

nVision 13 axence®

User manual

Axence nVision Help

Total Network Visualization and Management

Copyright © 2023 Axence sp. z o. o. sp. j.

Axence nVision gives you everything you need to manage your network in an efficient and effective manner. The application consists of 6 modules, which offer: proactive network monitoring and visualization, hardware and software inventory, user monitoring, remote technical support, data leakage prevention and users activity monitoring.

Axence nVision Help

Copyright ©2023 Axence sp. z o. o. sp. j. All rights reserved.

The entire risk of the use or the result of the use of this software and documentation remains with the user. No part of this documentation may be reproduced in any means, electronic or mechanical, for any purpose, except as expressed in the Software License Agreement.

This software and documentation are copyrighted. All other rights, including ownership of the software, are reserved to Axence Inc.

Axence Inc., Axence nVision and Axence netTools are trademarks or registered trademarks of Axence Inc. All other product and brand names are trademarks or registered trademarks of their respective owners.

Contents

| | |
|--|-----------|
| | 0 |
| Part I Introduction | 1 |
| 1 Axence nVision modules | 2 |
| 2 Axence nVision versions | 3 |
| 3 Functionality of modules | 3 |
| 4 Administrator Access Log | 8 |
| 5 Axence account | 9 |
| Description | 9 |
| Registration | 10 |
| Log in | 12 |
| Language management | 14 |
| Manage Axence account | 14 |
| Activation | 15 |
| Part II Requirements and configuration | 19 |
| 1 System requirements | 20 |
| 2 Ports | 22 |
| 3 Remote nVision Console | 23 |
| 4 Window layout | 24 |
| 5 Configuration | 27 |
| Basic configuration | 27 |
| Monitoring and managing Windows with WMI | 28 |
| Monitoring and blockades | 30 |
| Monitoring settings | 30 |
| Blocking settings | 33 |
| Settings migration (nVision 9 to 10) | 36 |
| User accounts | 36 |
| Monitoring settings | 36 |
| Blocking settings | 38 |
| Blockade notifications | 39 |
| Screenshots | 40 |
| DataGuard settings | 40 |
| Alerts and reports | 41 |
| Downgrade to nVision 9 | 41 |
| Main program settings | 42 |
| Information for advanced users | 45 |
| 6 nVision performance | 45 |
| 7 “Report a problem” function | 46 |
| 8 GSM device configuration | 47 |
| Part III Network discovery and monitoring | 49 |
| 1 Introduction | 50 |
| 2 Host status concept | 50 |
| 3 Discovering the network | 51 |
| Discovering the network | 51 |
| Network discovery wizard | 53 |

| | |
|---|------------|
| Adding a new host | 55 |
| 4 Monitoring | 55 |
| Introduction to monitoring | 55 |
| Concepts | 56 |
| Monitoring services | 57 |
| Service discovery and monitoring..... | 57 |
| Managing monitored services | 59 |
| Setting-up alert for services | 60 |
| Monitoring Windows services..... | 61 |
| Monitoring device and system performance | 61 |
| Performance counters and host status | 61 |
| Counter types..... | 62 |
| Managing performance counters..... | 62 |
| Setting-up alert for performance counter | 63 |
| Creating a counter on many hosts at once..... | 63 |
| Defining counter properties..... | 64 |
| Monitoring mail and web server | 66 |
| Mail and web server monitoring counters..... | 66 |
| Counter types..... | 66 |
| Defining counter properties..... | 67 |
| Monitoring routers and switches | 68 |
| SNMP monitoring..... | 68 |
| Monitoring switch ports..... | 68 |
| Monitoring node network traffic..... | 69 |
| MIB file compiling | 70 |
| SNMP traps | 71 |
| Syslog server | 74 |
| Wake On LAN | 77 |
| | |
| Part IV Hosts, maps and ActiveDirectory sync. | 81 |
| 1 Introduction | 82 |
| 2 Host info window | 82 |
| 3 Global Browser | 85 |
| 4 Maps | 90 |
| Overview | 90 |
| Map types | 90 |
| Map objects | 91 |
| Managing maps | 91 |
| Working with maps | 92 |
| Static map objects – properties | 96 |
| 5 Hosts | 98 |
| Overview | 98 |
| Host visualization | 99 |
| Managing hosts | 101 |
| 6 Styles | 101 |
| Overview | 101 |
| Defining styles | 102 |
| Managing styles | 104 |
| 7 Departments | 105 |
| Overview | 105 |
| Creating a department structure | 105 |
| Adding devices to departments | 106 |
| Reports | 107 |
| 8 SmartMaps | 107 |
| Overview | 107 |

| | |
|--|------------|
| Filters | 107 |
| Creating a filter | 108 |
| Creating a SmartMap | 109 |
| 9 ActiveDirectory devices | 110 |
| Part V nVision Agent | 113 |
| 1 Introduction | 114 |
| 2 Basic information about Agents | 114 |
| 3 Installing and uninstalling Agents | 115 |
| Overview | 115 |
| Installation by means of Active Directory (GPO) with the use of MSI installer | 115 |
| Remote installation with the use of the anti-virus software management console | 117 |
| Manual installation | 117 |
| Agent archiving | 118 |
| Uninstalling Agents | 118 |
| 4 Agent configuration | 118 |
| Agent password | 118 |
| Profile management | 119 |
| Profiles | 119 |
| Profiles - introduction | 119 |
| Creating a profile | 120 |
| Default profile | 121 |
| Editing a profile | 121 |
| Deleting a profile | 121 |
| Automations | 122 |
| Profiles automations | 122 |
| Creating a profile automation | 122 |
| Editing a profile automation | 122 |
| Deleting a profile automation | 123 |
| Policies | 123 |
| Policies - introduction | 123 |
| Creating a policy | 124 |
| Setting a default policy | 124 |
| Editing a policy | 124 |
| Deleting a policy | 125 |
| Agent settings | 125 |
| Agent profile settings | 125 |
| Monitoring and visibility settings | 126 |
| Web filtering profile | 130 |
| Integration with TCP/IP stack | 130 |
| 5 "Agents" view | 132 |
| Part VI Users in nVision | 133 |
| 1 General information | 134 |
| 2 Access log | 134 |
| 3 User information screen | 135 |
| 4 Synchronization with Active Directory | 136 |
| 5 User roles and rights management | 139 |
| Types of user roles | 139 |
| Available permissions | 140 |
| Interrelated permissions | 147 |
| Assigning permissions to user | 148 |
| Default user permissions | 150 |
| Assigning permissions in bulk | 150 |

| | |
|---|------------|
| Migration of permissions from version 10 | 152 |
| 6 Hierarchy of users | 156 |
| 7 User groups | 158 |
| User groups | 158 |
| Smart groups | 162 |
| Part VII Users module | 165 |
| 1 Introduction | 166 |
| 2 Overview | 167 |
| 3 Blocking access to selected applications | 167 |
| 4 Blocking access to selected websites | 169 |
| 5 Screenshots | 171 |
| 6 E-mails | 172 |
| 7 Printouts | 173 |
| Printout monitoring | 173 |
| Printout audit | 174 |
| Printing costs | 175 |
| Printer grouping | 177 |
| Part VIII Inventory module | 179 |
| 1 Introduction | 180 |
| General information | 180 |
| First steps | 181 |
| Migration from previous versions | 182 |
| 2 Assets | 182 |
| Assets tab | 182 |
| Assets properties | 184 |
| General | 184 |
| Documents | 186 |
| Actions | 189 |
| History | 192 |
| Alerts | 193 |
| Who Can Use | 195 |
| Barcodes | 197 |
| Assets settings | 198 |
| Basic information | 198 |
| Asset detection | 198 |
| Asset types | 200 |
| Asset type folders | 204 |
| Global fields | 205 |
| Action templates | 207 |
| Asset statuses | 208 |
| Document types | 210 |
| Protocol Templates | 211 |
| Protocols | 213 |
| Autonumbering | 214 |
| Asset creation and modification | 218 |
| Generating protocol | 220 |
| User information | 224 |
| Asset audit | 226 |
| Printing labels | 227 |
| Mobile application | 229 |
| 3 Hardware | 246 |

| | |
|--|------------|
| Introduction | 246 |
| Monitored data | 246 |
| Hardware audit | 248 |
| History | 249 |
| 4 System Information | 250 |
| Introduction | 250 |
| Monitored data | 250 |
| Windows services | 251 |
| Windows processes | 251 |
| Windows Event Log | 252 |
| Remote command execution | 253 |
| S.M.A.R.T. | 253 |
| 5 Software | 254 |
| General information | 254 |
| Detection and application properties | 255 |
| Applications..... | 255 |
| Application categories..... | 257 |
| Application templates | 260 |
| Built-in templates managment..... | 262 |
| Adding new application..... | 262 |
| Application installations..... | 263 |
| Licenses and users | 266 |
| Installation History | 269 |
| License management | 271 |
| Licenses list..... | 271 |
| Adding new license..... | 274 |
| License additional fields..... | 276 |
| License removal..... | 277 |
| License editing properties..... | 278 |
| License properties | 278 |
| Application installation..... | 279 |
| Documents | 282 |
| Assigned users..... | 284 |
| History | 286 |
| Alerts | 288 |
| Licensing methods | 290 |
| Rules | 290 |
| Serial numbers..... | 291 |
| License accounting methods..... | 292 |
| Multiple user installations | 295 |
| Serial numbers assignment..... | 298 |
| Multiple applications on device..... | 302 |
| Software audit | 304 |
| 6 Data import | 306 |
| Data import from CSV | 306 |
| Inventory scan import | 307 |
| 7 MSI Package manager | 309 |
| 8 Inventory events | 312 |
| | |
| Part IX DataGuard module | 315 |
| 1 Introduction | 316 |
| 2 Access rights | 316 |
| Access rights – introduction | 316 |
| Example of structure | 317 |
| Inherited rights | 319 |

| | |
|---|------------|
| 3 Hosts | 320 |
| Devices and media | 320 |
| Management | 321 |
| Connected devices | 323 |
| Changing a device name | 324 |
| 4 Trustees | 325 |
| Trustees – introduction | 325 |
| Managing via user hierarchy | 326 |
| Managing trustees | 326 |
| Active Directory users | 327 |
| Access log | 329 |
| Access log for users | 331 |
| 5 Local directories monitoring | 331 |
| Audit local directories - introduction | 331 |
| Configuration | 332 |
| Audit exclusions | 334 |
| 6 Alerts | 335 |
| Alerts for DataGuard | 335 |
| Creating an alert | 336 |
| 7 Security | 337 |
| Windows Defender | 337 |
| Windows BitLocker | 338 |
| Windows Firewall | 339 |
| 8 Audit | 339 |
| 9 Quick help – typical rights configuration scenario | 339 |
| 10 Quick help – setting default access rights to USB devices | 343 |
| 11 Setting default access rights to USB devices | 344 |

Part X HelpDesk module 347

| | |
|---------------------------------------|------------|
| 1 Introduction | 348 |
| 2 Management and configuration | 349 |
| Configuration | 349 |
| HTTPS access | 350 |
| Settings | 356 |
| E-mail settings | 358 |
| User management | 360 |
| Priorities | 361 |
| Categories and folders | 363 |
| Trouble ticket forms | 368 |
| 3 HelpDesk interface | 369 |
| Starting the HelpDesk interface | 369 |
| User registration | 371 |
| Logging in | 373 |
| Password reset | 374 |
| Main views | 375 |
| Text editor | 376 |
| Chat | 377 |
| User zone | 379 |
| Search bar | 380 |
| 4 Trouble tickets | 382 |
| Trouble tickets - overview | 382 |
| Ticket list | 383 |
| Adding a ticket | 385 |

| | |
|--|------------|
| Ticket visibility settings | 386 |
| Ticket processing | 390 |
| Adding a comment | 390 |
| Adding attachments and screenshots | 391 |
| Editing a ticket subject | 391 |
| Multi-ticket operations | 392 |
| Closing a ticket | 392 |
| Editing ticket details | 392 |
| Setting the ticket processing time | 392 |
| VNC connection | 393 |
| Related tickets | 394 |
| Merging tickets | 395 |
| Deleting a ticket | 396 |
| 5 Whistleblower Protection | 396 |
| Whistleblower Protection - introduction | 396 |
| Restricting access to anonymous tickets | 398 |
| Anonymous ticket - restricted access | 398 |
| Anonymous ticket - ticket visibility | 404 |
| Anonymous ticket - ticket assignment | 409 |
| Anonymous ticket - automations | 409 |
| Anonymous Tickets | 410 |
| Launching Anonymous Tickets | 410 |
| Configuring anonymous tickets | 411 |
| Anonymous ticket link visibility | 412 |
| Processing an anonymous ticket | 413 |
| Adding an anonymous ticket | 415 |
| 6 Knowledge base | 417 |
| Knowledge base - overview | 417 |
| Article list | 418 |
| Adding an article | 419 |
| Editing an article | 420 |
| Deleting an article | 421 |
| 7 Event log | 422 |
| 8 Reports | 424 |
| Report generation | 424 |
| Tickets reports | 427 |
| Closed ticket reports | 427 |
| Activity reports | 440 |
| Unclosed tickets reports | 447 |
| SLA reports | 454 |
| Closed tickets under SLA reports | 454 |
| SLA metric course reports | 455 |
| SLA violation reports | 455 |
| 9 Absence plan | 456 |
| 10 Trouble ticket assignment | 457 |
| 11 Automations | 458 |
| Automations - overview | 458 |
| Automation list | 459 |
| Adding an automation | 460 |
| Automation conditions | 462 |
| Automation actions | 465 |
| Editing an automation | 465 |
| Activating/deactivating an automation | 466 |
| Deleting an automation | 467 |
| 12 SLA metrics | 467 |

| | |
|---|------------|
| Overview | 467 |
| SLA metric types | 468 |
| SLA metric conditions | 468 |
| SLA metric validity time | 469 |
| Creating and versioning SLA metrics | 470 |
| Violation of SLA | 471 |
| SLA metrics in tickets | 472 |
| 13 Announcements | 473 |
| 14 File distribution | 477 |
| 15 Windows processes | 483 |
| 16 Remote command execution | 484 |
| 17 Remote access | 486 |
| 18 End-user remote access | 487 |
| Part XI SmartTime module | 491 |
| 1 Introduction | 492 |
| General information | 492 |
| Trial version | 492 |
| Getting started | 493 |
| 2 Module configuration | 493 |
| Installation | 493 |
| Importing and deleting data | 495 |
| Starting SmartTime | 496 |
| Productivity levels | 497 |
| Setting the productivity and category | 497 |
| 3 Users and their permissions | 499 |
| User roles | 499 |
| Managers and superiors | 500 |
| Blocking access to data | 503 |
| Data available to users | 504 |
| 4 Groups | 506 |
| Group information | 506 |
| Special markings | 507 |
| 5 Application settings | 508 |
| General information | 508 |
| Application identification | 510 |
| Application settings | 511 |
| 6 Activity | 513 |
| Access to specific activities | 513 |
| Individual user activity | 513 |
| Activity on the selected day..... | 513 |
| Activity over time chart..... | 515 |
| Activity in the selected period..... | 516 |
| User group activity | 518 |
| Activity on the selected day..... | 518 |
| Activity in the selected period..... | 519 |
| Activity of subordinates | 520 |
| 7 Contacts | 522 |
| 8 System time | 525 |
| Part XII AdminCenter | 527 |
| 1 Introduction | 528 |

| | |
|--|------------|
| 2 Management and configuration | 528 |
| Enabling AdminCenter | 528 |
| User permissions | 529 |
| Free version limitations | 530 |
| 3 Starting AdminCenter | 530 |
| 4 Navigation within AdminCenter | 530 |
| 5 Dashboard management | 531 |
| Basic information | 531 |
| Creating new dashboard | 532 |
| Editing a dashboard | 532 |
| Dashboard edit mode | 532 |
| Changing the size of the grid | 533 |
| Adding widgets | 534 |
| Modifying widgets | 535 |
| Available widgets | 537 |
| Network module widgets | 537 |
| Inventory module widgets | 541 |
| Users module widgets | 544 |
| DataGuard module widgets | 549 |
| HelpDesk module widgets | 551 |
| SmartTime module widgets | 553 |
| Deleting a dashboard | 555 |
| Sharing a dashboard | 556 |
| Part XIII Reports | 559 |
| 1 Introduction | 560 |
| 2 Creating reports | 560 |
| 3 Segment types for host reports | 562 |
| 4 Segment types for map reports | 569 |
| 5 Segment types for user reports | 579 |
| 6 Segment types for group reports | 580 |
| Part XIV Alerting | 585 |
| 1 Introduction | 586 |
| 2 Concepts | 586 |
| 3 Managing alerts | 587 |
| Requirements | 587 |
| Alert management window | 588 |
| Inherited alerts | 591 |
| Alert escalation | 592 |
| 4 Events | 593 |
| Configuration | 593 |
| Event types | 593 |
| Managing events | 595 |
| Defining event properties | 597 |
| Rising, falling and reset thresholds | 604 |
| 5 Actions | 604 |
| Introduction | 604 |
| Action types | 605 |
| Managing actions | 606 |
| Defining action properties | 606 |
| Setting up actions | 612 |

| | |
|--|------------|
| Defining custom alert messages | 613 |
| 6 Raised alerts | 615 |
| Processing alerts | 615 |
| Event log | 615 |
| Part XV Web access | 619 |
| 1 How to get access to nVision via Web browser? | 620 |
| 2 How to create Web Access user accounts? | 621 |
| 3 Window layout | 623 |
| 4 Audit | 624 |
| Part XVI Database backups | 629 |
| 1 How to make a backup of my Atlases? | 630 |
| 2 Automatic backup | 630 |
| 3 Database size | 631 |
| 4 Backup folder change | 632 |
| Part XVII Frequently Asked Questions | 635 |
| 1 Agent data reset | 636 |
| 2 Agent installation with use of Active Directory | 636 |
| 3 Antivirus software proper setup | 642 |
| 4 Cloning the disk image with Agent installed | 642 |
| 5 Configuration of Agents installed on mobile computers | 642 |
| 6 Duplicated hosts | 643 |
| 7 File system audit | 643 |
| 8 Generating reports on Windows Server systems | 643 |
| 9 Hosts merging | 644 |
| 10 How "Uninstall nVision Agent" option works | 645 |
| 11 Installing Agent through WMI | 645 |
| 12 Launching SNMP in Linux system | 645 |
| 13 Monitoring multiple locations in nVision | 646 |
| 14 Moving nVision to another machine | 646 |
| 15 Not all users have been imported from Active Directory | 647 |
| 16 OFFLINE inventory scanner parameters | 647 |
| 17 Ports used by nVision | 648 |
| 18 Printouts monitoring | 648 |
| 19 Silent installation and uninstallation of nVision Agent | 648 |
| 20 Updating and archival versions of nVision | 649 |
| 21 Virtual machines | 650 |
| Index | 651 |

Part



1 Introduction

1.1 Axence nVision modules

Axence nVision® – network, application and employee monitoring, hardware and software inventory

Axence nVision® consists of 5 functional modules that can be installed in any combinations and managed from one console.

| | | |
|---|---|---|
| Proactive network monitoring and visualization |  Network | <p>The Network module monitors mail servers and Web addresses, TCP/IP and Windows services, application status and operation, and switches and routers (port mapping, network traffic, SNMP monitoring). The network is automatically detected and presented on interactive maps.</p> |
| Hardware and software inventory |  Inventory | <p>The Inventory module automatically collects the information about hardware and software of Windows machines. It enables auditing and the verification of license usage and offers information about program installation or configuration change.</p> |
| Advanced user monitoring |  Users | <p>The Users module monitors and reports the activity of users working on Windows machines: the actual activity (work) time, application usage, visited web pages and network transfer.</p> |
| Remote technical support for users |  HelpDesk | <p>The HelpDesk module enables a quick technical support for users by means of remote access to the workstations. It helps to solve the reported problems in a quick and effective manner.</p> |
| Protection against data leaks by port blocking |  DataGuard | <p>The DataGuard module manages the access rights for all I/O ports and physical devices utilized by the users to copy files from a company machine or to run external software.</p> |
| Visualization and better time management |  SmartTime | <p>The SmartTime module monitors and reports the activity of users working on machines. It enables the data collected at the web browser level to be visualized and displayed. It allows for better management of work time and enables the superiors to view the activity of their subordinates.</p> |
| Alerting and events | | <p>You can define a wide range of events when an alert should be raised. Events may be defined based on any</p> |



monitored parameter and service: computer or service down, page content changed, e-mail server problems, MS SQL server parameters out of range, and much more.

Each event may trigger one or more of the notification and corrective actions, such as desktop notification, e-mail, SMS or ICQ message. Alerts are stored in the event log, so you can analyze them later.

1.2 Axence nVision versions

A list of nVision versions, together with functions and improvements they introduce, can be found on the [changelog website](#).

1.3 Functionality of modules

The table below compares the functionality of nVision modules. All modules may be ordered independently.

| Functionality | Network | Inventory | Users | HelpDesk | DataGuard | SmartTime |
|--|---------|-----------|-------|----------|-----------|-----------|
| Network discovery and visualization | | | | | | |
| nVision server: network scanning and monitoring, detection of devices and TCP/IP services, remote access with browser and automatic backup | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| nVision Console: interactive network maps, user maps, departments, smart maps, pop-up menu with definable own tools | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| nVision Console: simultaneous work of multiple administrators, management of user rights, admin access log | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Network monitoring | | | | | | |
| TCP/IP services: response time and correctness, packets received/lost statistics (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL, etc.) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| WMI counters: CPU load, memory usage, disk usage, network traffic, etc. | ✓ | - | - | - | - | - |
| Windows actions: service status change (start, stop, restart), event log entries | ✓ | - | - | - | - | - |
| SNMP v1/2/3 counters (network traffic, temperature, humidity, power supply) | ✓ | - | - | - | - | - |

| Functionality | Network | Inventory | Users | HelpDesk | DataGuard | SmartTime |
|--|---------|-----------|-------|----------|-----------|-----------|
| voltage, toner level, etc.) | | | | | | |
| Support for syslog messages | ✓ | - | - | - | - | - |
| SNMP traps | ✓ | - | - | - | - | - |
| Routers and switches: port mapping and network traffic monitoring | ✓ | - | - | - | - | - |
| File distribution with use of WMI | ✓ | - | - | - | - | - |
| MIB file compiler | ✓ | - | - | - | - | - |
| Alerts and reports | | | | | | |
| Event/action alerts (e.g. when important parameters fall outside of the user-defined range) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Notifications (on desktop, by e-mail, by SMS) and repair actions (program launch, computer restart, etc.) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Reports (for user, group, device, network maps or entire atlas) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Everyday report on employee productivity | - | - | - | - | - | ✓ |
| Hardware and software inventory | | | | | | |
| List of applications and Windows updates on single workstation (based on system registry and disk scan) | - | ✓ | - | - | - | - |
| Software serial numbers (keys) | - | ✓ | - | - | - | - |
| Information on executable files and register entries on a workstation | - | ✓ | - | - | - | - |
| Information on multimedia files (mp3, avi, etc.) and zip archives and their metadata (file title and author, contents of zip file) | - | ✓ | - | - | - | - |
| Overview of workstation hardware | - | ✓ | - | - | - | - |
| Details of workstation hardware configurations (model, motherboard, CPU, memory, disk drives, adapters, etc.) | - | ✓ | - | - | - | - |
| System info (startup commands, user accounts, shared folders, SMART details, windows task scheduler monitoring, etc.) | - | ✓ | - | - | - | - |
| Hardware and software inventory audit | - | ✓ | - | - | - | - |

| Functionality | Network | Inventory | Users | HelpDesk | DataGuard | SmartTime |
|--|---------|-----------|-------|----------|-----------|-----------|
| Possibility to distribute and uninstall software by MSI packages | - | ✓ | - | - | - | - |
| Management of installations/uninstallations of the MSI package manager-based software | - | ✓ | - | - | - | - |
| Software template database | - | ✓ | - | - | - | - |
| License management | - | ✓ | - | - | - | - |
| Hardware and software change history | - | ✓ | - | - | - | - |
| Assets: IT assets register database (defining own fixed asset types, their attributes and values, attachments, data import from CSV file) | - | ✓ | - | - | - | - |
| Alerts: software installation, change in hardware and system resources | - | ✓ | - | - | - | - |
| Offline inventory scanner | - | ✓ | - | - | - | - |
| Scanning and printing barcodes and QR codes | - | ✓ | - | - | - | - |
| Android application enabling inventory taking with use of barcodes (for archiving and comparing fixed asset audits) | - | ✓ | - | - | - | - |
| Scanning user files and ability to preview them | - | ✓ | - | - | - | - |
| User activity monitoring and visualization | | | | | | |
| User activity overview | - | - | ✓ | - | - | - |
| Detailed work time (activity/break start and end time) | - | - | ✓ | - | - | ✓ |
| Used applications (actively and non-actively, i.e. the total time of application running, the time of actual use by a user and the information on processes with enhanced permissions) | - | - | ✓ | - | - | ✓ |
| Blocking of launched applications | - | - | ✓ | - | - | - |
| Visited web pages (number of page visits, with headers and duration of visits) | - | - | ✓ | - | - | ✓ |
| Blocking web pages | - | - | ✓ | - | - | - |

| Functionality | Network | Inventory | Users | HelpDesk | DataGuard | SmartTime |
|--|---------|-----------|-------|----------|-----------|-----------|
| Printouts: Audit (per printer, user, computer), printing costs | - | - | ✓ | - | - | - |
| Sent and received e-mails (headers) | - | - | ✓ | - | - | - |
| Bandwidth usage: user-generated network traffic (incoming and outgoing, local and in the Internet) | - | - | ✓ | - | - | - |
| Static remote view of user desktop (without access) | - | - | ✓ | ✓ | - | ✓ |
| Screenshots (user work history "screen by screen") | - | - | ✓ | - | - | - |
| Activity data available from the web browser | - | - | - | - | - | ✓ |
| Determination of the productivity level and application category | - | - | - | - | - | ✓ |
| Access of superiors to their subordinates' data | - | - | - | - | - | ✓ |
| Insight into their own activity data by users | - | - | - | - | - | ✓ |
| Help for network users | | | | | | |
| Trouble ticket database in the web browser | - | - | - | ✓ | - | - |
| Creating and managing trouble tickets (assigning to administrators with e-mail notification) | - | - | - | ✓ | - | - |
| Comments, attachments and screenshots in the trouble tickets | - | - | - | ✓ | - | - |
| Internal instant messenger (chat) | - | - | - | ✓ | - | - |
| Messages sent to users/machines with available mandatory receipt confirmation | - | - | - | ✓ | - | - |
| Static remote view of user desktop (without access) | - | - | ✓ | ✓ | - | - |
| Remote access to machines (an employee and administrator can see the same window) with possible request for consent from the user and optional mouse/keyboard blocking | - | - | - | ✓ | - | - |

| Functionality | Network | Inventory | Users | HelpDesk | DataGuard | SmartTime |
|---|---------|-----------|-------|----------|-----------|-----------|
| File distribution and running tasks (if a computer is turned off when the distribution is started, it will be performed after the machine is turned on) | - | - | - | ✓ | - | - |
| Integration of the user database with Active Directory | - | - | - | ✓ | ✓ | - |
| Assigning HelpDesk employees to tickets' categories | - | - | - | ✓ | - | - |
| Processing tickets from e-mail messages | - | - | - | ✓ | - | - |
| Knowledge base | - | - | - | ✓ | - | - |
| Remote command execution (ability to send command lines to workstations) | - | - | - | ✓ | - | - |
| SLA metrics, i.e. support of the guaranteed service level agreements. | - | - | - | ✓ | - | - |
| Device/data media access control | | | | | | |
| Devices currently connected to computers | - | - | - | - | ✓ | - |
| List of all devices connected to computers in the network | - | - | - | - | ✓ | - |
| Audit (history) of connections and operations on mobile storage devices and network shares | - | - | - | - | ✓ | - |
| Management of access rights (writing, launching, reading) for devices, computers and users (e.g. authorization of company encrypted flash memory drives, and blocking of employees' private drives) | - | - | - | - | ✓ | - |
| Central configuration by setting policies for the entire network, for selected network maps and for Active Directory groups and users | - | - | - | - | ✓ | - |
| Integration of user and group database with Active Directory | - | - | - | ✓ | ✓ | ✓ |
| Alerts: portable device connected/disconnected, file operation on a portable device | - | - | - | - | ✓ | - |
| Miscellaneous | | | | | | |
| Protection of Agent against deleting | - | ✓ | ✓ | ✓ | ✓ | ✓ |

| Functionality | Network | Inventory | Users | HelpDesk | DataGuard | SmartTime |
|-----------------|---------|-----------|-------|----------|-----------|-----------|
| Axence netTools | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Windows Agent | — | ✓ | ✓ | ✓ | ✓ | ✓ |

1.4 Administrator Access Log

nVision allows the Administrator Access Log to be viewed.

To navigate to the Access Log, select the **Users** tab from the map panel, and click the **Access Log** tab. Information on actions taken by all Administrators including the date and exact time can be viewed here.

The clock and calendar icons allow information from the last hour/day/week/month to be viewed. The calendar icon allows information from a specific day to be viewed.

The screenshot displays the Axence nVision 11 Administrator Access Log. The interface includes a navigation pane on the left with 'Users' selected. The main area shows a table of user activities:

| Name | Date & time | Object | Action | Details |
|---------------|---------------------|-------------------|------------|--|
| Administrator | 24.03.2020 14:10:27 | Console | Logged in | IP Address = 127.0.0.1; Computer name = Mikuz@DESKTOP-NQDNH1 |
| Administrator | 24.03.2020 13:22:39 | Console | Logged out | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@DESKTOP-NQDNH1 |
| Administrator | 24.03.2020 13:22:25 | Console | Logged in | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@DESKTOP-NQDNH1 |
| Administrator | 23.03.2020 16:00:18 | Console | Logged out | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| Administrator | 23.03.2020 10:26:38 | Counter | Created | Nazwa = HTTP; Typ = Zmiana treści strony; Urządzenie = WIN10, 192.168.69.206 |
| Administrator | 23.03.2020 10:22:35 | Counter | Created | Nazwa = www.pl; Typ = Zmiana treści strony; Urządzenie = WIN10, 192.168.69.206 |
| Administrator | 23.03.2020 10:22:03 | Device | Viewed | Urządzenie = WIN10, 192.168.69.206 |
| Administrator | 23.03.2020 10:21:02 | Console | Logged in | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| Administrator | 23.03.2020 10:16:25 | Console | Logged out | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| Administrator | 23.03.2020 10:12:54 | Console | Logged out | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| Administrator | 21.03.2020 00:09:26 | Console | Logged out | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| Administrator | 20.03.2020 11:11:52 | Device | Viewed | Urządzenie = WIN10, 192.168.69.206 |
| Administrator | 20.03.2020 10:00:56 | User | Modified | Nazwa = Hello; Ustawienia |
| Administrator | 20.03.2020 10:00:47 | User | Viewed | Nazwa = Hello |
| Administrator | 20.03.2020 09:56:18 | Device | Viewed | Urządzenie = Poseidon3266, 192.168.0.27 |
| Administrator | 19.03.2020 15:13:43 | User | Modified | Nazwa = Mikuz; Ustawienia |
| Administrator | 19.03.2020 15:07:13 | Desktop preview | Viewed | Nazwa = Mikuz@WIN10; Urządzenie = WIN10, 192.168.69.206 |
| Administrator | 19.03.2020 15:07:12 | User | Viewed | Nazwa = Mikuz |
| Administrator | 19.03.2020 15:06:42 | Console | Logged in | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| Administrator | 19.03.2020 14:58:08 | Console | Logged out | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| Administrator | 19.03.2020 14:58:05 | Console | Logged in | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| Administrator | 19.03.2020 14:48:08 | Console | Logged out | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| Administrator | 19.03.2020 10:47:20 | License | Modified | Oprogramowanie = Licencja testowa |
| Administrator | 19.03.2020 10:37:54 | License | Modified | Oprogramowanie = Licencja google |
| Administrator | 19.03.2020 10:36:37 | Console | Logged in | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| Administrator | 19.03.2020 10:36:11 | Console | Logged out | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| Administrator | 17.03.2020 10:59:20 | Console | Logged in | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| Administrator | 16.03.2020 17:37:03 | Console | Logged out | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| Administrator | 16.03.2020 13:35:56 | Report | Viewed | Nazwa = DO audyt; Atlas |
| Administrator | 16.03.2020 13:35:50 | Report definition | Modified | Nazwa = DO audyt; Raport dla = Mapa |
| Administrator | 16.03.2020 13:35:33 | Report definition | Created | Nazwa = DO audyt; Raport dla = Mapa |

To display the **Access Log** for a specific Administrator, double left-click their account name, navigate to the **Events** tab, and then open the **Access Log** tab.

| Date & time | Object | Action | Details |
|---------------------|-------------------|------------|---|
| 24.03.2020 14:25:09 | User | Viewed | Name = Administrator |
| 24.03.2020 14:19:27 | Console | Logged in | IP Address = 127.0.0.1; Nazwa komputera = Mikuz@DESKTOP-NQDNH1 |
| 24.03.2020 13:22:39 | Console | Logged out | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@DESKTOP-NQDNH1 |
| 24.03.2020 13:22:25 | Console | Logged in | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@DESKTOP-NQDNH1 |
| 23.03.2020 16:00:18 | Console | Logged out | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| 23.03.2020 10:26:38 | Counter | Created | Nazwa = HTTP; Typ = Zmiana treści strony; Urządzenie = WIN10, 192.168.69.206 |
| 23.03.2020 10:22:35 | Counter | Created | Nazwa = www.wp.pl; Typ = Zmiana treści strony; Urządzenie = WIN10, 192.168.69.206 |
| 23.03.2020 10:22:03 | Device | Viewed | Urządzenie = WIN10, 192.168.69.206 |
| 23.03.2020 10:21:02 | Console | Logged in | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| 23.03.2020 10:16:25 | Console | Logged out | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| 23.03.2020 10:12:54 | Console | Logged in | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| 21.03.2020 00:01:26 | Console | Logged out | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| 20.03.2020 11:11:52 | Device | Viewed | Urządzenie = WIN10, 192.168.69.206 |
| 20.03.2020 10:08:56 | User | Modified | Nazwa = Hello; Lastname |
| 20.03.2020 10:00:47 | User | Viewed | Nazwa = Hello |
| 20.03.2020 09:56:18 | Device | Viewed | Urządzenie = Poseidon3266, 192.168.0.27 |
| 19.03.2020 16:13:43 | User | Modified | Nazwa = Mikuz; Uprawnienia |
| 19.03.2020 16:07:13 | Desktop preview | Viewed | Nazwa = Mikuz@WIN10; Urządzenie = WIN10, 192.168.69.206 |
| 19.03.2020 15:07:12 | User | Viewed | Nazwa = Mikuz |
| 19.03.2020 15:06:42 | Console | Logged in | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| 19.03.2020 14:58:06 | Console | Logged out | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| 19.03.2020 14:55:05 | Console | Logged in | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| 19.03.2020 14:48:08 | Console | Logged out | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| 19.03.2020 10:47:20 | License | Modified | Oprogramowanie = Licencje testowa |
| 19.03.2020 10:37:54 | License | Modified | Oprogramowanie = Licencje google |
| 19.03.2020 10:36:37 | Console | Logged in | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| 19.03.2020 10:36:11 | Console | Logged out | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| 17.03.2020 10:59:20 | Console | Logged in | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| 16.03.2020 17:37:03 | Console | Logged out | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| 16.03.2020 13:35:56 | Report | Viewed | Nazwa = DG audyt; Alias |
| 16.03.2020 13:35:50 | Report definition | Modified | Nazwa = DG audyt; Nazwa raportu = Mapa |
| 16.03.2020 13:35:33 | Report definition | Created | Nazwa = DG audyt; Nazwa raportu = Mapa |
| 16.03.2020 08:48:59 | Console | Logged in | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| 14.03.2020 00:07:37 | Console | Logged out | Adres IP = 127.0.0.1; Nazwa komputera = Mikuz@WIN10 |
| 13.03.2020 14:08:40 | Device | Viewed | Nazwa = Aktywacja; Urządzenie = Mikuz |

1.5 Axence account

1.5.1 Description

To improve the comfort of our Users, along with the Axence nVision® update to version 7.5, we have introduced the Axence Account, enabling you to manage licenses.

- Starting from version 7.5, Axence nVision® license has no license key in the form of .ALS file (old keys are valid only for older versions, e.g. 7.1, 6, etc.).
- At the moment **the license has the form of an activation code** which is manually pasted into the programme or downloaded from the Axence Account. ([How to activate the full version of Axence nVision® ?](#))
- The activation code generated by Axence is automatically sent directly to the assigned Axence Account user (in the case of the first purchase, the administrator also receives licensing information by e-mail).

• Who should have an Axence Account set up?

Each license is associated with an Axence Account which should be created for a specified user, preferably the administrator, who will be responsible for Axence nVision® within a given company. ([Enter Axence Account >>](#)) Thus, Axence nVision® will automatically download all updates or license changes.

• Who can set up an Axence Account?

The Account may be created by the user on their own or by Axence (at the user's request).

• What data are necessary to create an Axence Account?

The following information is necessary to set up an Axence Account:

- full name of the administrator (or another specified user who will be responsible for Axence nVision® within the company/ institution),
- an e-mail address,
- name of the company/institution which owns the license.
- If a user already has an Axence Account set up, this information will allow them to be found in the user database and to merge their account with the new license.

- **Do I have to have an Axence Account for trial licenses?**

Yes, the requirement to create the Axence Account applies to all types of licenses: trial, time-limited and time-unlimited ones.

- **If you already are our Customer:**

We have already created an Axence Account for you and we have generated the license for version 7.5. Please check your mailbox and proceed according to the received instructions. If you have received no information, please contact our Sales Department at: sales@axence.net.

Each license change, including expansion of the license, change of the Maintenance Agreement period, or extension of the license validity period, is performed with the use of the Axence Account, and the Customer does not receive any additional/ new code. The automatically modified license is sent to Axence nVision®.

1.5.2 Registration

In nVision 7.5, integration with Axence Account was introduced. The account facilitates purchase and the easy management of licenses – both the free ones and the paid licenses for Axence nVision®.


Axence accounts are being set automatically on the e-mail address from the order form. For accounts set automatically, an email with a link to reset the password is sent.

Axence Account can be registered:

- during Axence nVision® installation - **click here to display the step-by-step instruction** (Internet access is required);
1. In the license-selection window, click the **I want to get free license for Axence nVision®** option, then click **Next** button:

Axence nVision 11

License change


 The license change will require the current license settings to be reset.

Do you want to delete the current settings and configure a new Axence nVision license?

2. Fill the e-mail address field, and then fill the form:

Axence nVision 11

Register free license

 Create a free license to:

- monitor an unlimited number of network devices
- get details on up to 10 workstations

* E-mail address:

Providing data and granting consent are voluntary but necessary to receive a non-paid license. The data controller is Axence Sp. z o.o. Sp. K., NIP (Tax Identification Number): 6751399589. Purpose of processing: conclusion and performance of license agreement, and direct marketing of the data controller on the basis of the granted consent. The consent is voluntary and may be withdrawn at any moment, which shall not affect the legal compliance of the processing that has taken place on the basis of the consent prior to its withdrawal. The consent may be withdrawn by sending a relevant request to the following address: dane.osobowe@axence.net.

Ordering a paid license or ending the use of software is not automatically understood as withdrawing the marketing consent (it may be withdrawn at any time in the way described above). Withdrawal of consent may block the non-paid license.

More: [Privacy Policy](#).

nv Axence nVision 11 ✕

Register free license

Please fill in the missing information required to register the free license.

* **E-mail address:**

* **First name:**

* **Last name:**

* **Organization:**

* **Phone number:**

* I hereby grant my consent to receiving marketing information from Axence Sp. z o.o. Sp. K. to the indicated email address and phone number

Registration means that you give your consent to the processing of the above-mentioned personal data for the purposes of direct marketing from Axence Sp. z o.o. Sp. K. by email or over the phone.

Providing data and granting consent are voluntary but necessary to receive a non-paid license.

[Start again](#)

The data controller is Axence Sp. z o.o. Sp. K., NIP (Tax Identification Number): 6751399589. Purpose of processing: conclusion and performance of license agreement, and direct marketing of the data controller on the basis of the granted consent. The consent is voluntary and may be withdrawn at any moment, which shall not affect the legal compliance of the processing that has taken place on the basis of the consent prior to its withdrawal. The consent may be withdrawn by sending a relevant request to the following address: dane.osobowe@axence.net

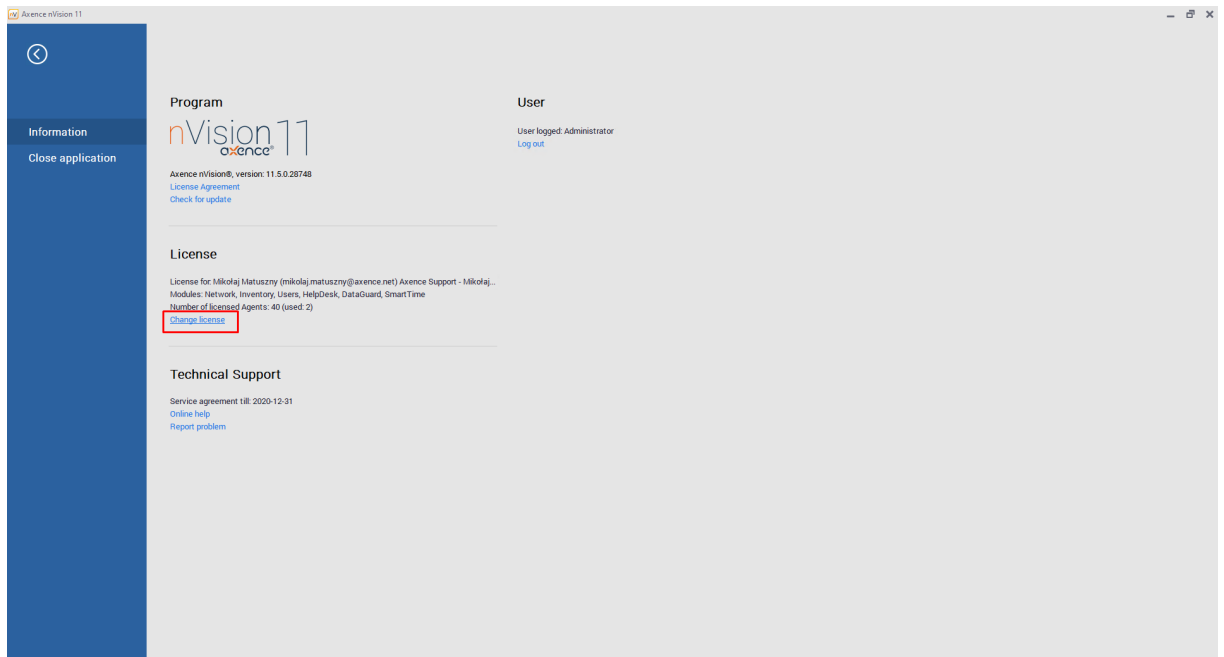
Ordering a paid license or ending the use of software is not automatically understood as withdrawing the marketing consent (it may be withdrawn at any time in the way described above).
Withdrawal of consent may block the non-paid license.

More: [Privacy Policy](#).

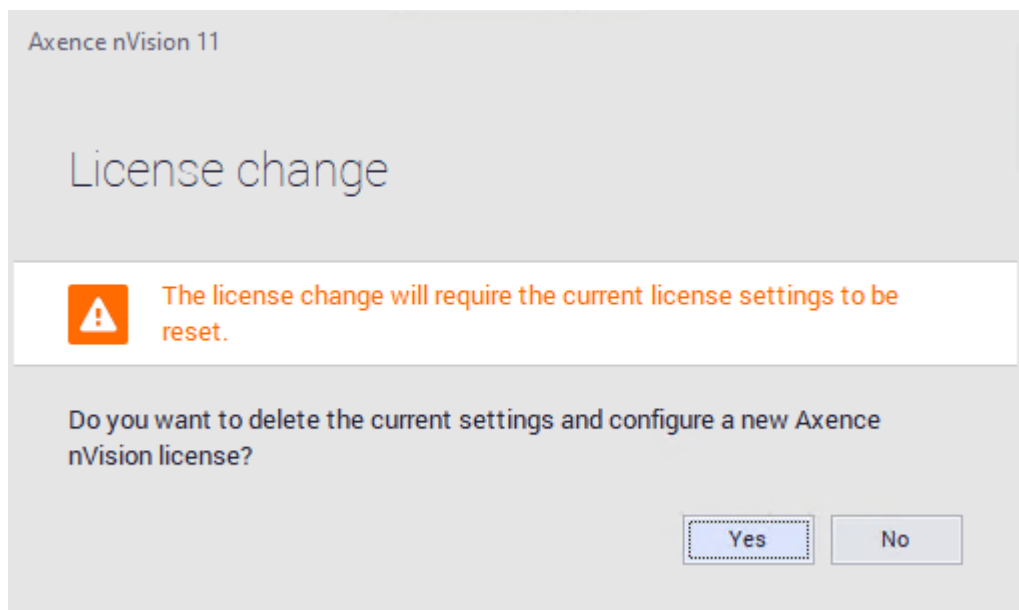
- with the use of a web browser at <https://account.axence.net/>.

1.5.3 Log in

To log in to an Axence account, select the **Axence nVision** tab in the upper left corner of the window, and then click **Change license** button in the **License** section.



The following window will be displayed:



By clicking on **Yes** button, you will remove the currently installed license key, and the Axence account login window will be displayed (*data gathered in monitoring and nVision's configuration will be kept*). Then enter the e-mail address and password of the registered account associated with the license.

1.5.4 Language management

In order to change language, go to **Edit profile** settings after logging in:

The screenshot shows the 'Settings' page of an Axence account. On the left sidebar, the 'Edit profile' link is highlighted with a red arrow. The main content area is divided into two sections: 'Settings' and 'Account settings'. The 'Settings' section contains input fields for 'First name' (Mikołaj), 'Last name' (1), 'Company' (Axence), 'Phone' (791736965), and a dropdown for 'Language' (English). A 'Save changes' button is located below these fields. The 'Account settings' section shows the email address 'mikołaj@axence.net' and two buttons: 'change e-mail' and 'change password'.

1.5.5 Manage Axence account

To manage an Axence account, log in at: <https://account.axence.net>.

The screenshot shows the 'Your Axence nVision licenses' page. It features a table with two license entries. Each entry includes a 'LICENSE CODE', a 'Deactivate' button, 'MODULES' (Network, Inventory, Users, Helpdesk, Dataguard, Smarttime), 'Issued for' information, 'Agents (used/licensed)' count, 'Used by' information, 'Expiration date', and 'Service agreement till'.

| LICENSE CODE: | MODULES: | Issued for: | Agents (used/licensed): | Used by: | Expiration date: | Service agreement till: |
|--------------------|---|---|---|------------------------------|------------------|-------------------------|
| 99KHQK-TBMV6-CWBXF | NETWORK, INVENTORY, USERS, HELPDESK, DATAGUARD, SMARTTIME | Axence Support - Mikołaj Matuszyny Licencja testowa Versions: 10, 11 | 2 / 40 Last update: 1:38 PM, 3/24/2020 | DESKTOP-NDQNH1 (89.64.55.73) | 12/31/2020 | 12/31/2020 |
| W6692J-FVX2R-9T96H | NETWORK, INVENTORY, USERS, HELPDESK, DATAGUARD, SMARTTIME | Axence Versions: 9, 10, 11 (Free) | 1 / 10 Last update: 8:41 AM, 11/5/2019 | WIN10VM (31.172.177.154) | PERPETUAL | NO AGREEMENT |

At the bottom of the page, there is a link: [How to activate the full version of Axence nVision Pro](#)

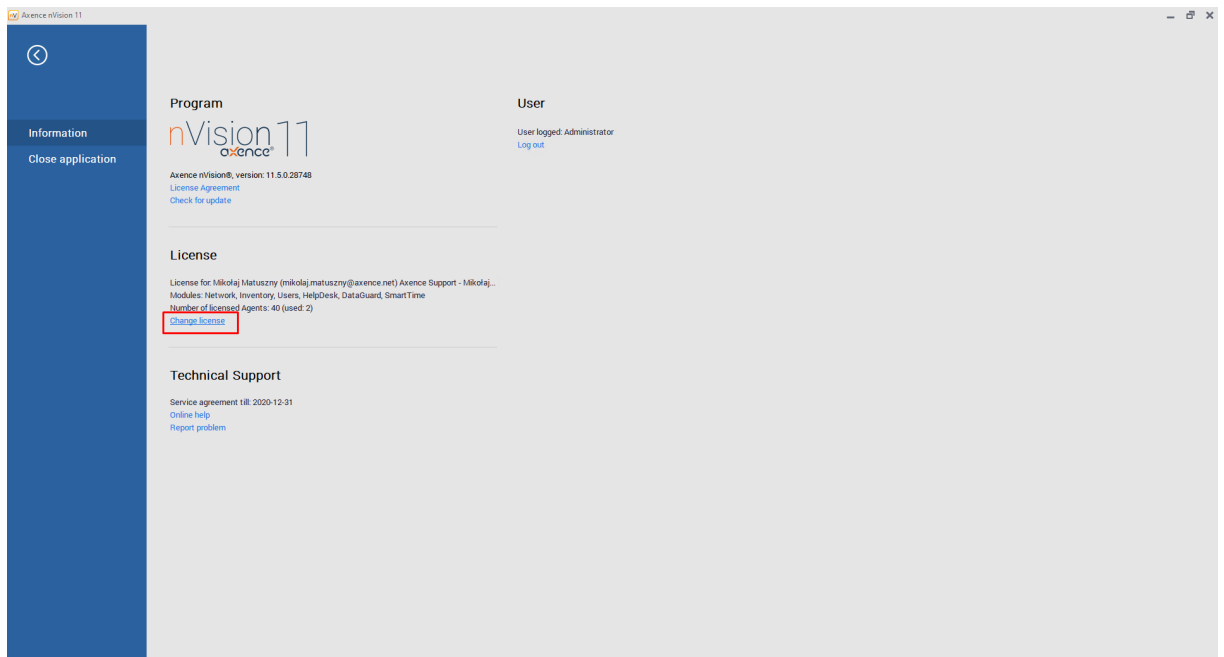
The main page of Axence account includes an administration panel in the left part of the window. The panel offers links to the following sub-pages:

| Menu | Description |
|-----------------|--|
| Your licenses | Enables details on purchased licenses to be viewed. |
| Request a quote | Enables contact with the Axence's Commercial Department for a quote. |

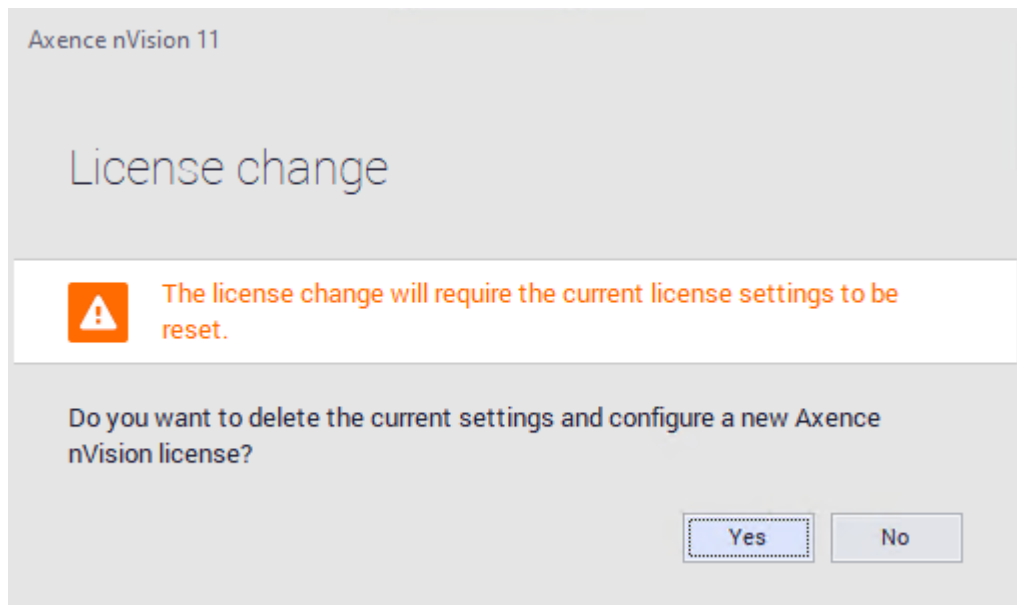
| | |
|-----------------------------|---|
| Edit profile | Enables the basic account information to be viewed and edited. |
| We are currently working on | Shows a list of functions on which programming work is currently in progress. |

1.5.6 Activation

Details of used license are displayed after clicking **Axence nVision** in the window's ribbon.



In order to enter the license key, click **Change license**. The following window will be displayed:





By clicking on **Yes** button, you will remove the currently installed license key, and the Axence account login window will be displayed (*data gathered in monitoring and nVision's configuration will be kept*).

In the license-selection window, click the **I want to use my own Axence nVision® license** option, then click the **Next** button:

Axence nVision 11

License for Axence nVision

| | |
|---|---|
| <input type="radio"/> I want to use a free Axence nVision license |  nVision server requires Internet access. |
| <input checked="" type="radio"/> I want to use my commercial Axence nVision license |  nVision server does not require Internet access, but it is recommended. |

Next Cancel

Free version activation:

In order to activate free license, you have to select **I want to get free license for Axence nVision®** option, even if the free license has been created before.

If there is no active Internet connection (**Axence nVision** service cannot connect to the activation server), follow the onscreen instructions:

Online activation

1. Enter the e-mail address and password of the registered Axence account associated with the license. Click the **Next** button:

Axence nVision 11


Log in to Axence Account

* E-mail address:

* Password:

[Forgot password?](#)

[Start from beginning](#)

 You do not have a license for Axence nVision Pro ?
Please make an inquiry or contact sales@axence.net

2. In the **Enter license** window, type or paste the license key copied from e-mail or [Axence Account](#) webpage.
3. After clicking the **Enter license** button, nVision is activated.

Offline activation

Follow the onscreen instructions.

1. On the machine with Internet access, visit the following webpage:
<https://account.axence.net/#/offline>.
2. Fill in the offline-license generating form:
Computer's name: *(any computer name)*
License key: *(the license-key copied from You're the webpage*
<https://account.axence.net/licenses> e.g.: 4B4MC9-MG4PQ-XYZXY-XYZXY)
Machine key: *(12-alphanumeric key copied from **Enter license** window in step 1).*
3. In the offline-license generating form, click the **Download the offline license** button, then **Save the file**.
4. Save and copy the offline-license **AxenceOfflineKey.txt** file on hard drive on nVision Server machine, click the **Import license** button and select the file. Click **Enter license** button.

Part



2 Requirements and configuration

2.1 System requirements

| Operating system (with up to date Service Pack installed) | nVision Server ¹ | nVision Console | nVision Agent |
|---|-----------------------------|-----------------|----------------|
| Windows XP | ✗ | ✗ | ✓ ² |
| Windows Server 2003 | ✗ | ✗ | ✓ ² |
| Windows Vista | ✗ | ✓ ² | ✓ ² |
| Windows Server 2008 | ✗ | ✓ ² | ✓ ² |
| Windows 7 | ✓ ² | ✓ ² | ✓ ² |
| Windows Server 2008 R2 | ✓ ² | ✓ ² | ✓ ² |
| Windows 8 | ✗ | ✓ ² | ✓ ² |
| Windows Server 2012 | ✓ | ✓ | ✓ |
| Windows 8.1 | ✓ | ✓ | ✓ |
| Windows Server 2012 R2 | ✓ | ✓ | ✓ |
| Windows 10 | ✓ | ✓ | ✓ |
| Windows Server 2016 | ✓ | ✓ | ✓ ³ |
| Windows Server 2019 | ✓ | ✓ | ✓ ³ |

1 - In production environment, the nVision Server should be installed on server editions of Microsoft Windows system due to hosting limitations included in EULA of Microsoft Windows system client editions.

2 - Installation is possible, but the software is no longer supported for this system version.

Please remember that in case of any technical problems, we might not be able to find a solution. We highly recommend to update to a newer Windows operating system (supported by the manufacturer). [Microsoft Product and Services Lifecycle Information](#)

3 - On this version of Windows system, with SecureBoot enabled, the network filtering, e-mail monitoring and DataGuard may not work.

nVision Server must operate at a static IP address.

nVision server:

- double core CPU,
- 4 GB RAM,
- 10 GB of free disk space,
- 64-bit operating system,
- Windows Server operating system, version: 2008 R2 or newer.

Recommended for monitoring more than 1000 Agents:

- nVision on a dedicated physical machine (not virtual),
- quad core processor,
- minimum 8GB RAM (for each additional 1000 Agents further 8GB RAM),
- fast hard disk.

Required CPU speed and memory usage are related to the number of monitored devices and the scope of monitoring.

*In order to achieve the best possible performance, the nVision server installation on fast **SSD disks** is recommended.*

For more information on required configuration of large nets (more than 250 Agents), see chapter [nVision performance](#)^[45]

nVision Console:

- double core CPU,
- 2 GB RAM,
- 400 MB of free disk space,
- 64-bit operating system,
- Windows Vista or newer,
- nVision Server connected to LAN, TCP port 4436,
- for proper generation of reports, Internet Explorer 8.0 or newer is required (the latest available version is recommended).

nVision Agent:

- single core CPU,
- 128 MB RAM,
- 100 MB of free disk space,
- Windows XP or newer,
- nVision Server connected to TCP port 4436.

To guarantee the correct operation of nVision Server, nVision Consoles, nVision Agents and net-Tools, add the installation folder

(e.g.: “C:\Program Files (x86)\Axence”) to the list of exclusions of the anti-virus software on each machine – examples:

- [Eset Antivirus](#)
- [Kaspersky Antivirus 2018](#)
- [AVG Antivirus](#).

When the exclusion is added, restart the configured machines.

Browsers monitored by nVision:

- Internet Explorer,
- Microsoft Edge,
- Mozilla Firefox,
- Google Chrome.

2.2 Ports

To enable communication between the Agents and nVision, it is necessary to open specific ports on the devices with Agents and on the device with nVision running. Agents and nVision automatically open the required ports in Windows Firewall. However, if any other firewall is present, these ports must be opened manually. These ports must also be open on the router, if the Agents work outside of the local network containing the nVision machine.

Ports open on the device with nVision

| TCP port | Description |
|-------------|---|
| 4434 | diagnostic information |
| 4436 | Communication with Agents (permanent connection). |
| 8080* | WebAccess – access to nVision via web browser. * Configurable value. Can be changed in nVision: Tools / Options / Services Configuration / Web Access . |

Ports open on the remote devices

If the ports on the device with the Agent are closed, the Agent will continue to collect monitored data and send them to nVision; however, some operations made in nVision will not have an immediate effect in the Agent.

| TCP port | Description |
|--------------------|---|
| 4433 | I diagnostic information. |
| 135, 139, 445, 593 | WMI, including the monitoring of Windows counters (Monitoring and managing Windows with WMI ^[28]). Important: Windows counters can also be monitored by Agents (see Monitoring Windows services ^[67]). |

Additionally, when monitoring TCP/IP services, the respective ports on the remote device, depending on the monitored service e.g. TCP 80 for HTTP, must be open.

For more information about the remote access and permanent connection between the Agent and nVision, see the chapter [Remote access](#) ^[486].

For more information about configuring Agents on mobile machines, see the chapter [Configuration of Agents installed on mobile machines](#) ^[642].

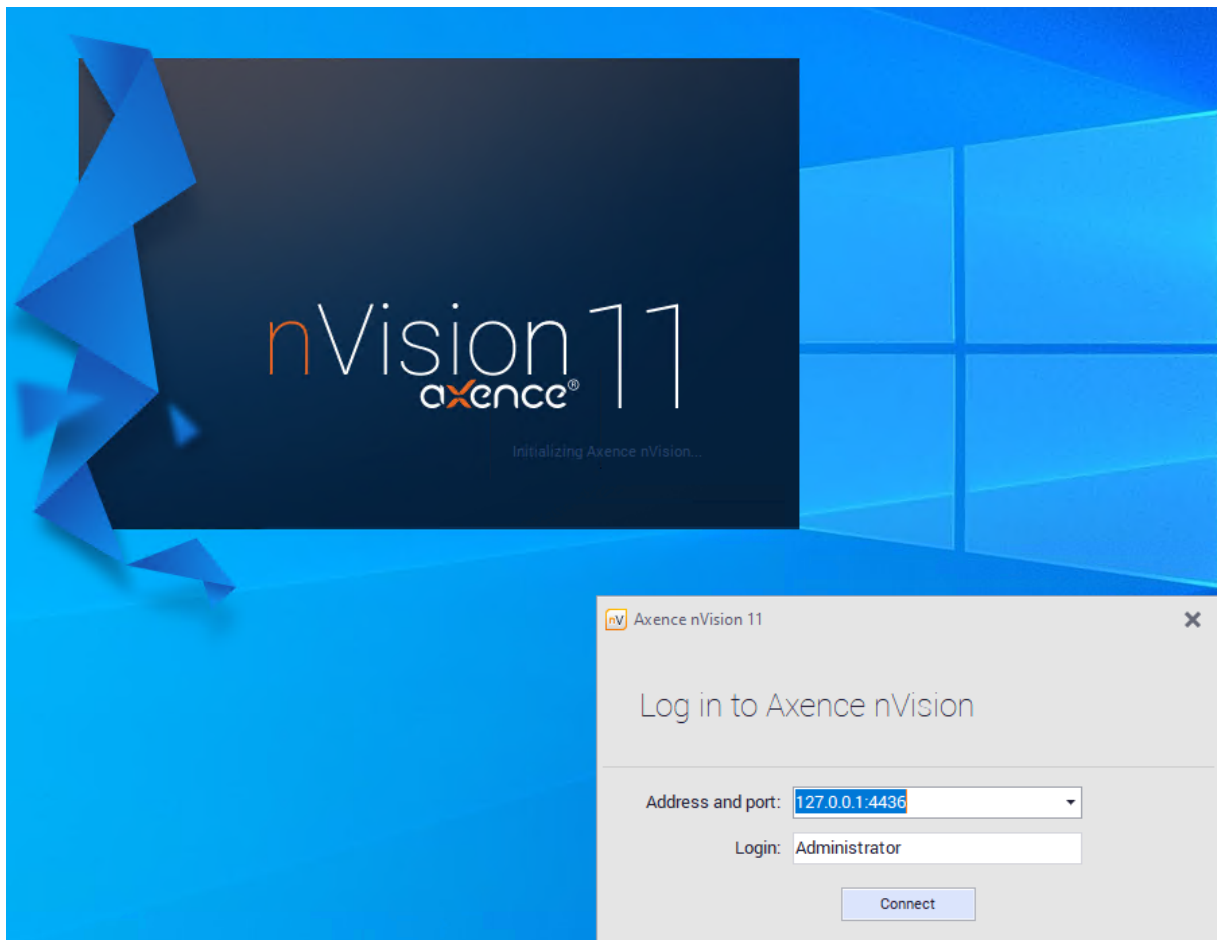
2.3 Remote nVision Console

Version 7 of nVision introduced the option to separate the installation of nVision Console from the nVision Server. The installation of a remote Console allows for the simultaneous work of several Administrators with the software.

To install only the nVision management console, **use the same setup file as in the case of the basic Server installation**. The setup will allow the choice of the components which are to be installed – select option **“Install only the management console”**.

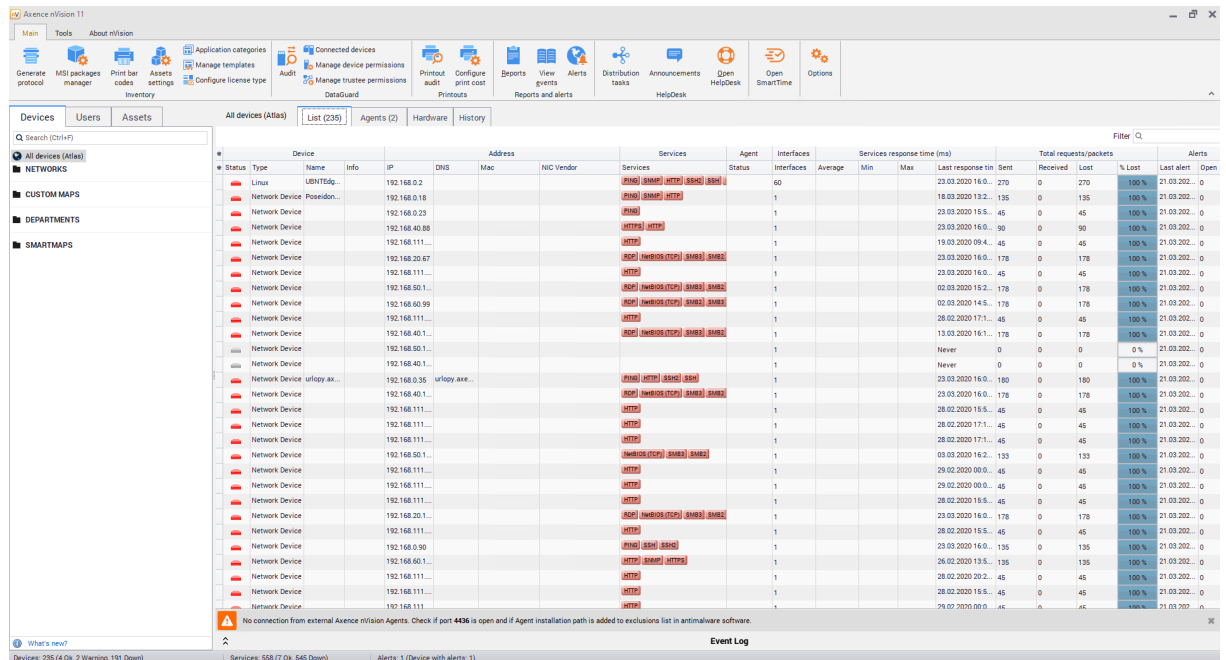
When the Console is installed and the nVision installation folder is added to the scanned exclusions of the anti-virus software, the software can be run.

In the login dialog box, enter the login and password of the nVision Administrator, the IP address and the port of the remote computer where nVision Server is installed:



2.4 Window layout

The nVision window layout is intuitive and easy to use.



Menu bar

The nVision functions are grouped into in 3 tabs on the menu bar:

+ “About nVision” tab

This tab presents information about nVision version, logged in user, entered license and service contract termination date.

+ “Main” tab

| Group | Functions | Description |
|-----------|-------------------------------|---|
| Inventory | Generate protocol | Allows to generate asset transfer protocols . ^[220] |
| | Asset settings | Asset settings management ustawieniami zasobów . ^[198] |
| | Application categories | Categories creation and management . ^[257] |
| | Print bar codes | Manage printouts of bar codes for assets. |
| | Configure license type | Allows to configure additional fields . ^[276] for all licenses. |
| DataGuard | Manage templates | Allows to manage software templates synchronized with the / |
| | MSI packages manager | Allows to manage software installation via MSI packages . ^[477] |
| | Audit | Allows the review of the history of connections and file operations on external media. |
| DataGuard | Connected devices | Presents a list of devices connected to hosts with Agents. |
| | Manage devices | Allows the configuration of access rights to devices connected to Agents . ^[321] |

| | | |
|---------------------------|---------------------------------------|---|
| | Manage trustees | Allows the configuration of access rights to media for users ^[326] . |
| Printouts | Printout audit | Allows a list of printouts performed by users ^[174] to be displayed. |
| | Configure Printing costs | Allows the configuration of Printing costs ^[175] . |
| Reports and alerts | Reports | Allows the preparation of templates and generation of reports ^[560] . |
| | Event log | Displays all generated alerts ^[615] . |
| | Alerts | Configuration of alerts for Atlas ^[588] . |
| HelpDesk | Open HelpDesk | Opens the Helpdesk web interface ^[375] . |
| | Distribution tasks | Allows files to be uploaded and executed remotely on Agents ^[477] . |
| | Messages | Allows for easy provision of information ^[473] to users with an installed Agent. |
| | Configuration | Opens the Helpdesk settings ^[356] window. |
| SmartTime | Opens SmartTime web interface. | |
| Settings | Opens nVision main settings. | |

+ "Tools" tab

| Group | Functions | Description |
|--------------------------|----------------------------|--|
| Devices and users | Add user | Creates a new user account. |
| | Add group | Creates a new group. |
| | Add device | Allows an icon to be added for a new device (e.g. the one undetectable by ping scanning). |
| | Show duplicated devices | Presents a list of devices with duplicated IP/MAC addresses or DNS names. |
| | Create counter for devices | Allows the creation of performance counter on multiple devices ^[63] . |
| Tools | Run netTools | Runs netTools . |
| | Discover new network | Runs the network discovery wizard ^[53] . |
| | Distribute file with WMI | Opens the distribution with WMI menu |
| SNMP and Syslog | SNMP trap server | Server configuration and review of collected SNMP traps ^[71] . |
| | Syslog server | Server configuration and review of collected Syslog messages ^[74] . |
| | MIB compiler | Allows MIB files to be imported ^[70] . |
| Agents | Install nVision Agent | Allows the preparation of the Agent installer file in the form of MSI package ^[115] . |

| | | |
|----------------|-----------------------------------|--|
| | Uninstall nVision Agent | Allows for the remote uninstallation of Agents that connect with the Server. |
| | Import inventory scans | Allows for the inventory of computers without installed Agents. |
| | Propagate new Atlas address | Enables Agents to be prepared for moving nVision server installation to another machine ^[646] . |
| | Manage your Agent profiles | Management of Agent configuration ^[125] . |
| | Inventory scanner executable file | Allows the inventory scanner file to be saved. |
| | Options | Allows the nVision operation options ^[324] to be changed. |
| | Atlas properties | Basic Atlas properties (visualization style, ignored devices, etc.) |
| | Filters for smart maps | Allows the creation of smart maps ^[107] that group devices complying with specific conditions. |
| Options | Filters for smart groups | Allows the creation of smart groups that group user accounts complying with specific conditions. |
| | Manage | Configuration of: events ^[593] and actions ^[605] , alerts, icon visualization styles, additional tools, login credentials and departments ^[105] . |

Atlas panel

The Atlas panel is located in the left part of the window and divided into two tabs: **Devices, Users and Assets**.

The **Devices** tab presents a list of all devices grouped as maps. To find out more about maps, see the chapter [Atlases, maps and hosts](#) ^[82].

After selecting devices in the tree, the list is presented in the central view.

The **Users** tab presents the nVision user accounts and their groups. Both the accounts and groups are carriers of monitoring and blockade settings.

See the [monitoring](#) ^[30] and [locking settings](#) ^[33].

The **Assets** tab presents a list of all assets created in the program. It also gives you the ability to create application templates and check what programs are installed. Detailed information is presented in the [dedicated chapter](#) ^[182].

2.5 Configuration

2.5.1 Basic configuration

Planning the monitoring

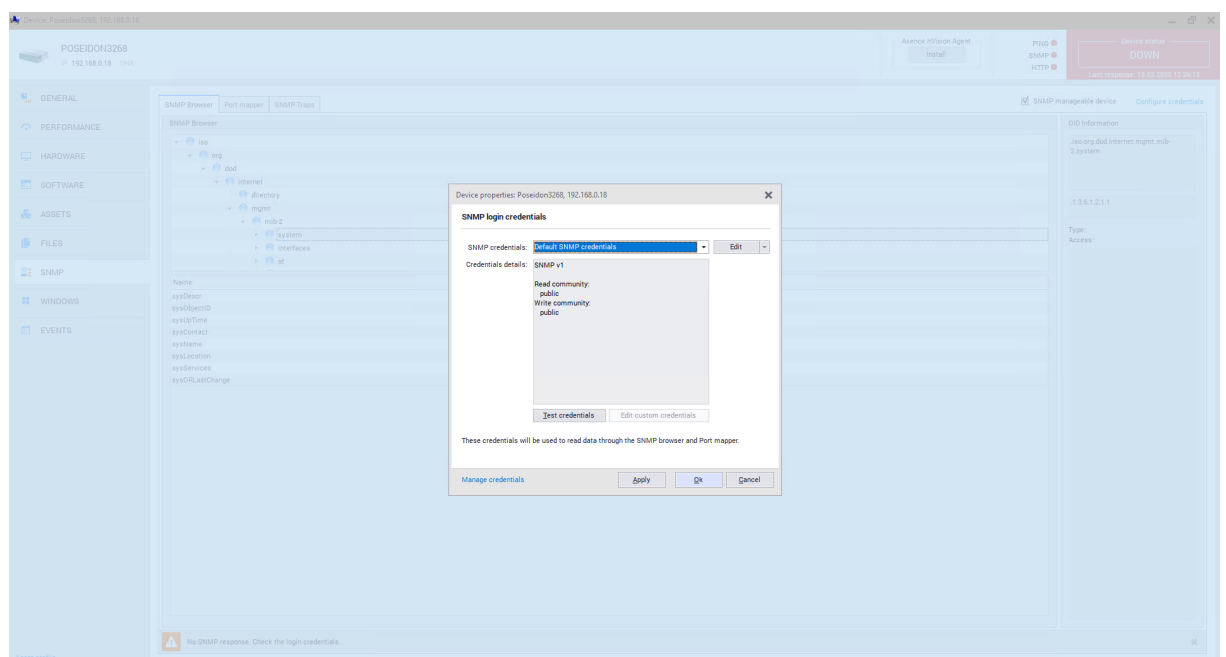
To successfully monitor all devices in your network you must perform several steps even before you start the nVision network scanner. This is a list of all steps you need to take to be able to fully utilize all nVision features:

+ Properly configure SNMP devices

To successfully monitor all devices in your network you must perform several steps even before you start the nVision network scanner. First of all you have to properly configure SNMP devices (the most important is setting the proper IP address and SNMP community). For more information about SNMP device configuration you should refer to the appropriate device documentation.

Configuring credentials

To monitor SNMP, you also need to provide the SNMP community. You can specify the community in the **Host info** window on the SNMP tab.



Requirements for monitoring SNMP devices

| Monitoring | Protocols used | Requirements |
|--|----------------|--|
| SNMP performance counters | SNMP | <ul style="list-style-type: none"> • Login credentials properly set • Host configured as SNMP manageable • At least one interface checked as supporting SNMP. |
| Ports and interfaces on switches and routers | | <ul style="list-style-type: none"> • SNMP properly configured on the remote host. |

| Monitoring | Protocols used | Requirements |
|------------|----------------|--------------|
|------------|----------------|--------------|

Network traffic

- Availability of specific SNMP OIDs and tables on the remote host.

Additionally to the above requirements, the firewall on the remote host must be properly configured. The following table lists the ports that must be open:

| Protocol or monitor | Required open ports |
|---------------------|---------------------|
| SNMP | UDP 161,162 |

+ Enable WMI on all Windows machines

Enabling WMI is described in detail in the [Monitoring and managing Windows with WMI](#)^[28] topic. In order for the WMI to operate correctly, the login credentials (i.e. Windows credentials on the specific station) should be properly configured.

+ Install nVision Agents

Possible methods of installing Agents are described in detail in section [Installing and uninstalling Agents](#)^[115].

+ Open specific ports on the computer running nVision and on remote computers

Agents and nVision automatically open the required ports in Windows Firewall. However, if any other firewall is present, these ports must be opened manually.

The ports are listed in the topic [Ports](#)^[22].

Related topics

 [Requirements](#)

 [Remote access](#)

 [Installing and uninstalling Agents](#)

 [Agent settings](#)^[125]

2.5.2 Monitoring and managing Windows with WMI

Enabling monitoring of Windows counters

WMI (used by WinTools, resource information selection and Windows performance counters monitoring) is fully enabled on Windows 2003 Server. But you need to perform several operations if you would like to get information from Windows XP Professional, Vista and Windows 7 computers. To speed up the whole operation, we prepared a program (WMIEnable.exe, available from the nVision installation folder) which automatically performs all necessary operations. To enable WMI, just run this program on the remote machine. You can run it from the login script, thus enabling WMI on all Windows XP, Vista and Windows 7 machines in your network at once. **If you are using any third party firewall on the remote host, then you also need to open the following ports on your own: TCP 135, 139, 445, 593.**

To be able to use WinTools or read resources from Windows, keep in mind that the remote system must have exactly the same login credentials (user name and password) as the user logged in on the computer running netTools and nVision. This is due to the limitations of the Home edition.

WMIEnable

This program enables WMI on the Windows XP Professional and Vista computers. This is exact list of operations performed by this program:

1. DCOM is enabled by setting registry key

```
[ HKEY_LOCAL_MACHINE\Software\Microsoft\OLE\EnabledCOM]
value to "Y".
```

2. Remote UAC on Windows Vista is enabled by setting registry key

```
[ HKLM SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy]
value to 1.
```

3. The WMI ports (**TCP 135, 139, 445, 593**) are opened on the Windows firewall by performing the following command:

```
netsh firewall set service RemoteAdmin
```

4. Access to WMI on Windows Vista is enabled by adding a firewall exception for **Windows Management Instrumentation (WMI)**.

5. Authorization model is set to "Local user authorize as themselves" by setting registry key

```
[ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\forceguest ]
value to 0.
```

In almost all cases the system restart is not necessary and WMI will be enabled right after the program execution, but you can also force Windows system restart after the above parameters are set by running the program with the **/restart** parameter. The program will not restart the system if it is not able to change system settings.

If the WMI is still not working

If you have run the WMIEnable program and WMI is still not working, then verify the following:

1. Enter **Local Security Settings (secpol.msc /s)** and select **Local Policies -> User Rights Assignment -> Access this computer from network**. Check if all necessary users/groups are added here. At least the Administrators group or Administrator should be present.
2. Enter **Group Policy (gpedit.msc)** and select **Windows Settings -> Security Settings -> Local Policies -> Security Options -> Network access: Sharing and security model for local accounts**. Set this option to **Classic – local user authorize as themselves**.
3. Check if WMI is operational by running the **wbemtest** command. WMI is running if this program can run properly.
4. Check if the following services are running:
COM+ Event System
Remote Access Auto Connection Manager
Remote Access Connection Manager
Remote Procedure Call (RPC)

Remote Procedure Call (RPC) Locator
Remote Registry
Server
Windows Management Instrumentation
Windows Management Instrumentation Driver Extensions
WMI Performance Adapter
Workstation

Memory leaks with outdated Rpcrt4.dll

If monitoring Windows counters, please make sure that you have the latest Rpcrt4.dll installed. All previous versions cause serious memory leaks in the system, which can lead to a system crash. This problem is described by Microsoft at <http://support.microsoft.com/?kbid=911262>.

Your Rpcrt4.dll should have the following version (or higher):

| System | Version | File size |
|--------------|---------------|-----------|
| Windows 2003 | 5.2.3790.2900 | 643.072 |
| Windows XP | 5.1.2600.2810 | 582.144 |

Problem of RPC calls and high-numbered ports

By default, a RPC call uses ports from the one-time use range (1024-5000) during assigning ports to RPC application for listening in the TCP end point. Such behavior may limit access to these ports, and cause trouble in operating with nVision Agents. Information on how to configure a RPC call to use secure ports and facilitate port protection can be found at <http://support.microsoft.com/kb/908472>.

Connecting between different operating systems

You cannot connect to a computer that is running a Starter, Basic, or Home Windows edition.

More information:

http://msdn.microsoft.com/en-us/library/windows/desktop/aa389284%28v=vs.85%29.aspx#failure_to_connect

2.5.3 Monitoring and blockades

2.5.3.1 Monitoring settings

Unlike in nVision 9 (where settings were saved as a set of rules, i.e. in Agent profiles), the latest version of Axence nVision 10 configures the user monitoring and website and application blocking settings on user groups.

It is properties where the Administrator should configure the monitoring options as user accounts inherit their settings. Of course, each user account may be assigned to more than one group. If this is the case, the effective monitoring settings are applied in accordance with the principles described below.

The basic carriers of monitoring settings in the latest version of nVision are: Atlas, User groups, and user account.

Atlas – default settings

Atlas is the primary object in nVision that contains the essential, global monitoring settings. It means that the user account which does not belong to any of the groups will adopt monitoring settings that are assigned to the Atlas.

Possible configurations:

- Monitoring

| Setting | Possible values | Default value |
|-------------------------------|--|---------------|
| Bandwidth usage | monitor /don't monitor | monitor |
| Visited web pages | monitor /don't monitor | monitor |
| Application usage | monitor /don't monitor | monitor |
| Work time | monitor /don't monitor | monitor |
| Printouts | monitor /don't monitor | monitor |
| E-mails | monitor/ don't monitor | don't monitor |
| Send activity over time | monitor/ don't monitor | don't monitor |
| Activity breaks | monitor /don't monitor | monitor |
| Save breaks above "X" minutes | minutes | 5 minutes |
| Monitoring time | At any time / between / except (hours, days of the week) | at any time |

- Remote access

| Setting | Possible values | Default value |
|---------------------------------|-----------------------------|---------------|
| Enable desktop preview | enable /don't enable | enable |
| Enable remote access | enable /don't enable | enable |
| Show notification | don't notify /notify | don't notify |
| Ask for user consent | don't ask/ ask | ask |
| Enable if user does not respond | enable /don't enable | enable |

- Displaying Agent

| Setting | Possible values | Default value |
|---|-------------------------|---------------|
| Show Agent icon | show /don't show | show |
| After logging in show information about Agent | show /don't show | show |
| Show information about user activity overview | show /don't show | show |

By default, the Atlas contains the set of monitoring settings so that each new user is covered by the maximally restrictive monitoring.

User groups

User groups may contain any number of user accounts and sub-groups. If a user group is not a sub-group, then its parent object, from which it inherits settings, is the Atlas.

In the configuration of group (or sub-group) settings, you can only define the settings that are less restrictive exceptions than the parent settings (of the Atlas or group which contains the specific sub-group). For example, the printout monitoring is enabled at the Atlas level. So, at the group level, you can only disable printout monitoring. This approach allows a certain user group to be excluded from monitoring.

Possible exception configurations at the group level:

- Monitoring

| Setting | Possible values |
|-------------------------|---|
| Bandwidth usage | don't monitor |
| Visited web pages | don't monitor |
| Application usage | don't monitor |
| Work time | don't monitor |
| Printouts | don't monitor |
| E-mails | don't monitor |
| Send activity over time | don't monitor |
| Activity breaks | don't monitor |
| Monitoring time | The monitoring time can only be set in the Atlas or individually for each user. |

- Remote access

| Setting | Possible values |
|---------------------------------|-----------------|
| Enable desktop preview | don't enable |
| Enable remote access | don't enable |
| Show notification | notify |
| Ask for user consent | ask |
| Enable if user does not respond | don't enable |

- Displaying Agent

| Setting | Possible values |
|---|-----------------|
| Show Agent icon | don't show |
| After logging in show information about Agent | don't show |
| Show information about user activity overview | don't show |

By default, no group contains any exceptions from the parent settings (Atlas).

The exceptions defined for a group are also propagated to all its sub-groups. In no way you can "exclude" a group from the propagation of settings or exceptions from the parent entities.

The exceptions defined for a group affect the settings of all users who belong to it (except for those who have individual settings defined). If a user is in more than one group, all exceptions from all these groups apply to them.

⊕ User

The user account can be subject to monitoring settings which are the result of Atlas and group settings, or may use the individual monitoring settings.

The monitoring and usage blockade settings can be configured in the **User info** window that is displayed after double-clicking on the user account name.

The **individual settings** allow the configuration of individual monitoring settings that will apply only to the user account for which they are set, regardless of the global settings and group exceptions.

The **resulting setting** is the global Atlas settings after considering the exceptions from all groups to which the specific user account belongs. If the user account belongs to several groups for which different settings of the same monitoring parameter are configured, the result will be the application of the less restrictive setting (e.g. don't monitor the application usage).

For each of the settings the Administrator can choose the application of the resulting or individual setting (e.g. the resulting setting will be the working time setting and that assigned individually will be the application usage setting).

The introduction of the new model of monitoring settings allows the application of the intuitive way of aggregating settings which results from the fact that the specific user account belongs to multiple groups (the account will be covered by all exceptions from the groups it belongs to).

A completely new approach to the management of monitoring settings indicates that group settings cannot be used to increase the rights, but only to limit them. This allows the use of the good practice of using Axence nVision 10 – building transparent network monitoring rules.

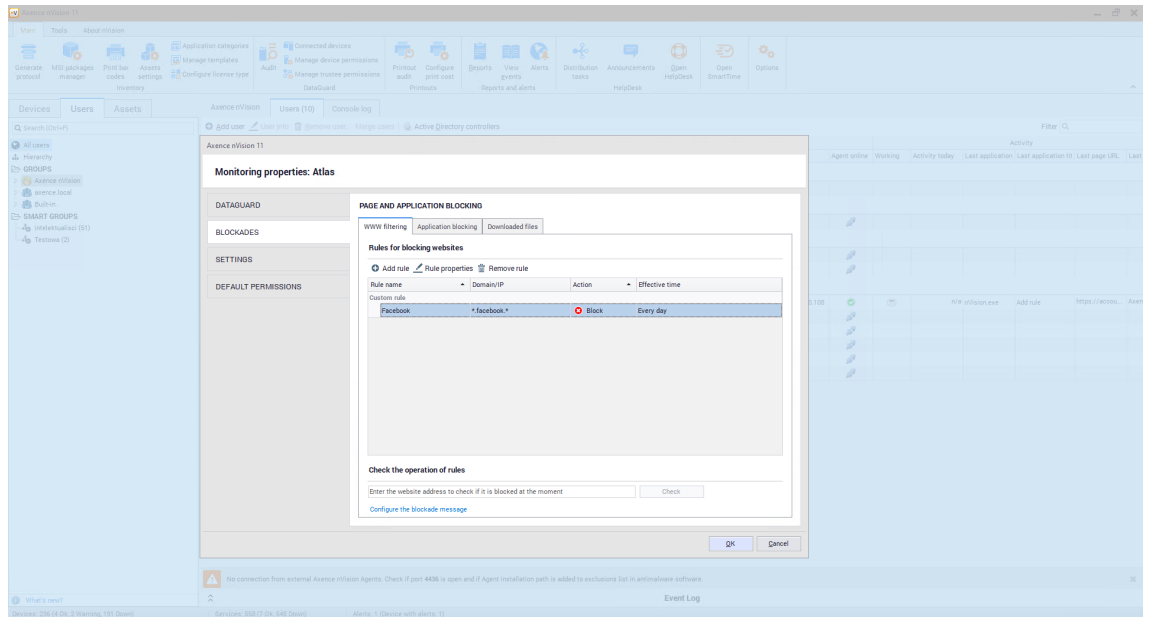
For example: enabling the work time and application usage monitoring on a global level, and then disabling this setting by way of exceptions at the user group level.

2.5.3.2 Blocking settings

The basic carriers of blocking settings in the latest version of nVision are: Atlas, User groups, and user account.

Unlike the monitoring settings (which have a predefined list of possible settings), the blocking settings are based on defining as many blocking rules as you like.

The Atlas does not contain any default blocking settings unless they have been created as a result of the data migration from nVision 9.



+ Blocking websites

In nVision 10, the default website blocking action: “Block all websites except for the following ones” has been removed. If the Administrator has not configured any website blocking rules, access to all websites is still possible (nVision behaves as if the default action was always set to “Enable for all websites except for the following ones”). In practice, this means that the website which does not match any of the defined rules is not blocked.

In the program, you can define as many website blocking rules as you like.

Each rule contains its own name, type of action, domain (or IP address) and effective validity time.

- The rule’s action is one of the two options: “Allow” or “Block”.
- Domain (or IP address) is a pattern to which the visited websites will be matched. In the pattern, you can use the “*” which indicates matching of any string.
- The effective validity time is a time pattern in which you can specify the days of the week or hours within the day. If the validity time has been defined, the rule is ignored outside this time.

If the visited website matches more than one rule, then:

- If all of these rules have the “Block” action set, the website is blocked.
- If at least one of these rules has the “Allow” action set, the website is not blocked.

If the website being visited does not match any rule, it is also not blocked.

+ Blocking applications

Similarly to website blocking, you can define as many application blocking rules as you like in nVision.

Each rule contains its own name, name of executable file to be blocked and effective validity time.

- For the application blocking rules, you cannot define the “Allow” action (each of these rules always comes with the “Block” action).

- You can also use the “*” in the pattern of the name of the executable file to be blocked.

If the application being run does not match any rule, it is not blocked.

▣ Blocking downloaded file extensions

Similarly to website blocking, you can define as many downloaded file extension blocking rules as you like.

Each rule contains its own name and file extension to be blocked.

- For the downloaded file extension blocking rules, you cannot define the “Allow” action (each of these rules always comes with the “Block” action).
- You cannot also use the “*” in the pattern of file extension to be blocked.
- The downloaded file extension blocking rules do not have the effective validity times (they are valid all the time).

If the extension of the file to be downloaded does not match any rule, it is not blocked.

Inheriting blocking settings

Atlas

Atlas is the primary object in nVision 10 that contains the essential, global blocking settings. It means that the user account which does not belong to any of the groups will adopt monitoring settings that are assigned to the Atlas.

Atlas does not inherit settings from any other entity.

The Atlas does not contain any default blocking settings unless they have been created as a result of the data migration from nVision 9.

User groups

Each user group contains all blocking rules of the Atlas and parent groups it belongs to.

At the group level, you cannot modify in any way the rules inherited from the Atlas or parent groups. You also cannot remove them or exclude from inheritance.

At the group level, you can define as many individual rules to be added to the set of inherited rules as you like.

The individual rules defined in a group are inherited by all descendant groups assigned to it.

User

The user account uses the rules inherited from groups (and the Atlas) and the individual rules.

For a single user you can disable inheriting the blocking rules from the Atlas and groups.

If the user has the rule inheritance function **enabled**, the summary collection of the following is applicable to them:

- rules inherited from the Atlas (if the user is not assigned to any group),
- rules inherited from all the groups the user is assigned to,
- individual rules defined at the level of this user.

If the user account is assigned to several groups for which different blocking rules are configured, the resulting blocking rules will be applied.

If the user has the rule inheritance **disabled**, only the individual rules are applicable to them.

Summary

- If any website was blocked globally, you can define the group of users who will have access to it.
- If any website was not blocked globally, you can define the group of users for whom it will be blocked.
- If a user is assigned to a group that has the “Allow” rule set for any website, you cannot override it by the “Block” rule and assign the user to another group.
- The “White List” function (“Block all websites except for the following ones”) can still be executed by means of the “Block” rule for the “*” domain.
- If any application or downloaded file extension was blocked globally, you cannot unlock them at the group level.
- If any application or downloaded file extension was not blocked globally, you can define the group of users for whom these entities will be blocked.
- At the user setting level, you can always define an individual set of rules, regardless of the inheritance mechanism operation.

2.5.4 Settings migration (nVision 9 to 10)

2.5.4.1 User accounts

As a result of the data migration from nVision 9 to user accounts synchronized with Active Directory, the activity will be copied from device icons in the older version of the program.

For each Windows local account from nVision 9 Agent which someone logged in to at least once, a user account will be created in nVision 10.

In version 11 of nVision, the rights included in user roles (User, HelpDesk Employee and Administrator) have been restructured into a new system of rights. Please read the [chapter](#)¹³⁹ which describes these changes in detail.

2.5.4.2 Monitoring settings

The monitoring settings available in Agent profiles in nVision 9 were moved to users and groups in the new version of nVision 10.

+ Default settings

The default settings are settings that were migrated from nVision 9 and assigned to the Atlas. Determination of the default monitoring settings in nVision 10 comes down to the aggregation of all settings in the Agent profile from nVision 9 that were used by at least one user account, whereas:

- if the selected option was monitored in at least one Agent profile in nVision 9, it is monitored in the default settings after data migration to nVision 10,
- if activity over time was being sent in at least one profile, it is sent in the default settings after migration,
- if breaks in activity were detected in at least one profile, they are also detected after migration,

- the migrated break time in the default settings is the minimum time selected from all existing Agent profiles,
- the monitoring time range in the default settings is the sum of all the time ranges in existing Agent profiles:
 - if time ranges do not overlap, a new range is determined during data migration, starting at the earliest and ending at the latest time from all existing profiles (e.g. the ranges of 8:00 - 12:00 and 15:00 - 18:00 will be migrated to the range of 8:00 - 18:00),
 - special case: if the continuous monitoring time was set for at least one profile, the default setting after migration will also be continuous monitoring,
- if any profile in nVision 9 allowed desktop preview, remote access or bypassing the user's approval for remote access, they will also be allowed in the migrated default settings,
- if any profile in nVision 9 allowed the Agent icon to be displayed, it will also be allowed in the default settings.

+ Group settings

In the migration process, user groups are created, and they are the carrier of monitoring settings from the existing Agent profiles. Each group contains monitoring settings such that the user belonging to this group is covered by the same monitoring settings as those in the Agent profile in nVision 9.

During data migration, the parent group "Monitoring" is created and includes 3 built-in subgroups:

- Groups from profiles,
- Groups from maps,
- Groups from devices.

The parent group and the built-in subgroups do not contain any built-in settings.

In the built-in subgroups, the user groups will be created and take the names after:

- monitoring profiles used in nVision 9,
- maps if they used individual settings in nVision 9,
- devices if they used individual settings (i.e. did not use the Agent profile or map settings).

Then, the accounts of users that were working on devices in the relevant profiles in nVision 9 will be added to the groups.

Additional information:

- The monitoring time range at the profile (group) level is not migrated. You may not establish these ranges at the group level in version 10 of the program. All time ranges from all profiles are aggregated into a single global range in the settings.
- None of the users receives individual settings in the migration process.
- As a result of the migration, the effective rights of the user working on more than one computer may be increased. For example, if the user was working on a computer with **enabled** monitoring and on another one where it was **disabled** in nVision 9, after migration the user **will not** be monitored on both computers (because the "Don't monitor" exception will apply to the user on both computers).
- The monitoring and blocking settings in nVision were connected with the device icon and the map on which the device was located. Thus, it was possible to define different security policies for new users (depending on the computer location). In nVision 10, there is a single set of default rights for each new user, therefore the Administrator has to manually create groups with rights and assign new users to them each time.

2.5.4.3 Blocking settings

⊕ Blocking websites

Default settings

The default settings are settings that were migrated from nVision 9 and assigned to the Atlas. Determination of the default website blocking settings in nVision 10 comes down to the aggregation of all “Block” rules in the Agent profile from nVision 9. Thus, a default set containing all website blocking rules is created.

Group settings

In the migration process, user groups are created, and they are the carrier of website blocking settings.

During data migration, the parent group “Filtering” is created and includes 3 built-in subgroups:

- Groups from profiles,
- Groups from maps,
- Groups from devices.

The parent group and the built-in subgroups do not contain any built-in settings.

In the built-in subgroups, the user groups will be created and take the names after:

- monitoring profiles used in nVision 9,
- maps if they used individual settings in nVision 9,
- devices if they used individual settings (i.e. did not use the Agent profile or map settings).

Then, the accounts of users that were working on devices in the relevant profiles in nVision 9 will be added to the groups.

Method for transferring settings:

- For the Atlas and each of the networks and Agents using the individual website blocking rules, the groups of blocking settings are created and placed in the parent group “Filtering”. Users are assigned to the groups (similarly to the transfer of monitoring settings).
- Each group of website blocking settings contains all the filtering rules that were previously assigned to the profile. These rules are set as individual rules for each of the groups.
- For each “Block” rule from the default settings which does not interfere with any individual group rule, the opposite “Allow” rule is created and assigned as an individual rule of the group. This action unlocks the websites that have not been locked so far, but could be locked as a result of the migration.
- After the transfer of settings, the removal of redundant rules in the default settings is performed: the “Block” rules that are included in other rules are removed (e.g. the rule for the “*.pl” domain contains the rule for the “domain.pl” website).

Additional information:

- In the migration process, none of the users receives individual website filtering rules.
- As a result of migration, the user that was working on more than one computer may have less websites blocked.
- If the global settings block the “*” domain and the individual group settings block the “domain.pl” domain only, the “Allow” rule will not be created for the “*” domain at the group level because this would make the “domain.pl” blocking rule ineffective. For this reason,

after migration, some of the groups may potentially block more websites than the corresponding profiles in version 9 of the program.

+ Blocking applications

Default settings

The default settings for blocking application execution are created by aggregating all existing blocking rules from all profiles (similarly to the default website blocking rules).

Group settings

During data migration, the parent group “Blocking” is created and includes 3 built-in subgroups:

- Groups from profiles,
- Groups from maps,
- Groups from devices.

The parent group and the built-in subgroups do not contain any built-in settings.

In the built-in subgroups, the user groups will be created and take the names after:

- monitoring profiles used in nVision 9,
- maps if they used individual settings in nVision 9,
- devices if they used individual settings (i.e. did not use the Agent profile or map settings).

Then, the accounts of users that were working on devices in the relevant profiles in nVision 9 will be added to the groups.

However, these settings will always be ineffective because the default settings will always be as restrictive or even more so. The purpose of this migration is only to find out what these profiles previously contained.

+ Blocking downloaded file extensions

Default settings

The default settings for blocking downloaded file extensions are created by aggregating all existing rules from all profiles (similarly to the default website blocking rules).

Group settings

Similarly to the migration of the application blocking rules, the settings in profiles are transferred to the corresponding subgroups that were previously created in the parent group “Filtering”. These settings are also ineffective and retained for information purposes only.

Additional information:

- The port blocking settings are not migrated to the user as they are interrelated with the device settings in nVision 10.
- Settings from all application blocking profiles and downloaded file extension blocking profiles are merged into one item of the default settings and apply to all users after migration. If you were using various profiles on multiple devices, the manual adjustment of the program configuration will be required after the migration process.

2.5.4.4 Blockade notifications

In nVision 10, for each of the following 4 types of blocking notifications, you can configure **exactly one version** of:

- notification of blocking a website,

- notification of blocking an application,
- notification of blocking a file,
- notification of blocking ports.

Therefore, during the migration process, the number of unique blockade notifications in version 9 will be checked, and the most numerous notification (for each of the 4 types listed above) will be copied to the new version of the system.

To configure blockade notifications:

1. On the ribbon, select the **Tools and Options** page, and then click **Options**.
2. Select the **Messages and blockades** tab.

2.5.4.5 Screenshots

The screenshots taken at the device level in version 9 of the program will be transferred to the user for whom they were taken.

The device level screenshot collection setting is not migrated. After the migration process, this setting must be enabled manually at the level of each of the users for whom screenshots are to be saved.

By assumption, the screenshot mechanism is temporary and enabled periodically, hence its settings are not migrated.

2.5.4.6 DataGuard settings

Default rights

As a result of the migration of settings from nVision 9, a set of default rights is created by aggregating the rights that have been granted so far to the Agents and to the superior entity of Active Directory (the highest level of “AD trustees”) so that it will include the maximally restrictive set of rights. As a result of the aggregation, more restrictive are:

- blocking the carrier,
- enabling the audit of file operations on the carrier.

Setting the maximally restrictive set of rights as the “Default rights” is necessary to ensure the continuity of data protection against data leaks for each new user directly after the migration.

Transferring DataGuard settings:

- The parent group “DataGuard Rules” with no defined custom settings will be created.
- The DataGuard rights assigned to the Atlas in nVision 9 are compared to the default rights in nVision 10. Then, the “Group from Atlas” is created as a subgroup of the “DataGuard Rules” parent group where any rights different from the default rights are assigned. The rights with the same values as those that previously existed in the Atlas are assigned to this group. The assigned rights are the individual rights for this group.
- For each map a group named “Group from map X” is created. It is a subgroup of the Atlas group or the superior map from the previous version of the program. Any rights different from the rights of the superior map group or the Atlas group are assigned to this group as individual rights.
- For each Agent that was using the individual DataGuard rights, the “Group from device X” is created where users working on this Agent in nVision 9 are assigned.
- The account of each non-domain user is placed in groups corresponding to the Agents they were working on. If a user was working on more than one computer, they will be assigned to all groups corresponding to the Agents they were working on.

The result of the migration is the representation of rights resulting from the structure of Atlas, maps and Agents in nVision 9 by means of a diagram of user groups which is simplified as much as possible. The final structure of nVision 10 only includes the groups that change the rights in any way. The DataGuard rights of domain users are not changed.

Additional information:

- After the migration to nVision 10, more restrictions may be imposed on each new user, even if they are created on an Agent that previously had no blockades in the DataGuard module.
- As the superior entity of “Active Directory” that aggregated rights for all users from AD is deleted, all settings which were defined in it will be lost. The remaining rights of groups and users from Active Directory are in no way modified during the migration process.
- As a result of the migration, it may turn out that users from Active Directory receive higher restrictions. This may be the case when the data carrier in nVision 9 was blocked at the Atlas level and a user from Active Directory had access to it as the additional rule providing access to this carrier was defined in the superior entity of “Active Directory”.
- Program in version 10 irretrievably loses the ability to define DataGuard rules at the host level. Thus, it is no longer possible to block and audit users on indicated devices only. Each user always has the same set of rules regardless of the computer they are currently logged on to.

2.5.4.7 Alerts and reports

Alerts

Alerts are in no way processed during the migration. Like in nVision 9, you can also configure alerts at the device icon level in nVision 10. Alerts created in nVision 9 will be transferred in the same form to device objects in the new version.

Reports

As a result of the data migration to nVision 10, the reports with information on user activity from specific maps or on indicated devices will be lost. Templates for these reports will still be available in the system, but a report generated by means of them will be empty. This is due to the fact that the user activity segments were moved to the section of reports generated for groups.

Therefore, before the migration process is started, the required reports for maps and devices using the existing templates should be drawn up, and then the report templates in the context of groups after the migration should be reconstructed manually.

2.5.4.8 Downgrade to nVision 9

Running the Axence nVision 10 installer will automatically backup the nVision 9 database. The backup copy contains program settings as well as data collected in monitoring.

To restore the data from nVision 9:

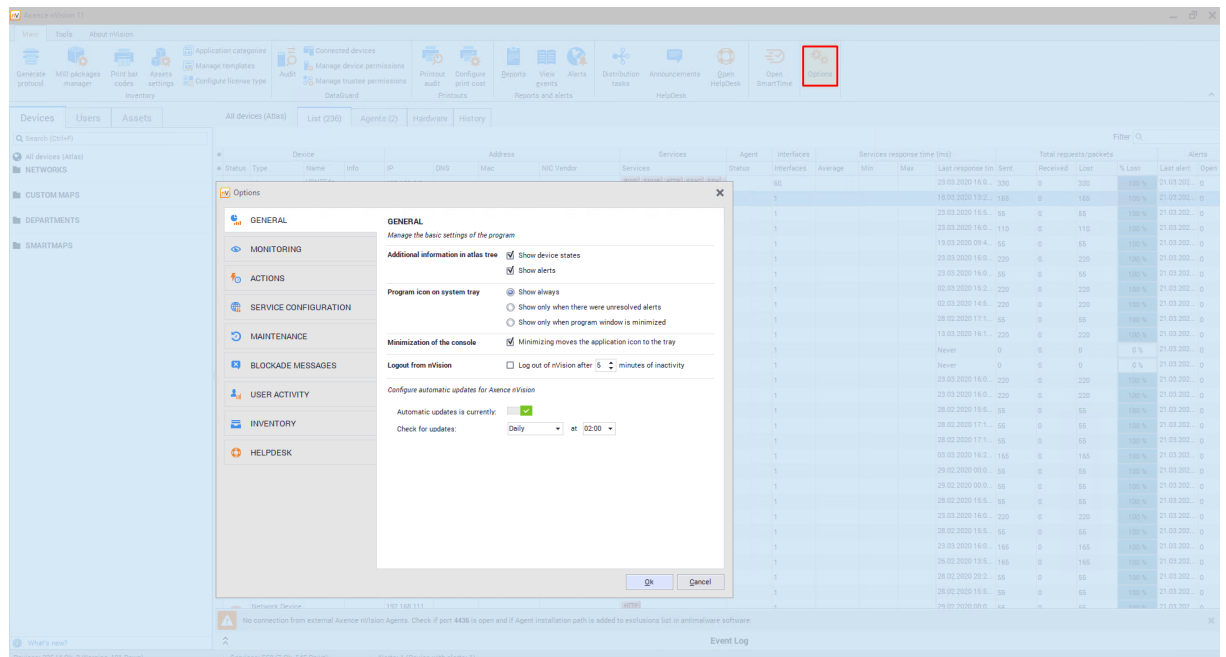
- If the installation of nVision 10 (or the migration process) is not successful and the Server does not start in the new version, the Agents will not be upgraded. If this is the case:
 - stop the “Axence nVision” service,
 - delete the **nVision.exe** file from the program installation path on the server,
 - download the nVision 9 installer (<https://cdn.axence.net/nVision9.zip>),
 - install the program,
 - restore the database backup copy by launching the **DBRestore** tool (by default: C:\Program Files (x86)\Axence\nVision\Backups).


- If upgrade to nVision 10 is successful and the program starts, the Agents that connected to the server will be automatically upgraded to the latest version.
In this situation, to make a full downgrade to nVision 9:
 - uninstall Agents (e.g. by running the relevant command from the context menu in the nVision console 10),
 - disable the nVision console,
 - stop the “Axence nVision” service,
 - delete the **nVision.exe** file from the program installation path on the server,
 - download the nVision 9 installer (<https://cdn.axence.net/nVision9.zip>),
 - install the program,
 - restore the database backup copy by launching the **DBRestore** tool (by default: C:\Program Files (x86)\Axence\nVision\Backups),
 - re-install Agents from the installer copied from the folder specified after clicking in the nVision console: [menu] **Agents / Install nVision Agents**.




2.5.5 Main program settings




To change program options:



1. On the ribbon, select the **Main** page, and then click **Options**.
2. Select the desired tab.
3. Edit properties according to the description below.



| Tab | Options | Description |
|--|---|---|
|  General | Additional information in the tree | Additional icons that are displayed in the map tree, next to the map name. Possible settings: <ul style="list-style-type: none"> • host states, • alerts, • both or nothing. |

| Tab | Options | Description |
|--|--|--|
| | Program icon on system tray | <ul style="list-style-type: none"> • always, • only on unresolved alerts, • only when minimized. |
| | Minimize console | Determines whether minimization moves the application icon to the tray. |
| | Log out of nVision | Logging out of nVision after the inactivity time as set in this option. |
| | Automatic updates | At this tab, you can enable automatic updates and change interval of checking for new versions of nVision. |
|  Monitoring | Services | The list of TCP services that will be scanned on each host by Axence nVision®. If you would like any service to be discovered automatically by nVision, you have to add this service to this list. |
| | Discover services on every interface | Check this option to scan for services on all the host addresses/interfaces. If unchecked, services will be scanned on the primary address only. |
| | Resolve addresses every X minutes | Time interval according to which nVision resolves IP addresses =>DNS. |
| | Maximum concurrent incoming Agent connections | <p>This parameter determines how many Agents can send information at the same time, e.g. about user activity.</p> <p>Note: use lower values if you encounter too high bandwidth usage.</p> |
|  Actions | | Some actions require being setup to function correctly, for example sending an ICQ message requires a UIN/password to login to the ICQ server. For a description of each action setup refer to Setting up actions topic ^[612] . |
|  Setting up services | | <p>Web Access can be enabled in this tab. If you want to learn more about Web Access, see How to get access to nVision via Web browser?^[620] and How to create Web Access user accounts?^[621].</p> <p>In this tab, you can also change API server settings for access from mobile applications. If you want to learn more, see Mobile application topic.</p> |
| | WebAccess console | Define the port number for access via Web browser ^[620] . |
| | HelpDesk | Define the port number for the port on which HelpDesk will be running. To enable encrypted communication in |

| Tab | Options | Description |
|--|--|--|
| | | HelpDesk, you must install a certificate for the domain ^[350] . |
| | SmartTime | Define the port number for the port on which SmartTime will be running. |
| | API Server | Define the port number for the Mobile Fixed Assets application for Android. |
| | Clean-up all data in database | Set the number of days after which the old data (of specific type) are removed from the database. |
| | Backup | Automatic backup profiles are managed in this tab. To learn more, see Automatic backup ^[630] . In addition to program setup, backup also includes the data collected in network monitoring, inventory data and HelpDesk module data. |
|  Maintenance | Restart nVision if not responding for X minutes | Axence nVision® is a very stable program, but we understand that it may be used to monitor critical assets. Therefore, it has a failover feature that will automatically restart the program in case of any problems to ensure continuous network monitoring. Check this option and set the time in minutes if you want Axence nVision® to restart if not responding. |
|  Blockade messages | | In this tab, you can setup your own messages that will be displayed in the case of an attempt to: <ul style="list-style-type: none"> • access a blocked website, • run a blocked application, • make an operation on external carrier in DataGuard, • download a file with locked extension by the browser. |
| | Applications | Defines groups of applications. You can create, edit and delete groups. The name of the application's executable file is compared to the name of file run by the process user. They are used in the user activity monitoring module (Users). |
|  User activity | Local networks | Defines addressing of local networks. A list of proxy ports separated with commas. They are used in the user activity monitoring module (Users) for monitoring of bandwidth usage and appropriate classification of network traffic (LAN/Internet traffic). |
| | Protocol patterns | Defines groups of protocol patterns – they are used in the user activity monitoring module (Users) for monitoring of bandwidth usage. You can create, edit and delete groups. The packet will be included in the |

| Tab | Options | Description |
|--|----------------|---|
| | | selected group if it meets at least one of the criteria: application's executable file name or ports on which it is running. |
| | Domains | Defines groups of visited webpages. You can create, edit and delete groups. |
|  Inventory | | This tab presents a list of directories that are not scanned during inventory monitoring. You can create, edit and delete entries. In this tab, you can also create the categories of file extensions that will be detected by Agents. |
|  HelpDesk | | This tab enables the management of HelpDesk's core settings ^[356] and tickets processing ^[358] options. Remember to configure also the HelpDesk port in the Remote Web access tab of nVision. |

2.5.6 Information for advanced users

The following functions are recommended for advanced users only.

Agent service calls from the browser

In all of the following calls substitute *_IP with the IP address of the machine on which the nVision Server or Agent is installed.

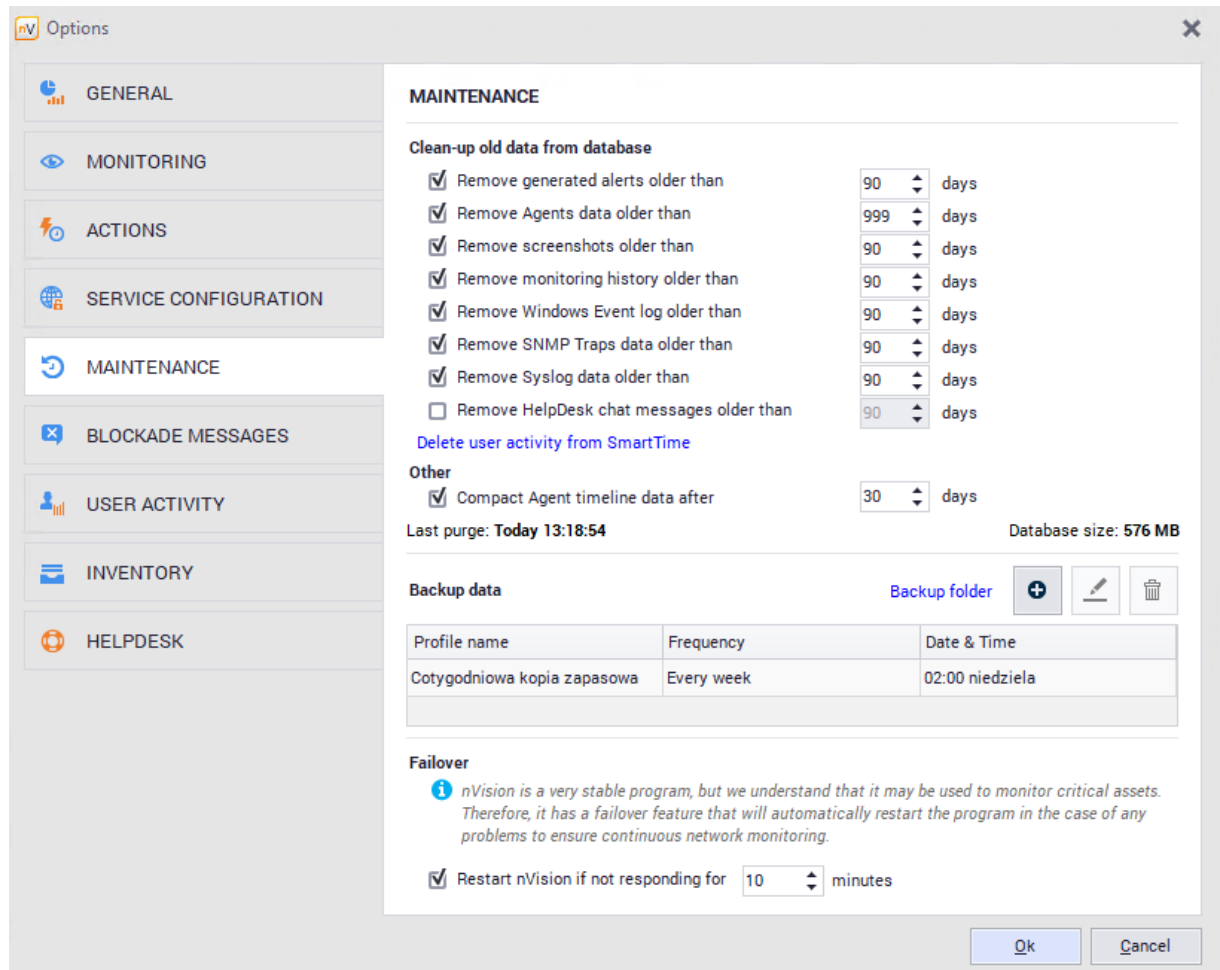
1. Checking information on the active Server:
http://SERVERS_IP:4434
2. Checking information on the active Agent (checking the Machine GUID):
http://AGENTS_IP:4433
3. Checking information of the active Atlases:
http://AGENTS_IP:4433/atlasses
4. Downloading Agent setup file:
http://SERVERS_IP:4436/nVAgentInstall.exe
5. Downloading Remote Console setup file:
http://SERVERS_IP:4436/nVisionSetup.exe

2.6 nVision performance

In case of a large number of Agents that send their data to nVision, perform the following actions to obtain high performance.

More than 250 Agents

1. Navigate to the main program configuration and click the **Maintenance** tab.
2. Enable the **Compact Agent timeline data after** option.



More than 1000 Agents

1. Navigate to the **Settings** window for the Atlas or group or to the **User info** window.
2. In the **Settings** window, change the **Send timelines data** to **Don't monitor**.

2.7 “Report a problem” function

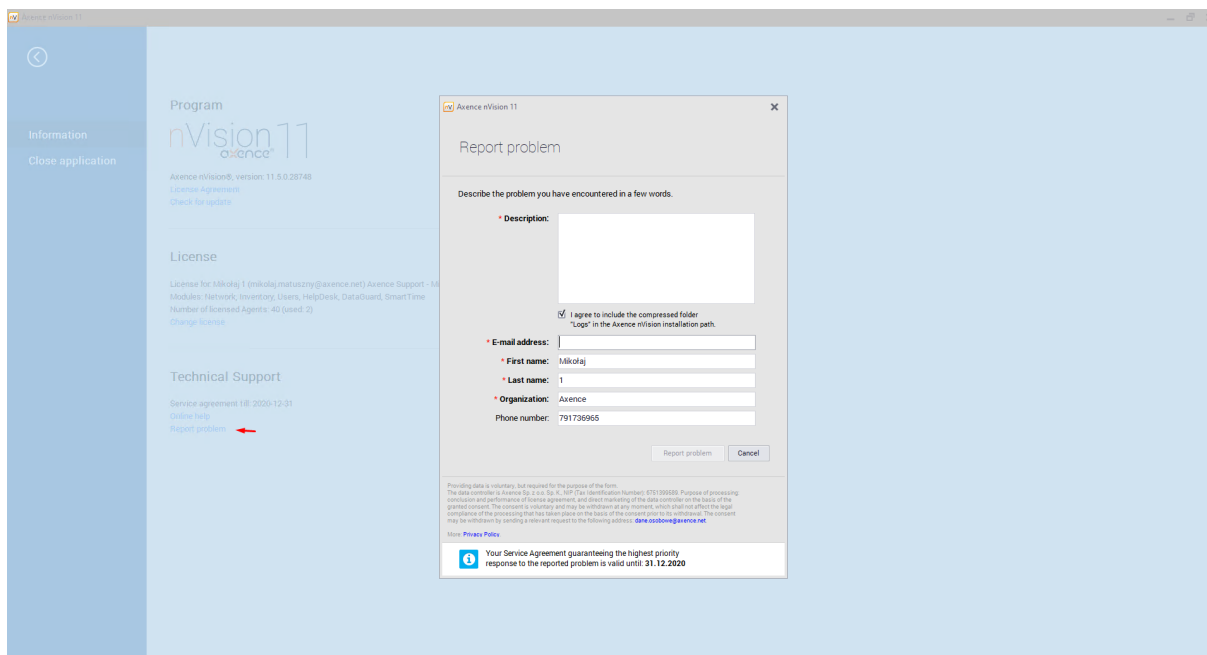
Axence nVision® 10 offers simplified problem reporting, available by using the **Axence nVision / Report a problem** option in the menu bar. The purpose of the function is provide the Administrator with an easy way to report any observed issues or faults in the software operation.

In order for the function to work, the machine needs to have an active connection with the installed Axence nVision® Server with the Internet.

To report a problem:

1. Click the **About nVision** page in the menu bar and then the **Report a problem** link.

- In the new **Report a problem** dialog box, fill in a brief form:



- Checking the **I agree to attach the compressed “Logs” folder from Axence nVision® installation path** field will add an attachment with a cleaned and compressed (2MB) archive of the nVision Server log folder (by default: C:\Program Files (x86)\Axence\nVision\Logs). Sending the software runtime logs facilitates the problem analysis and shortens the report processing time.
- When the **Report a problem** button is clicked, the message is sent to: pomoc@axence.net.

The first response from a Technical Support Employee is sent within a few hours and not later than on the next working day (in the case of problems requiring a thorough log analysis, the time can be longer).

The administrator can check the ticket status by logging into <https://service.axence.net/hc/en-us/requests> portal with the e-mail address given in the **Report a problem** form. The link for the password setup is sent automatically to the specified e-mail address after the ticket is created. The password can also be reset manually with use of the form available at: https://axence.zendesk.com/auth/v2/login/password_reset.

2.8 GSM device configuration

nVision enables an admin alert notification to be defined by means of SMS messages.

Sending notifications via SMS is a convenient way of informing in case of occurrence of predefined [events](#)⁵⁹³, such as significant change in the website content (attack suspected), files copied to the mobile device, or hardware resources changed. Messages can be sent via mobile phones connected via USB, COM and cable driver and the GSM modem (usually also connected via USB). It is easy, because many operators provide long-term SIM cards.

Important: operators do not guarantee immediate delivery of SMS. In the case of critical notifications do not rely on SMS text messages or e-mails.

Tested devices

The following common telephones and modems were tested for cooperation with the software:

- Falcom: Twist, Swift, Samba 55, Samba 75,
- iTegno: WM1080A, WM1080A1I, WM1080A1E, 3000, 3232E, 3232I, 3898,
- Multitech: MTCBA-G-UF1, MTCBA-G-UF2,
- Nokia: N30, N32, 6100, 6210, 6220, 6310, 6310i, 6820 (Bluetooth), 8910,
- Siemens: TC35, TC35i, TC45, TC65, MC35, MC35i, MC45, MC55, MC65, MC75, A65, AC75, AC45, C35, C45, M35, M45, S35,
- SIMCOM: SIM100S, SIM100T,
- Sony Ericsson: T310, T610, T630, T68, T68i, K310, K320, K500, K510, K600, K700, K750i, K800i, V800, W300, W550, W600, W700, W800i, W810, W900, Z1010, GC75, GC79, GC83, GC85, GC89,
- Teltonika: T-ModemUSB, T-ModemCOM,
- Wavecom: Fastrack M1206B, Fastrack M1306B, Integra, WMOi3.

In addition to the models listed above, all USB modems should function properly.

Note: GSM device needs to be configured using software provided by its manufacturer (especially SIM-card's PIN needs to be entered).

If you want to learn more about notification actions, go to [Defining action properties](#)⁶⁰⁶ topic.

Part



3 Network discovery and monitoring

3.1 Introduction

Requirements and planning

Please read the [Requirements and configuration](#)^[20] topics before you start monitoring your network. These topics describe how to configure hosts and nVision to get all the information you need.

Discovering the network

nVision has a built-in very advanced automatic network scanner allowing you to not only discover all hosts in your network, but also it can discover all routers and go through them to scan all neighboring networks. It discovers all hosts and services running on them, like: HTTP, FTP, mail, database servers, etc.

You can add as many networks to the Atlas as you need. When adding a network, it will be scanned for hosts so first you have to go through the network discovery wizard to define scanning options.

When the discovery process is finished, the program will create a network map or a set of maps for all discovered IP networks. The networks will be created as a tree. This tree shows network dependencies between them.

For more information about network discovery refer to [Discovering the network](#)^[51] topic.

Monitoring hosts

nVision can monitor network services, system and SNMP counters. It not only monitors them, but also logs all the information and allows viewing historical data for reporting purposes.

For more information about network monitoring refer to [Monitoring](#)^[55] topic.

Host status

Host status in nVision is such an important idea that we dedicated it separate topic for it: [Host status concept](#)^[50]. You should definitely read it to fully understand how nVision presents host status.

3.2 Host status concept

Host status as calculated value

Unlike in other similar products, host status in nVision can be changed by events. You can define conditions when a host is considered to have a status <Unknown>, <Up>, <Down> or <Warning>. Of course, host status changes also automatically to reflect the status of services.

Automatic host status changes

Host status is initially set to <Unknown>. It changes when nVision starts to monitor services. After the first service is determined to be running, status changes to <Up>. The status is <Warning> when one or more services are down, but there is still at least one responding service. The host status changes to <Down> when every service is down i.e. not responding.

Host status changed by event

It is very important to understand that nVision also determines the host status according to currently raised events. For this purpose you can define the **Change host status to** field of each event. When an event for a host is raised, then host status may change according to the host status value defined in this event.

There are three host status values that you can define in this field: <No change>, <Warning> and <Down>. Status <Down> has the biggest priority, which means that if there is at least one event raised with such status, then the host status also becomes <Down> (no matter the status of services). If there are several events with <Warning> and <Down> status raised, then the host status will also be <Down>. If there are only a few events raised with <Warning> status, then the host status becomes <Warning> (unless it is already <Down> due to all services being down - then the status remains <Down>).

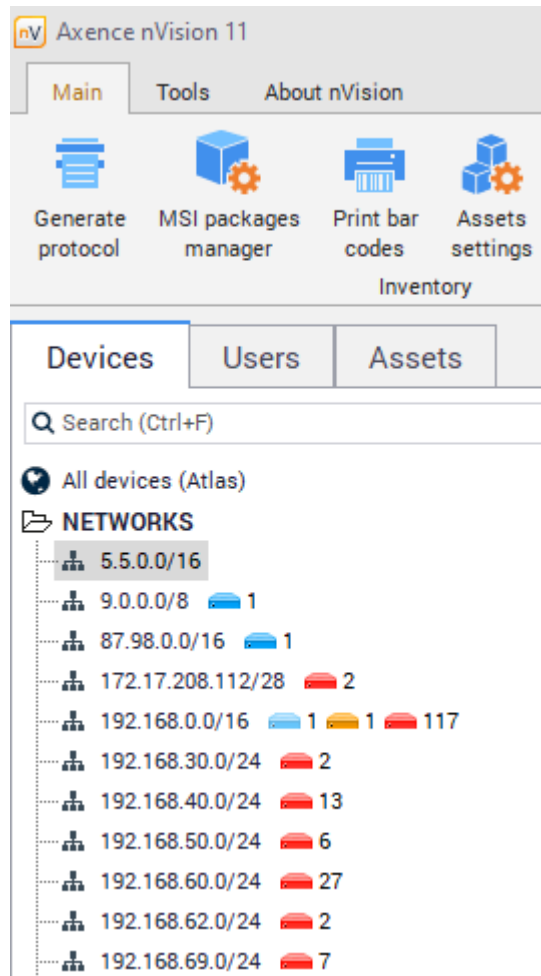
3.3 Discovering the network

3.3.1 Discovering the network

You can add as many networks to the Atlas as you need. When adding a network, it will be scanned for hosts so first you have to go through the network discovery wizard to define scanning options.

1. Click the **Discover new network** option (on the **Tools** tab).
The Scan network wizard will open. This wizard will help you to scan your network, discover all hosts and create maps of your network.
2. Follow the screens of the wizard. For a description of all options available in it, refer to [Network discovery wizard](#)⁵³ topic.

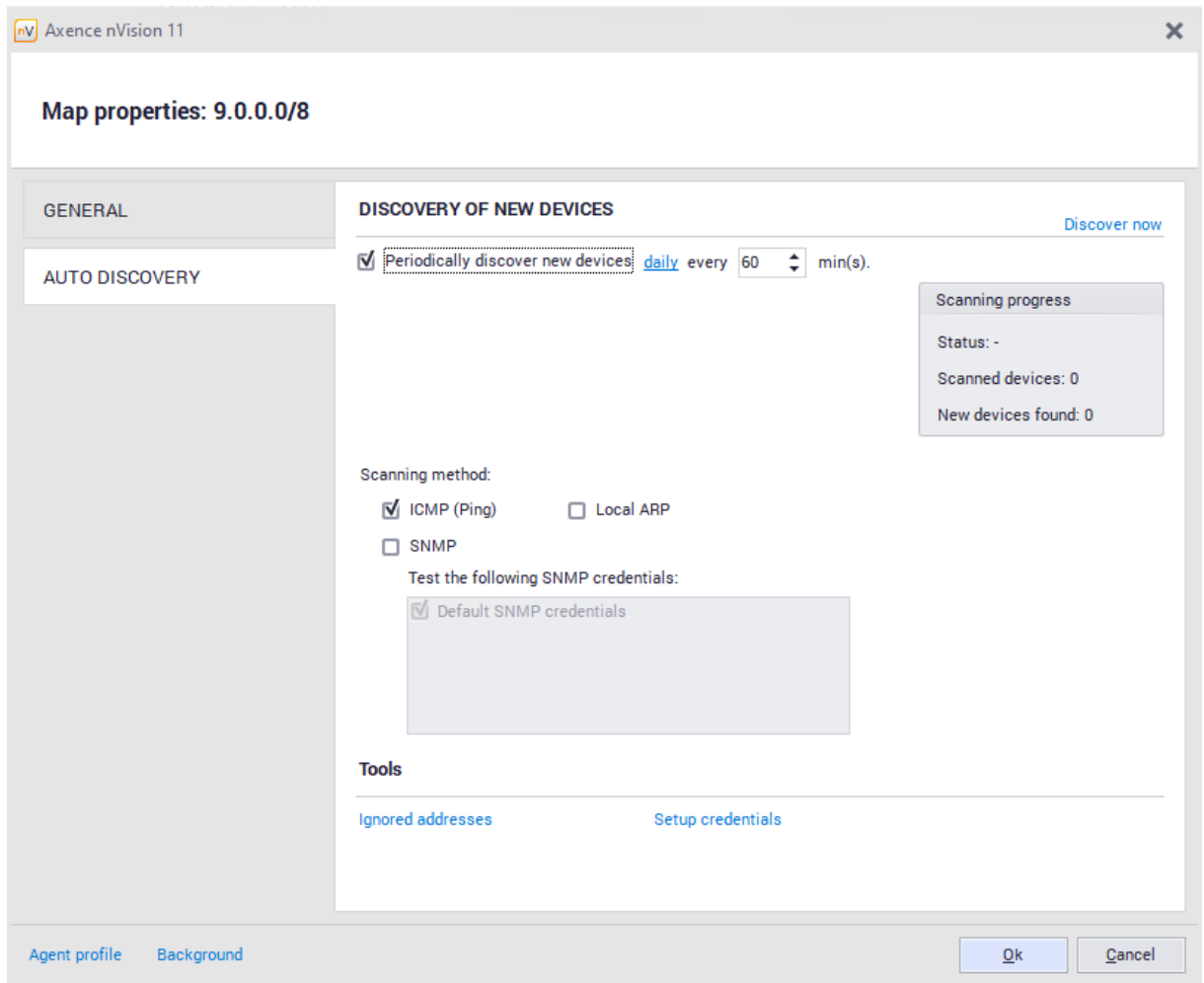
When the discovery process is finished, the program will create a network map or a set of maps for the discovered network. The networks will be created as a tree. This tree shows network dependencies between them - the networks created as children are networks connected to the parent map. Let's see the following example:



As you can see, the network 192.168.0.0 is a child of the network 172.17.208.112. It means that those networks are connected through a router. nVision discovers all routers and connected networks, which allows you to see the network logical structure.

nVision can also discover hosts automatically by selecting the **Discover a new host** option from the map context menu. This process can be carried out periodically.

1. Select the map on which you want to enable the automatic discovery.
2. Open the **Map properties** window and select the **Automatic discovery** tab, which allows the discovery process to be configured and started. This tab also shows the current status and progress on the status bar.
3. Select the **Periodically discover new hosts** option.
4. Configure the frequency and time of discovery.
5. You can also start the discovery by clicking the **Discover now** button.



3.3.2 Network discovery wizard

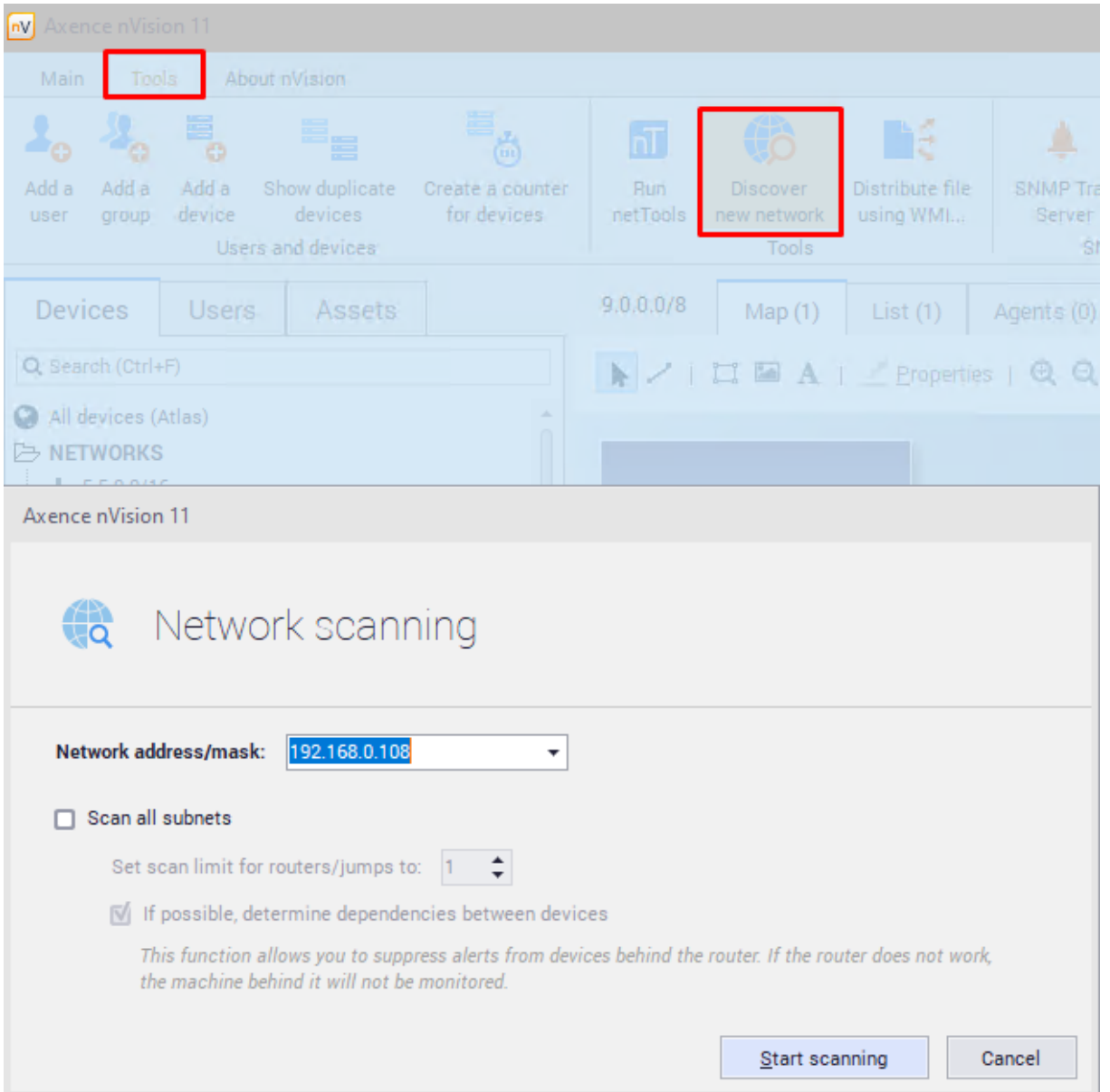
The network discovery wizard helps you to define all options required to properly scan a new network. This wizard opens when you want to add a new network or when you are creating a new Atlas.

New network scan options

They allow you to define which network will be scanned and how.

| Property | Description |
|------------------|---|
| Address | Enter the IP/DNS address of the host located in the network you want to scan. The program automatically enters the local address, which you can leave unchanged if you want to scan your local network. |
| Mask | The network mask. In most cases you need not to change this field which defaults to "255.255.255.0". If changed it can result in a very long discovery time. |
| Scan all subnets | Check if you have a router in your network and also want to scan neighboring networks behind this router. |

| Property | Description |
|---|---|
| | nVision can scan not only the network you entered, but it can also go “through” routers in this network and scan all connected networks. This function works if the router is SNMP manageable and you will provide (or already provided) the SNMP community. The program will read the routing table from the router and try to scan all networks connected to this router. |
| Set scan limit for routers/jumps to | Allows you to limit the number or hops (routers) while scanning. |
| If possible, determine dependencies between devices | This feature allows for the limiting of the alerts from devices behind the router. If the router is inactive, the devices behind it will not be monitored. |



Click **Scan**. This will start the discovery process. You will be able to see the discovery progress. You can stop the network discovery anytime. If you stop it before it finishes scanning the network, you will still be able to add the networks and hosts discovered so far.

When the discovery process is finished, you will see a message specifying the number of hosts/networks discovered. Click the **OK** button to close the scanner window and add all discovered hosts and networks to the Atlas.

3.3.3 Adding a new host

For instructions on how to add a new host, refer to [Managing hosts](#)^[101] topic.

3.4 Monitoring

3.4.1 Introduction to monitoring

What can be monitored?

nVision can monitor the following:

- **Host status**

This is monitored for every host and it allows you to get reports about each host availability over time.
- **Services**
 - Availability: in case the service stops responding nVision will present such information on the map and can raise an alert.
 - Performance: response time and percent of packets lost. You can monitor any TCP/UDP service. There is a large predefined list of available services including MS SQL Server, Oracle, Notes/Domino, etc.
- **Mail and web servers**

Specific service tests: nVision has several built-in probes that can check the performance of several high level features of service. It includes probes such as:

 - Web page load time – measures the time of loading a specific web page.
 - Web page contents change – checks for any change of web page contents.
 - POP3 Login time – measures the time it takes to successfully login to a POP3 server.
 - SMTP send time – measures the time it takes to successfully send an e-mail with an SMTP server.
- **Routers and switches (MRTG)**
 - Network interfaces: status and in/out network traffic.
 - Switch ports: the information about every port status, MAC and IP of computers connected to any port and their total network in/out traffic.
 - Host network traffic: the network traffic generated by a network device (monitoring RMON with SNMP)

- **Performance counters**

- SNMP: you can monitor any SNMP counter that returns numeric values.
- Windows: nVision allows monitoring Windows counters, which helps to monitor system performance itself and also the performance of applications running on it. So you can monitor counters of such services like MS SQL Server, Exchange server, etc.

Visualization

nVision has the ability to present all the monitored parameters (both for services and counters) on clear charts. Not only you get the reports of the values over time, but you can watch them in real-time also.

Monitoring time

When you setup the monitoring time in the host properties, it does not mean that the services and counters will be monitored exactly every such period. When nVision has to monitor a large network with many hosts, the monitoring interval may increase because nVision can send only a specific number of requests per second. Consequently, host monitoring time is just the shortest time that can be used for monitoring services and counters. In case of several number of hosts this time may increase significantly.

How monitoring data is handled

nVision collects all monitoring data in the program's memory first. This information is gathered in the form of consecutive probes stored at the time of each poll. You can see all of those probes on the 15-minute chart only. After all gathered data exceeds the limit of allocated memory then the oldest probe is removed every time a new one is added.

Monitoring information is saved to the database in 1-minute averages. Therefore, when viewing performance charts for long intervals you can see those data with a 1-minute resolution at best. nVision does not save all probe values because the program is designed to monitor large networks. In such networks with many hosts, the amount of data gathered every day is significant and it would be not possible to process it in reasonable time. It would also fill up even a very large hard drive very fast.

3.4.2 Concepts

Service scanner and monitor

After discovering all hosts in your network, nVision scans for services running on them. It scans only a sub range of all available services. To read how to select services to be scanned, refer to [Program Options](#)^[42] topic.

Service scanner not only checks if a service port is open. It also sends a specific request and checks if a response matches predefined criteria. If so, the service is being added to the host and nVision starts to monitor it.

The service monitor uses a similar mechanism as the service scanner: it sends specific requests to the TCP/UDP port (service) and logs the response time and percent of requests (packets) lost. It also checks if the received response matches specific criteria.

Counter monitor

You can also monitor several types of counters with nVision. The table below lists available counters:

| Counter type | Description |
|---------------------|---|
| Host status | Indicates host status for every minute. Allows reporting of hosts availability. |
| SNMP | SNMP counters are provided by SNMP protocol available on routers and most servers. They allow the information such as network transfer, number of users, CPU utilization, etc. to be monitored. |
| Windows | nVision can monitor all Windows counters including those provided by non-system applications like MS SQL Server or Exchange Server. |
| Page load time | Measures the loading time of a specific web page. |
| Page content change | Indicates selected web page changes. |
| POP3 login time | Checks the time to login to the POP3 server. |
| SMTP send time | Measures the time required to send an e-mail. |

Host status

Unlike in other similar products, host status in nVision is a calculated value, not a hard coded one. So you can define conditions when a host is considered to have status <Up>, <Down> and <Warning>. For more information about host status refer to [Host status concept](#) topic.

3.4.3 Monitoring services

3.4.3.1 Service discovery and monitoring

How services are detected and monitored

nVision monitors UDP/TCP services based on a predefined set of rules. It not only checks if the specific port is open, but sends a request and waits for a response. Then, the response is examined to meet specific criteria. Only those services where a response is valid are considered as properly functioning services. The same mechanism is used to discover services running on hosts. It ensures that services are not mistakenly discovered when any service is running on the port supposed to be for another one. For example if FTP would be running on port 80, nVision will not discover service HTTP, as the response is not valid as an HTTP response.

Service down

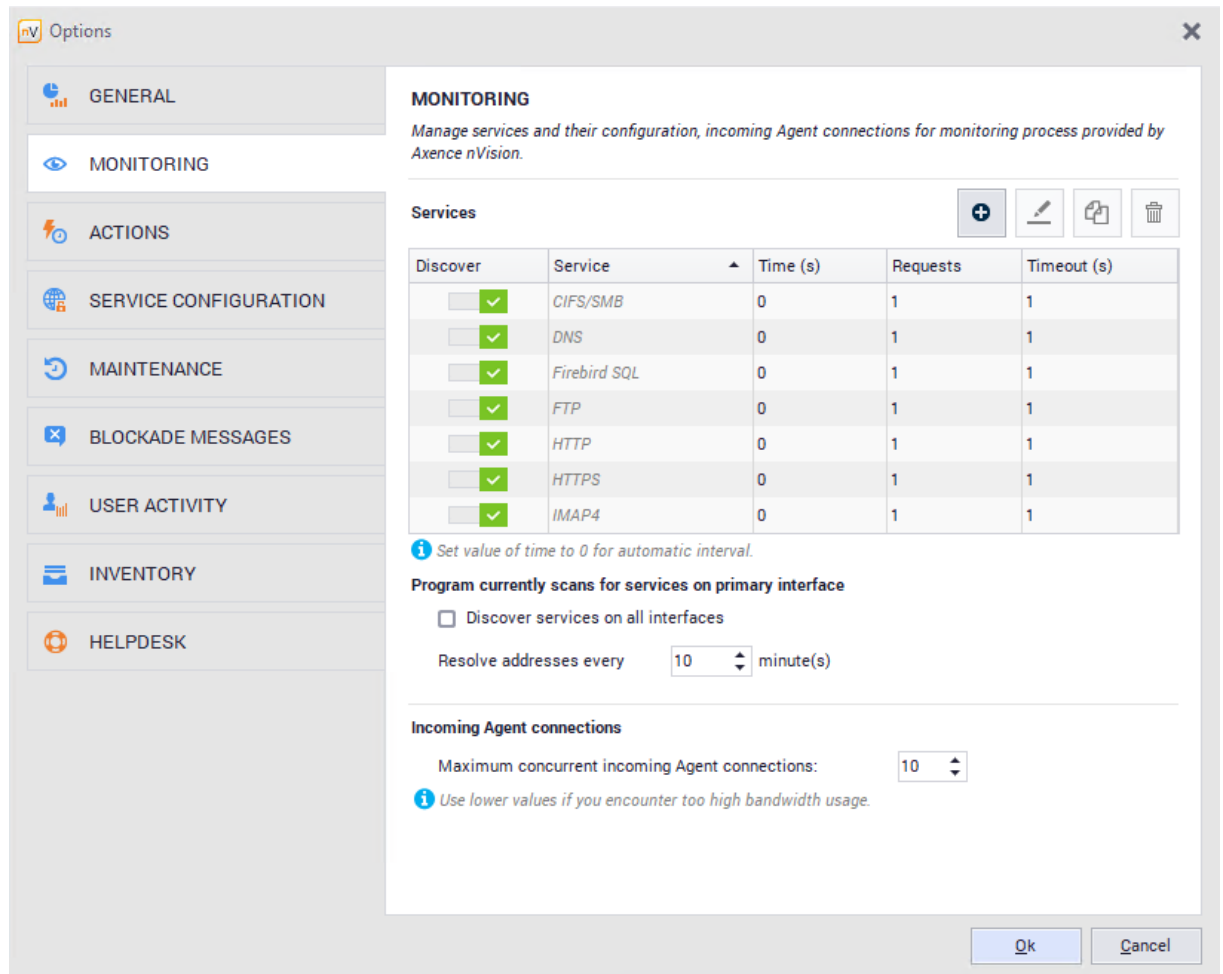
After a service stops responding, then it gets the status <Down>. You can see that as a red colored icon in the service grid (available on the **Services** tab in the **Host Info** window).

Leading service

There is always one **leading** service for each host. This service is indicated by bold font in the service grid located in the **Host info** window. The **leading** service is the most important service of the host. Its response time can be presented on the host icon.

How to monitor hosts and services?

After discovering hosts in your network, nVision automatically scans for the most important services running on them. So, there is no need to take any further actions in addition to discovering the network to begin monitoring of hosts and their services. However, you can add a new service manually or by calling the service discovery tool.



Options

MONITORING
Manage services and their configuration, incoming Agent connections for monitoring process provided by Axence nVision.

Services

| Discover | Service | Time (s) | Requests | Timeout (s) |
|-------------------------------------|--------------|----------|----------|-------------|
| <input checked="" type="checkbox"/> | CIFS/SMB | 0 | 1 | 1 |
| <input checked="" type="checkbox"/> | DNS | 0 | 1 | 1 |
| <input checked="" type="checkbox"/> | Firebird SQL | 0 | 1 | 1 |
| <input checked="" type="checkbox"/> | FTP | 0 | 1 | 1 |
| <input checked="" type="checkbox"/> | HTTP | 0 | 1 | 1 |
| <input checked="" type="checkbox"/> | HTTPS | 0 | 1 | 1 |
| <input checked="" type="checkbox"/> | IMAP4 | 0 | 1 | 1 |

Set value of time to 0 for automatic interval.

Program currently scans for services on primary interface

Discover services on all interfaces

Resolve addresses every minute(s)

Incoming Agent connections


Maximum concurrent incoming Agent connections:

Use lower values if you encounter too high bandwidth usage.

Ok Cancel

Adding services

To add a new service to the default list of monitored services:

1. Go to nVision settings located on main toolbar. Navigate to the  **Monitoring** tab.
2. If you want to add a service, click the add button and select the service that is to be monitored from the list. To manage the service definitions, click the **Manage services** button.

Services on hosts

A list of monitored services including charts that represent the response time and percent of packets/requests lost is available in the [Host status](#)^[82] window.

For more information about services refer to [Managing hosts](#)^[101] topic.

3.4.3.2 Managing monitored services

This topic provides more information on how to manage service monitoring.

Opening host info window in the Services tab

With this window you can list, modify, create and remove monitored services. It not only lists all Services, but also presents charts, where you can review the service response time value over time. Charts can present the service monitoring information in real-time.

1. Double-click the host icon or select **Host info** from its context menu.
2. Select **Performance / Services** tab.

Adding a new service to the monitor or modifying existing one

1. Open **Host info** window on the **Performance / Services** tab.
2. Click the add icon (located on the right-bottom side of the services grid) to add a new service or select the existing service and click the edit icon to modify service properties. The **Service properties** window will open.
3. Now you have to configure the options. This is described in detail in the following table.

| Property | Description |
|-----------------------|--|
| Service to monitor | |
| Name | Select the service you want to monitor. This field cannot be changed when editing the existing service. To start monitoring another service, you have to create it. |
| On interface/IP | Select the address on which this service will be monitored. |
| Monitoring parameters | |
| Monitoring time | After selecting Auto , nVision will control the monitoring interval to ensure frequent polls (based on the number of |

| Property | Description |
|----------|--|
| | monitored hosts). If you want to set this to any specific value, then select Set and enter this value in the edit box. |
| Requests | This is the number of requests sent on each poll. For all TCP services this value should be set to 1, as the protocol has its own mechanism to prevent lost requests (TCP services have their own mechanism to repeat lost requests, so it usually does not make sense to enter a higher value). For ICMP and UDP based services, you should set it to 2-3 to ensure that one incidentally lost packet will not trigger false alerts. |
| Timeout | The time to wait for a response. If not received by that time, a request is considered lost. For ICMP and UDP services value of 1000 - 2000 ms will be usually sufficient. For TCP services, because of their nature, you should enter much higher values of 15 000 - 30 000 ms. |

+ Deleting a service

1. Open **Host info** window on the **Performance / Services** tab.
2. Select a service to delete.
3. Click the dustbin icon to delete the service.

+ Rediscovering host services

1. Open **Host info** window on the **Performance / Services** tab.
2. Click the **Discover again** option.
nVision will start scanning for new services on all interfaces/addresses of the host. When finished, new services will be added to the list and monitoring of the new services will start.

+ Selecting a leading service

For information about the leading service refer to the [Monitoring services](#) ⁵⁷ topic.

1. Open **Host info** window on the **Performance / Services** tab.
2. Select a service and select **Set as leading** from its context menu.
The leading service is indicated by bold font.

3.4.3.3 Setting-up alert for services

If you would like to be notified when any service experiences any problems then you need to create an alert. This topic describes all the necessary steps that are required to do that.

1. Click the **Alerts** icon located on the **Main** page ribbon to open the alerts window.
2. Click the **Add alert** icon located on the main toolbar to create a new alert.
The alert properties window will open. With this window you will create an event that will trigger the alert and add actions to be executed when the alert is raised.

3. Click the **New** button located on the right side of the event combo box. This will allow you to create an event.
For services you should select the **Service down** or the **Service performance** event type. Create an event according to the information in the [Event properties](#)^[597] topic.
4. Click the add icon and define the action to be executed when an alert is raised. You can select any existing action or also create a new action. To create a new action, click the New button located on the right side of the action combo box. Create an action according to the information in the [Action properties](#)^[606] topic.

3.4.3.4 Monitoring Windows services

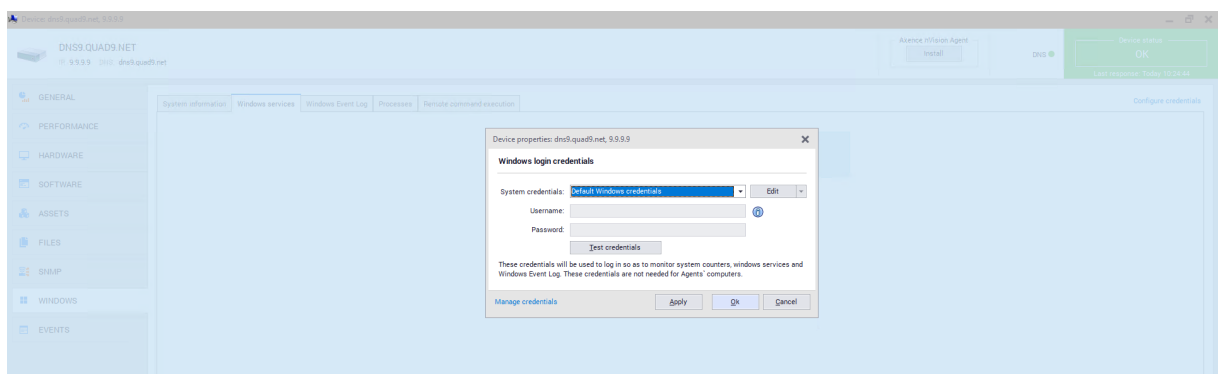
nVision can monitor Windows services. In case of any problem with any service (i.e. service going down) you can configure an alert action that may start or restart the service. Service monitoring is performed with WMI or by Agents.

In order to monitor by WMI, you have to properly configure credentials in the host properties window. Also WMI has to be enabled on the remote host. Please refer to [Requirements and configuration](#)^[27] topic for more information.

To monitor Windows services without opening remote access to WMI, [install Agents](#)^[115].

To turn Windows service monitoring on:

1. Open the [Host properties window](#)^[82].
2. Select the **Windows** tab.
3. Navigate to the **Windows services** window, click the **Configure login credentials** link and enter the details of the administrator account on the remote host.



3.4.4 Monitoring device and system performance

3.4.4.1 Performance counters and host status

nVision can monitor several types of performance counters and host status.

Host status

This is a built in counter which monitors and logs the host status. This counter is logged every minute so you could track host availability over time.

Windows and SNMP counters

nVision can monitor Windows counters using WMI or Agents. The counters can be used to monitor Windows system performance, application performance (MS Exchange, IIS, SQL etc.), switches and routers (network traffic, errors, etc.), etc.

Specific service test (mail and web server monitoring)

This is a group of counters designed to monitor mail and web servers. For more information please refer to the [Monitoring mail and web server](#)^[66] topic.

3.4.4.2 Counter types

There are several general groups of counters. The following list describes the Host availability and Counter groups. For more information about the Specific service test group, please refer to the [Monitoring mail and web server](#)^[66] topic.

| Host availability | |
|-------------------|--|
| Host status | This counter stores the host status for reporting purposes. It is a built-in counter and cannot be removed. |
| Counters | |
| SNMP counter | You can measure any SNMP counter with a numeric value format. The program may also read the whole table column and log min/max/avg/sum of its cell values. |
| Windows counter | You can measure any Windows counter with numeric value format. Windows provides system and application counters. So it allows monitoring the system itself as well as programs like SQL Server or Exchange Server. |

Host specific counters

Some events have all the information required to check them already defined, including host address. Such events are called host specific. In general, all events of the **Specific service test** type are host specific.

3.4.4.3 Managing performance counters

This topic provides more information on how to manage performance counters.

+ Opening Host info window on the Performance counters tab

With this window you can list, modify, create and remove counters. It not only lists all counters, but also presents charts where you can review the counter value over time.

1. Double-click the host icon or select the **Host info** from its context menu.
2. Select the **Performance / Performance counters** tab.

+ Creating a new counter or modifying an existing one

1. Open the **Host info** window on the **Performance / Performance counters** tab.

2. Click the add icon located on the right-bottom side of the counter grid to add a new counter or select the existing counter and click the edit icon to modify its properties.
The **Counter properties** window will open.
3. If you are creating a new counter, then select the counter type on the list and click the **Next** button. To find out about counter types, refer to the [Counter types](#)^[62] topic.
4. Configure the counter options (depending on the counter type you selected). This is described in details in the [Defining counter properties](#)^[64] topic.
5. Click the **Finish** button.

+ Deleting a counter

1. Open the **Host info** window on the **Performance / Performance counters** tab.
2. Select a counter to delete.
3. Click the delete icon to delete the counter.

3.4.4.4 Setting-up alert for performance counter

This topic describes how to setup an alert to be triggered when a performance counter value goes out of range. For example, let's assume you would like to create an alert, which will notify you when a mail queue on any of your MS Exchange servers is too big. You will need such a counter on every host running Exchange server and the event defined to trigger an alert. nVision provides a tool to easily define an alert and automatically create the necessary counters on each host running MS Exchange.

1. Click the **Alerts** icon located on the **Main** page ribbon to open the alerts window.
2. Click the **Add alert** icon located on the main toolbar to create a new alert.
The alert properties window will open. With this window you will create an event that will trigger the alert and add actions to be executed when the alert is raised.
3. Click the **New** button located on the right side of the event combo box. This will allow you to create an event.
For counters you should select one of the **Specific service tests** or **Counters** event type. Create an event according to the information in the [Event properties](#)^[597] topic.
4. Click the add icon and define the action to be executed when an alert is raised. You can select any existing action or also create a new action. To create a new action, click the **New** button located on the right side of the action combo box.

Create an action according to the information in the [Action properties](#)^[606] topic.

3.4.4.5 Creating a counter on many hosts at once

In many cases it is necessary to create the same counter on several hosts. You can do that using the automatic counter creation mechanism. It allows creating the same Windows or SNMP counter on many hosts.

It can also create it only on those hosts that support such counter by testing if it is present on the remote machine.

1. Select **Create a counter for a group of hosts** from the **Tools and options** page on the ribbon.
The **Counter definition wizard** will open.

2. Select **Windows** or **SNMP**.
3. Select the counter and enter monitoring time.
4. Select **All** to create the counter on all hosts or select **Selected** to select hosts. Select hosts in the grid using Ctrl + Click and Shift + Click.
5. Check **Create only if the host supports the counter** if you want nVision to verify if the counter is present on the remote host before creating it. With this tool you can quickly create many counters only on hosts that have this counter.

Counter patterns

There is also a second option that allows you to easily set the same counter on different devices. For this purpose, we can use the so-called counter patterns. All created counters form a list of counters that can be used multiple times. Counter patterns can be added only on devices that support the given counter - the program will check if it is available on the remote device.

To use a counter pattern you have to:

1. Open the appropriate computer settings window.
2. Click on the **Performance** section.
3. Click on the **Counters** tab and then click on the "X" icon
4. In the window for adding a counter, click the **Duplicate existing counter** option, and then select an appropriate counter pattern from the list.
5. Click the Next button, and then click the **Finish** button.
6. After completing the above steps, the selected counter will be added to your computer.

3.4.4.6 Defining counter properties

This topic describes properties of different counter types from the **Counters** group.

Windows threshold

| Property | Description |
|----------|--|
| Name | The name that will be displayed on the list. |
| Counter | The counter to be monitored. To choose the counter, click the *** icon and select the appropriate class, counter and instance. You may need to setup credentials first so nVision could connect with the remote host and read the counter list. |

| Property | Description |
|---------------------|---|
| Monitoring interval | After selecting Auto , nVision will control the monitoring interval to ensure frequent polls (based on the number of monitored hosts). If you want to set this to any specific value, then select Set and enter this value in the edit box. |

Notes

- nVision will try to login to the remote host using the credentials defined in host properties.
- Windows counters are not monitored if the host is <Down>.

SNMP threshold

| Property | Description |
|--------------------------|--|
| Name | The name that will be displayed on the list. |
| Choose SNMP counter | The counter to be monitored. To choose the counter, click the "" icon and select the appropriate SNMP counter. It is possible to read the whole table column and log min/max/avg/sum of its cell values. You may need to setup the SNMP read community first so nVision could connect with the remote host and read the counter list. |
| Enter SNMP counter OID | The counter to be monitored. When entering OID manually, you are responsible to provide a correct value. If this OID is not valid then the counter will not read any value. |
| Absolute | The program will store the value that has been read. |
| Average per second, unit | Based on the consecutive counter values, nVision will calculate the rate per second and store this value. This is a good option if you monitor the number of bytes sent/received and you want to monitor bandwidth usage. You can also select the units in which this value will be stored. |
| Monitoring interval | After selecting Auto , nVision will control the monitoring interval to ensure frequent polls (based on the number of monitored hosts). If you want to set this to any specific value, then select Set and enter this value in the edit box. |

Notes

- nVision will try to login to the remote host using the credentials defined in host properties.
- Windows counters are not monitored if the host is <Down>.

3.4.5 Monitoring mail and web server

3.4.5.1 Mail and web server monitoring counters

nVision has several special counters designed to monitor mail and web servers. These counters not only connect to the server, but also perform some test to ensure proper server operation: test the page load time and content, list incoming e-mails and try to send a test e-mail. To perform such test operations, you have to create the appropriate counter on the **Performance counters** tab in the **Host info** window. For more information about counter (test) types and operations performed, refer to the [Counter types](#)^[66] topic. For information about creating counters refer to the [Managing performance counters](#)^[62] topic.

3.4.5.2 Counter types

The following list describes only Specific service test group responsible for mail and web server testing. For information about other groups (Host availability and Counters) please refer to the [Monitoring device and system performance](#)^[61] topic.

Specific service test

| | |
|-------------------------|---|
| Web page load time | Measures specific web page load time. |
| Web page content change | Checks for any accidental changes to the specific web page content. |
| POP3 login time | Measures the time required to login to the mail server. |
| Send mail time | Measures the time required to send an e-mail message. |
| Test HTTPS connection | Tests HTTPS connection; it is possible to use a client certificate. |

Host specific counters

Some events have all the information required to check them already defined, including host address. Such events are called host specific. In general, all events of the **Specific service test** type are host specific.

3.4.5.3 Defining counter properties

This topic describes defining properties of different counter types from the **Specific service test** group.

+ Web page load time

This counter measures specific web page load time. When adding a counter for a given page, when the counter is read for the first time, the page is downloaded to the folder on the server (C: \ Program Files (x86) \ Axence \ nVision \ Downloaded Webpages) - provided that "its" is not there yet (downloaded the page may be in a folder, e.g. if the nVision database was restored using DBRestore).

| Property | Description |
|---------------------|---|
| Page URL | The page address of the page to be checked |
| Monitoring interval | After selecting Auto , nVision will control the monitoring interval to ensure frequent polls (based on the number of monitored hosts). If you want to set this to any specific value, then select Set and enter this value in the edit box. |

+ Web page content change

This counter indicates percentage changes to your web page content.

| Property | Description |
|---------------------|---|
| Page URL | The page address of the page to be checked |
| Monitoring interval | After selecting Auto , nVision will control the monitoring interval to ensure frequent polls (based on the number of monitored hosts). If you want to set this to any specific value, then select Set and enter this value in the edit box. |

+ POP3 login time

This counter measures the time required to login to the mail server and check the list of available mails.

| Property | Description |
|---------------------|---|
| POP3 server address | The address of the mail server. |
| Username | The username required to login. |
| Password | The password required to login. |
| Monitoring interval | After selecting Auto , nVision will control the monitoring interval to ensure frequent polls (based on the number of monitored hosts). If you want to set this to any specific value, then select Set and enter this value in the edit box. |

+ Send mail time

This counter measures the time required to send an e-mail message.

| Property | Description |
|------------------------|---|
| SMTP server address | The address of the mail server. |
| Authorization required | Check this field if your SMTP server requires authorization to allow sending e-mail. |
| Username | The username required to login. |
| Password | The password required to login. |
| Send e-mail message to | The e-mail address where the message will be sent. The time of sending this message will be measured. |
| Reply address | If this address is not set properly or blank most mail servers will reject an e-mail. Enter the e-mail address, which you know will be accepted by the mail server (your e-mail address most likely). |
| Monitoring interval | After selecting Auto , nVision will control the monitoring interval to ensure frequent polls (based on the number of monitored hosts). If you want to set this to any specific value, then select Set and enter this value in the edit box. |

3.4.6 Monitoring routers and switches

3.4.6.1 SNMP monitoring


With nVision you can monitor the following information with SNMP:




- **Interfaces:** status and current network traffic. You can also configure monitoring of network in/out traffic on every interface. Such information is available then on the **Performance counters** tab and you may see charts presenting the traffic.
- **Switch ports:** nVision automatically reads SNMP information related to switch ports if possible. When such information is available, then you will see a **Port mapper** tab in the **Host info** window. This tab shows the information about every port status, MAC and IP of computers connected to any port and their total/current network in/out traffic.
- **Network traffic:** some switches and routers collect the information about the network traffic generated by each device. This information is available with RMON tables. nVision automates the process of monitoring the network traffic generated by a specific host.

This helps to extensively monitor your network infrastructure, status of your switches, routers and network traffic.

3.4.6.2 Monitoring switch ports

nVision automatically reads port information for every SNMP-manageable switch. This information is presented in graphical form in the **Host info / SNMP / Port mapper** window. The following table lists the meaning of every image:

| Icon | Description |
|---|---|
|  | The port is active, but nothing is connected to it. |

| Icon | Description |
|---|---|
|  | The port is active with plug connected. |
|  | The port is inactive (disabled) and nothing is connected to it. |
|  | The port is inactive (disabled) with plug connected. |

The tab may not be available in the beginning (after the network is scanned). It will show automatically only when nVision reads the SNMP information from the “dot1dBasePortTable” table (OID: 1.3.6.1.2.1.17.1.4), which may take some time. If the tab is not shown for a long time, please make sure that SNMP on this host is available and you properly configured the SNMP community in the host properties.

To enable port mapping on a switch:

1. Navigate to the **Host info** window.
2. In the **General** tab, check **Enable monitoring** field (services, counters, SNMP, port mapping, Windows).
3. In the **SNMP / SNMP browser** tab, check the **SNMP manageable device** field and click the **Configure login credentials** – link, and then configure a correct SNMP community (set in the device management panel). Make sure the login credentials are correct by clicking the **Test login data** button (the test should terminate with “SNMP community test successful” message).

The port mapping tab should appear in the **Device information** window.

If the above settings are configured correctly and the mapper port tab is still not generated, make sure the table “dot1dBasePortTable” is available at the given device (by reading its contents in the “SNMP” tab according to the tree specified in the link below).

<http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en&translate=Translate&objectInput=1.3.6.1.2.1.17.1.4#oidContent>

3.4.6.3 Monitoring node network traffic

Some switches and routers collect the information about the network traffic generated by each device. This information is available with RMON SNMP tables. nVision automates the process of monitoring the network traffic generated by a specific host.

Monitoring host network traffic

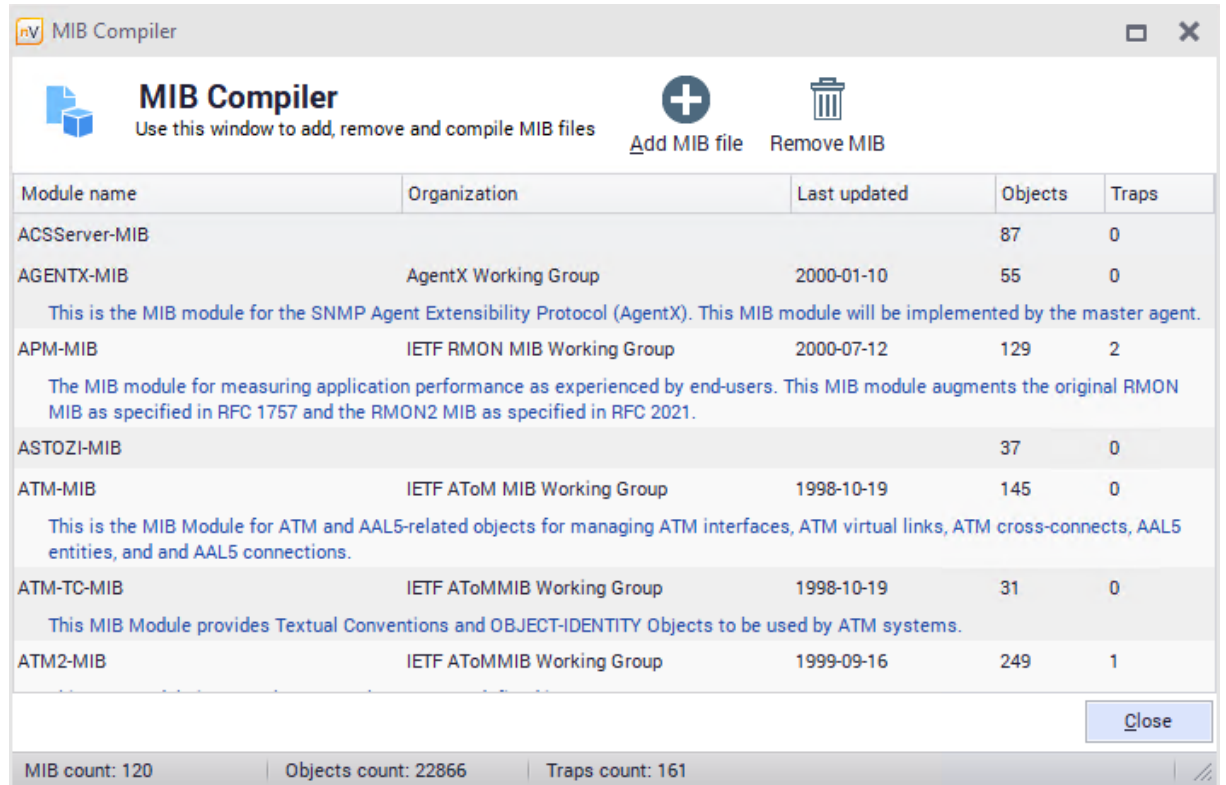
1. Open **Host info** window.
2. Navigate to the **Port mapper** tab. If such tab is not available, it means that there is no such information for this device. [Please refer to the ⁶⁸Monitoring switch ports⁶⁸](#) topic for more information.
3. Select the grid row which lists the information for the host, which you would like to monitor. Select **Monitor host network traffic** from the context menu.
This will create two SNMP monitoring counters (for incoming and outgoing traffic). These counters will be available on the **Performance counters** tab.

3.4.7 MIB file compiling

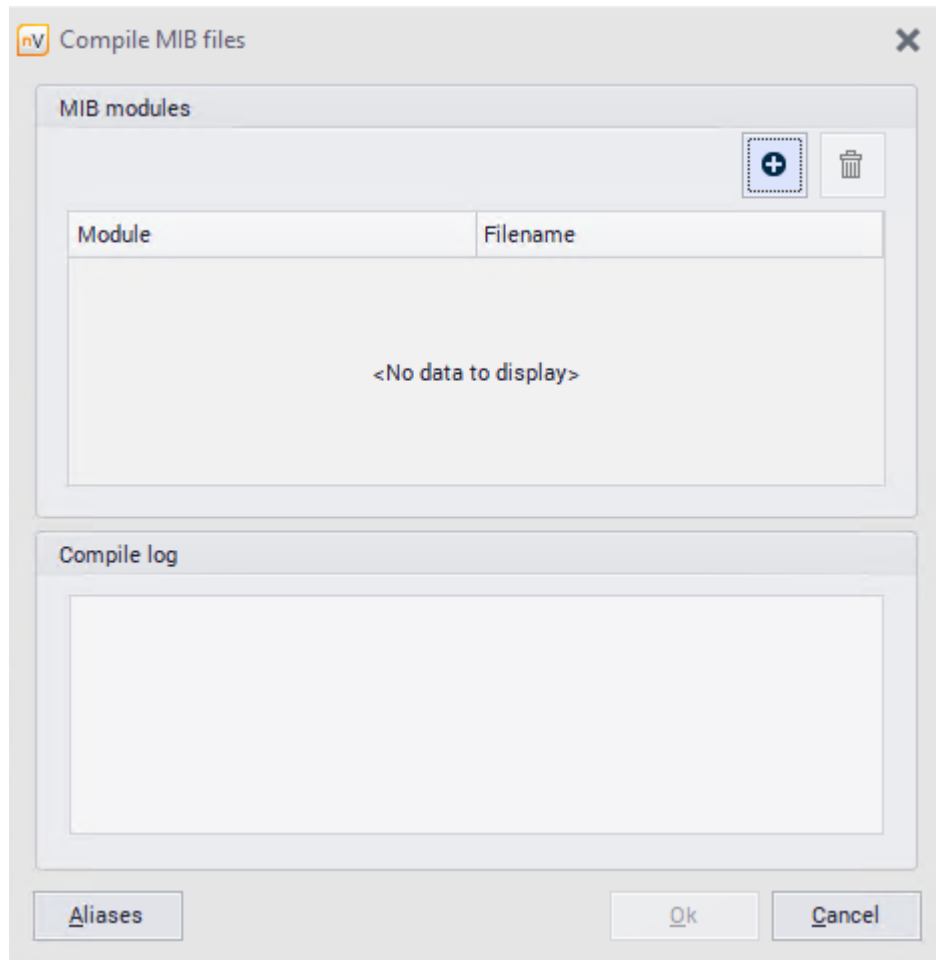
MIB compiler enables you to add new, remove and compile MIB files, which facilitates gathering SNMP information from all network devices: switches, routers, printers, VoIP devices etc. The program can now effectively monitor thousands of different SNMP devices.

To use MIB compiler:

- Select **MIB compiler** from the **Tools** tab on the ribbon. A MIB compiler window will open.



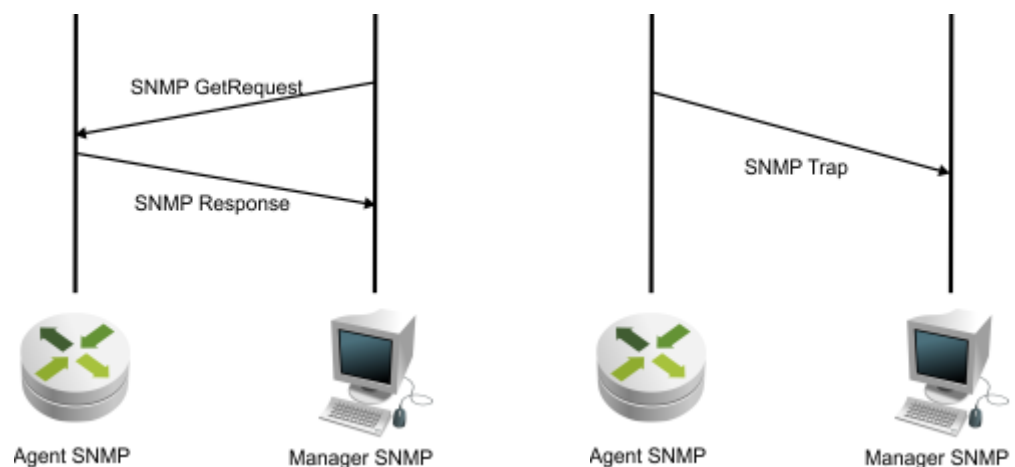
1. If you want to add a new file, click the add button.
2. Add a MIB module by clicking the add button and selecting a file from its localization. Compile log is shown after compilation.



3. You can also define aliases in the Aliases editor (the **Aliases** button).

3.4.8 SNMP traps

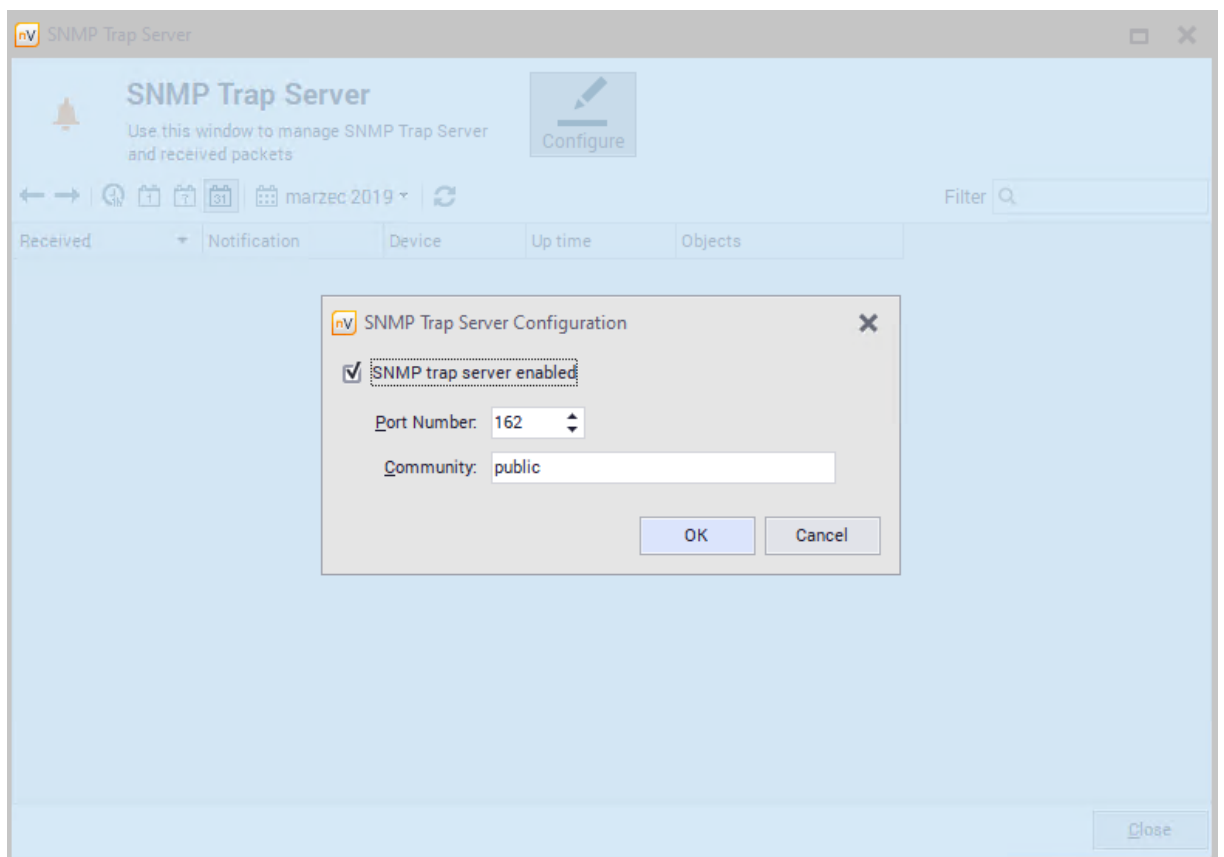
The SNMP Trap allows SNMP Agents to report the change of its status to the manager, if a specified event takes place. The following diagram presents the differences between a contact established by a manager (on the left) and Trap message sent by the Agent (on the right).



SNMP Trap Server

To manage the SNMP Trap server:

1. Select **SNMP Trap Server** from the **Tools** tab on the ribbon.
2. Traps detected by the server are displayed in the SNMP Trap Server window. You can choose the period of the displayed data (hour, day, week, month).
3. To configure the server, click the **Configure** button in the top part of the window.
4. Set the listening port and access policy options. Mark the **Server autostart** field, if it should be launched automatically on application startup.



SNMP Trap as action

To define the SNMP Trap as an action:

1. Select **Manage actions** from the **Tools** tab on the ribbon.
2. In the Action Definition Wizard window, enter the action name and select **Send SNMP Trap**.
3. Fill out the fields **Host name**, **Port**, **Community** and **PDU type**.

4. The **Notification ID** field is required if enterpriseSpecific is selected as **Service type**.
5. According to the specification of the SNMP Trap, it is possible to specify the SNMP Agent address if different than the address of the sending device, and MIB object with additional notification details.


Related topics

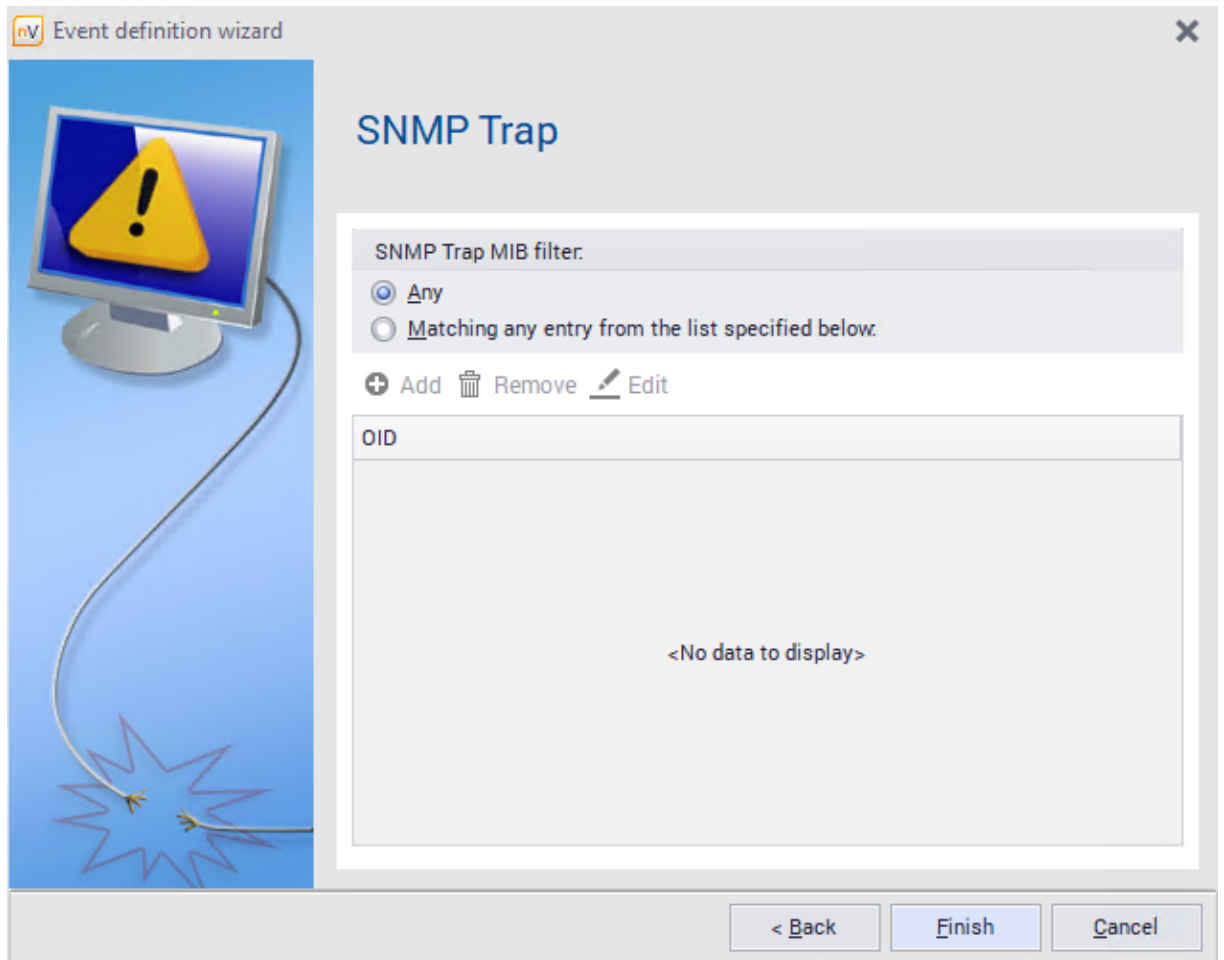
 [Alerting](#)

 [Actions](#) ⁶⁰⁴

SNMP Trap as event

To define the **SNMP Trap** event:

1. Select **Manage events** from the **Tools and options** tab on the ribbon.
2. Enter the event name and select the event type **Other / SNMP Trap**. Select **Next**.
3. In the Event definition wizard set the **MIB Filter**. If the second option is chosen,  **OIDs** of MIB objects to be included in the defined event.



Related topics

 [Alerting](#)

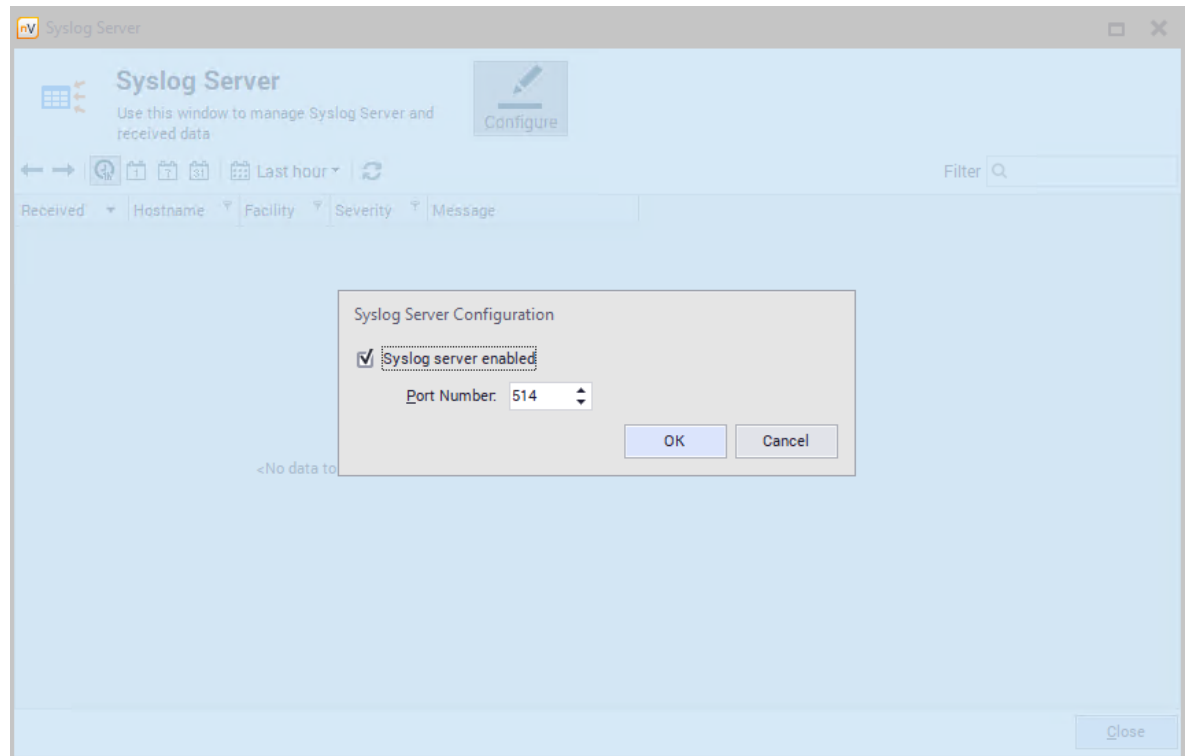
 [Events](#) 593

3.4.9 Syslog server

Syslog server

To manage the Syslog server:

1. Select **Syslog server** from the **Tools** tab on the ribbon.
2. Messages detected by the server are displayed in the Syslog Server window. You can choose the period of the displayed data (hour, day, week, month).
3. To configure the server, click the **Configure** button in the top part of the window.
4. Set the listening port. Mark the **Server autostart** field, if it should be launched automatically on application startup.

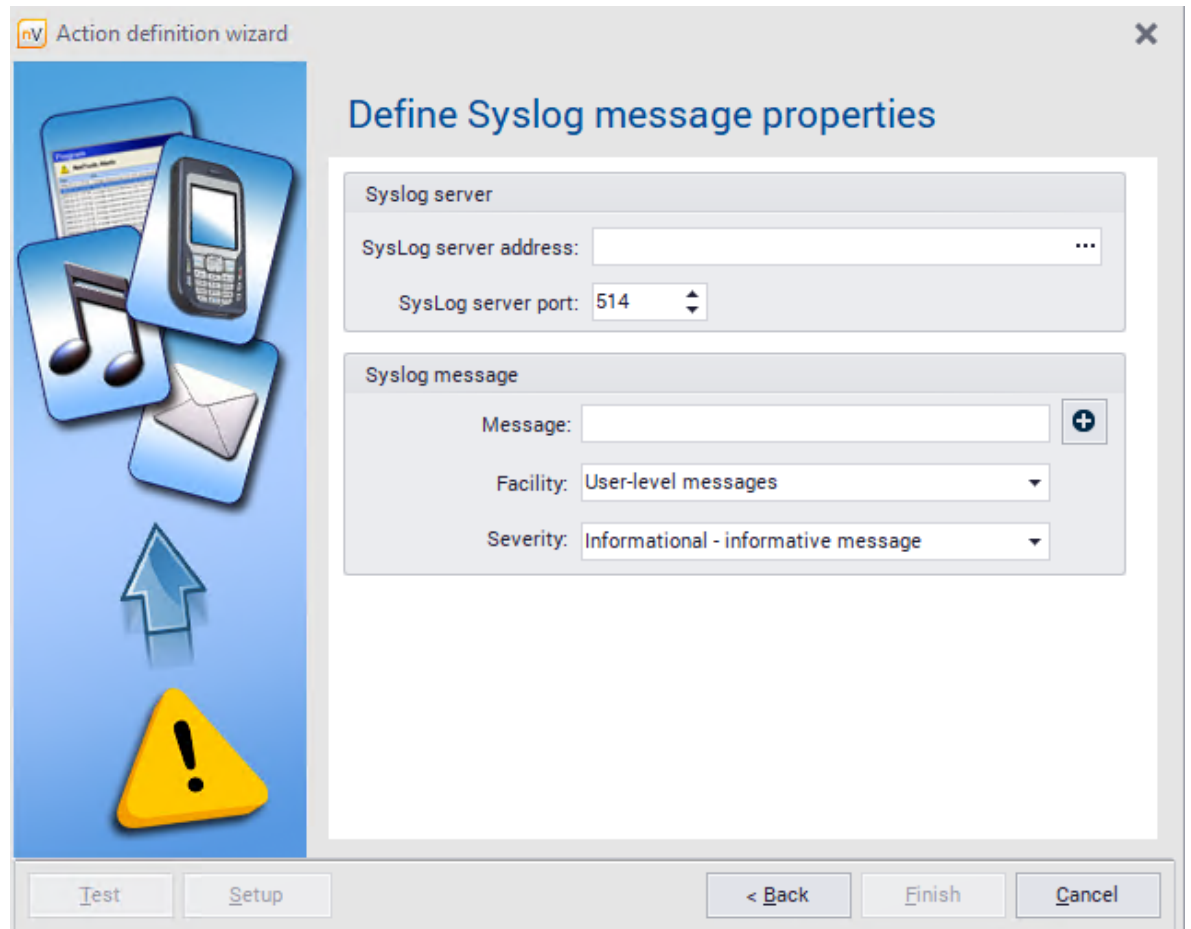


5. In the administration panel of a particular device, give the address and port of the Syslog server to which messages will be sent. It is the address of the nVision server and the port configured in 4.

+ SysLog message as action

To define the SysLog message as an action:

1. Select **Manage actions** from the **Tools and options** tab on the ribbon.
2. In the Action Definition Wizard window, enter the action name and select **Send SysLog message**.
3. Fill out the **Address** and **Server port** fields and the Syslog message to be sent.




Related topics

 [Alerting](#)

 [Actions](#) ⁶⁰⁴

SysLog message as event

To define the **SysLog message** event:

1. Select **Manage events** from the **Tools and options** tab on the ribbon.
2. Enter the event name and select the event type **Other / SysLog message**. Select **Next**.
3. In the Event definition wizard window, set the **SysLog keywords filter**. The event may consider **Any** Syslog messages or those matching to the keywords. If the second option is chosen,  **Add** keywords to be included in the defined event.

Related topics

 [Alerting](#)

 [Events](#) ⁵⁹³

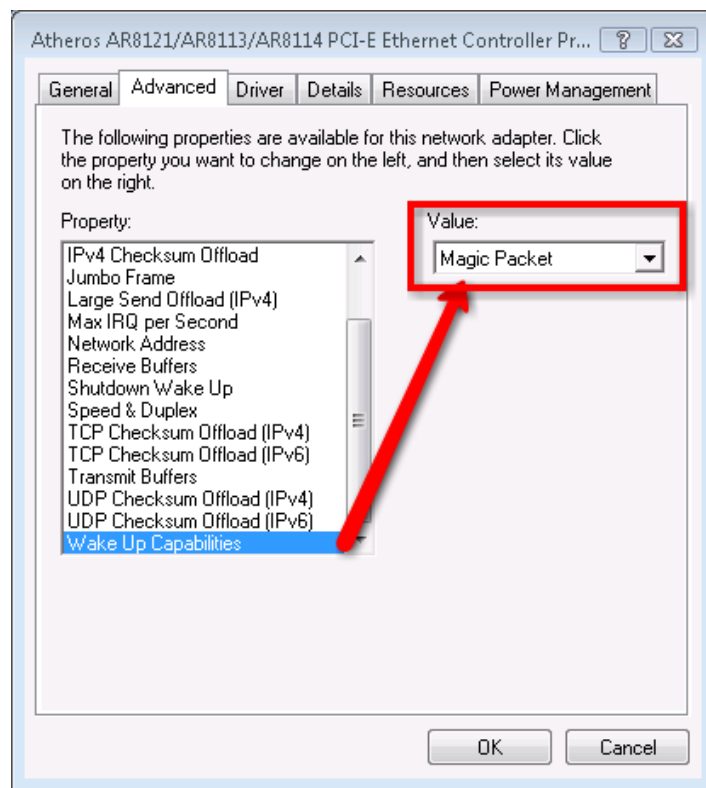
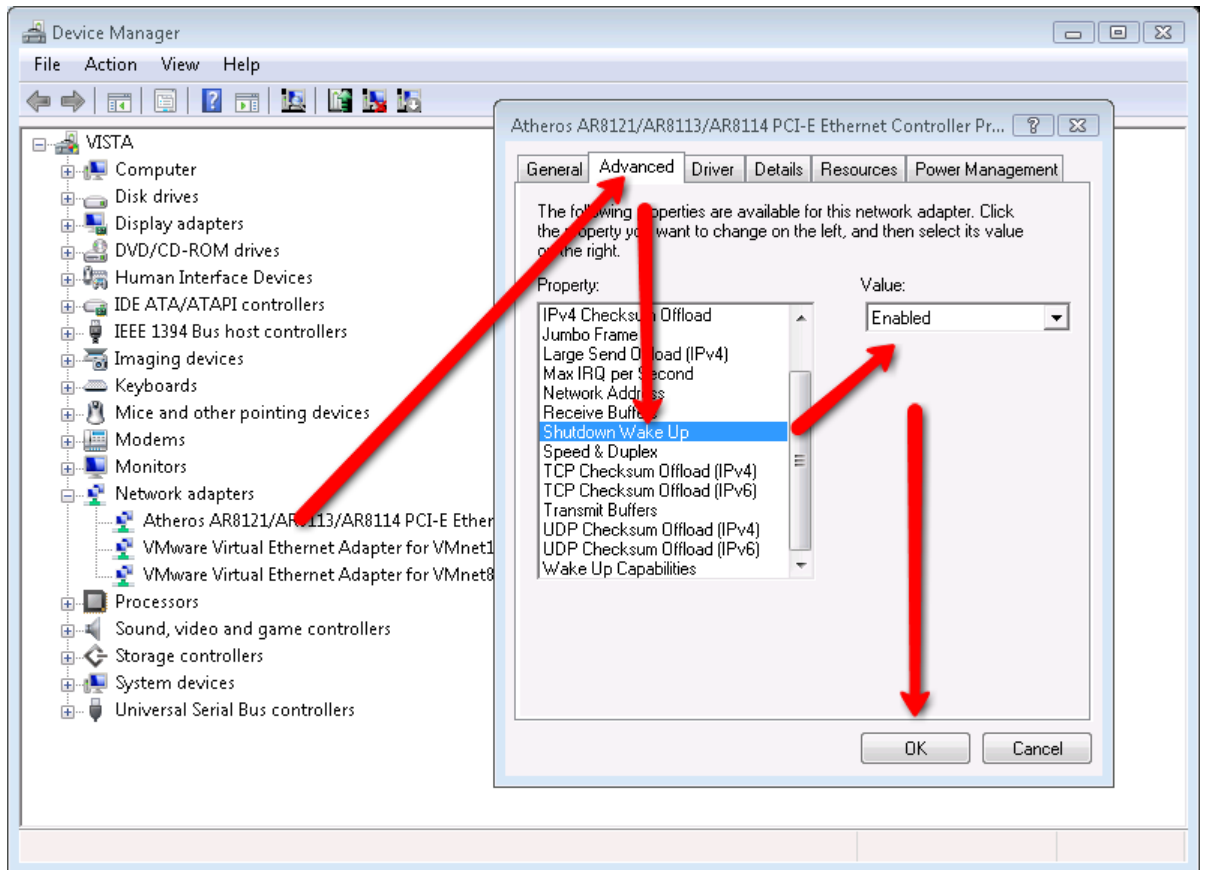
3.4.10 Wake On LAN

The Wake On LAN feature allows machines to be turned on remotely. It is available, if the MAC address of the machine to be turned on or woken up is known (in case of an error, the relevant message is displayed). Apart from this, the machine must be preconfigured (as described below) and, if the machine will be woken up from outside of LAN, port redirection must be set up in the router.

⊕ Configuration of the device to be woken up

The settings depend on a specific device. Examples of requirements and settings:

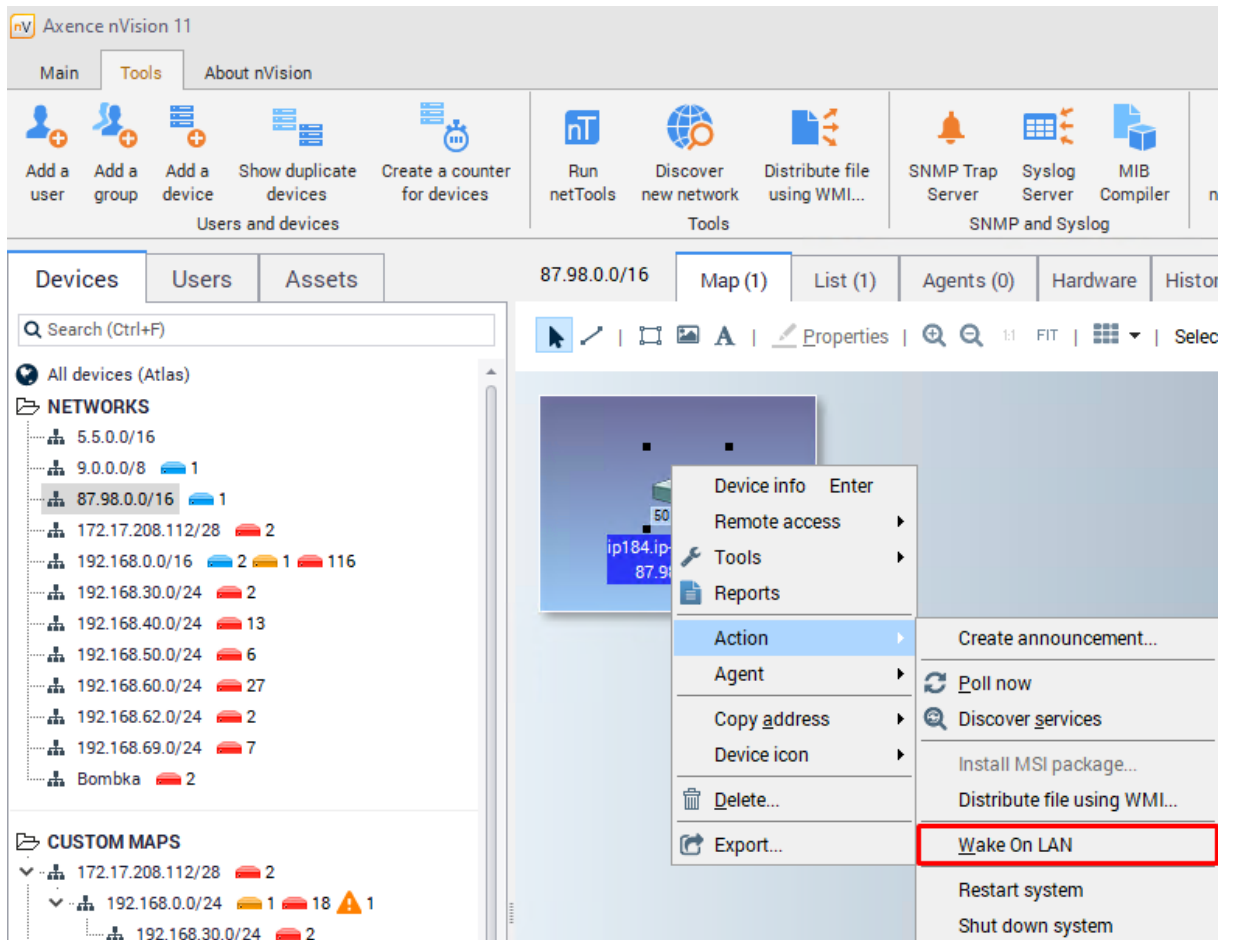
1. To enable Wake On LAN feature, an ATX power adapter, at least 1A, +5Vsb is necessary.
2. BIOS settings:
in Power (Management) or Advanced tab, enable Wake On LAN – the option can have different names, e.g. Wake On LAN, MAC Resume From S3/S4, MACPME Power Up Control, Power On By Onboard LAN, Power Up By Onboard LAN, Resume by LAN, Resume By WOL, Resume on LAN, Resume on LAN/PME#, Wake on LAN from S5, Wake Up On LAN, WakeUp by Onboard LAN or WOL (PME#) From Soft-Off.
3. Network adapter settings:
 - a. Navigate to the network adapter settings in Windows / Control Panel / Device Manager.
 - b. Set the options in the Energy Management tab to enable the waking up of the machine (option names depend on the network adapter, e.g. “Allow the device to wake the machine from sleep mode”).
 - c. Enable waking and Wake On LAN in the Advanced tab – option names can differ depending on the network adapter. Examples of settings are presented below:



⊕ Waking up of the device

To wake up the monitored device, perform one of the following steps:

1. In the map or device view in the main nVision window, right click the device and select **Wake On LAN**.



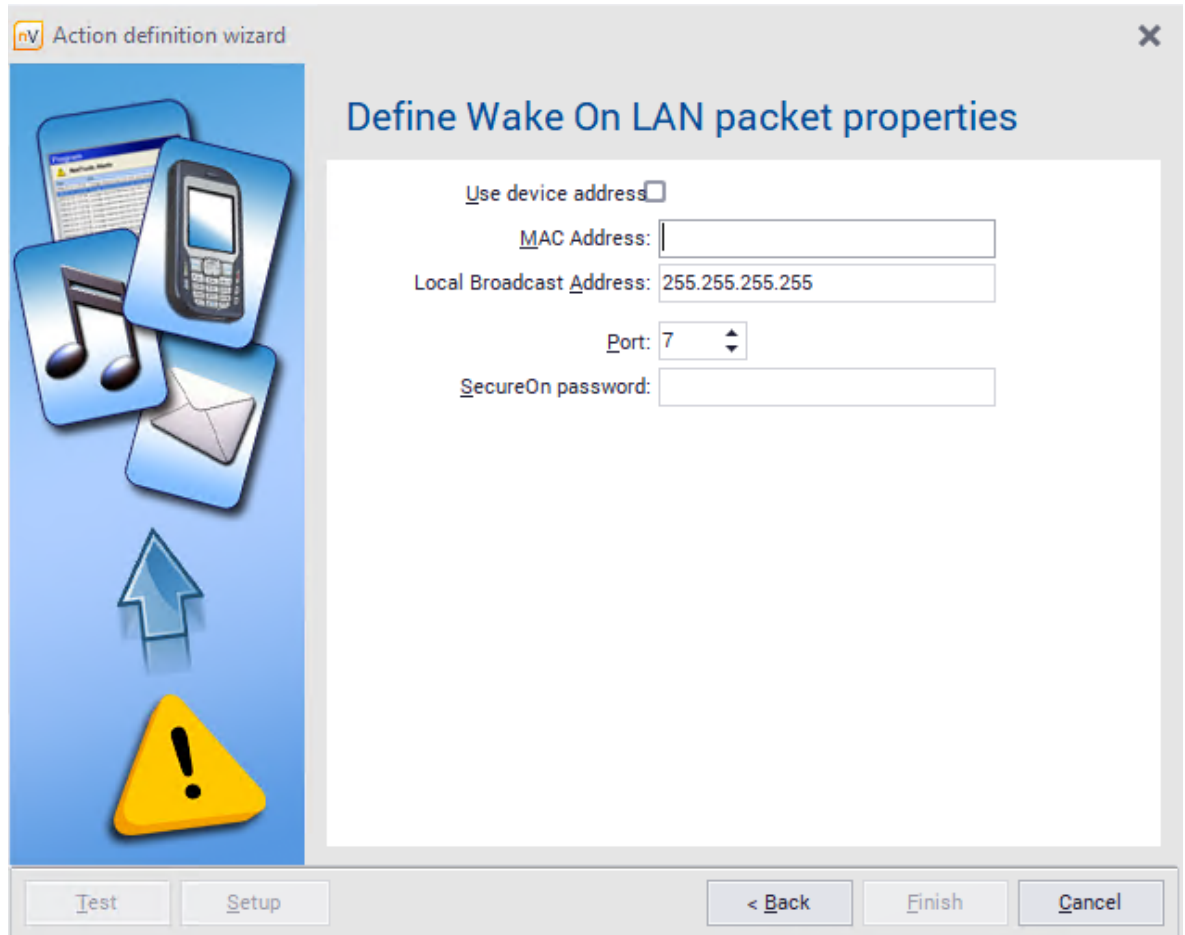
2. In the device info window, **General** tab, right click the interface where the packet should be sent to, and select **Wake On LAN**.

