related to the monitor, motherboard, or hard drive.

All available options from the Details tab can be utilized for customization.



# 2. Software configuration changes

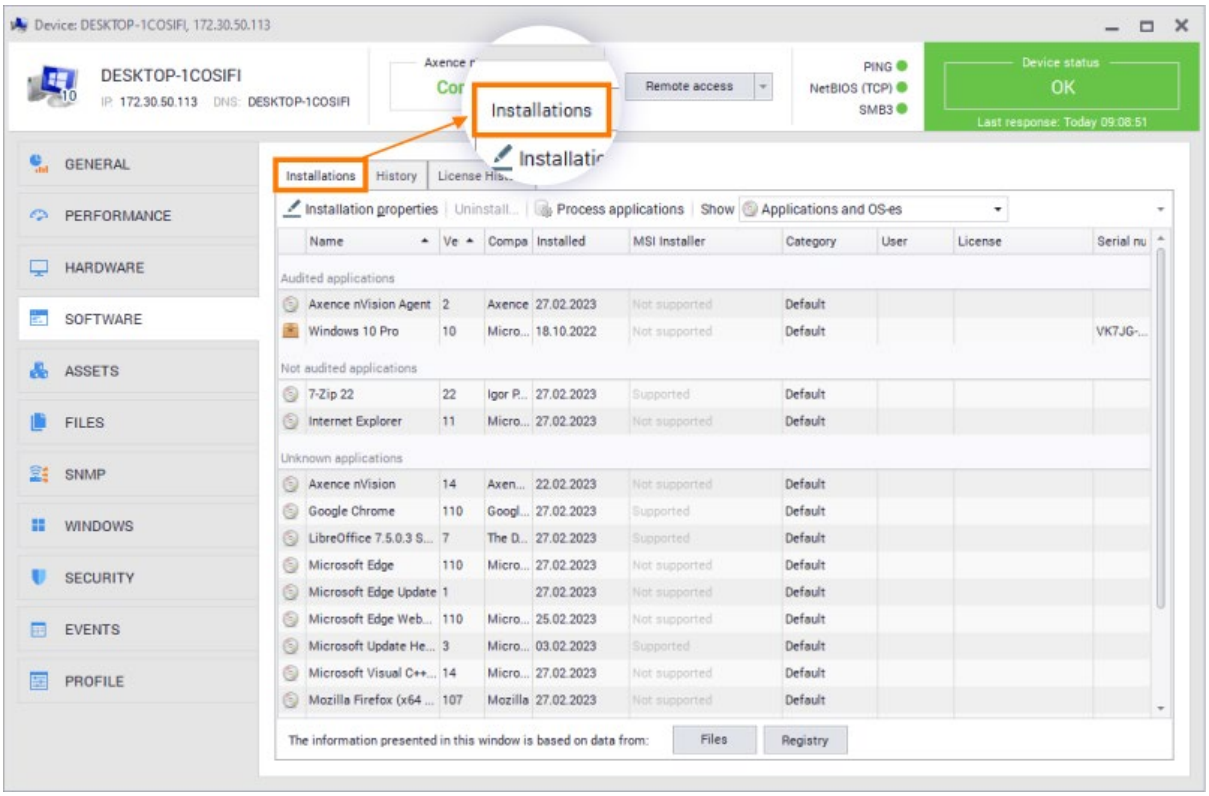
## I. Always up-to-date information about the software

The software inventory function within nVision empowers users with comprehensive control over the applications installed on monitored computers. It facilitates efficient management of software licenses, ensures compliance with legal regulations, and enables effective monitoring of media files. To gather accurate and comprehensive information about installed programs, it is necessary to install the nVision Agent on each computer intended for monitoring.

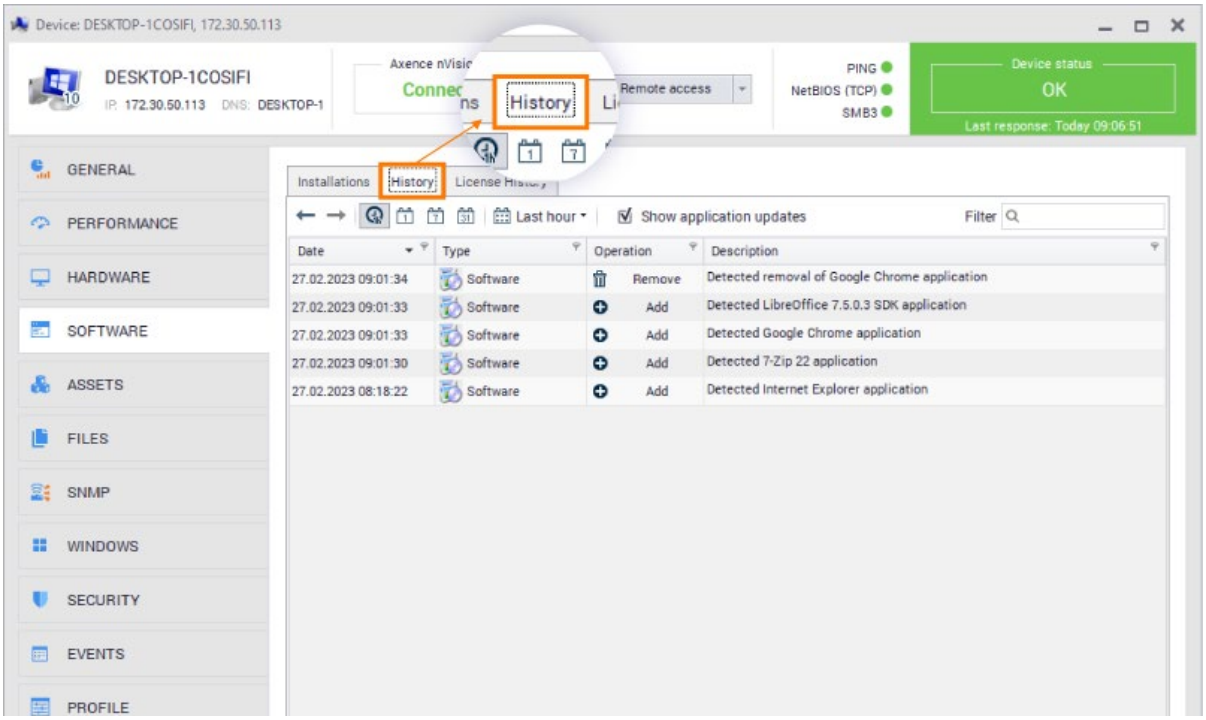
In the Device information window, when you go to the Software tab, you can see the current software configuration of the device.

The software information is divided into three tabs in nVision:

1. **Installation** - allows you to view a list of detected applications on a given device.



2. **History -** displays log of installation changes on a given device.




3. **License history -** displays log of application modifications on a given device.

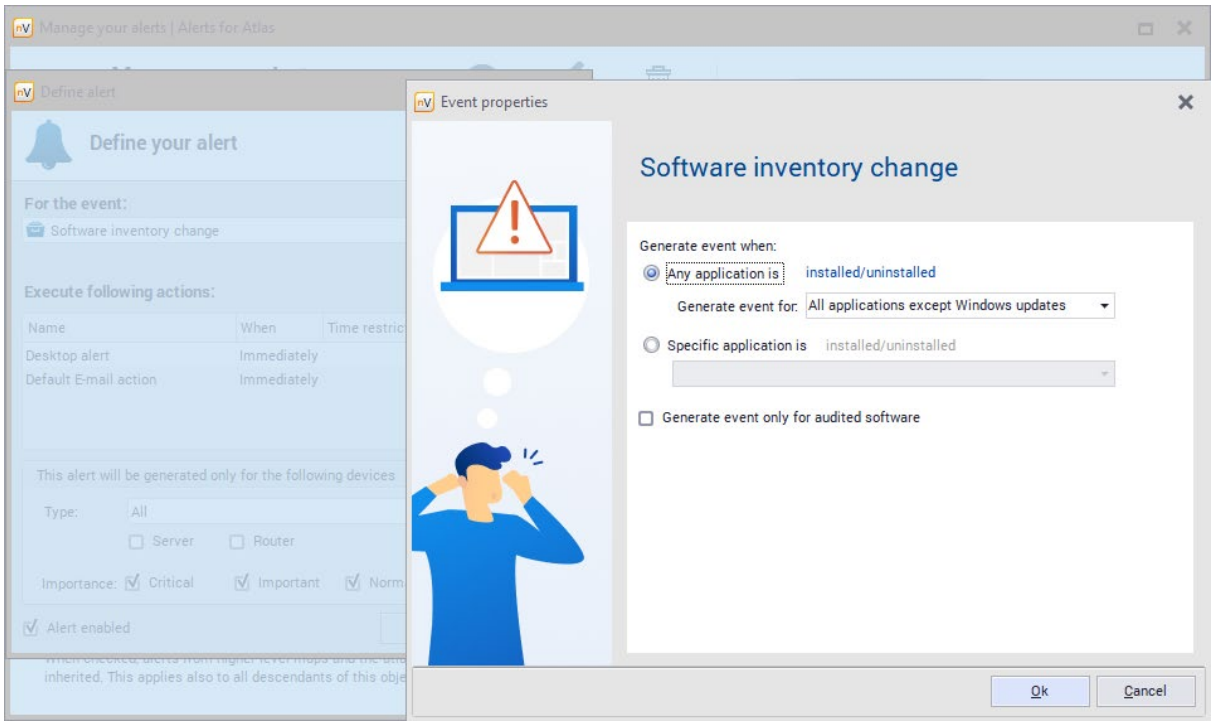
## II. Alerts on any/selected change

Axence nVision® provides the flexibility to customize alerts according to your preferences. These alerts are designed to promptly notify the Administrator when specific conditions or events occur within the system. By tailoring the alerts to your requirements, you can ensure that the Administrator receives notifications in the most suitable manner (e.g., e-mail message, Slack message, or desktop alert).

Specifically, you can configure alerts to notify the Administrator when the following events occur:

1. **Application Installation or Uninstallation:**
   - any application is installed or uninstalled on the workstation - an exception can be specified - e.g., disable Windows update.
   - a specific application is installed or uninstalled on the workstation - select an application in the list.

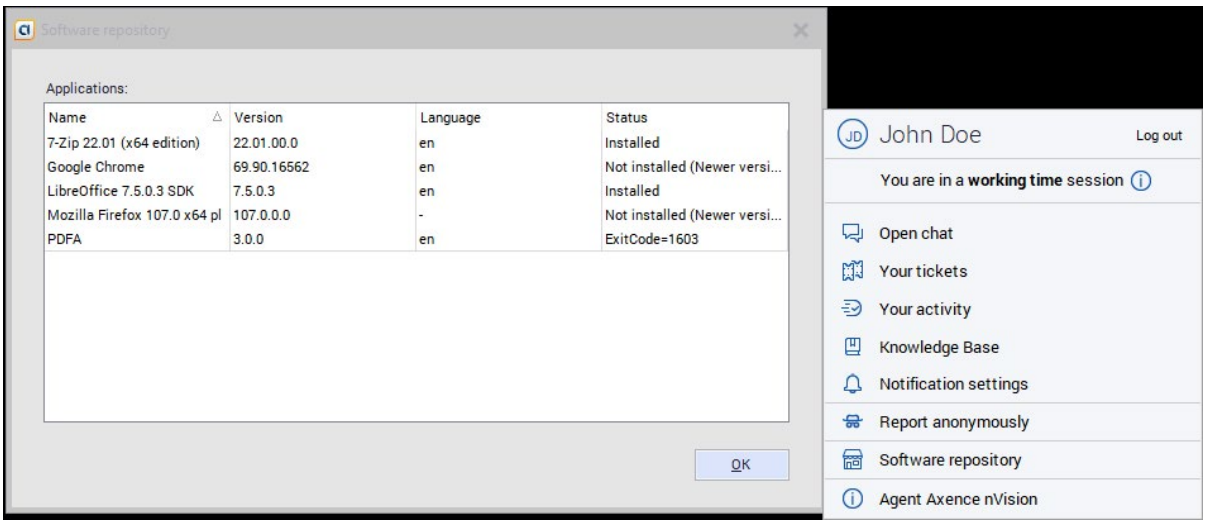
2. **Software Audit Inclusion:**
    - additionally, the Administrator can specify that the alert will be triggered only for applications that are included in the software audit.



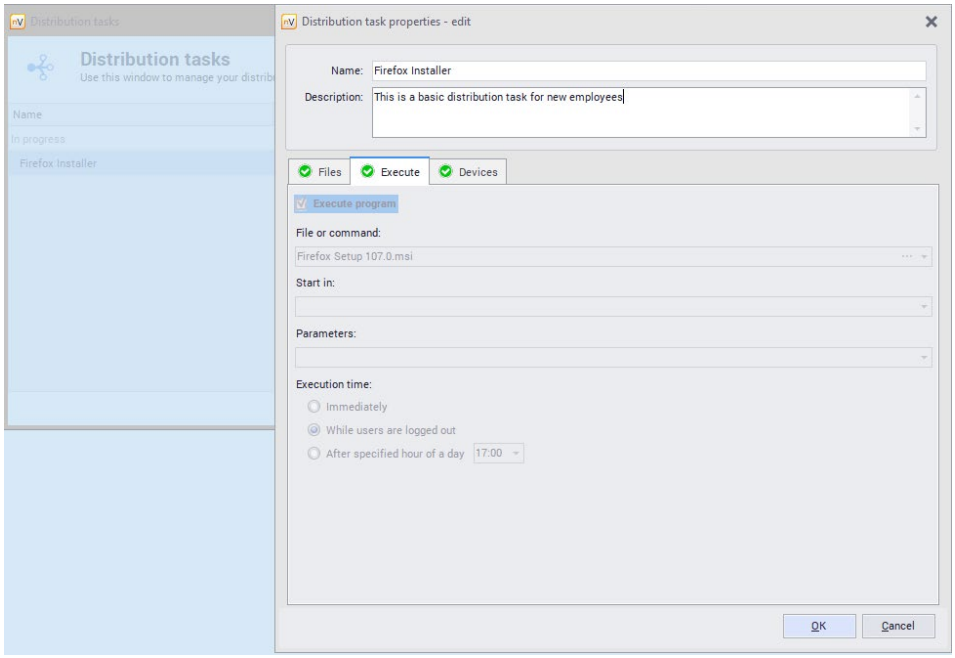

# 3. Remote deployment and installation of mandatory applications

In a remote work setup, remote deployment and installation of mandatory applications bring significant advantages. It ensures consistent application access, saves time and costs, boosts efficiency and productivity, enables centralized management and control, enhances security and compliance, and offers scalability and flexibility.

1. **For employees** - they can quickly access the required applications without any delays. It may streamline the onboarding process for new employees, enabling them to start working more efficiently from day one. Additionally, updates and patches can be easily distributed to remote workstations, ensuring all employees have the latest features and security enhancements.




2. **For IT teams** - they can ensure that remote workstations are equipped with the necessary security applications and updates. Mandatory applications, such as antivirus software or security patches, can be remotely installed. This approach also helps in maintaining compliance with organizational security policies and regulations.



**Software repository:** The nVision Agent simplifies the process of managing software installations on computers that are being monitored. The management of software installations is done through a software repository, which serves as a centralized hub for storing and organizing the necessary software packages.

Using the console, Administrators can easily add MSI packages to the repository. They also have the flexibility to prioritize installations, which becomes important when multiple packages need to be installed within a specific group. Additionally, Administrators can set additional launch parameters to further customize the installation process according to specific requirements.

**Remote distribution and installation** is done as follows:

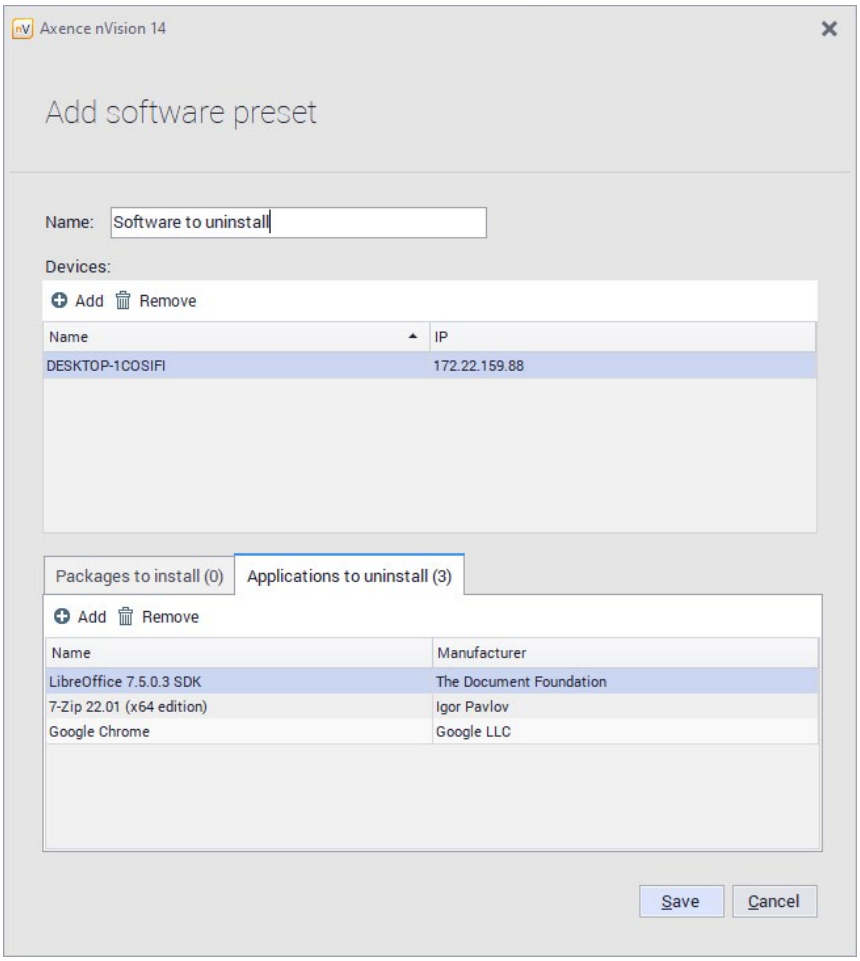
1. **Package Installation:** The Agent initiates the installation of packages only after successfully downloading all the packages configured for it, taking into account the priorities specified in the package properties.

2. **Application Installation:** The Agent permits application installation under the following conditions:
   - *Absence of Application:* The Agent proceeds with installation if the application is not installed at all on the target system.
   - *Upgrade:* The Agent installs the application when it detects an older version installed on the target system, replacing it with the version received by the Agent.

3. **Application Integrity Check:** The Agent performs periodic checks to ensure the presence of all applications assigned to the target system within the packages. These checks are conducted irrespective of the option selected regarding software information scanning in the Agent's profile.
   - *Deficiency Detection:* If the Agent identifies any deficiencies or missing applications during the integrity check, it triggers the reinstallation process.
   - *Reinstallation Process:* The Agent reinstalls the applications that are found to be deficient or missing from the target system, ensuring their proper installation and functioning.

# 4. Remote deinstallation of “unwanted” applications

The nVision Agent offers a convenient feature to uninstall applications that are deemed unsuitable for installation on workstations due to a variety of reasons.




## Operation Scheme:

The nVision Agent follows the same operation scheme for uninstallation as it does for installation. It diligently executes the following steps to ensure effective removal of unwanted applications:

1. **Periodic Application Check:** At regular intervals, the Agent performs checks to determine if the specified application for removal is installed on the workstation. By conducting these periodic scans, the Agent remains vigilant in identifying any instances of the targeted application.

2. **Uninstallation Procedure:** Once the Agent detects the presence of the designated application, it proceeds with the uninstallation process. Employing the same level of attention to detail as during the installation procedure, the Agent ensures that the application is removed effectively and thoroughly.

### Administrator's Role:

The Administrator plays a crucial role in configuring the nVision Agent's uninstallation functionality:

1. **Information Collection:** First, the Agent collects relevant data by monitoring the registry entries of installed applications. Additionally, it extracts installation information from MSI packages to enhance the accuracy of the uninstallation process.

2. **Generating the Uninstallation List:** On the basis of information collected by the Agent, the Administrator has the ability to create a comprehensive list of applications (packages) that should be uninstalled. This list serves as a reference for the nVision Agent, guiding it in identifying the applications to be removed.

## 5. Drive failure alert

In Axence nVision®, you have the capability to establish a highly effective alert system that will promptly inform Administrators of potential drive failures using various communication methods (e.g. email, Slack messages, or desktop alert).

The alert is triggered by a change in the status of S.M.A.R.T (Self-Monitoring, Analysis and Reporting Technology), which is a robust monitoring system integrated into most drives. By configuring this alert, you can ensure timely notifications and take proactive measures to address any imminent drive issues.

# USERS

## 6. Overall and detailed activity summary of the employee working on a PC

Activity summaries of employees working on PCs aid in identifying patterns or irregularities that may be responsible for technical problems or system failures. This valuable information enables prompt troubleshooting and resolution of problems, minimizing downtime and optimizing system performance. It helps IT teams pinpoint the root causes of issues and take necessary actions to ensure smooth operations and a productive work environment.

The Agent, integrated with Axence nVision®, diligently tracks user activity on Windows computers, providing valuable insights into their behavior. The software collects the following information:

1. **Actual Activity (Work) Time:** Inactivity (Break) Time corresponds to periods when users remain idle, not pressing keys or moving the mouse.

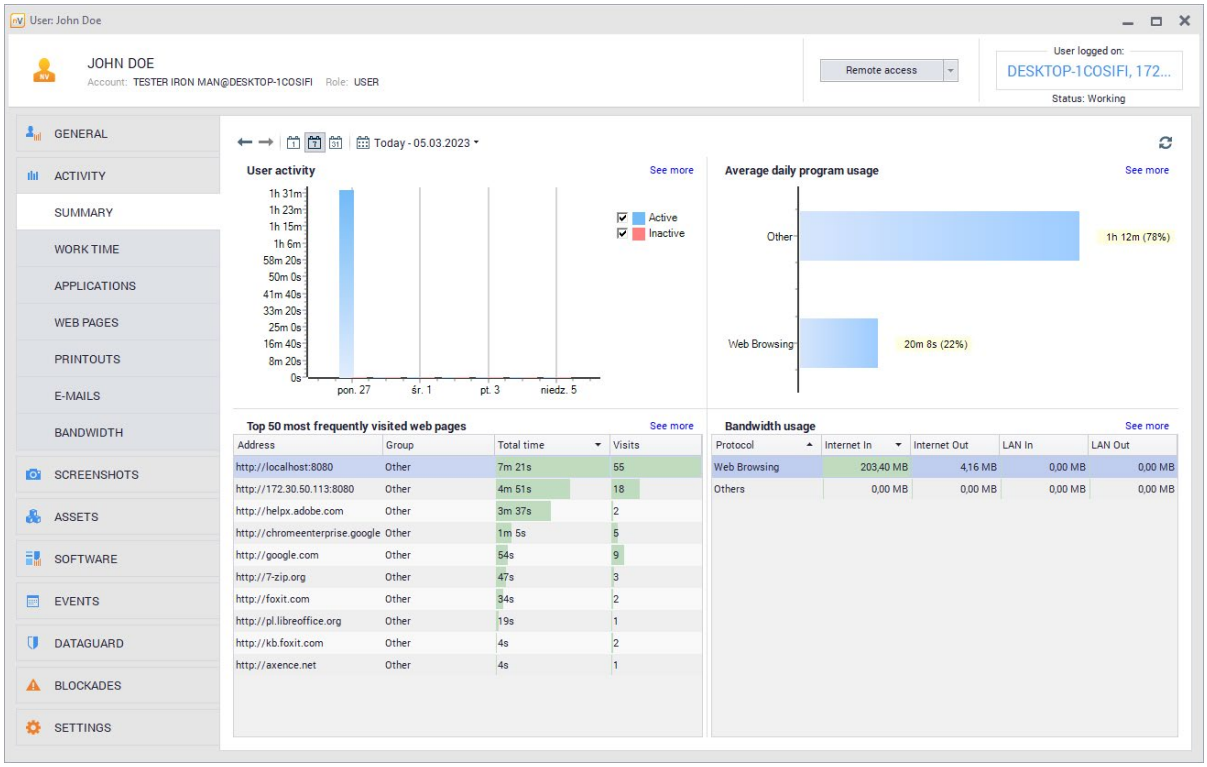
2. **Program Usage Time:** This data is grouped to facilitate analysis and comprehension of user activity patterns.

3. **List of Visited Websites:** The Agent analyzes low-level network information to retrieve a comprehensive list of websites visited.