Wake On LAN as action

To define Wake On LAN as action:

1. Select **Manage actions** from the **Tools and options** tab on the ribbon.
2. In the Action Definition Wizard window, enter the action name and select the **Send Wake On LAN packet** type.
3. If you want to use the address of the host where the action is being defined, mark **Use host address** field and go to item 5. Otherwise, it is necessary to define the host (item 4).
4. Specify the MAC address of the device and one of the following target addresses for the Wake On LAN packet:
 - a. broadcast address: 255.255.255.255 (if the device is within the same LAN),
 - b. broadcast address of the subnet (if the device is in another LAN – e.g. 192.168.0.255 for subnet 192.168.0.1 with mask 255.255.255.0),

- c. IP address of the router configured for packet redirection (if the device is located outside of LAN).
5. It is not necessary to specify SecureOn password; however, some network adapters may require it. The password format is six bytes in hexadecimal notation: AA:BB:CC:DD:EE:FF.



The screenshot shows a software window titled "Action definition wizard" with a close button (X) in the top right corner. The main content area is titled "Define Wake On LAN packet properties". On the left side, there is a vertical blue bar containing several icons: a smartphone, a music note, an envelope, an upward-pointing arrow, and a yellow warning triangle with an exclamation mark. The main area contains the following fields and controls:

- Use device address
- MAC Address:
- Local Broadcast Address:
- Port: (with up/down arrow buttons)
- SecureOn password:

At the bottom of the window, there are four buttons: "Test", "Setup", "< Back", and "Finish", followed by a "Cancel" button.

Part

IV

4 Hosts, maps and ActiveDirectory sync.

4.1 Introduction

Atlas

The atlas is a set of maps holding monitored hosts along with defined alerts, events, visualization styles etc.

Atlas tree

The atlas tree lists all available maps. There are several map types, described in detail in the [Map types](#)^[90] topic. The atlas tree is designed to allow you to select the map, which is presented on the right side of the window, and set map properties, etc. You can change the order of maps in the tree (refer to the [Managing Maps](#)^[91] topic for more information).

Maps

The map is a graphical representation of your network or a part of it. It holds the hosts for visualization. There are several types of maps. For more information please refer to the [Map types](#)^[90] topic.

Styles

All map objects (except text) use the style mechanism. Style determines how the object is presented. For example it defines colors, fonts, frames, etc. To change the object appearance you have to select its style while defining object properties. For more information about styles, refer to [Styles](#)^[101] and [Maps](#)^[90] topics.

Hosts

A host is a representation of any physical device present in your network. It can have several IPs and nVision can monitor all services running on this host on any of its addresses. It means that multi-IP hosts like routers or web servers can be represented in nVision as one icon (object) and all of its interfaces, addresses and services will be monitored.

4.2 Host info window

To see host info, double-click the host icon or select **Host info** from its context menu.

General

The tab presents:

- basic information about the host being monitored: host name, importance, department, type,
- the **Monitor if this host is up**: field allows setting the “parent” host (a host will not be monitored and alerts will not be raised if the “parent” host is down),
- additional information in **info 1 / info 2** fields: downloaded by the Agent from the description of the machine and domain being monitored,
- additional fields for notes,
- list of all addresses and interfaces available on a given machine.

Performance

Services

nVision can monitor ICMP, TCP and UDP services. You can see all monitored services listed in the grid available in the Services tab. The information about response time and requests sent/received is presented for each service. After you select one or more services, you will see the chart showing response time and % of requests/packets lost (only if one service is selected). You can see historical data in several time periods (e.g. the last 15 minutes, 1 hour, 1 day, 1 week, 1 month and a whole year). To select the appropriate period, just select the corresponding icon on the chart toolbar. To scroll the chart backward and forward, use the arrow icons located on the chart toolbar. For more information about services refer to the [Monitoring services](#)^[57] chapter.

Performance counters

nVision can monitor several types of performance counters (for the complete list of available counters refer to the [Counter types](#)^[62] topic). You can see all monitored counters listed in the grid available in the **Performance counters** tab. The information about last and minimum/maximum/average value is presented for each counter (except the Host status counter which does not have min/max/avg values). After you select a counter, you will see the chart showing its value. You can see historical data in several time periods (e.g. the last 15 minutes, 1 hour, 1 day, 1 week, 1 month and a whole year). To scroll the chart backward and forward, use the arrow icons located on the chart toolbar. For information about counters refer to the [Monitoring performance](#)^[61] chapter.

Bandwidth usage

This tab shows the bandwidth usage by processes that are grouped according to the settings in the nVision's [options](#)^[42]. To monitor the bandwidth usage, it is necessary to install an Agent and enable this option in the [Agent settings](#)^[125].

Inventory

Hardware

This tab contains the information about hardware configuration of the machine monitored by the Agent, a list of connected devices and the [history of connections and file operations](#)^[339] on external data media.

Software

This tab shows a list of all applications installed on computers. For more information, see the Hardware and software inventory topic.

Fixed assets

This tab shows a list of assets for a given host. It also allows detected events to be managed. For more information, see the Fixed assets topic.

User files

Shows a list of files in the specified format scanned by the Agent according to the settings in the [Agent profile](#)^[125].

File manager

Allows data to be transferred between the local computer (nVision server) and the workstation being managed.

History

This tab shows the history of changes in hardware configuration and programs installed on the host. It also displays the information about IP address from which the Agent has connected to the nVision server. If this is a public address, you can double-click the row to open a new browser window with the web page that presents the estimated address geolocation.

SNMP

SNMP browser

If the host is SNMP manageable, you will see a SNMP tab with a SNMP browser. In order for the data to be read, configure the SNMP community data after clicking the **Configure credentials** link on this tab.

Port mapper

The port mapper tab shows a list of all devices connected to the switch port. It is available only when nVision is able to read the [appropriate SNMP information](#)^[68] from the host (which is available mostly on switches).

SNMP traps

The SNMP Traps tab presents the list of all generated [SNMP traps](#)^[71].

Windows

System information

Information about the operating system collected in the Inventory module.

Windows services

Shows a list of Windows services [monitored on a given host](#)^[61].

In order to monitor by WMI, you have to properly configure credentials in the host properties window. Also WMI has to be enabled on the remote host. Please refer to [Requirements and configuration](#)^[27] topic for more information.

To monitor Windows services without opening remote access to WMI, [install Agents](#)^[115].

Windows event log

Shows a list of events saved in the Windows Log, monitored according to the specific criteria on a given host.

In order to monitor by WMI, you have to properly configure credentials in the host properties window. Also WMI has to be enabled on the remote host. For more information refer to the [Requirements and configuration](#)^[27] topic. To monitor Windows services without opening remote access to WMI, install Agents.

Processes

Shows a list of processes currently running on a given host.

Remote commands execution

Allows a command line to be run remotely on the host. This function can apply to several machines at the same time.

Events

Event log

This is a list of all raised alerts on the host along with the action execution log for every alert. You can view alerts sorted by several fields and also filter them to see only alerts that are interesting to you. Click the **Configure device alerts** link to create individual [alerts](#)^[588].

Syslog

The Syslog tab presents the list of all generated [Syslog messages](#)^[74].

4.3 Global Browser

Searching for a specific piece of information from a number of datasets, e.g. Users, Resources, Maps, Devices, Documents, etc., has been quite onerous so far, since to find an object you should first have accessed a window with the relevant list and then filtered it. This inconvenience has been eliminated by the introduction of the **global browser** which is used to search multiple datasets in one place. This global browser is located at the top of the console, above the menu bar. The global browser is always available in the main window of the nVision console and its display is not affected by the currently viewed bookmark.

To use the global browser:

1. Click in the search box and enter the keywords/property names to be searched (the search starts with at least 3 characters in the search box).
2. Double-click the object that appears in the list and you will be taken to the appropriate tab. For instance, when you click the user's name, the account window for this user appears.

The screenshot shows the Axence nVision 13 interface. The top navigation bar includes "Main", "Tools", and "About nVision". The "Global search (Ctrl+G)" button is highlighted with a red box. Below the navigation bar, there are several tool icons for "Generate protocol", "MSI packages manager", "Print bar codes", "Asset settings", "Inventory", "Management", "Configuration", "Reports and alerts", "Alerts", "Distribution tasks", "Announcements", "Open HelpDesk", "Open SmartTime", "Open AdminCenter", and "Options". The main content area is divided into "Devices", "Users", and "Assets" sections. The "Devices" section is active, showing a search bar with "Search (Ctrl+F)" and a list of devices. A red box highlights the search bar. The device list table has columns for Status, Type, Name, Info, IP, DNS, Address, Services, Agent, Interfaces, Services response time (ms), Total requests/packets, and Alerts. The table contains multiple rows of device data, including IP phones from various vendors like Linksys and Cisco. At the bottom, there is an "Event Log" section and system status indicators: "Devices: 226 (83 OK, 16 Warning, 105 Down)", "Services: 644 (283 OK, 335 Down)", and "Alerts: 1 (Device with alerts: 1)".

This screenshot is similar to the one above, showing the same Axence nVision 13 interface. In this view, the search bar in the "Devices" section is highlighted with a red box and contains the text "Enter at least 3 characters...". The rest of the interface, including the navigation bar, tool icons, and the main table of device details, is identical to the previous screenshot. The system status at the bottom remains the same: "Devices: 226 (84 OK, 15 Warning, 105 Down)", "Services: 644 (283 OK, 335 Down)", and "Alerts: 1 (Device with alerts: 1)".

The screenshot shows the Avicene nVision 13 interface. A red box highlights the 'User Administrator Bob' profile in the top-left navigation pane. The main area displays a table of network devices with columns for IP, DNS, Address, Services, Agent, Interfaces, Services response time (ms), and Alerts. The table lists various devices like IP Phones and Network Devices with their respective configurations and status.

| IP | DNS | Address | Services | Agent | Interfaces | Services response time (ms) | Total requests/packets | Alerts |
|---------------|-----------------|---------|--------------|-------|------------|-----------------------------|------------------------|---------------|
| 192.168.111.1 | labortis.v... | | [P10] [HTTP] | | 1 | | 28.02.2020 15:5... | Today, 08:... |
| 192.168.111.1 | adipiscing... | | [P10] [HTTP] | | 1 | | 28.02.2020 15:5... | Today, 08:... |
| 192.168.111.1 | curae.felis... | | [P10] [HTTP] | | 1 | | 28.02.2020 15:5... | Today, 08:... |
| 192.168.111.1 | mettiam... | | [P10] [HTTP] | | 1 | | 29.02.2020 00:0... | Today, 08:... |
| 192.168.111.1 | commodo... | | [P10] [HTTP] | | 1 | | 10.22.2021 12:5... | Today, 08:... |
| 192.168.111.1 | metus.p... | | [P10] [HTTP] | | 1 | | 10.22.2021 12:5... | Today, 08:... |
| 192.168.111.1 | curae.hend... | | [P10] [HTTP] | | 1 | | 10.22.2021 11:3... | Today, 08:... |
| 192.168.111.1 | congue.pot... | | [HTTP] [P10] | | 1 | | 28.02.2020 15:5... | Today, 08:... |
| 192.168.111.1 | convallis.a... | | [HTTP] [P10] | | 1 | | 10.22.2021 12:5... | Today, 08:... |
| 192.168.111.1 | consectet... | | [HTTP] [P10] | | 1 | | 20.02.2020 11:3... | Today, 08:... |
| 192.168.111.1 | facilisi... | | [P10] [HTTP] | | 1 | | 28.02.2020 15:5... | Today, 08:... |
| 192.168.111.1 | tincidunt.tu... | | [P10] [HTTP] | | 1 | | 10.22.2021 12:5... | Today, 08:... |
| 192.168.111.1 | netus.aliqu... | | [P10] [HTTP] | | 1 | | 10.22.2021 12:5... | Today, 08:... |
| 192.168.111.1 | parturient... | | [P10] [HTTP] | | 1 | | 28.02.2020 20:2... | Today, 08:... |
| 192.168.111.1 | utrisque.tur... | | [P10] [HTTP] | | 1 | | 06.10.2021 12:5... | Today, 08:... |
| 192.168.111.1 | vivamus.a... | | [P10] [HTTP] | | 1 | | 29.02.2020 00:0... | Today, 08:... |
| 192.168.111.1 | gravitate... | | [P10] [HTTP] | | 1 | | 28.02.2020 17:1... | Today, 08:... |
| 192.168.111.1 | accumsan... | | [P10] [HTTP] | | 1 | | 28.02.2020 17:1... | Today, 08:... |
| 192.168.111.1 | posuere.su... | | [P10] [HTTP] | | 1 | | 28.02.2020 15:5... | Today, 08:... |
| 192.168.111.1 | sociosqu... | | [P10] [HTTP] | | 1 | | Today, 10:22:38 | Today, 08:... |
| 192.168.111.1 | fames.sod... | | [P10] [HTTP] | | 1 | | 05.06.2019 07:2... | Today, 08:... |
| 192.168.111.1 | habitate... | | [HTTP] [P10] | | 1 | | 28.02.2020 17:1... | Today, 08:... |
| 192.168.111.1 | lectus.sen... | | [HTTP] [P10] | | 1 | | 29.02.2020 00:0... | Today, 08:... |
| 192.168.111.1 | molestie.q... | | [HTTP] [P10] | | 1 | | 28.02.2020 17:1... | Today, 08:... |
| 192.168.111.1 | luctus.pun... | | [HTTP] [P10] | | 1 | | 10.22.2021 12:5... | Today, 08:... |
| 192.168.111.1 | fames.vita... | | [HTTP] [P10] | | 1 | | 29.02.2020 00:0... | Today, 08:... |
| 192.168.111.1 | maecenas... | | [HTTP] [P10] | | 1 | | Today, 10:22:41 | Today, 08:... |
| 192.168.111.1 | suspendis... | | [HTTP] [P10] | | 1 | | 28.02.2020 17:1... | Today, 08:... |
| 192.168.111.1 | parturient... | | [P10] [HTTP] | | 1 | | 28.02.2020 15:5... | Today, 08:... |

The screenshot shows the user profile page for 'ADMINISTRATOR BOB' in Avicene nVision 13. The page is divided into several sections: GENERAL, USER INFO AND STATUS, ROLE AND PERMISSIONS, and ACTIVITY PREVIEW. The USER INFO AND STATUS section contains fields for User name (bob), Full name (Administrator Bob), E-mail address, Account enabled (checked), Password (Change), Created (02.05.2022 10:22:00), Last login, and Phones. The ROLE AND PERMISSIONS section shows the role as Administrator and the application as nVision. The ACTIVITY PREVIEW section shows the account type (nVision), supervisor (n/a), and direct reports (n/a). The bottom section shows a list of documents with columns for Date, Name, Type, File name, Extension, File size, and Description.

Global browser rules

The global browser works according to the following rules:

1. Search results are not case-sensitive.
2. The global browser ignores Polish characters (a, c, e, l, n, ó, s, z, z); for instance, if you want to search for a user named Maczynski, you can enter both "Maczynski" and "Maczynski" in the global browser. The search result will be the same.
3. The global browser also finds the search item when the string entered in the search box occurs in some of the items being searched; for instance, when you type "Print", the list of search results may include "Printer".

4. The global browser does not recognize any special characters such as a space, an asterisk (*), quotation marks (""), or a question mark (?). Any non-alphanumeric characters are considered as part of the search term by the global browser.

List of objects to search for

| Search item | Searched properties / keywords |
|---|--|
| Document | document name file name description |
| Group, smart group | name |
| Hierarchy | element name |
| Map (network) | map name network IP address |
| Department, user map, smart map, OU (Organizational Unit) from Active Directory | name |
| Resource type | name |
| Document type | name |
| (Device) host | device name DNS name IP address MAC address |
| User | user name full name e-mail address position phone number local account name (shown in the Related Accounts section) |
| Resource | name serial number inventory number "location" field |
| Software audit, Applications, Licenses | element name |
| Generate protocol | element name |

| | |
|---|---|
| MSI package manager | |
| Print barcodes | |
| Resource settings | |
| Application categories | |
| Manage templates | |
| Configure license type | |
| DataGuard audit | |
| Connected devices | |
| Manage devices | |
| Manage trustees | |
| Printout audit | |
| Configure printing costs | |
| Reports | |
| Event log | |
| Alerts | |
| Distribution tasks | |
| Messages | |
| Open HelpDesk | |
| Open SmartTime | |
| Open AdminCenter | |
| Options | |
| Show duplicated devices | |
| SNMP trap server | |
| Syslog server | |
| MIB compiler | |
| Filters for smart maps | |
| Filters for smart groups | |
| Manage events | |
| Manage actions | |
| Manage styles | |
| Manage tools | |
| Manage accounts | |
| Manage departments | |
| Options - Setting up services | phrase "Options - " + bookmark name |
| Options - Maintenance | |
| Options - Blockade messages | |
| Options - HelpDesk | |
| Resource settings - Resource types | phrase "Resource settings - " + bookmark name |
| Resource settings - Resource type folders | |

| | |
|--|--|
| Resource settings - Resource statuses | |
| Resource settings - Resource detection | |
| Resource settings - Global fields | |
| Resource settings - Action templates | |
| Resource settings - Data sources | |
| Resource settings - Document types | |
| Resource settings - Protocol settings | |

4.4 Maps

4.4.1 Overview

The map is a graphical representation of your network or a part of it. The map can contain icons, links between them and three types of static objects available for your convenience: shape, picture and text. The full list of map objects is described in the [Map objects](#)^[97] topic.

There are three map types: network, routing and custom - described in the [Map types](#)^[90] topic.

Styles

All map objects (except text) use the style mechanism. Style determines how the object is presented. For example it defines colors, fonts, frames, etc. To change the object appearance you have to select its style while defining object properties.

All new objects are created with default style. Default style means that the object will use the default map style. The default map style can be set to any specific style or to atlas default style. Atlas always has a default style selected. When you start the program for the first time, all objects will use those atlas default styles. You can adjust styles later. To read more about styles, refer to the [Managing styles](#)^[104] topic.

4.4.2 Map types

There are three map types in nVision. This topic describes each of them and discusses their characteristics.

| Map type | Description | Allowed operations |
|----------|---|--|
| Network | The map created by the program as a representation of the discovered IP network. nVision can periodically rescan such network and add new hosts. | <ul style="list-style-type: none"> Renaming is allowed, but even when renamed, the map still represents the same network. |

| Map type | Description | Allowed operations |
|--|---|---|
| | | <ul style="list-style-type: none"> Delete – when the network map is deleted it also deletes all hosts belonging to this network. All other operations are allowed without limitations. |
| Custom | This is map created by the user. It can consist of any hosts copied or moved from any other map. | <ul style="list-style-type: none"> All operations are allowed without limitations. |
| Smart map ^[107] | A smart map groups devices, which meet the specified conditions at a given moment. Smart maps are based on user-defined filters – the map is generated dynamically . | <ul style="list-style-type: none"> You can change the map name, but even after such a change the map shows the same network. You cannot remove or arrange device icons. What happens at each stage? |

4.4.3 Map objects

The map can contain icons, links between them and three types of static objects available for your convenience: shape, picture and text. Here is a full list of map objects:

| Map objects | Description |
|-------------|---|
| Icons | Hosts are represented by icons. The icon represents the status of the host - refer to the topic Host visualization ^[99] for more information about host visualization. |
| Link | Icons can be linked together to show logical or physical connections between hosts. |
| Shape | Background object used to group icons. |
| Picture | Similar to the shape, but a specific image file is used as content. |
| Text | Text which you can place anywhere on the map. |

Object precedence

Objects on the map have a precedence. It means that some objects are always painted over others. For example, icons are always painted over any other object type. However, you can change the precedence of objects of one type. You can bring objects to the front or send them to the back which changes the way the overlapping objects are painted.

4.4.4 Managing maps

This topic discusses all aspects related to managing maps.

Creating new map

1. In the Atlas tree, select the map or folder under which you want to create a new map. You can select Custom group.

2. Select **New / Map** from the context menu.

Note

- New maps can be created only in the Custom maps group.

Editing map properties

1. Select the map.
2. Select **Properties** from the context menu.
3. Set map properties according to the description in the table below.
4. You can also open the alert management window for this map - just click on the link under the **Alerting policy** label available at the bottom of the window.

| Property | Description |
|----------|---|
| Name | Map name |
| Network | This is the network which is visualized by the network map (look at Map types ^[90] topic to see what is network map). This is a read-only field. |

Default map styles – determine how maps and hosts will be visualized. Refer to the [Styles](#)^[101] topic for more information about styles.

| | |
|--------------------|-----------------------------------|
| Host visualization | Default icon visualization style. |
| Shape style | Default shape style. |
| Line style | Default line style. |

Removing the map

1. Select the map.
2. Select **Remove** from the context menu.

4.4.5 Working with maps


This topic describes all tools required to work with a map.

Tools

The tools are available on the map toolbar located usually at the left side of the map window (the map toolbar may be moved to any map edge). The tools allow you to select objects on the map, link icons and create background objects like shapes, pictures and texts.


Tool – selection

Selection is the default tool. It allows you to select objects on a map, drag them, arrange them and perform specific actions like opening the host status window or properties window.

To use the selection tool, click the  icon in the map toolbar. This tool will be active until you select any other tool.


Tool – linking icons

The linking icons tool allows you to link icons together – i.e. draw graphical connections between host icons on the map.

1. To use the linking icons tool, click the  icon in the map toolbar. This tool will be active until you select any other tool.
2. To link two icons, just click them in succession, i.e.:
 - Click one of the icons you want to link. The link line will appear indicating that now you have to click the next icon to link.
 - Click the next icon. The link will be created between those two icons.
3. Now, you can repeat steps 2-3 to link another icon pair.


Tool – creating shapes

This tool allows creating different shapes on the map (background graphical objects – rectangles, ellipses, etc.).

1. Click the  tool icon in the map toolbar. This tool will be active until you create a shape. Then the active tool will change back to selection.
2. Click and hold the left mouse button in the place where you want to have the top-left corner of the shape and drag the cursor to the place where the bottom-right corner should be. Release the button.


Tool – creating pictures

This tool allows creating pictures on the map. After creating a picture, you have to set it up by selecting the graphics file to be shown.

1. Click the  tool icon in the map toolbar. This tool will be active until you create a picture. Then the active tool will change back to selection.
2. Click and hold the left mouse button in the place where you want to have the picture's top-left corner and drag the cursor to the place where bottom-right corner should be. Release the button.
3. The picture properties window will show. You have to select the image file now and [set options](#)^[96] to properly create the picture.

Tool – creating texts


This tool allows creating texts on the map. After creating a text, you have to set it up by selecting the font and entering the text to be shown.

1. Click the  tool icon in the map toolbar. This tool will be active until you create a text. Then the active tool will change back to selection.
2. Click the place where you want to have the text.

3. The text properties window will show. You have to enter the text now and [set options](#)^[96] to properly create the text.

Tool - Grid aligning icons

This tool allows you to precisely arrange icons on the network map, as well as align icons on the network map according to the grid. To align icons on the network map:

1. Click on the  icon on the map toolbar.
2. In the window that opens, click the **Yes** button.

The icons on the network map will be aligned to the closest waypoint on the grid. It will also display a grid on the map (dots representing grid landmarks).

To disable the display of the grid, click the above icon again.

Working with map objects

Copying objects to other map

1. Select the object or objects.
2. Select **Copy To...** from the context menu.
The map selection window will open.
3. Select the map to which the selected object(s) will be copied.

Deleting objects

1. Select the object or objects.
2. Select **Delete** from the context menu.

Changing the order of objects (bring to front / send back)

You can change the order of objects of the same type – the way they are painted and how they overlap. The precedence of different type objects is fixed (refer to the [Map objects](#)^[97] topic for more information).

- To show the object above any other object, select **Position / Bring to front** from the object context menu.
- To put the object under all other objects, select **Position / Send back** from the object context menu.


Other operations

Automatic map arrangement

There are two ways to arrange your map automatically: using the map arrangement function and using the map layout assistant.

Arrange all


This function is best for a network or custom map, especially if hosts are not linked together. It just places icons in several rows.

1. Click the  icon located in the map toolbar and select **Arrange all** from the menu.
2. Select how you would like to arrange the map and click OK.

By selecting **Connections from port mapper** option, the icons will be linked automatically with switches they are connected with (in order to enable this function, the [monitoring switch ports](#)^[68] must be enabled at switch icon's properties).

Arrange linked hosts


To arrange a routing map (or any other map where all hosts are linked) properly, the icons may not be just placed in rows since such arrangement will produce unreadable map with all icon links crossing each other. Thus, you need to use the Arrange linked hosts option, which will arrange the whole map to avoid crossings and make the whole map readable as much as possible.

1. Click the arrow at the  icon located in the map toolbar and select **Arrange linked hosts** from the menu.
2. The option will be turned on and arranging the map will begin. You can interact with the arrangement process to adjust it to your needs. You can move icons and add/remove links between them.


Zoom – changing a map scale

You can adjust the scale in which the map is presented. The default scale is 100% and you can set this scale anytime by the clicking 1:1 icon.

Zoom in

To enlarge the map, click the  icon.

Zoom out

To reduce the map, click the  icon.

Zoom to fit

To have the map scale adjusted automatically so it adapts to the map size, click the **FIT** icon. nVision will try to show the whole map at the biggest possible scale.

Locking the map

If the map arrangement is finished and you want to make sure that something will not be changed by mistake, you can lock the map by clicking the **Edit map** switch in the upper right corner of the window. Objects cannot be moved or resized on the locked map, but you can still edit host properties.

4.4.6 Static map objects – properties

This topic discusses modifying static map object properties. For more information about map objects refer to the [Map objects](#)^[91] topic and for the information about creating objects refer to Working with the map topic.

Link

Icons can be linked together to show logical or physical connections between hosts.

1. Double-click the link or select **Properties** from its context menu.
2. Set the properties according to the description in the table below.

| Property | Description |
|----------|--|
| Caption | The caption to be shown over the link line. |
| Style | The style with which the link will be painted. Refer to Styles ^[101] topic for more information about styles. |

Shape

Background object used to group icons.


1. Double-click the shape or select **Properties** from its context menu.
2. Set the properties according to the description in the table below.

| Property | Description |
|----------|---|
| Text | The text to be shown on the shape. |
| Style | The style with which the shape will be painted. Refer to Styles ^[101] topic for more information about styles. |

Picture

Similar to the shape, but a specific image file is used as content.

1. Double-click the picture or select **Properties** from its context menu.
2. Set the properties according to the description in the table below.

| Property | Description |
|-----------|--|
| File name | The image file name. Enter it or select by clicking the  icon. |
| Show | Determines the way the picture is sized: <ul style="list-style-type: none"> • Normal – no image sizing, but when you try to down-size it, only a part of the image will be shown (if the image is bigger than the picture size it will be clipped). • Stretch – the image will be sized to match the size of the picture object. |

| Property | Description |
|-------------------|--|
| | <ul style="list-style-type: none"> • Tile – the image will be tiled to fill the picture object rectangle. |
| Actual size (1:1) | Image fully shown with no sizing available. |
| Keep aspect ratio | When sizing, keep image aspect ratio (proportions) unchanged. |
| Transparent | If the image has any transparency layer - use it. |
| Opacity | Sets the opacity of the image. |

Text


Text which you can place anywhere on the map.

1. Double-click the text or select **Properties** from its context menu.
2. Set the properties according to the description in the table below.

| Property | Description |
|------------|----------------------|
| Text | The text on the map. |
| Font name | Font of the text. |
| Size | Font size. |
| Font color | Color of the text. |
| Angle | Angle of the text. |
| Shadow | The text shadow. |

Background

1. Select **Background** from the map context menu.
2. Select the background type and set its properties according to the description in the table below.

| Property | Description |
|-------------|---|
| Gradient | Select beginning and ending colors and a direction of filling. |
| Solid color | Select a color. |
| Map | Select the map to be shown as a background. |
| Texture | Select the texture. |
| Picture | <p>Enter the image file name or select by clicking the  icon. Set the show mode:</p> <ul style="list-style-type: none"> • Normal – image shown in the top-left corner. • Center – image centered on the map. |

| Property | Description |
|----------|---|
| | <ul style="list-style-type: none">• Stretch – the image will be sized to match the size of the map.• Tile – the image will be tiled to fill the map. |

4.5 Hosts

4.5.1 Overview

Hosts are visualized on the maps as icons. The same host can be shown as an icon on an unlimited number of maps.

Host properties and info

There are two main windows related to the host: host properties and host info. You can setup the host properties, monitoring and alerting options with host properties window. The host info window presents all the information gathered by the monitor. You will see SNMP information (for SNMP manageable hosts), services and counters performance information, and charts.

Finding the device

You can easily find the device with the search engine located on the main toolbar in the right hand section of the main nVision window and in the **Device Information** window. A list of properties which are taken into account during searching can be found below:

- Name
- IP, DNS, and MAC addresses of each interface
- Info1 and Info2.

When you keep entering characters in the search box, the results that contain the entered string are filtered out.

To find a device where at least one of the above fields contains:

- a string ending with the entered characters – should finish with a | ,
e.g.:
54|
- a string starting with the entered characters – should be preceded with a | ,
e.g.:
|AABBCC
- the exactly the entered string – should start and finish with a | ,
e.g.:
|office-pc|.

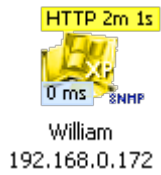
Important: DNS identification is turned on only if IP - DNS lookup gives the same result in both directions.

4.5.2 Host visualization


There is a wealth of information regarding the host status presented along with the host icon. That information helps to quickly check the whole network status and find problematic hosts.

Sample host icon

The host icon presents a wide range of information right on the map – displayed in these examples:



- Host type Windows XP
- Leading service (usually PING) response time is 10ms
- Host status <Warning> (yellow icon) because service HTTP has been down for 4min 1s
- This is SNMP manageable host



- Host type Linux server
- Host status <Down> (red icon) since 1 day 2h
- There are 3 currently open (unresolved) alerts.

Visualization options

The following table lists all possible information that can be presented graphically along with the host icon.

| Name | Description |
|--------------------------------------|--|
| Icon with a caption, host status: Up | The base form of the icon. It shows the type of the host and the name or address of the host in the caption. |
| Host status: Down | The icon is colorized in red and the duration of the down status is written at the top of the icon. For more information about host status refer to Events ^[593] topic. |
| Host status: Warning | The icon is colorized in yellow. It means that at least one service does not respond or a warning alert was raised on the host. For more information about host status refer to Events ^[593] topic. |
| Host status: Archived | The icon is greyed out. It means that the given device Agent data were archived. For more information, see Agent Archiving ^[118] chapter. |
| Non responding service(s) | The name of the problematic service with the duration of the problem is written on the icon. |
| Response time of selected service | Last or average response time of the selected service is placed at the bottom of the icon. Usually it shows the average PING response time. Its background changes its color according to the service performance. |

| Name | Description |
|--------------------|--|
| Alerts | This icon, located at the right side of the host icon, indicates non acknowledged alerts raised on the host. |
| SNMP manageability | This icon, located at the right side of the host icon, indicates that the host is SNMP manageable. |
| Performance chart | You can see up to 6 performance bars that show service response times or any counter. |

4.5.3 Managing hosts

This topic discusses various aspects of managing the host and its services.

+ Setting host properties

1. Select **Host info** from icon context menu.
2. Set host properties according to the description available in the [Host properties](#)^[82] topic.

+ Adding a host

1. Select **Add host** from the **Tools** tab on the ribbon.
2. Enter the host DNS name or IP address and the mask.
3. You can also setup host type and importance options.

+ Deleting a host icon

1. Select **Delete** from the icon context menu.
2. Confirm delete. When deleting the last host icon in the specific host, the whole host will be removed along with all its data. So you can safely remove icons from custom maps, even if icons of those same hosts are still located on other network maps.

+ Displaying host info window

1. Select **Host info** from the icon context menu or double-click the icon.
2. View the host info window – the description of the information presented in this window is located in the [Host info window](#)^[82] topic.
3. You can leave this window on the desktop and still work with the program. The information presented in the window will be automatically refreshed to reflect changes and the host status.
4. You can open an unlimited number of host info windows.

+ Managing host services & counters

+ Managing services

For information about services refer to the [Monitoring services](#)^[57] chapter.

+ Managing performance counters

For information about counters refer to the [Monitoring device and system performance](#)^[67] chapter.

4.6 Styles

4.6.1 Overview

Styles define the map visualization. This topic discusses default styles and setting styles for specific objects. To read about creating and editing styles, refer to the [Managing styles](#)^[104] topic.

Default styles

Atlas default styles

Atlas default styles are defined in the Atlas properties. Those styles define the default styles, which are used by all new and existing objects that have their style defined to <default> (however, the map holding those objects can override Atlas styles). When a map is created, its styles and styles of all objects it contains are set to <default>, thus the atlas styles will be applied. Of course, when you change Atlas default styles, it changes the appearance of such maps and objects.

To change the default Atlas styles, do it in the Atlas properties window.

Map default styles

A map has its own default styles, similar to the Atlas's. With those styles you can override global styles to more specific ones. You can also use <default> as the map default style. Then the style defined in the Atlas properties will be used.

The <default> style in that case means that the map is using the style defined in the Atlas properties. You can consider it as a reference to the Atlas style. Therefore, the <default> style cannot be edited or deleted, because it is only a reference.

Map object styles

Host visualization style

With host visualization style you define how the host is presented on the map. You can decide which information is displayed along with the icon: down time, information about non-responding services, last response time, SNMP and alert indicators, etc.

Shape style

Shape style fully defines the appearance of the shape (background map object): frame, colors, etc.

Link style

Link style defines graphical properties of links between icons.




4.6.2 Defining styles

This topic describes the properties of different style types. For information about creating, editing and removing styles, refer to the [Managing styles](#)^[104] topic.

Host visualization style

With host visualization style you define how the host is presented on the map. Here is the list of this style properties with the description.

| Property | Description |
|----------|--------------------|
| Name | Name of the style. |

| Property | Description |
|-------------------------------|---|
| When changing state blink for | The duration of icon blinking after a host status change. Blinking helps to easily locate the hosts that changed status. |
| Icon Caption | Defines the text of the icon caption. |
| Transparent caption | The icon caption will be transparent if this option is checked. |
| Host and services down time | If checked then in case of host down you will see the duration of down time. If the host is up, but some services are not responding, you will see the information about down services with the duration of down time. |
| Leading service response time | This property defines if the specific service last response time should be shown in the icon. |
| SNMP manageability | If the host is SNMP manageable the  icon will be shown at the bottom-right side. |
| Alert warning | If the host has unacknowledged alerts, the  icon along with the number of open alerts will be shown at the right side. |
| Agent installed | If the Agent is installed on the host, the  icon will be shown at the right side. |

Shape style

Shape style fully defines the appearance of the shape (background map object): frame, colors, etc.

| Property | Description |
|---------------------|--|
| Style name | Name of the style. |
| Shape type | Type of the shape. Currently there are 4 types available: rectangle, rounded rectangle, ellipse and star. |
| Font name | The font name of the shape caption. |
| Font color and size | Color and size of the caption font. |
| Background | <ul style="list-style-type: none"> Solid – shape background is painted with the selected color. Gradient – paints gradient background with the defined colors and direction. |
| Frame | <ul style="list-style-type: none"> Color – frame color. Size - width of the frame. |
| Opacity | Defines transparency of the shape. |
| Shadow | Defines the size of the shadow. |

Line style

Line style defines graphical properties of links between icons.

| Property | Description |
|----------------------|--|
| Style name | Name of the style. |
| Thickness | Width of the link line. |
| Color | Line color. |
| Type | <ul style="list-style-type: none"> • Simple – straight line. • Polyline – broken line. |
| Font name | Name of the font. |
| Font size and color | Size and color of the font. |
| Show caption on line | If marked, caption is shown on the line. |


4.6.3 Managing styles

All map objects (except text) use the style mechanism. Style determines how the object is presented. For example, it defines colors, fonts, frames, etc. To change the object appearance, you have to select its style while defining object properties.


+ Style management window

1. Select **Manage styles** from the **Tools** tab on the ribbon.
2. Select the style type to manage (i.e. host, shape or link) in the navigation bar located on the right side of the window.


+ Creating new style

1. Open the style management window.
2. Click the  icon.
3. Define the style according to the information available in the [Defining styles](#)^[101] topic.

+ Editing the style

1. Open the style management window.
2. Select the style to edit and click the  icon.
3. Change the style properties according to the information available in the [Defining styles](#)^[101] topic.

+ Removing styles

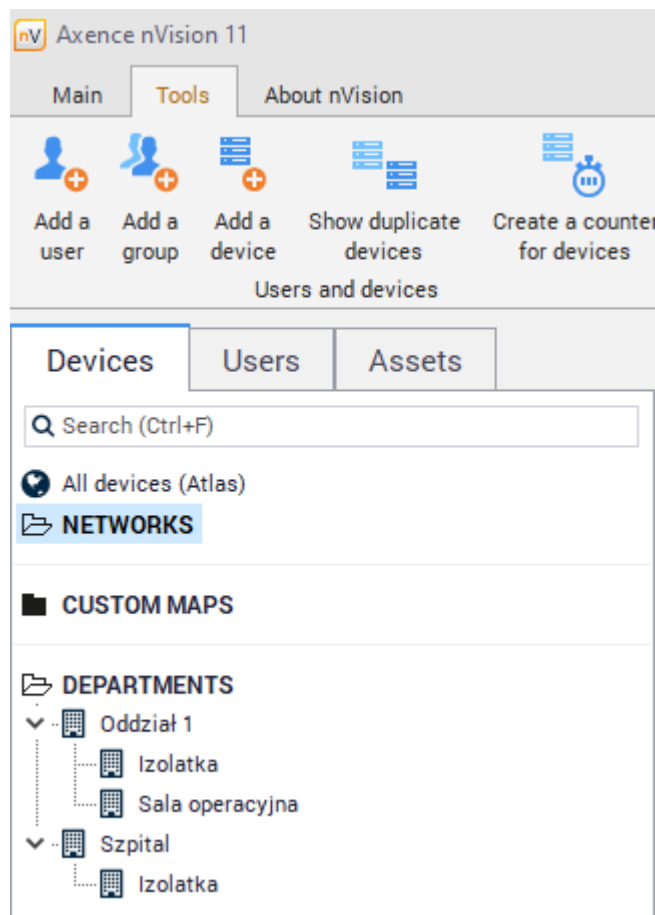
1. Open the style management window.
2. Select the style to edit and click the  icon.

4.7 Departments

4.7.1 Overview

Departments allow the reflection of the real structure of a monitored computer group in nVision. Therefore, it allows for easier browsing, management and the creation of reports related to selected devices.

The department list is displayed in the left part of the application window, below the networks and user maps. It has a hierarchical structure, which allows the relationship of the dependency of organizational units (parent/subsidiary department) to be represented. An example hierarchy is presented in the image below.



Related topics

[Creating a department structure](#) ¹⁰⁵

[Adding devices to departments](#)

[Reports](#) ¹⁰⁷

[SmartMaps](#) ¹⁰⁷


4.7.2 Creating a department structure

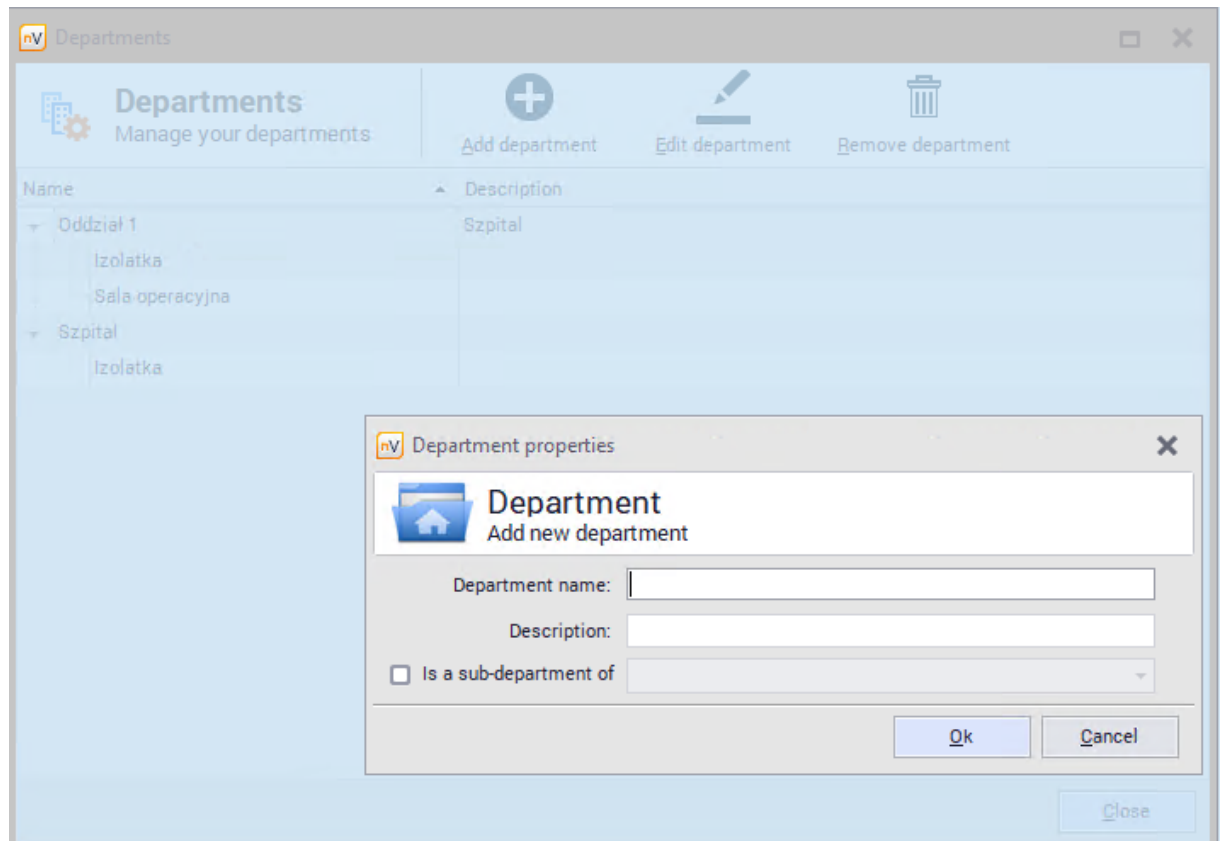
When creating the department hierarchy, start from the most general units and go towards the lowest sub-departments in the hierarchy. Branches enable to graphically determine the relationships only. In


terms of operation, they are “at the same level”. Such a procedure will facilitate the creation process, as it will not be necessary to go back to sub-department properties to supplement information.

To create a department structure:

Select the **Manage departments** option from the **Tools** tab. The department window will open, displaying all the departments defined for the atlas.

1. To create a new department, click the  **Add department** button. In the department property dialog, enter the name of the created department and an optional description. If it is a sub-department, mark an appropriate field and select a parent department.



2. Confirm the entered changes and the created department will appear in the list. Repeat the above procedure, until all departments are created.
3. If it is necessary to make corrections, click the  **Edit department** button.

4.7.3 Adding devices to departments

To put a device into a previously created department:

1. Navigate to the **Device info** window, **General** tab.
2. Expand the menu at the **Department** field and select a department from the list. Click **OK** and close the window.

4.7.4 Reports

It is possible to generate reports for selected departments. To create such a report, right click the department for which the report will be created, and select the **Reports** option. You can also select the specific departments directly in the report generation window.

To learn more about the report creation, see [Reports](#) ^[560] section.

4.8 SmartMaps

4.8.1 Overview

Smart maps differ from the traditional ones due to their dynamic operation. Smart maps include devices which meet the specified conditions at the given moment. It is possible to set the refresh frequency for the map and for the set of conditions (i.e. filter) to be checked.

The operation of smart maps is based on user-defined filters. To enable the proper operation of the smart map, associate it with an appropriate filter.

Related topics

 [Filters](#) ^[107]

 [Creating a filter](#)

 [Creating a SmartMap](#)

 [Departments](#) ^[105]

4.8.2 Filters

The following table presents the conditions, which can be used for filter creation:

| Group | Conditions |
|---------------------|---|
| Host properties | <ul style="list-style-type: none"> • Name • Info1/Info2 • Device type • Server / Router • Importance • Status |
| Monitoring services | <ul style="list-style-type: none"> • Service installed (e.g. SMTP) • Working/not working |
| Monitoring counters | <ul style="list-style-type: none"> • Counter installed (e.g. CPU) |
| Alerts | <ul style="list-style-type: none"> • Open alerts exist |
| Agents | <ul style="list-style-type: none"> • Agent installed • Agent working/not working • Agent version is outdated |

Departments

- Department name
- Device without assigned department

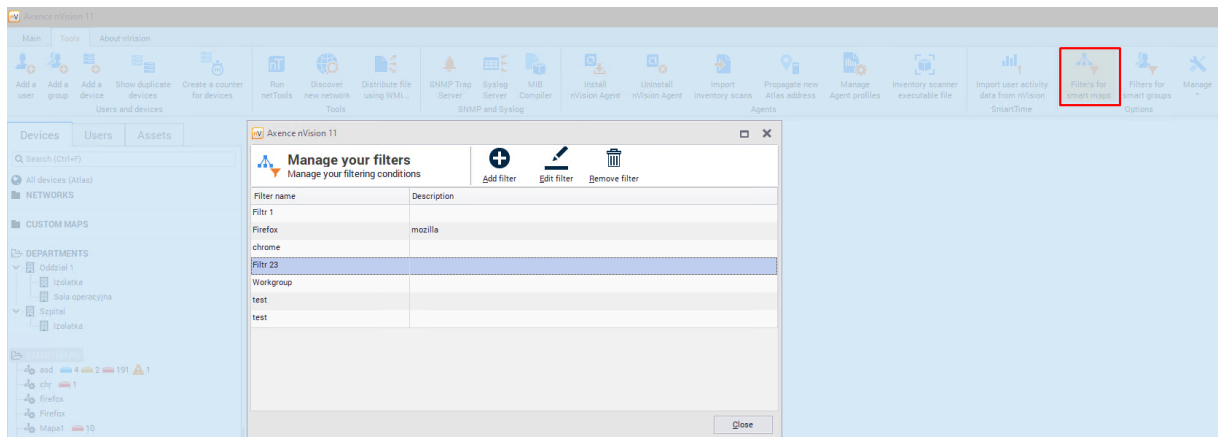
Software inventory

- Installed application exists
- The given application is not installed

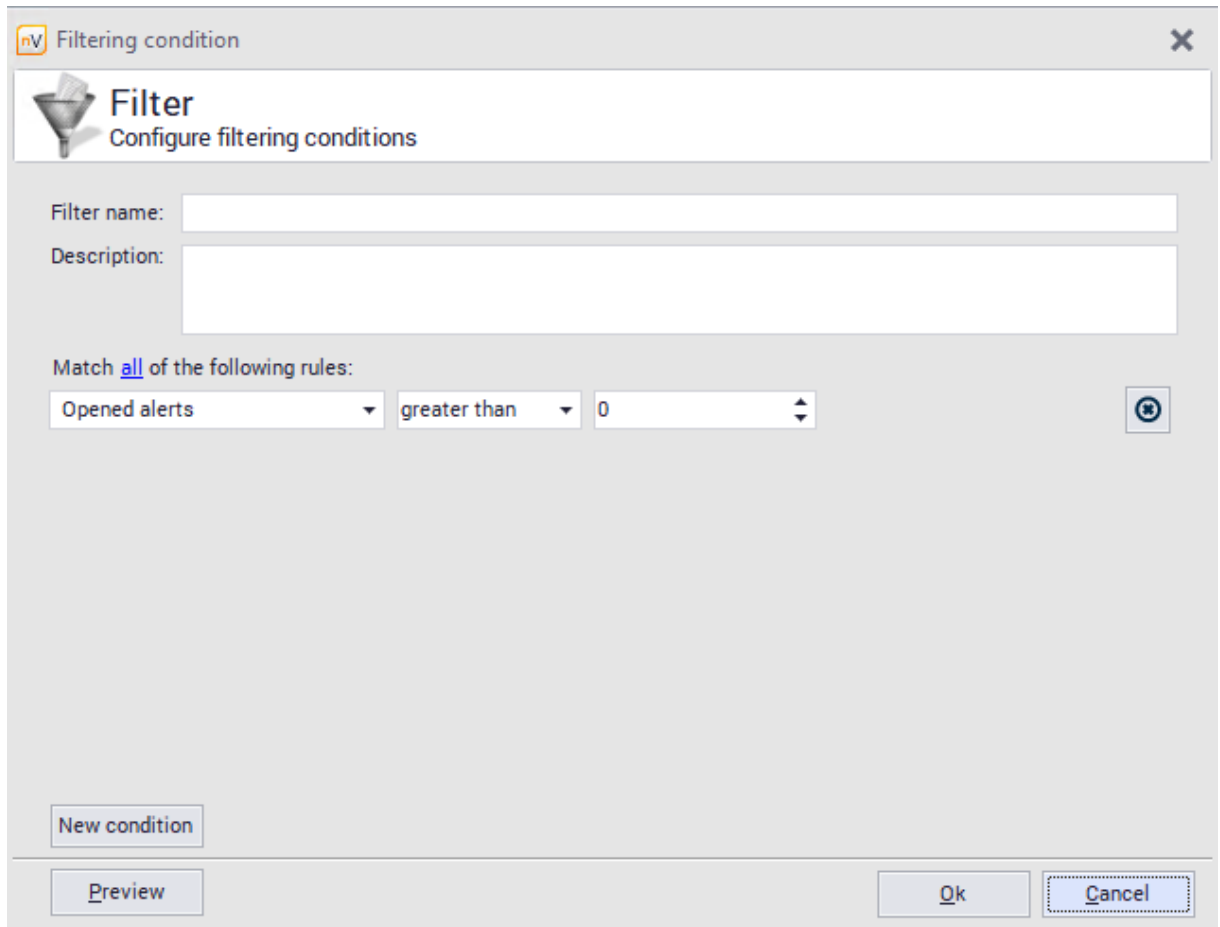
4.8.3 Creating a filter

To create a filter:

1. Select **Filters for smart maps** from the **Tools** page on the ribbon. In the Managing filters window, click the  **Add filter** button.



2. In the Filter conditions dialog, enter **Filter name** and **Description**. Then set the filter conditions. To add another condition, click the **New condition** button. To use an alternative instead of the sum of conditions, click the word all – to change it to at least one of. An example of a filter with conditions is presented in the image below.




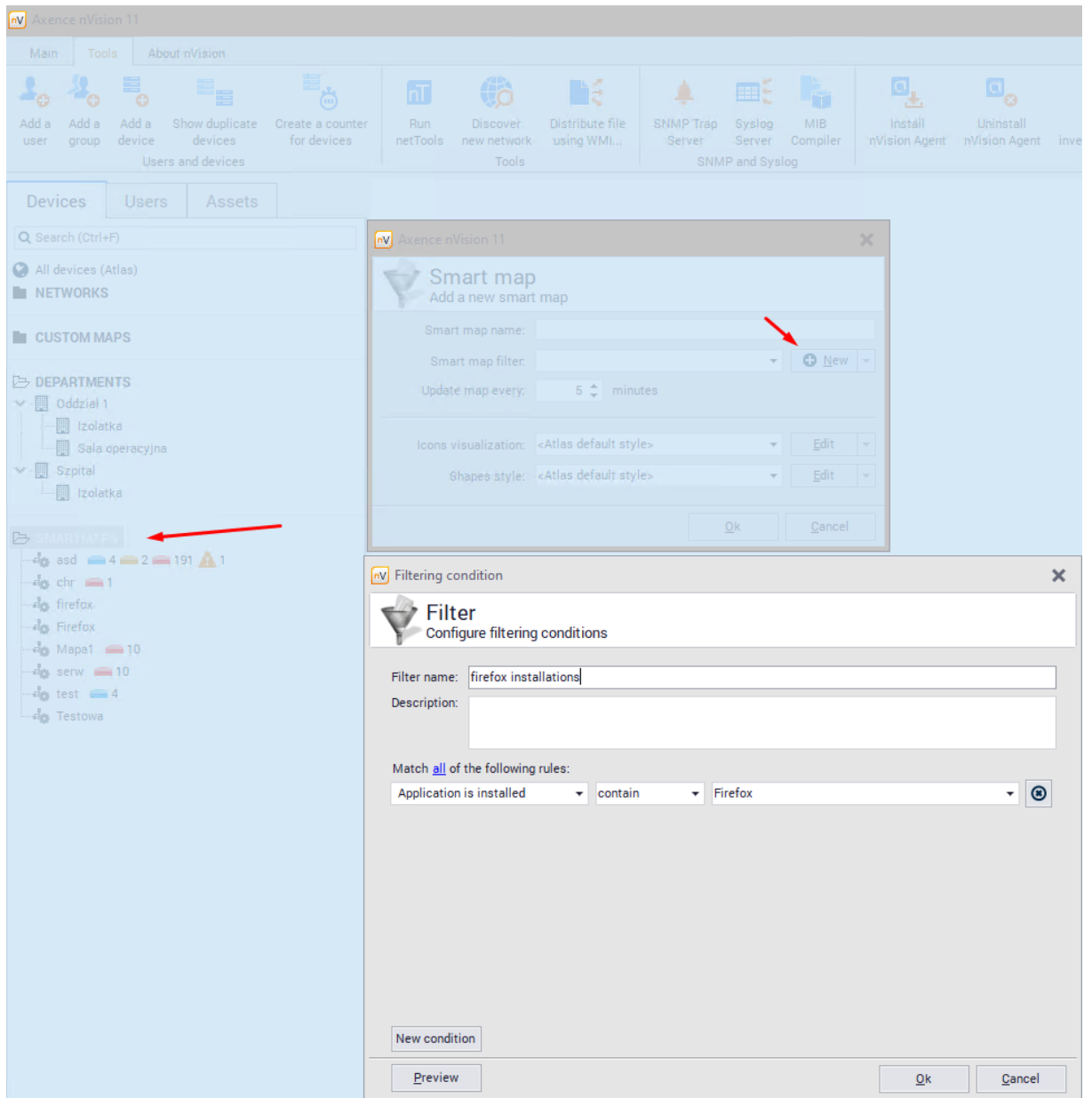
The screenshot shows a dialog box titled "Filtering condition" with a close button in the top right corner. The dialog contains a header with a funnel icon, the word "Filter", and the text "Configure filtering conditions". Below the header, there are two text input fields: "Filter name:" and "Description:". Underneath, there is a section "Match all of the following rules:" with a dropdown menu showing "Opened alerts", a "greater than" operator, and a numeric input field with "0". To the right of the rule is a plus icon button. At the bottom of the dialog, there are four buttons: "New condition", "Preview", "Ok", and "Cancel".

3. To view the list of devices meeting the defined conditions, click the **Preview** button. When the changes are accepted, the newly created filter will appear in the filter list.

4.8.4 Creating a SmartMap

To create a smart map:

1. Right click the **SmartMaps** in the list in the left part of the nVision window. Select the option **New / Smart map**.
2. In the smart map properties window, enter the **Name** and select a **Filter** from the list which will be associated with the created map. If such a filter has not been created yet, expand the menu at the **Edit** button, select the  **Create new** option and proceed according to the [Creating filter](#)¹⁰⁸ description.
3. Set the map refresh time and visualization styles. In the case of smart maps it is not possible to set the graphical elements manually – smart maps are created automatically.



4.9 ActiveDirectory devices

nVision enables the import and synchronization of data from ActiveDirectory. The following objects can be synchronized:

- Users,
- Groups
- Computers,
- Organizational units

Adding a domain controller is described in the [next chapter](#).^[136]

After successful synchronization with the domain, information about organizational units of the devices should be visible in host information window:

Device: ZENDESKSAMURAJ-1 (192.168.56.1) (ZendesSamuraj-MJ.axence.local)

Device status: OK (Last response: Today 11:43:03)

PERFORMANCE AND RESOURCES

- CPU:** 30% (Model: Intel(R) Core(TM) i5-2500K)
- RAM:** 34% (Total: 31,71 GB, Used: 10,67 GB, Free: 21,04 GB)
- System disk:** 44% (Total: 232,27 GB, Used: 102,87 GB, Free: 129,41 GB)

Basic information:

- Device name: ZENDESKSAMURAJ-1
- Importance: Normal
- Department: Wsparcie
- Type: Windows 10
- Role: Server Router
- Info 1: axence.local
- Info 2: ZendesSamuraj-MJ

OU: axence.local / Active Computers / User machines

It is also possible to display all devices belonging to the selected organizational unit. To do this, select a specific organizational unit from the devices tab:

Active Directory controllers

| Status | IP | Info | Agent | Name | DNS Address | Operating system |
|--------|-------------|--------------------|-------|------|-------------|------------------------------|
| ✓ | 192.168... | axence.local La... | ✓ | | | Windows 10 Pro 10.0 (1904... |
| ✓ | 192.168... | axence.local | ✓ | | | Windows 10 Pro 10.0 (1904... |
| ✓ | 192.168... | axence.local La... | ✓ | | | Windows 10 Pro 10.0 (1904... |
| ✓ | 10.71.17... | axence.local La... | ✓ | | | Windows 10 Pro 10.0 (1904... |
| ✓ | 192.168... | axence.local Ze... | ✓ | | | Windows 10 Pro 10.0 (1904... |
| ✓ | 192.168... | axence.local Su... | ✓ | | | Windows 10 Pro 10.0 (1904... |
| ✓ | 192.168... | axence.local Ko... | ✓ | | | Windows 10 Pro 10.0 (1904... |
| ✓ | 192.168... | axence.local Ko... | ✓ | | | Windows 10 Pro 10.0 (1904... |
| ✓ | 192.168... | axence.local Ko... | ✓ | | | Windows 10 Pro 10.0 (1904... |
| ✓ | 192.168... | axence.local CR... | ✓ | | | Windows 10 Pro 10.0 (1904... |
| ✓ | 192.168... | axence.local Ko... | ✓ | | | Windows 10 Pro 10.0 (1904... |
| ✓ | 192.168... | axence.local La... | ✓ | | | Windows 10 Pro 10.0 (1904... |
| ✓ | 192.168... | axence.local La... | ✓ | | | Windows 10 Pro 10.0 (1904... |
| ✓ | 192.168... | axence.local Ko... | ✓ | | | Windows 10 Pro 10.0 (1904... |
| ✓ | 192.168... | axence.local La... | ✓ | | | Windows 10 Pro 10.0 (1904... |
| ✓ | 192.168... | axence.local | ✓ | | | Windows 10 Pro 10.0 (1836... |
| ✓ | 192.168... | axence.local Ko... | ✓ | | | Windows 10 Pro 10.0 (1904... |

Part



5 nVision Agent

5.1 Introduction

Agents are programs running on monitored hosts. They are necessary for:

- User activity monitoring,
- Hardware and software inventory,
- DataGuard protection and
- HelpDesk (some features).

5.2 Basic information about Agents

Security

All information sent by the Agent is secured with TLS 1.2. The database is also password protected. To ensure that only one nVision instance can communicate with the Agent, set the Agent password in nVision.

Agent-generated network traffic

All data are compressed before sending and uncompressed after reaching nVision. Agents send small packages every few hours (this parameter can be set in nVision). Daily traffic generated by a single Agent is approx. 100 kB. The first package sent after Agent installation can be bigger (up to approx. 500 kB). The Agent is updated automatically when a new nVision installation is detected. This operation can increase the network traffic (it is necessary to send the Agent's installation file). To prevent the network from being significantly burdened, the number of connections between Agents and nVision can be limited to a single connection (Agents will be updated one after the other).

Resources

An Agent stores approx. 30 - 50 MB of data. CPU usage should be very low (0 - 5%), up to 15% for short periods. One module, which can cause a significant CPU load is the monitoring of data sent by the users. It is caused by a Windows mechanism, which can appear on older systems, sending large amounts of data (e.g. database servers). Disabling network traffic monitoring in the profile of an Agent installed on such a computer is recommended.

Features

Files executable by Agents must be added to the exception list of the anti-virus software and DEP list in Windows. The nVision Agent has the function of e-mail monitoring and website blocking. These functions use TCP/IP stack integration and are disabled by default. This results from the fact that anti-virus software does not allow for correct integration and can lead to connection loss.

5.3 Installing and uninstalling Agents

5.3.1 Overview

The Agent can be installed in several ways. Select the one which is most appropriate to your needs:

- [Installation by means of Active Directory \(GPO\) with the use of MSI installer](#)^[115],
- [Remote installation with the use of the anti-virus software management console](#)^[117],
- [Manual installation](#)^[117].

Installing a new version of the Agent

The Agent has an automatic update mechanism. It checks for a new Agent version every time it connects with nVision. If a new Agent version is available (after you install a new nVision version), the Agent will download it and restart automatically.

Agent archiving

For more information on how to uninstall Agent and release its license without losing the user activity data, see [Agent archiving](#)^[118] chapter.

Uninstalling Agents

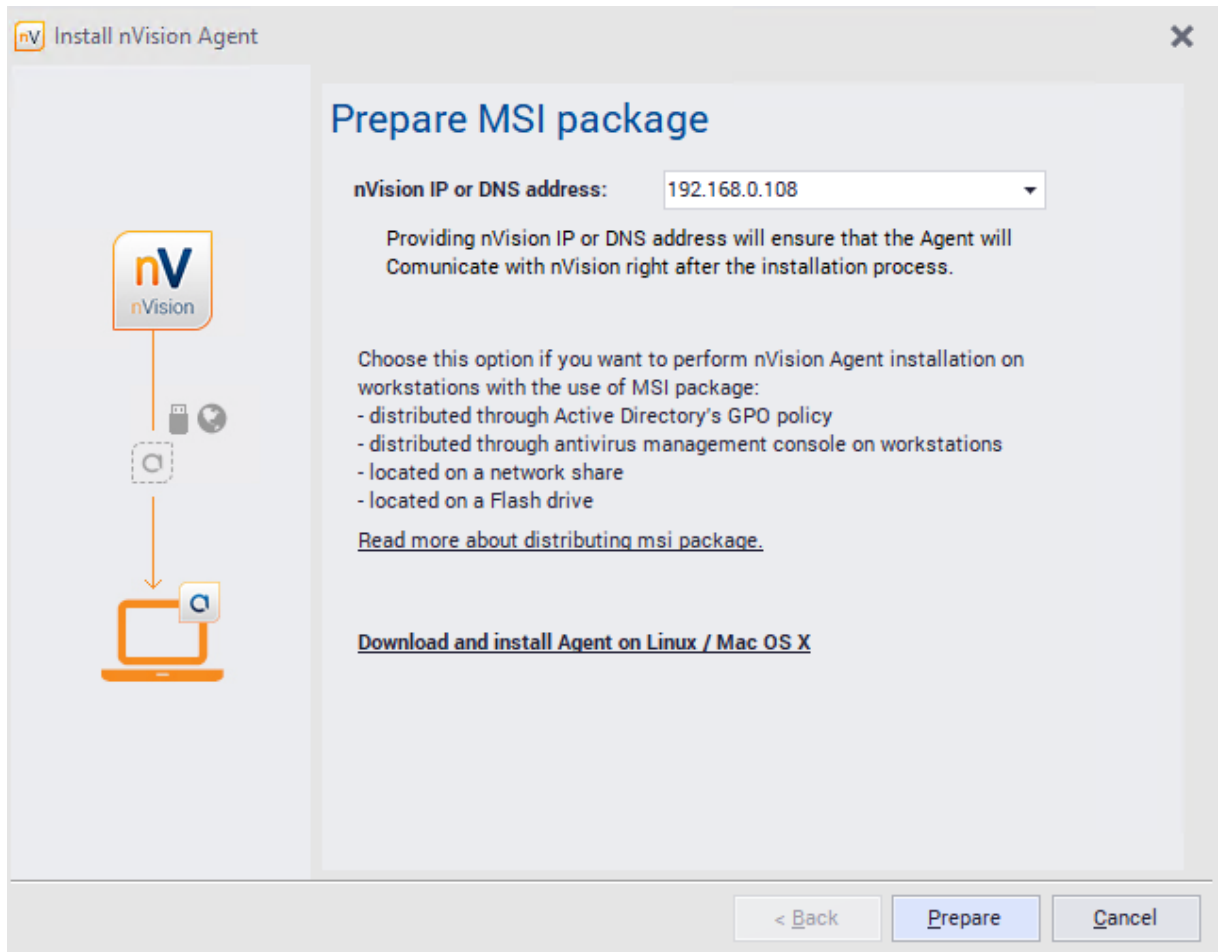
Refer to [Uninstalling Agents](#)^[118] topic.

5.3.2 Installation by means of Active Directory (GPO) with the use of MSI installer

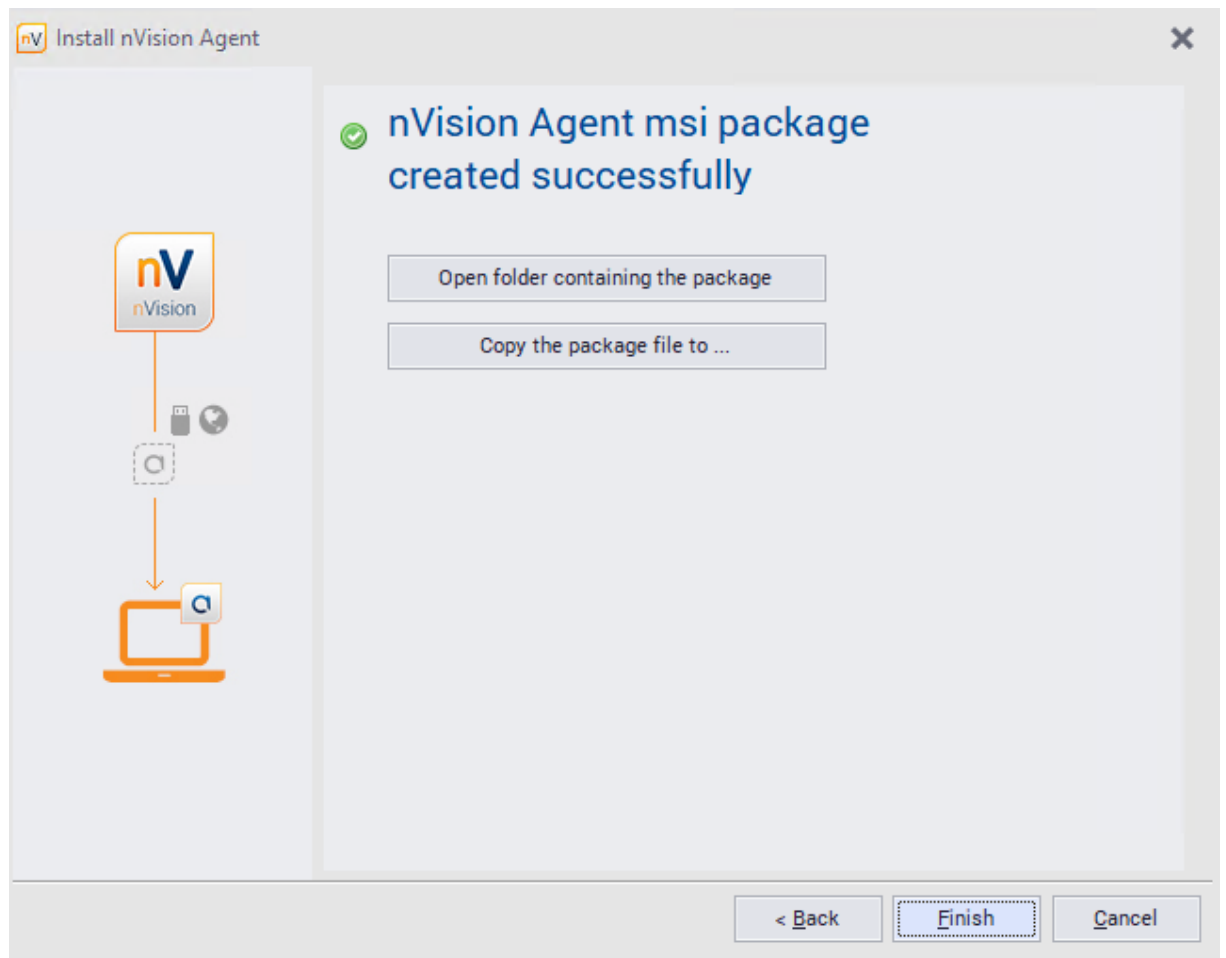
MSI Agent installation package

The following chapter describes how to prepare an MSI Agent installation package. It can be used both for installation through Active Directory and for manual installation on selected computers. In such cases please remember that MSI installation is performed in the non-interactive mode. To install the Agent service, the installation requires local computer administrator rights.

1. Select **Install nVision Agent on Tools tab**



2. Give the IP address where the Agent will send its data to. By default, this is the address of the computer where nVision runs. However, if the Agent is installed on a computer working outside the company and the Agent will send the data through the Internet, enter here the public IP address or the DNS name of the router where the TCP 4434 port will be redirected to the nVision machine. The entered address is permanently stored in the MSI package built on the next step. To change the address, you need to rebuild the package.
3. Click one of the buttons, respectively, to open the folder with the prepared MSI installation package or to copy it to the specified folder.



Related topics

 [Agent installation with use of Active Directory](#) ⁶³⁶

5.3.3 Remote installation with the use of the anti-virus software management console

The generated Agent installation package can also be distributed with the use of remote anti-virus software management consoles. Please refer to your software developer's guides in order to remotely install nVision Agent.

5.3.4 Manual installation

In order to install Agents manually, perform one of the following:

- Copy nvagentinstall.exe file on flash memory drive or network resource (this file is located in the "Agents" subdirectory of the nVision directory). Execute the file on each computer where you want to install the Agent.
- You may also prepare an MSI installation package and execute it on each computer or distribute by means of Active Directory GPO (details in the [Installation by means of Active Directory \(GPO\) with the use of MSI installer](#) ¹¹⁵ chapter).

5.3.5 Agent archiving

The Agent archiving tool allows to disable Agents on devices, which should not be monitored, without the loss of data collected by the Agents. Archiving of Agent data has the following results:

- Agent is uninstalled and its license is **released**,
- user activity data are **saved**,
- inventory and assets data are **deleted**,
- service and counter monitoring is **disabled**.

Archiving of Agent data

To archive Agent data:

1. In nVision, right click the icon of device with Agent.
2. Choose **Agent / Archive**. Click **OK**.
3. After archiving the Agent is presented with "Archived" status.

5.3.6 Uninstalling Agents

To uninstall Agents remotely, select the **Agent / Uninstall...** option from the context menu of each host. Uninstallation is performed without the use of WMI, so Agents will be uninstalled whether WMI is or is not enabled on the host. Agents will be uninstalled automatically after starting up and connecting to the console.

You can also uninstall the Agent manually by executing the file uninst000.exe located in the Agent folder.

5.4 Agent configuration

5.4.1 Agent password

Agent in Axence nVision® is password protected from being uninstalled by the user (even that with the administrator rights in Windows).

The password that protects the Agent from being uninstalled is simultaneously the password of the **Administrator** account built into nVision (the basic account with **Administrator** login – its name is bold in the view of the [Users](#) window). The Agent is automatically password protected after the installation, upon the first successful connection to the nVision Server.

⊕ Agent's password in Axence nVision® 8 and older versions.

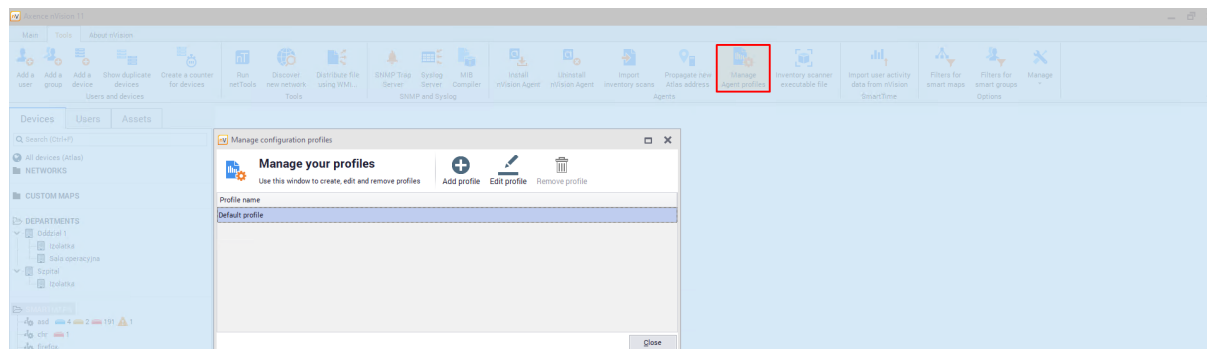
To change the Agent password in the Atlas:

1. Choose **Atlas / Properties**.
2. In the Atlas properties window, click the **Agent password** button.
3. Enter old and new passwords, then press **OK**.

5.4.2 Profile management

If many Agent profiles are defined, it is recommended to use the profile management tool for profile creation and editing. For this purpose:

1. Select the **Manage your Agent profiles** option on the ribbon (in the **Tools and options** page). The **Manage configuration profiles** window will open.



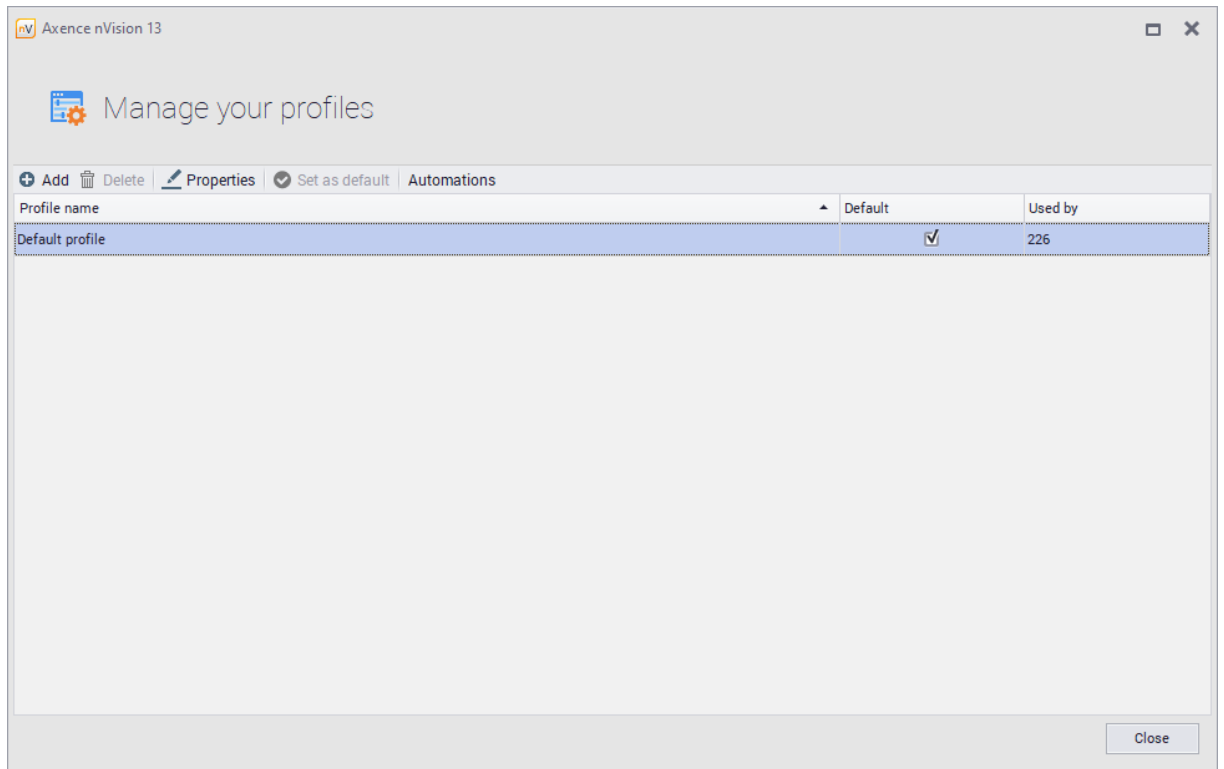
2. The defined profiles are displayed in the list. To **Add**, **Edit** or **Remove profile**, use the appropriate button.
3. If a new profile is to be created, click the **Add profile** button and in the displayed **Agent configuration** window enter the name of the created profile and set its properties. The properties are described in the [Agent settings](#) ¹²⁵ section.

5.4.3 Profiles





5.4.3.1 Profiles - introduction

Profiles are sets of policies. A single profile is composed of one policy of each kind. The configuration and management of profiles, i.e. viewing, adding, editing, deleting profiles (the default policy cannot be removed) or indicating which profile is to be the default one, are only available to the administrator with the appropriate rights.

The profiles and [policies](#) have been introduced as a new solution for the [Agent Profiles](#) that have ceased to exist since Axence nVision® version 13.



Related topics:

-  [Creating a profile](#)
-  [Setting the default profile](#)
-  [Editing a profile](#)
-  [Deleting a profile](#)
-  [Profile automations](#)
-  [Policies](#)

5.4.3.2 Creating a profile

To create a new profile:

1. In the nVision console, click the **Tools** tab.
2. Click the **Manage profiles** button.
3. In the Profile Management window, click the **Add** button or right-click in the list of profiles and then click the **Add** button.
4. Configure the profile, and then click **OK**.

Once you have completed the steps above, the profile you have created will be displayed in the list of profiles.

5.4.3.3 Default profile

The default profile is the profile assigned to each new Agent detected in nVision (unless the [profile automation](#) mechanism assigns a different profile to the Agent). The default profile cannot be deleted.

To set the default profile:

1. In the nVision console, click the **Tools** tab.
2. Click the **Manage profiles** button.
3. Click the profile that appears in the list of profiles (it cannot be set as the default one!) and click the **Set as default** button or right-click the profile you want to set as the default one, and then click the **Set as default** button.
4. Click in the default profile setting confirmation window.

Once you have completed the steps above, the selected profile will be the default profile (the **Default** column checkbox in the list of profiles is checked).

5.4.3.4 Editing a profile

To edit a profile:

1. In the nVision console, click the **Tools** tab.
2. Click the **Manage profiles** button.
3. In the Profile Management window, click the selected profile, click the **Properties** button above the list or right-click the selected profile in the list and then click the **Properties** button.
4. Configure the selected profile, and then click **OK**.

Once you have completed the steps above, the profile configuration will be edited successfully.

5.4.3.5 Deleting a profile

To delete a profile:

1. In the nVision console, click the **Tools** tab.
2. Click the **Manage profiles** button.
3. In the Profile Management window, click the selected profile, click the Delete button above the list or right-click the selected profile in the list and then click the **Delete** button.
4. Click **Yes** in the profile deletion confirmation window.

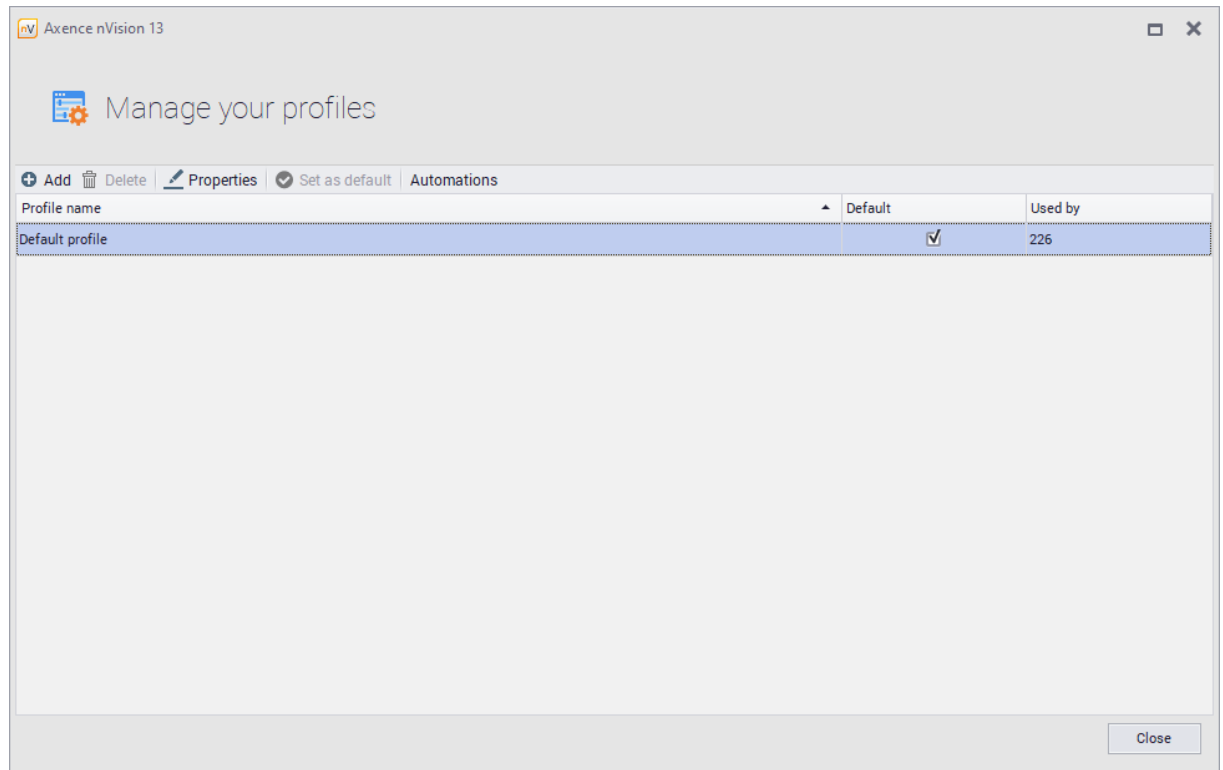
Once you have completed the steps above, the selected profile will be deleted and will not be displayed in the list anymore. If you delete a profile that is used in a given device, the default profile will be set for that particular device.

Note! The default profile cannot be deleted. If you want to delete a profile that is the default one, you must first set a different default profile.

5.4.3.6 Automations

5.4.3.6.1 Profiles automations

The profile automation mechanism allows you to create a rule to assign specific profiles to new devices. The automation can replace the assignment of the default profile. The administrator who has access to all maps and departments in nVision can view, create, reorder, edit, and delete rules.



5.4.3.6.2 Creating a profile automation

To create an automation rule:

1. In the nVision console, click the **Tools** tab.
2. Click the **Manage profiles** button.
3. Click the **Automations** tab.
4. In the Profile Automation window, click the **Add** button or right-click in the list of profiles and then click the **Add** button.
5. Configure the rule (the **Rule name** and the defined **Condition** are required).
6. Click **OK**.

Once you have completed the steps above, the new automation rule will be displayed in the list.

5.4.3.6.3 Editing a profile automation

To edit an automation rule:

1. In the nVision console, click the **Tools** tab.
2. Click the **Manage profiles** button.
3. Click the **Automations** tab.
4. In the Profile Automation window, select the automation and click the **Properties** button or right-click the specific automation line and then click the **Properties** button.

5. Configure the rule (the **Rule name** and the defined **Condition** are required).
6. Click **OK**.

Once you have completed the steps above, the automation rule properties will be updated.

5.4.3.6.4 Deleting a profile automation

To delete an automation rule:

1. In the nVision console, click the **Tools** tab.
2. Click the **Manage profiles** button.
3. Click the **Automations** tab.
4. In the Profile Automation window, select automation and click the **Delete** button or right-click the specific automation line and then click the **Delete** button.
5. Click **Yes** in the automation rule deletion confirmation window.

Once you have completed the steps above, the selected automation rule will be deleted and will not be displayed in the list anymore.

5.4.4 Policies

5.4.4.1 Policies - introduction

Policies are sets of defined settings that are automatically applied by the Agent installed on a specific machine. The Agent periodically verifies that the policy settings and the settings of the particular machine are identical. If not, the Agent reconciles them so that they are compatible with the assigned policy. Each policy has its own name. In addition, policies are divided into different types which are distinguished by the subject of the settings they regulate. Policies of different types are clearly separated from each other, i.e. they are not displayed in the same list and their previews are available in separate tabs. In each policy type, there is a so-called default policy (which is automatically indicated in each newly created profile). The default policy cannot be deleted. The configuration and management of policies, i.e. viewing, adding, editing, deleting policies (the default policy cannot be removed) or indicating which policy is to be the default one, are only available to the administrator with the appropriate rights.





To display the policy configuration panel:

1. In the nVision console, click the **Tools** tab.
2. Click the **Manage** button.
3. In the drop-down list, click the **Manage policies** button.

Available policy types

1. Scanning user files
2. Windows Defender
3. Windows Firewall
4. nVision Agent compatibility

Related topics:

-  [Creating a policy](#)
-  [Setting the default policy](#)
-  [Editing a policy](#)
-  [Deleting a policy](#)

5.4.4.2 Creating a policy

To create a new policy:

1. In the nVision console, click the **Tools** tab.
2. Click the **Manage** button.
3. In the drop-down list, click the **Manage policies** button.
4. In the Policy Management window, click the **Add** button or right-click in the list of policies and then click the **Add** button.
5. Configure the selected policy type, and then click **OK**.

Once you have completed the steps above, the policy you have created will be displayed in the list of policies.

5.4.4.3 Setting a default policy

The default policy is a policy that is automatically assigned to each newly created profile. The list of policies of each type must include the default policy. The default policy cannot be deleted.

To set the default policy:

1. In the nVision console, click the **Tools** tab.
2. Click the **Manage** button.
3. In the drop-down list, click the **Manage policies** button.
4. Click the policy that appears in the list of policies (it cannot be set as the default one!) and click the **Set as default** button or right-click the policy you want to set as the default one, and then click the **Set as default** button.
5. Click **Yes** in the default policy setting confirmation window.

Once you have completed the steps above, the selected policy will be the default policy.

If the selected policy is already the default policy, the **Set as default** button will be grayed out.

5.4.4.4 Editing a policy

To edit a policy:

1. In the nVision console, click the **Tools** tab.
2. Click the **Manage** button.
3. In the drop-down list, click the **Manage policies** button.
4. In the Policy Management window, click the selected policy, click the **Properties** button above the list or right-click the selected policy in the list and then click the **Properties** button.
5. Configure the selected policy, and then click **OK**.

Once you have completed the steps above, the policy configuration will be edited successfully.

5.4.4.5 Deleting a policy

To delete a policy:

1. In the nVision console, click the **Tools** tab.
2. Click the **Manage** button.
3. In the drop-down list, click the **Manage policies** button.
4. In the Policy Management window, click the selected policy, click the **Delete** button above the list or right-click the selected policy in the list and then click the **Delete** button.
5. Click **Yes** in the policy deletion confirmation window.

Once you have completed the steps above, the selected policy will be deleted and will not be displayed in the list anymore. If you delete a policy that is used in the profile, the default policy will be set for that particular profile.

Note! The default policy cannot be deleted. If you want to delete the policy that is the default one, you must first set a different default policy.

5.4.5 Agent settings

The data collected by the Agent and its behavior depend on:

- Agent profile configuration,
- Agent configuration for selected group or user.

The individual settings are described in detail in the following subsections.

5.4.5.1 Agent profile settings

In order to change the Agent's profile, select the **Manage your Agent profiles** option on the ribbon (in the **Tools** page).

Agent profile settings are divided into 2 tabs:

General

General settings allow to:

- enable scanning user files by extensions.
The legality of the files kept by the user may constitute a problem. Therefore, nVision allows files with an extension suggesting the involvement of copyrights to be monitored. It is possible to add and remove the files from the list of monitored user files. In particular, to add the most common multimedia file extensions to the list, click the **Add multimedia extensions** button. To monitor a different file type, enter their extension in the list (comma separated),
- define the TCP ports on which traffic in applications is to be blocked by the Agent.

Compatibility

- Monitoring bandwidth usage
Allows the monitoring of total inbound and outbound transfers, with a division into local and Web transfer, and the bandwidth usage by browsers, e-mail client, etc.
- Application blocking integration

Allows the Agent to block the applications defined in nVision configuration.

- DataGuard integration

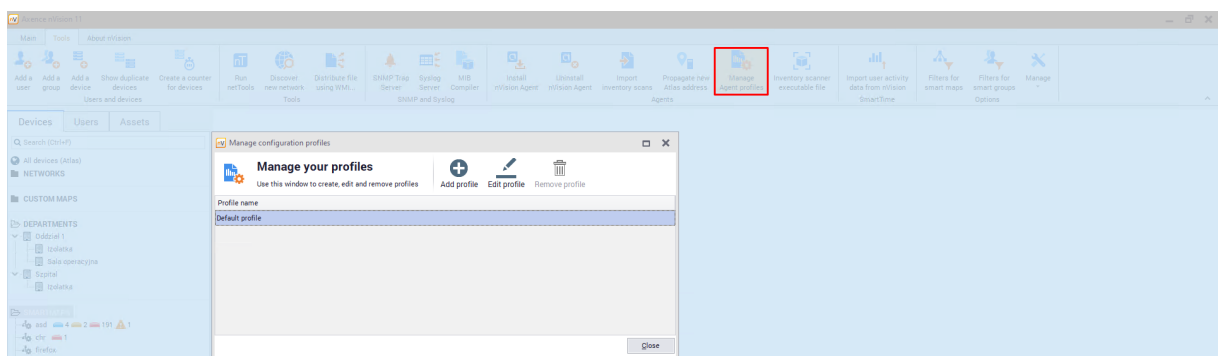
If data protection is enabled, data media used by the user are monitored and access rights management is enabled.

- Integration with TCP/IP stack

If this option is unchecked, blocking websites and monitoring e-mail headers is impossible. **If there are problems with specific applications or access to web pages (e.g. internet banking websites) after the integration is enabled on the computer with Agent, add the process names of these applications or domains to the exception list.**

- Monitor SSL/TLS traffic

This option allows monitoring e-mail headers even where such correspondence is encrypted.

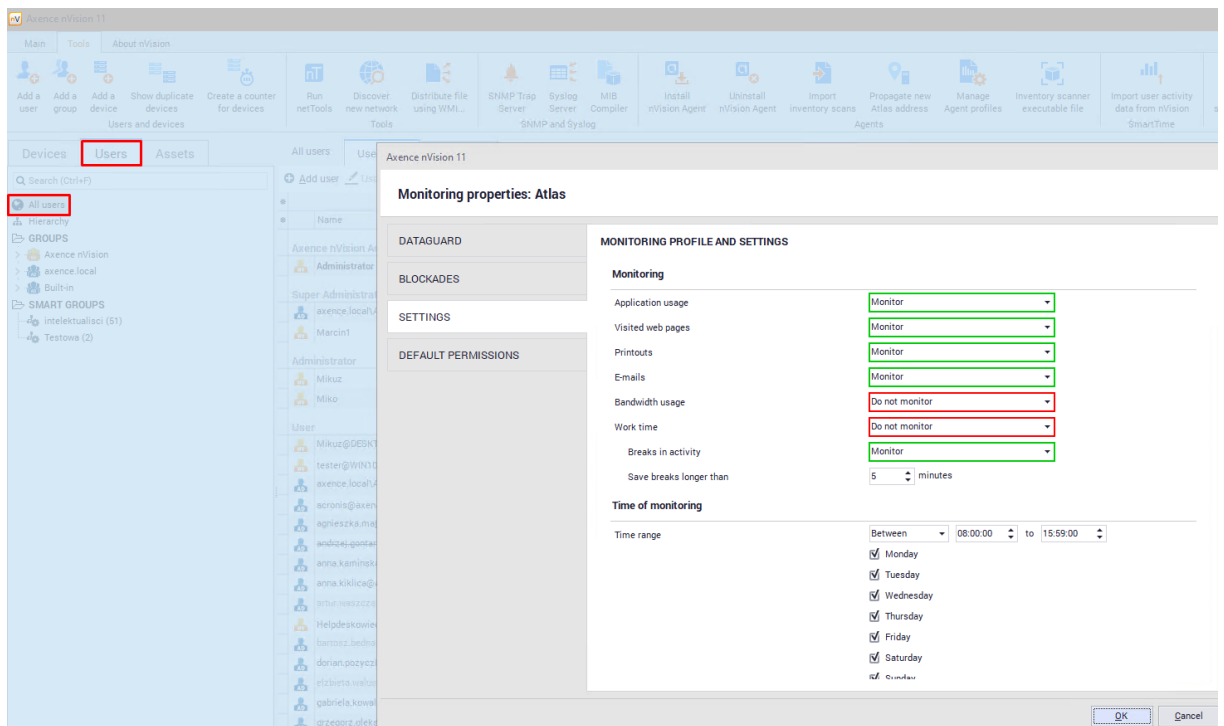


5.4.5.2 Monitoring and visibility settings

The second part of Agent configuration is Agent monitoring and visibility settings.

These settings can be defined for the Atlas (all users), user groups and individuals. They can be found in different locations:

1. The **Users / Atlas info / Settings** window:



The **Group information / Settings** window.

2. The **Group information / Settings** window.

Atlas is the “general” setting, which by default is inherited by groups and users. However, this behavior can be changed for individual units by navigating to the above-mentioned setting windows.

The settings include a few sections:

- **Monitoring**

The Administrator can specify what information is to be collected by the Agent. In addition, it can be determined here whether or not the breaks in activity (i.e. the time when the user does not type any characters from the keyboard or does not use the mouse) are to be monitored.

Axence nVision 11

Monitoring properties: Atlas

DATAGUARD

BLOCKADES

SETTINGS

DEFAULT PERMISSIONS

MONITORING PROFILE AND SETTINGS

Monitoring

| | |
|-------------------------|----------------|
| Application usage | Monitor |
| Visited web pages | Monitor |
| Printouts | Monitor |
| E-mails | Monitor |
| Bandwidth usage | Do not monitor |
| Work time | Do not monitor |
| Breaks in activity | Monitor |
| Save breaks longer than | 5 minutes |

Time of monitoring

Time range: Between 08:00:00 to 15:59:00

- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday
- Sunday

OK Cancel

Monitoring time

This section defines the time periods during which the Agent should monitor the user activity.

Axence nVision 11

Monitoring properties: Atlas

DATAGUARD

BLOCKADES

SETTINGS

DEFAULT PERMISSIONS

MONITORING PROFILE AND SETTINGS

E-mails: Monitor

Bandwidth usage: Do not monitor

Work time: Do not monitor

Breaks in activity: Monitor

Save breaks longer than: 5 minutes

Time of monitoring

Time range: Between 08:00:00 to 15:59:00

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

Desktop preview and remote access

Allow desktop preview: Allow

Allow remote access: Allow

OK Cancel

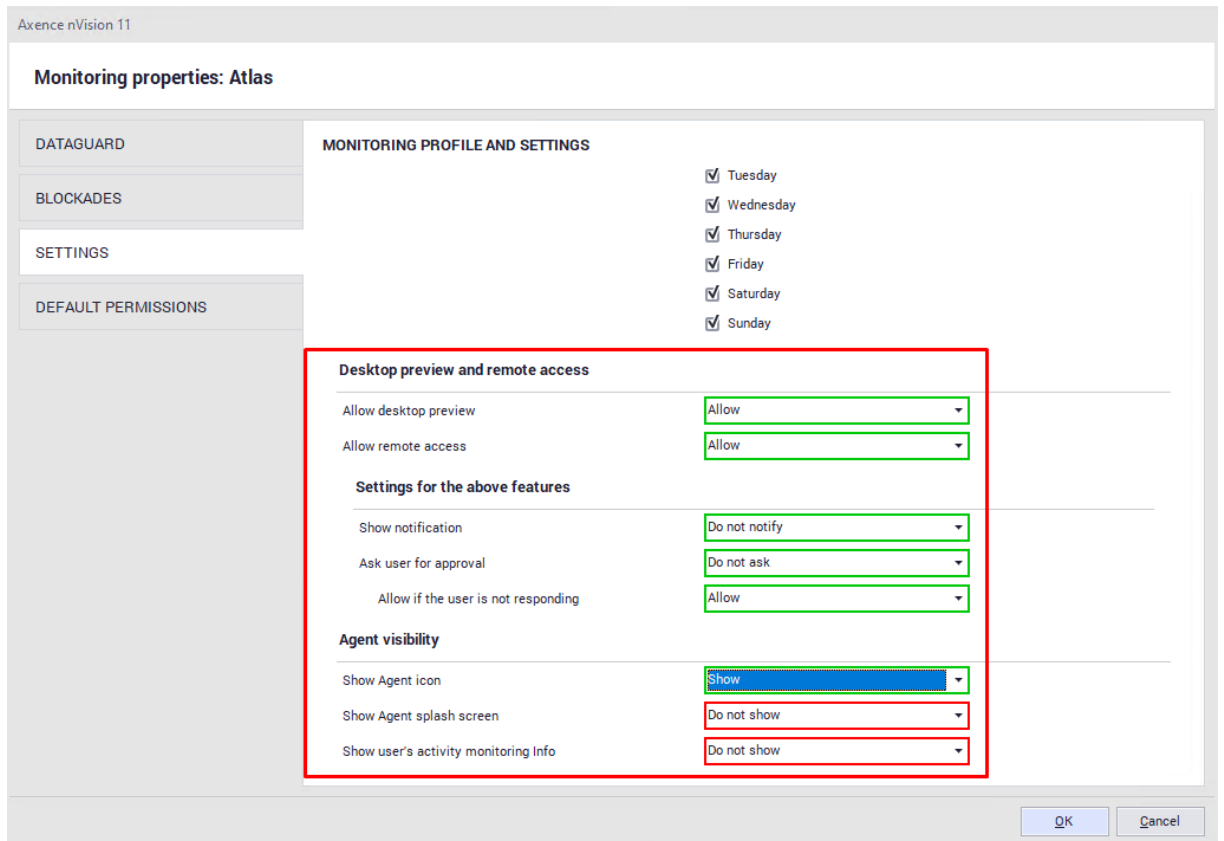
Desktop preview and remote access

The settings in this section allow you to define whether or not:

- remote access or desktop preview is allowed,
- the user must agree for taking over control of their machine,
- the user is informed when control of their machine is taken over.

• Agent visibility

The last section determines the visibility of the Agent and its icon on the taskbar.



5.4.6 Web filtering profile

The Agent profile allows selected websites to be blocked. To ensure proper blocking, it is necessary to check the **Turn on TCP/IP stack integration** option in the **Compatibility** tab. To learn more, see the [cannot block websites](#)^[130] section.

Website blocking is performed in a manner independent of the application or port. Websites are recognized on the basis of the request prefix. Blocking is executed on the level of:

- IP address,
- exact domain (on http level),
- regular expressions for the domain (also on http level).

Adding filtering rules is described in section [How to block access to selected websites?](#)^[169]


5.4.7 Integration with TCP/IP stack

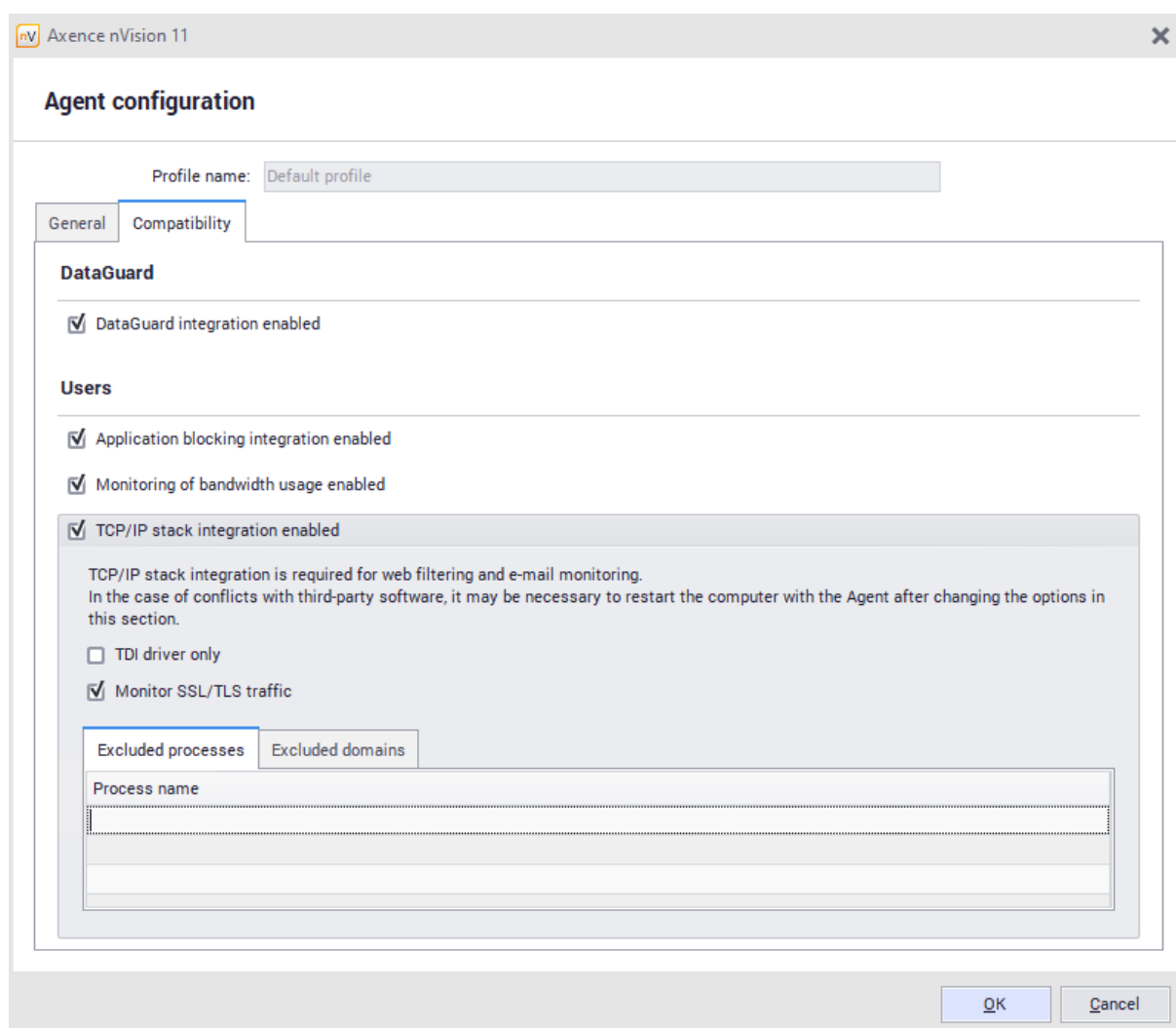
Monitoring e-mails and blocking websites is only possible for machines with the installed Agent and enabled integration with the TCP/IP stack. To learn more on Agent installation, see the [Installing and uninstalling Agents](#)^[115] section.

The following protocols are supported at the moment: HTTP, HTTPS, SMTP:25, SMTP:587, SMTP via SSL, POP3 via SSL and POP3:110. The following protocols are not supported at the moment: IMAP, MAPI.

Enable integration with TCP/IP stack

If the Agent is installed, the reason for the problems with monitoring e-mails and blocking websites may be a disabled integration with the TCP/IP stack. By default, this integration is disabled due to the necessity of earlier tests, mostly in the scope of cooperation with anti-virus software. To enable TCP/IP stack integration:

1. Select the **Managing Agent profiles** option in the menu bar (in the **Tools and options** page).
2. Create a new profile or select the profile used by Agents, and then click the  **Edit profile** button.
3. In the profile configuration, check the **Turn on TCP/IP stack integration** option in the **Compatibility** tab.



4. **On the tested computers, add all contents of the directory `c:\Program Files\Axence\nVision Agent 2\` including subfolders to the exception list of anti-virus software.**
5. Restart the computers.

- If no negative symptoms, e.g. network loss, occur during the next few system restarts, it means that TCP/IP stack integration can be toggled on for the remaining machines.

5.5 “Agents” view

The “Agents” view in the main nVision window presents the following information:

- host status,
- host name,
- Agent version,
- Agent online (yes/no),
- last connection time,
- last data received,
- pending instructions (Agent uninstallation, Atlas address change, host data reset),
- status,
- configuration,
- screenshots,
- free disc space,
- free physical memory,
- CPU usage (average for the last minute),
- last logged-on user,
- bandwidth data (last hour)
- and other.

| Device | Agent | Configuration | Status | System disk | Free physical me | CPU usage | Last logged-on user |
|--|--------------------------------|---|---------|-------------|------------------|-----------|------------------------|
| WIN10 192.168.69.206 Info: AED-133 Version: 2.0.4.28748 Status: 23.05.2020 16:00 | 2.0.4.28748 Today, 11:05:00 | < Use map "192.168.69.0/24" profile: Default profil. | Warning | 10.9 | 10.0 | 0/0 | n/a |
| DESKTOP-W0QNH1T 192.168.0.108 WORKGROUP Version: 2.0.4.28748 Status: Green | 2.0.4.28748 Today, 11:05:00 | < Use map "192.168.0.0/16" profile: Default profile > | Green | 28.53 GB | 1.79 GB | 31 % | Mikusz@DESKTOP-W0QNH1T |

Part



6 Users in nVision

6.1 General information

User accounts in nVision can be created in a few ways:

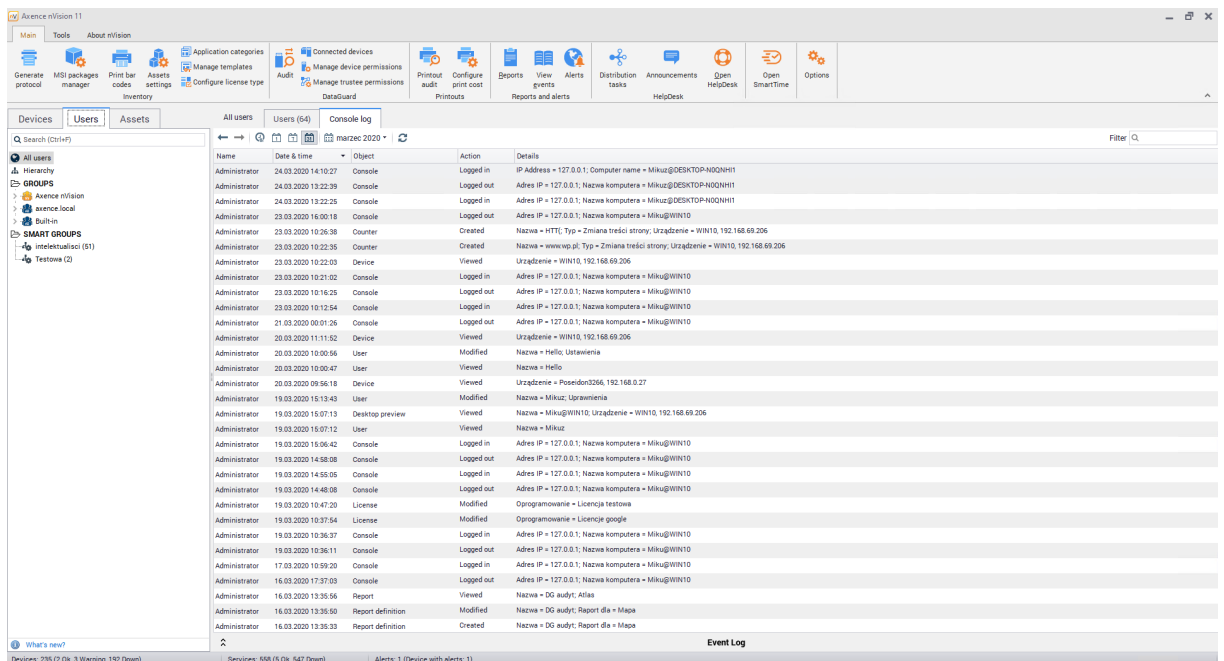
- manually via the Administrator in nVision (all types) – in the **Users** tab, after clicking the **Add user** button,
- via the Administrator by downloading the account list from Active Directory controller – in the **Users** tab, after clicking the **Active Directory controllers** button and configuring the domain controller,
- independently by the users (only the “User” type) in the HelpDesk web interface, without additional account activation, with activation via e-mail, or with manual activation via the Administrator,
- logging in to the Windows account should result in the creation of nVision account for this user (unless an account with such a SID already exists in nVision). Each Windows local account should have a unique SID.

The list of all users is available in the **Main / Users** tab. The list is divided into sections corresponding to the individual roles in nVision:

| Axence nVision | | | | | | | | | | Users (8) | | | | Console log | | | |
|------------------------------|--------------------|-----------------|----------------|-----------|---------|------------------|------------------|----------------|---------------|------------------------------|---------|----------------|------------------|------------------------|------------------|---------------|--|
| | | | | | | | | | | Active Directory controllers | | | | | | | |
| | | | | | | | | | | User | | | | Device | | | |
| Name | Full name | Email | Domain | Activated | Enabled | Last login | Created | Name | IP | Agent online | Working | Activity today | Last application | Last application title | Last page URL | Last activity | |
| Axence nVision Administrator | | | | | | | | | | | | | | | | | |
| Administrator | Administrator | | Axence nVision | ✓ | ✓ | 06.03.2020 09... | 01.07.2019 16... | | | | | | | | | | |
| Super Administrator | | | | | | | | | | | | | | | | | |
| Marcin1 | Marcin Marcinowski | | Axence nVision | ✓ | ✓ | | 05.11.2019 09... | | | | | | | | | | |
| Administrator | | | | | | | | | | | | | | | | | |
| Mikuz | | mikolaj.matu... | Axence nVision | ✓ | ✓ | 23.03.2020 19... | 02.07.2019 14... | | | | | | | | | | |
| Miko | Testowy user miko | nvision@axen... | Axence nVision | ✓ | ✓ | 26.02.2020 19... | 25.07.2019 10... | | | | | | | | | | |
| User | | | | | | | | | | | | | | | | | |
| Mikuz@DESKTOP-NQ... | | | Axence nVision | ✓ | ✓ | 25.03.2020 19... | 24.03.2020 14... | DESKTOP-NQDNH1 | 192.168.0.108 | ✓ | | | n/A nVision.exe | Axence nVision 11 | https://www.r... | The i | |
| tester@WIN10VM | | | Axence nVision | ✓ | ✓ | 10.10.2019 09... | 10.10.2019 09... | | | | | | | | | | |
| Helpdeskowalec | asid | | Axence nVision | ✓ | ✓ | 05.08.2019 11... | 05.08.2019 11... | | | | | | | | | | |
| Hello | Ole | | Axence nVision | ✓ | ✓ | 20.03.2020 19... | 11.07.2019 11... | | | | | | | | | | |

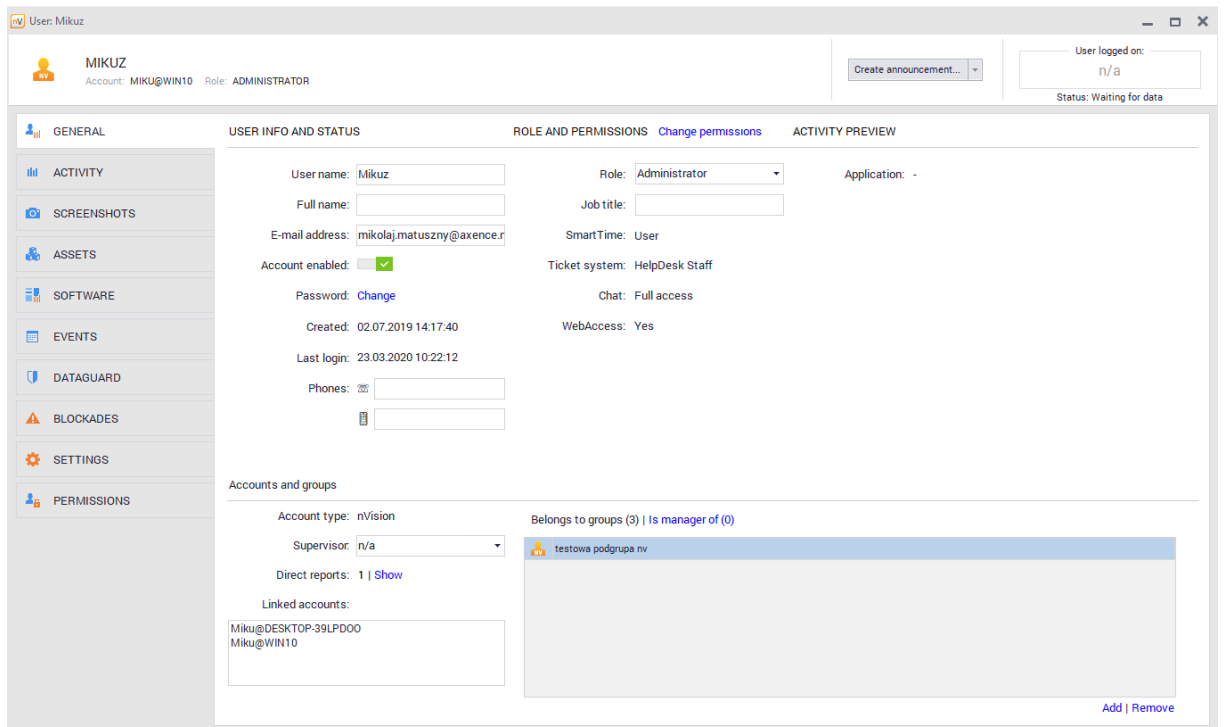
6.2 Access log

The access log is located in the **Main / Users / Access Log** tab. It stores any operations taken by the Administrator with regard to user accounts (e.g. creation of an account, modification of settings).



6.3 User information screen

After selection of user from the list, you can navigate to the user information screen.



This program area provides basic information about the selected person. The following account attributes can be identified:

- User – the name under which the user can log in to the nVision console and to the HelpDesk module,

- Full name,
- E-mail address,
- Desk (and mobile) phone number,
- Role – user roles are described in chapter [Types of user roles](#).
- Title,
- Group membership – allows to view the groups which the selected user is a member of,
- Superior – user that is higher in the hierarchy than the currently selected person. A person who has subordinates will have access to the activity data for each of their subordinates in the SmartTime module,
- Attachments – additional attachments related to the selected user.

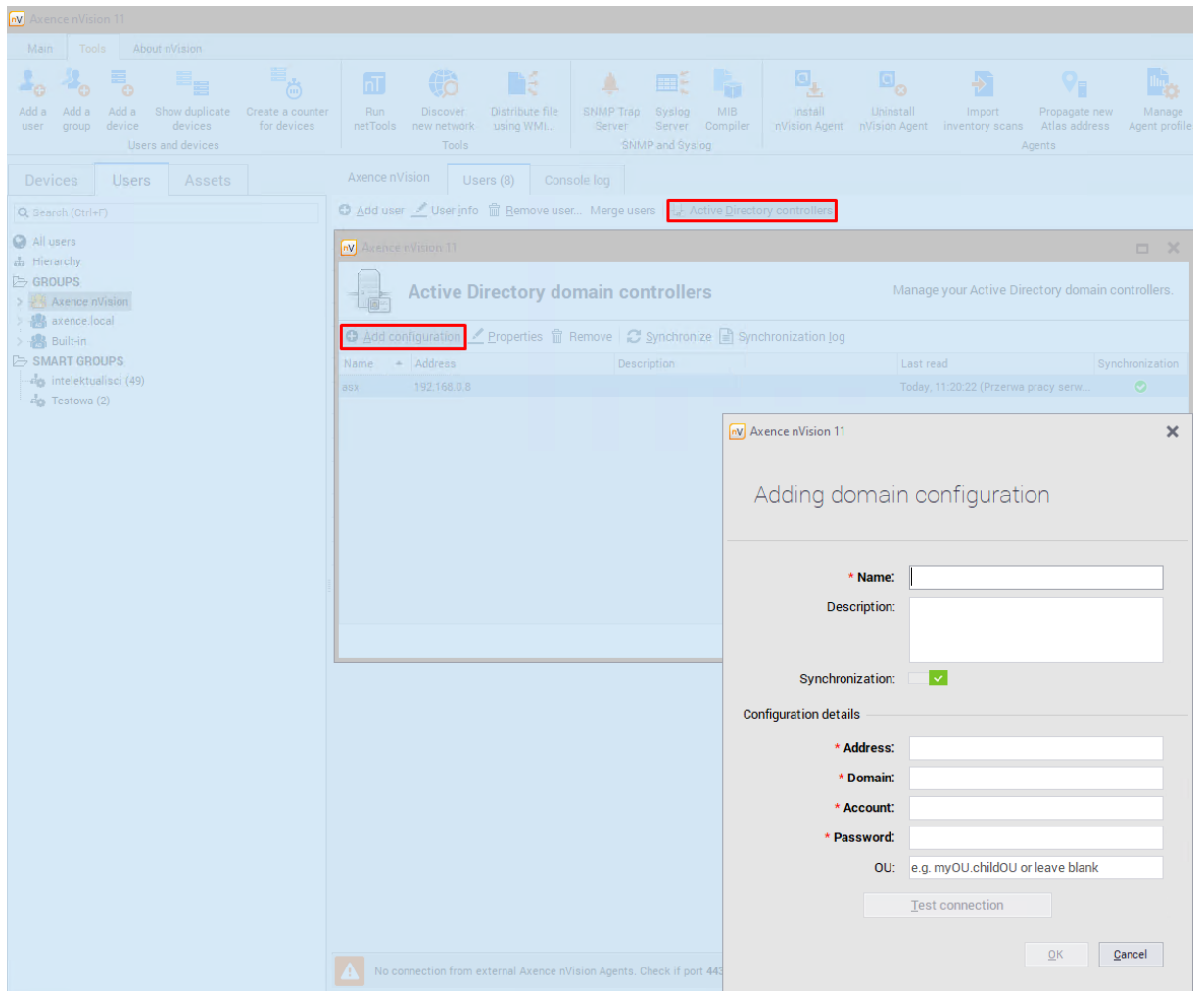
In addition, the user information screen provides information about user rights in various areas of the program. For accounts created in nVision, you may modify all the above-mentioned attributes.

6.4 Synchronization with Active Directory

It is possible to synchronize users existing in Active Directory with the nVision database. **However, it should be borne in mind that this synchronization is performed in one way only, which means that nVision reads data from Active Directory, but cannot make any changes. This means that most of the fields in the user information screen will not be available for editing.**

Adding domain controller

To make the synchronization between Active Directory and nVision, add the domain controller. To do this, navigate to the **Main / Users / Active Directory Controllers** tab. Then click the **Add configuration** button and define the required parameters:



If the data entered are correct, all users and groups created in Active Directory will be read.

Synchronization of selected organizational units (OUs)

In the configuration of domain controller, you can specify OUs with which the list of user accounts is to be synchronized. Specify OUs in the following form: MainOUName.SubOUName.

For example, when “Axence.Users.Krakow.Support” is entered in the “OU” field, then only the users from the Organizational Unit ‘Support’ in the Krakow branch of Axence will be taken from the entire forest.local domain:

Axence nVision 11

Adding domain configuration

* Name: test

Description:

Synchronization:

Configuration details

* Address:

* Domain: axence.local

* Account:

* Password:

OU: Axence.Users.Krakow.Support

Test connection

OK Cancel

Synchronization log

The synchronization log provides information on communication between nVision and Active Directory. This feature may be helpful if you encounter errors related to the synchronization.

Synchronized user attributes

| Attribute in Active Directory | Name in nVision |
|-------------------------------|-----------------|
|-------------------------------|-----------------|

displayName

First name + last name

| Attribute in Active Directory | Name in nVision |
|-------------------------------|---------------------|
| primaryGroupid | Belongs to group |
| manager | Superior |
| Managed by (group setting) | Group manager |
| title | Title |
| telephoneNumber | Phone number |
| mobile | Mobile phone number |
| mail | E-mail address |

6.5 User roles and rights management

6.5.1 Types of user roles

In version 11 of the program, the rights granted to users have been reorganized. The new system of rights identifies three global user roles:

- **super administrator,**
- **administrator,**
- **user.**

The “HelpDesk employee” role which entitles the user to process tickets in the HelpDesk module was moved to the **User information / Rights / HelpDesk** screen.

The individual roles are described in detail below, and the process of granting access rights to specific modules is described in section [Management of access to program functions](#)¹⁴⁸.

⊕ Super administrator

A person having the super administrator rights:

- Can manage the entire program and the **rights of other administrators,**

- Can manage the rights of any other administrators and super administrators (except for the built-in administrator account). Can create, edit and delete other administrators and super administrators. In particular, they can also edit all properties of their own accounts,
- Has always unlimited access to all system functions. Their access to modules, maps or users cannot be disabled,

User with the super administrator role may be deprived of access to chats to hide their accounts on the contact list.

⊕ Administrator

A person having the administrator rights:

- Cannot grant or take back the administrator or super administrator roles,
- Cannot edit the login, first and last name, e-mail address, password, role and rights in other administrator and super administrators accounts. Cannot also activate/deactivate or delete them,
- Can change their own login, first and last name, e-mail address and password. Cannot change their own roles or rights. Cannot also activate/deactivate or delete their own accounts,
- Can edit the properties of users they have access to (login, first and last name, e-mail address, password, etc.). Cannot change their roles or rights,
- Can have access to the nVision administration console and the selected configuration settings of individual modules,

Can be granted the HelpDesk and SmartTime administrator role (the prerequisite is to have access to the relevant modules).

⊕ User

User is a person that does not configure technical aspects of the program, but only uses it within the rights assigned to them:

- Cannot be granted access to the nVision administration console or the module configuration options,
- Cannot play the HelpDesk or SmartTime administrator role,
- **Can play the HelpDesk support employee role,**

Can be granted access to WebAccess.

6.5.2 Available permissions

This chapter describes the rights that may be granted to users under each of the roles.

| Module/functionality | Right | Value | Description |
|---------------------------------------|---|-----------------------------------|--|
| nVision administration console | Access to the nVision desktop console | Yes/No | User can log in to the nVision administration console. |
| | Access to the management of Agent visibility settings | Yes/No | User may manage the settings of the Agent icon visibility and the Agent screen visibility after logging in. |
| | Access to the Agent menu | Yes/No | User has access to the menu where they can execute remote commands on a machine with Agent (including disabling or uninstalling the Agent itself). |
| | Access to the WebAccess console | Yes/No | User can log in to the nVision's remote WebAccess interface. If user is not the administrator, this option allows to define maps and branches on which the user will be able to open the map view, view the device information and enable remote access. |
| | Access to maps and branches | Access to all or selected objects | <p>Access to all: user can see the selected maps and branches. They have access to creating, editing and deleting them.</p> <p>Access to selected: user can see the selected maps and branches only. They cannot create new objects (or delete the existing ones). They can edit only those maps and branches they have access to. They cannot also create sub-branches in the branches managed by them.</p> |
| | Access to users and groups | Access to all or selected objects | <p>Access to all: user can see all users and groups and have access to creating, editing and deleting them.</p> <p>Access to selected: user can see the selected users and groups only. They cannot create new users and groups, or delete the existing ones. They can edit only those they have access to. They cannot also create sub-groups in the groups managed by them. They cannot change the users' (and groups') membership of groups</p> |

| Module/functionality | Right | Value | Description |
|----------------------|--|--------|--|
| | | | other than those they have access to. They cannot delete or add any user (or group) to a group not managed by them. |
| Network | Access to the management of the Network module functions | Yes/No | This right allows access to the Network module components via the nVision administration console. If user does not have access to the administration console, this setting is ineffective. |
| Inventory | Access to the management of the Inventory module functions | Yes/No | This right allows access to the Inventory module components via the nVision administration console. If user does not have access to the administration console, this setting is ineffective. * Further options are only available when access to the module management is enabled. |
| | Access to the management of settings in Agent profiles * | Yes/No | User can manage the Agent profiles and edit settings from the Inventory module in them. |
| | Access to the file manager * | Yes/No | User can use the file manager function. This setting is shared with the HelpDesk module (the function is available in both modules). |
| | Access to the MSI package manager * | Yes/No | User can use the MSI package manager function. |
| Users | Access to the management of the Users module functions | Yes/No | This right allows access to the Users module components via the nVision administration console and enables to grant the administrator rights in the SmartTime interface. * Further options are only available when access to the module management is enabled. |

| Module/functionality | Right | Value | Description |
|----------------------|---|--------|---|
| | Access to the management of settings in Agent profiles * | Yes/No | User can manage the Agent profiles and edit settings from the Users module in them. |
| | Access to the management of desktop preview settings * | Yes/No | User can manage the desktop preview settings for the users they have access to. This setting is shared with the HelpDesk module (the function is available in both modules). |
| | Access to the management of monitoring settings * | Yes/No | User can manage the monitoring settings for the users they have access to. This setting is shared with the SmartTime module (the function is available in both modules). |
| | Access to the management of blocking settings * | Yes/No | User can manage the blocking settings for the users they have access to. |
| DataGuard | Access to the management of the DataGuard module functions | Yes/No | This right allows access to the DataGuard module components via the nVision administration console (in Delphi). If user does not have access to the console, this setting is ineffective. |
| | Access to the management of settings in Agent profiles (yes/no) | Yes/No | User can manage the Agent profiles and edit settings from the DataGuard module in them. |
| HelpDesk | Access to the management of the HelpDesk module functions | Yes/No | This right allows access to the HelpDesk module components via the nVision administration console and enables to grant the administrator rights in the ticket system. * Further options are only available when access to the module management is enabled. |

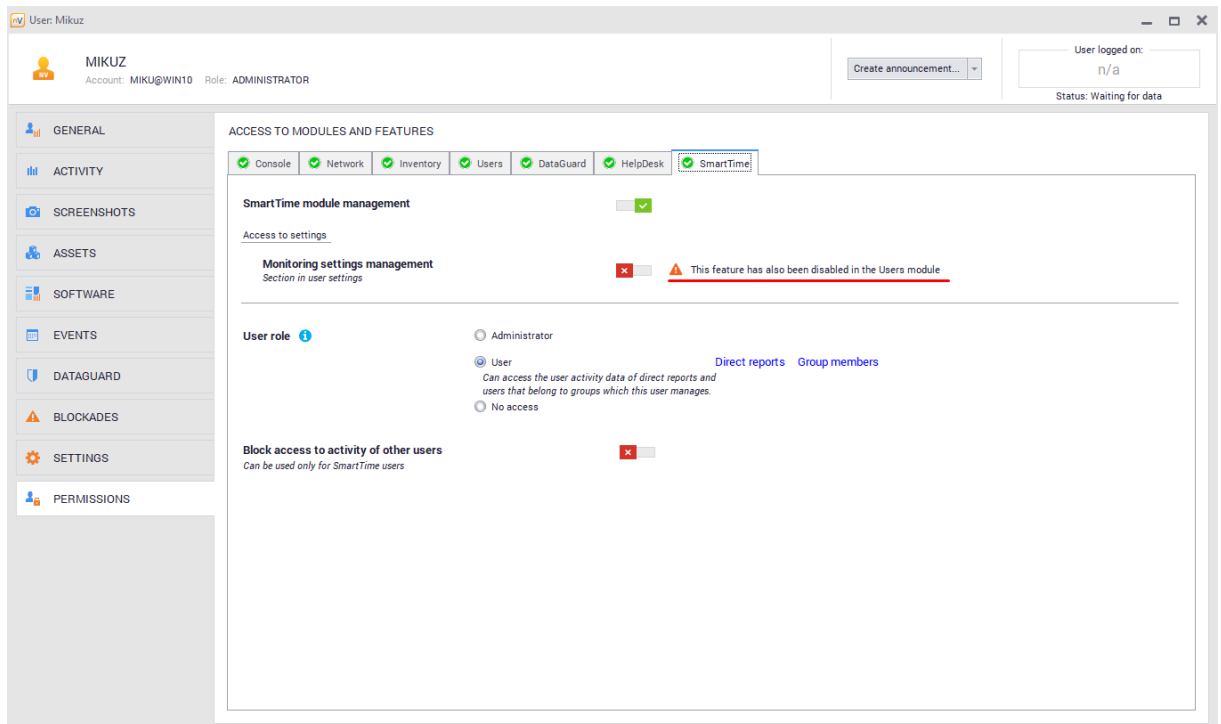
| Module/functionality | Right | Value | Description |
|----------------------|--|-------------------|---|
| | Access to the management of access settings * | Yes/No | User can manage the remote access settings for the users they have access to. |
| | Access to the management of desktop preview settings * | Yes/No | User can manage the desktop preview settings for the users they have access to. This setting is shared with the Users module (the function is available in both modules). |
| | Access to the file manager * | Yes/No | User can use the file manager function. This setting is shared with the Inventory module (the function is available in both modules). |
| | Access to remote management tools * | Yes/No | User can use the remote command execution, HelpDesk distribution task and process management functions. |
| | Level of rights in the ticket system | Administrator | This right is available to users that have access to the management of the HelpDesk module functions. Users with the administrator role have access to technical settings of the HelpDesk. |
| | | HelpDesk employee | Users with this role can perform operations related to ticket processing in the HelpDesk module. They can also plan their absences. |
| | | User | User with the user role can only create new tickets and view those for which they are observers. |
| | Level of rights in the Chat system | Full access | User can log in to the chat and make full use of its features. |

| Module/functionality | Right | Value | Description |
|----------------------|--|----------------------------------|--|
| | | Access to technical support only | <p>This right is only available if user has the “user” role in the ticket system.</p> <p>User can log in to the chat, but may use a limited number of its features.</p> <p>On the contact list, they can only see the users with the “administrator” or “HelpDesk employee” role in the HelpDesk, and can chat with them only.</p> <p>They can only be seen on the contact list by the users with the “administrator” or “HelpDesk employee” role.</p> |
| | | No access | <p>User cannot log in to the chat (when they try to log in, the message on lack of permissions is displayed). They cannot see the “Open chat” option in the Agent.</p> <p>A person with this right is also not shown on anybody’s contact list and cannot be chatted with.</p> |
| SmartTime | Access to the management of the SmartTime module functions | Yes/No | <p>This right allows access to the SmartTime module components via the nVision administration console and enables to grant the administrator rights in the web interface.</p> <p>* Further options are only available when access to the module management is enabled</p> |
| | Access to the management of monitoring settings * | Yes/No | <p>User can manage the monitoring settings for the users they have access to.</p> <p>This setting is shared with the Users module (the function is available in both modules).</p> |

| Module/functionality | Right | Value | Description |
|----------------------|---|---------------|--|
| | Level of rights in the web interface * | Administrator | <p>This right is only available when someone has full access to the management of users and access to the management of the SmartTime module functions.</p> <p>A person with this role can manage all technical settings on side of the SmartTime. They can also see the activity data of all users.</p> |
| | | User | <p>User has always access to their data.</p> <p>If they are set as group managers and have access to the group data enabled, they can manage the settings of their groups and see the activity data of their members.</p> <p>They can see the activity data of all their subordinates in the hierarchy.</p> |
| | | No access | <p>User cannot log in to the SmartTime interface (when they try to log in, the message on lack of permissions is displayed).</p> <p>They cannot see SmartTime links in any other part of the program.</p> <p>They are still shown as users in SmartTime and their data can be viewed by their superiors and the administrator.</p> |
| | Block access to data of any other users | Yes/No | <p>This setting is only available if the user's level of rights in the SmartTime web interface is set as "user".</p> <p>This option blocks the activity visibility for any other users and overwrites any rights resulting from the groups and from the hierarchy.</p> |

6.5.3 Interrelated permissions

When assigning rights to users, some settings are interrelated with one another in various modules. Enabling or disabling such a setting in one module will result in switching it to the same position in the interrelated module. A change in setting that is interrelated with other module will display the relevant message:



The table below presents the settings interrelated with one another in various modules: These settings are described in detail in chapter [Available rights](#).

| Interrelated modules | Right |
|---------------------------------|---|
| Inventory & HelpDesk | Access to file manager functions. |
| Users & HelpDesk | Management of remote access settings. |
| Users & SmartTime | Management of monitoring settings. |
| HelpDesk & Users | Management of desktop preview settings. |

6.5.4 Assigning permissions to user

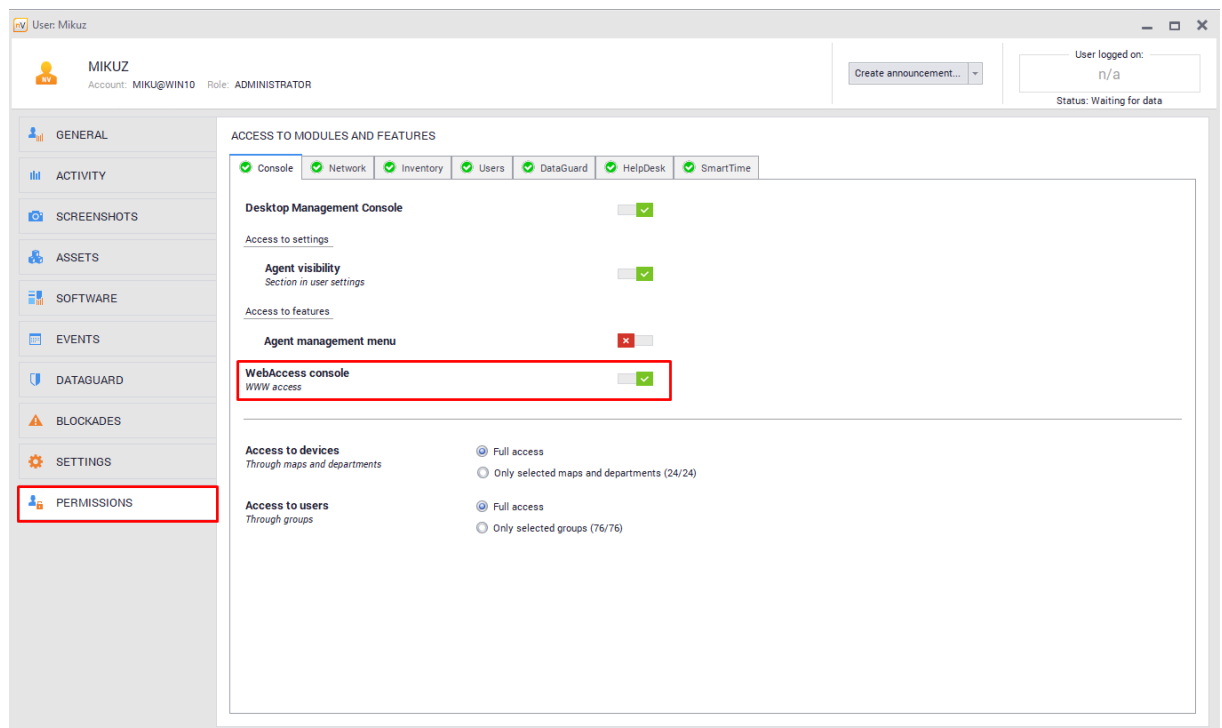
To manage rights of a specific user, you must log in to the built-in administrator account or to an account with the super administrator role.

A person with the super administrator role has always **unlimited access** to all functions of the program. Their access to modules, maps or users cannot be disabled selectively.

Note: The module access rights for the built-in Axence nVision Administrator account (i.e. the administrator whose account was created when you started nVision for the first time) cannot be changed.

✚ Modification of user with "Administrator" role

To modify the rights, navigate to the **User information** screen, and then to the **Permissions** tab:

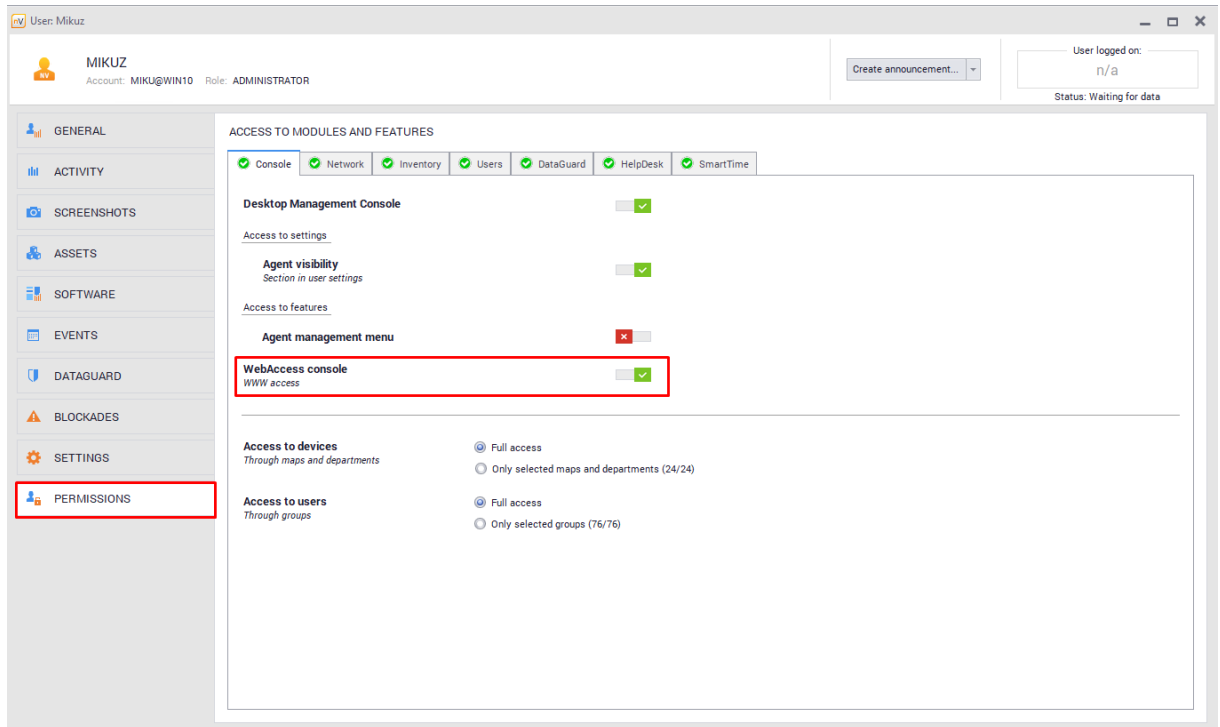


The screenshot displays the user management interface for user MIKUZ (Account: MIKU@WIN10, Role: ADMINISTRATOR). The 'PERMISSIONS' tab is selected in the left sidebar. The main content area shows 'ACCESS TO MODULES AND FEATURES' with a row of toggle switches for Console, Network, Inventory, Users, DataGuard, HelpDesk, and SmartTime, all of which are turned on. Below this, there are sections for 'Desktop Management Console', 'Access to settings', 'Agent visibility', 'Access to features', and 'Agent management menu'. The 'WebAccess console' (WWW access) is highlighted with a red box and is turned on. At the bottom, there are sections for 'Access to devices' and 'Access to users', each with radio button options for 'Full access' and 'Only selected'.

For users with the “administrator” role, it is possible to modify any rights described in chapter [Available rights](#).

✚ Modification of user with "User" role

To modify the rights, navigate to the **User information** screen, and then to the **Permissions** tab.



For accounts with the “user” role, it is possible to modify the following rights:

nVision Administration Console

- Access to the WebAccess console: **YES/NO**
- Access to maps and branches (only available if access to the WebAccess console is enabled).

HelpDesk module

Level of rights in the HelpDesk ticket system:

- HelpDesk employee,
- user.

Access to Chat:

- full access,
- access to technical support only (only available if the person in the ticket system has the “user” role),
- no access.

SmartTime module

Level of rights in the web interface:

- user,
- no access.

Block access to data of any other users: **YES/NO**

All settings are described in chapter [Available rights](#).

6.5.5 Default user permissions

It is possible to define the **default rights to be assigned to the newly created users and the users imported from Active Directory**. To do this, navigate to the **Users** tab, and then to the **Atlas information / Default rights** screen:

Axence nVision 11

Monitoring properties: Atlas

DATAGUARD

BLOCKADES

SETTINGS

DEFAULT PERMISSIONS

DEFAULT PERMISSIONS

Permissions automatically applied to all new users that are imported from Active Directory or created manually.

Administrator role

- Granted automatically for users that belong to the 'Domain Administrators' group
- Not granted automatically

SmartTime

- User
Can access the user activity data of direct reports and users that belong to groups which this user manages.
- No access

Chat

- Full access
- Technical support only i
- No access

Ticket system

- User

WebAccess console
WWW access

- No access

OK Cancel

6.5.6 Assigning permissions in bulk

To facilitate the configuration of rights for a significant number of users, you can use the option of assigning rights in bulk.

After you select a greater number of users by **right-clicking**, navigate to the **Properties** of selected accounts.

The **General** tab enables to define a superior for selected users, enable or disable them, and add selected persons to or delete from the group.

Note: Accounts imported from Active Directory do not allow the superior, group or account activity to be changed.

Multiple user properties

GENERAL

PERMISSIONS

BASIC INFORMATION

Supervisor: No change

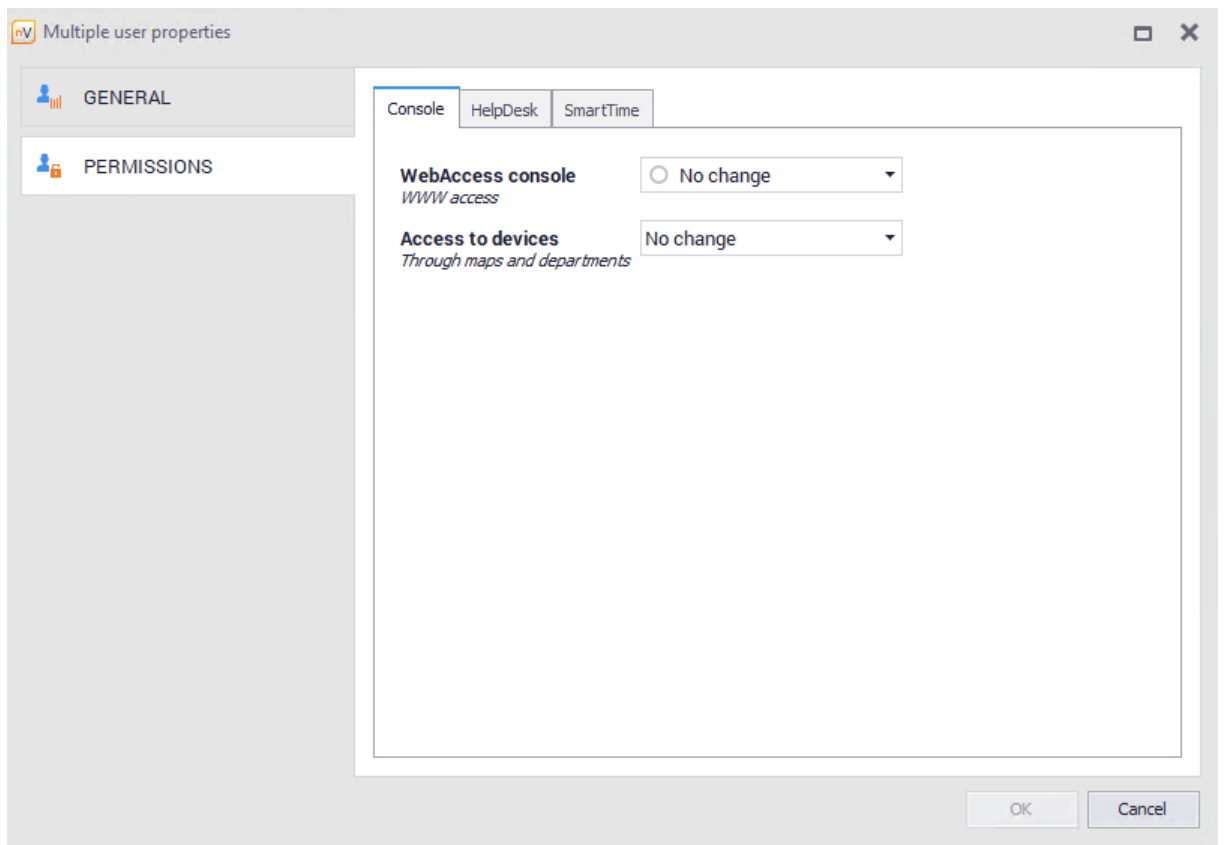
Account enabled: No change

Add all users to the following groups:

Add | Remove

OK Cancel

By using the **Permissions** tab, you can assign rights to selected parts of the program in bulk:



6.5.7 Migration of permissions from version 10

Below is described the way of migrating user rights for individual roles:

+ Role "User" in nVision 10

User is always migrated with the following settings:

- Role: "user"
- nVision administration console
 - Access to the WebAccess console: "no"
 - Access to maps and branches: "no"

HelpDesk module

- Level of rights in the HelpDesk ticket system: "user",
- Level of rights in the Chat system: "full access",

SmartTime module

- Level of rights in the web interface: "user",

Block access to data of any other users: "no".

± Role "HelpDesk employee" in nVision 10

HelpDesk employee is always migrated with the following settings:

- Role: "user".

nVision Administration Console

- Access to the WebAccess console: "yes",
- Access to maps and branches: the same settings as in the WebAccess configuration window in nVision 10.

HelpDesk module

- Level of rights in the HelpDesk ticket system: "HelpDesk employee",
- Level of rights in the Chat system: "full access",

SmartTime module

- Level of rights in the web interface: "user",

Block access to data of any other users: "no".

± Role "Administrator" in nVision 10

If user had the "Management of administrator rights" option enabled, they are always migrated as "super administrator" with the chat option enabled regardless of any other settings.

Otherwise, user is migrated to the normal administrator role and their settings are migrated as follows:

nVision Administration Console

- o Access to the nVision desktop console: "yes",
- o Access to the management of Agent visibility settings:
 - The same value as the "Management of the user monitoring and blocking settings" right in nVision 10,
- o Access to the Agent menu:
 - The same value as the "Allow for access to the Agent menu" in nVision 10,
- o Access to the WebAccess console: "yes",
- o Access to maps and branches:
 - If user had prior access to all objects, then "full access" is assigned. Otherwise, they only retain the objects they had access to in nVision 10,

o Access to users and groups:

- If user had prior access to all objects, then “full access” is assigned. Otherwise, they only retain the objects they had access to in nVision 10,

Network

o Access to the management of the Network module functions:

- The same value as the “Network” checkbox in the “Rights to the nVision modules” in version 10.

Inventory

o Access to the management of the Inventory module functions:

- The same value as the “Inventory” checkbox in the “Rights to the nVision modules” in version 10,

o Access to the management of settings in Agent profiles:

- If the “Inventory” checkbox in nVision 10 was set to “No”, this right is always migrated as “No”,
- Otherwise, this right has the same value as the “Management of Agent profiles” checkbox in nVision 10,

o Access to the file manager:

- If both the “Inventory” and the “HelpDesk” checkboxes in version 10 are set to “No”, this right is always migrated as “No”,
- Otherwise, the same value as the “Allow to use the file manager” checkbox in nVision 10.

o Access to the MSI package manager:

- If the “Inventory” checkbox in nVision 10 was set to “No”, this right is always migrated as “No”,
- Otherwise, this right has the same value as the “Allow to use the MSI package manager” checkbox in nVision 10.

Users

o Access to the management of the Users module functions:

- The same value as the “Users” checkbox in the “Rights to the nVision modules” in version 10,

o Access to the management of settings in Agent profiles:

- If the “Users” checkbox in nVision 10 was set to “No”, this right is always migrated as “No”,
- Otherwise, this right has the same value as the “Management of Agent profiles” checkbox in nVision 10,

o Access to the management of desktop preview settings:

- If both the “Users” and the “HelpDesk” checkboxes in version 10 are set to “No”, this right is always migrated as “No”,

- Otherwise, this right has the same value as the “Management of the user monitoring and blocking settings” checkbox in nVision 10,
- o Access to the management of monitoring settings,
- o Access to the management of blocking settings:
 - If the “Users” checkbox in nVision 10 was set to “No”, both rights are always migrated as “No”,
 - Otherwise, both rights have the same value as the “Management of the user monitoring and blocking settings” checkbox in nVision 10.

DataGuard

- o Access to the management of the DataGuard module functions:
 - The same value as the “DataGuard” checkbox in the “Rights to the nVision modules” in version 10,
- o Access to the management of settings in Agent profiles:
 - If the “DataGuard” checkbox in nVision 10 was set to “No”, this right is always migrated as “No”,
 - Otherwise, this right has the same value as the “Management of Agent profiles” checkbox in nVision 10.

HelpDesk

- o Access to the management of the HelpDesk module functions:
 - The same value as the “HelpDesk” checkbox in the “Rights to the nVision modules” in version 10,
- o Access to the management of remote access settings:
 - If the “HelpDesk” checkbox in nVision 10 was set to “No”, the rights are always migrated as “No”,
 - Otherwise, this right has the same value as the “Management of the user monitoring and blocking settings” checkbox in nVision 10,
- o Access to the management of desktop preview settings:
 - If both the “Users” and the “HelpDesk” checkboxes in version 10 are set to “No”, this right is always migrated as “No”,
 - Otherwise, this right has the same value as the “Management of the user monitoring and blocking settings” checkbox in nVision 10,
- o Access to the file manager:
 - If both the “Inventory” and the “HelpDesk” checkboxes in version 10 are set to “No”, this right is always migrated as “No”,
 - Otherwise, the same value as the “Allow to use the file manager” checkbox in nVision 10,
- o Access to remote management tools:

- If the “HelpDesk” checkbox in nVision 10 was set to “No”, the rights are always migrated as “No”,
 - Otherwise, this right has the same value as the “Allow to use the remote management tools” checkbox in nVision 10,
- o Level of rights in the ticket system:
- If the “HelpDesk” checkbox in nVision 10 was set to “Yes”, user is assigned the “administrator” role. Otherwise, they are assigned the “user” role.
- o Level of rights in the Chat system: always “full access”.

SmartTime

- o Access to the management of the Business View module functions:
- If user had the “Users” checkbox in the “Rights to the nVision modules” in nVision 10 and access to all users and groups, they are assigned the right to manage the Business View module,
 - In any other case, this setting is migrated as “No”,
- o Access to the management of monitoring settings:
- If user was assigned the right to manage the Business View module, this right has the same value as the “Management of the user monitoring and blocking settings” checkbox in nVision 10,
 - Otherwise, this setting is migrated as “No”,
- o Level of rights in the web interface:
- If user was assigned the right to manage the Business View module, they are assigned the “administrator” role. Otherwise, they are assigned the “user” role.
- o Block access to data of any other users: always “No”.

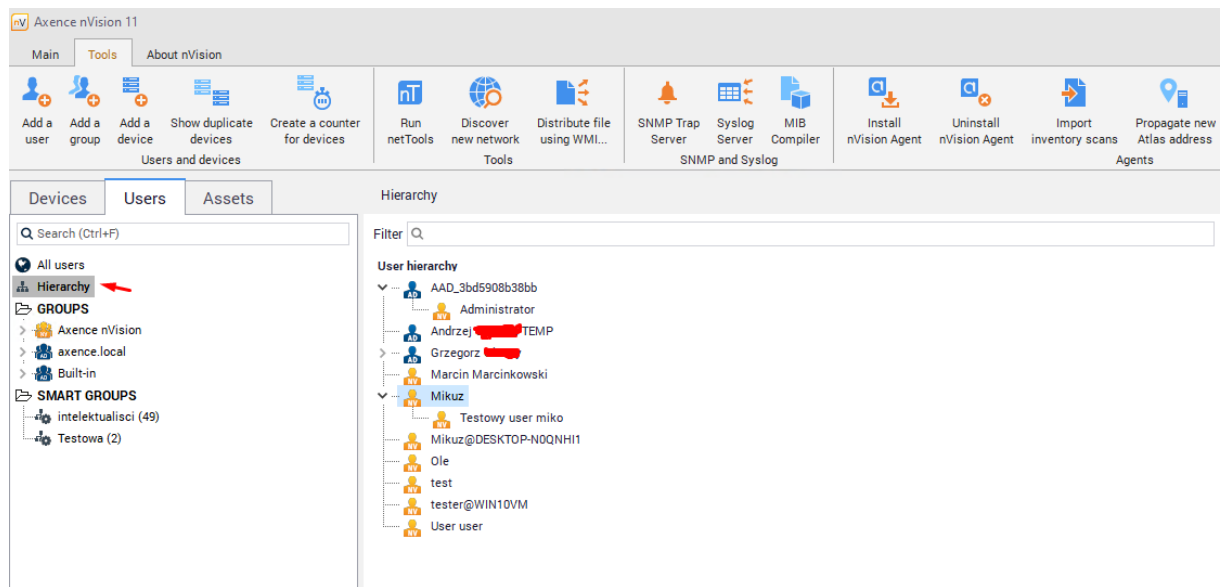
6.6 Hierarchy of users

The hierarchy of users was introduced in version 11 of nVision. It enables to determine the relationships among users.

Each user has the “superior” field, which may be left blank or contain exactly one user. The hierarchy of users is built only based on the relationships contained in this field. Any users that do not have a superior are located on the root level, but there is no relationship among them in the hierarchy.

This feature is closely related to the SmartTime module where a user that is higher in the hierarchy (superior) may have access to specific activities of a user that is lower in the hierarchy (subordinate). For more information about this relationship, refer to SmartTime chapter.

To view the hierarchy of users, click the **Hierarchy** button in the **Main / Users** tab:



Creating a hierarchy

The hierarchy of users can be created in two ways:

The first one is to **drag and drop users in the hierarchy view**. Please note that you cannot change the superiors/subordinates of the users downloaded from Active Directory.

The second way is to define the superior in the user information screen. To do this, navigate to this screen for the selected user and modify the “superior” field:

The screenshot displays the Axence nVision 11 user management interface. The top navigation bar includes 'Main', 'Tools', and 'About nVision'. Below this, there are several tool icons for tasks like 'Generate protocol', 'MSI packages manager', 'Print bar codes', 'Assets settings', 'Application categories', 'Manage templates', 'Configure license type', 'Audit', 'Manage device permissions', 'Manage trustee permissions', 'Printout audit', 'Configure print cost', 'Reports', 'View events', 'Alerts', 'Distribution tasks', and 'Announcements HelpDesk'.

The main interface is divided into 'Devices', 'Users', and 'Assets' tabs. The 'Users' tab is active, showing a search bar and a 'Hierarchy' section. The hierarchy tree on the left shows a structure under 'Axence nVision' with groups like 'Structure', 'IT', 'test', and 'marketing'. The 'test' group is expanded, showing 'Programmers' and 'marketing' sub-groups. The 'marketing' group is selected, showing a list of users including 'Mikuz'.

The user profile for 'Mikuz' is displayed on the right. It includes the following information:

- GENERAL:** MIKUZ, Account: MIKU@WIN10, Role: ADMINISTRATOR
- USER INFO AND STATUS:**
 - User name: Mikuz
 - Full name: [Empty]
 - E-mail address: mikolaj.matuszny@axence.r
 - Account enabled:
 - Password: [Change](#)
 - Created: 02.07.2019 14:17:40
 - Last login: 23.03.2020 10:22:12
 - Phones: [Empty]
- ROLE AND PERMISSIONS:** [Change permissions](#)
 - Role: Administrator
 - Job title: [Empty]
 - SmartTime: User
 - Ticket system: HelpDesk Staff
 - Chat: Full access
 - WebAccess: Yes
- Accounts and groups:**
 - Account type: nVision
 - Supervisor: Administrator
 - Direct reports: 1 | [Show](#)
 - Linked accounts: Miku@DESKTOP-39LPDOO
 - Belongs to groups (4) | Is manager of (0)
 - marketing
 - Programmers

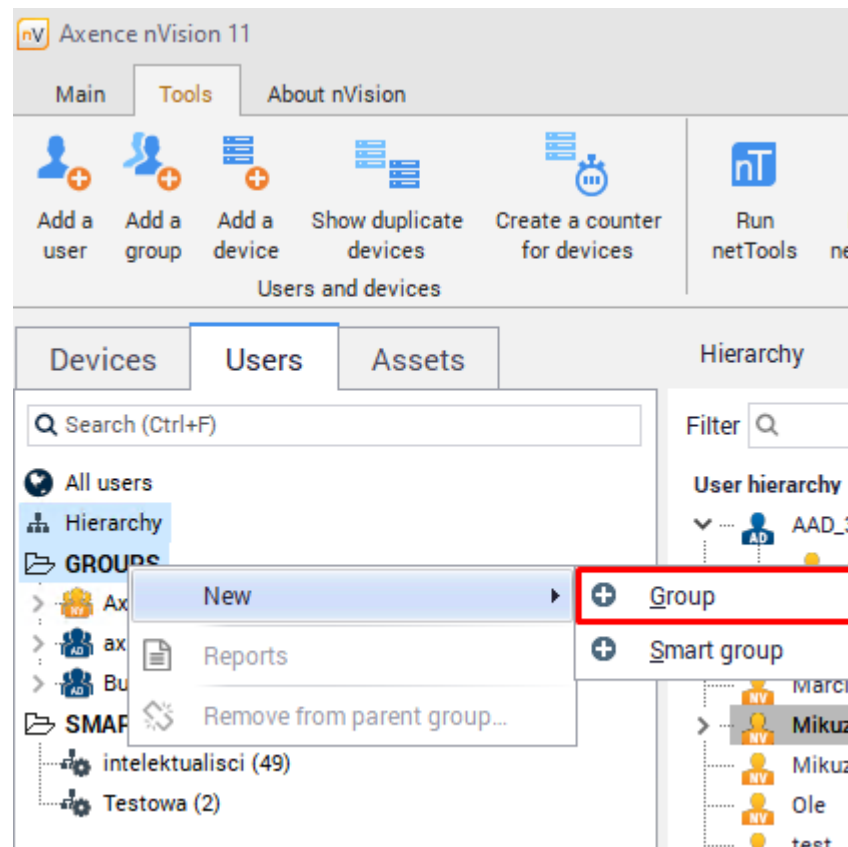
6.7 User groups

6.7.1 User groups

Groups allow to entering a greater number of users into a single organizational unit. This may prove useful when you want to assign access to a corporate pendrive or block access to web pages for greater group of users.

Adding a group

To add a group, right-click the **Groups** button, and then select **New / Group** from the context menu.



Adding users to a group

Users can be added to groups in the group property screen for the given group or directly in the user information screen for the selected user.

Group: test

test
Manager: No manager

GENERAL

DATAGUARD

BLOCKADES

SETTINGS

INFORMATION

Name: Manager:

Created: 18.02.2020 15:01:16 Access to activity:

Type: Axence nVision

Domain: -

Users and groups

Users in the group:

<No data to display>

[Add](#) | Remove

Belongs to groups | [Subgroups](#)

<No data to display>

[Add](#) | Remove

User: Mikuz

MIKUZ
Account: MIKU@WIN10 Role: ADMINISTRATOR

Create announcement...

User logged on: n/a
Status: Waiting for data

GENERAL

ACTIVITY

SCREENSHOTS

ASSETS

SOFTWARE

EVENTS

DATAGUARD

BLOCKADES

SETTINGS

PERMISSIONS

USER INFO AND STATUS

User name: Role: Application: -

Full name:

Job title:

E-mail address: SmartTime: User

Account enabled:

Ticket system: HelpDesk Staff

Password: [Change](#) Chat: Full access

Created: 02.07.2019 14:17:40 WebAccess: Yes

Last login: 23.03.2020 10:22:12

Phones:

Accounts and groups

Account type: nVision

Supervisor:

Direct reports: 1 | [Show](#)

Linked accounts:

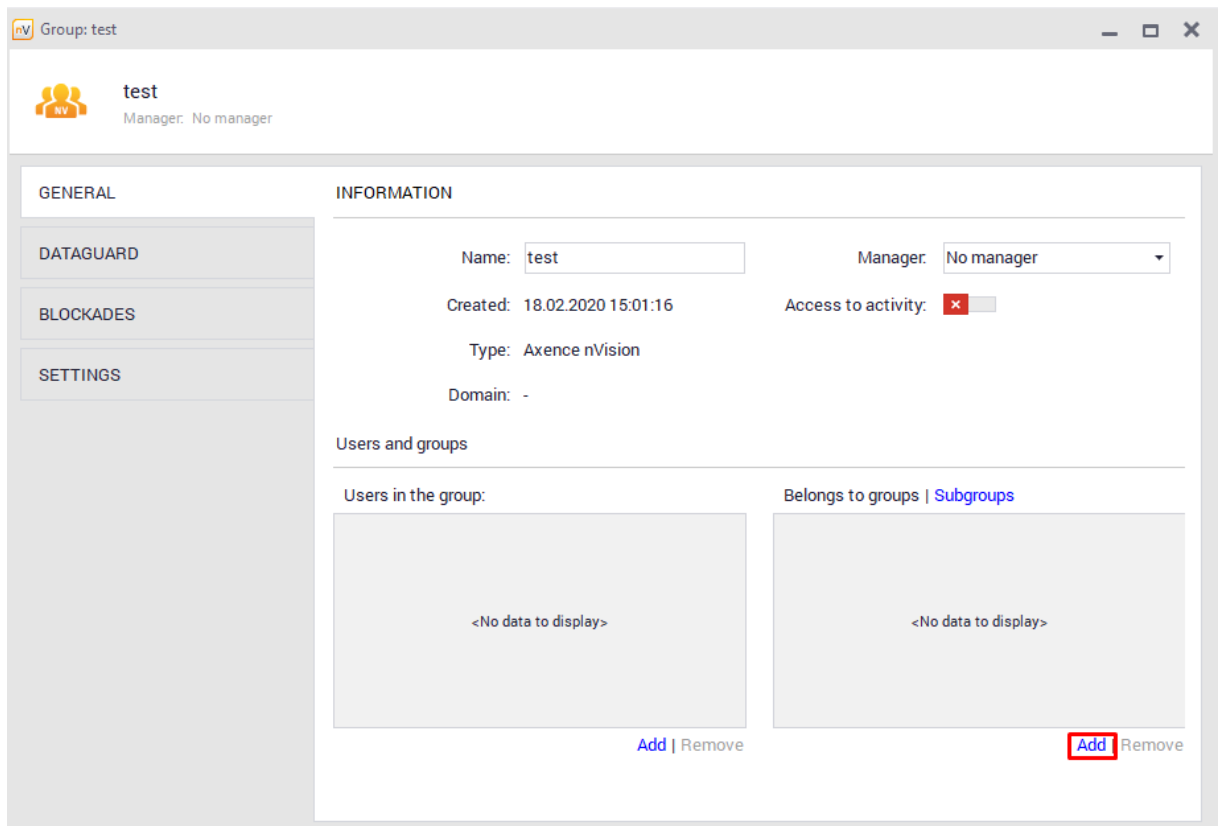
Miku@DESKTOP-39LPD00
Miku@WIN10

Belongs to groups (3) | Is manager of (0)

[Add](#) | Remove

Subgroups

Subgroups are lower in the hierarchy than the selected group. They allow inheriting settings from the parent group and modifying selected settings. A subgroup can be defined in the group property screen.



Group settings

When in the group property screen, you can modify the following attributes:

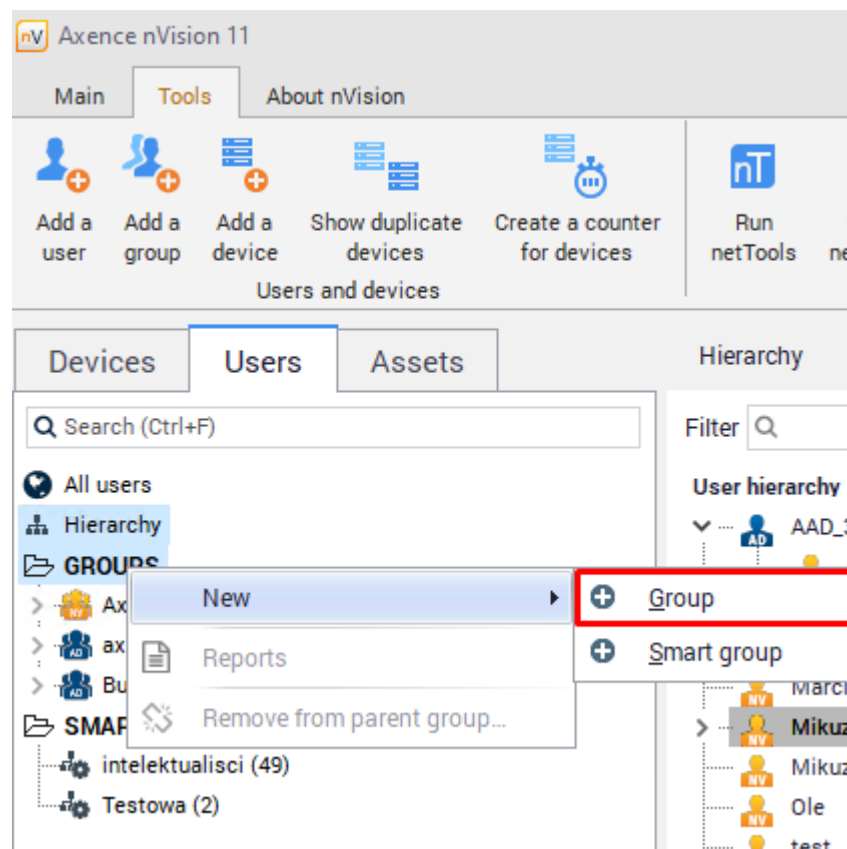
- Group name,
- Group manager – this feature is connected with the SmartTime module. Group manager has access to their own data as well as data of the entire group and individual members. This user can also edit the group productivity exceptions. If they edit productivity exceptions for such a group, they can see the global list of applications, their productivities and categories, however they cannot edit these items. For more information, refer to this [chapter](#).
- Group members,
- Subgroups,
- DataGuard module settings,
- Filtering websites, blocking applications and downloaded files,
- Monitoring, remote desktop and Agent visibility settings.

6.7.2 Smart groups

Smart groups differ from normal groups of users in that they are created dynamically. To create a smart group requires the definition of certain conditions to be met by users to be added to this group.

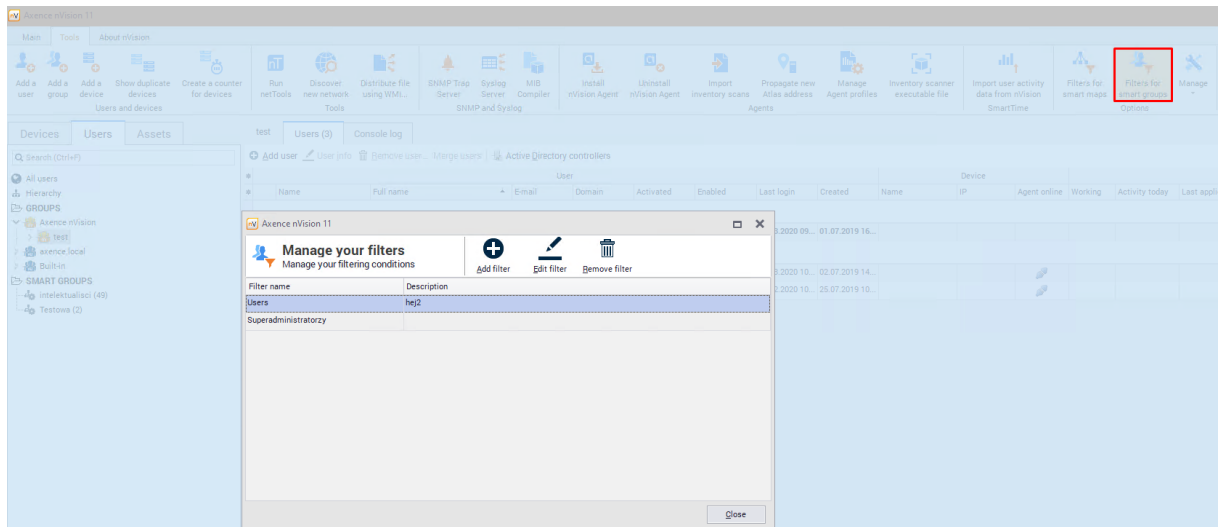
Creating a smart group

To add a smart group, right-click the **Groups** button, and then select **New / Smart group** from the context menu.



Creating a smart group filter

The next step is to create a filter. To do this, select **Filters for smart groups** on **Tools** tab or click **Add** near filter field while creating Smart Group



With the above filter in place, users with the “super administrator” role whose names begin with “A” will be added to the smart group.

Refresh time

The last step is to define the interval for checking the conditions defined in filters. The default setting is 5 minutes.

Part



7 Users module

7.1 Introduction

Axence nVision® is equipped with an Agent designed to monitor user activity on Windows workstations. It collects the following information:

- Activity/inactivity time. Inactivity (break) is the time, when the user does not press any keys and does not move the mouse.
- Application usage time. This is grouped for easier analysis of the user activity.
- Visited web pages. The Agent analyzes low level network information to get this list.
- Hardware and software inventory (see the 'Hardware and software inventory' chapter).
- Data on sent e-mail messages.
- Printing information.

The Agent automatically sends the information about user activity every 1 hour. The hardware inventory is scanned every 24 hours.

User activity monitoring requirements

In order to collect user activity information, you have to install the nVision Agent on the remote host (which will also enable nVision to collect the inventory). You also have to open TCP port 4434 on the computer running nVision. Please refer to [Requirements and configuration](#)^[27] topic for more information.

Please note, that all the communication between Agents and nVision requires authorization and no data may be communicated if the Agents and nVision are properly configured.

User activity information

1. Open the **User info** window.
2. Go to the **User activity** tab.
3. Select the page you would like to see:
 - Summary,
 - Work time,
 - Applications,
 - Websites,
 - Printouts,
 - E-mails,
 - Bandwidth usage.

4. Select the time period of the presented data.

It is possible to view data concerning all users who were using this computer by expanding the **Users** menu in the upper part of the window.

Computers with DHCP assigned address

When a computer has a new IP address assigned by DHCP, then it will be updated in the nVision database upon a connection between the Agent and nVision. Therefore, you do not have to do that manually.

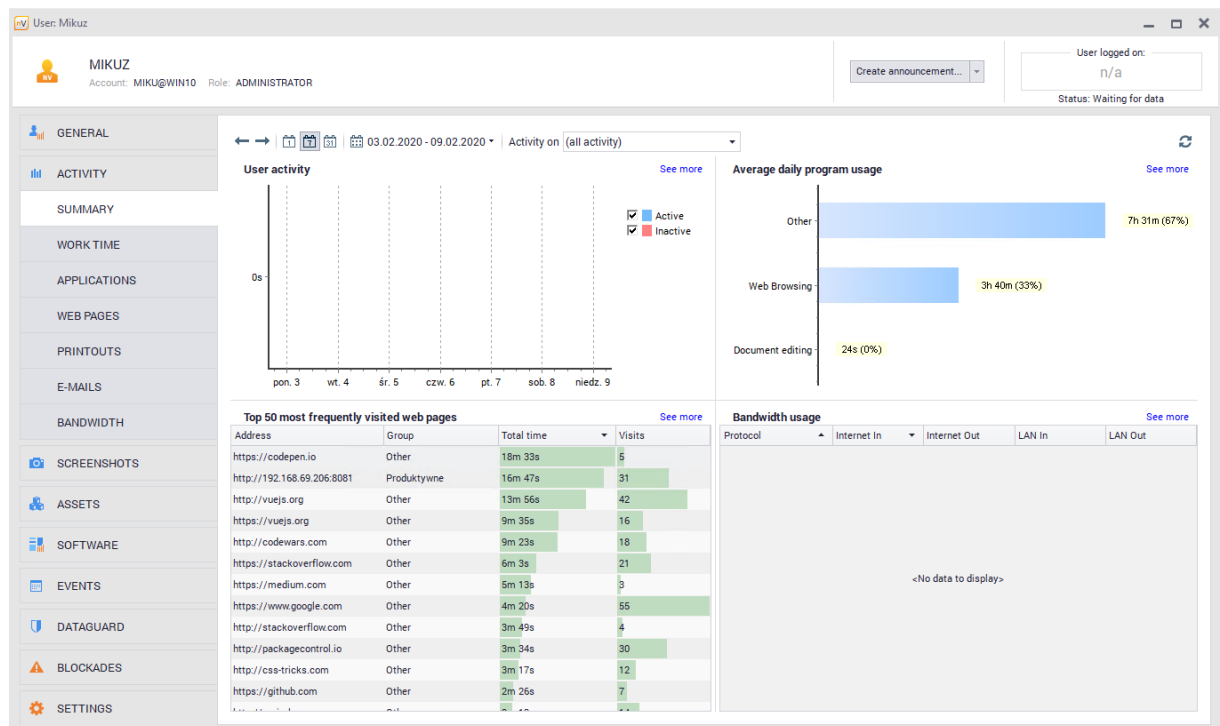
7.2 Overview

To view general information about user activity, go to the **User info** window, **User activity / Summary** tab.

Also, find out about the [monitoring settings](#)^[30] model.

This tab shows information about:

- user activity (active/inactive time),
- average daily program usage by groups configured in [nVision options](#)^[42],
- top 50 most frequently visited web pages,
- bandwidth usage in the local network and the Web, with a division into inbound and outbound traffic.



More details about network traffic can be found in the **Bandwidth usage** tab.


7.3 Blocking access to selected applications

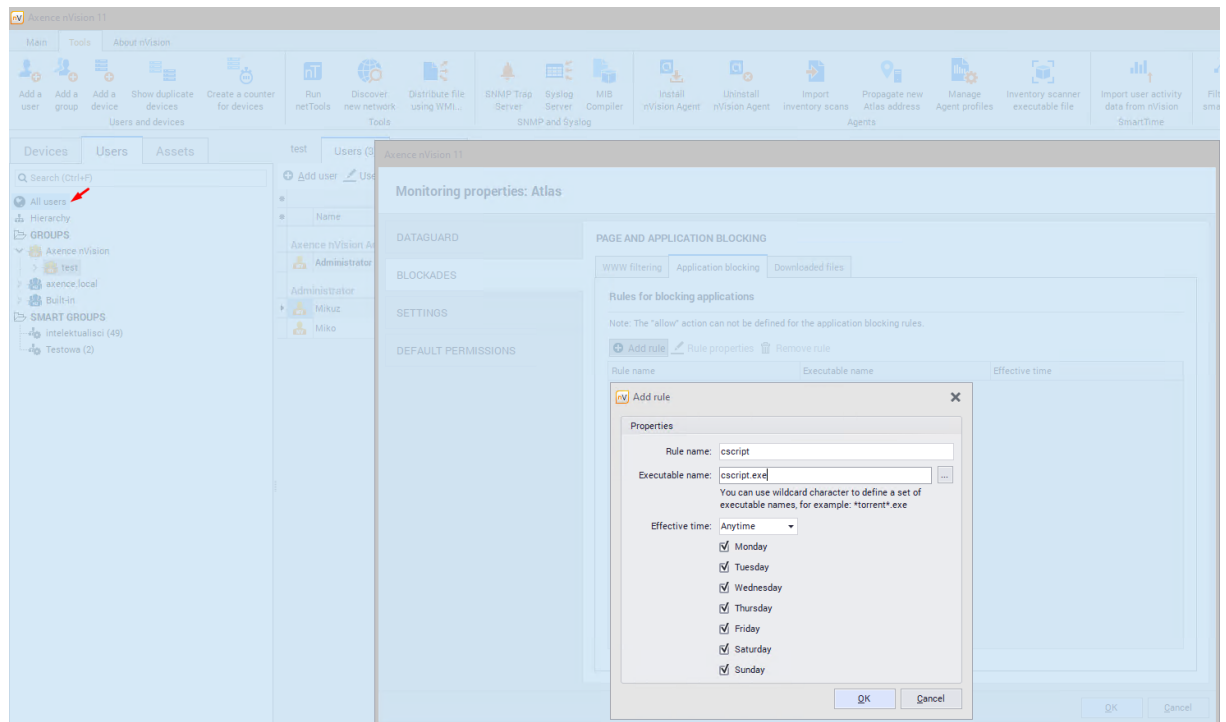
Applications can be blocked for a workstation with an installed nVision Agent by the proper configuration of the Agent. By default, all applications can be executed.

The model blocking settings are presented in the [Blocking settings](#)^[33] chapter.

Blocking applications

To block an application:



1. Navigate to the **Atlas information**, **Group information** or **User information** window. Switch to the **Blockades** tab.
2. Open the **Blocking applications** page.
3. Click the  **Add rule** button.
4. Enter the rule name, executable file name and effective time. Click **OK**.

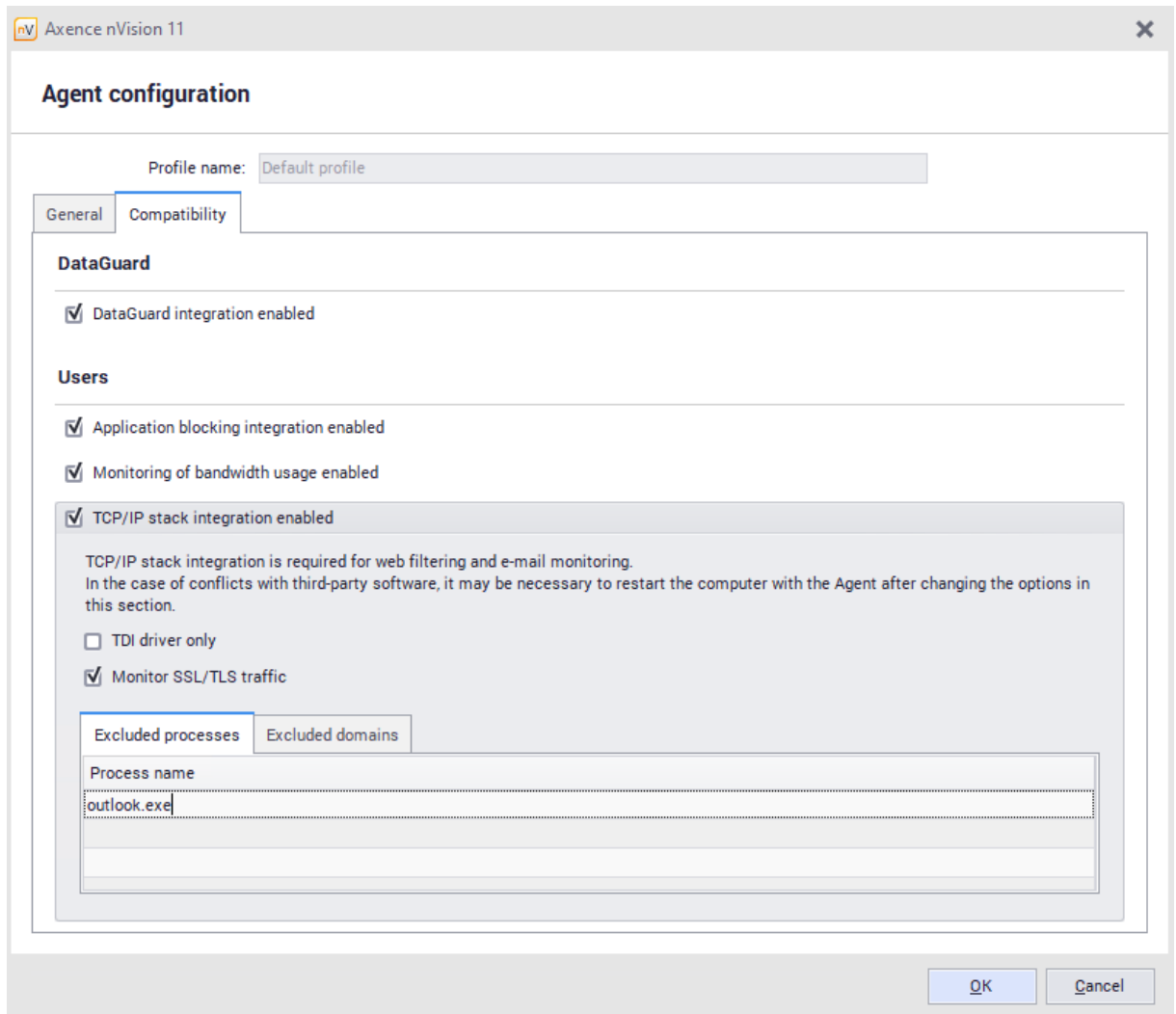


In the [nVision options](#) ^[42], you can configure the text of the notification to be shown to users when they make an attempt to start a blocked application.

Excluding processes from blocking rules in the Agent profile

To exclude processes for all the devices used, you must properly configure the Agent profile.

1. Navigate to the **Tools and options** tab, and then to the **Manage Agent profiles** menu.
2. Select the Agent profile to be edited  or create a new one  that will suit your needs.
3. In the **Edit** window, navigate to the **Compatibility** tab, and then to the **Excluded processes** tab.
4. Add the processes to be blocked and confirm with **OK**.



7.4 Blocking access to selected websites

Websites can be blocked for a workstation with an installed nVision Agent by means of Agent profiles. By default, all websites can be accessed. To enable blocking, toggle on the integration with TCP/IP stack in the **Compatibility and performance** tab. To learn how to do this, see the chapter [I cannot block websites](#)^[130].

The following protocols are supported at the moment: HTTP, HTTPS, SMTP:25, SMTP:587, SMTP via SSL, POP3 via SSL and POP3:110. The following protocols are not supported at the moment: IMAP, MAPI.

Blocking access to websites

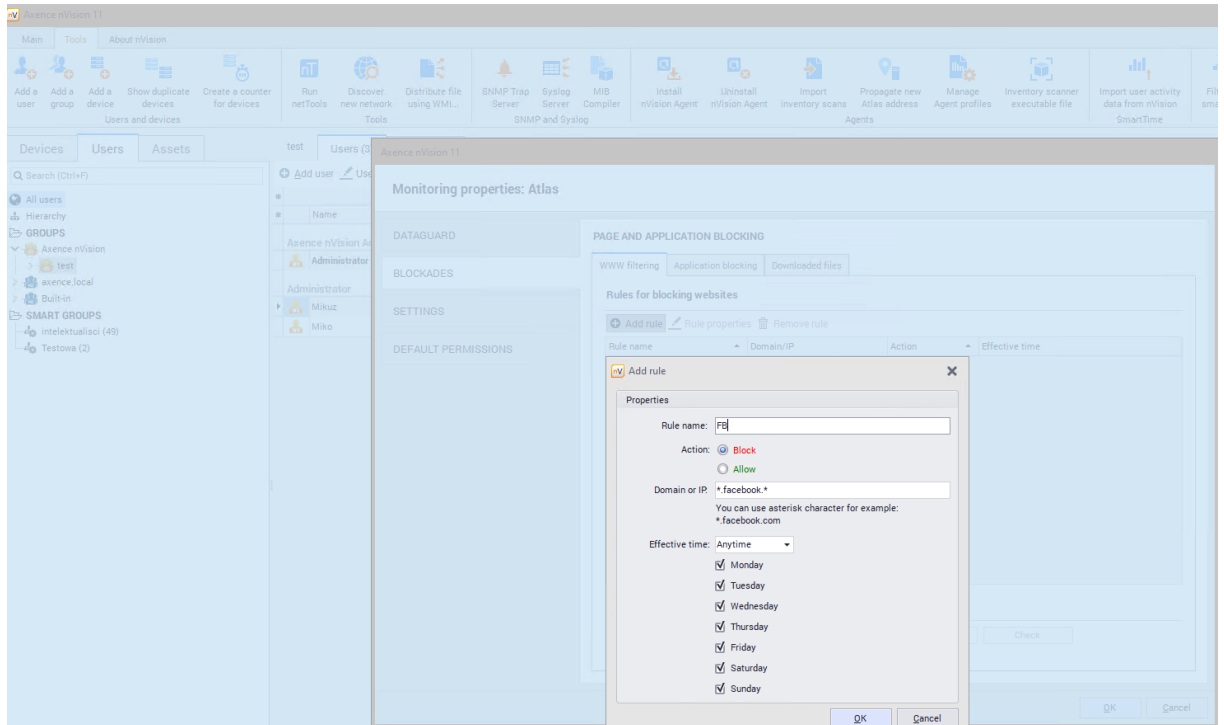
The model blocking settings are presented in the [Blocking settings](#)^[33] chapter.

To block access to a website:

1. Navigate to the **Atlas information**, **Group information** or **User information** window. Switch to the **Blockades** tab.
2. Select the **Web filtering** page.
3. Click the **Add rule** button.



4. Enter the rule name, select the **Block** action and enter an IP address or domain to be blocked. An example of the rule is shown on the image below.

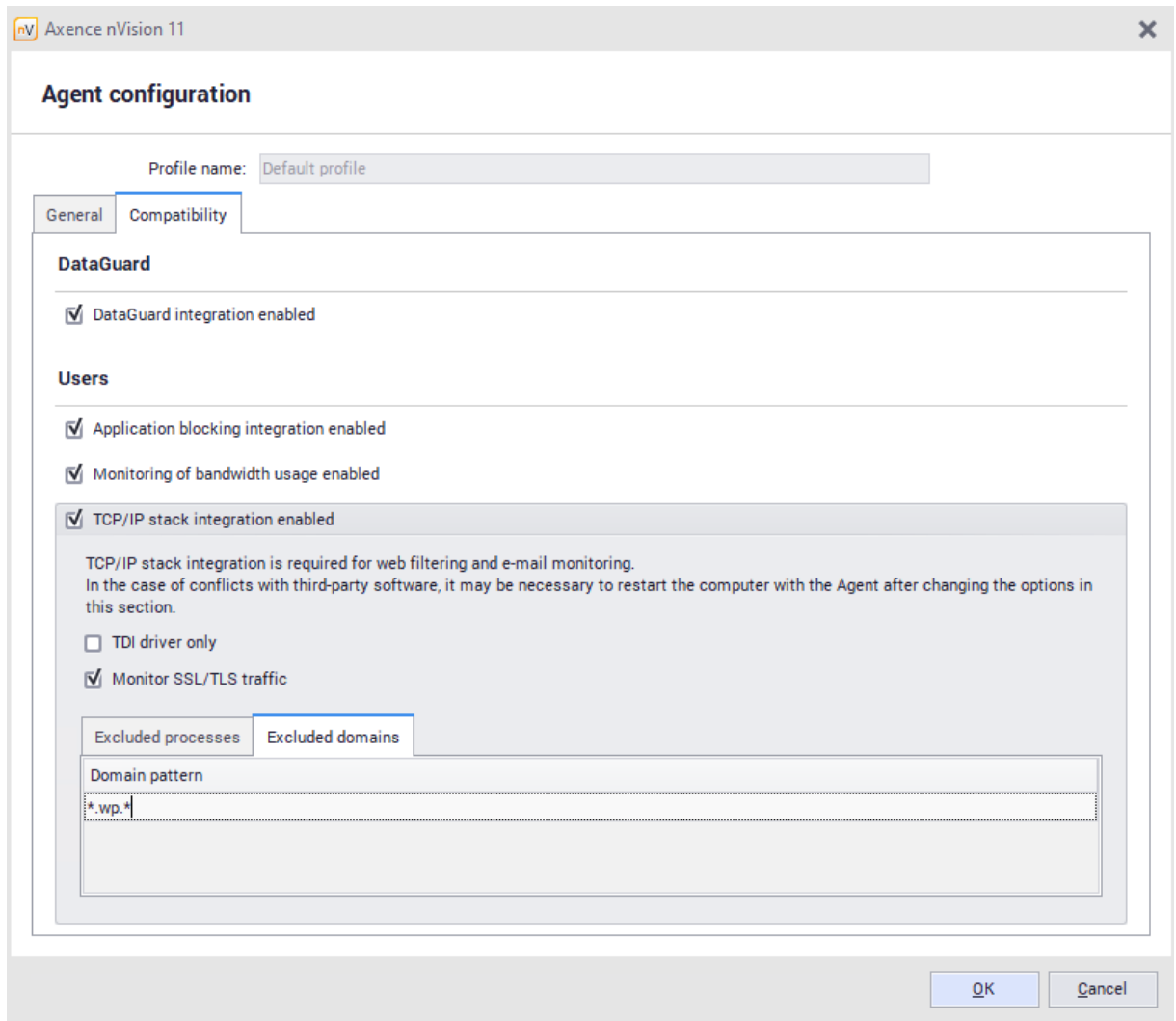
In the [nVision options](#) ^[42], you can configure the text of the notification to be shown to users when they visit a blocked website.



Excluding domains from blocking rules in the Agent profile

To exclude domains for all the devices used, you must properly configure the Agent profile.

1. Navigate to the **Tools and options** tab, and then to the **Manage Agent profiles** menu.
2. Select the Agent profile to be edited  or create a new one  that will suit your needs.
3. In the **Edit** window, navigate to the **Compatibility** tab, and then to the **Excluded domains** tab.
4. Add a domain to be blocked and confirm with **OK**.



Time window

It is possible to set the time window (hours and days) when the given website will be blocked. For example, you can block access on business days during working hours. Thus, outside of the time window devoted to work, the user will be able to access the blocked website.

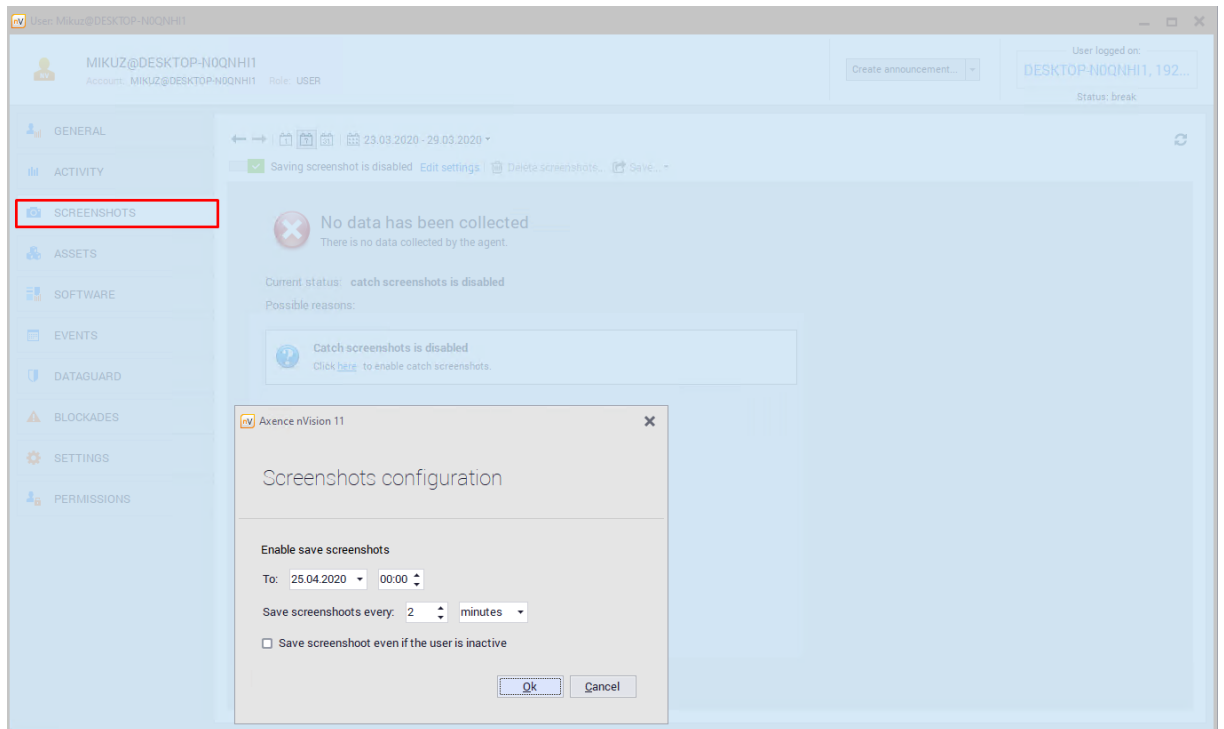
Problems


If any problems with blocking websites occur, see the chapter [I cannot block websites](#)^[130] to find a solution.

7.5 Screenshots

Saving screenshots is disabled by default. If you want to save screenshots cyclically:

1. Go to the **Screenshots** tab in the **User info** window.
2. If there is no data collected and the Agent is installed, **Enable screenshots saving**.



3. Set how often and until when you want the screenshots to be taken.
4. Wait for Agent to send data or refresh .
5. You can view screenshots and save them as *.jpeg files.

7.6 E-mails

If you want to monitor e-mails, enable this option in Agent settings (see [Agent settings](#)^[125]).

If you encounter any problems with monitoring e-mails, refer to [I cannot block websites and monitor e-mails](#)^[130] topic.

Monitoring e-mails is only possible for machines with the installed Agent and enabled integration with the TCP/IP stack.

The following protocols are supported at the moment:

- SMTP:25,
- SMTP:587,
- SMTP via SSL,
- POP3 via SSL,
- POP3:110.

The following protocols are not supported at the moment: IMAP, MAPI.

Important: Monitoring covers inbound and outbound mail. Sender, recipient, subject and size are recorded. Mail content is not monitored.

7.7 Printouts

7.7.1 Printout monitoring

It is possible to monitor printing on machines with installed Agents (if the appropriate option in the [monitoring settings](#) ^[30] is marked).

To enable printout monitoring:

1. Navigate to the Settings window for the Atlas or group or to the User info window.
2. Go to the **Settings** tab.
3. In the **Printouts** option, select **Monitor**.

The screenshot shows a web interface for user settings. The user is MIKUZ@DESKTOP-NOQNH11, with account MIKUZ@DESKTOP-NOQNH11 and role USER. The interface is titled 'MONITORING PROFILE AND SETTINGS'. The 'Monitoring' section includes the following settings:

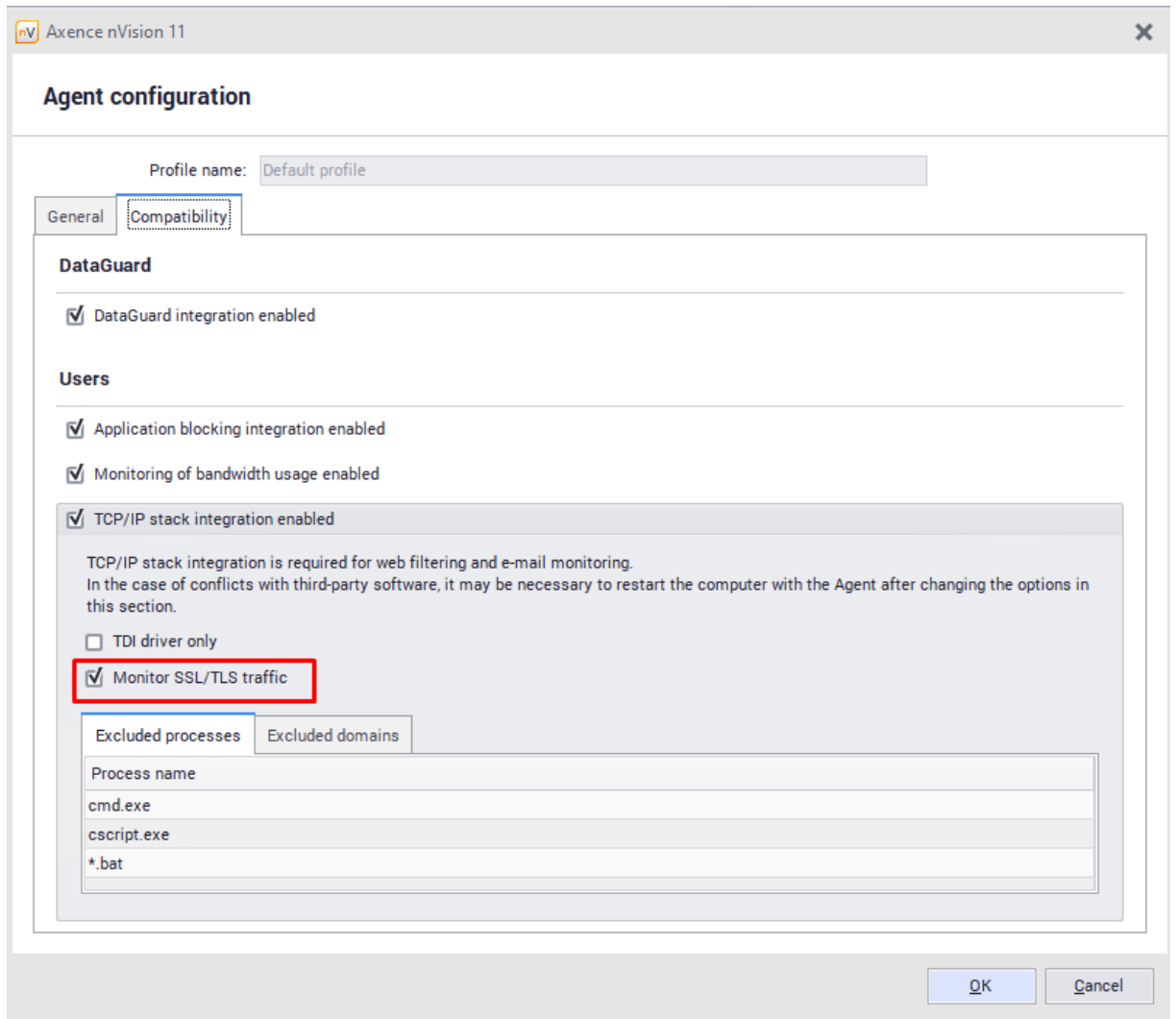
| Setting | Value | Source |
|-------------------------|----------------------------|----------------------|
| Application usage | Monitor (inherited) | Inherited from Atlas |
| Visited web pages | Monitor (inherited) | Inherited from Atlas |
| Printouts | Monitor (inherited) | Inherited from Atlas |
| Emails | Monitor (inherited) | Inherited from Atlas |
| Bandwidth usage | Do not monitor (inherited) | Inherited from Atlas |
| Work time | Do not monitor (inherited) | Inherited from Atlas |
| Breaks in activity | Monitor (inherited) | Inherited from Atlas |
| Save breaks longer than | Settings (inherited) | Inherited from Atlas |

The 'Time of monitoring' section includes:

| Setting | Value | Source |
|------------|----------------------|----------------------|
| Time range | Settings (inherited) | Inherited from Atlas |

The 'Time range' is set to 'Between 08:00:00 to 15:59:00' with checkboxes for days of the week: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday.

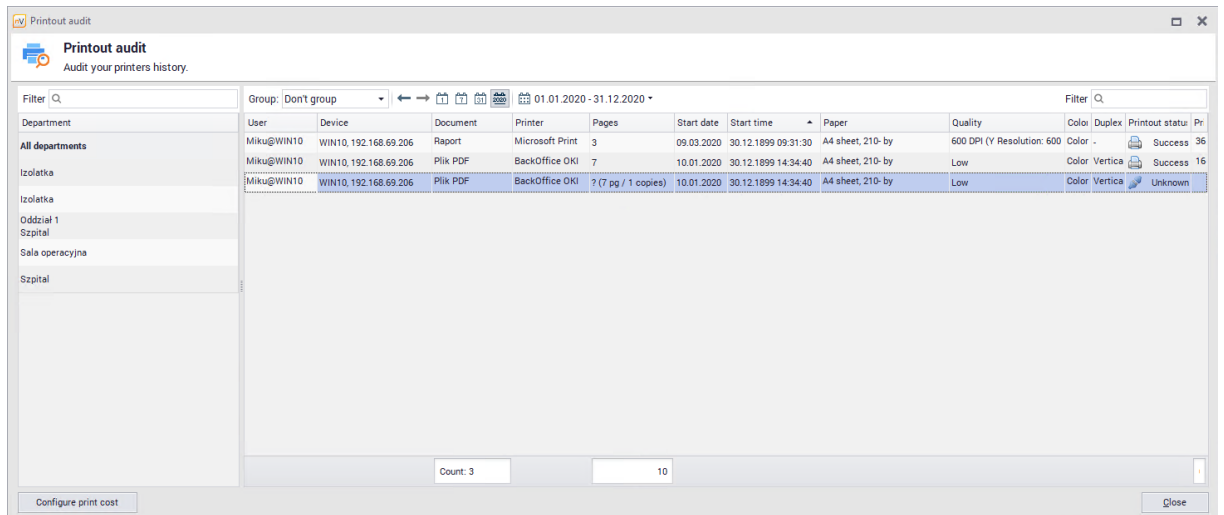
If the mail server uses SSL/TLS encryption, you need to select the relevant option in the Agent profile to monitor correspondence:



7.7.2 Printout audit

The printout audit window allows the printing history in selected periods to be viewed (day, week, month or year). Data are sorted in chronological order. To facilitate searching for necessary information, grouping options are available – by users, devices and printers.