### Employee Activity Information Categories:

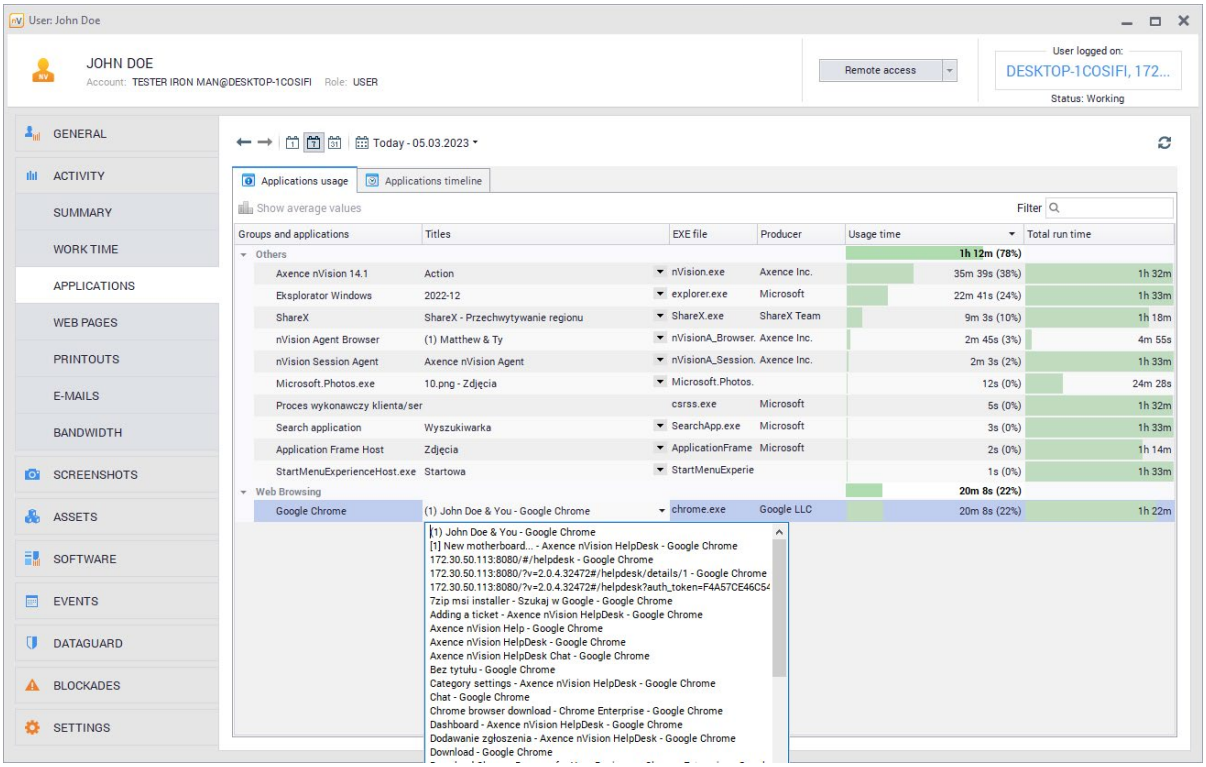
1. **General (Summary):** These parameters encompass essential metrics, including:
   - *User Activity (Active/Inactive):* Provides an overview of whether the user is actively engaged or inactive.
   - *Average Daily Program Usage:* Presents the average amount of time spent using programs per day.
   - *Top 50 Most Frequently Visited Websites:* Highlights the web pages that have been accessed most frequently by the user.

- *Bandwidth Usage on the Local Network and Internet:* Breaks down the utilization of bandwidth into incoming and outgoing traffic, both on the local network and the Internet.




2. **Detailed** (Available in Other Tabs):
   - *Work Time:* Offers a detailed breakdown of user activity on a daily and weekly basis. It includes intervals categorized by status, such as Active, Break, or Not Logged In, providing insights into the user's work patterns.
   - *Applications:* Provides a comprehensive list of applications utilized by the user. It includes Usage Time, which denotes the time spent on each application within specific time intervals, Total Run Time, indicating the overall duration of application usage, and also Applications Timeline showing app usage during the day, date, time, app name, and even 'suspicious activity'.
   - *Web Pages:* Displays a list of web pages visited by the user. It includes information on the time spent on each page and the total number of visits to individual web pages, allowing for an understanding of web browsing habits.
   - *Printouts:* Presents a record of printouts made by the user.
   - *Emails:* Offers a list of emails sent and received by the user.

- *Bandwidth:* Visualizes link usage through graphs, allowing for a visual representation of bandwidth consumption.



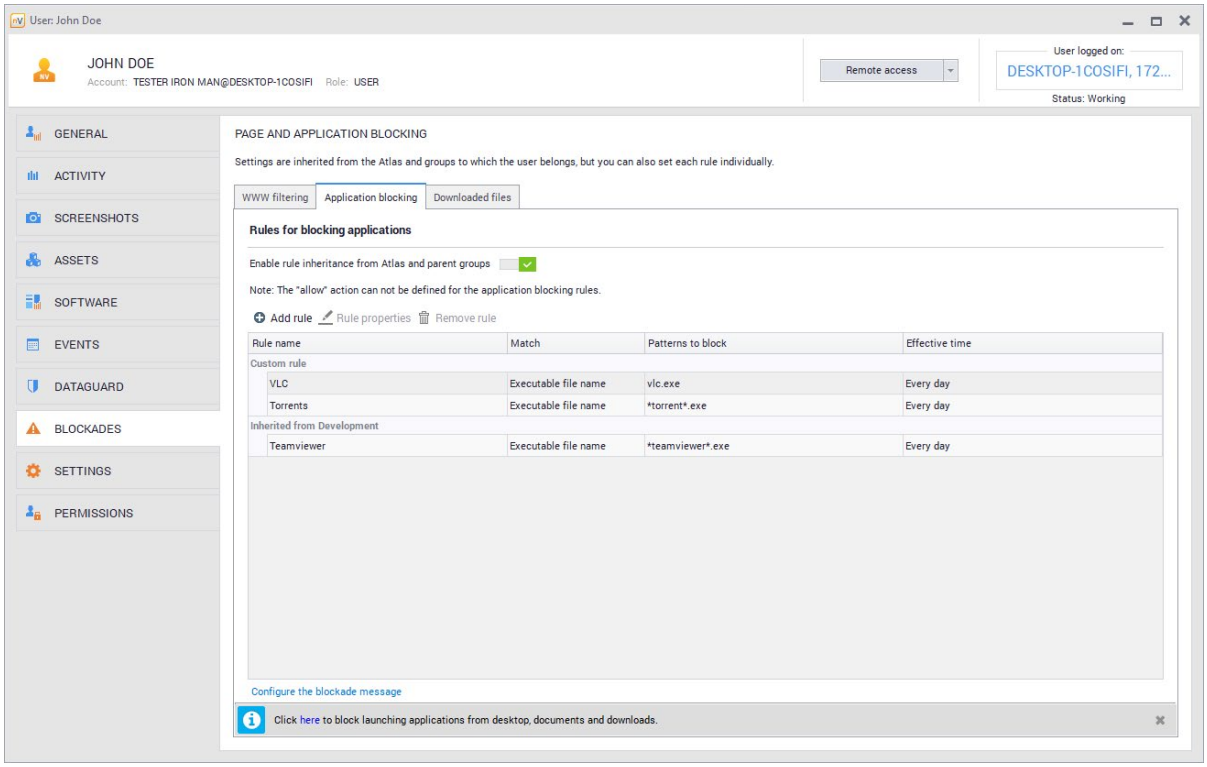

# 7. Blockades minimizing the risk of attacks and data leaks

Axence nVision® optimizes security and productivity by implementing blockades, thus preventing attacks, data leaks, and unnecessary application usage.

1. **Application Blocking:** When configuring application blocking in Axence nVision®, Administrators have the flexibility to adjust various parameters, including:
   - Rule Name: Assign a descriptive name to the blocking rule for easy identification and management.
   - Match: Choose between two options - executable file name or executable full path - to define how the application should be identified for blocking purposes.

- *Patterns to Block:* Specify the specific patterns or criteria that should trigger the application blocking.
- *Effective Time:* Determine the days and hours during which the blocking rule should be active. Administrators can customize the schedule to align with specific timeframes when the blocking should take effect.

**Blockage Message:** In addition, nVision allows you to create a blockade message, which will be displayed when a user tries to run an application that is blocked.




2. **Web Access Blocking:** When setting up a web access blocking, Administrators have the ability to customize several parameters, including:
   - *Rule Name:* Assign a descriptive name to the blocking rule for easy identification and management.
   - *Action:* Choose between "Block" or "Allow" to determine whether access to a particular website should be restricted or permitted. Unlike application access blocking, rules can be created to specifically allow the use of certain websites.
   - *Domain or IP:* Enter the IP address or domain name that you wish to block. Each domain or IP address should be placed on a separate line. The "*" character can be used as a wildcard, matching any string of characters within the domain or IP address.

- *Effective time:* Configure the days and hours during which the web access blocking should be active. Administrators can specify the timeframes during which the blocking rule should be in effect, providing control over when access to specific websites is restricted or allowed.

**Blockage Message:** In addition, nVision allows you to create a blockade message, which will be displayed when a user tries to run an application that is blocked.

Axence nVision® allows Administrators to configure both application access blocking and website access blocking at different levels:

1. globally (Atlas level),
2. within specific groups,
3. or assigned to individual users.

In cases where access to a website is globally blocked at the Atlas level, Administrators can implement more granular control by making the website accessible for users within a specific group. To achieve this, a rule can be added to the group configuration, explicitly allowing (Allow) the use of the website in question. This rule effectively overrides the global blocking restriction for users within that particular group, ensuring they can access the website despite it being blocked for other users.

## 8. An intuitive communication channel for employees when they encounter a problem

The HelpDesk module in Axence nVision® presents a comprehensive suite of functionalities that greatly simplifies the process of delivering technical support and resolving various issues faced by employees within the organization.

Accessible to all users with nVision account, HelpDesk serves as an indispensable tool for streamlining the reporting and resolution of problems. At its core, HelpDesk empowers users to submit tickets detailing their problems. To enhance the clarity and comprehensiveness of these problem descriptions, users can conveniently attach relevant files and screenshots. Once submitted, these tickets are efficiently processed and addressed by administrators and support staff.

Its interactive ticket database creates a valuable knowledge base that continually grows with each technical issue and its corresponding resolution. These solved tickets become an invaluable resource for both users and technical support staff, fostering efficient problem-solving.

HelpDesk is a highly sophisticated tool that allows technical staff to configure numerous settings and customize the module to meet the organization's specific requirements.

**Ticket management:** HelpDesk in Axence nVision® offers a range of powerful features that facilitate seamless ticket management and streamline the support process:

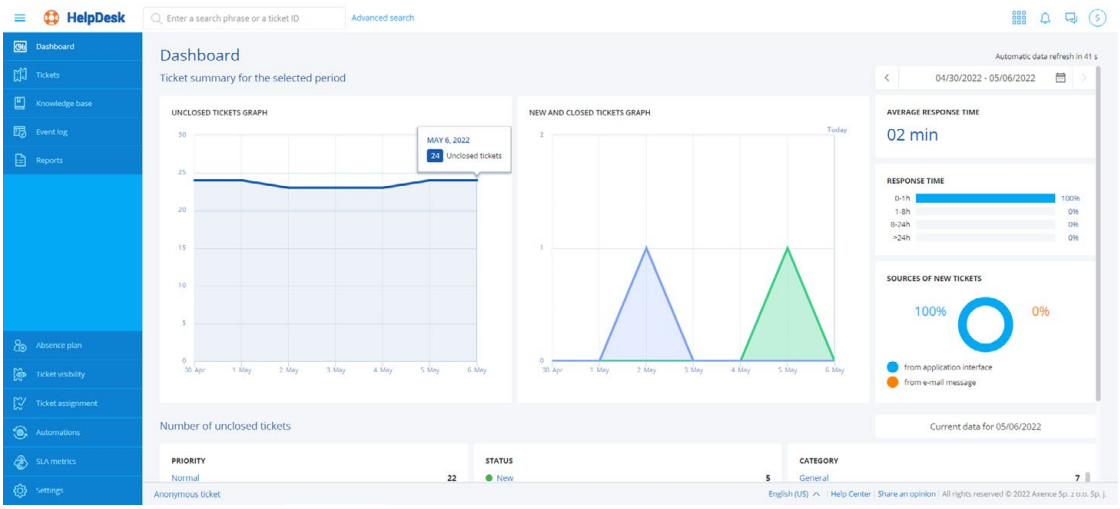
1. **Ticket Categories:** HelpDesk allows Administrators to create, edit, and delete ticket categories. When users submit a new ticket, they can select a relevant category to classify their issue accurately.

2. **Priorities:** Administrators have the flexibility to create, edit, and delete priority levels for tickets. These priorities assist in determining the urgency and importance of each ticket, aiding support personnel in efficiently managing their workload.

3. **Submission Forms:** HelpDesk enables the creation, editing, and deletion of submission forms. These forms consist of additional questions assigned to specific ticket categories, guiding users to provide more detailed information. Users can select predefined answers or enter their own responses into the provided fields.

4. **Ticket Assignment Rules:** Administrators can establish ticket assignment rules, automating the process of assigning tickets to the appropriate Administrators and support staff. These rules are particularly useful when designating specific employees to handle certain ticket categories or user groups, ensuring efficient and targeted ticket allocation.

5. **Automations:** HelpDesk empowers Administrators to create automations that simplify management tasks. Depending on the organization's needs, these automations can streamline processes such as changing ticket categories, modifying ticket status, adding internal comments, or including users in the watch list. Automations help streamline workflows and reduce manual effort.



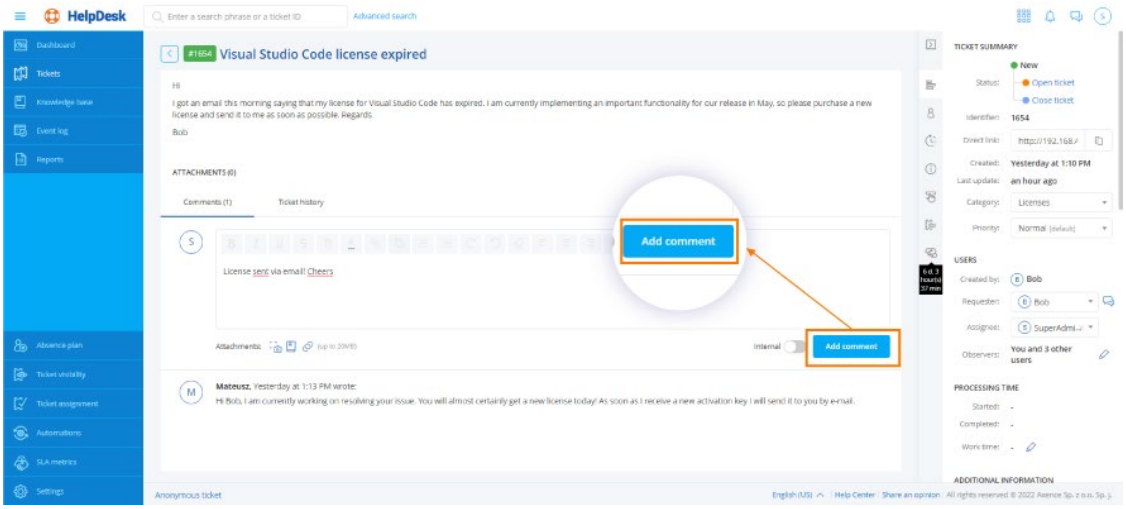

**Ticket processing:** Once a ticket is assigned to an assignee in HelpDesk, various actions can be performed to manage and resolve the issue efficiently. Some of the key actions available to the assignee are:

1. **Change Category, Status, or Priority:** The assignee has the ability to modify the category, status, or priority of the ticket as needed. This ensures accurate classification and prioritization of the issue within the HelpDesk system.

2. **Change Requester:** In cases where the problem concerns another person or a different user account, the assignee can update the requester information associated with the ticket. This ensures that the correct individual is associated with the ticket and receives updates on its progress.

3. **Add an Observer:** The assignee can include additional individuals as observers on the ticket. Observers are kept informed about the ticket progress and updates, allowing them to stay involved or informed about the resolution process.

4. **Add a Comment:** The assignee can provide comments within the ticket to communicate important information about the progress or status of the ticket. Observers can also use comments to request additional information from the requester. This fosters effective communication within the HelpDesk system.



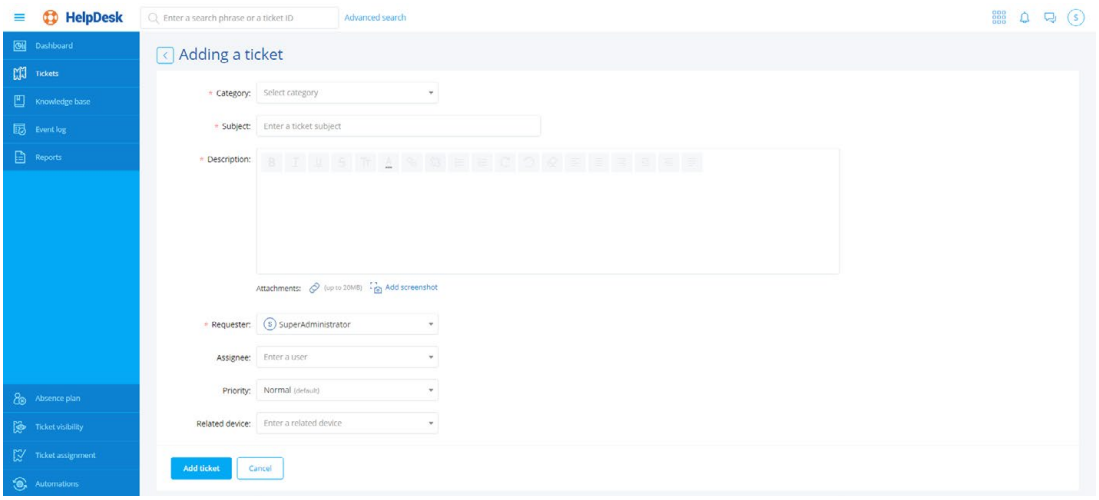

**Ticket progress tracking:** During the ticket lifecycle, the requester can continue to add comments, either to answer questions or seek further clarification. This ensures that all communication remains centralized within HelpDesk. The assignee and other actively involved parties receive notifications and emails to stay informed about the ticket's progress.

By leveraging these ticket processing features, HelpDesk enables smooth collaboration and effective communication, ensuring efficient resolution of issues while keeping all stakeholders informed.

## Creating tickets

To create a ticket in the HelpDesk interface:

1. Open a web browser and enter the HelpDesk address.
2. Alternatively, if you are already logged in as an agent, open the agent menu and select Your tickets.
3. In the Your tickets section, locate and click on the Add ticket option.
4. Depending on your role in HelpDesk, the number of available options may vary. As a user, select a category, enter the subject of your ticket, and describe your problem. If the issue requires it, add an attachment (up to 20 mb) or a screenshot.
5. Click add ticket button to create a ticket. If you have filled out the form correctly, the ticket will be created.



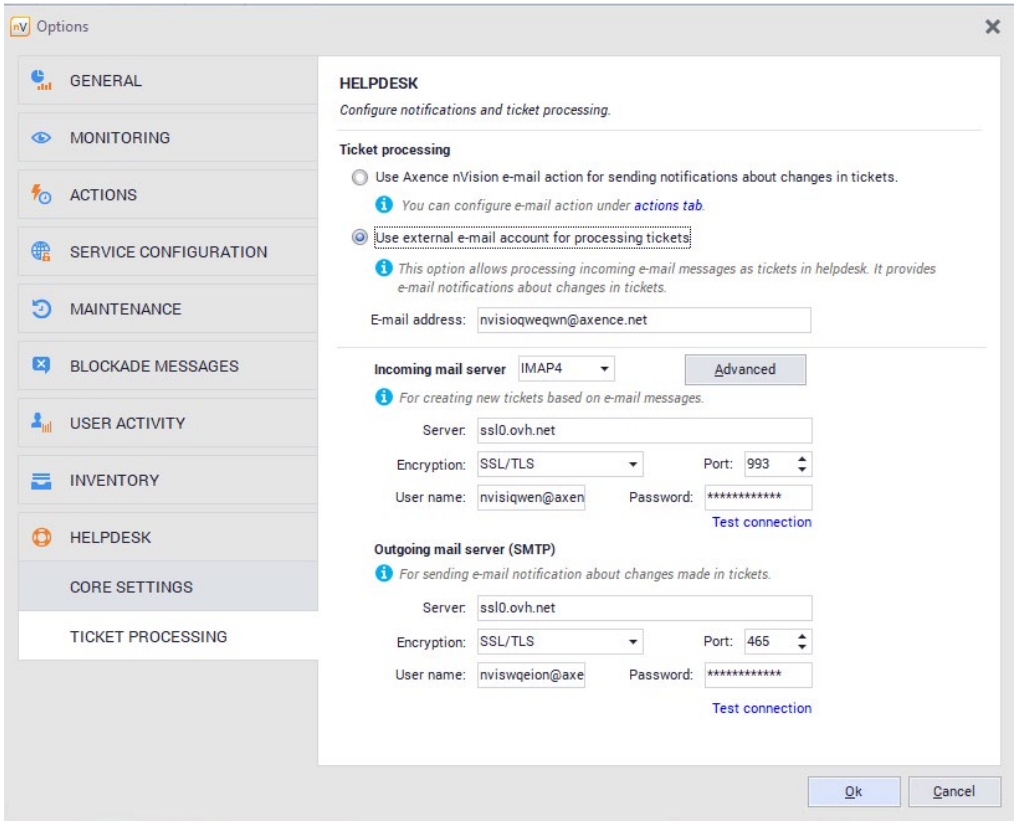

## E-mail processing

This option enables e-mail notifications about changes made in the tickets to be sent and also allows e-mail messages sent by users to the defined e-mail address to be processed. As a result of this, users can create new tickets without access to the HelpDesk ticket database. In order for the tickets to be created, the requester must have a unique e-mail address assigned to their

account in nVision. This means that a user without an nVision account will not be able to create a new ticket by sending an e-mail message.

### To use HelpDesk settings for e-mail processing:

1. Open the HelpDesk settings by selecting the Options menu.
2. Navigate to the HelpDesk section within the options menu.
3. Locate the Ticket processing option and click on it.
4. In the ticket processing settings, choose the Use external e-mail account for processing tickets option.
5. Specify the e-mail address where the trouble reports should be sent. This address will serve as the mailbox that nVision HelpDesk will monitor to create tickets based on received messages.
6. Configure the incoming and outgoing mail server settings according to your email provider's specifications. This information is necessary for HelpDesk to communicate with the designated mailbox.
7. To ensure the entered settings are correct, click the Test connection button to verify the connection to the mail server.

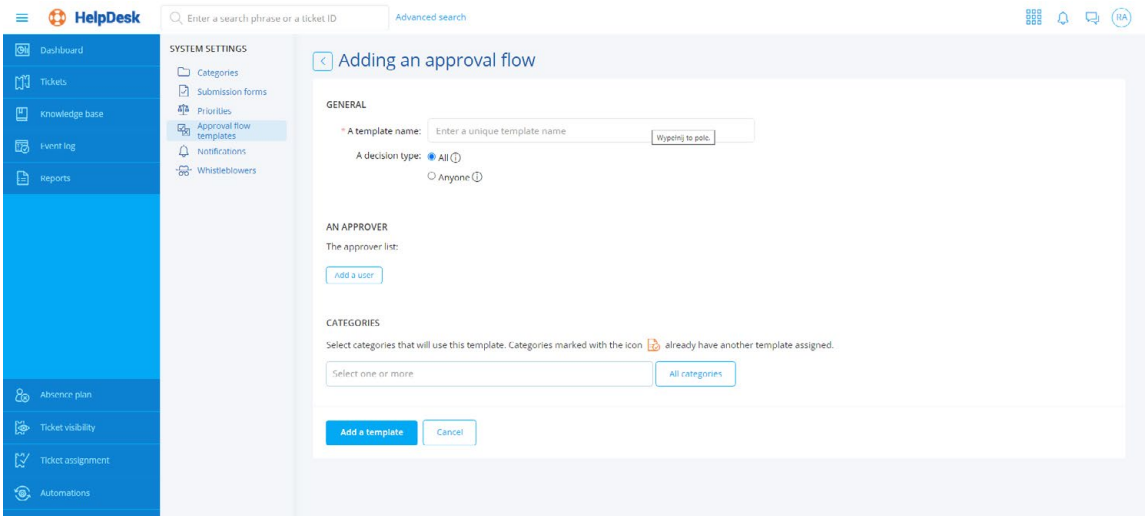


**Note:** It is important to note that all messages in the inbox of the specified e-mail address will be deleted. It is recommended to create a dedicated account solely for ticket processing purposes.

## Adding a new automation for ticket processing

### To add a new automation in HelpDesk:

1. In the automation list, locate and click the Add automation button.
2. Fill in the following fields:
   - *Name:* Specify the name of the new automation.
   - *Description (optional):* Add a short description of the automation's operation.
3. Determine the automation status after it has been created.
4. Specify the automation trigger type based on when it should be performed. Choose from the following options:
   - Daily: An automatic procedure for checking the list of unclosed tickets is launched every day. Conditions defined by the administrator are checked, and corresponding actions are taken. For example, you can set the status to Closed for tickets not updated for 14 days.
   - After a new ticket has been created.
   - After a ticket has been updated.



5. Define the condition application logic:
    - Specify whether the automation should be applied if the processed ticket meets any or all of the conditions defined below.
    - To add another condition, click the Add condition link.
6. Specify the actions to be taken if the trouble ticket meets the conditions:
    - To add another action, click the Add action link.
7. Save the automation by clicking the Add automation button.

Please note that automations can be edited, deleted, deactivated, and reactivated. However, automations do not allow the creation of automation chains, where multiple automations trigger each other.

## Ticket visibility

HelpDesk provides three levels of ticket visibility. Each level determines which tickets users can browse.

1. Basic Visibility: Users can browse tickets in which they are the reporter, the assignee, the approver, or are listed as observers.
2. Expanded Visibility: Users can browse tickets in which they are the reporter, the assignee, the approver, or are listed as observers. In addition, users with expanded visibility can browse tickets based on the following criteria:
    - Category is equal to <selected categories>.
    - Category is not equal to <selected categories>.
    - Requester belongs to a group <selected groups>.
    - Requester does not belong to a group <selected groups>.
3. Full Visibility: Users with full visibility can browse all tickets, regardless of their role or ticket attributes.

# 9. Ticket approval flows

In organizations where approval from multiple individuals is required for various processes such as equipment purchasing or access granting, HelpDesk offers a robust ticket approval flow feature.

**Ticket approval flow templates** are associated with specific ticket categories in HelpDesk. They allow you to define the following parameters:

1. **Decision Type:**
   - *All:* All designated Approvers must accept the ticket for it to proceed.
   - *Anyone:* At least one Approver from the list needs to accept the ticket.

2. **Approver List:**
   - *Dedicated User:* You can select a specific Approver from the list of all users in the system.
   - *Selected by Ticket Creator:* The ticket creator has the option to choose the Approver when creating a new ticket.
   - *Selected by HelpDesk Staff:* The Approver is selected by the HelpDesk staff, typically based on the information provided within the ticket.

**Notifications:** Once a ticket enters the approval flow in HelpDesk, the designated Approvers are notified through HelpDesk notifications or by email. This ensures that Approvers are promptly informed about pending tickets requiring their approval.