To perform a printout audit, click **Printout audit** on the ribbon (in the **Main** page). The **Printout audit** window will open.



The screenshot shows the 'Printout audit' window with a table of print jobs. The table has columns for User, Device, Document, Printer, Pages, Start date, Start time, Paper, Quality, Color, Duplex, and Printout status. The data is as follows:

| User | Device | Document | Printer | Pages | Start date | Start time | Paper | Quality | Color | Duplex | Printout status |
|------------|-----------------------|----------|-----------------|---------------------|------------|---------------------|-------------------|----------------------------|-------|---------|-----------------|
| Miku@WIN10 | WIN10, 192.168.69.206 | Raport | Microsoft Print | 3 | 09.03.2020 | 30.12.1899 09:31:30 | A4 sheet, 210- by | 600 DPI (Y Resolution: 600 | Color | - | Success 36 |
| Miku@WIN10 | WIN10, 192.168.69.206 | Plik PDF | BackOffice OKI | 7 | 10.01.2020 | 30.12.1899 14:34:40 | A4 sheet, 210- by | Low | Color | Vertica | Success 16 |
| Miku@WIN10 | WIN10, 192.168.69.206 | Plik PDF | BackOffice OKI | ? (7 pg / 1 copies) | 10.01.2020 | 30.12.1899 14:34:40 | A4 sheet, 210- by | Low | Color | Vertica | Unknown |

If the printout data are not collected, even though the computers with Agents have the printout monitoring options checked, see the section [Users' printouts are not monitored](#)⁶⁴⁸.

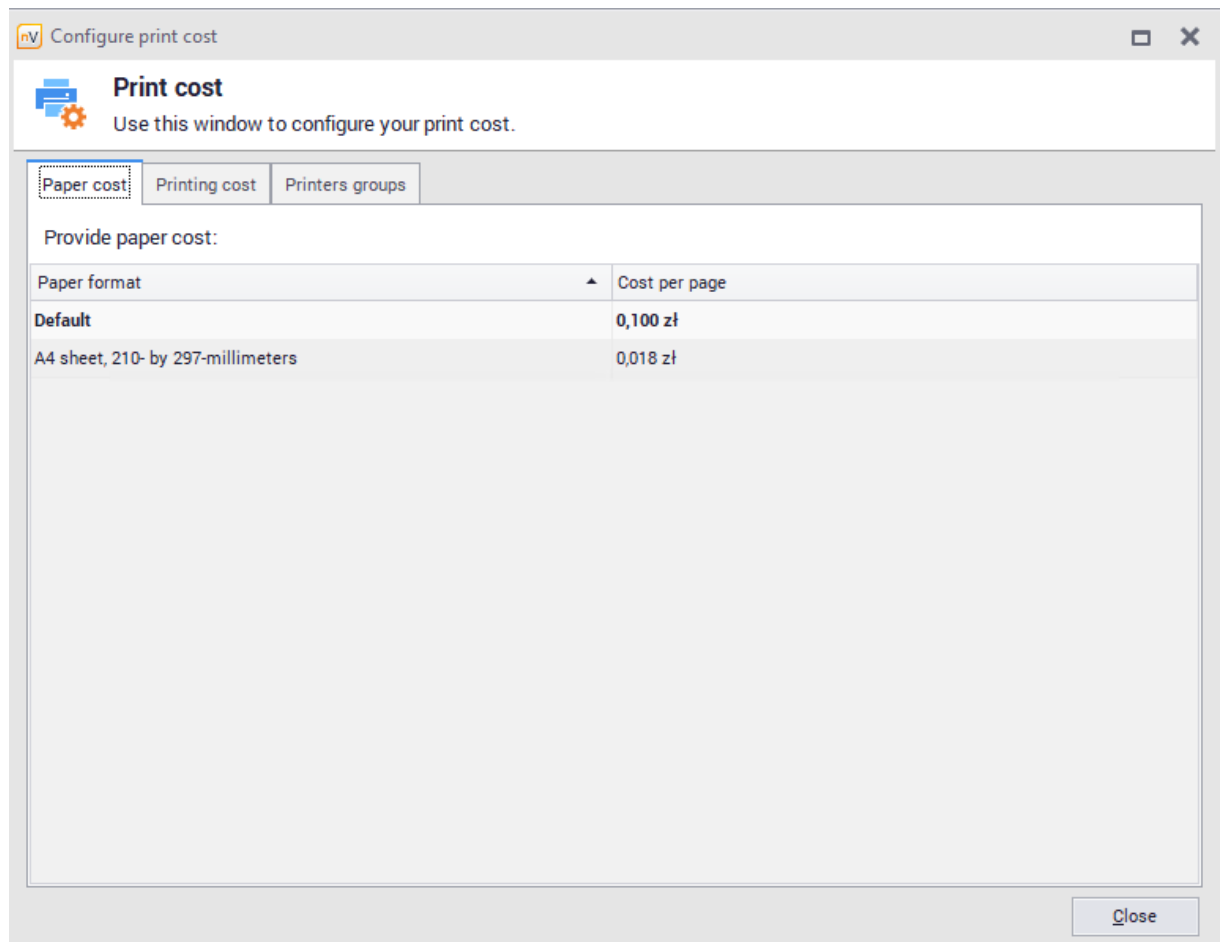
7.7.3 Printing costs

Printout monitoring allows the costs borne in relation to document printing to be discovered. To ensure the proper cost assessment, configure the expenses, including the costs of paper and printing on specific printers.

Configuration

To configure the printing costs:

1. Select **Configure printing costs** in the menu bar (in the **Main** page). You can also do this from the level of the **Printout audit** window by means of the appropriate button. In both cases the **Configure print cost** window will open.
2. In the **Paper cost** tab specify the costs for paper formats (A3, A4, A5, envelope). The cost specified in the **Default** cell will be used for all formats for which the specific cost is not determined.



3. In the **Printing cost** tab specify the printing costs for specific printers. You can also specify different costs for black and white and color printouts or use default values. If the printer does not have a color mode, right-click to mark the appropriate option.

Print cost
Use this window to configure your print cost.

Paper cost | **Printing cost** | Printers groups

Provide print cost of a single page per printer toner/ink:

| Paper format | Cost of 1 page (b/w) | Cost of 1 page (color) |
|---|----------------------|------------------------|
| Default | | |
| A4 sheet, 210- by 297-millimeters | <i>Default</i> | 123,000 zł |
| BackOffice OKI MC352 (przekierowana sesja: 2) | | |
| A4 sheet, 210- by 297-millimeters | <i>Default</i> | 23,000 zł |
| Microsoft Print to PDF | | |
| A4 sheet, 210- by 297-millimeters | <i>Default</i> | <i>Default</i> |

Close

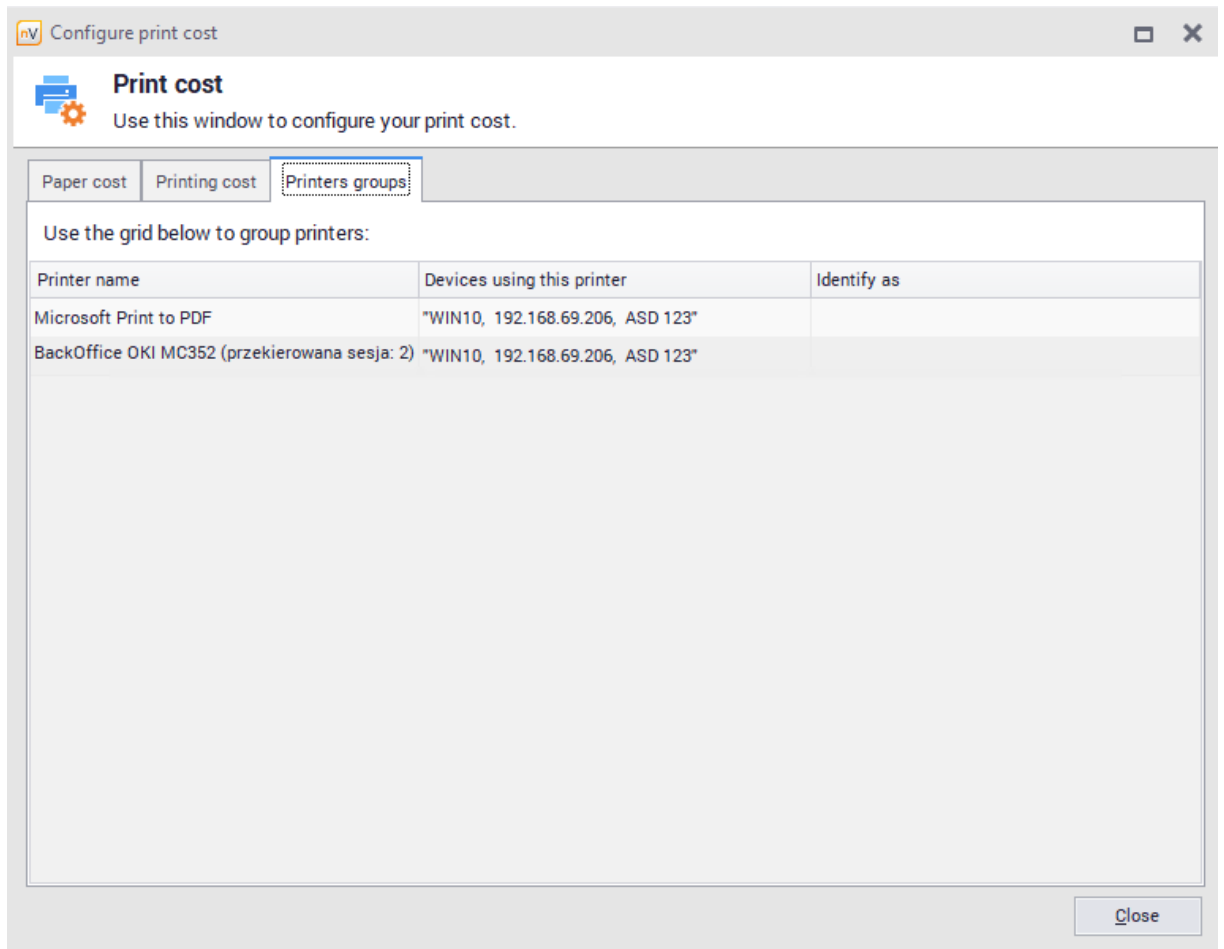
- To retrieve the default value of a field in both tabs, right click the field and select the option **Set cell value as default**.

Printing cost audit

Printing costs are displayed in the last column of the **Printout audit** window. At the bottom, the total printing cost for the given period is also specified.

7.7.4 Printer grouping

To reduce the number of entries and to avoid reporting printing costs for repeating devices, it is possible to group printers. The function is available in the **Printers groups** tab (the **Configure printing costs** window).



The printer grouping tab contains a list of printers with information about the machines which were performing printing on these devices. Printouts identified as other assume their printing costs, but in all other presentations (printout audit, reports) are still considered as independent printers.

Practical information

While grouping printers, note the entries referring to the same device which has different names on a given machine, as well as devices used by multiple users. Also select one entry which will be used as the basis for the creation of the given printer group, because nVision blocks the ability to create cyclical associations.

To remove the association for a given printer, right click to expand the menu for the given entry and select the option **Clear 'identify as'**.

Part



8 Inventory module

8.1 Introduction

8.1.1 General information

The **Inventory** module automatically collects information about the hardware configuration of each computer and the software installed on it. 'Collect' task is performed by the nVision Agent once a day for each computer. Automatic download of hardware configuration and installed software data requires installation of the nVision Agent on selected hosts.

To enhance data synchronization for a selected device, select **Agent / Collect inventory** from the context menu of the selected device. You can also perform an inventory for the entire map (all computers) by selecting **Inventory** option from the context menu in the map tree. Please note that synchronization time for map data depends on the number of devices.

Device Information

Information about resources, software and hardware can be found in tabs located in **Device Information** window. Please note, this data may not be available immediately after scanning the network. They will appear automatically as soon as the Agents finish scanning the computers and send the data:

The screenshot displays the nVision Agent interface for a device named 'DESKTOP-NOQNH1' (IP: 192.168.0.108). The interface is divided into several sections:

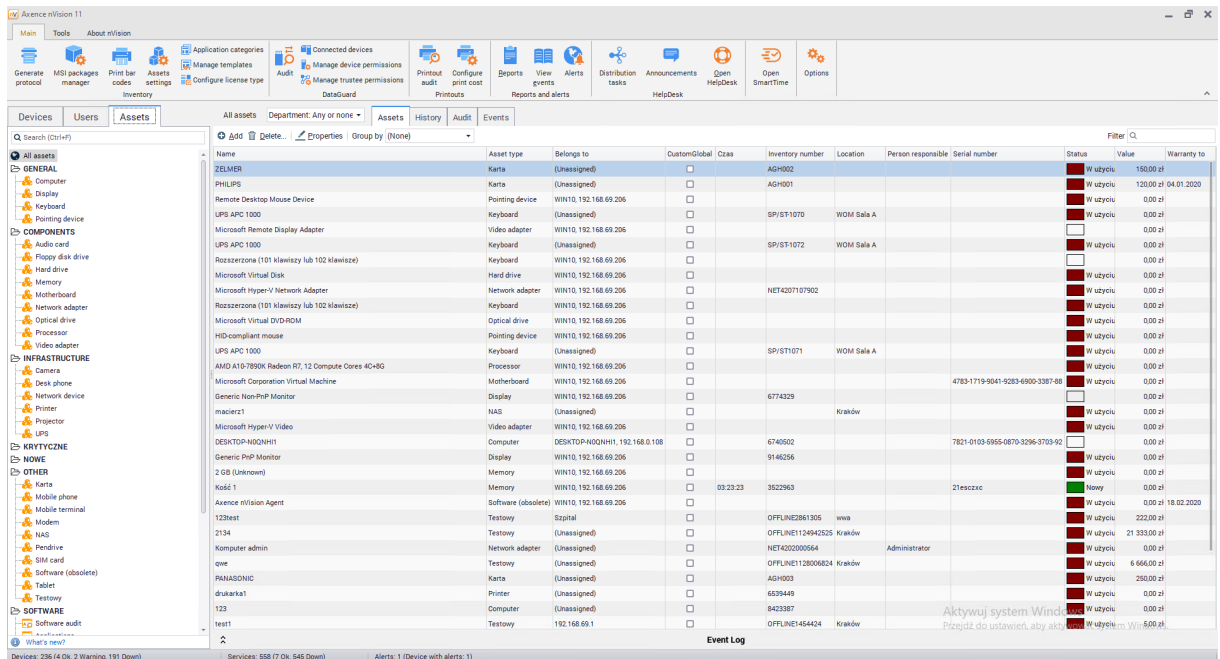
- General Information:** Model: Virtual Machine, Architecture: x64-based PC, S/N: 7821-0103-8965-0870-3296-3703-92.
- Operating system:** Name: Microsoft Windows 10 Pro, Upgrade: 1909, Version: 10.0.18363.592, S/N: 00030-80000-00000-AA93Z.
- Display:** Monitor: Generic PnP Monitor, Generic Non-PnP Monitor; Monitor S/N: Count: 2; Video controller: Microsoft Hyper-V Video, Microsoft Remote Display; Resolution: 1024 x 768.
- Drives:** Hard drive: Microsoft Virtual Disk; Hard drive S/N: Total space on hard drives: 50 GB; Total free space: 29 GB; Number of hard drives: 1; Floppy: ; DVD: .
- Printers:** Microsoft XPS Document Writer, Microsoft Print to PDF, Fax.
- Network:** Network adapter: Microsoft Hyper-V Network Adapter.
- Memory:** Total memory: 4 GB; Available memory: 2.98 GB.
- Sound:** Sound device: none.

The interface also shows a 'Device status' warning banner indicating a 'Last response' on 18.03.2020 13:20:07. At the bottom right, there is a message: 'Aktywuj system Windows. Przejdź do ustawień, aby aktywować system Windows.'

Assets

Starting from nVision 11.5, the phrase of a **'fixed asset'** has been replaced by the phrase of a **'asset'**.

Assets can be assigned to departments or users. Assets assigned to users are described in the [user assets](#) ²²⁴ chapter. The list of all assets will be displayed after clicking the **Assets** tab in the main console window:



See ["Assets"](#)¹⁸² chapter to view new features.

Software

The software section can be accessed by clicking **Asset** tab in the main window pane and consists of three sections:

- Software audit - displays list of detected applications, enables audit snapshot,
- Applications - displays list of applications which installations can be detected by the Agent. Application installations can be assigned to users,
- Licenses - allows to view, modify and add licenses. license can be bound with multiple applications and users.

History

Axence nVision shows the history of all assets statuses and actions performed on the asset. This information is presented in a list, including date, time and information about the user who performed the action. More information is described in the [* hyperlink *](#) chapter.

nVision agent inventory process

Automatic hardware and software inventory process requires installed nVision Agent on given computer. The administrator can specify which information is to be read by the Agent. The configuration window has been described [here](#)¹⁹⁸.

More information about nVision Agent installation is described in the [Installing and Uninstalling Agents](#)¹¹⁵ chapter.

Manual inventory process

Hardware and software inventory process can also be performed agent-less.

8.1.2 First steps

When starting work with the Inventory module, the Administrator should perform a few basic steps that will allow to customize the module. These steps may include the following:

1. Specification of resources, which must be automatically detected on computers with Agent installed, described in the [Asset autodetection](#)¹⁹⁸ chapter .

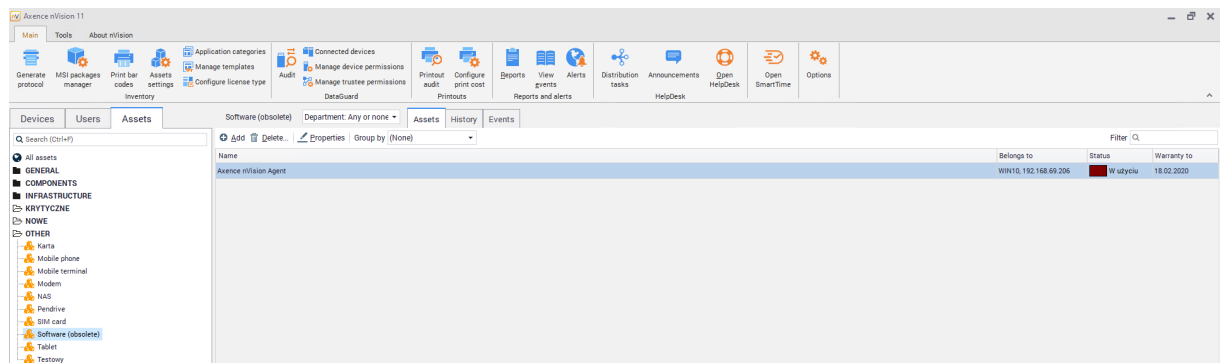
2. Add resource and folders types that will group these types. The activities are described in the [Asset types](#) [200] and [Asset types folders](#) [204] chapters.
3. Adding additional fields, statuses and activity templates available from the [Asset settings](#) [198] window.
4. [Adding documents](#) [186] and associating them with resources or [licenses](#) [282].
5. Adding licenses for the audited applications and determining the [associated applications](#) [278].
6. Modifying the method of assigning licenses and change of related settings (assigning users to the application, changing the assigned serial numbers). To know how to assign a license, read the [licensing methods](#) [290] chapter.

8.1.3 Migration from previous versions

Assets Types

All types of assets (formerly: types of fixed assets) that were created by the user in the previous version of the module will be moved to the built-in folder "Other" types after migration.

The "Software" type will receive "(obsolete)" and will be placed in the "Other" folder:



Additional fields

The value of the "old" **Responsible person** field will be moved as a global field called **Responsible person** (obsolete).

Statuses

If the field "in service" was checked (regardless of the value of the field "in warehouse") the asset will receive the status "In repair".

If the "in warehouse" field was checked without "in service" marked field, the asset will receive the status "In working condition".

Other assets will receive "In Use" status.

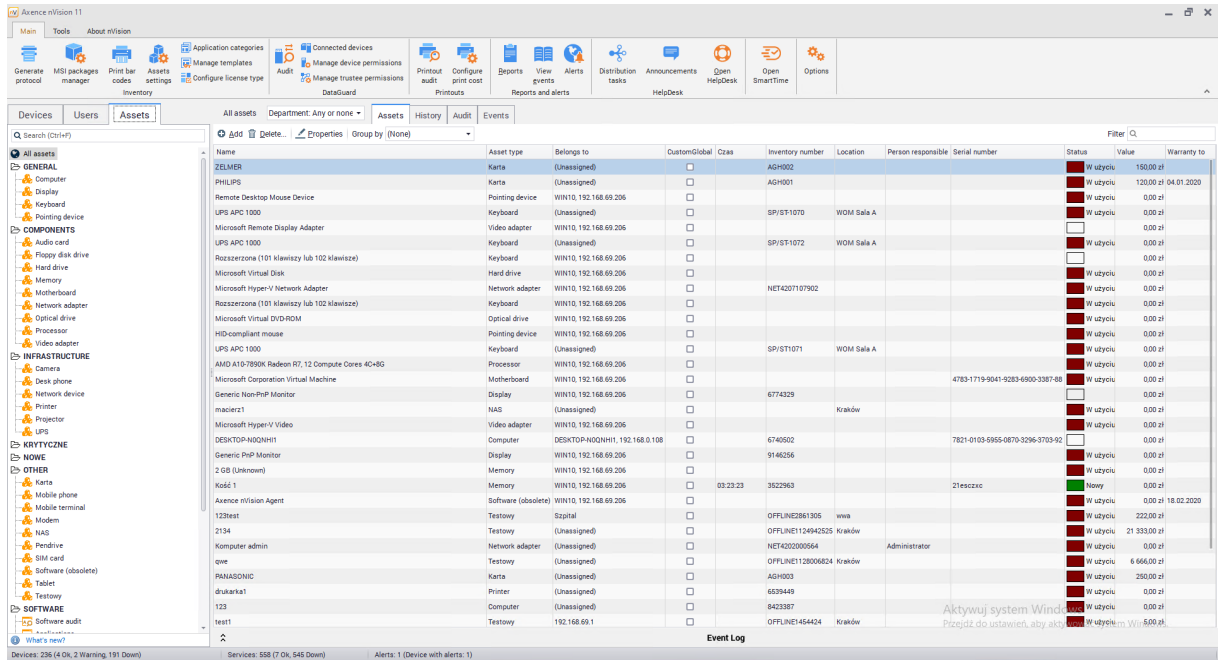
Documents

All current attachments are converted during migration into documents of the "Other" type. Document name will be amended with file name.

8.2 Assets

8.2.1 Assets tab

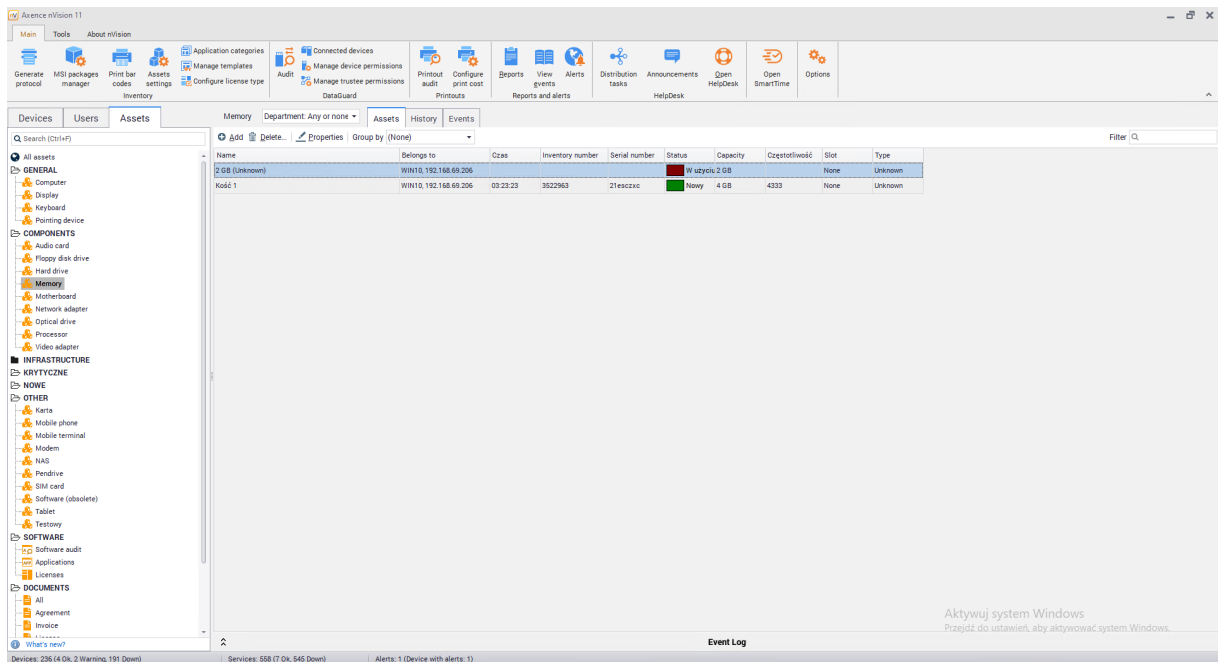
In nVision 11.5 a "assets" tab has been added that allows displaying assets saved in the database. To access it, go to the **Main** tab and then select **Assets**:



The list of folders with their assigned types, list of applications and licenses as well as the document section divided into categories will be displayed on the left side of the screen The administrator can create their own folders and categories of documents. These settings are described in the chapters [resource type folders](#) [204] and [document types](#) [210].

Assets

There are several ways to present resource data. Click on all assets to display a list of all collected assets. By selecting an asset type from the list, a list of all assets of this type of asset will be displayed. The table presenting data on a given type of resource will also contain data from additional and global fields, but only if a value has been entered. The following screenshot presents the table for the "Memory" type with the "Frequency" as additional field and the "Time" as global field:

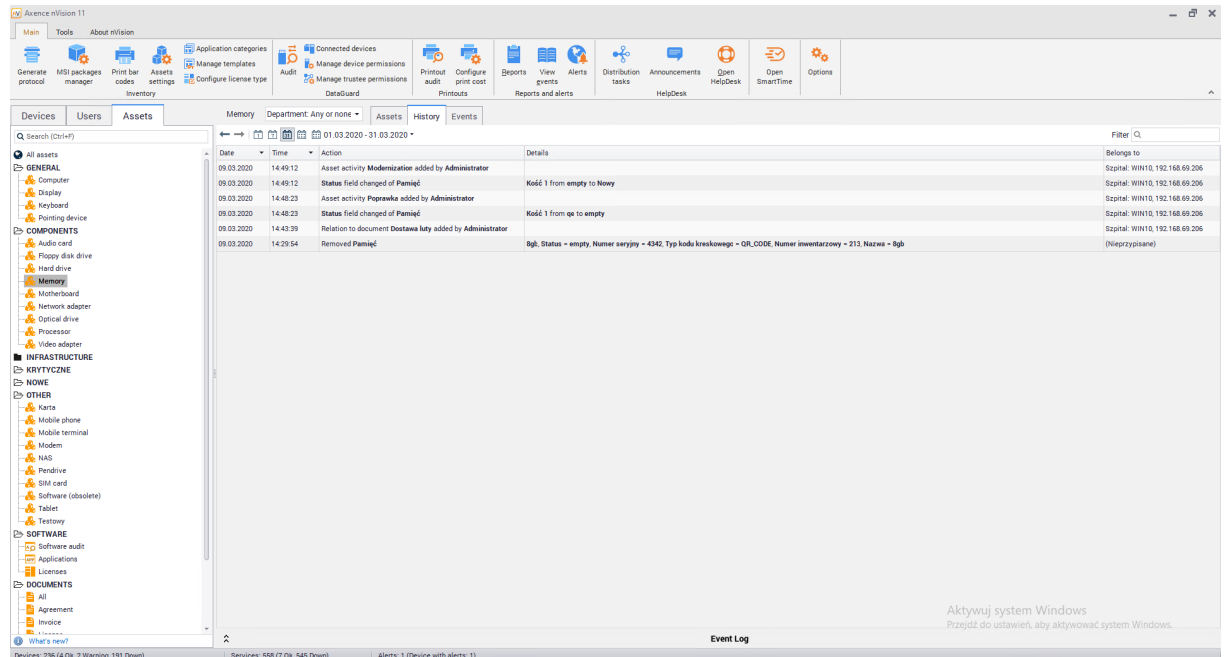


You can filter the list, edit the asset, delete it or add a new asset by using the buttons at the top of the window. The process of adding a new resource is described in a [separate chapter](#) [218].

A few additional tabs are visible above the asset table. They include:

- History

Shows the history of operations performed on the selected asset type. See [history](#)^[192] chapter for more information about data stored in History.



- Events

Events were described in [dedicated chapter](#)^[312]

Software

By selecting an item in the software section (the list on the left of the screen), a list of all applications detected by Agents will be displayed. Detection and configuration of software inventory is described in [this chapter](#)^[254]

Documents

By selecting an item in the documents section (the list on the left of the screen), a list of documents of the selected category along with the established relations to assets will be displayed. "All" position displays all documents added to nVision. Use the buttons above the table to add, delete, edit or open the selected document.

More information about documents can be found in [documents](#)^[186] and [document types](#)^[210] chapters.

8.2.2 Assets properties

8.2.2.1 General

In nVision 11.5 the phrase of a **'fixed asset'** has been replaced by the phrase of a **'asset'**. Anything that Administrator would like to catalogue can be called 'asset'. Example of assets may include: printers, computers, IP phones, and all types of equipment or licenses that have been purchased by the organization.

The asset properties window has been replaced with several tabs

- General,
- Documents,
- Actions,
- History,
- Alerts,

- User Access.

The following items will be visible in the **General** tab:

Basic information

- Name - name assigned to the asset,
- Asset type - information about asset type. Configuration of types is described in [asset types](#)^[200] chapter,
- Belongs to ... - a branch or device associated with the asset,
- Responsible person - nVision user assigned to the asset,
- Status - current status of the asset is marked with color. The status can be changed manually or by adding a change action. More information about statuses can be found in [asset status](#)^[208] chapter
- Inventory number,
- Serial number,
- Barcode.

Additional fields

- Global fields - a field available in each type of asset. See [global fields](#)^[205] chapter for more information
- Additional fields - a field available only in the selected asset type, defined at the moment of creating or editing the type. For more information see [asset types](#)^[200] chapter

The screenshot displays the 'Asset' management window for 'Kość 1'. The interface is divided into a left sidebar with navigation options (GENERAL, DOCUMENTS, ACTIONS, HISTORY, ALERTS, WHO CAN USE) and a main content area. The main area is titled 'BASIC INFORMATION' and contains several input fields and buttons:

- Name:** Kość 1
- Asset type:** Memory (with a 'Configure' button)
- Belongs to:** WIN10, 192.168.69.206
- Person responsible:** (empty field with a 'Transfer' button)
- Status:** Nowy (with a dropdown arrow)
- Serial number:** 21esczxc
- Inventory number:** 3522963 (with a 'Generate' button)
- Bar code:** QR_CODE (with an 'Options' button)

Below the basic information is a QR code and an 'ADDITIONAL FIELDS' section. This section includes a search filter and a table of asset attributes:

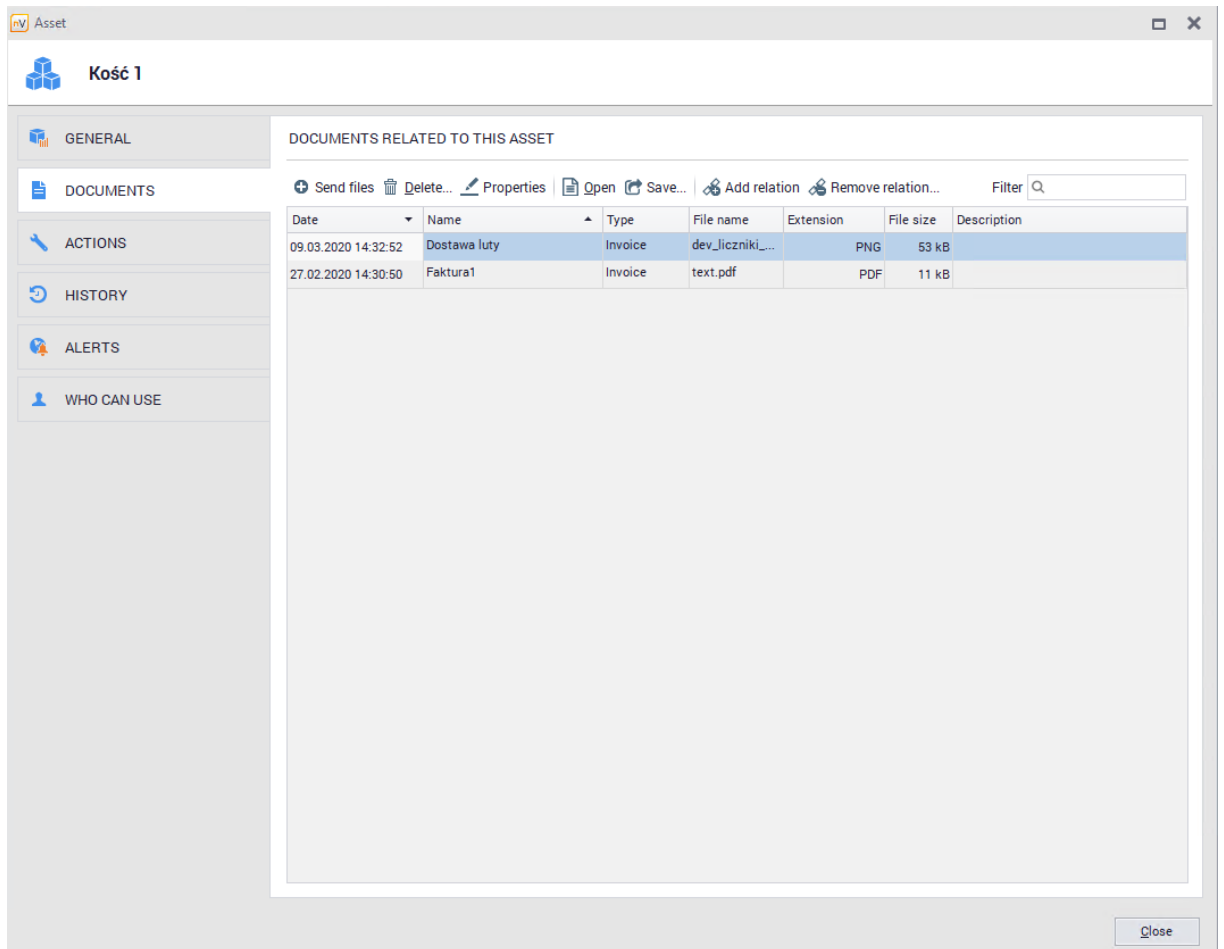
| Name | Value |
|-------------------------------------|--------------------------|
| Specific asset type fields | |
| Bits | |
| Capacity | 4 GB |
| Częstotliwość | 4333 |
| Osoba odpowiedzialna (przestarzałe) | |
| Slot | None |
| Speed | |
| Type | Unknown |
| Global fields | |
| CustomGlobal | <input type="checkbox"/> |

A 'Close' button is located at the bottom right of the window.

Information about the assets that user can use will also be displayed in the user information window. More information available in [user assets](#)²²⁴ chapter.

8.2.2.2 Documents

The **Documents** tab allows you to add, display and delete documents related to the selected asset. The documents associated with the selected asset will be visible in the table:



The screenshot shows a web application window titled 'Asset' with a sub-header 'Kość 1'. On the left is a sidebar with navigation options: GENERAL, DOCUMENTS, ACTIONS, HISTORY, ALERTS, and WHO CAN USE. The main area is titled 'DOCUMENTS RELATED TO THIS ASSET' and contains a toolbar with 'Send files', 'Delete...', 'Properties', 'Open', 'Save...', 'Add relation', and 'Remove relation...'. Below the toolbar is a table with the following data:

| Date | Name | Type | File name | Extension | File size | Description |
|---------------------|--------------|---------|------------------|-----------|-----------|-------------|
| 09.03.2020 14:32:52 | Dostawa luty | Invoice | dev_liczniki_... | PNG | 53 kB | |
| 27.02.2020 14:30:50 | Faktura1 | Invoice | text.pdf | PDF | 11 kB | |

A 'Close' button is located at the bottom right of the window.

Adding new document

To add new document simply click the send files option. The window for adding a new document will be displayed:

The screenshot shows a dialog box titled "Adding a new document" from the software "Axence nVision 11". The dialog is divided into two main sections. The top section, "Document information", contains several fields: a dashed box for file selection with the text "Drag files or click to select", a text input for "Name", a dropdown for "Document type" with an edit icon, a text area for "Description", and a dropdown for "Department" currently set to "No department". The bottom section, "Relations", is titled "Link documents with assets" and includes "Add" and "Remove" buttons, a "Related assets" header, and a list containing the item "Kość 1". At the bottom of the dialog are three buttons: "Back", "Add document", and "Cancel".

Window is divided into two sections - document information section and document relations with assets.

Document information

The required fields are marked with ' * '.

- File - select or drag a file to the selected place,
- Name - the name of the document visible in nVision,
- Document type - select one item from the list - adding new document types is described [document categories](#) ^[210] chapter

- Description - additional text fields describing the document,
- Chapter - additional field to specify a branch.

Relations

To associate a document with an asset, click the **Add button** and select assets from the list

Document removal

To remove the document, click **Delete** button.

Please note that deleting a document from a selected asset results in complete removal of this document from nVision. A deleted document that was associated with other assets will no longer be visible in the nVision console, and the relation will be deleted.

Document edition

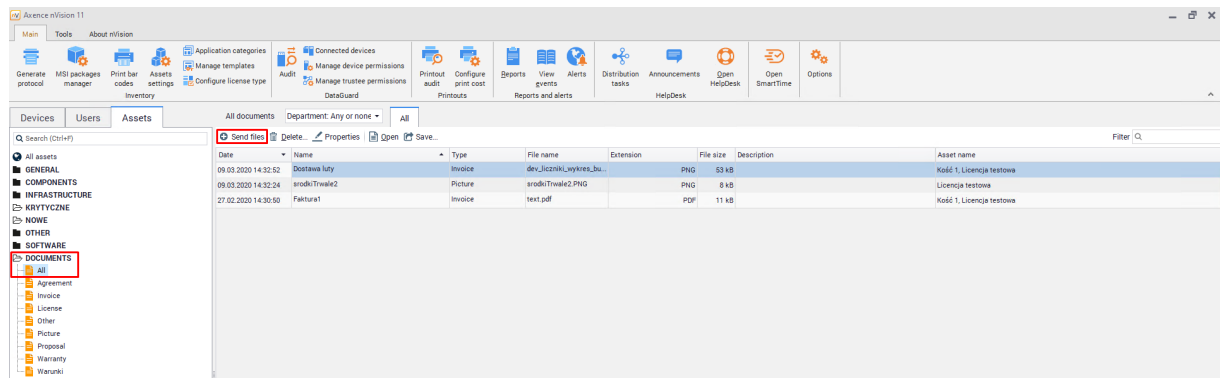
Added documents can be edited by double-clicking on the selected item or by clicking the **Properties** button.

Adding and deleting relations

To add or remove an asset link to a document, use the **Add Relation** and **Delete Relation** buttons. Then select an item from the list.

Alternative process for adding documents

You can also add **Documents** by using the "**Assets**" tab displayed in the main nVision window. At the bottom of the list in the documents section, click first the document type then the **Send files** button located at top window pane. A window for adding a new document will be opened:



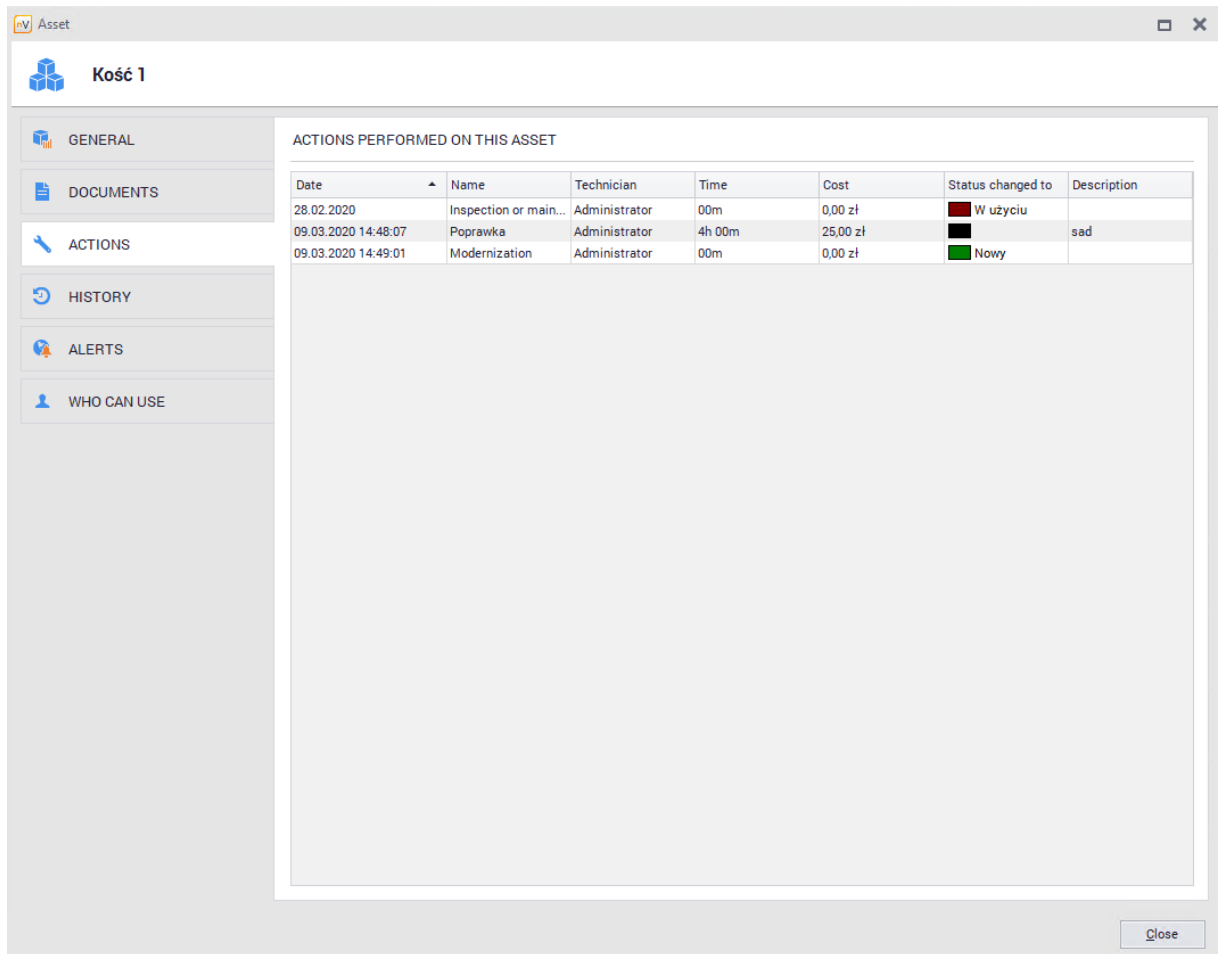
Saving and opening of added document

Documents can be opened from nVision and saved if necessary. To perform such actions, use the **Open** or **Save** buttons.

8.2.2.3 Actions

The **Action** tab allows you to add, display and remove activities performed on the selected asset. This allows to precisely describe the cost and activities carried out on individual assets.

Actions associated with the selected asset will be visible in the table:



The screenshot displays the 'Asset' management interface for 'Kość 1'. The left sidebar contains navigation options: GENERAL, DOCUMENTS, ACTIONS, HISTORY, ALERTS, and WHO CAN USE. The main area shows a table of actions performed on the asset.

| Date | Name | Technician | Time | Cost | Status changed to | Description |
|---------------------|-----------------------|---------------|--------|----------|-------------------|-------------|
| 28.02.2020 | Inspection or main... | Administrator | 00m | 0,00 zł | ■ W użyciu | |
| 09.03.2020 14:48:07 | Poprawka | Administrator | 4h 00m | 25,00 zł | ■ | sad |
| 09.03.2020 14:49:01 | Modernization | Administrator | 00m | 0,00 zł | ■ Nowy | |

A 'Close' button is located at the bottom right of the main content area.

Adding new action

To add a new action, select the **Add action** option. The window for adding a new action will be displayed:

Adding asset activity

* Activity name: +

* Technician: Administrator

* Date of execution: 25.03.2020 14:41:26

Cost: zł

Execution time: hours
 minutes

Current asset status: Nowy

Change status to: No change

Description:

Add activity Cancel

Required fields are marked with ' * '.

- Name - name of the activity selected from the list of activity templates. Clicking the button will open the window where new activity template can be add,
- Technician - select the user responsible for the selected activity,
- Date of Execution - required field with 'date' format,
- Execution time - select set hours or minutes for action execution
- Cost - additional information field,
- Change status to - status that will be set after adding the activity (multiple option to choose),
- Description - additional text field

Removing actions

Select the action to be removed and press **Remove** button.

Editing actions

Added activities can be edited by double clicking on selected position and/or by clicking **Properties** button.

General activity configuration is described in the [asset actions](#) ²⁰⁷ chapter.

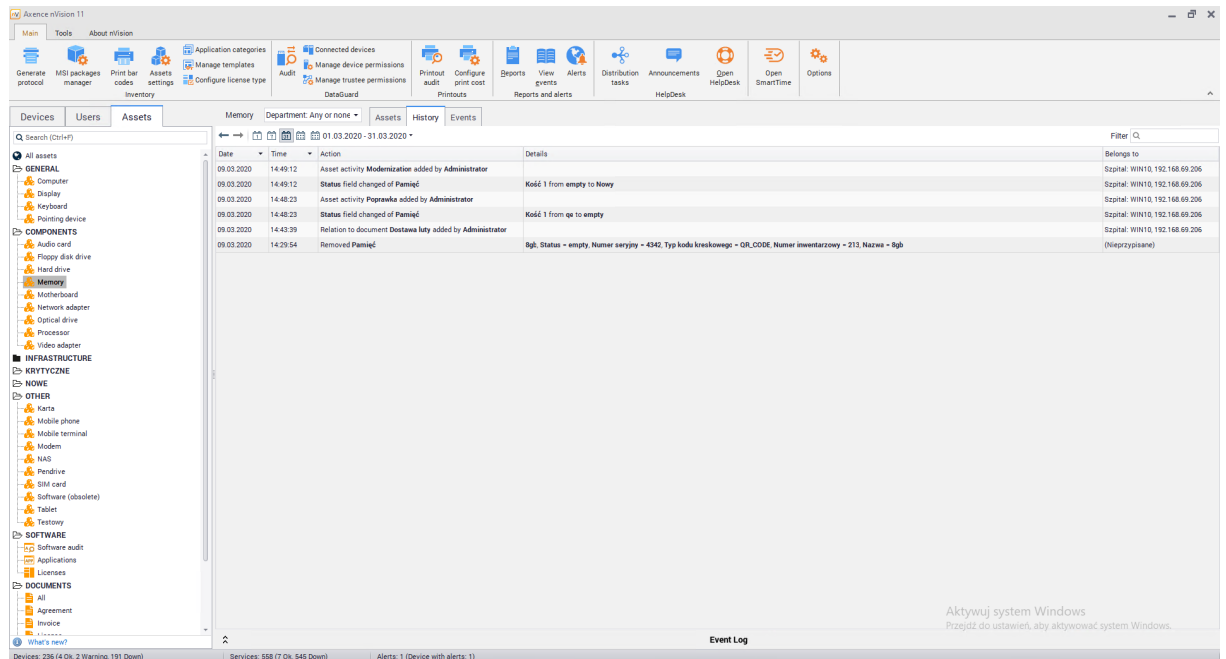
8.2.2.4 History

The **History** tab in the asset properties window allows you to see a list of all changes made to the selected asset. The entries will include the date, description and person who made the change:

The screenshot shows the 'ASSET HISTORY' window for asset 'Kość 1'. The window has a sidebar with navigation options: GENERAL, DOCUMENTS, ACTIONS, HISTORY (selected), ALERTS, and WHO CAN USE. The main area displays a table of activity history with the following data:

| Date | Time | Action | Details |
|------------|----------|---|---------------------------|
| 09.03.2020 | 14:49:12 | Asset activity Modernization added by Administrator | |
| 09.03.2020 | 14:49:12 | Status field changed of Pamięć | Kość 1 from empty to Nowy |
| 09.03.2020 | 14:48:23 | Asset activity Poprawka added by Administrator | |
| 09.03.2020 | 14:48:23 | Status field changed of Pamięć | Kość 1 from qe to empty |
| 09.03.2020 | 14:43:39 | Relation to document Dostawa luty added by Administrator | |

To view the history of changes for all assets, go to the **Assets** tab located in the main window and then select **All assets / History**:



8.2.2.5 Alerts

Asset alerts can be created for individual assets or for a selected type of assets. Alerts allow to configure notification for the Administrator when certain conditions are met.

Alert for selected asset type

To create alert for selected asset type:

1. Open the resource editing window, go to the **Alerts tab**.
2. Click **Add button**, then select **Add alert for type** option.
3. In the **Alert rules configuration window** select event(field) for which you want to create the alert and set the date the alert is to be created. Enter alert description and click **OK**. Optionally you can also set the e-mail to get reminder messages.

Configure alerts rule for Memory type
Use this window to configure alert condition and description.

Configuration

Automatically create alerts week(s) before time

for field

Description:

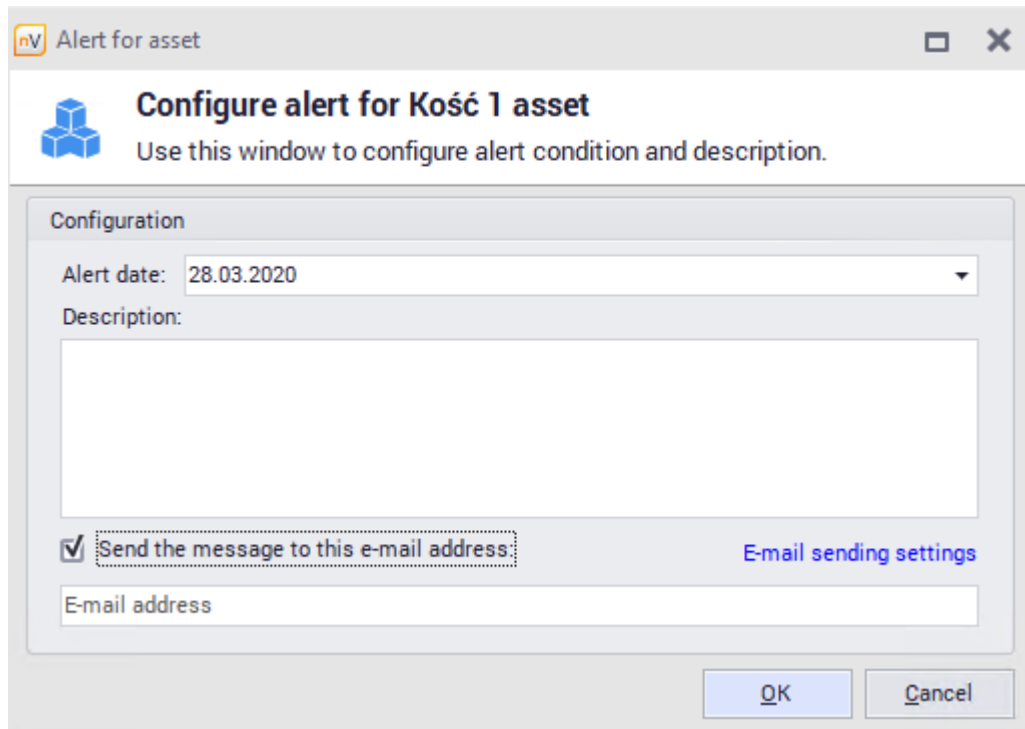
Send the message to this e-mail address: [E-mail sending settings](#)

A different method of adding alerts for selected asset types is described in [asset types](#)^[200] chapter.

Alert for selected asset

To create alert for selected asset:

4. Open the resource editing window, go to the **Alerts tab**.
5. Click **Add button**, then select **Add alert for this asset** option.
6. In the **Alert rules configuration window** select event(field) for which you want to create the alert and set the date the alert is to be created. Enter alert description and click **OK**. Optionally you can also set the e-mail to get reminder messages.



Alert for asset

Configure alert for Kość 1 asset
Use this window to configure alert condition and description.

Configuration

Alert date: 28.03.2020

Description:

Send the message to this e-mail address [E-mail sending settings](#)

E-mail address

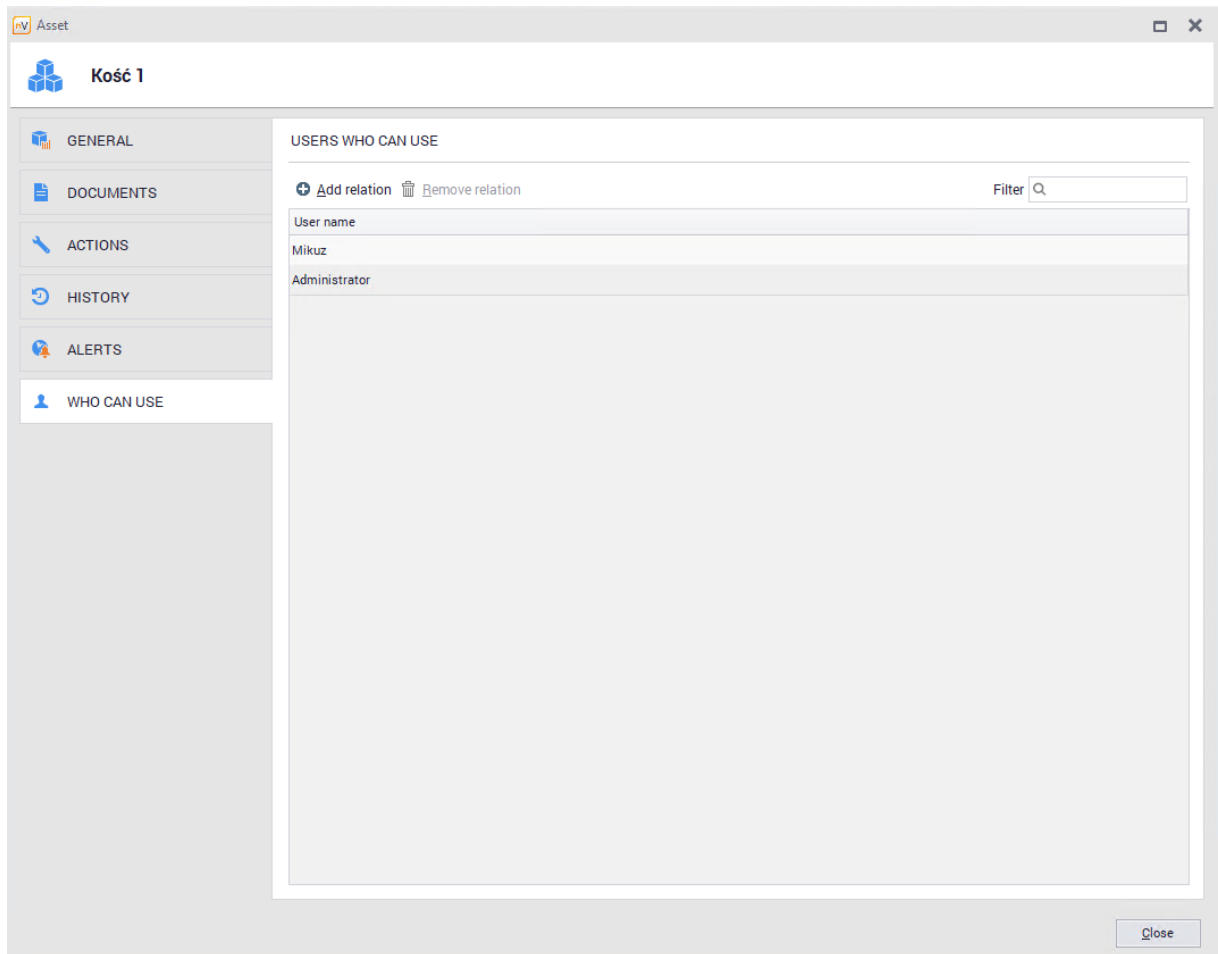
OK Cancel

To know more about alerts, see [alerting](#)⁵⁸⁶ chapter.

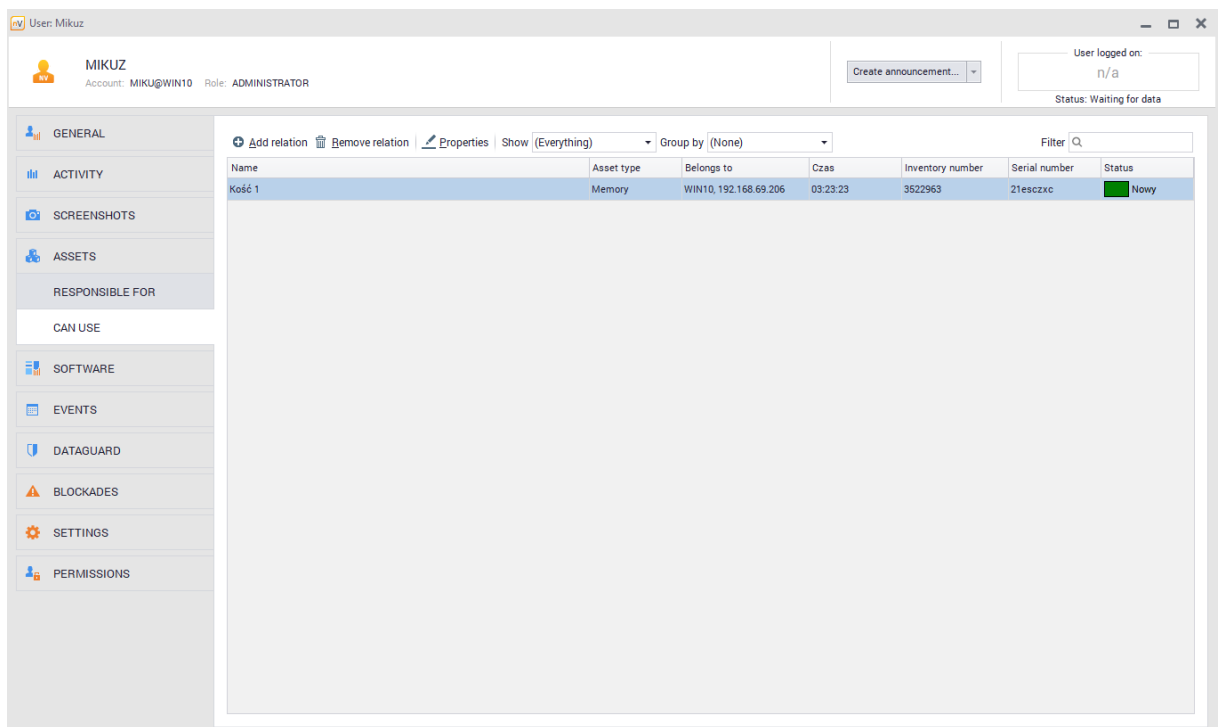
8.2.2.6 Who Can Use

The **Who Can Use** tab presents information about users who have access to the selected asset, but are not necessarily responsible for it. Each asset can have any number of users who use it. Relation is only auxiliary - it does not grant any access or permissions for users set to use the asset.

To add an authorized user to the asset, use the **Add Relation** button and select users from the list:



Information about resources that the user can use will be displayed in the user information window after switching to the **Assets / Can Use** tab:



8.2.2.7 Barcodes

Kody kreskowe mogą zostać przypisane do poszczególnych zasobów w nVision. Zasoby z nVision można powiązać z rzeczywistymi urządzeniami poprzez naklejenie na nich etykiet z kodem kreskowym. Identyfikator zaszyty w kodzie kreskowym oznacza jednocześnie (unikalny) numer inwentarzowy zasobu. Jeśli urządzenia posiadają już swoje unikalne identyfikatory z kodem kreskowym, to istnieje możliwość aktualizacji numeru inwentarzowego za pośrednictwem aplikacji mobilnej.

Aby dowiedzieć się więcej o drukowaniu etykiet, przejdź do rozdziału [Drukowanie etykiet](#)^[227]. Aby dowiedzieć się więcej o instalowaniu i korzystaniu z aplikacji mobilnej, przejdź do rozdziału [Aplikacja mobilna](#)^[229].

Podstawowe informacje

Każdy zasób posiada pole zawierające numer inwentarzowy. Może on zostać podany ręcznie lub wygenerowany poprzez kliknięcie przycisku **Generuj**. Standardowo numer taki składa się z 7 cyfr, jest prezentowany w postaci kodu kreskowego QR Code i jest unikalny. Liczba 7-cyfrowa można przedstawić w postaci każdego ze wspieranych rodzajów formatów kodu kreskowego (jednowymiarowe: CODABAR, COD 39, CODE 93, CODE 128, EAN 8, EAN 13, UPC A, UPC E; dwuwymiarowe: QR CODE).

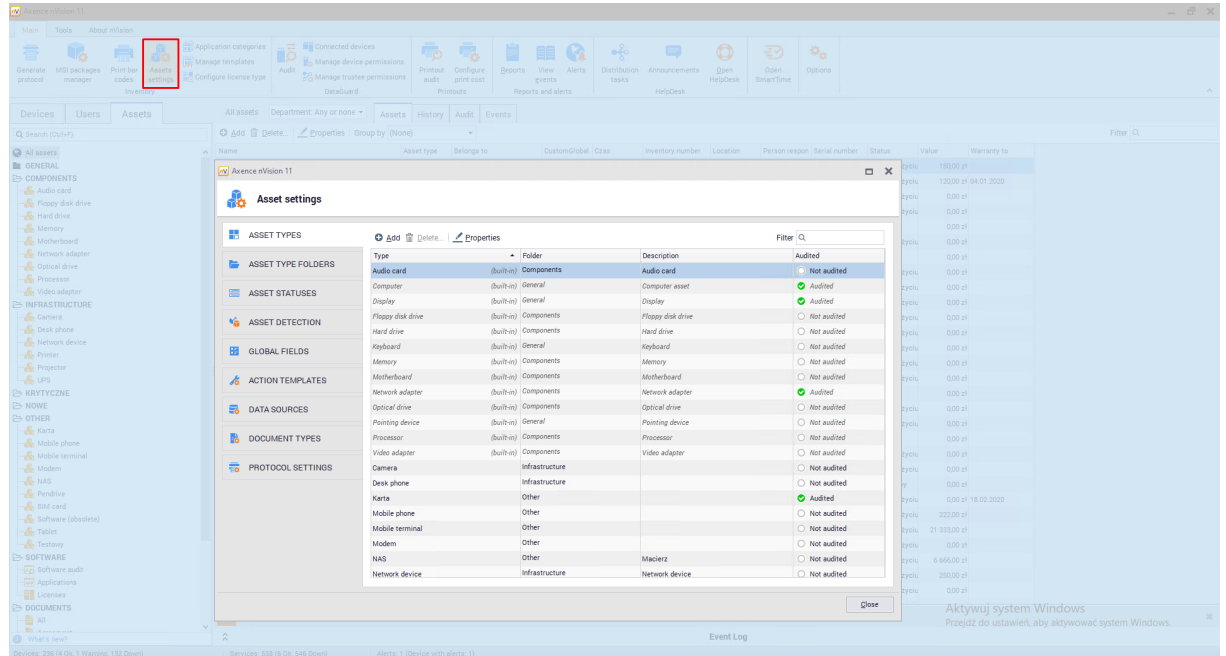
The screenshot shows the WinTest application interface. The main window is titled "WinTest" and displays the "BASIC INFORMATION" section for an asset named "WinTest". The asset type is "Computer", and it belongs to "WinTest, 192.168.69.206 (WIN10)". The status is "Nowy". The serial number is "4783-1719-9041-9283-6900-3387-88" and the inventory number is "4270568". A dropdown menu for "Bar code" is open, showing options: QR_CODE (selected), CODE_128, CODE_39, CODE_93, EAN_13, EAN_8, and UPC_CODE. A QR code is displayed next to the dropdown. Below the dropdown is an "ADDITIONAL FIELDS" section with a table of asset details.

| Name | Value |
|----------------------------|-----------------------|
| Specific asset type fields | |
| Description | AT/AT COMPATIBLE |
| Info 1 | ASD |
| Info 2 | |
| Manufacturer | Microsoft Corporation |
| Model | Virtual Machine |
| Original username | Miku |
| OS type | x64-based PC |
| Global fields | |
| Location | |

8.2.3 Assets settings

8.2.3.1 Basic information

The asset settings window allows the Administrator to configure asset properties according to his needs. To display the asset settings window click **Asset settings** button located on **Main** ribbon.



The settings window has been divided into several tabs:

- Asset Types,
- Asset Types Folders,
- Asset Status,
- Asset Detection,
- Global fields,
- Activity templates,
- Data sources,
- Document Types,
- Document Types

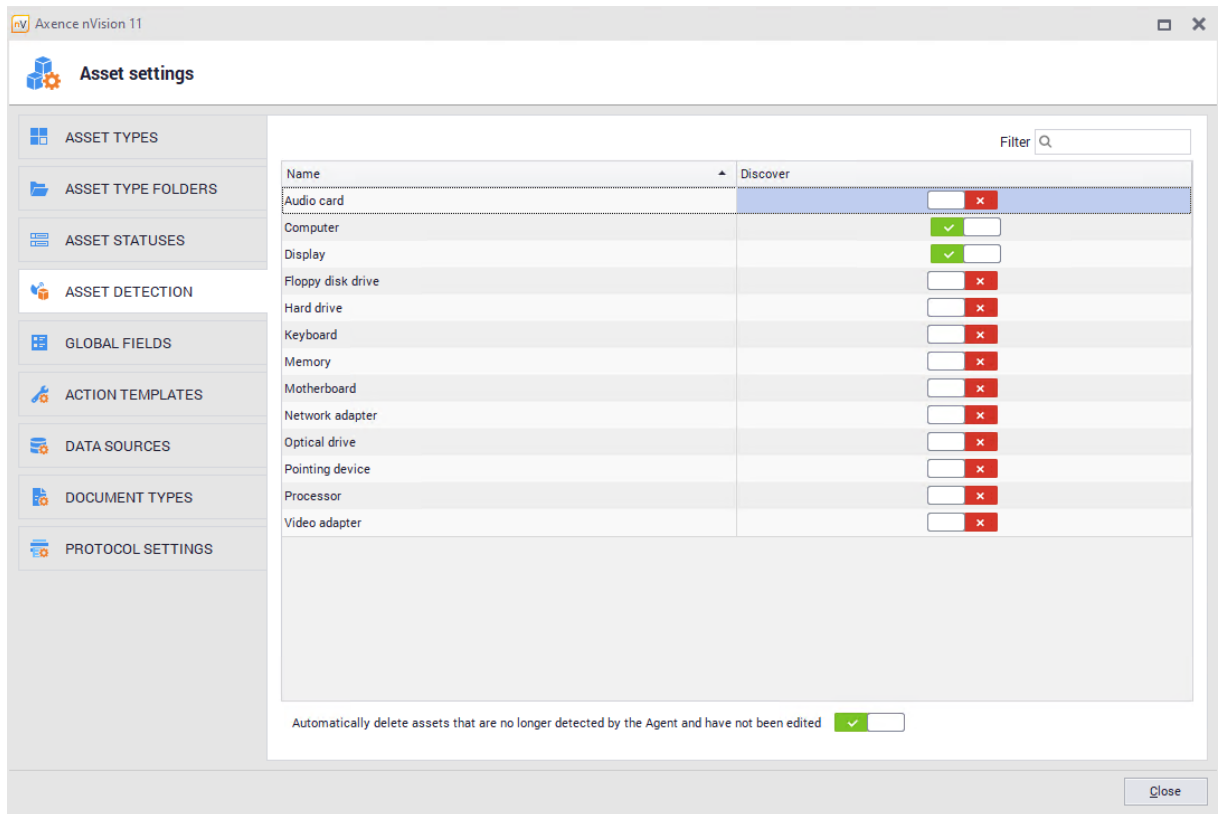
Each tab is described in detail in following chapters.

8.2.3.2 Asset detection

The Asset Detection tab allows to specify what resources will be automatically created based on the data collected by the Agent.

Automatic asset adding

Go to **Asset Settings** window, then open the **Asset Detection** tab. Here you can specify automatic detection only for the types of assets visible in the list in this window. Positions in this list cannot be edited:



The screenshot shows the 'Asset settings' window in Axence nVision 11. The left sidebar contains navigation options: ASSET TYPES, ASSET TYPE FOLDERS, ASSET STATUSES, ASSET DETECTION, GLOBAL FIELDS, ACTION TEMPLATES, DATA SOURCES, DOCUMENT TYPES, and PROTOCOL SETTINGS. The main area displays a table with columns for 'Name' and 'Discover'. The 'Discover' column contains checkboxes for each asset type. The 'Computer' and 'Display' rows have their checkboxes checked (green checkmarks), while all other rows have unchecked checkboxes (red 'x' marks). At the bottom of the table, there is a checkbox labeled 'Automatically delete assets that are no longer detected by the Agent and have not been edited', which is also checked. A 'Close' button is located at the bottom right of the window.

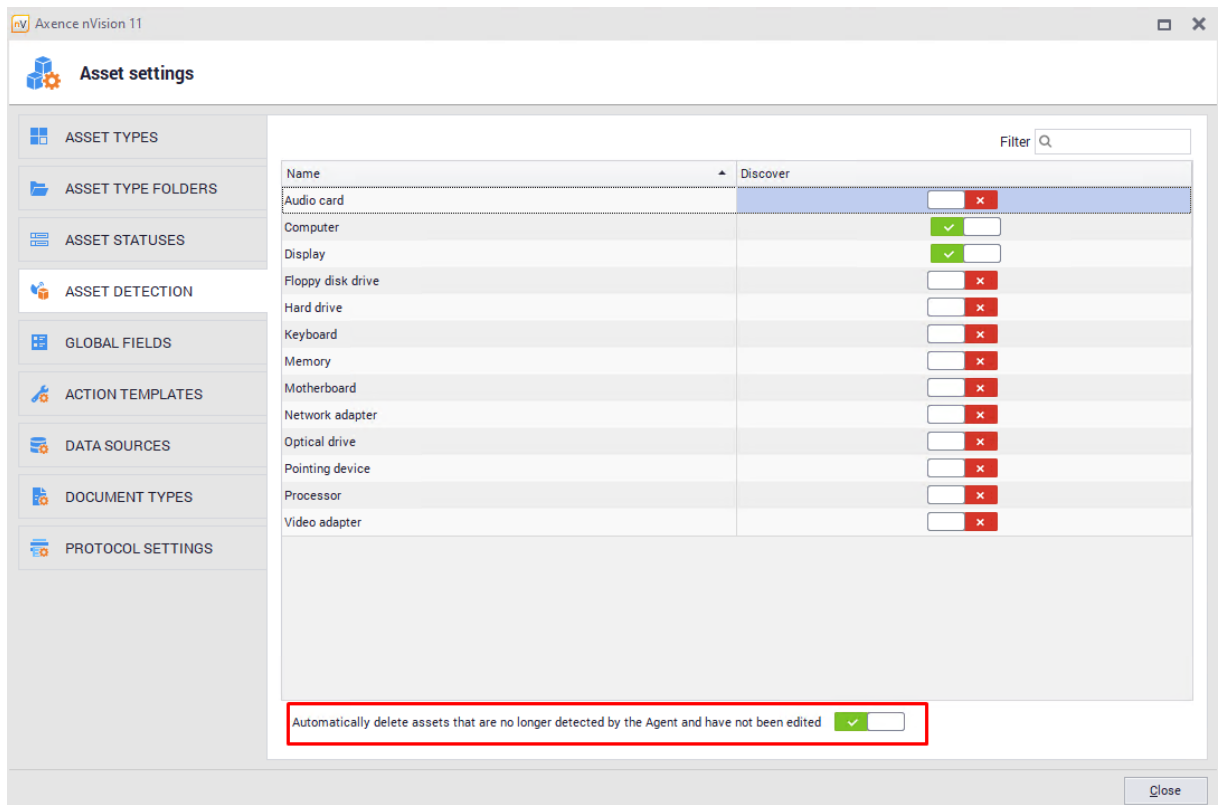
| Name | Discover |
|-------------------|-------------------------------------|
| Audio card | <input type="checkbox"/> |
| Computer | <input checked="" type="checkbox"/> |
| Display | <input checked="" type="checkbox"/> |
| Floppy disk drive | <input type="checkbox"/> |
| Hard drive | <input type="checkbox"/> |
| Keyboard | <input type="checkbox"/> |
| Memory | <input type="checkbox"/> |
| Motherboard | <input type="checkbox"/> |
| Network adapter | <input type="checkbox"/> |
| Optical drive | <input type="checkbox"/> |
| Pointing device | <input type="checkbox"/> |
| Processor | <input type="checkbox"/> |
| Video adapter | <input type="checkbox"/> |

Automatically delete assets that are no longer detected by the Agent and have not been edited

By default, "Computer" and "Display" assets are automatically detected. To enable automatic detection for the selected type simply switch the button in the **discover** column by the selected position.

Automatic asset removal

For automatic asset removal simply click the switch placed at the bottom of the asset discovery tab:



This screenshot is identical to the one above, showing the 'Asset settings' window. A red rectangular box highlights the checkbox at the bottom of the table, labeled 'Automatically delete assets that are no longer detected by the Agent and have not been edited', which is checked.

If the automatically detected resource becomes invisible to the Agent, then:

- if the **switch is on**, then asset **remains unchanged**. It is default setting for new nVision installations.
- if the **switch is off**, then **asset will be removed** provided it has not been edited by Administrator.

Removing device(host) does not remove the assets which have been automatically created by Agent if the switch was off.

8.2.3.3 Asset types

Asset Types tab is available in the **Asset Settings** window, which allows you to display the resource types from existing database and define new types. Types help for better categorization of individual resources.

The Administrator can add, edit and delete asset types, with the exception of built-in types that have the additional security settings described in this chapter. The data is shown in table:

| Type | Folder | Description | Audited |
|-------------------|-----------------------|-------------------|--|
| Audio card | (built-in) Components | Audio card | <input type="radio"/> Not audited |
| Computer | (built-in) General | Computer asset | <input checked="" type="radio"/> Audited |
| Display | (built-in) General | Display | <input checked="" type="radio"/> Audited |
| Floppy disk drive | (built-in) Components | Floppy disk drive | <input type="radio"/> Not audited |
| Hard drive | (built-in) Components | Hard drive | <input checked="" type="radio"/> Not audited |
| Keyboard | (built-in) General | Keyboard | <input type="radio"/> Not audited |
| Memory | (built-in) Components | Memory | <input type="radio"/> Not audited |
| Motherboard | (built-in) Components | Motherboard | <input type="radio"/> Not audited |
| Network adapter | (built-in) Components | Network adapter | <input checked="" type="radio"/> Audited |
| Optical drive | (built-in) Components | Optical drive | <input type="radio"/> Not audited |
| Pointing device | (built-in) General | Pointing device | <input type="radio"/> Not audited |
| Processor | (built-in) Components | Processor | <input type="radio"/> Not audited |
| Video adapter | (built-in) Components | Video adapter | <input type="radio"/> Not audited |
| Camera | Infrastructure | | <input type="radio"/> Not audited |
| Desk phone | Infrastructure | | <input type="radio"/> Not audited |
| Keys | Other | | <input checked="" type="radio"/> Audited |
| Mobile phone | Other | | <input type="radio"/> Not audited |
| Mobile terminal | Other | | <input type="radio"/> Not audited |
| Modem | Other | | <input type="radio"/> Not audited |
| NAS | Other | Macierz | <input type="radio"/> Not audited |
| Network device | Infrastructure | Network device | <input type="radio"/> Not audited |
| Pendrive | Other | | <input type="radio"/> Not audited |
| Printer | Infrastructure | Printer | <input checked="" type="radio"/> Audited |

Each asset type is placed in one folder. **The Assets tab**, available from the main program window allows you to display the folders and their associated types.

▣ Built-in asset types

nVision contains a list of built-in assets types, which include the following:

- **Basic (folder):**
 - Computer,
 - Display,

- Keyboard,
- Pointing device.
- Components (folder):
 - Hard drive,
 - Memory,
 - Optical Drive,
 - Motherboard,
 - Processor,
 - Network adapter,
 - Video adapter,
 - Audio card,
 - Floppy disk drive,
- Infrastructure devices (folder):
 - Printer,
 - Network device,
 - Desk phone,
 - Camera,
 - UPS,
 - Projector,
- Mobile devices (folder)
 - Mobile phone,
 - Tablet,
 - SIM Card,
 - Modem,
 - Pendrive,
 - Mobile terminal
- Other (folder):
 - Car,
 - Software (obsolete).

For built-in asset types:

- You cannot change the name or delete the built-in type.
- You cannot change the built-in folder.
- You can add additional fields for the built-in type, but you cannot delete fields that already exist

Each asset type has the following properties:

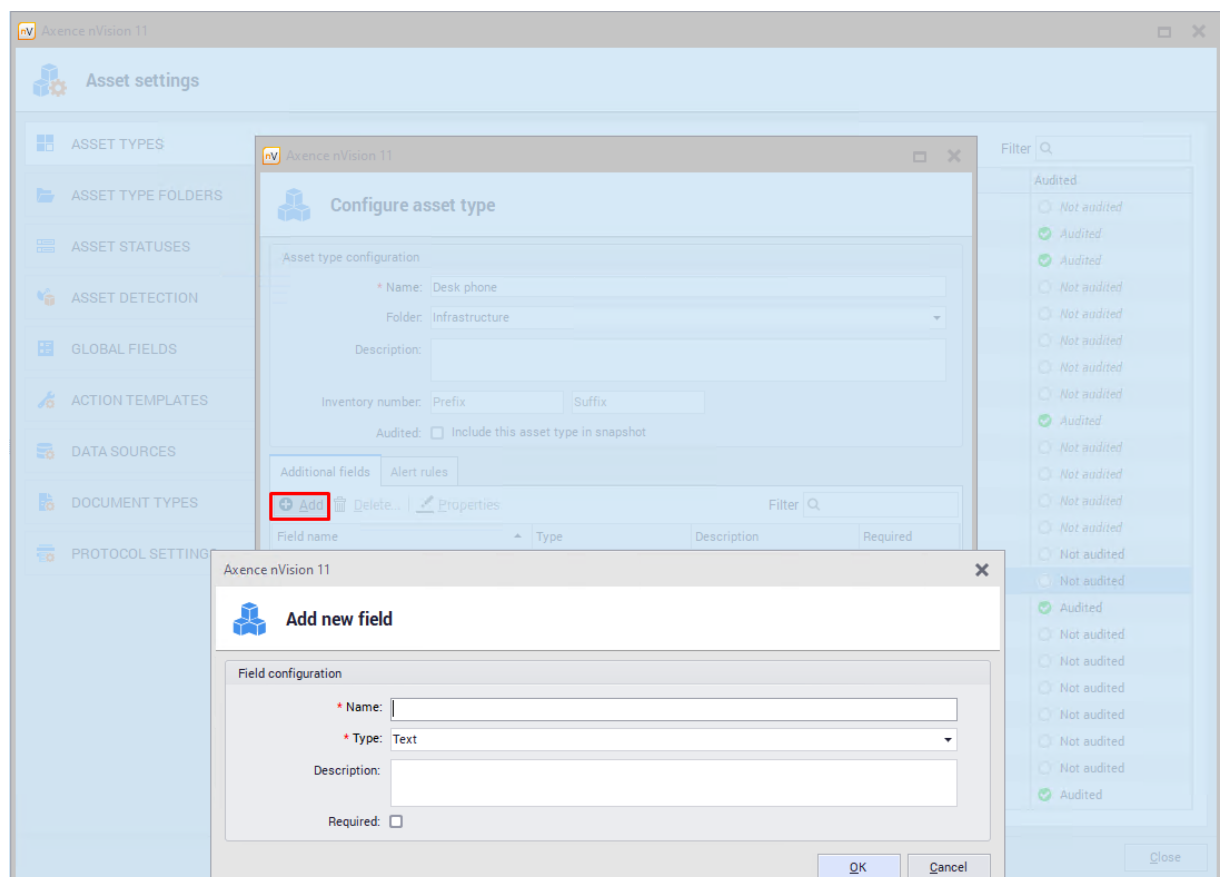
- Name - type name,
- Folder - folder where type is stored
- Inventory number - sets prefix and suffix for selected type
- Audited - mark to set, if the assets of particular type should be stored in audit archive

By double-clicking the asset type in the table, you can view its properties. Alternatively, you can use the Properties button.

Properties window presents the properties of the selected item together with **Additional fields** and **Alert rules** tabs.

Additional fields

Additional fields allow the Administrator to add field, which will be filled only with type for which it has been configured:



You can add global fields that will be visible and can be filled for each resource. **Global fields** are described in [the next chapter](#).

Alert rules

Asset alerts can be created for individual assets or for a selected type of assets. Alerts allow to configure notification for the Administrator when certain conditions are met.

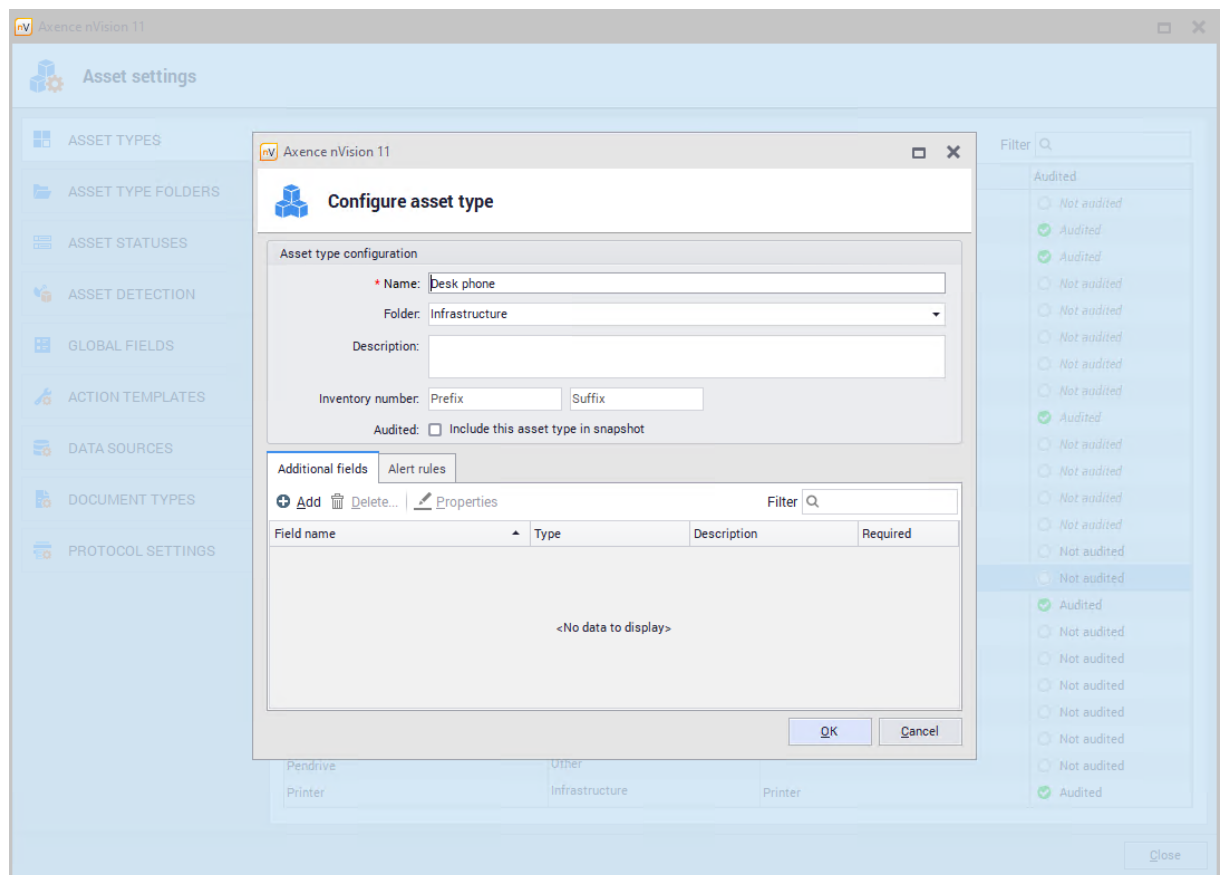
The **Asset rule** tab allows you to add an alert for a selected resource type.

To add an alert:

- Go to **Alert rules** tab and click **Add**.
- In the **Alert rules configuration window** select event(field) for which you want to create the alert and set the date the alert is to be created.

Adding new asset type

To add a new asset type, go to the **Asset Types** tab in the **Asset Settings** window and click the **Add** button. The new asset type wizard will appear:



Then fill the configuration fields. The required fields are "Name" and "Folder". You can also add additional fields for the asset type you are creating. Once the configuration, is complete, confirm the settings by pressing **OK**.

In the "Folder" field it is only possible to select an item from the list of available folders. For more information about folders, see [folder types](#) chapter.

Removing asset type

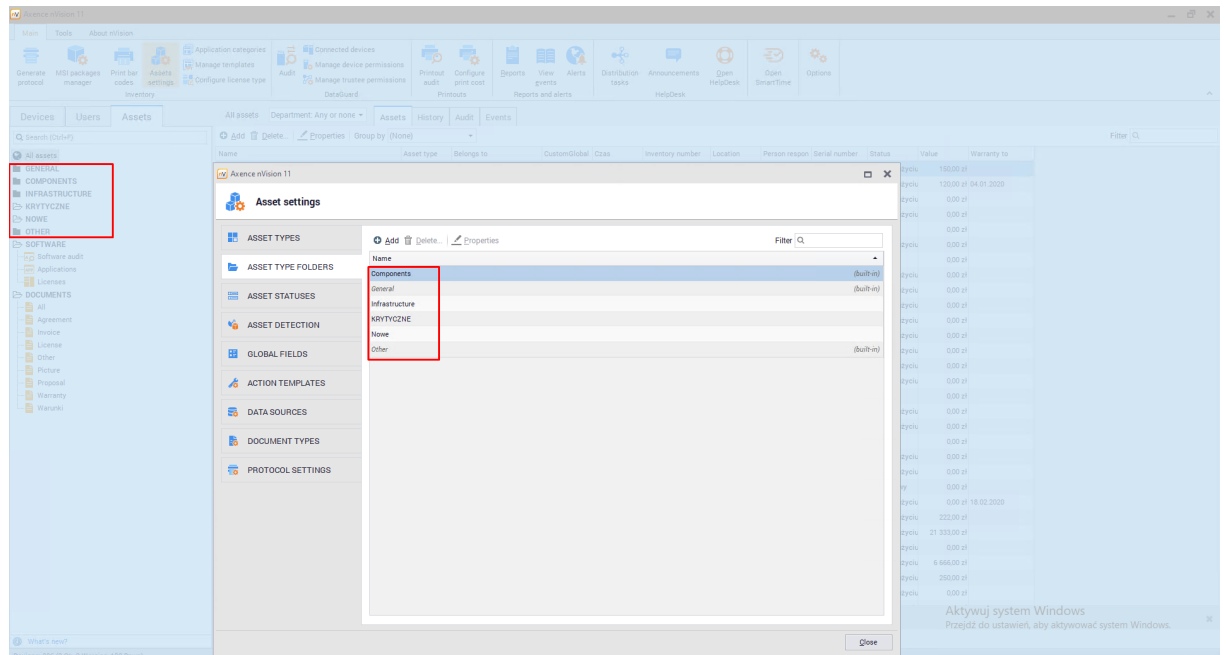
To delete an existing (non-built-in) asset type, go to the **Asset Types** tab in the **Asset Settings** window and click the **Delete** button.

If the selected type is in use, removing it will also delete all assets of this type.

8.2.3.4 Asset type folders

Asset type folders allow the Administrator to assign types to organizational units. The **Assets** tab, available from the main program window, allows you to display the folders and their types.

It is possible to display and modify the list of available folders. To do so, go to **Asset settings** window and then to the **Asset Type Folder** tab, you can display and modify the list of available folders:



Adding new asset folder

To add a folder, go to the **Asset Settings** window and then to the **Asset Type Folders** tab. Click the **Add** button, then enter the name of the new folder.

Adding an asset type to a selected folder is described in the [asset types](#) ²⁰⁰ chapter.

Removing new asset folder

To delete a folder, go to the **Asset Settings** window and then **Asset Type Folders** tab. After clicking **Delete**, the selected item will be deleted. After deleting the folder, all asset types present in this folder will be moved to the "Other" folder.

Built-in folders

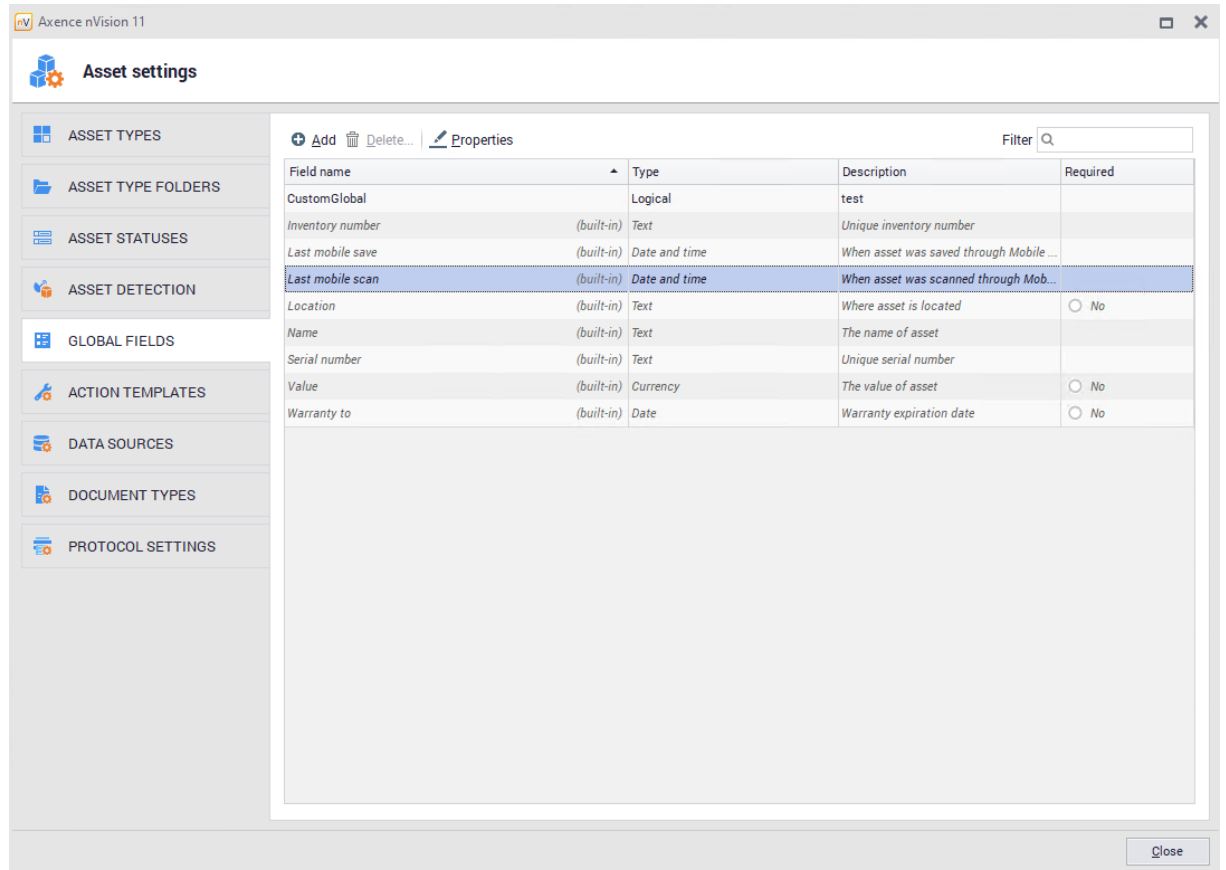
nVision offers several built-in folders for asset types::

- Basic (built-in),
- Components (built-in),
- Infrastructure devices,
- Mobile devices,
- Other (built-in).

Folders marked as built-in cannot be deleted or edited.

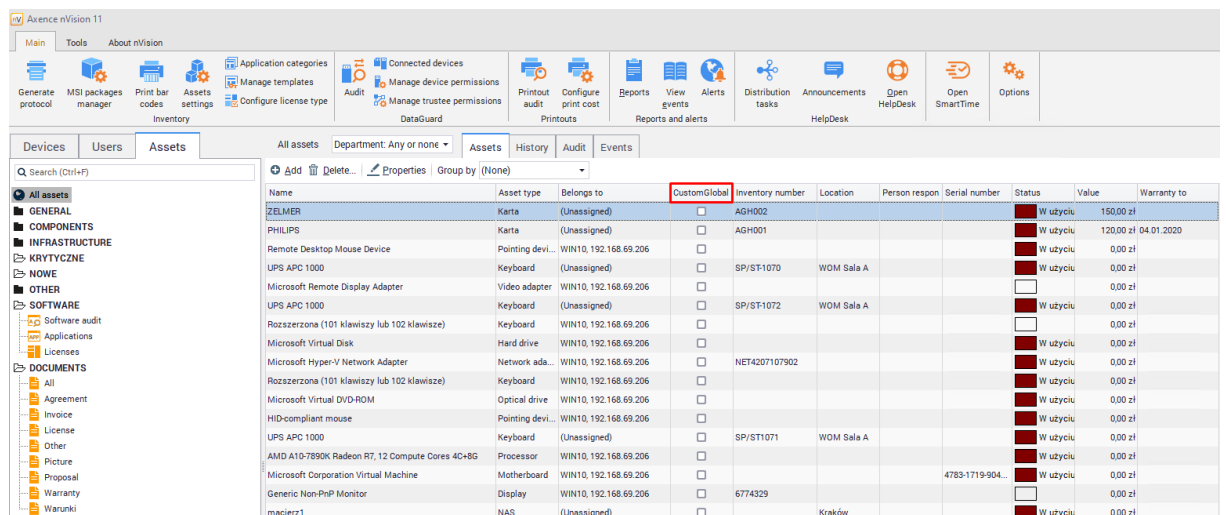
8.2.3.5 Global fields

Global Fields tab in the **Asset Settings** window allows the Administrator to add additional fields to all types of assets. The Administrator can create his own global fields that will store data of the selected type. Global fields must have unique names. All created global fields are presented in tabular form:



| Field name | Type | Description | Required |
|------------------|--------------------------|---|--------------------------|
| CustomGlobal | Logical | test | |
| Inventory number | (built-in) Text | Unique inventory number | |
| Last mobile save | (built-in) Date and time | When asset was saved through Mobile ... | |
| Last mobile scan | (built-in) Date and time | When asset was scanned through Mob... | |
| Location | (built-in) Text | Where asset is located | <input type="radio"/> No |
| Name | (built-in) Text | The name of asset | |
| Serial number | (built-in) Text | Unique serial number | |
| Value | (built-in) Currency | The value of asset | <input type="radio"/> No |
| Warranty to | (built-in) Date | Warranty expiration date | <input type="radio"/> No |

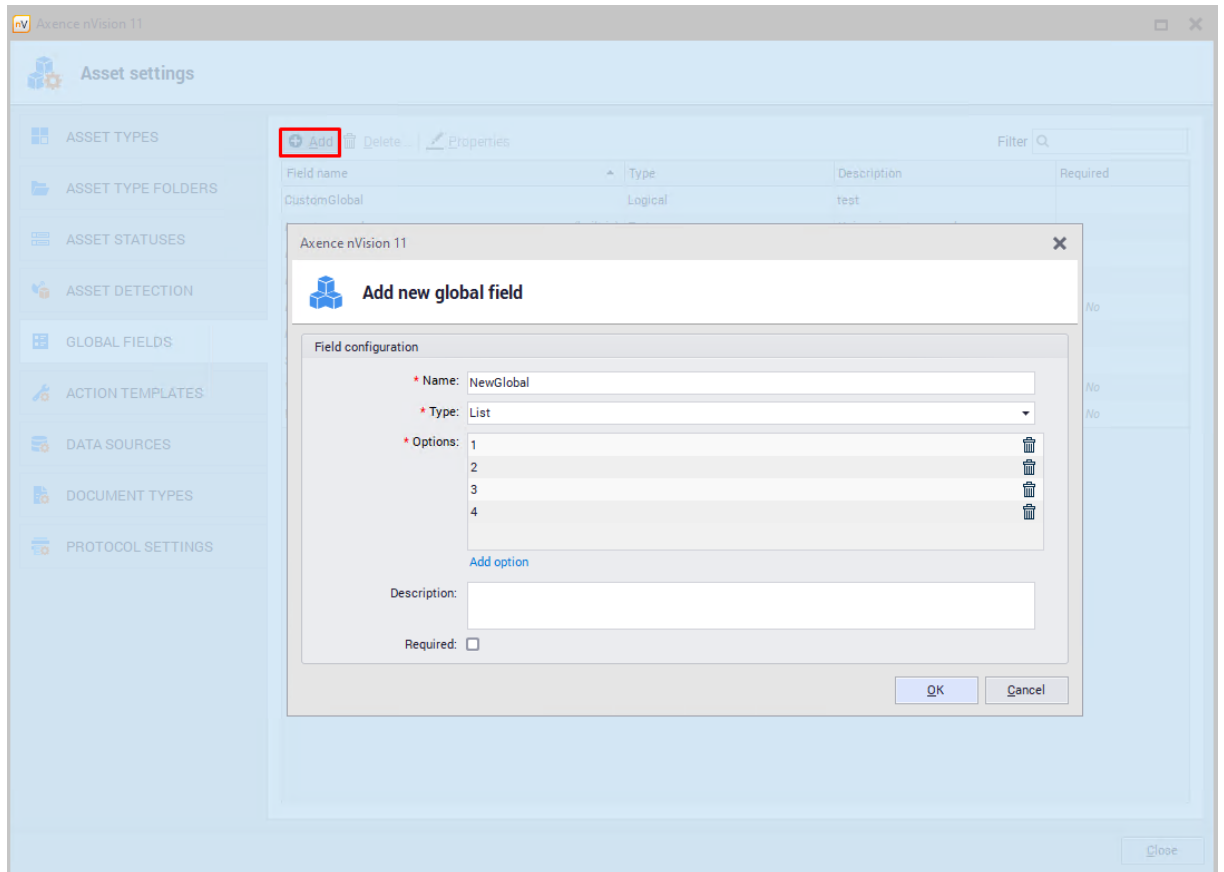
Global fields allow you to add additional information about the resource and extend the possibilities of selecting assets from the list. For example: after adding the 'CustomGlobal' global field, an additional column will be created with the value set to this field. By clicking the filter icon in this column you can filter lists in every column:



| Name | Asset type | Belongs to | CustomGlobal | Inventory number | Location | Person respon | Serial number | Status | Value | Warranty to |
|---|------------------|-----------------------|--------------------------|------------------|------------|---------------|------------------|----------|-----------|-------------|
| ZELMER | Karta | (Unassigned) | <input type="checkbox"/> | AGH002 | | | | W użyciu | 150,00 zł | |
| PHILIPS | Karta | (Unassigned) | <input type="checkbox"/> | AGH001 | | | | W użyciu | 120,00 zł | 04.01.2020 |
| Remote Desktop Mouse Device | Pointing devi... | WIN10, 192.168.69.206 | <input type="checkbox"/> | | | | | W użyciu | 0,00 zł | |
| UPS APC 1000 | Keyboard | (Unassigned) | <input type="checkbox"/> | SP/ST1070 | WOM Sala A | | | W użyciu | 0,00 zł | |
| Microsoft Remote Display Adapter | Video adapter | WIN10, 192.168.69.206 | <input type="checkbox"/> | | | | | | 0,00 zł | |
| UPS APC 1000 | Keyboard | (Unassigned) | <input type="checkbox"/> | SP/ST1072 | WOM Sala A | | | W użyciu | 0,00 zł | |
| Rozszerzona (101 klawiszy lub 102 klawisze) | Keyboard | WIN10, 192.168.69.206 | <input type="checkbox"/> | | | | | | 0,00 zł | |
| Microsoft Virtual Disk | Hard drive | WIN10, 192.168.69.206 | <input type="checkbox"/> | | | | | W użyciu | 0,00 zł | |
| Microsoft Hyper-V Network Adapter | Network ada... | WIN10, 192.168.69.206 | <input type="checkbox"/> | NET4207107902 | | | | W użyciu | 0,00 zł | |
| Rozszerzona (101 klawiszy lub 102 klawisze) | Keyboard | WIN10, 192.168.69.206 | <input type="checkbox"/> | | | | | W użyciu | 0,00 zł | |
| Microsoft Virtual DVD-ROM | Optical drive | WIN10, 192.168.69.206 | <input type="checkbox"/> | | | | | W użyciu | 0,00 zł | |
| HID-compliant mouse | Pointing devi... | WIN10, 192.168.69.206 | <input type="checkbox"/> | | | | | W użyciu | 0,00 zł | |
| UPS APC 1000 | Keyboard | (Unassigned) | <input type="checkbox"/> | SP/ST1071 | WOM Sala A | | | W użyciu | 0,00 zł | |
| AMD A10-7890K Radeon R7, 12 Compute Cores 4C+8G | Processor | WIN10, 192.168.69.206 | <input type="checkbox"/> | | | | | W użyciu | 0,00 zł | |
| Microsoft Corporation Virtual Machine | Motherboard | WIN10, 192.168.69.206 | <input type="checkbox"/> | | | | 4783-1719-904... | W użyciu | 0,00 zł | |
| Generic Non-PnP Monitor | Display | WIN10, 192.168.69.206 | <input type="checkbox"/> | 6774329 | | | | | 0,00 zł | |
| macierz1 | NAS | (Unassigned) | <input type="checkbox"/> | | Kraków | | | W użyciu | 0,00 zł | |

Adding global field

To add a global field, go to the **Asset settings / Global fields** window and click **Add**. The new global field configuration window will open:



Once the fields are filled, confirm the configuration with the **OK** button.

Removing global field

To delete a global field, go to the **Asset settings / Global fields** window and select **Delete**. **Deleting a global field will affect all the values it posses being lost on all assets.**

Built-in global fields

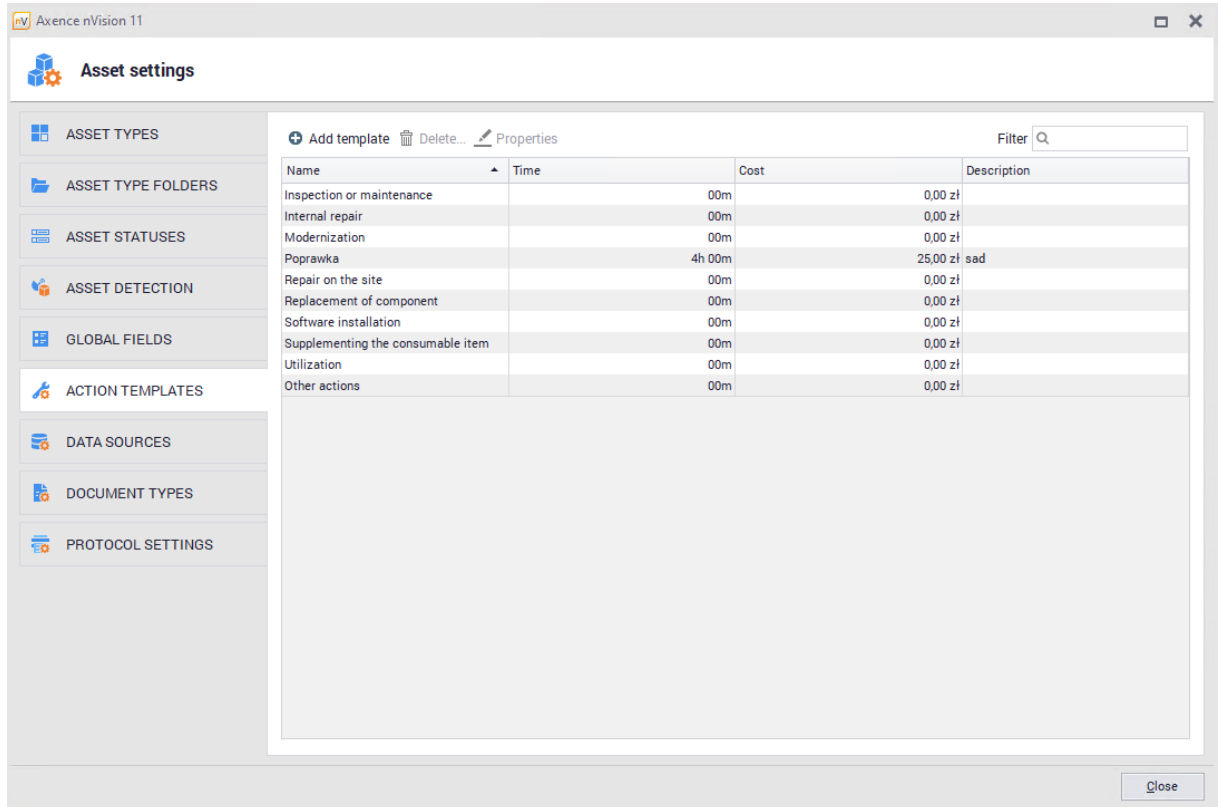
nVision offers several built-in global fields:

- Warranty to,
- Location,
- Name,
- Inventory number,
- Serial number,
- Last mobile save,
- Last mobile scan,
- Value.

Global fields marked as built-in cannot be deleted or edited.

8.2.3.6 Action templates

The functionality of adding activities for an asset allows you to add, display and delete activities performed on a selected asset. You can precisely describe the cost and activities carried out on individual assets. Task templates allow the Administrator to define a series of actions that can be performed on an asset. Using templates, assigning activities to a resource takes a few seconds and gives the possibility of fast edition (e.g. cost) at the time of adding.



Adding new action

To add a new action, go to the **Asset Settings** and select **Action Templates**. Click **Add template** button, the window for adding new asset action template will open.

"**Name**" is the only required field. The Administrator can add costs or date of performance information.

"**Change status to**" field will allow you to automatically change the asset status after adding the selected action to the asset

Adding actions to an asset is described [asset actions](#)¹⁸⁹ chapter.

Built-in actions

nVision offers several built-in action types::

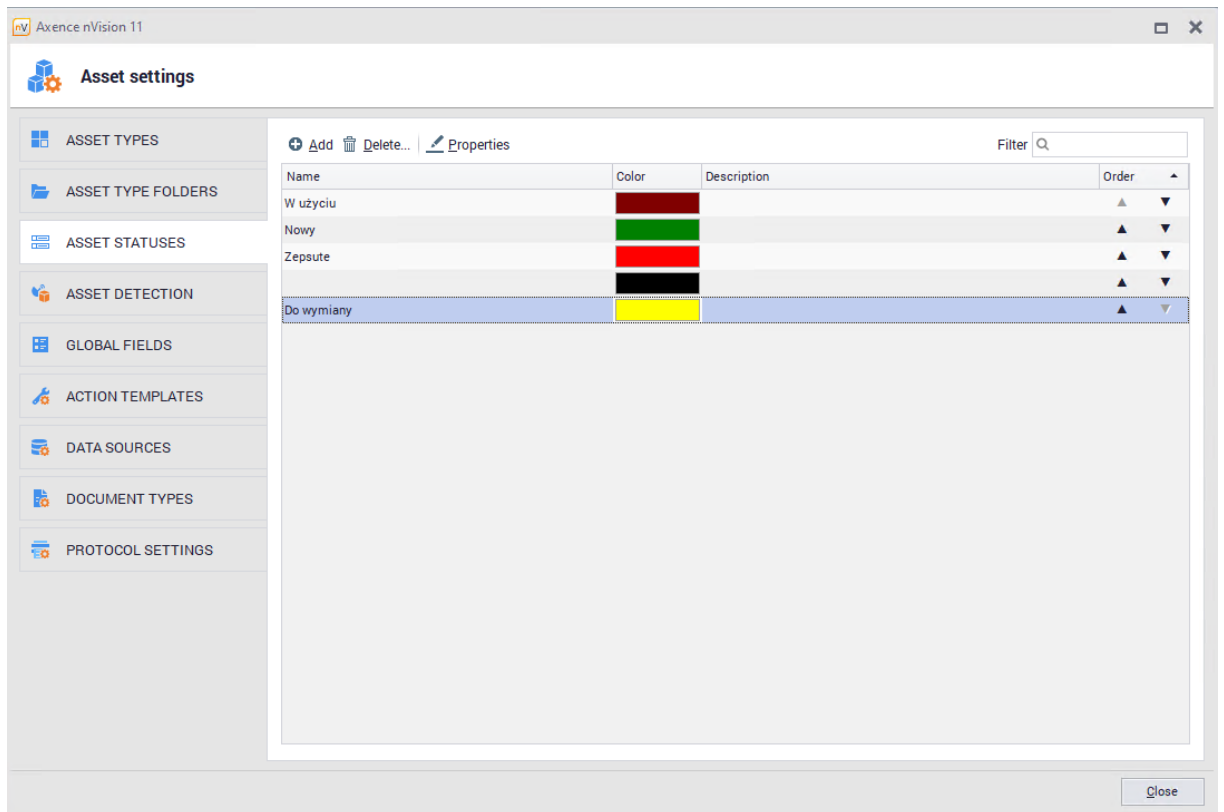
- Upgrade,
- Internal repair,
- External repair,
- Maintenance,
- Software installation,
- Component replacement,
- Resupplementation,

- Utilization,
- Other action.

The Administrator can edit and remove items from the list of built-in actions (excluding the "Other action" item).

8.2.3.7 Asset statuses

Asset statuses tab allows adding additional asset distinction and categorization. Each asset must always have exactly one status set. The list of available statuses is available in the **Asset settings / Asset statuses** tab:



All statuses are presented on the asset lists so that it is possible to filter and sort by status (according to the order of statuses in the list):

| Name | Asset type | Belongs to | Custom/Global | Inventory number | Location | Person respon | Serial number | Status | Value | Warranty to |
|---|------------------|----------------------|-------------------------------------|------------------|------------|---------------|------------------|--------|------------------------|-------------|
| Microsoft Virtual Disk | Hard drive | WIN10_192.168.69.206 | <input checked="" type="checkbox"/> | 7745617 | | | | Used | 0.00 zł | |
| Kość 1 | Memory | WIN10_192.168.69.206 | <input type="checkbox"/> | 3522963 | | | | New | 0.00 zł | |
| test2 | Testowy | (Unassigned) | <input type="checkbox"/> | OFFLINE1252996 | Kraków | | | New | 223.00 zł | |
| ZELMER | Karta | (Unassigned) | <input type="checkbox"/> | AGH002 | | | | Used | 150.00 zł | |
| PHILIPS | Karta | (Unassigned) | <input type="checkbox"/> | AGH001 | | | | Used | 120.00 zł (04.01.2020) | |
| Remote Desktop Mouse Device | Pointing devi... | WIN10_192.168.69.206 | <input type="checkbox"/> | | | | | Used | 0.00 zł | |
| UPS APC 1000 | Keyboard | (Unassigned) | <input type="checkbox"/> | SP/ST1070 | WDM Sala A | | | Used | 0.00 zł | |
| UPS APC 1000 | Keyboard | (Unassigned) | <input type="checkbox"/> | SP/ST1072 | WDM Sala A | | | Used | 0.00 zł | |
| Microsoft Virtual Disk | Hard drive | WIN10_192.168.69.206 | <input type="checkbox"/> | | | | | Used | 0.00 zł | |
| Microsoft Hyper-V Network Adapter | Network ada... | WIN10_192.168.69.206 | <input type="checkbox"/> | NET4207107902 | | | | Used | 0.00 zł | |
| Rozszerzona (101 klawiszy lub 102 klawisze) | Keyboard | WIN10_192.168.69.206 | <input type="checkbox"/> | | | | | Used | 0.00 zł | |
| Microsoft Virtual DVD-ROM | Optical drive | WIN10_192.168.69.206 | <input type="checkbox"/> | | | | | Used | 0.00 zł | |
| HID-compliant mouse | Pointing devi... | WIN10_192.168.69.206 | <input type="checkbox"/> | | | | | Used | 0.00 zł | |
| UPS APC 1000 | Keyboard | (Unassigned) | <input type="checkbox"/> | | | | | Used | 0.00 zł | |
| A10-7800K Radeon R7, 12 Compute Cores 4C+8G | Processor | WIN10_192.168.69.206 | <input type="checkbox"/> | SP/ST1071 | WDM Sala A | | | Used | 0.00 zł | |
| Microsoft Corporation Virtual Machine | Motherboard | WIN10_192.168.69.206 | <input type="checkbox"/> | | | | 4783-7119-904... | Used | 0.00 zł | |
| macieci1 | NAS | (Unassigned) | <input type="checkbox"/> | | | Kraków | | Used | 0.00 zł | |
| Microsoft Hyper-V Video | Video adapter | WIN10_192.168.69.206 | <input type="checkbox"/> | | | | | Used | 0.00 zł | |
| Generic PnP Monitor | Display | WIN10_192.168.69.206 | <input type="checkbox"/> | 9146256 | | | | Used | 0.00 zł | |
| 2 GB (Unknown) | Memory | WIN10_192.168.69.206 | <input type="checkbox"/> | | | | | Used | 0.00 zł | |
| Axence nVision Agent | Software (ob... | WIN10_192.168.69.206 | <input type="checkbox"/> | | | | | Used | 0.00 zł (18.02.2020) | |
| 123test | Testowy | Szpital | <input type="checkbox"/> | OFFLINE2861305 | wwa | | | Used | 222.00 zł | |
| 2134 | Testowy | (Unassigned) | <input type="checkbox"/> | OFFLINE1249425 | Kraków | | | Used | 21 333.00 zł | |
| Komputer admin | Network ada... | (Unassigned) | <input type="checkbox"/> | NET4202000564 | | Administrator | | Used | 0.00 zł | |
| qwe | Testowy | (Unassigned) | <input type="checkbox"/> | OFFLINE1280068 | Kraków | | | Used | 6 666.00 zł | |
| PANASONIC | Karta | (Unassigned) | <input type="checkbox"/> | AGH003 | | | | Used | 250.00 zł | |
| drukarka1 | Printer | (Unassigned) | <input type="checkbox"/> | 6539449 | | | | Used | 0.00 zł | |
| 123 | Computer | (Unassigned) | <input type="checkbox"/> | 8423387 | | | | Used | 0.00 zł | |
| test1 | Testowy | 192.168.69.1 | <input type="checkbox"/> | OFFLINE1454424 | Kraków | | | Used | 5.00 zł | |

Adding new asset status

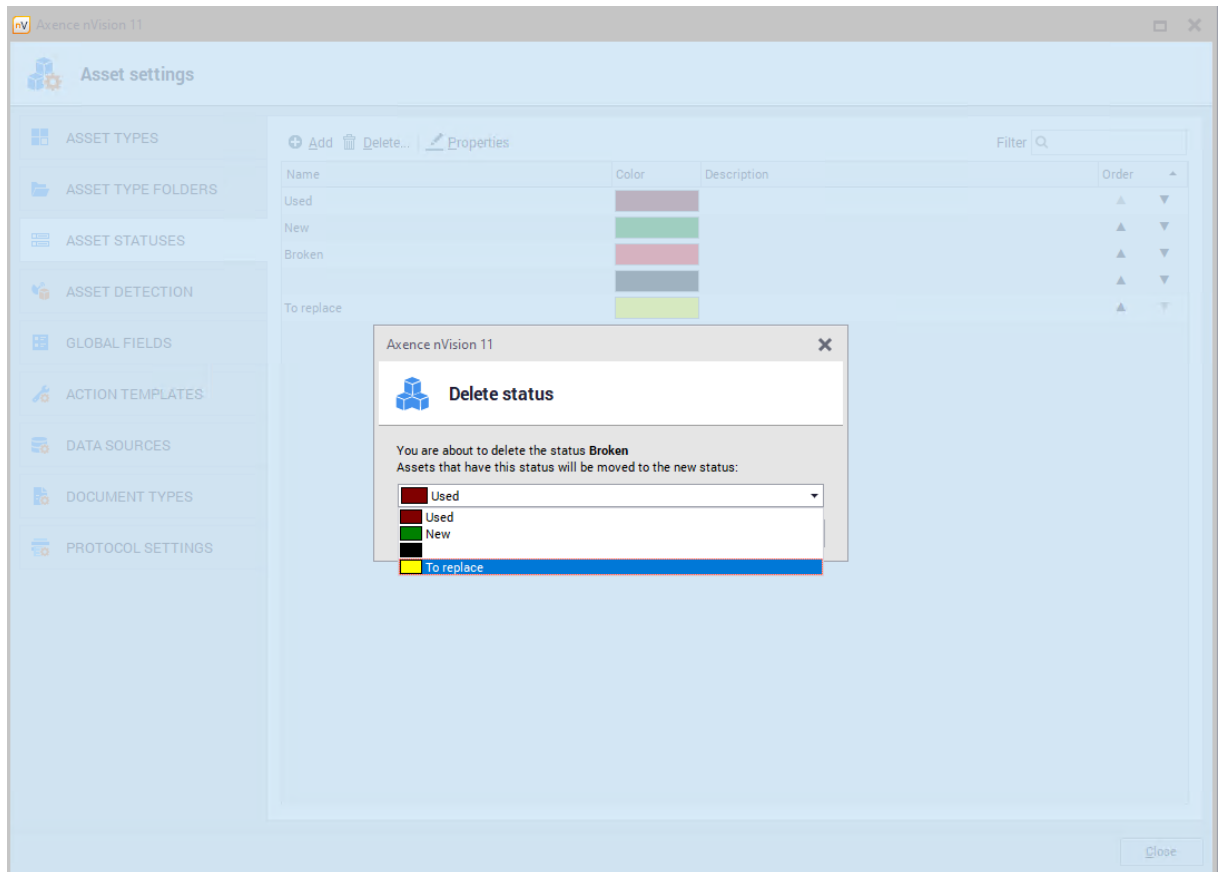
To add a new status, go to the **Asset Settings** window and select **Asset statuses**. After clicking the **Add** button, the window for adding a new status will open.

Fields "Name" and "Color" are required. The Administrator can include additional information and determine whether the status should be the default for new resources.

Adding status to a n asset is described in the [asset status](#) ^[208] chapter.

Removing asset status

To remove status, go to the **Asset Settings** window and select **Asset Statuses**. Status can be deleted by selecting it from the list and clicking **Delete** button. You must indicate a new status for assets that currently use the removed status.



Built-in statuses

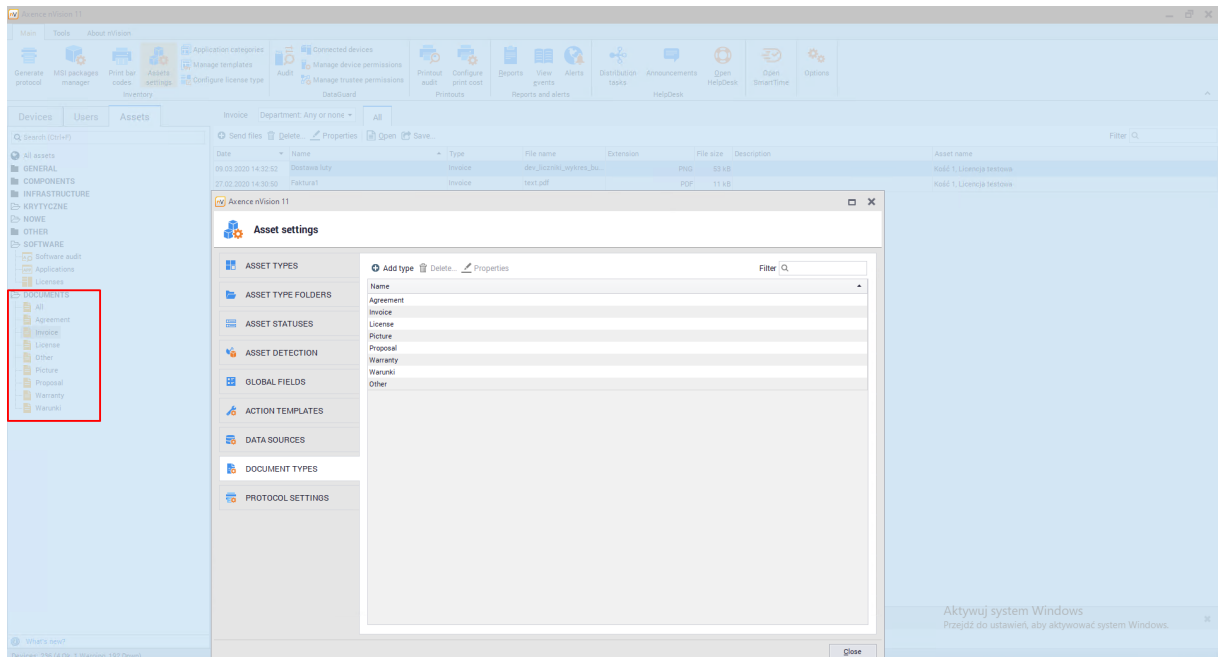
nVision offers several built-in status types:

- New (default for new resources);
- In use;
- In storage - operational;
- In storage - broken;
- In repair;
- To be disposed;
- Sold;
- Disposed;
- Lost.

8.2.3.8 Document types

Document types tab allows you to link an attachment (file) to an asset. The administrator can add, edit or delete document types.

Document types allow for more precise categorization of documents added to the program's database. You can also display documents by type from the **Asset** window in the main program console:



Adding new document type

To add a new document type, go to the **Asset Settings** and select **Document Types**. Click the **Add type** button, the window for adding a new type will open.

Types can be assigned to documents while documents are added or edited. These operations are described in [documents](#) ¹⁸⁶ chapter.

Removing document types

To delete a document type, go to the **Asset Settings** window and select **Document Types**. Click **Delete** button to remove the selected item. Documents which type has been deleted will be assigned to the "Other" type.

Built-in document types

nVision offers several built-in document types:

- Invoice,
- Contract,
- Request,
- License,
- Warranty,
- Picture,
- Other (special type which cannot be edited or removed).

8.2.3.9 Protocol Templates

In the nVision 13.5 version, the functionality of the protocol template generator was introduced, replacing the existing solution, which allows for the generation of resource transfer protocols. The functionality of generating templates allows you to create many different templates depending on the requirements and needs of a given organization.

Protocol templates can be copied, deleted (all protocol templates cannot be deleted - nVision must have at least 1 protocol template) and edited. Every Administrator with access to the Inventory module in nVision has access to both the protocol generator and the list of created templates.


After going to the **Asset Settings** tab, and then to the **Protocol templates** tab, the Administrator has the option to set certain constants for each property protocol, and to add a [protocol template](#)^[220].

The administrator can configure globally some of the protocol parameters, e.g. :

- Company's data

1. Logo

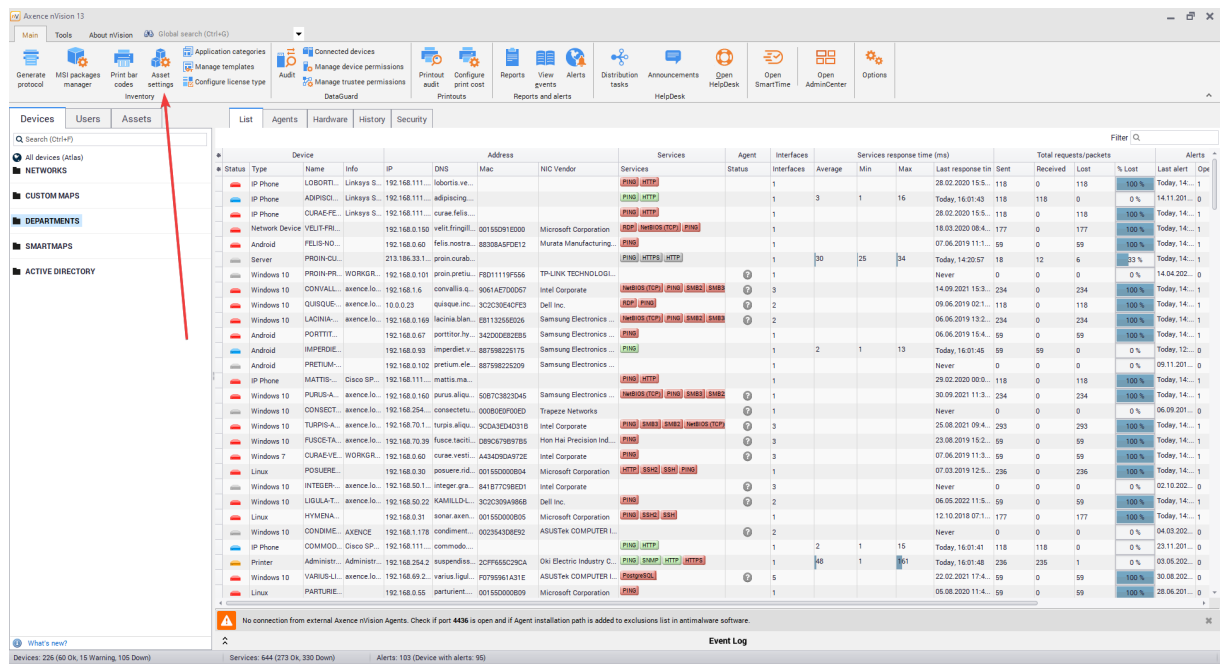
It is possible to add a logo that will be added to the header of all protocol templates. To add a logo,

click the icon  and select a graphic file. To remove the logo, use the button .

2. Address

To add an address to the protocol header, this text field must be completed.

The process of adding protocol templates and generating protocols from them is described in the [Generating protocols](#)^[220] chapter.

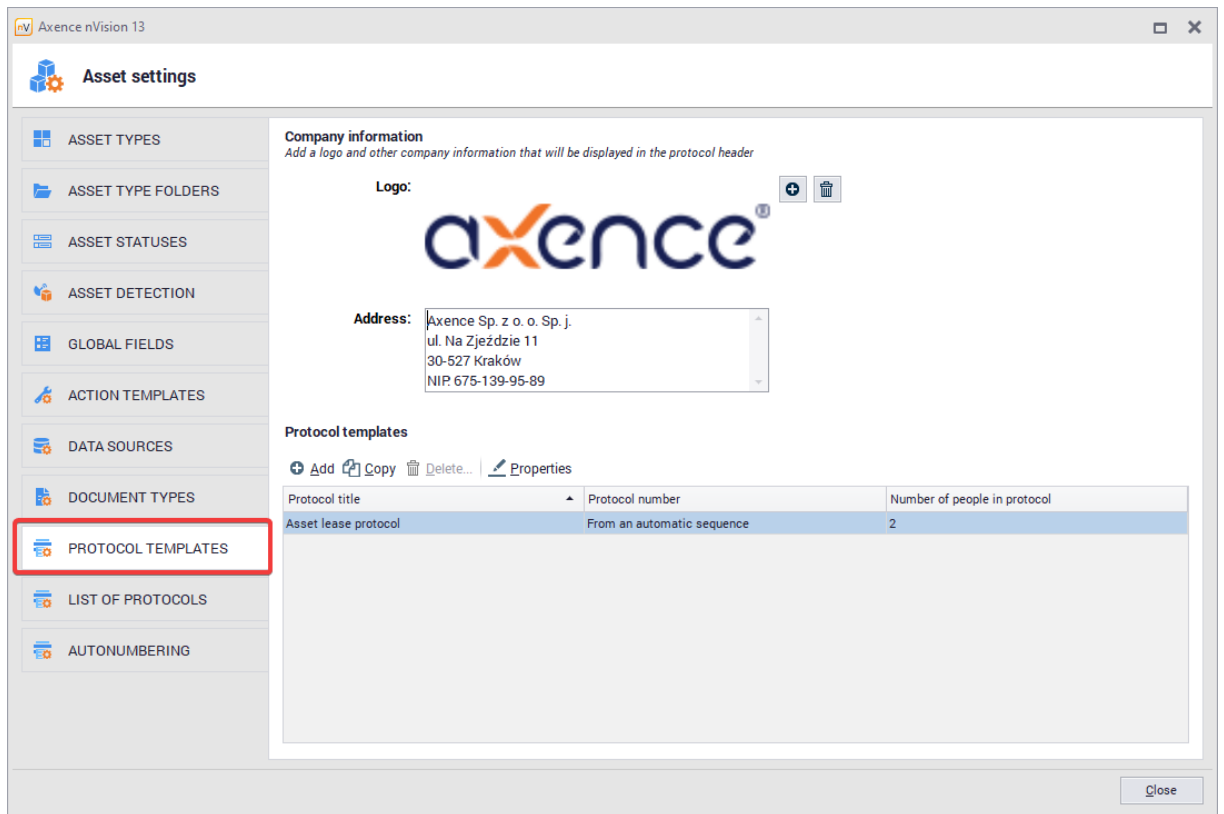


The screenshot shows the Axence nVision 13 interface. The top navigation bar includes tabs for Main, Tools, About nVision, and Global search (Ctrl+G). Below this is a toolbar with icons for various functions like Generate protocol, MSI packages manager, Print bar codes, Asset settings, Configure license type, Connected devices, Manage device permissions, Audit, Manage trustee permissions, DataGuard, Printout, Configure print cost, Reports, View, Alerts, Distribution tasks, Announcements, Open HelpDesk, Open SmartTime, Open AdminCenter, and Options.

The main content area is divided into several sections. On the left, there are navigation tabs for Devices, Users, and Assets. The 'Assets' tab is selected, and a red arrow points to it. Below the navigation tabs is a search bar and a list of categories: All devices (Atlas), NETWORKS, CUSTOM MAPS, DEPARTMENTS, SMARTMAPS, and ACTIVE DIRECTORY.

The central part of the screen displays a table of devices. The table has columns for Status, Type, Name, Info, IP, DNS, Mac, NIC Vendor, Services, Agent, Interfaces, Services response time (ms), and Total requests/packets. The table contains multiple rows of device information, including IP phones, network devices, servers, and various operating systems like Windows 10, Linux, and Android.

At the bottom of the interface, there is a status bar showing 'Devices: 226 (80 OK, 15 Warning, 105 Down)', 'Services: 644 (273 OK, 330 Down)', and 'Alerts: 133 (Device with alerts: 95)'. There is also an 'Event Log' section.



8.2.3.10 Protocols

In the nVision 13.5 version, the functionality of the [protocol template generator](#)^[220] was introduced. In **Asset Settings**, in the **Protocols** tab, Administrators who have access to the Inventory module in nVision can view the list of protocols generated by the system in the form of a table. The table consists of several columns:

- Protocol title
- Protocol number
- Date
- Assets (count)
- People (count)

The table can be filtered by the protocol title and also searched by keywords using the search engine.

The following actions are available from the protocol history window:

- Add - opens the protocol generation window
- Delete - deletes the given protocol
- Open - opens the given protocol in the browser
- Save - allows you to export a given protocol in .PDF format

nV Axence nVision 13
✕

New protocol template

Basic informations

* **Protocol title:**

* **Protocol number:**

Protocol description:

Closing remarks:

People names

Names for people who participate in the activity described by the protocol (for example: "Returner", "Receiver", "Acceptor" etc.)

* **Number of people in protocol:**

* **Name of 1st person:**

* **Name of 2nd person:**

Protocol columns

Add (up to 10) columns that will be included in the protocol

| Column name | Field type (not displayed in reports) |
|----------------------|---------------------------------------|
| <No data to display> | |

8.2.3.11 Autonumbering

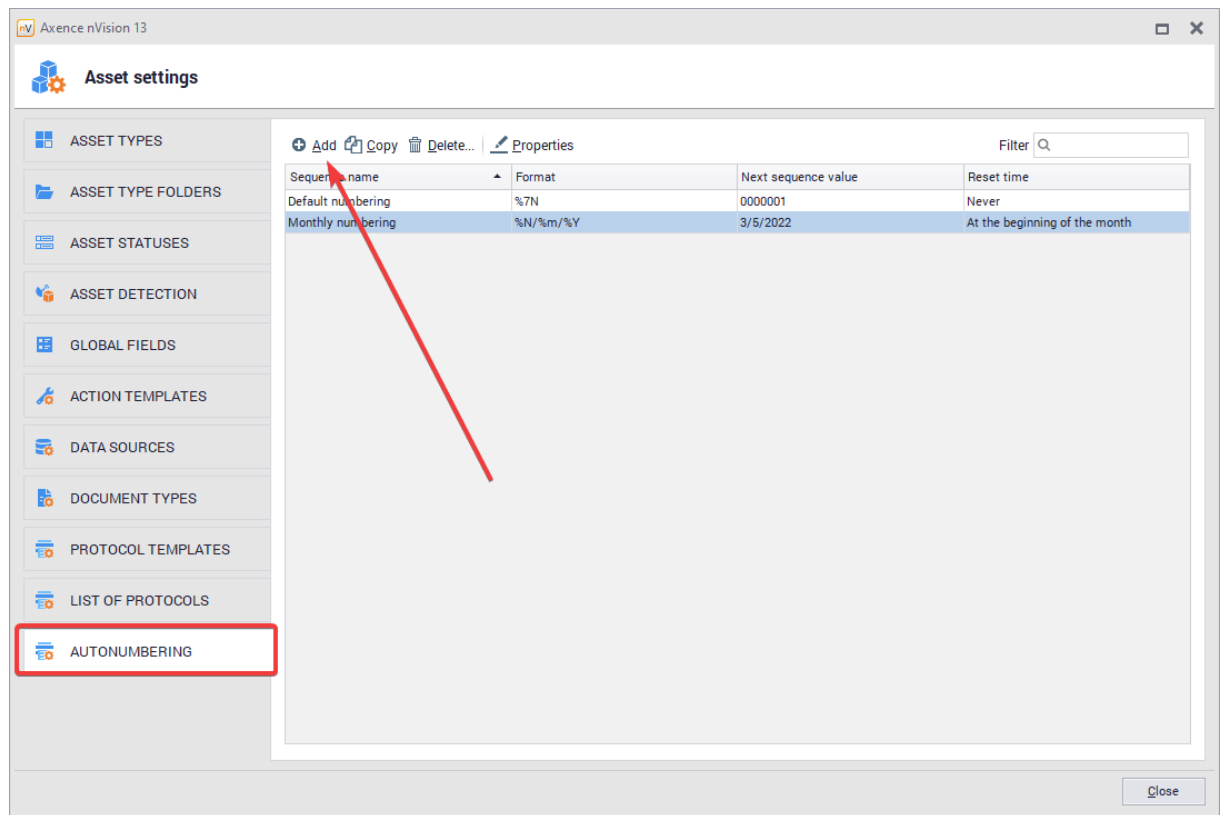
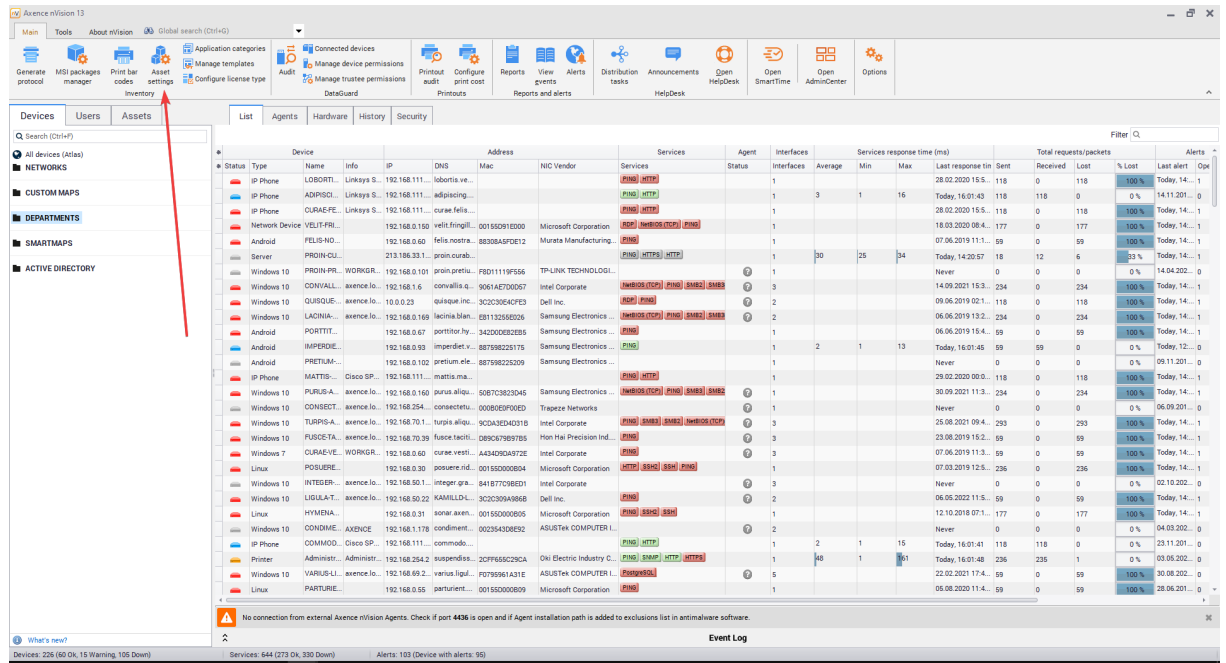
The autonumbering functionality has been introduced in nVision 13.5. This chapter describes how to add an auto-numbering sequence and how it applies to your system.

Autonumbering is primarily used to facilitate the inventory of assets and documents in the nVision console. Having created several autonumbering sequences, e.g. due to the type of asset, protocol or license, we can easily and transparently track the progress and changes in our organization.

Adding an auto-numbering sequence

To add an autonumbering sequence:

1. In the main nVision console window, click on the **Main tab**, and then on **Asset settings**.
2. Click on the **AutoNumber** tab.
3. Click on **Add button**.



In the window for adding autonumbering sequences, certain parameters have to be configured. First of all, establish a unique name for the AutoNumber sequence (there cannot be two sequences with the same name in your system), and then proceed to creating the AutoNumber Sequence format.

The auto-number sequence format consists of several elements. The format must contain the **%xN** variable - where x is the number of digits, e.g. if we enter **%5N**, the sequence number will consist of five digits. The format may also contain other optional elements:

- **%D** - current day, with a zero in front, **%d** - without a zero in front
- **%M** - current month, with a zero in front, **%m** - without a zero in front
- **%R** - current month (written in Roman characters)
- **%Y** - current year
- any text, e.g. a hint as to what type of an asset is autonumbered

An example of an autonumbering sequence: **Printer %4N %D %M %Y**, that will translate into **Printer 0241 05 07 2022**.

Additionally, you can set whether the sequence is to be reset, so its value will be reduced to 1. Available reset options:

- never (default)
- at the beginning of the month
- at the beginning of the year

The auto-numbering sequence can be edited (after selecting a specific sequence and clicking on the **Properties** button), deleted (after selecting and clicking on the **Delete** button, or copied (after selecting and clicking on the **Copy** button).

There is no autonumbering sequence limit in nVision, therefore, depending on the needs, size of the organization, types of supported assets, licenses or documents, the administrator can create an appropriate number of unique auto-numbering sequences.

Assign an autonumbering sequence to an asset type

The procedure for adding an AutoNumber sequence is described above. Having at least 1 autonumbering sequence ready, we can use it in practice, i.e. assign it to a given type of resource.

To do this, you must:

1. In the main nVision console window, click on the **Main** tab, and then on **Asset settings**. By default, the **Asset Types** tab is displayed, this is where we assign the autonumbering sequence.
2. If no asset type exists in the system, you must [add](#)²⁰⁰ it first
3. When you have an asset type ready, you need to select it - by clicking on it in the table, and then clicking the **Properties** button (the autonumbering sequence can also be assigned when adding a new resource type).
4. Click on the **Inventory number** field, and then select **Automatically from sequence** from the pull-out list.
5. After completing the above step, a previously unavailable field will be displayed below the Inventory number field. Click on them, and then from the list select the sequence that you want to assign to the given type of asset.
6. To confirm the changes made, click the **OK** button.

From now on, the selected autonumbering sequence will apply to the selected asset type. The same autonumbering sequence can be used for many different types of protocol, assets or licenses, but as it can create unnecessary confusion, it is recommended to create separate, unique autonumbering sequences for different types of objects (even if the only difference between the sequences will be on their unique name).

Assign an autonumbering sequence to a protocol template

Autonumbering sequences can be assigned not only to a asset type, but also, inter alia, to also to the individual protocol templates. The procedure is the same as for resources. First, add an auto-numbering sequence and create a protocol template on the system.

To assign an auto-number sequence to a document type you must:

1. In the main nVision console window, click on the **Main** tab, and then on **Asset settings**.
2. Click on the **Protocol templates** tab..
3. Click on the protocol displayed on the list, and then click on the **Properties** button (the autonumbering sequence can also be assigned when adding a new protocol template)
4. Click the **Protocol number** field, and then select **Automatically from sequence** from the drop-down list.
5. After completing the above step, a previously unavailable field will be displayed below the Protocol number field. Click on them, and then from the list select the sequence that you want to assign to the given type of an asset.
6. To confirm the changes made, click the **OK** button.

From now on, the selected autonumbering sequence will apply to the selected asset type. The same autonumbering sequence can be used for many different types of protocol, assets or licenses, but as it can create unnecessary confusion, it is recommended to create separate, unique autonumbering sequences for different types of objects (even if the only difference between the sequences will be on their unique name).

Assign an autonumbering sequence to a license

You can assign an autonumbering sequence to a license in two ways. First of all, it can be done already at the stage of configuring a new license type. For this you should:

1. In the main nVision console window, click on the **Main** tab and then on **Configure license type**.
2. Click the **Inventory number** field, and then select **Automatically from sequence** from the pull-out list.
3. After completing the above step, a previously unavailable field will be displayed below the Inventory number field. Click on them, and then from the list select the sequence that you want to assign to the given license type.
4. The next step is to correctly fill in the remaining fields of the form, and then click the **Ok** button.

From now on, the selected autonumbering sequence will apply to the selected asset type. The same autonumbering sequence can be used for many different types of protocol, assets or licenses, but as it can create unnecessary confusion, it is recommended to create separate, unique autonumbering

sequences for different types of objects (even if the only difference between the sequences will be on their unique name).

The auto-numbering sequence can also be assigned to a license type that already exists in the system. To do this::

1. In the main nVision console window, click on the **Main** tab, and then on **Assets**.
2. Then find the **Software folder** and click **Licenses**.
3. The list on the right will display all the licenses saved in the nVision system. To view the properties of a selected license, double-click it or select the appropriate license and click the **Properties** button.
4. In the license information window, click on the **Inventory number** field, and then select **Automatically from sequence** from the pull-out list.
5. After completing the above step, a previously unavailable field will be displayed below the Inventory number field. Click on them, and then from the list select the sequence that you want to assign to the given license type.

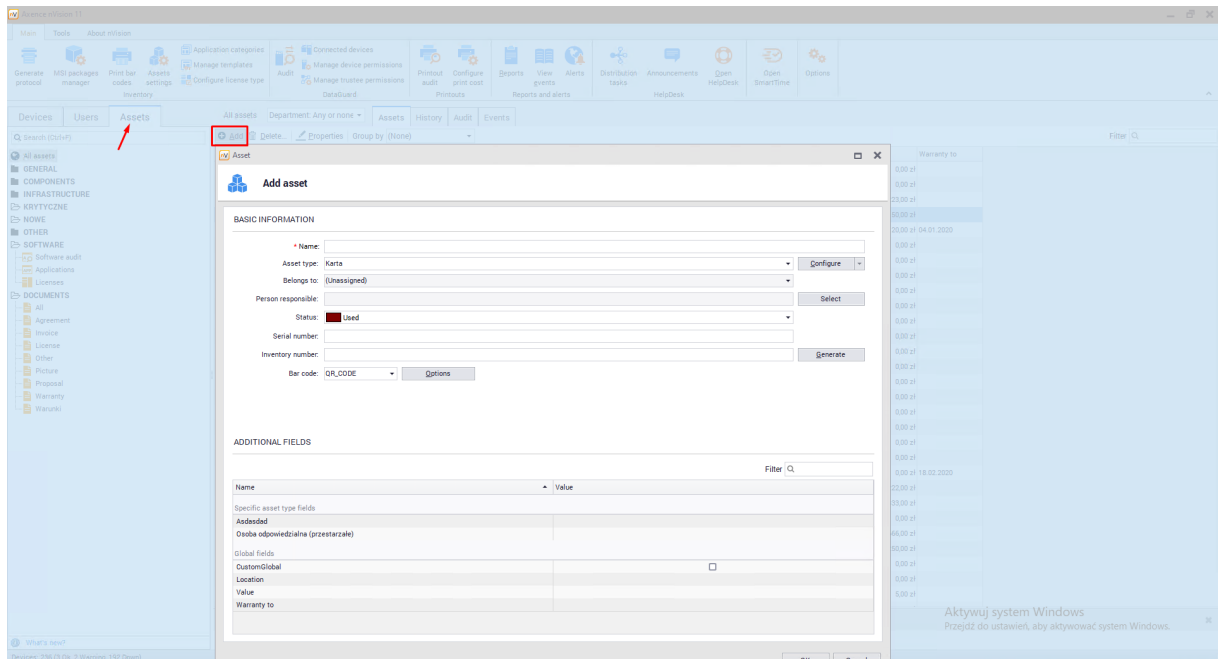
From now on, the selected autonumbering sequence will apply to the selected asset type. The same autonumbering sequence can be used for many different types of protocol, assets or licenses, but as it can create unnecessary confusion, it is recommended to create separate, unique autonumbering sequences for different types of objects (even if the only difference between the sequences will be on their unique name).

8.2.4 Asset creation and modification

Assets in nVision can be created automatically using data from the Agent or manually. The configuration and removal of automatic asset detection is described in the chapter [asset autodetection](#).¹⁹⁸

Adding new asset

To add a new asset, go to the **Assets tab** accessible from the main program window. To add a new asset, select the **Add** option from the toolbar above the assets table or select **Add** from the context menu. The window for adding a new resource will open:



The next steps include completing the individual fields that specify assets properties. The available fields are explained in the [asset properties](#) ¹⁸⁴ chapter.

Asset modification

To change the asset properties, go to the **Assets** tab available from the main program window. Find the asset on the list, go to the properties window, select appropriate button or double-clicking on the selected item. The asset editing window will open:

The screenshot shows the 'Asset' management window for 'Kość 1'. The interface is divided into a left sidebar with navigation options (GENERAL, DOCUMENTS, ACTIONS, HISTORY, ALERTS, WHO CAN USE) and a main content area. The main area is titled 'BASIC INFORMATION' and contains several fields:

- Name:** Kość 1
- Asset type:** Memory (with a 'Configure' button)
- Belongs to:** WIN10, 192.168.69.206
- Person responsible:** (empty field with a 'Transfer' button)
- Status:** New (indicated by a green square)
- Serial number:** 21esczxc
- Inventory number:** 3522963 (with a 'Generate' button)
- Bar code:** QR_CODE (with an 'Options' button)

Below the basic information is a QR code and an 'ADDITIONAL FIELDS' section. This section includes a search filter and a table with the following data:

| Name | Value |
|-------------------------------------|--------------------------|
| Specific asset type fields | |
| Bits | |
| Capacity | 4 GB |
| Częstotliwość | 4333 |
| Osoba odpowiedzialna (przestarzałe) | |
| Slot | None |
| Speed | |
| Type | Unknown |
| Global fields | |
| CustomGlobal | <input type="checkbox"/> |

A 'Close' button is located at the bottom right of the window.

Available modifications and explanations are described in the [asset properties](#) ¹⁸⁴ chapter.

Asset removal

To remove a resource, go to the **Assets** tab available from the main program window. Find the asset in the list, click the **Delete** button or select the option from the context menu.

8.2.5 Generating protocol

In the nVision 13.5 version, the functionality of the protocol template generator was introduced, replacing the existing solution, which allows for the generation of asset transfer protocols. The functionality of generating templates allows you to create many different templates depending on the requirements and needs of a given organization.

Protocol templates can be copied, deleted (all protocol templates cannot be deleted - nVision must have at least 1 protocol template) and edited. Every Administrator with access to the Inventory module in nVision has access to both the protocol generator and the list of created templates.

To go to the template generator tab, in the main console window, click the **Asset settings** button (located on the main toolbar), and then select the **Protocol templates** tab.

The screenshot shows the Axence nVision 13 interface with the 'Assets' tab selected. The main area displays a table of network devices with columns for Status, Type, Name, Info, IP, DNS, Address, Services, Agent, Interfaces, Services response time (ms), Total requests/packets, and Alerts. A red arrow points to the 'Assets' tab in the top navigation bar.

| Status | Type | Name | Info | IP | DNS | Address | Services | Agent | Interfaces | Average | Min | Max | Last response (m) | Sent | Received | % Lost | Last alert | |
|----------------|--------------|--------------|----------------|---------------|----------------|--------------|---------------------------|-----------------------------------|------------|---------|-----|-----|--------------------|------|----------|--------|--------------|--------------|
| IP Phone | LOBORTL | Linksys G... | lobortl.v... | 192.168.111.1 | lobortl.v... | | [PNS] [HTTP] | | 1 | | | | 28.02.2020 15:5... | 118 | 0 | 100 % | Today, 14... | |
| IP Phone | ADPISCI | Linksys G... | adpiscio... | 192.168.111.1 | adpiscio... | | [PNS] [HTTP] | | 1 | 3 | 1 | 16 | 28.02.2020 15:5... | 118 | 0 | 100 % | Today, 14... | |
| IP Phone | CURAEFE | Linksys G... | curae fel... | 192.168.111.1 | curae fel... | | [PNS] [HTTP] | | 1 | | | | 28.02.2020 15:5... | 118 | 0 | 100 % | Today, 14... | |
| Network Device | VELIFSL | | velif.fingl... | 192.168.0.160 | velif.fingl... | 00150291E200 | Microsoft Corporation | [PNS] [HTTP] [TCP] [PNS] | 1 | | | | 18.03.2020 08:4... | 177 | 0 | 100 % | Today, 14... | |
| Android | FELISNO | | felis.nostr... | 192.168.0.60 | felis.nostr... | 8830B48FD212 | Mureta Manufacturing | [PNS] | 1 | | | | 07.06.2019 11:1... | 99 | 0 | 100 % | Today, 14... | |
| Server | PROIN-CU | | proin.cura... | 213.186.33.1 | proin.cura... | | | [PNS] [HTTPS] [HTTP] | 1 | 30 | 25 | 34 | Today, 14:20:57 | 18 | 12 | 6 | 33 % | Today, 14... |
| Windows 10 | PROIN-PR | WORKING | proin.pret... | 192.168.0.101 | proin.pret... | F8D1119F556 | TP-LINK TECHNOLOGI... | | 1 | | | | Never | 0 | 0 | 0 | 0 % | 14.04.202... |
| Windows 10 | CONVALL | axence.io | convall.g... | 192.168.1.6 | convall.g... | 9061AET00067 | Intel Corporate | [HTTPS(TCP)] [PNS] [SMTP] [SMTP] | 3 | | | | 14.09.2021 15:3... | 234 | 0 | 234 | 100 % | Today, 14... |
| Windows 10 | OURSQUE | axence.io | oursque.i... | 192.168.0.23 | oursque.i... | 3C2C30E4CFE3 | Dell Inc. | [TCP] [PNS] | 2 | | | | 09.06.2019 02:1... | 118 | 0 | 118 | 100 % | Today, 14... |
| Windows 10 | LACINIA | axence.io | lacinia.bl... | 192.168.0.169 | lacinia.bl... | E811326E0205 | Samsung Electronics | [HTTPS(TCP)] [PNS] [SMTP] [SMTP] | 2 | | | | 06.06.2019 13:2... | 234 | 0 | 234 | 100 % | Today, 14... |
| Android | PORTIT | | portitor.hy... | 192.168.0.67 | portitor.hy... | 342D008E2E85 | Samsung Electronics | [PNS] | 1 | | | | 06.06.2019 15:4... | 99 | 0 | 99 | 100 % | Today, 14... |
| Android | IMPERDIE | | imperdiet... | 192.168.0.93 | imperdiet... | 88798823175 | Samsung Electronics | [PNS] | 1 | 2 | 1 | 13 | Today, 16:01:45 | 99 | 59 | 0 | 0 % | Today, 12... |
| Android | PRETIAM | | pretium.e... | 192.168.0.102 | pretium.e... | 88798823209 | Samsung Electronics | [PNS] | 1 | | | | Never | 0 | 0 | 0 | 0 % | 09.11.201... |
| IP Phone | MATTIS | Cisco SP... | mattis.ma... | 192.168.111.1 | mattis.ma... | | | [PNS] [HTTP] | 1 | | | | 29.02.2020 00:0... | 118 | 0 | 118 | 100 % | Today, 14... |
| Windows 10 | PURUS-A | axence.io | purus.ali... | 192.168.0.160 | purus.ali... | 5087C3823045 | Samsung Electronics | [HTTPS(TCP)] [PNS] [SMTP] [SMTP] | 1 | | | | 30.09.2021 11:3... | 234 | 0 | 234 | 100 % | Today, 14... |
| Windows 10 | CONSECT | axence.io | consectu... | 192.168.254 | consectu... | 00080E090ED | Trapeze Networks | | 1 | | | | Never | 0 | 0 | 0 | 0 % | 06.09.201... |
| Windows 10 | TURPSA-L | axence.io | turpsa.ali... | 192.168.70.1 | turpsa.ali... | 9CDA3ED4D31B | Intel Corporate | [PNS] [SMTP] [SMTP] [SMTP] [SMTP] | 3 | | | | 25.08.2021 09:4... | 293 | 0 | 293 | 100 % | Today, 14... |
| Windows 10 | FUSCE-TA | axence.io | fusce.tact... | 192.168.70.39 | fusce.tact... | 086267969789 | High Precision Ind... | [PNS] | 2 | | | | 23.08.2019 16:2... | 99 | 0 | 99 | 100 % | Today, 14... |
| Windows 7 | CURPAE-VE | WORKING | curae vest... | 192.168.0.60 | curae vest... | A43492047472 | Intel Corporate | [PNS] | 3 | | | | 07.06.2019 11:3... | 99 | 0 | 99 | 100 % | Today, 14... |
| Linux | POURJERE | | pourjere... | 192.168.0.30 | pourjere... | 001550300804 | Microsoft Corporation | [HTTP] [SMTP] [SMTP] [SMTP] | 1 | | | | 07.03.2019 12:5... | 236 | 0 | 236 | 100 % | Today, 14... |
| Windows 10 | INTEGEB | axence.io | integere... | 192.168.80.1 | integere... | 841877048E01 | Intel Corporate | | 2 | | | | Never | 0 | 0 | 0 | 0 % | 02.10.202... |
| Windows 10 | LIGULA-T | axence.io | ligula.t... | 192.168.0.22 | ligula.t... | 3C2C309A9868 | Dell Inc. | [PNS] | 2 | | | | 06.05.2022 11:5... | 99 | 0 | 99 | 100 % | Today, 14... |
| Linux | HYMENA | | hymar aren... | 192.168.0.31 | hymar aren... | 0015309A0005 | Microsoft Corporation | [PNS] [SMTP] [SMTP] | 1 | | | | 12.10.2019 07:1... | 177 | 0 | 177 | 100 % | Today, 14... |
| Windows 10 | CONDIME | AXENCE | condimend... | 192.168.1.178 | condimend... | 00235410E892 | ASUSTek COMPUTER L... | | 2 | | | | Never | 0 | 0 | 0 | 0 % | 04.03.202... |
| IP Phone | COMMODO | Cisco SP... | commodo... | 192.168.111.1 | commodo... | | | [PNS] [HTTP] | 1 | 2 | 1 | 15 | Today, 16:01:41 | 118 | 118 | 0 | 0 % | 23.11.201... |
| Printer | Administr... | Administ... | suspendis... | 192.168.254.2 | suspendis... | Z0FF65529CA | Ok! Electric Industy C... | [PNS] [SMTP] [HTTP] [HTTP] | 1 | 48 | 1 | 60 | Today, 16:01:48 | 236 | 235 | 1 | 0 % | 03.05.202... |
| Windows 10 | VARUS-L-L | axence.io | varus.ligul... | 192.168.89.2 | varus.ligul... | F079561A31E | ASUSTek COMPUTER L... | [HTTPS(TCP)] [PNS] | 5 | | | | 22.02.2021 17:4... | 99 | 0 | 99 | 100 % | 30.08.202... |
| Linux | PARTURIE | | parturient... | 192.168.0.55 | parturient... | 001550000809 | Microsoft Corporation | [PNS] | 1 | | | | 05.08.2020 11:4... | 99 | 0 | 99 | 100 % | 28.06.201... |

The screenshot shows the 'Asset settings' window in Axence nVision 13. The 'Protocol templates' tab is selected. The 'Company information' section displays the Axence logo and address: 'Axence Sp. z o. o. sp. j. ul. Na Zjeździe 11 30-527 Kraków NIP 675-139-95-89'. The 'Protocol templates' table is also visible.

| Protocol title | Protocol number | Number of people in protocol |
|----------------------|----------------------------|------------------------------|
| Asset lease protocol | From an automatic sequence | 2 |

Protocol configuration

The general settings for all handover protocols are described in the [Protocol settings](#)^[213] chapter.

In the Protocol templates tab, the Administrator can modify many parameters. The protocol template consists of three sections - Basic Info, People Names, Protocol Columns.

Basic info

- Protocol title * (it is also the name of the template. The title of the protocol template must be unique, i.e. nVision cannot create two protocol templates with the same name. The protocol is displayed as centered, bold text),
- Protocol number * (Two available options: assigned manually / automatically from sequence. Manual broadcasting means that the Administrator will have to fill in the protocol number manually each time. Using the auto-numbering option requires selecting the [autonumbering sequence](#)^[214]),
- Protocol description, (displayed in front of the table with the protocol columns)
- Final remarks, (displayed after the table with protocol columns)

People names

- Number of people on the protocol * (from 1 to 6)
- Names of individual people * (They will be displayed at the bottom of the generated protocol. In the window for adding a protocol template, only the number of people and their names are selected, when generating a given protocol from the template, it is also necessary to indicate a specific user - his name will be displayed under the name of the person in the protocol .)

* - required fields

Protocol columns

Protocol columns (Admin can define up to 10 columns that will be included in the protocol)

Additional fields in the template generator are divided into two types: global and local - depending on the resource, e.g. the processor may require additional and different parameters than the printer.

Global fields:

- Value
- Warranty to
- Model
- Bar code type
- Inventory number
- Last mobile scan
- Last mobile save
- Name
- Serial number
- Location
- Person responsible
- Status

The fields added in the window for adding a new protocol template are displayed in the form of a table (column name / field type). You can delete the added fields (**Delete** button) and change their position on the list (**Move up** / **Move down** buttons). There is also an **Add Asset Type** option that adds a column to the log template called **Asset Type**.

After completing the configuration of the protocol template, create it by clicking the **Ok** button. The created protocol template will be displayed in the list of all templates.

By default, nVision includes 6 protocol templates:

- Asset hand-over protocol
- New asset receipt protocol
- Asset disposal protocol
- Asset release protocol
- Asset lease protocol
- Asset return protocol

Basic informations

* Protocol title:

* Protocol number:

Protocol description:

Closing remarks:

People names
Names for people who participate in the activity described by the protocol (for example: "Returner", "Receiver", "Acceptor" etc.)

* Number of people in protocol:

* Name of 1st person:

* Name of 2nd person:

Protocol columns
Add (up to 10) columns that will be included in the protocol

+ Add field Remove ▲ Move up ▼ Move down + Add asset type

| Column name | Field type (not displayed in reports) |
|----------------------|---------------------------------------|
| <No data to display> | |



OK Cancel

Generating a report

The protocol generation window will be opened after clicking the Generate protocol button visible on the main toolbar:

This window can also be opened when the user responsible for the asset is changed.

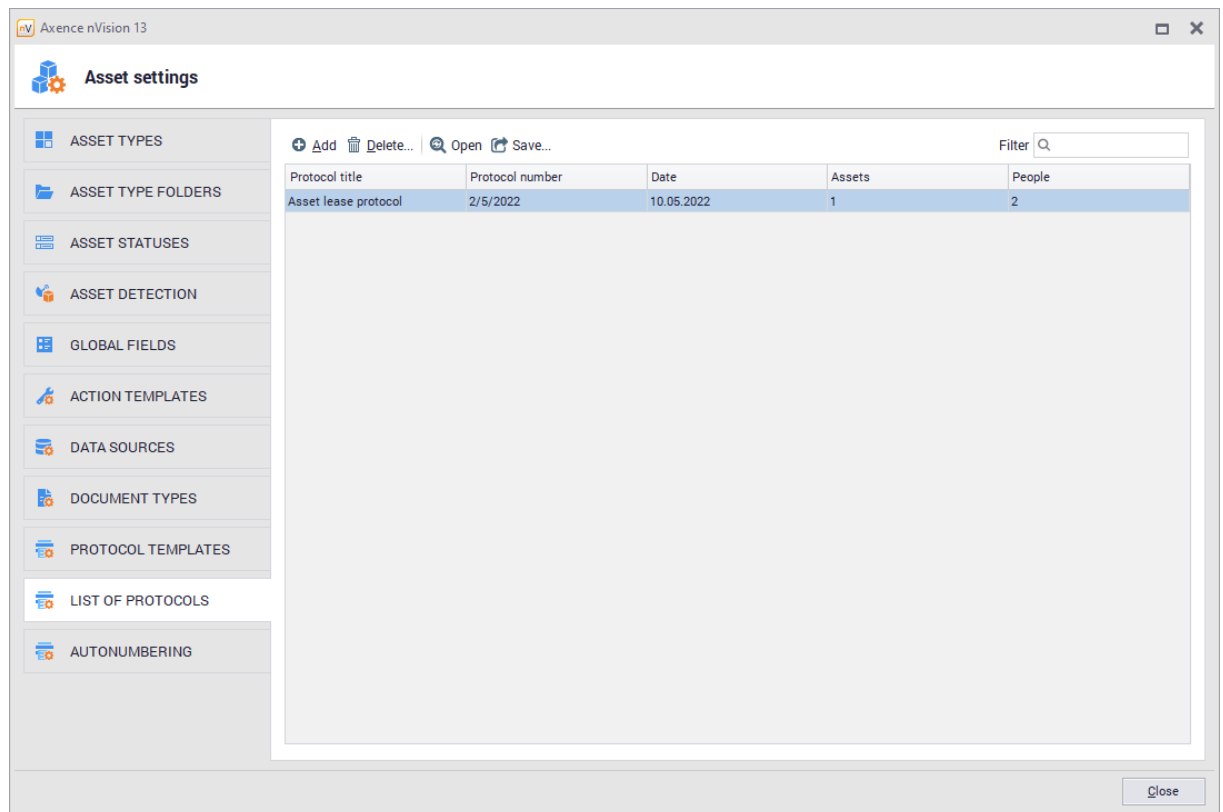
There are several fields in the protocol template generation window (different from the protocol template adding window) that must be filled in by the Administrator. The most important of them is the **Protocol template** - click on this field to display a list of all nVision protocol templates. The Administrator should

choose one of them. In the protocol generation window, you can create a new template (by clicking on ) and edit the existing one (by clicking on )

In addition, it is necessary to fill in the **Date** field, which displays today's date by default, but the Administrator can change it freely. In the further part of the form there are fields, the names of which will differ depending on the selected template, they should be completed by selecting users who take part, for example, in the transfer of the resource. The last required element of the form is adding a resource / resources (optionally commented).

After configuring all the fields, click the Generate button. The log is generated and exported in .PDF format.

All generated reports are displayed in the Protocols tab in Asset Settings.



8.2.6 User information

To view all assets assigned to the selected user, go to the **User Information** window and then go to the **Assets** tab.

In the **Responsible for** tab you can find information about the assets in which the selected user has been designated as the person responsible for the asset:

User: Mikuz

MIKUZ
Account: MIKU@WIN10 Role: ADMINISTRATOR

Create announcement...

User logged on: n/a
Status: Waiting for data

GENERAL
ACTIVITY
SCREENSHOTS
ASSETS
RESPONSIBLE FOR
CAN USE
SOFTWARE
EVENTS
DATAGUARD
BLOCKADES
SETTINGS
PERMISSIONS

Assets Documents History Events

Add Delete... Properties Show (Everything) Group by (None) Filter

| Name | Asset type | Belongs to | Inventory number | Person responsible | Serial number | Status |
|----------|------------|----------------------------|------------------|--------------------|----------------------------------|--------|
| Komputer | Computer | MIKOLAJ-PC, 192.168.69.201 | 0085933 | Mikuz | 4783-1719-9041-9283-6900-3387-88 | Used |

Defining the person responsible for the asset is possible at the time of editing or creating the asset. In the Can use tab you can find information about assets that can be used by selected user:

User: Mikuz

MIKUZ
Account: MIKU@WIN10 Role: ADMINISTRATOR

Create announcement...

User logged on: n/a
Status: Waiting for data

GENERAL
ACTIVITY
SCREENSHOTS
ASSETS
RESPONSIBLE FOR
CAN USE
SOFTWARE
EVENTS
DATAGUARD
BLOCKADES
SETTINGS
PERMISSIONS

Add relation Remove relation Properties Show (Everything) Group by (None) Filter

| Name | Asset type | Belongs to | Czas | Inventory number | Serial number | Status |
|--------|------------|-----------------------|----------|------------------|---------------|--------|
| Košć 1 | Memory | WIN10, 192.168.69.206 | 03:23:23 | 3522963 | 21esczxc | Nowy |

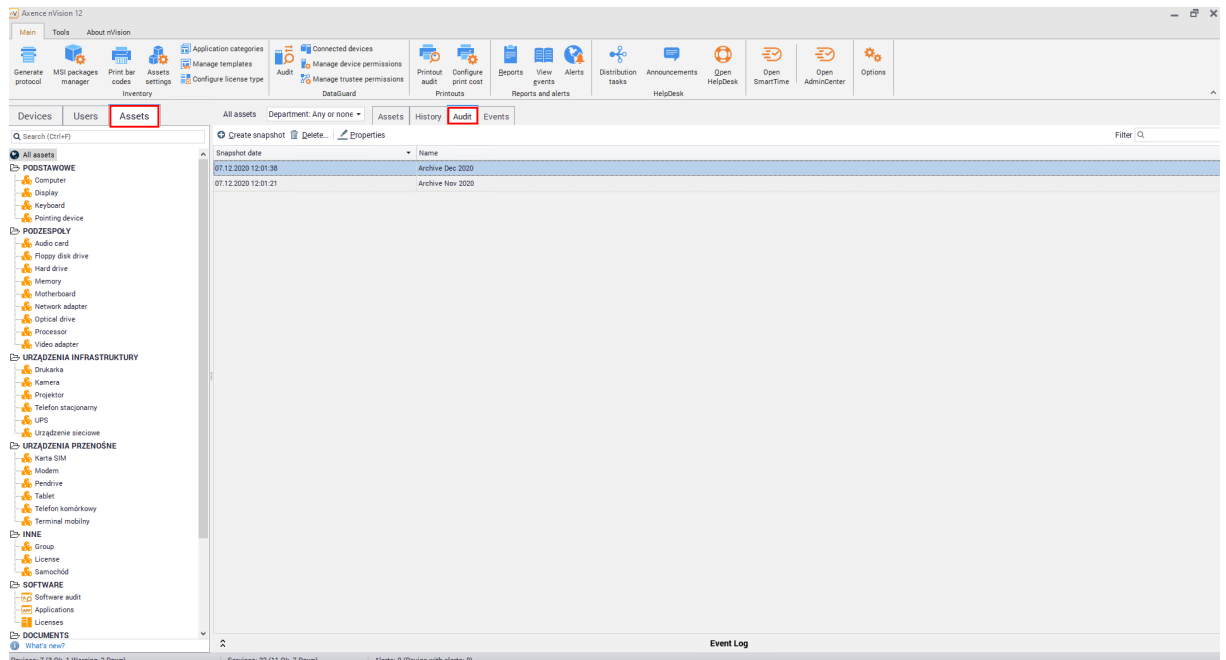
Setting the access to assets for particular users is available during asset [edition](#) ¹⁹⁵.

8.2.7 Asset audit

The audit of assets consists in comparing two snapshots, i.e. the archived states of assets. Any two snapshots or the selected snapshot and current state can be compared.

To perform the audit of assets:

1. In the main nVision window, select the **Assets** tab. Then select **All assets** from the list on the left and navigate to the **Audit** tab visible above the table of assets.



2. The prerequisite for a snapshot is that the number of events waiting for user acceptance is zero. Otherwise, you will be asked to accept all the events before it is possible to name the snapshot.
3. Select the archive (snapshot) to be compared and open its **Properties**.
4. During the audit, the individual types of assets are compared, provided that they were saved in both compared snapshots.
5. By double-clicking the chosen snapshot, , select the archives for comparison in the **Compare audit archive** window and use the **Show (state)** and **Audit status** options (described below).

Audit state and status

The **Show (state)** and **Audit status** options limit the number of displayed records and enable quick access to the most important information. The dependencies between states and statuses are presented in the table below:

| State | Possible status |
|-----------|--|
| Unchanged | <ul style="list-style-type: none"> • Audited • Unaudited |

| State | Possible status |
|---------|---|
| Added | <ul style="list-style-type: none">• Audited• Unaudited |
| Deleted | <ul style="list-style-type: none">• Unaudited |
| Changed | <ul style="list-style-type: none">• Audited• Unaudited |

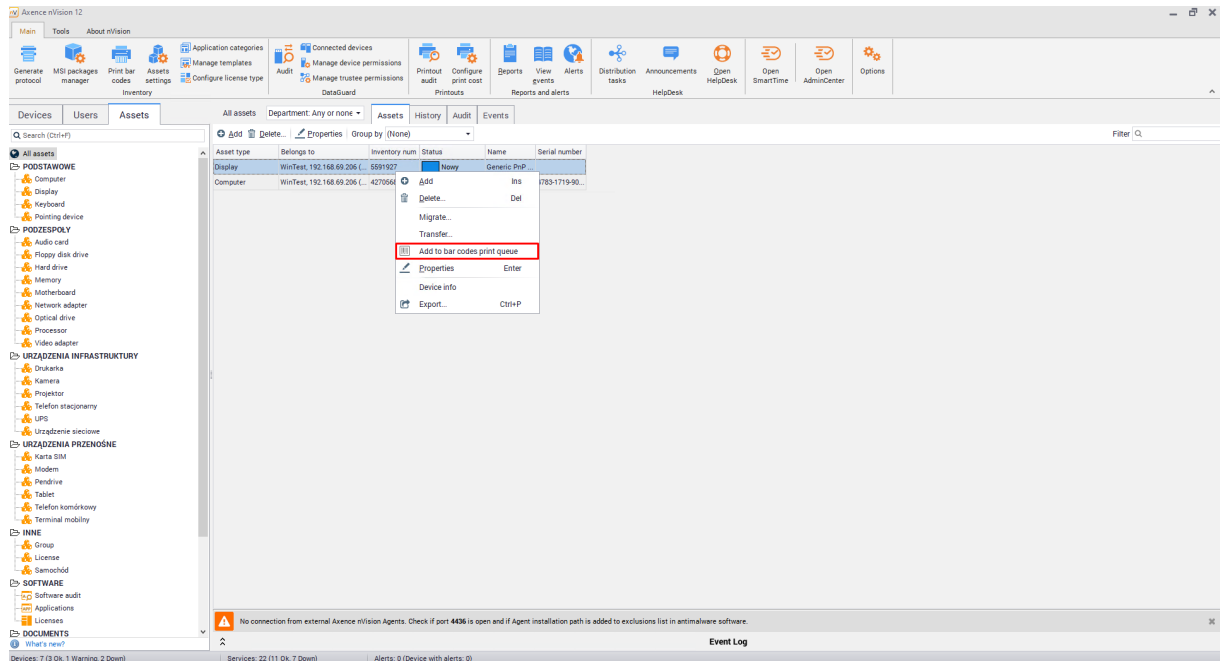
The **Audited/Unaudited** status is closely related to whether a mobile application was used between the two snapshots which are compared in the audit.

Important: if [Mobile application](#)²²⁹ is used, all devices (barcodes) should be scanned. Those that have not been scanned will be considered as unaudited and should be treated as the missing ones. The use of mobile application consists in searching for an asset by scanning the barcode or by means of other parameters (e.g. entering a part of the name) and saving.

8.2.8 Printing labels

To print labels for selected assets, use the **Add to bar codes print queue** option. This can be made in one of the following two ways:

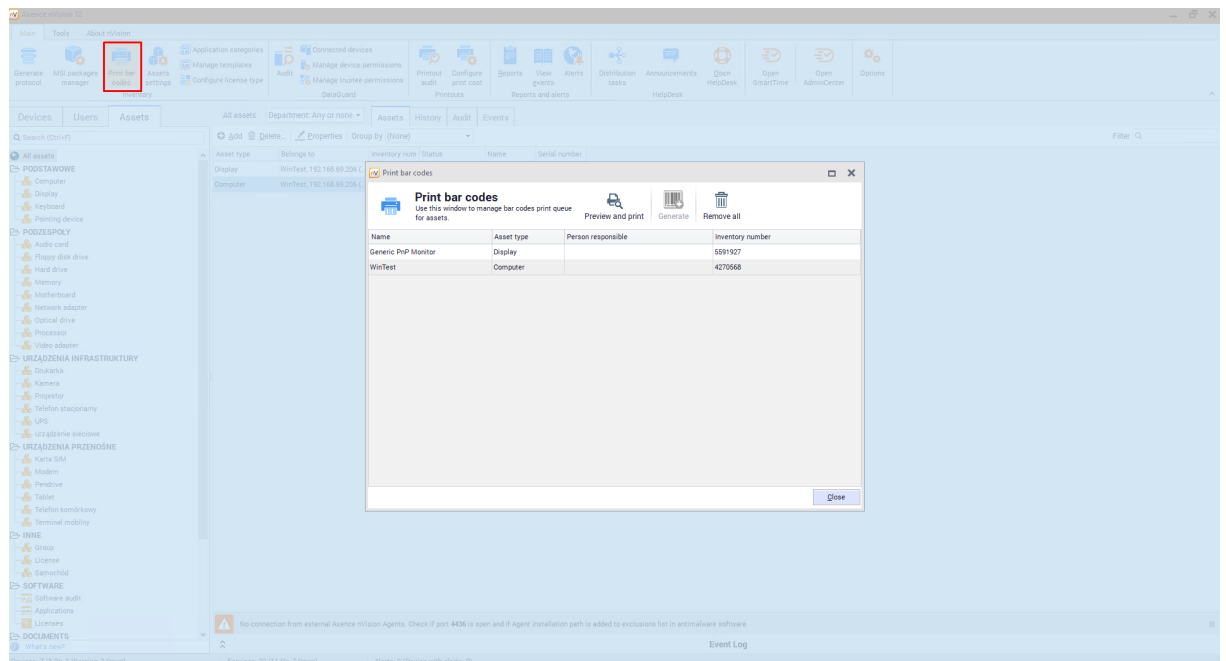
1. In the specific asset editing window (see the following screenshot).
2. In the **Assets** tab displayed in the main application window, by selecting the **Add to bar codes print queue** option from the context menu of the selected asset.





Printing

After all assets whose labels are to be printed have been added to the queue, perform the following procedure:

1. In the main nVision window, select the **Print barcodes** option.
2. All the assets for which the above-mentioned **Add to...** option was used are displayed in the **Print barcodes** window.



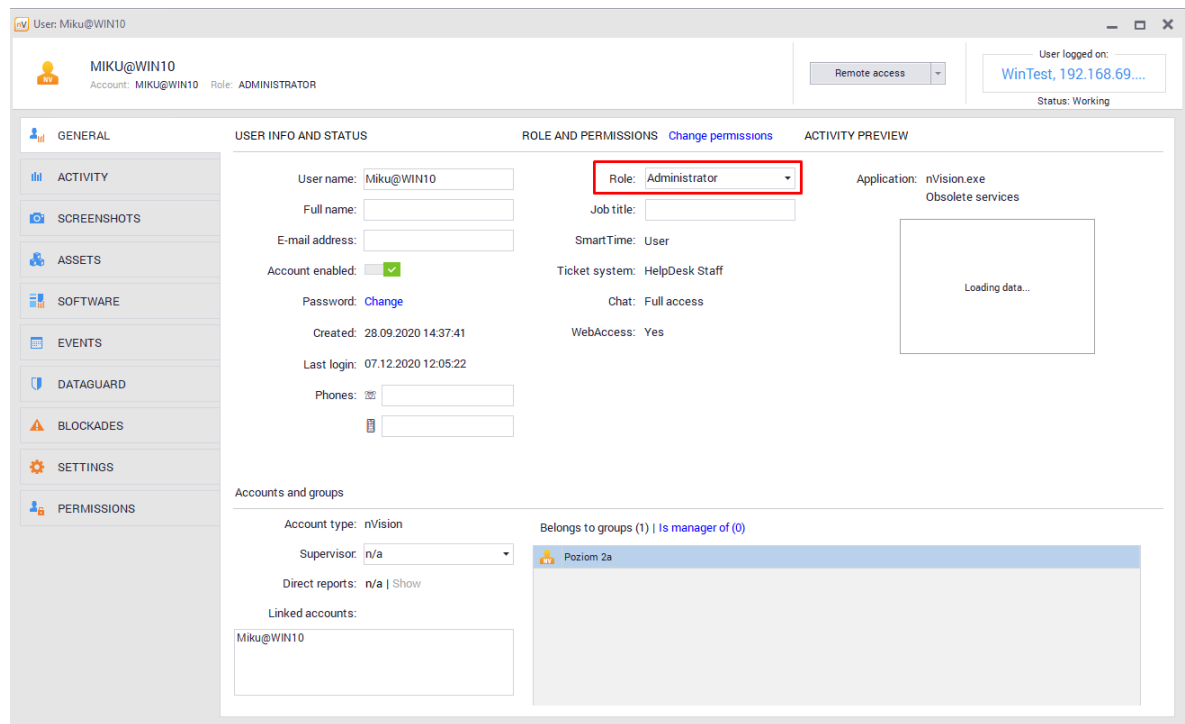
3. In order to remove a specific asset from the list, select the **Remove** option in the context menu. To clear the list, use the **Remove all** option. Note: the above-mentioned options do not remove assets, but only items to be printed.
4. If there is still at least one selected asset without an assigned inventory number, the  button is active to automatically fill in the missing data.
5. To go to the next step, press the  button.
6. The print preview screen reflects the settings of the selected printer, in particular paper size and page orientation in 1:1 scale. The block, whose parameters are being configured, is a single rectangle with a barcode and other information to be printed on the label. The number of blocks per page results directly from set margins and dimensions. Barcodes are printed in a manner allowing the fixed size of a single point (bar) in millimeters, regardless of the print resolution (accuracy).
The following screenshot presents a typical print preview for A4 page. In the case of label printers, the preview will show only one block and the number of pages will be equal to the number of labels to be printed.
7. Select **Print / Print all** to print all pages. When finished, the **Print preview** and the **Print barcodes** windows will be closed automatically and the list of assets for printing will be cleared.

8.2.9 Mobile application

Preparing nVision console for access from mobile applications

User account

The system administrator's login data are required to authorize the mobile application. The relevant account should be created in the **Users** window by selecting the **Add** option or use an account that was previously synchronized with Active Directory.



Working with the mobile application

Download

The application is available for download under the name "Assistant Inventory" from the Google Play store - <https://play.google.com/store/apps>

or directly from Axence:

<https://axence.net/downloads/app-android-assistant-inventory>

Logging in

On the login screen, enter the address of the computer on which the nVision console works. When working outside the corporate Wi-Fi network, it may be necessary to properly redirect the port on the access router. By selecting the **Remember me** option, the entered password will be remembered and the next time the application is started, the data in the login form will be automatically filled.

To log in to the application, enter the correct data for the account existing in nVision in the **Login** and **Password** fields, and then click the **Log In** button.. Please note that only users with the **Administrator** or **Super Administrator** role in the nVision console have access to the mobile application. A regular user cannot log in to the Inventory Assistant application.

Caution: Inventory Assistant application uses the same port as the nVision console, i.e. **TCP 4336**.

Inventory Assistant

nVision server address

Login

Enter login or e-mail address

Password



Remember me

LOG IN

Main screen options



1. **Add an asset** – option to create a new asset. First, enter the type of fixed asset, and then the rest of the data in the asset edit window. The **Add asset** button confirms the changes made. The resource added in this way will be included in nVision.

← Add asset

Name

Type
Computer

Inventory number

Belongs to

Person responsible

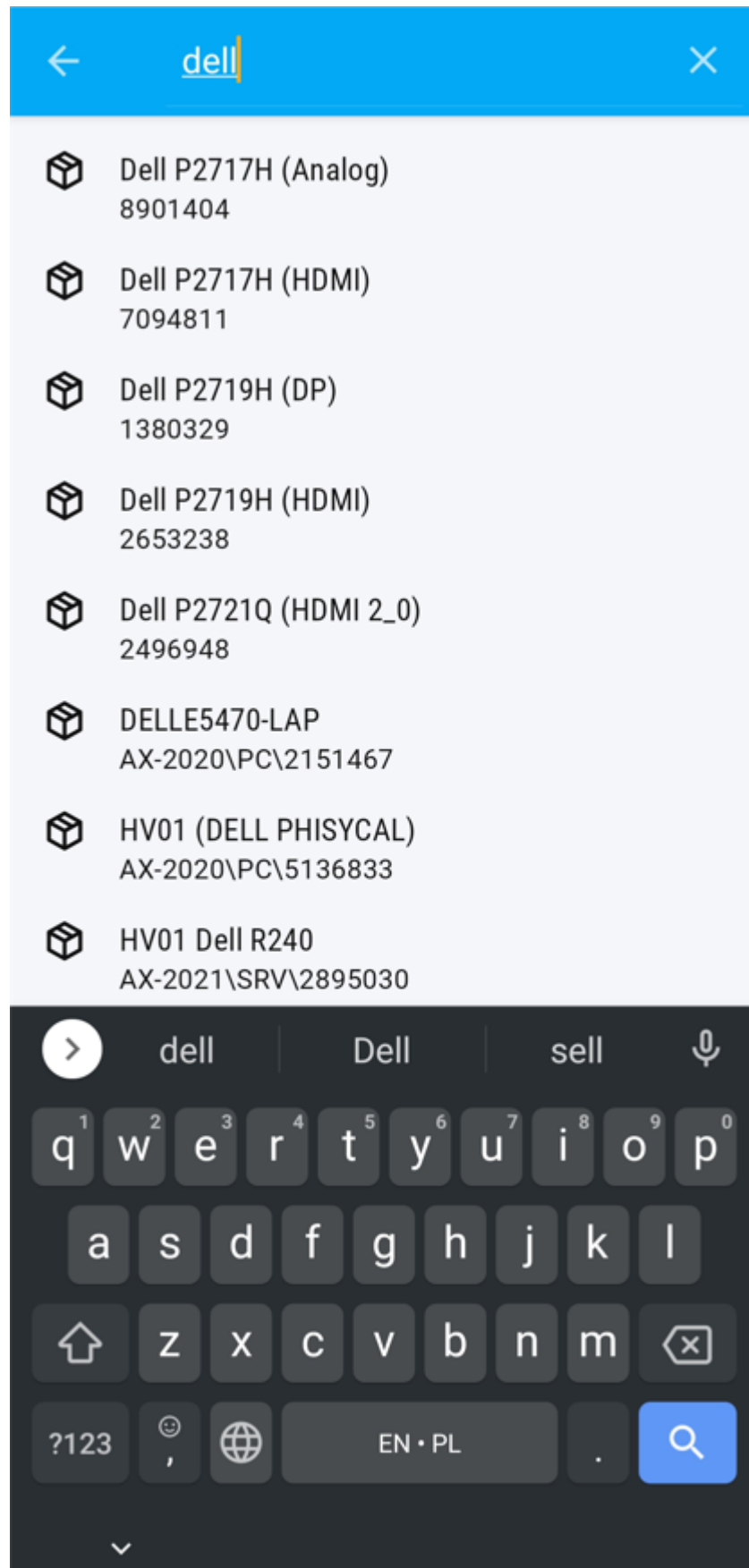
Status

Serial number

Specific asset type fields


Info 1

2. **Scan** – scanning the barcode. If there is an asset with an assigned code in the database, it will be displayed. Otherwise, the application suggests creating a new asset with the entered code as **Inventory number**.
3. **Search asset** – searching assets by name, type and (optionally) department. The search starts after entering 1 character into the search field. If at least one matching resource is found, a selection list will be displayed. Selecting a record from the list opens the resource in edit mode. Pressing the **Back** button will take you back to the list of found results. In addition, the search engine remembers recently searched resources, which greatly facilitates the work.




Other options in Assistant Inventory app


1. **Edit an asset** - Inventory Assistant allows you to edit information about a given resource. Information edited in this way is updated in the nVision console. To edit an asset, first find it using the search engine.


← Dell P2717H (HDMI) 


Name
Dell P2717H (HDMI)

Type
Display

Inventory number 
7094811


Belongs to 
Management: FUSCE-SEMPER, 192.168.20.6

Person responsible 


Status 
New

Serial number
4P9HC88BBKBL

Specific asset type fields


Manufacturer
Dell Inc 


2. **Add an activity** - This option allows you to adding activities, i.e. updating information that does not relate to the resource, but relates to it directly. To display the tab for adding activities, click on the icon displayed in the tab of a specific resource.


← Dell P2717H (HDMI) 


Name
Dell P2717H (HDMI)

Type
Display

Inventory number 
7094811


Belongs to 
Management: FUSCE-SEMPER, 192.168.20.6

Person responsible 

Status 
New

Serial number
4P9HC88BBKBL

Specific asset type fields

Manufacturer
Dell Inc 

When adding an activity, first of all, select the activity by clicking on the **Activity name** field and selecting the appropriate activity template from the pull-down list. The list of activities is a closed directory - new activity templates can be added in the nVision console: Asset settings> Activity templates> Add template). The remaining fields to be completed are:

- Cost
- Execution hours
- Execution mins
- Change status to (there is an information about current asset's status above it)
- Description

← Add activity

Activity name ▼

Cost

Execution hours

Execution mins

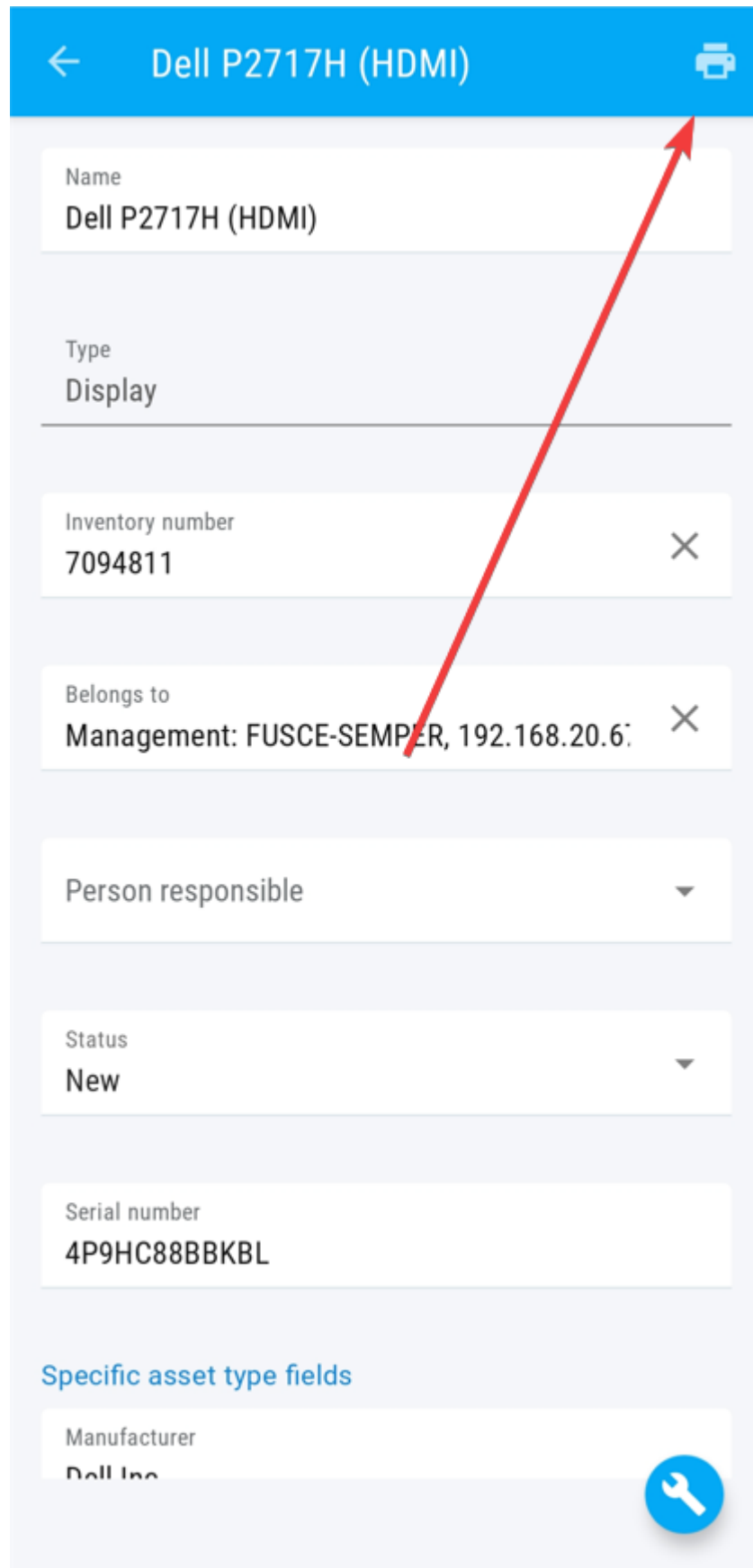
Current asset status

New

Change status to ▼

Description

3. **Print label** - The nVision mobile application, apart from barcode scanning, also enables label printing. To print a label, the device on which the Inventory Assistant is installed should be connected to the printer. To display the label printing tab, click the icon displayed in the tab of a specific resource.





The screenshot displays the details for a Dell P2717H (HDMI) asset. The interface includes a blue header with a back arrow, the asset name, and a printer icon. The asset details are organized into several sections:


- Name:** Dell P2717H (HDMI)
- Type:** Display
- Inventory number:** 7094811 (with a close icon)
- Belongs to:** Management: FUSCE-SEMPER, 192.168.20.6 (with a close icon)
- Person responsible:** (dropdown menu)
- Status:** New (dropdown menu)
- Serial number:** 4P9HC88BBKBL
- Specific asset type fields:**
 - Manufacturer:** Dell Inc (with a settings icon)

From the label printing tab, you can select a label template, share the label and select the printer you want to use. After selecting the appropriate label template, its visualization and asset parameters will

be displayed below, along with information about which of them will be printed. After completing the configuration, in order to print the label, click the **PRINT** button.

← Print label 



Select label template
Default 



Label dimensions
30x20 mm

Barcode type
QR_CODE

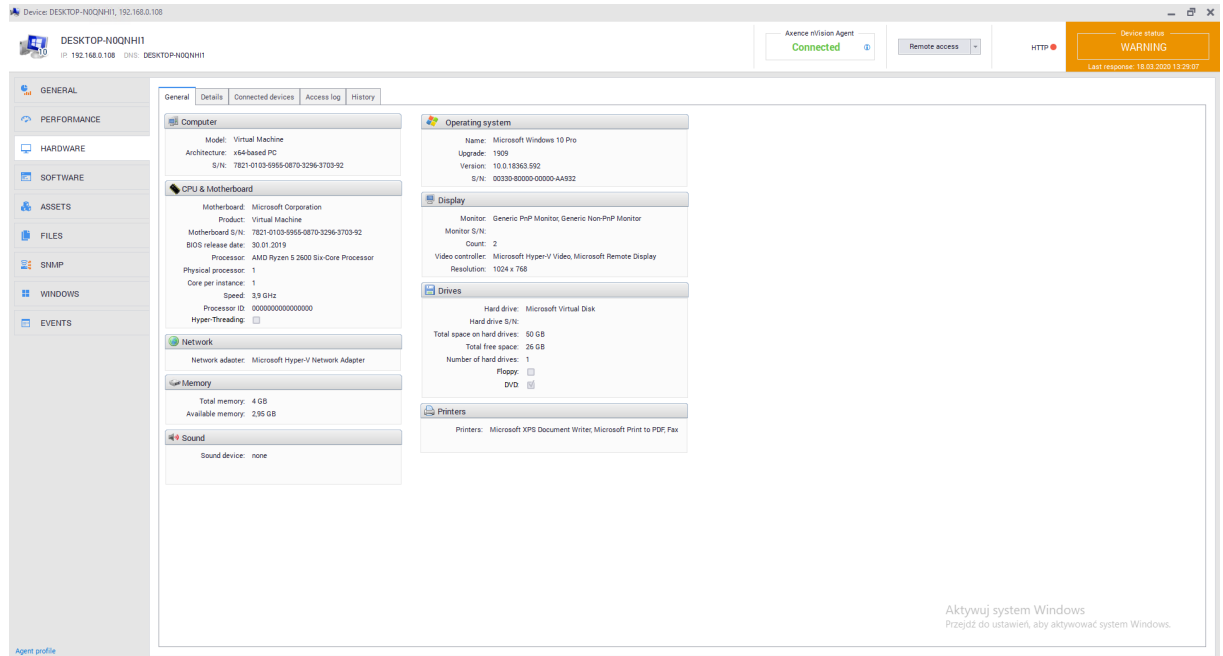
| | |
|--------------------|---------|
| Border | Printed |
| Company | Printed |
| Asset name | Printed |
| Asset type | Printed |
| Person responsible | Printed |
| Inventory number | Printed |
| IP Address | Printed |
| Location | Printed |

 PRINT 

8.3 Hardware

8.3.1 Introduction

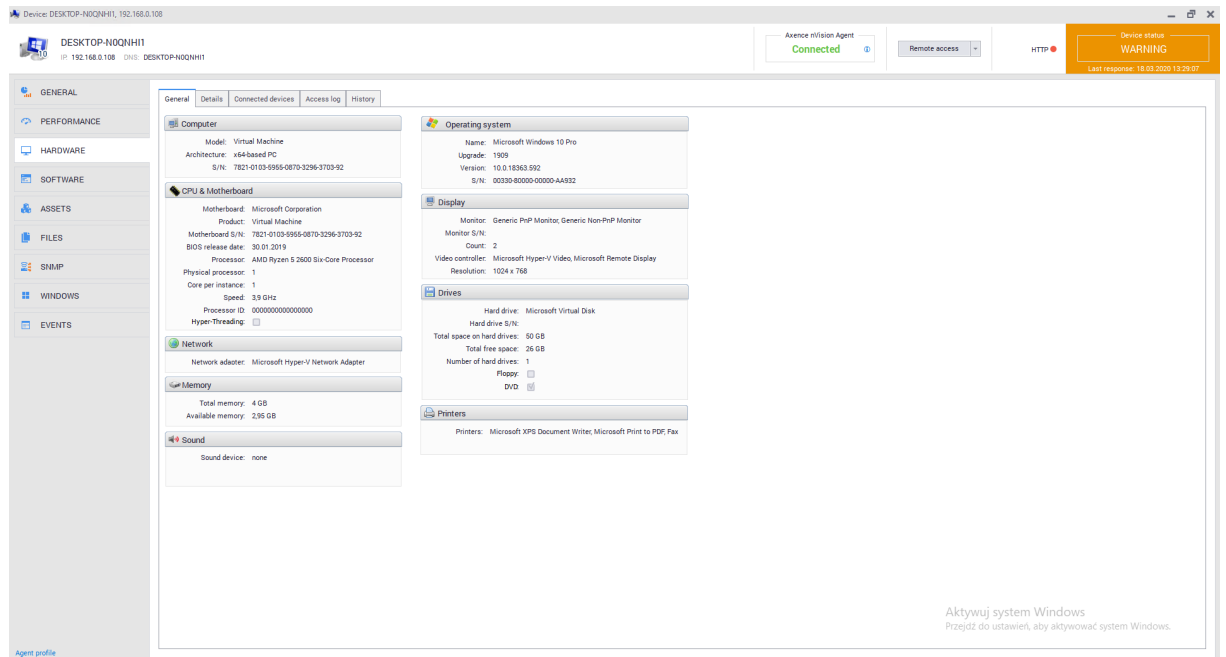
Equipment inventory allows you to control the number and type of devices in monitored networks. nVision provides detailed information about all components of the device and all devices connected to it. You need to install the nVision Agent on every computer to be monitored.



Scanning hardware information function is always **enabled**. In the device information window, after navigating to the **Hardware** tab, you can view the current hardware configuration of the device. Inventory of hardware and software can also be performed without installing Agents.

8.3.2 Monitored data

The collected device data can be viewed in the **Device Information** window after going to the **Hardware** tab. Due to the large amount of information collected, data has been divided into three tabs: **General**, **Details** and **History**. Fields **Connected devices** and **Access log** are a part of Data Guard module.



General view

The general view shows the most important information about the equipment associated with the device. In particular - selected information about the computer, processor, memory, operating system, display and more.

It is not possible to manually amend the missing data.

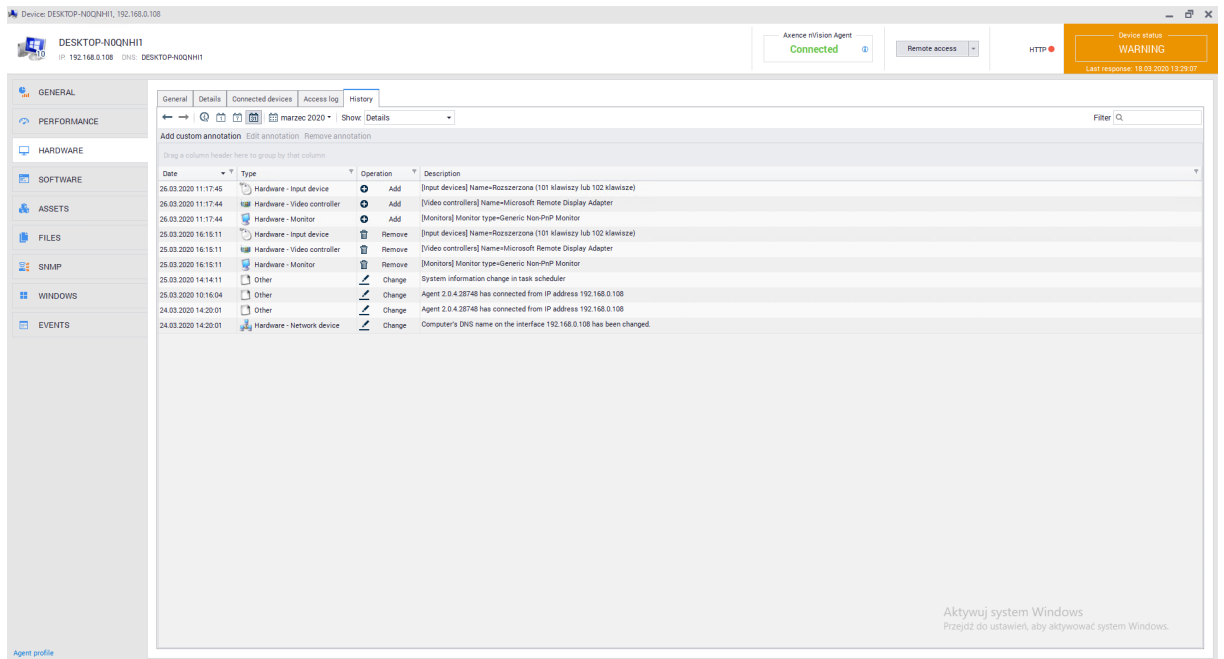
Detailed view

To access the information about the hardware on the monitored computer, go to the **Details** tab. You can view data divided into categories:

- Operating system
- Computer
- CPU & Motherboard
- BIOS
- Processors
- Memory
- Floppy drives
- Hard drives
- Optical drives
- Logical drives
- Monitors
- Video controllers
- Input devices
- Sound devices
- Network devices
- Printers
- Ports

History

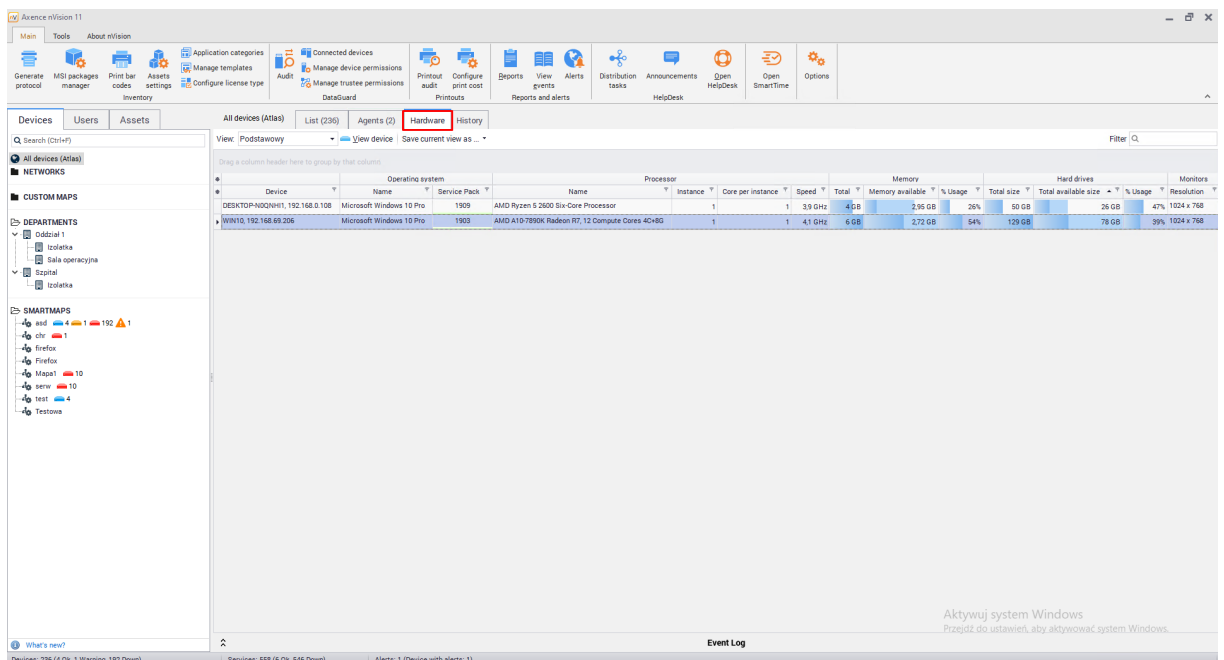
The **History** tab gives access to a list of all hardware modifications made on the selected device:



The history of all modified devices with installed Agent is described in the [History](#) ²⁴⁹ chapter.