Administrators have the flexibility to modify the flow within an existing ticket. The following actions can be performed:

1. **Modify the Order of Approvers:** Administrators can rearrange the order in which Approvers are listed within the approval flow. This allows for customization and adjustment based on specific requirements or changes in organizational processes.

2. **Add, Delete, or Change Decision Type:** Administrators have the ability to add or remove Approvers from the flow, as well as change the decision type (e.g., switching from “All” to “Anyone” or vice versa). This flexibility allows for dynamic adjustments in the approval process.

3. **Delete the Approval Flow:** If necessary, Administrators can completely remove the approval flow from the ticket. This action is useful in cases where the approval process is no longer required or if there are changes in the organizational workflow.

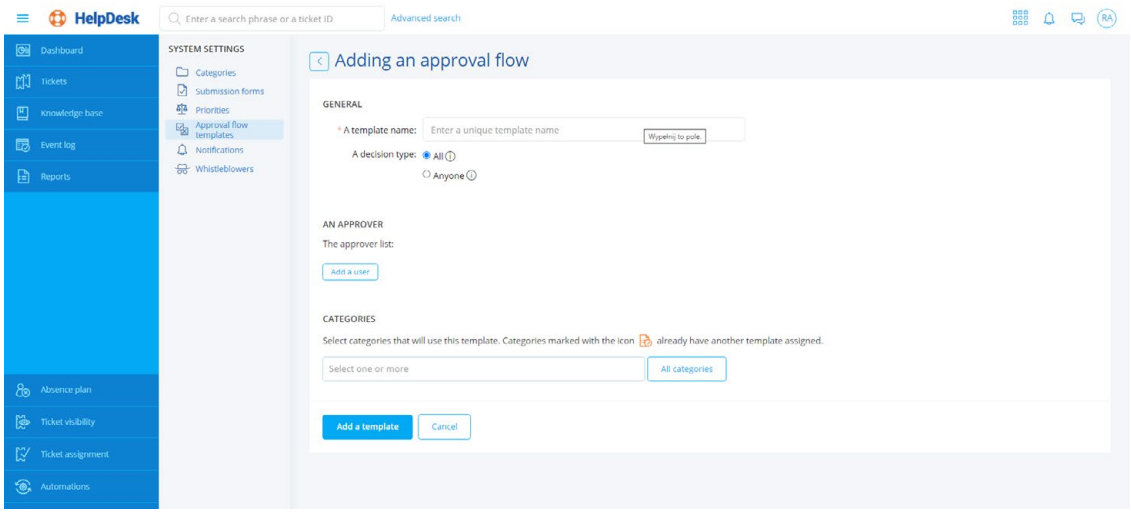
4. **Load Approval Flow Templates:** HelpDesk enables Administrators to load predefined templates for ticket approval flows. By using existing templates, Administrators can save time and effort in configuring approval flows, ensuring consistency and efficiency.

5. **Withdraw User Decisions:** In case of errors or mistakes, Administrators can withdraw the decision made by an Approver. HelpDesk automatically recalculates the final decision based on the remaining Approvers' responses.

## Creating approval flow templates

To create a new approval flow template, follow these instructions:

1. Go to the Settings tab.
2. Look for the Approval Flow templates option and and click on it.
3. In the Approval Flow templates section, locate and click on the Add a template button,
4. Enter a template name,
5. Add user(s) to the approver list,
6. Optionally choose a category that will use this template (we advise you to do so),
7. Create a new template by clicking on Add a template button.




After creating the template, it will be available in two locations: within the added ticket, where it can be added by an administrator, and in the form for creating a new ticket, if the user selects the appropriate category.

## 10. Software repository with approved application for self-installation

The Software Repository feature in HelpDesk enables Administrators to provide users with a curated list of applications that have been thoroughly tested and deemed safe for self-installation. This feature simplifies the process of deploying authorized software to users within the organization. Here's how it works:

1. **Adding MSI Packages:** Administrators utilize the HelpDesk console to add the appropriate MSI packages, which contain the installation files for the desired applications. These MSI packages serve as the foundation for the software repository.

2. **Creating Software Presets:** After adding the MSI packages, Administrators create software presets, defining specific sets of applications. They can select the user group(s) that will have access to these applications.

3. **Assigning Applications:** Administrators determine which applications are included in each software preset. This allows them to customize the available application list based on the needs of different user groups.

4. **User Access and Installation:** Users who belong to a group associated with a specific software preset can access the Software Repository from the Agent's menu. They gain the ability to independently install selected applications, view the status of installed applications, and perform other relevant actions.

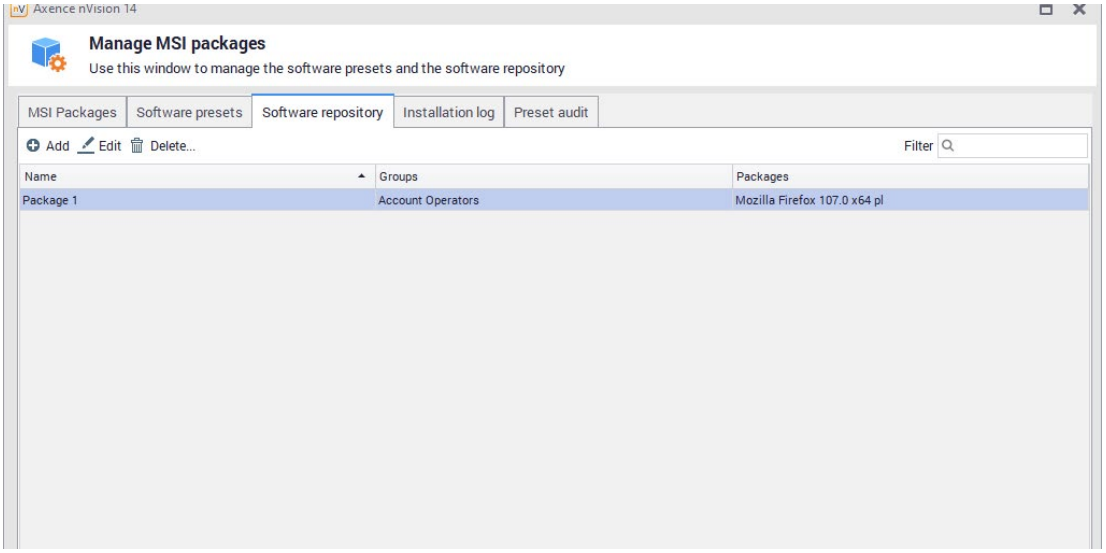
The Software Repository feature simplifies the process of software installation by providing users with a convenient and secure way to access approved applications. By leveraging the Software Repository, organizations can streamline application deployment and empower users with self-installation capabilities, enhancing productivity and flexibility within the workforce.

## Managing MSI packages

To manage MSI packages:

1. Select the MSI Package Manager option from the main menu.
2. In the Manage MSI Packages window, click the Add button.
3. In the dialog box, browse and select the MSI installer file.
4. In the package addition window, set the installation priority (considered when installing multiple packages within a group) and additional execution parameters (copied from the MSI installer manufacturer's page). Click Save.
5. Go to the Software Sets tab and click the Add button. Create a new group by specifying:
   - Group name
   - Devices on which the specified applications should be installed or uninstalled
   - Packages to be installed (created in step 4) or applications to be uninstalled (based on information collected by Agents monitoring registry entries of installed applications)

6. Click Save. The execution status on devices is presented in the Software Sets tab of the Manage MSI Packages window.
7. Both packages and software sets can be edited by double-clicking or selecting and clicking the Edit button. There is also an option to change the priority and download the MSI package.
8. In the Audit Sets tab, you can check the progress of installations.



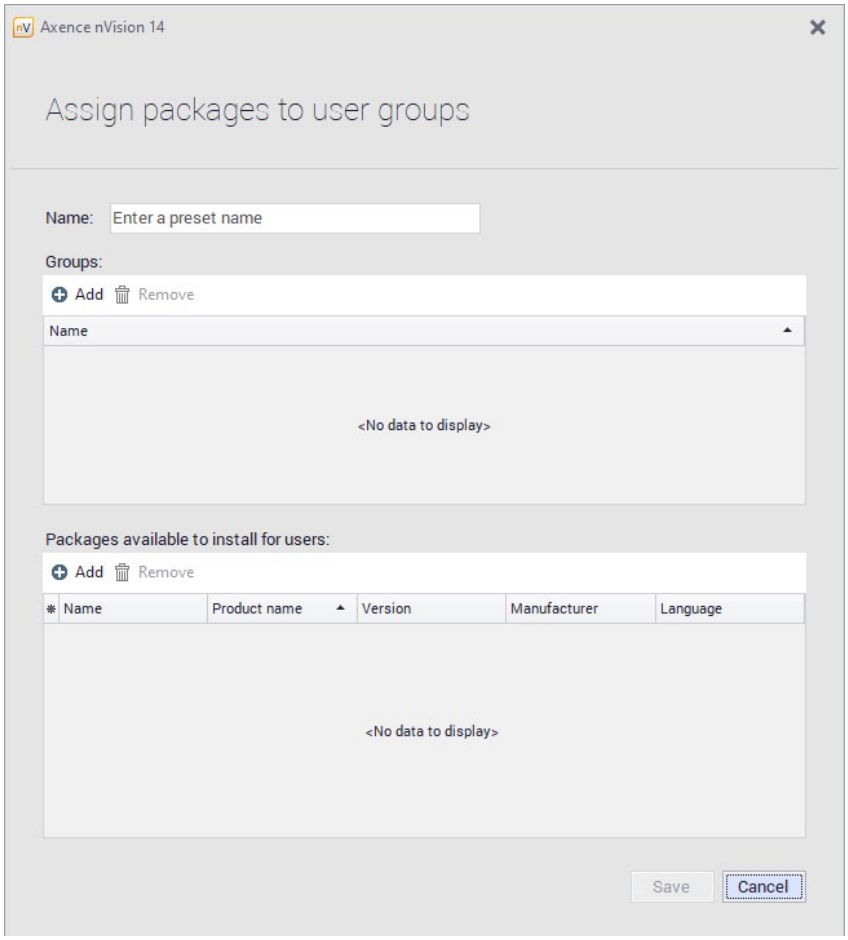

**Note:** The software repository in the nVision console is solely for assigning previously added MSI packages to specific user groups. Therefore, it is necessary to first add the MSI packages. Additionally, there should be at least one group in nVision to which the MSI package can be assigned. Once the packages are added and user groups are created (with appropriate users added to them), you can fully utilize the software repository functionality.

## Assigning an MSI package to a user group

To assign an MSI package to a user group:

1. Select the MSI Package Manager option from the main menu.

2. Click the Software repository tab and then click the Add button.
3. In the package assignment window, configure several required parameters:
   - *Name:* This field must be filled in.
   - *Groups:* Select the groups whose users will have access to specific applications. To add a group, click the Add button and choose the appropriate group(s) from the list. You can add multiple groups.
   - *Packages available for user installation:* Select the packages added in nVision (in the MSI Packages tab) that will be made available to users for self-installation. To add a package, click the Add button, then select the desired packages in the package selection window. Confirm the selection by clicking the Add button.
4. After configuring the above parameters, click the Save button to confirm your choices.



# 11. Knowledge base

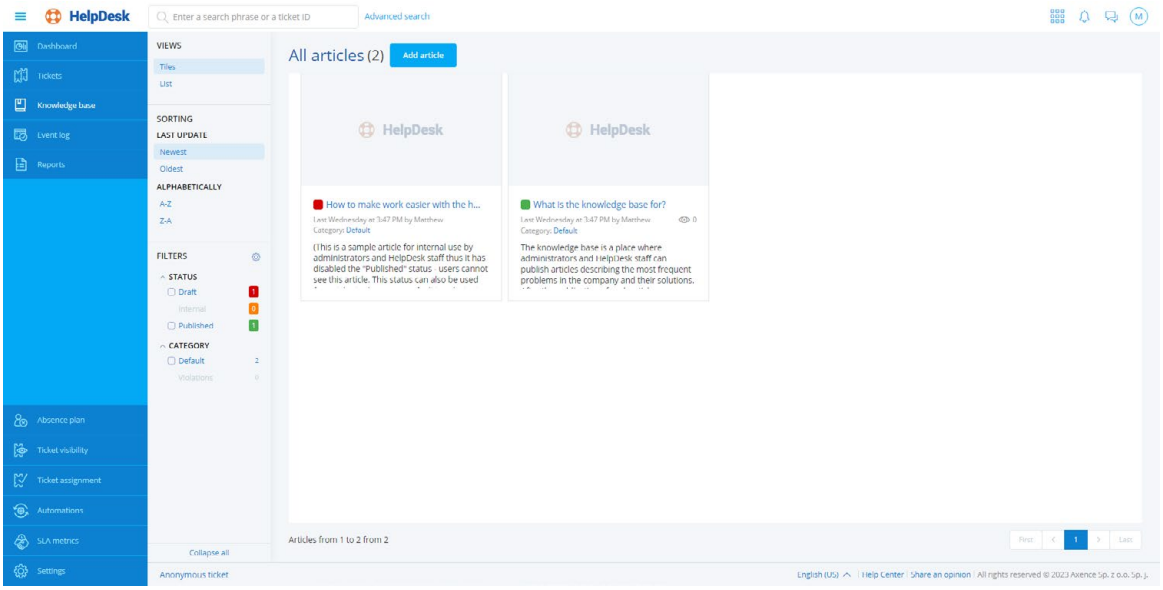
The Knowledge Base feature in HelpDesk provides a dedicated tab for Administrators and employees to publish informative articles, enabling efficient knowledge sharing within the organization. Whether it's guiding employees through specific procedures or offering valuable insights on various topics, the Knowledge Base serves as a versatile tool to address organizational needs. Here's what you need to know:

1. **Article Purpose and Flexibility:** Articles in the Knowledge Base serve multiple purposes, such as guiding employees through procedures, processes, or providing informative content on topics like cyber security. Each organization can utilize the Knowledge Base in ways that suit their specific requirements and goals.