8.3.3 Hardware audit

To go to the **Hardware** inventory audit, go to the Devices tab available from the main program window, and then select the **Hardware** tab above the list of devices:



Here you can view all hardware data gathered by Agents installed on monitored computers and hardware scans that have been imported into the program. For ease of use, the option of grouping data using views is enabled. You can use one of the existing views (e.g. All columns, Basic, Multimedia) or create your own.

Creating custom view

To create your own view, select the columns that you want to add and follow with the steps as below:

1. Select the **All columns** view from the list of available views.
2. Click on one of the buttons * located in the upper left corner of the table. The upper one contains the list of column groups (listed in the [Monitorowane dane](#) chapter), and the lower one lists all columns that can be displayed. Select the columns you want to display.
3. To save the created view, click the **Save current view as** button and enter a unique view name. From now on you can select the created view from the list.

8.3.4 History

The **History** tab allows to view changes in hardware and software in a selected period of time for all monitored devices belonging to a given Atlas.

To view the history of hardware changes, go to **Devices** tab available from the main program window, then select the **History** tab above the list of devices:

| Device | Date | Type | Operation | Description |
|----------------------|---------------------|-----------------------------|-----------|---|
| WIN10.192.168.69.206 | 10.03.2020 10:15:30 | Other | Change | Agent 2.0.4.28692 połączył się z adresem IP 192.168.69.206 |
| WIN10.192.168.69.206 | 10.03.2020 10:14:42 | Other | Change | Agent 2.0.4.28683 połączył się z adresem IP 192.168.69.206 |
| WIN10.192.168.69.206 | 09.03.2020 08:56:39 | Other | Change | Zmiana w informacjach systemowych w harmonogramie zadań |
| WIN10.192.168.69.206 | 09.03.2020 08:56:32 | Other | Change | Agent 2.0.4.28683 połączył się z adresem IP 192.168.69.206 |
| WIN10.192.168.69.206 | 09.03.2020 08:55:44 | Other | Change | Agent 2.0.4.28678 połączył się z adresem IP 192.168.69.206 |
| WIN10.192.168.69.206 | 09.03.2020 08:34:56 | Other | Change | Zmiana w informacjach systemowych w harmonogramie zadań |
| WIN10.192.168.69.206 | 09.03.2020 08:34:49 | Other | Change | Agent 2.0.4.28678 połączył się z adresem IP 192.168.69.206 |
| WIN10.192.168.69.206 | 09.03.2020 08:33:01 | Hardware - Input device | Add | [Urządzenia wejściowe] Name=Rozszerzona (101 klawiszy lub 102 klawisze) |
| WIN10.192.168.69.206 | 09.03.2020 08:33:00 | Hardware - Video controller | Add | [Karty graficzne] Name=Microsoft Remote Display Adapter |
| WIN10.192.168.69.206 | 09.03.2020 08:33:00 | Hardware - Monitor | Add | [Monitor] Monitor type=Generic Non-PnP Monitor |
| WIN10.192.168.69.206 | 06.03.2020 17:34:42 | Hardware - Input device | Remove | [Urządzenia wejściowe] Name=Rozszerzona (101 klawiszy lub 102 klawisze) |
| WIN10.192.168.69.206 | 06.03.2020 17:34:42 | Hardware - Video controller | Remove | [Karty graficzne] Name=Microsoft Remote Display Adapter |
| WIN10.192.168.69.206 | 06.03.2020 17:34:42 | Hardware - Monitor | Remove | [Monitor] Monitor type=Generic Non-PnP Monitor |
| WIN10.192.168.69.206 | 06.03.2020 12:34:08 | Other | Change | Agent 2.0.4.28678 połączył się z adresem IP 192.168.69.206 |
| WIN10.192.168.69.206 | 06.03.2020 12:33:26 | Other | Change | Agent 2.0.4.28667 połączył się z adresem IP 192.168.69.206 |
| WIN10.192.168.69.206 | 05.03.2020 10:25:13 | Other | Change | Agent 2.0.4.28667 połączył się z adresem IP 192.168.69.206 |
| WIN10.192.168.69.206 | 05.03.2020 10:23:27 | Other | Change | Agent 2.0.4.28655 połączył się z adresem IP 192.168.69.206 |
| WIN10.192.168.69.206 | 04.03.2020 09:58:02 | Other | Change | Agent 2.0.4.28655 połączył się z adresem IP 192.168.69.206 |
| WIN10.192.168.69.206 | 04.03.2020 09:57:29 | Other | Change | Agent 2.0.4.28645 połączył się z adresem IP 192.168.69.206 |
| WIN10.192.168.69.206 | 03.03.2020 09:54:19 | Other | Change | Agent 2.0.4.28645 połączył się z adresem IP 192.168.69.206 |
| WIN10.192.168.69.206 | 03.03.2020 09:53:33 | Other | Change | Agent 2.0.4.28624 połączył się z adresem IP 192.168.69.206 |
| WIN10.192.168.69.206 | 02.03.2020 09:36:37 | Other | Change | Zmiana w informacjach systemowych w harmonogramie zadań |
| WIN10.192.168.69.206 | 02.03.2020 08:38:40 | Other | Change | Zmiana w informacjach systemowych w harmonogramie zadań |
| WIN10.192.168.69.206 | 02.03.2020 08:38:34 | Other | Change | Agent 2.0.4.28624 połączył się z adresem IP 192.168.69.206 |
| WIN10.192.168.69.206 | 02.03.2020 08:36:43 | Hardware - Input device | Add | [Urządzenia wejściowe] Name=Rozszerzona (101 klawiszy lub 102 klawisze) |
| WIN10.192.168.69.206 | 02.03.2020 08:36:43 | Hardware - Video controller | Add | [Karty graficzne] Name=Microsoft Remote Display Adapter |
| WIN10.192.168.69.206 | 02.03.2020 08:36:43 | Hardware - Monitor | Add | [Monitor] Monitor type=Generic Non-PnP Monitor |
| WIN10.192.168.69.206 | 02.03.2020 08:36:43 | Hardware - Optical drive | Remove | [Napęd optyczny] Name=Microsoft Virtual DVDROM |

For convenient history view, you can group information relative to one of the columns by dragging its header to the blue field above the list. You can also add notes (after clicking the **Add own annotation** button) and comments to selected entries (right mouse button on the selected entry / **Add comment**).

| Device | Date | Type | Operation | Description |
|----------------------|---------------------|-----------------------------|-----------|---|
| WIN10.192.168.69.206 | 10.03.2020 10:15:30 | Other | Change | Agent 2.0.4.28692 połączył się z adresem IP 192.168.69.206 |
| WIN10.192.168.69.206 | 10.03.2020 10:14:42 | Other | Change | Agent 2.0.4.28683 połączył się z adresem IP 192.168.69.206 |
| WIN10.192.168.69.206 | 09.03.2020 08:56:39 | Other | Change | Zmiana w informacjach systemowych w harmonogramie zadań |
| WIN10.192.168.69.206 | 09.03.2020 08:56:32 | Other | Change | Agent 2.0.4.28683 połączył się z adresem IP 192.168.69.206 |
| WIN10.192.168.69.206 | 09.03.2020 08:55:44 | Other | Change | Agent 2.0.4.28678 połączył się z adresem IP 192.168.69.206 |
| WIN10.192.168.69.206 | 09.03.2020 08:34:56 | Other | Change | Zmiana w informacjach systemowych w harmonogramie zadań |
| WIN10.192.168.69.206 | 09.03.2020 08:34:49 | Other | Change | Agent 2.0.4.28678 połączył się z adresem IP 192.168.69.206 |
| WIN10.192.168.69.206 | 09.03.2020 08:33:01 | Hardware - Input device | Add | [Urządzenia wejściowe] Name=Rozszerzona (101 klawiszy lub 102 klawisze) |
| WIN10.192.168.69.206 | 09.03.2020 08:33:00 | Hardware - Video controller | Add | [Karty graficzne] Name=Microsoft Remote Display Adapter |
| WIN10.192.168.69.206 | 09.03.2020 08:33:00 | Hardware - Monitor | Add | [Monitor] Monitor type=Generic Non-PnP Monitor |
| WIN10.192.168.69.206 | 06.03.2020 17:34:42 | Hardware - Input device | Remove | [Urządzenia wejściowe] Name=Rozszerzona (101 klawiszy lub 102 klawisze) |
| WIN10.192.168.69.206 | 06.03.2020 17:34:42 | Hardware - Video controller | Remove | [Karty graficzne] Name=Microsoft Remote Display Adapter |

8.4 System Information

8.4.1 Introduction

System information are collected by the nVision Agent. To gather this data, you must install Agents on all computers that you want to monitor.

To go to the system information window, select the device and go to the **Device Information** window. Then select the **Windows** tab.

The screenshot shows the Axence nVision Agent interface for a device named DESKTOP-N0K (IP: 192.168.0.108, DNS: DESKTOP-N0QNH11). The device status is WARNING, with a last response of 18.03.2020 13:29:07. The interface is divided into several sections:






- Top Bar:** Device name, IP, DNS, Agent status (Connected), Remote access dropdown, HTTP status, and Device status (WARNING).
- Left Sidebar:** Navigation menu with categories: GENERAL, PERFORMANCE, HARDWARE, SOFTWARE, ASSETS, FILES, SNMP, WINDOWS, and EVENTS.
- Main Content Area:** System information window for Microsoft Windows 10 Pro. It includes tabs for System information, Windows services, Windows Event Log, Processes, and Remote command execution. The System information tab is active, showing a list of system properties.




| Property | Value |
|---|--------------------------|
| Boot device | \Device\HarddiskVolume2 |
| Build number | 18363 |
| BuildType | Multiprocessor Free |
| Caption | Microsoft Windows 10 Pro |
| CodeSet | 1250 |
| CountryCode | 48 |
| CreationClassName | Win32_OperatingSystem |
| CSCreationClassName | Win32_ComputerSystem |
| CSDVersion | |
| CSName | DESKTOP-N0QNH11 |
| CurrentTimeZone | 60 |
| DataExecutionPrevention_Available | True |
| DataExecutionPrevention_32BitApplications | True |
| DataExecutionPrevention_Drivers | True |
| DataExecutionPrevention_SupportPolicy | 2 |
| Debug | False |
| Description | |
| Distributed | False |
| EncryptionLevel | 256 |
| ForegroundApplicationBoost | 2 |
| FreePhysicalMemory | 1382556 |
| FreeSpaceInPagingFiles | 1416296 |
| FreeVirtualMemory | 1890684 |
| InstallDate | 24.03.2020 11:28:09 |
| LargeSystemCache | |
| LastBootUpTime | 25.03.2020 09:10:02 |
| Local datetime | 25.03.2020 13:14:04 |

In this section you can find System Information, Windows Services and Windows Event Log tabs. The Processes and Remote Command Execution tabs are associated with the HelpDesk module, while the other belong to Inventory module.

8.4.2 Monitored data

Table shows the system data that can be monitored

| Data | Description |
|--|---|
|  Operating system | Detailed information about the operating system, including name, manufacturer, version, serial number and other. |
|  Startup commands | List of startup commands including name, command, user and location of executed files |
|  Environment | Information about environment variables. |
|  Local users | Data on local users includes the account name, information related to the password (whether it is mandatory or has expired), account status (enabled/disabled) and other. |
|  Groups and users | Information about user groups with description |

| Data | Description |
|--|---|
|  Routing table | The computer's routing table. |
|  Network shares | Information about resources, disks and shared folders. |
|  S.M.A.R.T. | Information collected using the S.M.A.R.T system. To change the drive for information display, select it from the menu at the top of the window. To learn more about the S.M.A.R.T. system, see S.M.A.R.T. ^[253] chapter |
| Task scheduler | Presents information about running Windows applications along with the schedule dates, last launches and the result of the last launch |

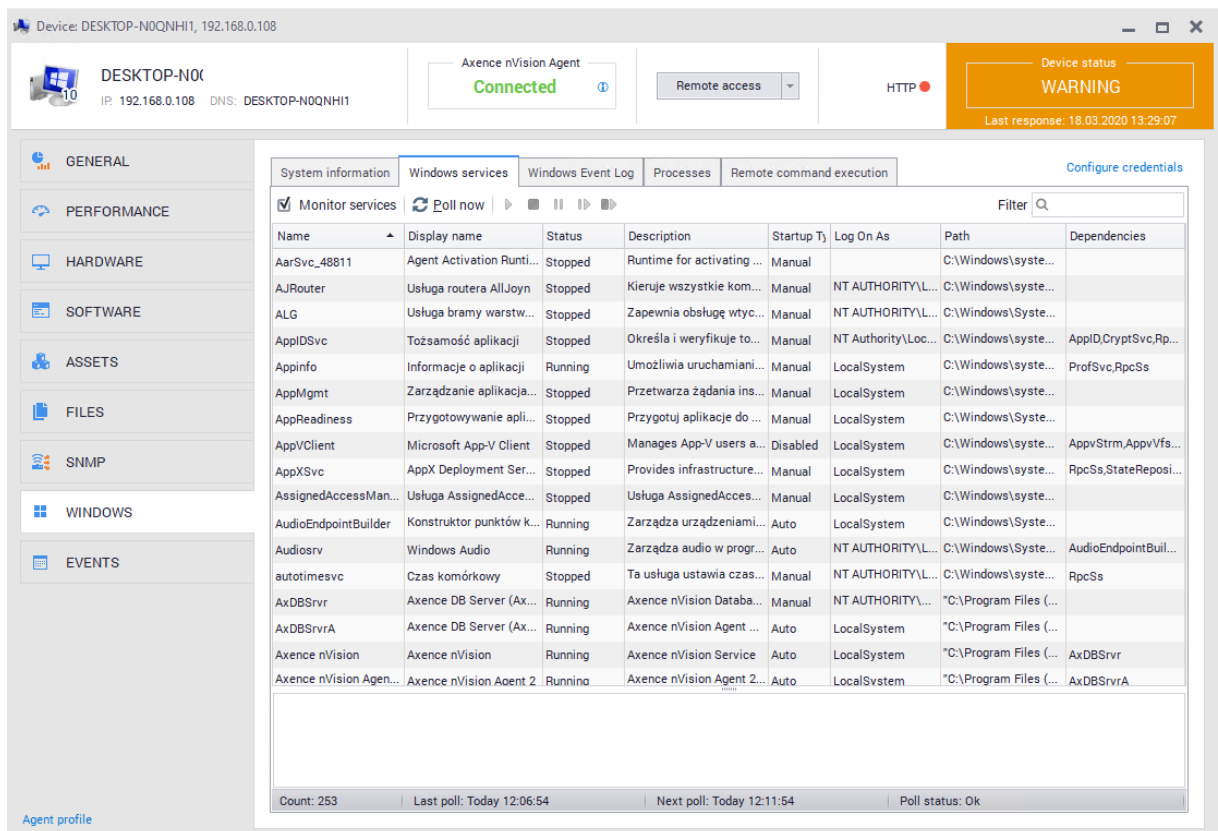
8.4.3 Windows services

The Inventory module includes a feature that allows you to monitor Windows services.

Windows Services tab displays all services associated with the device. By checking the **Monitor services** box, you can enable the visibility of this list.

This view allows you to get detailed information about individual items in the table.

Windows service tab gives you the option to start, pause, stop or resume the service. Such actions can be performed using the buttons available on the bar above the list or in the context menu of a given service (right click of the mouse).



| Name | Display name | Status | Description | Startup Type | Log On As | Path | Dependencies |
|------------------------|---------------------------|---------|----------------------------|--------------|---------------------|------------------------|----------------------|
| AarSvc_48811 | Agent Activation Runti... | Stopped | Runtime for activating ... | Manual | | C:\Windows\sysme... | |
| AJRouter | Usługa routera AllJoyn | Stopped | Kieruje wszystkie kom... | Manual | NT AUTHORITY\L... | C:\Windows\sysme... | |
| ALG | Usługa bramy warstw... | Stopped | Zapewnia obsługę wtyc... | Manual | NT AUTHORITY\L... | C:\Windows\Syste... | |
| AppDSvc | Tożsamość aplikacji | Stopped | Określa i weryfikuje to... | Manual | NT Authority\Loc... | C:\Windows\sysme... | AppID,CryptSvc,Rp... |
| Appinfo | Informacje o aplikacji | Running | Umożliwia uruchamiani... | Manual | LocalSystem | C:\Windows\sysme... | ProfSvc,RpcSs |
| AppMgmt | Zarządzanie aplikacja... | Stopped | Przetwarza ządania ins... | Manual | LocalSystem | C:\Windows\sysme... | |
| AppReadiness | Przygotowywanie apli... | Stopped | Przygotuj aplikacje do ... | Manual | LocalSystem | C:\Windows\Syste... | |
| AppVClient | Microsoft App-V Client | Stopped | Manages App-V users a... | Disabled | LocalSystem | C:\Windows\sysme... | AppvStrm,AppvVfs... |
| AppXSvc | AppX Deployment Ser... | Stopped | Provides infrastructure... | Manual | LocalSystem | C:\Windows\sysme... | RpcSs,StateReposi... |
| AssignedAccessMan... | Usługa AssignedAcce... | Stopped | Usługa AssignedAcce... | Manual | LocalSystem | C:\Windows\sysme... | |
| AudioEndpointBuilder | Konstruktor punktów k... | Running | Zarządza urządzeniami... | Auto | LocalSystem | C:\Windows\Syste... | |
| Audiosrv | Windows Audio | Running | Zarządza audio w progr... | Auto | NT AUTHORITY\L... | C:\Windows\Syste... | AudioEndpointBuil... |
| autotimesvc | Czas komórkowy | Stopped | Ta usługa ustawia czas... | Manual | NT AUTHORITY\L... | C:\Windows\sysme... | RpcSs |
| AxDBSrvr | Axence DB Server (Ax... | Running | Axence nVision Databa... | Manual | NT AUTHORITY\... | "C:\Program Files (... | |
| AxDBSrvrA | Axence DB Server (Ax... | Running | Axence nVision Agent ... | Auto | LocalSystem | "C:\Program Files (... | |
| Axence nVision | Axence nVision | Running | Axence nVision Service ... | Auto | LocalSystem | "C:\Program Files (... | AxDBSrvr |
| Axence nVision Agen... | Axence nVision Agent 2 | Running | Axence nVision Agent 2... | Auto | LocalSystem | "C:\Program Files (... | AxDBSrvrA |

To force checking the current services status, use the  **Poll now** button .

8.4.4 Windows processes

HelpDesk module allows you to view the system processes with management options. More information is available in [the following chapter.](#)^[483]

8.4.5 Windows Event Log

The Inventory module allows you to monitor Windows event log.

The screenshot displays the Axence nVision Agent interface for a device named 'DESKTOP-NOQNH11' with IP 192.168.0.108. The device status is 'WARNING' with a last response of 18.03.2020 13:29:07. The 'Windows Event Log' tab is selected, showing the 'Monitor Event Log' option checked and 'Poll now' button. The interface includes a table of events and a detailed description of a specific event.

| Type | Logfile | Time | Source | Category | Event | User |
|--------|---------|---------------------|----------------------------|----------|-------|-------------------|
| System | | 26.03.2020 12:06:20 | Microsoft-Windows-Distribu | (None) | 10028 | ZARZADZANIE NT\SY |
| System | | 26.03.2020 12:03:56 | Microsoft-Windows-Distribu | (None) | 10028 | ZARZADZANIE NT\SY |
| System | | 26.03.2020 12:00:00 | EventLog | (None) | 6013 | n/a |
| System | | 26.03.2020 11:59:10 | Service Control Manager | (None) | 7040 | ZARZADZANIE NT\SY |
| System | | 26.03.2020 11:57:06 | Service Control Manager | (None) | 7040 | ZARZADZANIE NT\SY |
| System | | 26.03.2020 11:57:04 | Service Control Manager | (None) | 7040 | ZARZADZANIE NT\SY |
| System | | 26.03.2020 11:56:53 | Microsoft-Windows-Distribu | (None) | 10028 | ZARZADZANIE NT\SY |
| System | | 26.03.2020 11:55:00 | Service Control Manager | (None) | 7040 | ZARZADZANIE NT\SY |
| System | | 26.03.2020 11:52:08 | Microsoft-Windows-Distribu | (None) | 10028 | ZARZADZANIE NT\SY |
| System | | 26.03.2020 11:49:45 | Microsoft-Windows-Distribu | (None) | 10028 | ZARZADZANIE NT\SY |
| System | | 26.03.2020 11:45:02 | Microsoft-Windows-Distribu | (None) | 10028 | ZARZADZANIE NT\SY |
| System | | 26.03.2020 11:41:24 | Service Control Manager | (None) | 7040 | ZARZADZANIE NT\SY |
| System | | 26.03.2020 11:39:20 | Service Control Manager | (None) | 7040 | ZARZADZANIE NT\SY |
| System | | 26.03.2020 11:39:18 | Service Control Manager | (None) | 7040 | ZARZADZANIE NT\SY |
| System | | 26.03.2020 11:37:14 | Service Control Manager | (None) | 7040 | ZARZADZANIE NT\SY |

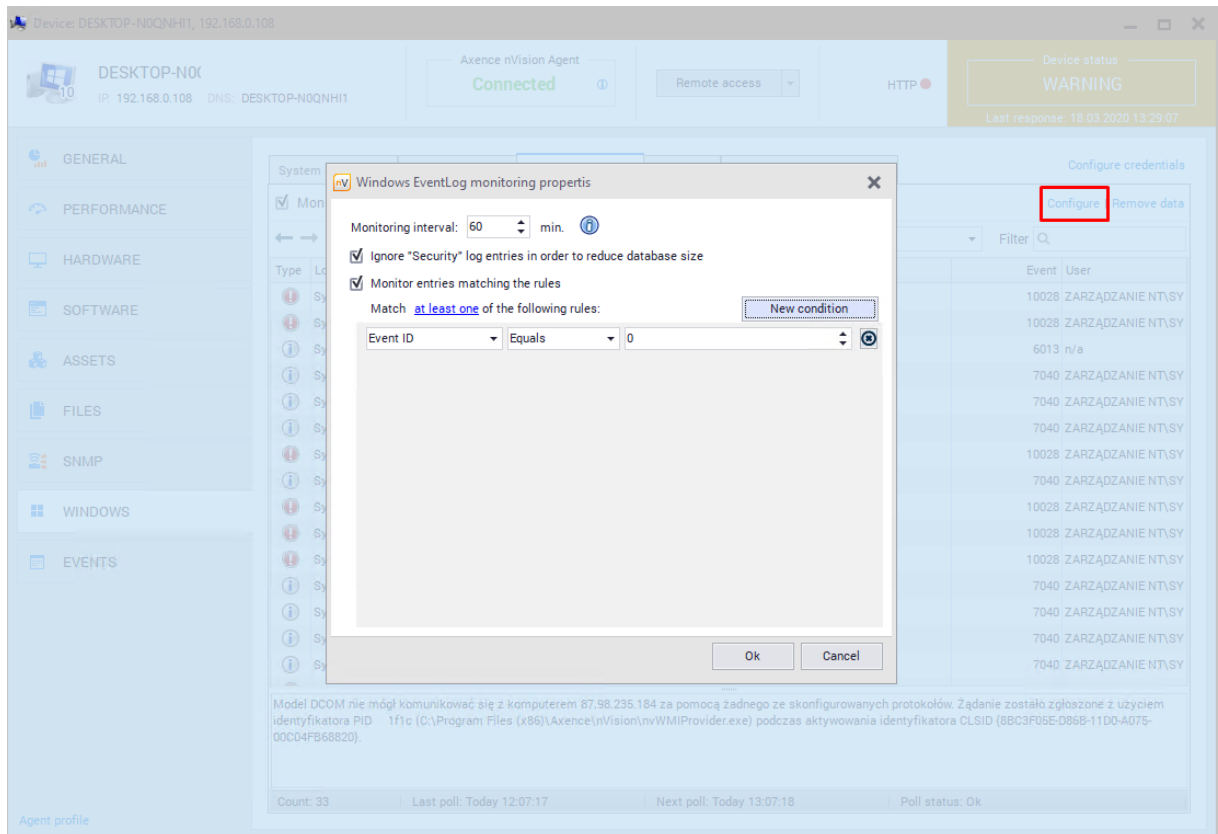
Count: 33 | Last poll: Today 12:07:17 | Next poll: Today 13:07:18 | Poll status: Ok


Model DCOM nie mógł komunikować się z komputerem 87.98.235.184 za pomocą żadnego ze skonfigurowanych protokołów. Żądanie zostało zgłoszone z użyciem identyfikatora PID 1f1c (C:\Program Files (x86)\Axence\nVision\nvWMIProvider.exe) podczas aktywowania identyfikatora CLSID {8BC3F05E-D86B-11D0-A075-00C04FB68820}.

To run the event log monitoring, go to **Device Information / Windows**, then select **Windows Event Log** tab and choose **Monitor event log** option.

WARNING! Enabling event log synchronization for a large number of devices can significantly load the network and increase the size of the database.

By default, nVision updates the event log every hour. Using the **Configure** option, you can modify both the monitoring interval and specify additional rules. Setting a low monitoring interval may result in high network load. The default Windows Event Log monitoring filter does not collect user login information.



To force immediate event log synchronization, click  **Poll now** button.

8.4.6 Remote command execution

Remote command execution is a part of the HelpDesk module. See chapter [remote cmd](#)⁴⁸⁴ for more information.

8.4.7 S.M.A.R.T.

S.M.A.R.T. (ang. Self-Monitoring, Analysis and Reporting Technology) is a system for monitoring and notification of hard disk operation errors to increase the security of stored data. The use of this system allows to anticipate and prevent impending failures (e.g. by monitoring the temperature overheating risks).

S.M.A.R.T. monitors many parameters of the hard disk by constant access to a device status.

Monitoring includes:

- number of start / stop cycles (Start / Stop Count),
- disk temperature (Celcius),
- frequency of errors during reading process (Read Error Rate),
- the number of reallocated sectors (Reallocated Sector Count),
- the number of attempts to start the disk axis (Spin Retry Count).

Error analysis, based on the prediction of disk damage based on constantly monitored parameters (attributes), allows for earlier notice about potential problems.

8.5 Software

8.5.1 General information

Software inventory function enables control over applications installed on the computers of monitored users. It allows to control the legality of programs and multimedia files, in line with licenses management. In order to collect information about installed programs, you must install the nVision Agent on each of the computers to be monitored.

In nVision 11.5 an "assets" tab has been added, allowing to display resources, applications, licenses and documents saved in the database. To access it, select the **Main** tab and then select **Assets**:

| Name | Asset type | Belongs to | CustomGlobal | Czas | Inventory number | Location | Person responsible | Serial number | Status | Value | Warranty to |
|---|---------------------|-------------------------------|--------------|----------|-------------------|------------|--------------------|----------------------------------|----------|--------------|-------------|
| ZELMER | Karta | (Unassigned) | | | AGH002 | | | | W użyciu | 150,00 zł | |
| PHILIPS | Karta | (Unassigned) | | | AGH001 | | | | W użyciu | 120,00 zł | 04.01.2020 |
| Remote Desktop Mouse Device | Pointing device | WIN10, 192.168.69.206 | | | | | | | W użyciu | 0,00 zł | |
| LPS APC 1000 | Keyboard | (Unassigned) | | | SP/ST1070 | WOM Sala A | | | W użyciu | 0,00 zł | |
| Microsoft Remote Display Adapter | Video adapter | WIN10, 192.168.69.206 | | | | | | | | 0,00 zł | |
| LPS APC 1000 | Keyboard | (Unassigned) | | | SP/ST1072 | WOM Sala A | | | W użyciu | 0,00 zł | |
| Rozszerzona (101 Klawiszy lub 102 Klawisze) | Keyboard | WIN10, 192.168.69.206 | | | | | | | | 0,00 zł | |
| Microsoft Virtual Disk | Hard drive | WIN10, 192.168.69.206 | | | | | | | | 0,00 zł | |
| Microsoft Hyper-V Network Adapter | Network adapter | WIN10, 192.168.69.206 | | | NET4201707902 | | | | W użyciu | 0,00 zł | |
| Rozszerzona (101 Klawiszy lub 102 Klawisze) | Keyboard | WIN10, 192.168.69.206 | | | | | | | W użyciu | 0,00 zł | |
| Microsoft Virtual DVD-ROM | Optical drive | WIN10, 192.168.69.206 | | | | | | | W użyciu | 0,00 zł | |
| HID-compliant mouse | Pointing device | WIN10, 192.168.69.206 | | | | | | | W użyciu | 0,00 zł | |
| LPS APC 1000 | Keyboard | (Unassigned) | | | SP/ST1071 | WOM Sala A | | | W użyciu | 0,00 zł | |
| AMD A10-7890K Radeon R7, 12 Compute Cores 4D+8G | Processor | WIN10, 192.168.69.206 | | | | | | | | 0,00 zł | |
| Microsoft Corporation Virtual Machine | Motherboard | WIN10, 192.168.69.206 | | | | | | 4783-1719-9041-9285-6900-3387-84 | W użyciu | 0,00 zł | |
| Generic Non-PS/2 Monitor | Display | WIN10, 192.168.69.206 | | | 6774329 | | | | | 0,00 zł | |
| macierz1 | NAS | (Unassigned) | | | | Kraków | | | W użyciu | 0,00 zł | |
| Microsoft Hyper-V Video | Video adapter | WIN10, 192.168.69.206 | | | | | | | W użyciu | 0,00 zł | |
| DESKTOP-NQDNH1 | Computer | DESKTOP-NQDNH1, 192.168.0.108 | | | 6740602 | | | 7821-0103-8985-0870-3296-3703-92 | W użyciu | 0,00 zł | |
| Generic PHP Monitor | Display | WIN10, 192.168.69.206 | | | 9146256 | | | | W użyciu | 0,00 zł | |
| 2 GB (Unknown) | Memory | WIN10, 192.168.69.206 | | | | | | | W użyciu | 0,00 zł | |
| Kość 1 | Memory | WIN10, 192.168.69.206 | | 03.23.23 | 3522963 | | | 21esczxc | Nowy | 0,00 zł | |
| Axence nVision Agent | Software (obsolete) | WIN10, 192.168.69.206 | | | | | | | W użyciu | 0,00 zł | 18.02.2020 |
| 129test | Testowy | Szpital | | | OFFLINE2861305 | wma | | | W użyciu | 222,00 zł | |
| 2154 | Testowy | (Unassigned) | | | OFFLINE1124942526 | Kraków | | | W użyciu | 21 333,00 zł | |
| Computer admin | Network adapter | (Unassigned) | | | NET420008564 | | | | W użyciu | 0,00 zł | |
| ose | Testowy | (Unassigned) | | | OFFLINE112800824 | Kraków | Administrator | | W użyciu | 6 666,00 zł | |
| RAMASOJNIC | Karta | (Unassigned) | | | AGH003 | | | | W użyciu | 200,00 zł | |
| drukarka1 | Printer | (Unassigned) | | | 6579449 | | | | W użyciu | 0,00 zł | |
| 133 | Computer | (Unassigned) | | | 8423387 | | | | W użyciu | 0,00 zł | |
| test1 | Testowy | 192.168.69.1 | | | OFFLINE1454424 | Kraków | | | W użyciu | 5,69 zł | |

The list of folders with their assigned types, the list of applications and licenses, and the document section divided into categories will be displayed on the left side of the screen. The administrator can create his own folders and document categories. These settings are described in the [foldery typów zasobów](#)^[204] and [typy dokumentów](#)^[210] chapters.

This chapter focuses on software. The remaining segments of the **Assets** tab are described in the **Assets** chapter.

Software

The software section consists of three sections:

- Software audit - displays list of detected applications, enables audit snapshot
- Applications - displays list of applications which installations can be detected by the Agent,
- Licenses - allows to view, modify and add licenses.

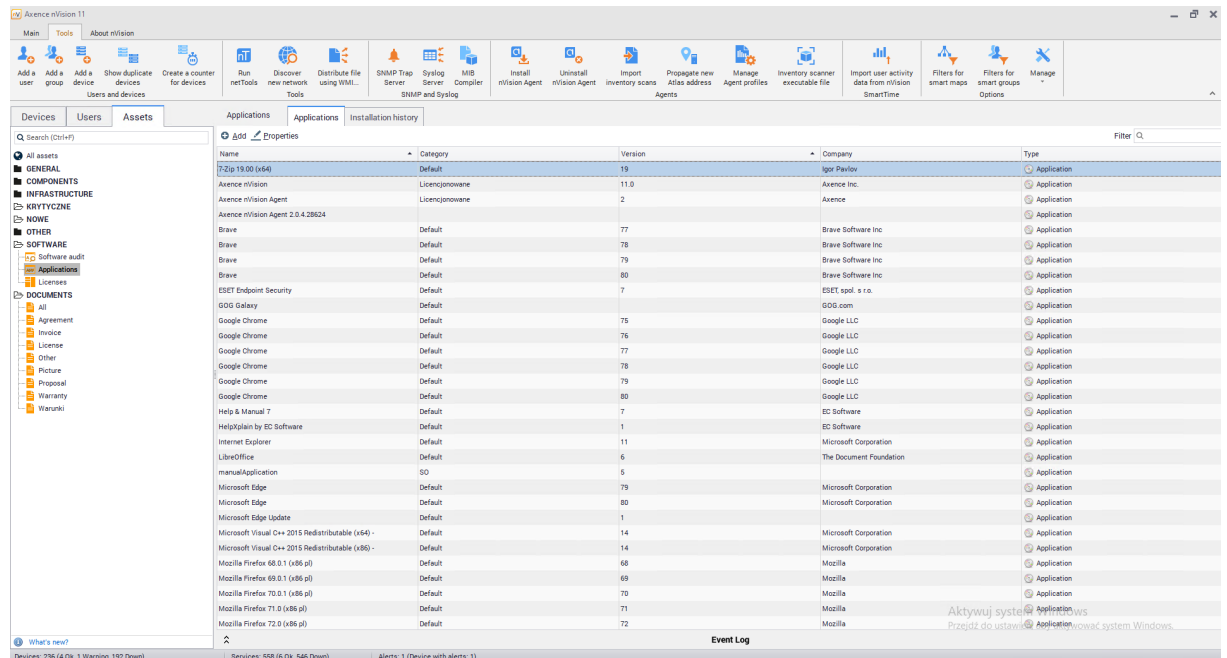
Each of items shown above is described in the following chapters.

In nVision 11.5, programs and software templates have been combined into one object called the 'application'. This allows more application management more powerful and intuitive. Also, the possibility of various settlements of license usage (e.g. per user) has been introduced. To assign a license to an application, the application must be marked as audited.

8.5.2 Detection and application properties

8.5.2.1 Applications

To display the list of applications, select the **Assets** tab visible in the main program window, and then scroll down for **Applications** in the **Software** section:



| Name | Category | Version | Company | Type |
|---|----------------|---------|-------------------------|-------------|
| 7-Zip 19.00 (x64) | Default | 19 | Igor Pavlov | Application |
| Avance nVision | Licencjonowane | 11.0 | Avance Inc. | Application |
| Avance nVision Agent | Licencjonowane | 2 | Avance | Application |
| Avance nVision Agent 2.0.4.28524 | | | | Application |
| Brave | Default | 77 | Brave Software Inc | Application |
| Brave | Default | 78 | Brave Software Inc | Application |
| Brave | Default | 79 | Brave Software Inc | Application |
| Brave | Default | 80 | Brave Software Inc | Application |
| ESET Endpoint Security | Default | 7 | ESET spol. s r.o. | Application |
| GOG Galaxy | Default | | GOG.com | Application |
| Google Chrome | Default | 75 | Google LLC | Application |
| Google Chrome | Default | 76 | Google LLC | Application |
| Google Chrome | Default | 77 | Google LLC | Application |
| Google Chrome | Default | 78 | Google LLC | Application |
| Google Chrome | Default | 79 | Google LLC | Application |
| Google Chrome | Default | 80 | Google LLC | Application |
| Help & Manual 7 | Default | 7 | EC Software | Application |
| HelpPolish by EC Software | Default | 1 | EC Software | Application |
| Internet Explorer | Default | 11 | Microsoft Corporation | Application |
| LibreOffice | Default | 6 | The Document Foundation | Application |
| manualApplication | SO | 5 | | Application |
| Microsoft Edge | Default | 79 | Microsoft Corporation | Application |
| Microsoft Edge | Default | 80 | Microsoft Corporation | Application |
| Microsoft Edge Update | Default | 1 | | Application |
| Microsoft Visual C++ 2015 Redistributable (x64) - | Default | 14 | Microsoft Corporation | Application |
| Microsoft Visual C++ 2015 Redistributable (x86) - | Default | 14 | Microsoft Corporation | Application |
| Mozilla Firefox 68.0.1 (x86 pt) | Default | 68 | Mozilla | Application |
| Mozilla Firefox 68.0.1 (x86 pl) | Default | 69 | Mozilla | Application |
| Mozilla Firefox 70.0.1 (x86 pt) | Default | 70 | Mozilla | Application |
| Mozilla Firefox 71.0 (x86 pl) | Default | 71 | Mozilla | Application |
| Mozilla Firefox 72.0 (x86 pl) | Default | 72 | Mozilla | Application |

The displayed list contains applications that:

- have been detected on the host with installed Agent and have been assigned to the embedded application patterns,
- have been manually added by the Administrator,
- were detected on the host with the installed Agent through a system registry scan and a pattern was created for them.

Patterns based on which application installations are detected are described in detail in the [App template](#) ²⁶⁰ chapter.

Applications on the selected host

Going to the **Device Information** window and then to the **Software / Installations** tab you can see the list of applications installed on the selected host:

Device: WIN10, 192.168.69.206

Axence nVision Agent
Disconnected

Remote access

NetBIOS (TCP)
SMB2
SMB3

Device status
DOWN
Last response: 23.03.2020 16:00:21

GENERAL
PERFORMANCE
HARDWARE
SOFTWARE
ASSETS
FILES
SNMP
WINDOWS
EVENTS

Agent profile

Installations History

Installation properties Uninstall... Process applications Filter Q

| Name | Ver | Compar | Installed | MSI Installer | Category | User | License | Serial number |
|---------------------------------|------|-----------|------------|------------------|----------------|---------------|----------------|---------------|
| Audited applications | | | | | | | | |
| 7-Zip 19.00 (x64) | 19 | Igor P... | 03.02.2020 | Waiting for data | Default | Mikuz | Licencja te... | 53412 |
| Axence nVision | 11.0 | Axenc... | 10.12.2019 | Waiting for data | Licencjonowane | | | |
| Google Chrome | 80 | Googl... | 10.02.2020 | Waiting for data | Default | Administrator | | |
| Mozilla Firefox 73.0.1 ... | 73 | Mozilla | 19.02.2020 | Waiting for data | Default | Mikuz | Licencja te... | 4422004 |
| Security Update (KB44... | | Micro... | 12.06.2019 | Waiting for data | Default | | | |
| Windows 10 Pro | 10 | Micro... | 01.07.2019 | Waiting for data | SO | Mikuz | | |
| Not audited applications | | | | | | | | |
| Axence nVision Agent | 2 | Axence | 05.12.2019 | Waiting for data | Licencjonowane | Administrator | | |
| Brave | 80 | Brave ... | 11.02.2020 | Waiting for data | Default | | | |
| Internet Explorer | 11 | Micro... | 05.12.2019 | Waiting for data | Default | | | |
| LibreOffice | 6 | The D... | 21.11.2019 | Waiting for data | Default | | | |
| Security Update (KB45... | | Micro... | 12.06.2019 | Waiting for data | Default | | | |
| Security Update (KB45... | | Micro... | 20.08.2019 | Waiting for data | Default | | | |
| Security Update (KB45... | | Micro... | 10.03.2020 | Waiting for data | Default | | | |
| Update (KB4551762) | | Micro... | 16.03.2020 | Waiting for data | Default | | | |
| Unknown applications | | | | | | | | |
| ESET Endpoint Security | 7 | ESET, ... | 17.01.2020 | Waiting for data | Default | | | |
| GOG Galaxy | | GOG c... | 07.01.2020 | Waiting for data | Default | | | |

The information presented in this window is based on data from: Files Registry

Application properties

To go to the application properties, double-click on the item in the list or click the **Properties** button above the list:

Axence nVision 11

Applications

7-Zip 19.00 (x64)

APPLICATION PROPERTIES AND TEMPLATE

TEMPLATE

INSTALLATIONS

LICENSES

USERS

Name: 7-Zip 19.00 (x64)

Type: Application

Category: Default

Description:

Company: Igor Pavlov

Version: 19

Audited: Yes

Autodetection: Yes Manage

Close

Aktuj system Windows
Przejdź do ustawień

Properties window will be opened. The individual elements shown here are described in the following chapters.

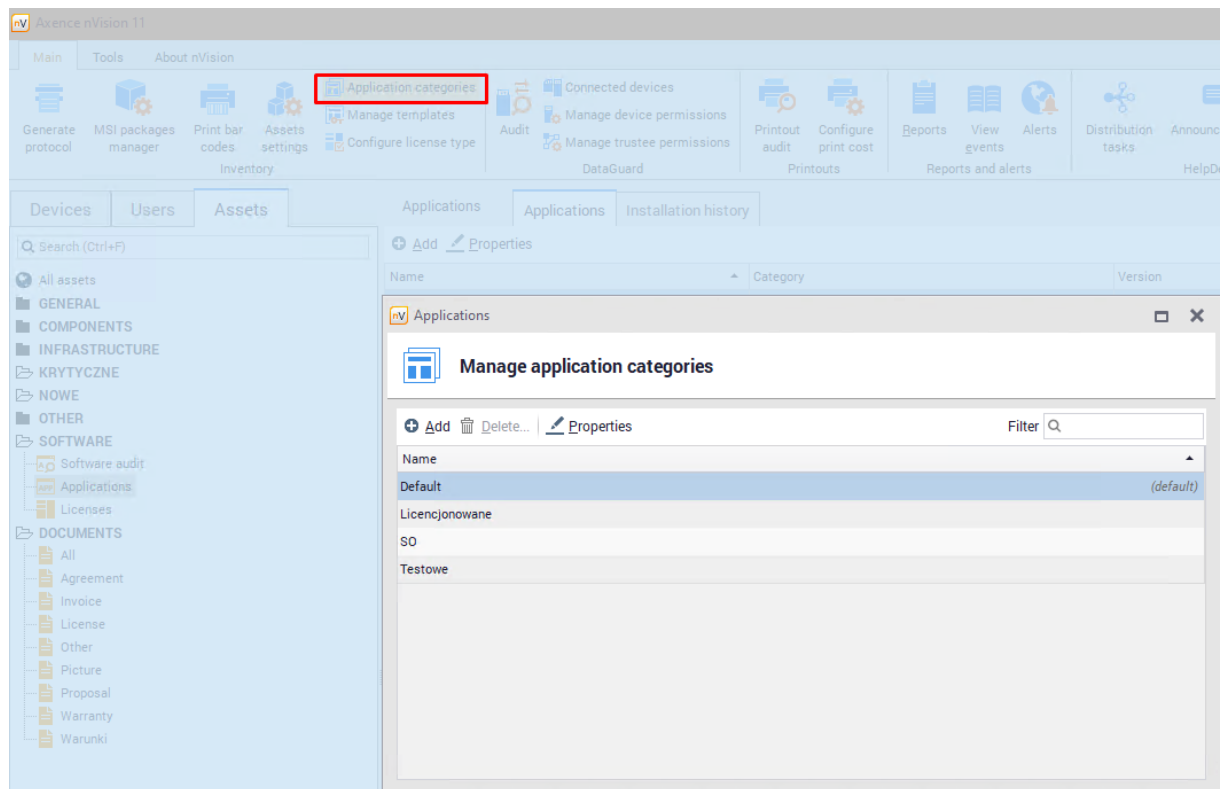
An important parameter of the application is the "Audited" field - if the application is audited, it is possible to assign a license to it.

8.5.2.2 Application categories

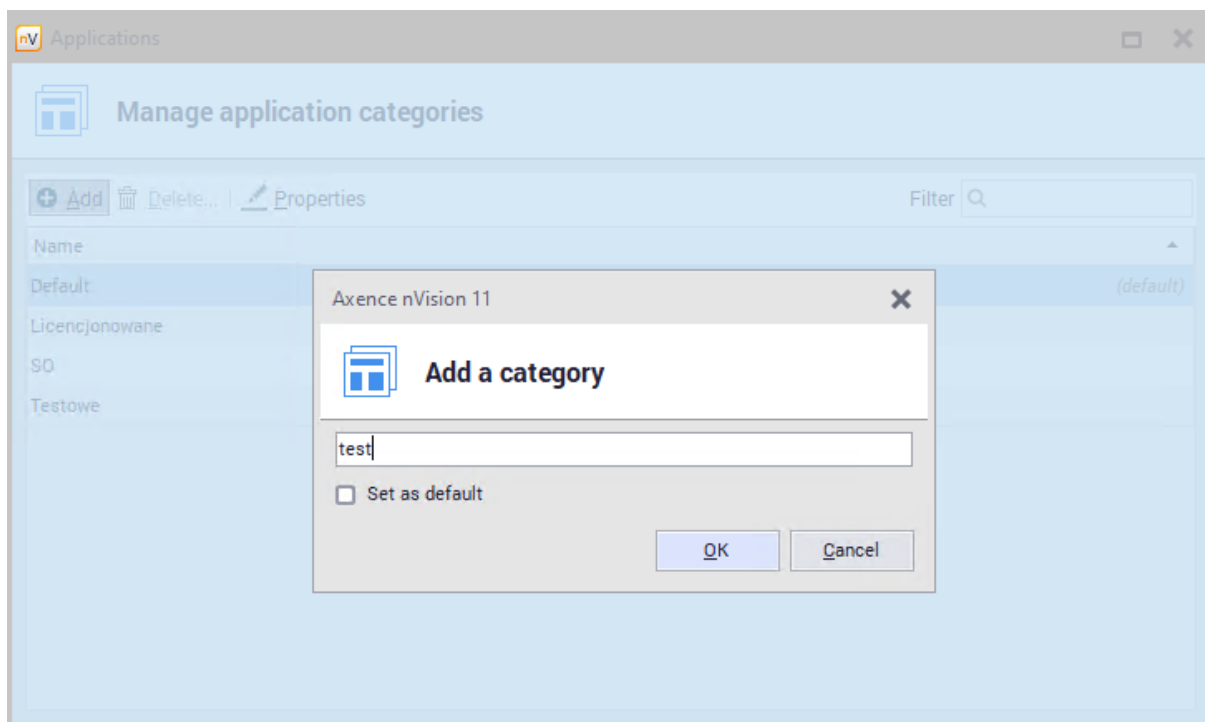
The Administrator has the option of assigning the application to categories that can be created and edited if need to. The categories allow to create your own way of organizing applications displayed in the program. Initially, the program contains only one "Default" category.

Creating new category

To create a new category, click the **Application categories** button on the main toolbar of the program. A list of categories will appear:



To create a new category, click the **Add** button and enter the name of the new category. While creating a category, you can specify a default category. This means that for **newly detected applications**, the selected category will be used as the default. A maximum of one category can be specified as default.

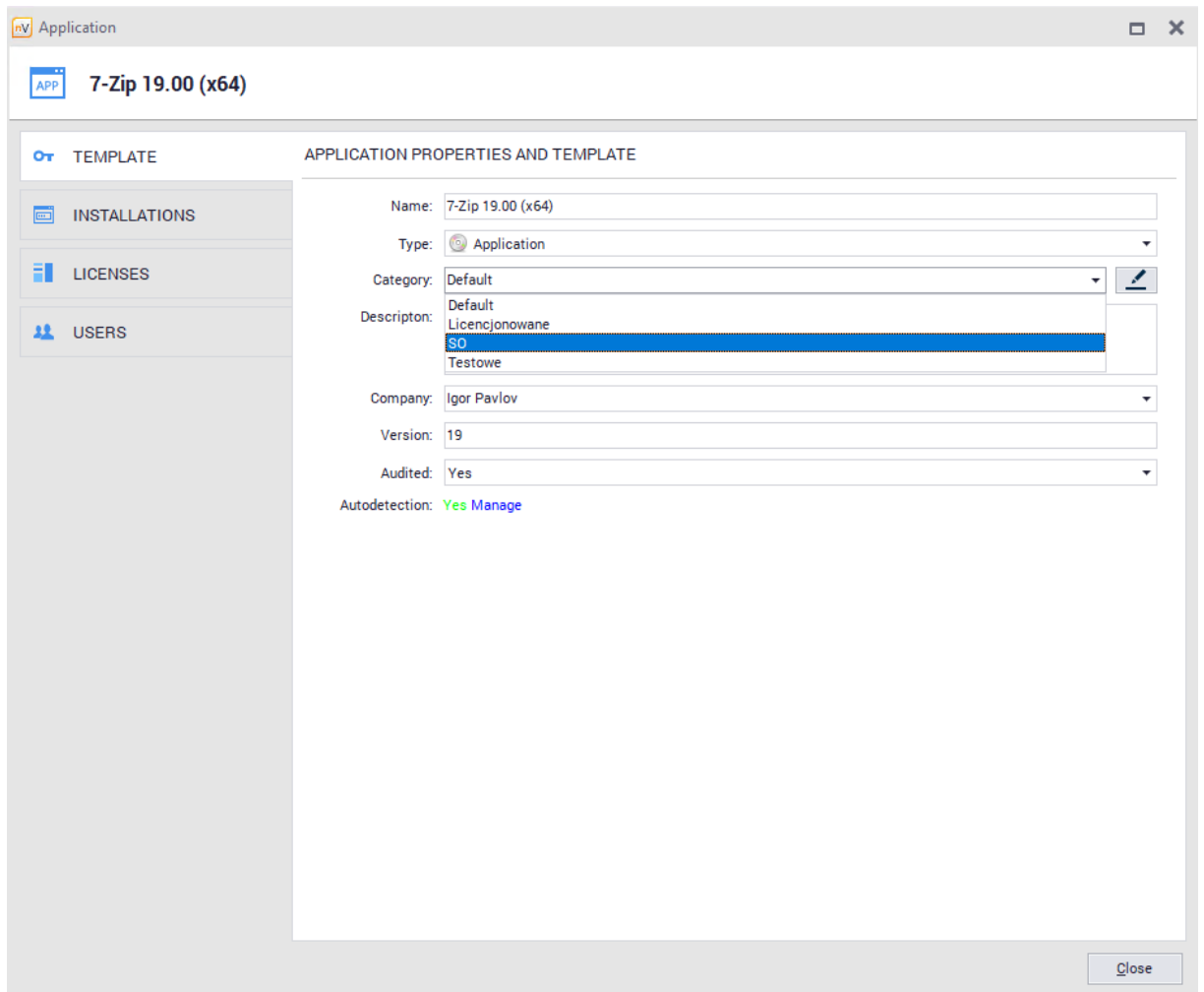


Removing category

To delete a category, go to the **Application Categories** window from the main toolbar, select the category on the list and click **Delete**. All applications that were in this category will be moved to the default category.

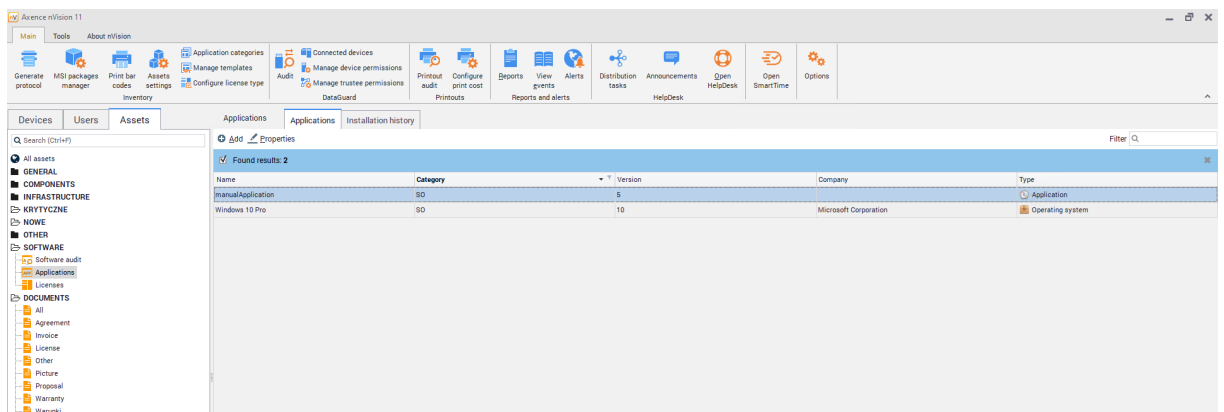
Assigning application to category

To assign an application to a category, select the appropriate item when creating or editing the application:



Category use case

Categories can support other administrative activities eg. present applications belonging to the selected category. Such information can be displayed in the **Assets** tab available from the main program window:



8.5.2.3 Application templates

Application templates are used to identify the installation of various types of applications. Patterns are divided into two types - created locally and synchronized with the Axence pattern database. Together with the nVision program, approx. 600 manually created patterns are provided to recognize the most-used applications.

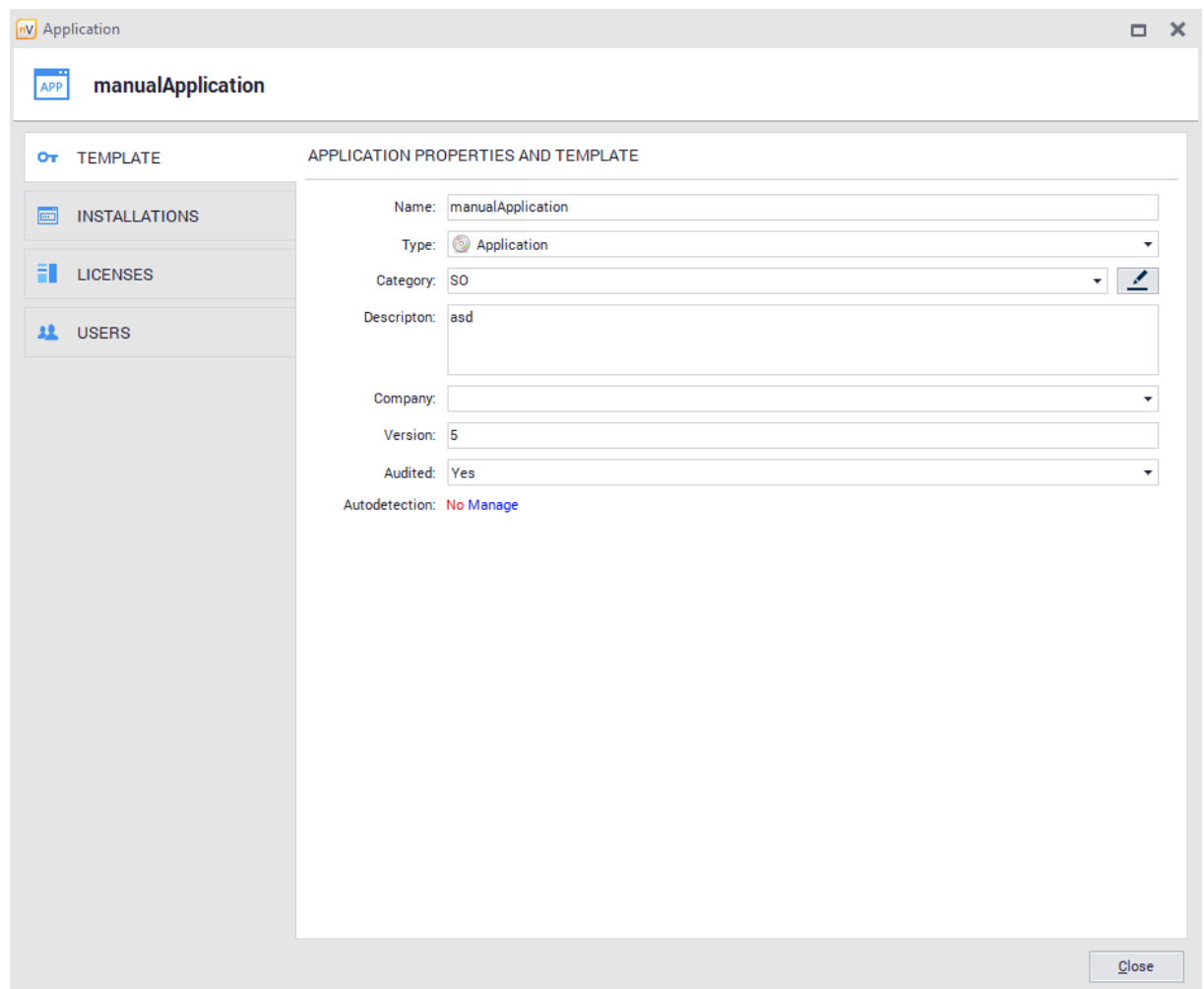
nVision distinguishes the following types of patterns:

- Applications and operating systems
- Security updates,
- Drivers,
- Operating Systems.

In the further part of the chapter, all four as above are to be understood as applications.

Application pattern

By going to the **Assets** tab visible in the main program window, and then double-clicking on any item on the **Application** list in the **Software** section, you can edit the application. The first available tab is pattern that defines basic information about the application:



The screenshot shows a window titled "Application" with a sub-header "manualApplication". The window is divided into two main sections: "TEMPLATE" on the left and "APPLICATION PROPERTIES AND TEMPLATE" on the right. The "TEMPLATE" section has a sidebar with icons for "INSTALLATIONS", "LICENSES", and "USERS". The "APPLICATION PROPERTIES AND TEMPLATE" section contains the following fields:

- Name: manualApplication
- Type: Application (dropdown menu)
- Category: SO (dropdown menu)
- Descriptor: asd (text input field)
- Company: (empty dropdown menu)
- Version: 5 (text input field)
- Audited: Yes (dropdown menu)
- Autodetection: No Manage (text with a link)

A "Close" button is located at the bottom right of the window.

Application has following attributes:

- Name,
- Type,
- Category,

- Description (optional),
- Company (optional),
- Version (optional),
- Audited,
- Autodetection.

After clicking the **Manage** button next to the **Autodetection** item, the automatic installation detection settings window will open. To enable automatic application detection, its pattern must contain at least one registry or file entry that is marked as identifying:

AUTODETECTION SETTINGS

To enable autodetection of the application, the application template must contain at least one registry template or at least one file template that is marked as identifying the application.

Autodetection:

REGISTRY

| Name | Version | Company | Identification |
|------------------------------|---------|-----------------------|-------------------------------------|
| OS: Microsoft Windows 10 Pro | * | Microsoft Corporation | <input checked="" type="checkbox"/> |

FILES

| File name | Version | Company | Product name | Original file name | Identification |
|----------------------|---------|---------|--------------|--------------------|----------------|
| <No data to display> | | | | | |

Autodetection of installed applications

The registry entries are checked first. If there the application already **has an entry in the registry**, it is considered to **be installed on the computer**. If the entry is not present, the files marked in the patterns as identifying are searched (most often it is the *.exe file that allows program run). If found, the application is considered to be on the computer. Otherwise (no registry entries and identification files) the application will not be detected.

Patterns synchronized with Axence database

The templates included in nVision were created manually based on the programs most frequently used by users. More information on managing embedded patterns is described in the [builtin templates](#) ^[262] chapter.

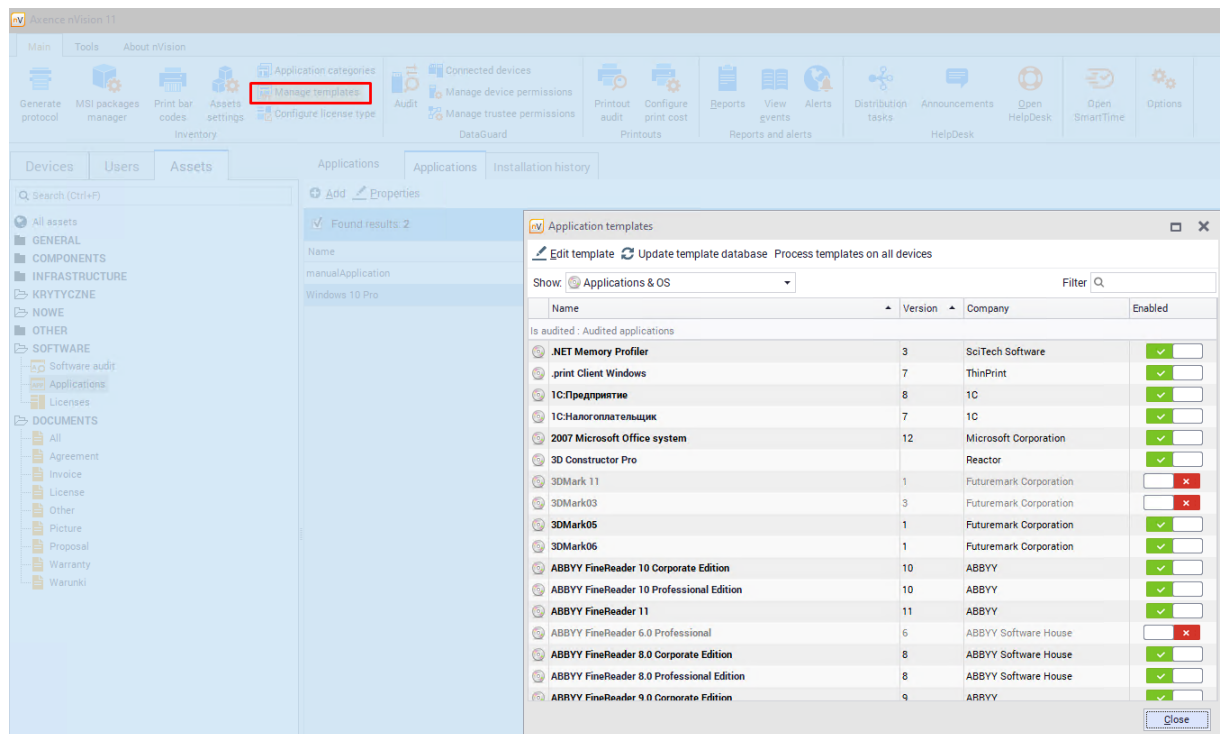
Patterns created automatically

Other templates are created automatically by nVision based on entries in the registers of monitored computers. Applications detected with this method are displayed in the list of detected and unknown applications where type of license is unknown to them.

These patterns can be edited, updated with license type, files associated with the application or files identifying it. If the Administrator is aware of an application from the list of detected and unknown, then it is recommended to edit its template.

8.5.2.4 Built-in templates management

To go to the built-in templates management window, select **Manage templates** from the main toolbar:



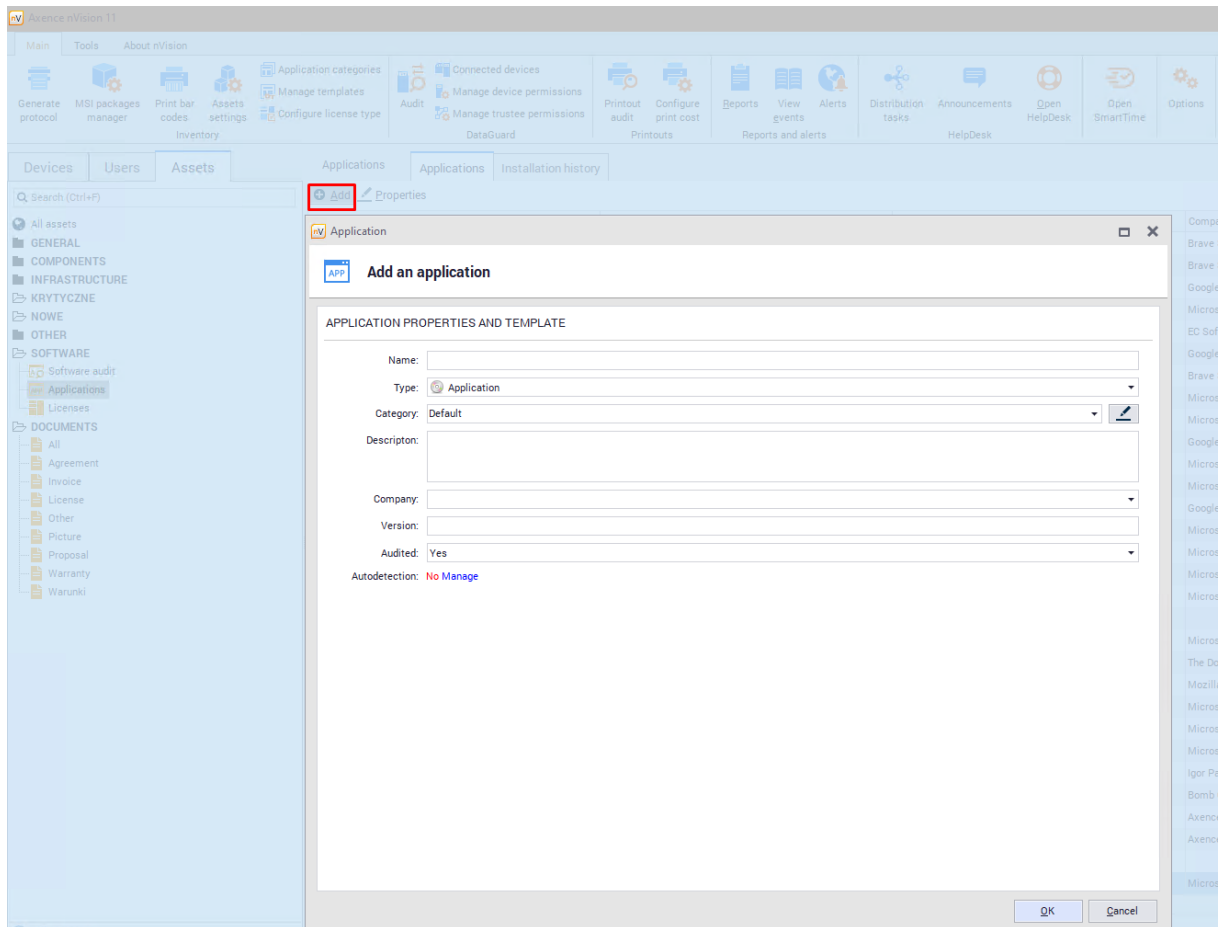
Patterns visible on the list have been synchronized with the Axence database and only the category to which they belong can be modified. Administrator has the ability to disable selected items using the context menu or by switch located on the right side of the window.

Patterns database update

Click **Update template database** button and nVision will download the latest available templates from the Axence server and add them to nVision.

8.5.2.5 Adding new application

To add a new application, go to the **Assets** tab visible in the main program window, scroll down for **Applications** in the **Software** section. Above the list of applications, locate and click the **Add** button. The window for adding a new application will open



In the next step, enter the values for the required fields such as "Name", "Type" and "Category". The remaining fields are optional.

The option of automatic application discovery has been described in [app template](#)^[260] chapter.

8.5.2.6 Application installations

Installations are instances of applications that have been automatically detected on computers with installed Agents. You cannot manually add or remove installations. Installations can also be assigned to users and licenses.

If you need to edit the application, go to the **Assets** tab visible in the main program window and double-click on any item on the **Application** list in the **Software** section, .

The **Installations** tab allows you to see a list of devices on which the installation of the selected application has been detected:

Application

APP Mozilla Firefox 73.0.1 (x86 pl)

TEMPLATE

INSTALLATIONS

LICENSES

USERS

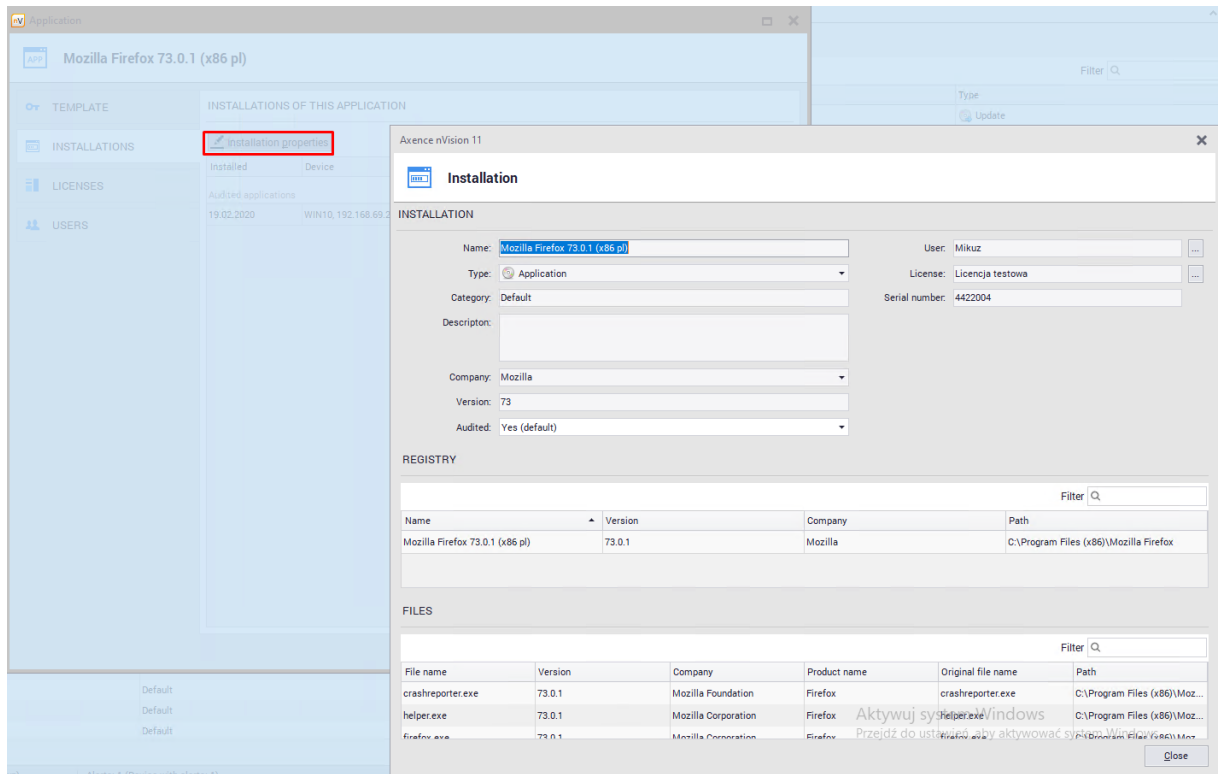
INSTALLATIONS OF THIS APPLICATION

Installation properties Filter

| Installed | Device | MSI Installer | User | License | Serial number |
|----------------------|-----------------------|------------------|-------|------------------|---------------|
| Audited applications | | | | | |
| 19.02.2020 | WIN10, 192.168.69.206 | Waiting for data | Mikuz | Licencja testowa | 4422004 |

Close

Double-clicking an item on the installation list or selecting Properties option allows you to view detailed information about the selected installation:



In the installation properties window you can assign user and license. This will impact the [licensing methods](#) on certain configurations.

If the application is audited, it is possible to exclude its selected installation from the audit. To achieve this, change the value of the **Audited** field in the installation properties window:

Axence nVision 11

Installation

INSTALLATION

Name: Mozilla Firefox 73.0.1 (x86 pl) User: Mikuz

Type: Application License: Licencja testowa

Category: Default Serial number: 4422004

Descriptor:

Company: Mozilla

Version: 73

Audited: Yes (default)

REGISTRY

Exclude from audit

| Name | Version | Company | Path |
|---------------------------------|---------|---------|--|
| Mozilla Firefox 73.0.1 (x86 pl) | 73.0.1 | Mozilla | C:\Program Files (x86)\Mozilla Firefox |

FILES

| File name | Version | Company | Product name | Original file name | Path |
|-------------------|---------|---------------------|--------------|--------------------|-------------------------------|
| crashreporter.exe | 73.0.1 | Mozilla Foundation | Firefox | crashreporter.exe | C:\Program Files (x86)\Moz... |
| helper.exe | 73.0.1 | Mozilla Corporation | Firefox | helper.exe | C:\Program Files (x86)\Moz... |
| firefox.exe | 73.0.1 | Mozilla Corporation | Firefox | firefox.exe | C:\Program Files (x86)\Moz... |

Close

8.5.2.7 Licenses and users

To edit applications, go to the **Assets** tab visible in the main program window, then double-click on any item on the **Applications** list in the **Software** section.

Licenses

Licenses tab allows to display a list associated with selected application:

Application

Mozilla Firefox 73.0.1 (x86 pl)

TEMPLATE

INSTALLATIONS

LICENSES

USERS

LICENSES FOR THIS APPLICATION

+ Add Delete... Properties Group by (None) Filter

| Belongs to | Name | Person responsible | Purchase date | Quantity | Usage |
|------------|------------------|--------------------|---------------|----------|-------|
| Szpital | Licencja testowa | Mikuz | 05.03.2020 | 5 | 2 |

Close

To add a new license associated with the selected application, click the **Add** button and fill in the required fields:

nV License
 □ ×

+ **Add license**

BASIC INFORMATION

* Name:

Asset type: Configure

Department: Select

Person responsible:

Inventory number:

Quantity: ▼

Unlimited

RELATED APPLICATIONS

+ Assign application
 - Unassign application
 Filter Q

| Name | Version | Company |
|---------------------------------|---------|---------|
| Mozilla Firefox 73.0.1 (x86 pl) | 73 | Mozilla |

ADDITIONAL FIELDS

Filter Q

| Name | Value |
|-------------------------------------|------------|
| Expiration date | |
| License type | |
| Osoba odpowiedzialna (przestarzałe) | |
| Purchase date | 26.03.2020 |
| Supplier | |
| Value | |

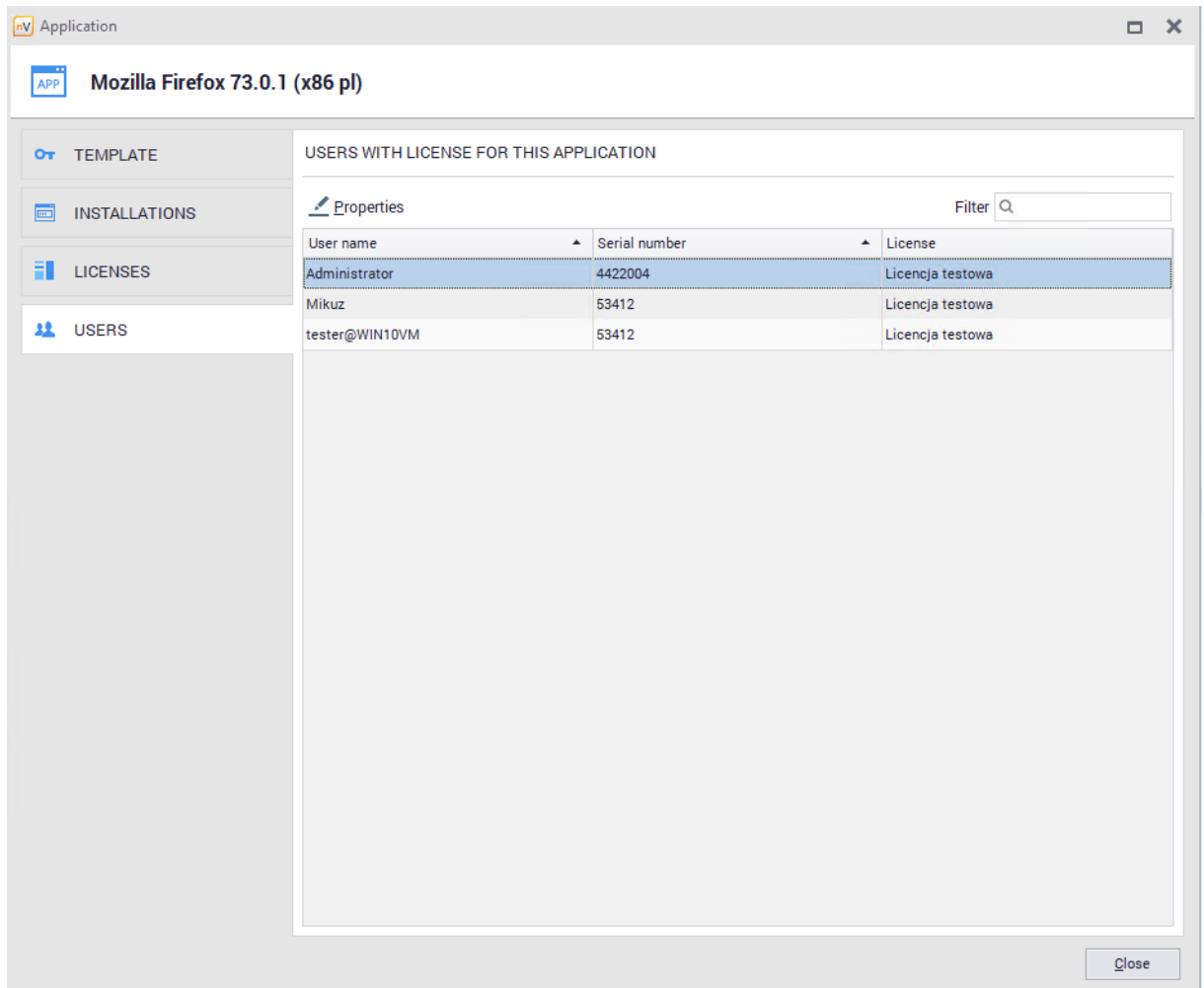
OK
Cancel

Creating new licenses is described in [add license](#)^[274] chapter.

Existing licenses can be associated with any applications. This process has been described in [general information](#)^[278] chapter.

Users

Licenses tab allows to display users assigned to the license **associated with the application**:



Process of associating users with licenses is described in [license users](#)²⁸⁴ chapter.

8.5.2.8 Installation History

The installation history feature allows you to collect information about removed and installed applications on computers with the Agent installed.

To go to the installation history, select the **Assets** tab in the main program window, then scroll down for **Applications** in the **Software** section. The installation history of all applications will be displayed above the application list:

The screenshot shows the Axence nVision 11 main interface. The 'Applications' tab is active, displaying a table of installation history for a selected host. The table columns are Date, Type, Operation, and Description. The data shows various software updates and applications installed or removed on the host.

| Date | Type | Operation | Description |
|---------------------|------------------|-----------|--|
| 26.03.2020 01:20:39 | Software updates | Remove | Detected removal of Update (KB4528760) application |
| 26.03.2020 01:20:39 | Software updates | Remove | Detected removal of Update (KB4532938) application |
| 26.03.2020 01:20:38 | Software updates | Add | Detected Update (KB451762) application |
| 26.03.2020 01:20:38 | Software updates | Add | Detected Security Update (KB4537799) application |
| 26.03.2020 01:20:38 | Software updates | Add | Detected Update (KB4534132) application |
| 26.03.2020 01:20:38 | Software updates | Add | Detected Security Update (KB4541338) application |
| 26.03.2020 01:20:38 | Software updates | Add | Detected Mozilla Firefox 74.0 (x64 pl) application |
| 24.03.2020 14:24:01 | Software | Add | Detected Mozilla Maintenance Service application |
| 24.03.2020 14:24:00 | Software updates | Add | Detected Update (KB4513661) application |
| 24.03.2020 14:24:00 | Software updates | Add | Detected Update (KB4517245) application |
| 24.03.2020 14:24:00 | Software | Add | Detected Internet Explorer application |
| 24.03.2020 14:23:59 | Software | Add | Detected Windows 10 Pro application |
| 24.03.2020 14:23:59 | Software | Add | Detected Axence nVision Agent application |
| 24.03.2020 14:23:59 | Software updates | Add | Detected Security Update (KB4532939) application |
| 24.03.2020 14:23:59 | Software updates | Add | Detected Update (KB4528760) application |
| 24.03.2020 14:23:59 | Software updates | Add | Detected Update (KB4532938) application |
| 24.03.2020 14:23:59 | Software | Add | Detected Axence nVision application |
| 24.03.2020 14:23:59 | Software updates | Add | Detected Security Update (KB4516115) application |
| 16.03.2020 11:08:43 | Software updates | Remove | Wykryto usunięcie aplikacji Update (KB4540673) |
| 16.03.2020 11:08:43 | Software updates | Add | Wykryto aplikację Update (KB4551762) |
| 10.03.2020 20:47:30 | Software updates | Remove | Wykryto usunięcie aplikacji Update (KB4532693) |
| 10.03.2020 20:47:30 | Software updates | Add | Wykryto aplikację Update (KB4540673) |
| 10.03.2020 19:50:32 | Software updates | Add | Wykryto aplikację Security Update (KB4541338) |

Installation history of selected host

Go to the Device Information window, select **Software / History** tab to see the **installation history** of the selected host:

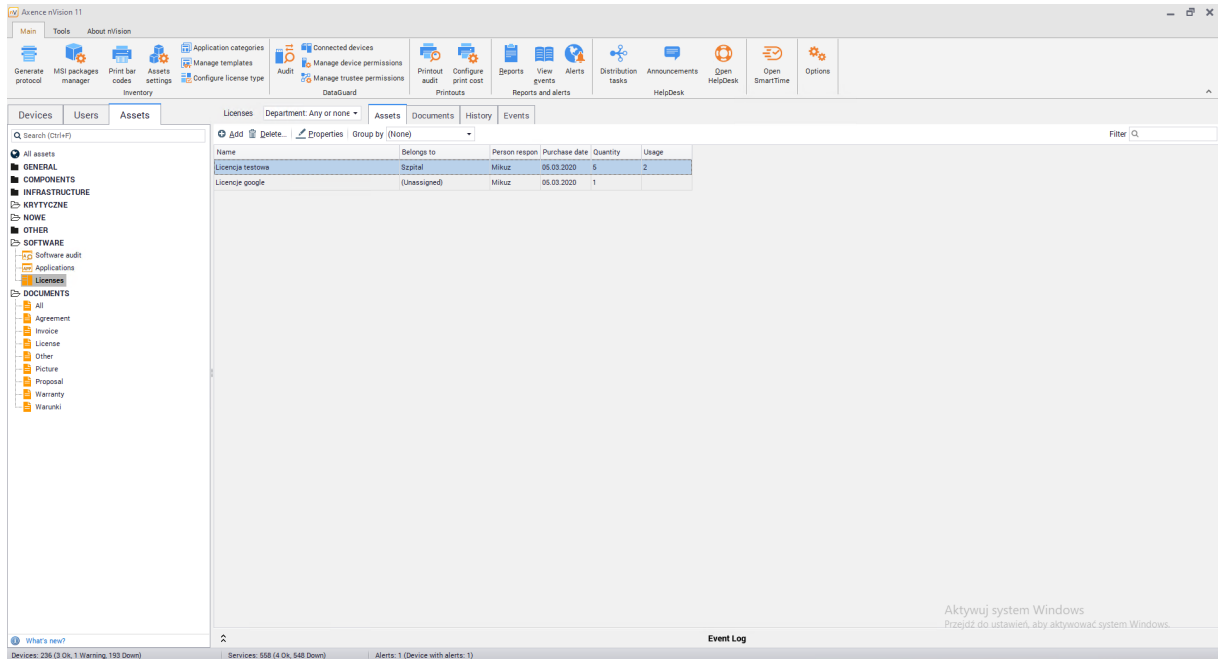
The screenshot shows the Device Information window for host WIN10 (IP: 192.168.69.206). The 'History' tab is active, displaying a table of software installations and updates. The table columns are Date, Type, Operation, and Description. The data shows various software updates and applications installed or removed on the host.

| Date | Type | Operation | Description |
|---------------------|------------------|-----------|--|
| 19.02.2020 14:48:56 | Software | Remove | Detected removal of Mozilla Firefox application |
| 19.02.2020 14:48:54 | Software | Add | Detected Mozilla Firefox 73.0.1 (x86 pl) application |
| 14.02.2020 17:45:51 | Software updates | Add | Wykryto aplikację Security Update (KB4524244) |
| 13.02.2020 08:45:21 | Software updates | Remove | Wykryto usunięcie aplikacji Update (KB4528760) |
| 13.02.2020 08:45:21 | Software updates | Add | Wykryto aplikację Update (KB4532693) |
| 13.02.2020 05:41:28 | Software updates | Remove | Wykryto usunięcie aplikacji Update (KB4532938) |
| 13.02.2020 05:41:28 | Software updates | Add | Wykryto aplikację Security Update (KB4537759) |
| 13.02.2020 05:41:28 | Software updates | Add | Wykryto aplikację Update (KB4534132) |
| 13.02.2020 04:46:59 | Software updates | Add | Wykryto aplikację Security Update (KB4538674) |
| 11.02.2020 04:40:35 | Software | Remove | Wykryto usunięcie aplikacji Brave |
| 11.02.2020 04:40:34 | Software | Add | Wykryto aplikację Brave |
| 10.02.2020 09:41:10 | Software | Remove | Wykryto usunięcie aplikacji Microsoft Edge |
| 10.02.2020 09:41:10 | Software | Remove | Wykryto usunięcie aplikacji Google Chrome |
| 10.02.2020 09:41:07 | Software | Add | Wykryto aplikację Microsoft Edge |
| 10.02.2020 09:41:07 | Software | Add | Wykryto aplikację Google Chrome |
| 03.02.2020 15:12:16 | Software | Add | Detected Mozilla Firefox application |
| 03.02.2020 12:08:18 | Software | Add | Detected Sublime Text 3 application |
| 03.02.2020 11:07:51 | Software | Add | Detected 7-Zip 19.00 (x64) application |

8.5.3 License management

8.5.3.1 Licenses list

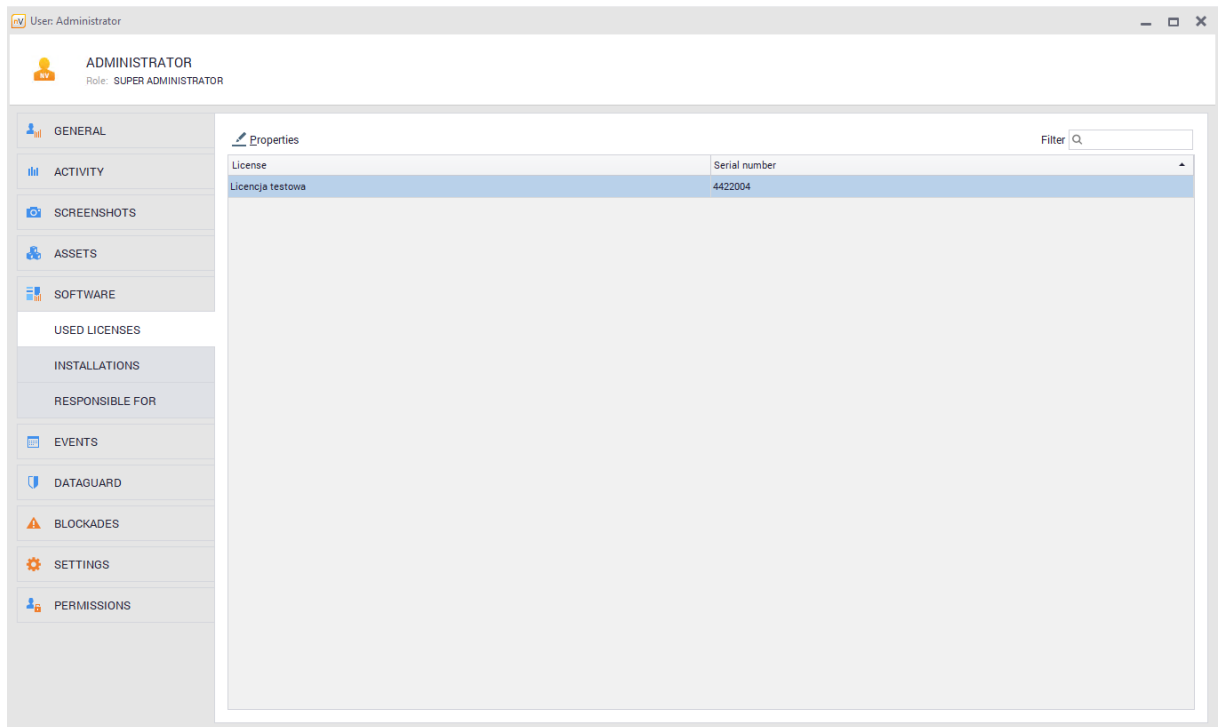
To display licenses list, go to the **Assets** tab in the main program window, and then scroll down for **Licenses** in the **Software** section. List displayed all licenses added to nVision:



Licenses are always created manually by the Administrator. Licenses can be associated with users or installations of selected applications. **Licenses can only be assigned to audited applications.**

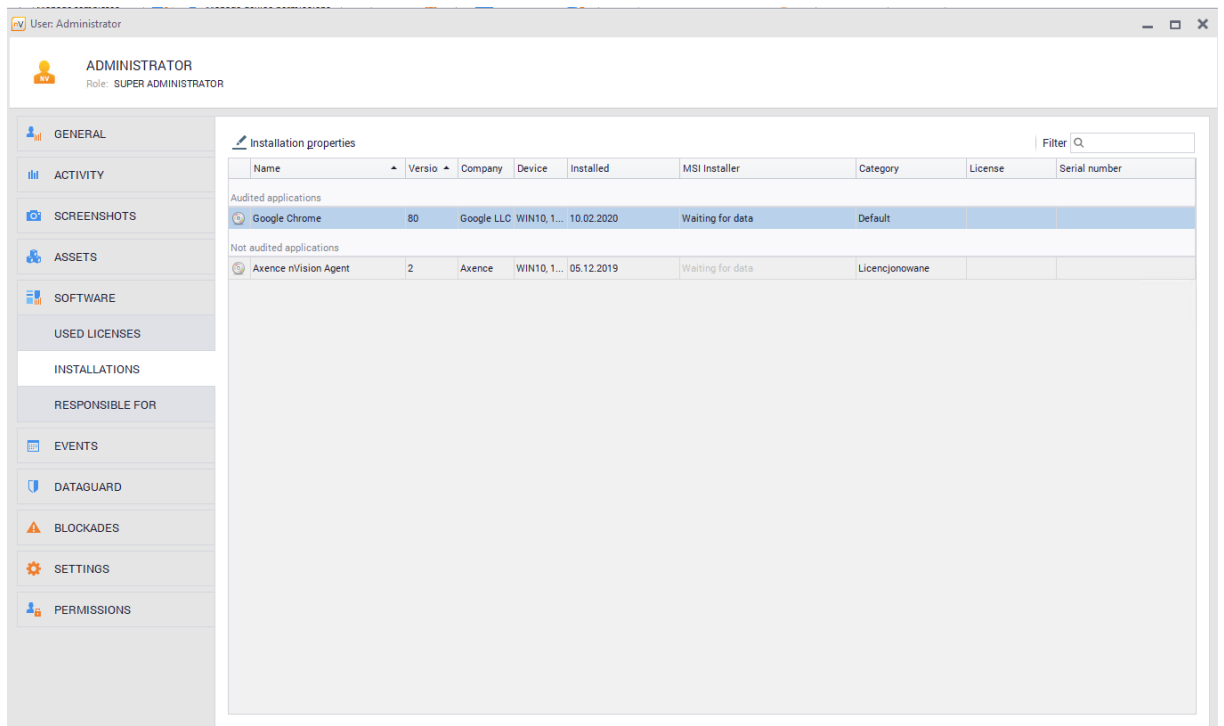
Licenses assigned to user

To view the licenses assigned to user, go to the user information window and select the **Software / Licenses Used** tab:



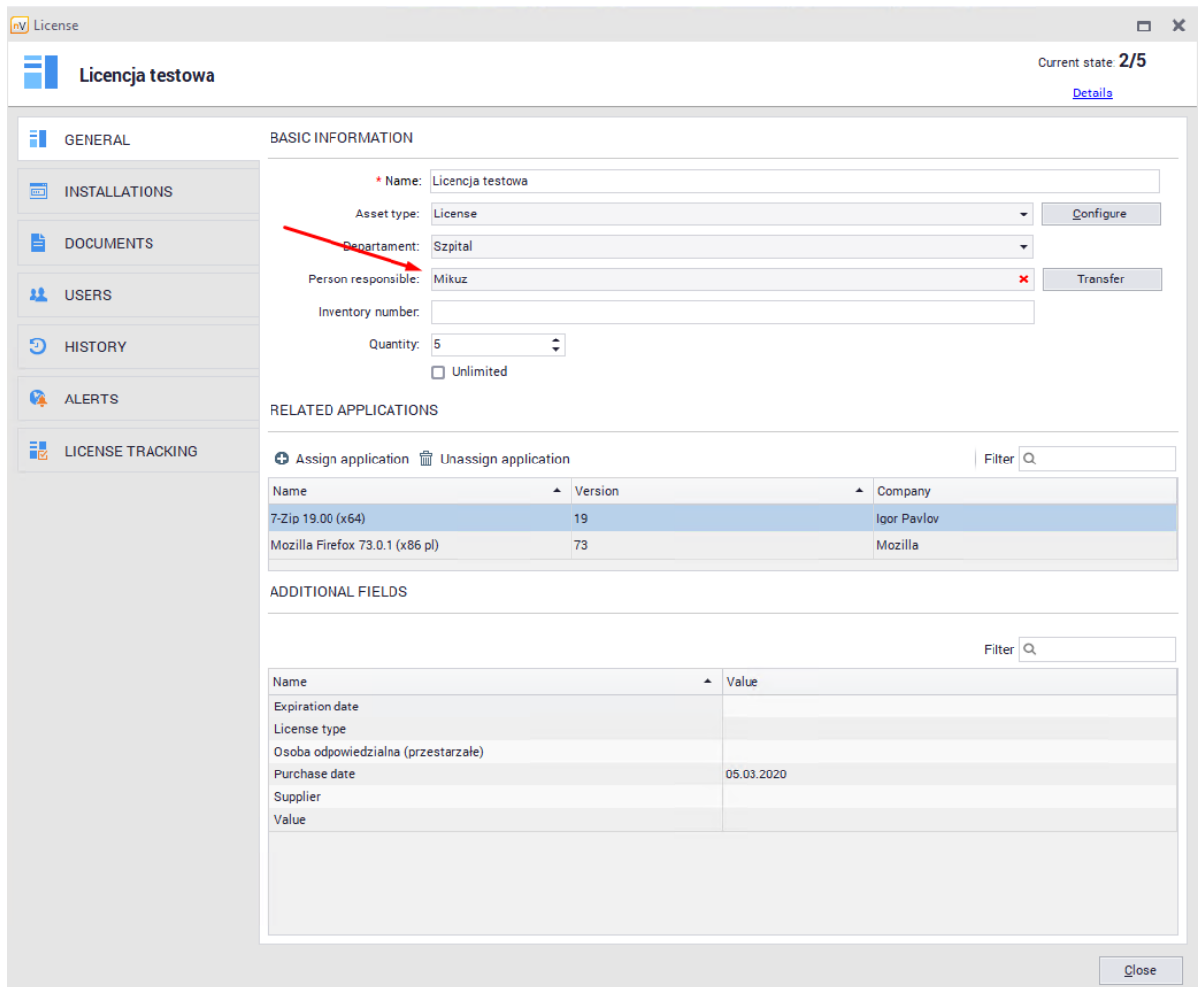
Application installations assigned to user

To view the application installations assigned to the user, go to user information window and then select the **Software / Installations** tab



License responsibility

In the license properties window you can specify the person responsible for the selected license:

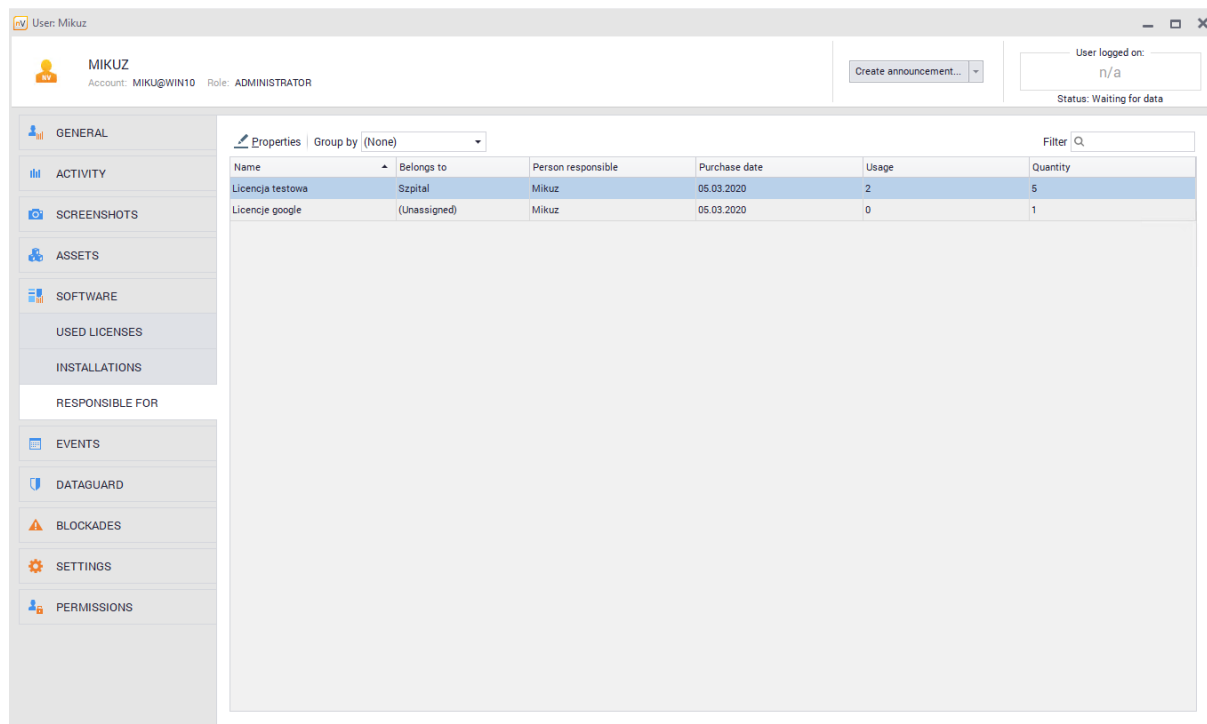


The screenshot shows a software window titled "Licencja testowa" with a "Current state: 2/5" indicator. The interface is divided into several sections:

- GENERAL**: A sidebar menu with options: INSTALLATIONS, DOCUMENTS, USERS, HISTORY, ALERTS, and LICENSE TRACKING.
- BASIC INFORMATION**: Fields for Name (Licencja testowa), Asset type (License), Department (Szpital), Person responsible (Mikuz), Inventory number, and Quantity (5). There are "Configure" and "Transfer" buttons.
- RELATED APPLICATIONS**: A table with columns Name, Version, and Company. It lists "7-Zip 19.00 (x64)" and "Mozilla Firefox 73.0.1 (x86 pl)".
- ADDITIONAL FIELDS**: A table with columns Name and Value. It lists fields like Expiration date, License type, Osoba odpowiedzialna (przestarzała), Purchase date (05.03.2020), Supplier, and Value.

A red arrow points to the "Person responsible" field, which is set to "Mikuz".

To view the licenses for which the user is responsible, go to user information window and then select the **Software / Responsible** tab:

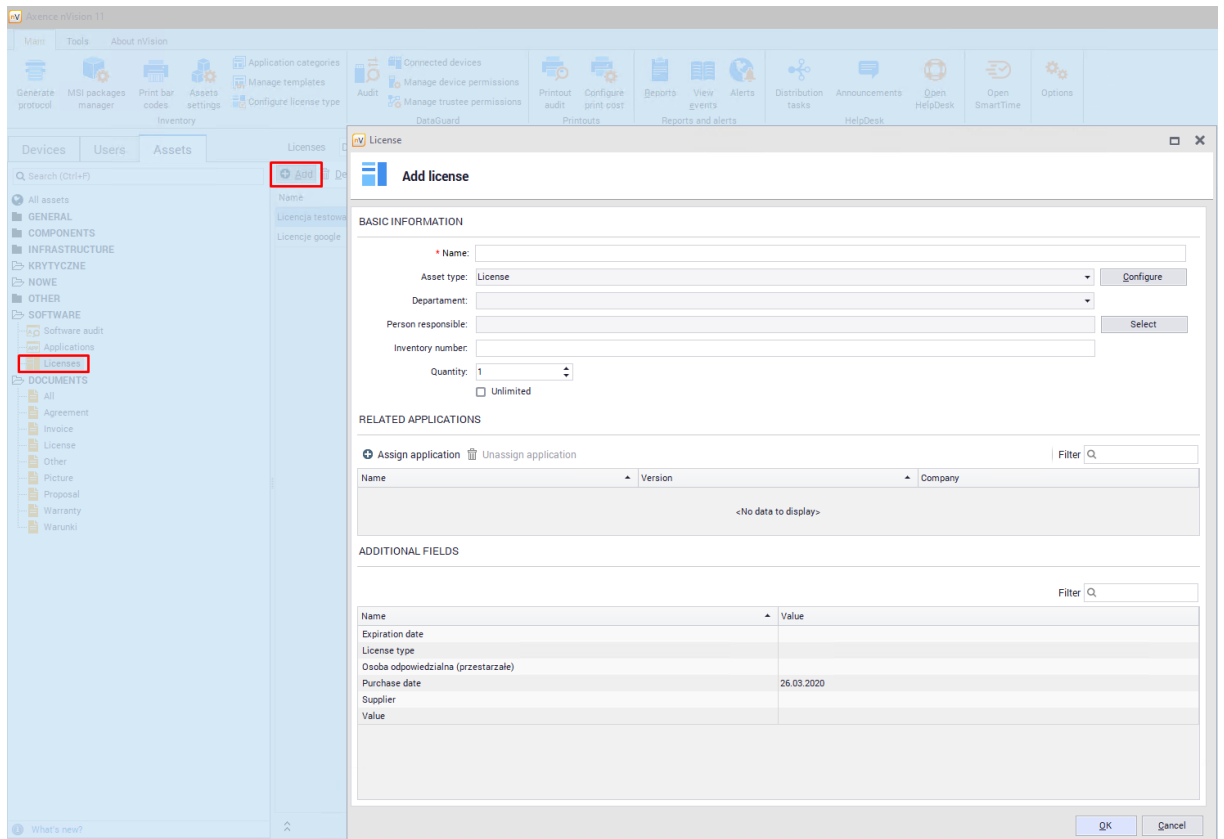


The screenshot displays the Axence nVision user interface. At the top, the user profile for 'MIKUZ' is shown, with account 'MIKU@WIN10' and role 'ADMINISTRATOR'. A 'Create announcement...' button is visible. The main content area is divided into a left sidebar with navigation options and a main table area. The sidebar includes: GENERAL, ACTIVITY, SCREENSHOTS, ASSETS, SOFTWARE, USED LICENSES, INSTALLATIONS, RESPONSIBLE FOR, EVENTS, DATAGUARD, BLOCKADES, SETTINGS, and PERMISSIONS. The main table area shows a list of licenses with the following data:

| Name | Belongs to | Person responsible | Purchase date | Usage | Quantity |
|------------------|--------------|--------------------|---------------|-------|----------|
| Licencja testowa | Szpital | Mikuz | 05.03.2020 | 2 | 5 |
| Licencje google | (Unassigned) | Mikuz | 05.03.2020 | 0 | 1 |

8.5.3.2 Adding new license

To add a new license, go to the **Assets tab** in the main program window and then scroll down for **Licenses** in the **Software** section. Above the license list, click the **Add** button. The window for adding a new license will open:



Standard description fields include:

- Name,
- Department (optional),
- Person responsible (optional),
- Inventory number (optional),
- Related applications (you can only assign license to audited applications),
- Quantity.

Additional license configuration options are described in the following chapter.

Alternative license add process

You can add a license directly from the application edition window - select an item from the list of applications, go to its properties window, select the **Licenses** tab. In the upper part of the window you will see the **Add** button, which will open the window for adding licenses:

Add license

BASIC INFORMATION

* Name: Mozilla Firefox 73.0.1 (x86 pl)

Asset type: License Configure

Department: (Unassigned)

Person responsible: Select

Inventory number:

Quantity: 1 Unlimited

RELATED APPLICATIONS

Assign application Unassign application Filter

| Name | Version | Company |
|---------------------------------|---------|---------|
| Mozilla Firefox 73.0.1 (x86 pl) | 73 | Mozilla |

ADDITIONAL FIELDS

Filter

| Name | Value |
|-------------------------------------|------------|
| Expiration date | |
| License type | |
| Osoba odpowiedzialna (przestarzałe) | |
| Purchase date | 26.03.2020 |
| Supplier | |
| Value | |

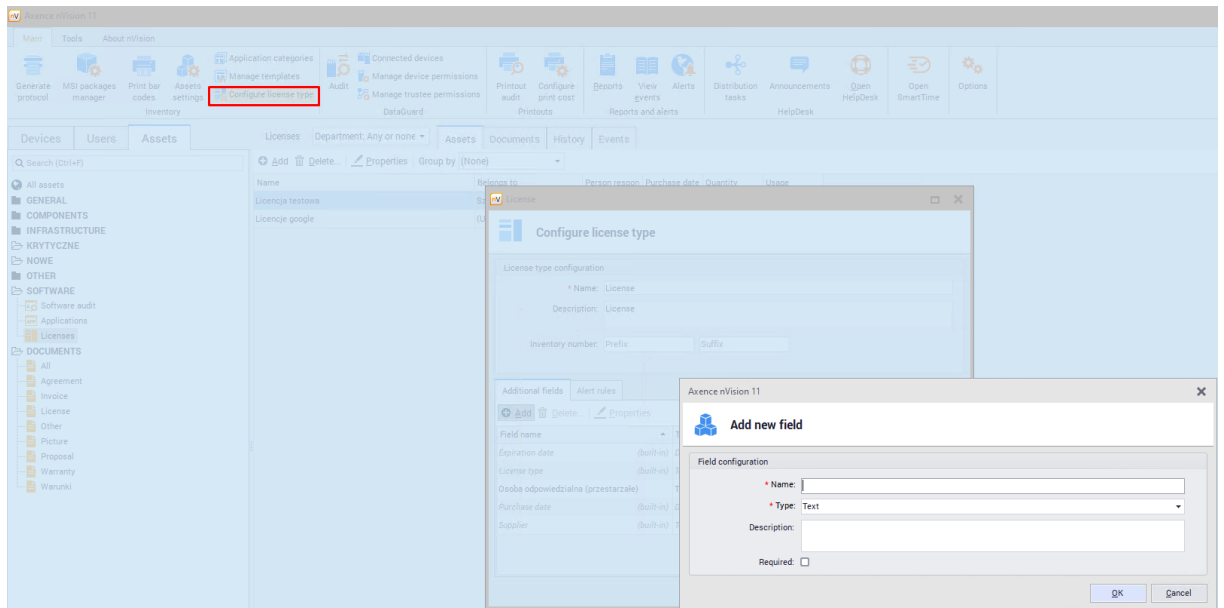
OK Cancel

License created with this process will be automatically bound with application, to which it's been added.

8.5.3.3 License additional fields

Additional fields for licenses

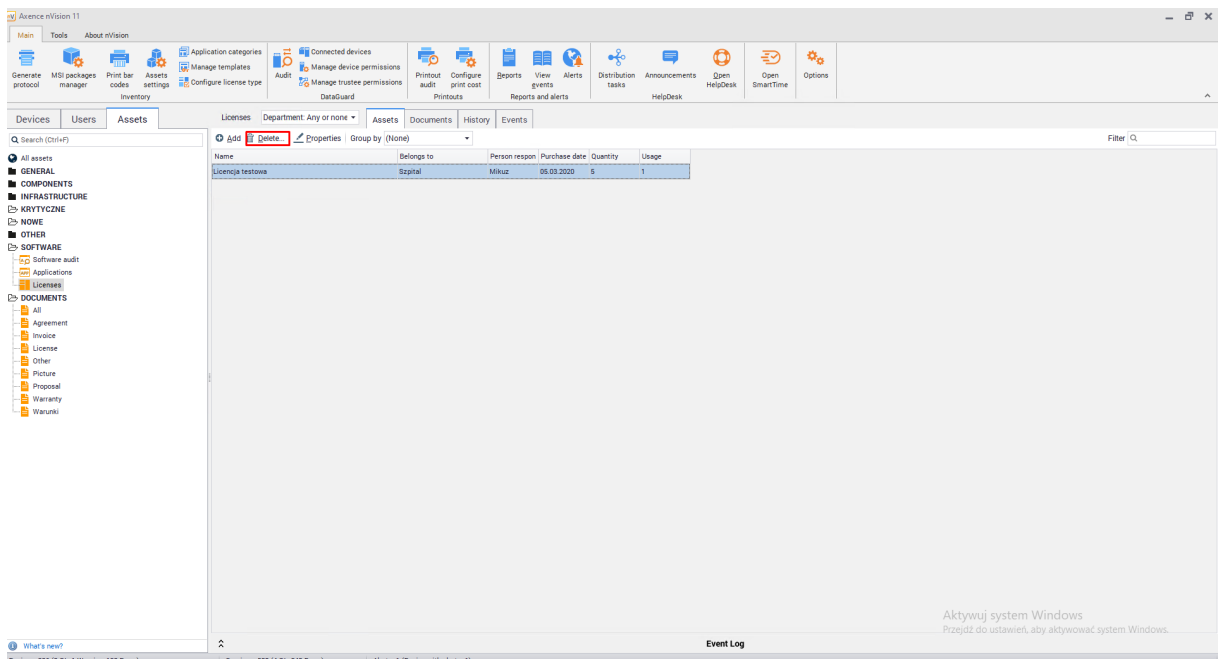
To add an additional field for all licenses, select **Configure license type** on the main toolbar. This will open the configuration window where additional fields can be added:



You cannot add additional fields for single licenses.

8.5.3.4 License removal

To remove a license, go to the **Assets** tab in the main program window, and then scroll down for **Licenses** in the **Software** section. After selecting the item to be deleted, click the **Delete** button above the license list:



Removing the license will result in deleting all assignments to other objects. If installations or users were assigned to the license, these associations will be removed.

Removing assigned applications

Removing the application associated with the license will result in **removal from the license properties** of the installation and other entries related to the application. To remove an associated application, remove the selected item from the list of related applications in the license properties window:

License

Licencja testowa Current state: 1/5
[Details](#)

GENERAL

INSTALLATIONS

DOCUMENTS

USERS

HISTORY

ALERTS

LICENSE TRACKING

BASIC INFORMATION

* Name: Licencja testowa

Asset type: License Configure

Departament: Szpital

Person responsible: Mikuz Transfer

Inventory number:

Quantity: 5 Unlimited

RELATED APPLICATIONS

Assign application Unassign application Filter

| Name | Version | Company |
|---------------------------------|---------|-------------|
| 7-Zip 19.00 (x64) | 19 | Igor Pavlov |
| Mozilla Firefox 73.0.1 (x86.pl) | 73 | Mozilla |

ADDITIONAL FIELDS Filter

| Name | Value |
|-------------------------------------|------------|
| Expiration date | |
| License type | |
| Osoba odpowiedzialna (przestarzałe) | |
| Purchase date | 05.03.2020 |
| Supplier | |
| Value | |

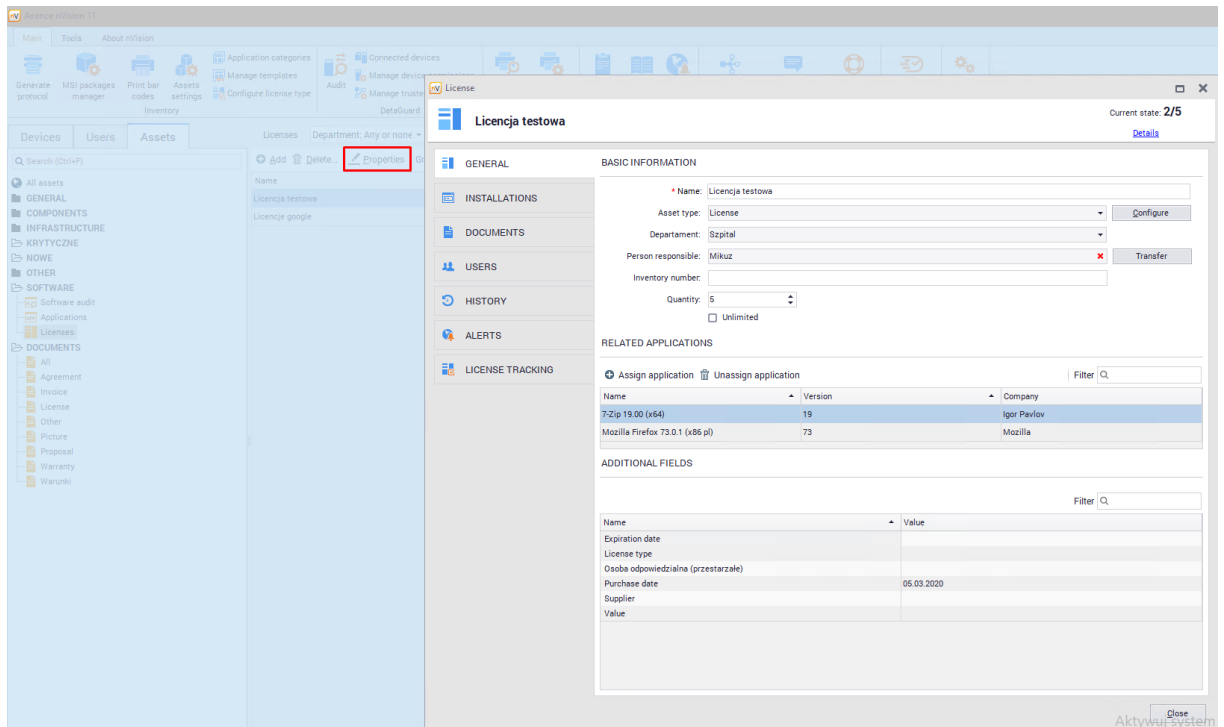
Close

8.5.3.5 License editing properties

8.5.3.5.1 License properties

To access the **License Properties** window, select the **Assets** tab in the main program window, and then scroll down for **Licenses** in the **Software** section.

After selecting an item from the list, click the **Properties** button or double-click on the selected license:



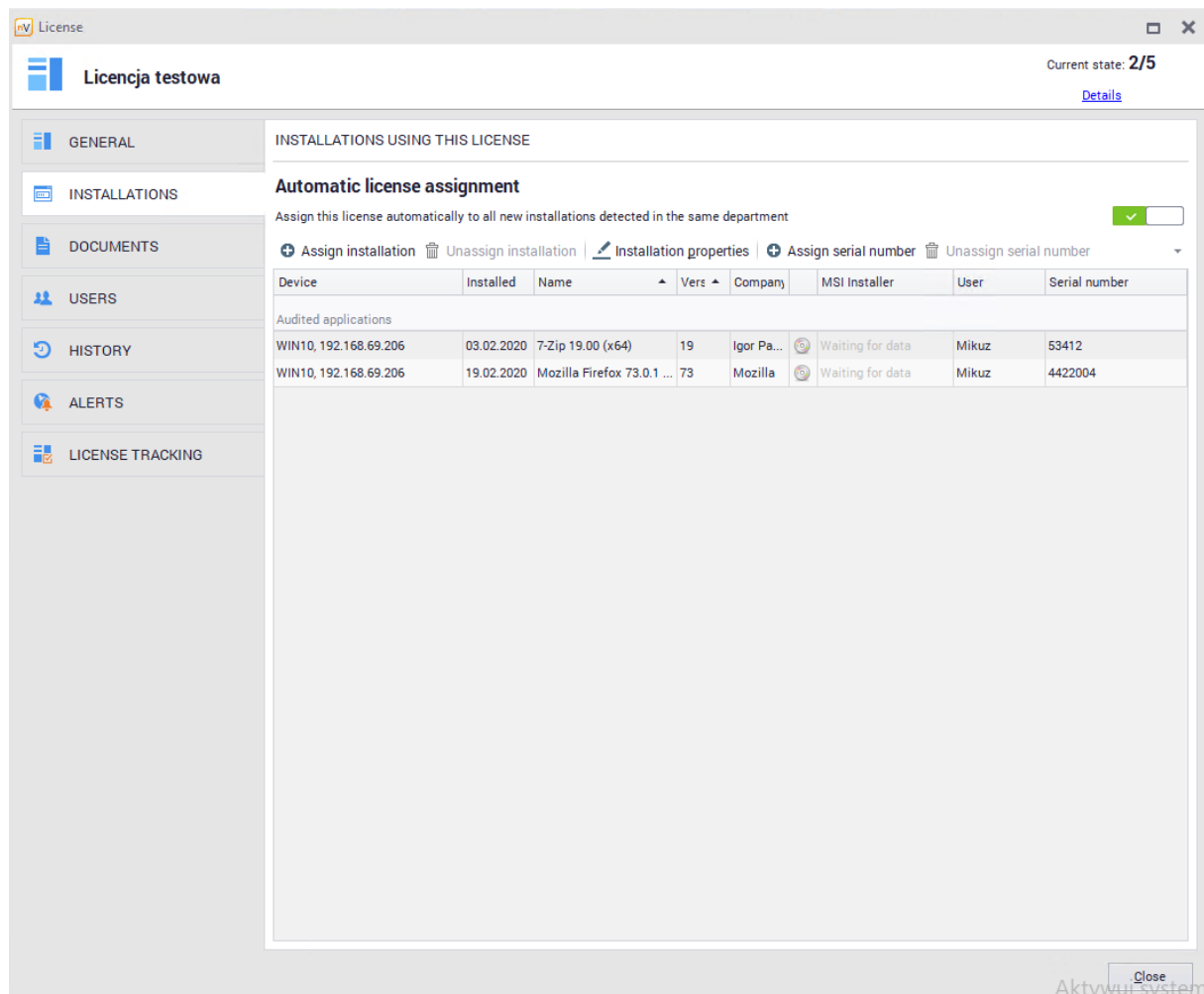
The license properties window will open, showing several tabs described in the following chapters. The General tab allows you to edit basic license information. This window includes three sections:

- **Basic information** - basic license properties.
- **Related Applications** - license related applications. **Licenses can only be assigned to audited applications.**
- **Additional fields** - additional fields for the selected license.

In the top right corner you will find the Current status field, which informs about the current licenses usage status. The usage depends on the configuration described in the [licensing methods](#) ²⁹⁰ chapter:

8.5.3.5.2 Application installation

The **Properties** includes the **Installations** tab which presents information about detected application installations that are associated with the edited license:



License

Licencja testowa

Current state: 2/5

Details

GENERAL

INSTALLATIONS USING THIS LICENSE

Automatic license assignment

Assign this license automatically to all new installations detected in the same department

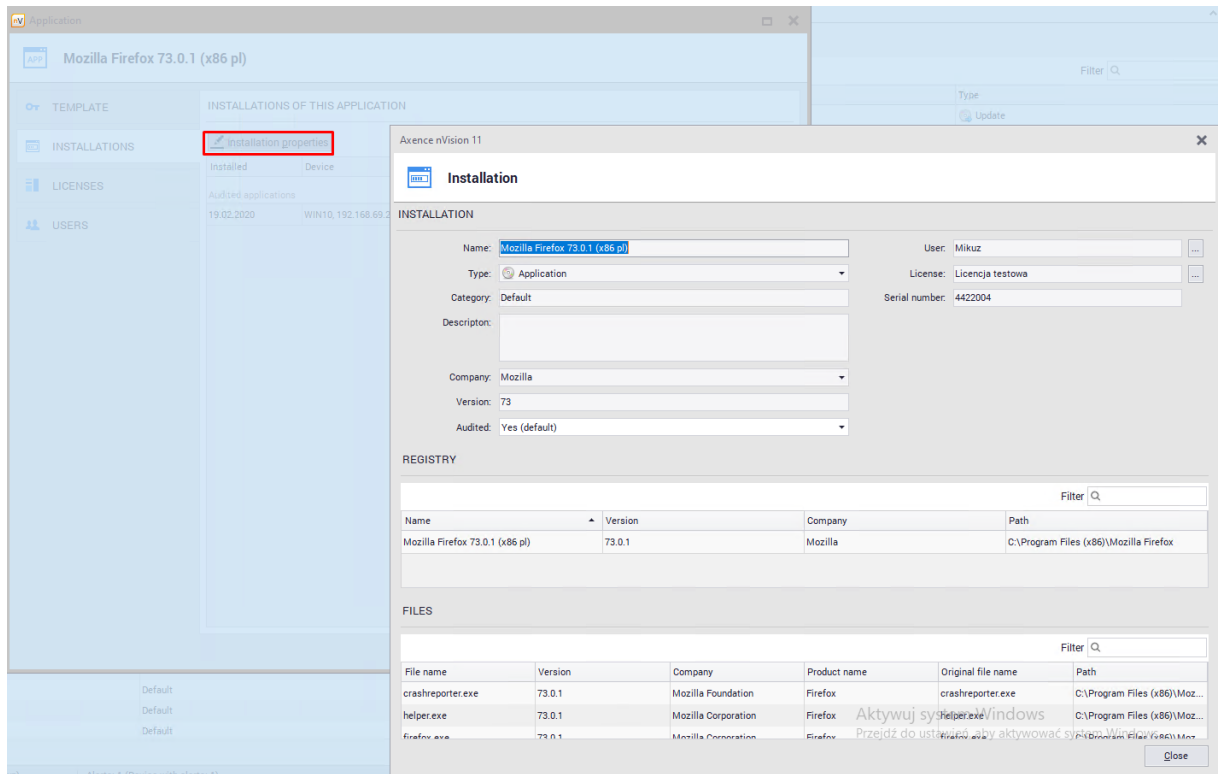
Assign installation Unassign installation Installation properties Assign serial number Unassign serial number

| Device | Installed | Name | Verz | Company | MSI Installer | User | Serial number |
|-----------------------|------------|----------------------------|------|------------|------------------|-------|---------------|
| Audited applications | | | | | | | |
| WIN10, 192.168.69.206 | 03.02.2020 | 7-Zip 19.00 (x64) | 19 | Igor Pa... | Waiting for data | Mikuz | 53412 |
| WIN10, 192.168.69.206 | 19.02.2020 | Mozilla Firefox 73.0.1 ... | 73 | Mozilla | Waiting for data | Mikuz | 4422004 |

Close

Aktywui System

Double-clicking the selected installation or selecting the **Properties** button a window with detailed information of this installation will be displayed:



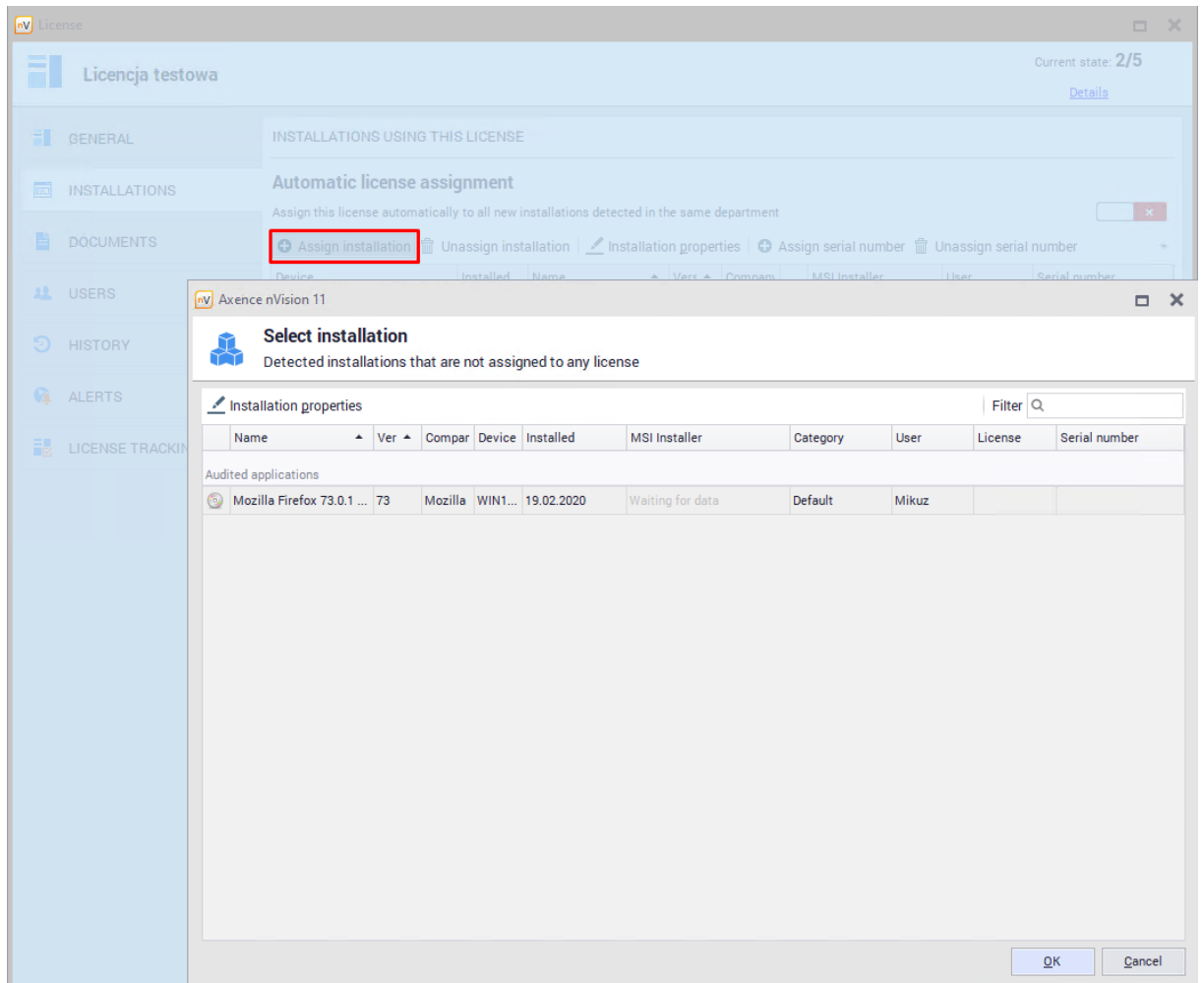
This function is described in [app instances](#) ²⁶³ chapter.

Assignment to installations

A switch is available at the top of the installation tab window that allows you to automatically assign licenses to new detected installations. Turning it on will automatically add more items to the list of installations once they are detected.

Adding instances

If the automatic license assignment is enabled, new items will appear once the installations are detected. To manually add an installation associated with the license application, click the **Assign installation** button and select an item from the list:



Removing instances

To remove the installation associated with the license application, select the item from the list and click the button **Unassign installation**.

If automatic license assignment is enabled, the deleted item may return to the installation list despite deletion.

Installation serial number

To assign a serial number to the installation, select an item from the list and then click the **Assign Serial Number** button.

Installations with the same serial number can be configured for using only one license. More information is described in [licensing methods](#) ²⁹⁰ chapter.

8.5.3.5.3 Documents

The **Documents** tab in the **License Properties** window allows you to add, display and delete documents related to the selected license.

The documents associated with the selected are displayed in the table:

License

Licencja testowa

Current state: 1/5

[Details](#)

GENERAL

INSTALLATIONS

DOCUMENTS

USERS

HISTORY

ALERTS

LICENSE TRACKING

DOCUMENTS RELATED TO THIS LICENSE

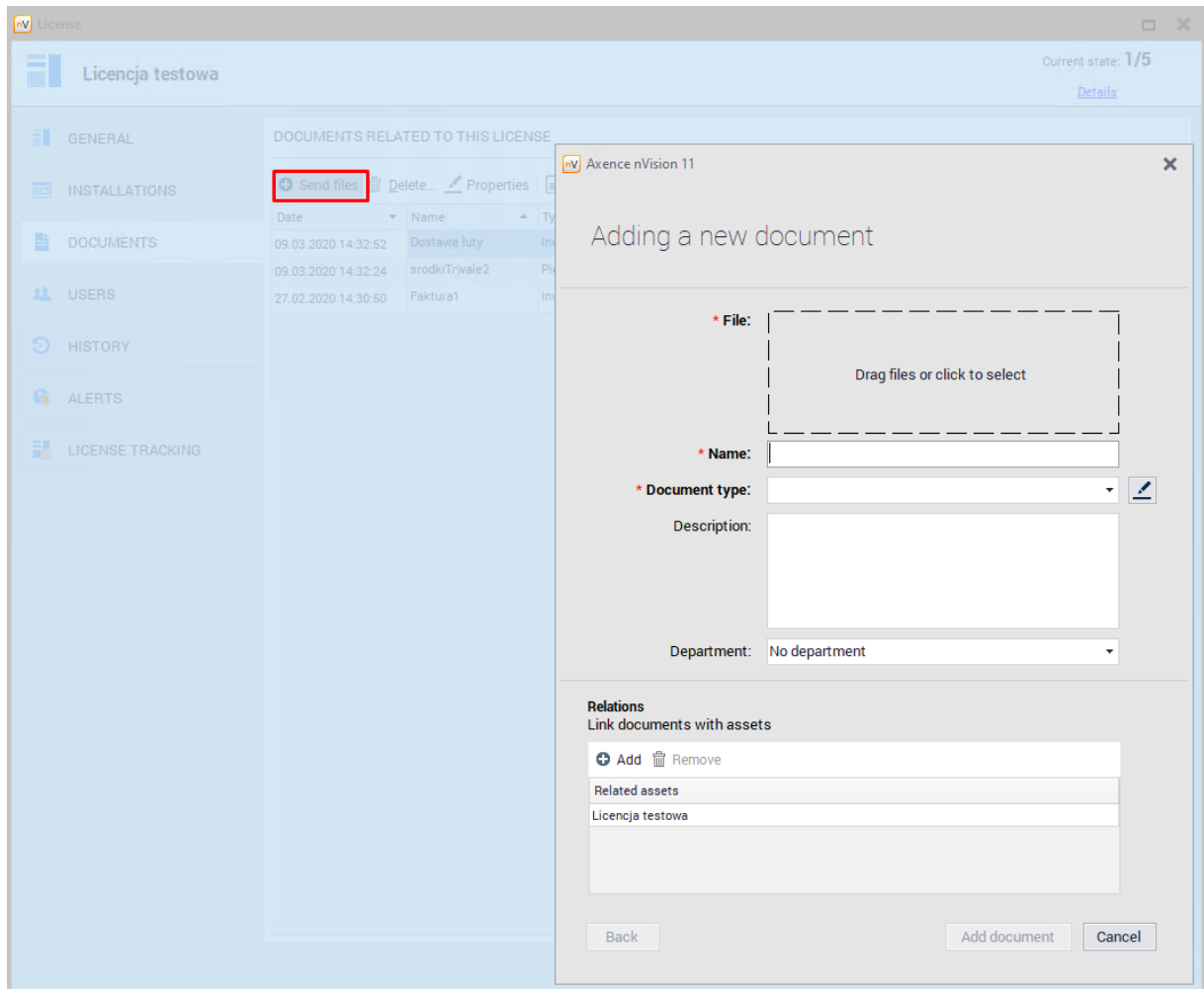
Send files Delete... Properties Open Save... Add relation Remove relation... Filter

| Date | Name | Type | File name | Extension | File size | Description | Asset name |
|---------------------|---------------|---------|--------------|-----------|-----------|-------------|------------------|
| 09.03.2020 14:32:52 | Dostawa luty | Invoice | dev_liczn... | PNG | 53 kB | | Licencja testowa |
| 09.03.2020 14:32:24 | srodkiTrwale2 | Picture | srodkiTr... | PNG | 8 kB | | Licencja testowa |
| 27.02.2020 14:30:50 | Faktura1 | Invoice | text.pdf | PDF | 11 kB | | Licencja testowa |

Close

Adding new document

To add a new document, select **Send files** button. A new window will be displayed to add a new document:



Displayed window has two sections: information section and section with document relations with assets.

Document Information

All required fields are marked with ' * '.

- File - select or drag & drop file here,
- Name - document name visible in nVision,
- Document Type - select from available positions on the list - adding new document types has been described in [separate topic](#).^[210]
- Description - add-on description fields
- Department - add-on fields for department selection

Relations

To link the document with license, click **Add** button and select license from the list.

8.5.3.5.4 Assigned users

The **Users** tab in the **License Properties** window allows you to add and remove relationships between the selected license and users.

Users assigned to the selected license will be listed in the table:

Licencja testowa

Current state: 1/5

[Details](#)

GENERAL

INSTALLATIONS

DOCUMENTS

USERS

HISTORY

ALERTS

LICENSE TRACKING

USERS ASSIGNED TO THIS LICENSE

[Add relation](#) [Remove relation](#) [Properties](#) Filter

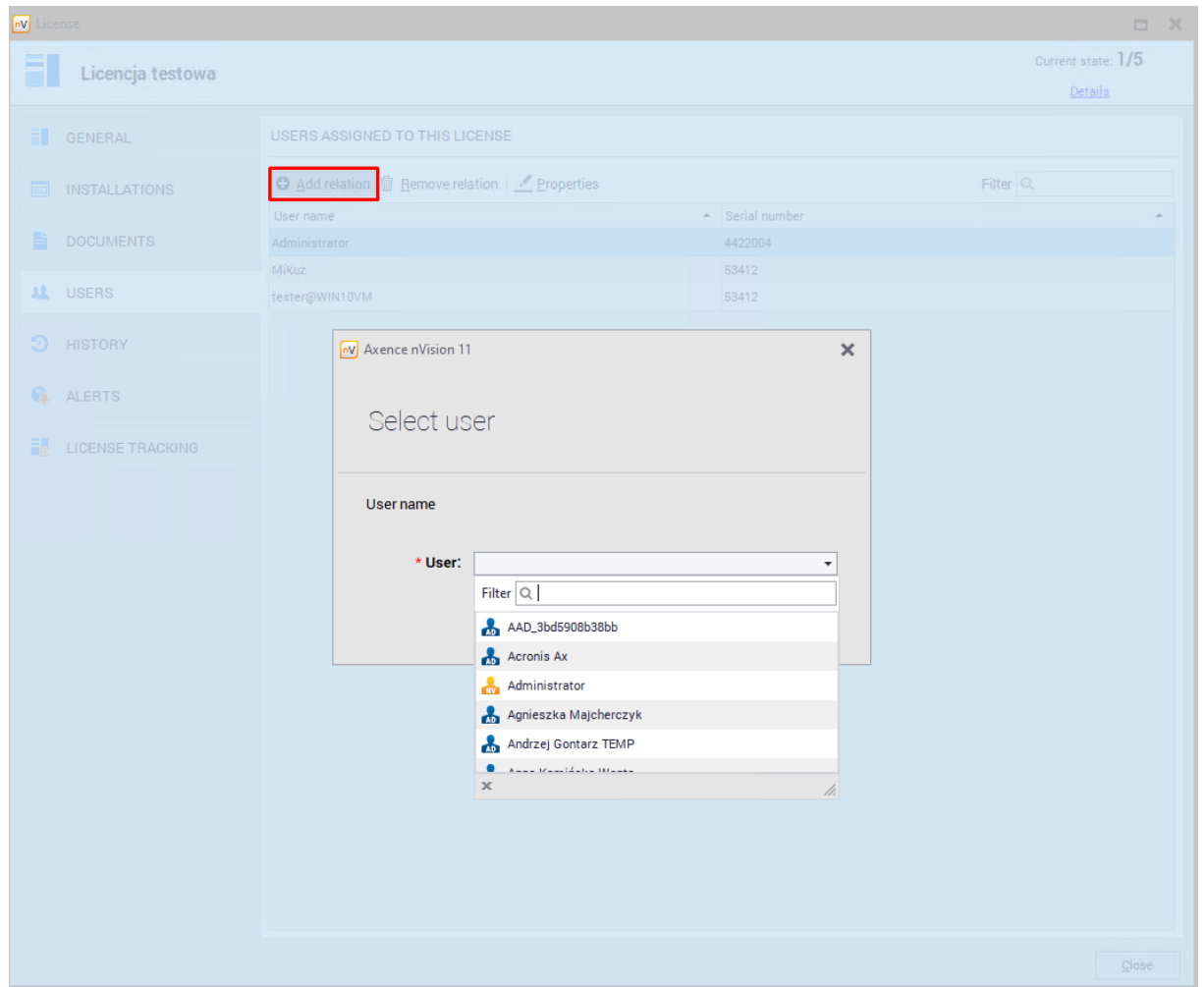
| User name | Serial number |
|----------------|---------------|
| Administrator | 4422004 |
| Mikuz | 53412 |
| tester@WIN10VM | 53412 |

[Close](#)

User assignment is crucial when the application is licensed for a selected number of users. More information about license accounting configuration is described in [licensing methods](#) ²⁹⁰ chapter.

Adding relation

To add relation with user, click **Add relation**. A window with user selection will be displayed:



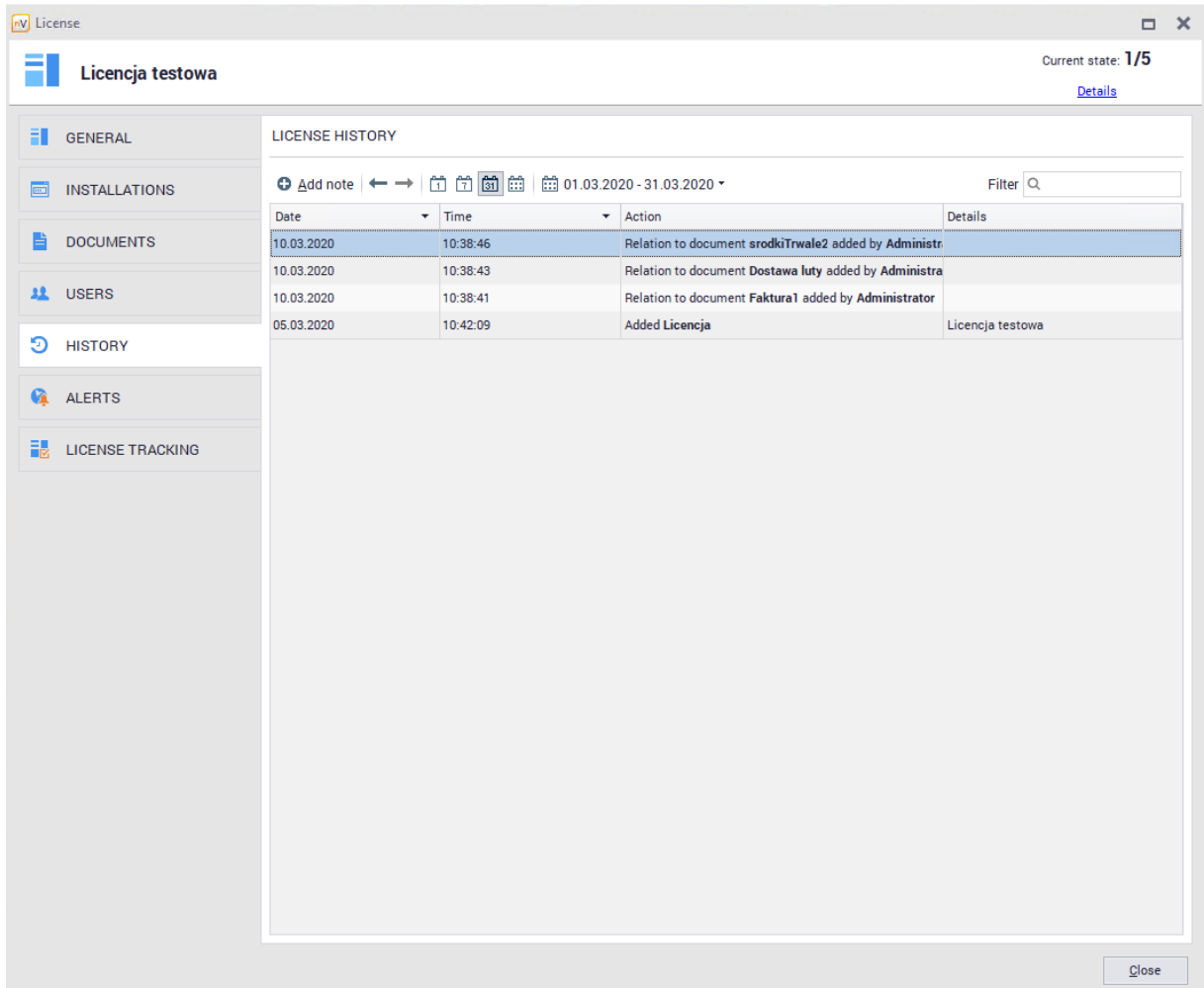
Once you select User, confirm choice by clicking **Add relation** button.

Removing relation

To remove the relation with the user, select relation from list and confirm choice by clicking **Delete relation** button.

8.5.3.5.5 History

License History feature allows you to collect information about license modifications. To view the history, select the **History** tab visible in the **License properties** window:



Licencja testowa Current state: 1/5 [Details](#)

LICENSE HISTORY

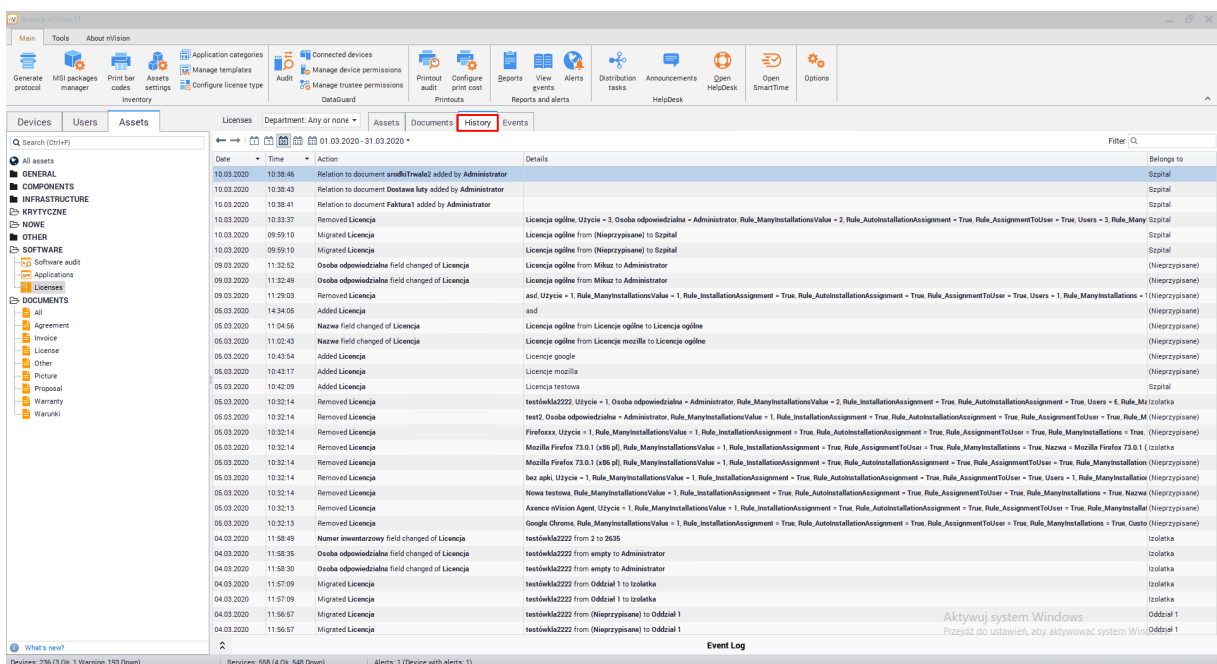
01.03.2020 - 31.03.2020

| Date | Time | Action | Details |
|------------|----------|---|------------------|
| 10.03.2020 | 10:38:46 | Relation to document srodkiTrwale2 added by Administrator | |
| 10.03.2020 | 10:38:43 | Relation to document Dostawa luty added by Administrator | |
| 10.03.2020 | 10:38:41 | Relation to document Faktura1 added by Administrator | |
| 05.03.2020 | 10:42:09 | Added Licencja | Licencja testowa |

[Close](#)

All licenses history

To access the history of all licenses, select the **Assets** tab in the main program window, and then scroll down for **Licenses** in the **Software** section. The **History** tab will appear above the license list:



Assets | Licenses | Department: Any or none | Assets | Documents | **History** | Events

| Date | Time | Action | Details | Belongs to |
|------------|----------|---|---|----------------|
| 10.03.2020 | 10:38:46 | Relation to document srodkiTrwale2 added by Administrator | | Szpital |
| 10.03.2020 | 10:38:43 | Relation to document Dostawa luty added by Administrator | | Szpital |
| 10.03.2020 | 10:38:41 | Relation to document Faktura1 added by Administrator | | Szpital |
| 10.03.2020 | 10:33:37 | Removed Licencja | Licencja ogólna. Użycie = 3. Osoba odpowiedzialna = Administrator. Rule_ManyInstallationsValue = 2. Rule_AutoInstallationAssignment = True. Rule_AssignmentToUser = True. Users = 3. Rule_Many | Szpital |
| 10.03.2020 | 09:59:10 | Migrated Licencja | Licencja ogólna from (Nieprzyznane) to Szpital | Szpital |
| 10.03.2020 | 09:59:10 | Migrated Licencja | Licencja ogólna from (Nieprzyznane) to Szpital | Szpital |
| 09.03.2020 | 11:32:52 | Osoba odpowiedzialna Field changed of Licencja | Licencja ogólna from Mikuz to Administrator | (Nieprzyznane) |
| 09.03.2020 | 11:32:49 | Osoba odpowiedzialna Field changed of Licencja | Licencja ogólna from Mikuz to Administrator | (Nieprzyznane) |
| 09.03.2020 | 11:29:03 | Removed Licencja | asd. Użycie = 1. Rule_ManyInstallationsValue = 1. Rule_InstallationAssignment = True. Rule_AutoInstallationAssignment = True. Rule_AssignmentToUser = True. Users = 1. Rule_ManyInstallations = 1 | (Nieprzyznane) |
| 08.03.2020 | 14:34:05 | Added Licencja | asd | (Nieprzyznane) |
| 06.03.2020 | 11:04:56 | Nazwa Field changed of Licencja | Licencja ogólna from Licencja ogólna to Licencja ogólna | (Nieprzyznane) |
| 06.03.2020 | 11:02:43 | Nazwa Field changed of Licencja | Licencja ogólna from Licencja mozilla to Licencja ogólna | (Nieprzyznane) |
| 06.03.2020 | 10:43:54 | Added Licencja | Licencja google | (Nieprzyznane) |
| 06.03.2020 | 10:43:17 | Added Licencja | Licencja mozilla | (Nieprzyznane) |
| 06.03.2020 | 10:42:09 | Added Licencja | Licencja testowa | Szpital |
| 05.03.2020 | 10:32:14 | Removed Licencja | testówk2222. Użycie = 1. Osoba odpowiedzialna = Administrator. Rule_ManyInstallationsValue = 2. Rule_InstallationAssignment = True. Rule_AutoInstallationAssignment = True. Users = 6. Rule_M | izolanka |
| 05.03.2020 | 10:32:14 | Removed Licencja | test2. Osoba odpowiedzialna = Administrator. Rule_ManyInstallationsValue = 1. Rule_InstallationAssignment = True. Rule_AutoInstallationAssignment = True. Rule_AssignmentToUser = True. Rule_M | (Nieprzyznane) |
| 05.03.2020 | 10:32:14 | Removed Licencja | Firefox. Użycie = 1. Rule_ManyInstallationsValue = 1. Rule_InstallationAssignment = True. Rule_AutoInstallationAssignment = True. Rule_AssignmentToUser = True. Rule_ManyInstallations = True | (Nieprzyznane) |
| 05.03.2020 | 10:32:14 | Removed Licencja | Mozilla Firefox 73.0.1 (x86.pl). Rule_ManyInstallationsValue = 1. Rule_InstallationAssignment = True. Rule_AssignmentToUser = True. Rule_ManyInstallations = True. Nazwa = Mozilla Firefox 73.0.1 | izolanka |
| 05.03.2020 | 10:32:14 | Removed Licencja | Mozilla Firefox 73.0.1 (x86.pl). Rule_ManyInstallationsValue = 1. Rule_InstallationAssignment = True. Rule_AutoInstallationAssignment = True. Rule_AssignmentToUser = True. Rule_ManyInstallations = True | (Nieprzyznane) |
| 05.03.2020 | 10:32:14 | Removed Licencja | bez apki. Użycie = 1. Rule_ManyInstallationsValue = 1. Rule_InstallationAssignment = True. Rule_AutoInstallationAssignment = True. Rule_AssignmentToUser = True. Users = 1. Rule_ManyInstallations | (Nieprzyznane) |
| 05.03.2020 | 10:32:14 | Removed Licencja | Nowa testowa. Rule_ManyInstallationsValue = 1. Rule_InstallationAssignment = True. Rule_AutoInstallationAssignment = True. Rule_AssignmentToUser = True. Rule_ManyInstallations = True. Nazwa | (Nieprzyznane) |
| 05.03.2020 | 10:32:13 | Removed Licencja | Agence nVision Agent. Użycie = 1. Rule_ManyInstallationsValue = 1. Rule_InstallationAssignment = True. Rule_AutoInstallationAssignment = True. Rule_AssignmentToUser = True. Rule_ManyInstallations | (Nieprzyznane) |
| 05.03.2020 | 10:32:13 | Removed Licencja | Google Chrome. Rule_ManyInstallationsValue = 1. Rule_InstallationAssignment = True. Rule_AutoInstallationAssignment = True. Rule_AssignmentToUser = True. Rule_ManyInstallations = True. Custo | (Nieprzyznane) |
| 04.03.2020 | 11:38:49 | Numer inwentarzewy Field changed of Licencja | testówk2222 from 2 to 2635 | izolanka |
| 04.03.2020 | 11:38:35 | Osoba odpowiedzialna Field changed of Licencja | testówk2222 from empty to Administrator | izolanka |
| 04.03.2020 | 11:38:30 | Osoba odpowiedzialna Field changed of Licencja | testówk2222 from empty to Administrator | izolanka |
| 04.03.2020 | 11:37:09 | Migrated Licencja | testówk2222 from Oddział 1 to izolanka | izolanka |
| 04.03.2020 | 11:37:09 | Migrated Licencja | testówk2222 from Oddział 1 to izolanka | izolanka |
| 04.03.2020 | 11:36:57 | Migrated Licencja | testówk2222 from (Nieprzyznane) to Oddział 1 | Oddział 1 |
| 04.03.2020 | 11:36:57 | Migrated Licencja | testówk2222 from (Nieprzyznane) to Oddział 1 | Oddział 1 |

Aktywuj system Windows
Przejdź do ustawień, aby aktywować system Windows

Event Log

History of individual licenses on the workstation

In nVision 13.5, the ability to track the license history on individual workstations has been added.

To view the license history on a workstation:

- Select the **Software** tab in the settings window of the selected device.
- Click on the **License history** tab. This tab displays information on the licenses assigned to the software installed on a given device. The list can be sorted by the appropriate parameter, select the period for which information will be displayed, or filter the data using the search engine. The data is presented in the form of a table.

The following parameters are displayed in the table:

- Date
- Time
- Action, e.g. Manually assigned a license to an installation / Automatically assigned a license to an installation / Withdrawal of a license to an installation
- Details, e.g. data about the device on which the application using the given license is installed
- Belongs to - data of the user who uses the license (the field may be blank, then information is displayed that the license is not assigned to a specific user)

Zakładka **Historia licencji** pozwala również na szybkie przejście do okna konfiguracji licencji, która jest używana na danej stacji roboczej. Aby wyświetlić okno informacji licencji, należy dwukrotnie kliknąć w odpowiedni zapis (rzad) w tabeli.

Zakładka Historia licencji pozwala również na szybkie przejście do okna konfiguracji licencji, która jest używana na danej stacji roboczej. Aby wyświetlić okno informacji licencji, należy dwukrotnie kliknąć w odpowiedni zapis (rzad) w tabeli.

8.5.3.5.6 Alerts

License alerts feature, which is located inside **License properties** tab can be created for individual licenses or for a group of licenses. Alerts allow to configure notification for the Administrator when certain conditions are met.

Alerts for selected license

To create alert for selected asset type:

1. Open the resource editing window, go to the **Alerts** tab.
2. Click **Add** button, then select **Add alert for this license**.
3. In the **Alert rules configuration window** select event(field) for which you want to create the alert and set the date the alert is to be created. Enter alert description and click **OK**. Optionally you can also set the e-mail to get reminder messages.

Alert for asset

Configure alert for Kość 1 asset

Use this window to configure alert condition and description.

Configuration

Alert date: 28.03.2020

Description:

Send the message to this e-mail address: [E-mail sending settings](#)

E-mail address

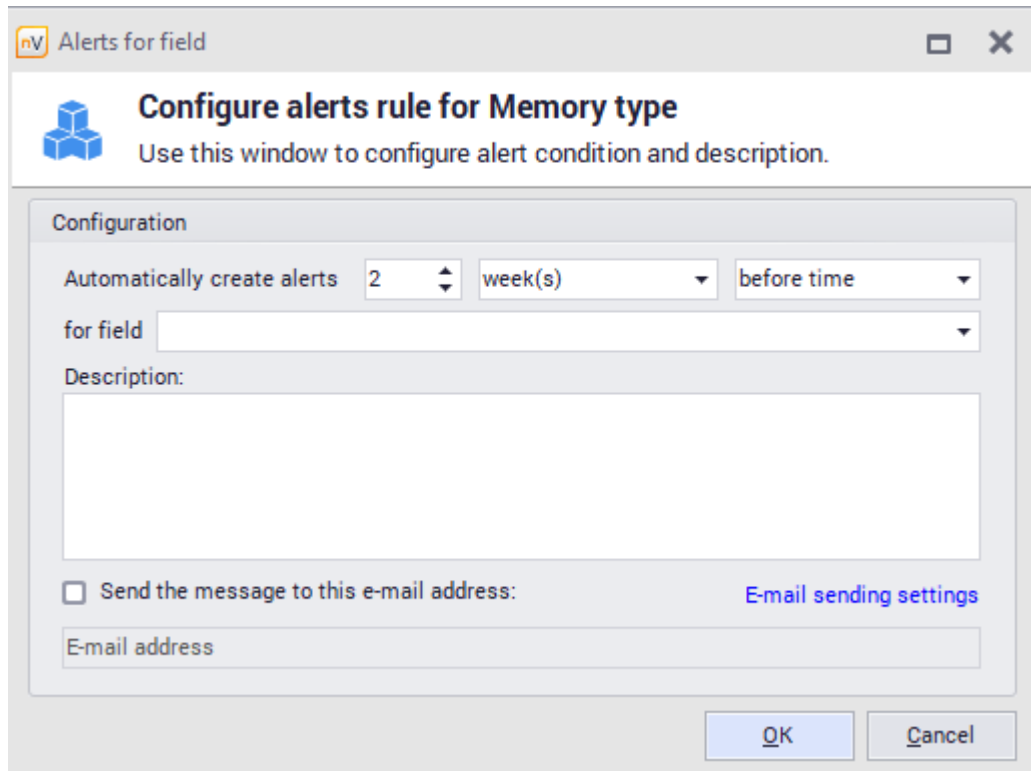
OK Cancel

A different method of adding alerts for selected asset types is described in [asset types](#)^[200] chapter.

Alerts for all licenses

To create alert for all licenses:

4. Open the resource editing window, go to the **Alerts tab**.
5. Click **Add** button, then select **Add alert for this license**.
6. In the **Alert rules configuration window** select event(field) for which you want to create the alert and set the date the alert is to be created. Enter alert description and click **OK**. Optionally you can also set the e-mail to get reminder messages.



To know more about alerts, see [alerting](#) ⁵⁸⁶ chapter.

8.5.3.5.7 Licensing methods

8.5.3.5.7.1 Rules

The **Rules** tab located under the **License tracking window** gives you extensive options for license accounting configuration. The configuration will affect how many licenses and how they will be downloaded.

Licencja testowa

Current state: 1/5

[Details](#)

GENERAL

INSTALLATIONS

DOCUMENTS

USERS

HISTORY

ALERTS

LICENSE TRACKING

RULES

SERIAL NUMBERS

LICENCE TRACKING RULES

Assignment to installations
Assignment to an installation will use up one license.

Assignment to users
Assignment to a user will use up one license.

Multiple installations of one user
The number of installations that when assigned to one user will use up only one license:
1

Serial number
Installations and users that have the same serial number assigned will use up only one license.

Multiple applications on one device
Installing more than one application on one device will use up only one license.

CURRENT LICENSES

Usage: 1/5 Filter

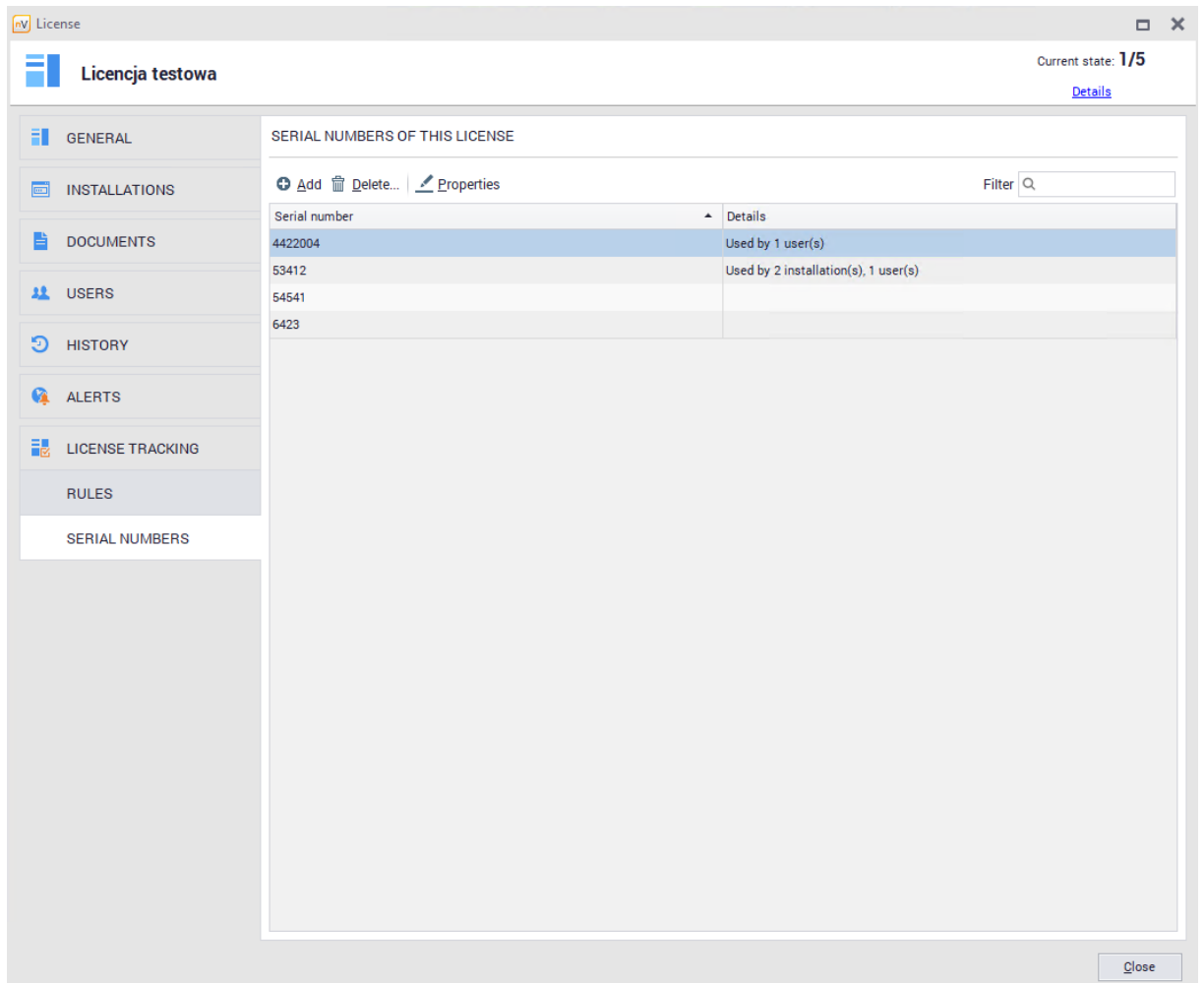
| License usage | Tracking rule | Details |
|---------------|----------------------------|--|
| 1 | Assignment to installation | 7-Zip 19.00 (x64), Version 19, Mikuz, Serial number 53412, WIN10, 192.168.69.206 |

[Close](#)

Below the licensing policy settings you can see a list of currently used licenses with description. Individual options and use cases are explained in the subsections of this chapter.

8.5.3.5.7.2 Serial numbers

Serial numbers tab allows you to define serial numbers compatible with the edited license. Serial numbers can be assigned to users using licenses or for installations assigned to licenses.

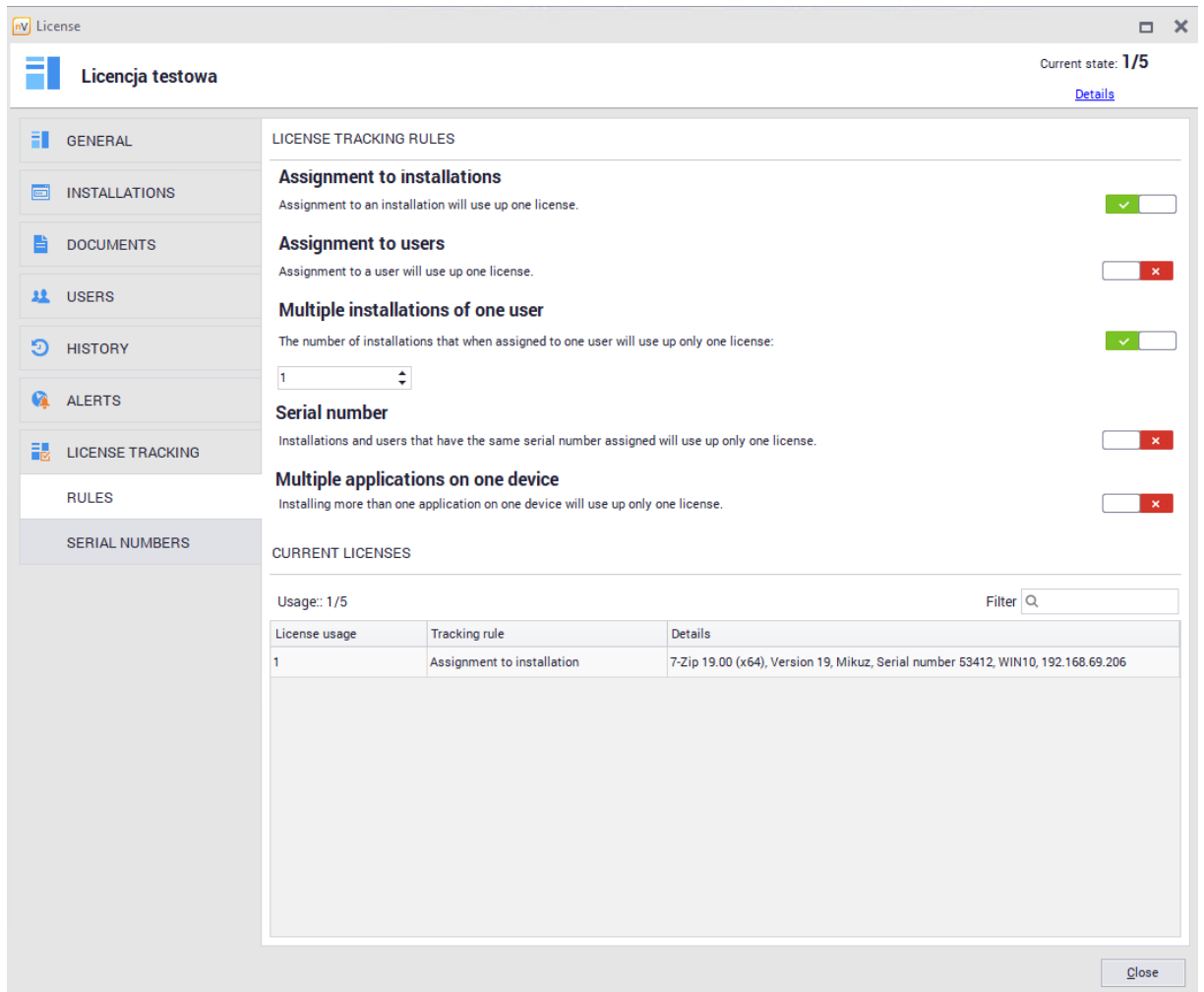


To assign a serial number to a user, go to the **Users** tab in the **License Properties** window and then indicate the serial number by adding or editing the associated user.

To assign a serial number to the installation, go to the **Installations** tab in the **License Properties** window, then select an item from the list and click the **Assign Serial Number** button.

8.5.3.5.7.3 License accounting methods

The **License tracking** tab in the **License properties** window gives you extensive options for configuring the license accounting method. The configuration will affect how many licenses and how they will be downloaded.



Licencja testowa Current state: 1/5 [Details](#)

LICENCE TRACKING RULES

- Assignment to installations**
Assignment to an installation will use up one license.
- Assignment to users**
Assignment to a user will use up one license.
- Multiple installations of one user**
The number of installations that when assigned to one user will use up only one license:
1
- Serial number**
Installations and users that have the same serial number assigned will use up only one license.
- Multiple applications on one device**
Installing more than one application on one device will use up only one license.

CURRENT LICENSES

Usage: 1/5 Filter

| License usage | Tracking rule | Details |
|---------------|----------------------------|--|
| 1 | Assignment to installation | 7-Zip 19.00 (x64), Version 19, Mikuz, Serial number 53412, WIN10, 192.168.69.206 |

License can be accounted either to an installation or user:

- **Assignment to installation**

Turning this option on will affect the installation of the application being associated with the license is detected on the host and assigned to the license (automatically or manually). Then one license from pre-defined pool in the license properties will be used.

Licencja testowa Current state: **2/5**
[Details](#)

LICENSE TRACKING RULES

Assignment to installations
Assignment to an installation will use up one license.

Assignment to users
Assignment to a user will use up one license.

Multiple installations of one user
The number of installations that when assigned to one user will use up only one license:
1

Serial number
Installations and users that have the same serial number assigned will use up only one license.

Multiple applications on one device
Installing more than one application on one device will use up only one license.

CURRENT LICENSES

Usage: 2/5 Filter

| License usage | Tracking rule | Details |
|---------------|----------------------------|--|
| 1 | Assignment to installation | 7-Zip 19.00 (x64), Version 19, Mikuz, Serial number 53412, WIN10, 192.168.69.206 |
| 2 | Assignment to installation | Mozilla Firefox 73.0.1 (x86 pl), Version 73, Mikuz, WIN10, 192.168.69.206 |

- **Assignment to user**

Turning this option on means, that [user assignment to license](#)²⁸⁴ will result in using one license from the pool of specified licenses

Licencja testowa Current state: **3/5**
[Details](#)

LICENSE TRACKING RULES

Assignment to installations
Assignment to an installation will use up one license.

Assignment to users
Assignment to a user will use up one license.

Multiple installations of one user
The number of installations that when assigned to one user will use up only one license:
1

Serial number
Installations and users that have the same serial number assigned will use up only one license.

Multiple applications on one device
Installing more than one application on one device will use up only one license.

CURRENT LICENSES

Usage: 3/5 Filter

| License usage | Tracking rule | Details |
|---------------|--------------------|--------------------------------------|
| 1 | Assignment to user | Administrator, Serial number 4422004 |
| 2 | Assignment to user | Mikuz, Serial number 53412 |
| 3 | Assignment to user | tester@WIN10VM, Serial number 53412 |

See the following chapters for more information about other license accounting possibilities

8.5.3.5.7.4 Multiple user installations

Modification of described settings can be found in the **License tracking** tab in the **License properties** window. The following configuration allows you to configure the license in such a way that several installations assigned to the same user will result in the use of one license from the pool specified in the license properties.

To assign a user to an installation, use the **Installations** tab in the **License Properties** window. After double-clicking the selected item, assign the selected person to the installation:

Axence nVision 11

Installation

INSTALLATION

Name: 7-Zip 19.00 (x64) User: Mikuz

Type: Application License: Licencja testowa

Category: Default Serial number: 53412

Descriptor:

Company: Igor Pavlov

Version: 19

Audited: Yes (default)

REGISTRY

| Name | Version | Company | Path |
|-------------------|---------|-------------|-------------------------|
| 7-Zip 19.00 (x64) | 19.00 | Igor Pavlov | C:\Program Files\7-Zip\ |

FILES

| File name | Version | Company | Product name | Original file name | Path |
|---------------|---------|-------------|--------------|--------------------|-------------------------|
| 7zG.exe | 19.00 | Igor Pavlov | 7-Zip | 7zg.exe | C:\Program Files\7-Zip\ |
| 7z.exe | 19.00 | Igor Pavlov | 7-Zip | 7z.exe | C:\Program Files\7-Zip\ |
| Uninstall.exe | 19.00 | Igor Pavlov | 7-Zip | Uninstall.exe | C:\Program Files\7-Zip\ |

Close

Example: applications assigned to user Mikuz:

License

Licencja testowa

Current state: 2/5

Details

GENERAL

INSTALLATIONS USING THIS LICENSE

Automatic license assignment

Assign this license automatically to all new installations detected in the same department

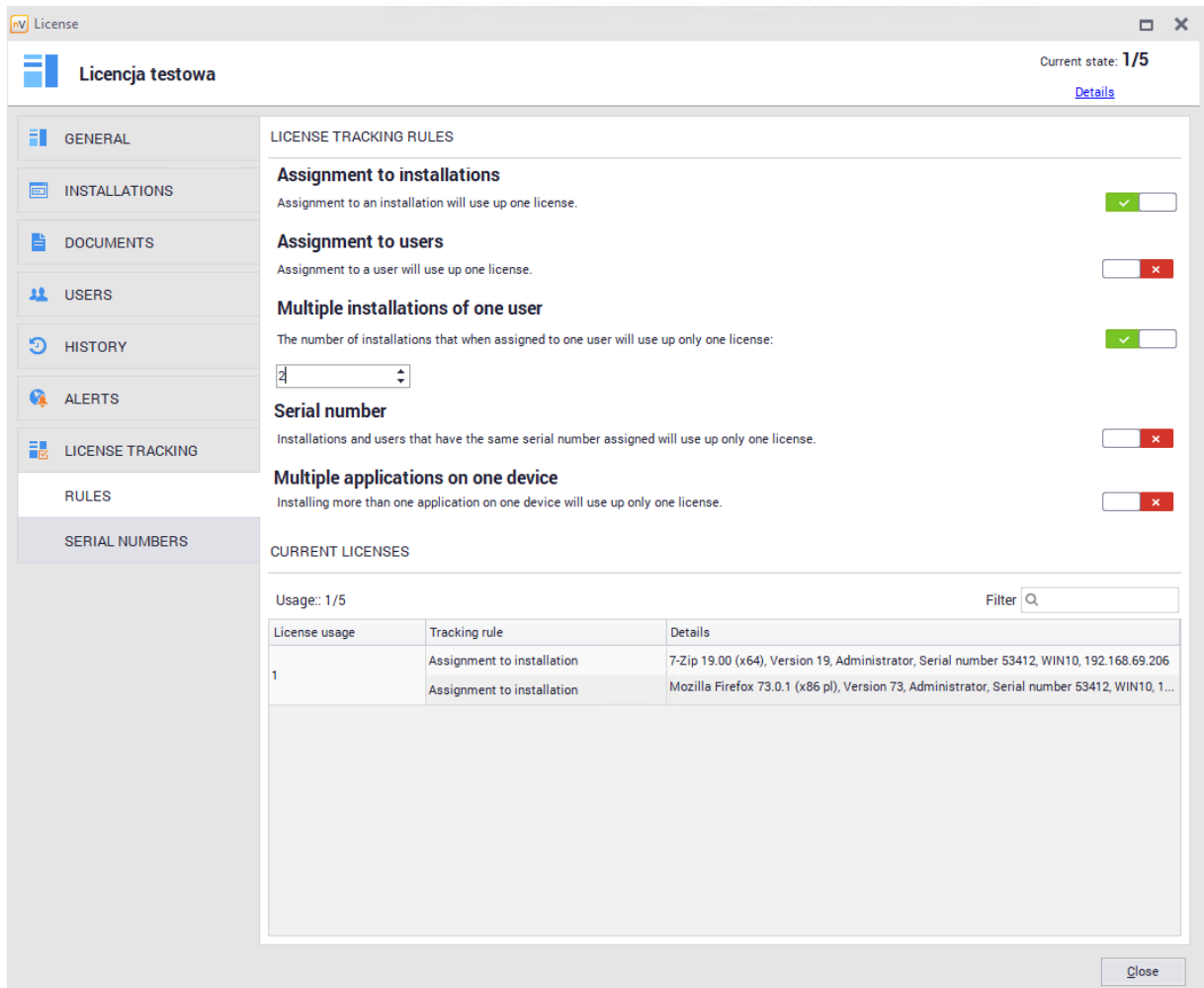
Assign installation Unassign installation Installation properties Assign serial number Unassign serial number

| Device | Installed | Name | Ver | Company | MSI Installer | User | Serial number |
|-----------------------|------------|----------------------------|-----|------------|------------------|-------|---------------|
| Audited applications | | | | | | | |
| WIN10, 192.168.69.206 | 03.02.2020 | 7-Zip 19.00 (x64) | 19 | Igor Pa... | Waiting for data | Mikuz | 53412 |
| WIN10, 192.168.69.206 | 19.02.2020 | Mozilla Firefox 73.0.1 ... | 73 | Mozilla | Waiting for data | Mikuz | 4422004 |

Close

Aktywul System

License Tracking / Rules tab shows active options for **assigning to installation** and multiple (in this case, 2) single user installations. For this purpose, 2 licenses are used from the pool:



Changing the number of installations assigned to single user, to 3rd one only one license will be used:

8.5.3.5.7.5 Serial numbers assignment

Modification of described settings can be found in the **License tracking** tab in the **License properties** window.

The following configuration allows you to configure the licenses to use only **one license** from the selected pool in license properties for the **installations and users with the same serial number**.

Defining and assigning serial numbers has been described in [serial numbers](#) ²⁹¹ chapter.

To assign a serial number to user, use the Installations tab in the **License Properties** window. After double-clicking the selected item, assign the selected person to the installation:

License

Licencja testowa

Current state: 3/5

Details

GENERAL

INSTALLATIONS

DOCUMENTS

USERS

HISTORY

ALERTS

LICENSE TRACKING

INSTALLATIONS USING THIS LICENSE

Automatic license assignment

Assign this license automatically to all new installations detected in the same department:

Assign installation Unassign installation Installation properties Assign serial number Unassign serial number

| Device | Installed | Name | Vers | Company | MSI Installer | User | Serial number |
|-----------------------|------------|----------------------------|------|------------|---------------|---------------|---------------|
| Audited applications | | | | | | | |
| WIN10, 192.168.69.206 | 03.02.2020 | 7-Zip 19.00 (x64) | 19 | Igor Pa... | Not supported | Administrator | 53412 |
| WIN10, 192.168.69.206 | 19.02.2020 | Mozilla Firefox 73.0.1 ... | 73 | Mozilla | Not supported | Administrator | 53412 |

Close

To assign a serial number to installation, go to **Installations** tab, selected item and click **Assign serial number**. **License Tracking / Rules** tab allows you to set rules for:

- installations with assigned same serial number

License

Licencja testowa

Current state: 1/5

[Details](#)

GENERAL

INSTALLATIONS

DOCUMENTS

USERS

HISTORY

ALERTS

LICENSE TRACKING

RULES

SERIAL NUMBERS

LICENSE TRACKING RULES

Assignment to installations
Assignment to an installation will use up one license.

Assignment to users
Assignment to a user will use up one license.

Multiple installations of one user
The number of installations that when assigned to one user will use up only one license:

Serial number
Installations and users that have the same serial number assigned will use up only one license.

Multiple applications on one device
Installing more than one application on one device will use up only one license.

CURRENT LICENSES

Usage: 1/5

| License usage | Tracking rule | Details |
|---------------|----------------------------|--|
| 1 | Assignment to installation | 7-Zip 19.00 (x64), Version 19, Administrator, Serial number 53412, WIN10, 192.168.69.206 |
| | Assignment to installation | Mozilla Firefox 73.0.1 (x86 pl), Version 73, Administrator, Serial number 53412, WIN10, 192.168.69.206 |

Close

- license users with assigned same serial number

Licencja testowa

Current state: 2/5

[Details](#)

GENERAL

INSTALLATIONS

DOCUMENTS

USERS

HISTORY

ALERTS

LICENSE TRACKING

RULES

SERIAL NUMBERS

LICENCE TRACKING RULES

Assignment to installations
Assignment to an installation will use up one license.

Assignment to users
Assignment to a user will use up one license.

Multiple installations of one user
The number of installations that when assigned to one user will use up only one license: 2

Serial number
Installations and users that have the same serial number assigned will use up only one license.

Multiple applications on one device
Installing more than one application on one device will use up only one license.

CURRENT LICENSES

Usage: 2/5

| License usage | Tracking rule | Details |
|---------------|--------------------|--------------------------------------|
| 1 | Assignment to user | Administrator, Serial number 4422004 |
| 2 | Assignment to user | tester@WIN10VM, Serial number 53412 |

[Close](#)

- installations and license users with assigned same serial numbers

License

Licencja testowa Current state: 2/5 [Details](#)

GENERAL

INSTALLATIONS

DOCUMENTS

USERS

HISTORY

ALERTS

LICENSE TRACKING

RULES

SERIAL NUMBERS

LICENSE TRACKING RULES

Assignment to installations
Assignment to an installation will use up one license.

Assignment to users
Assignment to a user will use up one license.

Multiple installations of one user
The number of installations that when assigned to one user will use up only one license:

Serial number
Installations and users that have the same serial number assigned will use up only one license.

Multiple applications on one device
Installing more than one application on one device will use up only one license.

CURRENT LICENSES

Usage: 2/5 Filter

| License usage | Tracking rule | Details |
|---------------|----------------------------|--|
| 1 | Assignment to installation | 7-Zip 19.00 (x64), Version 19, Administrator, Serial number 53412, WIN10, 192.168.69.206 |
| | Assignment to installation | Mozilla Firefox 73.0.1 (x86 pl), Version 73, Administrator, Serial number 53412, WIN10, 192.168.69.206 |
| | Assignment to user | Mikuz, Serial number 53412 |
| | Assignment to user | tester@WIN10VM, Serial number 53412 |
| 2 | Assignment to user | Administrator, Serial number 4422004 |

8.5.3.5.7.6 Multiple applications on device

Modification of described settings can be found in the **License tracking** tab in the **License properties** window. The following configuration allows you to configure the licenses to use only one license from the selected pool in license properties **for many installations of different applications (associated with the license)** within one device.

Related applications are shown in the **License Properties / General window**

License Tracking / Rules tab allows you need to enable **Assignment to installations** and **Multiple applications on one device** options. Linked applications installed within same device will use one license only:

License

Licencja testowa

Current state: 1/5

[Details](#)

GENERAL

INSTALLATIONS

DOCUMENTS

USERS

HISTORY

ALERTS

LICENSE TRACKING

RULES

SERIAL NUMBERS

LICENSE TRACKING RULES

Assignment to installations

Assignment to an installation will use up one license.

Assignment to users

Assignment to a user will use up one license.

Multiple installations of one user

The number of installations that when assigned to one user will use up only one license:

2

Serial number

Installations and users that have the same serial number assigned will use up only one license.

Multiple applications on one device

Installing more than one application on one device will use up only one license.

CURRENT LICENSES

Usage: 1/5

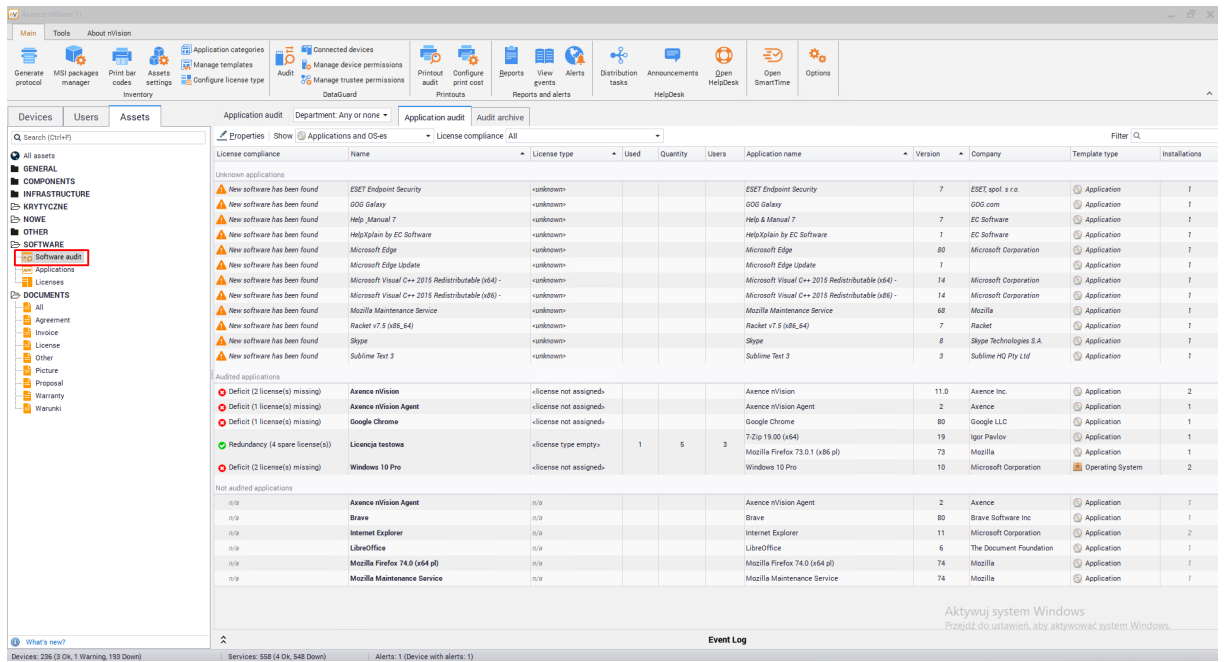
Filter

| License usage | Tracking rule | Details |
|---------------|----------------------------|--|
| 1 | Assignment to installation | 7-Zip 19.00 (x64), Version 19, Administrator, Serial number 53412, WIN10, 192.168.69.206 |
| | Assignment to installation | Mozilla Firefox 73.0.1 (x86 pl), Version 73, Administrator, Serial number 53412, WIN10, 192.168.69.206 |

Close

8.5.4 Software audit

To go to the **software audit**, enter **Assets** tab visible in the main program window, then scroll for **Software audit** in the **Software** section:

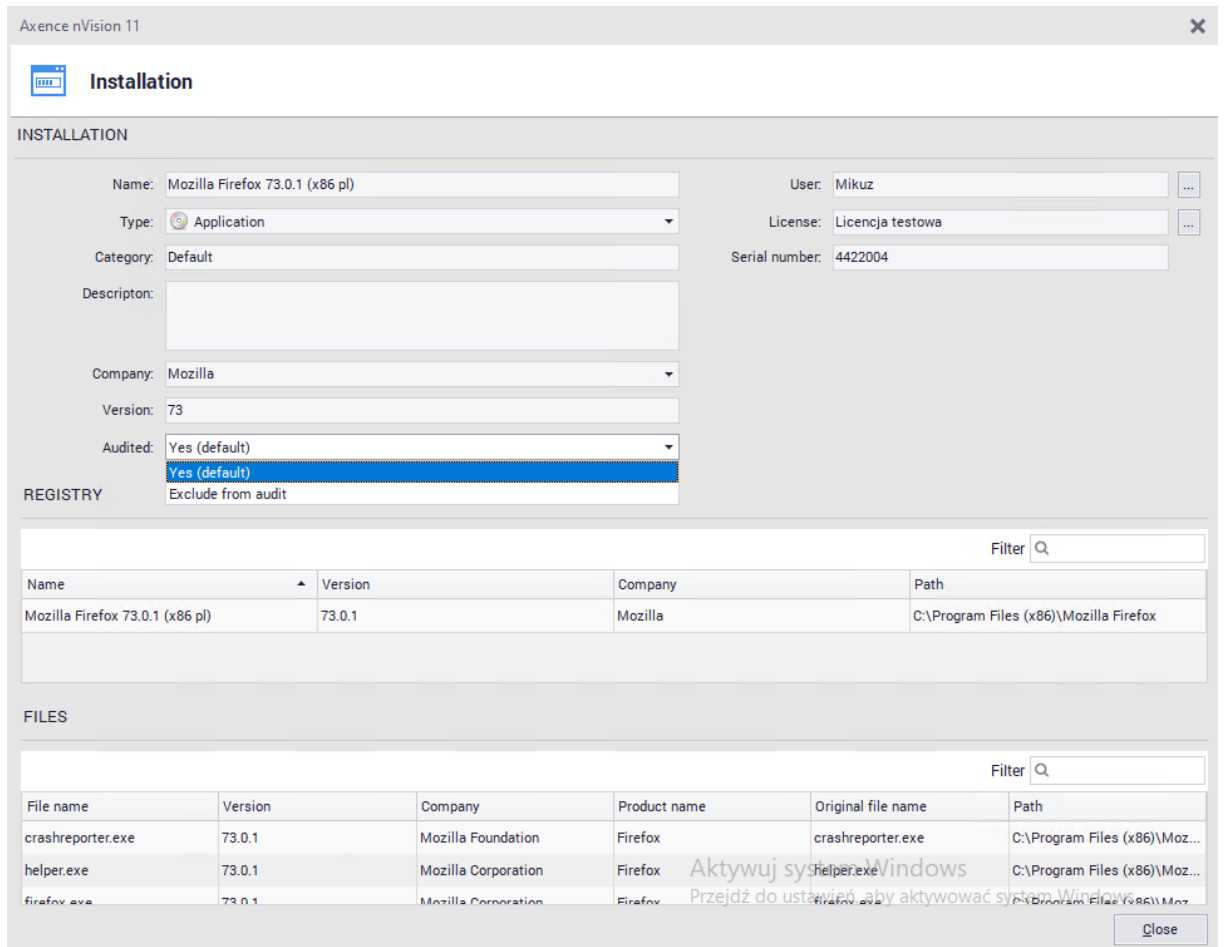


The **Software Inventory Audit** window contains a list of applications detected on the monitored computers. If the programs are recognized, the type of license and the number of licenses held appears in comparison with the number of licenses used (Installations column), i.e. the number of workstations on which a given application is installed and associated with a given license.

Devices with installed applications and licenses

Select an item from the list and go to its properties to view the application properties.

In the **Installations** tab you can view the devices where the application is installed. If the application is audited, it is possible to exclude its selected installation from the audit. - simply change the value of the **Audited** field in the **installation properties** window:



In the **License** tab, you can add, remove and edit licenses for each application. More information is described in [users and licenses](#) ²⁶⁶ chapter.

Audit archive


You can view the changes in the installed software for the selected period.

8.6 Data import

8.6.1 Data import from CSV

You can import asset data to nVision. The condition for successful data import is to place them in a csv file and divide the data so that one file contains assets of one type. You can manage these files in Asset settings / Data sources window.

To add a data file for import in nVision:

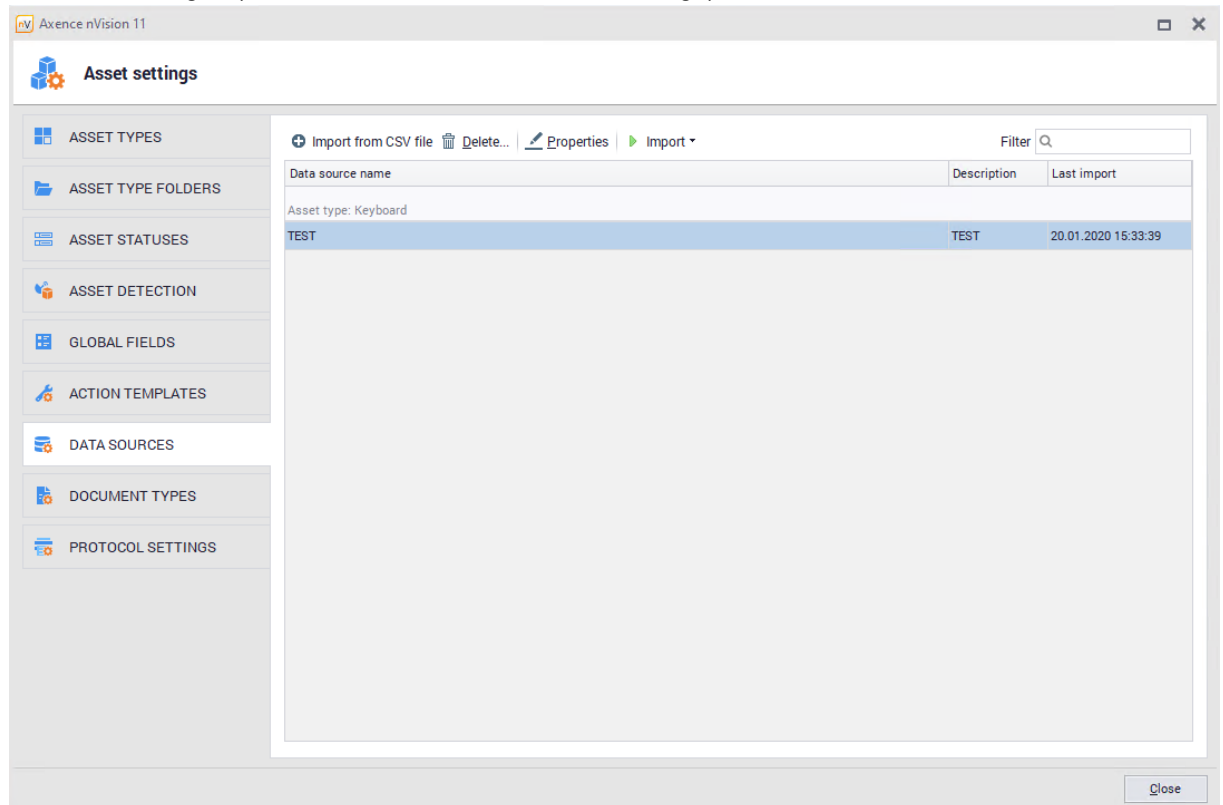
1. Select the option Assets settings from the main toolbar and then go to the Data sources tab.
2. Click the  Import from CSV file button.
3. Enter Name, data Description and Asset type to be assigned to this data.
4. In the CSV Options, indicate the path to the data file, specify the separator and the occurrence of headers. The file preview will be presented below

5. Indicate in Import configuration tab which column (or set of columns) of the source identifies the resource (is unique for a given resource).

6. Associate the CSV source columns with target field names. If necessary, go to Asset Type (by clicking Configure button) and add to it additional fields corresponding with selected columns.

7. To test the ability to import data, click Test button. then click OK.

The added file will be shown at the list of data sources. Now you can easily import data from this file eg. if its been changed (without the need to reset all the settings):



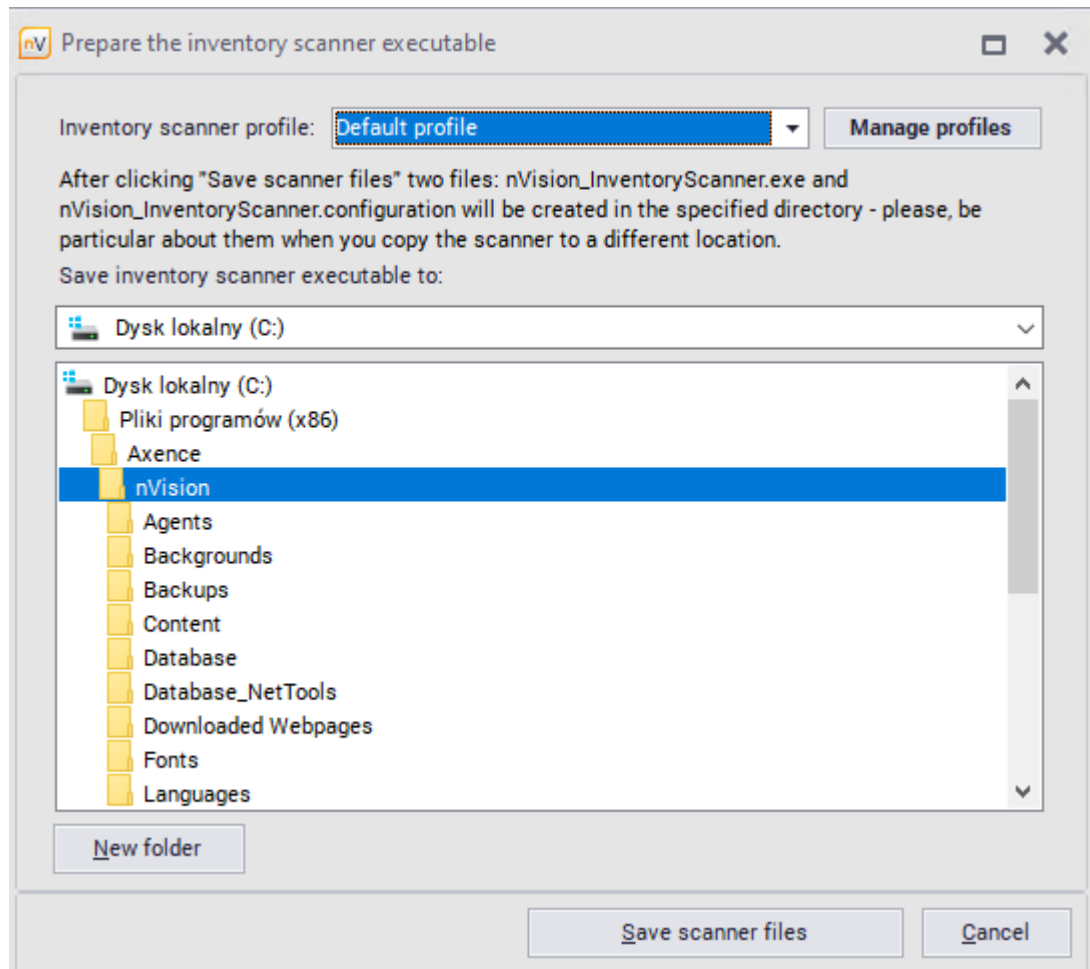
From the data source management window you can add data sources, delete them, change their properties and import data from them, as well as import data from Agents and view import logs.

8.6.2 Inventory scan import

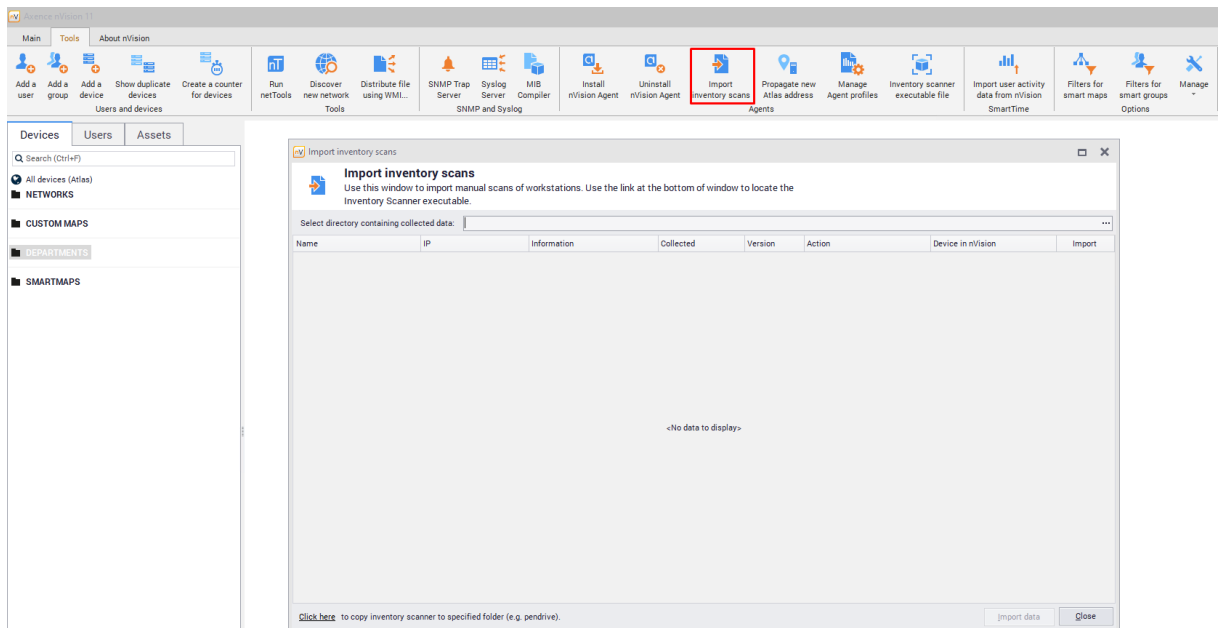
The inventory scanner is a portable tool that allows manual collection and download of device data without Agent installation. It can also be used if the scanned computer cannot be connected to the network.

To manually import inventory scans, follow these steps:

1. Prepare executable file from inventory scanner
 - a. In the Tools tab select the Inventory scanner executable option.
 - b. Select the location where the inventory scanner files are to be created (e.g. flash drive).
 - c. Set the inventory scanner profile, i.e. what information will be collected by the scanner. You can select from the list an existing profile, edit an existing profile or create a new one.
 - d. Click the Save Scanner Files button.



2. Perform inventory scan. If you copy the scanner to another location, make sure both scanner files are copied (nVision_InventoryScanner.exe and nVision_InventoryScanner.config). Run the inventory scanner executable file (nVision_InventoryScanner.exe) on the computer to be scanned to start the scanning process.
3. Data import
 - a. After scanning, copy the created folders (Data and Logs) to the location that will be visible from the nVision console.
 - b. In the window of importing inventory scans (Import inventory scans in the Tools tab) select the folder where the scans are located (i.e. the Data folder previously copied).



- c. Check, if Import field is selected for scanned device, then click Import data button.
- d. If the data import has been successfully completed, the message is shown (Import successful).

8.7 MSI Package manager

Axence nVision Agent also enables management of software installations on monitored computers through:

- Installing required company programs
- Uninstalling unauthorized programs

Software installation management is based on a repository of MSI package files. An MSI package is an object created based on an installation file with the extension MSI, which is compatible with Windows Installer (https://en.wikipedia.org/wiki/Windows_Installer). Installation packages are considered unique when the properties of the MSI file differ in terms of product code (productCode), product version (productVersion), and product language (productLanguage). The Agent's functionality also allows for installing updates but does not permit downgrading applications.

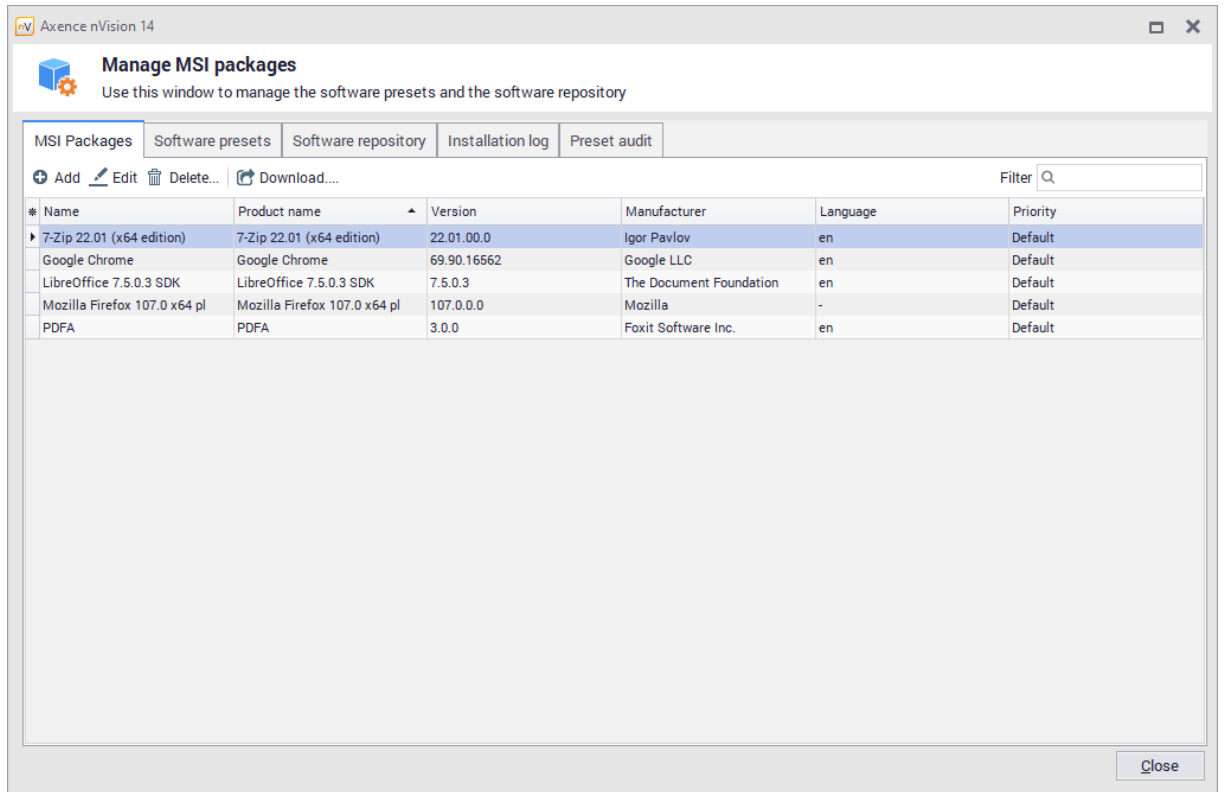
Agent Operation Scheme:

1. The Agent installs packages only after downloading all the ones configured for it, taking into account priorities specified in the package properties.
2. Agent action permits installation only if the application is either not installed at all or is installed in an older version than what the Agent received (update). The Agent periodically checks if all applications from the packages assigned to it are installed. If any are missing, it initiates a reinstallation. This process occurs independently of the option to scan information about software in the Agent's profile.

The list of applications (packages) for uninstallation is generated based on information collected by Agents through monitoring the registry entries of installed applications and reading information about installations from MSI packages. The Agent periodically checks if an application marked for removal has been installed; if detected, it proceeds with its uninstallation.

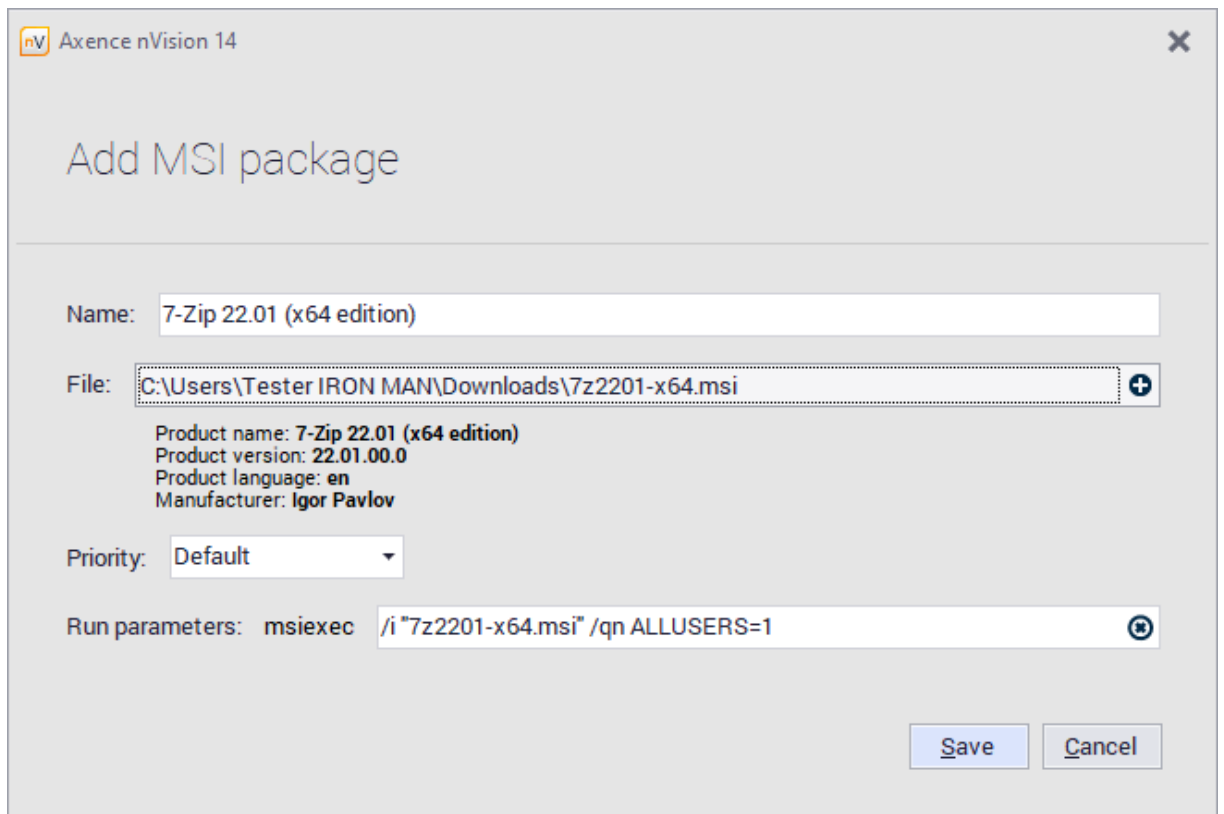
To manage MSI packages and software presets through the MSI packages manager:

1. Select "**MSI package manager**" from the main program menu.
2. In the "**Manage MSI Packages**" window, click the "**Add**" button.



3. In the dialog box, specify the MSI installer file.

4. In the package addition window, set the installation priority (considered when installing multiple packages within one group) and additional launch parameters (copied from the MSI installer's manufacturer's page). Click "Save."



NOTE! Removing launch parameters or entering incorrect launch parameters can result in the MSI package not being correctly installed on the workstation.

5. Go to the "**Software presets**" tab, click the "**Add**" button. Create a new group by specifying:

- Preset name,
- Devices on which the designated 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 through monitoring the registry entries of installed applications). Click "**Save**." The task execution status on devices is presented in the next tab of the "Manage MSI Packages" window, i.e., "**Preset audit**".

Edit software preset

Name:

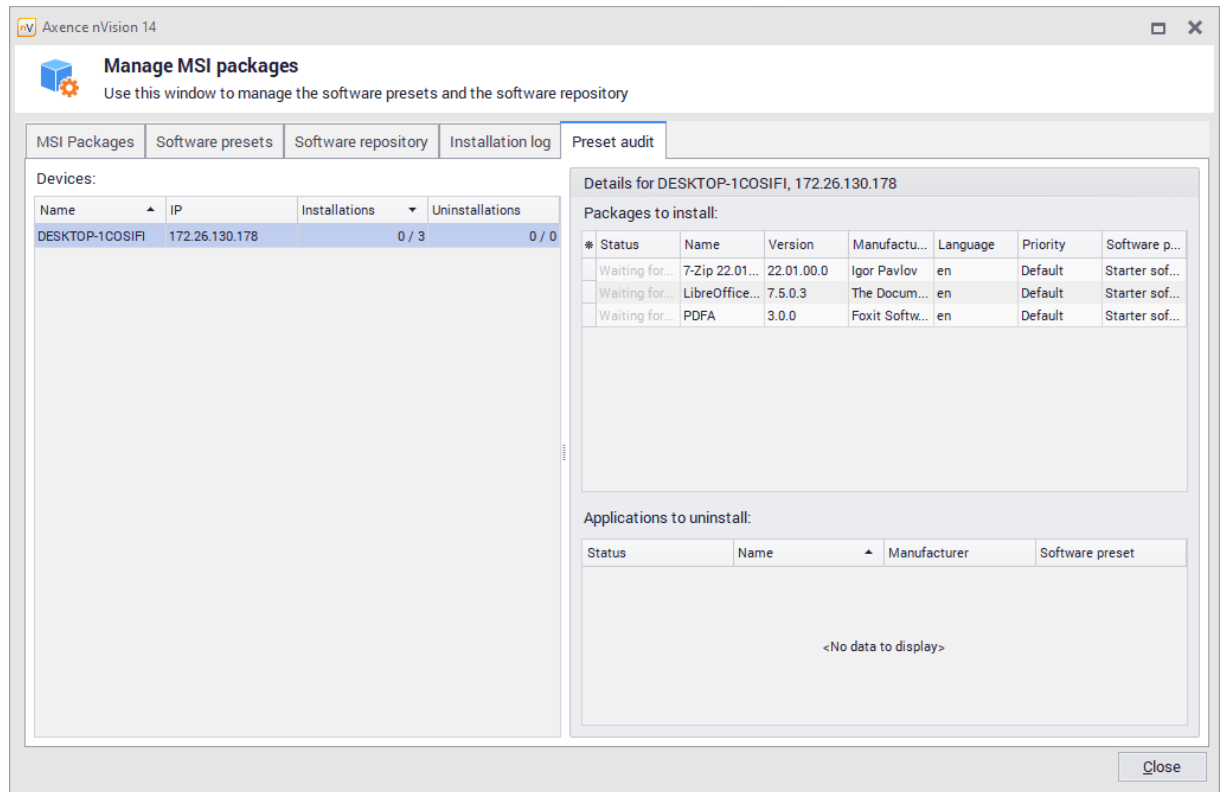
Devices:

| Name | IP |
|-----------------|----------------|
| DESKTOP-1COSIFI | 172.26.130.178 |

Packages to install (3) Applications to uninstall (0)

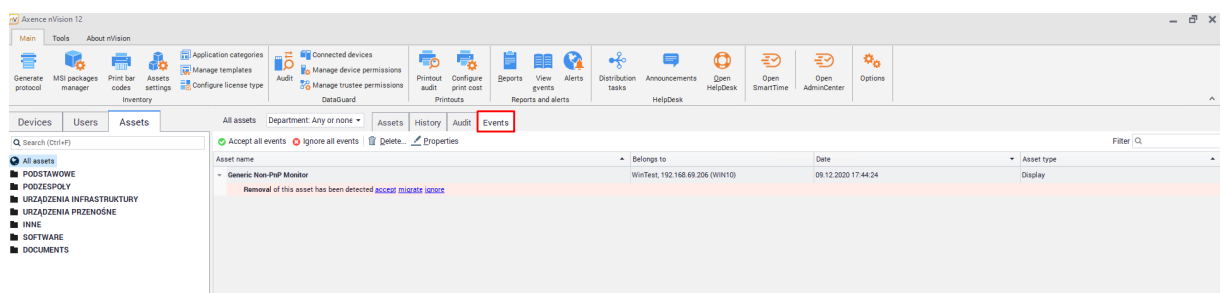
| * Name | Product name | Version | Manufacturer | Language | Priority |
|----------------------|----------------------|------------|---------------------|----------|----------|
| 7-Zip 22.01 (x64...) | 7-Zip 22.01 (x64...) | 22.01.00.0 | Igor Pavlov | en | Default |
| LibreOffice 7.5.... | LibreOffice 7.5.... | 7.5.0.3 | The Document F... | en | Default |
| PDFFA | PDFFA | 3.0.0 | Foxit Software I... | en | Default |

Both packages and software presets 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 in the "Preset audit" tab, where you can check the progress of the installation.



8.8 Inventory events

If the removal or change of any asset or application is detected by the agent, nVision does not decide to remove it from the list or change its properties. Information of such an event is presented in the **Events** tab. An example of the event list is shown below.



Review the displayed events and perform one of the available actions:

- **Ignore** does not change the asset status and the asset is still allocated in the same location; this action is advisable for devices periodically connected and disconnected, e.g. a mouse connected to a laptop.
- **Move** describes the situation when the given device is disconnected from the computer and moved to another location. e.g. a display is reconnected to another computer; specify the new allocation.
- **Accept** means deleting the asset - it is disposed of and will not appear in the asset list anymore.

If there are multiple similar events, you do not have to consider them separately. Simply use the button to **Accept** or **Ignore** all events. Asset properties can also be managed here.

Part



9 DataGuard module

9.1 Introduction

Axence nVision® DataGuard allows the management of data access rights and the protection of data. In particular, the application of data protection improves corporate security, prevents against infecting the corporate network with viruses distributed on flash drives and protects against data leaks.

Blocking ports and media

All devices and media considered as logical disks can be blocked, including:

- flash drives,
- portable hard disk drives,
- Wi-Fi, Bluetooth, IrDA,
- photo cameras and portable MP3 players, working in *multimedia device* mode – WPD,
- floppy disk drives,
- SD slots.

Managing access rights

Managing access rights can take place on different levels (atlas, map, Active Directory users, workstations). On each level, you can grant the appropriate rights related to the use of media and the rights to audit, read, write and execute files to specific users. Managing access rights by means of nVision facilitates the configuration of computer groups, and the authorization of corporate flash drives and hard disk drives and blocking private **devices**. For more information, see [Access rights](#)^[316].

9.2 Access rights

9.2.1 Access rights – introduction

Implementation

There are two possible scenarios for implementing DataGuard module in the given system:



1. **Blocking all/most rights** on the atlas level, and then allowing some of these down the hierarchy tree.
2. **Allowing for all actions** on the atlas level and blocking on the level of maps and for specific workstations.

Choosing one of the above strategies depends on the nature of the system, where the data protection is implemented.

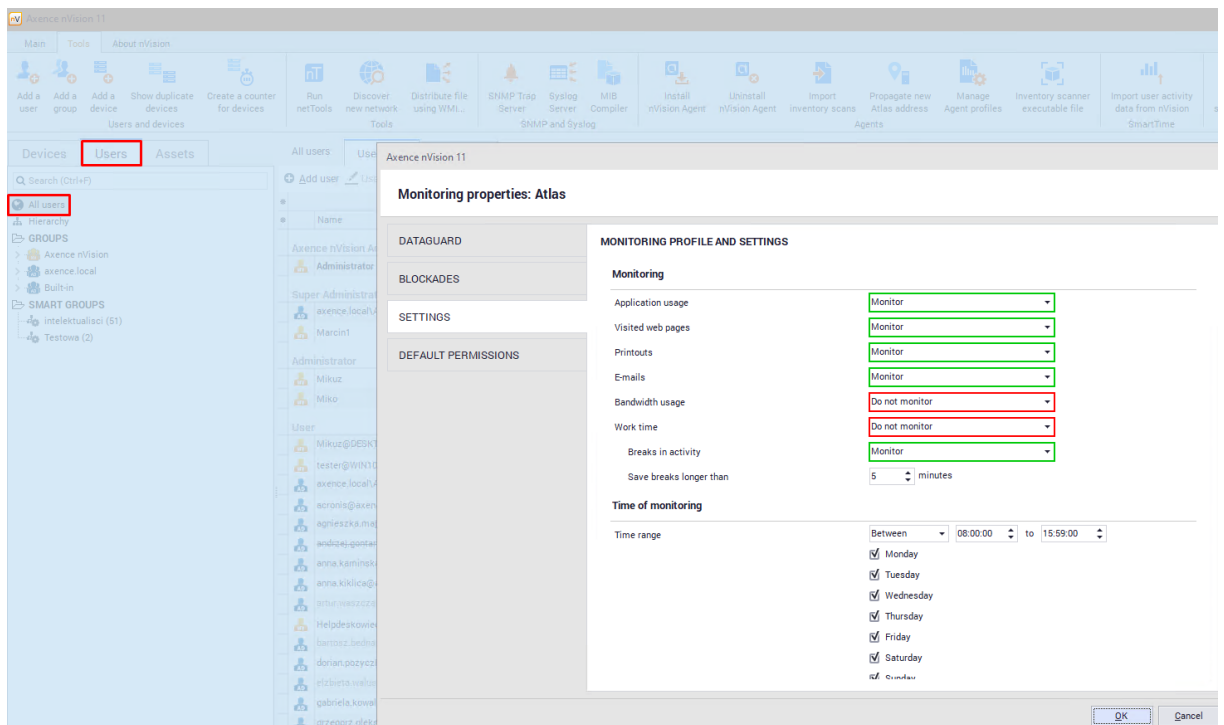
Access rights can be assigned for the following categories:

- **Audit** – determines whether access to the given device should be logged. Logging includes information on file renaming, creating, copying or deleting and access with writing.
- **Reading** – ability to read information from the specified medium.
- **Writing** – ability to write information on the specified medium.

- **Executing** – ability to run programs located on the specified medium.

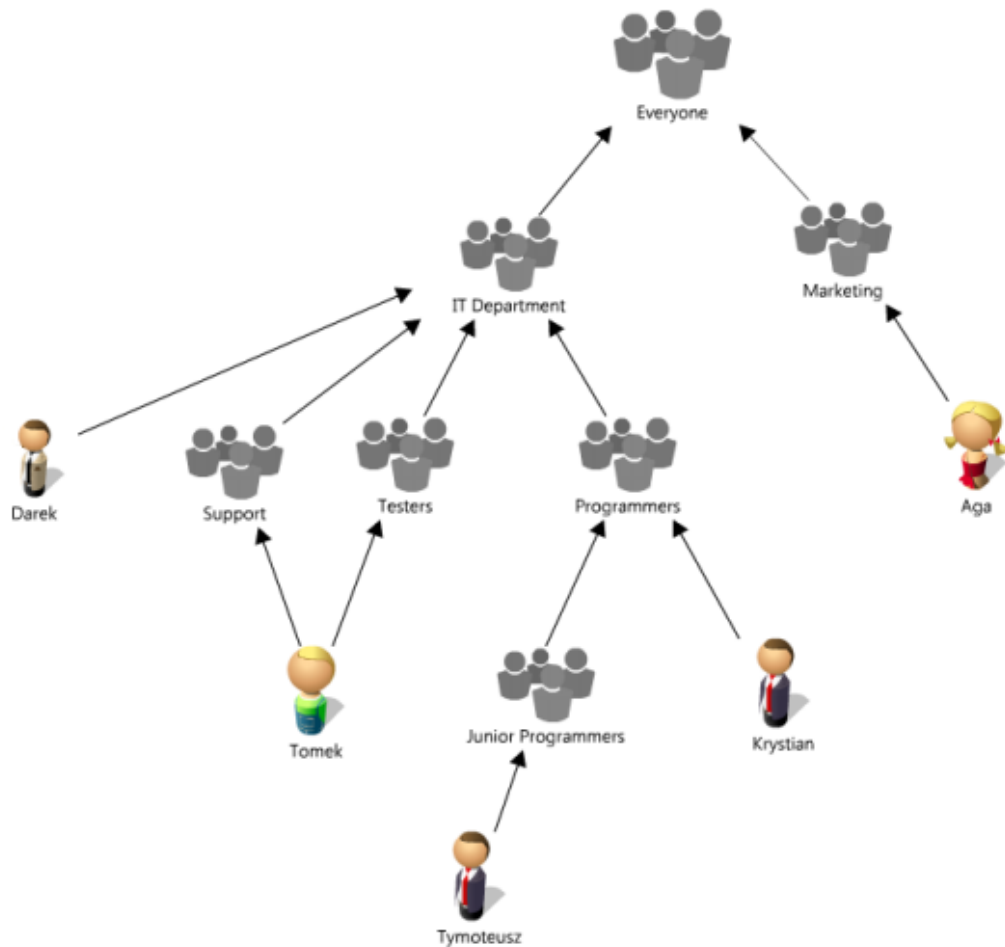
Each category (reading, writing, executing) can have one of two states:  **allow** or  **block**. An audit can be **enabled** or **disabled**. Devices without a file system can have only one access right category. It has the value of **enabled**, if the user is allowed to use the device, and **disabled**, if the opposite is true.

To define access rights to media, go to the atlas, group or user properties.



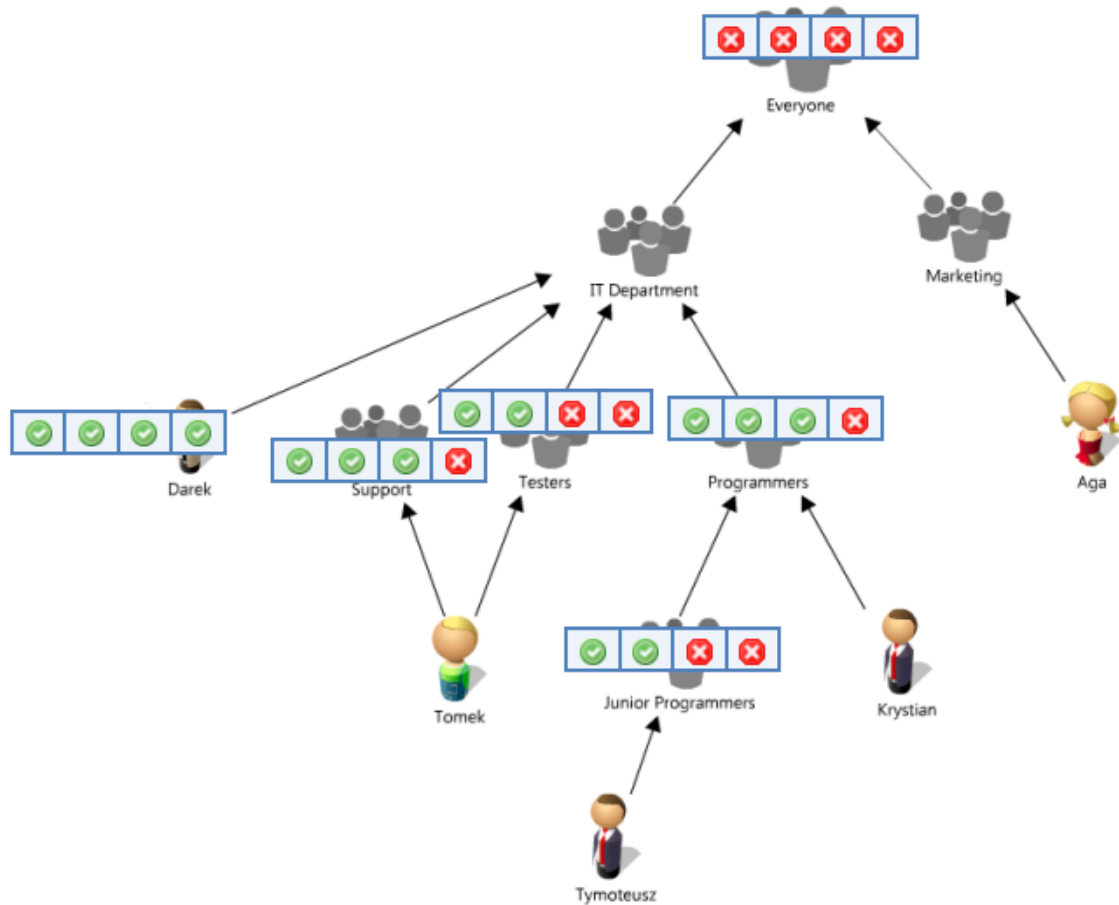
9.2.2 Example of structure

Below is an example structure, which will be used as a basis for discussing the rules of defining rights in the DataGuard module.



The rights can be defined on the level of internal nodes and leaf hosts. Rights effective for leaf nodes are calculated in the following manner: the subsequent nodes, starting from the leaf towards the root (in the present case - *Everyone*), are searched until the first node with assigned rights is found. These rights will be valid for the leaf node.

Please consider the fact that the given computer can belong to several different maps. In the present situation, this is the case of user *Tomek* whose workstation belongs to two maps: *Support* and *Testers*. In this case the effective rights are calculated on each path to the root, and the logical sum of calculated rights is considered as valid. In other words, if the right effective for any path allows for action in the given category, such action will also be allowed for the considered leaf node.



Rights effective for the leaf hosts:

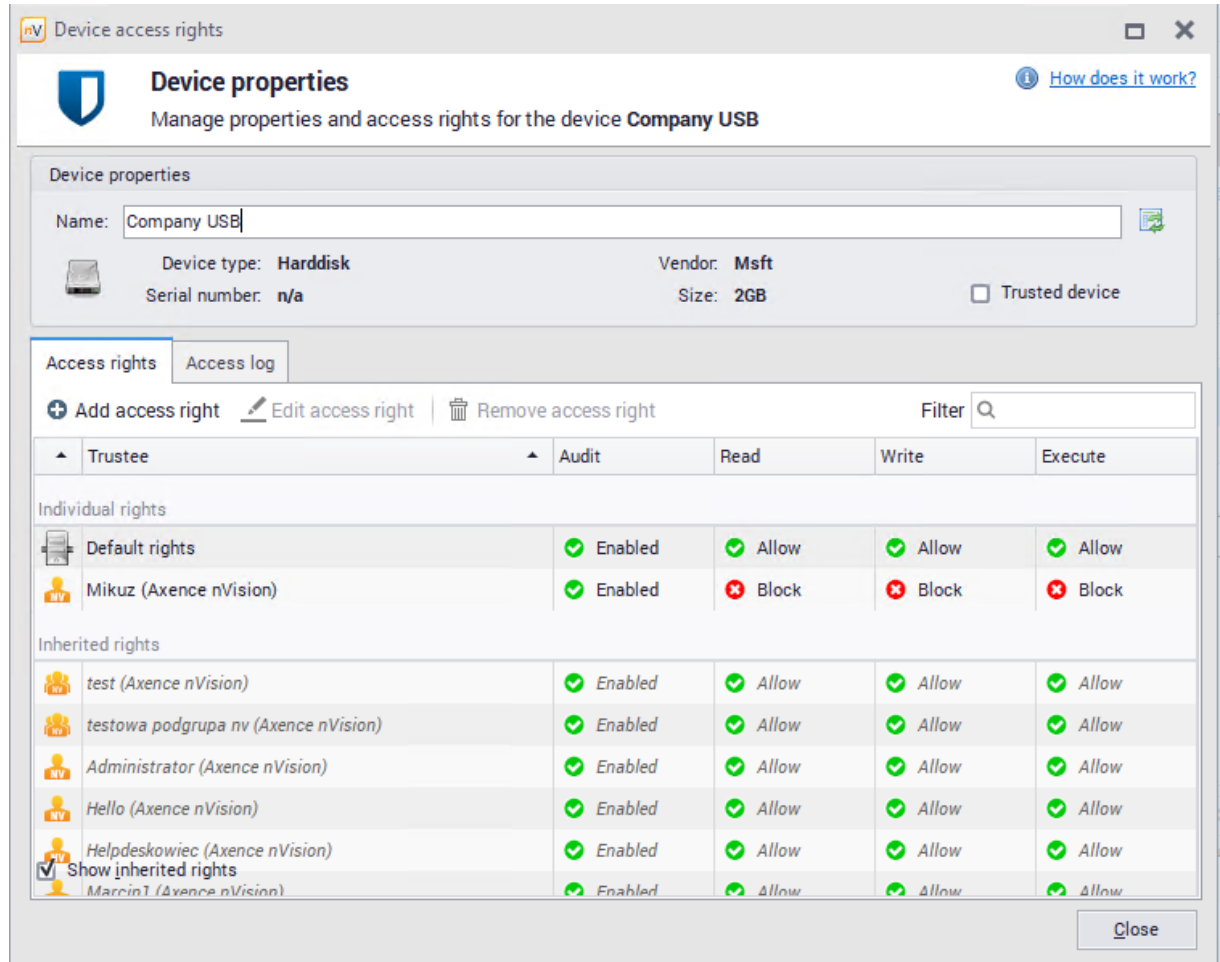
| Workstation | Effective rights | Description |
|-------------|------------------|--|
| Aga | | No rights. Effective right is calculated on the basis of affiliation to group <i>Everyone</i> . |
| Krystian | | No right to execute files. Rights result from affiliation to group <i>Programmers</i> . |
| Tymoteusz | | No writing and executing rights. Rights result from affiliation to group <i>Junior Programmers</i> . |
| Tomek | | No right to execute files. Tomek belongs to two groups with defined rights: <i>Support</i> and <i>Testers</i> . In this case, the sum of their rights is taken into consideration. |
| Darek | | Full rights, assigned individually. |

9.2.3 Inherited rights

The rights for the specific workstation or map can be assigned directly or inherited from parent levels. These are displayed in the above mentioned sequence, i.e. first the individually assigned rights, then the inherited rights. What is more, inherited rights are marked in gray and italics. It allows you to distinguish

at a glance, which rights are specific for the given workstation, and which are the result of the rights granted on higher levels.

In the case of multiple maps and workstations, using the option of hiding inherited rights by means of the **Show inherited rights** button in the lower left corner of the device properties window is recommended.









9.3 Hosts

9.3.1 Devices and media






Devices and media are divided into several categories. Each category is marked with an appropriate icon.

Devices based on file system

| Icon | File system devices |
|---|---------------------|
|  | hard disk drives |
|  | optical devices |
|  | USB storage devices |
|  | virtual volumes |

| Icon | File system devices |
|---|---------------------|
|  | SD cards |
|  | floppy devices |

Other devices

| Icon | Device type | Examples of devices |
|---|----------------------------------|--|
|  | network or communication devices | Bluetooth radio receivers, infrared devices, network adapters, modems |
|  | portable devices | wireless communication devices |
|  | ports | Firewire, multi-port serial adapters, cable transfer devices, PCMCIA and multi-function devices, COM and LPT ports |
|  | printers | printers |
|  | PnP devices | imaging devices, smart cards, other devices |

Assigning rights

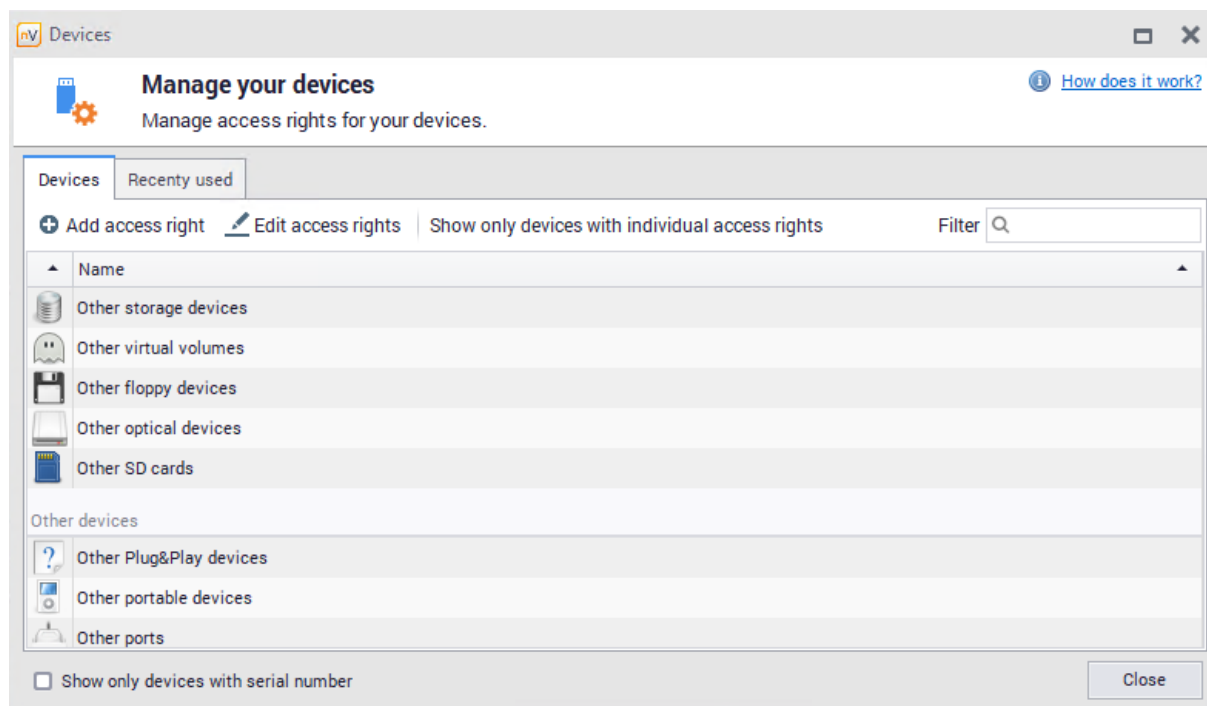
File system devices can have assigned access rights in each of the four categories described in the section [Access rights](#)^[316]. In turn, other devices can only have assigned rights related to the permission to use the device (the given device can be blocked or allowed). nVision automatically detects connected devices and media and assigns each of them to one of the above categories, depending on the device type.

9.3.2 Management

To manage the device access rights, click the **Manage devices** button in the main toolbar.

The following image presents an example of the **Devices** window. The upper part of the list includes specific devices discovered by nVision, the last specified group are **Other devices**. It includes all the remaining devices, i.e. still undefined ones, sorted into categories.

In order to show devices with individual DataGuard rights configured, press **Show only devices with individual access rights** button. Double-clicking on device name opens its properties window where the groups or hosts with individual permissions are specified.

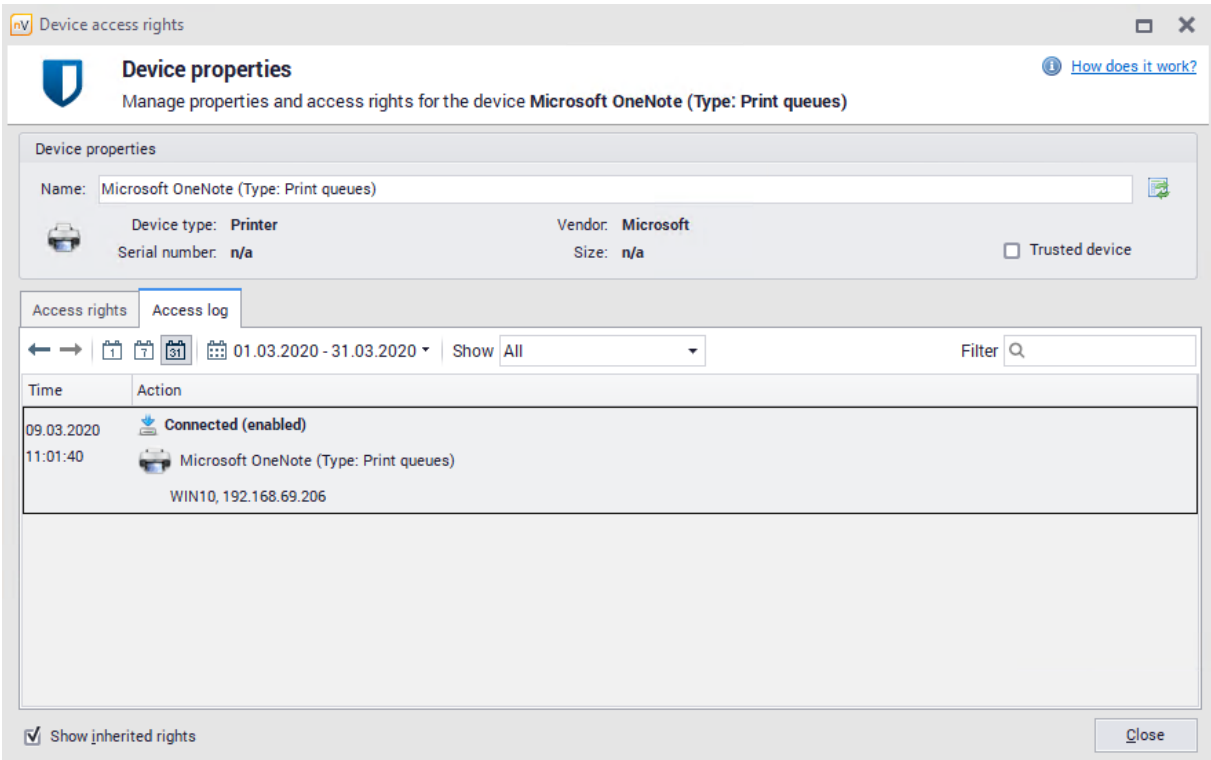


The connecting and disconnecting of a device is always monitored. Detected devices appear in the appropriate categories in the list.

To learn more about flash drive blocking, see section [How to set the access rights to USB media?](#)^[344].

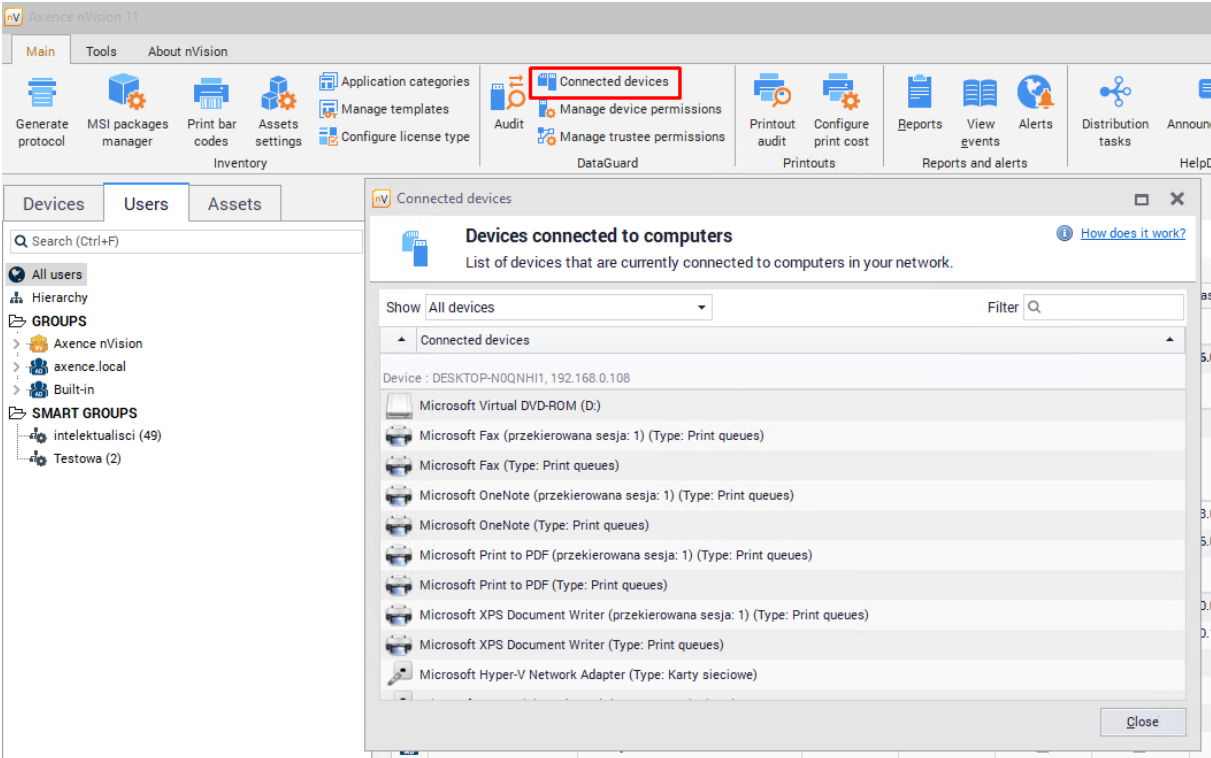
Recently used devices

The **Recently used** tab in the **Devices** window shows the list of recently used devices. All changes related to the connecting and disconnecting of the device are monitored. To review the history of monitored devices, select period (day, week or month) and if necessary, use arrows to view previous or next periods. If the amount of data is significant, use the option to search for required information.



9.3.3 Connected devices

To review the currently connected devices, select the **Connected devices** option in the main toolbar.



It is also possible to view devices connected to a given computer from the level of the **Host info** window specific for a given computer (**Inventory / Hardware / Connected devices** tab).

The most general view with the option to switch between workstations, maps and different functionalities of the DataGuard module is offered by the **Manage trustees** window. To learn more, see section [Managing trustees](#)³²⁶.

9.3.4 Changing a device name

Devices connected to monitored machines initially bear names assigned by nVision. It is possible to change such a name and to restore the default name.

To change the device name:

1. Navigate to **Device properties** tab by double-clicking the line with the selected device.
2. Enter the custom device name in the **Name** field.

Device properties

Manage properties and access rights for the device **Company USB**

Device properties

Name:

Device type: **Harddisk** Vendor: **Msft**

Serial number: **n/a** Size: **2GB** Trusted device

Access rights | Access log

+ Add access right | Edit access right | Remove access right | Filter

| Trustee | Audit | Read | Write | Execute |
|--------------------------------------|---------|-------|-------|---------|
| Individual rights | | | | |
| Default rights | Enabled | Allow | Allow | Allow |
| Mikuz (Axence nVision) | Enabled | Block | Block | Block |
| Inherited rights | | | | |
| test (Axence nVision) | Enabled | Allow | Allow | Allow |
| testowa podgrupa nv (Axence nVision) | Enabled | Allow | Allow | Allow |
| Administrator (Axence nVision) | Enabled | Allow | Allow | Allow |
| Hello (Axence nVision) | Enabled | Allow | Allow | Allow |
| Helpdeskowiec (Axence nVision) | Enabled | Allow | Allow | Allow |
| Show inherited rights | Enabled | Allow | Allow | Allow |
| Marcin1 (Axence nVision) | Enabled | Allow | Allow | Allow |

Close

To restore the default device name, click the  button on the right side of the **Name** field.

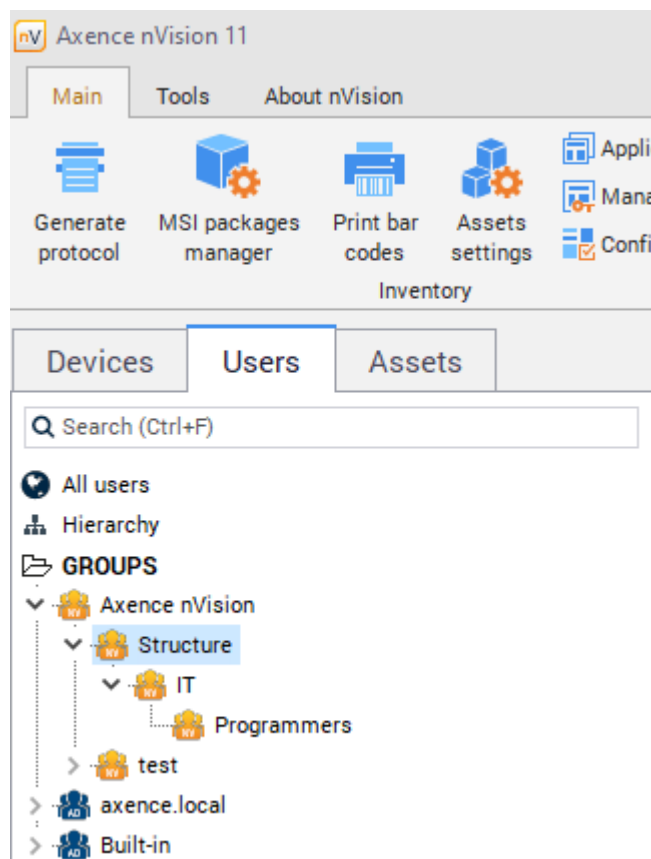
9.4 Trustees

9.4.1 Trustees – introduction

Trustees (trusted units) are workstations and computer groups for which the access rights are defined. Depending on the trust level, units can have various rights assigned. To learn more on the access rights, see section [Access rights](#)^[316].

User groups

Defining separate access rights for each user would be a time consuming operation. Therefore, grouping the individual workstations into maps created by the system administrator is recommended. If the created map structure reflects the real interdependencies between the users, it is possible to set the access rights in a quick manner. An example of map structure is presented below.





To learn more on the calculation of effective access rights for the above structure, see section [Example of structure](#)^[317].



There are two methods to manage the access rights:

- Management from the level of the properties of a given user, group or atlas – [Managing via user hierarchy](#)^[326]
- Management with the [Managing trustees](#)^[326] function

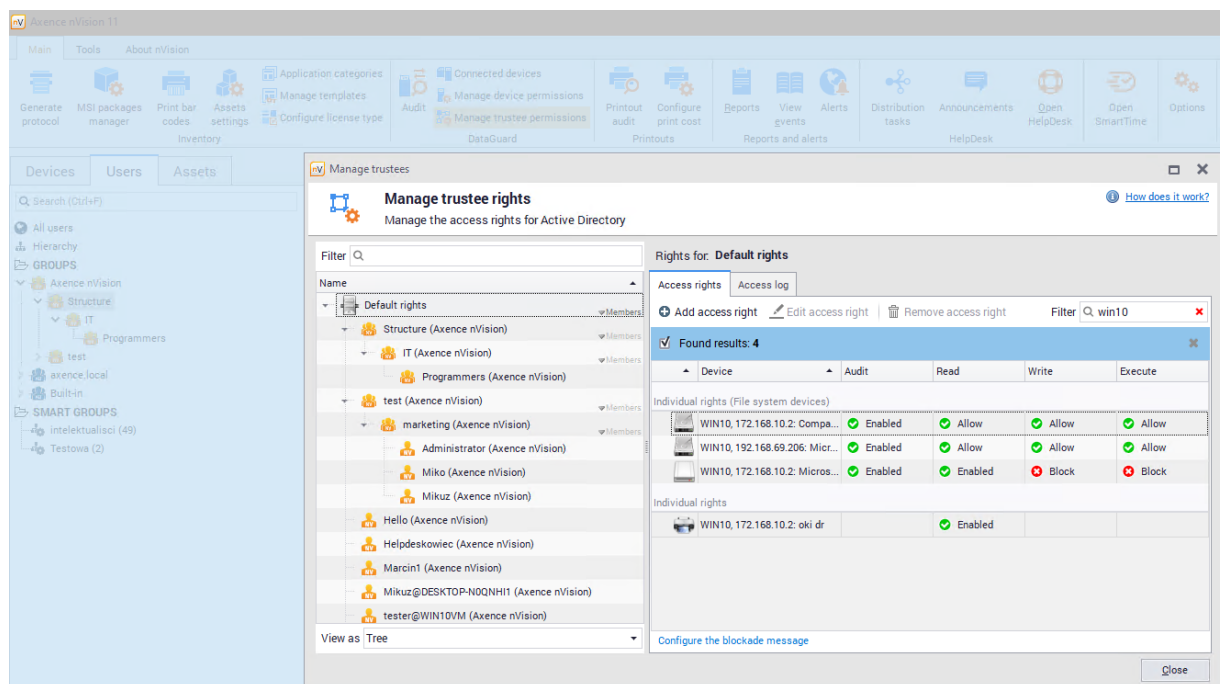
9.4.2 Managing via user hierarchy

To manage the access rights for a user, group or atlas (referred to as “units”):

1. Select a unit and right-click to open its  **Info** window.
2. Navigate to the DataGuard tab.
3. To change the previously defined rule, double-click the row with the chosen rule and go to step 5. To define a new rule, click the  **Add access right** button.
4. Use the list to select a device for which you will assign the rights.
5. Set the access rights and press **Enter**.



To the edit access rights to the selected device, use the  **Edit access rights** button. If you want to delete the previously granted rights, use the  **Remove access rights** button.

The screenshot below illustrates the case of setting individual rights to a virtual disk drive in the **Atlas info** window (the default right, most important in the hierarchy).



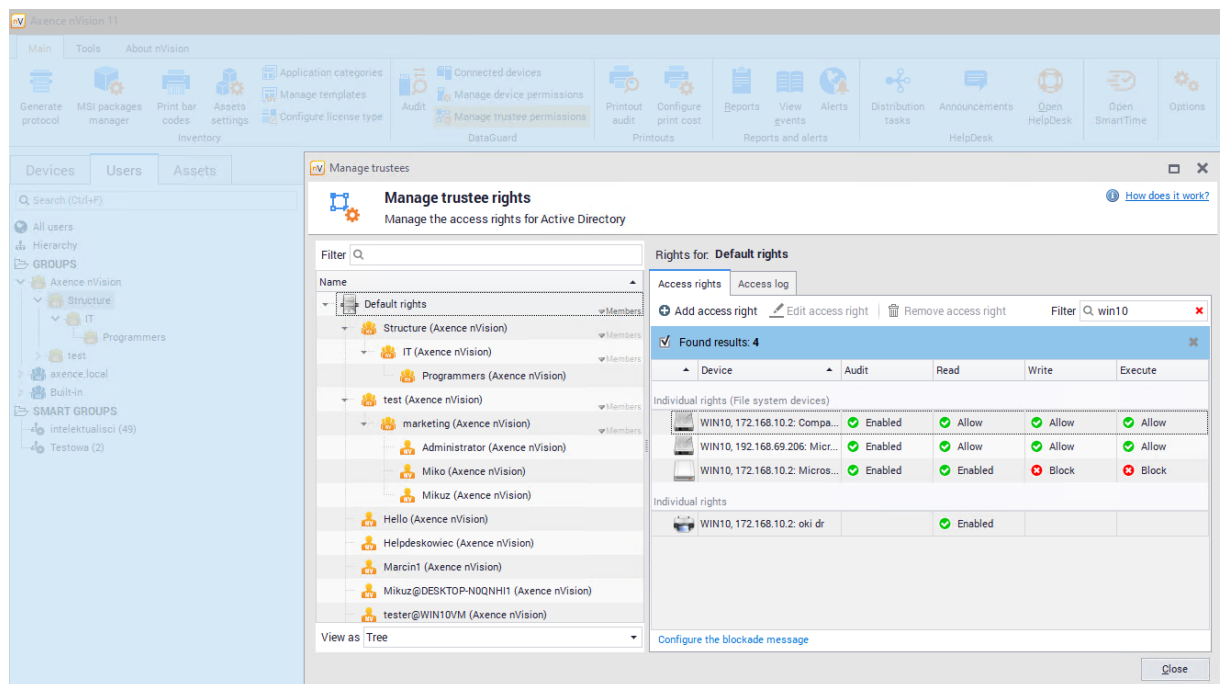
9.4.3 Managing trustees

To manage the access rights to all units:

1. In nVision’s main toolbar, select the **Manage trustees** option from the DataGuard section.
2. Select a unit in the list on the left side. If necessary, use the search function to find the appropriate unit quickly.
3. To change the previously defined rule, double-click the row with the chosen rule in the right part of the window or select the row and click the  **Edit access rights** button. To define a new rule, click the  **Add access right** button.

4. Use the list to select a device for which you will assign the rights.
5. Set the access rights and press **Enter**.

The rights assigned individually can also be edited directly in the management window. For this purpose, click the selected right to change it. Clicking the inherited access rights will open the **Define access rights** window.



9.4.4 Active Directory users

Data Guard module is integrated with Active Directory. Therefore, access rights can be assigned to AD users directly.



The screenshot displays the Axence nVision 11 software interface. The top navigation bar includes sections for Main, Tools, and About nVision. The main toolbar contains various management tools such as Generate protocol, MSI packages manager, Print bar codes, Assets settings, Manage templates, Configure license type, Connected devices, Manage device permissions, Audit, Manage trustee permissions, Printout audit, Configure print cost, Reports, View events, Alerts, Distribution tasks, Announcements, Open HelpDesk, and Open SmartTime.

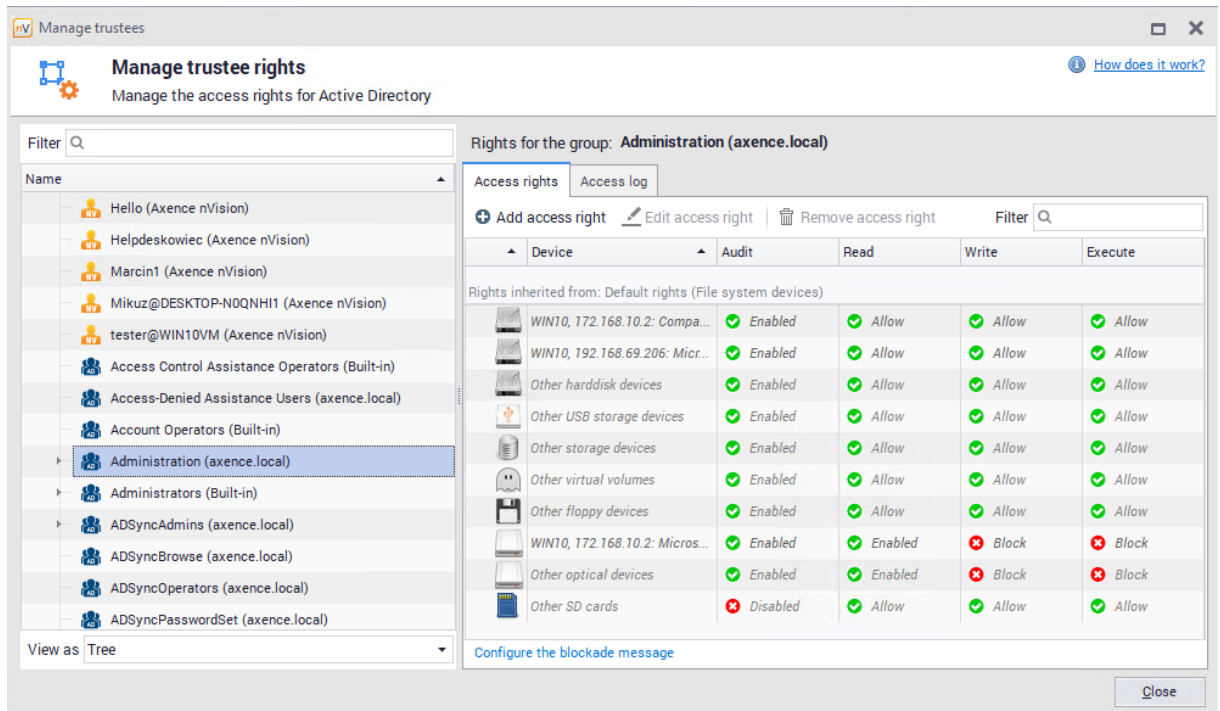
The interface is currently showing the 'Administration' group configuration. The left sidebar lists various system components and user groups, including 'axence local' and 'Administration'. The main panel displays the 'DATAGUARD' settings for the 'Administration' group. The 'Access rights' tab is active, showing a table of inherited rights from default file system devices.

| Device | Audit | Read | Write | Execute |
|---|-------|------|-------|---------|
| Rights inherited from: Default rights (File system devices) | | | | |
| WIN10, 172.168.10.2: Company USB | ✓ | ✓ | ✓ | ✓ |
| WIN10, 192.168.69.206: Microsoft Virtual Disk 2GB (D:) | ✓ | ✓ | ✓ | ✓ |
| Other harddisk devices | ✓ | ✓ | ✓ | ✓ |
| Other USB storage devices | ✓ | ✓ | ✓ | ✓ |
| Other storage devices | ✓ | ✓ | ✓ | ✓ |
| Other virtual volumes | ✓ | ✓ | ✓ | ✓ |
| Other floppy devices | ✓ | ✓ | ✓ | ✓ |
| WIN10, 172.168.10.2: Microsoft Virtual DVD-ROM (F:) | ✓ | ✓ | ✗ | ✗ |
| Other optical devices | ✓ | ✓ | ✗ | ✗ |
| Other SD cards | ✗ | ✓ | ✓ | ✓ |

Below the table, there is a section for 'Rights inherited from: Default rights' and a link to 'Configure the blockade message'.

To view and define access rights for AD users:

1. Select the **Manage trustees** option in the main toolbar in the DataGuard section.
2. Select a group or a user on the left side of the window. If necessary, use the search function to find the appropriate unit quickly.
3. To change the previously defined rule, double-click the row with the chosen rule in the right part of the window or click the  **Add access right** button. To define a new rule, click the  **Add access right** button.
4. Select a device for which you will assign the rights.
5. Set the access rights and press Enter.

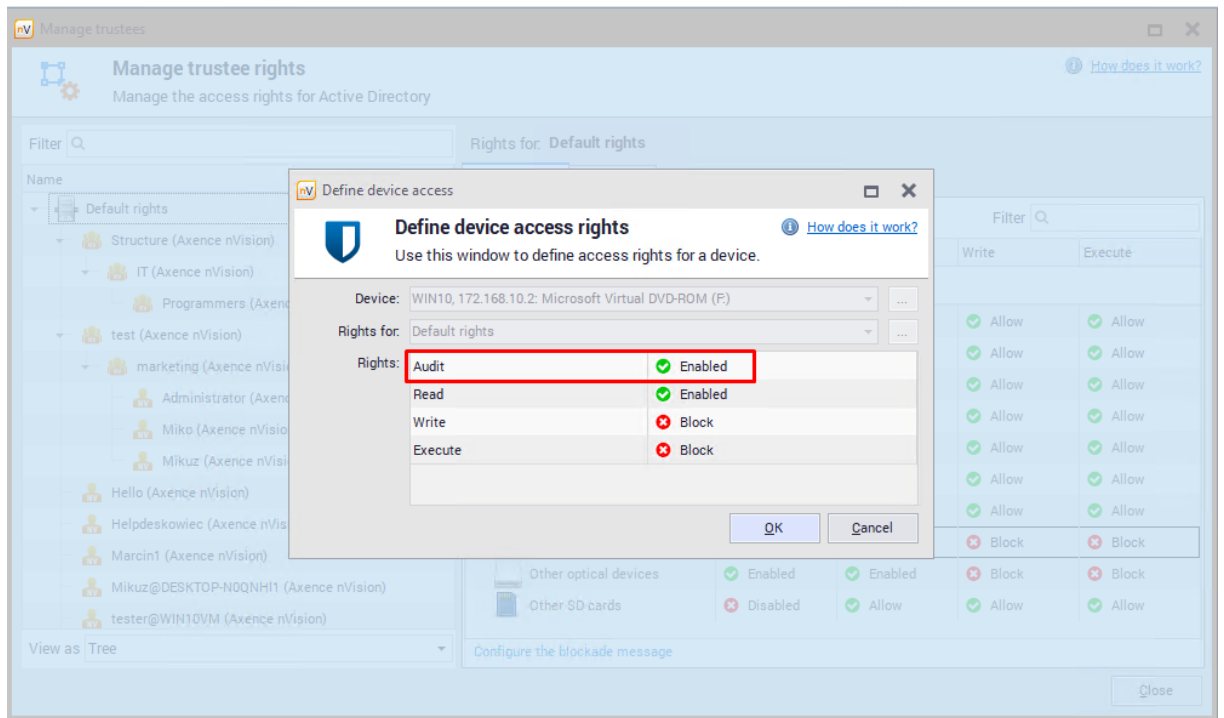


Remarks

- Active Directory trustees access rights have priority over workstation rights.
- Active Directory trustees access rights may be defined for file system devices and for devices with a serial number.
- If a circular dependency between imported AD units is detected, nVision breaks every dependency in that circle. Such a situation is reported by a message in the **Manage trustees** window.

9.4.5 Access log

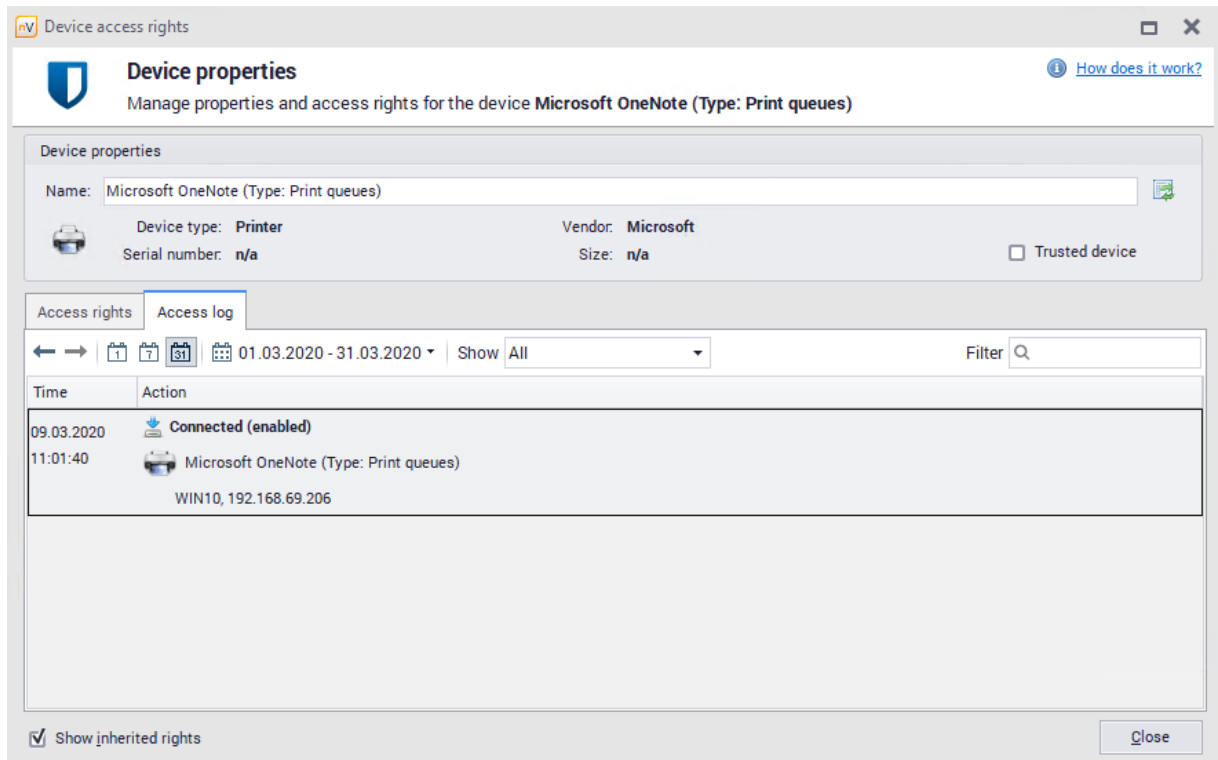
The access log stores information on the access to data and connected devices. To monitor access, enable audit for the device and unit (workstation, map, atlas) to be monitored. Rights can be defined individually or inherited (as shown below).



The connecting and disconnecting of a device is always monitored. **With audit toggled on, file creation, renaming, writing and deleting are also monitored.**

To view the access log:

1. Select the **Manage trustees** option in the main toolbar in the DataGuard section.
2. Navigate to the **Access log** tab.
3. Select a unit in the list on the left side. If necessary, use the search function to find the appropriate unit quickly.
4. Choose a period of information to be viewed.



9.4.6 Access log for users

To view the access log for users from the level of **Manage trustees** window:

1. Select the **Manage trustees** option in the main toolbar in the DataGuard section.
2. Select a group or a user on the left side of the window. If necessary, use the search function to find the appropriate unit quickly.
3. Navigate to the **Access log** tab.

All data relating to connections and disconnections of devices and data relating to file operations will be show in this tab (audit on these devices must be toggled on).

It is possible to limit the view to a specific day, week or month. Use the navigation arrows to read data concerning the period you are interested in.

To check other methods to view connected devices, see section [Connected devices](#) ³²³.

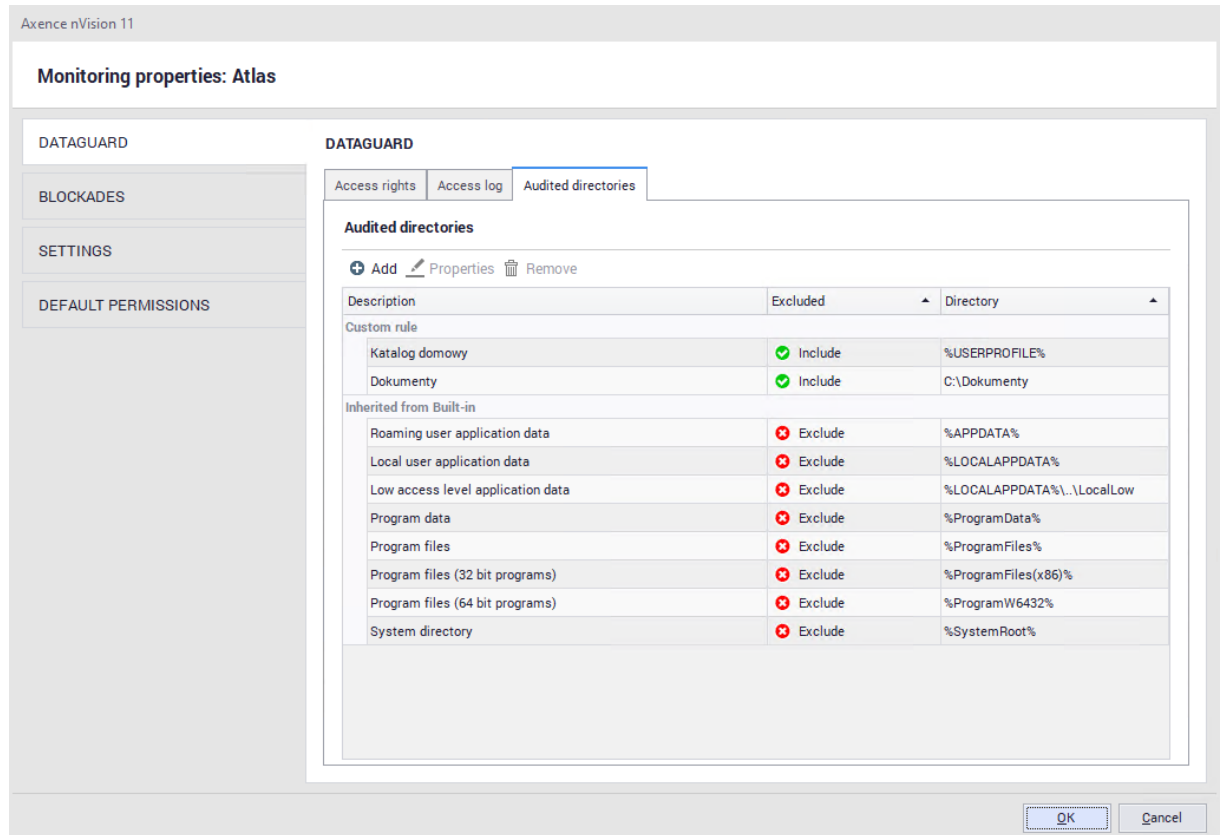
9.5 Local directories monitoring

9.5.1 Audit local directories - introduction

The DataGuard module in nVision 11.9 has been expanded with the auditing operations function performed on files in local directories.

Until now, the DataGuard module allowed auditing only at the level of the entire device, without the possibility of auditing the entire system disk. The purpose of extending the module was to enable the definition of additional auditing rules at the level of local directories (regardless of the disk and device on which the directory is located). Due to changes applied in nVision 11.9, it is possible to monitor operations also on system disks.

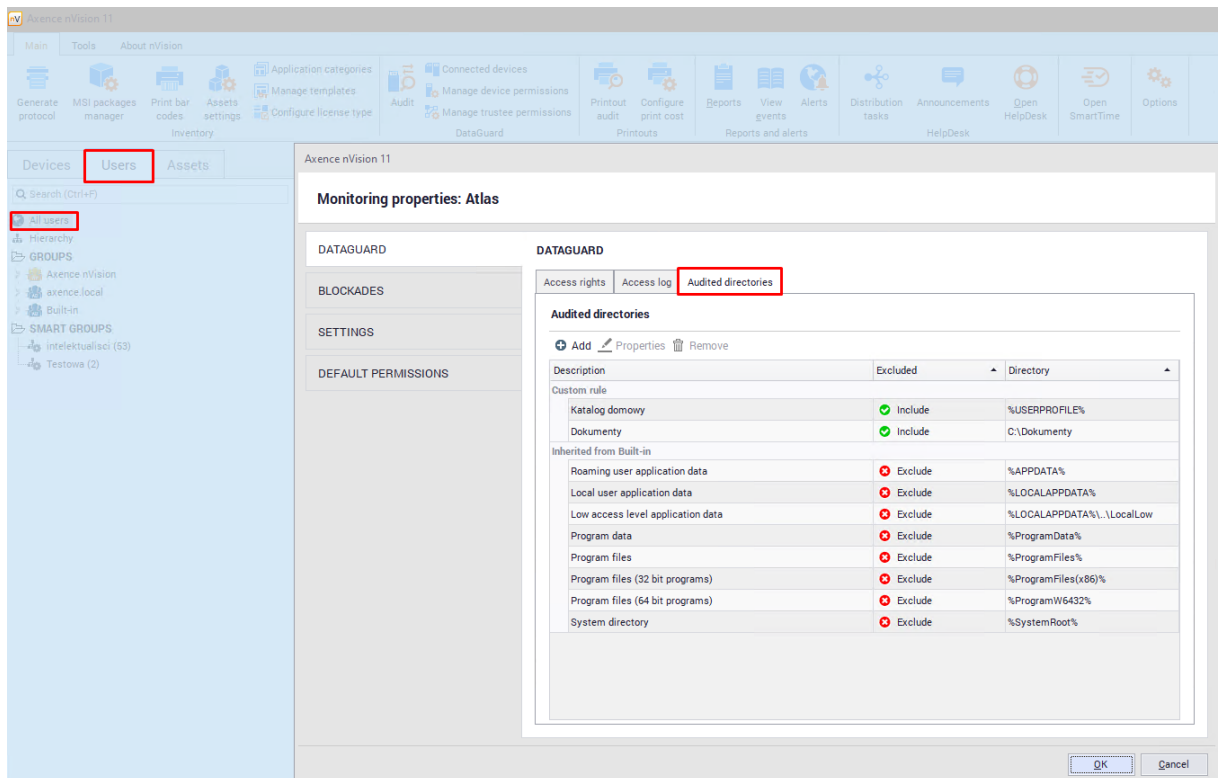
Defining the directories to be audited is done by the user (suchlike defining access rights to monitored devices), user group and Atlas level:



9.5.2 Configuration

Local directory monitoring settings can be defined for Atlas (all users), user groups and for individual users. They can be accessed from several locations:

1. Window: Users / Atlas / DataGuard / Audited directories:



2. Window: Group information / **DataGuard** / **Audited directories**

3. Window User information / **DataGuard** / **Audited directories**

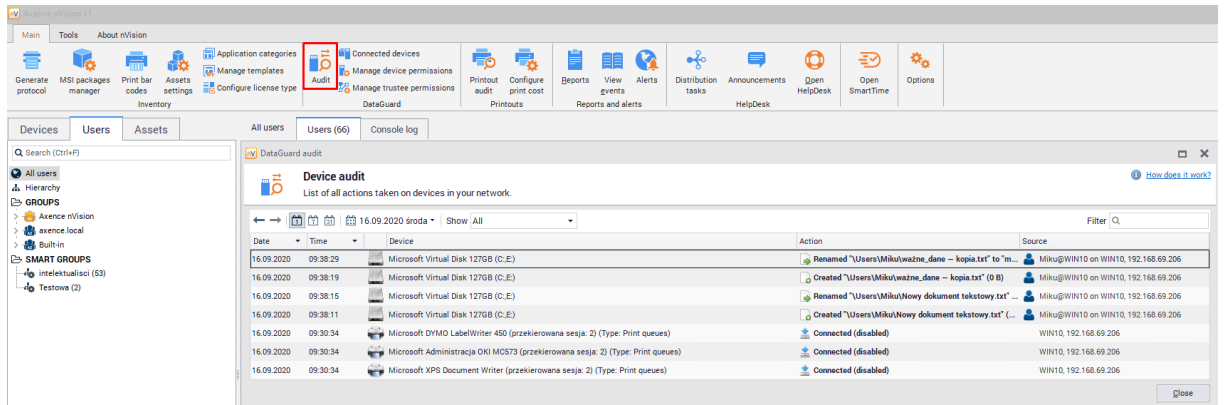
Atlas is a general setting that is inherited by groups and users by default. This setting can be changed for individual units by going to the settings windows mentioned above.

To add a directory in which file operations are to be monitored, click the **Add** button. A new window will open to create an entry. The rule name and directory path should be specified there. The directory path can be given:

- In absolute form, starting with a drive letter (for example "C: \") and ending with the full name of the directory of audited directory
- In a form containing an environment variable that begins and ends with the character "%". A variable can appear anywhere in the path and replace any part of it. For example, if "% USER-PROFILE%" is "C: \ Users", you can add "% USERPROFILE% \ Data \" as the monitored directory.

Each added audited directory automatically causes that **its entire content is audited** (including sub-directories and files).

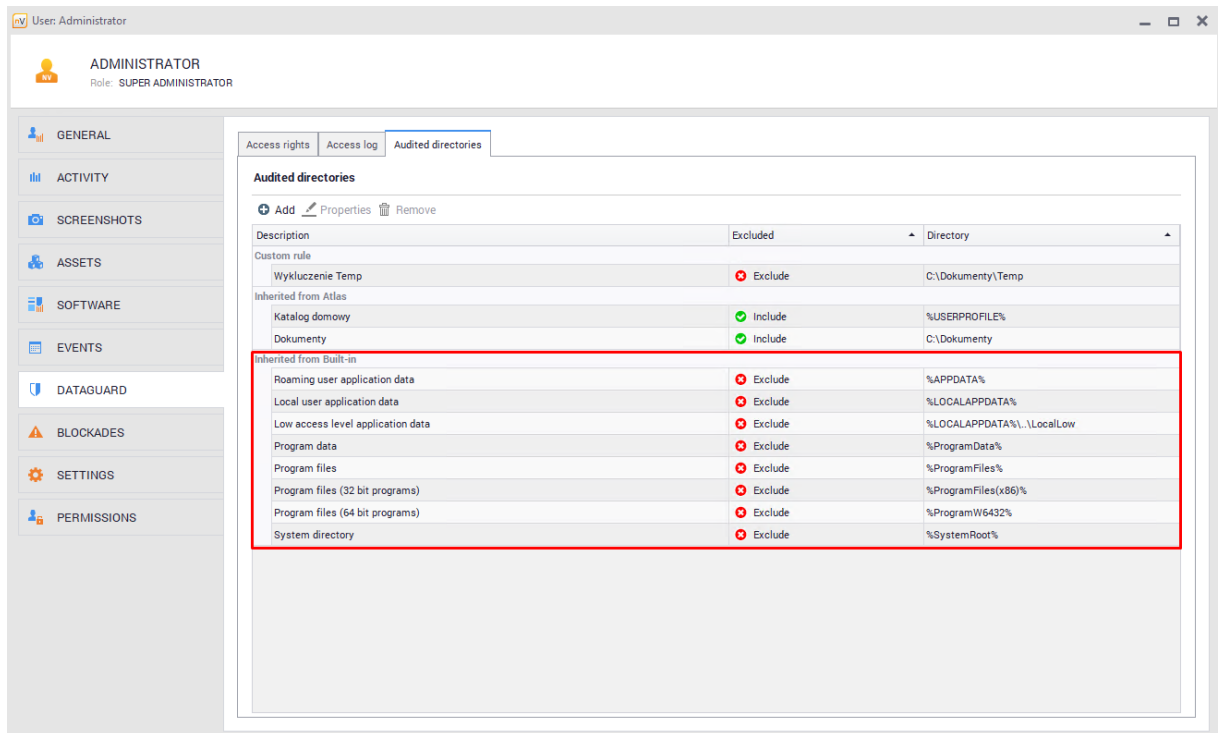
Once the rules are added, it will be possible to monitor file operations in a specific directory:



Default directories excluded from scanning

The DataGuard module has a list of built-in directories that are always excluded from system-wide scanning. The list of globally excluded directories is built into the program and cannot be edited.

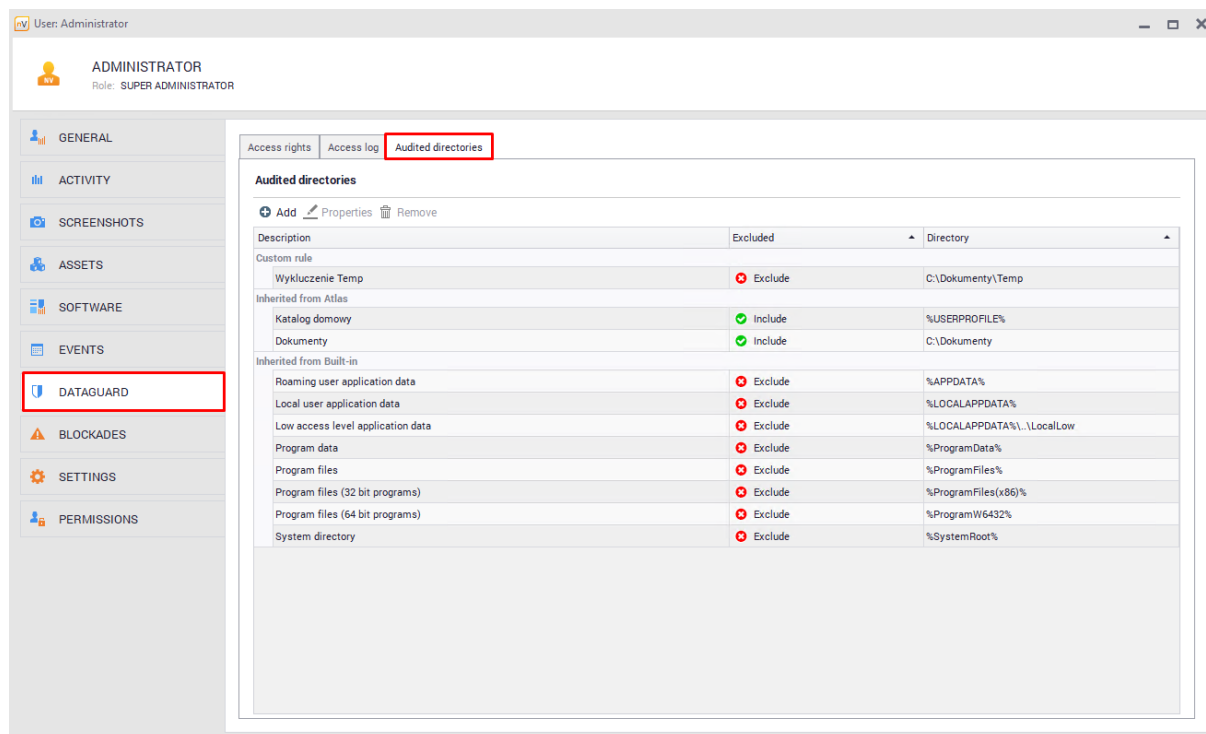
The list of excluded directories is visible in the DataGuard settings:



9.5.3 Audit exclusions

Excluded directories from auditing (exceptions) can be added for each user. This means that for a specific user, operations in the selected directory will not be monitored.

These settings can be assigned for a specific user only from the level of the DataGuard module settings window:



For example: when monitoring operations in the "C: \ Documents \\" directory, a directory "C: \ Documents \ Temp \\" can be added as a directory excluded from auditing for the selected user. "Documents" directory will be audited excluding the sub-directory "Temp".

To add a new exclusion, select the **Add** button and enter the description and path of the directory to be excluded from the audit.

9.6 Alerts

9.6.1 Alerts for DataGuard

Alerts for the DataGuard module allow a warning to be sent in the case of actions related to mobile devices and their connection status. In particular, the administrator can be informed about each attempt of theft of confidential information.

Event types

1. Mobile device connected or disconnected
 - Device is connected
 - Device is disconnected
2. File operation on the mobile device
 - File was created

- File was deleted
- File was renamed
- Data written to existing file


As an additional condition, a file name wildcard can be specified.

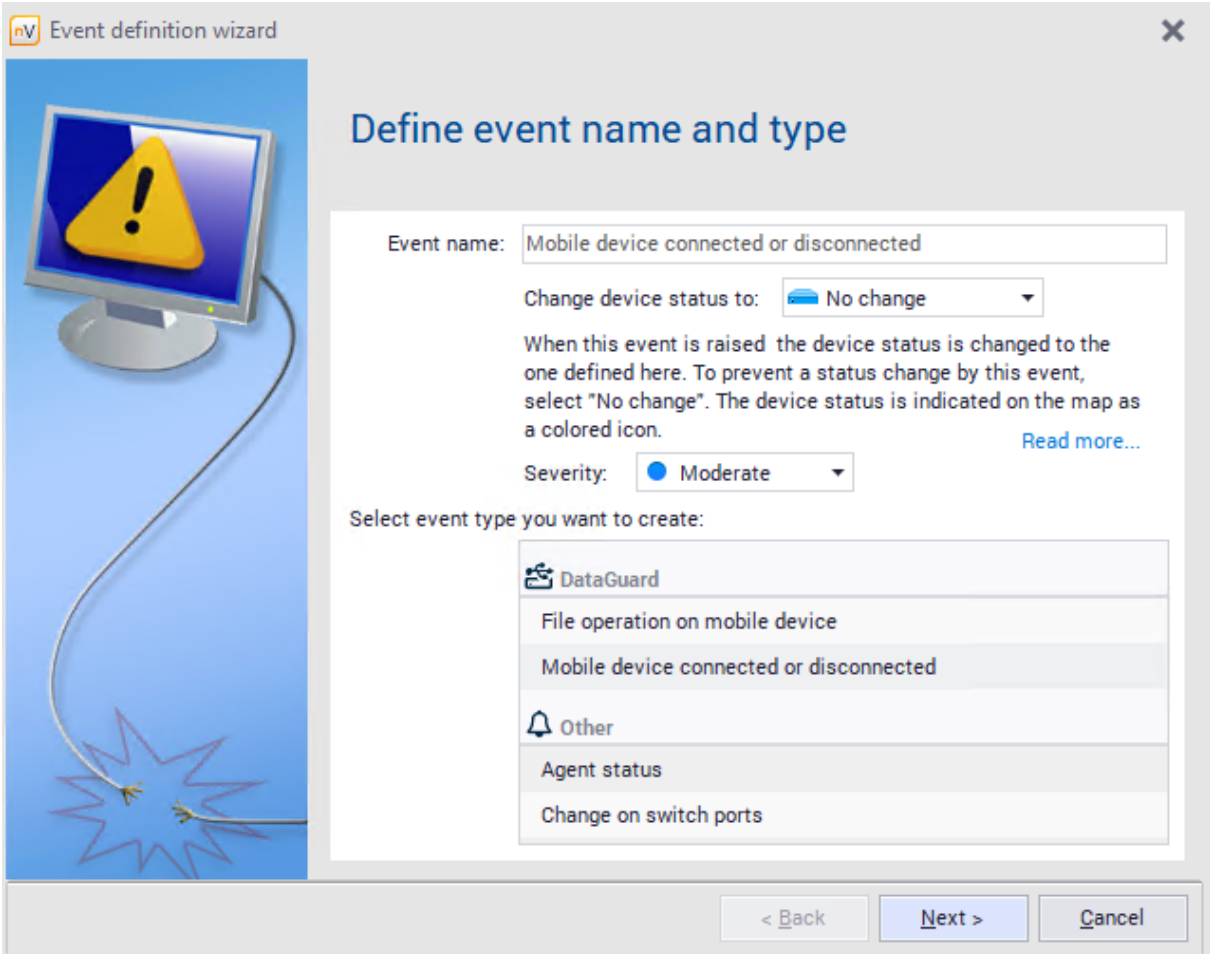
In the case of both selected event types, alerts can be generated for all devices or for specified devices selected from the list.

9.6.2 Creating an alert

To learn more about the alert creation process, see section [Alerting](#) ⁵⁸⁶.

Discovering the connection of a mobile device

1. Open the alert management window in the main toolbar.
2. Click the  **Add alert** button to create a new alert.
3. Click the **New** button in the alert definition window. Enter the event name and select the event type from the list: **Mobile device connected or disconnected**.

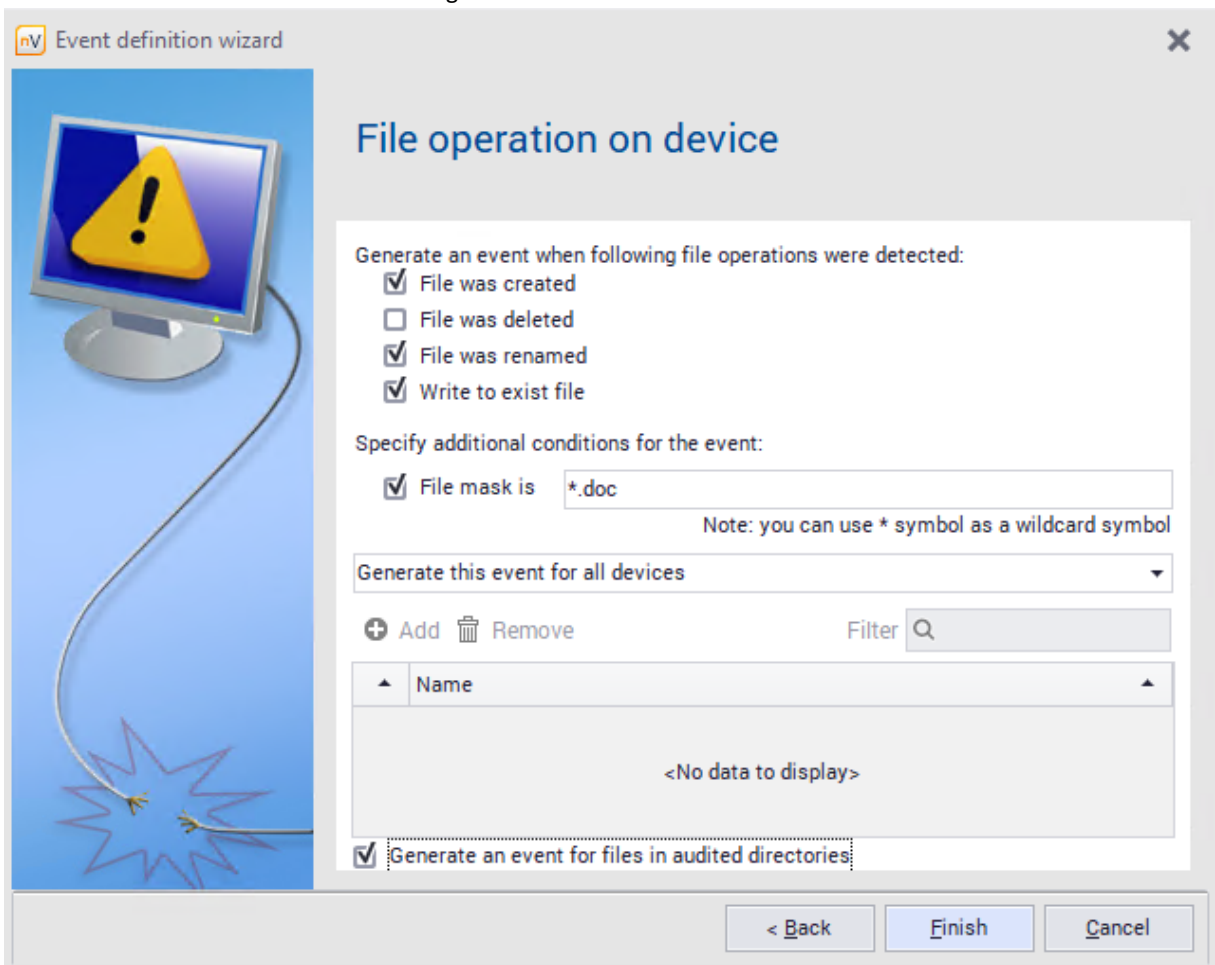


4. Click **Next**. Mark the **Device is connected** field and select the **Specified device**, e.g. **Other USB data media** from the list.

5. Then use the alert definition window to add actions to be performed when the event defined above occurs. Such a created alert will detect a situation when an unknown USB media is connected to the monitored computers.

File operation on device

Similarly, at step 3. choose event type: **File operation on device** and select desired configuration. There is a possibility to toggle **generate an event for files in audited directories** - selecting this option will include local directories audit in this alert configuration.



The screenshot shows the 'Event definition wizard' window for 'File operation on device'. The window title is 'nV Event definition wizard'. On the left, there is a graphic of a computer monitor displaying a yellow warning triangle with an exclamation mark, connected to a USB cable. The main content area is titled 'File operation on device' and contains the following options:

- Generate an event when following file operations were detected:
 - File was created
 - File was deleted
 - File was renamed
 - Write to exist file
- Specify additional conditions for the event:
 - File mask is (Note: you can use * symbol as a wildcard symbol)
- Generate this event for all devices (dropdown menu)
- Buttons: + Add, Remove, Filter (with search icon)
- Table with header 'Name' and content '<No data to display>'
- Generate an event for files in audited directories

At the bottom, there are three buttons: '< Back', 'Finish', and 'Cancel'.

9.7 Security

9.7.1 Windows Defender

Axence nVision® version 13 introduces the Windows Defender antivirus software control feature. This feature is available for computers with Windows 7 operating system or later.

To view the Windows Defender information on a particular device:

1. In the nVision console, click the **Devices** tab.
2. Click the **Security** tab.
3. Double-click the line with the selected device.
4. In the Device Info window, click the **Security** tab.
5. Click the **Windows Defender**.

The **Windows Defender** tab displays the following parameters:

- Real-time security
- Security from the cloud
- Automatic sample transfer
- Security against infringement
- Last scan
- Definition date
- Definition version

In addition, a list of threats detected by the antivirus software is displayed below.

Windows Defender - remote actions

The nVision console allows for remote interaction with Windows Defender on a machine which has the Agent installed. The available actions are as follows:

- Definition update
- Fast scan
- Full scan

To perform one of the above actions:

1. In the nVision console, click the **Devices** tab.
2. Click the **Security** tab.
3. Right-click the line with the specific device.
4. Select **Windows Defender** from the list, and then click one of the three actions.

Once the selected action is executed, the parameters that are displayed in the list, i.e. last scan date, definition date and definition version, will be updated.

You can create a [policy](#) to provide better control of the antivirus software.

9.7.2 Windows BitLocker

Axence nVision® version 13 introduces the BitLocker software control feature. This feature is available for computers with Windows 7 operating system or later.

To view the Windows Defender information on a particular device:

1. In the nVision console, click the **Devices** tab.
2. Click the **Security** tab, and then double-click the line with the selected device.
3. In the Device Info window, click the **Security** tab. If a tab other than BitLocker is displayed, click the **BitLocker** button.

The read parameters displayed in the **BitLocker** tab are as follows:

1. BitLocker:
 - System disk status
2. TPM:

- Version
- Enabled
- Activated

9.7.3 Windows Firewall

Enter topic text here.

9.8 Audit

To perform a device audit:

1. Select the **Audit** option in the main toolbar in the DataGuard section.
2. Choose a period of information to be viewed.

The screenshot shows the DataGuard software interface. The main toolbar at the top has the 'Audit' icon highlighted with a red box. The 'Device audit' window is open, displaying a table of actions taken on devices in the network. The table has columns for Date, Time, Device, Action, and Source. The data shows various actions such as 'Connected (enabled)', 'Disconnected (enabled)', and 'Disconnected when system was offline (enabled)' for different devices and users.

| Date | Time | Device | Action | Source |
|------------|----------|---|--|---|
| 30.03.2020 | 11:04:34 | Microsoft Fax (przekierowana sesja: 1) (Type: Print queues) | Connected (enabled) | DESKTOP-NOQNH11, 192.168.0.108 |
| 30.03.2020 | 11:04:34 | Microsoft OneNote (przekierowana sesja: 1) (Type: Print queues) | Connected (enabled) | DESKTOP-NOQNH11, 192.168.0.108 |
| 30.03.2020 | 11:04:34 | Microsoft Print to PDF (przekierowana sesja: 1) (Type: Print queues) | Connected (enabled) | DESKTOP-NOQNH11, 192.168.0.108 |
| 30.03.2020 | 11:04:34 | Microsoft XPS Document Writer (przekierowana sesja: 1) (Type: Print queues) | Connected (enabled) | DESKTOP-NOQNH11, 192.168.0.108 |
| 27.03.2020 | 15:01:50 | Microsoft OneNote (przekierowana sesja: 1) (Type: Print queues) | Disconnected (enabled) | DESKTOP-NOQNH11, 192.168.0.108 |
| 27.03.2020 | 15:01:50 | Microsoft Print to PDF (przekierowana sesja: 1) (Type: Print queues) | Disconnected (enabled) | DESKTOP-NOQNH11, 192.168.0.108 |
| 27.03.2020 | 15:01:49 | Microsoft XPS Document Writer (przekierowana sesja: 1) (Type: Print queues) | Disconnected (enabled) | DESKTOP-NOQNH11, 192.168.0.108 |
| 27.03.2020 | 15:01:49 | Microsoft Fax (przekierowana sesja: 1) (Type: Print queues) | Disconnected (enabled) | DESKTOP-NOQNH11, 192.168.0.108 |
| 27.03.2020 | 10:15:10 | Microsoft OneNote (przekierowana sesja: 1) (Type: Print queues) | Connected (enabled) | DESKTOP-NOQNH11, 192.168.0.108 |
| 27.03.2020 | 10:15:10 | Microsoft Print to PDF (przekierowana sesja: 1) (Type: Print queues) | Connected (enabled) | DESKTOP-NOQNH11, 192.168.0.108 |
| 27.03.2020 | 10:15:10 | Microsoft XPS Document Writer (przekierowana sesja: 1) (Type: Print queues) | Connected (enabled) | DESKTOP-NOQNH11, 192.168.0.108 |
| 27.03.2020 | 10:15:10 | Microsoft Fax (przekierowana sesja: 1) (Type: Print queues) | Connected (enabled) | DESKTOP-NOQNH11, 192.168.0.108 |
| 26.03.2020 | 23:30:27 | Microsoft Print to PDF (Type: Print queues) | Connected (enabled) | Mikuz@DESKTOP-NOQNH11 on DESKTOP-NOQ... |
| 26.03.2020 | 23:30:27 | Microsoft OneNote (Type: Print queues) | Connected (enabled) | Mikuz@DESKTOP-NOQNH11 on DESKTOP-NOQ... |
| 26.03.2020 | 23:30:27 | Microsoft Fax (Type: Print queues) | Connected (enabled) | Mikuz@DESKTOP-NOQNH11 on DESKTOP-NOQ... |
| 26.03.2020 | 23:30:27 | Microsoft XPS Document Writer (Type: Print queues) | Connected (enabled) | Mikuz@DESKTOP-NOQNH11 on DESKTOP-NOQ... |
| 26.03.2020 | 23:29:55 | Microsoft OneNote (Type: Print queues) | Disconnected when system was offline (enabled) | DESKTOP-NOQNH11, 192.168.0.108 |
| 26.03.2020 | 23:29:55 | Microsoft Print to PDF (Type: Print queues) | Disconnected when system was offline (enabled) | DESKTOP-NOQNH11, 192.168.0.108 |
| 26.03.2020 | 23:29:55 | Microsoft Fax (Type: Print queues) | Disconnected when system was offline (enabled) | DESKTOP-NOQNH11, 192.168.0.108 |
| 26.03.2020 | 23:29:54 | Microsoft XPS Document Writer (Type: Print queues) | Disconnected when system was offline (enabled) | DESKTOP-NOQNH11, 192.168.0.108 |
| 26.03.2020 | 15:18:42 | Microsoft Fax (przekierowana sesja: 2) (Type: Print queues) | Disconnected (enabled) | DESKTOP-NOQNH11, 192.168.0.108 |
| 26.03.2020 | 15:18:42 | Microsoft Print to PDF (przekierowana sesja: 2) (Type: Print queues) | Disconnected (enabled) | DESKTOP-NOQNH11, 192.168.0.108 |
| 26.03.2020 | 15:18:42 | Microsoft XPS Document Writer (przekierowana sesja: 2) (Type: Print queues) | Disconnected (enabled) | DESKTOP-NOQNH11, 192.168.0.108 |

Reviewing device access history can be also performed from the level of the **Manage trustees** window. To learn more, see section [Access log](#) ³²⁹.


9.9 Quick help – typical rights configuration scenario

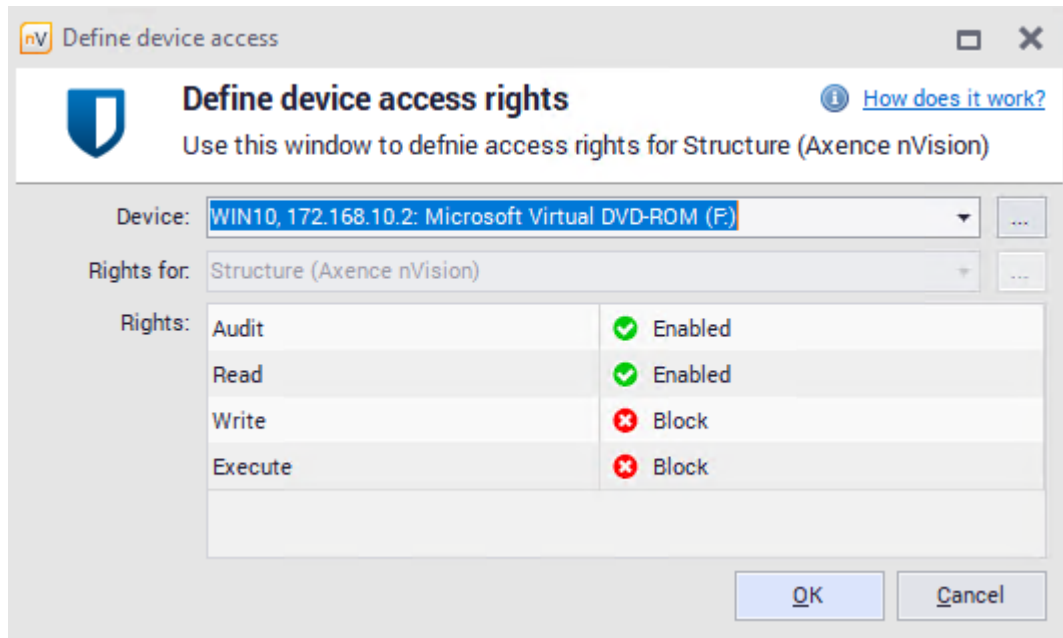
This section presents the scenario for setting access rights in a typical situation: operations on undefined USB devices are blocked (in particular, writing to files and executing files), while extended rights are assigned to a specific device, in this case - a corporate flash drive. A corporate flash drive is used by a certain group of users (in the following example - a department represented by *Support* map), which allows the transfer of corporate data between the workstations.

Blocking the rights to write and execute for undefined USB devices

To set the rights for a USB device:

1. Right click Atlas (**Users** tab) and navigate to the **Atlas info** window.

2. Navigate to the **DataGuard** tab and select the device group **Other USB storage devices** marked with the  icon. Press **Enter** or double-click the selected row.
3. Set the access rights as shown in the following image and press **Enter**.



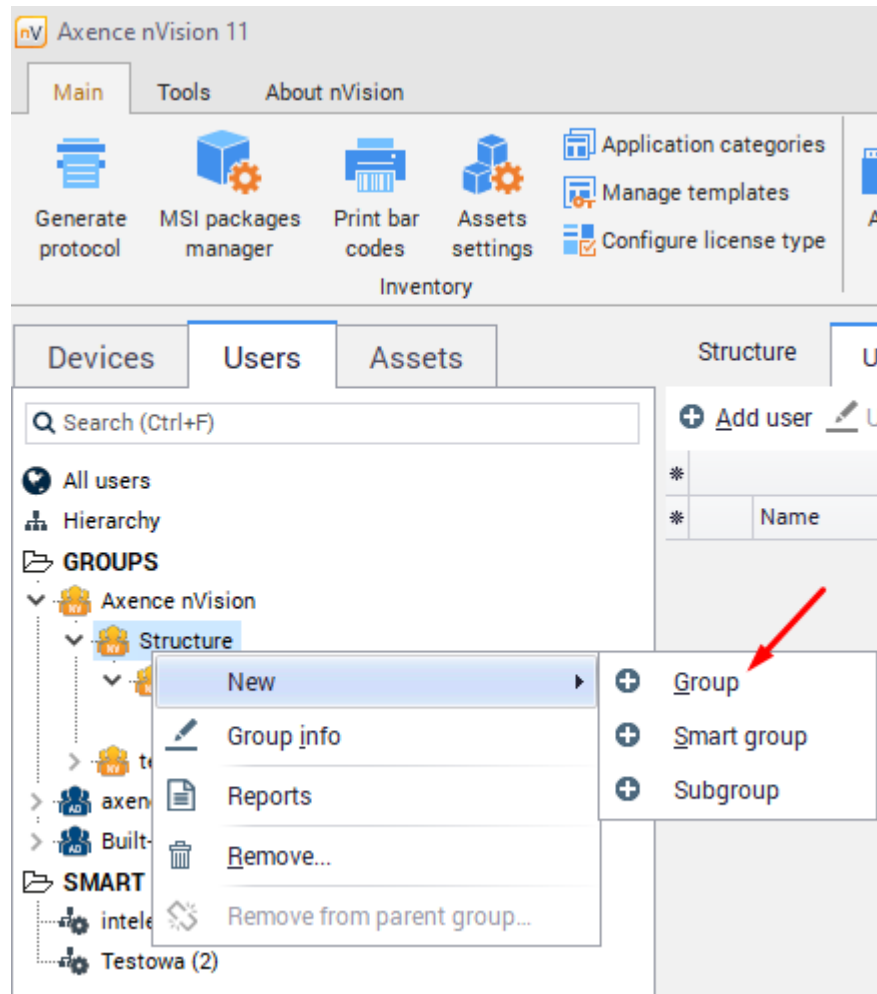
With such a configuration of rights, it is possible to read files from external media, but the ability to write data or run executables is blocked. If the audit is toggled on, users' actions related to external media are monitored, i.e. the information on read files and writing/execution attempts are collected. The connecting and disconnecting of an external device is always monitored, regardless of the audit option setting.

Creating a map of users utilizing the corporate flash drive

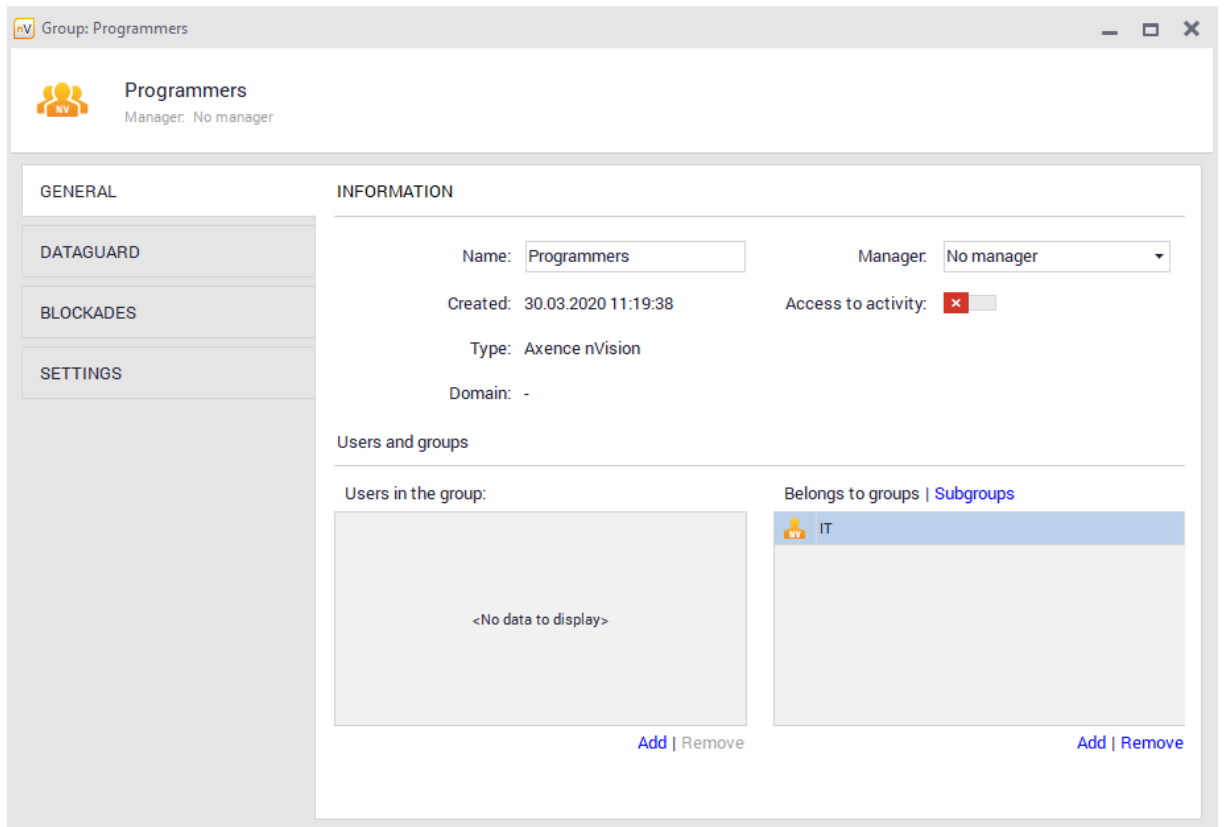
If the corporate flash drive is available for a certain department or user group, creating a group enabling the easy management of access rights for these users is recommended.

To create a group:

1. Right click the selected group or folder and select **New / Group** option.



2. Click the caption or use the **Properties** option to assign a name to the created map.
To add a group to another (parent) group, navigate to its properties.



The next step is to copy the appropriate users to the created group. For this purpose, just select the users and drag them to the appropriate group.

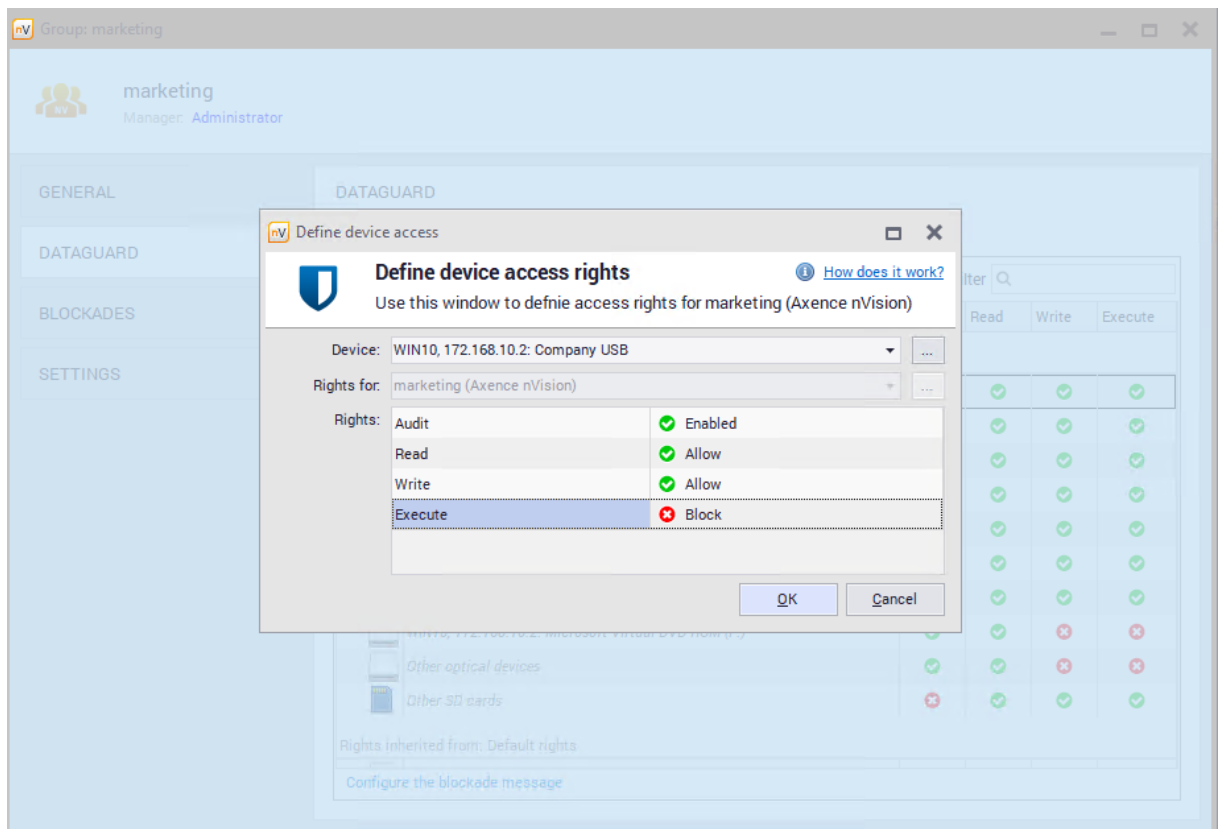
Setting rights for a corporate flash drive

A corporate flash drive allows data to be transferred within a certain group of users. Therefore, file reading and writing are allowed for the given device. Program execution is still blocked to prevent the distribution of viruses. The enabled audit allows all operations performed on the given USB drive to be monitored.

To set the access rights for a USB device:

1. In nVision's main toolbar, select the **Manage trustees** option from the DataGuard section.
2. Click the **Add access rights** button and select the corporate flash drive from the list.
3. Set the access rights as shown in the following image and press **Enter**.


Now users belonging to the Marketing group can read and write data from the Corporate Flash Disk" device.

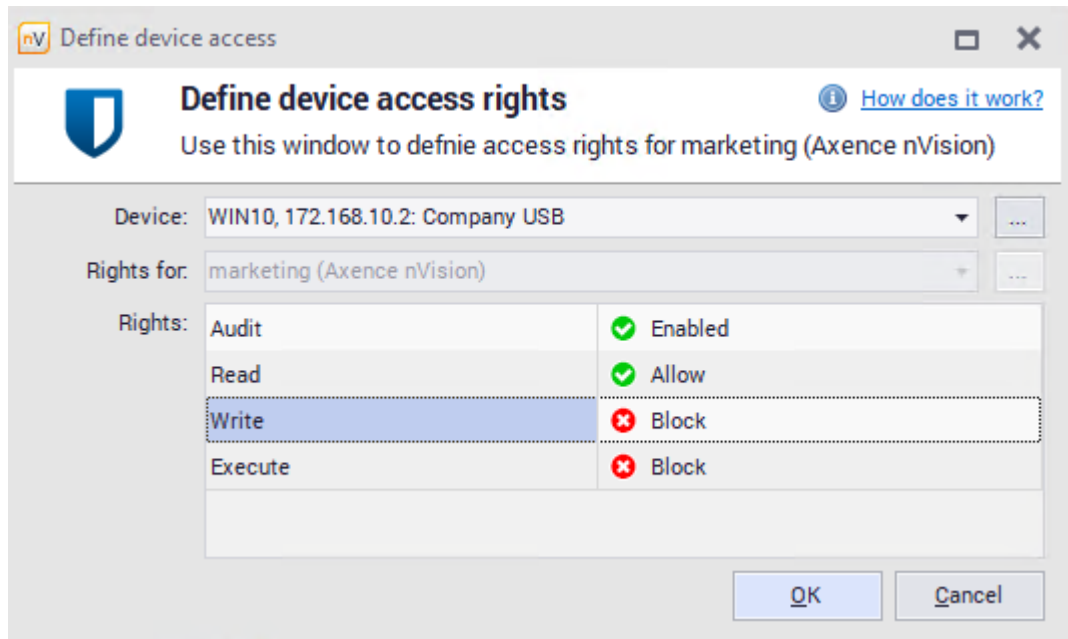


9.10 Quick help – setting default access rights to USB devices


A frequent cause of infecting computers with viruses is the distribution of malware via flash drives. These devices are started up automatically, which allows for the proliferation of viruses. The second factor posing a potential threat is the ability to copy sensitive data and carry it outside of the company on a USB flash drive. The DataGuard module ensures protection against those threats.

To block the ability to write and execute files on all USB devices (except for those for which the access rights were defined individually) for the entire atlas, i.e. for all users:

1. Right click Atlas (**Users** tab) and navigate to the **Atlas info** window.
2. Navigate to the **DataGuard** tab and select the device group **Other USB storage devices** marked with the  icon. Press **Enter** or double-click the selected row.
3. Set the access rights as shown in the following image and press **Enter**.



To set the default rights for specific groups and users or to check their settings:


1. In nVision's main toolbar, select the **Manage trustees** option from the DataGuard section.
2. Use the list to select the group or user for which the changes will apply.
3. Select the device group **Other USB storage devices** marked with the  icon. Press **Enter** or double-click the selected row.

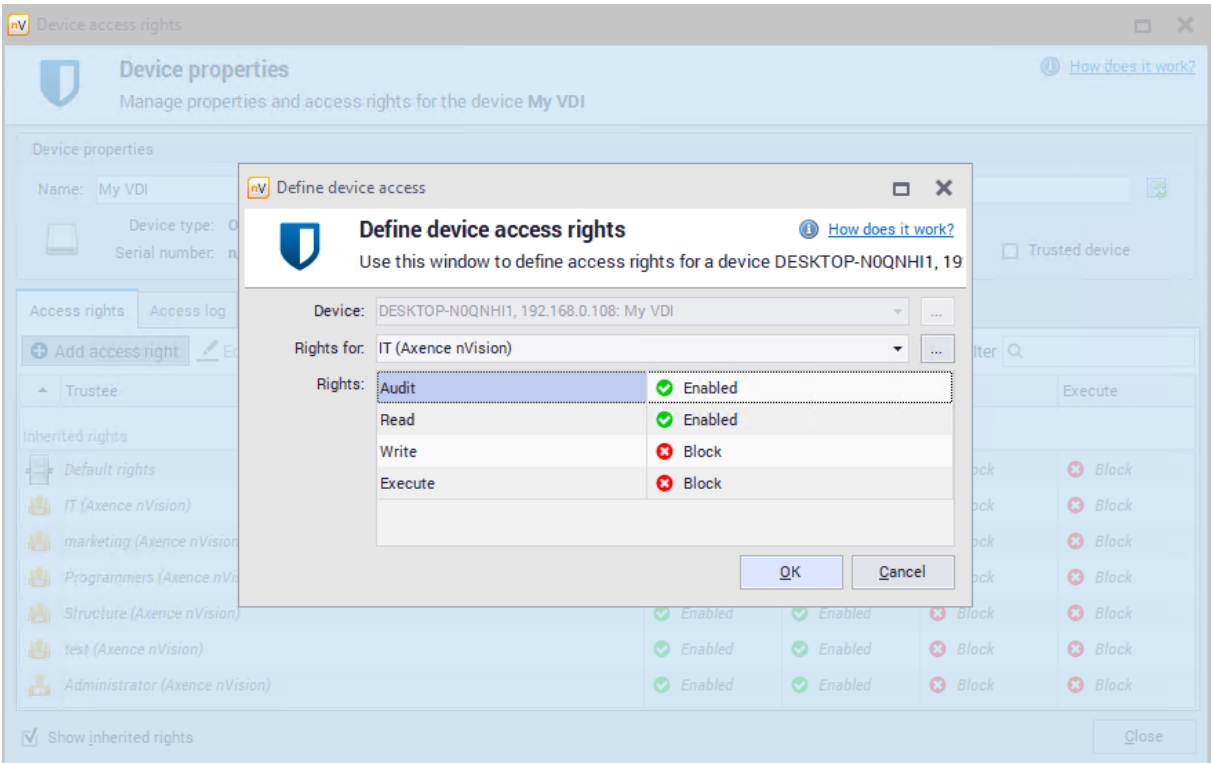
If a user connects a blocked device, a pop-up with a notification about blocking will be displayed from the Agent icon.

To learn more about flash drive blocking and setting access rights for specific devices detected by nVision, see section [How to set the access rights to USB media?](#)³⁴⁴.

9.11 Setting default access rights to USB devices

To block the ability to write and run files from a specific USB flash drive detected by nVision:

1. Click the **Connected devices** button located in the DataGuard section in the main toolbar.
2. Select the detected flash drive to be blocked in the list.
3. Click the  **Add access right** button.
4. Use the list to select the user, group or atlas for which the access rights will be set, and block it as presented in the image below. Press **Enter**.



For more information on setting default access rights to USB flash drives, see section [Quick Help – setting default access rights to USB devices](#)³⁴³.

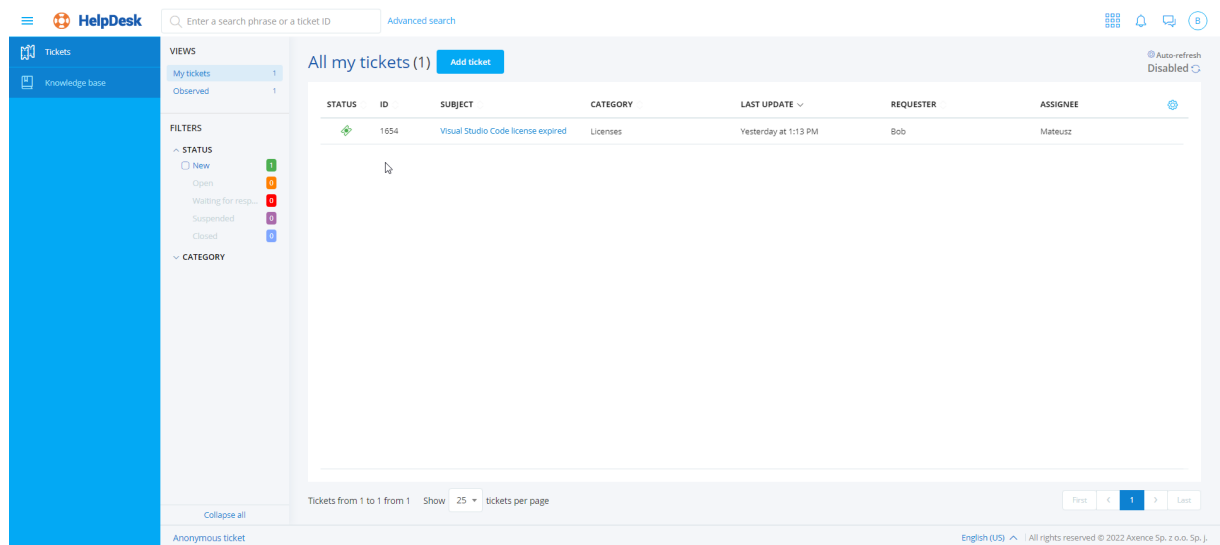
Part



10 HelpDesk module

10.1 Introduction

HelpDesk module provides the users with an interactive trouble ticket database, which simplifies reporting and solving problems. Moreover, the database is expanded on an ongoing basis with subsequent technical issues and the related histories of how issues have been solved, thus becoming a valuable knowledge base both for users and technical support employees.



HelpDesk interface

- The trouble ticket database allows the users to report their technical issues with the use of the trouble ticket creation mechanism. Trouble tickets can be created both by users with an installed Agent and without (after logging in or by e-mail).
- The trouble tickets are solved by HelpDesk employees.
- In the part for Administrators and HelpDesk employees, the incoming trouble tickets are processed and assigned to the appropriate person who receives notifications about the delegated problem which requires solving.
- A User can monitor the solving of the reported issue and its current status, as well as exchange information with the administrator, by means of comments, which can be entered and read by both parties.
- The knowledge base is a space where Administrators and HelpDesk employees can publish articles describing the procedures which have been used in a given organization and the most common issues and their solutions.

An example of the view of the trouble ticket database from the Administrator level is presented above.

Related topics

 [HelpDesk module configuration](#)

 [Settings](#)

 [Starting the HelpDesk interface](#)

 [Main views](#)

 [Announcements](#)

 [File distribution](#) 

10.2 Management and configuration

10.2.1 Configuration

To start using the HelpDesk module, enable and configure the following settings in the main nVision window.

HelpDesk access configuration

To run the HelpDesk functionality, first enable access to this module in nVision:

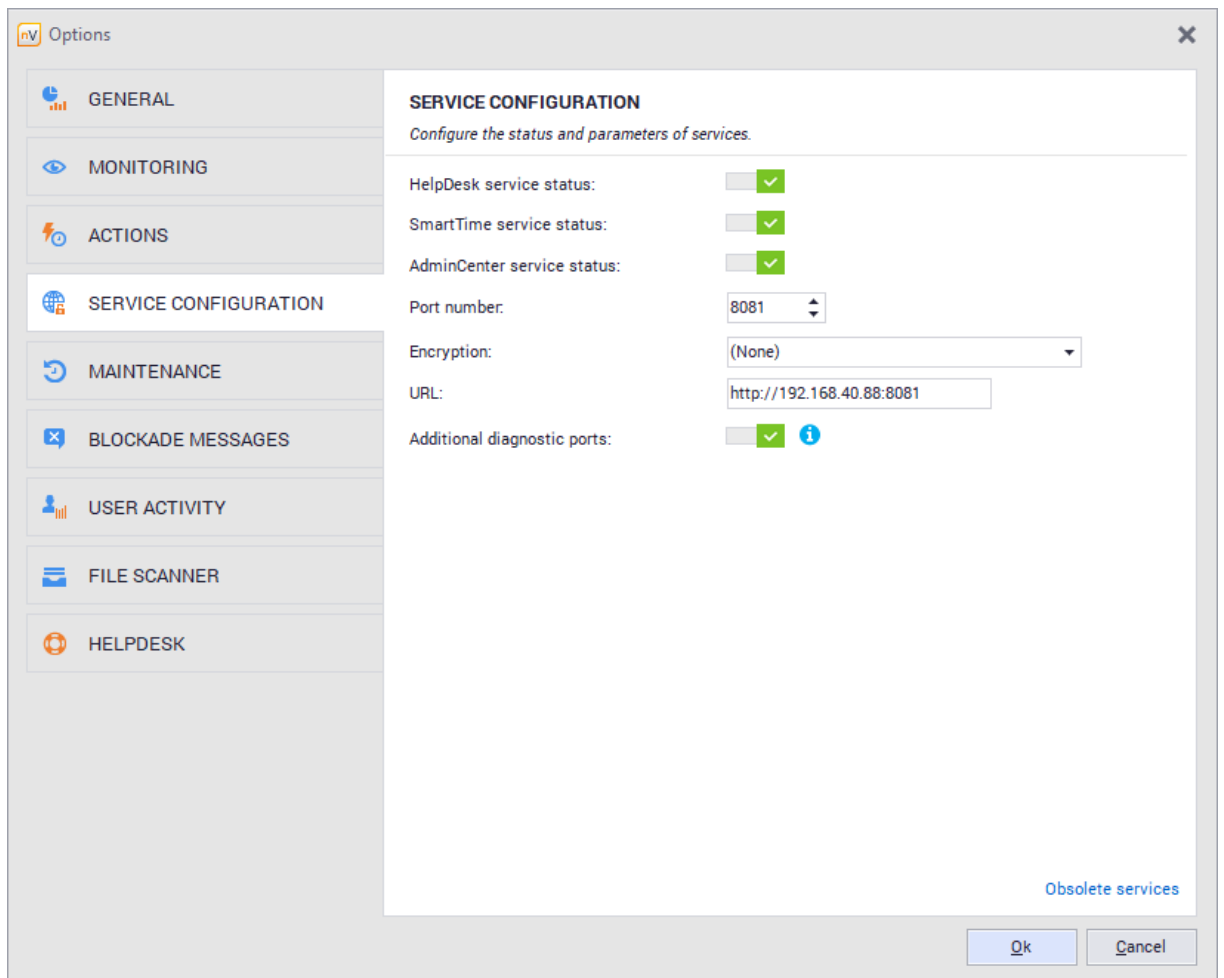
1. Click the **Main** tab in the nVision console.
2. Click the **Options** button.
3. Click the **Service Configuration** section.
4. Click the **Helpdesk Status** slider.

In addition, enter the port number under which the HelpDesk is to operate and the URL with the port number under which the HelpDesk will be accessible for the Agents.

URL is the IP address of the nVision Server where the HelpDesk runs. **Important:** replace **localhost** with the appropriate URL of the nVision Server, e.g. 192.168.0.100:8081 in the local network.

Related topics

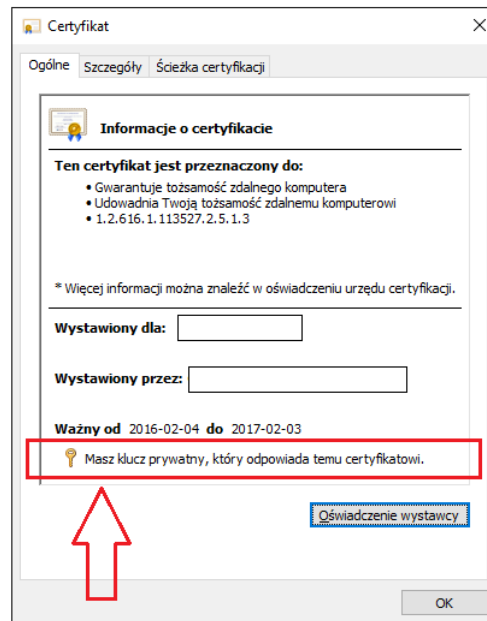
 [How to access nVision via Web browser?](#) 



10.2.2 HTTPS access

Requirements:

- An up-to-date certificate issued for the domain, where the HelpDesk is available, is a necessary prerequisite.
- The certificate must include a private key:



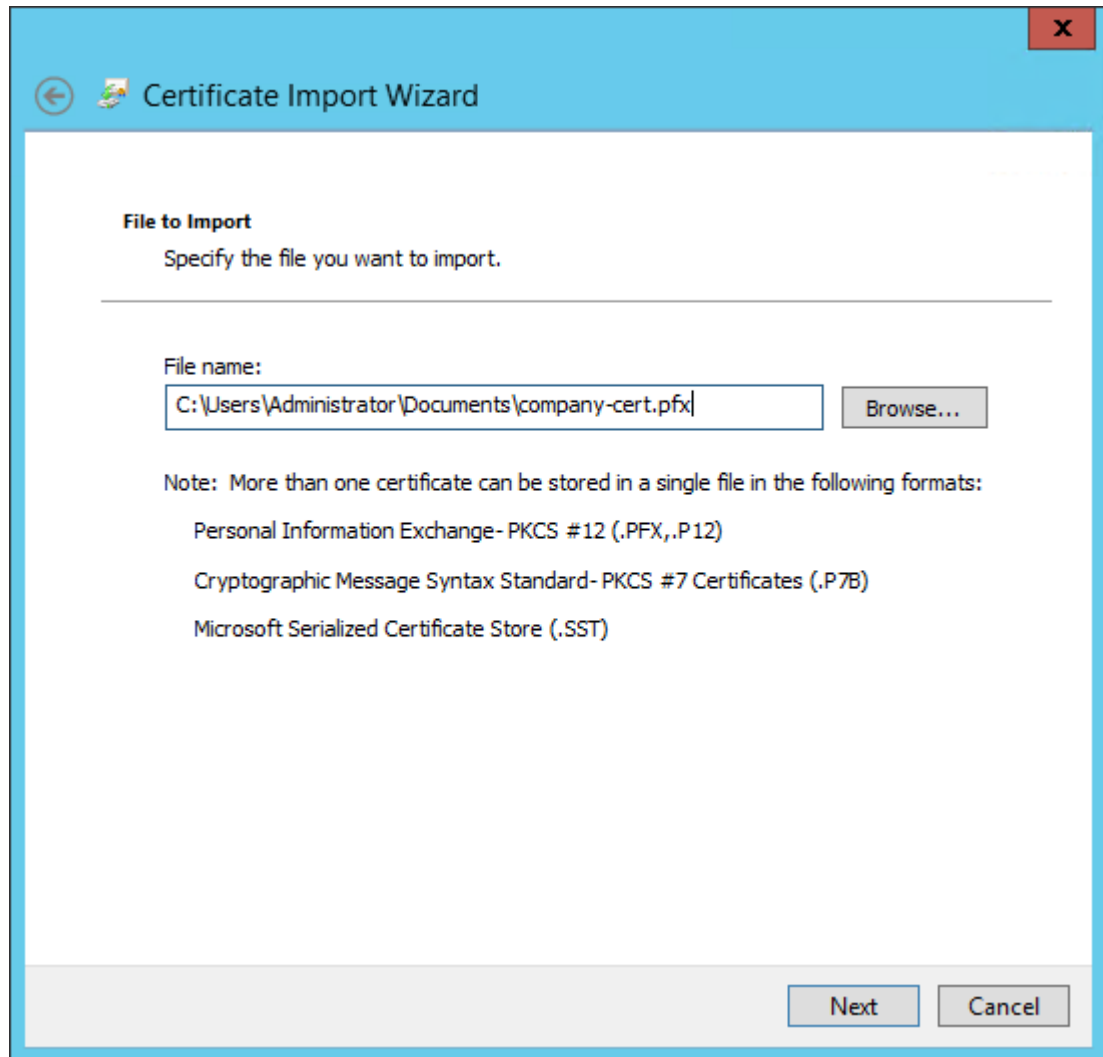
- The certificate must be installed in the personal certificate store of the server where Axence nVision® is installed (System Certificate Store / Local Machine / Personal). A certificate installed in the user store cannot be used to configure encrypted access to the HelpDesk.

How to install a certificate

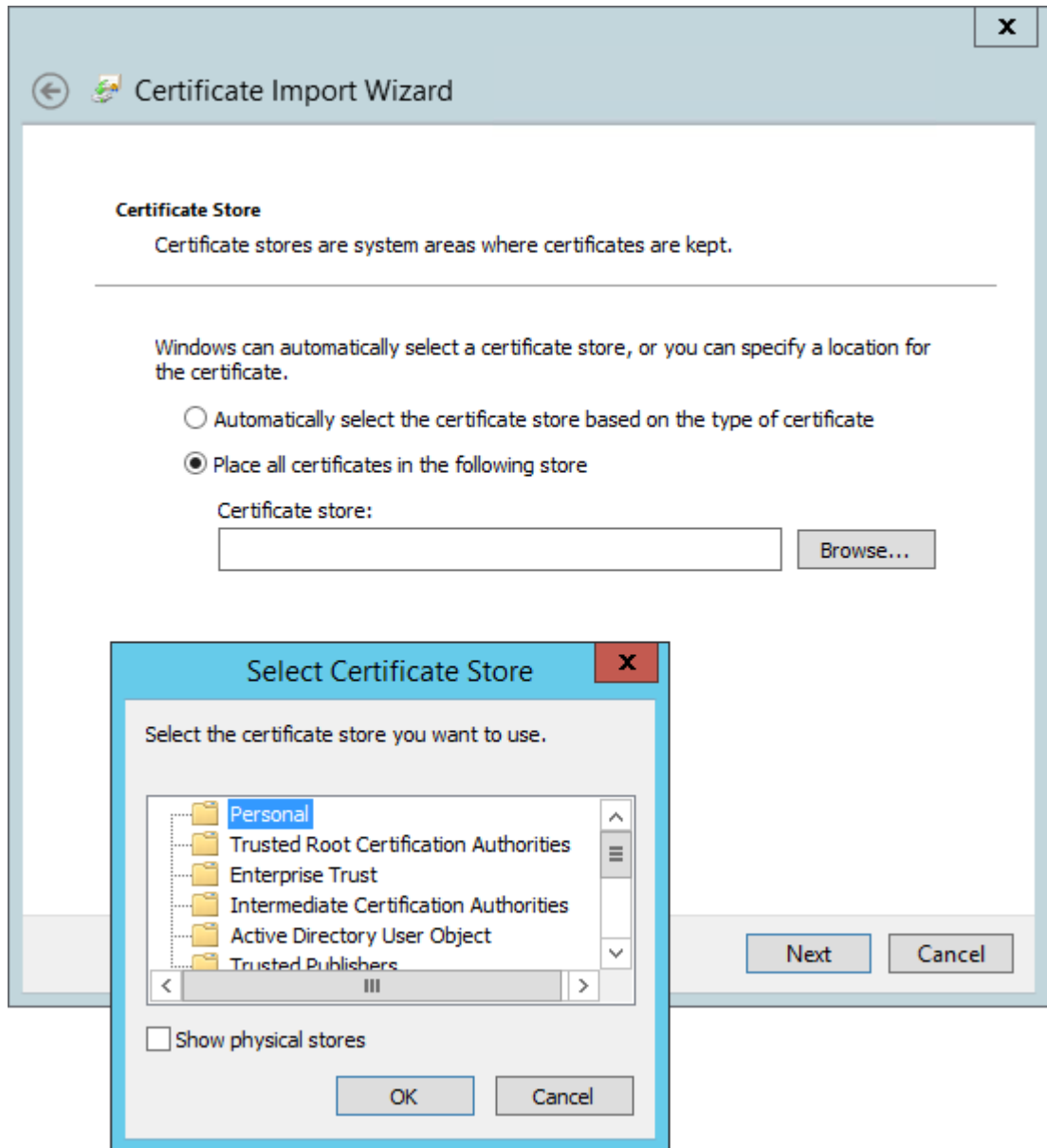
1. Double-click the certificate file. The window as shown below will open. Chose local machine and click the **Next** button:



2. Choose certificate-file path. Click the **Next** button,

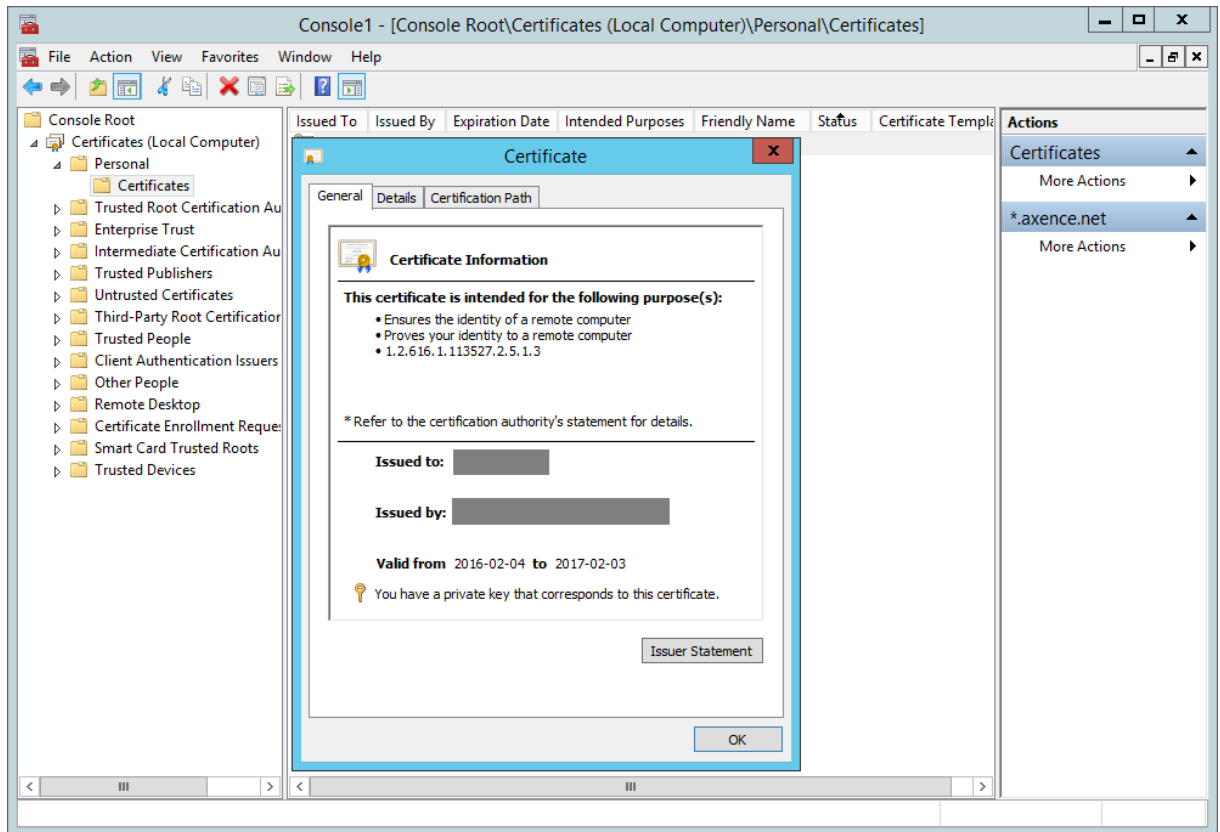


3. Choose Personal from certificate stores list:



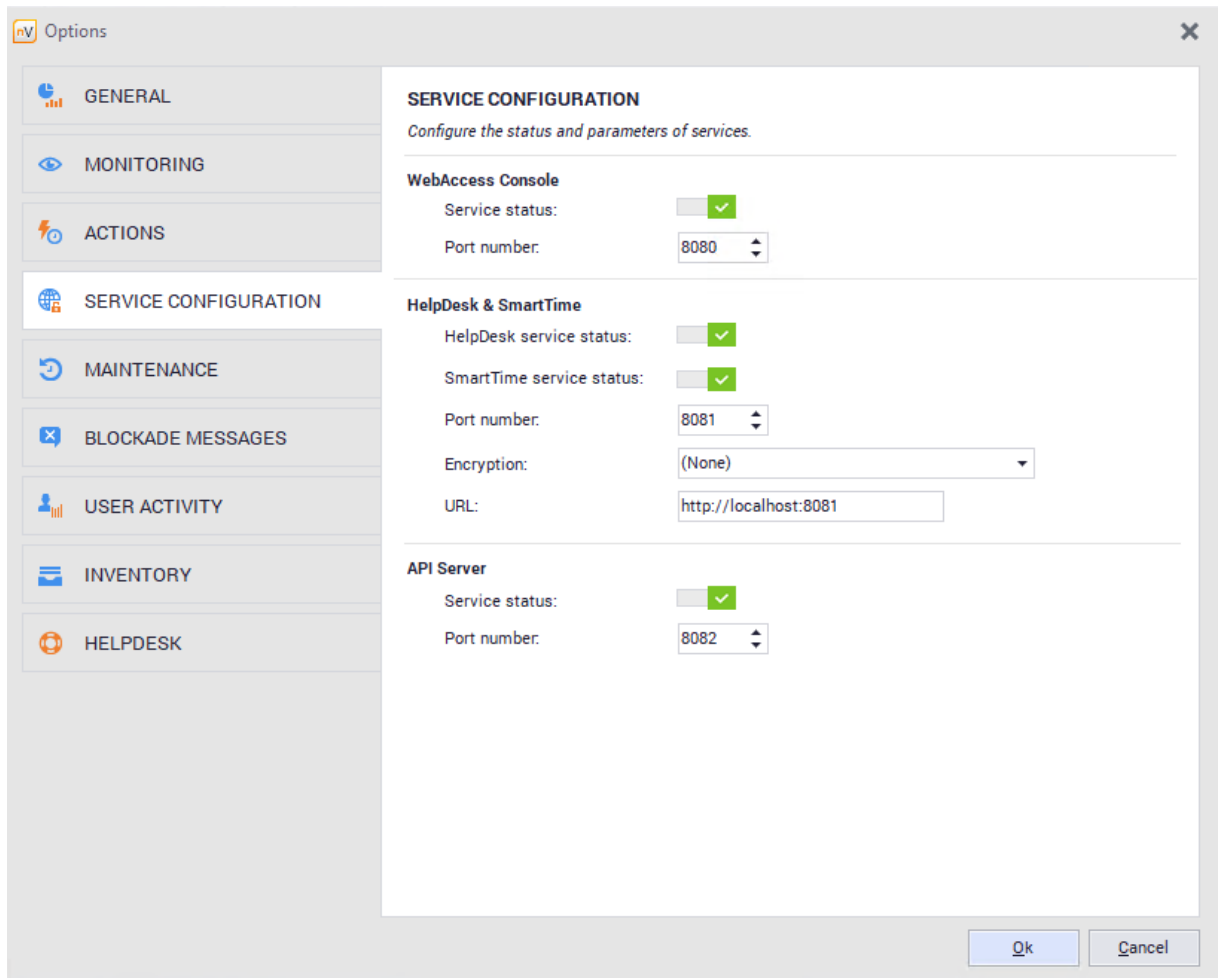
4. In order to verify the certificate:

```
launch: mmc.exe  
File \ Add/Remove snap-in ... \ Certificates \ Add \ Computer account \  
Local computer \ Finish
```

To configure secure access to the HelpDesk, navigate to nVision and remote access settings in the menu: **Tools / Options / Remote web access**.

In the **HelpDesk** section, use the **Encryption** list to select the certificates installed on the server:



After the certificate has been specified, the URL address of the HelpDesk will be automatically changed to `https://FQDN:port` – you have to configure FQDN to suit it to the actual DNS name (for which the certificate was issued) – preferably then copy the URL and see if it opens in the browser. If the test pass with success, then you can accept the **Options** window by clicking [OK] button and the URL will be sent to Agents.

10.2.3 Settings

In order to manage the HelpDesk settings, in the main nVision window expand the menu and enter **Configuration, HelpDesk** tab.

Settings are located in two groups:

- Core settings
- Ticket processing

| Field | Description |
|--------------|---|
| Custom title | Enter the text to be displayed on the HelpDesk module login window. You can also choose a logo by selecting an image from the disk. |

| Field | Description |
|---------------------------|---|
| Custom logo | Allows to download the graphics to be displayed as a logo on the HelpDesk interface. |
| Account self-registration | Users of the module can create accounts on their own by checking the field. Alternatively, the accounts can be created directly by the administrator. |
| Account activation mode | Active fields, if the users can create accounts on their own. Activation can be performed in one of the following ways: <ul style="list-style-type: none"> • None – the account is active once it has been created by the user. • Activation e-mail – to activate, click the link sent in an e-mail. This option allows the e-mail address given by the user to be verified. • Administrator activation – the account must be activated in nVision under the Users icon by checking the “Account activated” field in the respective line. |

HelpDesk chat

Check the field to enable the chat feature in nVision HelpDesk.

The screenshot shows the 'nV Options' dialog box with the 'HELPDESK' section selected in the left sidebar. The main area is titled 'HELPDESK' and contains the following settings:

- HelpDesk name:** A text field containing 'Axence nVision HelpDesk'. Below it is an information icon and the text 'It will be displayed on title bar in web browser.'
- Custom logo:** A section with a plus icon and a trash icon, and a preview image of the 'HelpDesk' logo.
- Account self-registration:** A checkbox that is checked.
- Account activation mode:** Three radio button options: 'Manual activation by administrator', 'Send activation e-mail' (which is selected), and 'No needed'.
- HelpDesk chat:** A checkbox that is checked.
- See also:** A link labeled 'Configure URL adress for HelpDesk'.

At the bottom right of the dialog box are 'Ok' and 'Cancel' buttons.

Related topics

 [Management and configuration](#)

 [User management](#)

 [User registration](#)

 [HelpDesk interface](#) ³⁶⁹

10.2.4 E-mail settings

The HelpDesk module can automatically send e-mail messages about new trouble tickets and changes in tickets, and can also process the users' trouble tickets sent to the defined e-mail address.

Action-related notifications

The default option, **Options / HelpDesk / Ticket processing | Use nVision e-mail action for sending notifications about changes in tickets**, enables e-mail notifications to be sent according to action settings.

To change [action](#) ⁶⁰⁴ settings, open **Tools and options / Manage actions**.

E-mail processing in HelpDesk

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 trouble tickets without access to the HelpDesk trouble ticket database. In order for the tickets to be processed, the requester must have a unique e-mail address assigned to their account in nVision.

To use HelpDesk settings for e-mail processing:

1. Open the **Options / HelpDesk / Ticket processing** option.
2. Select the **Use external e-mail account for processing tickets** option.
3. Define the **E-mail address** where the trouble reports should be sent (address of the mailbox in which nVision HelpDesk will detect messages and use them as a basis to create a ticket).
4. Configure the incoming and outgoing mail server settings. To test the entered settings, click the **Test connection** button.

The screenshot shows the 'Options' dialog box for the nV system, specifically the 'HELPDESK' tab. The left sidebar contains a navigation menu with the following items: GENERAL, MONITORING, ACTIONS, SERVICE CONFIGURATION, MAINTENANCE, BLOCKADE MESSAGES, USER ACTIVITY, INVENTORY, HELPDESK, CORE SETTINGS, and TICKET PROCESSING. The main content area is titled 'HELPDESK' and includes the following sections:

- HELPDESK**
Configure notifications and ticket processing.
- Ticket processing**
 - Use Axence nVision e-mail action for sending notifications about changes in tickets.
 - i** You can configure e-mail action under [actions tab](#).
 - Use external e-mail account for processing tickets:**
 - i** This option allows processing incoming e-mail messages as tickets in helpdesk. It provides e-mail notifications about changes in tickets.
- E-mail address:
- Incoming mail server** (IMAP4)
 - i** For creating new tickets based on e-mail messages.
 - Server:
 - Encryption: Port:
 - User name: Password:
 -
- Outgoing mail server (SMTP)**
 - i** For sending e-mail notification about changes made in tickets.
 - Server:
 - Encryption: Port:
 - User name: Password:
 -

At the bottom right of the dialog box are 'Ok' and 'Cancel' buttons.

Note!

All messages in the inbox of the e-mail address provided will be deleted! Create an account dedicated to ticket processing.

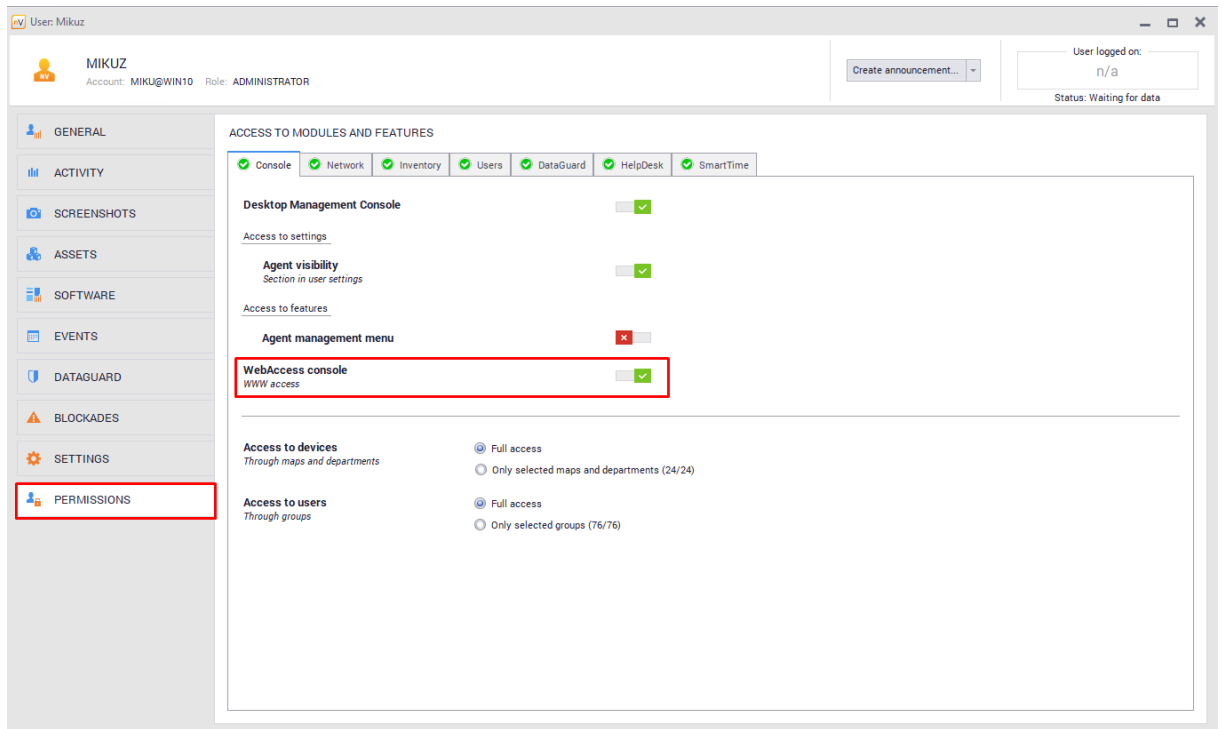
Related topics

 [Actions](#)

 [Management and configuration](#) ³⁴⁹

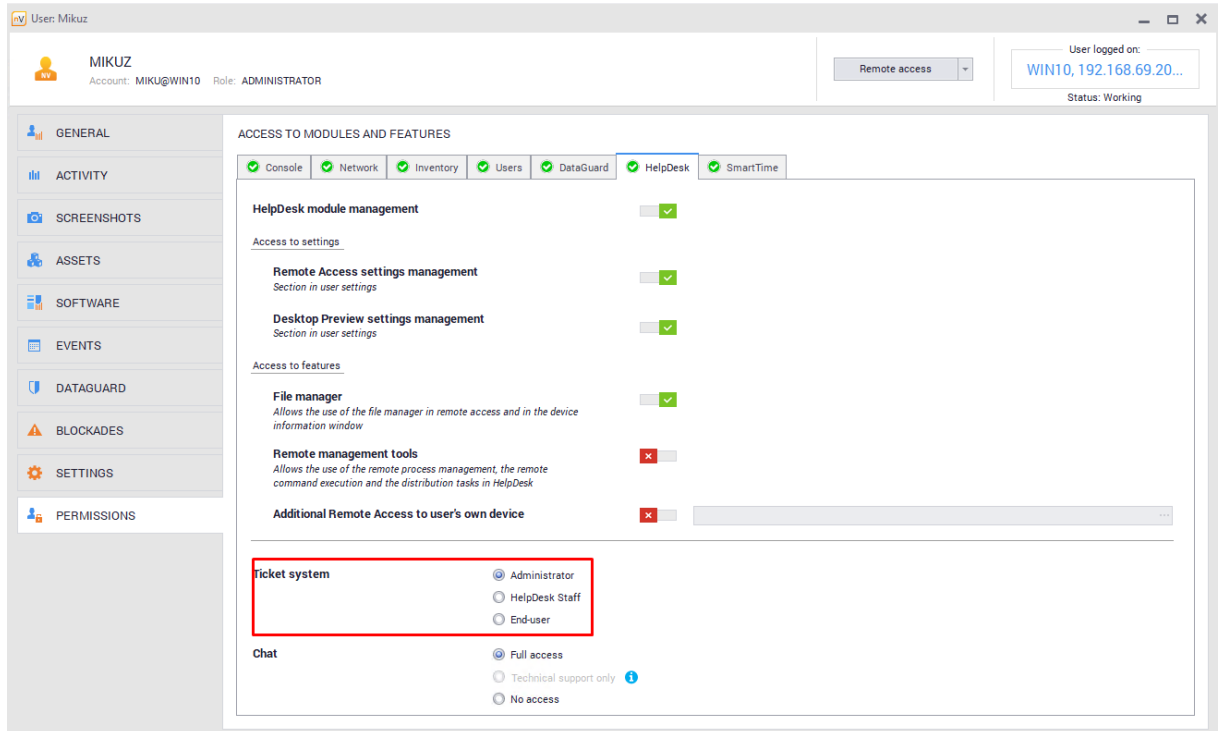
10.2.5 User management

Management of HelpDesk users is performed from the level of the **User info** window in nVision.



User types – roles in HelpDesk system


The user role can be changed in the user information window, using **Permissions / HelpDesk** tab:



| Type | Description |
|-----------------|--|
| End-user | Can create, edit and close tickets. Can see the articles published in the knowledge base and own tickets. |
| Help-Desk Staff | People who provide assistance. In addition to the above rights, they can change ticket status, delegate a ticket and remotely access the computer from which the ticket originated. They can also have assigned branches and trouble tickets from these branches will be automatically assigned to these people. |
| Administrator | A user of this type has the most extensive rights, can see and edit all tickets and options. Can manage messages and priorities, and is the only one who can send messages (described in section Messages ^[473]). The user also has all of the rights described above. |

Account creation

Accounts can be created in a few ways:

- manually via the Administrator in nVision (all types) – in the **Users** window, after clicking the **Add** button, 
- via the Administrator by downloading the account list from Active Directory controller – in the **Users** window, after clicking the **Active Directory controllers** button and configuring the domain controller,
- independently by the users (only “End-user” type) without additional account activation, with activation via e-mail, or with manual activation via the Administrator.

For more information on possible user account creation scenarios, see section [User registration](#)^[371].

User data change

To change user data (e.g. in order to set up a new password):

- In the **Users** window, double-click the line of the user to be edited.
- Enter the new user data and close the window.

Note: Names and e-mail addresses of users of all types must be unique.

Related topics

 [Settings](#)

 [User registration](#)

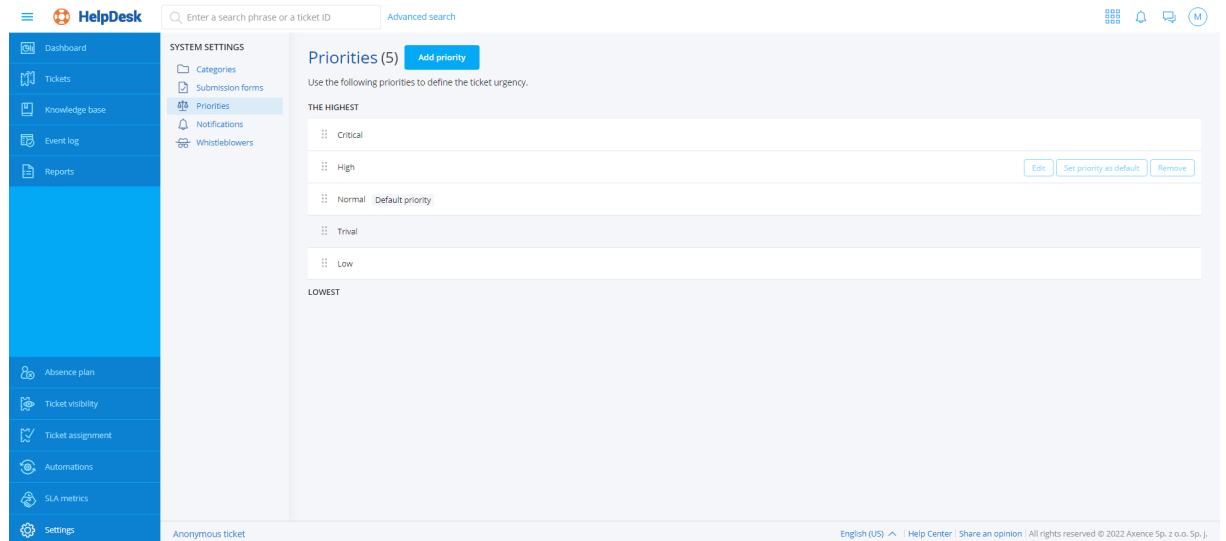
 [Management and configuration](#)^[349]

10.2.6 Priorities

Priorities allow the specification of the severity of the reported issue. The Administrator can manage the existing priorities and add new ones. When creating a ticket, User cannot select a priority - only Administrators and HelpDesk Employees may change this field. It is recommended to precede the

names with digits, setting the priorities in ascending or descending order, so that after alphabetical sorting, their order of importance can be still easily identified.

Note: exactly one default priority must exist at all times and cannot be deleted.



Priorities are managed from the level of the HelpDesk web interface.

To create a new priority:

1. Go to **Settings / Priorities** tab.
2. Click **Add priority** button.
3. Enter a new unique priority name and click **Add priority**.

To edit a priority:

1. Go to **Settings / Priorities** tab.
2. Select **Edit** option for the priority you want to edit.
3. Enter the new priority name and click **Save changes**.

To change the default priority:

1. Go to **Settings / Priorities** tab.
2. Select the **Set priority as default** option for the priority which should be the default one.
3. Click the **Set as default** button.

To delete a priority:

1. Go to **Settings / Priorities** tab.
2. Select the **Remove** option for the priority to be deleted.
3. Confirm the priority deletion by clicking **Remove priority**.

Related topics

 [HelpDesk](#)

 [Adding a ticket](#) ³⁸⁵

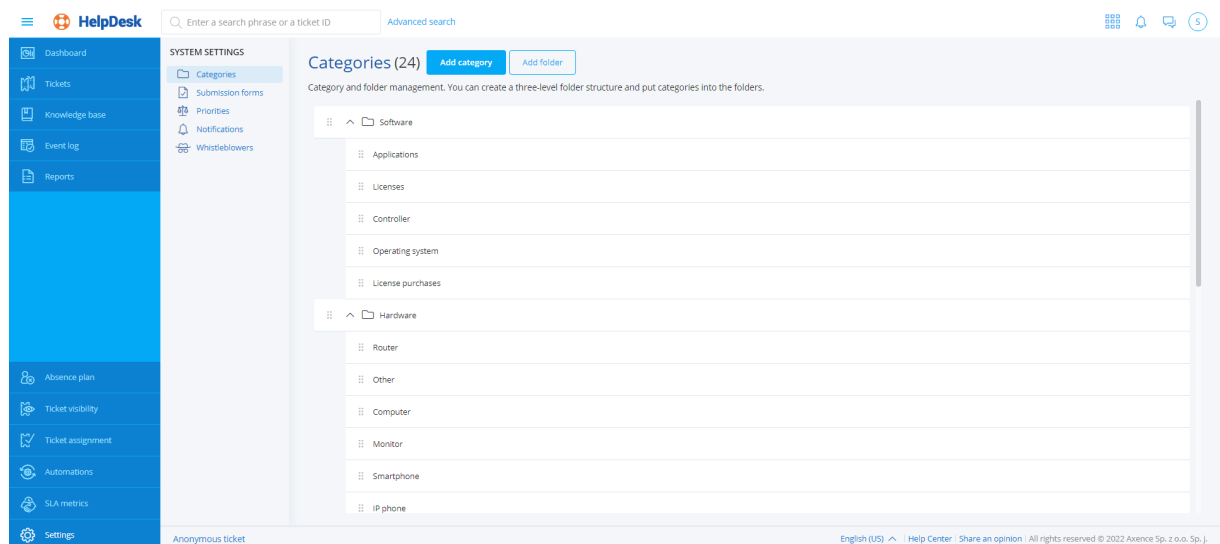
10.2.7 Categories and folders

Categories and folders enable tickets and articles to be assigned to the issue types they belong to. For instance, the Administrator can create the “Network” folder and include categories related to network access issues, software issues, hardware issues, etc. in this folder.

While creating a trouble ticket, the user selects the existing category which best suits their problem from the list. At the beginning, only one category, **Default**, is available.

Folders are used for the further categorization of tickets. They allow the creation of visually separated groups to which you can add categories.

Note: there must be exactly one default category in the HelpDesk. The default category cannot be deleted.



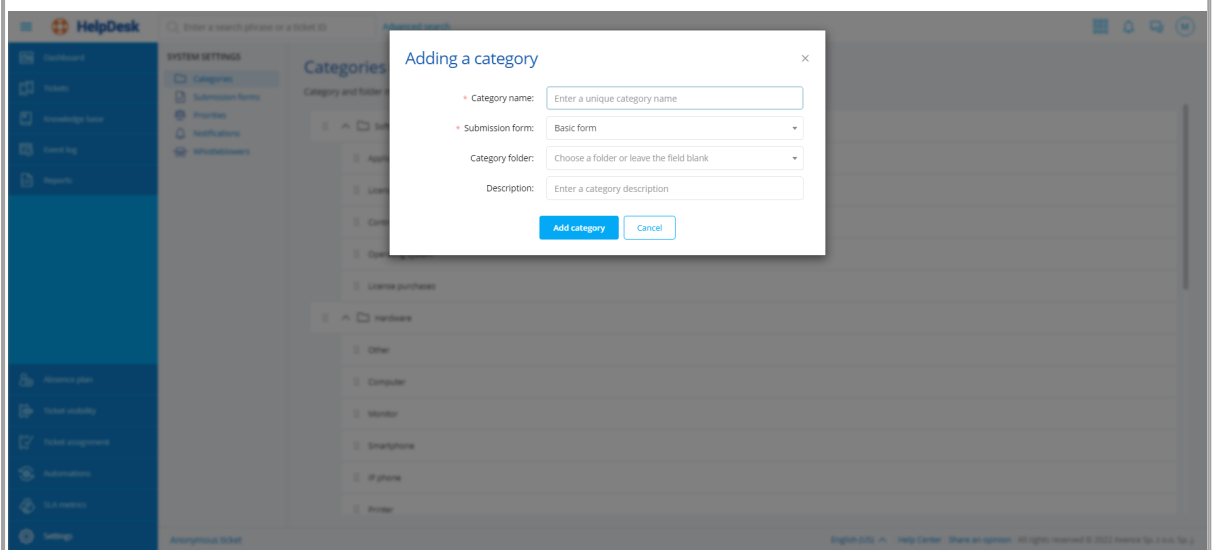
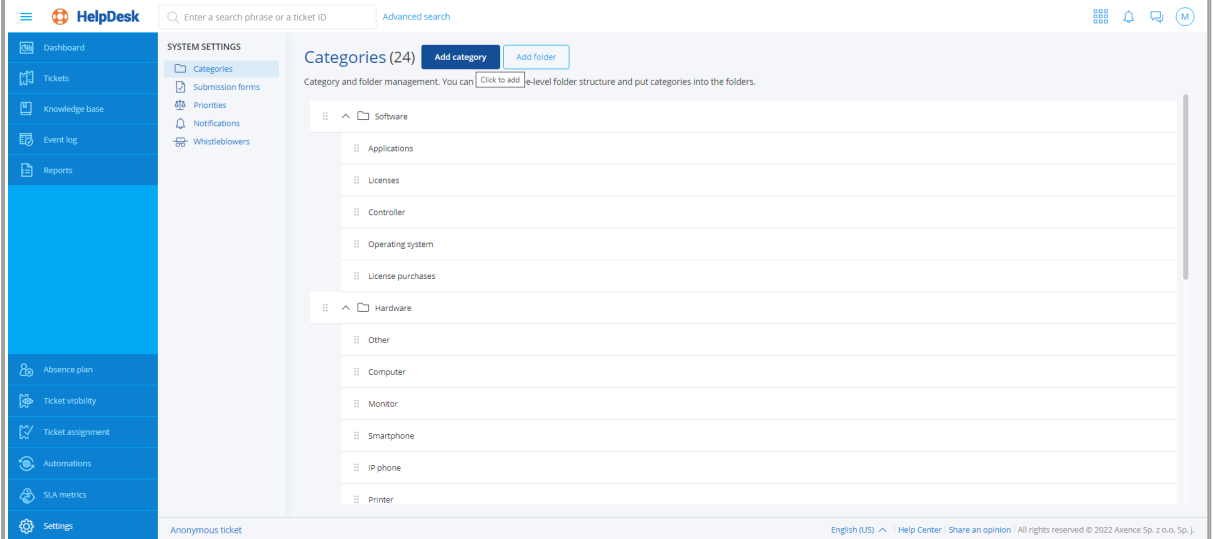
Category management options

Adding categories

To add a category, log in to the HelpDesk module as the Administrator and then:

1. In the flyout menu on the left side of the window, click the **Settings**.
2. Display the category settings by clicking the **Categories** button (optionally - it should be displayed by default when you click the Settings).
3. Click the **Add category** button.
4. Enter the unique category name in the **Category name** field (there cannot be two categories with the same name in the HelpDesk).
5. Select the appropriate **Trouble ticket form** from the list (by default, it is the Basic form).

6. Select the category folder from the list (optionally).
7. Enter the category description in the Description field (optionally).
8. Click the **Add category** button.



Editing categories

To edit a category, log in to the HelpDesk module as the Administrator and then:

1. In the flyout menu on the left side of the window, click the **Settings**.
2. Display the category settings by clicking the **Categories** button (optionally - it should be displayed by default when you click the Settings).
3. Hover over the category you want to edit and then click the **Edit** button.
4. Enter the unique category name in the **Category name** field (there cannot be two categories with the same name in the HelpDesk).
5. Select the appropriate **Trouble ticket form** from the list (by default, it is the Basic form).
6. Select the category folder from the list (optionally).
7. Enter the category description in the Description field (optionally).

8. Click the **Add category** button.

The screenshot displays the HelpDesk 'Categories' management page. The left sidebar contains navigation options like Dashboard, Tickets, Knowledge base, Event log, Reports, Absence plan, Ticket visibility, Ticket assignment, Automations, SLA metrics, and Settings. The main content area shows 'Categories (24)' with 'Add category' and 'Add folder' buttons. Below this, a tree view shows folders for 'Software' and 'Hardware'. Under 'Software', categories include Applications, Licenses, Controller, Operating system, and License purchases. Under 'Hardware', categories include Other, Computer, Monitor, Smartphone, IP phone, and Printer. A modal window titled 'Editing categories' is open, showing fields for 'Category name' (Controller), 'Submission form' (Basic form), 'Category folder' (Software), and 'Description'. The 'Save changes' button is highlighted.

Setting the default category

To set a category as the default one, log in to the HelpDesk module as the Administrator and then:

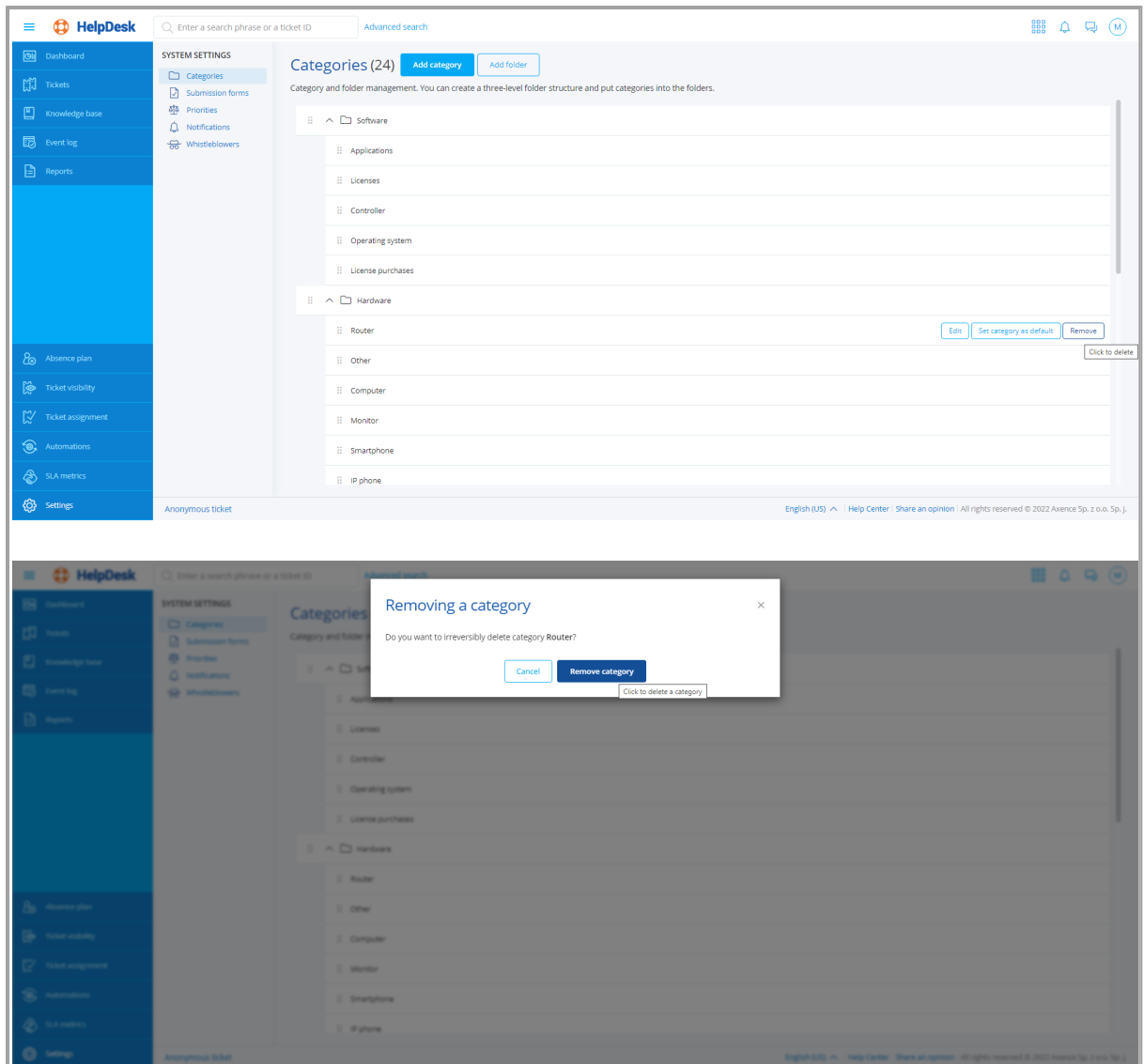
1. In the flyout menu on the left side of the window, click the **Settings**.
2. Display the category settings by clicking the **Categories** button (optionally - it should be displayed by default when you click the Settings).
3. Hover over the category you want to be the default category and then click the **Set category as default one** button.
4. In the Setting the default category window, click the **Set as default** button.

The screenshot displays the 'Categories (24)' management interface in the HelpDesk system. The left sidebar contains navigation options like Dashboard, Tickets, Knowledge base, and Settings. The main content area shows a tree view of categories. Under the 'Software' folder, categories include Applications, Licenses, Controller, Operating system, and License purchases. Under the 'Hardware' folder, categories include Other, Computer, Monitor, Smartphone, IP phone, and Printer. A modal dialog box is open, prompting the user to confirm setting 'License purchases' as the default category.

☰ Deleting a category

To delete a category, log in to the HelpDesk module as the Administrator and then:

1. In the flyout menu on the left side of the window, click the **Settings**.
2. Display the category settings by clicking the **Categories** button (optionally - it should be displayed by default when you click the Settings).
3. Hover over the category you want to edit and then click the **Delete** button.
4. In the category deletion window, click the **Delete** button.



The procedure of adding, editing or removing folders is similar.

It is also possible to assign HelpDesk- or Administrator-type users to a specific category, so the tickets of the given category are automatically forwarded to them. For more information see section [Assigning users to categories](#).

Category description in HelpDesk

In Axence nVision® version 13, the categories that appear in the HelpDesk have been expanded by adding the optional parameter named **Description**. The category description allows for the additional explanation of the specific category, which makes it much easier for the user to add a new trouble ticket, or, for instance, a GDPR clause or other useful information can be included in the description.

The category description in the HelpDesk is displayed in several forms, for instance

- a. as information that appears next to the category name and
- b. as a tooltip that appears when you hover over the relevant icon.

The category description may contain more than one character.

Examples of category description in the HelpDesk:

1. Category list in the Settings
2. Drop-down category list in the trouble ticket adding panel
3. Ticket list (with the table view configured accordingly)
4. Drop-down list in the browser

Related topics

 [HelpDesk](#) ³⁴⁸

 [Adding a ticket](#)

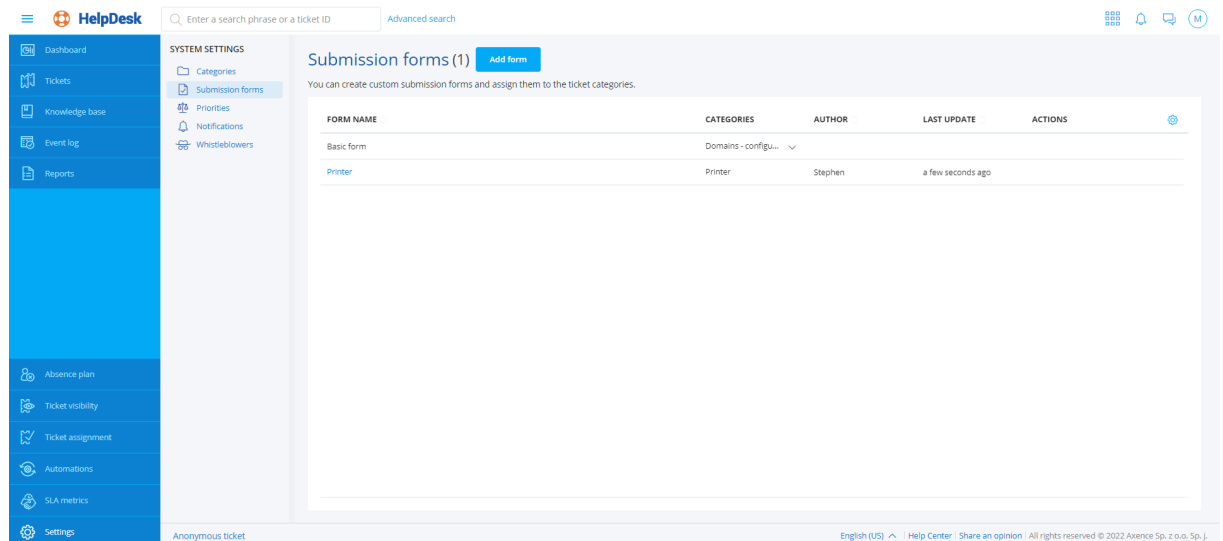
 [Adding an article](#) ⁴¹⁹

 [Configuring anonymous tickets](#)

10.2.8 Trouble ticket forms

Forms allow different scenarios to be configured upon creating a trouble ticket. When creating a trouble ticket, the user selects the category which is most applicable to the severity of the problem from the list. If the relevant trouble ticket form is assigned to this specific category in the system, the page will be updated to include additional fields that will facilitate the identification of a problem and its solution. The Administrator can manage the existing forms and add new ones.

Note: exactly one default priority must exist at all times and cannot be deleted.



The screenshot displays the 'Submission forms (1)' management page in the HelpDesk. The page includes a search bar, a navigation menu on the left, and a table of existing forms. The table has the following data:

| FORM NAME | CATEGORIES | AUTHOR | LAST UPDATE | ACTIONS |
|------------|----------------------|---------|-------------------|---------|
| Basic form | Domains - configu... | | | |
| Printer | Printer | Stephen | a few seconds ago | |

To create a new trouble ticket form:

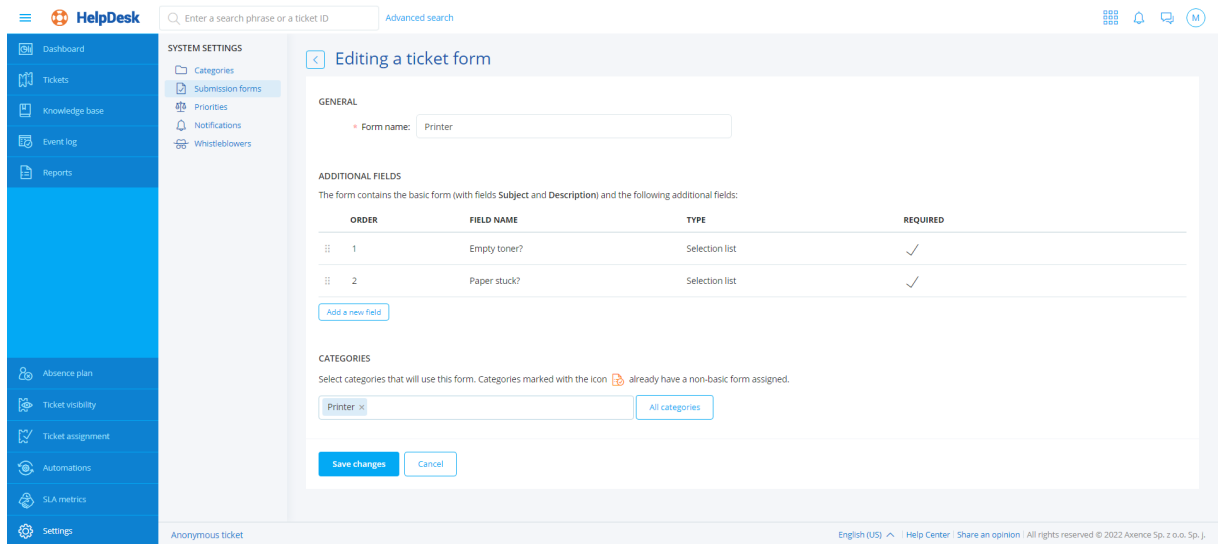
1. Go to the **Settings / Trouble ticket forms** tab.
2. Click the **Add form** button.
3. Enter the form name and specify the additional fields to appear when creating a trouble ticket.

The additional fields may take different types:

- text/numeric field,
- date,
- single- or multiple-selection list.

It is also possible to specify a default value, tips for the user or requirement for a specific field to send the ticket.

4. Select the categories in which this form will be used.



5. Click **Add form** to complete the adding of a new form.

To edit a trouble ticket form:

1. Go to the **Settings / Trouble ticket forms** tab.
2. Select **Edit** option for the form you want to edit.
3. Enter the new form name and modify the fields that you are interested in, then click **Save changes**.

To delete a trouble ticket form:

1. Go to the **Settings / Trouble ticket forms** tab.
2. Select the **Remove** option for the form to be deleted.
3. Confirm the form deletion by clicking **Remove priority**

10.3 HelpDesk interface

10.3.1 Starting the HelpDesk interface

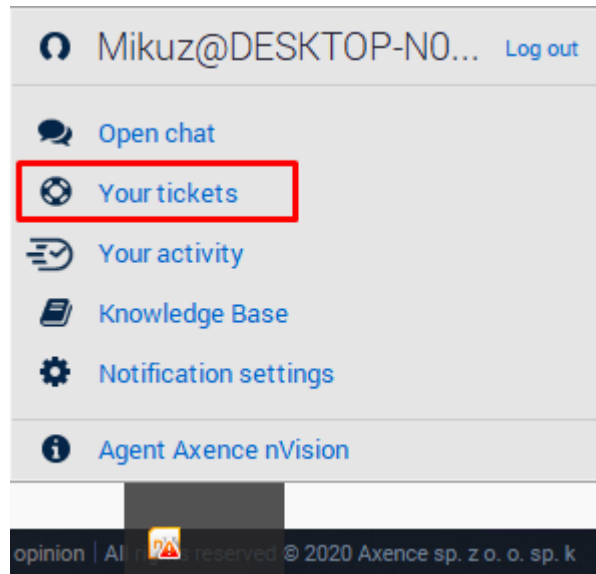
The HelpDesk interface can be started in several ways:

In the main nVision window

Click **HelpDesk**. The HelpDesk interface will be opened in the default browser.

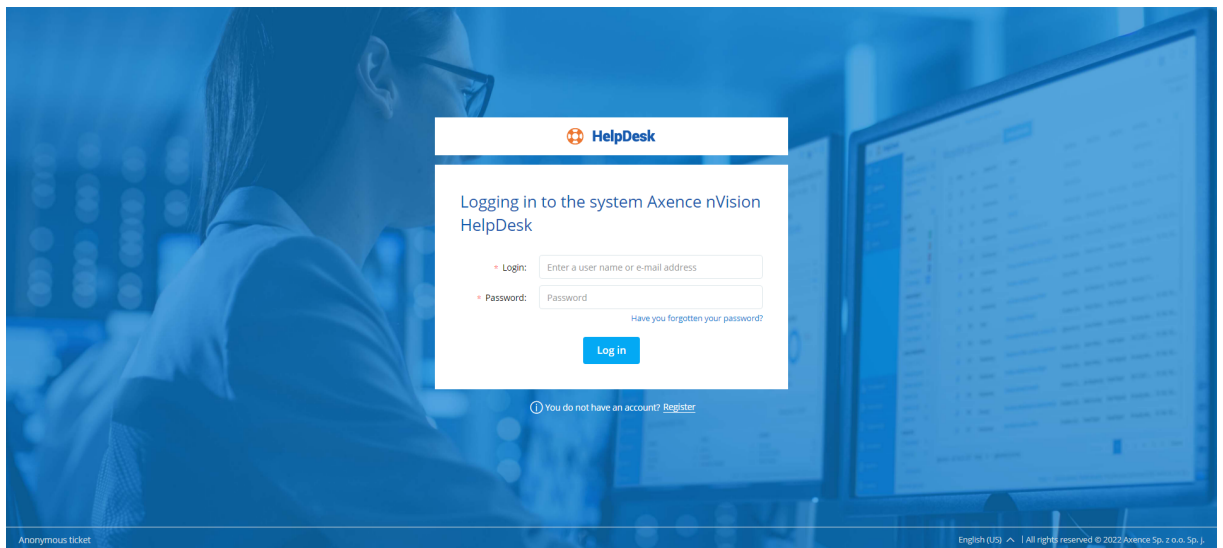
From Agent

Right-click the Agent icon in the task bar. A menu similar to the one below will be opened. The displayed options depend on the Agent settings. If you do not see the options related to the HelpDesk module, you need to [enable the HelpDesk in Agent settings](#)³⁴⁹. Select the **Log in to HelpDesk** option.



Directly in the browser

Enter or copy the HelpDesk system's URL address into the browser or click the link (e.g. sent by e-mail). The HelpDesk's URL address can be found by expanding the **Tools / Options / Services configuration** menu in the main nVision window.



Related topics

 [Management and configuration](#)

 [Settings](#)

 [User registration](#)

 [Logging in](#) 373


10.3.2 User registration

Possible user registration scenarios

Accounts for Administrator and HelpDesk (technical support) users can only be set up by the Administrator (also by the [synchronization with Active Directory](#)^[360]). In the case of self-registration by the user, only an end user account can be created. The account type can be later modified by the Administrator.

By the Administrator

To create a user account (of any type):

1. In the main nVision window go to the **Users** window.
2. In the **Users** tab, click the  **Add** button.
3. Enter the username and password for the entered user.
4. Define the user's **Role** (User, HelpDesk, Administrator).
5. Set the account as **enabled**.
6. You can enter the user details (e-mail, full name), and also other rights, depending on the defined user type.

Self-created by users, activated by the Administrator

Configuration:

1. In the main nVision window, expand the menu at the **HelpDesk** button, open the **Configuration / Core settings** option.
2. Check the **Account self-registration** field.
3. In the **Account activation mode** field, select the **Manual activation by administrator** option.

To create a user account:

1. [Run the HelpDesk interface](#)^[360]. If a user is not logged in, the HelpDesk interface login window will appear.
2. Click **Register** button.
3. In the user registration dialog box, enter your **E-mail address**, which is also the interface login.
4. Enter **Password** and **Full name**.
5. Click **Register** button.
6. You can log in to the system when the administrator activates the newly created account.

Self-created by users, activation by e-mail

Configuration:

1. In the main nVision window, expand the menu at the **HelpDesk** button, open the **Configuration / Core settings** option.

2. Check the **Account self-registration** field.
3. In **Account activation mode** field, select the **Send activation e-mail** option.

To create a user account:

1. [Run the HelpDesk interface](#)³⁶⁹. If a user is not logged in, the HelpDesk interface login window will appear.
2. Click **Register** button.
3. In the user registration dialog box, enter your **E-mail address**, which is also the interface login.
4. Enter **Password** and **Full name**.
5. Click **Register** button.
6. An activation e-mail will be sent to the entered e-mail address. To complete the registration process, you need to click the link in the e-mail. You can now log in to the HelpDesk interface.

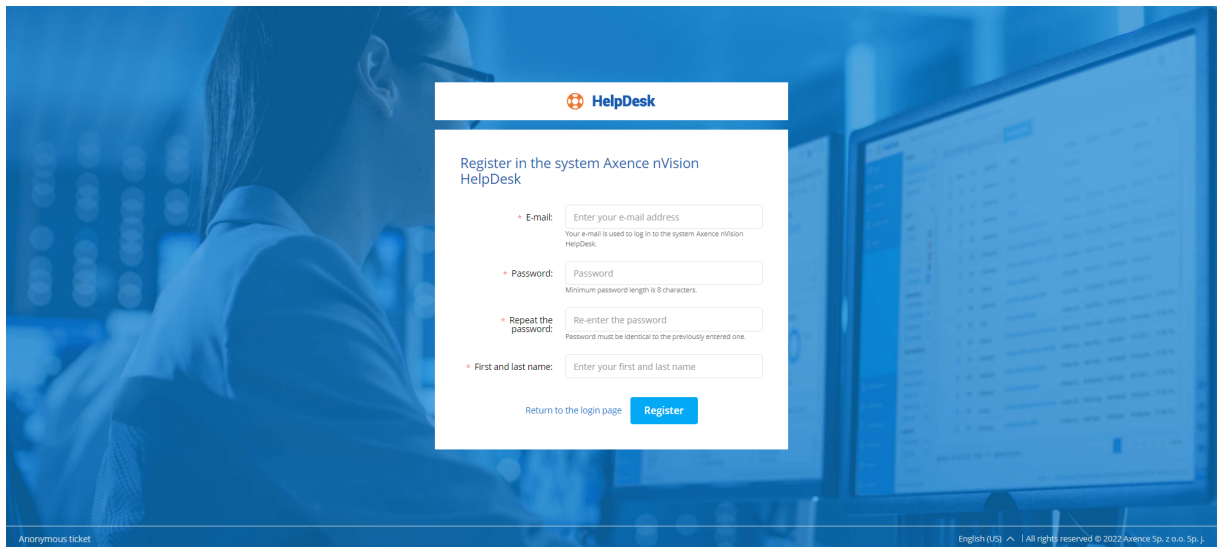
Self-created by users, without account activation

Configuration:

1. In the main nVision window, expand the menu at the **HelpDesk** button, open the **Configuration / Core settings** option.
2. Check the **Account self-registration** field.
3. In the **Account activation mode** field, select **No needed** option.

To create a user account:

1. [Run the HelpDesk interface](#)³⁶⁹. If a user is not logged in, the HelpDesk interface login window will appear.
2. Click **Register** button.
3. In the user registration dialog box, enter your **E-mail address**, which is also the interface login.
4. Enter **Password** and **Full name**.
5. Click **Register** button.
6. After the data is confirmed as valid (the e-mail address is unique and the password length is at least 8 characters), a registration completion message will appear. You can now log in to the HelpDesk interface.



Related topics

 [Starting the HelpDesk interface](#)

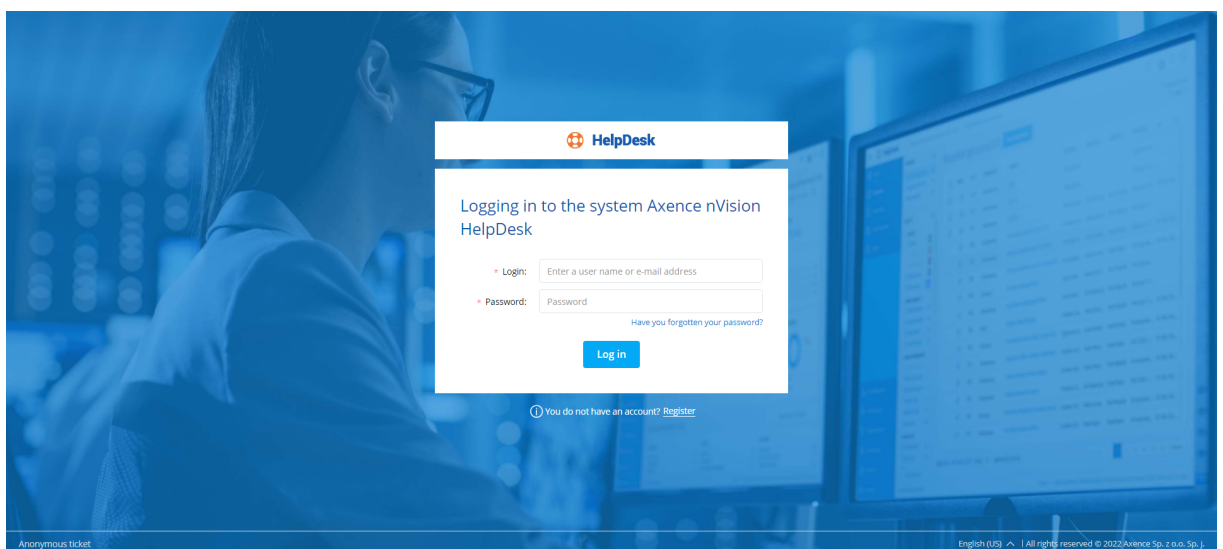
 [User management](#)

 [Settings](#) 356

10.3.3 Logging in

To log in to the HelpDesk interface:

1. [Run the HelpDesk interface](#) 369.
2. Enter **login** (username or e-mail address) and **password**. (If you enter the HelpDesk via the Agent, an attempt to auto-log in will be made.)
3. Click **Log in** button. If the entered data are correct, you can start using the HelpDesk interface.



Logging out

To log out of the HelpDesk interface:

1. Click the avatar in the [user zone](#)^[379] in the upper right corner of the HelpDesk interface.
2. Select **Log out** in the pop-up menu.

Related topics

 [Starting the HelpDesk interface](#)

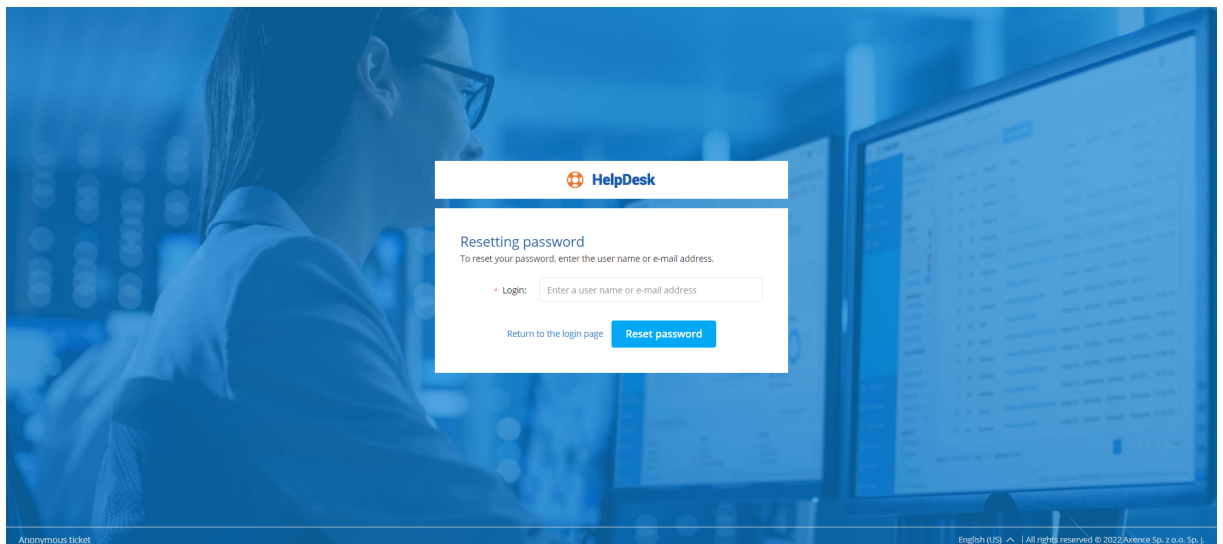
 [User registration](#)

 [Password reset](#)^[374]

10.3.4 Password reset

If the password has been forgotten:

1. [Run the HelpDesk interface](#)^[369] and click the **Reset password** link.
2. To reset the password, enter the username or e-mail address which was used to log in to the HelpDesk interface.
3. Click **Reset password** button. If the entered data are valid, a message with guidelines will be sent to the e-mail address. Otherwise, follow the onscreen instructions.
4. Open your mailbox and click the password resetting link in the message received from the HelpDesk.
5. Enter a new password and **Save settings**. You can now log in to your account with the new password.



Related topics

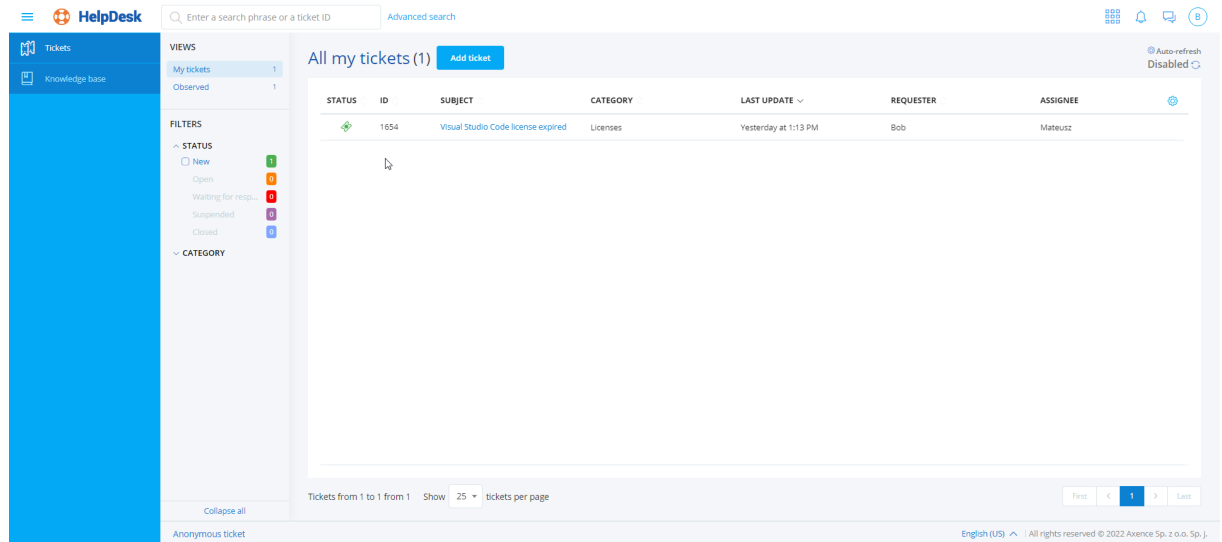
 [Starting the HelpDesk interface](#)

 [User registration](#)

 [Logging in](#)^[373]

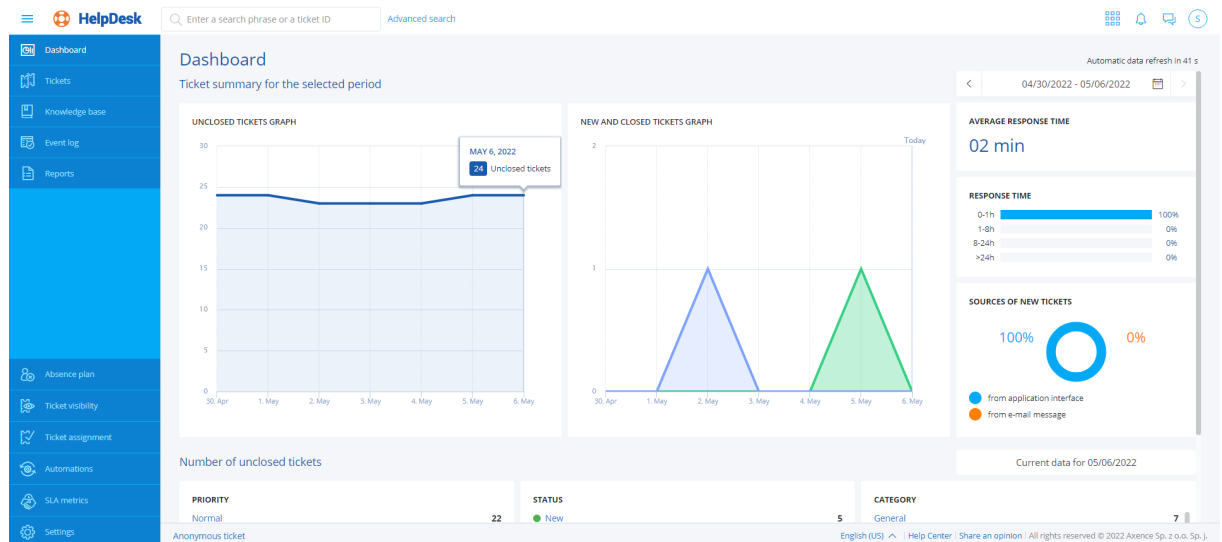
10.3.5 Main views

The main application views are ten views which can be opened by using the main navigation located on the left-hand side of the interface:



- Dashboard

General statistics about tickets are presented on dashboard, e.g. average response time, information about sources of new tickets, number of tickets by priority/status/category. A graph is also displayed, showing the number of tickets with a status other than “closed”.



- [Trouble ticket list](#) ³⁸³
- [Knowledge base](#) ⁴¹⁸
- [Event log](#) ⁴²²
- [Reports](#) ⁴²⁴
- [Trouble ticket assignment](#) ⁴⁵⁷
- [Automations](#) ⁴⁵⁸

- [SLA metrics](#)⁴⁶⁷
- Settings ([Categories](#), [Trouble ticket forms](#), Priorities, Notifications, [Whistleblowers](#))

When a selected view is expanded, a quick preview column will appear. The quick preview options differ depending on which item was selected in the main navigation (trouble tickets, articles, etc.). The quick preview option allows for simple and rapid access to various trouble ticket threads, article types, etc.

Page titles are created dynamically, depending on the selected view options.

Related topics

 [Trouble tickets - overview](#)

 [Knowledge base - overview](#)

 [Event log](#)

 [Automations](#)









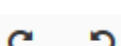
 [User zone](#)




 [Search bar](#)³⁸⁰

10.3.6 Text editor

The embedded text editor allows the entered article or ticket contents to be formatted.


Basic functions (adding/editing articles and trouble tickets)

| Function | Description |
|---|--|
|  | Bold. |
|  | Italic. |
|  | Underline. |
|  | Text style (options: Small, Regular, Large, Very Large). |
|  | Text color (selectable after the menu at the button is expanded). |
|  | Embedding a link in the text. Click the icon and in the dialog box enter the URL address where the link will direct to, and the displayed link text. |
|  | Numbered list. |
|  | Bulleted list. |
|  | Retry/undo. |

| Function | Description |
|---|---|
|  | Remove formatting. |
|  | Justification (options: left, center, right). |
|  | Toggle between HTML and Rich Text. |


Loading images (adding/editing articles)

To load an image into the article:

1. In the article [adding](#)^[419] or [editing](#)^[420] view, click the  **Upload image** button.
2. In the dialog box select the image to be added.
3. You can add the image title and an alternative text shown in the place of the image, if it cannot be displayed.
4. Select the image justification style (default: left).
5. Click the **Insert image** button.

Adding an external video (adding/editing articles)

To add an external video to the article:

1. In the article [adding](#)^[419] or [editing](#)^[420] view click the  **Insert video** button.
2. In the dialog box enter the link to the video.
3. Select the video justification style (default: center).
4. Click the **Insert video** button.

Related topics

 [Adding a ticket](#)

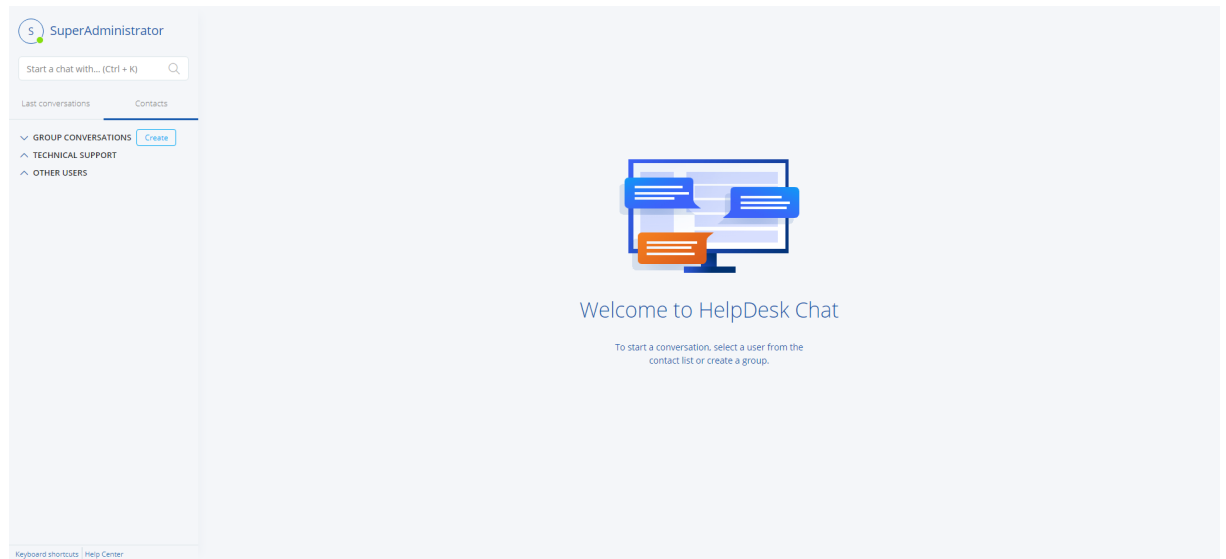
 [Adding a comment](#)

 [Adding an article](#)

 [Editing an article](#)^[420]


10.3.7 Chat

Chat conversations can be initiated and received both with the use of the HelpDesk module in the browser and via the Agent. The functionality is identical in both cases. A conversation can be conducted between the users who are present in the list in the **Users** window (see [User management](#)^[360]).