2. **Comprehensive Article Content:** Articles can include various components to enhance their effectiveness. These components may include embedded links to relevant resources, attachments for additional information, and eye-catching cover images.

3. **Statuses for Controlled Publishing:** Articles within the Knowledge Base can have different statuses:
   - *Draft:* Administrators can create and work on unfinished articles without publishing them. This status allows for collaboration and refinement before making articles available to users.
   - *Internal:* Articles with the internal status are accessible to Administrators and support staff only. They serve as a resource for internal guidance and knowledge sharing within the Helpdesk team.
   - *Published:* Once articles are ready for broader access, Administrators can set them as published. Published articles are available to all users within HelpDesk.

4. **User-Specific Access:** Administrators have the flexibility to restrict article access to specific user groups. This ensures that articles are tailored to the intended audience and relevant to their roles and responsibilities within the organization.




# 12. Closed-circuit communicator

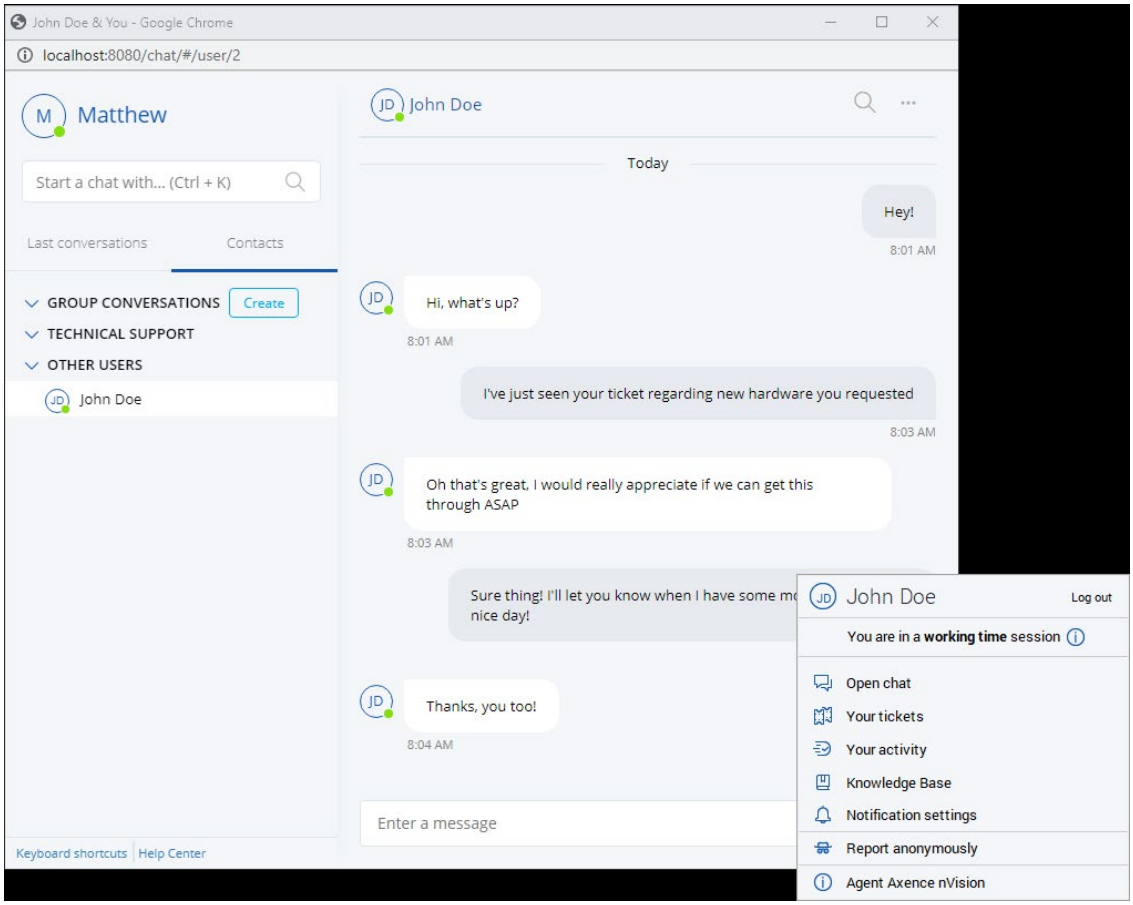
The HelpDesk Chat feature provides users with an instant messenger for efficient communication and collaboration. Along with the standard chat functions like sending and receiving messages, exchanging gifs and emoticons, and creating group conversations, HelpDesk Chat offers a range of additional capabilities:

1. **Closed/Internal Messaging:** HelpDesk Chat is designed as an internal messaging system, exclusively available to users added in nVision. This closed environment ensures secure and confidential communication within the organization.

2. **Accessibility:** Users can access the HelpDesk Chat feature via two different channels:
   - *Browser:* Chat is accessible through the HD (HelpDesk) > Chat section in the web browser interface.
   - *Agent Menu:* Users can also access the chat functionality directly from the Agent menu.

3. **Permission Levels:** HelpDesk Chat incorporates different permission levels to manage user access:
   - *No Access:* Administrators can restrict a user's access to the chat feature entirely.
   - *Technical Support Only:* Users with this permission level can interact with technical support staff, ensuring focused communication for issue resolution.
   - *Full Access:* Users with full access can enjoy all the features and capabilities of HelpDesk Chat.

4. **Message Search Engine:** The chat includes a powerful message search engine, allowing users to quickly locate specific parts of conversations. This feature enhances productivity and facilitates retrieving important information when needed.



### Enabling the Chat

To enable the chat feature in nVision HelpDesk:

1. Go to Options,
2. Open HelpDesk tab,
3. and then check the field next to the HelpDesk chat option.

## 13. ‘Aggressive’ announcements from IT

Axence nVision offers a powerful feature that enables Administrators to create announcements directly from the console. Announcements serve as a rapid and effective way to reach selected users and promptly communicate important information. Here’s what you need to know:

1. **Message Types:** When creating an announcement, administrators can choose from three types of messages to convey the appropriate urgency and importance:
   - *Information:* General messages to provide updates or share important information.
   - *Warning:* Messages indicating potential issues or concerns that require attention.
   - *Alert:* Critical messages that demand immediate action or response.

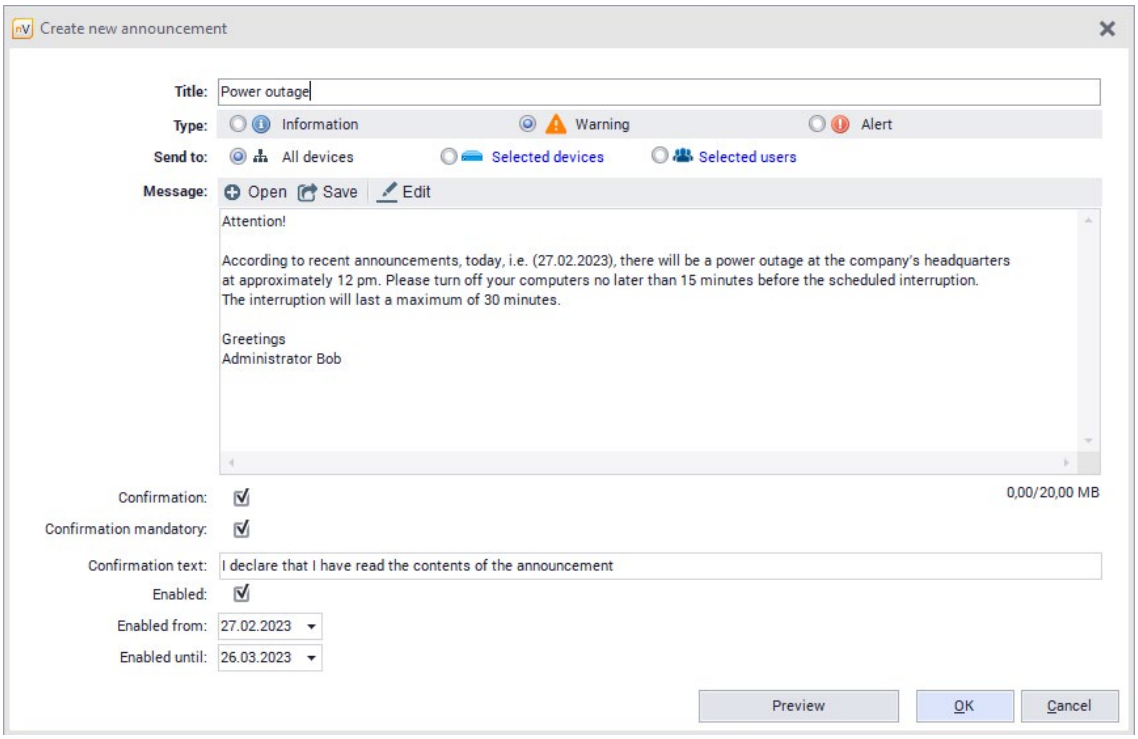
2. **Message Recipients:** Administrators have the flexibility to define the recipients of the announcement:
   - *All Devices:* The message will be delivered to all devices connected to the nVision system.
   - *Selected Users:* Administrators can choose specific users to receive the announcement.

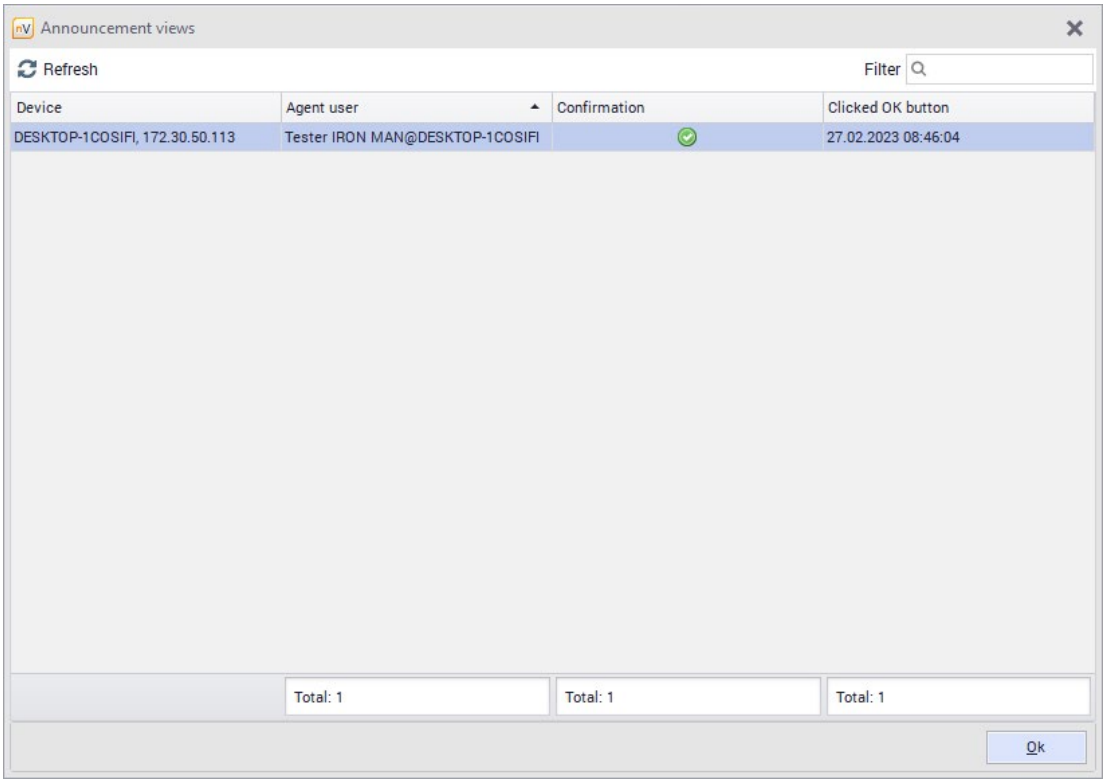
- *Selected Devices:* Targeted delivery to specific devices as per the Administrator's selection.

3. **Content and Multimedia:** Announcements can include various types of content to effectively convey the message, including text, images, and links. Administrators have the freedom to utilize these multimedia elements to enhance the clarity and impact of the message.

4. **Confirmation and Read Receipts:** To ensure message comprehension and track acknowledgment, Administrators can employ confirmation options:
   - *Confirmation:* Users can acknowledge receipt of the message voluntarily.
   - *Mandatory Confirmation:* Users are required to confirm receipt, accompanied by custom confirmation text, such as 'I confirm that I have read the message,' and a checkbox.