Chat users

After clicking the **Chat** button (both in the browser and in Agent options), a window with three user groups is displayed:

| Group | Description |
|-------------------|---|
| Favorites | People added to the list of friend, i.e. marked with star  . |
| Technical Support | HelpDesk- and Administrator-type users (see User management ^[360]). |
| Other users | All types of users. |


To add a user to your friends, click the star on the right-hand side of the username. From now on, the user will also be present in the friends (favorites) group. To remove a user from the friends list, click the star again.

Initiating a conversation from the HelpDesk interface

To use chat:

1. [Log in to the HelpDesk interface.](#) ^[369]



- Click the  button in the upper right part of the window. The chat window will open. Users currently logged in to the HelpDesk are marked in green, users not logged in – in grey.
- Click the name of the user you want to talk to.
- Type your message and press Enter. If the user is logged in (green in the user list), a chat window will appear on their desktop with the sent message.

Chat with the trouble ticket creator or with the person responsible for the ticket can be also initiated from the specific ticket by clicking the icon with the name of the appropriate user on the right of the ticket metrics.

▣ Initiating a conversation from the Agent

Initiating a conversation:

1. Right-click the Agent icon in the task bar. A menu similar to the one below will be opened. The displayed options depend on the Agent settings. If you do not see the options related to the HelpDesk module and chat, [enable the HelpDesk in Agent settings](#)³⁴⁹.
2. In the **Agent options** window select the **Open chat** option.
3. The chat window will open. It enables a conversation with another user to be started.


▣ Answering a conversation

Answering a conversation – possible scenarios:

- If you have an open chat window with the user list and you receive a message, a window will open, which allows a conversation with the user who sent you the message.
- If the window is closed, but you are logged in to the HelpDesk from the Agent, and you receive a message, notification about the received message appears.
- If you are not logged in to the HelpDesk, the message will appear when you next log in.

▣ Creating a group chat

To create a group chat, click the **Create a new group chat** link on the contact list.

During a private chat, you can create a group chat by clicking on the chat partner adding icon  in the upper part of the chat window.

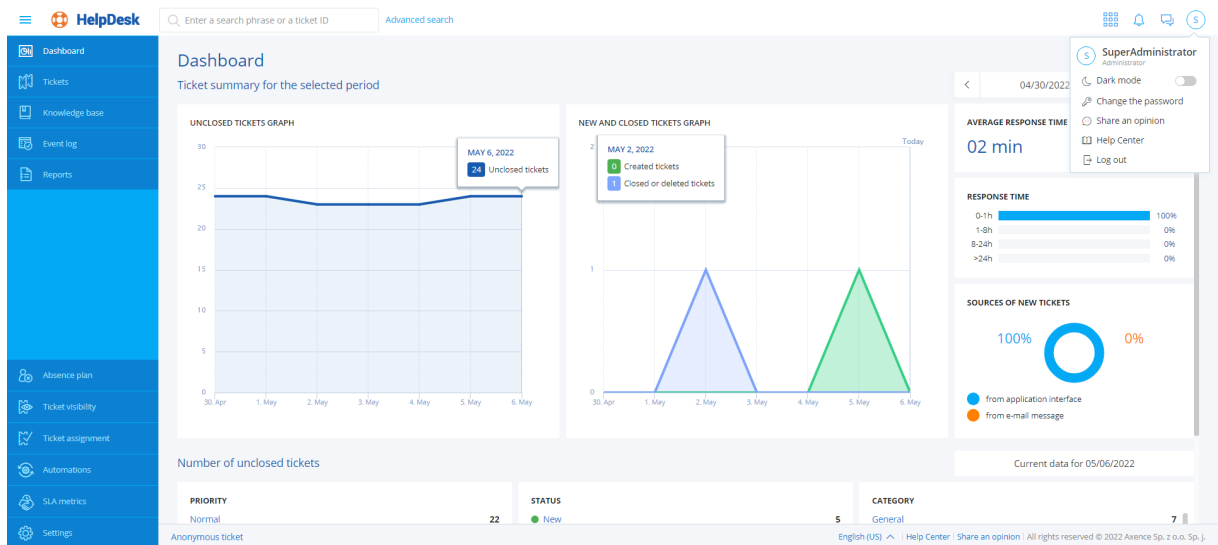
▣ Sending attachments

To send an attachment, click the attachment icon  in the message entry field.

Sending attachments is an experimental function and it is not supported in group chats.

10.3.8 User zone

The user zone is the area in the upper right corner of the HelpDesk interface. It contains a universal user avatar, as well as additional information and actions available to the logged in user.



| Icon | Description |
|------|--|
| | <p>Click the avatar to expand a pop-up menu with the following options (depending on the user type):</p> <ul style="list-style-type: none"> • Help Center (<u>Administrator and HelpDesk employee</u>) • Change password • Log out ³⁷³ |
| | <p>Click the icon to open chat ³⁷⁷.</p> |
| | <p>The icon displays the number of new notifications related to changes in trouble tickets. Click the icon to display the new notifications (Administrator and HelpDesk employee).</p> |
| | <p>Click this button to expand a list of available web modules. Click the module name to view the corresponding module, e.g. SmartTime</p> |

Related topics

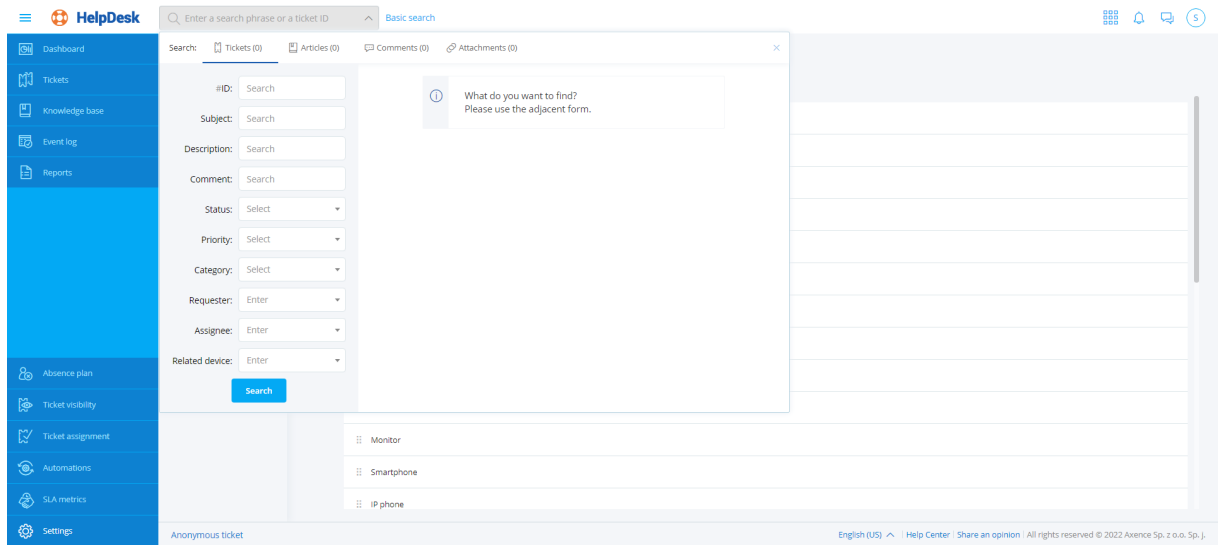
[Starting the HelpDesk interface](#)

[Main views](#) ³⁷⁵

10.3.9 Search bar

The search field in HelpDesk module is located in the upper part of the window. The search is performed first in the view that is currently displayed. The scope of the search depends on the role of the user and his permissions regarding the visibility of tickets.

It is possible to search through submissions, comments, attachments and articles. Attachment search only searches attachment names in tickets, comments, and knowledge base articles.



Advanced Search

To use the advanced search, click **Advanced Search** at the top of the window. In the advanced view, outside the searched area of the system (Report List / Knowledge Base) you can specify additional parameters that will narrow the list of search results. Available parameters change depending on the searched area (notifications, articles, comments, attachments).

When using an advanced search engine with the option to search for applications, it is possible to define the following parameters:

- ID,
- Subject,
- Description,
- Comment,
- Status,
- Priority,
- Category,
- Requester,
- Assignee,
- Related device.

Related topics

 [Main views](#)

 [User zone](#)

 [User management](#) 360

10.4 Trouble tickets

10.4.1 Trouble tickets - overview

The trouble ticket database allows the users to report technical issues with use of the HelpDesk interface and via e-mail. The incoming tickets are processed and assigned to specific HelpDesk support employees who are notified about the assigned problems which need to be solved.

Each ticket is assigned to a specific category and has a priority defined to it. Ticket management and processing is simple due to the mechanism of statuses describing the ticket life cycle.

The screenshot shows the HelpDesk interface. On the left, there is a navigation menu with 'Tickets' and 'Knowledge base'. The main area displays 'All my tickets (1)' with a table containing one ticket:

| STATUS | ID | SUBJECT | CATEGORY | LAST UPDATE | REQUESTER | ASSIGNEE |
|--------|------|------------------------------------|----------|----------------------|-----------|----------|
| New | 1654 | Visual Studio Code license expired | Licenses | Yesterday at 1:13 PM | Bob | Matheus |

Below the table, it shows 'Tickets from 1 to 1 from 1' and 'Show 25 tickets per page'. The footer includes 'Anonymous ticket' and 'English (US) | All rights reserved © 2022 Axence Sp. z o.o. Sp. j.'

Tickets statuses:

New – the ticket has been registered in system, but no action was performed by any user.

Open – the HelpDesk worker should update the ticket.

Waiting for response – the requester should update the ticket.

Suspended – ticket is set to suspended by HelpDesk worker (e.g. the issue should be discussed with third party).

Closed – the ticket has been closed by HelpDesk worker. Closed tickets cannot be deleted.

Related topics

[Starting the HelpDesk interface](#)

[Ticket list](#)

[Adding a ticket](#)

[Adding a comment](#)

[Categories](#)

[Priorities](#)

[Editing a ticket subject](#)

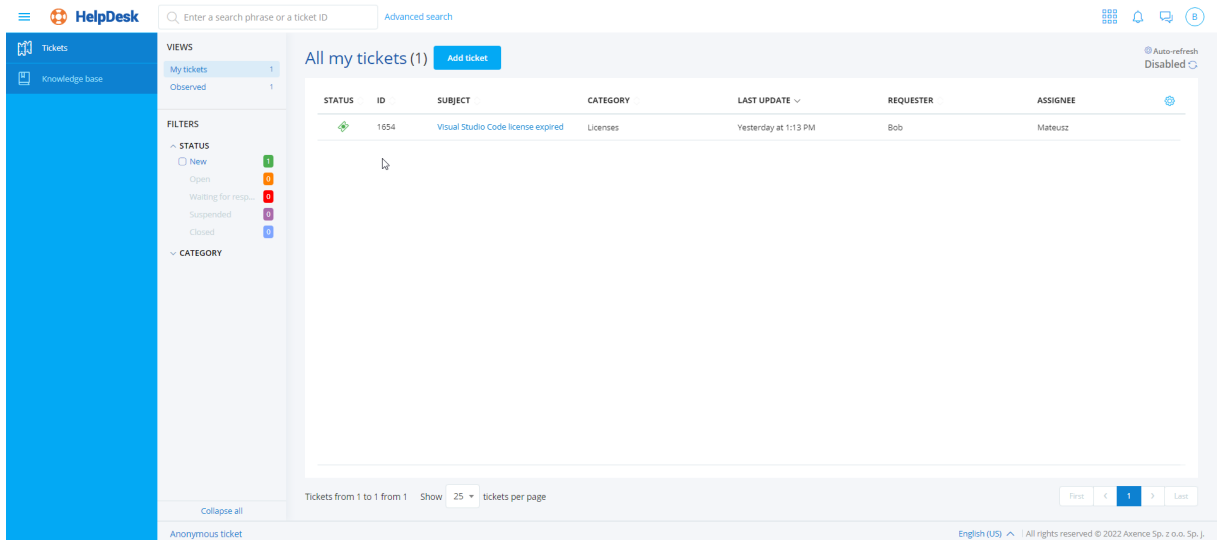
[Merging tickets](#)


 [VNC connection](#)

 [Deleting a ticket](#) ³⁹⁶

10.4.2 Ticket list

The ticket list is one of the main views of the HelpDesk interface. It shows information about trouble tickets sent to the HelpDesk system.



| STATUS | ID | SUBJECT | CATEGORY | LAST UPDATE | REQUESTER | ASSIGNEE |
|---|------|------------------------------------|----------|----------------------|-----------|----------|
|  | 1654 | Visual Studio Code license expired | Licenses | Yesterday at 1:13 PM | Bob | Mateusz |

In the left part of the window, there is the main navigation (see [Main views](#) ³⁷⁵) and the quick preview column. The quick preview allows you to rapidly display a data set from the specific area of interest. For instance, you can display new highest-priority tickets, which additionally belong to one of two selected categories.

Ticket list table

The main part of the described view is the ticket list table. It contains the following columns:

- Status (color marking on the left-hand side of the table line)
- ID
- Date of [SLA](#) ⁴⁶⁷ violation
- Priority
- Ticket subject
- Category
- Related device (column hidden in the Administrator view)
- Department (column hidden in the Administrator view)
- Date of creation (column hidden in the Administrator view)
- Date of last update
- Full name of the assignee
- Full name of the requester

To select the displayed columns or their sequence in the table, click the table settings button [gear icon] in the upper right corner of the table. To sort the table contents by a given column, click the arrow at the column name. Below the table you can select how many tickets are to be displayed per page, and also go to the next pages.

Important: Unread tickets are in bold font.

The screenshot displays the 'Table settings' dialog box in the HelpDesk interface. The dialog is titled 'Table settings' and contains a list of columns with checkboxes for selection and a plus sign for reordering. The columns are:

| Order | Column Name | Visibility |
|-------|---|------------|
| 1. | <input checked="" type="checkbox"/> ID | visible |
| 2. | <input checked="" type="checkbox"/> Priority | visible |
| 3. | <input checked="" type="checkbox"/> Subject | visible |
| 4. | <input checked="" type="checkbox"/> Category | visible |
| 5. | <input checked="" type="checkbox"/> Last update | visible |
| 6. | <input checked="" type="checkbox"/> Requester | visible |
| 7. | <input checked="" type="checkbox"/> Assignee | visible |
| 8. | <input type="checkbox"/> Device | invisible |
| 9. | <input type="checkbox"/> Department | invisible |
| 10. | <input type="checkbox"/> Created | invisible |

At the bottom of the dialog are 'Save settings' and 'Cancel' buttons. The background shows a table of tickets with columns for Requester and Assignee. The table is currently displaying 9 tickets per page, and the user is on page 1 of 1.

Ticket preview

Click the ticket icon or line on the right-hand side of the interface to open a quick preview of the ticket. The quick preview displays the title and the short ticket excerpt, and the action block. The block enables you to quickly and comfortably add an internal or public comment to the ticket. Below, the last comments, short ticket summary and the navigation bar are shown.

The screenshot displays the HelpDesk interface. On the left is a navigation sidebar with options like Dashboard, Tickets, Knowledge base, and Event log. The main area is divided into three sections: a 'QUICK PREVIEW' sidebar with filters for ticket status (All tickets, Assigned to me, New, Open, etc.), a central 'All tickets' table, and a 'TICKET PREVIEW' sidebar on the right.

| Status | ID | Priority | Subject |
|---------------------------------------|----|----------|---|
| ✔ | 2 | Minor | Printing issue |
| ✘ | 3 | Major | MS Word crashing problem |
| ✘ | 4 | Minor | new keyboard |
| ✘ | 5 | Minor | cannot login to webportal |
| ✘ | 6 | Minor | email automatic response |
| ✘ | 7 | Minor | Applications keep crashing |
| ✘ | 8 | Minor | slow download |
| ✘ | 9 | Minor | There is a problem with this website's security certifi |
| ✔ | 10 | Major | No response on call |

The 'TICKET PREVIEW' sidebar shows details for ticket ID 3: 'MS Word crashing problem'. It includes a 'Post internal comment' form, a 'Comment' button, and a 'See details' button at the bottom.

To go the detailed ticket view at once, click its subject.

Related topics

[Starting the HelpDesk interface](#)

[Trouble tickets - overview](#)

[Main views](#)

[Adding a ticket](#)

[Adding a comment](#)

[Categories](#)

[Priorities](#) ³⁶¹

10.4.3 Adding a ticket

To create a new trouble ticket in the HelpDesk interface:

1. In the **Tickets** view click the **Add ticket** button.
2. Enter the **Subject** of the ticket.
3. Enter the **Description** of the issue in the embedded [text editor](#) ³⁷⁶.
4. You can [Add attachment](#) ³⁹¹ to the ticket.

5. You can [Add screenshot](#)³⁹¹ if the Agent is installed on the device.
6. Fill in the **Requester** field (Administrator and HelpDesk employee may create a ticket on someone's behalf).
7. In the **Assignee** field use the list to select the person to whom the ticket is to be assigned (optionally).
8. Set the ticket's **Category** by selecting one of the available categories from the list. You can [add a new category](#)³⁶³ without interrupting the article creation process.
9. Set the ticket's **Priority** by selecting one of the available priorities from the list. You can [add a new priority](#)³⁶¹ without interrupting the article creation process.
10. Use the list to select the **Related device** which the ticket relates to (optionally).
11. After the ticket creation is complete, click the **Add ticket** button.

The screenshot shows the 'Adding a ticket' interface in the HelpDesk system. The left sidebar contains navigation options: Dashboard, Tickets, Knowledge base, Event log, Reports, Absence plan, Ticket visibility, Ticket assignment, Automations, SLA metrics, and Settings. The main form area has the following fields:

- Category:** Select category (dropdown)
- Subject:** Enter a ticket subject (text input)
- Description:** Rich text editor with various formatting options.
- Attachments:** (up to 20MB) and Add screenshot button.
- Requester:** SuperAdministrator (dropdown)
- Assignee:** Enter a user (dropdown)
- Priority:** Normal (default) (dropdown)
- Related device:** Enter a related device (dropdown)

At the bottom of the form are 'Add ticket' and 'Cancel' buttons. The footer of the interface shows 'Anonymous ticket' and 'English (US) | Help Center | Share an opinion | All rights reserved © 2022 Axence Sp. z o.o. Sp. j.'

Related topics

[Starting the HelpDesk interface](#)

[Trouble tickets - overview](#)

[Ticket list](#)

[Adding a comment](#)

[Merging tickets](#)³⁹⁵

10.4.4 Ticket visibility settings

The ticket visibility settings allow the ticket access restrictions to be configured for users with the **HelpDesk Employee** role.

You can check the current configuration in the **Ticket visibility** tab. The list will show all users with the **HelpDesk Employee** role:

Default settings

You can configure the default rights. They will be assigned to each new user who is granted the HelpDesk Employee role for the first time. If the default rule is edited, the users who have already been granted this role do not receive it in its updated form.

To edit the default settings, select the **Set the default rule** item:

The ticket visibility rule has the following configuration options:

1. Full visibility - selected user will have access to all trouble tickets
2. Restricted visibility - selected user will have access to tickets which **satisfy conditions**.

The following conditions are available:

- Ticket category **is equal to** or **is not equal to** the selected category,
- The reporter **belongs to** or **does not belong to** a specific group

The administrator can specify how many conditions (one or both) must be satisfied for the rule to work.

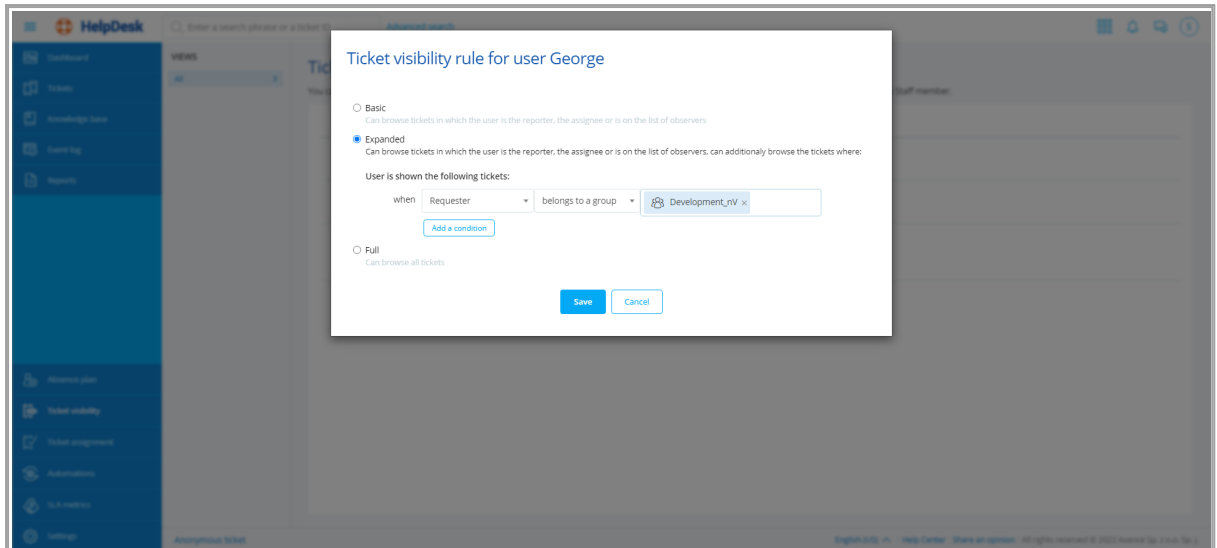
Editing a visibility rule

Each visibility rule can be edited. To edit a visibility rule, log in to the HelpDesk module as the Administrator and:

1. In the flyout menu on the left side of the window, click the **Ticket visibility**.
2. Select the HelpDesk Employee whose visibility rule you want to edit (when you hover over the field of the relevant HelpDesk Employee, the **Edit**, **Copy to...**, **Copy from default rule** buttons are displayed).
3. Click the **Edit** button.
4. Configure the visibility rule, and then click the **Save** button.

The screenshot displays the 'Ticket visibility' configuration interface. On the left is a navigation menu with 'Ticket visibility' selected. The main content area shows a table of visibility rules for three users: Bob, Devon, and George. Bob and Devon have 'Full visibility'. George has 'Expanded visibility' with a condition: 'requester belongs to a group: Development_nv'. Action buttons for editing and copying are present for the George row.

| USER | VISIBILITY RULE |
|--------|---|
| Bob | Full visibility |
| Devon | Full visibility |
| George | Expanded visibility: <ul style="list-style-type: none">requester belongs to a group: Development_nv |

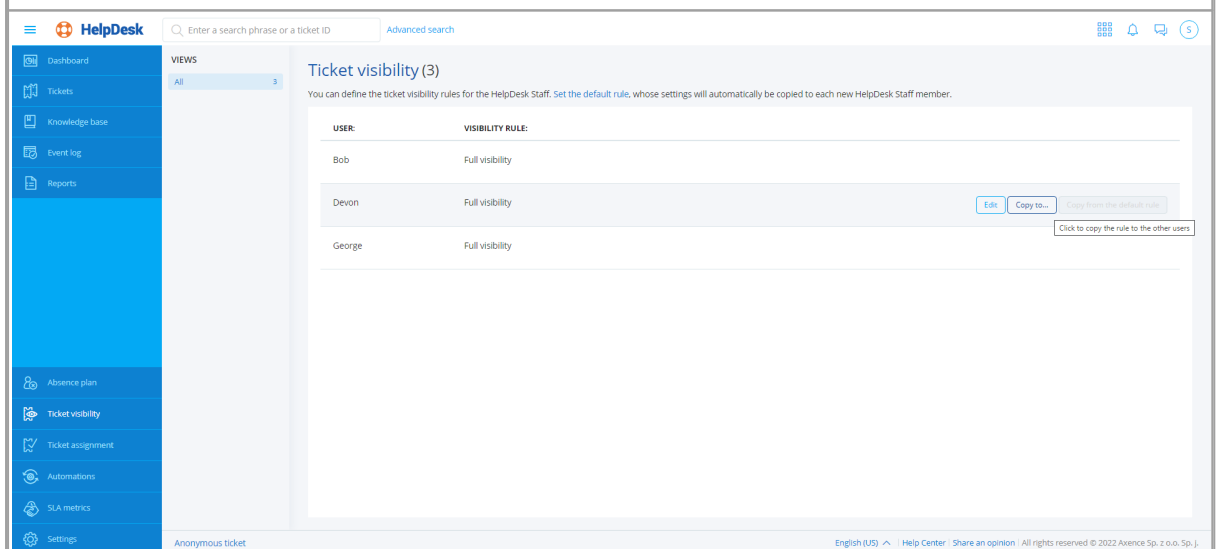


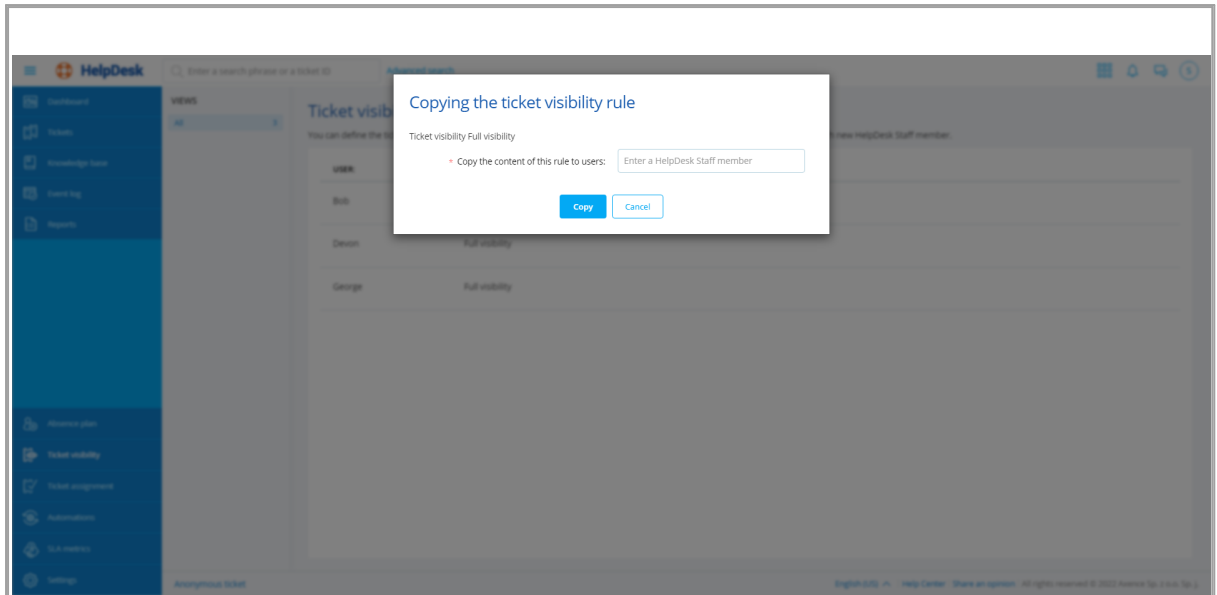
Once you have properly completed the steps above, the visibility rule for the specific HelpDesk Employee will be updated.

Copying a visibility rule

HelpDesk allows a visibility rule currently assigned to a HelpDesk Employee to be copied to another HelpDesk employee. To do this:

1. In the flyout menu on the left side of the window, click the **Ticket visibility**.
2. Select the HelpDesk Employee whose visibility rule you want to edit (when you hover over the field of the relevant HelpDesk Employee, the **Edit**, **Copy to...**, **Copy from default rule** buttons are displayed).
3. Click the **Copy to...** button.
4. In the ticket visibility copying window, select the HelpDesk employee to copy the rule to (you can select more than 1 employee), and then click the **Copy** button.



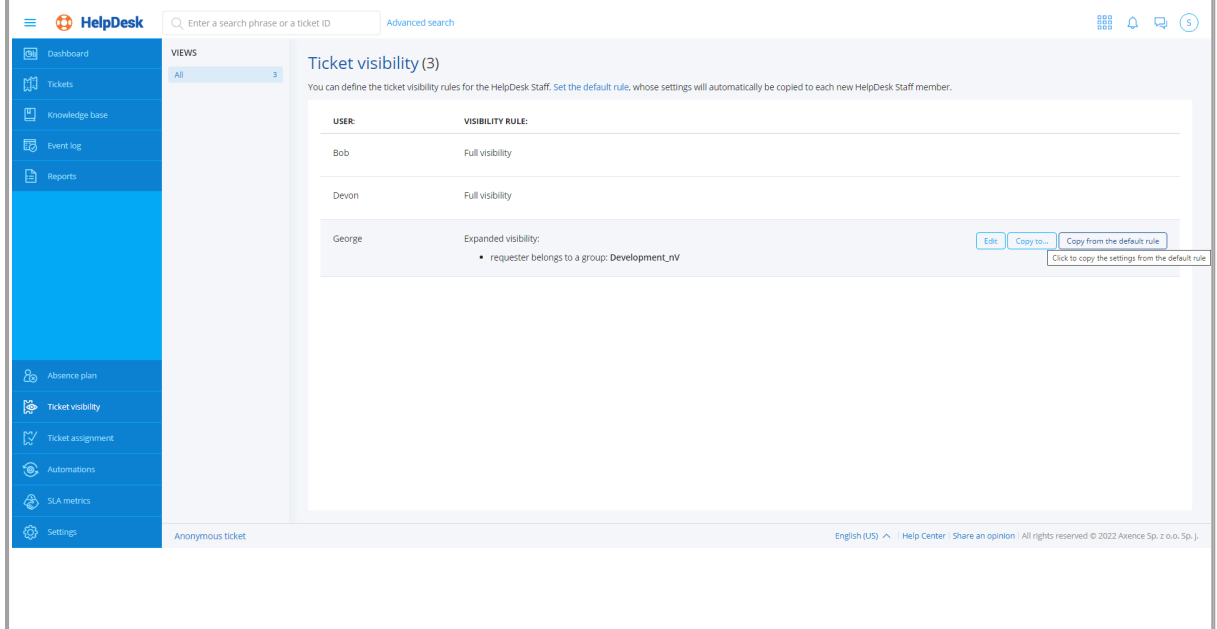


Assigning the default rule

HelpDesk allows the default rule to be copied to any HelpDesk employee (whose visibility rule is different from the default rule). To do this:

1. In the flyout menu on the left side of the window, click the **Ticket visibility**.
2. Select the HelpDesk Employee whose visibility rule you want to edit (when you hover over the field of the relevant HelpDesk Employee, the **Edit**, **Copy to...**, **Copy from default rule** buttons are displayed).
3. Click the **Copy from** button.

If the default rule and the employee's rule are identical, the **Copy from default rule** button is gray.



10.4.5 Ticket processing

10.4.5.1 Adding a comment

To add a comment to the ticket:

1. In the **Tickets** view click the ticket you want to process.
2. Enter a comment in the embedded [text editor](#)³⁷⁶ in the field below the ticket description.
3. You can [Add attachment](#)³⁹¹ to the ticket.
4. You can [Add screenshot](#)³⁹¹ if the Agent is installed on the device.
5. By default, the form is set to publish internal comments (orange background), which are visible only to Administrator and HelpDesk users. If a comment is to be visible to end users (white background), uncheck the **Internal** field. An end user can only add public comments.
6. You can add a link to the Knowledge Base article (only the Administrator and the Helpdesk support employee). To do this, click the **Select article** button and enter the title or select the article you want to sublink from the list. In this way, you can sublink multiple articles. To finish, click the **Select article** button.
7. To publish the comment, click the **Comment** button.

Related topics

[Starting the HelpDesk interface](#)


[Trouble tickets - overview](#)

[Ticket list](#)


[Adding an attachment](#)³⁹¹

10.4.5.2 Adding attachments and screenshots

To add a comment with an attachment to the ticket:


1. In the [Ticket adding](#) or 'Adding comment to a ticket' view click the  **icon**.
2. In the dialog box select the file to be attached.
3. Enter a comment and click the **Comment** button.

To add a comment with a screenshot to the ticket:

1. In the [Ticket adding](#) or 'Adding comment to a ticket' view click the  **icon**.
2. In the dialog box click the **Screenshot** button. An image of the user's desktop will be displayed.
Click the **Done** button to attach the displayed screenshot to the comment.
3. Enter a comment and click the **Comment** button.

Note: A screenshot can **only be added by the author of the ticket**, if the Agent with the configuration enabling screenshots is installed on their machine.

To add a comment with a link to an article in the knowledge base to the ticket:

1. In the 'Adding comment to a ticket' view click the  **icon**.
2. In the dialog box select the articles to be added to the comment. The selected articles will appear in the box. Click the **Add to comment** button to attach the selected articles to the comment.
3. Enter a comment and click the **Comment** button.

Note: The link to an article can only be added by a user with the Administrator or HelpDesk Employee role.

Related topics

 [Starting the HelpDesk interface](#)

 [Trouble tickets - overview](#)

 [Ticket list](#)

 [Adding a ticket](#)

 [Adding a comment](#) ³⁹⁰

10.4.5.3 Editing a ticket subject

To change the ticket subject:

1. In the **Tickets** view, click the ticket to be processed.
2. Hover over the ticket subject, and then click the pencil icon next to the ticket subject.
3. Enter the new ticket subject in the dialog box.
4. Click the **Save changes** button.

Related topics

 [Starting the HelpDesk interface](#)

 [Trouble tickets - overview](#)

 [Ticket list](#) 383

10.4.5.4 Multi-ticket operations

HelpDesk employees are able to simultaneously perform operations on multiple tickets.

To perform operations on a number of tickets at the same time, go to the ticket list. After selecting items from the list and clicking the **Actions** button, you can make a mass change to:

- Ticket status
- Category
- Priority
- Assignee

In addition, two other actions are available:

- Add comment
- Delete tickets

Moreover, you can add a comment to the selected ticket(s) or delete the selected ticket(s) (unrecoverable operation).

10.4.5.5 Closing a ticket

A ticket can be closed in two ways.

Closing from the ticket processing window.

To close a ticket, click the **Close the ticket** button on the right side of the window. The ticket closing window opens where the employee can specify the time spent on processing the ticket and add the last comment to the ticket:

Closing from the ticket list level

To close more than one ticket at a time, go to the ticket list. After the required items are selected, you can change the ticket status on a mass scale:

10.4.5.6 Editing ticket details

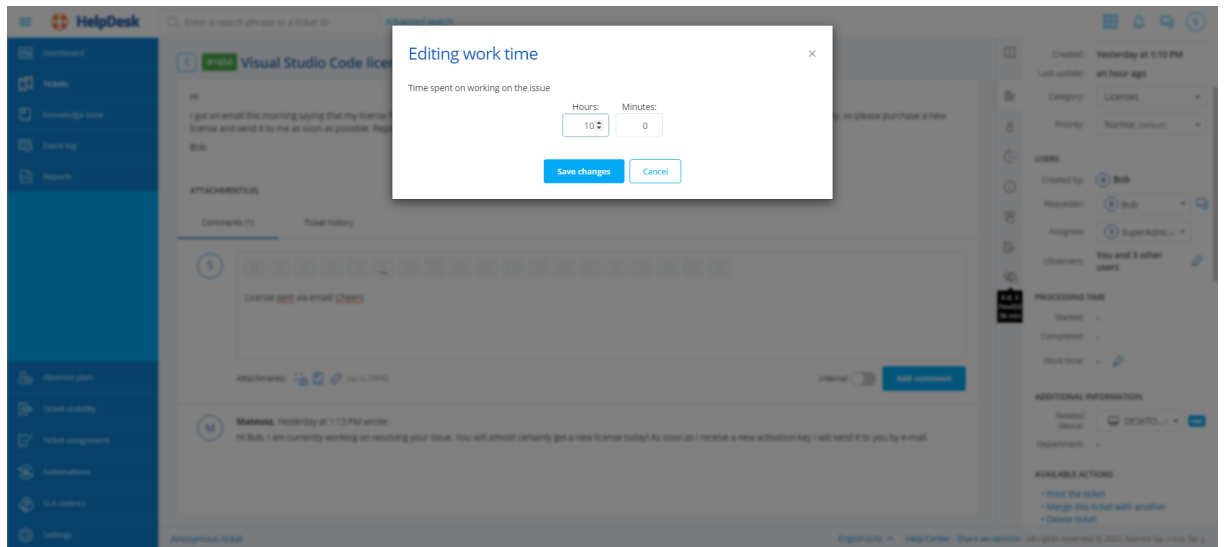
10.4.5.6.1 Setting the ticket processing time

Setting the ticket processing duration allows a retrospective performance analysis and the estimation of the time required to solve similar issues.

To set the ticket processing duration:

1. In the selected ticket view, in the **Processing time** section, click the pencil icon.
2. Enter the time for which the ticket was being processed.

3. In the dialog box set the ticket processing time and click **Save changes** button.



Related topics

 [Starting the HelpDesk interface](#)

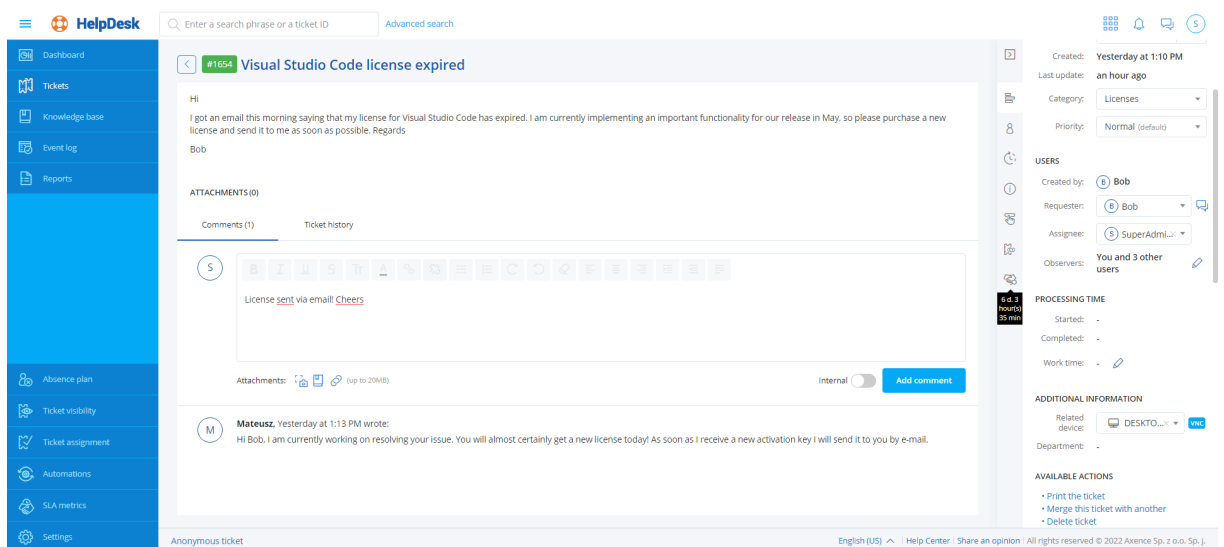
 [Trouble tickets - overview](#) ³⁸²

10.4.5.6.2 VNC connection

Note: the remote access feature is visible only for devices supporting such a function.

To make a remote connection with the device, which the given ticket pertains to:

1. In the selected ticket view, in the **Additional information** section, click **VNC** button on the right-hand side of the related device name.
2. In the dialog box select the user session which you want to connect to and click **Connect** button. As a result, a new browser tab with the remote connection will open.
3. To control connection options, use the menu in the upper right hand corner.



Related topics

 [Starting the HelpDesk interface](#)

 [Trouble tickets - overview](#) ³⁸²

10.4.5.6.3 Related tickets

The HelpDesk system allows tickets to be related. Each relation connects exactly two different tickets. Ticket relations can be created and deleted by any person with a HelpDesk Employee or Administrator role and are visible only for such users.

Information about related tickets is visible in the ticket summary(as the last option).

The HelpDesk system offers the following relation types:

- Association (the same content in both directions)

Ticket A is associated with ticket B

Ticket B is associated with ticket A

- Blocking

Ticket A blocks ticket B

Ticket B is blocked by ticket A

- Multiplication

Ticket A replicates ticket B

Ticket B is replicated by ticket A

- Reason and effect

Ticket A is a reason for ticket B

Ticket B is an effect of ticket A

- Follow-up

Ticket A is a follow-up to ticket B

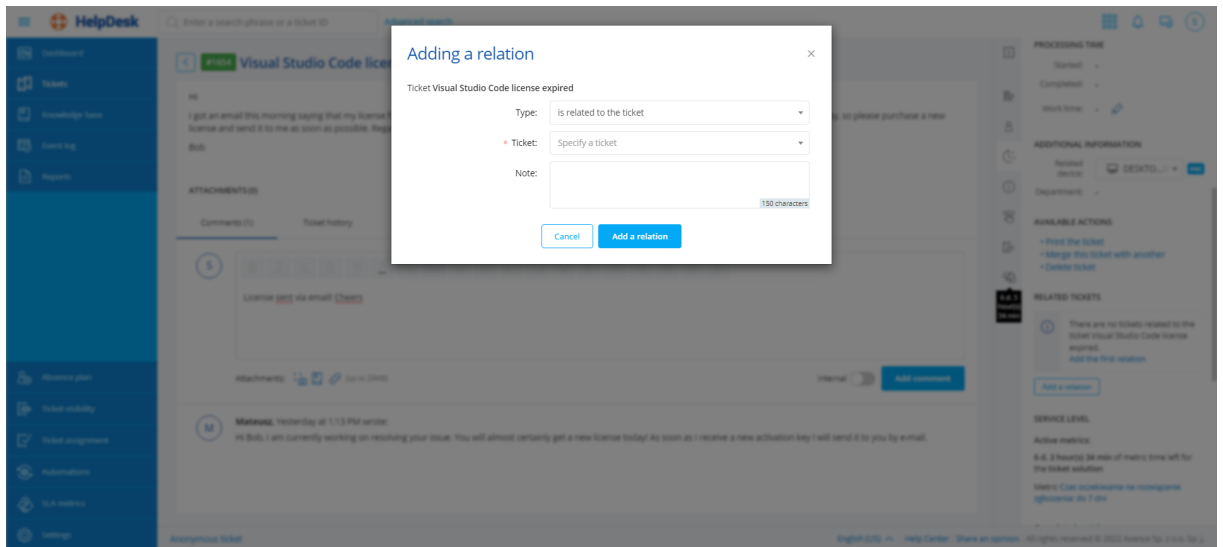
Ticket B is a followed up by ticket A

Creating and removing relations

To create a relation between tickets:

1. [Go to details](#) ³⁹² for one of the tickets.
2. Click **Add relation** button in the **Related tickets** section.
3. Specify:
 - relation type,
 - the other ticket to be related with the current one,
 - optionally: relation description (memo).

4. Click the **Add relation** button.



Additional information

- Each ticket can have a custom number of relations.
- Relations can be created and removed even when one or both related tickets are closed.
- Creating and removing relations does not generate notifications for any users participating in ticket processing.
- A ticket created by means of an e-mail message as a follow-up to a closed ticket (by responding to an e-mail notification) is, at the moment of creation, automatically related to the ticket, which is followed up. ("*<follow-up> ticket is a follow-up to ticket <closed ticket>*")
- Creating or removing a relation is not a ticket update and therefore does not change the last ticket update date and does not trigger automations.
- Removing a ticket appearing in any relations results in removing all such relations (regardless of their direction).

10.4.5.6.4 Merging tickets

Note: you can only merge tickets, which are not closed (i.e. their status is New, Open, Response pending, Suspended) and which originate from the same reporting person. The operation is irreversible.

To merge tickets:

1. In the **Tickets** view click the ticket which is to be merged with another ticket.
2. Click the **Merge this ticket with another** action in the ticket summary, in the **Available actions** section.
3. In the ticket merging dialog box specify the name or ID of the ticket which the current ticket will be added to.
4. Click the **Merge tickets** button.

Related topics

 [Starting the HelpDesk interface](#)

 [Trouble tickets - overview](#) ³⁸²

10.4.5.6.5 Deleting a ticket

Note: only the Administrator user can delete tickets (which are not in “closed” status). Ticket deletion operation is irreversible.

To remove a ticket:

1. In the **Tickets** view click the ticket to be deleted.
2. Click the **Delete ticket** action in the ticket summary, the **Available actions** section.
3. In the ticket deletion dialog box click the **Delete** button.

Related topics

 [Starting the HelpDesk interface](#)

 [Trouble tickets - overview](#) ³⁸²


10.5 Whistleblower Protection

10.5.1 Whistleblower Protection - introduction

As of 17 December 2021, in accordance with Directive 2019/1937 of the European Parliament and of the Council (EU) of 23 October 2019, the vast majority of companies and institutions will have to provide protection to their whistleblowers, i.e. individuals who, without any legal consequence, identify any irregularities that occur in the organization or establishment and report them using special procedures. These persons must be provided with confidentiality and personal data protection. Therefore, one of the new features in **Axence nVision® version 13** is the system for creating and processing anonymous tickets which meets the requirements of the above-mentioned directive.

NOTE! For anonymous tickets to work properly, you must correctly configure the HelpDesk in nVision®, as described further in this manual.






















Adding an anonymous ticket ×

 This ticket will remain anonymous and will not be associated with your account


* Category:

* Subject:

* Description:

B **I** **U** **S** **T** **A**                     

Providing your contact information is not obligatory.

 This data will not be used by the system to send you any updates or notifications. Only people approved by the administrator will have access to this data and can use it to contact you directly. After creating the ticket you will not be able to follow its processing.

Contact information:

The anonymous ticket setting panel - including, for instance, the legal materials to help implement appropriate procedures within your organization - can be found in the **Settings > Whistleblowers** section in the HelpDesk. The initial settings are available in two different configurations, depending on whether nVision has been previously used and updated to the latest version 13 or it is a new installation.

Current installations (update from an older version of nVision®)

To display the Anonymous ticket setting panel, **log in to the HelpDesk module as the Administrator** and:

1. In the flyout menu on the left side of the window, click the **Settings**.
2. Enter the whistleblower settings - **Whistleblowers**.

If you have already used nVision and updated it to version 13:

3. An additional message will appear in the anonymous ticket setting panel.
4. The anonymous ticket creation option is **disabled** by default.

If you click the “Yes, enable” button below the message, the anonymous ticket creation option will be **enabled**.

In addition, the category named Violations (with the category description - Anonymous violation tickets) will be created in the HelpDesk.

If you click the “No, do not enable” button, the message will no longer be displayed, the anonymous ticket creation option **will not be enabled**, and no category named Violations will be created in the HelpDesk.

You will need to manually enable the anonymous ticket creation option and create the category for anonymous tickets.

New nVision® installations

To display the Anonymous ticket setting panel, **log in to the HelpDesk module as the Administrator** and:

1. In the flyout menu on the left side of the window, click the **Settings**.
2. Enter the whistleblower settings by clicking the **Whistleblowers** link.

If you have not used nVision yet (new installation of nVision version 13):

3. In the anonymous ticket setting panel, the category created in the HelpDesk, **Violations** (with description - Anonymous violation tickets), is automatically assigned to anonymous tickets.
4. The anonymous ticket creation option will be **enabled** by default.

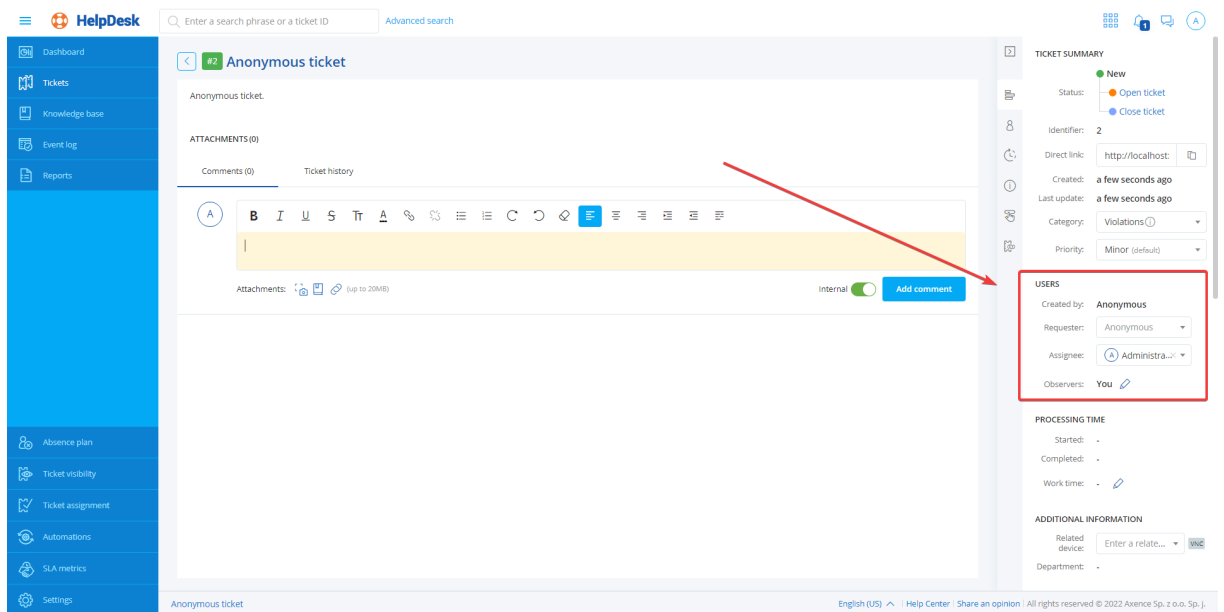
The screenshot displays the 'Tools for whistleblowers' configuration page. On the left sidebar, the 'Settings' icon is marked with a red '1'. The 'Whistleblowers' link in the 'SYSTEM SETTINGS' menu is marked with a red '2'. The 'CATEGORIES' dropdown menu, which contains 'Violations', is marked with a red '3'. The 'Allow the creation of anonymous tickets' toggle switch is marked with a red '4' and is currently turned on.

10.5.2 Restricting access to anonymous tickets

10.5.2.1 Anonymous ticket - restricted access

Since the Directive (EU) 2019/1937 of 23 October 2019 on the regulation of the legal status of the so-called whistleblowers applies, it is the primary responsibility of the employer to ensure the protection of the whistleblower’s identity and to organize the process of receiving and processing tickets in a safe manner. Axence nVision® software includes tools that allow these requirements to be met in one of the modules on the Helpdesk.

HelpDesk verifies on an ongoing basis that the user has access to a specific anonymous ticket. Access to an anonymous ticket can be granted from the ticket level by configuring the following fields: **Reporter**, **Assignee** or **Observers** (list of observers). If any change made to the ticket involves giving access to a user who has not previously had access to the anonymous ticket, the system will alert the user before the action is taken. The user who makes the change can read the message and decide whether they maintain their decision or maybe it is a mistake and the selected user should not be granted access to the anonymous ticket.



The screenshot displays the HelpDesk interface for an anonymous ticket. The main content area shows the ticket details, including attachments, comments, and a rich text editor. The right sidebar contains the 'TICKET SUMMARY' and 'USERS' sections. The 'USERS' section is highlighted with a red box, showing the following configuration:

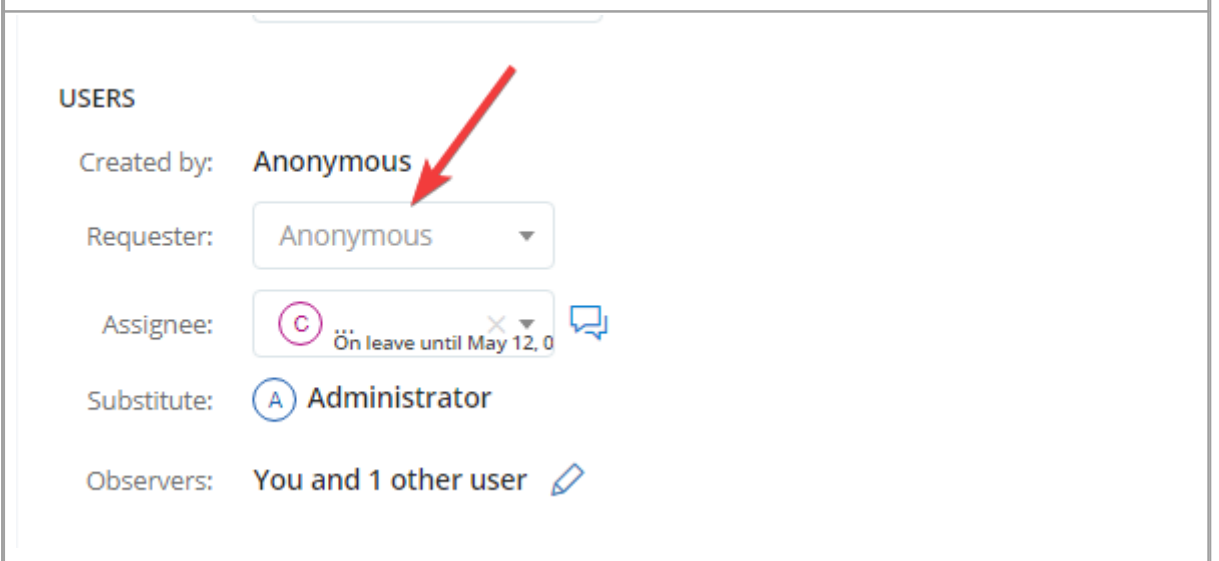
- Created by: Anonymous
- Requester: Anonymous
- Assignee: Administrator
- Observers: You

A red arrow points from the 'Add comment' button in the main content area to the 'USERS' section in the sidebar.

Giving access - Reporter

To give access to an anonymous ticket from the ticket level by setting the "Reporter" field:

1. Click the **Reporter** field.



The screenshot shows the 'USERS' section of the HelpDesk interface. The 'Requester' field is highlighted with a red arrow, indicating it is the field to be clicked. The 'Requester' field is a dropdown menu with 'Anonymous' selected. Other fields include 'Created by: Anonymous', 'Assignee: On leave until May 12, 0', 'Substitute: Administrator', and 'Observers: You and 1 other user'.

2. Select the user from the drop-down list (there is a browser at the top of the list).

USERS

Created by: **Anonymous**

Requester: Anonymous

Assignee:

Substitute: (A) Administrator

Observers: (C) Christopher
On leave until May 12, 04:00 P

PROCESSING TIME (S) Stephen

3. In the Ticket visibility extension window, confirm your choice by clicking the **Confirm** button. (Ensure that you are granting access to the ticket to the correct user.)

Ticket visibility extension ×

User Stephen will gain access to this ticket.
Are you sure you want to perform this action?

Confirm **Cancel**

4. Once you have properly completed the steps above, the selected user has been granted access to the anonymous ticket - his or her information will be displayed in the Reporter field.

USERS

Created by: **Anonymous**

Requester: (S) Stephen

Assignee: (C) On leave until May 12, 0

Substitute: (A) Administrator

Observers: You and 2 other users



Giving access - Assignee


To give access to an anonymous ticket from the ticket level by setting the “Reporter” field:


1. Click the **Assignee** field.

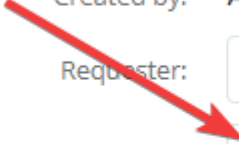
USERS

Created by: **Anonymous**

Requester:  Stephen 

Assignee: Enter a user 



Observers: **You and 2 other users** 






2. Select the appropriate HelpDesk Employee or Administrator from the drop-down list (there is a browser at the top of the list).

USERS


Created by: **Anonymous**

Requester:  Stephen 


Assignee: Enter a user 

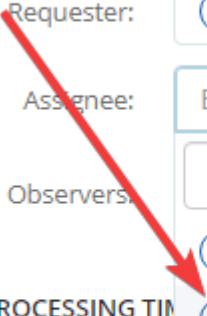
Observers:  



PROCESSING TIME

Started: 

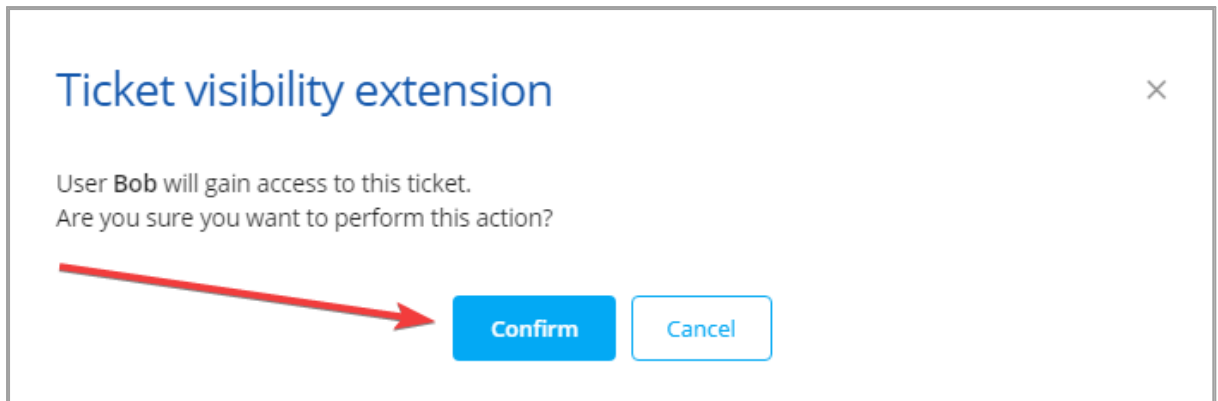
Completed: **Christopher**
On leave until May 12, 04:00 P

Work time: 

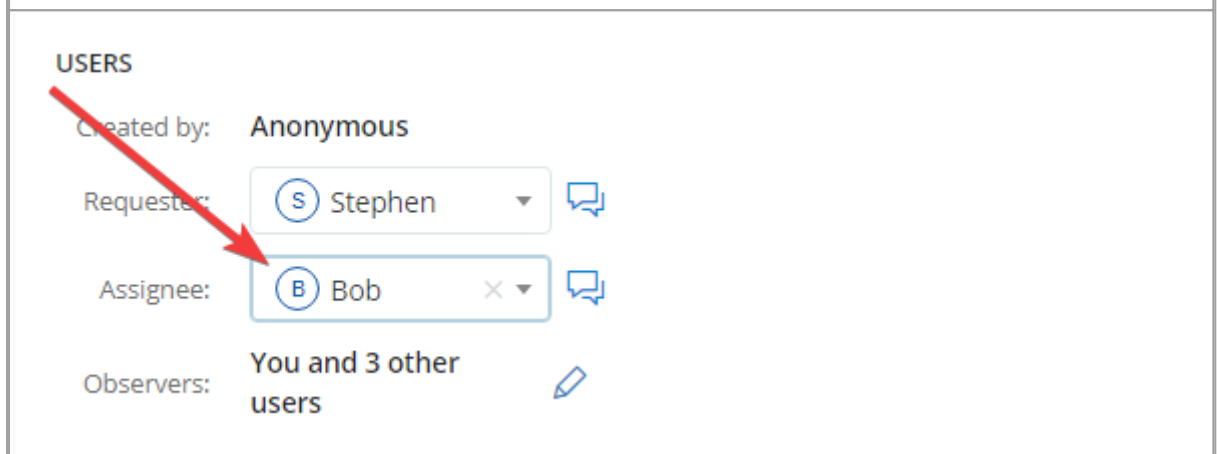


-  Administrator
-  Bob

3. In the Ticket visibility extension window, confirm your choice by clicking the **Confirm** button. (Ensure that you are granting access to the ticket to the correct assignee.)



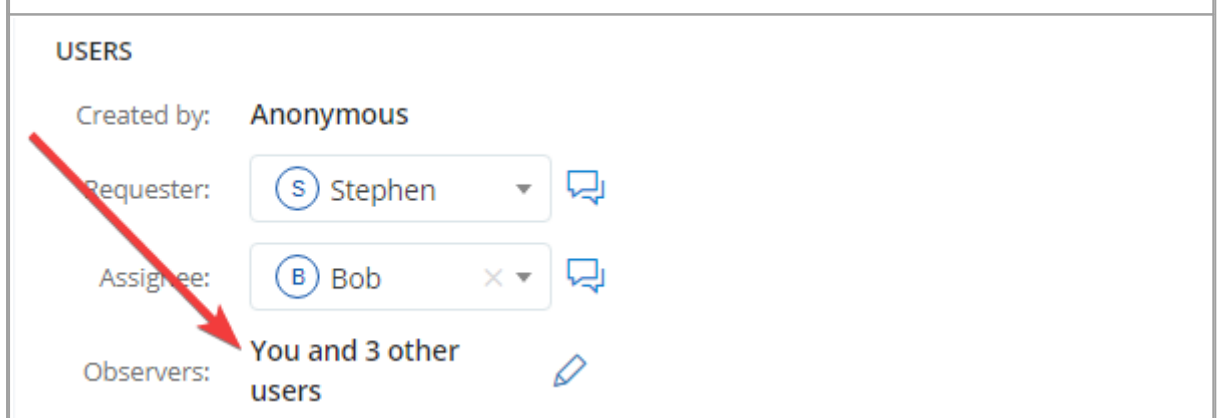
4. Once you have properly completed the steps above, the selected HelpDesk Employee / Administrator has been granted access to the anonymous ticket - his or her information will be displayed in the Assignee field.



Giving access - Observer

To give access to an anonymous ticket from the ticket level by setting the "Observers" field:

1. Click the  icon.




2. Select the appropriate user(s) from the drop-down list (there is a browser at the top of the list) in the **Appointing the ticket observers.**

Change ticket observers ✕

Select the users you want to set as ticket observers **Anonymous ticket:**


Observers: (A) Administrator ✕ (C) Christopher ✕ (S) Stephen ✕ - me
On leave until May 12, 04:00 PM

(B) Bob ✕ (R) Robert ✕

 User Robert will gain access to this ticket.

Save changes Cancel

3. In the **Appointing the ticket observers** window, confirm your choice by clicking the **Save changes** button. (Ensure that you are granting access to the ticket to the correct assignee.) The selected user or users will be displayed in the field. If the user you want to add to the list of the anonymous ticket observers does not have access to this ticket, a warning will be displayed.

4. Once you have properly completed the steps above, the selected user has been granted access to the anonymous ticket - the number of observers will be displayed in the Observers field. To check the list of observers, click the  icon.

Note! Anonymous ticket access is not granted from the ticket level only. The comprehensive protection of access to an anonymous ticket also requires configuration in other sections of the HelpDesk module:

1. [Ticket visibility](#)
2. [Ticket assignment](#)
3. [Automations](#)

User roles in HelpDesk - restricting access to an anonymous ticket

In nVision, we distinguish between the user roles and the roles in the Ticket system (HelpDesk). These roles are linked to each other, e.g. only a user with the Administrator or Super Administrator role can act as the Administrator in the HelpDesk. Depending on the user role and the HelpDesk role configuration, the ability to restrict access to an anonymous ticket may be disabled - this is the case with the Super Administrator role whose rights (except for a few exceptions) cannot be restricted in the entire nVision system.

Characteristics of the roles in HelpDesk - from the point of view of anonymous tickets:

1. User - the user with this role can add new anonymous tickets (if the feature is enabled). By default, the user does not have access to the anonymous ticket they have created themselves.
2. HelpDesk Employee - the user with this role may be able to add new anonymous tickets and may also be designated to process anonymous tickets. To grant or restrict access to anonymous tickets, it is necessary to correctly configure the HelpDesk, including but not limited to the following sections:

- Ticket visibility
- Ticket assignment
- Automations

3. Administrator - the user with this role has unrestricted access to all HelpDesk sections. The Administrator cannot have his access to anonymous tickets disabled or restricted.

Useful links:

 [User management](#) 360

10.5.2.2 Anonymous ticket - ticket visibility

In the HelpDesk, in the **Ticket visibility** section, you can expand or restrict the ticket visibility to users with the HelpDesk Employee role, i.e. configure the parameters that are very important in the case of restricting access to an anonymous ticket.

The visibility rule configuration is divided into two main options:

1. Setting the default rule, i.e. the ticket visibility configuration which will automatically be assigned to new HelpDesk Employees.
2. Editing the visibility rule for a specific HelpDesk Employee.

The screenshot displays the 'Ticket visibility' configuration interface. It features a table with the following data:

| USER | VISIBILITY RULE |
|-------------|------------------|
| Bob | Basic visibility |
| Christopher | Full visibility |
| Stephen | Basic visibility |

Annotations in the image include a red box labeled '1' pointing to the instruction 'Set the default rule' and another red box labeled '2' pointing to the 'Edit' button for the Stephen user's rule.

In the visibility rule configuration window, three visibility levels can be distinguished:

1. Basic - the HelpDesk Employee's ticket list will include the tickets for which the user is a reporter, assignee or observer
2. Extended - the HelpDesk Employee's ticket list will include the tickets for which the user is a reporter, assignee or observer and the tickets where:
 - a) Category is X
 - b) Category is not X
 - c) Reporter belongs to group Y
 - d) Reporter does not belong to group Y

Two conditions concerning different parameters can be combined with each other in such a way that one or both the conditions have to be fulfilled to activate the visibility rule. For this purpose, the **or** and **and** conjunctions are used, for instance:

- The category is X AND the reporter belongs to group Y
 - The category is not X OR the reporter does not belong to group Y
3. Full - all tickets will be displayed in the HelpDesk Employee's ticket list

Ticket visibility rule for user Stephen

1 Basic
Can browse tickets in which the user is the reporter, the assignee or is on the list of observers

2 Expanded
Can browse tickets in which the user is the reporter, the assignee or is on the list of observers, can additionally browse the tickets where:

User is shown the following tickets:

when is equal to

[Add a condition](#)

3 Full
Can browse all tickets

[Save](#) [Cancel](#)

An example ticket visibility configuration for a HelpDesk Employee whose task will be to proceed anonymous tickets could be like this:

Extended visibility rule - the HelpDesk Employee's ticket list will include the tickets for which the user is a reporter, assignee or observer and the tickets where the Category is <name of category for anonymous tickets>

Ticket visibility rule for user Stephen

Basic
Can browse tickets in which the user is the reporter, the assignee or is on the list of observers

Expanded
Can browse tickets in which the user is the reporter, the assignee or is on the list of observers, can additionally browse the tickets where:

User is shown the following tickets:

when is equal to

[Add a condition](#)

Full
Can browse all tickets

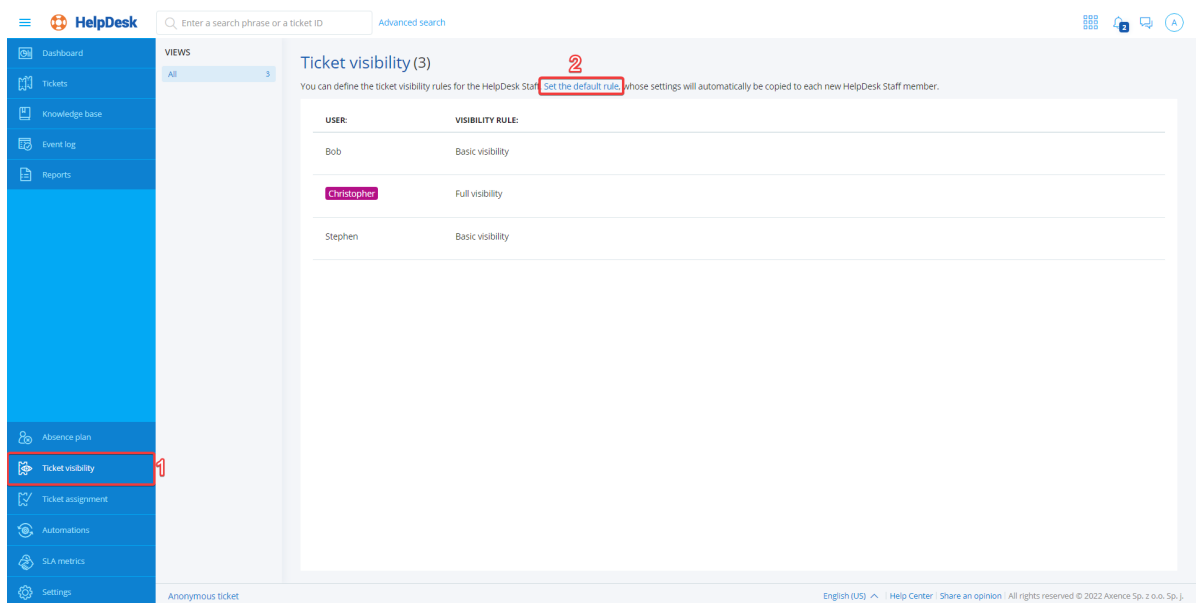
[Save](#) [Cancel](#)

Important: please note that in addition to setting the appropriate visibility rule for the HelpDesk Employee whose task will be to proceed anonymous tickets, it is also important to ensure that other HelpDesk Employees do not have access to the anonymous tickets, e.g. through the "Full" ticket visibility rule.

Setting the default rule

To set a rule as the default one, log in to the HelpDesk module as the Administrator and:

1. In the flyout menu on the left side of the window, click the **Ticket visibility**.
2. Click the **Set the default rule** link.
3. Configure the visibility rule, and then click the **Save** button.



The screenshot shows the HelpDesk interface. On the left, the 'Ticket visibility' menu item is highlighted with a red box and a red arrow labeled '1'. The main content area shows the 'Ticket visibility (3)' configuration page. A red box highlights the 'Set the default rule' link, with a red arrow labeled '2' pointing to it. Below this, there is a table with columns 'USER' and 'VISIBILITY RULE':

| USER | VISIBILITY RULE |
|-------------|------------------|
| Bob | Basic visibility |
| Christopher | Full visibility |
| Stephen | Basic visibility |

Default ticket visibility rule

Basic
Can browse tickets in which the user is the reporter, the assignee or is on the list of observers

Expanded
Can browse tickets in which the user is the reporter, the assignee or is on the list of observers, can additionally browse the tickets where:

User is shown the following tickets:

when is equal to

Full
Can browse all tickets

Once you have properly completed the steps above, the visibility rule in the HelpDesk will be updated.

Editing a visibility rule

To add a visibility rule, log in to the HelpDesk module as the Administrator and:

1. In the flyout menu on the left side of the window, click the **Ticket visibility**.
2. Select the HelpDesk Employee whose visibility rule you want to edit (when you hover over the field of the relevant HelpDesk employee, the **Edit**, **Copy to...**, **Copy from default rule** buttons are displayed).
3. Click the **Edit** button.
4. Configure the visibility rule, and then click the **Save** button.

The screenshot shows the HelpDesk interface. On the left sidebar, the 'Ticket visibility' option is highlighted with a red box and a red '1'. The main content area displays a table titled 'Ticket visibility (3)'. The table has two columns: 'USER' and 'VISIBILITY RULE'. The rows are: Bob (Basic visibility), Christopher (Full visibility), and Stephen (Basic visibility). The Stephen row is highlighted with a red box and a red '2'. To the right of the Stephen row, there are three buttons: 'Edit', 'Copy to...', and 'Copy from the default rule'.

Ticket visibility rule for user Stephen

Basic
Can browse tickets in which the user is the reporter, the assignee or is on the list of observers

Expanded
Can browse tickets in which the user is the reporter, the assignee or is on the list of observers, can additionally browse the tickets where:

User is shown the following tickets:

when is equal to

Full
Can browse all tickets

Once you have properly completed the steps above, the visibility rule for the specific HelpDesk Employee will be updated.

10.5.2.3 Anonymous ticket - ticket assignment

Ticket assignment rule configuration must be correct to properly restrict or extend access, among other things, to anonymous tickets. For more information on assigning tickets, click the link: [ticket assignment](#).

The screenshot shows the 'All ticket assignment rules (1)' configuration page in the HelpDesk interface. The page title is 'All ticket assignment rules (1)' with an 'Add rule' button. Below the title, it states 'Each new ticket will be assigned according to the following rules:'. A table is displayed with the following content:

| USER: | AUTOMATICALLY RECEIVES NEW TICKETS: | |
|---------------|-------------------------------------|-------------------------------------|
| Administrator | All | <input checked="" type="checkbox"/> |

At the bottom of the page, there is an 'EMBEDDED MECHANISM ACTIVATION SEQUENCE' section with a description: 'After ticket creation → Execute automation → Assign the ticket according to the rules. The algorithm selects the user who has the fewest unclosed tickets at the moment. If a few users have the same number of unclosed tickets, the person whose last received ticket is the oldest will be selected.' There is also a 'SEE ALSO' section with links to 'Help center - Ticket assignment' and 'Automations'.

10.5.2.4 Anonymous ticket - automations

The Automation section allows the effective and efficient anonymous ticket processing scheme to be created. You should be very careful when configuring automatic rules as you can mistakenly give access to anonymous tickets to someone who has not been designated to process them. For the guides on the main features of the Automation section, please refer to another part of this manual (links below).

Related topics:

[Automation list](#)

[Adding an automation](#) ⁴⁶⁰

[Automation conditions](#)

[Automation actions](#)

[Editing an automation](#) ⁴⁶⁵

[Activating/deactivating an automation](#) ⁴⁶⁶

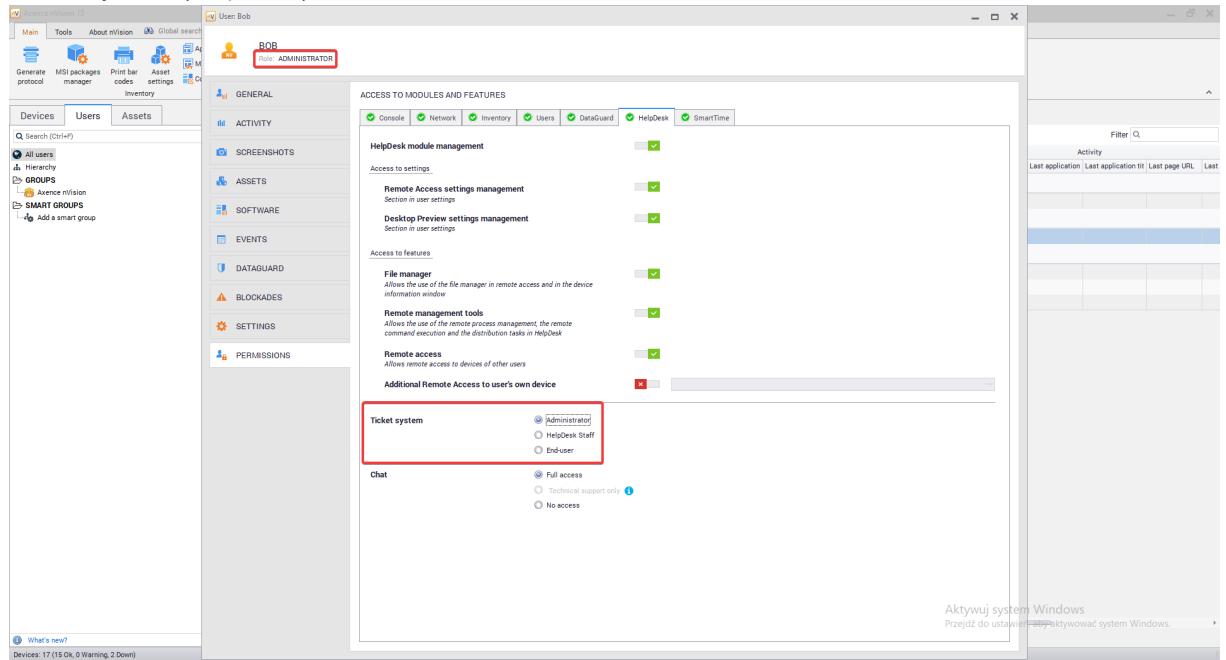
[Deleting an automation](#) ⁴⁶⁷

10.5.3 Anonymous Tickets

10.5.3.1 Launching Anonymous Tickets

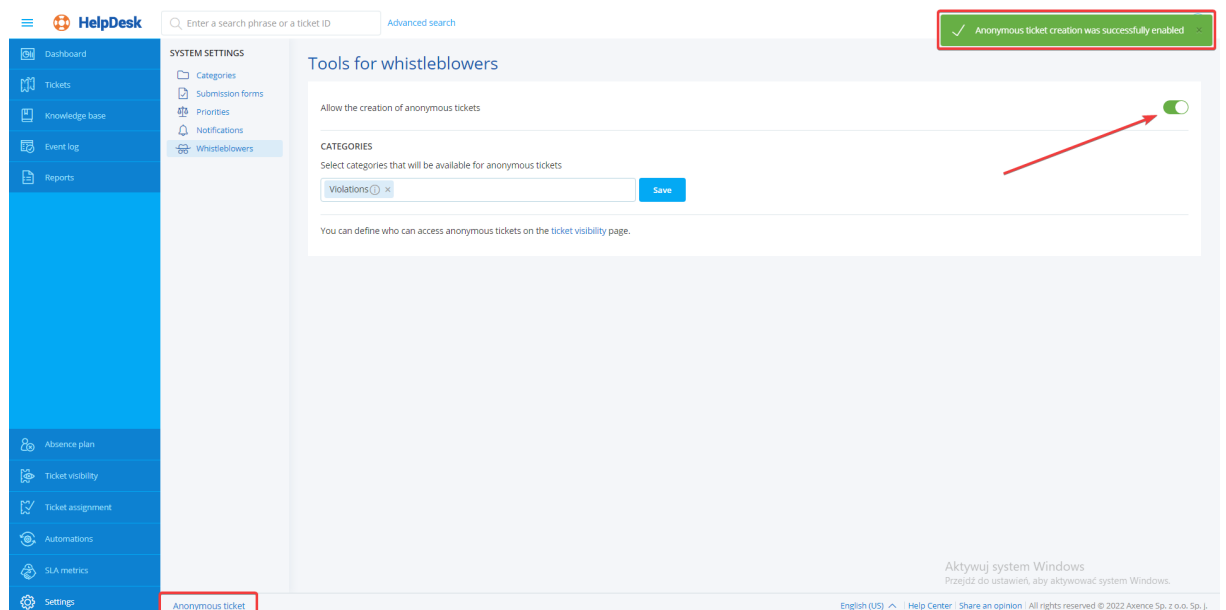
The add anonymous ticket feature in the HelpDesk is not enabled permanently - depending on the rules applicable within the specific organization or institution, it may either be enabled or disabled.

The anonymous ticket settings can only be configured by the user with the Administrator role in the Ticket system (HelpDesk).



To enable the Anonymous ticket feature, log in to the HelpDesk module as the **Administrator** and:

1. In the flyout menu on the left side of the window, click the **Settings**.
2. Enter the whistleblower settings - **Whistleblowers**.
3. Click the slider.



Once you have properly completed the steps above, a message will appear in the upper right corner of the window confirming that the creation of anonymous tickets has been enabled and on the left side of the footer a link which has not been visible so far will appear, i.e. **Anonymous ticket**.

You can disable the anonymous ticket creation feature at any time. To do this, click the slider again (if anonymous tickets are enabled). After clicking, a message confirming that the creation of anonymous tickets has been disabled and the Anonymous ticket link on the left side of the footer will disappear - creation of new anonymous tickets will not be possible from now on.

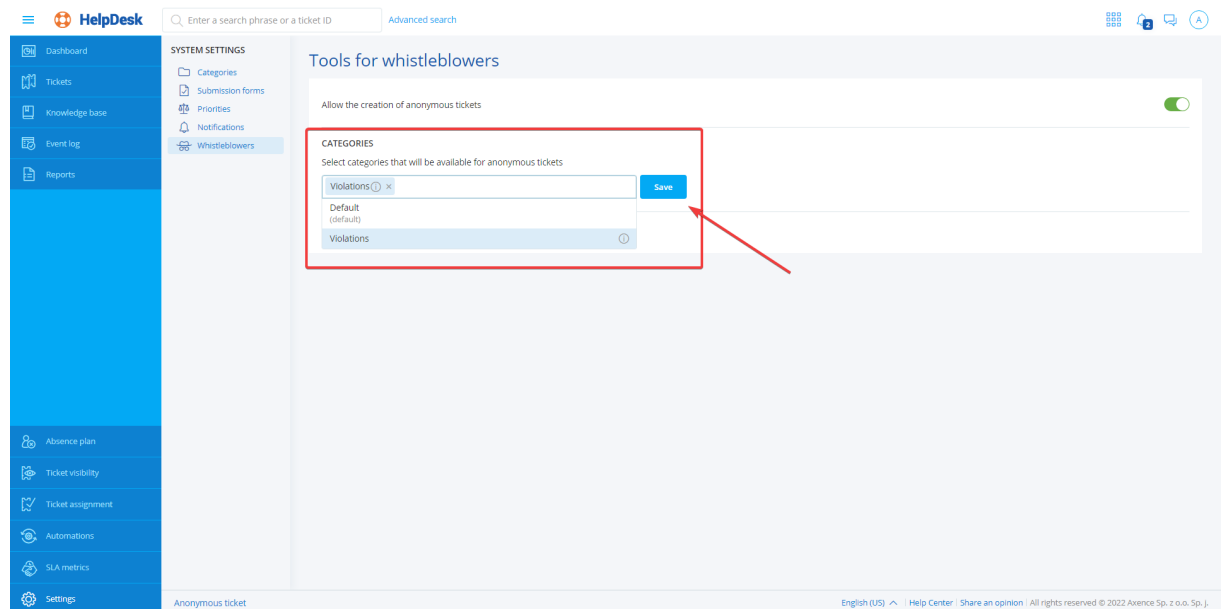
10.5.3.2 Configuring anonymous tickets

When configuring anonymous tickets, remember to select the appropriate category the anonymous tickets will be assigned to.

To select the [categories](#) that will be available when creating anonymous tickets, log in to the HelpDesk module as the Administrator and:

1. In the flyout menu on the left side of the window, click the **Settings**.
2. Enter the whistleblower settings - **Whistleblowers**.
3. Click the field to the left of the **Save** button.

After clicking, a list of all categories that exist in the HelpDesk will drop down. Select the category (you can select more than one category) and confirm your selection by clicking the **Save** button.



Anonymous tickets - no dedicated category

In the HelpDesk, the anonymous ticket settings allow for a situation where no specific category is assigned for the tickets created using the anonymous ticket form. **If this is the case, a message will be displayed and anonymous tickets will be assigned to the default category in the HelpDesk.** This is not recommended because anonymous tickets are very likely to be mixed with non-anonymous ones, and additionally anonymous tickets may be accessed by the users who would otherwise be deprived of such access.

Useful links:

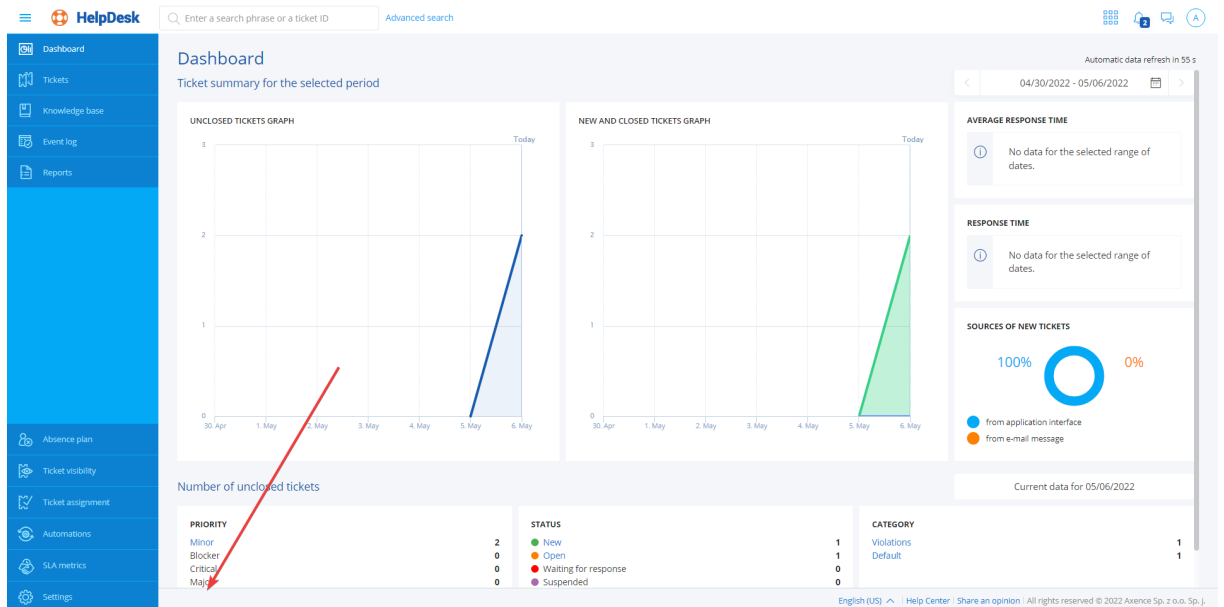
- [Adding categories](#)
- [Restricting access to an anonymous ticket](#)
- [Access restriction - ticket visibility](#)
- [Access restriction - ticket assignment](#)
- [Access restriction - automations](#)

10.5.3.3 Anonymous ticket link visibility

The anonymous ticket form is available in two locations (if the anonymous ticket creation feature is enabled) and displayed for both the user logged in to the HelpDesk/Agent and the user not logged in:

1) link in the HelpDesk's footer

| PRIORITY | STATUS | CATEGORY |
|----------|----------------------|------------|
| Minor | New | Violations |
| Blocker | Open | Default |
| Critical | Waiting for response | |
| Major | Suspended | |



2) in the Agent's drop-down menu

10.5.3.4 Processing an anonymous ticket

In terms of processing by the HelpDesk employees, an anonymous ticket does not differ in its form from the processing of a regular ticket. The most significant difference is that the individual reporting a specific violation does not usually have access to the ticket. This person cannot monitor the progress of work on the ticket or participate actively for instance by adding comments. However, there is an exception to this rule. In the anonymous ticket adding form, the reporter may provide their contact details. This information can then be used by the assignee to contact the reporter and grant access to the ticket, e.g. by setting him as the reporter or by adding him to the list of anonymous ticket observers.

To view an anonymous ticket, you must log in to the HelpDesk using the account of the user who has access to the specific anonymous ticket and then:

1. In the flyout menu on the left side of the window, click the **Tickets**.
2. In the ticket list, click the selected anonymous ticket:
 - a) click the link in the "Subject" column
 - b) click the specific anonymous ticket line, and then click the "View details" button at the bottom part of the flyout ticket preview on the right side of the window.

The screenshot shows the HelpDesk interface with a list of tickets. A red arrow points to the 'Anonymous ticket' subject in the table.

| STATUS | ID | PRIORITY | SUBJECT | CATEGORY | LAST UPDATE | REQUESTER | ASSIGNEE |
|--------|----|----------|------------------|------------|----------------|---------------|---------------|
| | 2 | Minor | Anonymous ticket | Violations | 39 minutes ago | Stephen | Bob |
| | 1 | Minor | No internet | Default | 3 hours ago | Administrator | Administrator |

Both the graphic and functional layout of an anonymous ticket is identical to that of a regular ticket. The difference is that:

1. The “Created by” field will always display “Anonymous” as the parameter
2. The “Reporter” field by default displays “Anonymous” - changes can be made during the processing of the ticket
3. If the reporter has provided their contact details, they will appear in the ticket content field, below the descriptive content of the ticket

The screenshot shows the details of an anonymous ticket. A red arrow points to the 'View details' button.

| STATUS | ID | PRIORITY | SUBJECT | CATEGORY | LAST UPDATE | REQUESTER |
|--------|----|----------|------------------|------------|----------------|---------------|
| | 2 | Minor | Anonymous ticket | Violations | 39 minutes ago | Stephen |
| | 1 | Minor | No internet | Default | 3 hours ago | Administrator |

Anonymous ticket
Anonymous ticket

COMMENTS

Add internal comment

Internal Add

Status: ● Open

ID: 2

Direct link: <http://localhost:8080/nhel>

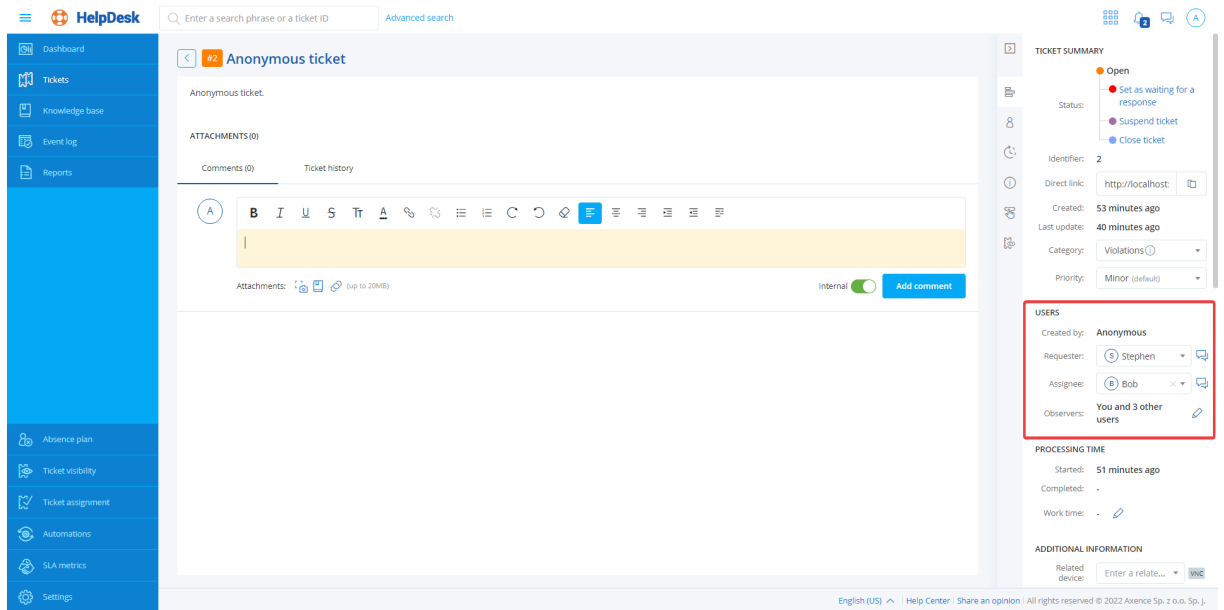
Created: 53 minutes ago

Last update: 40 minutes ago





Requester: Stephen

Assignee: Bob

[View details](#)



Useful links:

-  [Adding a comment](#) 390
-  [Adding attachments and screenshots](#)
-  [Editing a ticket subject](#)
-  [Closing a ticket](#)
-  [Restricting access to an anonymous ticket - overview](#)

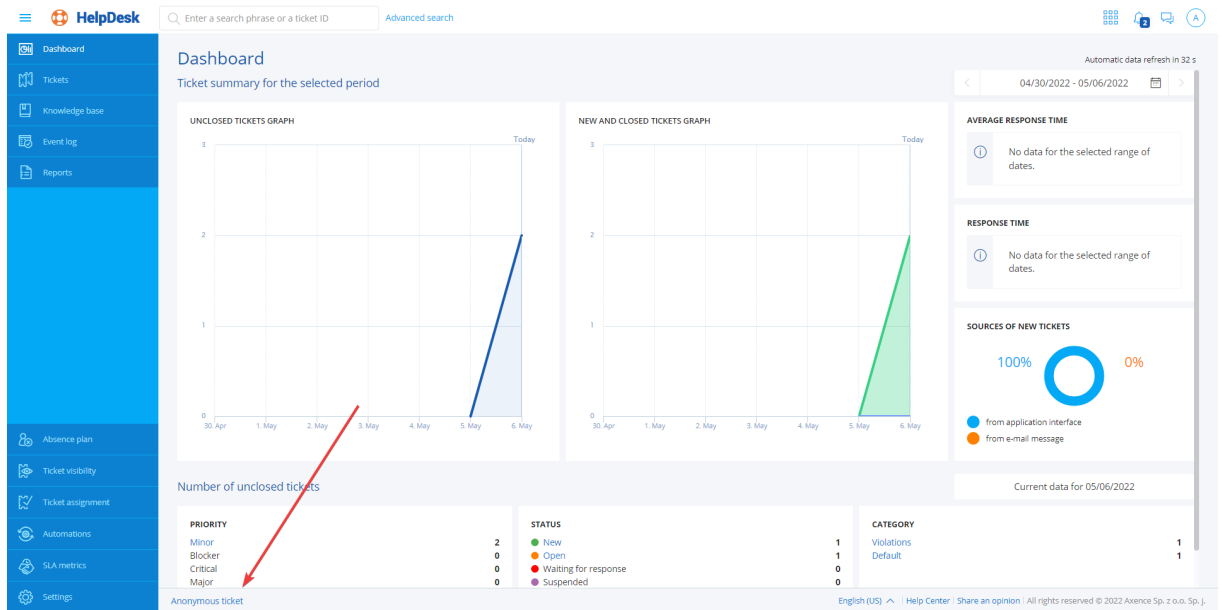
10.5.3.5 Adding an anonymous ticket

The creation of an anonymous ticket is very different from that of a regular ticket. The anonymous ticket is added using a special form. Besides, the reporter does not have access to the ticket after it has been created (unless they are granted access to the anonymous ticket in the course of its proceeding).

To add a new anonymous ticket from the HelpDesk interface:

1. Click the **Anonymous tickets** link in the footer.
2. Click the **Select category** field and then click the selected category name.
3. Enter the subject of the anonymous ticket.
4. Describe comprehensively the violation you want to report.
5. (OPTIONALLY) Provide your contact details so that the assignee can contact you - **Read carefully the message above the “Contact details” field!**
6. Click the **Add ticket** button.

Note! Make sure that the [anonymous ticket creation option](#) is enabled!



Adding an anonymous ticket

This ticket will remain anonymous and will not be associated with your account

2 Category: Select category

3 Subject: Enter a ticket subject

4 Description: [Rich text editor]

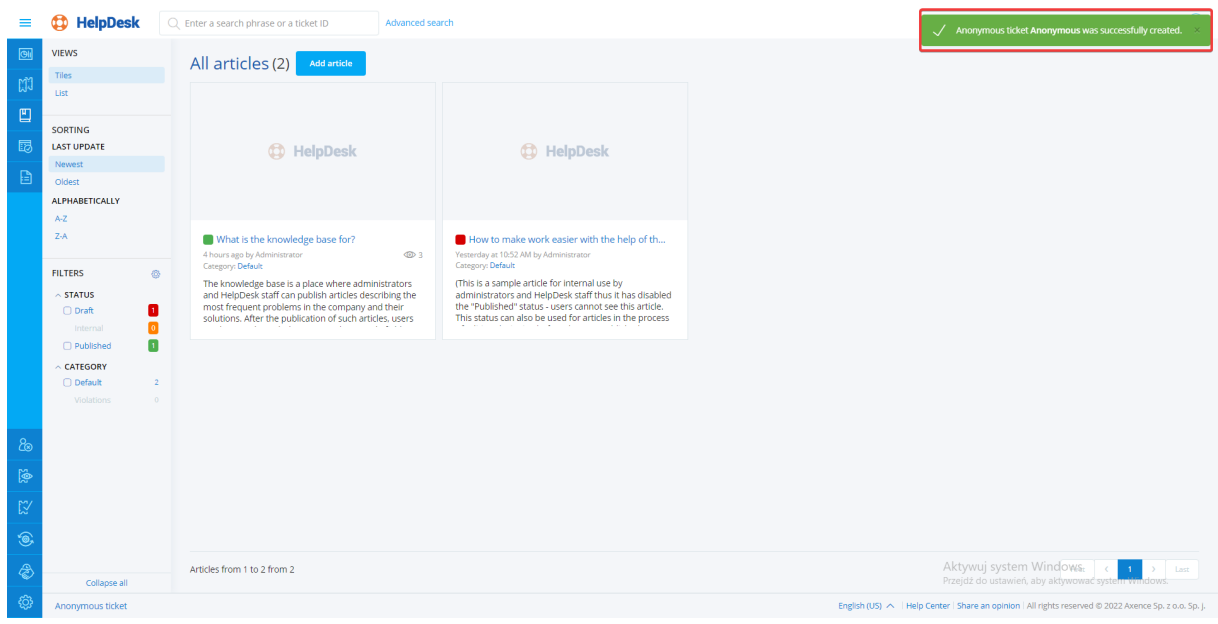
Providing your contact information is not obligatory.

5 1 This data will not be used by the system to send you any updates or notifications. Only people approved by the administrator will have access to this data and can use it to contact you directly. After creating the ticket you will not be able to follow its processing.

Contact information: Enter an e-mail address or a phone number 6

Add ticket Cancel

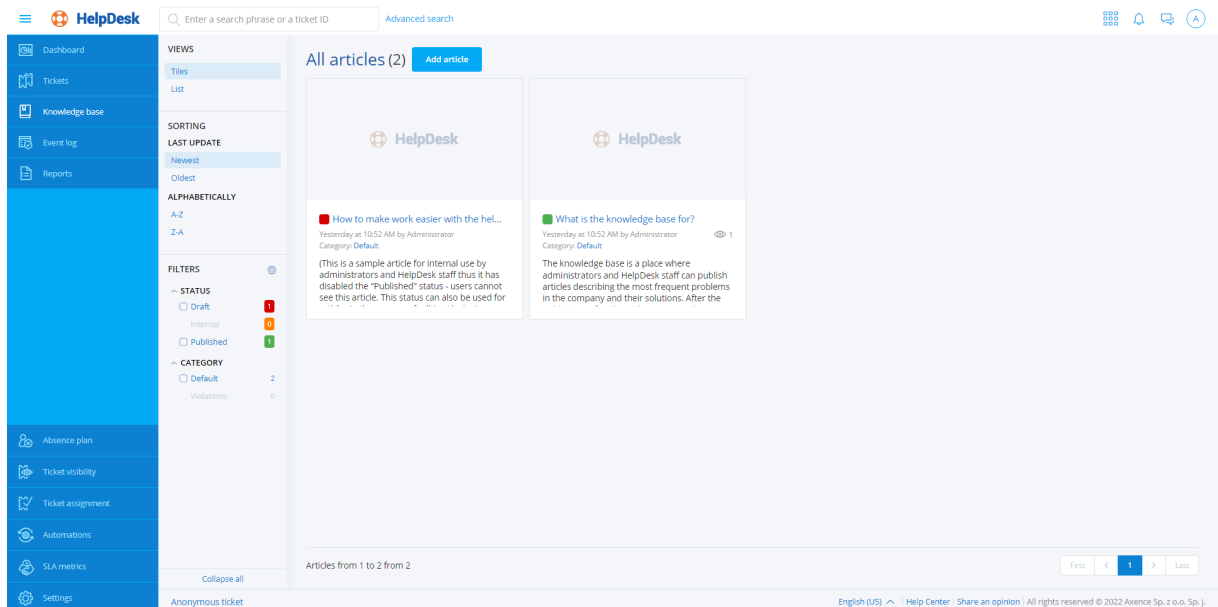
Once you have properly completed the steps above, the form window will close and the “Anonymous ticket <ticket name> has been successfully created” message will appear in the upper-right corner of the screen.



10.6 Knowledge base

10.6.1 Knowledge base - overview

The knowledge base is a space where Administrators and HelpDesk employees can publish articles describing the procedures used in the given organization, and the most common issues and their solutions. After such articles have been published, users can browse them or use the **Search** field to search for the article describing the solution to the issue which they have encountered. If the knowledge base search produces no results in the form of a description of the solution to the given issue, the user can create a trouble ticket and describe the issue.



Related topics

 [Starting the HelpDesk interface](#)

 [Article list](#)

 [Adding an article](#)

 [Editing an article](#)

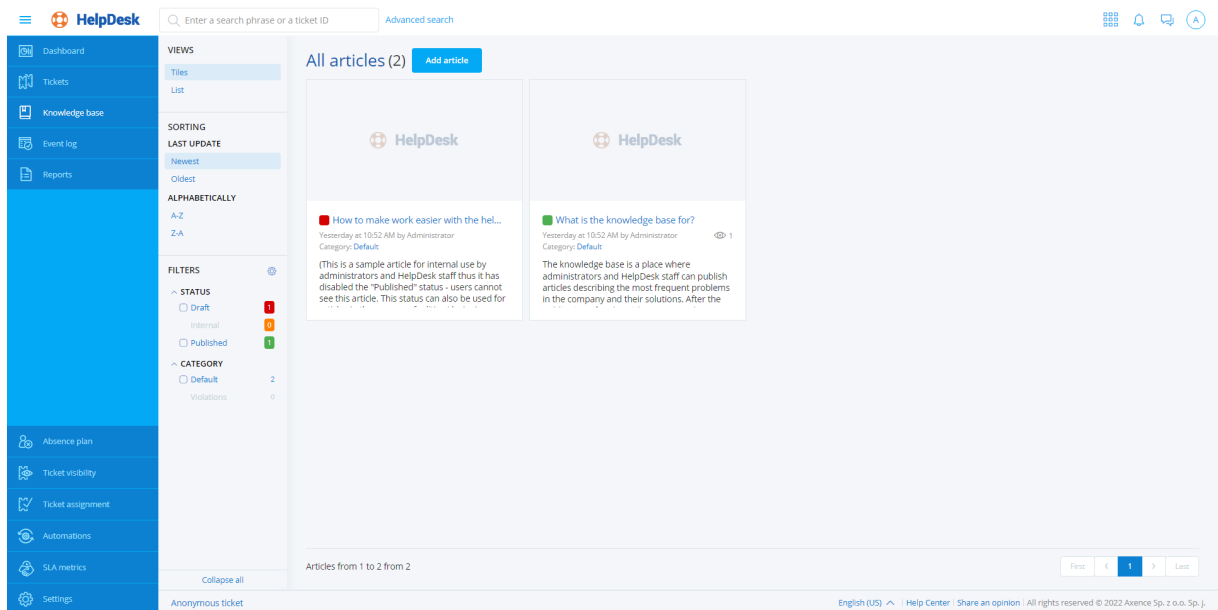
 [Deleting an article](#)

 [Trouble tickets - overview](#)

 [Search bar](#) ³⁸⁰

10.6.2 Article list

The article view shows the list of articles present in the knowledge base. The view is coherent with the [ticket list](#) ³⁸³ view.



In the left part of the window, there is the main navigation (see [Main views](#) ³⁷⁵) and the quick preview column. The quick preview allows you to rapidly display a data set from the specific area of interest. For instance, you can display unpublished articles, which, additionally, belong to one of the two selected categories.

Article list

The main part of the described view is the article list table. Each article is represented by a single tile. The following data are displayed within a tile:

- Article status (red – draft, green – published, orange - internal)
- Title
- Context actions: **editing** (only for the HelpDesk support employee and Administrator) and **deleting** (only for the Administrator)
- Article cover (if it was defined)
- Excerpt from the article text
- Date of creation
- Date of last update

- Category
- Number of article visits by end users (only for the HelpDesk support employee and Administrator)

To open the selected article, click its title.

Related topics

 [Starting the HelpDesk interface](#)

 [Knowledge base - overview](#)

 [Trouble tickets - overview](#)

 [Article list](#)

 [Adding an article](#)

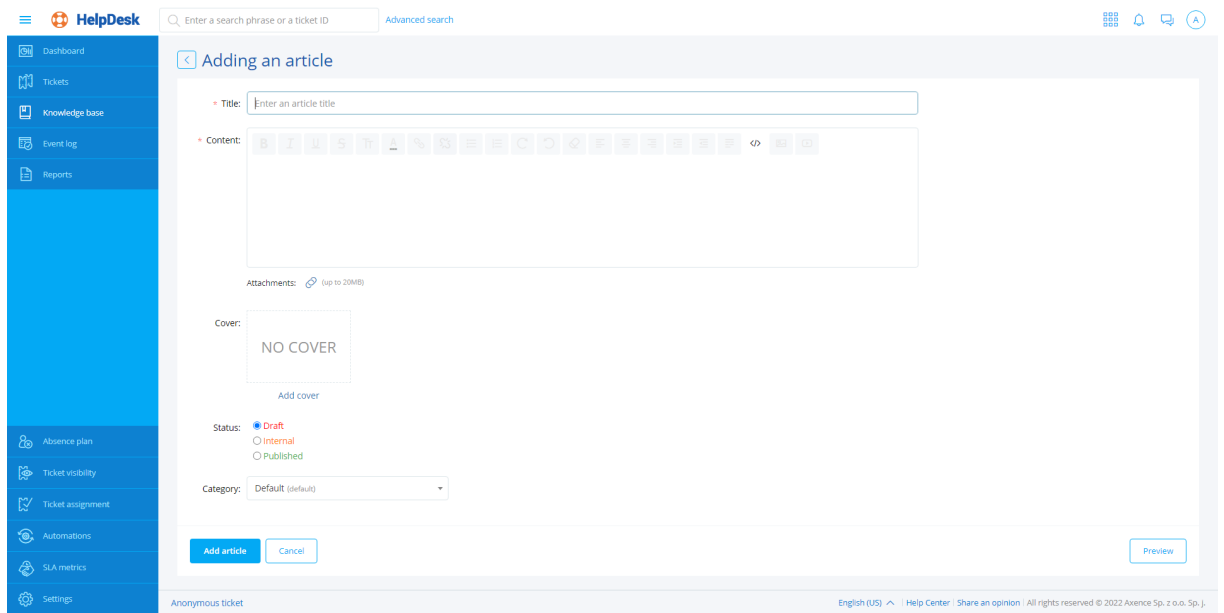
 [Editing an article](#)

 [Deleting an article](#)^[421]

10.6.3 Adding an article

To create a new article in the HelpDesk interface:

1. In the **Knowledge base** view click the **Add article** button.
2. Add article **Cover** (optionally).
3. Enter article **Title**.
4. Type the article contents in the embedded [text editor](#)^[376].
5. You can attach an image or a link to an external video with the use of **Upload image** and **Insert video** options.
6. Set the article **Status** as **Draft, Published or internal** (default setting: Draft). Articles marked as drafts are not visible to end users. Articles marked as internal are only visible to HelpDesk employees. You can [supplement the article and edit its status](#)^[420] at a later time.
7. Select the article's **Category** from the list of available categories. You can [add a new category](#)^[363] without interrupting the article creation process.
8. You can view the created article by clicking **Preview**. To return to the article editing window, click **Back to editing** button.
9. When the article is completed, click the **Add article** button.



Related topics

 [Logging in to the HelpDesk interface](#)

 [Knowledge base](#)

 [Article list](#)

 [Editing an article](#)

 [Deleting an article](#) ⁴²¹

10.6.4 Editing an article






To edit an article in the HelpDesk interface:

1. In the **Knowledge base** view click **Edit** button on the tile of the article to be edited.
2. To edit the article title, click the pencil icon on the right-hand side of the title, enter the new title and click **Save changes** button.
3. Modify the article contents in the embedded [text editor](#) ³⁷⁶.
4. You can attach an image or a link to an external video with the use of **Upload image** and **Insert video** options.
5. To change the article cover, in the article summary in the right-hand side of the window, click the pencil icon on the cover (or **Add cover**).
6. To change the article status, in the article summary in the right-hand side of the window select **Status: Draft, Published or Internal**.
7. To change the article category, in the article summary in the right-hand side of the window select **Category** from the list of available categories. You can [add a new category](#) ³⁶³ without interrupting the article creation process.

- You can view the created article by clicking **Preview**. To return to the article editing window, click **Back to editing** button.
- When modifications are complete, click the **Save changes** button.

The screenshot displays the HelpDesk interface. On the left is a blue sidebar with navigation options: Dashboard, Tickets, Knowledge base, Event log, Reports, Absence plan, Ticket visibility, Ticket assignment, Automations, SLA metrics, and Settings. The main content area shows an article titled 'What is the knowledge base for?' with a rich text editor containing the text: 'The knowledge base is a place where administrators and HelpDesk staff can publish articles describing the most frequent problems in the company and their solutions. After the publication of such articles, users can browse through them or use the 'Search' field to find an article describing the solution to the problem they have encountered. If a description of the solution for a problem cannot be found in the knowledge base, then the user can create a ticket describing the problem.' Below the editor are 'Save changes', 'Cancel', and 'Preview' buttons. On the right, an 'ARTICLE SUMMARY' panel shows 'NO COVER', 'Add cover', 'Direct link: http://localhost:1', 'Created: Yesterday at 10:52 AM', 'Last update: Yesterday at 10:52 AM by Administrator', 'Article read: 2 times', 'Status: Published', and 'Category: Default (default)'. The footer includes 'Anonymous ticket', 'English (US)', 'Help Center', 'Share an opinion', and 'All rights reserved © 2022 Axence Sp. z o.o. Sp. J.'

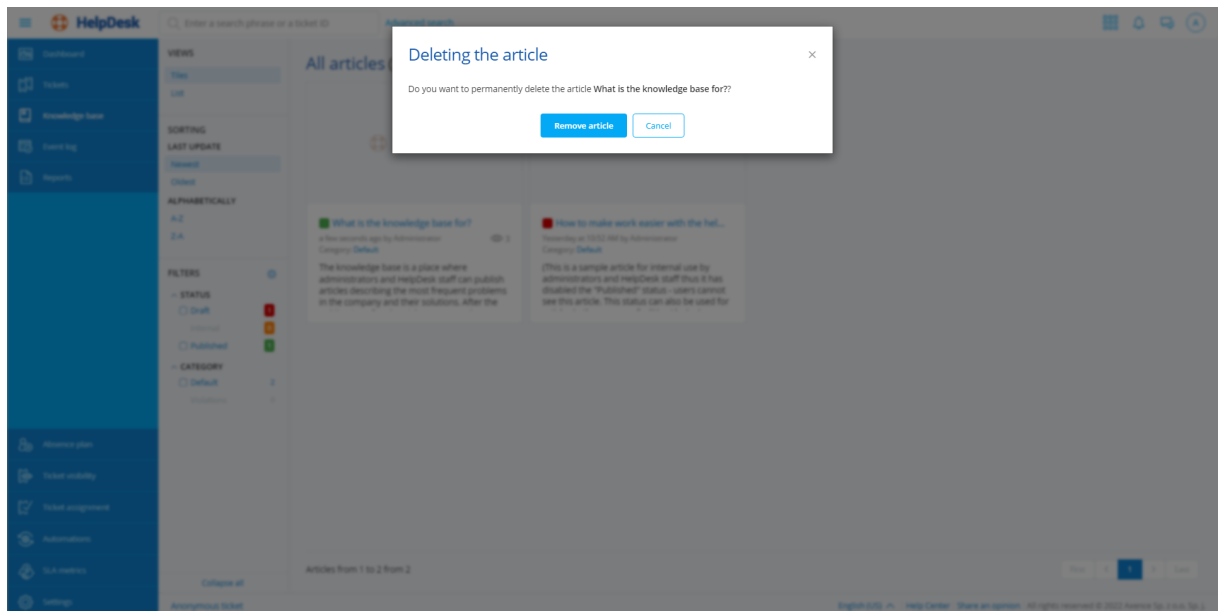
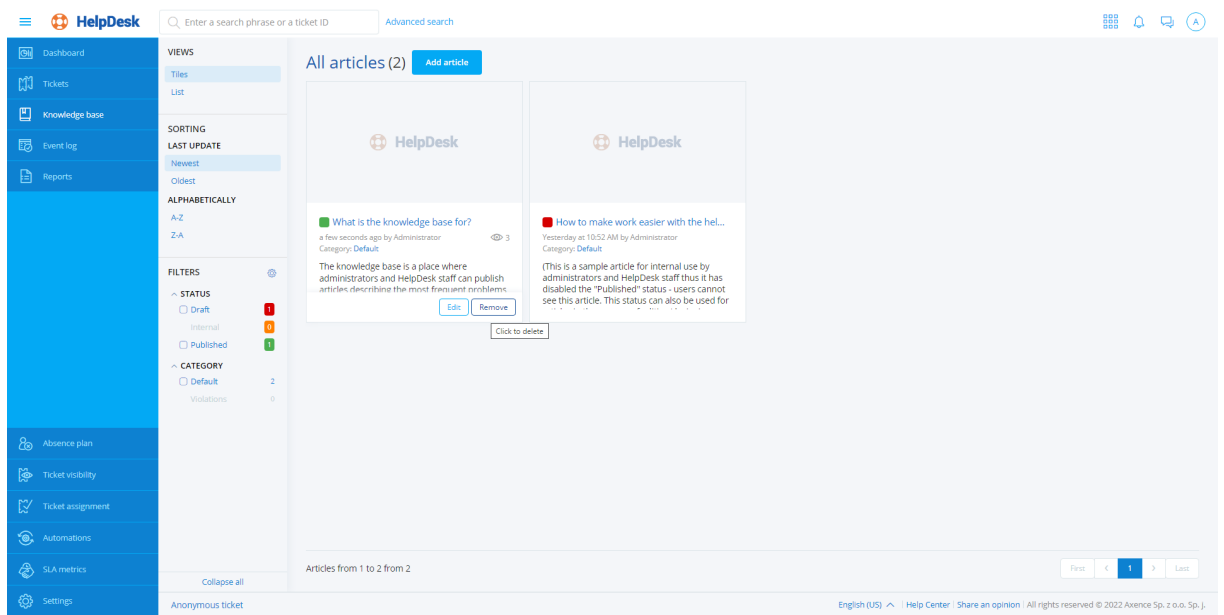
Related topics

-  [Logging in to the HelpDesk interface](#)
-  [Knowledge base](#)
-  [Article list](#)
-  [Adding an article](#)
-  [Deleting an article](#) ⁴²¹

10.6.5 Deleting an article

To delete an article in the HelpDesk interface:

- In the **Knowledge base** view click the **Remove** button on the tile of the article to be deleted.
- A dialog box will appear. Confirm your decision to delete an article by clicking the **Remove article** button. The deleted article cannot be restored.



Related topics

 [Logging in to the HelpDesk interface](#)

 [Knowledge base](#)

 [Article list](#)

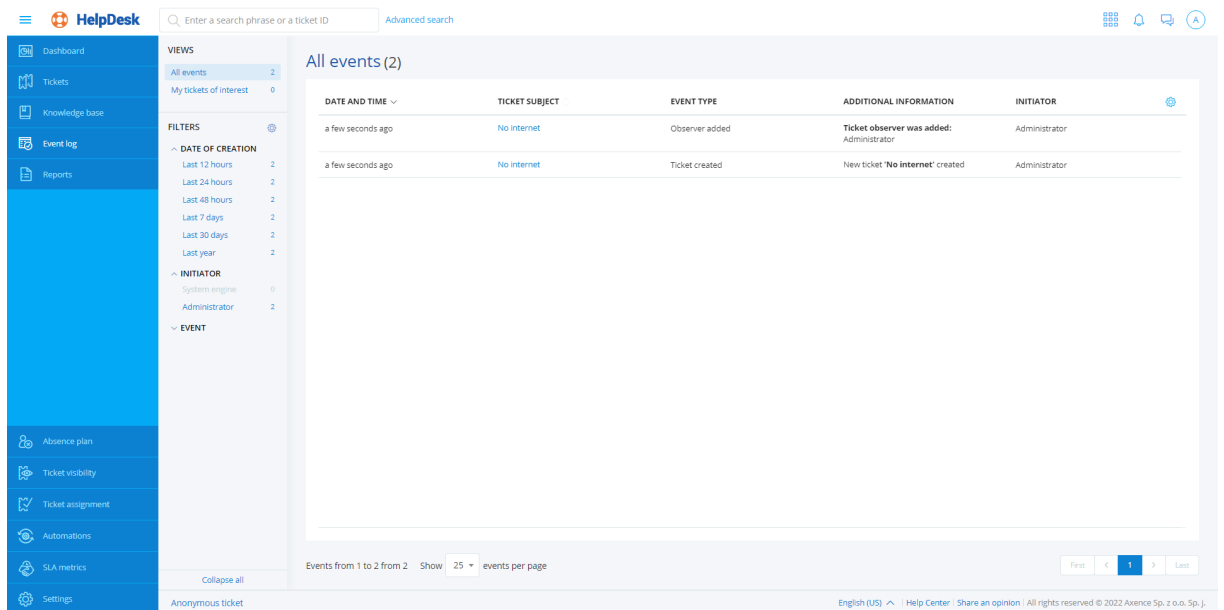
 [Adding an article](#)

 [Editing an article](#) ⁴²⁰

10.7 Event log

The event log view presents the list of all operations related to trouble tickets in the HelpDesk system. The event log allows the history of changes to tickets to be tracked, to optimize work and to clarify possible misunderstandings.

Note: the event log includes only ticket-related operations and it does not cover changes in the article database. The event log is visible for operations of Administrators and HelpDesk support employees.



The event log view is coherent with the [ticket list](#)^[383] and [article list](#)^[418] views. In the left part of the window, there is the main navigation (see [Main views](#)^[375]) and the quick preview column. The quick preview allows you to rapidly display a data set from the specific area of interest. For instance, you can display the events related only to applied automations and priority changes or all the events for a given ticket which have taken place in the last week.

To change the displayed columns or their sequence, click the table settings button [icon] in the upper right corner of the table. To sort the table contents by a given column, click the arrow at the column name. Below the table you can select how many tickets are to be displayed per page, and also go to the next pages.

Filters

The quick preview column in the left-hand side of the window offers the following event filters:

- all events related to the ticket object (default selection for the Administrator, option invisible for HelpDesk users),
- all events related to a ticket assigned to me (default selection for HelpDesk users),
- events from last week (option to select the types of displayed events),
- events from last month (option to select the types of displayed events),
- events from last year (option to select the types of displayed events),
- events by type (many items can be selected).

Filtering events by type includes the following options:

| Event type | Additional displayed information | Event initiator |
|--------------------------|--------------------------------------|--------------------|
| Comment added | Comment text | User name |
| Automation action failed | Name of the failed automation action | HelpDesk mechanism |

| Event type | Additional displayed information | Event initiator |
|---------------------------------|---|--------------------|
| Tickets merged | Name of the ticket, which was closed and merged into another ticket | User name |
| Automation started | Name of applied automation | HelpDesk mechanism |
| Ticket has been removed | Name of removed ticket | User name |
| Ticket has been created | Name of created ticket | User name |
| Work time has been changed | Ticket processing time | User name |
| Category has been changed | Current category | User name |
| Assignee changed | Name of the assigned user | User name |
| Related device has been changed | Name of related device | User name |
| Relation has been changed | Name of related ticket | User name |
| Priority has been changed | Current priority | User name |
| Status changed | Current status | User name |
| Subject has been changed | Current ticket subject | User name |
| Requester has been changed | Name of the requested user | User name |

Related topics

 [Starting the HelpDesk interface](#)

 [Main views](#)

 [Ticket list](#)

 [Article list](#)

 [Automations - overview](#) ⁴⁵⁸

10.8 Reports

10.8.1 Report generation

There are 32 types of HelpDesk module reports, covering the most common scenarios allowing statements to be generated for:

Tickets:

✓ [Closed tickets](#): ⁴²⁷

- ✓ Closed tickets by days
- ✓ Closed tickets by weeks
- ✓ Closed tickets by months
- ✓ Closed tickets by assignees
- ✓ Closed tickets by priorities
- ✓ Closed tickets by categories
- ✓ Closed tickets by departments
- ✓ [Activity and ticket response time:](#) ^[440]
 - ✓ Response time by days
 - ✓ Response time by weeks
 - ✓ Response time by months
 - ✓ Summary - number of events
 - ✓ User activity in tickets
 - ✓ First response time by users
- ✓ [Unclosed tickets reports:](#) ^[447]
 - ✓ Unclosed tickets summary
 - ✓ Unclosed tickets by assignees
 - ✓ Unclosed tickets by priorities
 - ✓ Unclosed tickets by categories
 - ✓ Unclosed tickets by departments

SLA reports:

- ✓ [Closed tickets under SLA reports](#) ^[454]
 - ✓ Closed tickets under SLA summary
 - ✓ Closed tickets under SLA by days
 - ✓ Closed tickets under SLA by weeks
 - ✓ Closed tickets under SLA by months
 - ✓ Closed tickets under SLA by assignees
 - ✓ Closed tickets under SLA by departments
- ✓ [SLA metric course reports](#) ^[455]
 - ✓ SLA metric course summary
 - ✓ SLA metric course by days
 - ✓ SLA metric course by weeks
 - ✓ SLA metric course by months
 - ✓ SLA metric course by assignees
 - ✓ SLA metric course by departments

✓ [SLA metric violation reports](#) 

- ✓ SLA violations by metric violation date
- ✓ SLA violations by ticket closure date

To generate a report:

1. Log in to the HelpDesk interface as the **Administrator**, navigate to the **Reports** view.
2. Select a report group, click the report type name.
3. In report wizard, specify the preconditions (arguments), range and the form in which the results are to be presented.
4. The generated report can be exported to **CSV** or **XLS**.

TICKETS REPORTS

Closed ticket reports are generated for tickets which have already completed the processing (in read-only form – cannot be edited). Reports of this group enable the control of ticket handling quality (for specific days, months, by individual technical support employees).

The reports are archival and unchangeable. Re-generation of a report with the same arguments will always produce the same results.

Activity and ticket response time reports summarize the total number of system events in a given period. Reports from this group offer information about the data volumes processed by the system.

The reports are archival and unchangeable. Re-generation of a report with the same arguments will always produce the same results.

Unclosed tickets reports show data on tickets currently being processed in the system. Reports from this group offer information about the current system status, e.g. the current number of tickets.

The reports work as views – re-generation of the report can produce different results each time.

SLA METRIC REPORTS

Closed tickets under SLA reports display the statistics of closed tickets processed under SLA metrics. This group of reports enables the investigation into how the service level agreement provisions were fulfilled.

The reports are archival. Re-generation of a report with the same arguments will always produce the same results.

SLA metric course reports display the events that occurred during the SLA metric run. The purpose of this group of reports is to monitor the tasks executed under the service level agreement.

SLA violation reports display the tickets with a violated SLA metric. The purpose of this group of reports is to investigate the incidents of service level agreement breaches.

Dates in reports pertain to the local time of the machine where the Axence nVision® Server (HelpDesk service) is installed.

10.8.2 Tickets reports

10.8.2.1 Closed ticket reports

Reports are generated for tickets which have already completed the processing (available in read-only form – cannot be edited). Reports of this group enable the control of ticket handling quality (for specific days, months, by individual technical support employees).

The reports are archival and unchangeable. Re-generation of a report with the same arguments will always produce the same results.

Reported data:

Response time – time from ticket creation to the first public comment by a user with “administrator” or “technical support” role.

Work time – duration of work on the ticket, entered by a technical support employee.

Average number of comments from requester – number of comments authored by the requester divided by the total number of tickets.

The total **time average** and **comment average** is a weighted value: *(number of objects in a row * row value)/total number of objects.*

Types of closed ticket reports (*click the report name to expand the description*):

Closed tickets by days

The report presents an overview of ticket processing in range of days.

Arguments:

| Argument name | Possible values | Selection method | Default value | Remarks |
|---------------------|---|------------------|-----------------------------|---|
| Closing date until: | date (range: 1 day) | date selection | last day of the last month | not possible to select the current day; maximum time from the start date: 100 days |
| Closing date from: | date (range: 1 day) | date selection | first day of the last month | no date limitations |
| Category: | (any), multiple choice from category list | multiple choice | (any) | - |

| Argument name | Possible values | Selection method | Default value | Remarks |
|----------------------------------|---|------------------|---------------|---------|
| Assignee: | (any), (none), multiple choice from assignee list | multiple choice | (any) | - |
| Department: | (any), (none), multiple choice from department list | multiple choice | (any) | - |
| Show unassigned tickets: | true, false | checkbox | true | - |
| Show tickets without department: | true, false | checkbox | true | - |
| Priority: | (any), multiple choice from priority list | multiple choice | (any) | - |

Reported data:

Example:

| Day | Number of closed tickets | Average response time | Time in 'Open' status | | Time in 'Waiting for response' status | | Time in 'Suspended' status | | Time from opening to closing | | Work time | | Average number of requester comments |
|-----------------|--------------------------|-----------------------|-----------------------|-------------|---------------------------------------|-------------|----------------------------|-------------|------------------------------|-------------|---------------|-------------|--------------------------------------|
| | | | average | total | average | total | average | total | average | total | average | total | |
| January 1, 2016 | 8 | 30 min | 1 h | 8 h | 1 h | 8 h | 1 h | 8 h | 1 h | 8 h | 1 h | 8 h | 3.5 |
| January 2, 2016 | 10 | 45 min | 1 h 30 min | 8 h 30 min | 1 h 30 min | 8 h 30 min | 1 h 30 min | 8 h 30 min | 1 h 30 min | 8 h 30 min | 1 h 30 min | 8 h 30 min | 4 |
| January 3, 2016 | 12 | 15 min | 30 min | 7 h 30 min | 7 h 30 min | 7 h 30 min | 30 min | 7 h 30 min | 30 min | 7 h 30 min | 30 min | 7 h 30 min | 4.5 |
| average | 10 | 29 min | 58 min | - | 58 min | - | 58 min | - | 58 min | - | 58 min | - | 4.07 |
| total | 30 | - | - | 24 h | - | 24 h | - | 24 h | - | 24 h | - | 24 h | - |

Visual presentation:

Chart: point/line chart of the number of tickets closed from the given day.

Chart: point/line chart of the average response time from the given day.

Chart: point/line chart of the average time in “open”, “waiting for response”, “suspended” status from the given day.

Chart: point/line chart of the average time from opening to closing from the given day.

Chart: point/line chart of the average work time from the given day.

Chart: bar chart of the total work time from the given day.

Chart: point/line chart of the average number of comments from the requester from the given day.

Closed tickets by weeks

The report presents an overview of ticket processing in range of weeks.

Arguments:

| Argument name | Possible values | Selection method | Default value | Remarks |
|----------------------------------|---|------------------|--|---|
| Closing date until: | date (range: 1 week) | date selection | last completed week | not possible to select the current week; maximum time from the start date: 15 weeks (105 days) |
| Closing date from: | date (range: 1 week) | date selection | four weeks back from the last completed week | no date limitations |
| Category: | (any), multiple choice from category list | multiple choice | (any) | - |
| Assignee: | (any), (none), multiple choice from assignee list | multiple choice | (any) | - |
| Department: | (any), (none), multiple choice from department list | multiple choice | (any) | - |
| Show unassigned tickets: | true, false | checkbox | true | - |
| Show tickets without department: | true, false | checkbox | true | - |
| Priority: | (any), multiple choice from priority list | multiple choice | (any) | - |

Reported data:*Example:*

| Week | Number of closed tickets | Average response time | Time in 'Open' status | | Time in 'Waiting for response' status | | Time in 'Suspended' status | | Time from opening to closing | | Work time | | Average number of requester comments |
|-----------------------|--------------------------|-----------------------|-----------------------|--------------|---------------------------------------|--------------|----------------------------|--------------|------------------------------|--------------|----------------------|--------------|--------------------------------------|
| | | | average | total | average | total | average | total | average | total | average | total | |
| January, 4 - 10 2016 | 100 | 30 min | 1 h | 100 h | 1 h | 100 h | 1 h | 100 h | 1 h | 100 h | 1 h | 100 h | 3.5 |
| January 11 - 17, 2016 | 150 | 45 min | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 4 |
| January, 18 - 24 2016 | 200 | 15 min | 30 min | 150 h | 30 min | 150 h | 30 min | 150 h | 30 min | 150 h | 30 min | 150 h | 4.5 |
| average | 150 | 28 min 59 sec | 56 min 40 sec | - | 56 min 40 sec | - | 56 min 40 sec | - | 56 min 40 sec | - | 56 min 40 sec | - | 4.11 |
| total | 450 | - | - | 450 h | - | 450 h | - | 450 h | - | 450 h | - | 450 h | - |

Visual presentation:

Chart: point/line chart of the number of tickets closed from the given week.

Chart: point/line chart of the average response time from the given week.

Chart: point/line chart of the average time in "open", "waiting for response", "suspended" status from the given week.

Chart: point/line chart of the average time from opening to closing from the given week.

Chart: point/line chart of the average work time from the given week.

Chart: bar chart of the total work time from the given week.

Chart: point/line chart of the average number of comments from the requester from the given week.

Closed tickets by months

The report presents an overview of ticket processing in range of months.

Arguments:

| Argument name | Possible values | Selection method | Default value | Remarks |
|----------------------------------|---|------------------|--|---|
| Closing date until: | date (range: 1 month) | date selection | last completed month | not possible to select the current month; maximum time from the start date: 3 months |
| Closing date from: | date (range: 1 month) | date selection | first month of the quarter with the last completed month | no date limitations |
| Category: | (any), multiple choice from category list | multiple choice | (any) | - |
| Assignee: | (any), (none), multiple choice from assignee list | multiple choice | (any) | - |
| Department: | (any), (none), multiple choice from department list | multiple choice | (any) | - |
| Show unassigned tickets: | true, false | checkbox | true | - |
| Show tickets without department: | true, false | checkbox | true | - |
| Priority: | (any), multiple choice from priority list | multiple choice | (any) | - |

Reported data:

Example:

| Month | Number of closed tickets | Average response time | Time in 'Open' status | | Time in 'Waiting for response' status | | Time in 'Suspended' status | | Time from opening to closing | | Work time | | Average number of requester comments |
|----------------|--------------------------|-----------------------|-----------------------|--------------|---------------------------------------|--------------|----------------------------|--------------|------------------------------|--------------|----------------------|--------------|--------------------------------------|
| | | | average | total | average | total | average | total | average | total | average | total | |
| January 2016 | 100 | 30 min | 1 h | 100 h | 1 h | 100 h | 1 h | 100 h | 1 h | 100 h | 1 h | 100 h | 3.5 |
| February 2016 | 150 | 45 min | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 4 |
| March 2016 | 200 | 15 min | 30 min | 150 h | 30 min | 150 h | 30 min | 150 h | 30 min | 150 h | 30 min | 150 h | 4.5 |
| average | 150 | 28 min 20 sec | 56 min 40 sec | - | 56 min 40 sec | - | 56 min 40 sec | - | 56 min 40 sec | - | 56 min 40 sec | - | 4.11 |
| total | 450 | - | - | 450 h | - | 450 h | - | 450 h | - | 450 h | - | 450 h | - |

Visual presentation:

Chart: point/line chart of the number of tickets closed from the given month.

Chart: point/line chart of the average response time from the given month.

Chart: point/line chart of the average time in "open", "waiting for response", "suspended" status from the given month.

Chart: point/line chart of the average time from opening to closing from the given month.

Chart: point/line chart of the average work time from the given month.

Chart: bar chart of the total work time from the given month.

Chart: point/line chart of the average number of comments from the requester from the given month.

Closed tickets by assignees

The report shows an overview of ticket processing for each technical support employee.

Arguments:

| Argument name | Possible values | Selection method | Default value | Remarks |
|----------------------------------|---|------------------|-----------------------------|--|
| Closing date until: | date (range: 1 day) | date selection | last day of the last month | not possible to select the current month; maximum time from the start date: 100 days |
| Closing date from: | date (range: 1 day) | date selection | first day of the last month | no date limitations |
| Category: | (any), multiple choice from category list | multiple choice | (any) | - |
| Assignee: | (any), (none), multiple choice from assignee list | multiple choice | (any) | - |
| Department: | (any), (none), multiple choice from department list | multiple choice | (any) | - |
| Show unassigned tickets: | true, false | checkbox | true | - |
| Show tickets without department: | true, false | checkbox | true | - |
| Priority: | (any), multiple choice from priority list | multiple choice | (any) | - |

Reported data:*Example:*

| Employee | Number of closed tickets | Average response time | Time in 'Open' status | | Time in 'Waiting for response' status | | Time in 'Suspended' status | | Time from opening to closing | | Work time | | Average number of requester comments |
|--------------|--------------------------|-----------------------|-----------------------|-------|---------------------------------------|-------|----------------------------|-------|------------------------------|-------|------------|-------|--------------------------------------|
| | | | average | total | average | total | average | total | average | total | average | total | |
| Jan Kowalski | 100 | 30 min | 1 h | 100 h | 1 h | 100 h | 1 h | 100 h | 1 h | 100 h | 1 h | 100 h | 3.5 |
| Piotr Nowak | 150 | 45 min | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 4 |

| Employee | Number of closed tickets | Average response time | Time in 'Open' status | | Time in 'Waiting for response' status | | Time in 'Suspended' status | | Time from opening to closing | | Work time | | Average number of requester comments |
|--------------|--------------------------|-----------------------|-----------------------|--------------|---------------------------------------|--------------|----------------------------|--------------|------------------------------|--------------|-----------|--------------|--------------------------------------|
| | | | average | total | average | total | average | total | average | total | average | total | |
| Anna Nowak | 200 | 15 min | 30 min | 150 h | 30 min | 150 h | 30 min | 150 h | 30 min | 150 h | 30 min | 150 h | 4.5 |
| total | 450 | - | - | 450 h | - | 450 h | - | 450 h | - | 450 h | - | 450 h | - |

| Employee | Number of closed tickets | Average response time | Time in 'Open' status | | Time in 'Waiting for response' status | | Time in 'Suspended' status | | Time from opening to closing | | Work time | | Average number of requester comments |
|---------------|--------------------------|-----------------------|-----------------------|------------|---------------------------------------|------------|----------------------------|------------|------------------------------|------------|-----------|------------|--------------------------------------|
| | | | average | total | average | total | average | total | average | total | average | total | |
| (no assignee) | 2 | 30 min | 1 h 30 min | 2 h 30 min | 1 h 30 min | 2 h 30 min | 1 h 30 min | 2 h 30 min | 8 h | 2 h 30 min | 8 h | 2 h 30 min | 3.5 |

Visual presentation:

Chart: bar chart of the number of closed tickets for the assignee + dotted line with mean value.

Chart: bar chart of the assignee's average response time + dotted line with mean value.

Chart: bar chart of the average time in "open", "waiting for response", "suspended" status for the assignee.

Chart: bar chart of the average time from opening to closing for the assignee + dotted line with mean value.

Chart: bar chart of the assignee's total work time + dotted line with mean value.

Chart: bar chart of the average number of requester's comments for the assignee + dotted line with mean value.

Closed tickets by priorities

The report shows an overview of ticket processing for specific ticket priorities.

Arguments:

| Argument name | Possible values | Selection method | Default value | Remarks |
|----------------------------------|---|------------------|-----------------------------|--|
| Closing date until: | date (range: 1 day) | date selection | first day of the last month | not possible to select the current month; maximum time from the start date: 100 days |
| Closing date from: | date (range: 1 day) | date selection | last day of the last month | no date limitations |
| Category: | (any), multiple choice from category list | multiple choice | (any) | - |
| Assignee: | (any), (none), multiple choice from assignee list | multiple choice | (any) | - |
| Department: | (any), (none), multiple choice from department list | multiple choice | (any) | - |
| Show unassigned tickets: | true, false | checkbox | true | - |
| Show tickets without department: | true, false | checkbox | true | - |
| Priority: | (any), multiple choice from priority list | multiple choice | (any) | - |

Reported data:*Example:*

| Priority | Number of closed tickets | Average response time | Time in 'Open' status | | Time in 'Waiting for response' status | | Time in 'Suspended' status | | Time from opening to closing | | Work time | | Average number of requester comments |
|----------|--------------------------|-----------------------|-----------------------|-------|---------------------------------------|-------|----------------------------|-------|------------------------------|-------|------------|-------|--------------------------------------|
| | | | average | total | average | total | average | total | average | total | average | total | |
| High | 100 | 30 min | 1 h | 100 h | 1 h | 100 h | 1 h | 100 h | 1 h | 100 h | 1 h | 100 h | 3.5 |
| Medium | 150 | 45 min | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 4 |

| Priority | Number of closed tickets | Average response time | Time in 'Open' status | | Time in 'Waiting for response' status | | Time in 'Suspended' status | | Time from opening to closing | | Work time | | Average number of requester comments |
|--------------|--------------------------|-----------------------|-----------------------|--------------|---------------------------------------|--------------|----------------------------|--------------|------------------------------|--------------|-----------|--------------|--------------------------------------|
| | | | average | total | average | total | average | total | average | total | average | total | |
| Low | 200 | 15 min | 30 min | 150 h | 30 min | 150 h | 30 min | 150 h | 30 min | 150 h | 30 min | 150 h | 4.5 |
| total | 450 | - | - | 450 h | - | 450 h | - | 450 h | - | 450 h | - | 450 h | - |

Visual presentation:

Chart: bar chart of the number of closed tickets for the priority + dotted line with mean value.

Chart: bar chart of the average response time for the priority + dotted line with mean value.

Chart: bar chart of the average time in "open", "waiting for response", "suspended" status for the priority.

Chart: bar chart of the average time from opening to closing for the priority + dotted line with mean value.

Chart: bar chart of the total work time for the priority + dotted line with mean value.

Chart: bar chart of the average number of requester's comments for the priority + dotted line with mean value.

Closed tickets by categories

The report shows an overview of ticket processing for specific ticket categories.

Arguments:

| Argument name | Possible values | Selection method | Default value | Remarks |
|---------------------|---|------------------|-----------------------------|---|
| Closing date until: | date (range: 1 day) | date selection | first day of the last month | not possible to select the current month; maximum time from the start date: 100 days |
| Closing date from: | date (range: 1 day) | date selection | last day of the last month | no date limitations |
| Category: | (any), multiple choice from category list | multiple choice | (any) | - |

| Argument name | Possible values | Selection method | Default value | Remarks |
|----------------------------------|---|------------------|---------------|---------|
| Assignee: | (any), (none), multiple choice from assignee list | multiple choice | (any) | - |
| Department: | (any), (none), multiple choice from department list | multiple choice | (any) | - |
| Show unassigned tickets: | true, false | checkbox | true | - |
| Show tickets without department: | true, false | checkbox | true | - |
| Priority: | (any), multiple choice from priority list | multiple choice | (any) | - |

Reported data:*Example:*

| Category | Number of closed tickets | Average response time | Time in 'Open' status | | Time in 'Waiting for response' status | | Time in 'Suspended' status | | Time from opening to closing | | Work time | | Average number of requester comments |
|--------------|--------------------------|-----------------------|-----------------------|--------------|---------------------------------------|--------------|----------------------------|--------------|------------------------------|--------------|------------|--------------|--------------------------------------|
| | | | average | total | average | total | average | total | average | total | average | total | |
| Printers | 100 | 30 min | 1 h | 100 h | 1 h | 100 h | 1 h | 100 h | 1 h | 100 h | 1 h | 100 h | 3.5 |
| Scanners | 150 | 45 min | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 4 |
| Monitors | 200 | 15 min | 30 min | 150 h | 30 min | 150 h | 30 min | 150 h | 30 min | 150 h | 30 min | 150 h | 4.5 |
| total | 450 | - | - | 450 h | - | 450 h | - | 450 h | - | 450 h | - | 450 h | - |

Visual presentation:

Chart: bar chart of the number of closed tickets for the category + dotted line with mean value.

Chart: bar chart of the average response time for the category + dotted line with mean value.

Chart: bar chart of the average time in "open", "waiting for response", "suspended" status for the category.

Chart: bar chart of the average time from opening to closing for the category + dotted line with mean value.

Chart: bar chart of the total work time for the category + dotted line with mean value.

Chart: bar chart of the average number of requester's comments for the category + dotted line with mean value.

Closed tickets by departments

The report shows an overview of ticket processing for specific ticket departments.

Arguments:

| Argument name | Possible values | Selection method | Default value | Remarks |
|----------------------------------|---|------------------|-----------------------------|---|
| Closing date until: | date (range: 1 day) | date selection | last day of the last month | not possible to select the current month; maximum time from the start date: 100 days |
| Closing date from: | date (range: 1 day) | date selection | first day of the last month | no date limitations |
| Category: | (any), multiple choice from category list | multiple choice | (any) | - |
| Assignee: | (any), (none), multiple choice from assignee list | multiple choice | (any) | - |
| Department: | (any), (none), multiple choice from department list | multiple choice | (any) | - |
| Show unassigned tickets: | true, false | checkbox | true | - |
| Show tickets without department: | true, false | checkbox | true | - |
| Priority: | (any), multiple choice from priority list | multiple choice | (any) | - |

Reported data:

Example:

| Department | Number of closed tickets | Average response time | Time in 'Open' status | | Time in 'Waiting for response' status | | Time in 'Suspended' status | | Time from opening to closing | | Work time | | Average number of requester comments |
|--------------|--------------------------|-----------------------|-----------------------|--------------|---------------------------------------|--------------|----------------------------|--------------|------------------------------|--------------|------------|--------------|--------------------------------------|
| | | | average | total | average | total | average | total | average | total | average | total | |
| Warsaw | 100 | 30 min | 1 h | 100 h | 1 h | 100 h | 1 h | 100 h | 1 h | 100 h | 1 h | 100 h | 3.5 |
| Wroclaw | 150 | 45 min | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 1 h 30 min | 200 h | 4 |
| Krakow | 200 | 15 min | 30 min | 150 h | 30 min | 150 h | 30 min | 150 h | 30 min | 150 h | 30 min | 150 h | 4.5 |
| total | 450 | - | - | 450 h | - | 450 h | - | 450 h | - | 450 h | - | 450 h | - |

| Department | Number of closed tickets | Average response time | Time in 'Open' status | | Time in 'Waiting for response' status | | Time in 'Suspended' status | | Time from opening to closing | | Work time | | Average number of requester comments |
|-----------------|--------------------------|-----------------------|-----------------------|------------|---------------------------------------|------------|----------------------------|------------|------------------------------|------------|-----------|------------|--------------------------------------|
| | | | average | total | average | total | average | total | average | total | average | total | |
| (no department) | 2 | 30 min | 1 h 30 min | 2 h 30 min | 1 h 30 min | 2 h 30 min | 1 h 30 min | 2 h 30 min | 8 h | 2 h 30 min | 8 h | 2 h 30 min | 3.5 |

Visual presentation:

Chart: bar chart of the number of closed tickets for the department + dotted line with mean value.

Chart: bar chart of the average response time for the department + dotted line with mean value.

Chart: bar chart of the average time in "open", "waiting for response", "suspended" status for the department.

Chart: bar chart of the average time from opening to closing for the department + dotted line with mean value.

Chart: bar chart of the total work time for the department + dotted line with mean value.

Chart: bar chart of the average number of requester's comments for the department + dotted line with mean value.

10.8.2.2 Activity reports

The reports summarize the total number of system events in a given period. Reports from this group offer information about the data volumes processed by the system.

The reports are archival and unchangeable. Re-generation of a report with the same arguments will always produce the same results.

Types of activity reports (*click the report name to expand the description*):

Response time by days

The report provides statistics related to the first response time in range of days, for the tickets with the technical support employee's first response taken in the specified period.

Arguments:

| Argument name | Possible values | Selection method | Default value | Remarks |
|------------------------|---------------------------------------|------------------|-----------------------------|---|
| Response date until: | date (range: 1 day) | date selection | last day of the last month | not possible to select the current day; maximum time from the start date: 100 days |
| Response date from: | date (range: 1 day) | date selection | first day of the last month | no date limitations |
| First response person: | (any), multiple choice from user list | multiple choice | (any) | list is limited to users with "administrator" or "technical support" role. |

Reported data:

Response time: time from ticket creation to the first public comment by a user with "administrator" or "technical support" role.

The total **time average** and comment average is a weighted value: *number of objects in a row * row value/total number of objects*.

Example:

| Day | Number of tickets with first response made | Number of tickets with response time | | | | Response time | |
|-----------------|--|--------------------------------------|---------------------------|----------------------------|----------------|---------------|------------|
| | | up to 1 h | more than 1 h - up to 8 h | more than 8 h - up to 24 h | more than 24 h | average | maximum |
| January 1, 2016 | 20 | 6 | 10 | 3 | 1 | 50 min | 2 h |
| January 2, 2016 | 43 | 12 | 20 | 9 | 2 | 1 h | 2 h 20 min |

| Day | Number of tickets with first response made | Number of tickets with response time | | | | Response time | |
|-----------------|--|--------------------------------------|---------------------------|----------------------------|----------------|----------------------|------------|
| | | up to 1 h | more than 1 h - up to 8 h | more than 8 h - up to 24 h | more than 24 h | average | maximum |
| January 3, 2016 | 14 | 3 | 5 | 6 | 0 | 1 h 10 min | 1 h 40 min |
| average | 25.67 | 7 | 11.67 | 6 | 1 | 59 min 13 sec | - |
| total | 77 | 21 | 35 | 18 | 3 | - | - |

Visual presentation:

Chart: point/line chart of the number of tickets with the first response taken from the given day.

Chart: point/line chart of the number of tickets with response time of up to 1 h, 1 to 8 h, 8 to 24 h, more than 24 h from the given day.

Chart: point/line chart of the average response time from the given day.

Response time by weeks

The report provides statistics related to the first response time in range of weeks, for the tickets with the technical support employee's first response taken in the specified period.

Arguments:

| Argument name | Possible values | Selection method | Default value | Remarks |
|------------------------|---------------------------------------|------------------|--|--|
| Response date until: | date (range: 1 week) | date selection | last completed week | not possible to select the current day; maximum time from the start date: 15 weeks (105 days) |
| Response date from: | date (range: 1 week) | date selection | four weeks back from the last completed week | no date limitations |
| First response person: | (any), multiple choice from user list | multiple choice | (any) | list is limited to users with "administrator" or "technical support" role. |

Reported data:

Response time: time from ticket creation to the first public comment by a user with "administrator" or "technical support" role.

The total **average response time** is a weighted value: *number of objects in a row * row value/total number of objects.*

Example:

| Week | Number of tickets with first response made | Number of tickets with response time | | | | Response time | |
|-----------------------|--|--------------------------------------|---------------------------|----------------------------|----------------|----------------------|------------|
| | | up to 1 h | more than 1 h - up to 8 h | more than 8 h - up to 24 h | more than 24 h | average | maximum |
| January, 4 - 10 2016 | 20 | 6 | 10 | 3 | 1 | 50 min | 2 h |
| January 11 - 17, 2016 | 43 | 12 | 20 | 9 | 2 | 1 h | 2 h 20 min |
| January, 18 - 24 2016 | 14 | 3 | 5 | 6 | 0 | 1 h 10 min | 1 h 40 min |
| average | 25.67 | 7 | 11.67 | 6 | 1 | 59 min 13 sec | - |
| total | 77 | 21 | 35 | 18 | 3 | - | - |

Visual presentation:

Chart: point/line chart of the number of tickets with the first response taken from the given week.

Chart: point/line chart of the number of tickets with response time of up to 1 h, 1 to 8 h, 8 to 24 h, more than 24 h from the given week.

Chart: point/line chart of the average response time from the given week.

Response time by months

The report provides statistics related to the first response time in range of months, for the tickets with the technical support employee's first response taken in the specified period.

Arguments:

| Argument name | Possible values | Selection method | Default value | Remarks |
|----------------------|-----------------------|------------------|----------------------------|--|
| Response date until: | date (range: 1 month) | date selection | first month of the quarter | not possible to select the current day; maximum time from the |

| Argument name | Possible values | Selection method | Default value | Remarks |
|------------------------|---------------------------------------|------------------|-------------------------------|--|
| | | | with the last completed month | start date: 3 months |
| Response date from: | date (range: 1 month) | date selection | last completed month | no date limitations |
| First response person: | (any), multiple choice from user list | multiple choice | (any) | list is limited to users with "administrator" or "technical support" role. |

Reported data:

Response time: time from ticket creation to the first public comment by a user with "administrator" or "technical support" role.

The total **average response time** is a weighted value: *number of objects in a row * row value/total number of objects*.

Example:

| Month | Number of tickets with first response made | Number of tickets with response time | | | | Response time | |
|----------------|--|--------------------------------------|-----------------|------------------|----------------|----------------------|------------|
| | | up to 1 h | 1 h - up to 8 h | 8 h - up to 24 h | more than 24 h | average | maximum |
| January 2016 | 200 | 60 | 100 | 30 | 10 | 50 min | 2 h |
| February 2016 | 430 | 120 | 200 | 90 | 20 | 1 h | 2 h 20 min |
| March 2016 | 140 | 30 | 50 | 60 | 0 | 1 h 10 min | 1 h 40 min |
| average | 256.67 | 70 | 116.7 | 60 | 10 | 59 min 13 sec | - |
| total | 770 | 210 | 350 | 180 | 30 | - | - |

Visual presentation:

Chart: point/line chart of the number of tickets with the first response taken from the given month.

Chart: point/line chart of the number of tickets with response time of up to 1 h, 1 to 8 h, 8 to 24 h, more than 24 h from the given month.

Chart: point/line chart of the average response time from the given month.

Summary - number of events

The report provides numerical event statistics in form of a summary.

Arguments:

| Argument name | Possible values | Selection method | Default value | Remarks |
|----------------------|---------------------|------------------|--|--|
| Activity date until: | date (range: 1 day) | date selection | yesterday | not possible to select the current day; unlimited maximum time from the start date. |
| Activity date from: | date (range: 1 day) | date selection | earlier of the following dates: <ul style="list-style-type: none"> • system installation/ migration date (zero date) • yesterday | no date limitations |

Reported data:

Example:

| Month | Number of tickets created from | | Total number of created tickets | Total number of closed tickets | Number of comments | | |
|------------------------|--------------------------------|-----------------------|---------------------------------|--------------------------------|--------------------|----------|-------|
| | e-mail messages | application interface | | | public | internal | total |
| Number | 500 | 1500 | 2000 | 1800 | 3500 | 4000 | 6500 |
| Average per day | 1.37 | 4.11 | 5.48 | 4.93 | 9.59 | 10.96 | 17.81 |

Visual presentation:

Chart: pie chart of the total number of tickets created from e-mail messages and the application interface.

Chart: bar chart of the number of created tickets and closed tickets.

Chart: pie chart of the total number of public comments and internal comments.

User activity in tickets

The report provides numerical user activity statistics in the specified period.

Arguments:

| Argument name | Possible values | Selection method | Default value | Remarks |
|------------------------|---------------------------------------|------------------|-----------------------------|---|
| Activity date until: | date (range: 1 day) | date selection | last day of the last month | not possible to select the current day; maximum time from the start date: 100 days |
| Activity date from: | date (range: 1 day) | date selection | first day of the last month | no date limitations |
| First response person: | (any), multiple choice from user list | multiple choice | (any) | list is limited to users with "administrator" or "technical support" role. |

Reported data:

Reports with which a user has been working: set of unique tickets, in relation to which the user performed any action (ticket editing, any comment) in the specified period.

The total **average response time** is a weighted value: *number of objects in a row * row value/total number of objects*.

Example:

| Employee | Public comments | | Public and internal comments | | Tickets with which the user has been working | |
|--------------|-----------------|-----------------|------------------------------|-----------------|--|-----------------|
| | number | average per day | number | average per day | number | average per day |
| Jan Kowalski | 15 | 5 | 25 | 8.33 | 10 | 3.33 |
| Piotr Nowak | 25 | 8.33 | 35 | 11.67 | 9 | 3 |
| Anna Nowak | 20 | 6.67 | 30 | 10 | 11 | 3.67 |
| total | 60 | | 90 | | 30 | |

Visual presentation:

Chart: bar chart of the number of public comments for the user + dotted line with mean value.

Chart: bar chart of the number of public and internal comments for the user + dotted line with mean value.

Chart: bar chart of the number of tickets with which the user has been working + dotted line with mean value.

Chart: bar chart of the daily average number of public comments for the user + dotted line with mean value.

Chart: bar chart of the daily average number of public and internal comments for the user + dotted line with mean value.

Chart: bar chart of the average daily number of tickets with which the user has been working + dotted line with mean value.

First response time by users

The report allows to compare the response times of specific technical support employees for the tickets with the first response taken in the specified period.

Arguments:

| Argument name | Possible values | Selection method | Default value | Remarks |
|------------------------|---------------------------------------|------------------|-----------------------------|---|
| Response date until: | date (range: 1 day) | date selection | last day of the last month | not possible to select the current day; maximum time from the start date: 100 days |
| Response date from: | date (range: 1 day) | date selection | first day of the last month | no date limitations |
| First response person: | (any), multiple choice from user list | multiple choice | (any) | list is limited to users with "administrator" or "technical support" role. |

Reported data:

Response time: time from ticket creation to the first public comment by a user with "administrator" or "technical support" role.

The total **average response time** is a weighted value: *number of objects in a row * row value/total number of objects.*

Example:

| User performing the first response | Number of tickets with first response made | Number of tickets with response time | | | | Response time | |
|------------------------------------|--|--------------------------------------|---------------------------|----------------------------|----------------|---------------|---------|
| | | up to 1 h | more than 1 h - up to 8 h | more than 8 h - up to 24 h | more than 24 h | average | maximum |
| Jan Kowalski | 200 | 60 | 100 | 30 | 10 | 50 min | 2 h |

| User performing the first response | Number of tickets with first response made | Number of tickets with response time | | | | Response time | |
|------------------------------------|--|--------------------------------------|---------------------------|----------------------------|----------------|---------------|------------|
| | | up to 1 h | more than 1 h - up to 8 h | more than 8 h - up to 24 h | more than 24 h | average | maximum |
| Piotr Nowak | 430 | 120 | 200 | 90 | 20 | 1 h | 2 h 20 min |
| Anna Nowak | 140 | 30 | 50 | 60 | 0 | 1 h 10 min | 1 h 40 min |
| total | 770 | 210 | 350 | 180 | 30 | - | - |

Visual presentation:

Chart: bar chart of the number of tickets for the user who performed the first response + dotted line with mean value.

Chart: bar chart of the number of tickets with response time of up to 1 h, 1 to 8 h, 8 to 24 h, more than 24 h for the user who performed the first response.

Chart: bar chart of the average response time for the user who performed the first response + dotted line with mean value.

10.8.2.3 Unclosed tickets reports

The reports show data on tickets currently being processed in the system. Reports from this group offer information about the current system status, e.g. the current number of tickets.

The reports work as views – re-generation of the report can produce different results each time.

Types of currently processed ticket reports (*click the report name to expand the description*):

Unclosed tickets summary

The report presents properties of all of the currently unclosed tickets. It allows to assess their progress and time when the tickets remain without solution.

Arguments:

| Argument name | Possible values | Selection method | Default value |
|---------------|---|------------------|---------------|
| Category: | (any), multiple choice from category list | multiple choice | (any) |
| Assignee: | (any), (none), multiple choice from assignee list | multiple choice | (any) |

| Argument name | Possible values | Selection method | Default value |
|----------------------------------|---|------------------|---------------|
| Department: | (any), (none), multiple choice from department list | multiple choice | (any) |
| Show unassigned tickets: | true, false | checkbox | true |
| Show tickets without department: | true, false | checkbox | true |
| Priority: | (any), multiple choice from priority list | multiple choice | (any) |

Reported data:

First response – the first public comment added by a user in “administrator” or “technical support” role.

Example:

| | Total number of unclosed tickets | Number of tickets in status | | | | Number of tickets | | Number of tickets | | Average time from creation for tickets without first response | Average time from creation for unclosed tickets |
|---------------|----------------------------------|-----------------------------|------|----------------------|-----------|----------------------|------------------------------|------------------------|--|---|---|
| | | new | open | waiting for response | suspended | assigned to assignee | not assigned to any assignee | without first response | for which the first response was taken | | |
| Number | 40 | 5 | 10 | 20 | 5 | 38 | 2 | 7 | 33 | 30 min | 1 h 10 min |

Visual presentation:

Chart: bar chart of the number of tickets in “new”, “open”, “waiting for response”, “suspended” status.

Chart: pie chart of the number of unclosed tickets not assigned and assigned to any assignee.

Chart: pie chart of the number of unclosed tickets without the first response and with the first response already taken.

Unclosed tickets by assignees

The report presents the current workload of the technical support employees within the system.

Arguments:

| Argument name | Possible values | Selection method | Default value |
|----------------------------------|---|------------------|---------------|
| Category: | (any), multiple choice from category list | multiple choice | (any) |
| Assignee: | (any), (none), multiple choice from assignee list | multiple choice | (any) |
| Department: | (any), (none), multiple choice from department list | multiple choice | (any) |
| Show unassigned tickets: | true, false | checkbox | true |
| Show tickets without department: | true, false | checkbox | true |
| Priority: | (any), multiple choice from priority list | multiple choice | (any) |

Reported data:

First response: the first public comment added by a user in “administrator” or “technical support” role.

The total **average time** is a weighted value: *number of objects in a row * row value/total number of objects.*

Example:

| Employee | Number of unclosed tickets | Number of tickets in status | | | | Number of tickets without first response | Average time without first response | Average time from ticket creation |
|----------------|----------------------------|-----------------------------|----------|----------------------|-------------|--|-------------------------------------|-----------------------------------|
| | | new | open | waiting for response | suspended | | | |
| Jan Kowalski | 10 | 1 | 3 | 5 | 1 | 1 | 30 min | 1 h |
| Piotr Nowak | 19 | 1 | 5 | 10 | 3 | 2 | 45 min | 1 h 30 min |
| Anna Nowak | 5 | 0 | 1 | 3 | 1 | 0 | - | 30 min |
| average | 10 | 0.67 | 3 | 6 | 1.67 | 1 | 40 min | 1 h 30 min |
| total | 30 | 2 | 9 | 18 | 5 | 2 | - | - |

| Employee | Number of unclosed tickets | Number of tickets in status | | | | Number of tickets without first response | Average time without first response | Average time from ticket creation |
|---------------|----------------------------|-----------------------------|------|----------------------|-----------|--|-------------------------------------|-----------------------------------|
| | | new | open | waiting for response | suspended | | | |
| (no assignee) | 1 | 1 | 0 | 0 | 0 | 0 | - | 10 min |

Visual presentation:

Chart: bar chart of the number of unclosed tickets for the assignee + dotted line with mean value.

Chart: bar chart of the number of tickets in “new”, “open”, “waiting for response”, “suspended” status.

Chart: bar chart of the number of tickets without the first response for the assignee + dotted line with mean value.

Chart: bar chart of the average time without the first response for the assignee + dotted line with mean value.

Chart: bar chart of the average time from ticket creation for the assignee + dotted line with mean value.

Unclosed tickets by priorities

The report presents the current number and status of unsolved tickets with the specified priority.

Arguments:

| Argument name | Possible values | Selection method | Default value |
|----------------------------------|---|------------------|---------------|
| Category: | (any), multiple choice from category list | multiple choice | (any) |
| Assignee: | (any), (none), multiple choice from assignee list | multiple choice | (any) |
| Department: | (any), (none), multiple choice from department list | multiple choice | (any) |
| Show unassigned tickets: | true, false | checkbox | true |
| Show tickets without department: | true, false | checkbox | true |
| Priority: | (any), multiple choice from priority list | multiple choice | (any) |

Reported data:

First response: the first public comment added by a user in “administrator” or “technical support” role.

The total **average time** is a weighted value: *number of objects in a row * row value/total number of objects*.

Example:

| Priority | Number of unclosed tickets | Number of tickets in status | | | | Number of tickets without first response | Average time without first response | Average time from ticket creation |
|----------------|----------------------------|-----------------------------|----------|----------------------|-------------|--|-------------------------------------|-----------------------------------|
| | | new | open | waiting for response | suspended | | | |
| High | 10 | 1 | 3 | 5 | 1 | 1 | 30 min | 1 h |
| Medium | 19 | 1 | 5 | 10 | 3 | 2 | 45 min | 1 h 30 min |
| Low | 5 | 0 | 1 | 3 | 1 | 0 | - | 30 min |
| average | 10 | 0.67 | 3 | 6 | 1.67 | 1 | 40 min | 1 h 30 min |
| total | 30 | 2 | 9 | 18 | 5 | 2 | - | - |

Visual presentation:

Chart: bar chart of the number of unclosed tickets for the priority + dotted line with mean value.

Chart: bar chart of the number of tickets in “new”, “open”, “waiting for response”, “suspended” status for the priority.

Chart: bar chart of the number of tickets without the first response for the priority + dotted line with mean value.

Chart: bar chart of the average time without the first response for the priority + dotted line with mean value.

Chart: bar chart of the average time from ticket creation for the priority + dotted line with mean value.

Closed tickets by categories

The report presents the current number and status of unsolved tickets with the specified category.

Arguments:

| Argument name | Possible values | Selection method | Default value |
|---------------|---|------------------|---------------|
| Category: | (any), multiple choice from category list | multiple choice | (any) |

| Argument name | Possible values | Selection method | Default value |
|----------------------------------|---|------------------|---------------|
| Assignee: | (any), (none), multiple choice from assignee list | multiple choice | (any) |
| Department: | (any), (none), multiple choice from department list | multiple choice | (any) |
| Show unassigned tickets: | true, false | checkbox | true |
| Show tickets without department: | true, false | checkbox | true |
| Priority: | (any), multiple choice from priority list | multiple choice | (any) |

Reported data:

First response: the first public comment added by a user in “administrator” or “technical support” role.

The total **average time** is a weighted value: *number of objects in a row * row value/total number of objects*.

Example:

| Category | Number of unclosed tickets | Number of tickets in status | | | | Number of tickets without first response | Average time without first response | Average time from ticket creation |
|----------------|----------------------------|-----------------------------|----------|----------------------|-------------|--|-------------------------------------|-----------------------------------|
| | | new | open | waiting for response | suspended | | | |
| Printers | 10 | 1 | 3 | 5 | 1 | 1 | 30 min | 1 h |
| Scanners | 19 | 1 | 5 | 10 | 3 | 2 | 45 min | 1 h 30 min |
| Monitors | 5 | 0 | 1 | 3 | 1 | 0 | - | 30 min |
| average | 10 | 0.67 | 3 | 6 | 1.67 | 1 | 40 min | 1 h 30 min |
| total | 30 | 2 | 9 | 18 | 5 | 2 | - | - |

Visual presentation:

Chart: bar chart of the number of unclosed tickets for the category + dotted line with mean value.

Chart: bar chart of the number of tickets in “new”, “open”, “waiting for response”, “suspended” status for the category.

Chart: bar chart of the number of tickets without the first response for the category + dotted line with mean value.

Chart: bar chart of the average time without the first response for the category + dotted line with mean value.

Chart: bar chart of the average time from ticket creation for the category + dotted line with mean value.

Closed tickets by departments

The report presents the current number and status of unsolved tickets with the specified priority.

Arguments:

| Argument name | Possible values | Selection method | Default value |
|----------------------------------|---|------------------|---------------|
| Category: | (any), multiple choice from category list | multiple choice | (any) |
| Assignee: | (any), (none), multiple choice from assignee list | multiple choice | (any) |
| Department: | (any), (none), multiple choice from department list | multiple choice | (any) |
| Show unassigned tickets: | true, false | checkbox | true |
| Show tickets without department: | true, false | checkbox | true |
| Priority: | (any), multiple choice from priority list | multiple choice | (any) |

Reported data:

First response: the first public comment added by a user in “administrator” or “technical support” role.

The total **average time** is a weighted value: *number of objects in a row * row value/total number of objects*.

Example:

| Department | Number of unclosed tickets | Number of tickets in status | | | | Number of tickets without first response | Average time without first response | Average time from ticket creation |
|------------|----------------------------|-----------------------------|------|----------------------|-----------|--|-------------------------------------|-----------------------------------|
| | | new | open | waiting for response | suspended | | | |
| Warsaw | 10 | 1 | 3 | 5 | 1 | 1 | 30 min | 1 h |
| Wroclaw | 19 | 1 | 5 | 10 | 3 | 2 | 45 min | 1 h 30 min |

| Department | Number of unclosed tickets | Number of tickets in status | | | | Number of tickets without first response | Average time without first response | Average time from ticket creation |
|----------------|----------------------------|-----------------------------|----------|----------------------|-------------|--|-------------------------------------|-----------------------------------|
| | | new | open | waiting for response | suspended | | | |
| Krakow | 5 | 0 | 1 | 3 | 1 | 0 | - | 30 min |
| average | 10 | 0.67 | 3 | 6 | 1.67 | 1 | 40 min | 1 h 30 min |
| total | 30 | 2 | 9 | 18 | 5 | 2 | - | - |

| Department | Number of unclosed tickets | Number of tickets in status | | | | Number of tickets without first response | Average time without first response | Average time from ticket creation |
|-----------------|----------------------------|-----------------------------|------|----------------------|-----------|--|-------------------------------------|-----------------------------------|
| | | new | open | waiting for response | suspended | | | |
| (no department) | 1 | 1 | 0 | 0 | 0 | 0 | - | 10 min |

Visual presentation:

Chart: bar chart of the number of unclosed tickets for the department + dotted line with mean value.

Chart: bar chart of the number of tickets in “new”, “open”, “waiting for response”, “suspended” status for the department.

Chart: bar chart of the number of tickets without the first response for the department + dotted line with mean value.

Chart: bar chart of the average time without the first response for the department + dotted line with mean value.

Chart: bar chart of the average time from ticket creation for the department + dotted line with mean value.

10.8.3 SLA reports

10.8.3.1 Closed tickets under SLA reports

Closed tickets under SLA reports display the statistics of closed tickets processed under SLA metrics. This group of reports enables the investigation into how the service level agreement provisions were fulfilled.

The reports are archival. Re-generation of a report with the same arguments will always produce the same results.

Reported data

The report only includes the metrics which have not been invalidated and are related to the tickets closed in the specified time interval.

Tickets with fulfilled SLA – counts the tickets with a metric which has not been violated and has completed its run due to an event which effectively closes it (first response, ticket closure).

Tickets with violated SLA – counts the tickets with a metric which has been violated and completed its run due to an event which effectively closes it.

SLA fulfillment (%) – number of tickets, for which the metric has been fulfilled / number of all tickets with any metric.

SLA violation / average / maximum / total – time running from the moment of violation (if a metric was exceeded by one hour, the violation time is one hour). Pertains only to the period when the metric was active. Includes all violated metrics (without the invalidated ones).

Average SLA measurement duration – average run time for all completed metrics. Pertains only to the period when the metric was active.

Total time average is counted by weight: *number of objects in a row * row value/total number of objects*.

10.8.3.2 SLA metric course reports

SLA metric course reports display the events that occurred during the SLA metric run. The purpose of this group of reports is to monitor the tasks executed under the service level agreement.

Reported data

The report does not include metrics in tickets removed by the administrator.

Tickets with SLA measurement – counts the tickets covered by the metric where the coverage started within the specified report time range.

Tickets with violated SLA – counts the ticket with a violated metric where the violation occurred within the specified report time range.

Tickets with completed measurement and fulfilled SLA – counts the tickets with a metric which has not been violated and has completed its run due to an event which effectively closes it (first response, ticket closure) within the specified report time range.

Tickets with completed measurement and violated SLA – counts the tickets with a metric which has been violated and has completed its run due to an event which effectively closes it within the specified report time range.

10.8.3.3 SLA violation reports

SLA violation reports display the tickets with a violated SLA metric. The purpose of this group of reports is to investigate the incidents of service level agreement breaches.

Reported data

The report contains one line per ticket with a violated SLA metric.

The report does not show tickets with invalidated metrics (even if the metrics had been violated). The report does not show tickets deleted by the administrator.

SLA violation is the time running from the moment of violation (if a metric was exceeded by one hour, the violation time is one hour). Pertains only to the period when the metric was active.

If the violated metric has not been completed yet or the ticket has not been closed yet, the cell displays an empty value.

The report does not perform any aggregation operations and does not include any visual representation.

If no ticket shows an SLA violation in the specified time range, the interface displays “No tickets with violated SLA metric” message instead of the table. Such a report cannot be exported.

10.9 Absence plan

The absence plan is a system for reporting the absences of HelpDesk Administrators and Employees. The purpose of the function is to plan the appropriate ticket system operation when the person assigned to ticket handling is absent.

*Absence plan **does not support** vacation management, understood as calculating the number of vacation days eligible for an individual employee.*

Absence times (start/end dates and hours) pertain to the local time of the machine where the Axence nVision® Server (HelpDesk service) is installed.

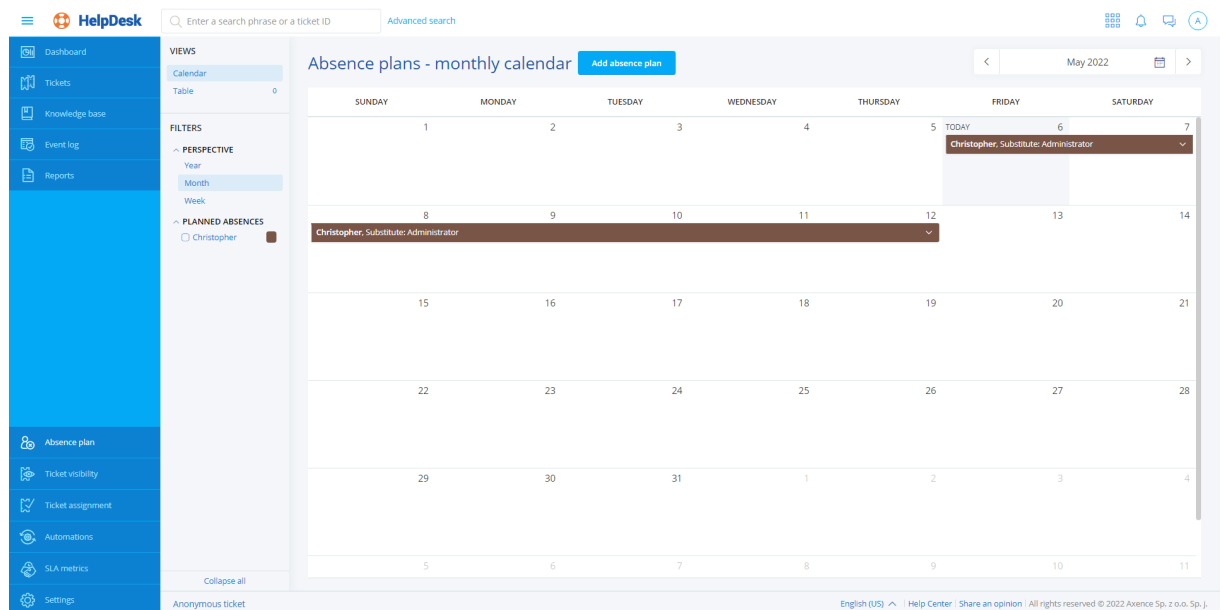
To add an absence plan, log in to the HelpDesk interface, go to the **Absence plan** view and click the **Add absence plan** button - a wizard will be displayed, which will allow to easily select the period of planned absence

Take the steps:

1. Find the name in drop-down list of the **HelpDesk employee** for whom the absence is to be planned.
2. Using the calendar, indicate the **period of employee's absence**
3. Select the deputy - the person who will receive notifications about changes in tickets assigned to the absent person. Then choose the color to mark the absence in the calendar. It is also possible to check the box that will extend the visibility of notifications for the person replacing absent employee.

In the period for which an absence is planned, tickets will still be assigned to the absent HelpDesk employee (according to [ticket assignment rules](#)^[457] and [automations](#)^[458]), and the substitute will receive e-mail notifications about new tickets assigned to the absentee and about the requesters' comments.

They can also see all the tickets assigned to the absentee. After the absence period is over, the defined substitution is disabled and the substitute will no longer receive the mentioned notifications.



10.10 Trouble ticket assignment

In the HelpDesk, in the **Ticket assignment** section, you can add, edit or delete the ticket assignment rules. The ticket assignment rules are used to automate the ticket assignment to a particular HelpDesk Employee or Administrator, thereby facilitating the work and effectively reducing the ticket processing time.

Adding a ticket assignment rule

| |
|---|
| To add a ticket assignment rule, log in to the HelpDesk module as the Administrator and: |
| 1. In the flyout menu on the left side of the window, click the Ticket assignment . |
| 2. Click the Add rule button. |
| 3. Click the Select user field, and then select the HelpDesk Employee or the Administrator from the drop-down list. |
| 4. Select whether the assignment rule is to apply to All or only the Selected tickets. |
| 5. If you have chosen the option for Selected tickets, configure the conditions for this rule. |
| 6. If you want the ticket assignment rule to be disabled after creation, click the slider (by default, the rule is enabled after creation). |
| 7. Click the Add rule button. |
| 8. Once you have properly completed the steps above, the ticket assignment rule will be created and the relevant message will appear in the upper right corner of the screen. |

Editing a ticket rule

| |
|---|
| To create a ticket assignment rule, log in to the HelpDesk module as the Administrator and: |
|---|

1. In the flyout menu on the left side of the window, click the **Ticket assignment**.
2. Hover over the user whose rule you want to activate/deactivate and click the **Edit** button.
3. In the ticket assignment rule edition panel, make changes to the rule, and then click the **Save changes** button.

Once you have completed the steps above, the ticket assignment rule will be permanently **deleted** and the relevant message confirming the successful completion of the action will appear in the upper right corner of the screen. The removed rule will not appear in the ticket assignment rule list.

Deleting a ticket rule

To create a ticket assignment rule, log in to the HelpDesk module as the Administrator and:

1. In the flyout menu on the left side of the window, click the **Ticket assignment**.
2. Hover over the user whose rule you want to activate/deactivate and click the **Delete** button.
3. In the ticket assignment rule deletion window, click the **Delete the rule** button.

Once you have completed the steps above, the ticket assignment rule will be permanently deleted and the relevant message confirming the successful completion of the action will appear in the upper right corner of the screen. The removed rule will not appear in the ticket assignment rule list.

Activating/deactivating a ticket assignment rule

To activate or deactivate a ticket assignment rule, log in to the HelpDesk module as the Administrator and:

1. In the flyout menu on the left side of the window, click the **Ticket assignment**.
2. Hover over the user whose rule you want to activate/deactivate and click the **slider**.

Once you have properly completed the steps above, the rule will be **activated or deactivated** and the relevant message will appear in the upper right corner of the screen. **From now on, new tickets will or will not be assigned according to the rule.**

Related topics

 [Categories](#)

 [User management](#)

 [Management and configuration](#) ³⁴⁹

10.11 Automations

10.11.1 Automations - overview

Automations are a brand new, breakthrough function of the Axence nVision® HelpDesk. The purpose is to noticeably accelerate the trouble ticket processing by HelpDesk employees. Their everyday work scenarios include many regular, recurring activities. These happen in specific conditions and call for actions defined within the workflow. Automations enable the time necessary for efficient ticket processing to be reduced and they also accelerate the response to events occurring in the network and to improve processes within the organization.

The HelpDesk module includes a few pre-built automations, which help to introduce the administrator to the structure of such mechanisms.

The screenshot displays the 'All automations (3)' page in the HelpDesk module. The interface includes a sidebar with navigation options such as Dashboard, Tickets, Knowledge base, Event log, Reports, Absence plan, Ticket visibility, Ticket assignment, Automations, SLA metrics, and Settings. The main content area shows a list of three automation rules, each with a title, description, 'WHEN' trigger, 'CONDITIONS', and 'ACTIONS'. The first rule is 'Marking the ticket as response pending', the second is 'Opening the ticket after a response from the person reporting', and the third is 'Opening the ticket after work on the ticket has been started'. Each rule has a status indicator (green for active, red for inactive) and a toggle switch. The page also includes a footer with language and copyright information.

10.11.2 Automation list

The defined automation rules are presented as a list showing the specific rules in the form of tiles.

A single tile representing the specific automation includes:

- automation title,
- context actions – allowing the editing, deleting and change of the status of the automation,
- automation status – as a colored bar: **red** – deactivated automation, **green** – active automation,
- automation description,
- automation trigger,
- list of conditions,
- list of actions.

The screenshot shows the 'All automations (3)' page in the HelpDesk interface. The left sidebar contains navigation options: Dashboard, Tickets, Knowledge base, Event log, Reports, Absence plan, Ticket visibility, Ticket assignment, Automations, SLA metrics, and Settings. The main content area displays three automation rules, each with a toggle switch to enable or disable it.

Automation 1: Marking the ticket as response pending
 Automation marks the ticket as response pending when the technical support engineer provides a public response to the person reporting the problem.
 WHEN: After update
 CONDITIONS: Public comment was not added by a user with the role 'User' and ticket status is equal to 'Open'
 ACTIONS: 01. Change status to 'Waiting for response'

Automation 2: Opening the ticket after a response from the person reporting
 Automation reopens the ticket when the person reporting responds to the technical support engineer.
 WHEN: After update
 CONDITIONS: Public comment was added by a user with the role 'User' and ticket status is equal to 'Waiting for response'
 ACTIONS: 01. Change status to 'Open'

Automation 3: Opening the ticket after work on the ticket has been started
 Automation opens the ticket when the technical support engineer starts to work on it or edits its properties.
 WHEN: After update
 CONDITIONS: Updater does not have a role of 'User' and internal comment was not added and ticket status is equal to 'New'
 ACTIONS: 01. Change status to 'Open'

At the bottom, there is an 'EMBEDDED MECHANISM ACTIVATION SEQUENCE' section with the following steps:
 After ticket creation: Execute automation > Assign the ticket according to the rules
 After ticket update and checked on the hour: Execute automation

Useful information >
 SEE ALSO
 Help center - Automations
 Ticket assignment

Anonymous ticket

English (US) | Help Center | Share an opinion | All rights reserved © 2022 Axence Sp. z o.o. Sp. J.

The left-hand part of the automation list displays a quick preview, which allows the automations to be efficiently filtered:

- state:
 - active,
 - deactivated,
- trigger:
 - performed when the trouble ticket is created,
 - performed when the trouble ticket is updated,
 - performed daily.

10.11.3 Adding an automation

The automation addition view enables the determination of the conditions and actions which are to be performed in a specified situation.

The screenshot shows the 'Adding an automation' form in the HelpDesk interface. The form is divided into three main sections: GENERAL INFORMATION, CONDITIONS, and ACTIONS. In the GENERAL INFORMATION section, there is a 'Name' field with the placeholder 'Enter a unique automation name' and a 'Description' field with the placeholder 'Enter a description of the automation' and a '300 characters' limit. Below these is a 'Status after creation' toggle switch. The CONDITIONS section includes a dropdown for 'If met' (set to 'all'), a dropdown for 'conditions for ticket' (set to 'after it has been created'), and a dropdown for 'Ticket priority' (set to 'Select priority'). There is also an 'Add a condition' button. The ACTIONS section includes a dropdown for 'Add action' and an 'Add action' button. At the bottom of the form, there are 'Add automation' and 'Cancel' buttons. The interface also shows a sidebar with navigation options like Dashboard, Tickets, Knowledge base, Event log, Reports, Absence plan, Ticket visibility, Ticket assignment, Automations, SLA metrics, and Settings. The footer includes 'Anonymous ticket' and 'English (US) | Help Center | Share an opinion | All rights reserved © 2022 Axence Sp. z o.o. Sp. J.'

To add an automation:

1. Log in to the HelpDesk interface.
2. In the main navigation, on the left-hand side of the interface, select **Automations**.
3. In the automation list click the **Add automation** button.
4. Fill in the fields:
 - **name** – specify the name of the new automation,
 - **description** – you can add a short description of the automation operation.
5. Determine the automation status after it has been created.
6. Specify the automation trigger type – when it should be performed:
 - daily – an automatic procedure for checking the list of unclosed tickets is launched every day. Within its operation, the conditions defined by the administrator are checked and determined actions are taken. **Example:** *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.
7. Define the condition application logic:

You can specify whether in order for the automation to be applied, the processed ticket should meet any or all of the conditions defined below.

To add another condition, click the **Add condition** link.
8. Specify the actions which are to be taken, if the trouble ticket meets the conditions:

To add another action, click the **Add action** link.
9. Save the automation by clicking the **Add automation** button.

10.11.4 Automation conditions

The automation rules which are created should be as simple as possible.

Automation conditions for a new trouble ticket:

| Object | Object options | Condition |
|------------------------------|-------------------------------------|-------------------------------|
| Ticket subject | contains at least one of the words | enter words divided by commas |
| | does not contain any of the words | |
| | contains all of the following words | |
| Ticket description | contains at least one of the words | enter words divided by commas |
| | does not contain any of the words | |
| | contains all of the following words | |
| Ticket priority | is equal to | select priority |
| | is not equal to | |
| | is higher than or equal to | |
| | is higher than | |
| | is lower than or equal to | |
| | is lower than | |
| | is the default priority | - |
| is not the default priority | - | |
| Ticket category | is equal to | select category |
| | is not equal to | - |
| | is the default category | - |
| | is not the default category | - |
| Requester | is equal to | enter the requester |
| | is not equal to | - |
| Related device | is equal to | enter the device name |
| | is not equal to | - |
| | is set | - |
| Department of related device | is set | - |
| | is not set | - |
| | is equal to | enter the department |
| | is not equal to | - |
| Ticket source | is set | - |
| | is not set | - |
| | is | enter the ticket source |
| Assignee | is not | - |
| | is equal to | enter the assignee |
| | is not equal to | |
| | is set | |
| | is not set | |
| | belongs to group | |
| does not belongs to group | | |

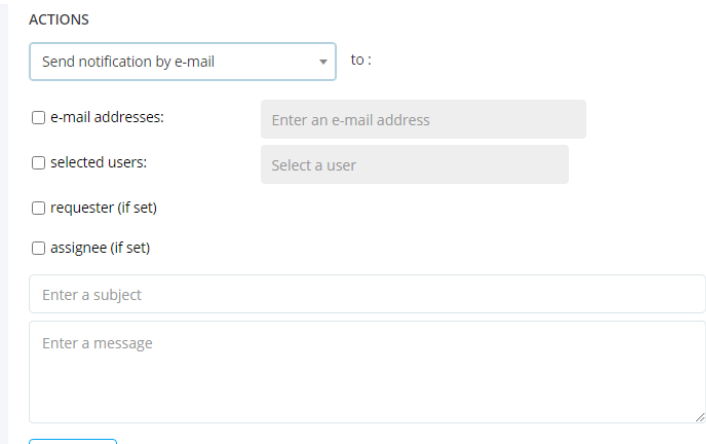
Automation conditions for an updated ticket

| Object | Object options | Condition |
|---------------------------|---|--|
| Ticket subject | was changed | - |
| | was not changed | |
| | contains at least one of the words | enter words divided by commas |
| | does not contain any of the words | |
| | contains all of the following words | |
| Ticket status | was changed | - |
| | was not changed | |
| | was changed to | New Open Waiting for response Suspended Closed |
| | was changed to status other than | |
| | was changed from | |
| | was changed from other than | |
| is equal to | | |
| | is not equal to | |
| Ticket priority | was changed | - |
| | was not changed | |
| | was changed to priority higher than or equal to | select priority |
| | was changed to priority higher than | |
| | was changed to priority lower than or equal to | |
| | was changed to priority lower than | - |
| | was changed to default | |
| | was changed to priority other than default | |
| | was changed to | select priority |
| | was changed to status other than | |
| | was changed from | |
| | was changed from other than | |
| | is equal to | |
| | is not equal to | |
| | is higher than or equal to | |
| is higher than | | |
| is lower than or equal to | | |
| is lower than | - | |
| is the default priority | | |
| | is not the default priority | |
| Ticket category | was changed | - |
| | was not changed | |
| | was changed to default | |

| | | |
|------------------|-------------------------------------|---|
| | was changed to other than default | |
| | was changed to | |
| | was changed to other than | |
| | was changed from | select category |
| | was changed from other than | |
| | is equal to | |
| | is not equal to | |
| | is the default category | - |
| | is not the default category | - |
| Requester | was changed | - |
| | was not changed | - |
| | was changed to | enter the requester |
| | was changed to other than | |
| | was changed from | |
| | was changed from other than | |
| | is equal to | |
| | is not equal to | |
| Related device | was changed | |
| | was not changed | - |
| | was changed to set | - |
| | was changed to not set | - |
| | was changed to | |
| | was changed to other than | |
| | was changed from | enter the device name |
| | was changed from other than | |
| Public comment | is equal to | |
| | is not equal to | |
| | is set | - |
| | is not set | - |
| Internal comment | was added | |
| | was not added | - |
| | was added by user with the role | Administrator HelpDesk Staff End-user |
| | was not added by user with the role | Administrator HelpDesk Staff End-user |
| Updater | was added | - |
| | was not added | - |
| Updater | was added by user with the role | Administrator HelpDesk Staff End-user |
| | was not added by user with the role | Administrator HelpDesk Staff End-user |
| Updater | has a role | Administrator HelpDesk Staff End-user |
| | does not have a role of | |

10.11.5 Automation actions

The following actions can be performed when the trouble ticket meets one or many of the conditions defined in the automation rule:

| Action | Description |
|------------------------------|---|
| Change category | Changes the ticket category. |
| Change priority | Changes the ticket priority. |
| Change status | Changes the ticket status. |
| Assign a related device | Adds the specified device to the trouble ticket summary as a related device. |
| Add text to subject | Adds predefined text, e.g. prefix "Important", at the beginning of the ticket subject line |
| Add internal comment | Adds a predefined internal comment to the ticket history |
| Send notification by e-mail | Sends an e-mail message defined by the administrator (subject + content) to selected users: |
| |  |
| Add to the list of observers | Adds selected users to the list of ticket observers. |

Actions are available depending on the selected automation conditions.

10.11.6 Editing an automation

To edit an automation:

1. Log in to the HelpDesk interface.
2. In the main navigation, on the left-hand side of the interface, select **Automations**.
3. In the automation list select the one to be edited.
4. In the automation's context menu (upper right corner of the tile), click the **Edit** link.
5. Change the name, description, status, conditions or automation actions, just as in the case of [Adding an automation](#)⁴⁶⁰.

6. Save changes by clicking the **Save changes** button.

The screenshot shows the 'Editing automations' page in the HelpDesk interface. The left sidebar contains navigation options like Dashboard, Tickets, Knowledge base, Event log, Reports, Absence plan, Ticket visibility, Ticket assignment, Automations, SLA metrics, and Settings. The main content area is titled 'Editing automations' and contains a form with the following sections:

- GENERAL INFORMATION:** Name: 'Marking the ticket as response pending', Description: 'Automation marks the ticket as response pending when the technical support engineer provides a public response to the person reporting the problem.', Current state: 'On'.
- CONDITIONS:** 'If met' set to 'all', 'conditions for ticket' set to 'after it has been edited'. Conditions include 'Public comment was not added by a user with t... User' and 'Ticket status is equal to Open'.
- ACTIONS:** 'Change status to' 'Waiting for response'.

At the bottom of the form, there are 'Save changes' and 'Cancel' buttons.

10.11.7 Activating/deactivating an automation

The created automations can be toggled off (deactivated) for a time when they should not be applied for trouble ticket processing, e.g. when the employee is on holiday. There is no need to remove the automation rule completely.

The screenshot shows the 'All automations (3)' page in the HelpDesk interface. The left sidebar has 'Automations' selected. The main content area displays a list of three automation rules, each with a toggle switch to activate or deactivate it:

- Marking the ticket as response pending:** Description: 'Automation marks the ticket as response pending when the technical support engineer provides a public response to the person reporting the problem.' WHEN: 'After update'. CONDITIONS: 'Public comment was not added by a user with the role 'User' and ticket status is equal to 'Open''. ACTIONS: '01. Change status to 'Waiting for response''. The toggle switch is currently turned off.
- Opening the ticket after a response from the person reporting:** Description: 'Automation reopens the ticket when the person reporting responds to the technical support engineer.' WHEN: 'After update'. CONDITIONS: 'Public comment was added by a user with the role 'User' and ticket status is equal to 'Waiting for response''. ACTIONS: '01. Change status to 'Open''. The toggle switch is currently turned on.
- Opening the ticket after work on the ticket has been started:** Description: 'Automation opens the ticket when the technical support engineer starts to work on it or edits its properties.' WHEN: 'After update'. CONDITIONS: 'Updater does not have a role of 'User' and internal comment was not added and ticket status is equal to 'New''. ACTIONS: '01. Change status to 'Open''. The toggle switch is currently turned on.

At the bottom, there is an 'EMBEDDED MECHANISM ACTIVATION SEQUENCE' section and a 'SEE ALSO' section with links to 'Help center - Automations' and 'Ticket assignment'.

To deactivate (or activate) an automation:

1. Log in to the HelpDesk interface.
2. In the main navigation, on the left-hand side of the interface, select **Automations**.
3. In the automation list select the one to be edited.

4. In the automation's context menu (upper right corner of the tile) click the **Deactivate** link (or **Activate**, if the automation is already disabled).
5. Confirm the action in the dialog box by clicking the **Deactivate (Activate)** button.

The automation rule can also be toggled on or off by changing the automation status during editing.

10.11.8 Deleting an automation

To delete an automation rule:

1. Log in to the HelpDesk interface.
2. In the main navigation, on the left-hand side of the interface, select **Automations**.
3. In the automation list select the one to be deleted.
4. In the automation's context menu (upper right corner of the tile) click the **Remove** link.
5. Confirm deleting in the dialog box by clicking the **Remove** button.

10.12 SLA metrics

10.12.1 Overview

SLA (*Service Level Agreement*) is an agreement about the guaranteed level of the provided service. The HelpDesk enables the definition of various SLA metrics which allow the monitoring of whether objectives set forth in the SLA agreement are duly executed.

The chapter on the execution of the service level compliance provisions is divided into the following articles:

- [SLA metric types](#)⁴⁶⁸
- [SLA metric conditions](#)⁴⁶⁸
- [SLA metric validity time](#)⁴⁶⁹
- [Creating and versioning SLA metrics](#)⁴⁷⁰
- [Violation of SLA](#)⁴⁷¹
- [SLA metrics in tickets](#)⁴⁷²

Related topics

 [Closed tickets under SLA reports](#)

 [SLA metric course reports](#)

 [SLA violation reports](#)⁴⁵⁵

10.12.2 SLA metric types

Each metric can have one of the two time measurement methods:

- **Waiting time for the first response**

The metric starts running when a trouble ticket is created.

The metric irrevocably stops when the first public comment, authored by a user with HelpDesk employee or administrator role, appears in the ticket.

- **Total waiting time for ticket solution**

The metric starts running when a trouble ticket is created.

The metric is suspended when the ticket status is changed to “waiting for response” or “suspended”.

The metric is restarted (continues) when the ticket status is changed to “open”.

The metric irrevocably stops when the ticket status is changed to “closed”.

10.12.3 SLA metric conditions

SLA metric can include a defined extensive list of conditions related to:

- ticket priority (*is equal to / is not equal to*),
- ticket category (*is equal to / is not equal to*),
- reporting person (*is equal to / is not equal to / belongs to group / does not belong to group*),
- assigned person (*is equal to / is not equal to / belongs to group / does not belong to group*),
- ticket source (*is an e-mail message / is a web application interface*).

Subsequent conditions can be combined only with the logical operator “AND” (i.e. all conditions are met). If a collection of N values is allowed within one condition, the entire item is considered as N conditions combined with the “OR”/“NOR” operator.

A ticket is eligible to be covered by the selected SLA metric if it meets all of its conditions in a continuous manner. If, due to change of a property (e.g. priority), the ticket no longer meets the metric conditions, it is automatically no longer covered by the metric. The metric which no longer covers a ticket automatically stops, regardless of whether it was fulfilled or not.

Analogically – if, after a change of a property the ticket is eligible to be covered by other additional metrics, it is automatically covered by such metrics. If the ticket is covered by the same metric once again, the system handles it as a restart (continuation) of the metric, not as the creation of another instance of the metric.

In certain cases, this may mean that after the change of ticket properties, the new SLA metric will be exceeded from the moment when it begins to cover the ticket.

Example:

There are two SLA metrics in the system:

- 1. Tickets with “high” priority shall be solved in 4 hours.*
- 2. Tickets with “critical” priority shall be solved in 2 hours.*

A ticket with “high” priority has already been processed for one hour. If its priority gets changed to “critical”, it is no longer covered by the first metric and it becomes covered by the second metric. There is only one hour left until the metric is exceeded.

10.12.4 SLA metric validity time

Note: All mechanisms described below are based on the time zone set on the server where the Axence nVision® application is installed. The HelpDesk system does not allow any time zone, other than the local time of the server (with Axence nVision®), to be indicated. It is also not possible to set different time zones for specific users.

Each SLA metric allows one of the two options to be selected during its creation:

- **Metric valid without interruptions (All day, all week).**
- **Metric valid only in specified intervals (Defined days of the week and times of the day):**
 - Validity hours can be defined separately for each day of the week (from Monday to Sunday). Each day of the week can have one time span (e.g. 09:00 to 17:00) or none (for days off work). Defining more than one time span for a given day of the week is not possible (e.g. Monday from 08:00 to 11:00, and then from 13:00 to 16:00).
 - A metric with the time span defined in such a manner is considered to be active in hours outside of the specified range, even though its time counter is not running during such periods.

Example:

A metric is valid from 08:00 to 16:00.

The metric requires the ticket to be solved within one hour.

The ticket covered by the metric appears at 15:30 and no-one starts to work on the ticket.

At 15:31 the metric is running, with 59 minutes left.

At 16:01 the metric is running, with 30 minutes left.

At 07:59 on the next day, the metric is running, with 30 minutes left.

At 08:15 on the next day, the metric is running, with 15 minutes left.

At 08:30 on the next day, the metric is exceeded.

When creating the SLA metric, along with the definition of the validity hours, you can also determine whether the metric should stop on days configured as days off work.

Calendar of days off work

If the selected metric is defined as bound by the calendar of days off work, it stops for the days which are indicated in such a calendar. Each day off overrides the metric validity hours which are specified in its configuration.

The calendar of days of work can be configured during the [creation of SLA metrics](#)^[470].

The system has a calendar of days off work where specific days can be defined as days off.

- A day off work shall be considered as a specific day of a specific month and of a specific year, starting on 00:00 (inclusively) and lasting until the hour of time quantum prior to 00:00 on the next day, according to the server time where the Axence nVision® application is installed.
- Persons authorized to edit the days off work are solely the users with the Administrator role; only days which have not started yet can be edited. If a day off has already started, there is no way to cancel its definition.
- Days off work can be defined only as single days (it is not possible to specify a range of dates, e.g. "December 24-26, 2017").
- Defining cyclical days off is not possible.
- The calendar of days off work is shared by all SLA metric definitions.

10.12.5 Creating and versioning SLA metrics

Creating user groups in Axence nVision®

To create a user group:

1. In the main window of the Axence nVision® console, click the [Users](#)^[360] section icon.
2. Go to the **Tools and options** tab.
3. Click the **Add group** button.

To add a user to the group:

1. Go to the **Users** section in the Axence nVision® Console.
2. Drag the selected users to the target group.

To create an SLA metric:

1. In the HelpDesk web interface, navigate (as an administrator) to the **SLA metrics** view.
2. Click the **Add SLA metric** button.
3. In the metric adding dialog box, enter the **metric properties**:
 - Name – for better identification of the SLA metric. Maximum length: 150 characters.
 - Description – (optional) additional description field; can be used by the user for any purpose. Maximum length: 300 characters.
 - [List of conditions](#)^[468] – a collection of conditions describing the tickets which the metric will be applied to.
 - [Metric type](#)^[468] – the method of time measurement by the given metric.
 - Time limit – the time value which, if exceeded, means that the SLA conditions are violated. Minimum value: 30 minutes, maximum value: 31 days.
 - Alert – an additional e-mail address for sending notifications on each metric violation (optional).
 - [Validity time](#)^[469] – a field allowing the selection of either the mode without interruption, or the mode where time runs only in specified periods.

- List of hours (optional) – if the interrupted mode was chosen, this field is used to define the hours within which the SLA limit is running (for a specific day of the week).
 - [Calendar of days off work](#)^[469] – true/false field, which decides whether the SLA metric is stopped during days off work. Click the *With exclusion of days off work* link to define the list of days off work.
4. To save the metric, click the **Add SLA metric** button.

Versioning of SLA metrics

SLA metric is a versioned entity where all of its properties, except for the name, are subject to versioning. The name is the parameter which remains common for subsequent metric versions and is editable at any time.

Adding a new metric is equivalent to the creation of its first version. When a version is set, its “validity start date” is set as the current date. It means that only tickets reported after this date can be covered by this version of the metric.

When a version of SLA metric is created, it is not possible to re-edit it. Once created, the SLA metric version can be only archived or archived with the simultaneous creation of a new version.

Archiving SLA metric version

When archiving, the “validity end date” in the metric is automatically set to the current date. It means that all tickets created after that date cannot be covered by the metric. Tickets currently covered by the archived metric will remain covered by this version until the end of their life cycle (if they meet metric conditions).

Creating a new SLA metric version

In the case of a valid SLA metric, you can create a newer version of it (always with the simultaneous archiving of the current version). It allows the continuity of such a metric to be maintained.

If a new metric version is created, the system automatically substitutes values from the older version into the respective data fields.

A new version of the metric can also be created for each metric which had previously been archived without creating a new version of it.

Formally, each new version is an independent SLA metric. Metrics are grouped by name only to support their change management processes.

To simplify the system, it is not possible to edit the version validity dates manually. The current version is always valid from the moment of its creation, and has no end date until it is archived.

10.12.6 Violation of SLA

Violation of SLA metric is the expiry of the time limit defined in the metric. Once violated, the metric is permanently visible in the history of metrics covering the given ticket (even if the ticket no longer fulfills its conditions).

A metric can be violated only once. If a violated metric ceases to cover a ticket (and was stopped due to this), and then starts to cover the ticket once again, the metric is treated as if it had been running without interruption from the very beginning.

Metric running time and the duration of ticket covered by the metric are measured and processed separately by the system.

Example:

A ticket has a “critical” priority and is covered by metric: “critical priority tickets shall be solved in 4 hours”.

The ticket is in “open” status all the time.

After 4 hours, the metric is exceeded.

After 5 hours, the ticket ceases to be of “critical” priority. The metric stops running, but it will be forever visible in the ticket as exceeded by one hour.

After 6 hours, the ticket still has the same metric visible as exceeded by one hour.

After 7 hours, the ticket is once again assigned with “critical” priority. The same metric is from now on visible as active and exceeded by 3 hours.

After 8 hours, the ticket status is changed to “closed”. The metric is irrevocably stopped with a state of exceeded by 4 hours.

When SLA metric violation occurs, a notification is generated (in the interface and as an e-mail message) to the person currently assigned to the ticket and to the e-mail address defined in the metric (if any).

For the purposes of ticket visualization in the ticket list, a dynamically generated “SLA violation date” column is defined. The column shows the earliest SLA violation date (also including overdue items) of all metrics active in relation to the ticket. If no metric is currently active, the column holds no value. If SLA time limit has expired, the value in the column is highlighted in orange.

If the ticket starts to be covered by a new SLA metric for which the time limit has already expired, the system also distributes notification about such a fact. However, each ticket cannot generate more than one time limit expiry notification for each SLA metric.

Example:

Ticket “X” is covered by metric “A”.

Metric “A” is violated.

Notification about the violation of metric “A” in ticket “X” is distributed.

Ticket “X” properties are edited in such a manner so that it is no longer covered by metric “A”.

The ticket properties are re-edited in such a manner that it is once again covered by (already overdue) metric “A”.

Repeated notification is not sent, as one notification about metric “A” in relation to ticket “X” has already been generated.

10.12.7 SLA metrics in tickets

A ticket can be covered by any number of metrics of any type. The metrics covering the ticket are only visible for users with “HelpDesk employee” or “Administrator” roles.

The [ticket details](#)³⁹² view (section "Service provision level") for the ticket covered with SLA metrics enables the metrics to be checked, according to the following classification:

1. Active metrics

These are metrics measuring the time until the first response (currently running) and metrics of the total ticket solution time (running or not running). The list must be sorted from the metric with the shortest time until expiry (or from the metric exceeded to the largest extent).

Sorting in such a way allows the user to focus on SLA metrics which are running or which can be restarted. It lets the user check the metrics which can be still fulfilled.

2. Completed metrics

These are metrics which are no longer running:

- metrics of **time of waiting for the first response** – after the first response is given,
- metrics of **total ticket solution time** – after the ticket is closed, or metrics which were violated and then ceased to cover the ticket (and therefore their run is also completed).

Completed metrics allow you to check in what period they covered the ticket, and whether they were violated or not.

It lets you confirm in detail whether the provisions of any SLA were violated in the history of work on the ticket.

For the purposes of ticket visualization in the ticket list, a dynamically generated "SLA violation date" column is defined. The column shows the earliest SLA violation date (also including overdue items) of all metrics active in relation to the ticket. If no metric is currently active, the column holds no value. If SLA time limit has expired, the value in the column is highlighted in orange.

Dates in the ticket list are not updated automatically and always show the system status at the moment when the list was loaded. Single ticket detail view is updated on a current basis (max. every minute).

If the ticket is closed, it cannot be covered by any new metrics (even if the users' assignment to groups are changed). All metrics stop running and the period covering the specific ticket is formally ended.

10.13 Announcements

The messaging mechanism available in HelpDesk module allows passing information to users with installed Agent in an easy way, setting their validity time, and collecting the message read notifications from the users.

A message can be created by the administrator after logging in to the **HelpDesk Console**, with use of the **Announcements** option located on the right-hand side of the interface.

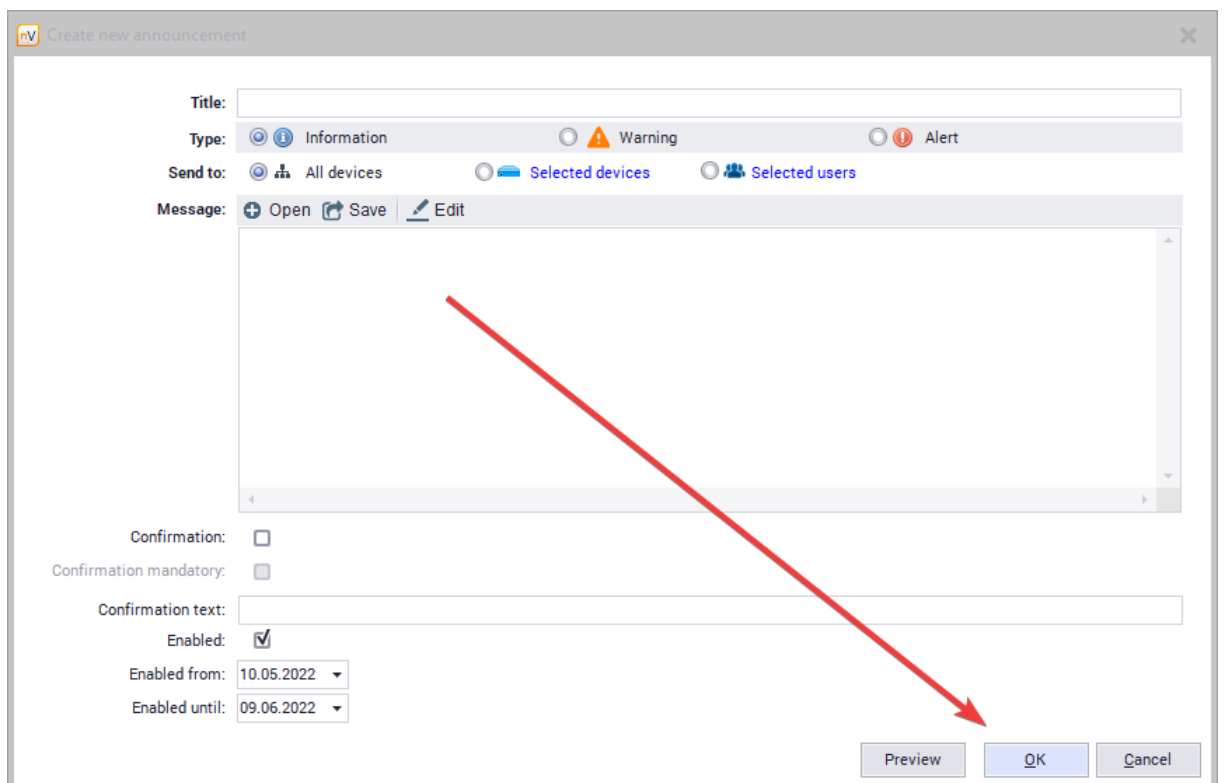
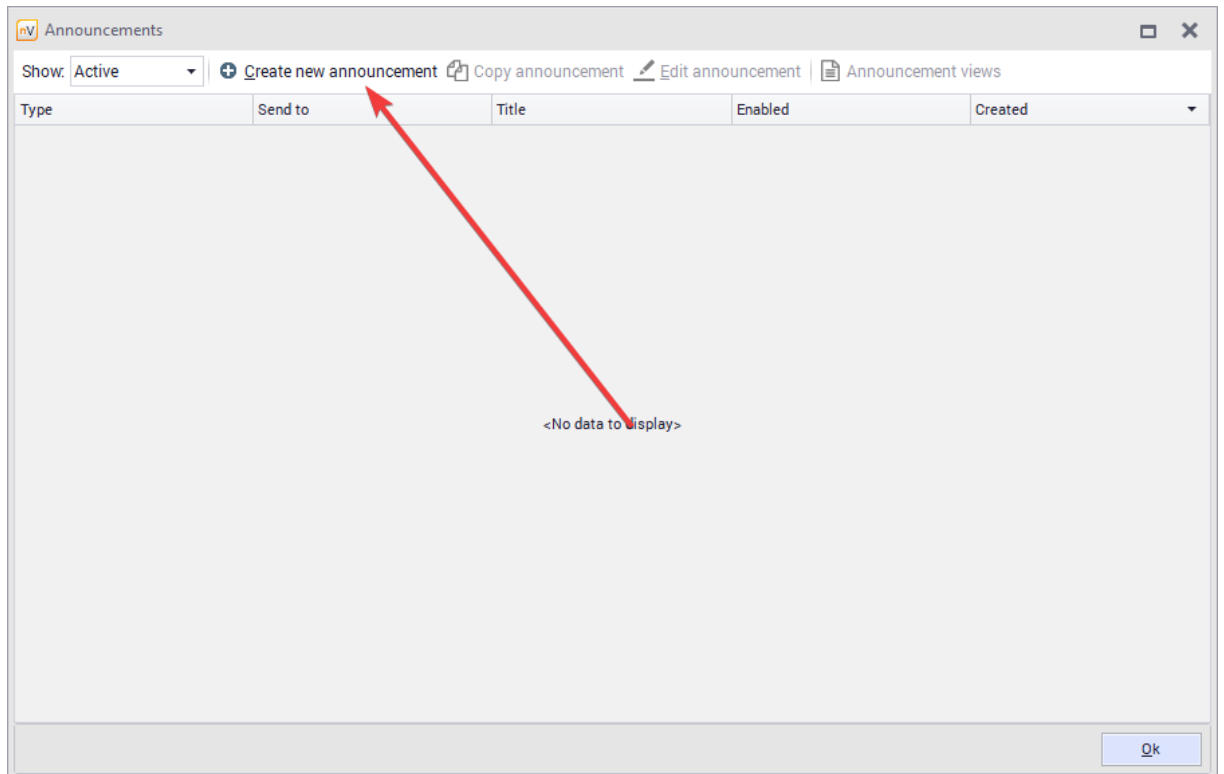
Creating a message

In order to create a new message, select **HelpDesk / Announcements / Create a new announcement** and fill in the fields described below.

| Field | Description |
|-------|-------------|
|-------|-------------|

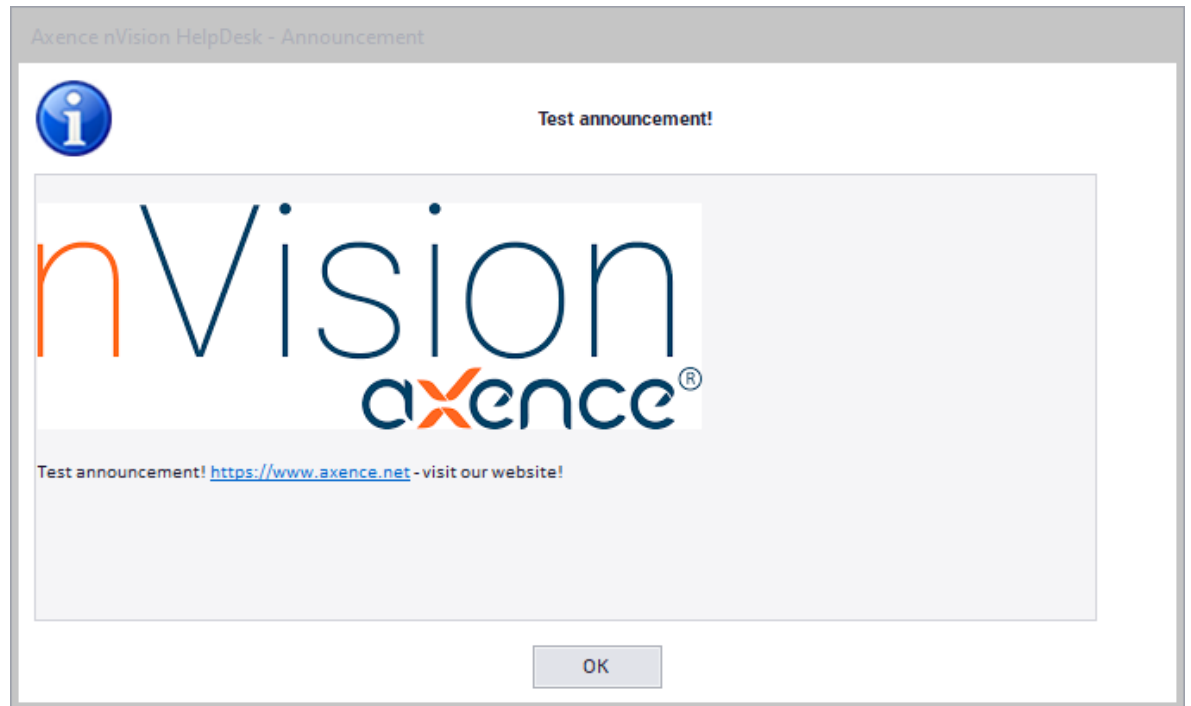
| | |
|--------------|--|
| Title | Message title. |
| Type | Depending on the type of information, one of the three available types can be chosen: Information , Warning , Alert . |
| Send to | Send message to All hosts , Selected hosts (choose from the list of hosts) or Selected users (choose from the list of users). |
| Message | Message contents. |
| Confirmation | If the Confirmation field is checked, the user will see the confirmation text presented below. Similarly, if the Mandatory confirmation field is checked, the user will not be able to use HelpDesk any further, before they confirm the reading of the message. |
| Enabled | An active (enabled) alert will be displayed in the time range specified by the start and end dates. It is possible to create an inactive message, i.e. one without a determined time of displaying. To change the message status or contents, click the Edit button. |

The screenshot displays the Axence nVision interface. The top navigation bar includes buttons for 'Main', 'Tools', 'About nVision', and 'Global search (Ctrl+G)'. Below this, there are several tool icons for tasks like 'Generate protocol', 'MFI packages manager', 'Print bar codes', 'Asset settings', 'Configure license type', 'Inventory', 'Connected devices', 'Management permissions', 'Printout audit', 'Configure print cost', 'Reports', 'View events', 'Alerts', 'Distribution tasks', 'Announcements', 'Open HelpDesk', 'Open SmartTime', and 'Open AdminCenter'. The main area shows a network map with a 'Network Device' section containing 'CONVALLIS-SOQIIS' and 'SUSPENSIOSEVENORIENT'. Below that is an 'IP Phone' section with a grid of 24 phone icons, each with a status indicator (e.g., 'Down: 801d 23h', 'Down: 815d 1h'). A red arrow points from the 'Helpdesk' button in the top bar to the 'SUSPENSIOSEVENORIENT' device in the network map.



Message layout

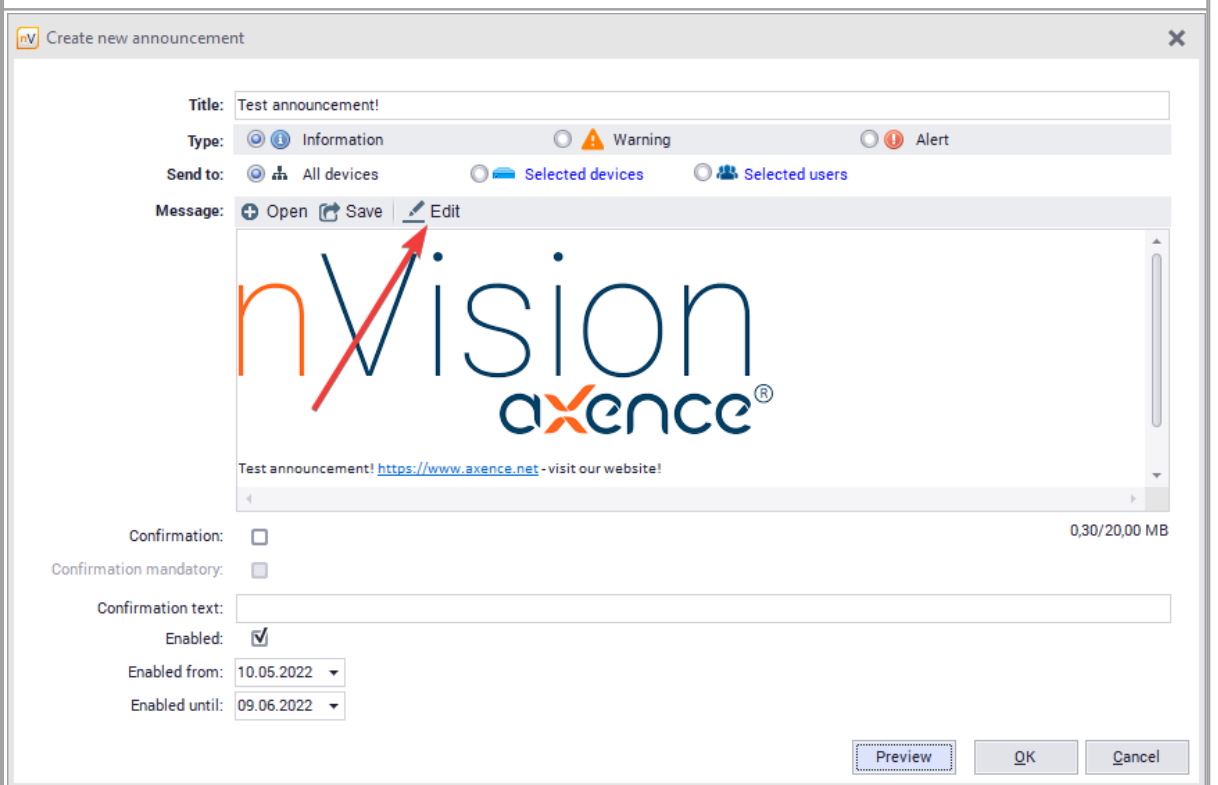
The message layout depends on the selected options. An example message is presented below.



Editing an announcement in the message

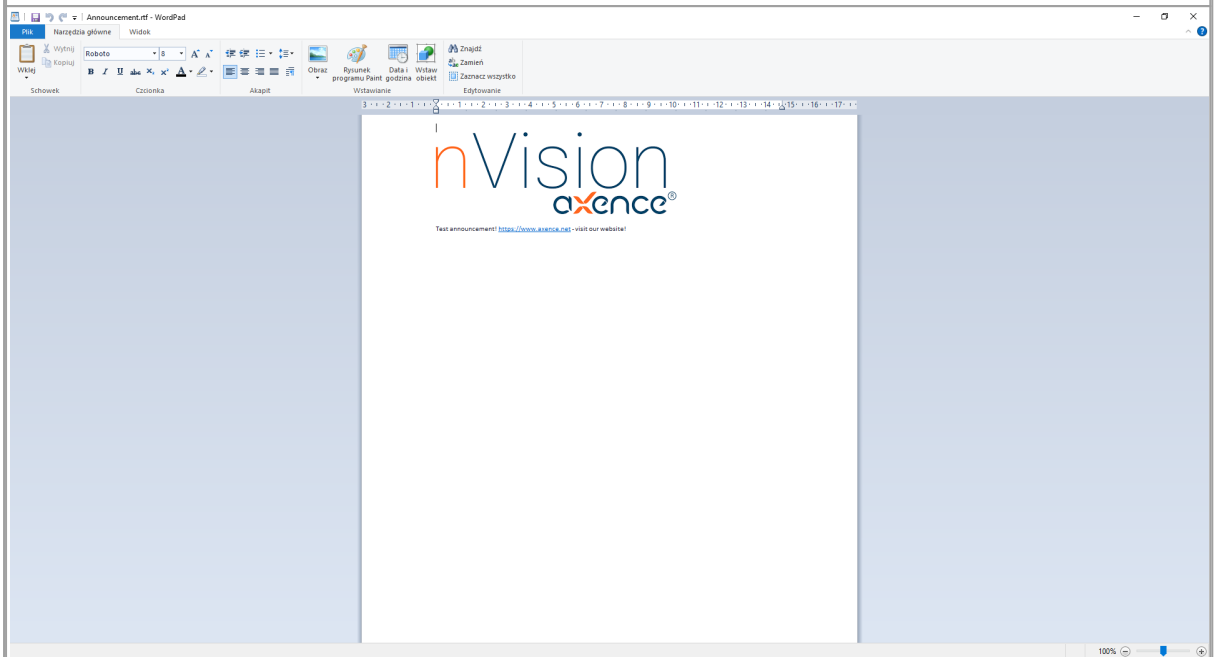
The nVision console allows you to edit the **Announcement** field in the message.

To edit the Announcement field in the message, click the **Edit** button in the message creation window.



After clicking, WordPad will open in a new window where you can edit the message, e.g. by adding an image, link, attachment (for instance by dragging a file into the word processor), or by formatting the

message text, etc.



When you finish editing the message:

1. Save the file
2. Close the word processor window


When you close the word processor, the comment text will be displayed in the **Announcement** field in the message creation window. Fill in the remaining fields in the form and your message will be ready for creation!

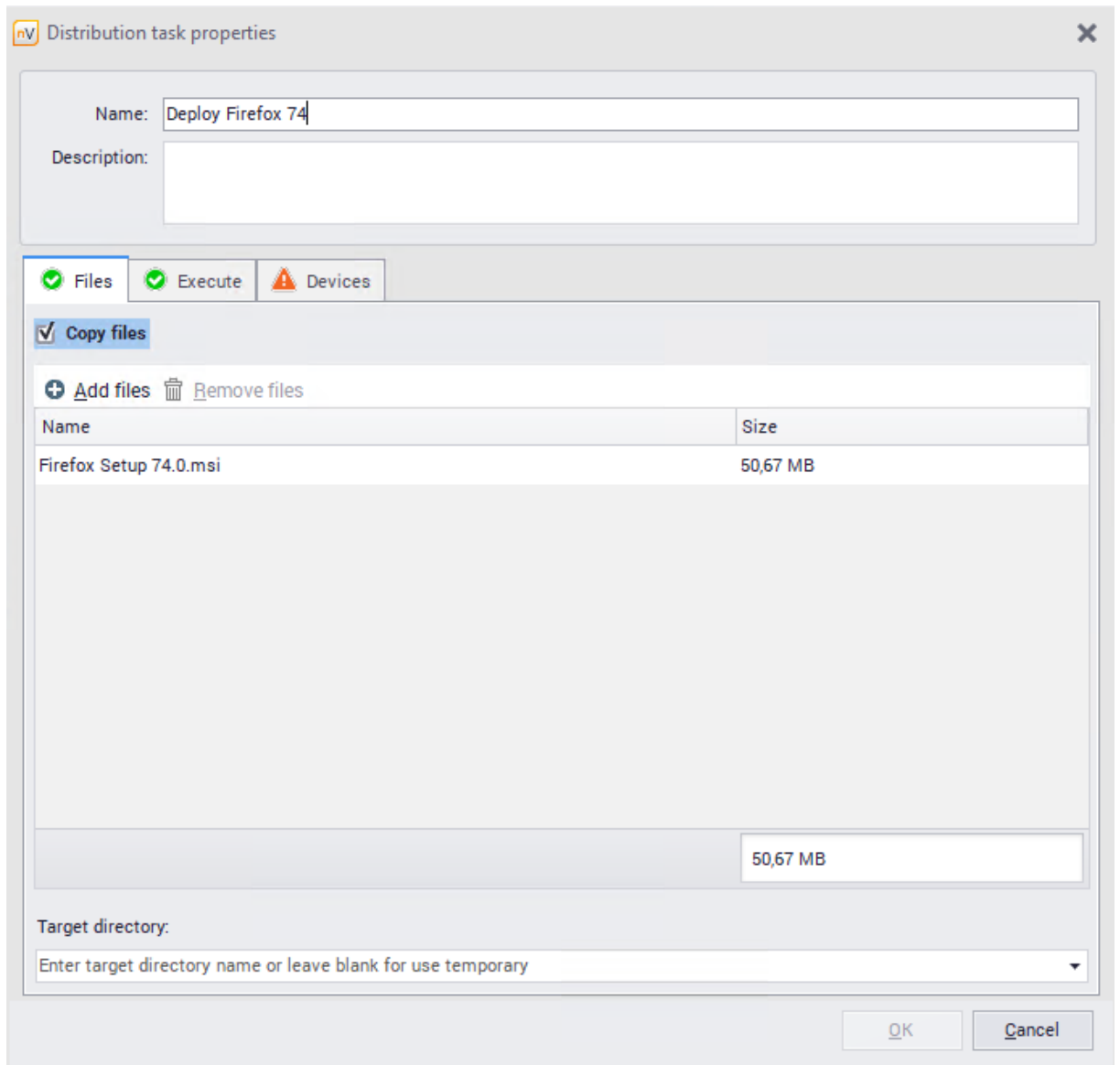
10.14 File distribution

File distribution with the use of Agents

Files can be distributed to workstations with an installed Agent. For more information about Agents, see the chapter [Agents](#) ¹¹⁴.

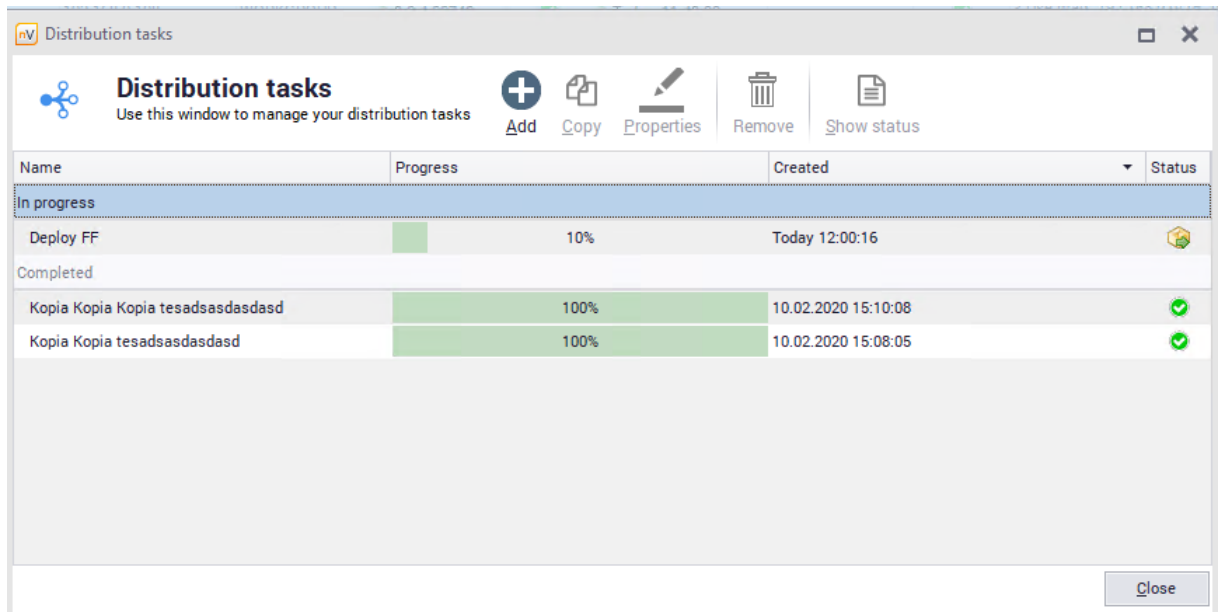
To distribute files:

1. Select the **Distribution tasks** in the main menu.
2. In the **Distribution tasks** window, select  **Add**. Specify the task **Name** and **Description** (optionally).



3. If you want to copy files, **Add** the files to be distributed. You can specify a **Destination folder**. If the field is left empty, a temporary folder will be used (C:\Windows\Temp).
4. If you want to run files, go to the **Execution** tab. Specify the execution folder and parameters (optionally, e.g. silent and unattended installation).
5. In the **Devices** tab, select **Add devices**. Use the list to add devices on which you want to run or distribute files. When the action is complete, click **OK**.

The created distribution task will be added to the list. If the destination machine is turned off, tasks will be queued and executed upon the first contact between the Agent and nVision. Progress can be checked at any time in the **Distribution tasks** window.

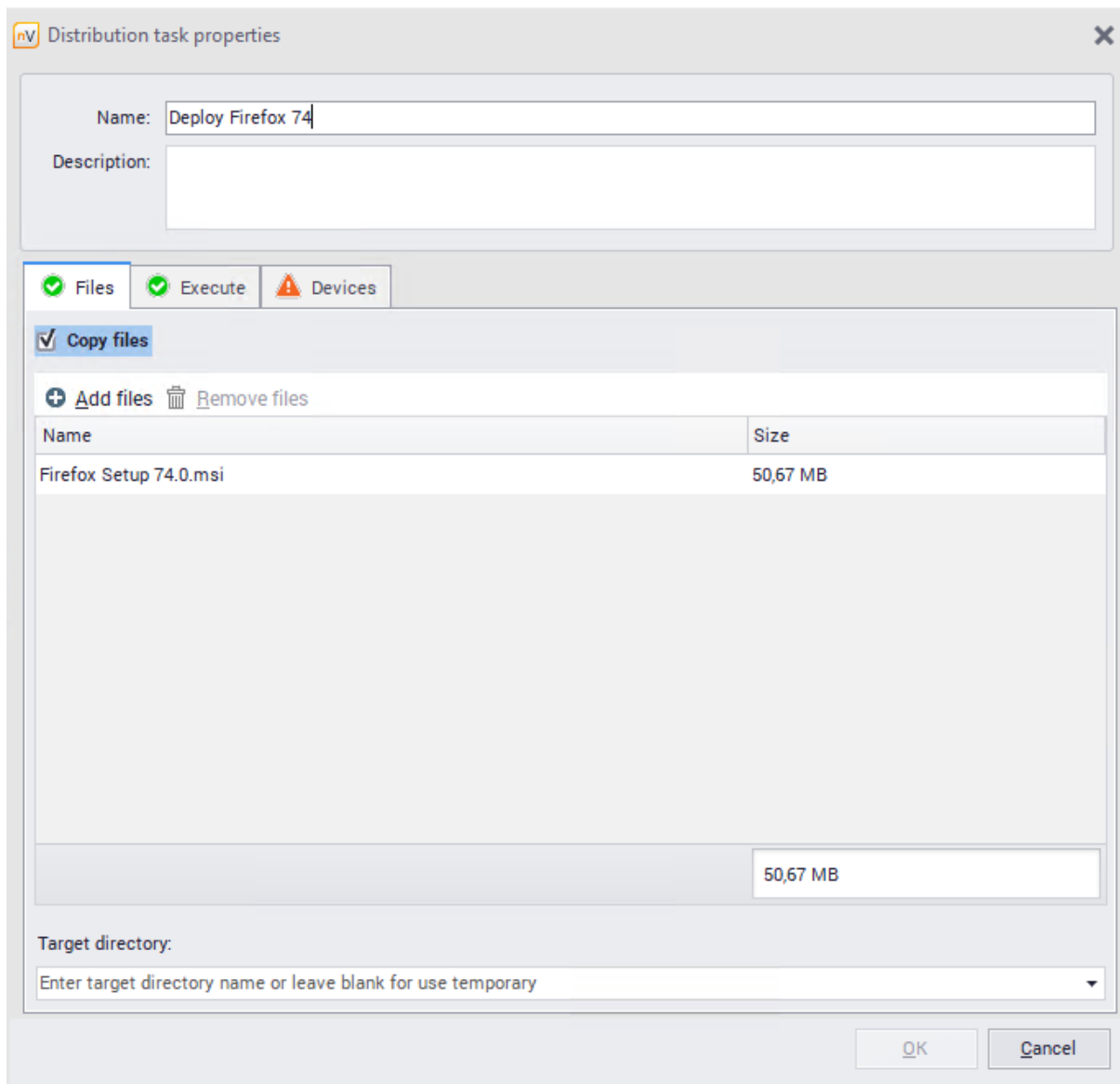


Pending tasks are also displayed in the **Agents** tab in the main nVision window.

Remote software installation with MSI package

To distribute and install an MSI package:

1. Select the **Distribution tasks** in the main menu.
2. In the **Distribution tasks** window, select **Add**. Specify the task **Name** and **Description** (optionally).
3. **Add** the MSI package to be distributed and specify the destination folder.



4. Navigate to the **Execution** tab, check the **Run program** field and fill the options as shown in the following screenshot.

The screenshot shows the 'Distribution task properties' dialog box with the following details:

- Name:** a
- Description:** (empty)
- Execute program:**
- File or command:** msiexec
- Start in:** C:\
- Parameters:** /i Firefox-74.0-pl.msi /qn
- Execution time:** Immediately, While users are logged out, After specified hour of a day (17:00)

5. In the **Devices** tab, select **Add devices**. Use the list to add the devices on which you want to distribute and run the MSI package. Then click **OK**.

The generation of the MSI package distribution task can also be automated in the following manner:

1. Check the Agent(s) icon.
2. Right click the Agent icon, use the pop-up menu to select **Agent / Install an MSI package**.
3. Select the MSI installer file in the dialog box.
4. When the installer file is specified, the distribution task properties window will appear with automatically filled task parameters. Along with adding the file, the following parameters will be filled automatically:
 - name,
 - description,
 - command,

- default parameters for silent installation (unattended by the user),
- devices on which the task is to be executed will be added automatically.

All of the described parameters can be edited.

5. To finish the wizard and perform the task, click **OK**.

Remote software uninstallation

The Agent also allows for the remote uninstallation of the software installed with use of MSI packages. During the workstation inventory, the Agent also collects information on the manner of software installation (through scanning registry entries). **The option of uninstallation from the level of the nVision Console is only available for the programs installed by the Windows Installer (MSI packages).**

The software uninstallation task is performed immediately, if the Agent is connected to the Axence nVision® Server. Otherwise, the task is queued and performed at the next connection.

To uninstall software remotely:

1. Navigate to **Device details / Inventory / Program** window.
2. Find the program to be uninstalled in the installed applications list. Select it.
3. Use the toolbar to select **Uninstall** or right click and select **Uninstall**.
4. The status in the **Uninstallation progress** column will change to **Pending**.

or

1. Go to the **Devices / view** menu, **Agents / Software audit**.
2. Find the program to be uninstalled in the detected applications list. Double-click its name to open the detected installations window.
3. Select the name of the machine from which the program will be uninstalled, and use the toolbar to select **Uninstall** or right click and select **Uninstall**.
4. The status in the **Uninstallation progress** column will change to **Pending**.

The **Uninstallation progress** column presents information on the remote uninstallation support and task status:

- Supported – remote uninstallation possible,
- Unsupported - remote uninstallation not possible,
- Pending – task was ordered, waiting for Agent connection,
- Task in progress – task is currently executed,
- Error – an error occurred (additional message is displayed in a “bubble” by the mouse cursor).

The task can be cancelled if the Agent has not connected with the nVision Server yet. To cancel the task, make sure the status in **Uninstallation progress** is displayed as **Pending**, right click and select **Abort uninstallation** in the pop-up menu.

File distribution with the use of WMI

nVision allows for the remote distribution of files to Windows machines. This is performed with use of WMI service, which requires the appropriate configuration of login credentials in device properties. Additionally, WMI service must be enabled on all remote machines.

To distribute files:

1. Right-click the Agent and select **Actions / Distribute file with WMI...**
2. Select the file to be distributed.
3. The selected file can be an executable file (e.g. installation file). It is possible to run such a file after it has been copied to a remote machine. This mechanism can be used to distribute programs or updates (fixes). Specify the runtime settings in the **Parameters** field and enable the **Run file when copied** option.
4. Select **All** to distribute a file to all machines or **Selected** to choose a specific group.
5. Click the **Install** button. A window will appear, displaying the distribution progress and allowing its successful completion to be checked.

10.15 Windows processes

The HelpDesk module displays active processes on the machines with installed Agents within the network.

To view the active processes on a selected host, navigate to the **Host info / Windows / Processes** window.

| PID | Process name | User | CPU 62% | Memory | Started |
|-------|--------------------------|-----------------|---------|-----------|---------------------|
| 7076 | ApplicationFrameHost.exe | Mikuz | 0% | 29 644 K | 30.03.2020 09:25:10 |
| 2828 | AxDBSrvr.exe | USLUGA SIECIOWA | 0% | 9 692 K | 30.03.2020 09:23:46 |
| 2808 | AxDBSrvrA.exe | SYSTEM | 0% | 23 564 K | 30.03.2020 09:23:46 |
| 8624 | Axence.nVision.Web.exe | SYSTEM | 0% | 159 400 K | 30.03.2020 09:26:12 |
| 3660 | AxenceSvcGuard.exe | SYSTEM | 0% | 856 K | 30.03.2020 09:23:50 |
| 5352 | browser_broker.exe | Mikuz | 0% | 8 252 K | 31.03.2020 11:54:09 |
| 2756 | conhost.exe | USLUGA SIECIOWA | 0% | 6 728 K | 30.03.2020 09:23:47 |
| 532 | csrss.exe | SYSTEM | 0% | 4 960 K | 30.03.2020 09:23:41 |
| 7464 | csrss.exe | SYSTEM | 0% | 4 092 K | 30.03.2020 11:02:15 |
| 452 | csrss.exe | SYSTEM | 0% | 4 872 K | 30.03.2020 09:23:41 |
| 7276 | ctfmon.exe | Mikuz | 0% | 16 012 K | 30.03.2020 11:02:20 |
| 7476 | dllhost.exe | Mikuz | 0% | 12 836 K | 30.03.2020 09:25:14 |
| 5276 | dllhost.exe | Mikuz | 0% | 7 028 K | 30.03.2020 09:24:42 |
| 5808 | dwm.exe | DWM-3 | 0% | 30 920 K | 30.03.2020 11:02:16 |
| 964 | dwm.exe | DWM-1 | 1% | 153 696 K | 30.03.2020 09:23:42 |
| 5464 | explorer.exe | Mikuz | 0% | 116 052 K | 30.03.2020 09:24:17 |
| 11224 | firefox.exe | Mikuz | 0% | 164 100 K | 31.03.2020 11:54:29 |
| 11784 | firefox.exe | Mikuz | 0% | 70 508 K | 31.03.2020 11:54:36 |
| 6624 | firefox.exe | Mikuz | 0% | 64 036 K | 31.03.2020 11:54:29 |
| 7504 | firefox.exe | Mikuz | 0% | 38 036 K | 31.03.2020 11:55:39 |
| 7784 | firefox.exe | Mikuz | 0% | 328 616 K | 31.03.2020 11:54:27 |

The process view also enables to stop the selected process, for example when it is not responding. To force the termination of a process, right-click on it and select **Terminate process**. You can also **close the whole process tree** by selecting the appropriate option from the context menu.

10.16 Remote command execution

When using the Agent within the HelpDesk module, it is possible to use the **remote command execution** feature (similar to Windows system command line).

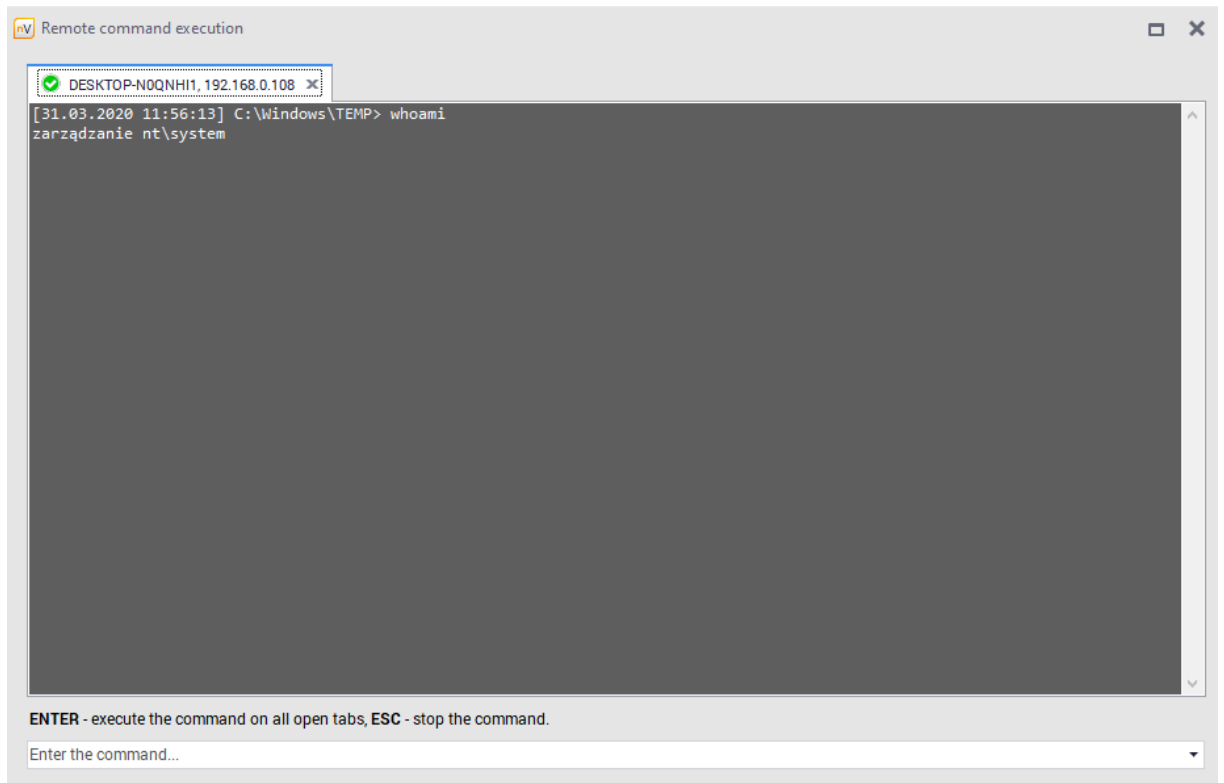
Perform the following steps:

1. Find the icon of the machine with the installed Axence nVision® Agent.
It is also possible to select several Agent icons – the remote command execution windows with tabs for all selected machines will open.
2. Select the icon of the computer with the Agent, right click it and select the **Web access / Remote command execution** option from the context menu.

The **Remote command execution** window can also be opened from the **Host info / Windows / Remote command execution** window.

3. A remote command execution window will open with the **Command** field where the required commands should be entered. To execute the command, click the **Execution** button or press **Enter**. When the remote command execution window is opened, a folder within which the commands will be executed and the result of **whoami** command (credentials on which command execution is based) are also displayed.

It is possible to execute commands on multiple hosts at the same time.



Examples of commands:

| Command | Action |
|----------------------|--|
| systeminfo | system overview, e.g. whether virtualization is working |
| ipconfig /all | network interface setup, including DNS server address |
| netsh wlan show all | wireless network setup, including currently detectable wireless networks |
| netstat -abfo | list of ports used by specific processes for listening / connecting |
| tracert <IP_nVision> | connection route between nVision Agent and nVision Server |
| query user | list of sessions for users logged in on the machine |
| tasklist /v | list of processes and sessions used by the processes, together with authorizations |
| taskkill /pid <PID> | termination of the selected process |
| tasklist /svc | list of services active on the machine |
| sc qc <SERVICE> | detailed information on the selected service |
| chkdsk c: /f /r /b | checking and repair of data on C: |

| Command | Action |
|---|--|
| dir c:\users\ <user>\downloads /a /s</user> | list of downloaded files in the selected user's folder |

10.17 Remote access

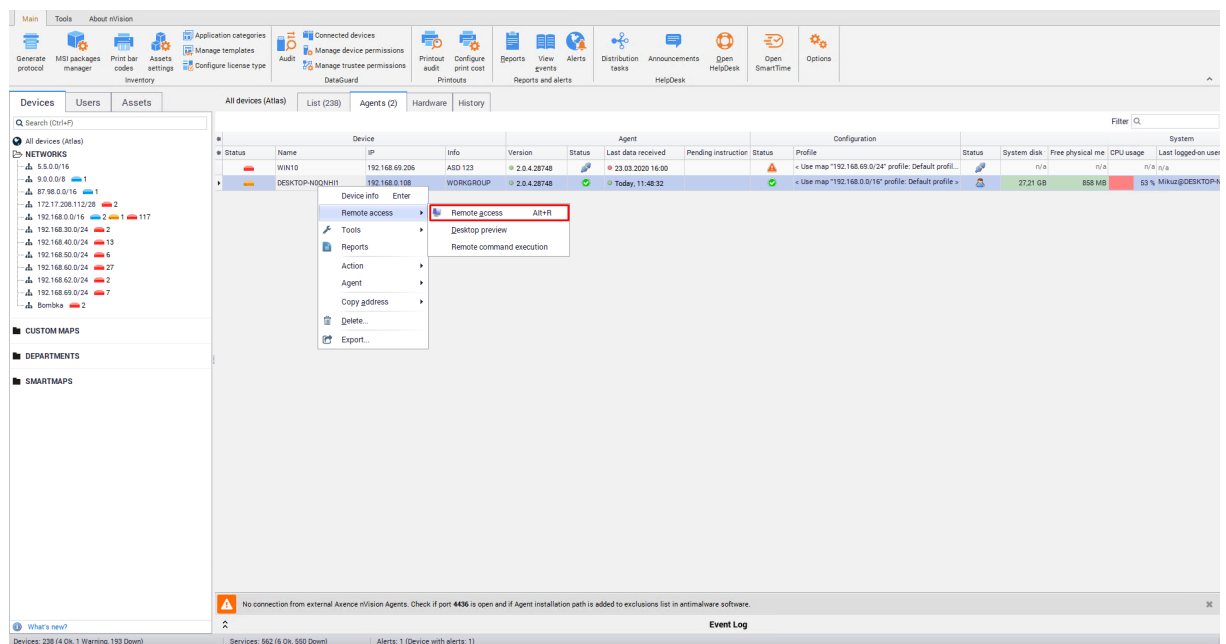
Requirements

The server, i.e. the central nVision program, must run on a static IP address.

Remote access tunneling in nVision

nVision listens on new TCP port 4436. During the installation, this port is configured only for Windows Firewall (to learn more, go to the [Ports](#) [22] topic).

The Agent establishes a connection with nVision – and the connection is maintained and used for communication. Therefore, remote access is available even if nVision cannot establish a direct connection to the Agent (e.g. the machine with the Agent is behind NAT). Remote access tunneling also works in nVision WebAccess.



Remote access options

In order to connect to the device remotely, right-click the device and select **Remote access** from the context menu. Then, select one of the **Access modes** in the remote access window:

| Option | Description |
|-----------------------------|---|
| View only | View user's window without the possibility of interfering with the user's device. |
| Concurrent access (default) | Both the user and the remotely connected administrator can perform actions on the device. |

| Option | Description |
|-------------------------------|---|
| Block user mouse | Remotely connected administrator can perform actions on the device. The user can perform actions using the keyboard, the mouse is locked. |
| Block user keyboard | Remotely connected administrator can perform actions on the device. The user can perform actions using the mouse, the keyboard is locked. |
| Block user mouse and keyboard | Remotely connected administrator can perform actions on the device. User's mouse and keyboard are locked. |

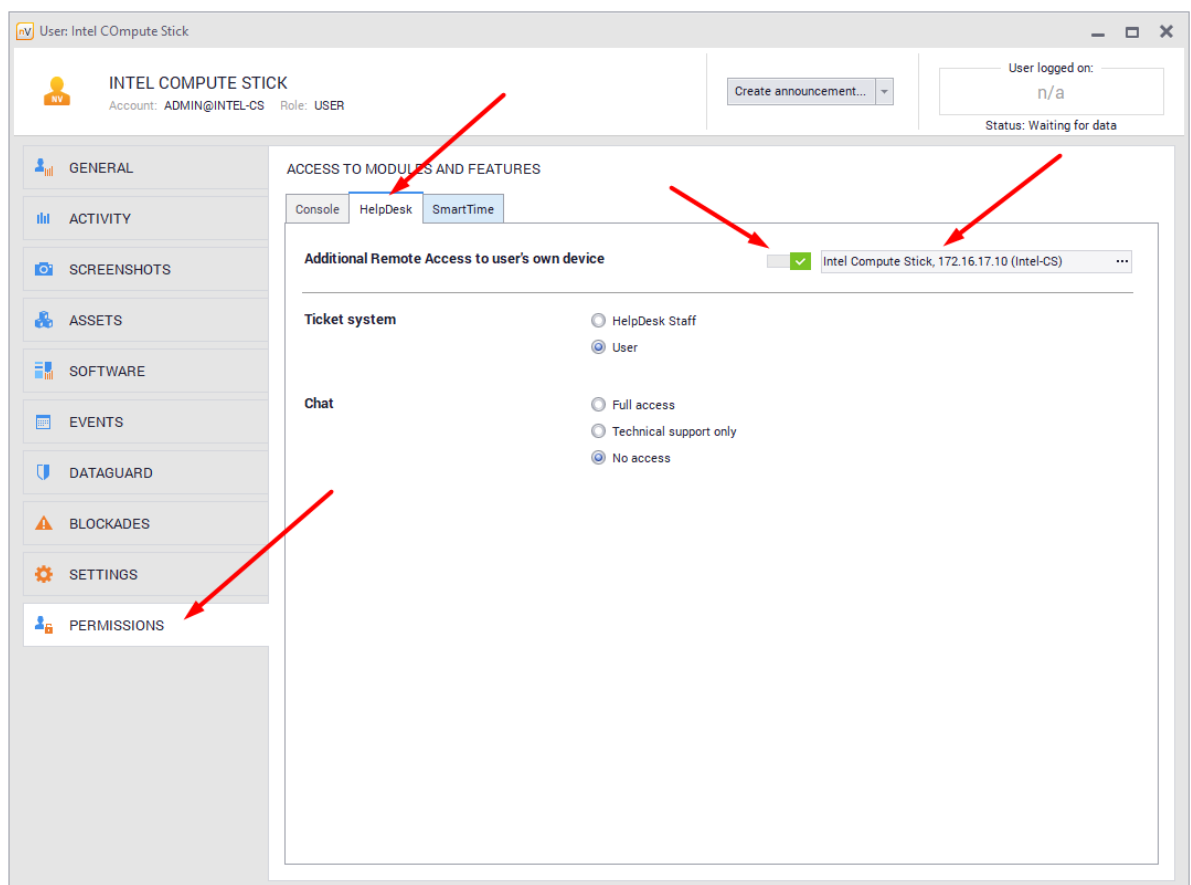
File manager

During the remote access session, it is possible use the file manager to transfer and copy data between workstation in a convenient manner.

10.18 End-user remote access

nVision 11.6 introduced the possibility of configuring remote user access to his computer. To configure this mechanism, follow the procedure described in this chapter.

1. On the edge router of the corporate network (with a public IP address), you should configure the redirection of incoming connections on the TCP port 4436 to the nVision server address in the local network (port-forwarding).
2. In the nVision console, enable "Additional remote access to own computer" in the "Permissions \ HelpDesk" tab in the user information window:



3. Indicate the computer to which the user can connect in the "Permissions \ HelpDesk" tab.

4. If the user, on the company computer with the Agent, works under a local Windows account, set the nVision account password in the "General" tab in the user information window:

- The value of the "User" field is the login for the remote connection.
- In the case of domain accounts, the user will establish a connection using his domain credentials, e.g. name@domain.local + domain password

User-side actions:

When running the nVision installer, select "Install only Axence nVision remote user access" next to the installation components selection step:

After starting, please provide your login details:

- **Address and Port:** Public IP address of the corporate router that has been configured with port forwarding
 - **Login:** user account name in Axence nVision console
 - **Password:** user account password in Axence nVision console
- After remote access is established, you must enter your computer logon credentials.

Part

XI

11 SmartTime module

11.1 Introduction

11.1.1 General information

SmartTime is a module that has been introduced in nVision 11. It allows users to view their activity in applications and superiors to verify the activities of their subordinates. The SmartTime module uses the nVision Agent to collect data on user activity in applications and displays them in a user-friendly manner in the web browser window.

The main features of the module are:

- View of activity data for employees and teams,
- Detailed list of visited web pages and used applications,
- Reports for managers - information about users who have not reached the preset productivity values,
- List of company employees' contacts.

Requirements for the collection of user activity

In order to collect user activity information, you **have to install the nVision Agent** on the remote device and open the TCP 4436 port on the computer running nVision. For more information, see the chapter Requirements and configuration.

Please note, that all the communication between Agents and nVision requires authorization and no data may be communicated if the Agents and nVision are properly configured.

11.1.2 Trial version

SmartTime is available in the trial version.

If the license covers the **Users** module, the **SmartTime** module will be activated automatically after downloading the nVision upgrade to version 11.

In the absence of the **Users** module, **SmartTime** will need to be activated manually in the nVision console by the administrator. When activating the module, the administrator will be asked for consent to enable the collection of user activity data.

When activating the **SmartTime** module **after 1 November 2019**, the test period will be available for **30 days**.

After the activation of the trial license of SmartTime, a notification bar with the remaining time will be displayed in nVision.

11.1.3 Getting started

After the SmartTime module is activated in nVision, the administrator should take a few steps to ensure the desired and efficient operation of the system.

Listed below are the first steps to be carried out (in nVision):

- Review the current hierarchy of users and assign the relevant superiors/supervisors/managers, if required ([Hierarchy and superiors](#)^[500]),
- Assign access rights to the module for users ([User roles](#)^[499]),
- Define the user groups and designate group managers to have access to the activity data for the members of their groups ([Groups and managers](#)^[500]),
- If necessary, import data from nVision – if you want to have access to historical data in SmartTime ([Importing data from nVision](#)^[495]).

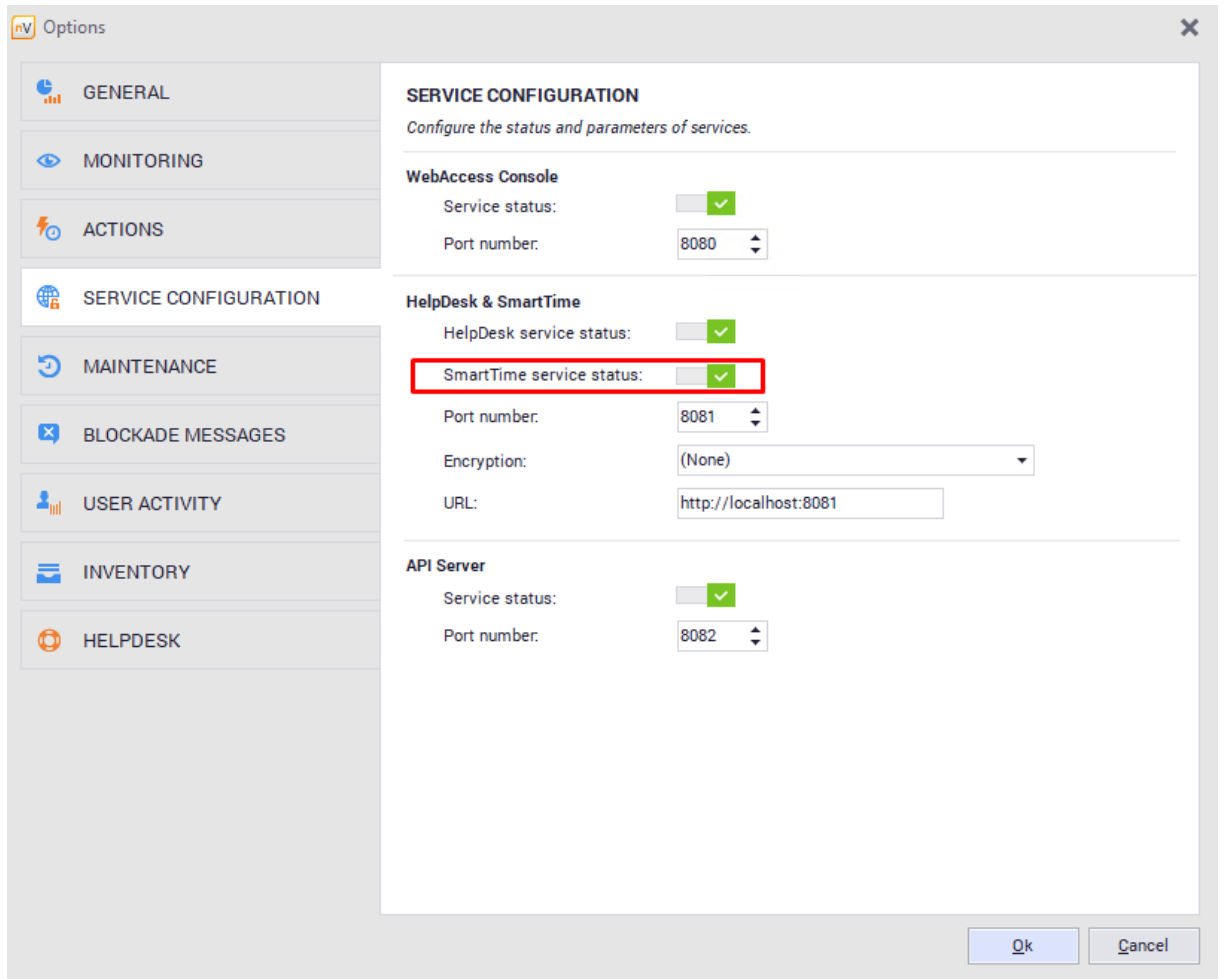
11.2 Module configuration

11.2.1 Installation

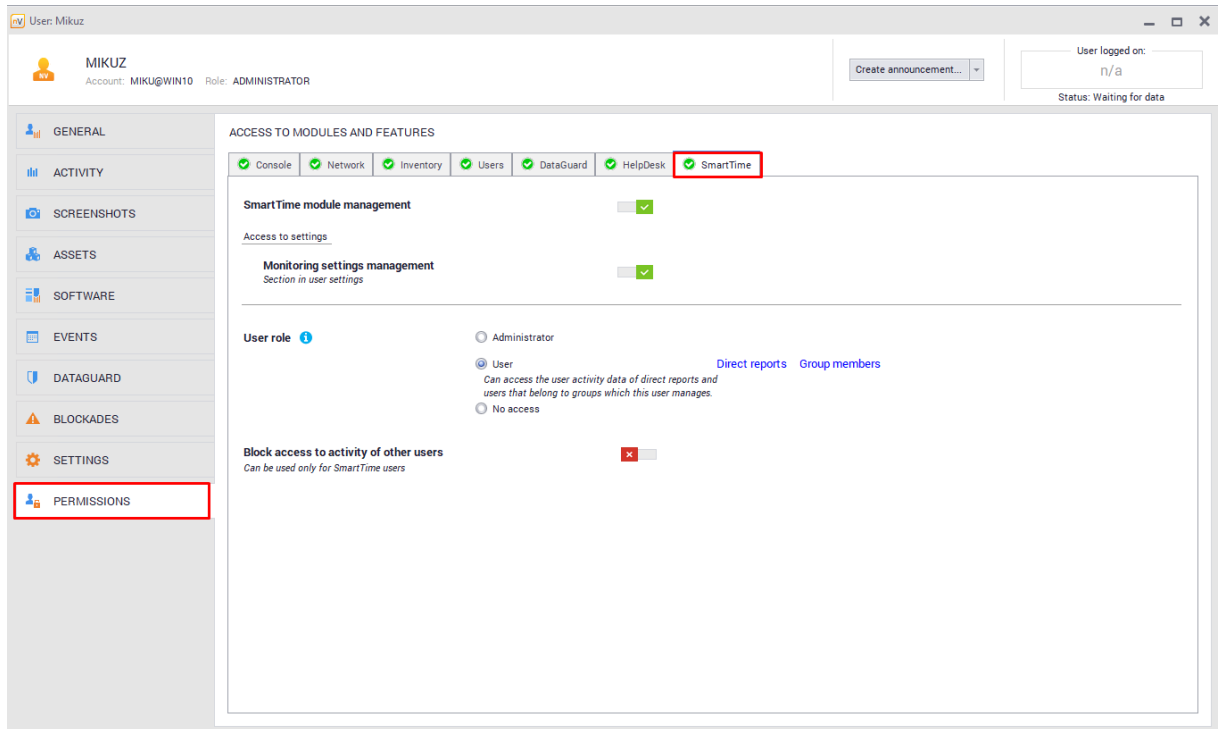
The SmartTime module is available from version 11 of Axence nVision. In order to collect user activity information, you **have to install the nVision Agent** on the remote device.

Access to the SmartTime module can be modified by the administrator at any time.

By going to the main options of the nVision program and then to the **Service configuration** tab, you can enable or disable the SmartTime module:



By default, the SmartTime module is automatically enabled after upgrading the software. Users also have access to the module and their data. To disable access to the data or module, select users on the list, select **Properties** in the context menu, and then navigate to the **Permissions / SmartTime** tab and modify the appropriate item:



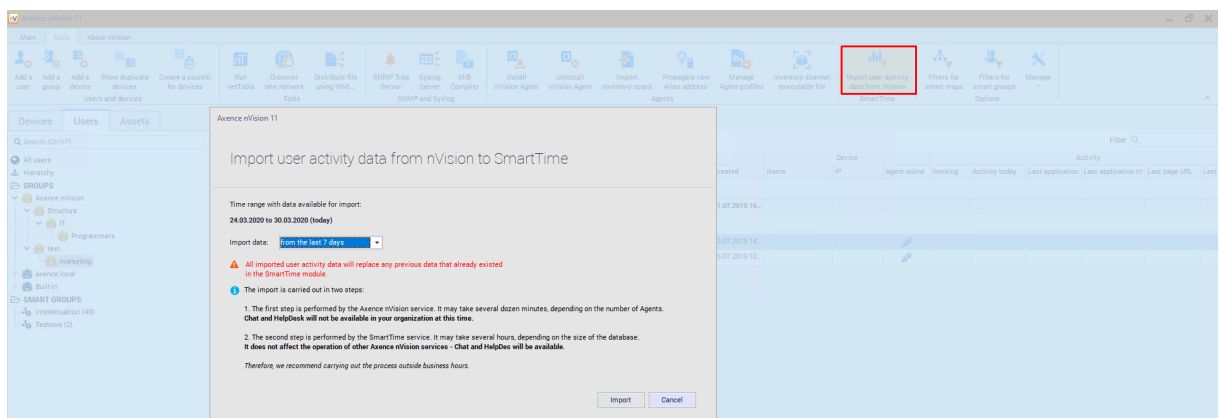
11.2.2 Importing and deleting data

Data collected by the SmartTime module are subject to full control by the administrator. They are sent and added every 20 minutes and upon disabling the system on which the agent is installed.

If the Users module was previously used, you can import the user activity data to the SmartTime module.

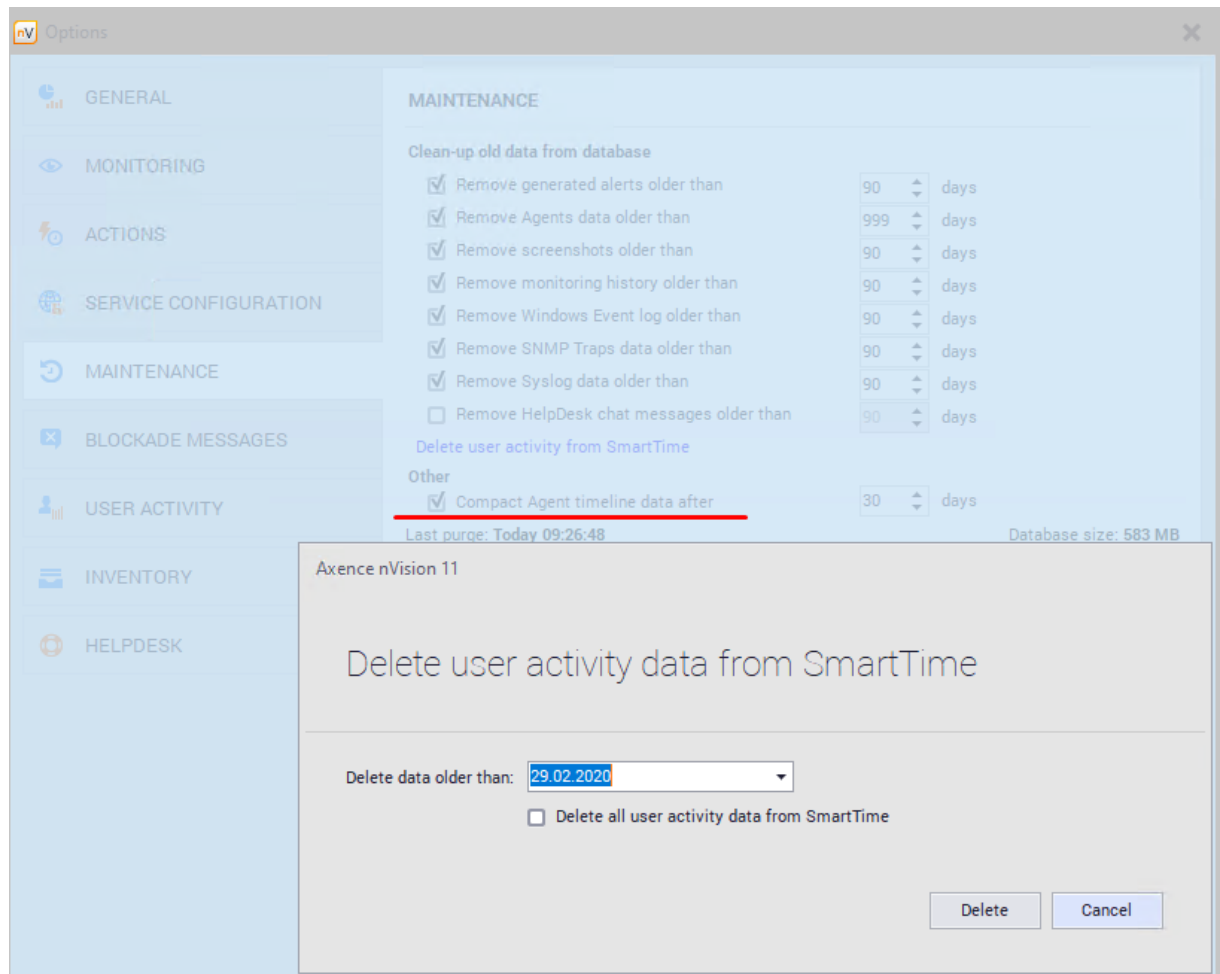
To do this, navigate to the **Tools** tab and select **Import activity data from nVision** in the SmartTime section.

The program will require you to specify the time from which the activity data are to be imported:



Note! All imported user activity data will replace the data collected by SmartTime over the selected period.

To delete the activity data collected in the SmartTime module, navigate to the main options of nVision and then to the **Maintenance** tab:



11.2.3 Starting SmartTime

You can access the SmartTime module in a few ways.

1. Access with the Agent icon

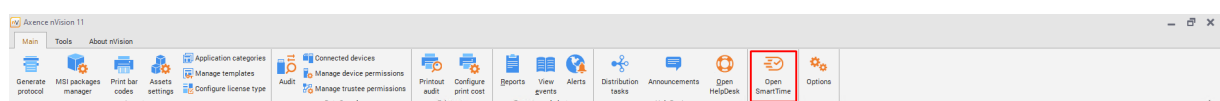
When you click the Agent icon, you can select **Your activity**. This will open the browser and start the SmartTime module.

2. Access from the HelpDesk module

To open the SmartTime module, click the appropriate icon at the top of the HelpDesk screen.

3. Access from the nVision console

To start SmartTime from the console, simply click **Open SmartTime** on the main toolbar:



11.2.4 Productivity levels

Applications in the SmartTime module are grouped into the following three main **productivity levels**:

- **Productive applications,**
- **Neutral applications,**
- **Unproductive applications.**

For defining the productivity of applications, refer to chapter [Applications](#)^[511].

Defining the productivity of applications does **not** apply to its category – these are two independent settings.

11.2.5 Setting the productivity and category

When in the **Settings** tab in the web interface, you can configure the SmartTime module.

The configuration in the **Productivity** tab allows you to define the following parameters:

- **Productivity threshold (%)** – the required daily productivity threshold. If specific employees do not reach the productivity threshold on a given day, as configured in this field, they will be added to the report that can be sent to their superiors. This option is set to 40% by default.
- **Unproductivity limit** (in minutes) – specifies the allowed time spent by users on unproductive applications. If employees exceed the time spent on unproductive applications on a given day, as configured in this field, they will be added to the report that can be sent to their superior. Such users will also be highlighted in the application. This option is set to 60 minutes by default.
- **Send the daily alarm** – specifies whether or not the daily alarm is to be sent to the superiors or managers. The alarm will be sent to each user. The email will include information about the employees who have not reached the required efficiency threshold or exceeded the allowed unproductive time on the previous day. Sending alarms is enabled by default.

The email is sent on the next day at 7 a.m.

- **Delete older than x days** – specifies the period for which the employee productivity data are stored. Clearing takes place once a day at midnight. This function is enabled and set to 365 days by default.

Each of the above-mentioned options may be **enabled** or **disabled**. To enable or disable a specific option, use the toggle next to each of the items.

The screenshot shows the 'Settings' page in the SmartTime application, with the 'Productivity' tab selected. The page features a blue sidebar on the left with navigation options: Activity, Applications, Group, Contacts, and Settings. The main content area is titled 'Settings' and contains four configuration items, each with a toggle switch on the right:

- Productivity threshold:** Set to 40%. Description: Daily productivity threshold required. If the employee does not reach the threshold value on a given day, they will be listed in the daily alarm.
- Unproductivity limit:** Set to 60 min. Description: Acceptable daily unproductive time. When an employee exceeds it, they will be listed in the daily alarm and highlighted in the application.
- Send the daily alarm:** Description: Superiors will receive an email at 7:00. The e-mail will contain information about employees who did not reach the required efficiency threshold or exceeded the unproductive time allowed on the previous day.
- Deleting data older than:** Set to 365 days. Description: After this period, employee productivity data will be deleted. Deleting data takes place once a day after midnight.

At the bottom of the page, there are links for 'Help', 'FAQ', and 'Privacy policy', along with the language 'English' and copyright information 'Copyright © 2020 Axence sp. z o. o. sp. k'.

The **Categories** tab allows you to define the categories to which the applications can be allocated.

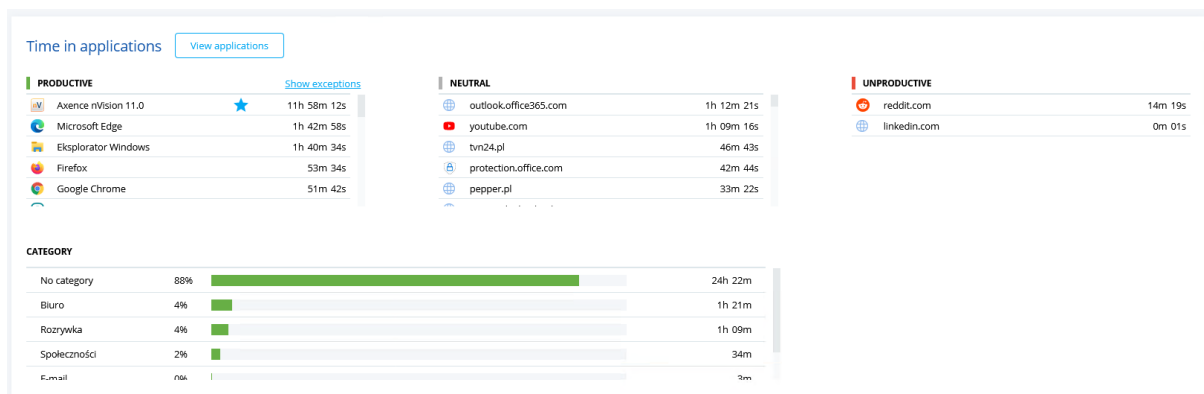
The screenshot shows the 'Settings' page in the SmartTime application, with the 'Category' tab selected. The page features a blue sidebar on the left with navigation options: Activity, Applications, Group, Contacts, and Settings. The main content area is titled 'Settings' and contains a list of categories to which applications can be assigned. At the top of the list is a blue button labeled 'Add a category'. Below it, the following categories are listed:

- Produkcja
- E-mail
- Spolecznosci
- Biuro
- Newsy
- Rozrywka
- Grafika
- Marketing

At the bottom of the page, there are links for 'Help', 'FAQ', and 'Privacy policy', along with the language 'English' and copyright information 'Copyright © 2020 Axence sp. z o. o. sp. k'.

To add a category, click **Add category**. Then enter the category name and confirm your selection.

For adding applications to categories, refer to chapter [Applications](#)⁵¹¹. By creating categories, you have the ability of the additional grouping of applications:



To change a name or delete a category, move the cursor over the selected category and select the appropriate icon.

Note! After the item is removed from the list, all applications assigned to this category will no longer have an assigned category.

11.3 Users and their permissions

11.3.1 User roles

Users may access the SmartTime module by using one of the following roles:

Administrator:

- This option is **only** available to the user that has access to the management of users and the modification of the Users module functionalities,
- The Administrator in the SmartTime module has access to the modification of settings for this module on the website,
- The Administrator has access to the activity data for all users.

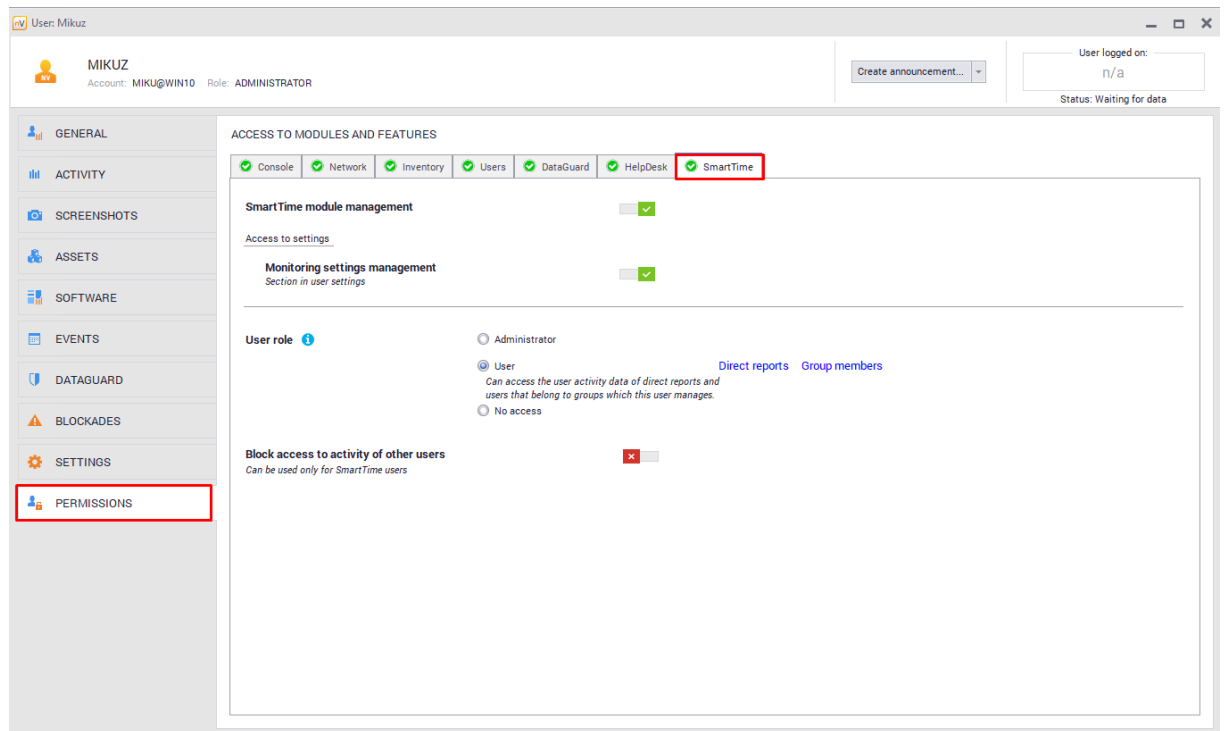
User:

- Users have access to the SmartTime module and can view data on their activity,
- If users are **group managers** and **have access to data enabled**, they can view the activity data for the group members (see the next section for more information),
- If users are superiors, they have access to their subordinate's activity data.

No access:

- People with this level of rights are not able to log in to SmartTime,
- They cannot see the navigation buttons in any part of the program,
- They are still shown in the list of SmartTime users – the activity data for these people can be viewed by their superiors and by the administrator.

These settings are located in **User information / Permissions / SmartTime**:



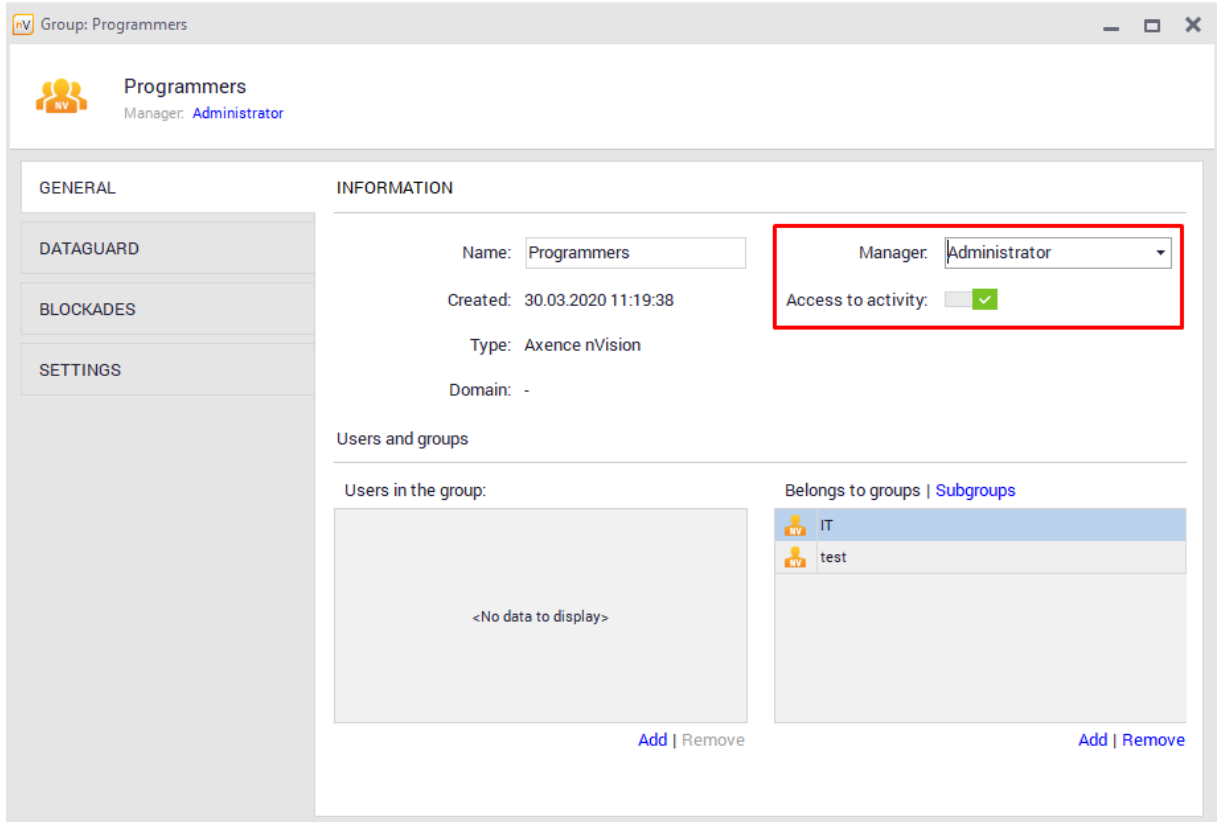
11.3.2 Managers and superiors

Group manager

The manager is a person that may have access to the activity data for all members of their groups. These persons may or may not be members of the groups managed by them.

To assign the group manager rights to a user, navigate to the **Group information** screen and select the appropriate person from the drop-down list in the **Manager** field.

By default, access to the activity data of other group members is **disabled** and the manager **does not have access to them**. To enable access to the data, click the toggle shown in the screenshot below:



The screenshot displays the 'Programmers' group configuration in the nVision console. The 'GENERAL' tab is active, showing the group name 'Programmers' and its manager 'Administrator'. The 'INFORMATION' section provides details: Name: Programmers, Created: 30.03.2020 11:19:38, Type: Axence nVision, and Domain: -. The 'Access to activity' checkbox is checked. The 'Users and groups' section is divided into 'Users in the group' (currently empty) and 'Belongs to groups | Subgroups' (listing 'IT' and 'test').

To check whether a user is a manager of any group, go to the **User information** screen for this user. The information will be displayed in the **Accounts and groups** section after clicking the appropriate option.

Note! When importing groups with assigned managers from Active Directory, it is not possible to modify this person in the nVision console (synchronized with the corresponding “managed to” field in Active Directory). Any changes should be made in the Active Directory.

Superiors and subordinates

These settings are related to the hierarchy of users in nVision. This functionality allows the administrator to define the relationships among employees. The **supervisor** field is assigned to each user, and it may be left blank or contain the user name. For users synchronized with Active Directory, the value in this field is a read-only value, and it is read from the field with the same name.

The screenshot displays the Axence nVision 11 user management interface. The 'Users' tab is selected, and the 'Hierarchy' view is active. A red box highlights the 'Administrator' group containing the user 'Mikuz'. Below, the 'User: Mikuz' profile is shown with details like 'Role: ADMINISTRATOR', 'Account: MIKU@WIN10', and 'Supervisor: Administrator' (highlighted with a red box).

To manage the hierarchy of users, select **Hierarchy** in the **Users** tab. In this list, you can drag and drop the users to define subordinates and superiors for them.

Alternatively, in order to define a superior for a specific user, navigate to the **User information** screen for this user and select the superior for the person from the drop-down list in the **Accounts and groups** section.

In the SmartTime module, the **superiors** will be able to verify the activity of **their subordinates**, even if **access to the activity data in the group is disabled**.

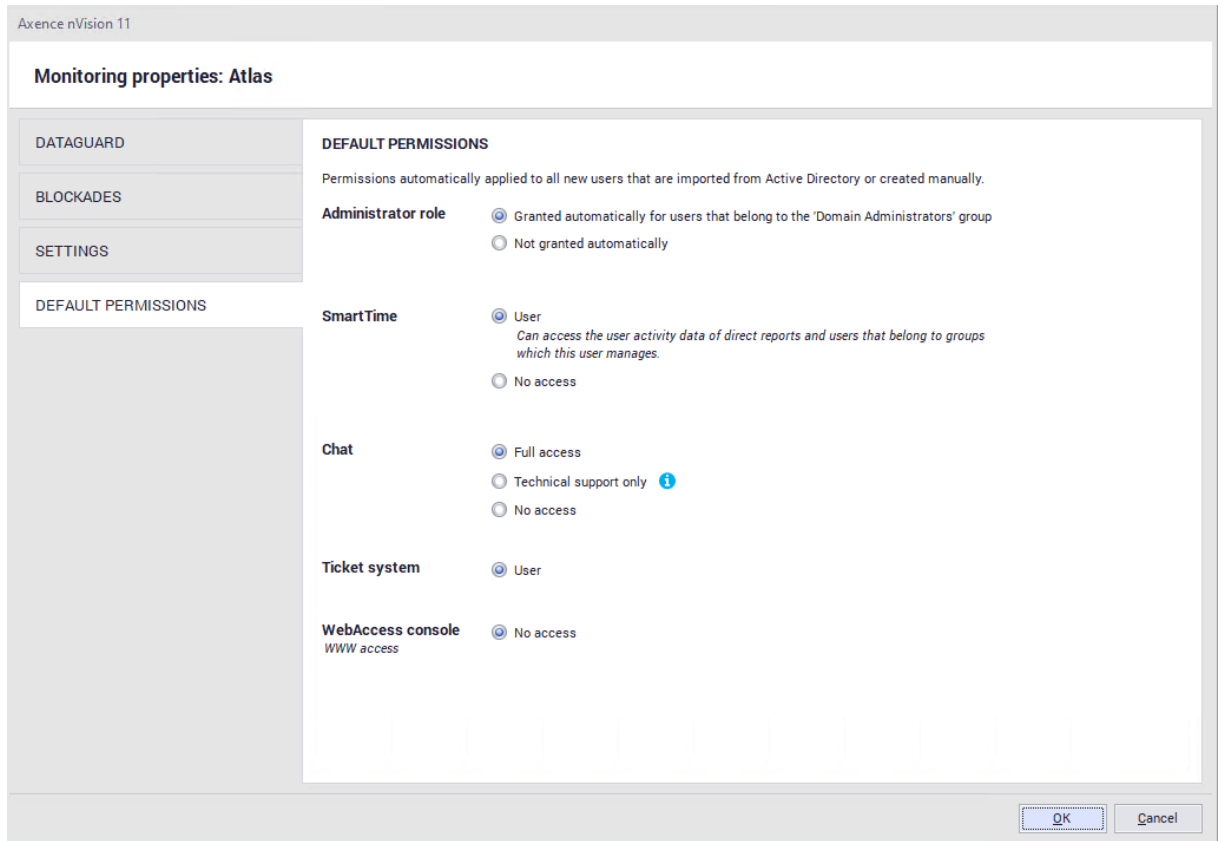
11.3.3 Blocking access to data

One of the user permissions setting items is to **Block access to specific activities**. By enabling this setting, the users (regardless of whether they are managers or superiors) will see only **their own data**.

These settings are located in **User information / Permissions / SmartTime**:

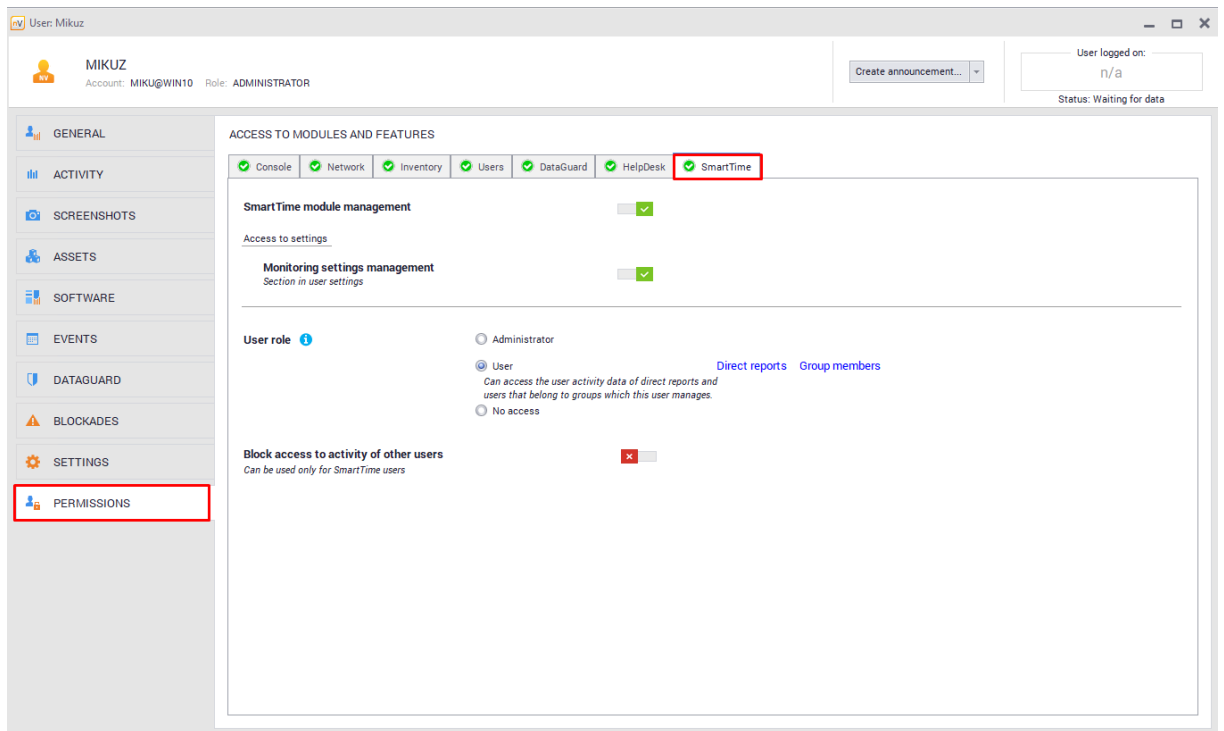
The screenshot shows a web application interface for user management. The user is logged in as MIKUZ (Account: MIKU@WIN10, Role: ADMINISTRATOR). The interface is divided into a left sidebar with navigation options (GENERAL, ACTIVITY, SCREENSHOTS, ASSETS, SOFTWARE, EVENTS, DATAGUARD, BLOCKADES, SETTINGS, and PERMISSIONS) and a main content area. The 'PERMISSIONS' tab is selected and highlighted with a red box. The main content area displays the 'ACCESS TO MODULES AND FEATURES' section, where 'SmartTime' is checked. Below this, there are three main sections: 'SmartTime module management' (checked), 'Monitoring settings management' (checked), and 'User role' (set to 'User'). The 'User role' section includes a description: 'Can access the user activity data of direct reports and users that belong to groups which this user manages.' There are also links for 'Direct reports' and 'Group members'. At the bottom, the 'Block access to activity of other users' setting is shown as unchecked (disabled).

By default, the newly added users will receive user access. To modify the default settings, go to the **Atlas information / Default permissions** and modify options in the **SmartTime** line:



11.3.4 Data available to users

Depending on the level of rights of the logged in person, the items related to the activity visible for that user will be displayed. These settings can be modified in **nVision** by going to the **User information**, and then to the **Permissions / SmartTime** tab:



The access rights are as follows:

- **User with no subordinates**

A person with the **user** role and no subordinates will only have access to their own activity data.

- **User with subordinates**

A person with the **user** role and subordinates will have access to the activity data for each subordinate (also each person that is lower than their subordinates in the hierarchy) and to their own activity.

- **User that is a group manager and has access to data of this group disabled**

A person with these rights has access to their data. If they have any subordinates, their activity will be displayed too.

- **User that is a group manager and has access to data of this group enabled**

A person with these rights has access to their own data as well as the data of the entire group and the individual members. Such users can also edit the group productivity exceptions. If they edit productivity exceptions for such a group, they see the global list of applications, their productivities and categories, however they cannot edit these items.

- **Administrator**

A person with the administrator rights has access to the activity data for each user and each group. The administrator has full access to all parts of the system, sees the global list of applications and can edit their productivities and categories. The administrator can also edit the productivity exceptions for all groups.

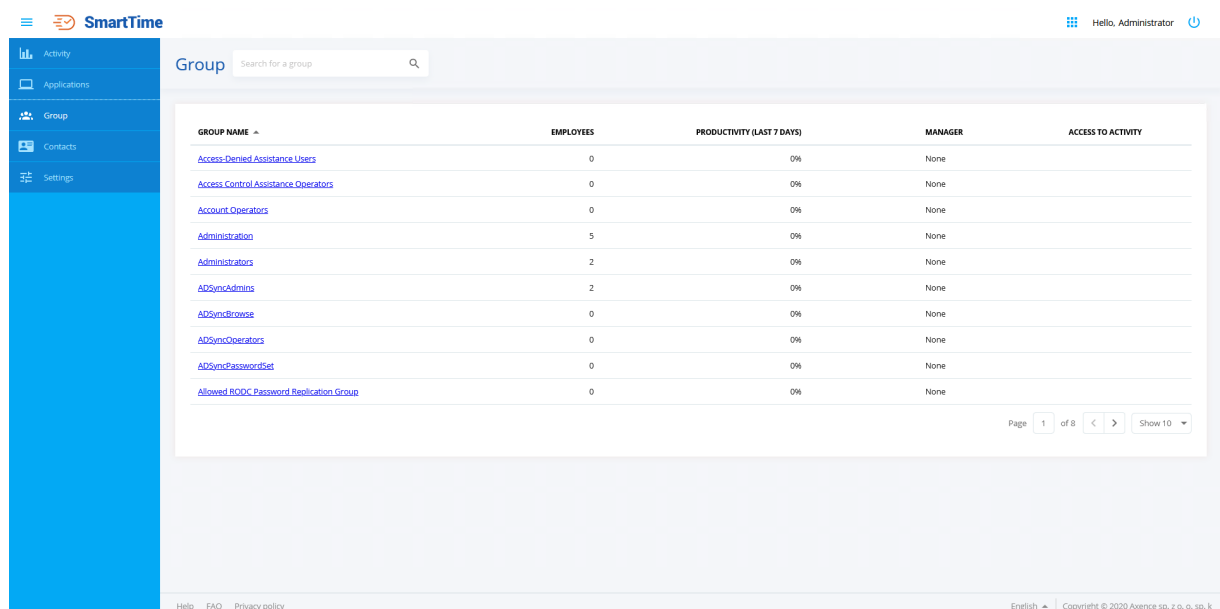
By going to the **User information** and then to the **Permissions / SmartTime** tab, you can enable **blocking access to the activity of other users**. A person with the lock enabled will only have access to their own activity data.

11.4 Groups

11.4.1 Group information

After selecting an item from the list of groups, you can go to **detailed** information. The following tabs are available there:

- Employees – a list of employees belonging to the group or subgroup (see the “relationship within the group” column),
- Belongs to – information about the parent group that the currently viewed group belongs to (this item is not displayed if the selected group does not belong to any other group),
- Subgroups – information about the subgroups of the currently viewed group,
- Application exceptions – provides information on whether or not any exceptions are defined for this group. The list of exceptions only includes **the applications in which the members of the selected group were active**. This tab also allows you to add exceptions for these applications.

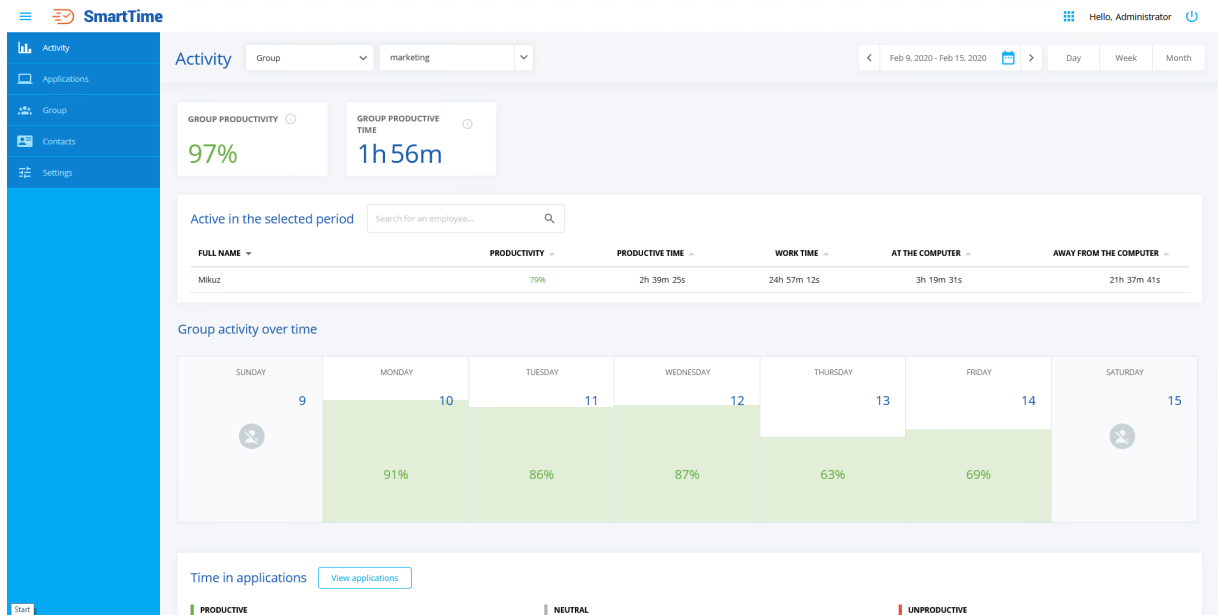


The screenshot shows the SmartTime application interface. The top navigation bar includes the SmartTime logo and a user profile for 'Hello, Administrator'. The left sidebar contains navigation options: Activity, Applications, Group (selected), Contacts, and Settings. The main content area is titled 'Group' and features a search bar. Below the search bar is a table with the following columns: GROUP NAME, EMPLOYEES, PRODUCTIVITY (LAST 7 DAYS), MANAGER, and ACCESS TO ACTIVITY. The table lists several groups, including 'Access-Denied Assistance Users', 'Access Control Assistance Operators', 'Account Operators', 'Administration', 'Administrators', 'ADSyncAdmins', 'ADSyncBrowse', 'ADSyncOperators', 'ADSyncPasswordRet', and 'Allowed RODC Password Delegation Group'. At the bottom of the table, there is a pagination control showing 'Page 1 of 8' and a 'Show 10' dropdown.

| GROUP NAME | EMPLOYEES | PRODUCTIVITY (LAST 7 DAYS) | MANAGER | ACCESS TO ACTIVITY |
|--|-----------|----------------------------|---------|--------------------|
| Access-Denied Assistance Users | 0 | 0% | None | |
| Access Control Assistance Operators | 0 | 0% | None | |
| Account Operators | 0 | 0% | None | |
| Administration | 5 | 0% | None | |
| Administrators | 2 | 0% | None | |
| ADSyncAdmins | 2 | 0% | None | |
| ADSyncBrowse | 0 | 0% | None | |
| ADSyncOperators | 0 | 0% | None | |
| ADSyncPasswordRet | 0 | 0% | None | |
| Allowed RODC Password Delegation Group | 0 | 0% | None | |

After clicking the **View productivity** button, the application will take you to the [page](#)⁵¹⁸ where the information on the productivity of the group as a whole and of individual members is displayed.

The **View applications** button displays the application settings for the selected group. The list will show **only the applications in which the members of the selected group were active**.



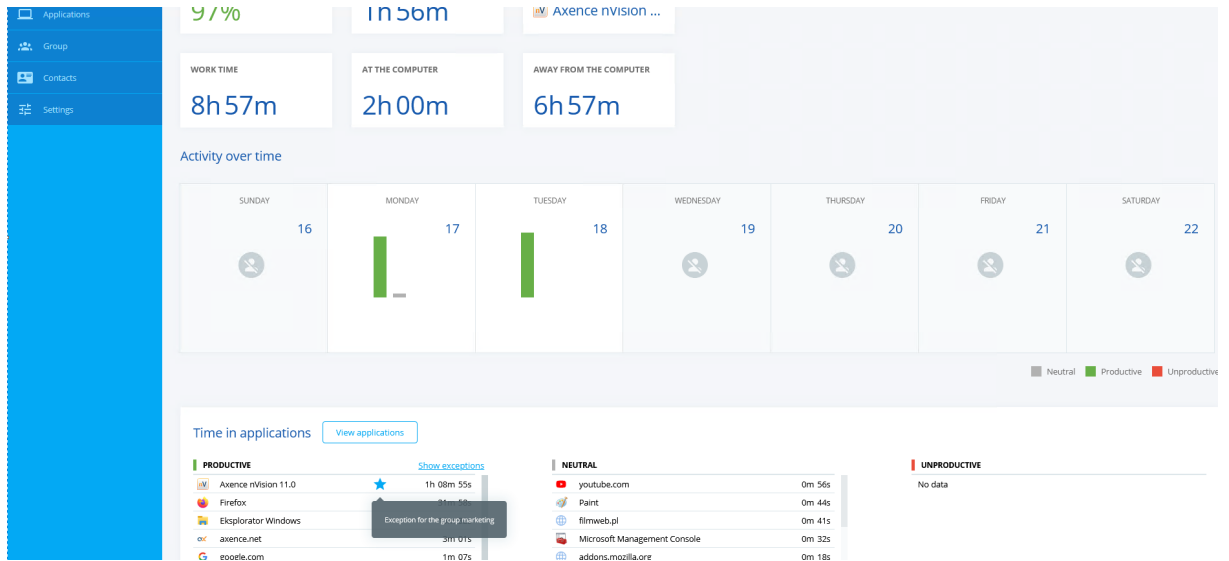
If the group manager does not have access to the data of this group enabled, the appropriate notification will be displayed (see the screenshot above).

11.4.2 Special markings

Special markings in the SmartTime module are used to allow for the better interpretation of activity data. These include:

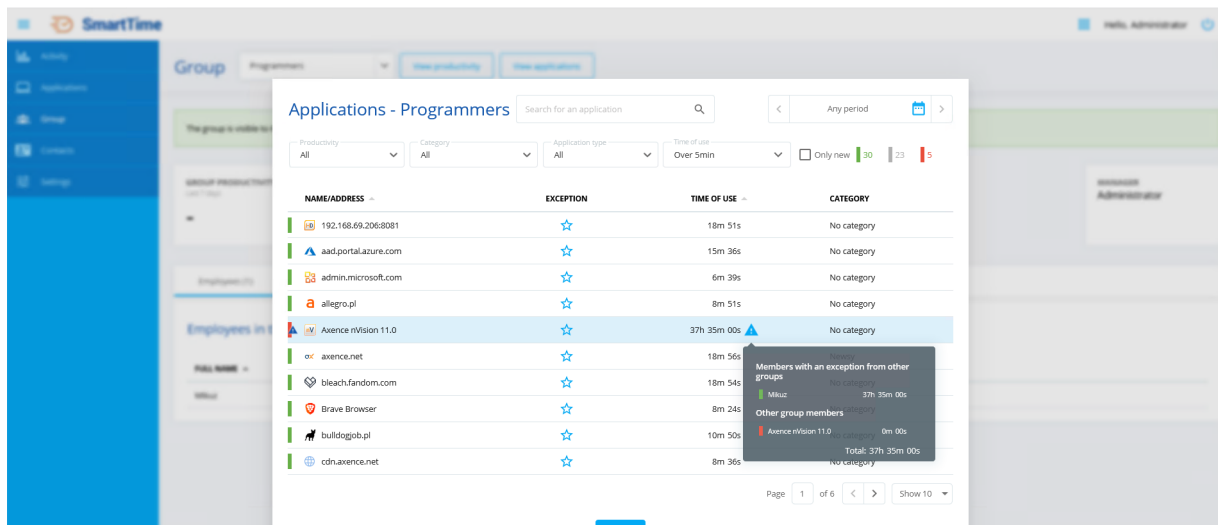
- **Asterisk**

An asterisk will be displayed on the user activity screen for the selected user if this user belongs to a group in which the application is added to exceptions:



Triangle

A triangle will be displayed on the group activity screen or after clicking the **View applications** button in the information screen for the selected group. The symbol appears when at least one of the group members has an exception for the selected application set in another group (which means that the user's time spent in this application is treated as productive). Move the cursor over the symbol to see additional information.



11.5 Application settings

11.5.1 General information

The **Applications** screen provides information concerning **all applications detected on all devices with the Agent** within the network. An application can be both a **program** run on a computer and a **web site** visited by the user. Only the **applications that were used** by users are displayed. If any program has a desktop (e.g. winword.exe) and web (Word online – www.office.com) version, it is always treated as two different applications.

Data collected by the SmartTime module are subject to full control by the administrator. They are sent and added every 20 minutes and upon disabling the system on which the Agent is installed.

Applications in the SmartTime module are grouped by the following three main **productivity levels**:

- **Productive applications,**
- **Neutral applications,**
- **Unproductive applications.**

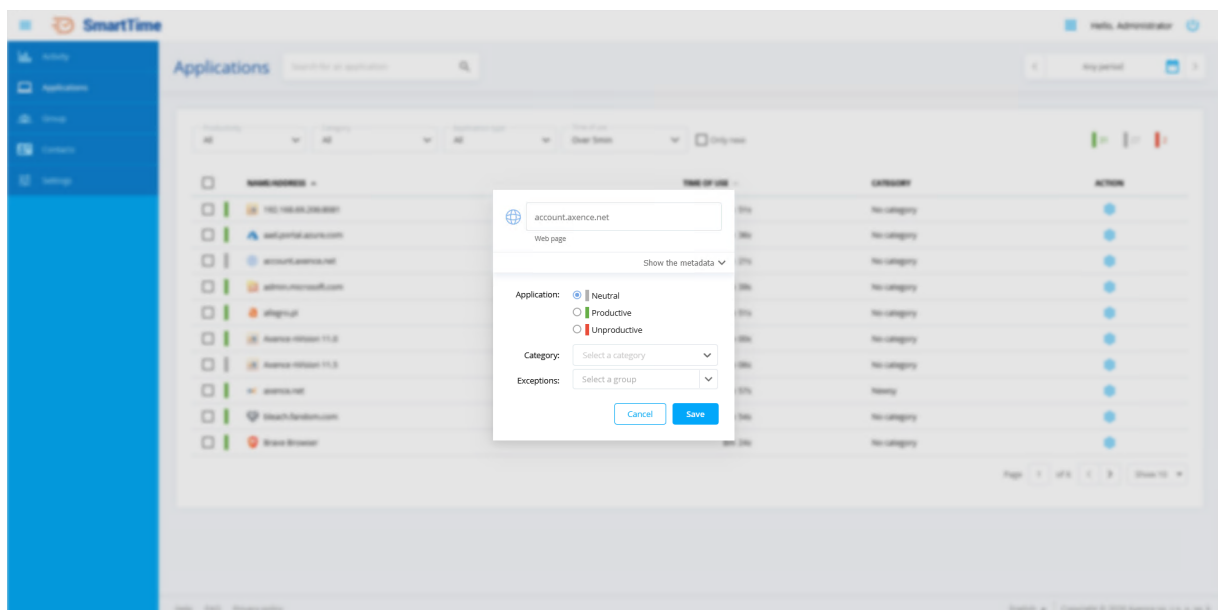
The above-mentioned productivity levels cannot be added, edited or deleted.

To make it easier to review the list of applications, the following filters have been developed:

- Calendar – allows the selection of the time period in which the applications were detected,
- Productivity – allows the application productivity to be defined,
- Category – allows the application category to be defined,
- Application type – allows the search to be narrowed down to **desktop applications** or **web pages** only,
- Usage time – specifies the time of application usage,
- New only – the applications that appeared in the system in the given time period are displayed.

The SmartTime module has a database of the most popular applications and is able to classify them as productive or unproductive. If an application not included in the database is detected, it is classified as neutral.

In order for the SmartTime module to utilize its full potential, the administrator should **regularly update** the list of applications in the system. To facilitate this, the **New only** option is available to show the new applications that appeared in the system **in the selected time period**.



11.5.2 Application identification

Applications in the SmartTime module are divided into two types:

- Windows programs;
- websites.

The SmartTime module treats Windows programs and websites as equal applications in terms of user activity. If any program has a desktop (e.g. winword.exe) and web (www.office.com) version, it is always treated as two different applications.

Windows applications

Each “Windows program” application has the following properties:

- Application detection date (date of the first time quantum of an activity connected with this application),
- Application name (friendly name displayed as the application title in the interface),
- File name (OriginalFileName),
- Product name (ProductName),
- Supplier name (Company).

The unique determinant of such an application is the combination of the OriginalFileName, ProductName and Company fields. This means that two programs with the same name of the executable file may be detected as two applications (if they differ, for example, in the “Company” field).

Websites

Each “website” application has the following properties:

- Date of application detection (date of the first activity connected with this application),
- Application name (friendly name displayed as the application title in the interface),
- Address (DNS name without “www” and without port or the IP address itself),
- Website titles (set of text values).

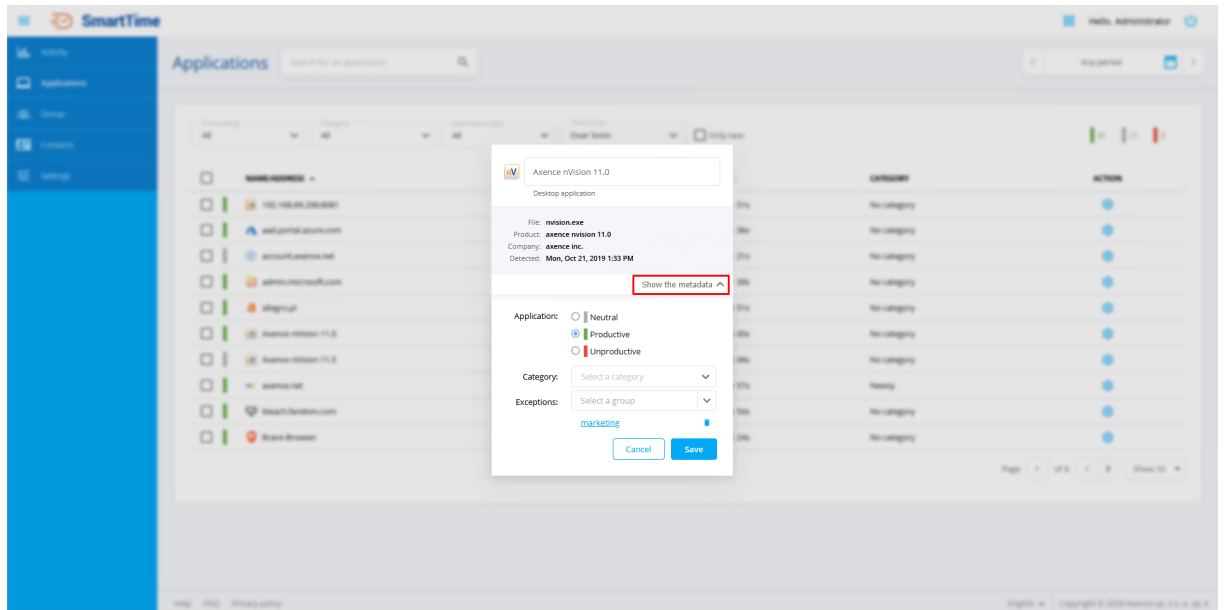
The unique determinant of such an application is the address only. This means that if any website uses different subdomains, each of them will be detected as a separate application. The information concerning protocol is automatically removed from the address.

Each user activity is matched to the application using the described unique determinant. If such an application does not yet exist in the system, a new one is automatically created.

The friendly application name is automatically retrieved from the executable file (for Windows programs) or from the most common site title (for websites).

Metadata

Metadata can be viewed by going to the **Applications** screen in the SmartTime module web interface. After clicking the gear icon next to the selected application, click **Show metadata**. The information concerning the application name, manufacturer and date of detection will be displayed:



11.5.3 Application settings

Individual application settings

To go to the application settings, click the appropriate icon in the **action** column next to the selected item from the list.

A few parameters can be set in the application settings screen:

- specification of application productivity (neutral, productive or unproductive),
- specification of application category (the categories previously created in the **Settings** screen are available – [click here for more information](#)⁴⁹⁷),
- specification of **exceptions** for the user groups,
- ability to change the application name in the list.

Exceptions

The productivity settings for specific applications are global settings. By specifying the **exception** for groups, you can classify unproductive applications as productive ones for selected groups.

Setting the exception for an unproductive or neutral application means that the time spent in this application by users belonging to a group with the exception set will be treated as productive.

To further explain the concept of exceptions, let's consider the following situation:

The **Facebook** application is marked globally as **unproductive** in the SmartTime system. The user **Jacek** is a member of the **Marketing** and **Production** groups. The administrator has added this application to exceptions in the **Marketing** group. The consequence of this action is the following events:

- The time spent on Facebook by the members of the **Marketing** group will be treated as productive when calculating their productivities,
- However, if Jacek spent some time on Facebook, this time will also be treated as **productive** in the **Productivity** screen of the **Production group** (and in his activity screen). By spending time on Facebook, the other members of the **Production** group that do not belong to the **Marketing** group will increase their time in **unproductive** applications. The information that Jacek's time spent on Facebook is treated as productive **will be highlighted accordingly** by the warning sign icon in the group productivity view.

Categories

The specification of categories for an application will allow for the better graphic representation of collected data in the **Activity** screen. Each category must have a unique name and each application can be assigned to **only one category**.

When installed, the SmartTime module will include the initial list of categories fed from the built-in predefined list. The initial categories are the special type of categories and the destination place where the automatically assigned applications will be saved. However, in the user interface, they do not differ at all from the categories created manually by the administrator.

Configuration of multiple applications at the same time

To facilitate the configuration of applications, the option for the bulk change of their settings is available. To do this, simply select the applications in the list by clicking the relevant box on the left side of the list. By clicking the box at the top, you can select all items displayed on this page.

After selecting the desired applications, the administrator may assign these items to a specific category and specify the productivity of these applications.

The screenshot displays the 'Applications' management page in the SmartTime system. The interface includes a sidebar with navigation options (Activity, Applications, Group, Contacts, Settings) and a top navigation bar with the user's name 'Hello, Administrator'. The main content area shows a table of applications with the following columns: NAME/ADDRESS, TIME OF USE, CATEGORY, and ACTION. A toolbar above the table provides bulk management options: 'Selected: 3', 'Move selected to' (dropdown set to 'Produkcja'), 'Move', 'Set productivity to' (dropdown set to 'Unproductive'), and 'Set'. Red arrows highlight these dropdown menus. The application list includes various domains and IP addresses, with their respective time of use and categories. For example, '192.168.69.206:8081' has a time of use of 18m 51s and is categorized as 'No category'. The 'Axence nVision' applications are also listed with their specific time of use and 'No category' status. The 'axence.net' application is categorized as 'Newsy'. The 'Brave Browser' application has a time of use of 8m 24s and is categorized as 'No category'. The footer of the page includes 'Help', 'FAQ', 'Privacy policy', 'English', and 'Copyright © 2020 Axence sp. z o. o. sp. k'.

11.6 Activity

The Activity screen provides information about the time spent in individual applications.

Depending on the level of rights of the logged in person, the items related to the activity visible for the logged in user will be displayed. This means that the page will look slightly different depending on who is viewing it.

By using the navigation at the top of the screen, the logged in persons may select their **users, groups or subordinates** and specify the time period they want to view the data from.

Once the item in the list is specified, you will see the statistics for the selected user. The subsections of this topic describe the individual views depending on the period and the person whose data are viewed.

11.6.1 Access to specific activities

Users may have access to their own activity data as well as the activity data of their subordinates or groups managed by them. Depending on the level of rights of the logged in person, the selected people whose activity is visible for that user will be displayed. This topic is described in detail in chapter [Data available to users](#)^[504].

11.6.2 Individual user activity

11.6.2.1 Activity on the selected day

The user productivity screen is divided into a few sections.

Statistics

The first element of the user productivity screen is the general information about their work on the computer:

- **Productivity** – the productivity is measured in the selected period. **This is the productive time in this period divided by the duration of the user's entire activity on the computer in this period.**
- **Productive time** – shows the amount of time spent by the user in applications classified as productive.
- **Most popular** – displays the name of the most popular application used by the user in the selected period.
- **Working time** – the system calculates the working time for each employee as the difference between the time of the first and last activity on each day.
- **On the computer** – this is the time during which the system detected user activity.
- **Away from the computer** – this is the time during which the system did not detect user activity.

Screenshot

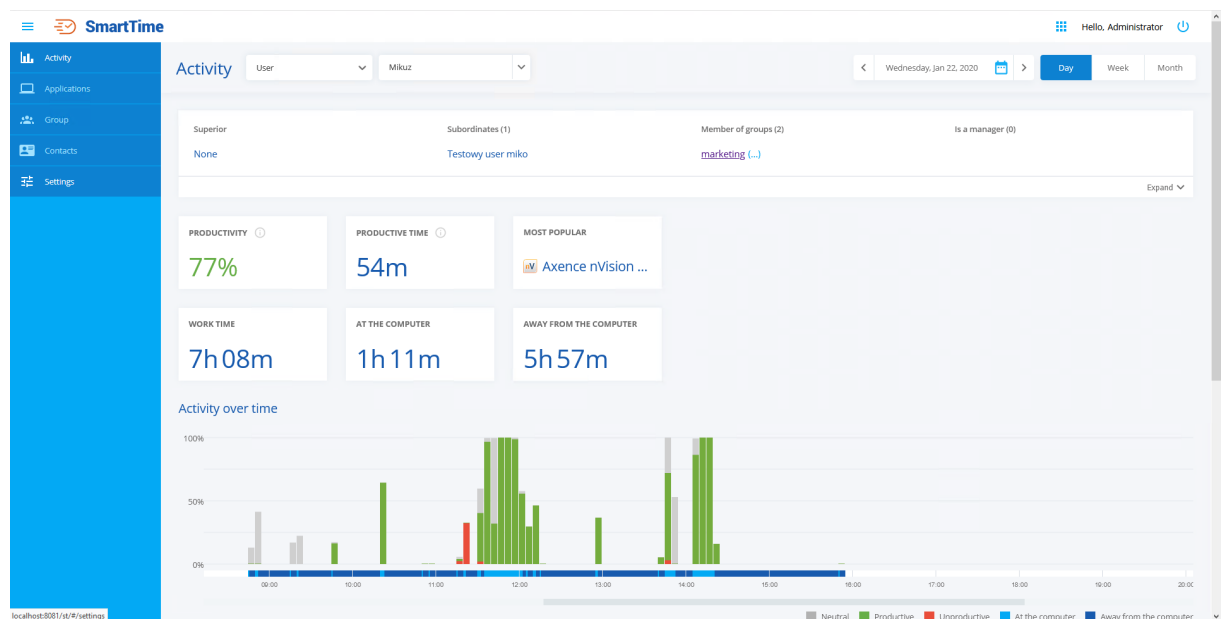
The screenshot makes it possible to view the user's screen snapshot. This allows the superior of this employee to get approximate information about what the user is doing at that moment. It is not possible to zoom in or see the screenshot in more detail. The aim is to provide a certain privacy for the user.

Activity over Time

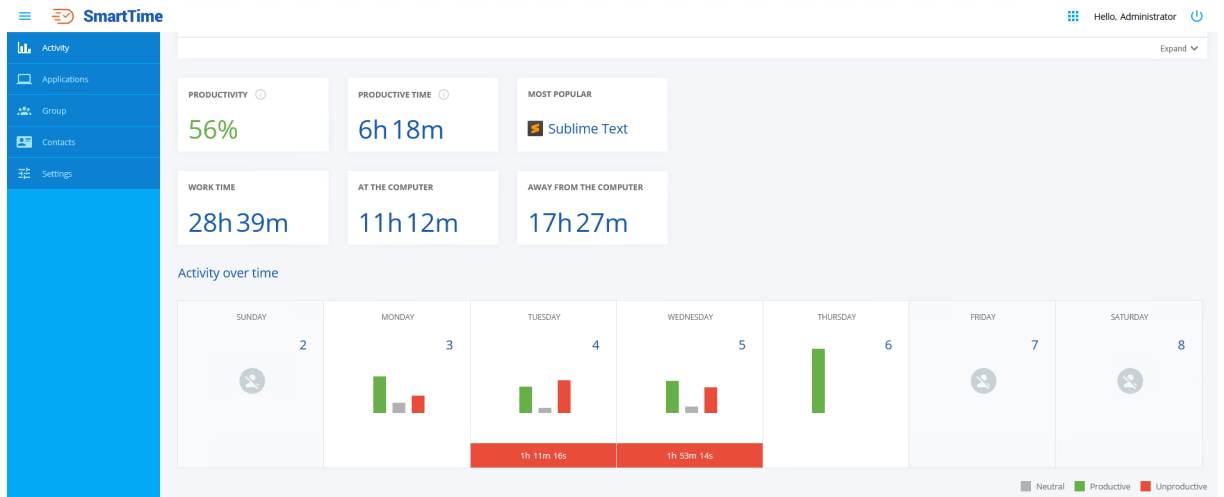
The next area of the productivity screen is Activity over Time. **This area looks different depending on the selected time period (day, week, month, period).**

The daily data are presented on a timeline. Information on used applications is presented as bars representing 5-minute intervals. The chart is described in detail in chapter [Activity over Time chart](#)⁵¹⁵.

The screenshot below shows the view of activities within a single day:



When the user exceeds the time spent in unproductive applications as defined in the configuration section on a given day, that day will be highlighted. The time displayed on a highlighted background is the user's inactivity time on that date:



Time spent in applications

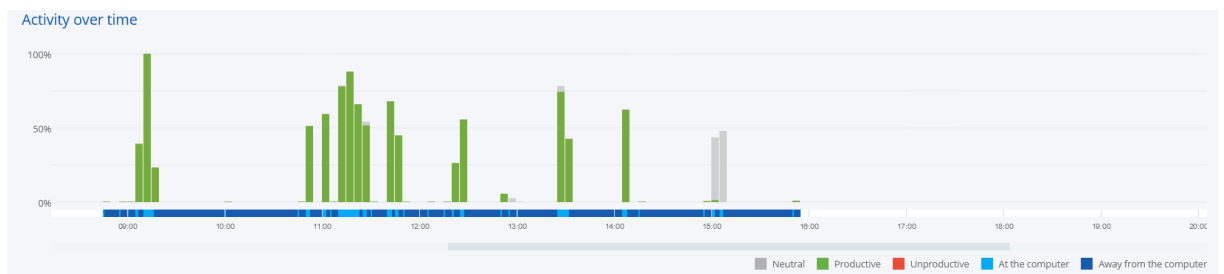
This part shows the time spent in applications by the user. This area of the SmartTime module is divided into three sections: productive, neutral and unproductive applications. The available information is shown as a list. The applications marked with an asterisk indicate that an exception has been applied to the application.

The **Show exceptions** option displays the applications for which the user group exceptions have been set. For more information about exceptions, refer to chapter [Applications](#) ⁵⁰⁸.

The **category** charts show the usage of the applications belonging to the individual categories. Information about the most and least common category applications can be found here.

11.6.2.2 Activity over time chart

The daily user data are presented on the Activity over Time chart. Information about the used applications is presented as **bars representing 5-minute intervals**. The chart allows you to carefully analyze the used applications:



The lower part of the chart shows the user activity time on a given day. In the above chart, the first activity on the selected day was recorded at around 9:00, while the last one at approximately 16:40. The slider can be used to move through the timeline.

On the left side of the chart, there is a percentage scale. It is provided to help visualize the application usage by the user in individual time quanta.

Below the activity chart, there is a legend which indicates the meaning of the colors used in the chart.

The first three items (Neutral, Productive, Unproductive) describe the colors of the bars visible in the chart.

The other two items (On the computer and Away from the computer) refer to the timeline. The colors applied to the timeline indicate when the user was working on the computer and when no activity was recorded at the workstation.

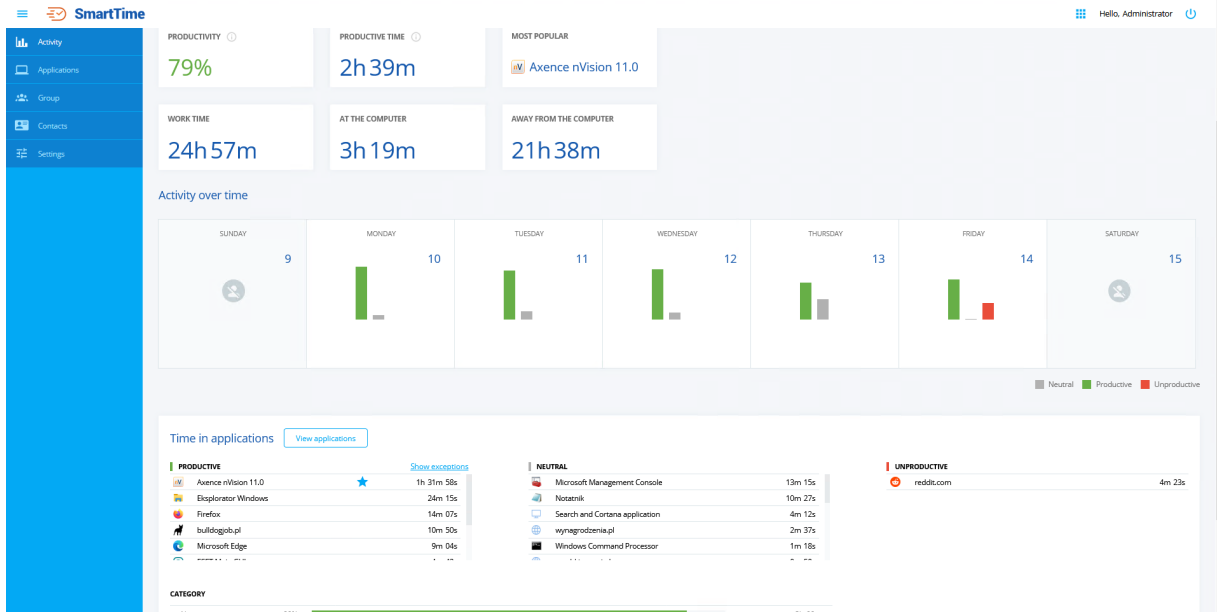
11.6.2.3 Activity in the selected period

When viewing the activity data for an individual user, the Activity over Time section **will look different depending on the selected time period (day, week, month, period)**.

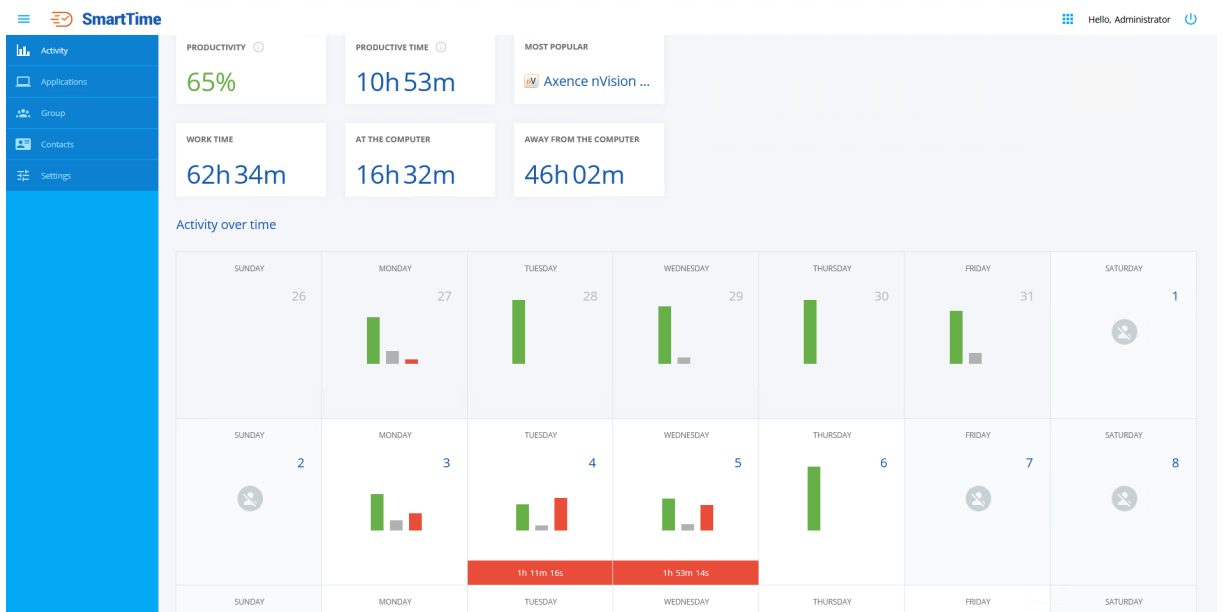
The daily data are presented on a timeline and were described in the previous chapter.

The **weekly and monthly** data are presented as a grid. It shows a summary of information about user productivity at the turn of the selected week or month. These are charts showing the percentage of usage of applications with specific productivity. The time displayed under the bars is the user's productivity time on a given day. By moving the cursor over the selected item, more accurate data is displayed. After clicking the selected day, a page containing information concerning that day only will appear.

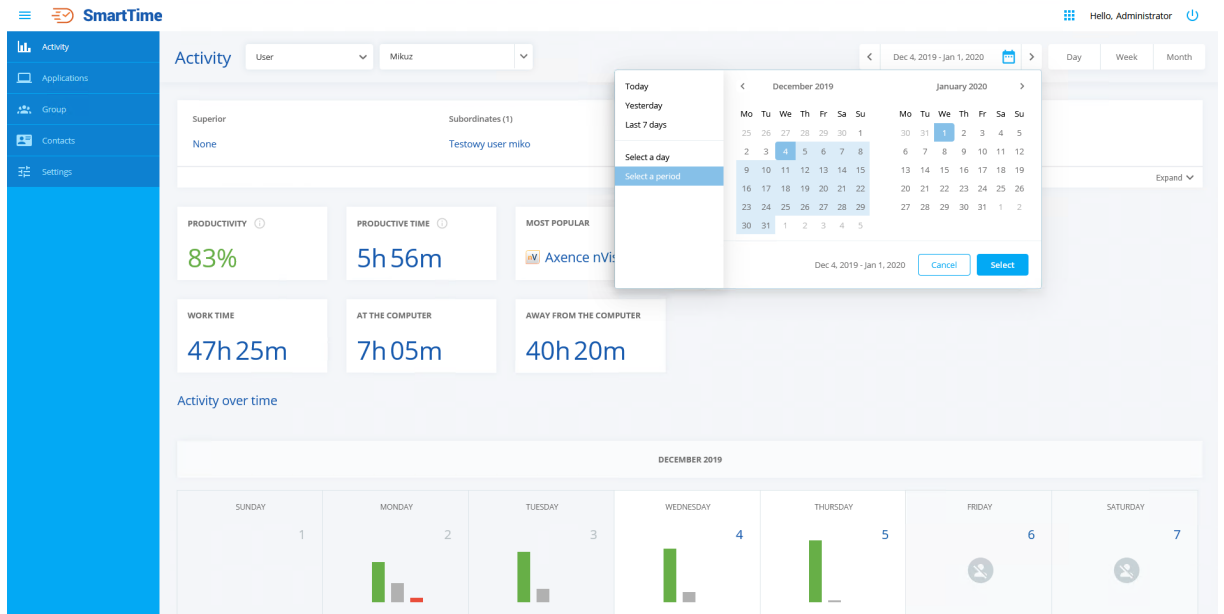
Activity view for selected week:



Activity view for selected month:



You can also specify any time period by selecting it from the calendar:



11.6.3 User group activity

11.6.3.1 Activity on the selected day

When displaying the **group activity** data, the following items are shown.

Statistics

- **Productivity** – productivity is measured in the selected period. **It is the sum of the productive time of the employees in the group, divided by the sum of the time of total activity on the computer in the selected period.**
- **Productive time of the group** – the sum of the time spent by the employees belonging to the group in the selected period.

When an application exception occurs, information that the user's time spent in the selected application is treated as productive will be highlighted accordingly by the warning sign icon in the group productivity view.

Active in a given period

Data on the activity of the group members for whom any activity was recorded in the selected time period will be displayed here.

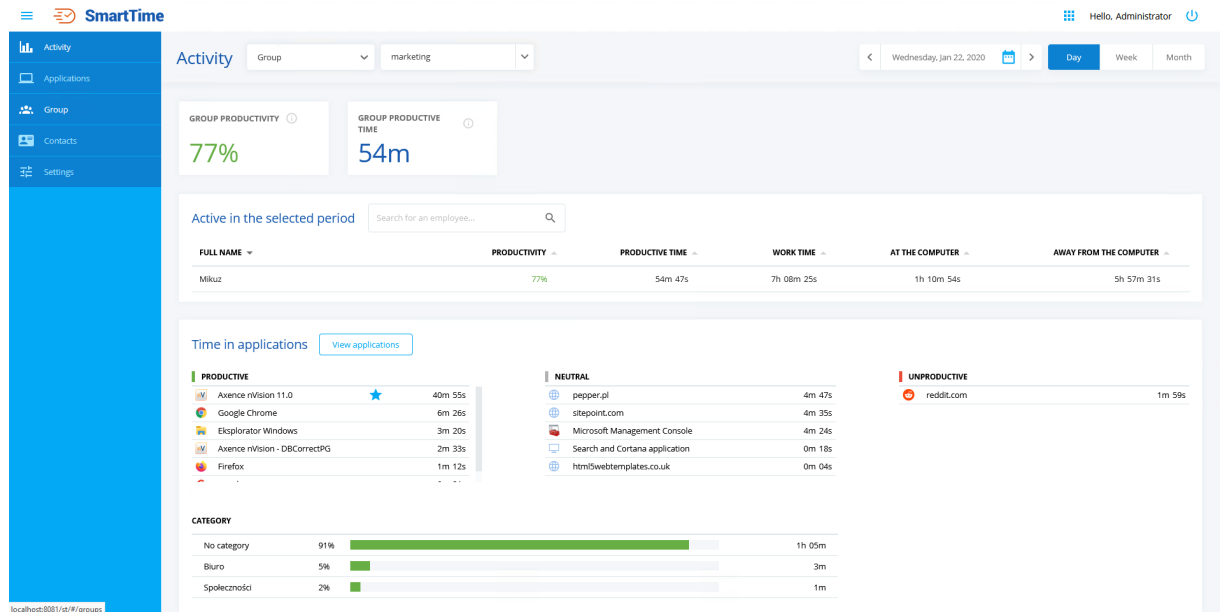
Time spent in applications

This part shows the total time spent in applications by the group members. This area of the SmartTime module is divided into three sections: productive, neutral and unproductive applications. The available

information is shown as a list. The applications marked with an asterisk indicate that an exception has been applied to the application.

After clicking **View all**, the list of applications in which the group was active will be displayed. In this screen, you can quickly add an exception to the displayed group by clicking on the **Asterisk** icon in the **Exception** column.

The **category** charts show the usage of the applications belonging to the individual categories. Information about the most and least common category applications can be found here.



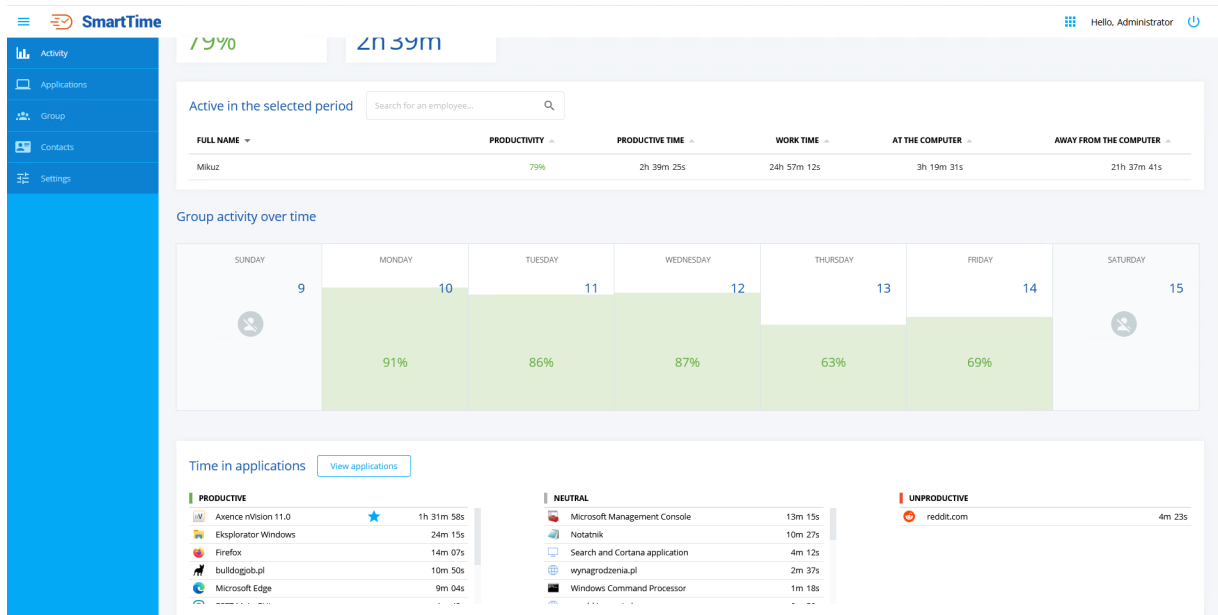
11.6.3.2 Activity in the selected period

When displaying the group activity for a period longer than one day, one more section is added to the statistics described in the previous [chapter](#)^[518], named **Group activity in a given period**.

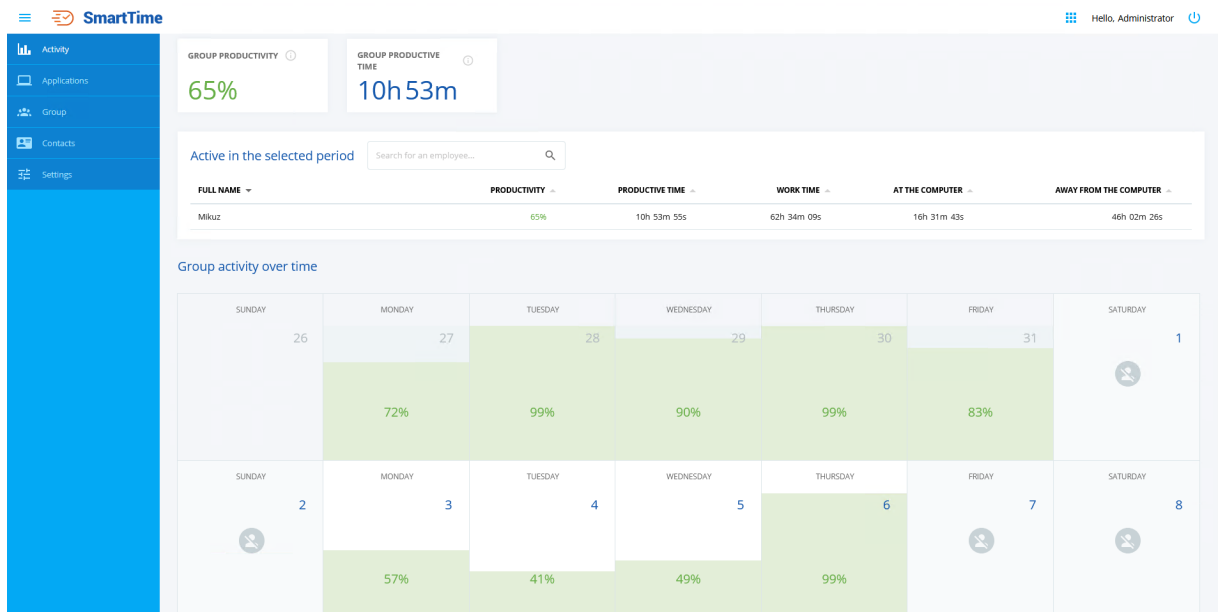
This part of the screen shows the grid indicating the group productivity in the selected time period. After clicking the selected tile, you will be moved to the detailed data for the selected day.

Similarly to the user activity view, you can select the time period from the calendar and view the activity for it.

Weekly activity view:



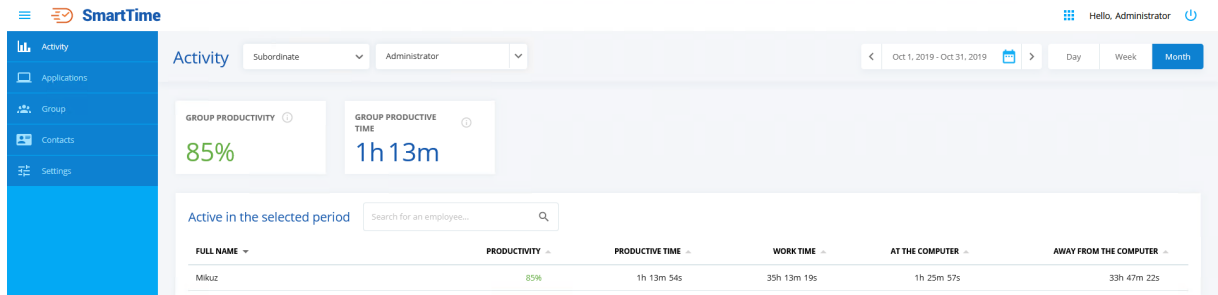
Monthly activity view:



11.6.4 Activity of subordinates

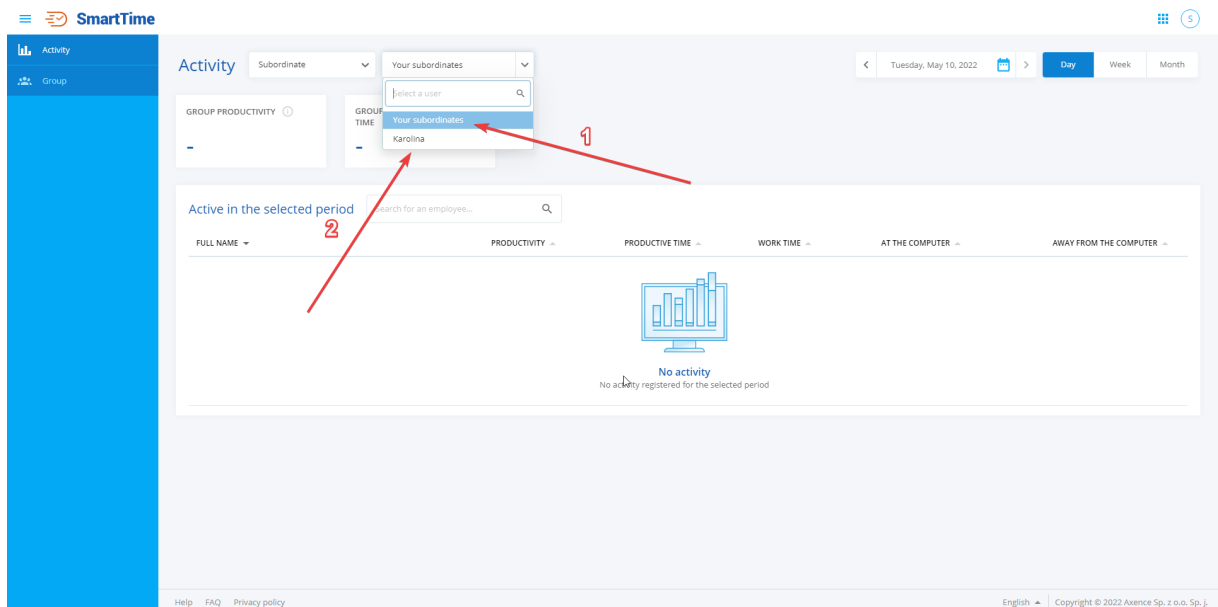
After selecting the activity of subordinates, the **activity data for all subordinates of the selected person** will be displayed. These data are presented in the same manner as the user group data.

The screenshot below shows the activity of all subordinates of the “User user” on selected day:



The option of displaying subordinates' activity distinguishes between two types of subordinates:

- The first type of subordinates is the so-called direct subordinate. The user (supervisor) who is currently logged in to SmartTime has access to the activities of his direct subordinates. The supervisor does not have to check each of his subordinates individually, because their activity is aggregated and is displayed after clicking on the **Your subordinates** option.
- The second type of subordinates is the so-called second-degree subordinates (subordinates of subordinates), i.e. users whose superior is subordinates of someone else. **For example:** Mariusz is Karolina's superior and Karolina is Robert's superior. In the SmartTime module, Mariusz has access to both Karolina's activity and her subordinates, i.e. Robert. Such subordinates are grouped depending on the person who is their supervisor. To view the activity of a second-degree subordinate, select a person from the list who is your direct subordinate



1. After clicking on **Your subordinates**, the activity of the logged in user's direct reports will be displayed.
2. After clicking on **Karolina**, the activity of the subordinates of the user Karolina (who is the subordinate of the logged in user) will be displayed..

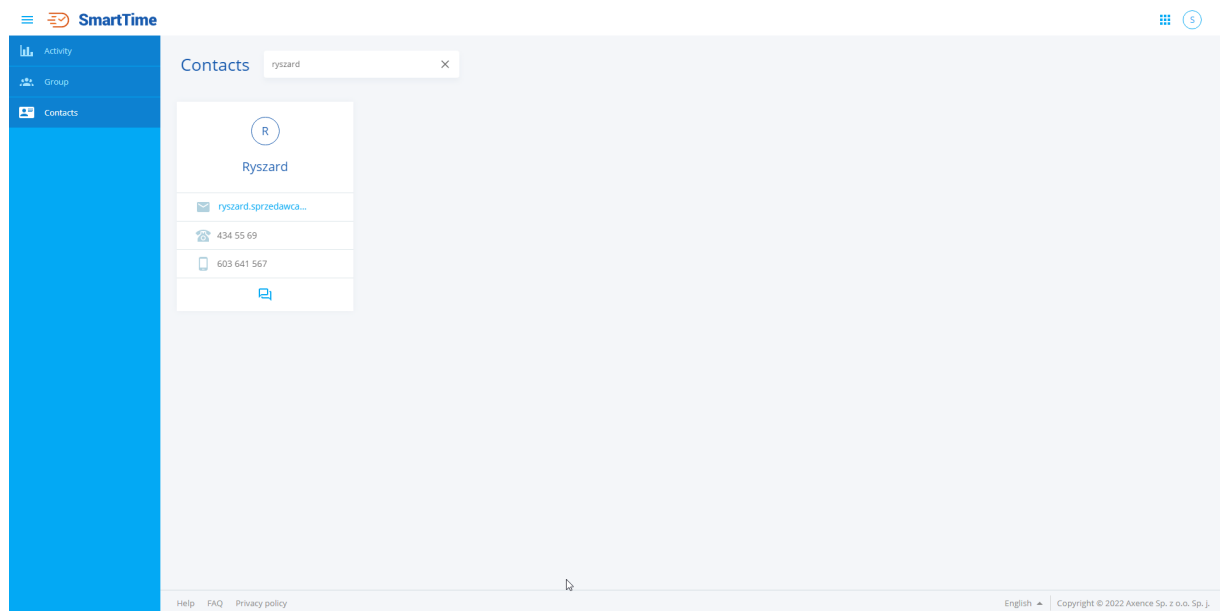
11.7 Contacts

The **Contacts** tab enables the contact data of the users in the nVision database to be searched for and checked if necessary.

The information displayed in this section are as follows:

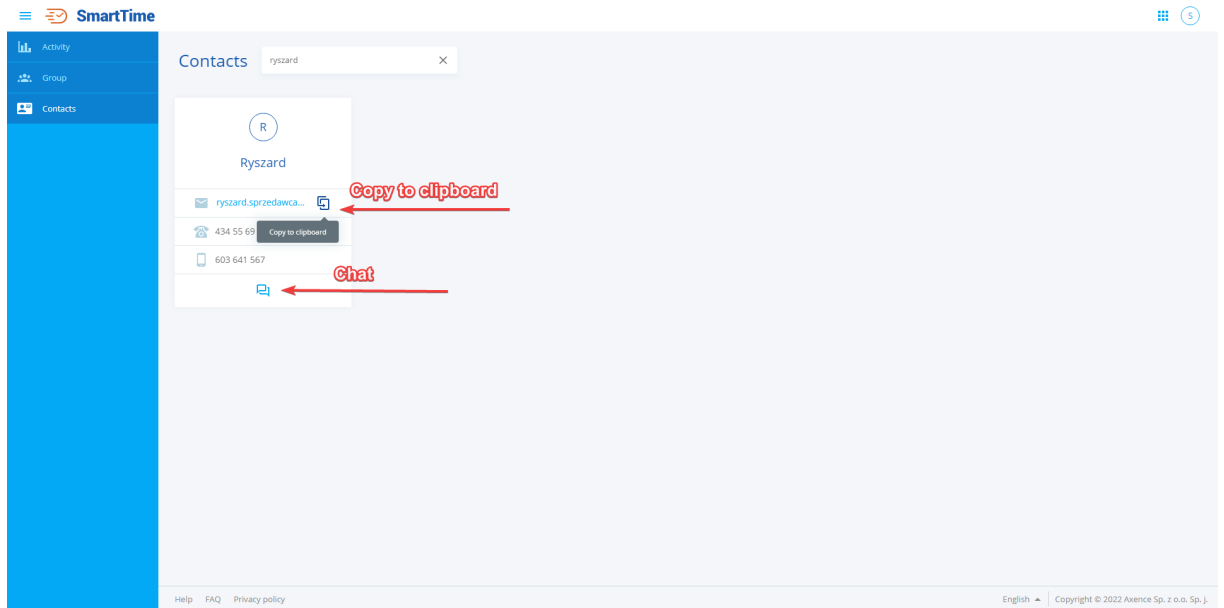
- First and last name of the user,
- E-mail address,
- Desk phone number,
- Mobile phone number.

The search engine in the upper part of the window allows you to quickly find the user you are interested in. The user is searched for by three parameters: **user name**, **first name** and **last name**, and **e-mail address**.



To quickly copy the e-mail address, desk phone number or mobile phone number of a given user, click on the **copy to clipboard** icon, which is displayed on the right, after hovering the cursor over the parameter of interest.

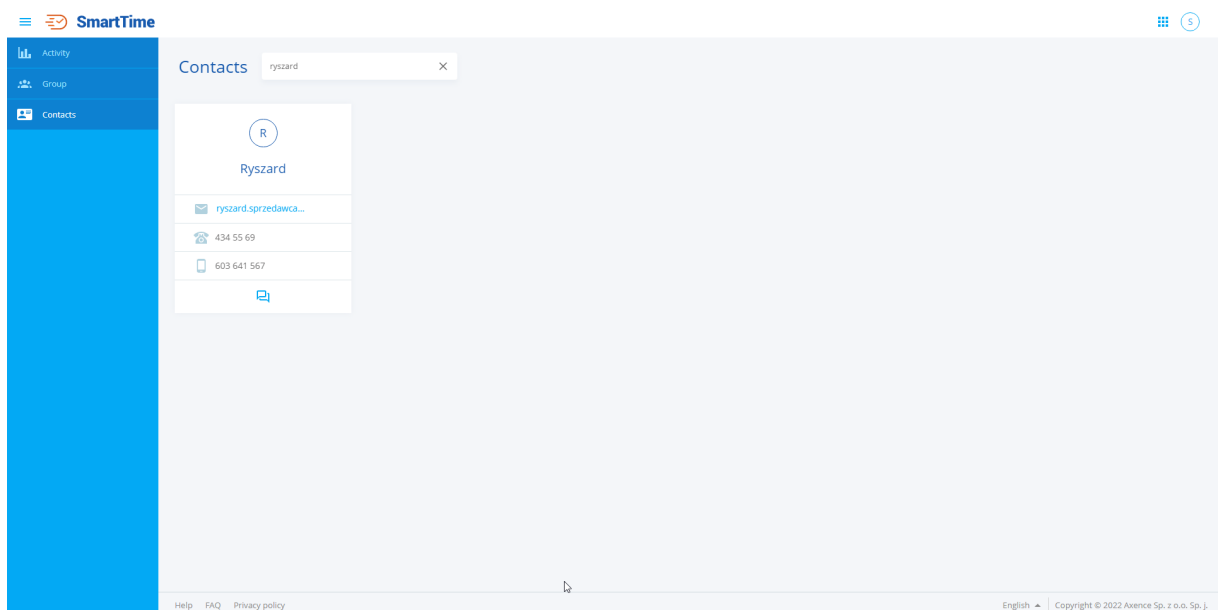
From the Contacts tab you can also go to the chat with the selected user. To start a conversation with a user, click the icon at the bottom of the user information field. After clicking on the icon, the chat will open in a new browser window.

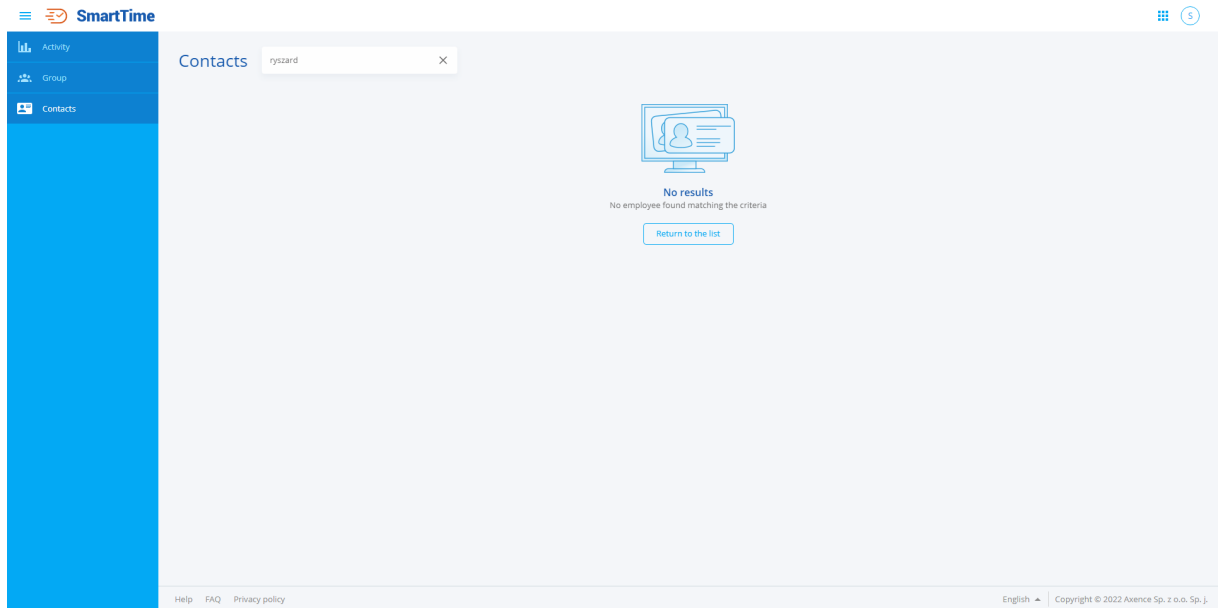


Note, if the chat access setting, both for the user currently logged in to SmartTime and the one we are looking for in the Contacts tab, is limited, the icon will not be available.

Restricting access to the Contacts tab

Axence nVision allows you to configure the user's access to the contact list. If the user has enabled access to contacts, it is displayed on the contact list and has access to it in the SmartTime module. If the user has disabled access to contacts, he does not appear in the contact list and he has no access to the contact list in the SmartTime module. This is a very useful feature as it allows you to hide technical accounts that would otherwise clutter your contact list.



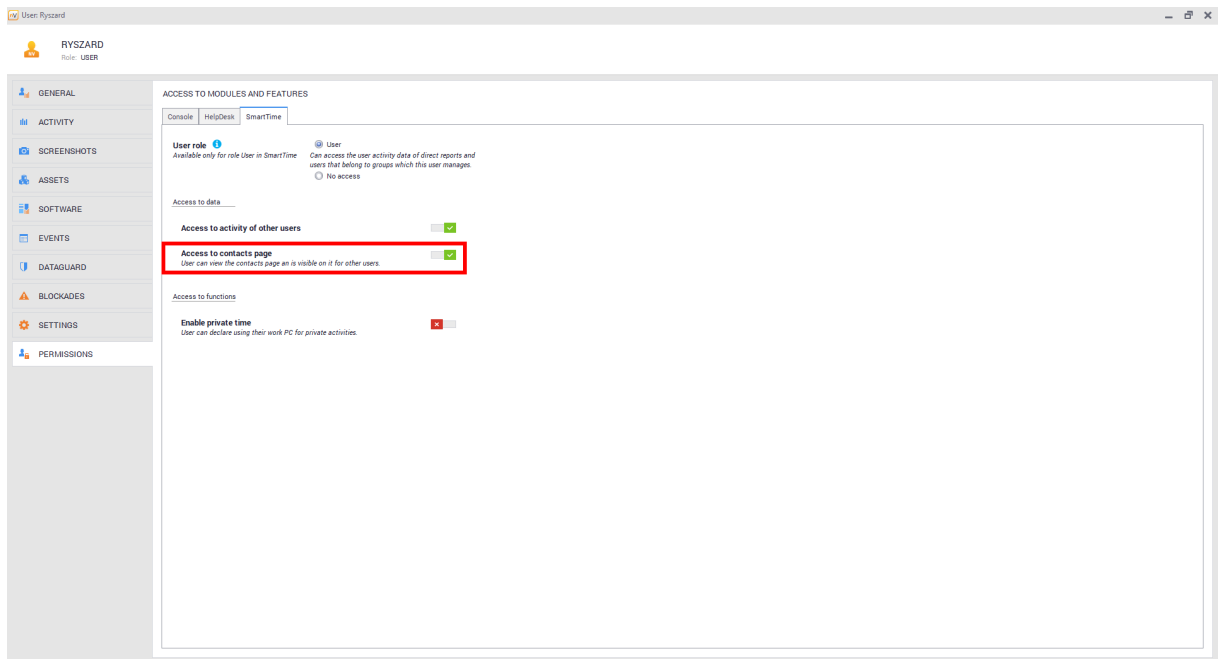


From the console level, we can limit access to the contact list for both a single user and a group of users, or set a default configuration for new users.

To configure access to the contact list for a single user:

1. Search for the appropriate user in the nVision console, and then open the user settings window.
2. Click on the **Permissions** tab.
3. Click on **SmartTime**.
4. By clicking on the slider, enable or disable access to the contact list.

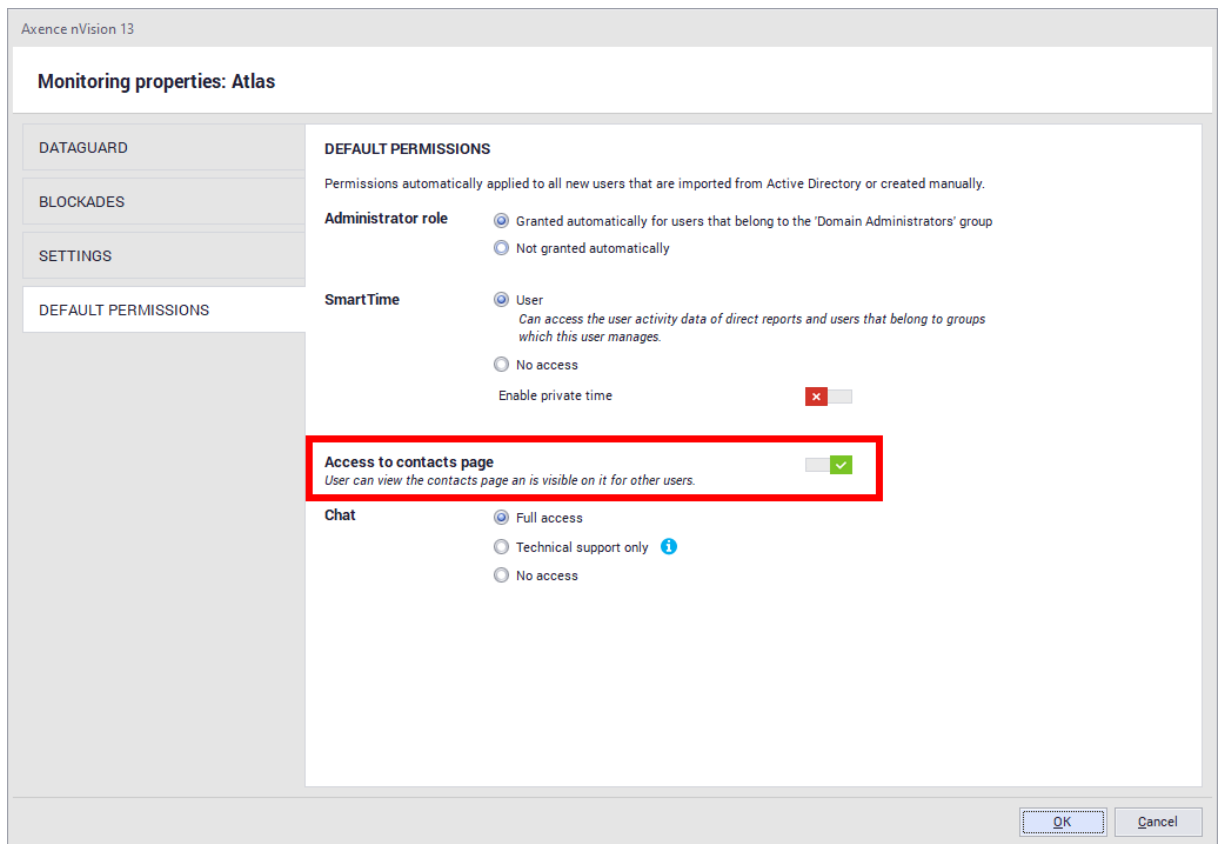
After clicking on the slider, the permissions of a given user will be updated.



To configure global contact list access settings:

1. Enter the **Atlas** settings.
2. Right-click **All Users** and then select **Atlas Information**.
3. Click the **Default Permissions** tab.

4. By clicking on the slider, enable or disable access to the contact list.
After clicking on the slider, the default settings for new users will be updated.



11.8 System time

The time and hours presented in the SmartTime module (for example on the activity chart) are always referred to the time of the machine on which the nVision server is installed. Data sent from the Agents are treated as if their events always took place in the server's time. If the customer is in a different time zone, the time is also not converted to the server's time zone.

Working time of employees

The system calculates the working time for each employee as **the difference between the time of the first and last activity** on each day.

For example, when the first user activity was detected at 9:00 and the last one at 12:00, the working time is three hours.

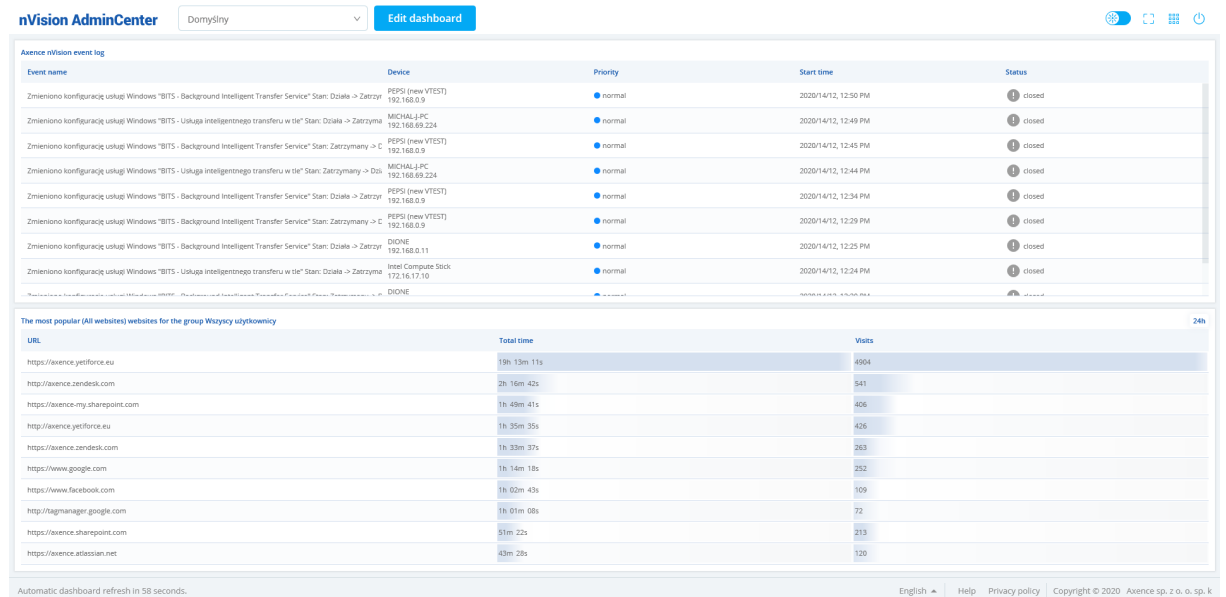
Part



12 AdminCenter

12.1 Introduction

AdminCenter is a portal that allows you to create an unlimited number of dashboards to show key network information. Any dashboard can be composed according to your individual requirements. A dashboard is an area of specific size where you can place a number of widgets. The dashboard size can be modified to suit the needs of the Administrator. For details on how to create, modify or share dashboards with other users in read-only mode, see the following sections.



The screenshot displays the nVision AdminCenter interface. At the top, there is a search bar with the text "Domyślny" and a dropdown menu, and a blue "Edit dashboard" button. The main content area is divided into two sections:

Axence nVision event log

| Event name | Device | Priority | Start time | Status |
|--|-------------------------------------|----------|---------------------|--------|
| Zmieniono konfigurację usługi Windows "BITS - Background Intelligent Transfer Service" Stan: Działalność -> Zatrzymano | PEPSI (new VTEST) 192.168.0.9 | normal | 2020/4/12, 12:50 PM | closed |
| Zmieniono konfigurację usługi Windows "BITS - Usługa inteligentnego transferu w tle" Stan: Działalność -> Zatrzymano | MICHAŁ J-PC 192.168.0.224 | normal | 2020/4/12, 12:49 PM | closed |
| Zmieniono konfigurację usługi Windows "BITS - Background Intelligent Transfer Service" Stan: Zatrzymano -> C... | PEPSI (new VTEST) 192.168.0.9 | normal | 2020/4/12, 12:45 PM | closed |
| Zmieniono konfigurację usługi Windows "BITS - Usługa inteligentnego transferu w tle" Stan: Zatrzymano -> Działalność | MICHAŁ J-PC 192.168.0.224 | normal | 2020/4/12, 12:44 PM | closed |
| Zmieniono konfigurację usługi Windows "BITS - Background Intelligent Transfer Service" Stan: Działalność -> Zatrzymano | PEPSI (new VTEST) 192.168.0.9 | normal | 2020/4/12, 12:34 PM | closed |
| Zmieniono konfigurację usługi Windows "BITS - Background Intelligent Transfer Service" Stan: Zatrzymano -> C... | PEPSI (new VTEST) 192.168.0.9 | normal | 2020/4/12, 12:29 PM | closed |
| Zmieniono konfigurację usługi Windows "BITS - Background Intelligent Transfer Service" Stan: Działalność -> Zatrzymano | DIONE 192.168.0.11 | normal | 2020/4/12, 12:25 PM | closed |
| Zmieniono konfigurację usługi Windows "BITS - Usługa inteligentnego transferu w tle" Stan: Działalność -> Zatrzymano | Intel Compute Stick 172.16.17.10 | normal | 2020/4/12, 12:24 PM | closed |

The most popular (All websites) websites for the group Wszyscy użytkownicy

| URL | Total time | Visits |
|----------------------------------|-------------|--------|
| https://axence.yetforce.eu | 19h 13m 11s | 4904 |
| http://axence.zendesk.com | 2h 16m 42s | 541 |
| https://axence-my.sharepoint.com | 1h 49m 41s | 406 |
| http://axence.yetforce.eu | 1h 35m 35s | 426 |
| https://axence.zendesk.com | 1h 53m 37s | 263 |
| https://www.google.com | 1h 14m 18s | 252 |
| https://www.facebook.com | 1h 02m 43s | 109 |
| http://tagmanager.google.com | 1h 01m 08s | 72 |
| https://axence.sharepoint.com | 51m 22s | 213 |
| https://axence.atlassian.net | 43m 28s | 120 |

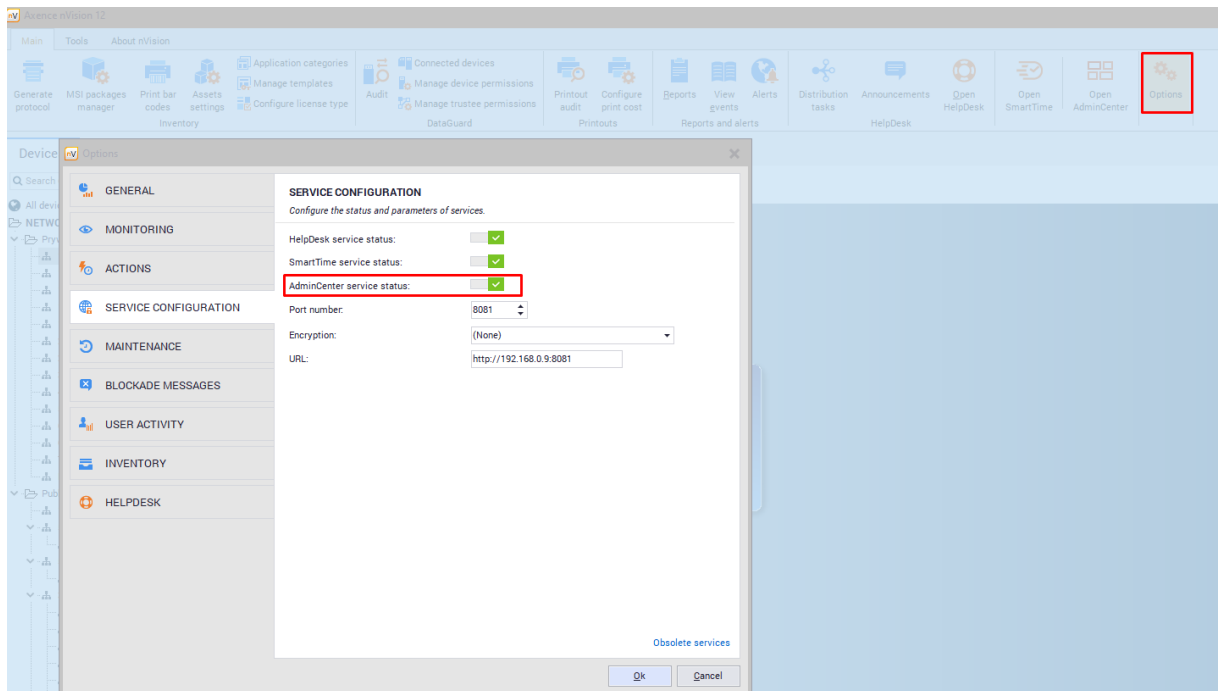
Automatic dashboard refresh in 58 seconds.

English | Help | Privacy policy | Copyright © 2020 Axence sp. z o. o. sp. k

12.2 Management and configuration

12.2.1 Enabling AdminCenter

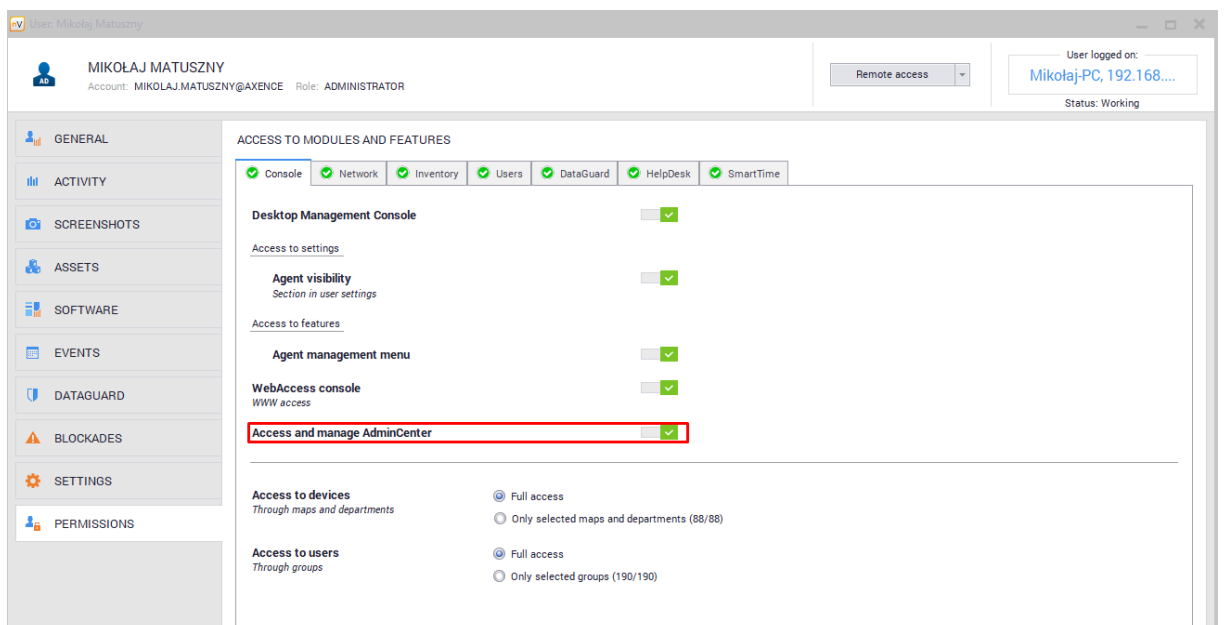
To enable AdminCenter, navigate to nVision main settings. In the **Service Configuration** tab, you can find the **AdminCenter service status** switch to enable this service:



12.2.2 User permissions

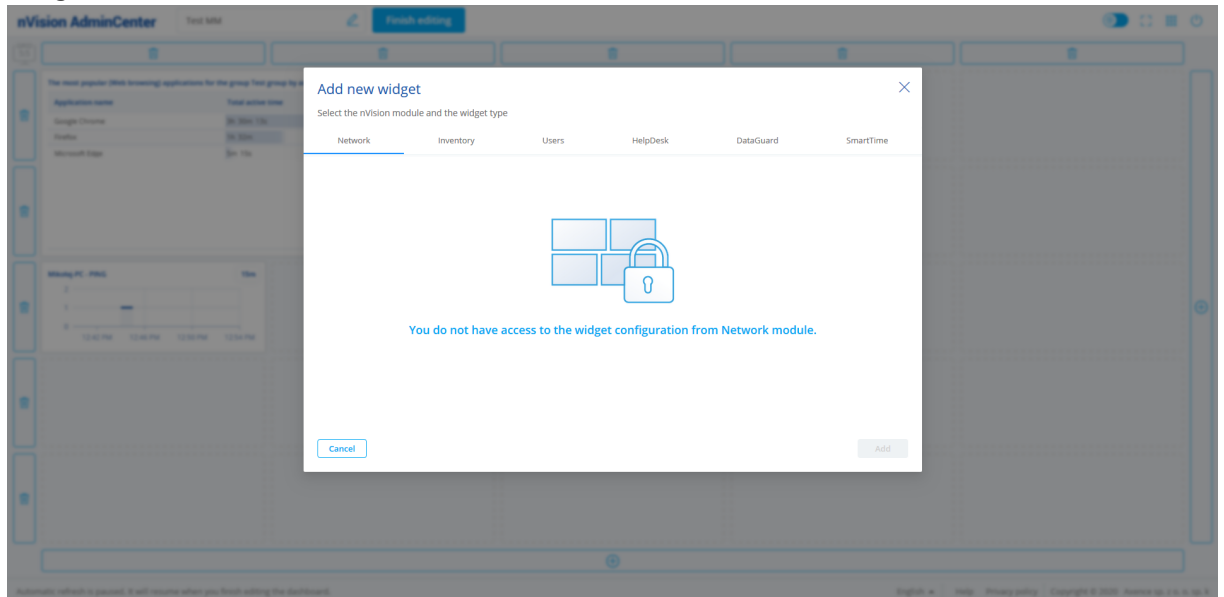
To access AdminCenter, the user must have the role of the **Administrator** or **Superadministrator**. A person with the **Superadministrator** role always has access to all the enabled AdminCenter functionalities.

If the user has the **Administrator** role, it needs to be specified whether they may have access to AdminCenter functionalities. To do this, navigate to the user information screen, then select the **Rights / Console** tab and enable the "**AdminCenter access and management**" option:



AdminCenter allows you to display widgets associated with the individual Axence nVision modules. If the **Administrator** logged in does not have access to the management of a specific module or

the module is not included in the software license, the Administrator will not be able to create widgets from that module. This information will be shown in AdminCenter:



12.2.3 Free version limitations

The AdminCenter functionality is available in two versions - full and free:

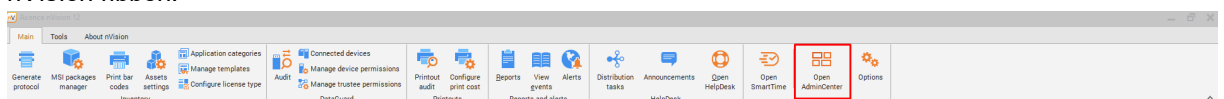
- The full version is included in each ProPerpetual license and in Freemium licenses with the purchased technical support service. It allows an unlimited number of dashboards to be created.
- The Freemium license without active technical support allows the use of AdminCenter functionalities, but the user can only create one dashboard with up to three widgets.

12.3 Starting AdminCenter

The AdminCenter portal can be started in two ways.

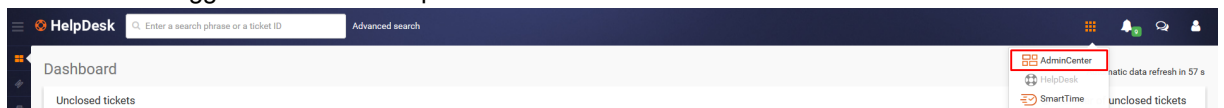
Accessing AdminCenter from the nVision console

To access AdminCenter from the nVision console, locate the Open AdminCenter button in the main nVision ribbon:



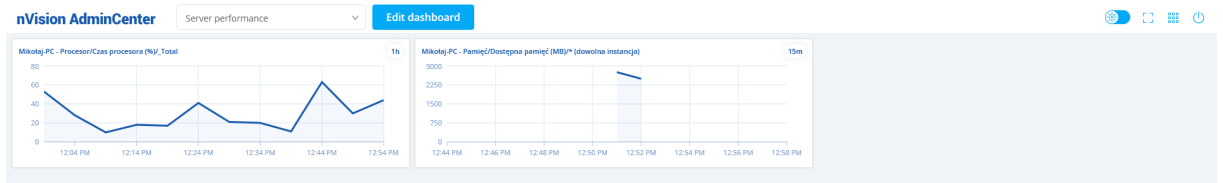
Accessing AdminCenter from the web browser

AdminCenter can also be started from SmartTime or HelpDesk. At the top of the browser window, there is a button to toggle between these portals:



12.4 Navigation within AdminCenter

The navigation buttons are located at the top of the browser window. Starting from the upper left corner of the screen, you can see a box that tells you which dashboard is currently displayed. By clicking the **Edit dashboard** button, you can enter the edit mode for the selected dashboard. Dashboard editing is described in detail [in the next section](#).



In the upper-right corner of AdminCenter, there are a few buttons. When you hover the mouse pointer over a button, a brief description of this button is displayed:



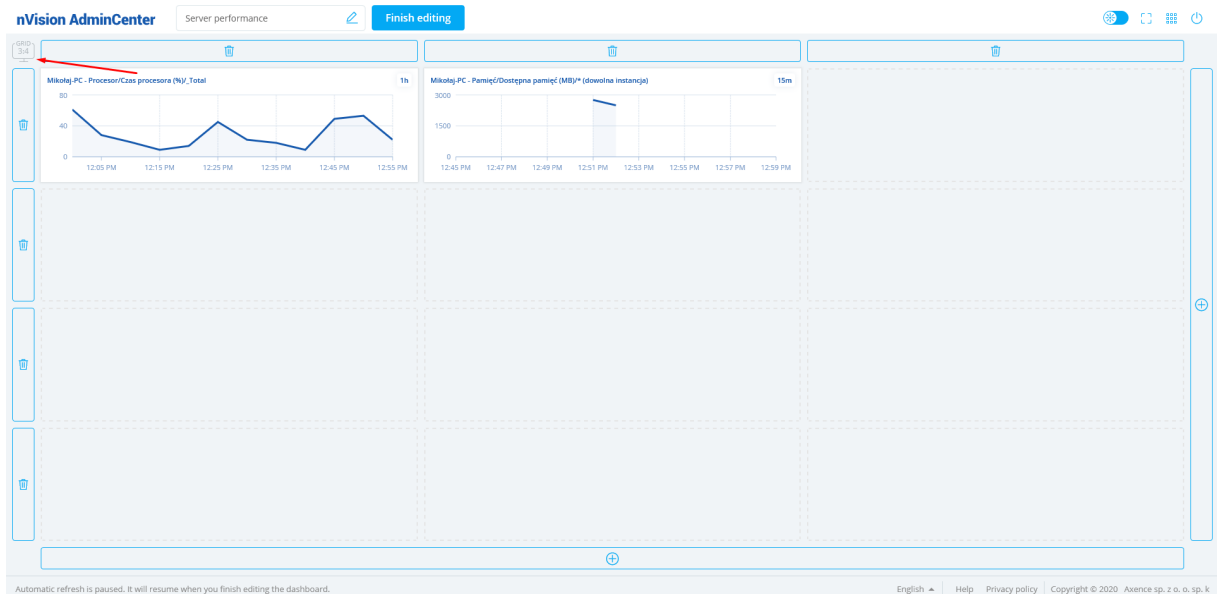
Below is a description of each of the buttons (from the left):

- Switches the AdminCenter color pattern (light or dark color pattern),
- Enters full screen mode,
- Switches to other nVision web-based applications (HelpDesk, SmartTime),
- Logs off the currently logged in user.

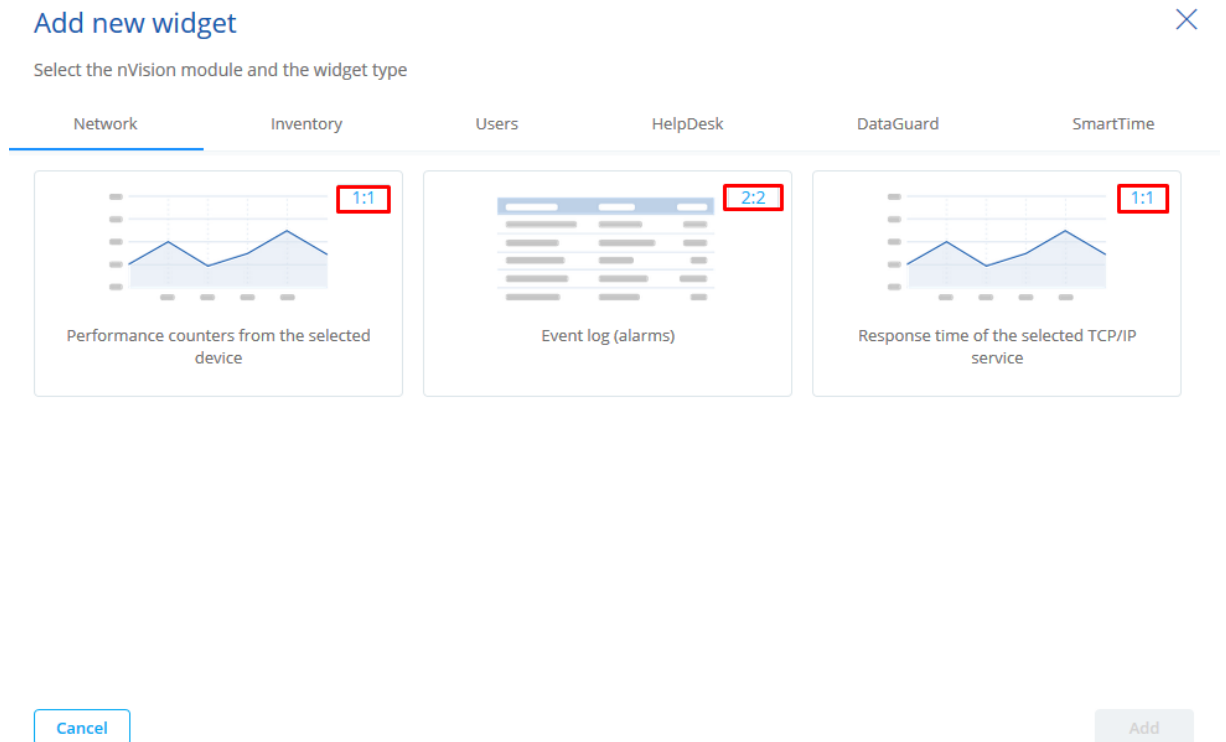
12.5 Dashboard management

12.5.1 Basic information

A dashboard is a grid of columns and rows where you can place a number of widgets. Each dashboard has a specific size which affects the maximum number of widgets that can be placed on it. The default size of a new dashboard is a grid consisting of three columns and four rows:



The size of the widget can be checked when adding it to a dashboard:

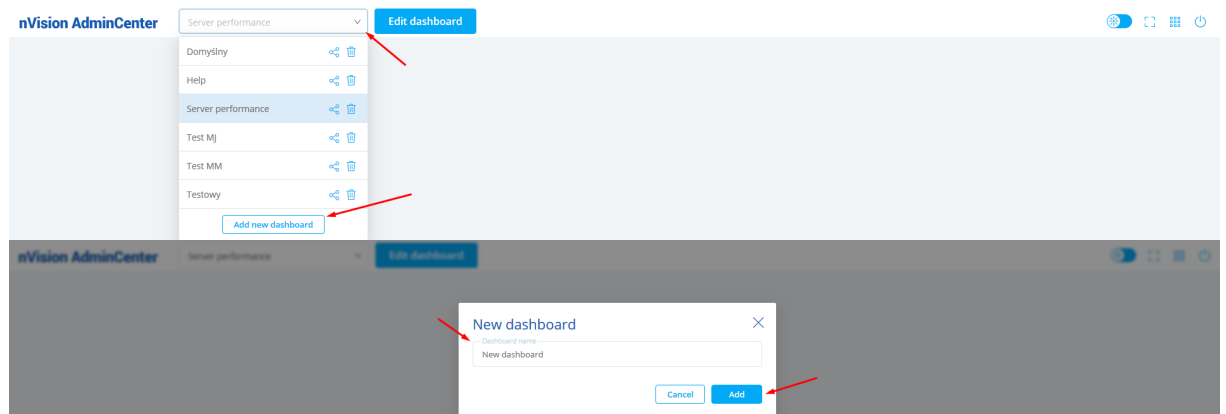


Detailed information on creating, modifying and removing dashboards is described in the following sections.

12.5.2 Creating new dashboard

Create a new dashboard in the following way:

1. Expand the list of available dashboards by clicking the box at the top of the screen.
2. Click the **Add new dashboard button** at the bottom of the list.
3. Enter the name of the new dashboard and confirm with the Add button.



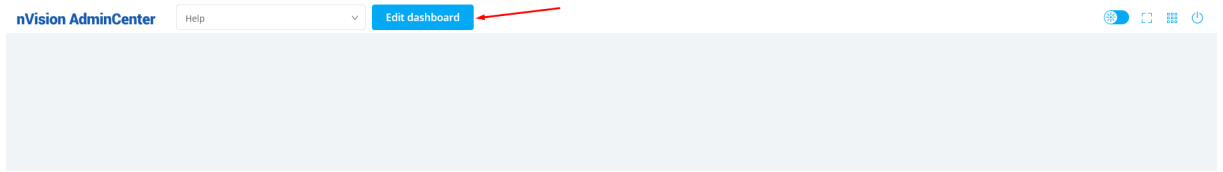
Once you have completed the steps above, the new dashboard will be added and you will be able to edit it. Dashboard editing is described in [the next section](#).⁵³²

12.5.3 Editing a dashboard

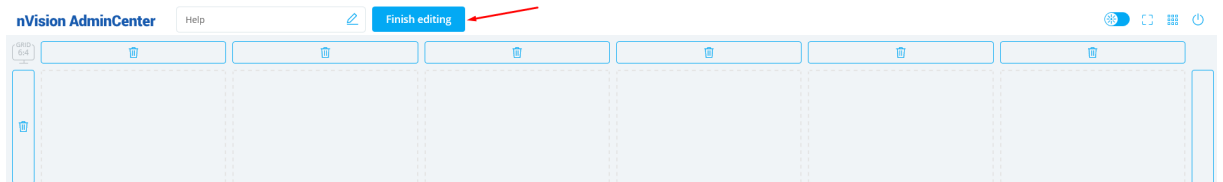
12.5.3.1 Dashboard edit mode

Entering and exiting the dashboard edit mode

To enter the dashboard edit mode, click the **Edit dashboard** button next to the name of the dashboard displayed:



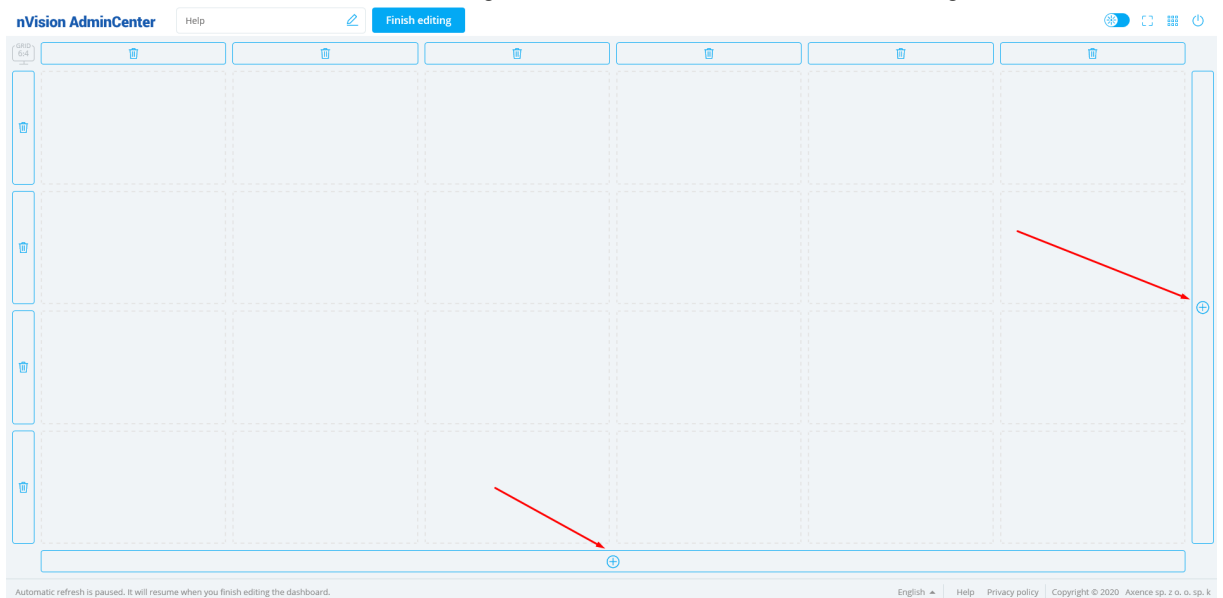
When you have finished modifying the dashboard, click the **Finish editing** button to save your changes:



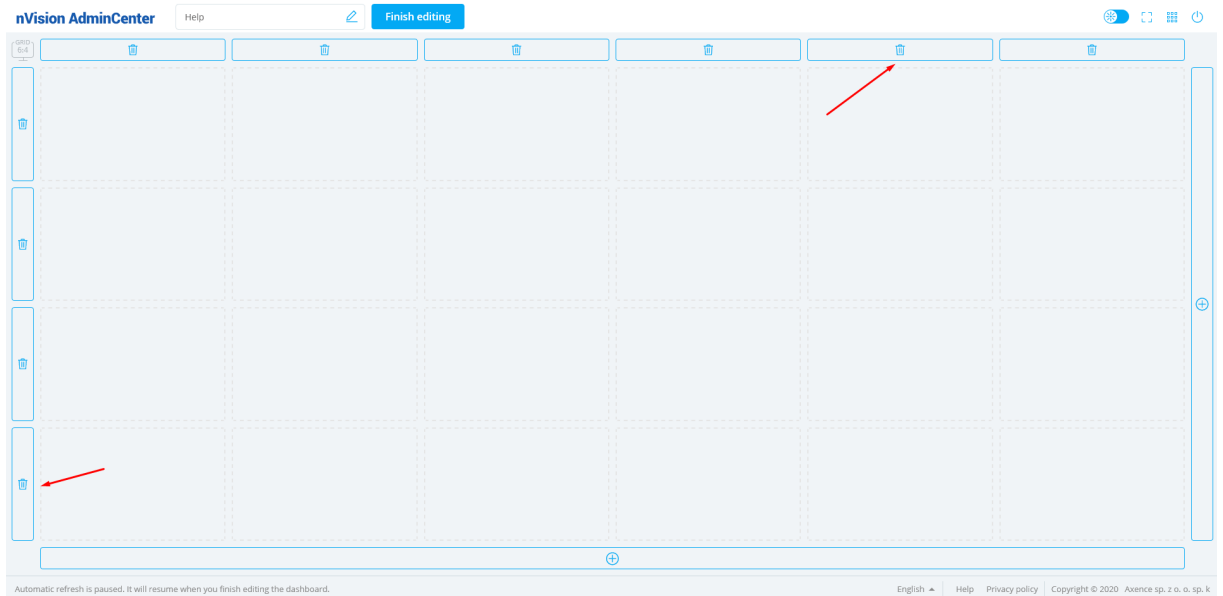
12.5.3.2 Changing the size of the grid

When you enter the dashboard edit mode, a grid appears on the screen where you can place widgets. You can increase the dashboard size so that you can place more widgets on it.

To add additional columns or rows to the grid, click the "+" button at the bottom right of the screen:



To decrease the dashboard size, delete a row or column by clicking the trash icon next to each item:

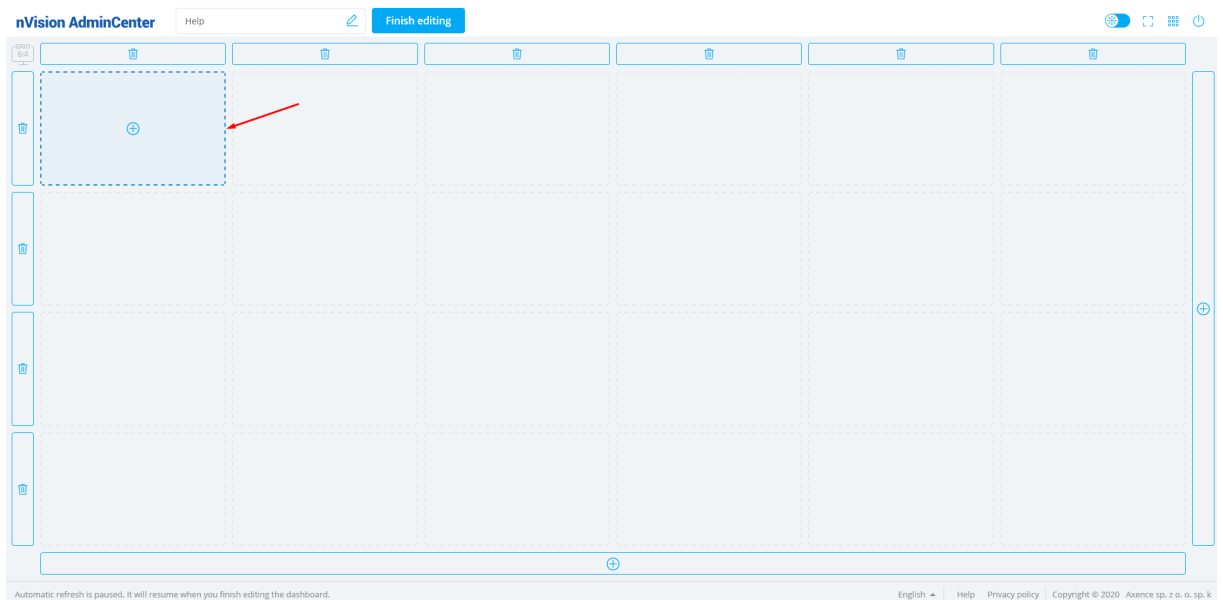


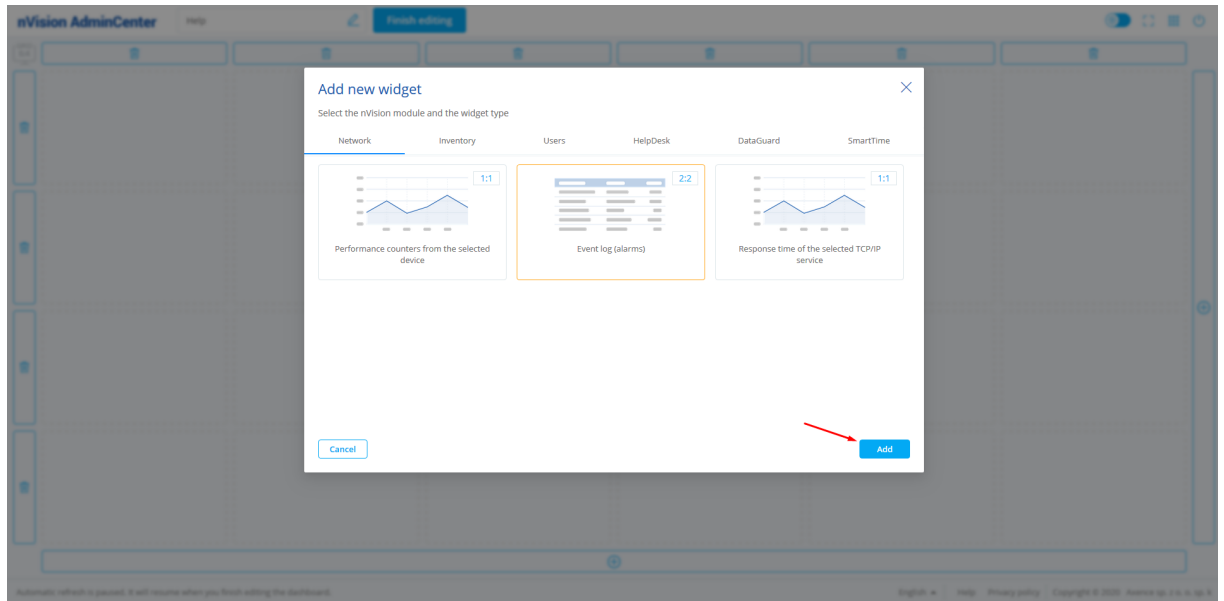
12.5.3.3 Adding widgets

Add a new widget to an existing dashboard in the following way:

1. Select a dashboard from the list, and then enter the edit mode.
2. Click the location on the grid where you want to place the new widget.
3. Select one of the available widgets. Widgets are described in detail in section [Available widgets](#).⁵³⁷
4. Click **Add** to confirm your selection.

Once you have completed the steps above, the widget will added to the dashboard.



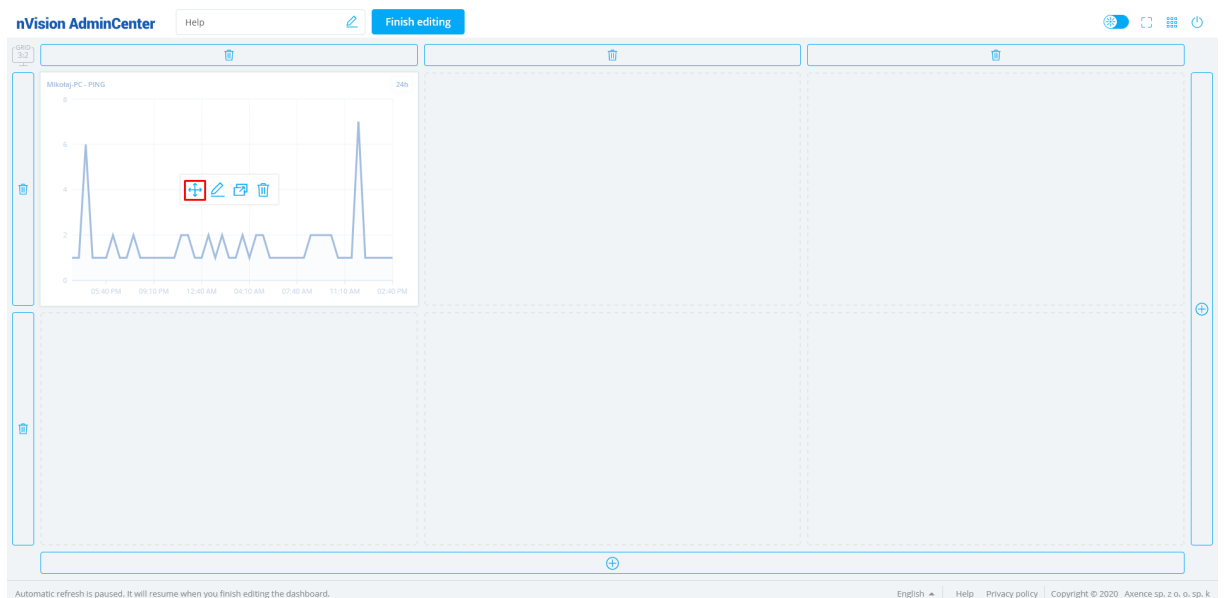


12.5.3.4 Modifying widgets

There are several modification options available for widgets added to the dashboard.

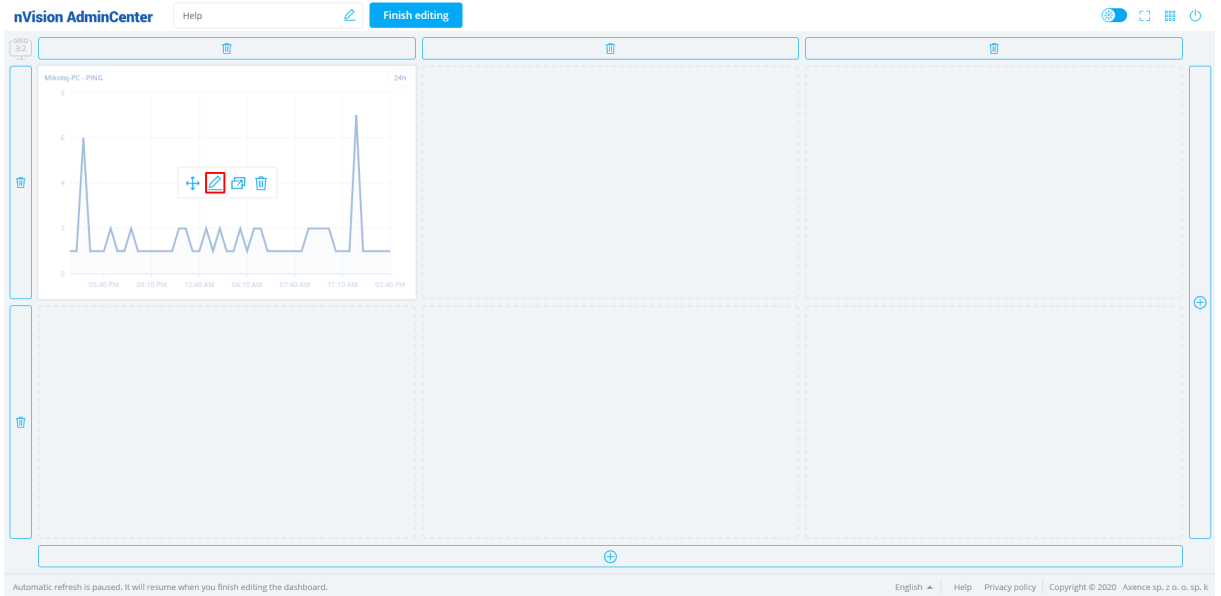
Moving a widget

To move a widget to a different location on the dashboard, simply hover your mouse over the arrow button, which appears after hovering over the widget, and drag it to the selected location:



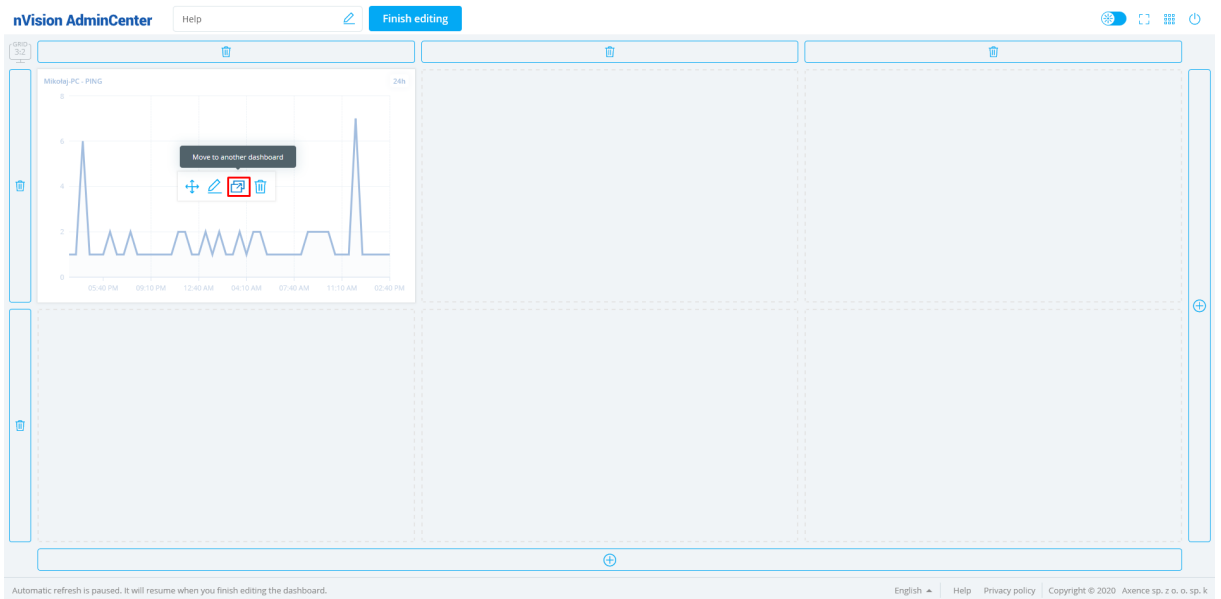
Editing a widget

To edit the widget configuration, click the pencil icon button which appears when you hover over the widget:



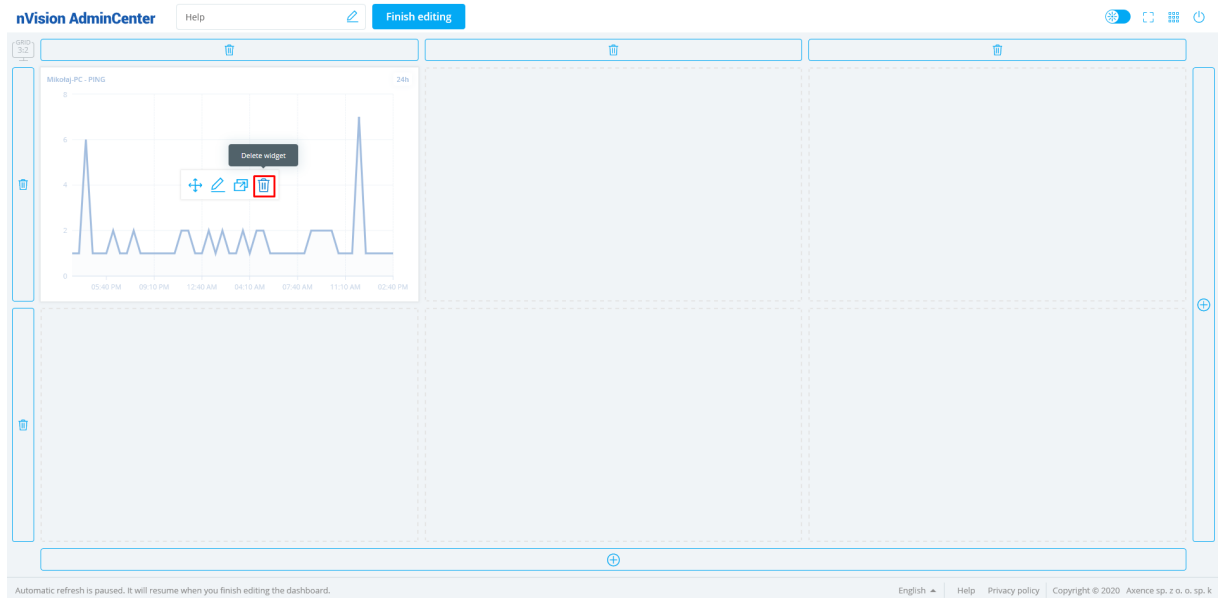
Moving a widget to another dashboard

To move a widget to another dashboard, select the movement button on the screenshot below, and then select the target dashboard and confirm with the **Move** button:



Deleting a widget

To delete a widget, click the trash icon button, and then confirm the delete operation with the **Delete** button:



12.5.4 Available widgets

AdminCenter allows you to create widgets to show data from any Axence nVision module. For adding widgets to dashboards, refer to the section [adding widgets](#)⁵³⁴.