5. **Timing and Availability:** Administrators can select the time interval during which the announcement will be sent to users, specifying the start and end time for message availability.






# 14. Remote support tools for IT

**Remote Access Preview Mode:** Axence nVision® provides a convenient and non-intrusive method for remotely connecting to a user's workstation. This feature, known as preview mode in the remote access options, allows Administrators to observe a user activity without interfering with their ongoing work. Here's how you can utilize this functionality:

1. **Establishing Remote Access:**
   - In the Axence nVision console, locate the device you want to connect to remotely.
   - Right-click on the device and select Remote Access from the context menu. This will open the Remote Access window.

2. **Access Modes:**
   - Within the Remote Access window, you will find different access modes to choose from.
   - Select the View only mode to enable preview mode. This mode allows Administrators to solely observe the user's activities without actively intervening.

3. **Observing User Activity:**
   - Once connected in preview mode, you will be able to see the user's screen and monitor their actions in real-time. This passive observation enables Administrators to gather information, diagnose issues, or provide guidance without directly interfering with the user's tasks.

**Note:** Please note that in preview mode, the Administrator does not have control or the ability to manipulate the user's actions. The primary focus is on passive observation to gather information or diagnose issues. This feature enables effective troubleshooting and support without interrupting or disturbing the user's workflow.

## Establishing Remote Access

To establish a remote connection directly within HelpDesk for a user who requires immediate technical support:

1. Display the details of the ticket associated with the user currently being processed.
2. Locate the VNC option next to the Related device. The related device is automatically selected during ticket creation if the Agent is installed on the user's workstation. Alternatively, you can manually choose the desired device from the list of all devices monitored by nVision.

# 15. Remote sessions to an employee

**Remote Access Concurrent Mode:** Axence nVision® also provides a remote access feature that allows Administrators to establish a simultaneous connection to a user's workstation. This unique mode, known as concurrent access, enables both the user and the remotely connected Administrator to perform actions on the device together. Here's how you can leverage this capability:

1. **Initiating Remote Access:**
   - To remotely connect to a device, begin by locating the desired device in the Axence nVision® console.
   - Right-click on the device and select Remote Access from the context menu. This will open the Remote Access window.

2. **Access Modes:**
   - Within the Remote Access window, you will find various access modes available. For concurrent access, select the Concurrent access mode. By choosing this mode, the Administrator gains the ability to establish a joint session with the user, allowing both parties to interact with the device simultaneously.

3. **Collaborative Support:**
   - Once connected in concurrent mode, both the Administrator and the user can perform actions on the workstation simultaneously. This collaborative approach empowers the Administrator to provide more direct and hands-on support, utilizing the connected workstation just like a regular user.

By enabling concurrent access, Axence nVision® enhances the support experience by fostering real-time collaboration between administrators and users. This mode enables efficient troubleshooting, guided assistance, and seamless cooperation, resulting in faster issue resolution and improved user satisfaction.

## 16. Control operations on local, network* and media files

**Monitoring Local Directories:** The monitoring of local directories in Axence nVision® allows you to keep track of file operations within specific locations. This feature provides flexibility at three levels: Atlas, Group, and User. Here's how you can utilize and configure the monitoring settings:

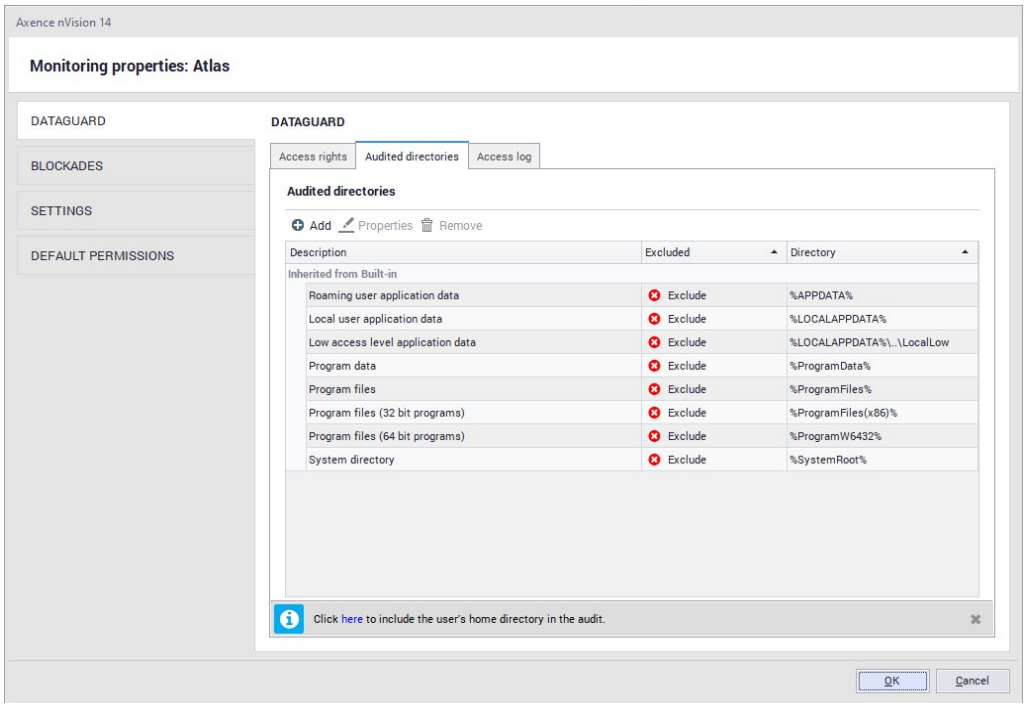
1. **Setting Levels:**
   - Atlas (Highest Level): The Atlas setting acts as the default configuration inherited by groups and users. Individual units can customize this setting by accessing the corresponding Setting windows.
   - Group Level: The monitoring settings can be customized for specific groups, allowing tailored monitoring configurations for different user segments.
   - User Level: Users can have personalized monitoring settings that cater to their specific requirements.

2. **Adding Monitored Directories:**
   - To add a directory for file operation monitoring, provide the rule name and the path to the target directory.
   - The path to the directory can be specified in two forms:
     - ◊ Absolute Form: Start with a drive letter (e.g., "C:\n") and include the full name of the monitored directory.
     - ◊ Environment Variable Form: Enclose an environment variable within "%" characters. The variable can replace any part of the path. For example, "%USERPROFILE%" can represent "C:\Users."

3. **Automatic Inclusion:**
   - When you add a directory for monitoring, the entire content within that directory, including subdirectories and files, is automatically included in the monitoring process.

4. **Monitoring Operations:**
   - After adding a rule, you will be able to monitor file operations within the specified directory. The system tracks and logs any relevant actions taking place in that location.

5. **Monitoring Operations:**
   - The DataGuard module maintains a list of built-in directories that are excluded from system-wide scanning. These directories cannot be modified and are always excluded from monitoring.
   - You can view the list of globally excluded directories in the DataGuard settings.





Axence nVision's local directory monitoring feature empowers you to stay informed about file operations in specific locations. By configuring the monitoring settings at the desired level and adding directories for monitoring, you can effectively track and manage file activities within your organization.

# 17. Storage media management

**Device Access Rights Management:** The DataGuard module in Axence nVision® offers media management capabilities, specifically focusing on creating and managing access rights for devices. This feature allows you to control and monitor device connections and disconnections on workstations. By utilizing the device access rights management feature, you can effectively control and monitor device connections, ensuring the security and proper usage of various media and devices within your organization.

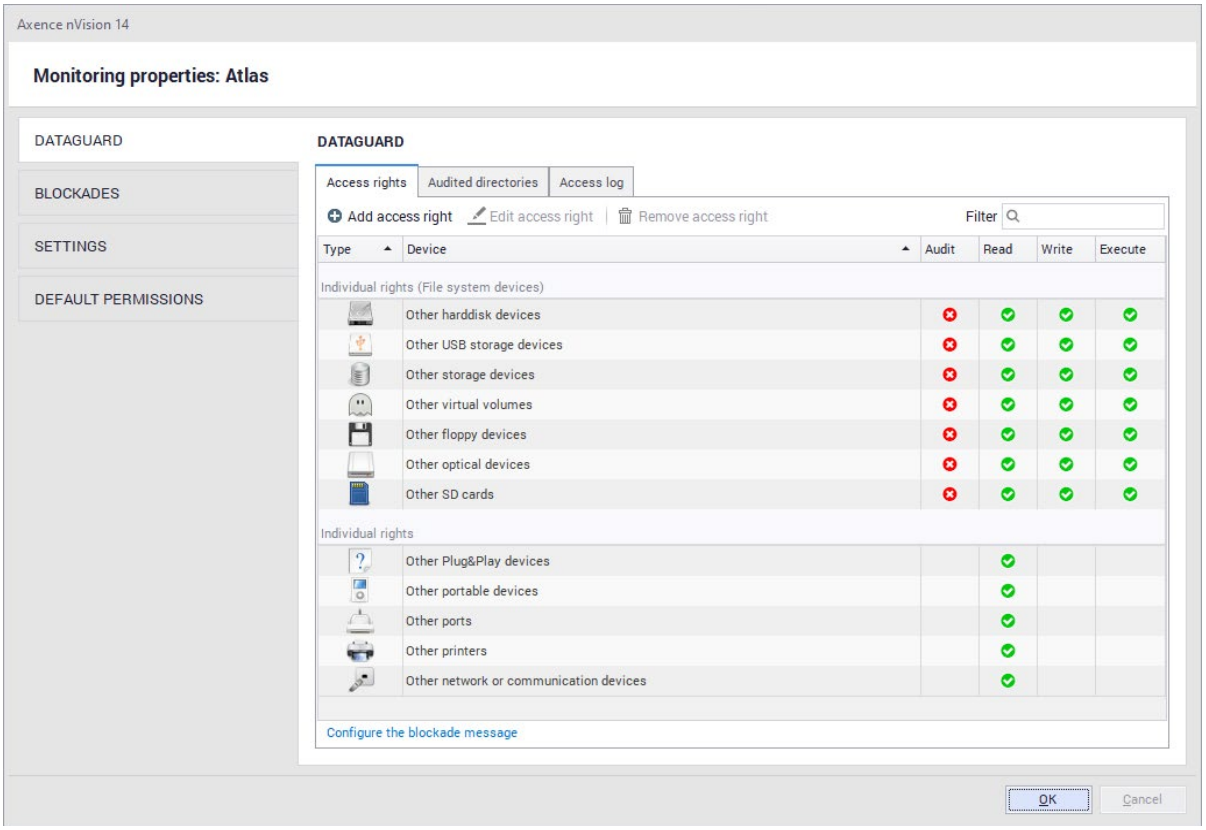
Here's what you need to know to utilize the device access rights management functionality:

1. **Access Right Parameters:**
   - *Audit:* Determines whether access to a specific device is logged. Logging includes activities such as file renaming, creation, copying, deletion, and write access.
   - *Read:* Grants the ability to read information from the specified media or device.
   - *Write:* Provides permission to write information to the designated media or device.
   - *Execute:* Allows running programs located on the specified media or device.

2. **Access Right Options:**
   - *Audit:* Enables or disables the logging of access to a device.
   - *Read:* Allows or blocks the ability to read information from the device.
   - *Write:* Allows or blocks the ability to write information to the device.
   - *Execute:* Allows or blocks the execution of programs located on the device.

3. **User and Group Access Rights:**
   - Access rights can be assigned directly to individual users or groups.
   - Access rights can also be inherited from higher levels, such as group or system settings.
   - The displayed order of rights is as follows: individually assigned rights are shown first, followed by inherited rights.

4. **Detectable Media and Devices:** The DataGuard module can detect and manage access rights for a wide range of media and devices, including:
   - Hard drives
   - Optical devices (CD/DVD drives)
   - USB data storage devices (e.g., USB flash drives, external hard drives)
   - Virtual volumes (virtual disk drives)
   - Data storage media, such as SD cards
   - Soft media (e.g., floppy disks)
   - Network and communication devices (Bluetooth receivers, infrared devices, network cards, modems)
   - Portable devices
   - Wireless communication devices
   - Ports (e.g., Firewire, serial ports)
   - Printers
   - Plug and Play (PnP) devices (imaging devices, smart cards, etc.)



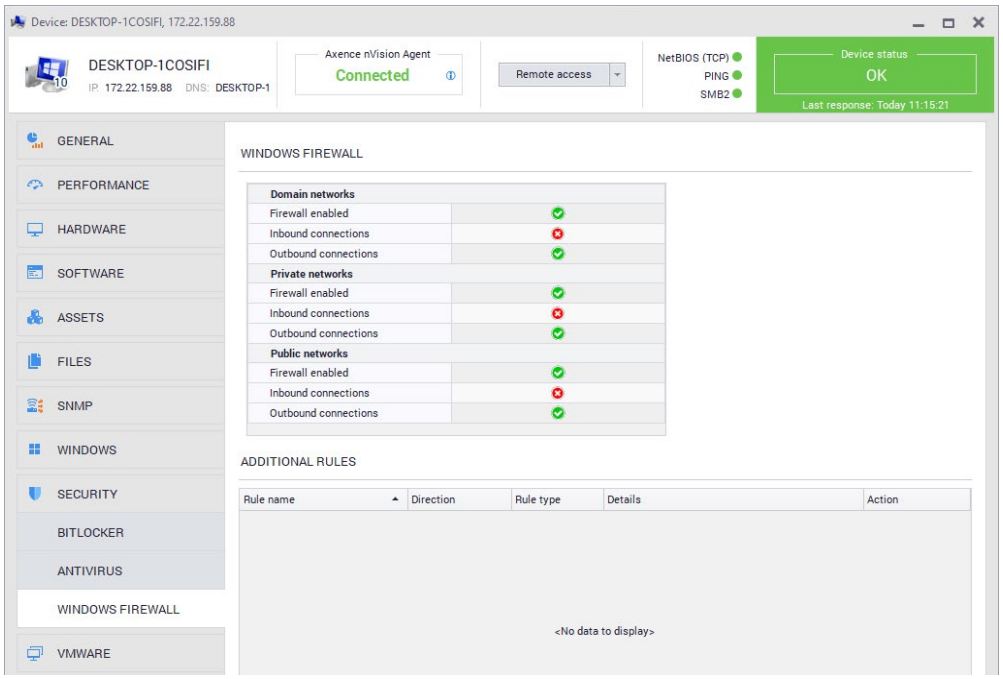
# 18. Knowledge of FW, AV and BitLocker settings

The DataGuard module in Axence nVision® empowers you with comprehensive capabilities to monitor and manage essential security aspects on workstations. With its functionality for Firewall, antivirus software (Windows Defender), and drive encryption (BitLocker), you can ensure robust security and protect sensitive data.

**Firewall Monitoring:**

1. **Viewing Firewall Settings:** To view the Firewall settings on a selected workstation, follow these steps:
   - Open the Settings window of the desired device.
   - Navigate to the Security tab and click on Windows Firewall.

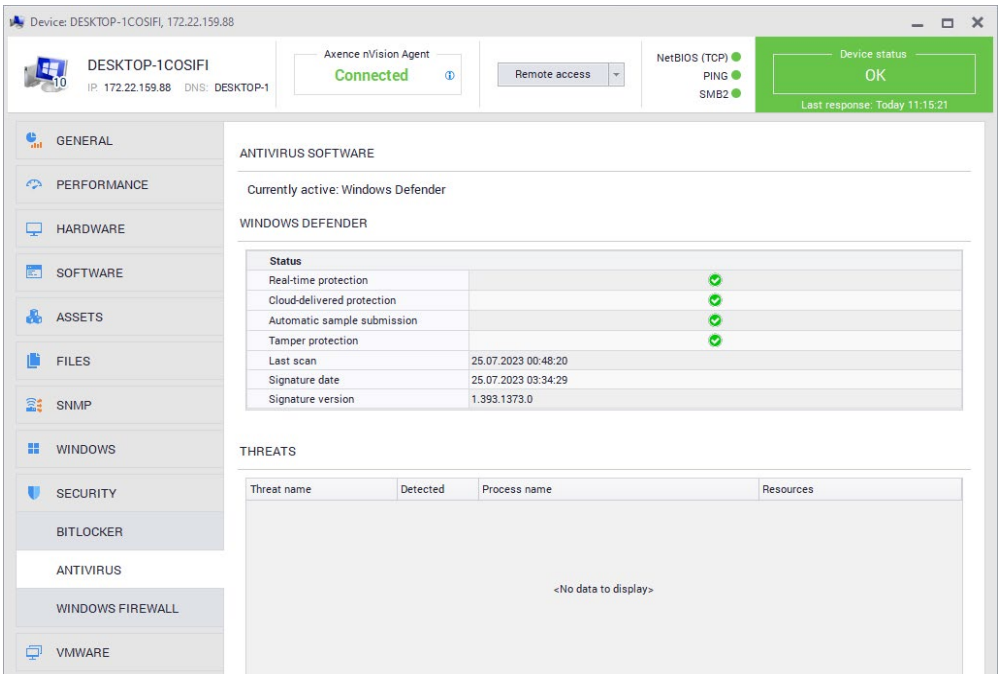
2. **Firewall Status and Parameters:** In this view, you can see the Firewall status and configure incoming and outgoing connections for three network types: domain, private, and public.




**Note:** nVision provides visibility into Firewall settings but does not offer additional configuration options beyond what Windows Firewall provides. It allows you to read and monitor the settings on the workstation.

## Windows Defender Monitoring:

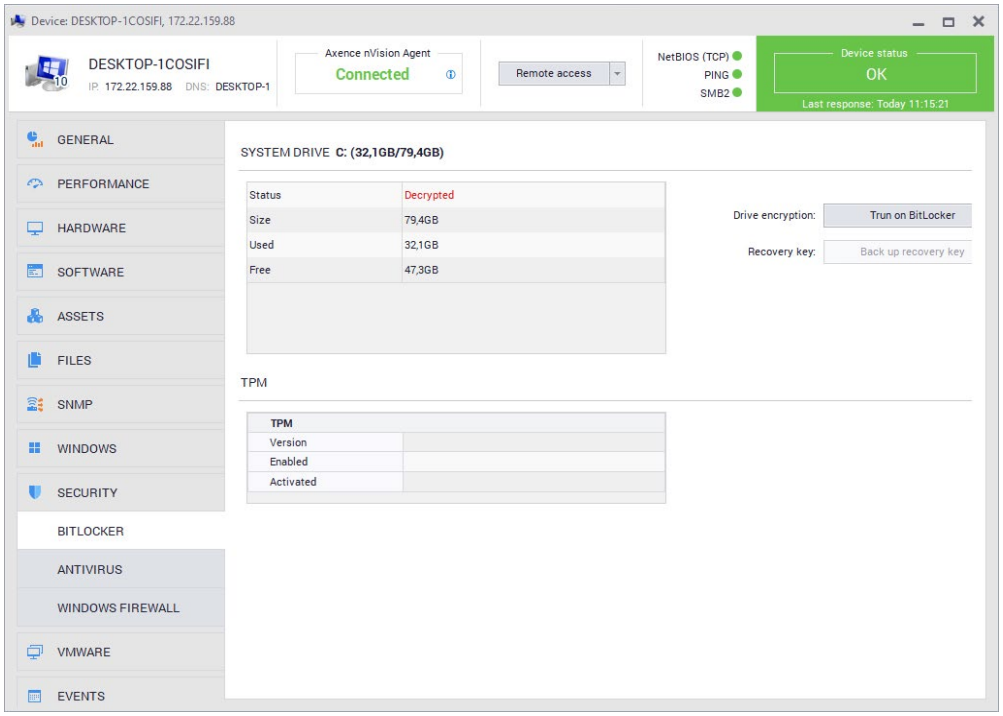
1. **Windows Defender Parameters:** The Windows Defender tab displays various parameters related to antivirus protection, including real-time protection, cloud protection, automatic sample uploading, infringement protection, last scanning information, and definition details.
2. **Threat Detection:** You can also view a list of detected threats by the Windows Defender antivirus software.




**Note:** The information displayed in the Security tab is retrieved using the Windows Defender API. nVision reflects the Windows security status, specifically the Virus and Threat Protection Settings configured on the workstation. While nVision allows you to view and edit these settings, please be aware that if Windows Defender is integrated with third-party antivirus software, those programs may overwrite any settings edited in nVision.

## BitLocker Drive Encryption Monitoring:

1. **Drive Encryption Status:** nVision retrieves and displays information about the drives on the workstation, indicating whether they are decrypted or encrypted. This provides visibility into the drive encryption status without the ability to modify the settings.

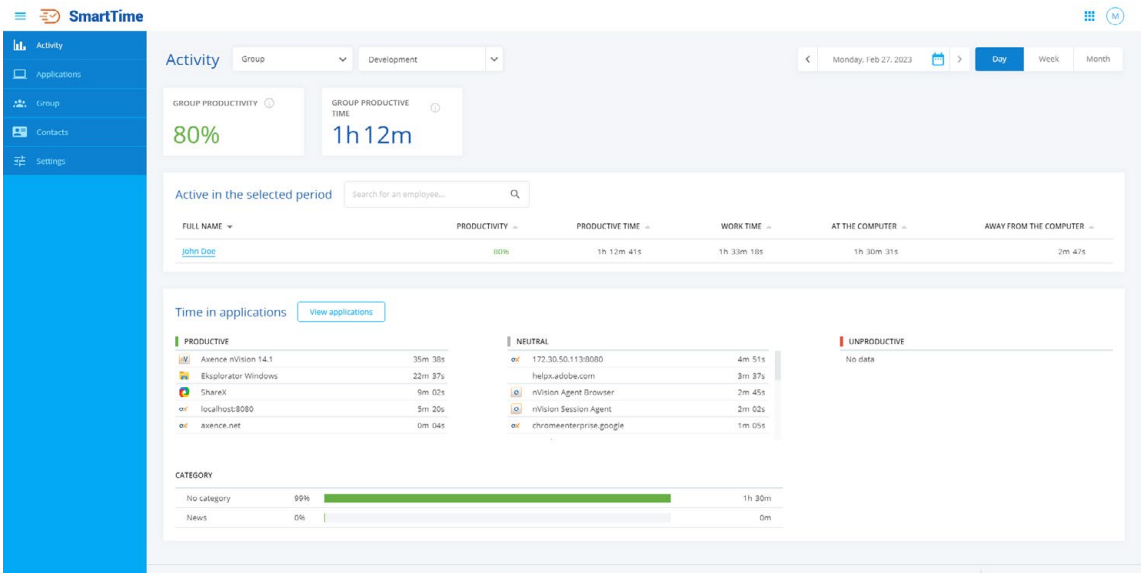



**Note:** The BitLocker parameters are for informational purposes only and cannot be edited within nVision.

## 19. Clear activity summary for the manager

The SmartTime module in Axence nVision® provides users with the ability to track their application activity, while allowing managers to monitor and verify the activities of their subordinates. By collecting user activity data through the nVision Agent, SmartTime presents this information in an easily accessible format within a web browser window.

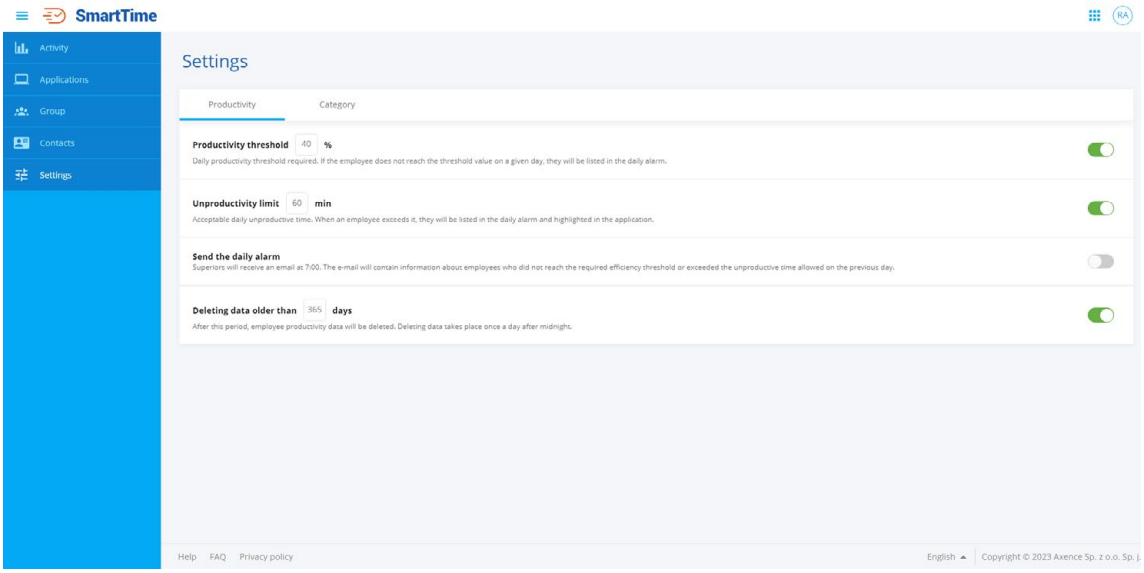
1. **Key features:**
   - *User Activity Data:* Gaining insights into the activity data of employees and teams, allowing you to assess their application usage and productivity levels.
   - *Visited Sites and Used Applications:* Access a detailed list of visited websites and applications used by users, providing a comprehensive overview of their digital activities.
   - *Manager Reports:* Generating reports specifically designed for managers, highlighting users who have not met specific productivity thresholds.




2. **Productivity Levels:** SmartTime categorizes applications into three productivity levels: Productive, Neutral, and Unproductive. Each level reflects the impact an application has on user productivity. You can customize productivity parameters for each group, manage users, and create exceptions for specific applications.

## 3. Thresholds and Settings:

- *Productivity Threshold:* Administrators can set a daily productivity threshold, expressed as a percentage, which users are expected to achieve in their application activity.
- *Unproductivity Limit:* Define a daily limit on the amount of time an employee can spend in applications categorized as unproductive in SmartTime.
- *Daily Alarm:* Mangers can receive daily email notifications, known as the "daily alarm," when users fail to meet the productivity threshold or exceed the unproductivity limit.



# Working **remotely?**

Let Axence make it even better for you.

Check out **axence.net** and discover tools that simplify and enhance your remote work setup.