The following sections describe all the available widgets grouped by module. Select an item in the list to go to the desired chapter:

- Network module widgets⁵³⁷
- Inventory module widgets⁵⁴¹
- Users module widgets⁵⁴⁴
- DataGuard module widgets⁵⁴⁹
- HelpDesk module widgets⁵⁵¹
- SmartTime module widgets⁵⁵³

12.5.4.1 Network module widgets

Performance counter for a selected device

The widget makes it possible to view a graph showing the values of a specific performance counter for the selected device.

The configuration requires the selection of the device, the performance counter, and time range for the data to be shown:

← Add new widget



Select widget details for Performance counters from the selected device

NETWORKS AND MAPS

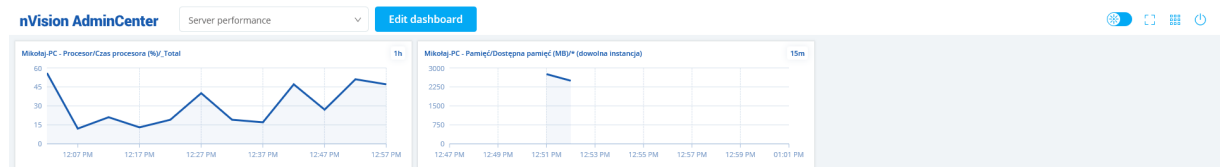
- Wszystkie urządzenia (Atlas)
- > Sieci
- > Mapy użytkownika
- > Oddziały
- > Inteligentne mapy

| NAME | IP | TYPE | PRIORITY |
|------------------------|-----------------|------------|----------|
| Mikołaj-PC | 192.168.69.201 | Windows 10 | normal |
| Telefon Mikołaja - 321 | 192.168.111.211 | IP Phone | normal |

Select a counter available on this device:

Select a time range of displayed data:

The screenshot below shows an example of the widget:



Note! To add a widget with a performance counter, the performance counter must be added to the device beforehand.

Event log (alerts)

The widget makes it possible to view a table with the event log, which is also visible in the nVision console. The administrator can narrow down the displayed results depending on the importance of the event:

[← Edit widget](#)

Select widget details for Event log (alarms)

NETWORKS AND MAPS

- Wszytkie urządzenia (Atlas)
- Sieci
- Mapy użytkownika
- Oddziały
- Inteligentne mapy

SHOW EVENTS BY SEVERITY

 Select all events Critical Important Normal Low[Cancel](#)[Back](#)[Update](#)

The screenshot below shows an example of the widget:

nVision AdminCenter ttt [Edit dashboard](#)

| Event name | Device | Priority | Start time | Status |
|---|------------------------------|-----------|----------------------|--------|
| Zmiana w informacjach systemowych w stanie S.M.A.R.T. [[C] TOSHIBA THNSN128GC | RP-OLD 192.168.0.206 | important | 2021/15/03, 11:02 AM | closed |
| Serwis SSH nie działa | Mikołaj-PC 192.168.69.239 | critical | 2021/15/03, 11:01 AM | open |
| Zmiana w informacjach systemowych w stanie S.M.A.R.T. [[C] TOSHIBA THNSN128GC | RP-OLD 192.168.0.206 | important | 2021/15/03, 10:46 AM | closed |
| Zmiana w informacjach systemowych w stanie S.M.A.R.T. [[C] TOSHIBA THNSN128GC | RP-OLD 192.168.0.206 | important | 2021/15/03, 08:46 AM | closed |
| Zmiana w informacjach systemowych w stanie S.M.A.R.T. [[C] TOSHIBA THNSN128GC | RP-OLD 192.168.0.206 | important | 2021/15/03, 07:05 AM | closed |
| Usługa Windows "wscsvc - Centrum zabezpieczeń" zatrzymana | MARCIN-XPS 192.168.50.232 | important | 2021/12/03, 06:20 PM | closed |
| Serwis SSH nie działa | Mikołaj-PC 192.168.69.239 | critical | 2021/12/03, 12:51 PM | closed |
| Zmiana w informacjach systemowych w stanie S.M.A.R.T. [[C] TOSHIBA THNSN128GC | RP-OLD 192.168.0.206 | important | 2021/12/03, 08:27 AM | closed |
| Zmiana w informacjach systemowych w stanie S.M.A.R.T. [[C] TOSHIBA THNSN128GC | RP-OLD 192.168.0.206 | important | 2021/12/03, 07:26 AM | closed |
| Urządzenie nie działa | MARCIN-XPS 192.168.50.232 | critical | 2021/11/03, 04:38 PM | closed |

Automatic dashboard refresh in 53 seconds. English Help Privacy policy Copyright © 2021 Axence sp. z o. o. sp. k

Response time of selected TCP/IP service

The widget makes it possible to view a graph showing the values of responses from the selected TCP/IP service for the selected device.

The configuration requires the selection of the device, the TCP/IP service and time range for the data to be shown:

← Edit widget



Select widget details for Response time of the selected TCP/IP service

NETWORKS AND MAPS

- Wszystkie urządzenia (Atlas)
- > Sieci
- > Mapy użytkownika
- > Oddziały
- > Inteligentne mapy

| NAME | IP | TYPE | PRIORITY |
|------------------------|-----------------|------------|----------|
| Mikołaj-PC | 192.168.69.201 | Windows 10 | normal |
| Telefon Mikołaja - 321 | 192.168.111.211 | IP Phone | normal |

Select the service available on this device:

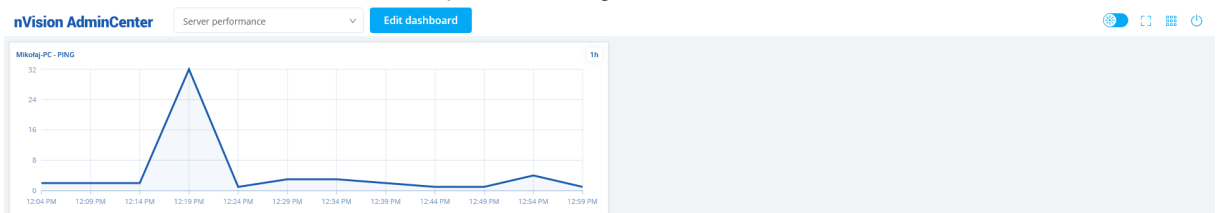
Select a time range of displayed data:

Cancel

Back

Update

The screenshot below shows an example of the widget:



Note! To add a widget with a response time of the TCP/IP service, the service must be added to the device beforehand.

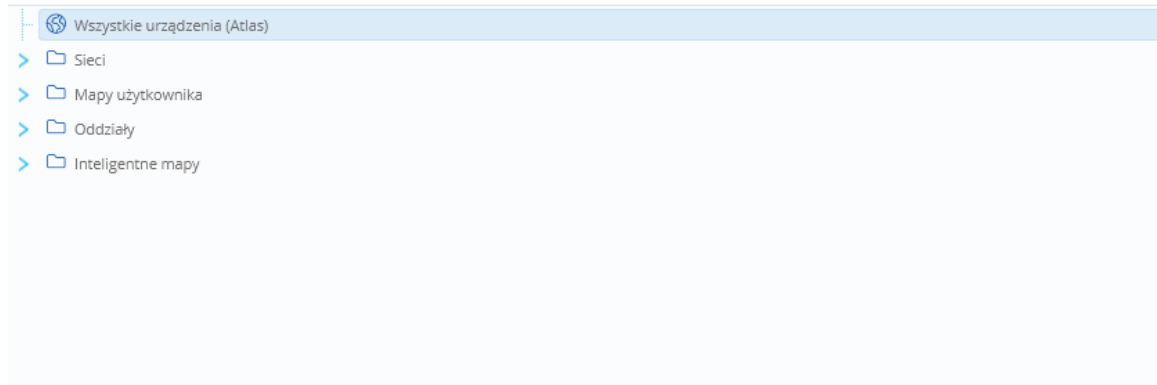
Recently discovered devices on the network

The widget allows you to view recently discovered devices on the network. It is possible to narrow down the results to a specific network map or department selected by the Administrator:

[← Add new widget](#)

Select widget details for Recently detected devices on the network

NETWORKS AND MAPS

[Cancel](#)[Back](#)[Add](#)

An example of a widget is shown in the screenshot below:

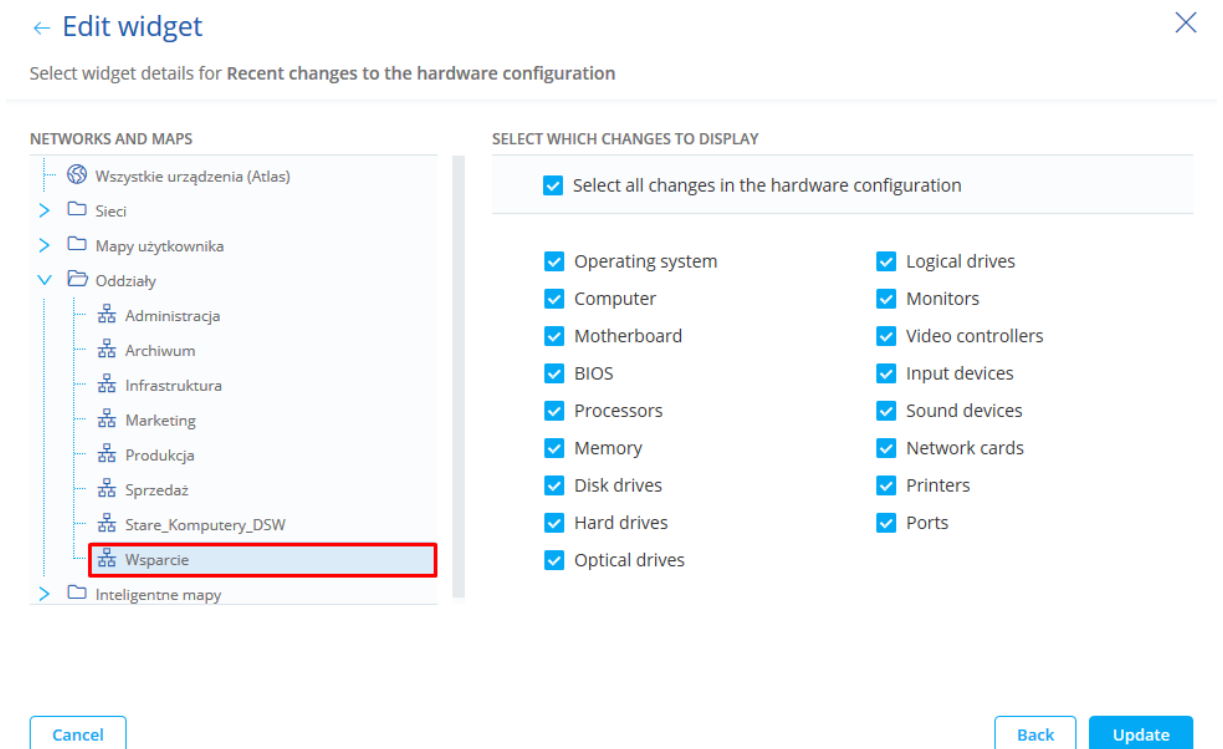
| Device | Available services | IP Address | Detection date |
|-----------------|--------------------|----------------|----------------------|
| DESKTOP-RBG47AH | | 10.0.2.15 | 2021/09/03, 10:19 AM |
| 10.10.20.30 | | 10.10.20.30 | 2021/03/03, 09:48 AM |
| 192.168.0.127 | PING | 192.168.0.127 | 2021/23/02, 02:42 PM |
| GOPINWO-XPS | | 192.168.69.209 | 2021/11/02, 05:01 PM |
| 192.168.69.245 | PING | 192.168.69.245 | 2021/08/02, 04:11 PM |

12.5.4.2 Inventory module widgets

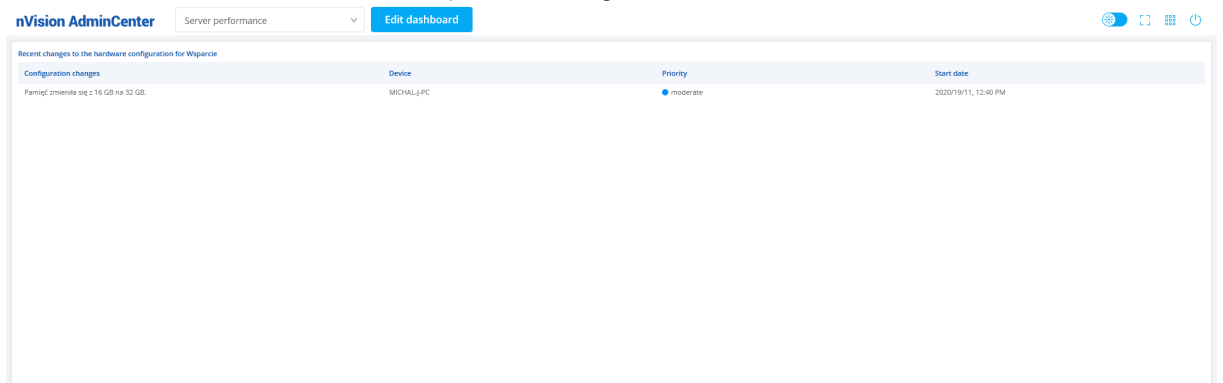
Recent changes in hardware configuration

The widget makes it possible to view a table with changes in the hardware configuration for a selected group of devices.

The configuration requires the selection of the map or department for which the data on changes in hardware configuration are to be shown. You can also define which machine components are to be included in this summary:



The screenshot below shows an example of the widget:



Recent changes in software configuration

The widget makes it possible to view a table with changes in the software configuration for a selected group of devices.

The configuration requires the selection of the map or department for which the data on changes in the configuration are to be shown. In addition, you can also define which operations are to be visible (installation, uninstallation, installation or uninstallation) and indicate the type of applications to be included in the summary (audited, unaudited, all applications):

← Edit widget



Select widget details for Recent changes to the software configuration

NETWORKS AND MAPS

- Wszystkie urządzenia (Atlas)
- > Sieci
- > Mapy użytkownika
- > Oddziały
- > Inteligentne mapy

SHOW THE FOLLOWING APPLICATION CHANGES

Uninstalled only

Audited applications only

Cancel

Back

Update

The screenshot below shows an example of the widget:

nVision AdminCenter Server performance Edit dashboard

| Recent changes to the software configuration for Wszystkie urządzenia (Atlas) | | | | | Recent changes to the software configuration for Wszystkie urządzenia (Atlas) | | | | |
|---|--|--------|------------|----------------------|---|-----------------------------------|--------|------------|----------------------|
| Actions | Application name | Device | Severity | Start date | Actions | Application name | Device | Severity | Start date |
| Uninstalled | Mozilla Firefox 82.0.3 (x64 pl) | | ● moderate | 2020/11/12, 08:13 AM | Installed | Mozilla Firefox 83.0 (x64 pl) | | ● moderate | 2020/11/12, 08:13 AM |
| Uninstalled | Google Chrome | | ● moderate | 2020/11/12, 11:47 AM | Installed | Intel(R) Dynamic Tuning | | ● moderate | 2020/11/12, 01:29 PM |
| Uninstalled | el Command Update for Windows 1 | | ● moderate | 2020/11/12, 11:47 AM | Installed | Realtek Audio Driver | | ● moderate | 2020/11/12, 01:29 PM |
| Uninstalled | Mozilla Firefox 75.0.1 (x64 pl) | | ● moderate | 2020/11/12, 11:10 AM | Installed | Google Chrome | | ● moderate | 2020/11/12, 11:47 AM |
| Uninstalled | Microsoft .NET SDK 5.0.100-rc2.20479.1 | | ● moderate | 2020/10/12, 03:59 PM | Installed | el Command Update for Windows 1 | | ● moderate | 2020/11/12, 11:47 AM |

Recent events on assets

The widget makes it possible to view a table with the events associated with assets (**Assets / Events** in the nVision console).

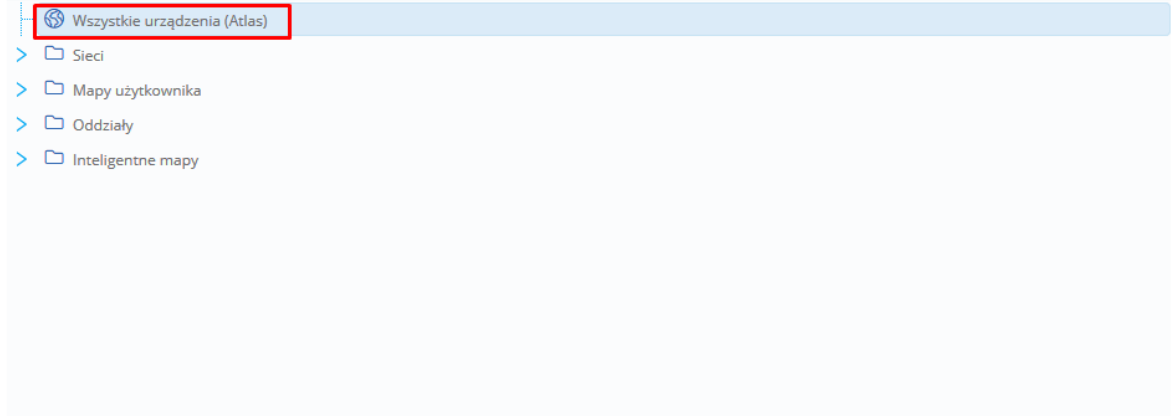
The configuration requires the selection of the map or department for which the data on asset events are to be shown.

← Add new widget



Select widget details for Recent resource management events

NETWORKS AND MAPS



Cancel

Back

Add

The screenshot below shows an example of the widget:

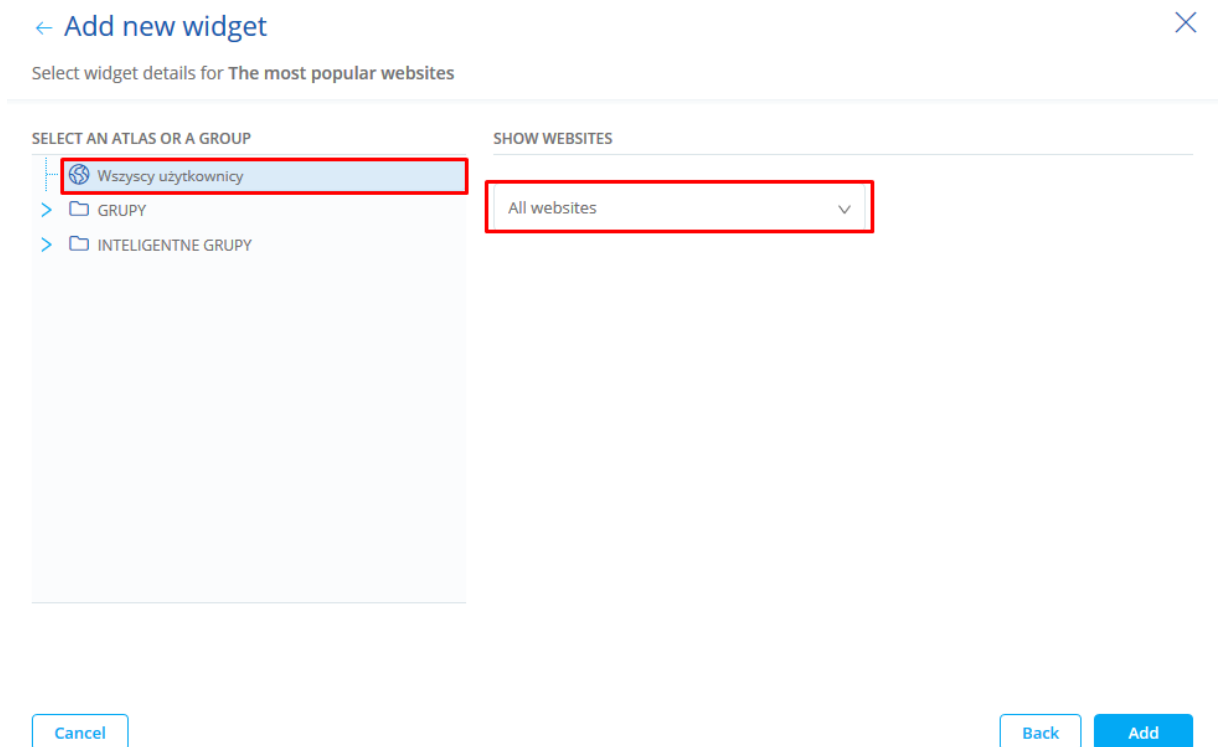
| Resource name | Resource type | Description | Date |
|---|---------------|--------------------------|----------------------|
| Acronis Backup | Licencja | Purchase new license | 2020/29/04, 12:00 AM |
| Acronis Backup | Licencja | sad | 2019/09/05, 12:00 AM |
| Microsoft Office Professional Plus 2019 | Licencja | sad | 2019/22/02, 12:00 AM |
| MarcinM-PC | Komputer | ALARM - KONIEC GWARANCJI | 2019/12/02, 12:00 AM |
| MarcinM-PC | Komputer | 1 | 2019/12/02, 12:00 AM |

12.5.4.3 Users module widgets

Top most visited websites

The widget shows the top most visited websites for a selected group of users in the last 24 hours.

The configuration requires the selection of the group of users and the category of websites. The categories of websites can be modified in the main nVision options using the **User activity / Domains** tab.



The screenshot below shows an example of the widget:

nVision AdminCenter Server performance Edit dashboard

The most popular (All websites) websites for the group Wszyscy użytkownicy

| URL | Total time | Visits |
|----------------------------------|-------------|--------|
| https://axence.yetforce.eu | 19h 39m 40s | 9108 |
| http://axence.zendesk.com | 2h 20m 19s | 575 |
| https://axence-my.sharepoint.com | 1h 50m 03s | 410 |
| http://axence.yetforce.eu | 1h 44m 21s | 443 |
| https://axence.zendesk.com | 1h 33m 37s | 263 |
| https://www.google.com | 1h 16m 55s | 263 |
| https://www.facebook.com | 1h 05m 24s | 118 |
| http://tagmanager.google.com | 1h 02m 28s | 73 |
| https://axence.sharepoint.com | 54m 35s | 235 |
| http://axence.atlassian.net | 46m 04s | 103 |

Top 10 applications with the longest run time

The widget shows the top 10 applications with the longest run time for a selected group of users.

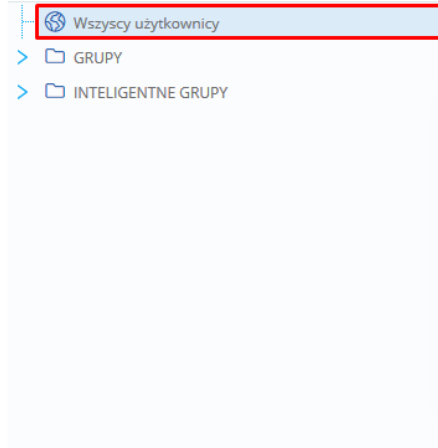
The configuration requires the selection of the group of users and the category of applications. The categories of applications can be modified in the main nVision options using the **User activity / Applications** tab.

← Add new widget

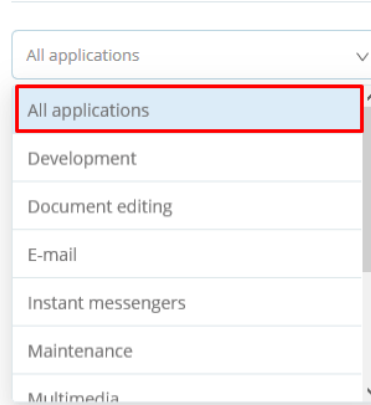


Select widget details for Top 10 applications by run time

SELECT AN ATLAS OR A GROUP



SHOW APPLICATIONS



Cancel

Back

Add

The screenshot below shows an example of the widget:

nVision AdminCenter Server performance Edit dashboard

The most popular (All applications) applications for the group Wszyscy użytkownicy by run time 24h

| Application name | Total run time | Application users |
|--|----------------|-------------------|
| Microsoft Teams | 487h 17m 04s | 31 |
| Shell Infrastructure Host | 431h 41m 14s | 44 |
| Runtime Broker | 431h 40m 05s | 44 |
| nVision Session Agent | 430h 58m 59s | 44 |
| Windows Shell Experience Host | 398h 24m 38s | 42 |
| COM Surrogate | 368h 39m 50s | 42 |
| Usermode Font Driver Host | 328h 52m 57s | 33 |
| Application Frame Host | 312h 47m 36s | 34 |
| Proces hosta dla usług systemu Windows | 309h 27m 39s | 35 |
| Proces hosta dla zadań systemu Windows | 309h 27m 38s | 35 |

Top 10 applications with the longest activity time

The widget shows the top 10 applications with the longest activity time for a selected group of users.

The configuration requires the selection of the group of users and the category of applications. The categories of applications can be modified in the main nVision options using the **User activity / Applications** tab.

← Add new widget



Select widget details for Top 10 applications by run time

SELECT AN ATLAS OR A GROUP

- 🌐 Wszyscy użytkownicy
- > 📁 GRUPY
- > 📁 INTELIGENTNE GRUPY

SHOW APPLICATIONS

All applications ▾

All applications

Development

Document editing

E-mail

Instant messengers

Maintenance

Multimedia

Cancel

Back

Add

The screenshot below shows an example of the widget:

nVision AdminCenter Server performance Edit dashboard

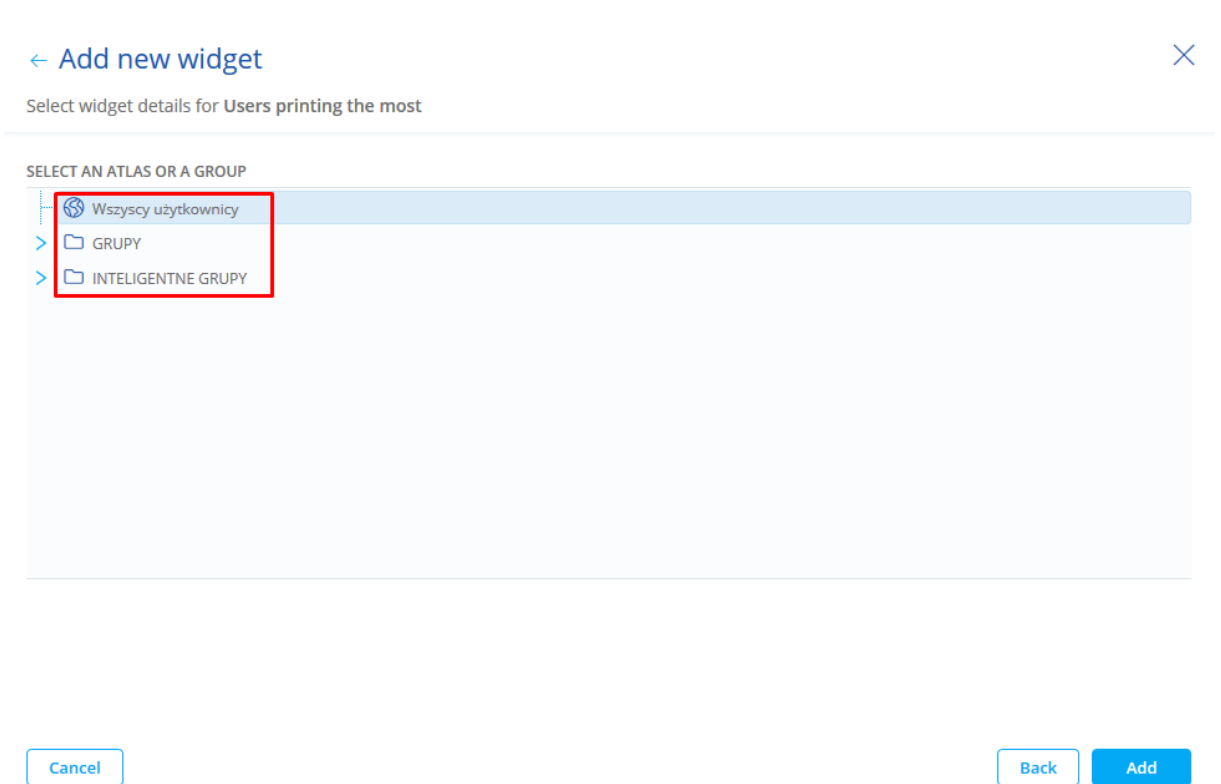
The most popular (All applications) applications for the group Wszyscy użytkownicy by active time 24h

| Application name | Total active time | Application users |
|------------------------------|-------------------|-------------------|
| Firefox | 39h 13m 05s | 21 |
| Microsoft Teams | 30h 48m 28s | 27 |
| Microsoft Outlook | 25h 04m 16s | 26 |
| Google Chrome | 13h 16m 21s | 9 |
| Podłączanie pulpitu zdalnego | 7h 33m 23s | 4 |
| SonicWall Global VPN Client | 6h 41m 12s | 6 |
| Eksplozator Windows | 4h 28m 27s | 30 |
| Vivaldi | 4h 19m 19s | 2 |
| Microsoft Excel | 2h 38m 41s | 12 |
| Microsoft Visual Studio 2019 | 1h 54m 01s | 2 |

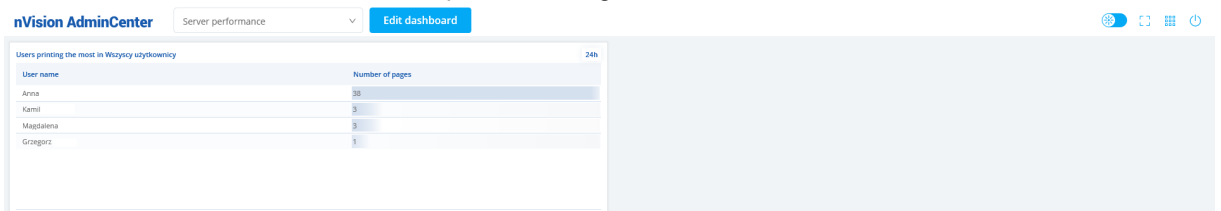
Users who print the most

The widget lists the users who have made the most prints in the last 24 hours.

The configuration requires the selection of the group of users for which the data are to be shown.



The screenshot below shows an example of the widget:



Users with highest bandwidth usage

The widget shows the statistics of bandwidth usage by users in the last 24 hours.

The configuration requires the selection of the group of users for which the data are to be shown and that the column by which the results are to be sorted is indicated.

← Add new widget



Select widget details for The highest bandwidth usage of users

SELECT AN ATLAS OR A GROUP

- Wszyscy użytkownicy
- > GRUPY
- > INTELIGENTNE GRUPY

ORDER RESULTS BY

WAN input

- WAN input
- WAN output
- LAN input
- LAN output

Cancel

Back

Add

The screenshot below shows an example of the widget:

nVision AdminCenter Server performance Edit dashboard

The highest bandwidth usage of users in Wszyscy użytkownicy 24h

| User name | Device | WAN Input | WAN Output | LAN Input | LAN Output |
|-----------|--------|-----------|------------|-----------|------------|
| | | 4.5 GB | 545.6 MB | 5.2 MB | 200.8 KB |
| | | 2.6 GB | 97.2 MB | 46.1 MB | 1.8 MB |
| | | 2.3 GB | 0 B | 3.7 MB | 0 B |
| | | 1.3 GB | 0 B | 3.1 MB | 0 B |
| | | 900.7 MB | 213.9 MB | 2.0 MB | 77.7 KB |
| | | 817.1 MB | 0 B | 844.0 KB | 0 B |
| | | 405.4 MB | 0 B | 6.8 MB | 0 B |
| | | 403.3 MB | 0 B | 10.9 MB | 0 B |
| | | 296.6 MB | 0 B | 12.2 MB | 0 B |
| | | 247.1 MB | 141.3 MB | 0 B | 0 B |

12.5.4.4 DataGuard module widgets

Last 10 devices attached

The widget lists the last 10 devices connected to machines with Agents.

The configuration requires the selection of the department or network map for which the events are to be shown. You can also narrow down the results by selecting the kind of device (trusted, untrusted, all) and the type of device (hard disk, floppy disk, etc.):

← Add new widget



Select widget details for The last 10 devices attached

SELECT ATLAS OR GROUP

Devices Users

- Wszystkie urządzenia (Atlas)
- > Sieci
- > Mapy użytkownika
- > Oddziały
- > Inteligentne mapy

SHOW DEVICES

All (trusted and untrusted) ▾

SHOW SELECTED DEVICE TYPES

Select all types

- Hard disk
- Floppy drive
- USB storage device
- Optical drive
- Storage device
- SD card
- Virtual volume
- Other

Cancel

Back

Add

The screenshot below shows an example of the widget:

nVision AdminCenter Server performance ▾ Edit dashboard

The last 10 devices attached (All) in the group Wszystkie urządzenia (Atlas)

| User name | Device | Device type | Device name | Date |
|-----------|--------|-------------|-------------------------------------|----------------------|
| | | Windows 10 | OneNote for Windows 10 | 2020/14/12, 01:35 PM |
| | | Windows 10 | SAMSUNG Mobile USB Modem | 2020/14/12, 12:31 PM |
| | | Windows 10 | Galaxy J5 (2016) | 2020/14/12, 12:31 PM |
| | | Windows 10 | OneNote for Windows 10 | 2020/14/12, 12:29 PM |
| | | Windows 10 | OneNote for Windows 10 | 2020/14/12, 11:48 AM |
| | | Windows 10 | SAMSUNG Mobile USB Modem | 2020/14/12, 11:53 AM |
| | | Windows 10 | Galaxy J5 (2016) | 2020/14/12, 11:53 AM |
| | | Windows 10 | HP w Support | 2020/14/12, 11:50 AM |
| | | Windows 10 | HP w Marketing | 2020/14/12, 11:50 AM |
| | | Windows 10 | SAMSUNG File-Stor Gadget USB Device | 2020/14/12, 10:59 AM |

Automatic dashboard refresh in 25 seconds. English ▾ Help Privacy policy Copyright © 2020 Axence sp. z o. o. sp. k

Last 10 operations on files

The widget lists the last 10 file operations for the selected department or map.

The configuration requires the selection of the department or network map for which the events are to be shown. You can also narrow down the results by selecting the type of file operations (created, modified, deleted, moved or renamed) and type of connected device:

← Edit widget



Select widget details for Last 10 file operations

SELECT ATLAS OR GROUP

Devices Users

- Wszystkie urządzenia (Atlas)
- Sieci
- Mapy użytkownika
- Oddziały
- Inteligentne mapy

SHOW SELECTED OPERATIONS ON FILES

Select all operations

Created

Deleted

Moved

Modified

Renamed

OPERATIONS ON DEVICES

All (trusted and untrusted) ▼

Select all types

Hard disk

USB storage device

Storage device

Virtual volume

Floppy drive

Optical drive

SD card

Other

Cancel

Back

Update

The screenshot below shows an example of the widget:

nVision AdminCenter ttt Edit dashboard 🌐 🔄 📱 🔌

Last 10 operations (All) on files (All (trusted and untrusted)) (USB storage device, Optical drive) in the group Wszystkie urządzenia (Atlas)

| User name | Device | Device type | Device name | Operation | Date |
|----------------|----------------------------|-------------|----------------------------------|-----------|----------------------|
| Piotr Wojtasik | PIWO-XP5(192.168.100.239) | Windows 10 | Wilk GOODRAM 2GB USB Device 2GB | Modified | 2021/02/03, 02:17 PM |
| Piotr Wojtasik | PIWO-XP5(192.168.100.239) | Windows 10 | Wilk GOODRAM 2GB USB Device 2GB | Created | 2021/02/03, 02:17 PM |
| Lukasz Piżuch | LukaszP-PC(192.168.40.152) | Windows 10 | ASMT 2115 USB Device 932GB | Modified | 2021/25/02, 10:47 AM |
| Lukasz Piżuch | LukaszP-PC(192.168.40.152) | Windows 10 | ASMT 2115 USB Device 932GB | Created | 2021/25/02, 10:47 AM |
| Lukasz Piżuch | LukaszP-PC(192.168.40.152) | Windows 10 | ASMT 2115 USB Device 932GB | Created | 2021/25/02, 10:47 AM |
| Piotr Wojtasik | PIWO-XP5(192.168.100.239) | Windows 10 | ASMT 2115 SCSI Disk Device 932GB | Created | 2021/23/02, 07:20 PM |
| Piotr Wojtasik | PIWO-XP5(192.168.100.239) | Windows 10 | ASMT 2115 SCSI Disk Device 932GB | Created | 2021/23/02, 07:20 PM |
| Piotr Wojtasik | PIWO-XP5(192.168.100.239) | Windows 10 | ASMT 2115 SCSI Disk Device 932GB | Created | 2021/23/02, 07:20 PM |
| Piotr Wojtasik | PIWO-XP5(192.168.100.239) | Windows 10 | ASMT 2115 SCSI Disk Device 932GB | Created | 2021/23/02, 07:20 PM |
| Piotr Wojtasik | PIWO-XP5(192.168.100.239) | Windows 10 | ASMT 2115 SCSI Disk Device 932GB | Created | 2021/23/02, 07:20 PM |

Automatic dashboard refresh in 56 seconds. English Help Privacy policy Copyright © 2021 Axence sp. z o. o. sp. k

12.5.4.5 HelpDesk module widgets

HelpDesk ticket statistics

The widget makes it possible to view a table with information on HelpDesk tickets in the last 24 hours. The configuration requires the selection of the properties by which tickets are to be grouped (priority, status or category):

← Add new widget



Select widget details for HelpDesk ticket statistics

SELECT A PROPERTY TO GROUP THE TICKETS BY

Priority ▼ ⓘ

Priority

Status

Category

Cancel

Back

Add

The screenshot below shows an example of the widget:

nVision AdminCenter Server performance Edit dashboard ⚙️ 🔄 📱 🔌

| HelpDesk tickets by priority | | 24h | |
|------------------------------|---------|-----|--|
| Priority | Tickets | | |
| Critical | 0 | | |
| High | 0 | | |
| Normal | 1 | | |
| Low | 0 | | |
| Trivial | 0 | | |

| HelpDesk tickets by status | | 24h | |
|----------------------------|---------|-----|--|
| Status | Tickets | | |
| New | 0 | | |
| Open | 0 | | |
| Waiting for response | 0 | | |
| Suspended | 1 | | |

Last 10 submitted tickets

The widget makes it possible to view a table with the last 10 tickets created in HelpDesk. No additional configuration is required for this widget.

The screenshot below shows an example of the widget:

The screenshot shows the 'The last 10 tickets submitted to HelpDesk' widget in the nVision AdminCenter. The table contains the following data:

| ID | Priority | Status | Category | Requester | Assignee | Subject |
|------|----------|----------------------|------------|-----------|----------|---|
| 1360 | Normal | Suspended | Komputer | | | Callisto - zmiana przeznaczenia - informacje i wykonane działania |
| 1358 | Normal | Suspended | Komputer | | | Analiza błądów/działania Laptopa Dell Latitude E5570. |
| 1356 | High | Suspended | Komputer | | | bardzo niska głośność głośnika w laptopie |
| 1353 | Normal | Suspended | ***Ogólne | | | Przeniesienie stanowiska pracy Pawła |
| 1352 | Normal | Suspended | Komputer | | | Konfiguracja komputera dla Grzegorz Wik w firmie na 2021 |
| 1333 | Normal | Suspended | Komputer | | | komputer się restartuje bez powodu |
| 1309 | Normal | Suspended | ***Ogólne | | | Nie działa DNS na maszynie wirtualnej |
| 1302 | Normal | Open | Inne | | | Zakup wyposażenia dla DSW: słuchawki i telefony komórkowe |
| 1301 | Normal | Suspended | Telefon IP | | | Ciągły restart telefonu cd |
| 1299 | Normal | Waiting for response | Komputer | | | Blokowanie komputera bez przyczyny |

The oldest 10 opened tickets

The widget makes it possible to view a table with the 10 oldest tickets opened in the HelpDesk module.

No additional configuration is required for this widget.

The screenshot below shows an example of the widget:

The screenshot shows the 'The oldest 10 tickets open in HelpDesk' widget in the nVision AdminCenter. The table contains the following data:

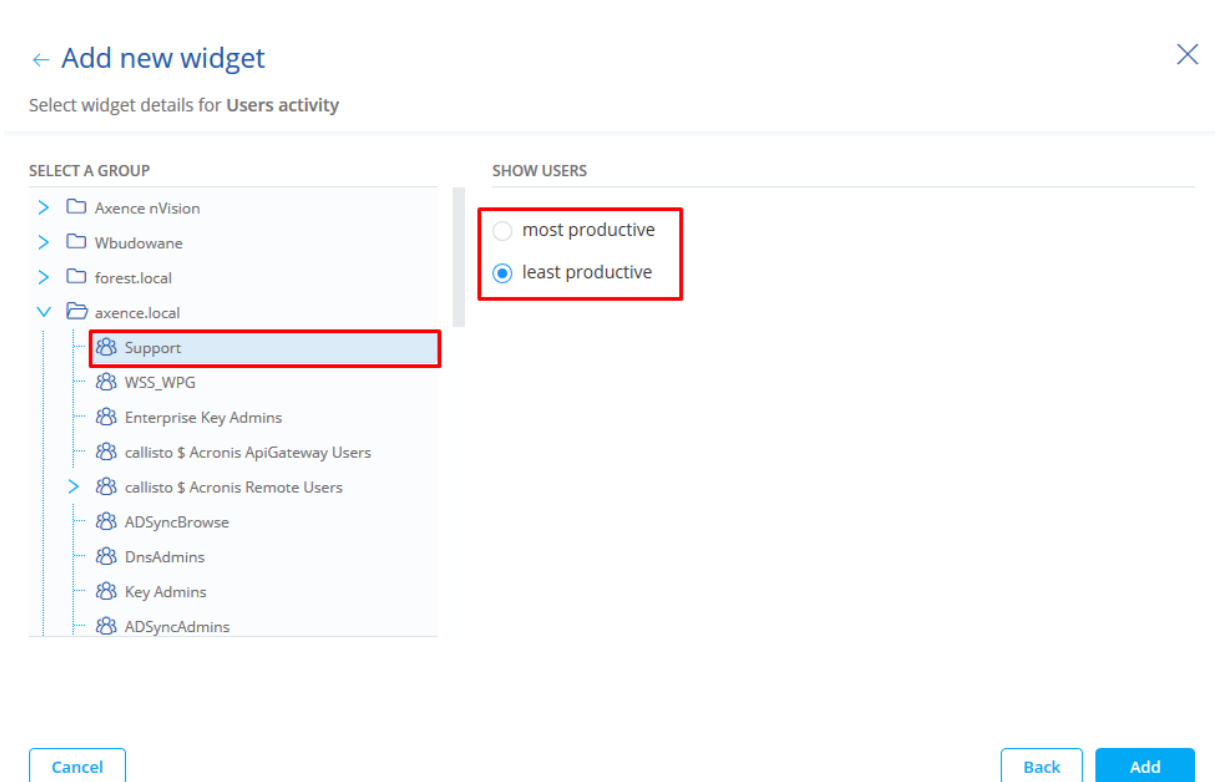
| Date | ID | Priority | Category | Requester | Assignee | Subject |
|----------------------|------|----------|-------------------|-----------|----------|---|
| 2017/19/07, 04:24 PM | 224 | Normal | Dostępny do usług | | | Zmiana hasła |
| 2019/10/06, 06:23 AM | 880 | Normal | Dostępny do usług | | | Resolwacja nazw DNS |
| 2020/27/03, 01:31 PM | 1170 | Normal | Inne | | | Poczta i Teams na tel priv |
| 2020/24/04, 07:01 AM | 1198 | Normal | Aplikacja | | | VPN - rozłączanie |
| 2020/09/10, 12:45 PM | 1295 | Normal | Inne | | | Uszkodzony kabel HDMI w s. konf. X.p. |
| 2020/12/10, 02:45 PM | 1299 | Normal | Komputer | | | Blokowanie komputera bez przyczyny |
| 2020/13/10, 12:58 PM | 1301 | Normal | Telefon IP | | | Ciągły restart telefonu cd |
| 2020/15/10, 04:34 PM | 1302 | Normal | Inne | | | Zakup wyposażenia dla DSW: słuchawki i telefony komórkowe |
| 2020/20/10, 11:12 AM | 1309 | Normal | ***Ogólne | | | Nie działa DNS na maszynie wirtualnej |
| 2020/19/11, 05:44 AM | 1333 | Normal | Komputer | | | komputer się restartuje bez powodu |

12.5.4.6 SmartTime module widgets

User activity

The widget shows a table representing the activity and productivity of users in a selected group.

The configuration requires the selection of a group of users and the way in which the results are to be sorted (the most productive or the most unproductive users):



The screenshot below shows an example of the widget:

| User name | Productivity | Productive time | Work time | At the computer | Away from the computer |
|-----------|--------------|-----------------|------------|-----------------|------------------------|
| | 96% | 3h 50m 29s | 4h 28m 30s | 3h 59m 54s | 28m 36s |
| | 97% | 3h 18m 21s | 4h 38m 57s | 3h 23m 46s | 1h 15m 11s |
| | 97% | 3h 52m 53s | 4h 40m 16s | 3h 57m 56s | 42m 20s |

Users with longest unproductive time

The widget shows the top 10 users with the longest unproductivity time in a selected group of users. The configuration requires the election of the group of users for which the data are to be shown.

← Add new widget



Select widget details for Users with the most unproductive time

SELECT A GROUP

> Axence nVision

▼ Wbudowane

- Storage Replica Administrators
- RDS Endpoint Servers
- Certificate Service DCOM Access
- Access Control Assistance Operators
- Users**
- Backup Operators
- IIS_IUSRS
- Event Log Readers
- Server Operators

Cancel

Back

Add

The screenshot below shows an example of the widget:

nVision AdminCenter Server performance Edit dashboard

The users with the most unproductive time in the group Users

| User name | Unproductive time | Productive time | Work time | At the computer | Away from the computer |
|-----------|-------------------|-----------------|-------------|-----------------|------------------------|
| | 36m 18s | 3h 49m 10s | 5h 38m 14s | 4h 47m | 51m 14s |
| | 22m 01s | 2h 58m 06s | 13h 11m 56s | 3h 39m 10s | 9h 32m 46s |
| | 15m 45s | 3h 41m 45s | 4h 56m 04s | 4h 09m | 47m 04s |
| | 9m 46s | 4h 58m 10s | 5h 42m 21s | 5h 12m 38s | 29m 43s |
| | 4m 43s | 3h 13m 35s | 4h 46m 03s | 3h 42m 16s | 1h 03m 47s |
| | 3m 35s | 3h 06m 28s | 5h 43m 57s | 3h 26m 19s | 2h 17m 38s |
| | 2m 37s | 4h 26m 52s | 5h 48m 17s | 4h 35m 56s | 1h 12m 21s |
| | 0m 42s | 4h 41m 05s | 5h 24m 43s | 4h 58m 28s | 26m 15s |
| | 0m 27s | 3h 52m 53s | 4h 40m 16s | 3h 57m 56s | 42m 20s |
| | 0m 19s | 4h 30m 59s | 5h 30m 33s | 5h 02m 49s | 27m 44s |

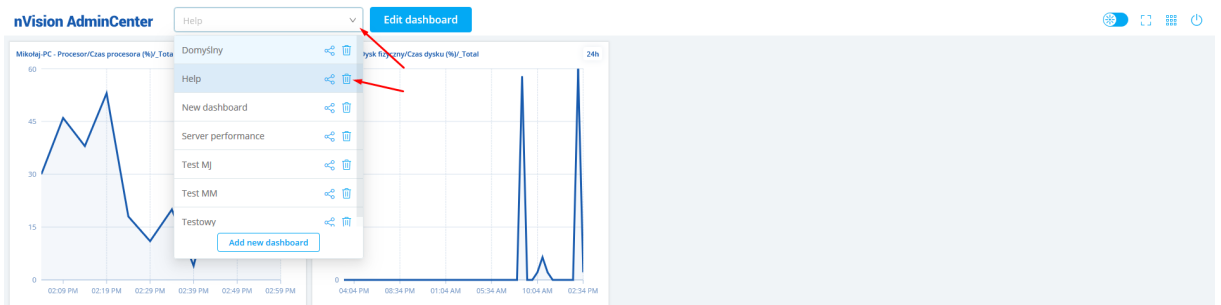
Automatic dashboard refresh in 51 seconds.

English Help Privacy policy Copyright © 2020 Axence sp. z o. o. sp. k

12.5.5 Deleting a dashboard

Delete an existing dashboard in the following way:

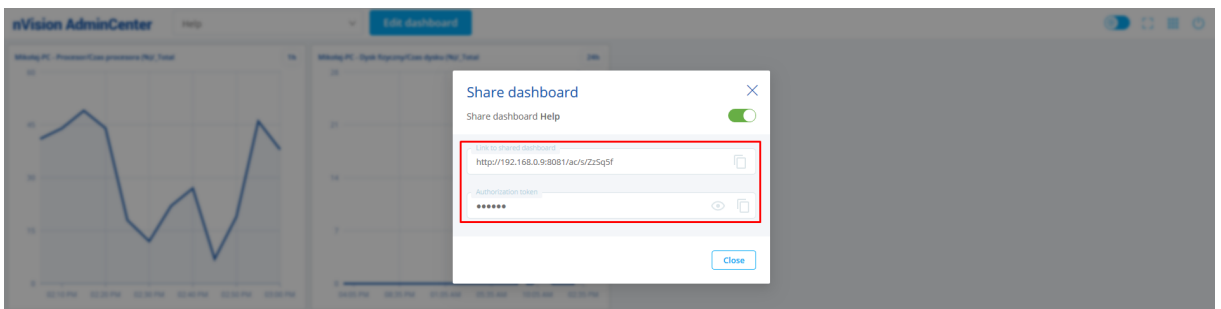
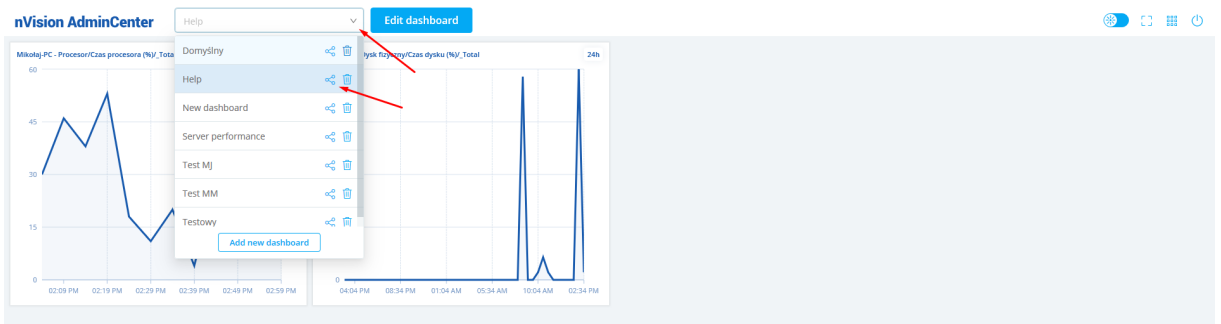
1. Expand the list of available dashboards by clicking the box at the top of the screen.
2. Click the trash can icon next to the item to be deleted.
3. Confirm the deletion by clicking the **Delete** button.



12.5.6 Sharing a dashboard

Sharing a dashboard

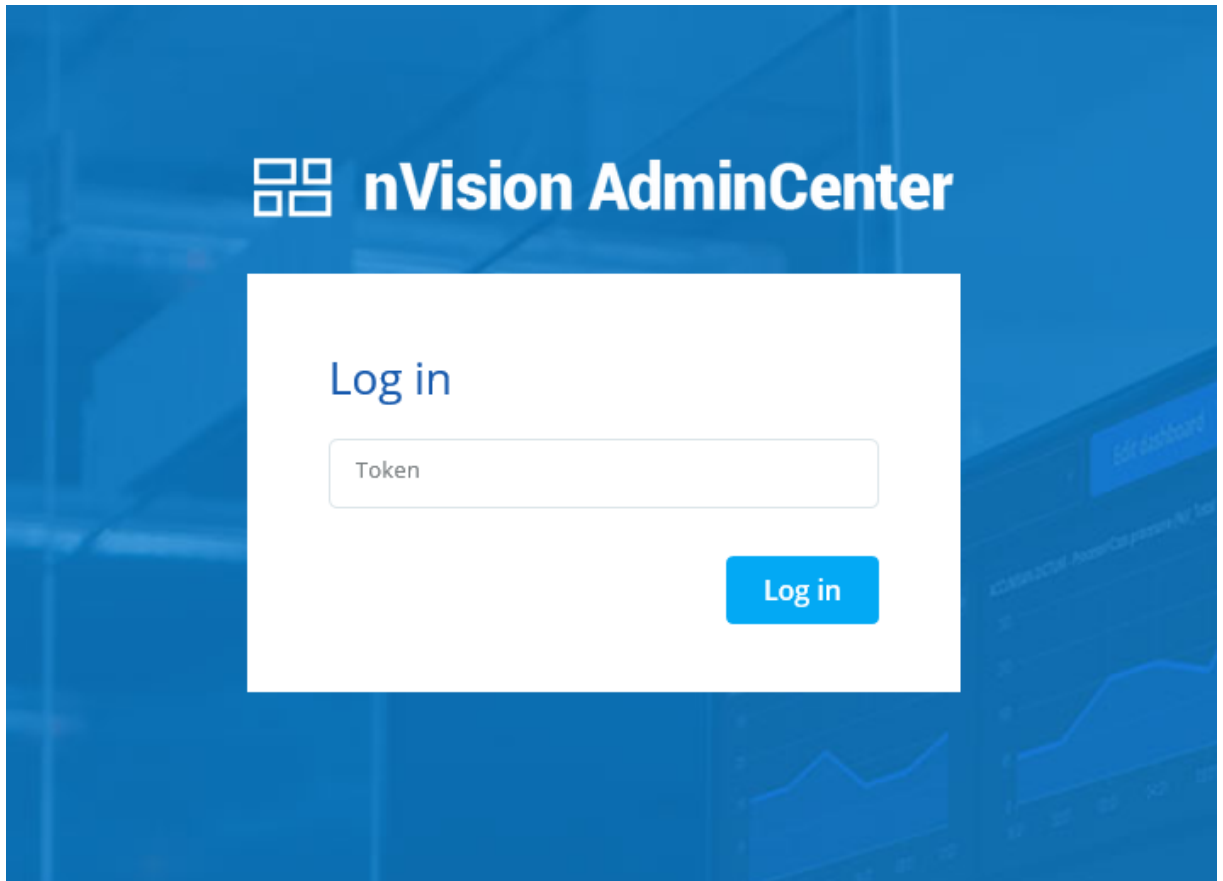
1. Share a dashboard in read-only mode with **any user** in the following way:
2. Press the **share** button next to the dashboard you want to share.
3. Move the **Share dashboard** slider. A unique link and access token allowing access to the dashboard will be displayed.
4. Copy the unique link and the access token and give them to the person who is to access the dashboard.



Opening a shared dashboard

Run a shared dashboard in the following way:

1. Use the link generated when sharing the dashboard to view it in your browser.
2. Enter the dashboard access token and click **Log in**.

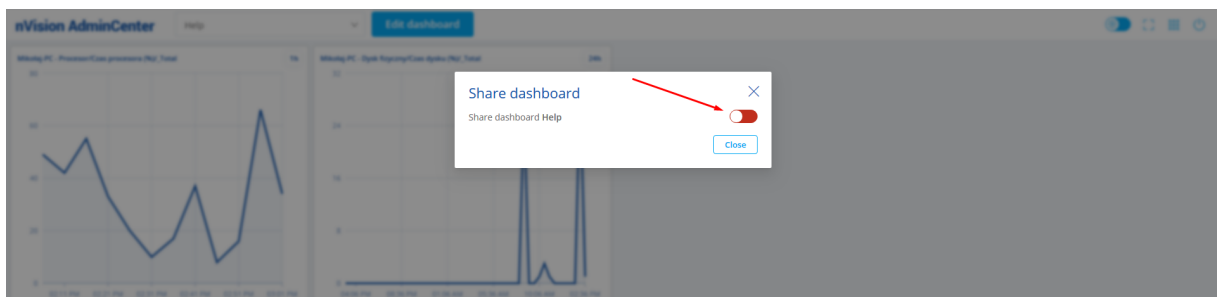
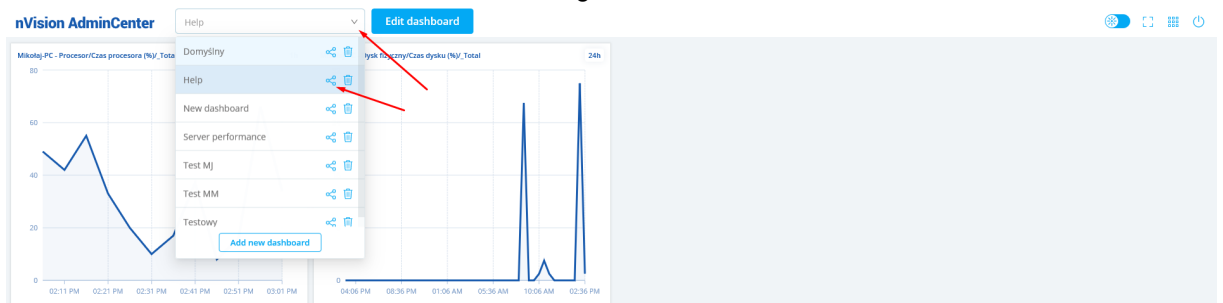


Once you have completed the steps above, the dashboard will be displayed without the ability to edit it. **It is not possible to share editable dashboards.**

Disabling the sharing of a dashboard

Disable the sharing of a dashboard in the following way:

1. Expand the list of available dashboards by clicking the box at the top of the screen.
2. Press the share button next to the dashboard which is currently shared.
3. Move the Share dashboard slider. The sharing of the dashboard will be disabled.



Part



13 Reports

13.1 Introduction

Axence nVision® includes very advanced, printable reports. There are several predefined reports, providing the most important information for every host and map. You can also easily create your own reports: read more in the [Creating reports](#) ⁵⁶⁰ topic.

Opening the report management window

Click the **Reports** button located in the navigation bar. This will open the report management window allowing you to view, print and create new reports.

nVision has several pre-defined basic reports. The administrator can also create their own reports, depending on their needs.

Viewing and printing reports

To prepare a report for a host, map, user or group:

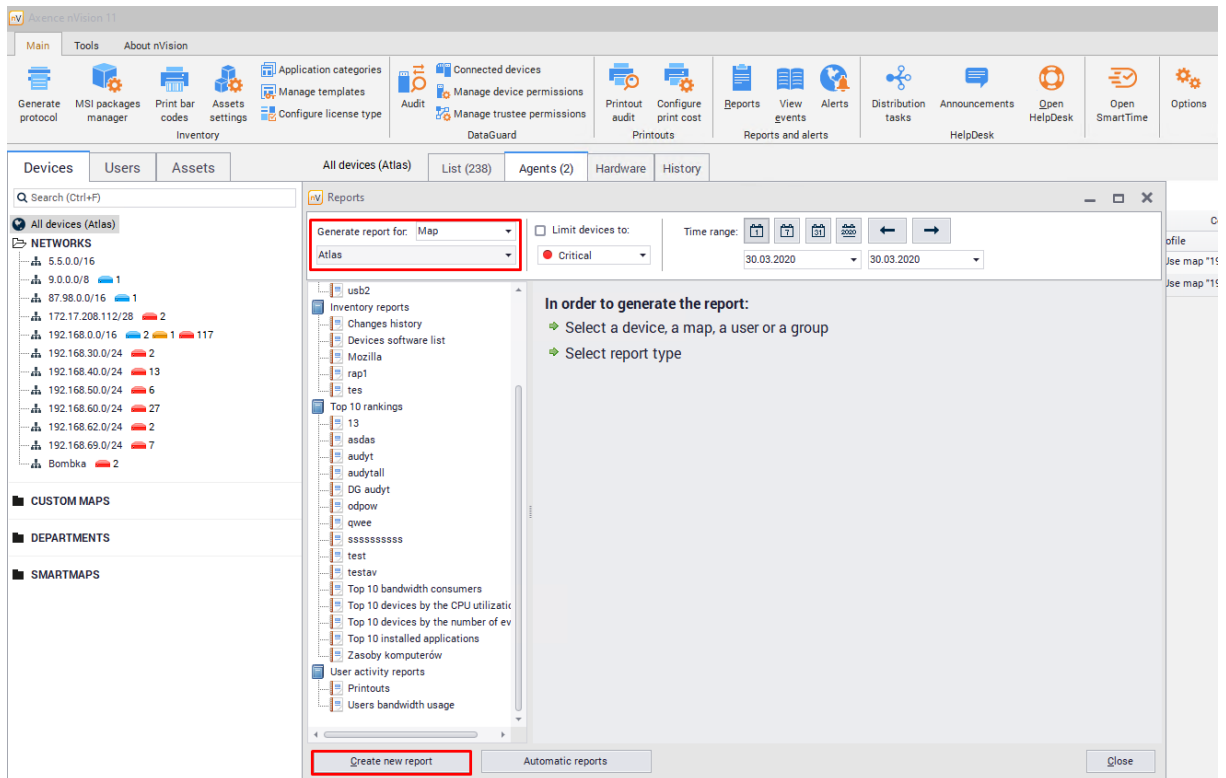
1. Select report type. There are different report types defined for a host, map, user and group.
2. Select a host/user or a map/group (depending on the choice you made in the previous step).
3. Select the report on the left side bar.
4. Select the time period of the report.
5. Click the **Prepare and show report** button. This button is displayed only when this report has never been prepared. Once it is ready, it will show automatically when you define the same options. It may only need an update if the data has changed (i.e. if the report included the current day).
6. After the report is prepared, you can print it by clicking the **Print** button located on the report toolbar.


13.2 Creating reports

Axence nVision® very easily allows creating new reports. You just construct them by selecting several predefined segments. Segments are data collectors, which collect data gathered by nVision and process it to present it in grids and on charts.

To create your own report:

1. Open the report management window by clicking the **Reports** button located in the navigation bar.
2. Select the **Host, Map, User** or **Group** item which defines the type of report to be created.
3. Select the category in which you would like the report to be created.
4. Click the **New report** button located in the bottom part of the window.



5. Enter the report name and description.
6. Add a new segment by clicking the  button located on the left side.
7. Enter the segment name and select segment type. Refer to the [Segment types for hosts](#)^[562] or [Segment types for maps](#)^[569] topic for more information.
8. Enter appropriate options as described in the [Segment types for hosts](#)^[562] or [Segment types for maps](#)^[569] topic.
9. Enter short and long descriptions. These descriptions will be shown above and below the segment on the report, respectively.

13.3 Segment types for host reports

This topic describes different host report segment types and defines their properties (if required).

Headers

Report header

Header with report details. This should be the first segment of every report.

Services

Services - general information

Lists all host services with the most important performance information.

Service performance chart

Presents charts with the response time and percent of packets lost of the selected or all services.

| Property | Description |
|-------------------------------|--|
| Generate for specific service | The chart will be generated only for the specified service. If it is not available on the host, then this segment will not be generated. |
| Generate for all services | The chart will be generated for every service available on the host. |
| Data presentation | Data may be presented in a normal way, distributed by hours of the day or by days of the week. |
| Show as | Defines how the chart will look like: <ul style="list-style-type: none"> • Service response time chart (default) – specialized chart designed to show response time and percent of lost packets on one chart. • Line chart • Table. |

Service think time

Presents the chart of service response compared to ping response.

Same properties as described in the table above.

Services – up/down time

Time when services are up and down.

Counters



Performance counters

List of all performance counters for a given host.



Performance counter chart

Presents a chart of counter values over time.

| Property | Description |
|-------------------|--|
| Counter | The chart will be generated for the selected counter. If it is not available on the host, then this segment will not be generated. |
| Data presentation | Data may be presented in a normal way, distributed by hours of the day or by days of the week. |
| Show as | Defines how the chart will look like: <ul style="list-style-type: none"> • Line chart • Area chart • Vertical bar chart • Table. |



Interface bandwidth

Shows bandwidth on every interface. May be presented in a table or multi-line chart.



Host counters list

Demonstrates a list of all counters for a particular host.



Total time of counter state or value

| Property | Description |
|----------|---|
| Counter | The chart will be generated for the selected counter. |
| Show as | Defines how the chart will look like: <ul style="list-style-type: none"> • Pie chart • Table. |



Min/max/avg uninterruptible counter state or value


This segment presents minimal, maximal and average uninterruptible counter state or value.

Services and counters



Distribution of range values

Presents a range of values for the selected counter or service.

| Property | Description |
|-------------|---|
| Data source | Optional: counter or service. |
| Data ranges | To add a new range, click the  button, give the title of the created range and provide boundary values. |
| Show as | Defines how the chart will look like: <ul style="list-style-type: none"> • Vertical bar chart • Pie chart • Table. |

Alerts



Most frequent events

A list of events sorted by their frequency.

| Property | Description |
|---------------------------------|---|
| Limit listing to x first events | Use this option if you want to constrain the list of events presented in the report. |
| Show as | Defines how the chart will look like: <ul style="list-style-type: none"> • Horizontal bar chart • Vertical bar chart • Pie chart • Table. |



Event log

Presents all event log entries for the selected time range.

**Number of alerts over time**

| Property | Description |
|-------------------|--|
| Data source | This segment may contain all events or one, selected from the list of events. |
| Data presentation | Data may be presented in a normal way, distributed by hours of the day or by days of the week. |
| Show as | Defines how the chart will look like: <ul style="list-style-type: none"> • Line chart • Table. |

**Total time of alert activeness / inactiveness**

Presents the total time when the selected alert was active.

**Min/max/avg event / no event time**

| Property | Description |
|--------------------|---|
| Data source | This segment may contain all events or one, selected from the list of events. |
| Calculate data for | The time of alert activeness or inactiveness may be calculated. |

**Windows event log**

Presents a list of entries in the Windows Event Log for selected hosts.

User monitoring**Printout audit**

Presents information about printed documents: not grouped or grouped by user, host or printer, sorted in the selected way.

**Bandwidth usage**

| Property | Description |
|----------|---|
| Display | What type of information will be presented: <ul style="list-style-type: none"> • Map / Atlas summary |

| Property | Description |
|------------------|---|
| | <ul style="list-style-type: none"> • Host details • Users ranking • Hosts ranking |
| Sort by | Data may be sorted according to connections: <ul style="list-style-type: none"> • with Internet, in • with Internet, out • local, in • local, out |
| Ranking settings | In order to obtain information about groups of protocols select option Show protocol groups details . |

Inventory



Changes in installed applications and hardware

Presents a list of changes in installed applications and hardware. May include add, remove and change operations for selected groups.



Hardware configuration

Hardware configuration may be presented in two ways – with selected view or selected columns. Available views enable presentation of overview information, multimedia, drives and other.



Host(s) software list

| Property | Description |
|---------------------|---|
| Show | Select the type of software that will be included in the report (software, updates, drivers). |
| License type | Software with the selected license type will be presented. |
| Show serial numbers | Select if you want serial numbers to be presented in the report. |
| Show licenses | Select if you want licenses to be presented in the report. |



Applications on hosts

Lists all hosts with installed applications, drivers and updates with selected license types.

| Property | Description |
|----------|---|
| Show | Select the type of software that will be included in the report |

| Property | Description |
|--------------|--|
| | (software, updates, drivers). |
| License type | Software with the selected license type will be presented. |



Fixed assets list

Presents a list of all fixed assets for Map/Atlas.

| Property | Description |
|---------------------------|---|
| Show | Select types of assets that will be included in this segment. |
| Show common fields | Common fields are: value, in maintenance, in warehouse, person responsible and inventory number. |
| Show type-specific fields | If marked, fields existing only for specific types will be presented. |
| Group by | Fixed assets may be grouped by: <ul style="list-style-type: none"> • (None) • Asset type • Belongs to • Name. |



Host's fixed assets list

Presents a list of all fixed assets for selected host(s).



Host's custom files list

Presents list of all Custom Files found on host(s)

| Property | Description |
|----------|--|
| Mask | Check this box if you want to search files that match to a given mask. |
| Size | You can set a minimum and maximum size of files. |
| Category | You can choose one or more out of the following options: <ul style="list-style-type: none"> • Audio • Video • Graphic • Other files. |
| Is legal | Shows result only for legal/illegal files. |



System information

Presents a list of startup commands, network shares or task schedule for specific hosts.

Others



Host status timeline

Table presenting all hosts status changes over time.



Host up/down time

Percent of host up/downtime.

| Property | Description |
|----------|--|
| Show as | Defines how the data will be presented: <ul style="list-style-type: none">• Horizontal bar chart• Vertical bar chart• Pie chart• Table. |



General host info

General information about the selected host.



Port mapper

Port mapper table.

DataGuard



DataGuard audit

Presents information about operations performed on protected files. Data may be presented for a specified user or device. The following operations may be included: device connected, device disconnected, file created, file renamed, file deleted, file written.



DataGuard known devices

List of devices used in network.

13.4 Segment types for map reports

This topic describes different map report segment types and defines their properties (if required).

Headers



Report header

Header with report details. This should be the first segment of every report.

Services



Services - general information

Lists all host services with the most important performance information.



Best/worst hosts by service performance

Lists hosts with the shortest or the longest response time.

| Property | Description |
|------------------------------------|--|
| Service | Select a service on the basis of which the devices will be compared. If a device does not have the selected service, it will not be included for comparison. |
| Sort by percentage of lost packets | The results will be sorted by the percentage of lost packets instead of response time. |
| Show the best devices | Select this option if you want to see the best devices (with the shortest response time or the lowest percentage of lost packets). |
| Show the worst devices | Select this option if you want to see the worst devices. |
| Limit the list | Select this option if you want to limit the number of devices displayed. |
| Show as | Determines how the segment will be presented: <ul style="list-style-type: none">• Horizontal bar chart• Vertical bar chart• Table. |



Service performance chart

Presents charts with the response time and percent of packets lost of the selected or all services.

| Property | Description |
|-------------------------------|--|
| Generate for specific service | The chart will be generated only for the specified service. If it is not available on the host, then this segment will not be generated. |
| Generate for all services | The chart will be generated for every service available on the host. |
| Show as | Defines how the chart will look like: <ul style="list-style-type: none"> • Service response time chart (default) – specialized chart designed to show response time and percent of lost packets on one chart. • Line chart • Table. |



Service think time

Presents the chart of service response compared to ping response.

Same properties as described in the table above.



Services – up/down time

Time when services are up and down.

Counters



Performance counters

List of all performance counters for a given host.



Performance counter chart

Presents a chart of counter values over time.

| Property | Description |
|----------|--|
| Counter | The chart will be generated for the selected counter. If it is not available on the host, then this segment will not be generated. |
| Show as | Defines how the chart will look like: <ul style="list-style-type: none"> • Line chart • Area chart • Vertical bar chart • Table. |



Best/worst hosts by the performance counter

Lists hosts with the best or the worst performance.

| Property | Description |
|------------------------|--|
| Performance counter | Select the performance counter on the basis of which the devices will be compared. If a device does not have a chosen performance counter, it will not be included for comparison. |
| Show the best devices | Select this option if you want to see a list of the best devices (with the lowest value of the performance counter). |
| Show the worst devices | Select this option if you want to see a list of the worst devices. |
| Limit the list | Enable this option if you want to limit the number of devices presented in the list. |
| Show as | Determines how the segment will be presented: <ul style="list-style-type: none"> • Horizontal bar chart • Vertical bar chart • Table. |



Interface bandwidth

Shows bandwidth on every interface. May be presented in a table or multi-line chart.



Host counters list

Demonstrates a list of all counters for a particular host.



Total time of counter state or value

| Property | Description |
|----------|---|
| Counter | The chart will be generated for the selected counter. |
| Show as | Defines how the chart will look like: <ul style="list-style-type: none"> • Pie chart • Table. |



Min/max/avg uninterruptible counter state or value

This segment presents minimal, maximal and average uninterruptible counter state or value.



Most/least available hosts by specific counter state or value

This segment presents the most/least available hosts by a specific counter state or value.



Most/least available hosts by longest uninterrupted counter state or value


This segment presents the best/worst hosts. You can also limit list length to first x applications.

Services and counters



Distribution of range values

Presents a range of values for the selected counter or service.

| Property | Description |
|-------------|--|
| Data source | Optional: counter or service. |
| Data ranges | To add a new range, click the  button, give the title of the created range and provide boundary values. |
| Show as | Defines how the chart will look like: <ul style="list-style-type: none"> • Vertical bar chart • Pie chart • Table. |

Alerts



Best/worst hosts by the number of events

Presents the most or least problematic hosts by the number of alerts.

| Property | Description |
|---------------------------------|---|
| Generate for all events | Compares the devices in terms of the number of occurrences of all events. |
| Generate for the selected event | Compares the devices in terms of the occurrences of the selected event. |
| Show the best devices | Select this option if you want to see the best devices (with the smallest number of events) |
| Show the worst devices | Select this option if you want to see the worst devices (with the most number of alarms). |
| Limit to | Enable this option if you want to limit the number of devices presented. |

| Property | Description |
|----------|--|
| Show as | Determines how the segment will be presented: <ul style="list-style-type: none"> • Horizontal bar chart • Vertical bar chart • Table. |



Most frequent events

A list of events sorted by their frequency.

| Property | Description |
|---------------------------------|---|
| Limit listing to x first events | Use this option if you want to constrain the list of events presented in the report. |
| Show as | Defines how the chart will look like: <ul style="list-style-type: none"> • Horizontal bar chart • Vertical bar chart • Pie chart • Table. |



Event log

Presents all event log entries for the selected time range.



Number of alerts over time

| Property | Description |
|-------------------|--|
| Data source | This segment may contain all events or one, selected from the list of events. |
| Data presentation | Data may be presented in a normal way, distributed by hours of the day or by days of the week. |
| Show as | Defines how the chart will look like: <ul style="list-style-type: none"> • Line chart • Table. |



Total time of alert activeness / inactiveness

Presents the total time when the selected alert was active.

**Min/max/avg event / no event time**

| Property | Description |
|--------------------|---|
| Data source | This segment may contain all events or one, selected from the list of events. |
| Calculate data for | The time of alert activeness or inactiveness may be calculated. |

**Windows event log**

Presents a list of entries in the Windows Event Log for selected hosts.

User monitoring**Printout audit**

Presents information about printed documents: not grouped or grouped by user, host or printer, sorted in the selected way.

**Bandwidth usage**

| Property | Description |
|------------------|---|
| Display | What type of information will be presented: <ul style="list-style-type: none"> • Map / Atlas summary • Host details • Users ranking • Hosts ranking |
| Sort by | Data may be sorted according to connections: <ul style="list-style-type: none"> • with Internet, in • with Internet, out • local, in • local, out |
| Ranking settings | In order to obtain information about groups of protocols select option Show protocol groups details . |

Inventory



Software inventory audit

Presents a list of installed applications.

| Property | Description |
|--------------------|--|
| Show | Defines the type of software that will be included in the report: only the applications and OSs, or also the updates the drivers. |
| License | Use the list to select the license types that will be included in the report. |
| License compliance | Select: <ul style="list-style-type: none"> • all • with assigned licenses • without assigned licenses • license number sufficient or redundant • license number deficit |



Changes in installed applications and hardware

Presents a list of changes in installed applications and hardware. May include add, remove and change operations for selected groups.



Hardware configuration

Hardware configuration may be presented in two ways – with selected view or selected columns. Available views enable presentation of overview information, multimedia, drives and other.



Host(s) software list

| Property | Description |
|---------------------|---|
| Show | Select the type of software that will be included in the report (software, updates, drivers). |
| License type | Software with the selected license type will be presented. |
| Show serial numbers | Select if you want serial numbers to be presented in the report. |
| Show licenses | Select if you want licenses to be presented in the report. |





Top installed applications

| Property | Description |
|------------------|---|
| Limit listing to | You can limit list length to first x applications. |
| Show | Select the type of software that will be included in the report (software, updates, drivers). |
| License type | Software with the selected license type will be presented. |



Hosts with applications installed

Hosts which (optionally) have or do not have the selected applications installed are shown. A list of selected applications is shown in the lower part of the window. To add an application, click it and press the  button. To remove an application from the list, click it and press the  button.



Applications on hosts

Lists all hosts with installed applications, drivers and updates with selected license types.

| Property | Description |
|--------------|---|
| Show | Select the type of software that will be included in the report (software, updates, drivers). |
| License type | Software with the selected license type will be presented. |



Fixed assets list

Presents a list of all fixed assets for Map/Atlas.

| Property | Description |
|----------|---|
| Show | Select the types of fixed assets that will be included in the report. |
| Group by | Fixed assets may be grouped by: <ul style="list-style-type: none"> • (None) • Asset type • Belongs to • Name. |



Host's fixed assets list

Presents a list of all fixed assets for selected host(s).



Host's customs files list

Presents list of all Custom Files found on host(s)

| Property | Description |
|----------|--|
| Mask | Check this box if you want to search files that match to a given mask. |
| Size | You can set a minimum and maximum size of files. |
| Category | You can choose one or more out of the following options: <ul style="list-style-type: none"> • Audio • Video • Graphic • Other files. |
| Is legal | Shows result only for legal/illegal files. |



System information

Presents a list of startup commands, network shares or task schedule for specific hosts.

Others



Host status timeline

Table presenting all hosts status changes over time.



Host up/down time

Percent of host up/downtime.

| Property | Description |
|----------|---|
| Show as | What type of information will be presented: <ul style="list-style-type: none"> • Horizontal bar chart • Vertical bar chart • Pie chart • Table. |



General host info

General information about the selected host. You can select the type of hosts and additional information to be displayed:

- addresses and interfaces
- SNMP information
- monitoring
- monitoring time
- alerts.



Port mapper

Port mapper table.




Map View

Presents a graphical view of the map.



Maps' uptime summary

This segment shows the total number of devices whose uptime value is in between the ranges you define. Ranges points are defined by clicking the  **Add point** button.

Example

Adding points 10, 50 and 90 results in creating four intervals:

1. Uptime $\geq 0\%$ and $< 10\%$
2. Uptime $\geq 10\%$ and $< 50\%$
3. Uptime $\geq 50\%$ and $< 90\%$
4. Uptime $\geq 90\%$ and $\leq 100\%$

DataGuard



DataGuard audit

Presents information about operations performed on protected files. Data may be presented for a specified user or device. The following operations may be included: device connected, device disconnected, file created, file renamed, file deleted, file written.



DataGuard known devices

List of devices used in network.

13.5 Segment types for user reports

The following chapter describes the types of segments in user reports and their properties (if necessary).

User monitoring



User activity

Presents general information about the user's work time. The user activity report can be displayed as a separate segment for each user or as an overview list.



Visited websites

Presents a list of websites visited by users on a host. You may narrow down the list to websites that match a given mask.



Websites ranking

Shows a ranking of visited websites with the possibility to limit the list to x first websites. Data may be sorted by the total time or the number of visits.



Breaks in work time

Presents a list of breaks in work time for the selected host.



Application usage timeline

Presents the timeline of application usage by users.



Summary application usage

Presents the summary application usage for the selected Map/Atlas or host.



Bandwidth usage

| Property | Description |
|----------|---|
| Display | What type of information will be presented: <ul style="list-style-type: none"> • Map / Atlas summary • Host details • Users ranking • Hosts ranking |

| Property | Description |
|------------------|---|
| Sort by | Data may be sorted according to connections: <ul style="list-style-type: none"> • with Internet, in • with Internet, out • local, in • local, out |
| Ranking settings | In order to obtain information about groups of protocols select option Show protocol groups details . |



List of e-mails

Presents a list of e-mails sent or received by users.



Summary of e-mails

Presents summary information about e-mails. E-mails can be sorted by sent, received and size.



Printout audit

Presents information about printed documents: not grouped or grouped by user, host or printer, sorted in the selected way.



Printing costs

This segment shows information about print cost.



User configuration

Presents the monitoring or blocking configuration for the user.

DataGuard



DataGuard access rights

Presents the information about access rights to DataGuard devices.

13.6 Segment types for group reports

The following chapter describes the types of segments in user group reports and their properties (if necessary).

User monitoring



User activity

Presents general information about the user's work time. The user activity report can be displayed as a separate segment for each user or as an overview list.



Visited websites

Presents a list of websites visited by users on a host. You may narrow down the list to websites that match a given mask.



Websites ranking

Shows a ranking of visited websites with the possibility to limit the list to x first websites. Data may be sorted by the total time or the number of visits.



Breaks in work time

Presents a list of breaks in work time for the selected host.



Application usage timeline

Presents the timeline of application usage by users.



Summary application usage

Presents the summary application usage for the selected Map/Atlas or host.



Bandwidth usage

| Property | Description |
|----------|--|
| Display | What type of information will be presented: <ul style="list-style-type: none">• Map / Atlas summary• Host details• Users ranking• Hosts ranking |
| Sort by | Data may be sorted according to connections: <ul style="list-style-type: none">• with Internet, in• with Internet, out |

| Property | Description |
|------------------|--|
| | <ul style="list-style-type: none"> • local, in • local, out |
| Ranking settings | In order to obtain information about groups of protocols select option Show protocol groups details . |



Website visitors ranking

Presents the ranking of website visitors.

| Property | Description |
|------------------------------------|--|
| Show ranking for selected option | Select this option if you want to display the ranking for websites matching the mask specified below. |
| Display | Select: hosts or users which visited the given website. |
| Limit listing to x first web sites | Use this option if you want to constrain the list of websites presented in the report. |
| Sort by | Data can be sorted by: <ul style="list-style-type: none"> • the total time • the number of visits. |



Application usage statistics

| Property | Description |
|-------------------|--|
| Application group | Information will be displayed for the selected groups of applications: <ul style="list-style-type: none"> • instant messengers, • web browsers • text editors • e-mail • programming • multimedia. |
| Executable file | Use the list to select the executable file the running of which is to be included in the segment. |
| Sort by | Data can be sorted by: <ul style="list-style-type: none"> • users • application usage time • application run time. |

| Property | Description |
|----------------------------------|--|
| Limit listing to x first records | Use this option if you want to constrain the list presented in the report. |



Application usage time statistics

Presents the application usage time statistics for the map.

| Property | Description |
|-------------------|---|
| Application group | Information will be displayed for the selected groups of applications: <ul style="list-style-type: none">• instant messengers,• web browsers• text editors• e-mail• programming• multimedia. |
| Executable file | Use the list to select the executable file the running of which is to be included in the segment. |



List of e-mails

Presents a list of e-mails sent or received by users.



Summary of e-mails

Presents summary information about e-mails. E-mails can be sorted by sent, received and size.



Printout audit

Presents information about printed documents: not grouped or grouped by user, host or printer, sorted in the selected way.



Printing costs

This segment shows information about print cost.

Part



14 Alerting

14.1 Introduction

This part describes how to use the alerting policies available in nVision. With alerting you can be notified in case of any problems in your network. When a host stops responding, when a service has a slower response or when some applications are having problems, nVision may send you a message, show the information on the screen, or even run a corrective action.

How it works

First, you have to define a set of events. The example of such an event is when a host stops responding. nVision will constantly monitor all hosts to check if any of the defined events took place on them. In our example the event will be raised when all services running on the host do not respond.

Now, we have an event but what should the program do with this event? We need to define a set of actions which can be run in case of the event happening. When events and actions are defined, then we can set alerts. The alert defines which actions should be executed if a specific event takes place.

All raised alerts are logged in the database so you could prepare reports about your network performance. If you would like to collect the information about a specific event, but you don't want any actions to be executed, then you need to define an alert with this event but with no actions. It will tell nVision to just collect those events to the database.

Let's summarize the process of setting the alert:

1. Create an event. The occurrence of such event will trigger an alert. Examples of events: host down, service performance problem, web page load time over a threshold, etc.
2. Create notification and corrective actions. You should create actions to be run when an event occurs. Example of actions: sending an e-mail or ICQ message, running an external application, restarting of Windows service, etc. This step is optional - you can create the alert without any action.
3. Create an alert. The alert defines which actions should be executed when a specific event occurs. When an alert is raised then the information about the event which triggered this alert will be stored to the program's event log. Such information will be stored even if the alert has no actions.

14.2 Concepts

This topic discusses concepts related to alerting.

Event

nVision constantly monitors your network, all hosts and services. As you can imagine – it can detect when a specific service slows down or stops responding at all. It will also detect when a whole host stops responding. For such situations you can define an event to be raised. Every event has its beginning and end time. For example in case of the host-not-responding event, the end will be when the host starts to respond. So with nVision you know not only when an event starts, but also when it ends. What's more, you can see a list of started events. For the purpose of this manual we call such events (that started and have not ended) open events.

You can also define your own events: let's say that you have to monitor an MSSQL Server. Then it's not enough to know how fast it responds to a simple request. You will most likely want to monitor several performance counters describing its current status to be able to react before any critical situation occurs.

For example, when free RAM memory is low or in case of cache performance degradation. Such events can be raised before any unrecoverable error allowing you to correct this situation quickly and prevent any data or productivity loss it might cause.

All raised events are logged in the program's event log. This allows making analyses of your network performance, for example to prepare reports showing the most problematic hosts or a report of the most frequent events.

Host status

Unlike in other similar products, host status in nVision is a calculated value, not a hard coded one. So you can define conditions when a host is considered to have status Up, Down or Warning. For more information about host status refer to [Host status concept](#)^[99] topic.

Action

You can define two general types of actions: notification and corrective. When an event occurs, nVision uses the action mechanism to notify the administrator about the problem or to run any external program to correct it. So before you define alerts, you need to define a set of actions which will be used to notify you.

You can define such actions as: e-mail, ICQ, pager or SMS message, sounds, dialog box and running an external program. For a complete list of available action types please read [Action Types](#)^[605] topic.

Alerts

Alert defines the program behavior in case of any network problems. First you select when the alert should be triggered - i.e. upon detecting a certain event. You also have to define which hosts should be checked for event occurrence. It can be defined directly for the host or at the atlas/map level. In such case the alert will be triggered if the event is raised on any host contained in the object for which an alert is defined (i.e. atlas, map or any descendant map).

14.3 Managing alerts

14.3.1 Requirements

To manage alerts, you have to familiarize yourself with several concepts first. You need to know what are events and actions. Before you start with alert management, please read at least the topic [Concepts](#)^[586], which discusses these issues.

Prerequisites

To begin managing alerts, you have to define a set of events first. Events tell nVision in which situation the alert should be raised. For example, after installation there is a predefined event: "Host down". It describes the event when the host stops responding. You should define events for all possible problematic situations you want to monitor.

After events are defined you will probably want to define some notification actions. Actions describe what nVision should do when an event is raised. For example an action may define how to notify you with an e-mail. However, it is possible to define alerts without actions - it is sometimes useful when you only need the information about an event for future reports and you don't need any notification.

After the above steps are done, you can start managing alerts. Please refer to the following topics describing available functions.

Where we can define alerts

Alerts can be defined on several levels of the atlas. First, we can define global alerts for the whole atlas. Such alerts will be inherited by all hosts in the atlas, which means that such alert conditions will be checked for every host and it can be raised on any host (if it meets the criteria defined in the alert; for example, an alert defined to be valid only for important hosts will not be raised on hosts with importance set to low).

Alerts can be also defined for each map. In this case, such alerts are inherited by all hosts on this map and also by all descendant maps in the atlas tree. And finally, alerts can be defined for each host.

You have then several ways of setting alerts to configure proper alerting based on the importance of your hosts, network, services, etc. Keep in mind that alerts are inherited from parent objects to descendants. Refer to [Inherited alerts](#)^[591] topic for more information.

14.3.2 Alert management window

To setup the program to notify you in case of any problems you use the alert manager window. This and the following topics provide more information on how to manage alerts.

Opening alert management window

With this window you can list, modify, create and remove alerts. To open this window, follow these steps.

1. Select the object for which you want to manage alerts. It can be any host, atlas or a map. In case you selected an atlas or a map, the alerts influence all hosts contained by those objects. Please read more about this in the topic [Inherited Alerts](#)^[591].
2. Select **Alerts** from the context menu.

To manage alerts for a specific host, navigate to the **Host info** window and click **Configure**:

The screenshot displays the Axence nVision Agent interface for a device named 'DESKTOP-N0QNH11'. The top status bar shows the device is 'Connected' and has a 'WARNING' status. Performance metrics include CPU usage at 18%, RAM usage at 64%, and system disk usage at 45%. The interface also shows up time, total time, and session time statistics, along with a 'Basic information' section for configuring the device's role, importance, and monitoring options.

Creating new alert or modifying existing ones

1. Open the alert management window for the object where you want to create an alert.
2. Click the **+** **Add alert** button to create a new alert or select the existing alert and click the **Edit alert** button.
3. In the **For the event** field, select the event for which you would like this alert. If the event is not defined yet, you can define it by clicking on the **New** button located on the right side. For more information about managing events, refer to the [Managing Events](#)^[595] topic.
4. The **Execute following actions** field allows you to add actions that will be run during the alert.

To add an action, click the **+** icon located on the left side of the action list. The **Action** window will display. Define action properties as follows:

| Property | Description |
|----------------------------|--|
| Execute action | Select the action to run. If the action is not defined yet, you can define it by clicking on the New button located on the right side. For more information about managing actions, refer to the Managing Actions ^[606] topic. |
| “When” group | |
| Immediately on event start | This is the default option meaning the action will be executed immediately the event is raised. |


| Property | Description |
|---------------------|--|
| After | Select "After" option and enter the number of minutes the program has to wait before the action is executed. Please remember that if the event ends before this time, the action will not be executed. |
| On event end | Sometimes we need a notification when the problematic situation ends. You can use this option to be notified for example when an important host starts to respond after it has been down. |
| Time restriction | In this field you can define time limits when the action may be executed. It is often necessary when you want to setup different notification schemes for your work time and home time. For example the program can send just an e-mail when you are at the office and send a pager notification when you are at home (where you might not be able to read your mail). |
| Repeat action every | Allows you to setup actions which will be executed repetitively until the event ends. Enter the number of minutes you would like to repeat the action. |

5. The last step allows you to restrict this alert to the specific host type and importance. This is helpful when you would like to setup a global alert for the whole atlas, but you don't want it to be raised for less important hosts – administrators usually don't care that the user's workstation has been turned off, but they want to know when a server goes down.
 - a) Select host type in the "Type" field.
 - b) Check all appropriate boxes next to the "Importance" label to limit an alert to hosts with such importance only.
6. Please be sure to check the "Alert enabled" box. If unchecked, the alert will not be active.


Note

- Modifying inherited alerts may affect other hosts, so proceed with caution.

Removing the alert

1. Open the alert management window for the object where you want to remove an alert.
2. Select the alert on the list.
3. Click the  **Remove alert** button located in the toolbar. Please remember that you can't remove inherited alerts (such alerts can be removed at the level where they have been defined).

Disabling or enabling the alert


1. Open the alert management window for the object where you want to disable or enable an alert.
2. Select the alert and click the  button.
3. To disable the alert, uncheck the **Alert enabled** box. To enable it, you have to make sure that this field is checked.

Filtering inherited alerts off

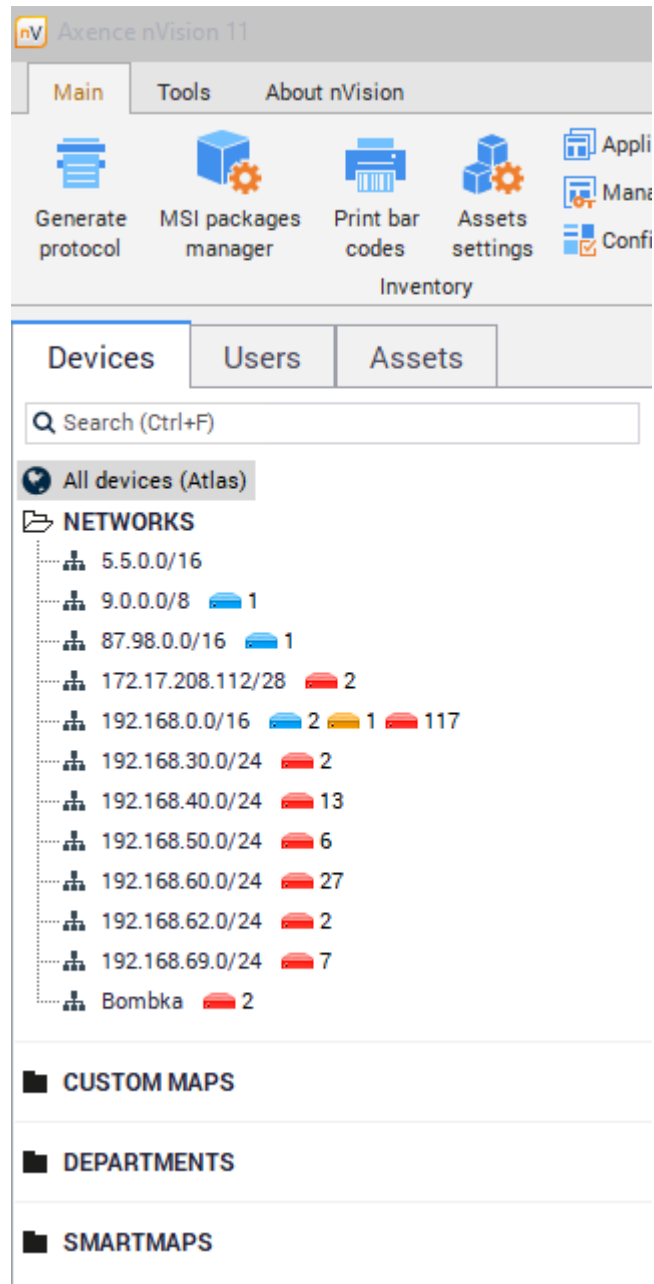
1. Open the alert management window for the object where you want to disable inherited alerts.
2. Check **Don't inherit alerts** if you don't want the inherited alerts to be generated for the selected object. If this box is currently checked and you would like to use alerts inheriting, just uncheck it.

14.3.3 Inherited alerts

As you know from previous topics, you can define an alert for the whole atlas and for the map - not only for one host. If the alert is defined for the whole atlas, then it is valid for all maps and all hosts meeting defined host type criteria (except those objects where inheritance is turned off). Read the [Managing alerts](#) topic to find out how to filter out inherited alerts. Inherited alerts are those alerts that have been defined elsewhere, but we see them on the list of the currently selected host or map.

Similarly, alerts defined for a map will be inherited by all maps which are descendants of this map. Descendant maps are those which names appear under the selected map name. You can hide or expand the whole tree of descendant maps using the  icon next to the map name.

Let's see an example of the atlas tree:



Filtering inherited alerts off

If you don't want alerts from higher level objects to be inherited, then you can filter them out. You can do that for every map and host independently.

1. Open the alert managing window for a map or a host.
2. Check **Don't inherit alerts** if you don't want the inherited alerts to be generated for the selected object. If this checkbox is currently checked and you would like to use alerts inheritance, just uncheck it.

14.3.4 Alert escalation

For especially important events you can use the alert escalation mechanism. It will trigger several actions for an event in predefined periods of time. For example, the first action can be run upon alert

start, the next one after 30 minutes and this action can be repeated every hour until the alert ends. When the event ends, another action can be run.

With this mechanism you can be sure that critical situations will be handled fast by the appropriate network administrator and in case that this administrator cannot deal with the problem, then another notification to a different person can be sent to avoid unhandled problems.

For information on how to setup actions to be run at different times and how to setup action repetitions, refer to [Managing Actions](#)^[606] topic.

14.4 Events

14.4.1 Configuration

To manage events, you have to familiarize yourself with the event concept first so please read the topic [Concepts](#)^[586], which discusses this issue.

Before you begin setting up alerts you need to define all events you would like to monitor. The program will monitor all hosts with the appropriate alert defined for an occurrence of defined alerts. When the event is detected then nVision takes two steps:

1. Generate all alerts based on this event. This will also cause the execution of actions defined in those alerts. Please remember that delayed actions may never be executed – it happens when an event ends before the action has been executed. Actions scheduled to run immediately on event start and on event end will be executed always (unless the program has been shut down).
2. The event is logged in the program event log. This allows performing future analyses of the host and network performance and helps preparing reports. To read about how to see events generated, read the topic [Event log](#)^[615].

When the problematic situation ends the event is also ended and it causes all actions scheduled to run upon event end to be executed.

Severity

Each event has defined a severity, which is designed for informational purposes. When notified, you will see the severity of the alert, which will help you to react faster to important ones.

Host status

Unlike in other similar products, host status in nVision is a calculated value, not a hard coded one. So you can define conditions when a host is considered to have status <Up>, <Down> or <Warning>. For more information about host status refer to [Host status concept](#)^[50] topic.

14.4.2 Event types

There are several general groups of events. The following list describes them:

| Event | Description |
|-------------------------------|--|
| Host and service availability | |
| Host down | None of the host services is responding. |
| Service down | The host service (HTTP, FTP etc.) is not responding. |

| Event | Description |
|--------------------------------|--|
| Service performance | Raised when a service experience unusual slow down or too many request/packets is lost. |
| Interface down | Generated when any interface changes its status to down. |
| Host status change | Can be generated for any host status change, even when a host changes a status from "Down" to "Up". |
| New host found | The event will be generated when the new host is found and added to the map. |
| Specific service test | |
| Web page load | With this event you can test your web page load time. |
| Web page content change rate | Allows preventing accidental changes to your web page content (i.e. changed by hackers). |
| POP3 login time | Raised when there is a problem logging to the mail server. |
| Send mail time | Checks for any problems while sending an e-mail message. |
| Counters | |
| SNMP threshold | You can check for a specific counter value. An event can be generated when this value rises too high (over a defined threshold) and when it falls too low. |
| Windows threshold | As above, for Windows system and Windows application counters. Allows monitoring health of programs like SQL Server or Exchange Server. |
| Windows | |
| New entry in Windows Event Log | Event informing about the occurrence of a new Windows Event Log entry. Entries can be filtered. |
| Windows service status change | Raised whenever the nVision discovers any changes to the windows service status. You can use it to monitor important services on remote machines and restart them in case of any problems. |
| Inventory | |
| System information change | Notifies about changes in startup commands, network shares, and S.M.A.R.T. status. |
| Software inventory change | Notifies about any program installation/uninstallation. |
| Hardware inventory change | Notifies about any hardware changes on all computers, where the inventory is being collected. |
| Users | |

| Event | Description |
|--|--|
| User visited domains from selected group | Generates the event when user visits specified domains. |
| User printed pages over the limit | Generates the event when user prints more than x pages (daily). |
| User used bandwidth over the limit | Generates the event when user downloads or uploads more than x MB (daily). |
| Other | |
| Time schedule | Generates the event within specified schedule (on specific days of week at specific time). |
| Agent status | Generates the event if Agent is not connected more than x days. |
| SNMP trap | Event informing about the received SNMP Trap message. |
| SysLog Message | Event informing about the received SysLog Message. |
| Change on switch ports | The event is generated if a device is connected, disconnected or its port has changed. |
| DataGuard | |
| Mobile device connected or disconnected | The event is generated if a device is connected or disconnected. You can define device types to be taken into account. |
| File operation on mobile device | Generates an event when following file operations are detected on a mobile device: file created, file deleted, file renamed, file written to existing file. You can specify additional conditions for the event (file mask). |


14.4.3 Managing events

To setup alerting, first you have to define all problematic situations when an alert is to be raised.

Opening event management window


With this window you can list, modify, create and remove events. To open this window, select the **Tools and options** tab, and then select **Manage events** from the main menu.

Creating new event

1. Open the event management window.
2. Click the  **Add event** button located in the toolbar. The **Event definition wizard** will open.
3. Enter the name of the event you would like to create in the **Event name** field.
4. Select the host status for this event in the **Host status field**. **This field determines the status of the host when the event is raised** Read more about host status in the topic [Events](#)^[593].
5. Select the severity of the event in the **Severity** field. This field is for informational purposes and it helps creating reports.

6. Select the event type on the list. To read more about event types, please read [Event types](#)⁵⁹³ topic.
7. Click the **Next** button,
8. Now you have to configure the event options (depending on the event type you selected). This is described in detail in the topic [Defining event properties](#)⁵⁹⁷.
9. Click the **Finish** button.

Modifying existing event

1. Open the event management window.
2. Select the existing event and click the  **Edit event** button. The **Event definition wizard** will open.
3. Now you have to configure the event options (depending on the event type you selected). This is described in detail in the topic [Defining event properties](#)⁵⁹⁷.
4. Click the **Finish** button.

14.4.4 Defining event properties

This topic describes defining the properties of different event types.

Host and service availability

Host down

This event is raised when every service on the host is not responding. You have to decide the way nVision determines the host is down. It can depend on number of minutes it does not respond or number of polls. This event will be monitored on every host that monitors at least one service.

| Property | Description |
|-----------------------------|---|
| Specified number of polls | <p>Check this option if you want the event to be raised after all host services polls fail a specified number of times (with timeout).</p> <p>Enter the number of failed polls in the edit box after which the event will be raised and the host status will change to down.</p> |
| Specified number of minutes | <p>Check this option if you want the event to be raised after all host services polls fail during specified number of minutes (with timeout). Please remember that this period is measured since last successful poll. If it will be smaller than the monitoring time, you may get false alerts between every host poll.</p> <p>Enter the number of minutes in the edit box after which the event will be raised and the host status will change to down.</p> |

Service down

This event is raised when a specific service is not responding. You have to decide the way nVision determines the service is down. It can depend on number of minutes it does not respond or number of polls.

| Property | Description |
|-----------------------------|--|
| Service | Select the service you want to monitor. This event will be monitored on every host that actually monitors the selected service. |
| Specified number of polls | <p>Check this option if you want the event to be raised after the specified number of service polls fail (with timeout).</p> <p>Enter the number of failed polls in the edit box after which the event will be raised.</p> |
| Specified number of minutes | <p>Check this option if you want the event to be raised after services polls fail during a specified number of minutes (with timeout). Please remember that this period is measured since the last successful poll. If it will be smaller than the monitoring time, you may get false alerts between every service poll.</p> |

| Property | Description |
|----------|---|
| | Enter the number of minutes in the edit box after which the event will be raised. |

Service performance

Raised when a service experiences unusual slow down or too many requests/packets are lost.

| Property | Description |
|----------------------------|--|
| Service | Select the service you want to monitor. This event will be monitored on every host that actually monitors the selected service. |
| Check last | The number of last minutes you would like to be checked. |
| Generate event when | Check at least one of the condition check boxes described below. If you check both then the event will be generated if at least one of the conditions is met. |
| Average/Each response time | <p>Check Average response time if you would like an event to be generated whenever a service experiences any slowdown.</p> <ul style="list-style-type: none"> nVision checks an average value as a default. You can change it to check every value by clicking on the Average label. The label text changes to Each then to indicate that every probe will be checked separately. Enter the response time threshold in milliseconds. The event will be generated when the response time is higher than this value. Enter the reset threshold in the next field. Please read the Rising, falling and reset thresholds ⁶⁰⁴ topic for more information about thresholds. |
| Lost packets percentage | <p>Check Lost packets percentage if you would like an event to be generated when the number of lost requests is too high.</p> <ul style="list-style-type: none"> Enter the threshold value. The event will be generated when the percent of packets lost is higher than this value. Enter the reset threshold in the next field. |

Interface down

This event will be generated (started) when any network interface goes down and it will end when the interface status is up again.

Host status change

Can be generated for any host status change, even when a host changes a status from "Down" to "Up". This event will be monitored on every host.

| Property | Description |
|---------------------|--|
| Generate event when | Select the status for which you would like an event to be raised. You can have an event raised whenever a host status changes to “Up”, “Warning” or “Down”. Just select the required option. |

New host found

The event will be generated when the new host is found and added to the map.

Specific service test

Web page load

With this event you can test your web page load time. This event will be monitored on every host that actually monitors any page load (has such counter defined).

| Property | Description |
|---------------------|---|
| Check last | The number of last minutes you would like to be checked. |
| Generate event when | <ul style="list-style-type: none"> nVision checks an average value as a default. You can change it to check every value by clicking on the Average label. The label text changes to Each then to indicate that every probe will be checked separately. Enter the page load time threshold in milliseconds. The event will be generated when the page load time is higher than this value. |
| End event when | Enter the reset threshold in the next field. Please read the Rising, falling and reset thresholds ⁶⁰⁴ topic for more information about thresholds. |

Web page content change rate

Allows preventing accidental changes to your web page content (i.e. changed by hackers). It will be raised whenever the probe discovers that the percent of page content has changed over the threshold. This event will be monitored on every host that actually monitors any page content change (has such counter defined).

| Property | Description |
|----------------------------------|--|
| Check last | The number of last minutes you would like to be checked. |
| Average page content change rate | <ul style="list-style-type: none"> nVision checks an average value as a default. However, you can change it to check every value by clicking on the Average label. The label text changes to Each then to indicate that every probe will be checked separately. Enter the page load time threshold in milliseconds. The event will be generated when the page load time is higher than this value. |

| Property | Description |
|----------------|---|
| End event when | The event will end when the page content returns to the (more) original and the percentage of change drops under the reset threshold. |

POP3 login time

Raised when there is a problem logging to the mail server. This event will be monitored on every host that actually monitors any POP3 login time (has such counter defined).

| Property | Description |
|-------------------------|--|
| Check last | The number of last minutes you would like to be checked. |
| Average POP3 login time | <ul style="list-style-type: none"> nVision checks an average value as a default. You can change it to check every value by clicking on the Average label. The label text changes to Each then to indicate that every probe will be checked separately. Enter the POP3 login time threshold in milliseconds. The event will be generated when the page load time is higher than this value. |
| End event when | Enter the reset threshold in the next field. Please read the Rising, falling and reset thresholds ⁶⁰⁴ topic for more information about thresholds. |

Send mail time

Checks for any problems while sending an e-mail message. This event will be monitored on every host that actually monitors any send mail time (has such counter defined).

| Property | Description |
|------------------------|--|
| Check last | The number of last minutes you would like to be checked. |
| Average send mail time | <ul style="list-style-type: none"> nVision checks an average value as a default. You can change it to check every value by clicking on the Average label. The label text changes to Each then to indicate that every probe will be checked separately. Enter the POP3 login time threshold in milliseconds. The event will be generated when the page load time is higher than this value. |
| End event when | Enter the reset threshold in the next field. Please read the Rising, falling and reset thresholds ⁶⁰⁴ topic for more information about thresholds. |

Counters

SNMP threshold

| Property | Description |
|----------------|--|
| Counter | Select the SNMP counter to be checked. Please remember that such counter will be checked only on hosts which actually monitor such counter. So to have the event properly working you have to setup such counter on every host. |
| Check last | The number of last minutes you would like to be checked. |
| Average value | <ul style="list-style-type: none"> nVision checks an average value as a default. You can change it to check every value by clicking on the Average label. The label text changes to Each then to indicate that every probe will be checked separately. Enter the POP3 login time threshold in milliseconds. The event will be generated when the page load time is higher than this value. |
| End event when | Enter the reset threshold in the next field. Please read the Rising, falling and reset thresholds ⁶⁰⁴ topic for more information about thresholds. |

Note

- Please note that setting long time periods to check may slow the program down. If the counter is polled very often then many probes are collected and checking all of them consumes CPU. Do not set this period to more than 10 minutes for hosts that are polled more often than every 10 seconds.

Windows threshold

| Property | Description |
|---------------|---|
| Counter | Select Windows counter to be checked. Please remember that such counter will be checked only on hosts which actually monitor such counter. So to have the event properly working you have to setup such counter on every host |
| Check last | The number of last minutes you would like to be checked. |
| Average value | <ul style="list-style-type: none"> nVision checks an average value as a default. You can change it to check every value by clicking on the Average label. The label text changes to Each then to indicate that every probe will be checked separately. |

| Property | Description |
|----------------|---|
| | <ul style="list-style-type: none"> Enter the POP3 login time threshold in milliseconds. The event will be generated when the page load time is higher than this value. |
| End event when | Enter the reset threshold in the next field. Please read the Rising, falling and reset thresholds ⁶⁰⁴ topic for more information about thresholds. |

Note

- Please note that setting long time periods to check may slow the program down. If the counter is polled very often then many probes are collected and checking all of them consumes CPU. Do not set this period to more than 10 minutes for hosts that are polled more often than every 10 seconds.

Windows

Windows service status change

| Property | Description |
|---------------------|--|
| Generate event when | Select the appropriate option when this event should be generated: when the service stops, pauses and/or starts. |
| All services | Select to generate this event for all Windows services. |
| Selected services | Select this option to monitor only one specific Windows service. Click the green plus icon and select the services to be monitored. |

New entry in Windows Event Log

This event will be generated when a new Windows Event Log entry meets the filter.

Other

Change on switch ports

| Property | Description |
|--|--|
| Generate event when | The event is generated if a device is connected, disconnected or its port has changed. |
| Only for new devices connected to the switch | Select to generate this event for new devices only. |

SNMP trap

| Property | Description |
|------------|---|
| MIB filter | Event will be triggered if the device sends a SNMP trap related to any OID or only to the selected OID. |

Time schedule

| Property | Description |
|---------------|---|
| Time schedule | The event is generated on specific days and at specific time as defined by the administrator. |

SysLog Message

| Property | Description |
|----------------|---|
| SysLog Message | The event is generated when the host sends SysLog message containing keywords specified in the filter set on configuration. |

Agent status

| Property | Description |
|--------------|---|
| Agent status | The event is generated if Agent is not connected for a specific number of days. |

**DataGuard****Mobile device connected or disconnected**

| Property | Description |
|--|--|
| Generate event when | The event is generated if a device is connected or disconnected. |
| Generate this event for specified devices type | Select the types of devices for which the event is generated. |

File operation on mobile device

| Property | Description |
|---|--|
| Generate event when | The event is generated if a file is created, deleted, renamed or written to existing file. |
| Specify additional conditions for the event | Provide a file mask if necessary. |

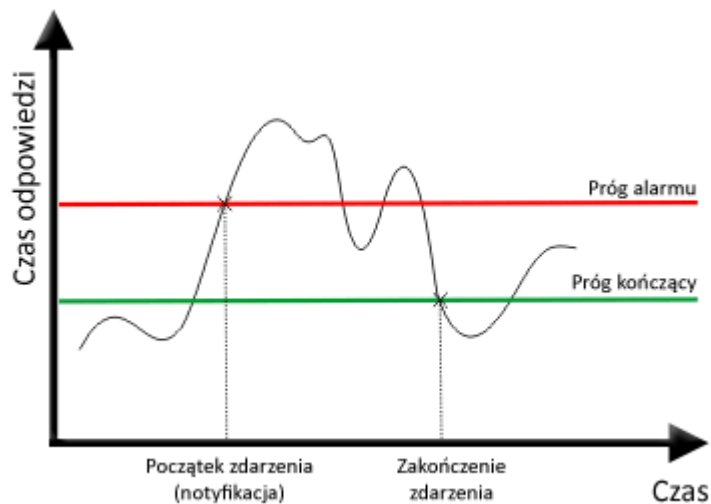
| Property | Description |
|--|---|
| Generate this event for specified devices type | Select the types of devices for which the event is generated. |

14.4.5 Rising, falling and reset thresholds

In most events, you define a threshold value, which indicates when an event should start. For example – in case of service it defines how slow a service can be before it triggers an event.

In case of some event types you also have to define the “reset” threshold for the event. This is important – otherwise an alert would be generated every time the condition is met. That could cause the same alert to be repeated every minute. The measured value must first fall below the reset threshold before the next alert is generated.

The red line indicates the alert threshold. When the response time or packet loss rate rises above this threshold, an alert will be generated. But for the next alert to be generated, this value must fall below the reset threshold. This prevents repeated alerts for the same event.



Rising and falling thresholds

The threshold discussed above is called rising, because it is generated when a measured value rises above it. But you can also define an event when a value should stay above a threshold. Then an event is generated when this value falls under a threshold and such threshold is called falling.

Note

- The reset threshold may not be higher than the alert threshold for rising thresholds and lower for falling thresholds.

14.5 Actions

14.5.1 Introduction

In most cases when you define an event you want to be notified when it occurs or you would like to set a corrective action to be executed. nVision allows you to create both types of actions: notification and

corrective. So before you define alerts, you need to define a set of actions which will be used to notify you.

You can define such actions as: e-mail, ICQ, pager or SMS message, sounds, dialog box and running an external program. For a complete list of available action types please read the [Action Types](#)⁶⁰⁵ topic.

14.5.2 Action types

There are several general groups of actions. The following list describes them:

| Action | Description |
|----------------------------|--|
| Desktop notification | |
| Desktop alert | A small information box will show at the defined position. This box does not steal the focus and it does not disturb you in your current task. |
| Sound | nVision will play a defined sound. |
| Speech | This allows alert information to be read by the computer speech synthesis engine. |
| Send message | |
| E-mail | An e-mail with alert information will be sent (<i>you can enter multiple addresses separated by semicolon (;)</i>). |
| ICQ | An ICQ message with alert information will be sent. |
| SMS via GSM | This action sends an SMS message via an attached GSM phone or modem. |
| SysLog Message | The SysLog message will be sent to the specified SysLog server. |
| Program or script | |
| Run program locally | With this option you can run any program on the local machine, for example to take some corrective action. |
| Run program remotely | With this option you can run any program on a remote machine, for example to take some corrective action. |
| Other | |
| Write to file | The alert information can be written to the file. |
| Send SNMP Trap | Sending of SNMP Trap message. |
| Send Wake On LAN packet | Sending of the packet turning on/waking up the selected device. |
| Windows | |
| Start/Stop Windows service | It controls the service on the remote Windows workstation. |
| Shutdown/restart computer | This action allows you to shutdown or restart the remote Windows workstation. |

| Action | Description |
|--------------------------------|---|
| Add entry to Windows Event Log | Creates an entry to Windows Event Log on a local or remote machine with Windows system. |



14.5.3 Managing actions

To setup nVision so that it notifies you, you have first to define all possible notification actions you would like to use. The following topics provide more information on how to manage actions:

Opening action management window

With this window you can list, modify, create and remove actions. To open this window, select **Tools / Manage actions** from the main menu.

Creating new action or modifying existing one

1. Open the action management window.
2. Click the  **Add action** button to create a new action or select an existing one and click the  **Edit action** button. The **Action definition wizard** will open.
3. If you are creating a new action, then enter its name in the **Action name** field and select the action type on the list. Click the **Next** button, To read more about action types, refer to the [Action types](#)^[605] topic.
4. Configure the action options (depending on the action type you selected). This is described in detail in the topic [Defining action properties](#)^[606].
5. At this point it may be necessary to define action setup options. These options are required to properly execute some actions (for example the program needs a mail server address to send an e-mail notification or a COM port to which the GSM is connected). Setting up the action is discussed in the topic [Setting up actions](#)^[612].
6. If all options are configured you can test the action by clicking the **Test** button. This will perform the action and you can verify if it is properly defined and working.
7. Click the **Finish** button.

14.5.4 Defining action properties

This topic describes defining properties of different action types.

Desktop notification

Desktop alert


A small information box will show at the defined position. This box does not steal the focus and it does not disturb you in your current task.

| Property | Description |
|----------|---|
| Message | Allows you to select the message format which will be displayed in the box. |

| Property | Description |
|----------|--|
| Auto | Select it to display the predefined message. |
| Custom | Select to define your own message. To read more about defining your own messages, please go to the topic Defining custom alert messages ⁶¹³ . |

Sound

The program will play a defined sound.

| Property | Description |
|--------------------------|--|
| nVision predefined sound | Select one of the predefined nVision sounds. |
| Windows system sound | Select one of the predefined Windows sounds. |
| Select file | Click the  icon and select the sound file to be played. |

Speech

This allows alert information to be read by the computer speech synthesis engine.

| Property | Description |
|----------|--|
| Message | Allows you to select the message format which will be read by the speech engine. |
| Auto | Select it to display the predefined message. |
| Custom | Select to define your own message. To read more about defining your own messages, please go to the topic Defining custom alert messages ⁶¹³ . |

Send message

E-mail

An e-mail with alert information will be sent.

| Property | Description |
|----------------|---|
| Email to | The e-mail address to which the alert message will be sent. You can enter several e-mail addresses dividing them by commas, semicolons or spaces. |
| Subject | The subject of e-mail message. In the subject you can use variables described in the Defining custom alert messages ⁶¹³ topic. |
| Message format | Allows you to select the message format which will be used to generate alert message. |
| HTML | This is the default message format. |

| Property | Description |
|------------|---|
| Short text | This is text only format with short information. |
| Long text | This is text only format with complete alert information. |
| XML | This is the alert information in XML format. You can use this if you would like to build your own external alert actions. Your program may receive e-mails with XML information, interpret them and do some additional tasks. |
| Custom | Select to define your own message. To read more about defining your own messages, please go to the topic Defining custom alert messages ^[613] . |

ICQ

The ICQ message with an alert information will be sent.

| Property | Description |
|----------------|--|
| ICQ number | The ICQ number to which the alert message will be sent. |
| Message format | Allows you to select the message format which will be used to generate alert message. |
| Custom | Select to define your own message. To read more about defining your own messages, please go to the topic Defining custom alert messages ^[613] . |

SMS via GSM

This action sends an SMS message via an attached GSM phone or modem.

| Property | Description |
|---------------|--|
| Phone number | The phone number to which the SMS message will be sent. It must start with a country code prefix (+1 for US). |
| Alert message | Check if you want the message to be presented on the phone screen immediately upon arrival. |
| Auto | This is the default message format. |
| Custom | Select to define your own message. To read more about defining your own messages, please go to the topic Defining custom alert messages ^[613] . |

SysLog Message

The SysLog message will be sent to the specified SysLog server.


| Property | Description |
|-----------------------|--|
| SysLog server address | The address of the SysLog server. |
| Syslog server port | The port on which the server operates. |

| Property | Description |
|----------|--|
| Message | Define your message in the edit box. To read more about defining your own messages please refer to the topic Defining custom alert messages ⁶¹³ . |

Program or script



Run program locally

With this option you can run any program on the local machine, for example to take some corrective action.

| Property | Description |
|-----------------|--|
| Run the program | Click the  icon and select the program to be run. |
| With parameters | Enter the parameters of the execution. You can use variables described in the Defining custom alert messages ⁶¹³ topic. |

Run program remotely


With this option you can copy and run any other program remotely, for example to take some corrective action.

| Property | Description |
|---|--|
| Copy local program to a remote host and run | <p>Selecting this option causes both actions: copying and running a program.</p> <p>Click the  button and select the source file of the local program to be run. Then, select the destination directory on the remote host.</p> |
| Run remote program | Click the  button and select the remote program to be run. |

Other

Write to file

The alert information can be written to a file.

| Property | Description |
|----------------|--|
| Write to file | Click the  button and select the file name where the alert message will be written. |
| Message format | Allows you to select the message format which will be used to generate the alert message. |
| HTML | This is the default message format. |
| Short text | This is text only format with short information. |

| Property | Description |
|-----------|---|
| Long text | This is text only format with complete alert information. |
| XML | This is the alert information in XML format. You can use this if you would like to build your own external alert actions. Your program may receive e-mails with XML information, interpret them and do some additional tasks. |
| Custom | Select to define your own message in the edit box. To read more about defining your own messages, please go to the topic Defining custom alert messages ^[613] . |

Send SNMP Trap

Sends a SNMP Trap to a remote device.

| Property | Description |
|-----------------|--|
| Host Name | DNS name or IP address of the remote device. |
| Port | UDP port number of the remote device. |
| Community | SNMP community name. |
| PDU type | PDU packet header type. |
| Agent | IP address of SNMP Agent. |
| Trap generic | Type of SNMP Trap. |
| Notification ID | It is required if Service type is defined as "enterpriseSpecific". |

Send Wake On LAN packet

Sends Wake On LAN packet to the remote device.

| Property | Description |
|-------------------------|---|
| Use host address | Identification is performed based on the IP and MAC addresses of the device. |
| MAC Address | Target device address in the following notation AA:BB:CC:DD:EE:FF. |
| Local Broadcast Address | Target address of the Wake On LAN packet. |
| Port | UDP port number of the remote device. |
| SecureOn password | SecureOn password of the remote device in hexadecimal notation, e.g. AA:BB:CC:DD:EE:FF. |

Windows

Start/Stop Windows service

It controls the service on the remote Windows workstation.

| Property | Description |
|--|---|
| Windows service, which has triggered the event | Check if you want this action to be performed on the host and service for which the event is generated. |
| Specific windows service | Select if you want the action to be executed on a specific Windows computer and for a specific service. |
| Host | Select the host on which the action is to be executed. |
| Service | Select the service. |
| Action | Select the action to perform: you can start, stop, restart, pause and resume the Windows service. |

Shutdown/restart computer

This action allows you to shutdown or restart the remote Windows workstation.

| Property | Description |
|---------------------------------------|---|
| Host, which the event has occurred on | Check if you want this action to be performed on the host for which the event is generated. |
| Specific host | Select if you want the action to be executed on a specific Windows computer. |
| Restart | Check to perform system restart. |
| Shutdown | Check to perform system shutdown. |

Add entry to Windows Event Log

This action allows you to write an entry to Windows Event Log of the selected host.

| Property | Description |
|---------------------------------------|---|
| Host, which the event has occurred on | Check if you want this action to be performed on the host for which the event is generated. |
| Specific host | Select if you want the action to be executed on a specific Windows computer. |
| Message type | Select a message type (Success, Error, Warning or Information). |

14.5.5 Setting up actions

Most actions require setup options to be defined before the program is able to execute them. For example the program needs a mail server address to send an e-mail notification, etc. This topic describes defining properties of each action type setup (some action types do not require setup).

The action setup may be edited in the program options window and during creation of an action or when editing its properties.

Desktop notification

Desktop alert

A small information box will show at the defined position. This box does not steal the focus and it does not disturb you in your current task.

| Property | Description |
|----------|---|
| Position | The position in which the information box will display on the desktop |
| Duration | Duration in seconds for how long the box will show. |
| Fade | Check this option if you want the information box to fade. |

Speech

This allows alert information to be read by the computer speech synthesis engine.

| Property | Description |
|---------------|--|
| Speech engine | The speech engine you want to be used. |
| Voice speed | Speed of the voice. |

Send message

E-mail

An e-mail with alert information will be sent.

| Property | Description |
|--------------------------|---|
| Reply to address | If this address is not set properly or blank most mail servers will reject an e-mail. Enter the e-mail address, which you know will be accepted by the mail server (your e-mail address most likely). |
| Connection | Set the timeout, the number and delay of retries. |
| Use external SMTP server | nVision uses its own built-in mail server. But you can use any external one. Just check this option and define the following properties. |

| Property | Description |
|------------------------|---|
| Address | The address of the external mail server. |
| Port | The port number on which the external mail server is operating. |
| Authorization required | If the server requires authorization, then check the appropriate box and enter your username and password in the Username/Password fields respectively. |
| User name | Username required to login. |
| Password | Password required to login. |

ICQ

The ICQ message with an alert information will be sent.

| Property | Description |
|------------|---|
| ICQ server | ICQ server address. |
| Port | The port number on which the server is operating. |
| UIN | The UIN nVision will use to login to the server. |
| Password | Password required to login. |

SMS via GSM

This action sends an SMS message via an attached GSM phone or modem.

| Property | Description |
|--------------------|---|
| COM port settings | Select a COM port, a baud rate, data bits, parity and stop bits. |
| SMS settings | Check the appropriate option for splitting long messages and for a custom service center number (SMSC). |
| Device information | Press the Detect device button to see its manufacturer and model. |

14.5.6 Defining custom alert messages

When defining alert notification options, you can also define your custom messages to be used as information to be sent/saved. nVision allows you to use several variable names, which are changed to the appropriate value when an alert is raised. This topic lists those variables and describes how to use them.


Variables

| Variable name | Description |
|---------------|--|
| \$Host.Name | Name of the host for which the alert is generated. |

| Variable name | Description |
|----------------------|--|
| \$Host.Type | Type of the host. To read more about host type or other host related variables defined here, check the topic Host properties. |
| \$Host.Importance | Host importance. See the topic Host properties. |
| \$Host.Status | Host status. It defines the status of the host in the moment when the alert message is composed. In case of delayed actions this status may be different than the status at the alert start. |
| \$Host.Info1 | Host Info1 field. See the topic Host properties. |
| \$Host.Info2 | Host Info2 field. See the topic Host properties. |
| \$Host.ParentHost | Host's parent host. See the topic Host properties. |
| \$Host.SNMPManagable | The information if the host is SNMP manageable. See the topic Host properties. |
| \$Host.SNMPSystem | The system description of the host read using SNMP. See the topic Host properties. |
| \$Host.SNMPLocation | The location of the host read using SNMP. See the topic Host properties. |
| \$Host.SNMPName | The name of the host read using SNMP. See the topic Host properties. |
| \$Alert.Name | Name of the alert - it is the name of the event that triggered the alert. |
| \$Alert.Description | Short description of the event. |
| \$Alert.Type | The type of the event. See the topic Event types ⁵⁹³ for more information. |
| \$Alert.Severity | Severity of the event which triggered the alert. |
| \$Alert.StartTime | The time when an alert has been raised. |
| \$Alert.Duration | The duration of the alert. |
| \$Alert.Resolution | Current resolution status of this alert. |
| \$Alert.Owner | The owner of the alert. |

How to use variables

When the program allows you to define your own message format, then you will be able to use variables.

You can just enter the variable name in the text of the message or you can use the  button. Click this button to get a list of available variables and select one. Then the variable name will be inserted in the text of the message in the cursor position.

14.6 Raised alerts

14.6.1 Processing alerts

How nVision processes alerts

In most network monitoring products, you can only define conditions to indicate when an alert is to be raised, but do not get any information about how long such conditions have existed. Also, you usually cannot setup actions to be executed when such conditions are no longer valid. In nVision, every alert raised has a start time and an end time. When the event conditions are met, nVision raises an alert. Then the program continually checks if such conditions are still valid and ends the alert when they are not. It means that you can see the start and end times of every alert along with its duration.

When an alert is raised, then it is called an open alert and the status of such alert is set to <Open>. It remains open until the conditions that caused it to be raised are not longer true, or if the condition required to end this alert is not yet true. After all conditions required to end the alert are met, nVision ends it and changes its status to <Closed>. It indicates not only that the alert ended, but that the event (that triggered this alert) also ended.

How actions are executed

When an alert is raised, all actions related to it and scheduled for immediate execution are started. All other actions set as delayed will be executed only if the alert is still open (i.e. raised). When an alert ends, the action being executed also ends. You can also stop action execution for currently open alerts by setting **Alert resolution**.

Every alert is raised with the Resolution set to "New". If you want to indicate that the alert notification has been successful and you are aware of the alert, then you must acknowledge the alert. To do that, just set alert resolution in nVision's Event Log to "Acknowledged". Similarly, when the problem causing an alert has been solved, then you can stop further actions by setting alert resolution to "Resolved". In general, changing the alert resolution has the effect of stopping the execution of remaining actions.

14.6.2 Event log



All raised alerts are logged by nVision and you can view them in the Event Log. There is a list of all raised alerts along with the action execution log for every alert. You can change the Alert resolution status and view alerts sorted by several fields and also filter them to see only the alerts that are interesting to you.

Icons used in the Alert & Action grids




Alert grid

| Icon | Description |
|------|-------------|
|------|-------------|




Status – indicates the status of the alert

| | |
|---|----------------------|
|  | Open alert |
|  | Closed (ended) alert |





Resolution – allows an administrator to manage alerts

| Icon | Description |
|---|--|
|  | New alert |
|  | The alert has been acknowledged by the administrator and no more actions will be executed. |
|  | The alert has been resolved by the administrator and no more actions will be executed. |




Event type – type of the event that raised the alert

| | |
|---|-----------------------------|
|  | Host & service availability |
|  | Specific service test |
|  | Counter |





Event severity – severity of the event that raised the alert

| | |
|---|--------------------|
|  | Low severity |
|  | Normal severity |
|  | Important severity |
|  | Critical severity |




Host status change


| | |
|---|---------|
|  | Up |
|  | Warning |
|  | Down |

Action grid

| Icon | Description |
|---|-------------------|
| Type – type of the action | |
|  | Desktop alert |
|  | Message |
|  | Program or script |
|  | Others |

Status – indicates the status of the action

| | |
|---|------------------------------------|
|  | Not executed yet |
|  | Action is currently being executed |
|  | Successfully executed |

| Icon | Description |
|---|--|
|  | Execution failed (see Info column for a problem explanation) |

Opening Event Log window

You can see alerts for a selected host only or for the entire atlas. To view the Event Log for atlas, select **Event Log** from the Reports and Alerts section. To view the Event Log for a single host, navigate to the **Host info** window and then to the **Events** tab.

Clearing Alerts (changing alert resolution)

To clear an alert, you have to change its Resolution to “Acknowledged” or “Resolved”.

1. Select an alert or several alerts.
2. Select **Acknowledge** or **Resolve** from the context menu.

For more information about alert resolution refer to the [Raised alerts](#)⁶¹⁵ topic.

Sorting & filtering

- You can sort both grids by any column just by clicking on the column header.
- You can filter events by status and resolution. To view only those alerts that have specific status/resolution, just select the appropriate entry in the **Filter** field.

Changing time period

You can view events for one day, week or a month. To select the time period, use the toolbar. To scroll through past alerts in the Event Log, use the arrows located on the toolbar. When scrolling, you will always see the current time range of presented alerts.

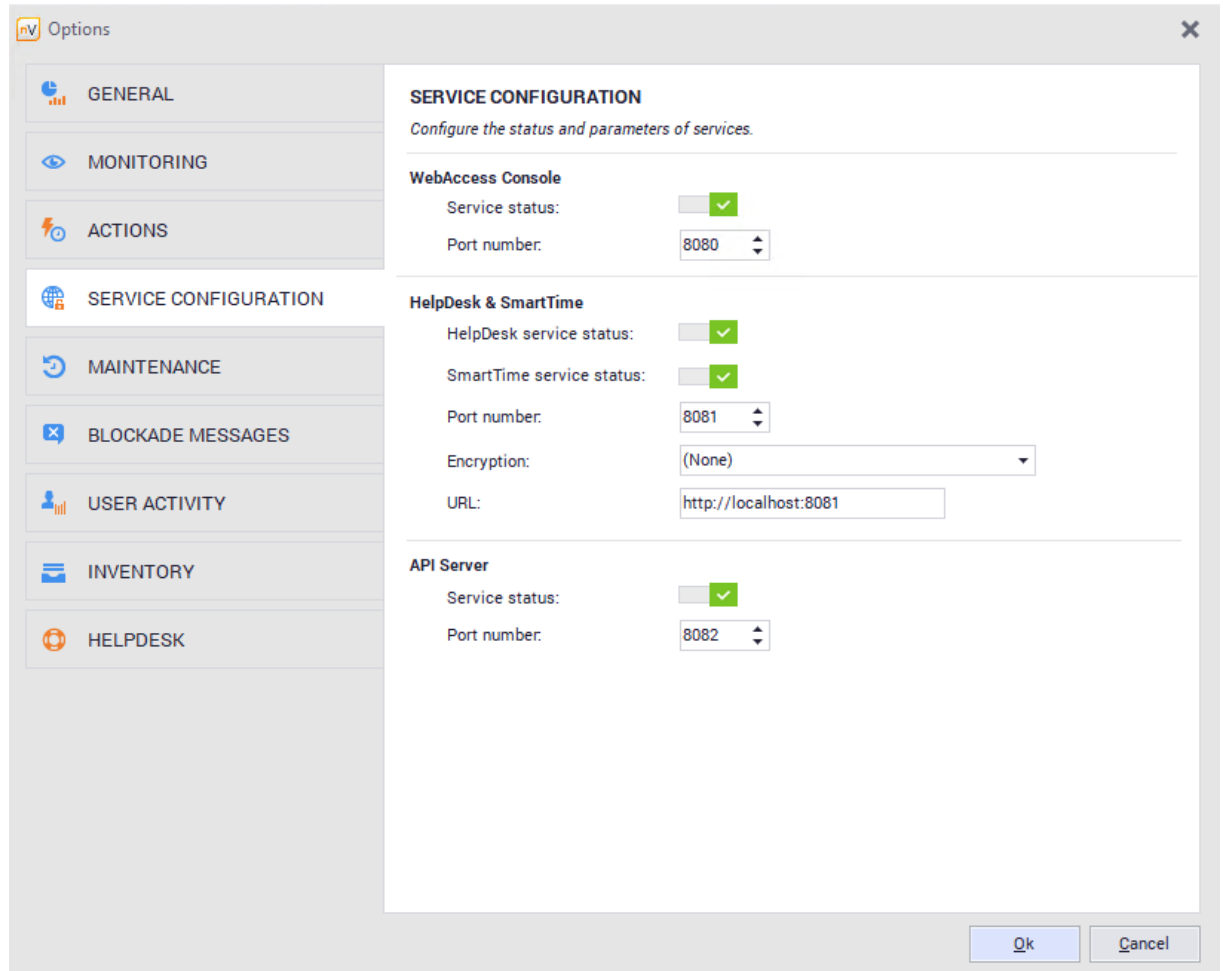
Part



15 Web access

15.1 How to get access to nVision via Web browser?

To allow access to nVision via a Web browser (in read-only mode), first enable the Web access in the nVision application:



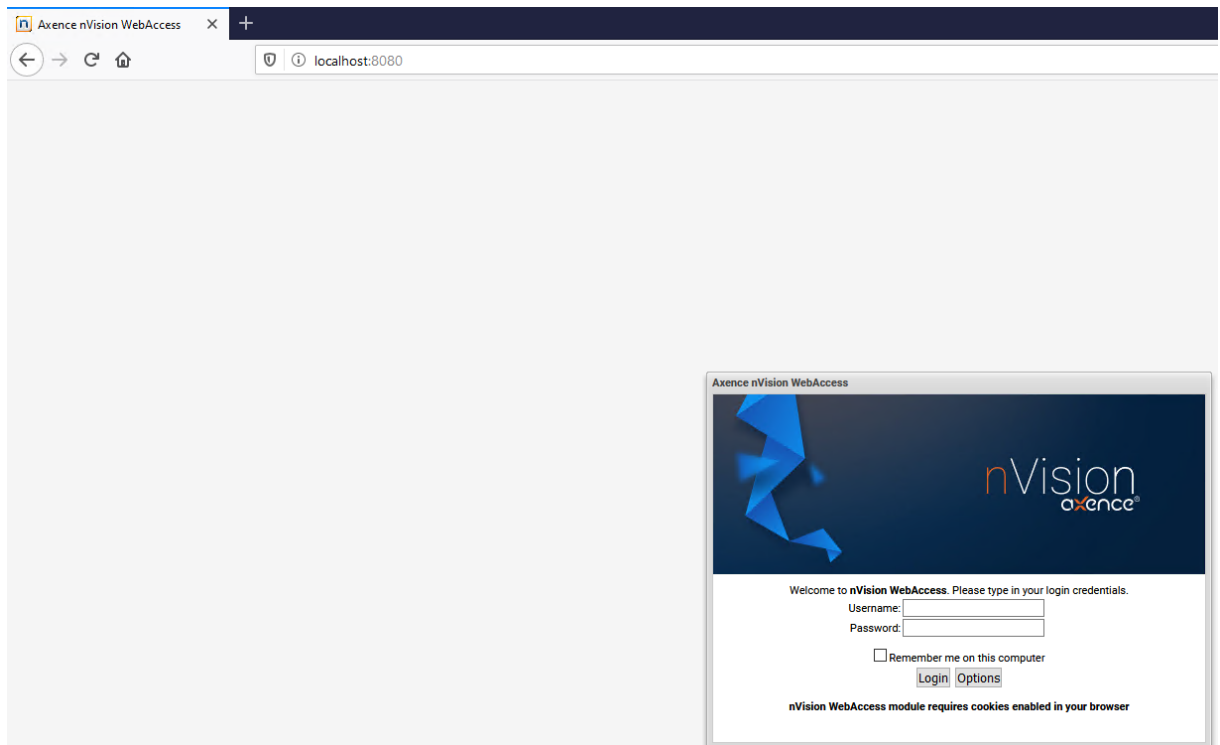
1. Select the **Options** icon in the main toolbar of nVision.
2. Navigate to the Service configuration tab, and then mark the **Enable Web access** option and enter the port number through which the Web Access will operate.

Warning! If Web access wasn't enabled prior to upgrading to nVision 14, it is no longer available.

Browser access

When the Web Access is toggled on in the manner described above, it is possible to use nVision by means of a Web browser. For this purpose, enter the IP address and port number of the machine running nVision in the browser address bar and then, after connecting to the access module, enter the user name and password to log in to nVision. Please notice that the Web Access is read-only, so no changes to nVision can be made through it.

The option of optimization for weaker machines (login window, **Options** button) allows the operation of the nVision Web Access module on slower computers, but increases bandwidth usage.



15.2 How to create Web Access user accounts?

It is possible to add multiple users who will have access to selected functionalities of nVision. To make this possible, their accounts should be properly configured. Please notice that the Web Access is read-only, so no changes to nVision can be made through it.

Web Access is enabled automatically for users of the **Administrator** type and may be enabled for users of the **HelpDesk** type. It is not possible for other user types to have Web Access.

Administrator users

Users of the Administrator type have access to all maps and devices, and also to reports, audit and access log.

HelpDesk users

The access rights to specific maps are defined for the HelpDesk user accounts:

- If the given map has no defined right, a default right is set for the given map.
- Users do not have access to audit, reports and the event log (the latter is visible only in device details, the global event log is not visible). The above-mentioned options are hidden for the users.
- The map for which the user has no “Map View” access right is not displayed in the atlas tree.

Access rights

| Access rights | Required rights | Description |
|---------------|-----------------|---|
| Map View | | Displaying the given map in the atlas tree. Allows all devices with the given map to be seen. |
| Host Info | Map View | Access to all device details (services, counter, user activity, inventory, etc.). |
| Remote access | | Ability to get remote access (VNC) to the devices from the given map. |

Assign tickets

To create the Web Access user account:

1. For a new user: create a new HelpDesk user account. Click the **Users** button and press the **Add** button; give the user name, the role (Help-Desk) and the password. Go to number 3.
2. For an existing user: click the **Users** button, and then right click the selected account and select the **User info** option.
3. In the **Access rights** tab, you can edit default rights and add rights for selected departments and maps.

The screenshot shows the nVision user management interface for user MIKUZ (Account: MIKU@WIN10, Role: ADMINISTRATOR). The 'PERMISSIONS' tab is selected in the left sidebar. The main content area displays 'ACCESS TO MODULES AND FEATURES' with a list of modules and their access status:

- Console:
- Network:
- Inventory:
- Users:
- DataGuard:
- HelpDesk:
- SmartTime:

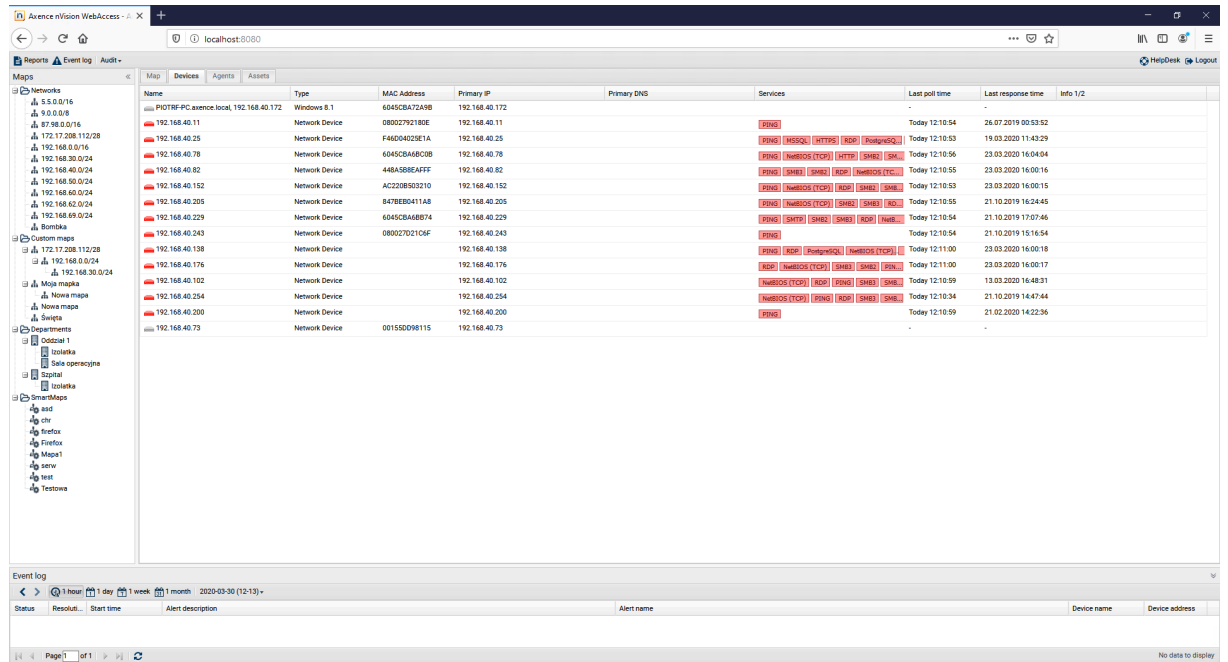
Under 'Access to settings', 'Agent visibility' is set to . Under 'Access to features', 'Agent management menu' is set to . The 'WebAccess console' option is highlighted with a red box and is set to . Below this, there are options for 'Access to devices' (Full access selected) and 'Access to users' (Full access selected).

To learn more about user accounts, see section [User management](#) ³⁶⁰.

15.3 Window layout

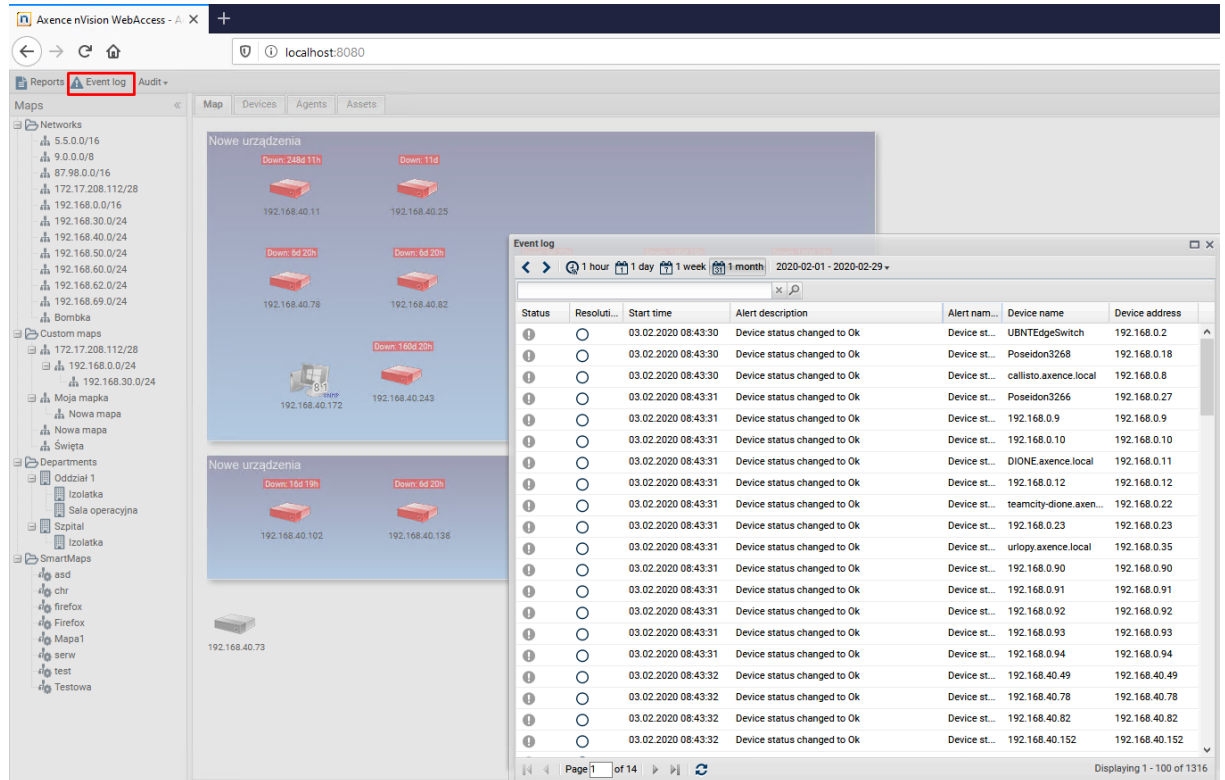
Atlas tree

Atlas tree located in the top left part of the window contains the list of all available networks, user maps, departments and smart maps. When the map is selected in the tree, it is displayed on the right. You can resize the atlas tree column width and also minimize it.



Event log

The event log bar (bottom part of the window) allows recent alerts to be checked quickly. The field where the events are presented can be resized or minimized. To open the event log in a separate frame, click the **Event log** button in the top part of the window.



Map

The tab contains a graphical presentation of the map selected in the atlas tree.

Hosts

The tab presents the list of devices belonging to the selected map.

Agents

The tab presents a list of devices with installed Agents. Among others, the basic stats and awaiting commands are displayed.

Fixed assets

The tab presents a list of all fixed assets.


15.4 Audit

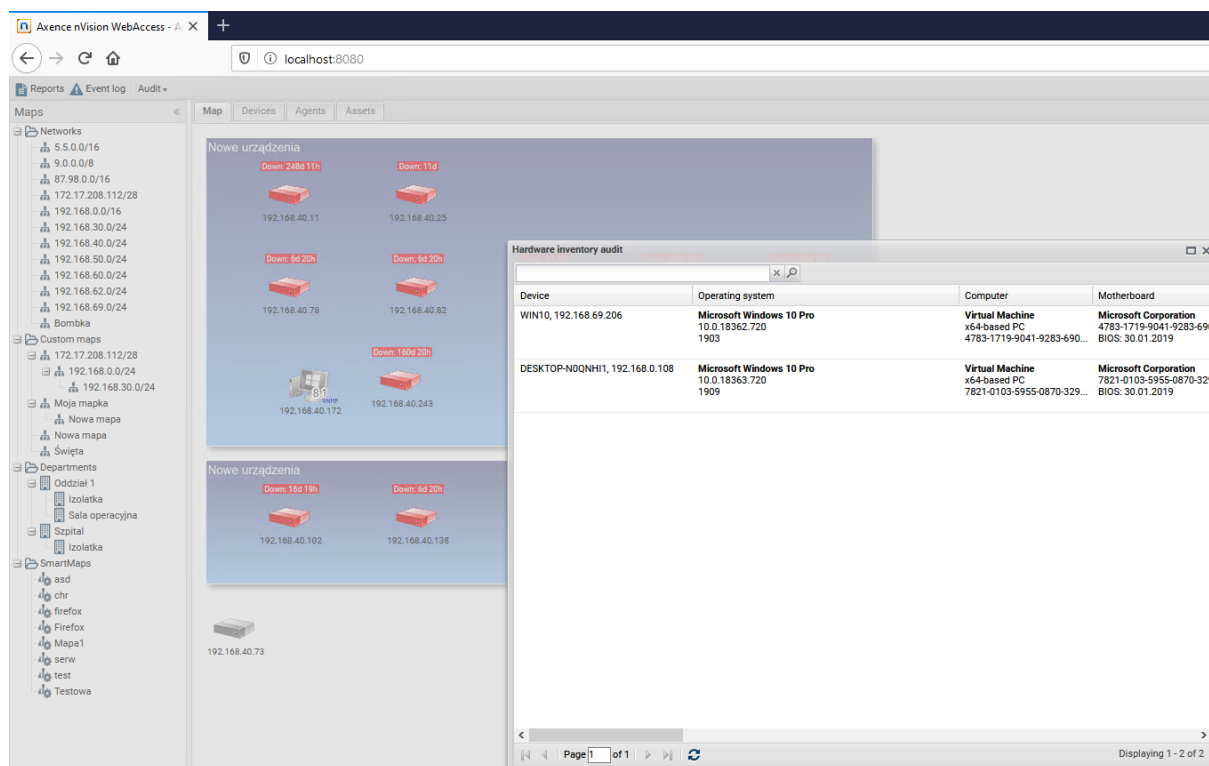
Axence nVision® automatically collects information on the hardware configuration of each machine with the Windows operating system and on the installed software.

Hardware

Hardware inventory allows the devices in the monitored networks to be controlled. The view displays information on the hardware configuration of all monitored devices – from the operating system to CPUs, displays and many others to local printers.

To view the hardware configuration of monitored devices:

1. Click the  **Audit** button in the top part of the window.
2. Select the **Inventory** option.
3. To find the required entries more quickly, use the search feature in the top part of the window.
4. To change the number of displayed columns, sorting or grouping methods, expand the menu at the column headers.




| Device | Operating system | Computer | Motherboard |
|-------------------------------|--|---|---|
| WIN10, 192.168.69.206 | Microsoft Windows 10 Pro 10.0.18362.720 1903 | Virtual Machine x64-based PC 4783-1719-9041-9283-690... | Microsoft Corporation 4783-1719-9041-9283-690... BIOS: 30.01.2019 |
| DESKTOP-N0QNH1, 192.168.0.108 | Microsoft Windows 10 Pro 10.0.18363.720 1909 | Virtual Machine x64-based PC 7821-0103-5955-0870-329... | Microsoft Corporation 7821-0103-5955-0870-329... BIOS: 30.01.2019 |

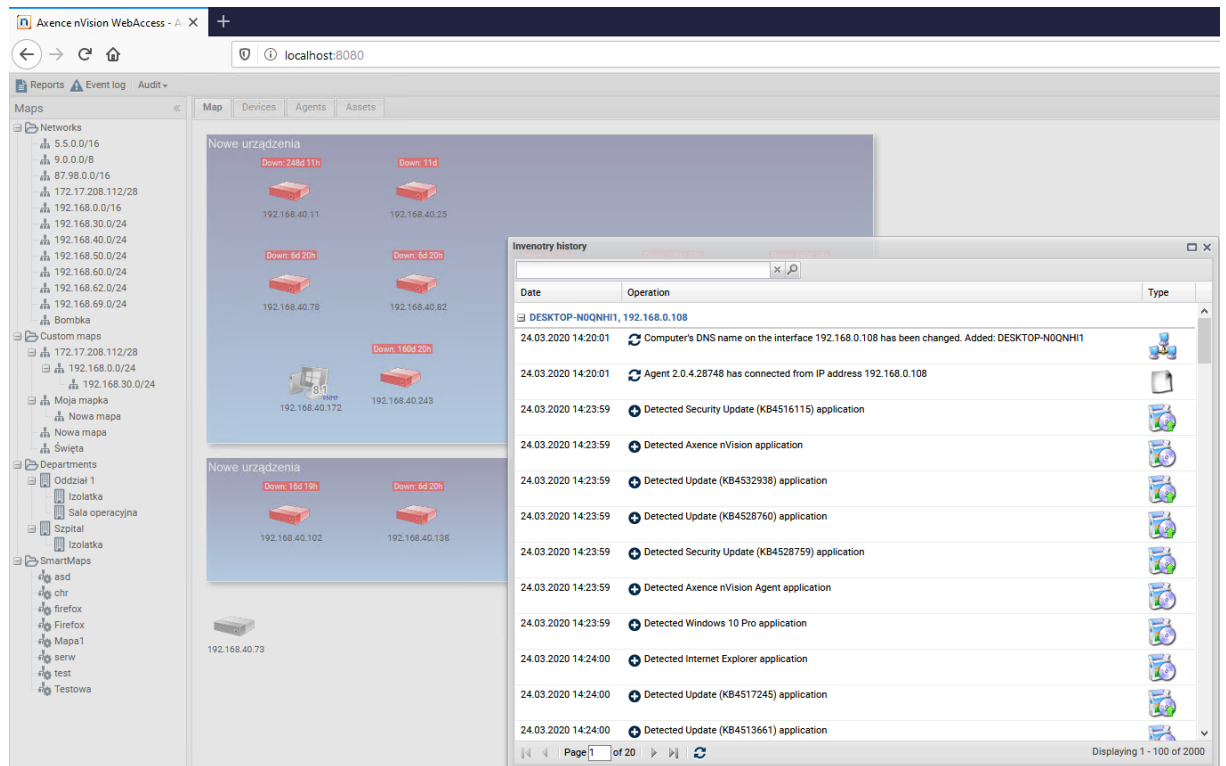
Inventory history

The tab contains information on the changes of hardware and software for all monitored devices.

To view the inventory history:

1. Click the  **Audit** button in the top part of the window.
2. Select the **Inventory history** option.
3. To find the required entries more quickly, use the search feature in the top part of the window.

- To change the number of displayed columns, sorting or grouping methods, expand the menu at the column headers.




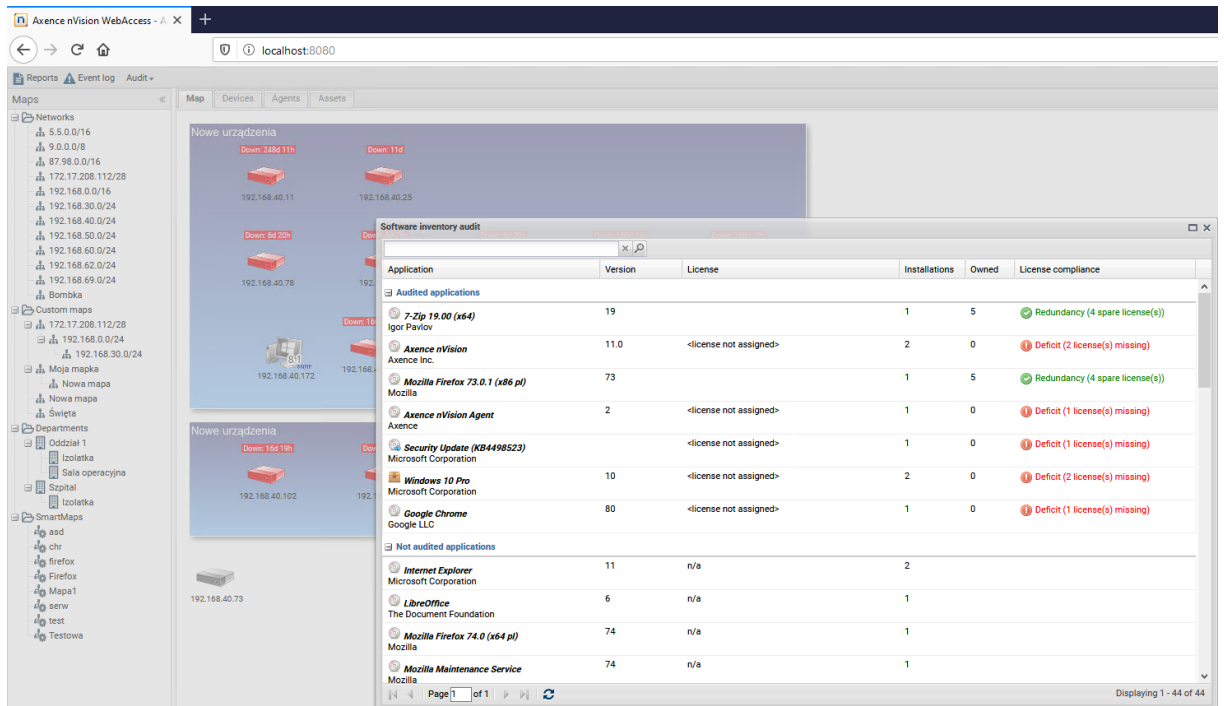
Software inventory audit

Software inventory allows the applications installed on the monitored user machines to be controlled. There are three categories of entries: audited applications (licensed software recognized by nVision and subject to auditing), non-audited applications (software recognized by nVision, not requiring licensing and not subject to auditing) and unknown applications (detected by nVision, but without a determined fingerprint).

In the case of audited applications, the information on the license type, number of instances within the monitored network and the number of owned licenses is displayed. The data are used to calculate the licensing compliance, which is visually presented and any surplus or missing licenses are highlighted.

To view the software inventory audit:




- Click the  **Audit** button in the top part of the window.
- Select the Software option.
- To find the required entries more quickly, use the search feature in the top part of the window.
- To change the number of displayed columns, sorting or grouping methods, expand the menu at the column headers.



Printouts

The printing audit window allows the printing history in selected periods (day, week or month) to be viewed. Data are sorted by printers, and then chronologically.



To view the printing audit:

1. Click the  **Audit** button in the top part of the window.
2. Select the  **Wydruki** option.
3. Select the period for the displayed data.
4. To find the required entries more quickly, use the search feature in the top part of the window.
5. To change the number of displayed columns, sorting or grouping methods, expand the menu at the column headers.
6. To check the details of the specific printing job, click the  button to expand the entry.

DataGuard

DataGuard audit window allows the history of printouts in the selected period (day, week or month) to be viewed. Data are sorted by printers, and then chronologically.

To view the printing audit:

1. Click the  **Audit** button in the top part of the window.
2. Select the  **DataGuard** option.
3. Select the period for the displayed data.
4. To find the required entries more quickly, use the search feature in the top part of the window.

5. To change the number of displayed columns, sorting or grouping methods, expand the menu at the column headers.

Part



16 Database backups

16.1 How to make a backup of my Atlases?

All atlases' information is stored in the `\Database\AtlasPG` directory.

To make a backup, use the **DBBackup** tool from `{nVision}\Backups` directory. Launching the **DBRestore** tool will restore nVision's database backup.

16.2 Automatic backup

Profiles

Creating backups is based on defined profiles. Each profile may specify:

- the directory where the created backups will be saved,
- the profile name,
- backup date.

The backup can store the selected data:


- collected Windows system log entries,
- generated alerts,
- counter and service monitoring history,
- user activity data,
- inventory data.

Backup rules

To configure backups, multiple profiles can be used. Each profile stores backup frequency (each day, week or month) and the time when the backup is to be performed. In each case the hour of the backup start is specified. If the backup is performed weekly, additionally set the weekday, if monthly – set the day of the month. In the case of large databases, creating backups can be a time-consuming task, therefore planning full backups for such times when it will not interfere with nVision operation in business hours is recommended.

Configuration

To configure the automatic creation of backups:

1. In the main menu of nVision select **Tools / Options**.
2. Select **Maintenance** from the list.
3. Add a new rule with the use of the  button or **Edit** one of the existing rules.
4. In the **Backup rules** window, select an existing profile or create a new one (to create a new profile, expand the menu at the **Edit** button, choose the **Add** option and configure the new profile settings).
5. Set the backup frequency and the times when the backup will be performed.

6. You can also define the number of stored backups.

16.3 Database size

As an effect of collecting a large amount of data in the monitored networks, the database size can grow rapidly. This chapter explains how to counteract the excessive database growth.

Database size management can be performed by means of:

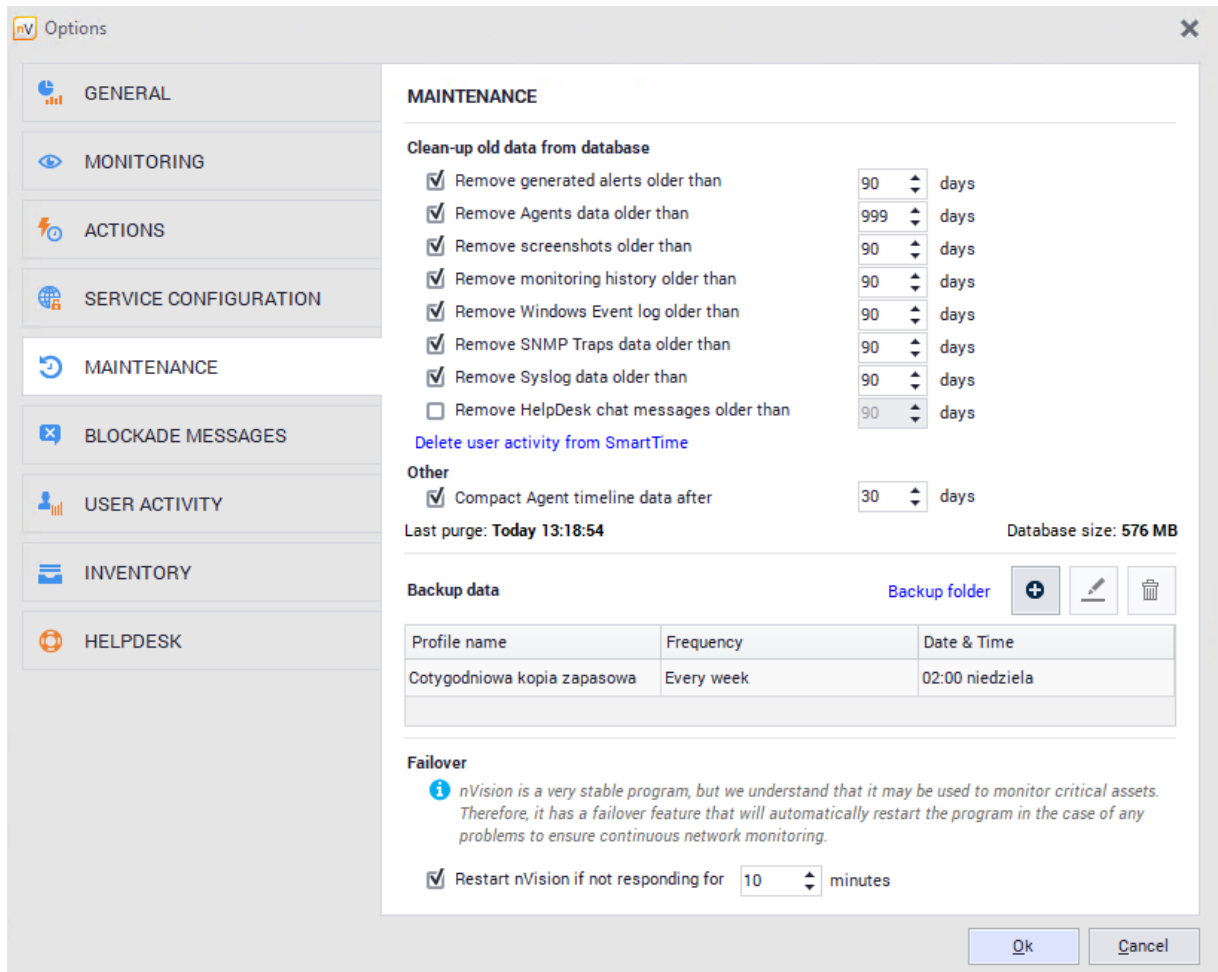
- Setting a time for the deletion of outdated data
- Compacting
- Windows event log monitoring options
- Database repairing

Setting the outdated data removal interval

To set the time after which the outdated data will be removed, use the cleaning option (**Options / Maintenance**). Data cleaning is performed once a day during the night.

Decreasing the time after which the outdated data are removed does not reduce the database size, but will stop its growth at a certain level. This is because the outdated data are not deleted from the database, but overwritten with the newly arriving data.

*Screenshots are the main reason of the huge size of nVision's database. Because of that fact, during turning of this functionality in the **Host info / User activity / Screenshots** ^[171] window, administrator has to point out a date when collecting them will be stopped.*



Windows Event Log monitoring options

The large growth of the database is most often the result of collecting data on user logons (Windows Event Log). If the monitoring of Windows Event Log does not need to be collected, toggle the respective field in the device **Properties**, the **Monitoring** tab. If the data should be collected, set the appropriate monitoring interval and check whether the logon entries ignore option is enabled in the configuration (enabled by default). This setting allows unnecessary entries to be filtered (approx. 99% of all entries).

16.4 Backup folder change

nVision allows you to change the default backup location. To do this, in the **Main** tab select **Options**, and then **Maintenance**. Next, select the highlighted **Backup folder** option and specify the new location:

The screenshot shows the 'Options' dialog box for nVision, with the 'MAINTENANCE' tab selected. The left sidebar contains navigation options: GENERAL, MONITORING, ACTIONS, SERVICE CONFIGURATION, MAINTENANCE (selected), BLOCKADE MESSAGES, USER ACTIVITY, INVENTORY, and HELPDESK.

MAINTENANCE

Clean-up old data from database

- Remove generated alerts older than 90 days
- Remove Agents data older than 999 days
- Remove screenshots older than 90 days
- Remove monitoring history older than 90 days
- Remove Windows Event log older than 90 days
- Remove SNMP Traps data older than 90 days
- Remove Syslog data older than 90 days
- Remove HelpDesk chat messages older than 90 days

[Delete user activity from SmartTime](#)

Other

- Compact Agent timeline data after 30 days

Last purge: Today 10:16:07 Database size: 577 MB

Backup data Backup folder + ✎ 🗑️

| Profile name | Frequency | Date & Time |
|-----------------------------|------------|-----------------|
| Cotygodniowa kopia zapasowa | Every week | 02:00 niedziela |

Failover

i nVision is a very stable program, but we understand that it may be used to monitor critical assets. Therefore, it has a failover feature that will automatically restart the program in the case of any problems to ensure continuous network monitoring.

- Restart nVision if not responding for 10 minutes

Ok Cancel

Note! Modification of this setting is only possible from the level of the local nVision console connected to the server using the address 127.0.0.1.

Part

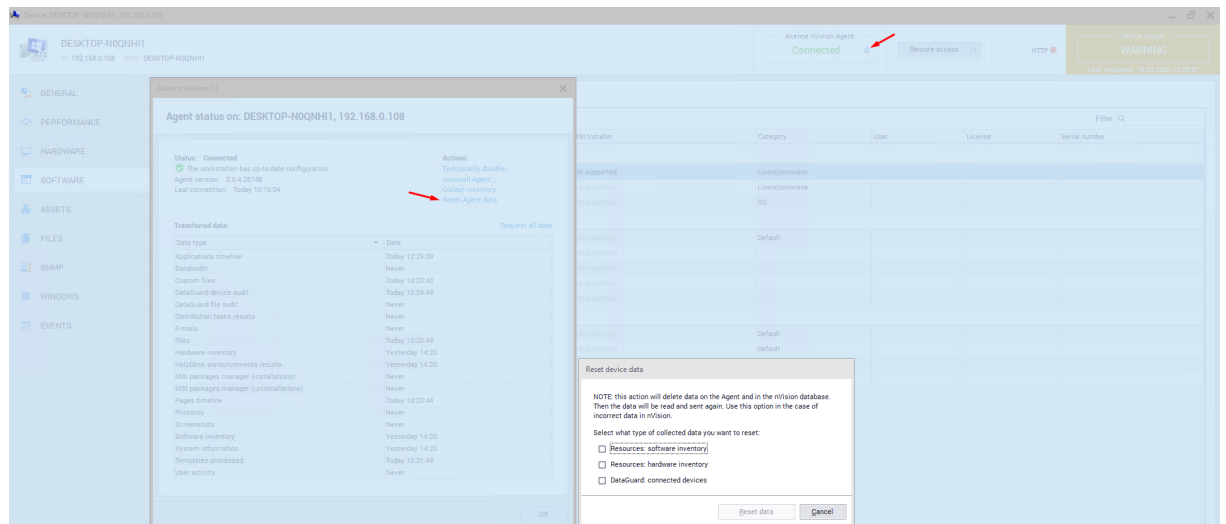


17 Frequently Asked Questions

17.1 Agent data reset

In order to solve certain problems with some missing monitoring data (e.g. gaps in User activity or outdated inventory data), it might be necessary to restart the Agent data.

This will result in the resending of the missing data if they are available in the Agent's database.



For this purpose, perform the following steps in the **Host Info** window:

1. Click the “i” icon in the upper part of the **Host Info** window.
2. In the **Actions** section, select **Reset host data**.
3. In the **Reset Agent data** dialog box mark the selected data types which should be reset. Click the **Reset data** button.

Note: Checking the **Force Agent on this host to reset all its data and collect it once again** option will delete the data collected by the Agent from its database and from nVision database, and will restart the data collection from the moment of resetting. This option should be used only in the case of resetting hardware and software inventory data.

17.2 Agent installation with use of Active Directory

Instructions for software distribution with use of Active Directory:

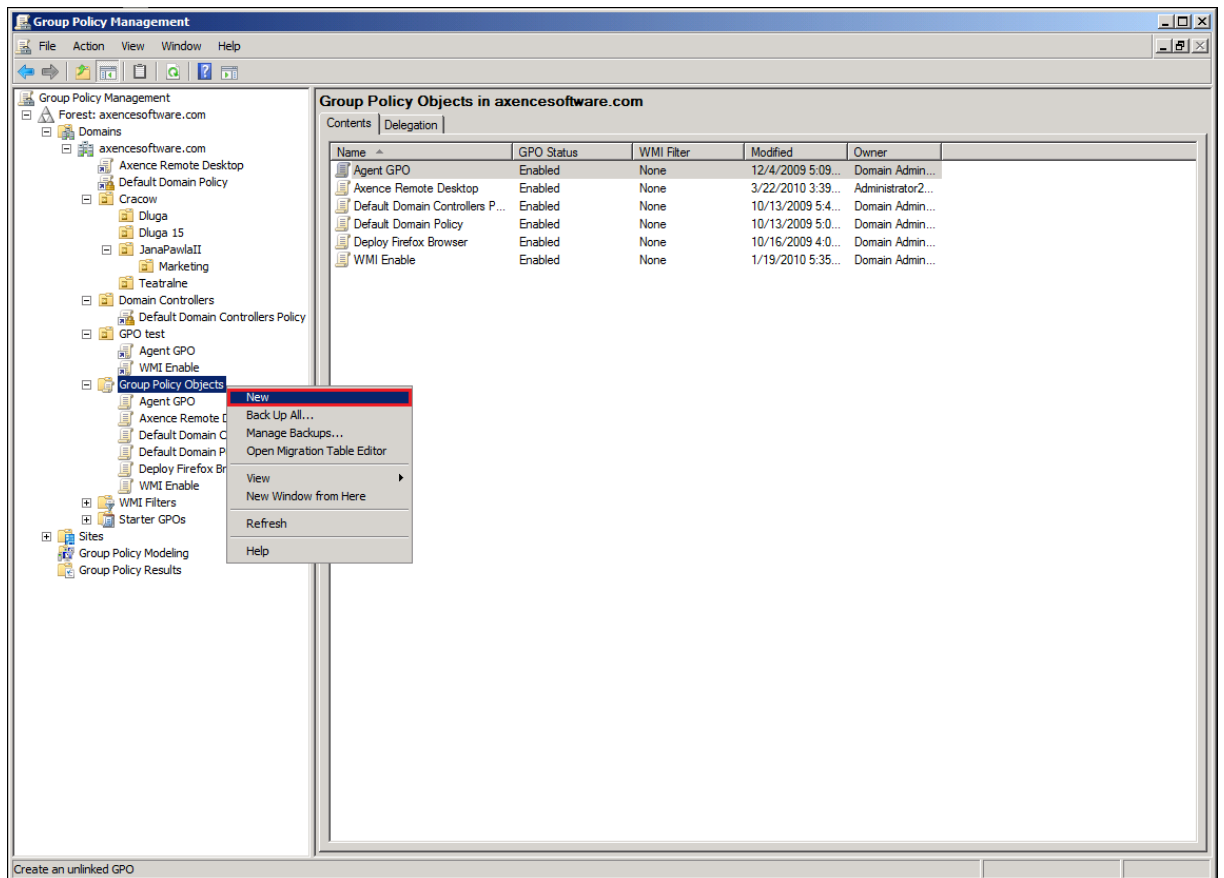
1. Place the **MSI package (nvagentinstall.msi)** in the shared folder on the server so as the workstations and domain controller (the server supporting Active Directory) can access it: create such a folder, copy the package there and set the sharing rights appropriately (resource access as follows:

```
\\ [ SERVER_NAME ] \ [ DIRECTORY_NAME ] \ nvagentinstall.msi
```

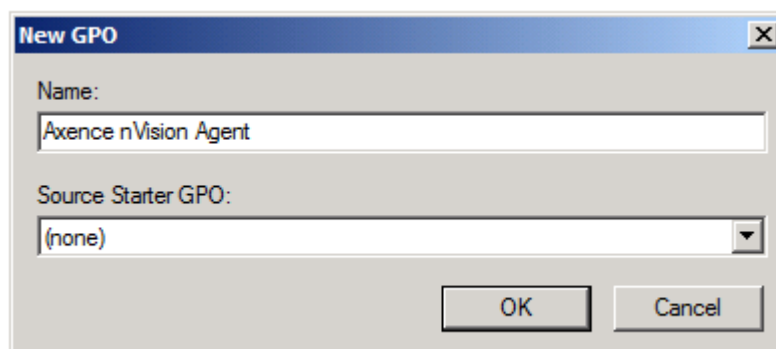
2. Run **Group Policy Management Console** – command:

```
gpmmc.msc
```

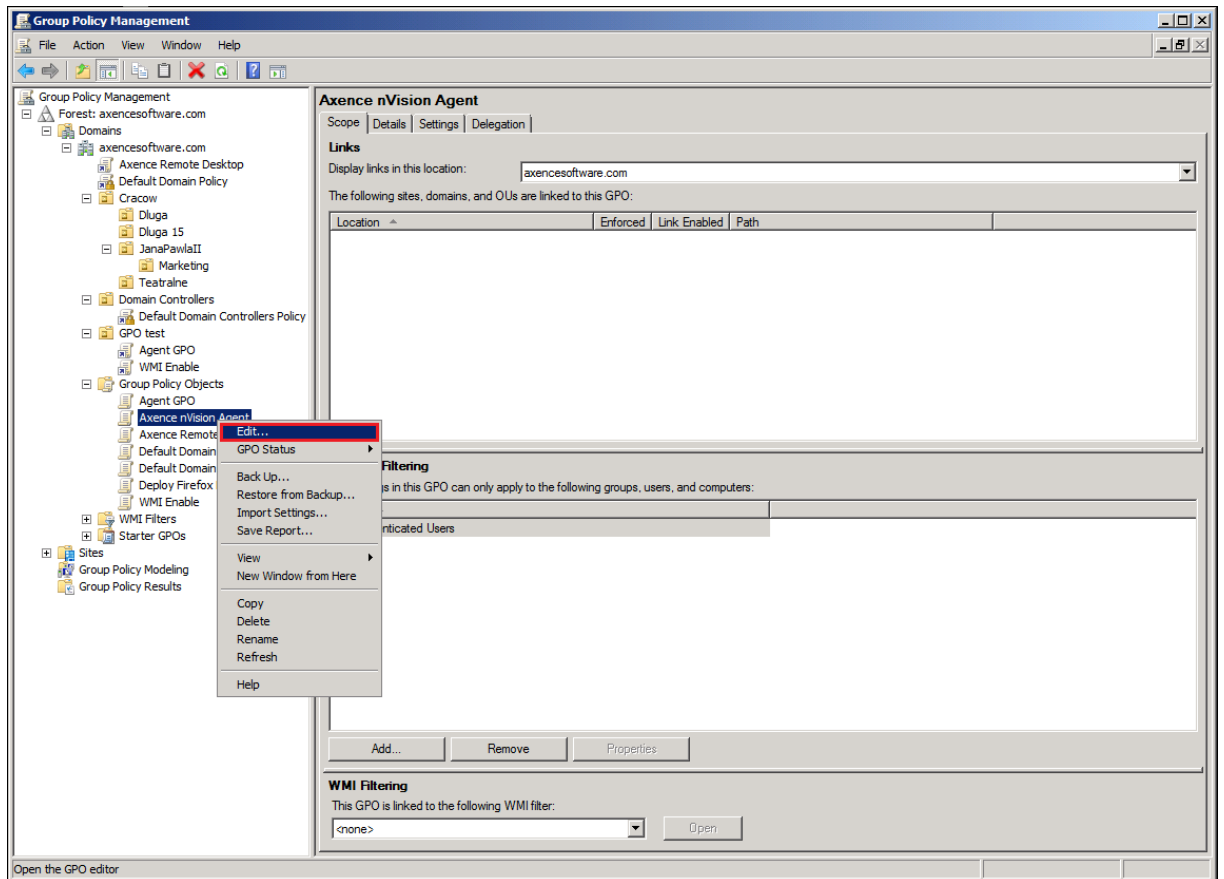
3. Create a new group policy object: select the **Group Policy Objects** folder, right-click it and select **New** from the drop-down menu.



4. In the **New GPO** dialog box, name the created Group Policy Object, e.g. Axence nVision Agent.



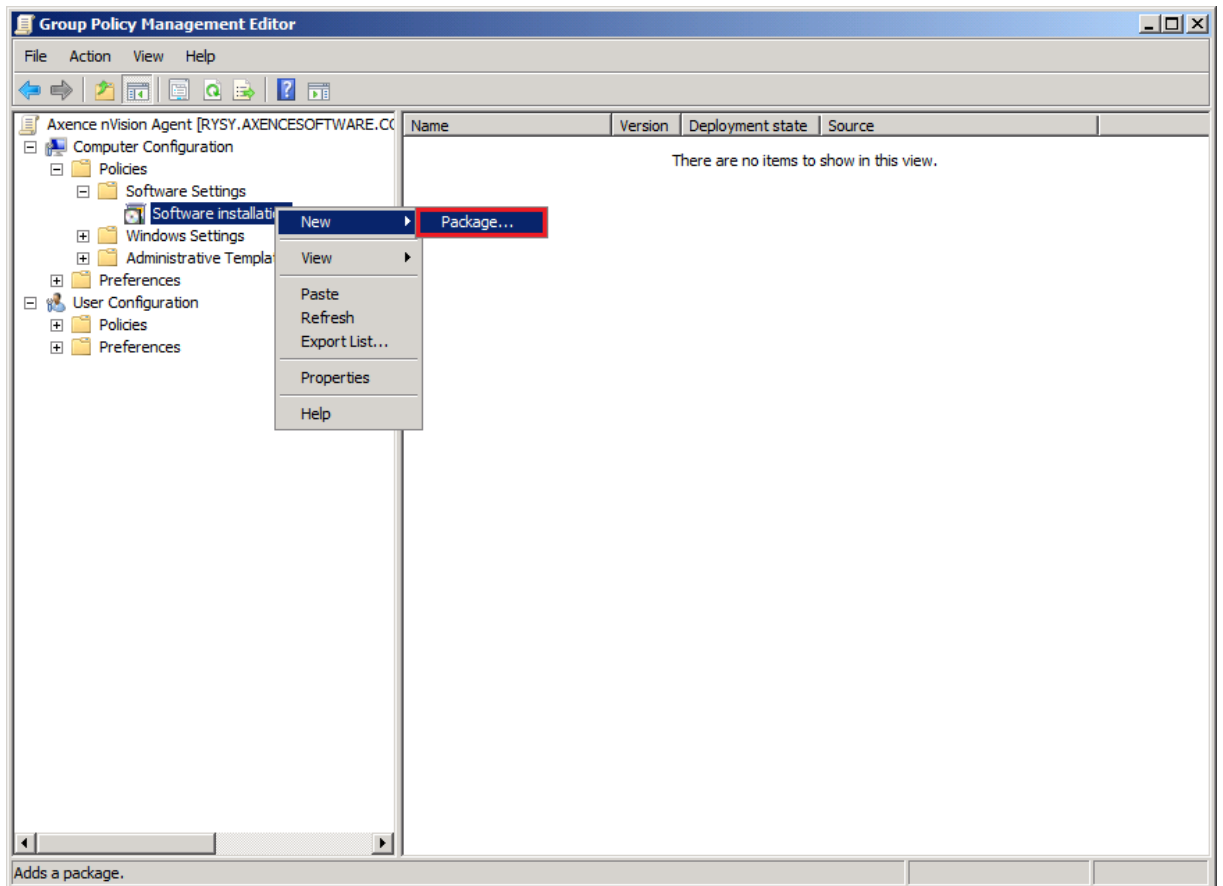
5. Navigate to edit the created GPO: right-click the object, select **Edit** from the drop-down menu.



6. In the **Group Policy Management Editor** dialog box, expand:

Computer Configuration \ Policies \ Software Settings \ Software installation

right-click it and select **New > Package** from the drop-down menu.

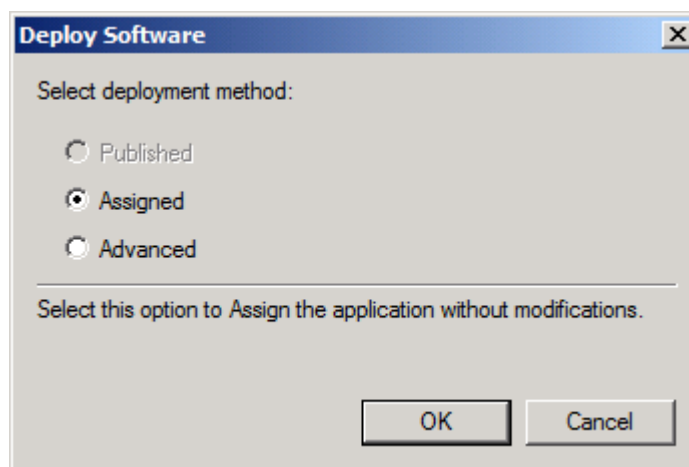


7. Select MSI package file in the resource sharing location (it is best to enter the address of the shared resource).

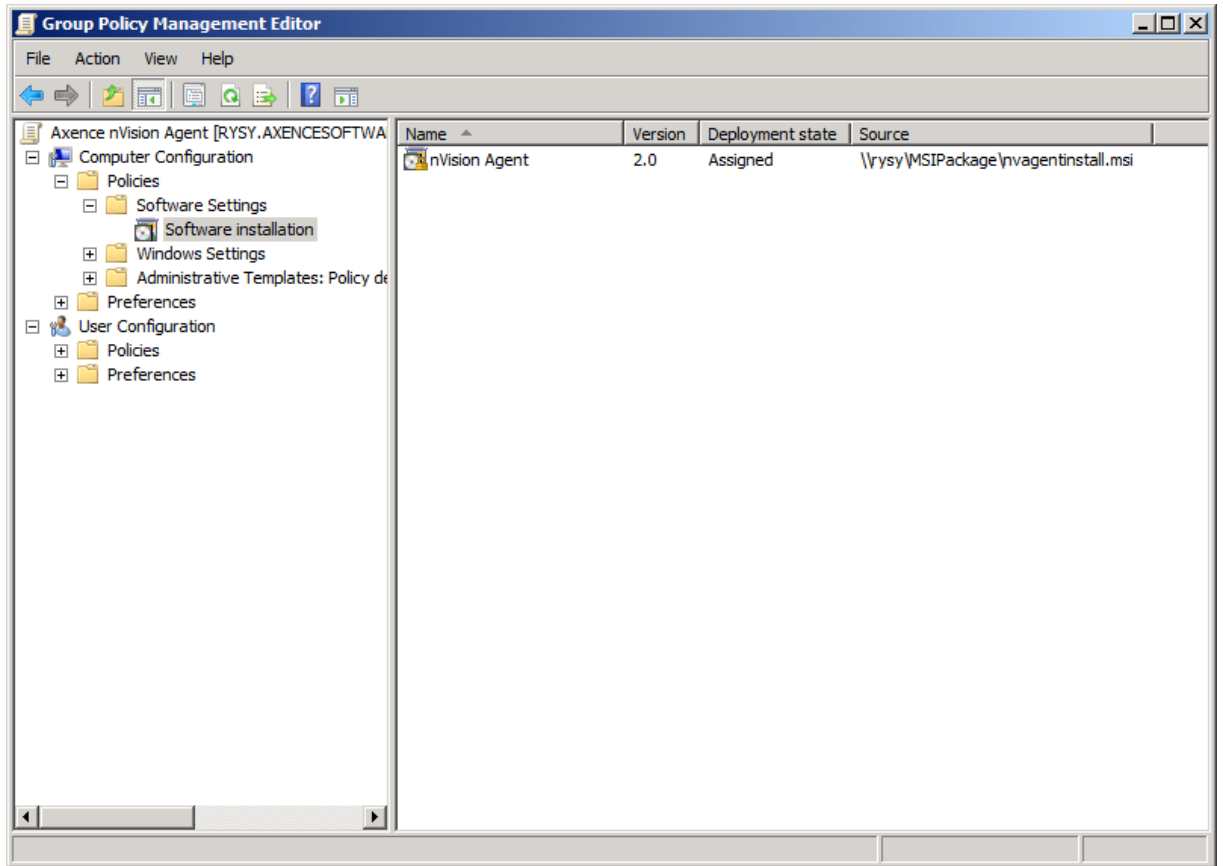
```
\\ [ SERVER_NAME ] \ [ DIRECTORY_NAME ] \
```

and choose the package type.

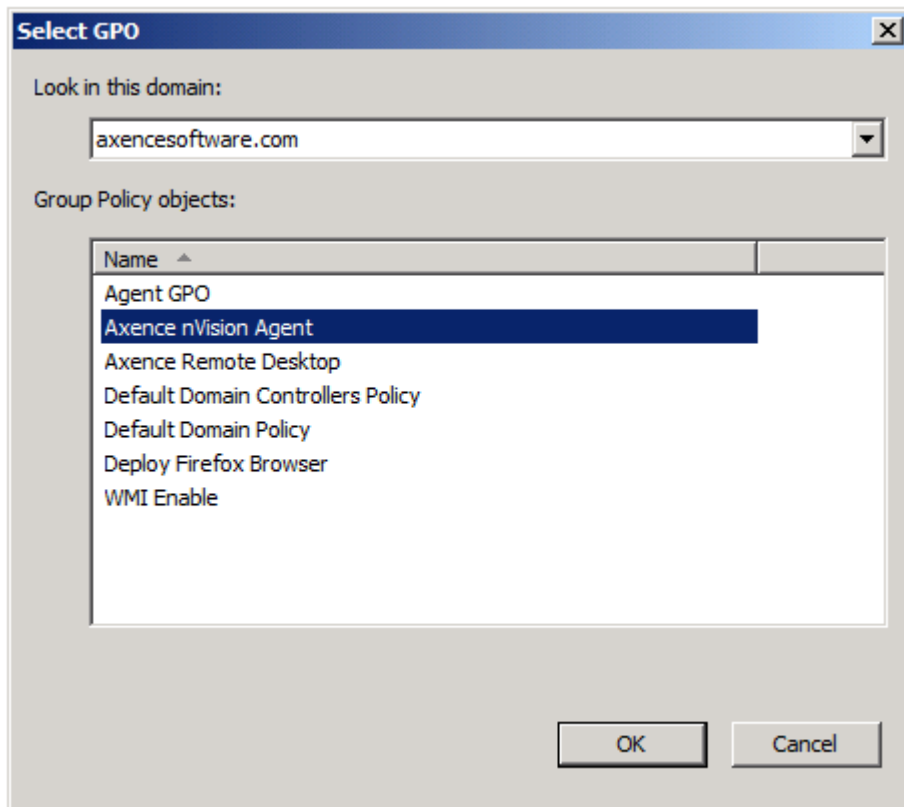
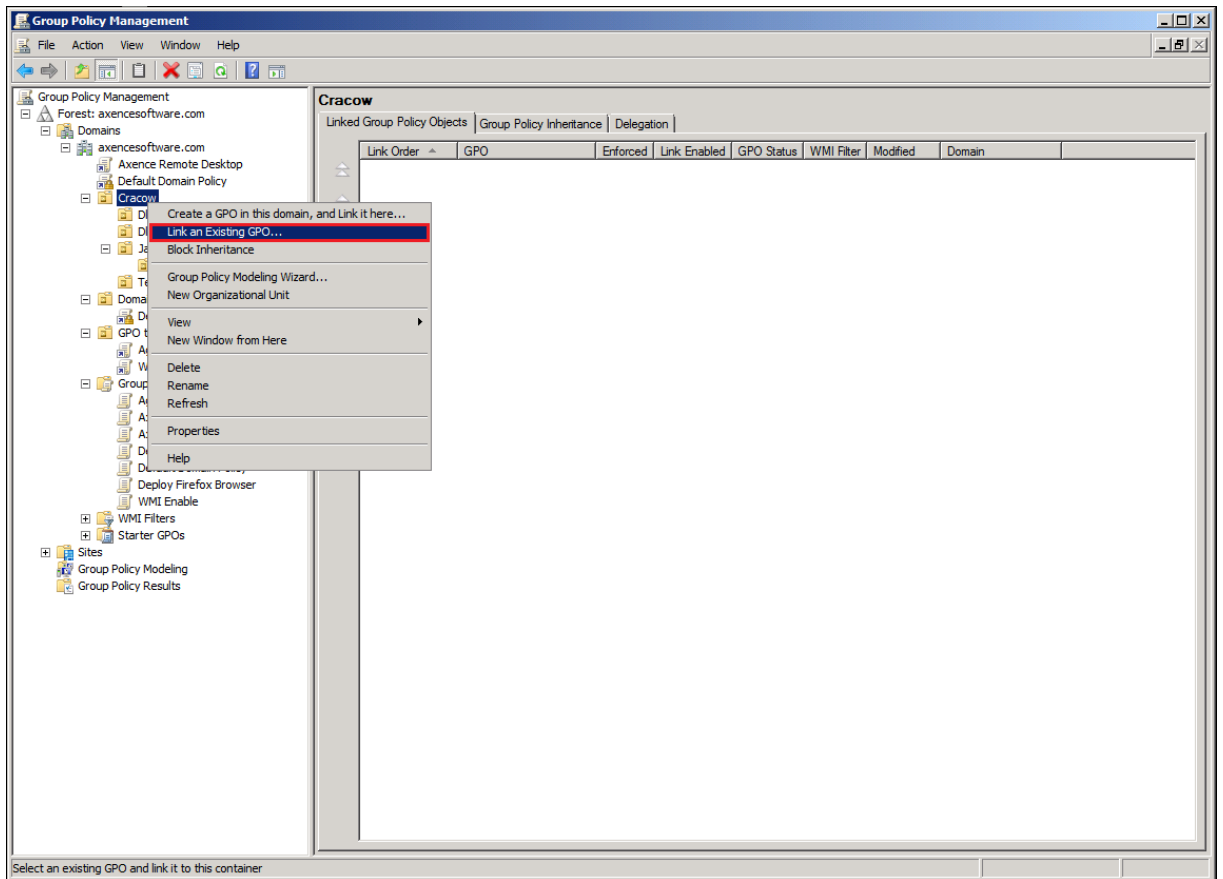
8. In the **Deploy Software** dialog box, select **Assigned**.



9. **nVision Agent** entry should appear in the **Group Policy Management Editor** dialog box.



10. Having created the GPO, return to the **Group Policy Management** dialog box and link the GPO to a container of the user group or machine group: select the container where the GPO should be assigned to, right-click it, select **Link an Existing GPO** from the drop-down menu, then select the created GPO.



11. The object created in such a manner should be distributed to workstations. The group policy updating can take a few hours; to accelerate it, execute command:

```
gpupdat e / f or ce / boot
```

on workstations to force the group policy updates, and in consequence, the installation of the MSI package with nVision Agent. In the case of failure, error messages can be found in the **Windows Event Log** of the workstations and the server.

17.3 Antivirus software proper setup

In order to assure the correct operation of nVision in accordance with program requirements, add the following folders to the anti-virus software exclusion list (disk operations and network connection):

- C:\Program Files\Axence*.*
- C:\Program Files (x86)\Axence*.*

including subfolders on:

- the machine where nVision Server is installed,
- the machines where nVision Consoles are installed,
- the machines where nVision Agents are installed.

Then restart these machines:

Examples:

- [Eset Antivirus](#)
- [Kaspersky Antivirus 2018](#)
- [AVG Antivirus](#).

17.4 Cloning the disk image with Agent installed

During installation, nVision Agent generates and saves its unique GUID identifier in the registry. If the Agent detects the change of machine SID, where it is installed on, it generates a new GUID during startup. The correct sequence of steps should include the preparation of the operating system with SysPrep utility before cloning the disk image to other machines. In such a case, when starting each cloned system, a new unique SID is generated, and Agents from these systems report in to nVision with different (unique) GUIDs and thus they create separate icons in nVision. Otherwise, each system reports to nVision under the same GUID, i.e. a few Agents send their data to the same icon in nVision.

If such a situation occurs, use SysPrep utility to reset SIDs on individual machines:

<http://technet.microsoft.com/en-us/library/cc721973>.

17.5 Configuration of Agents installed on mobile computers

In order to configure an Agent installed on a mobile machine (operating outside the local network):

1. open port **4436** on the router/firewall with an external address for incoming connections and redirect the traffic to port **4436** of the computer in the local network on which nVision Server is installed;
2. when installing nVision Agent on a mobile machine, provide it with an external **IP address of the router**.

If it is necessary to configure the connection of mobile machines with Agents, which at present are already using a local IP address of a computer with nVision, you can use the **Tools and options** tab, **Agents / Propagate new Atlas address** option and provide a new external IP address of the router. After propagating the new address (adding it to Atlas list in the configuration of nVision Agents), nVision Agents will attempt to connect with each of the addresses on their list. The connection will only be established if GUID and the password are identical in nVision Agent and in nVision Server. The Atlas to which the Agent cannot be connected for 21 days will be deleted from the nVision Agent's list of Atlases (if there is only one Atlas in the list, it will be never removed).

Related topics

 [Ports used by nVision](#) ⁶⁴⁸

17.6 Duplicated hosts

If duplicate devices, visible in the **Tools / Show duplicates** menu, appear in nVision, run the following command in the command line in relation to the duplicate IP addresses and DNS names:

```
ping -a IP_ADDRESS
```

and:

```
ping -4 DNS_NAME
```

and compare the results of these operations (there should be identical IP addresses and DNS names). If these do not match, look for the solution of the problem in incorrect DNS server configuration (aging / scavenging old records: <http://technet.microsoft.com/en-us/library/cc771677.aspx>) and/or too short IP address lease time on DHCP server (this time should not be shorter than aging / scavenging period of old DNS records).

17.7 File system audit

From the perspective of the file system, there is no such operation as “copy from... to ...”. The application, which “copies” the file, as a matter of fact creates a new file and fills it with the content read (acquired) from any source: another disk, network, external device connected to the computer, text entered from the keyboard in the application window, etc. Therefore it is not possible to log information about the data source in DataGuard.

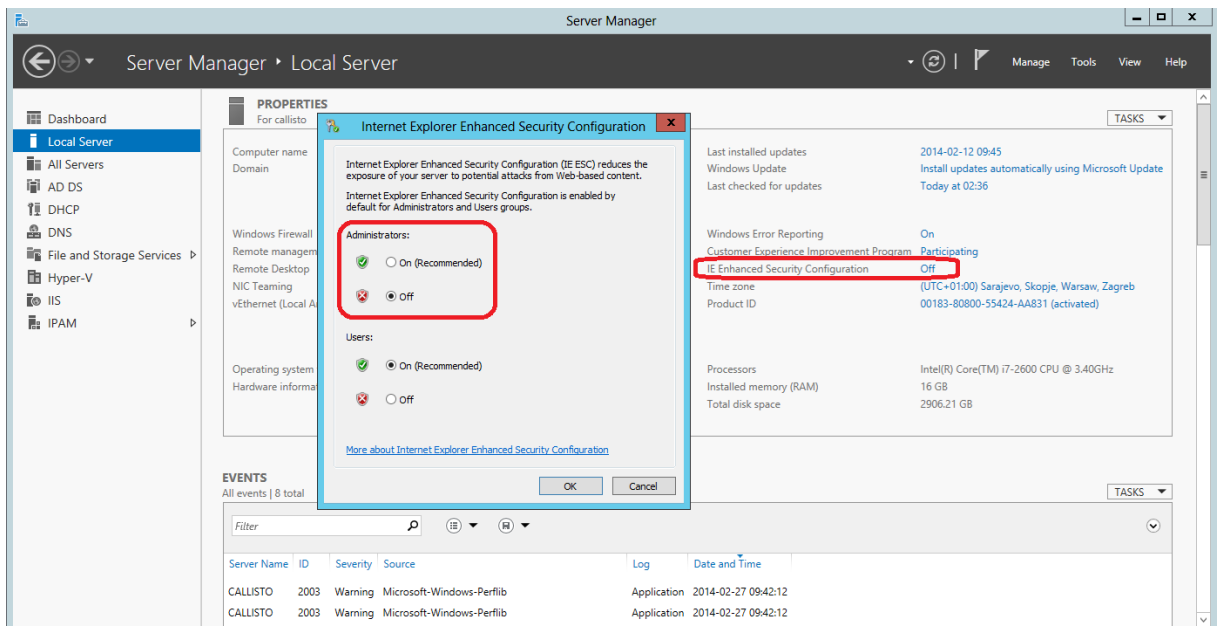
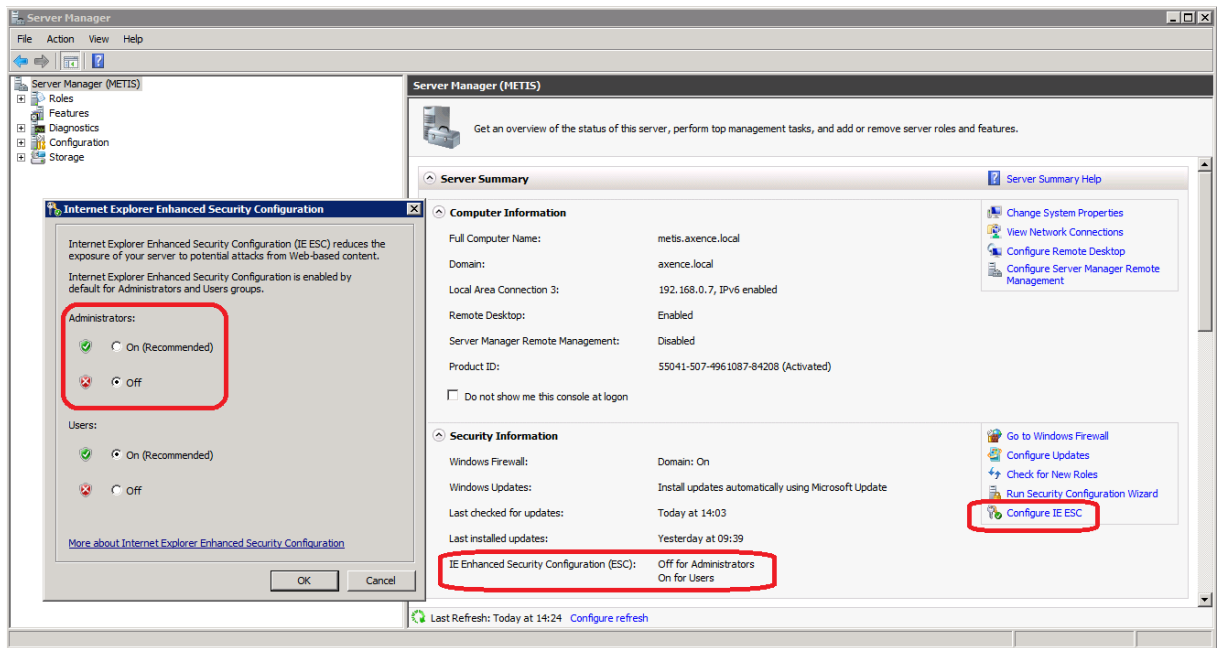
17.8 Generating reports on Windows Server systems

In case of problems with generating reports in nVision Console installed on Windows Server or in Internet Explorer on such a system, disable **IE ESC (Internet Explorer Enhanced Security Configuration) setting for administrators** on this system in the Windows Server configuration. After disabling it, restart nVision Console. Disabling this option changes web browser safety level on the server, therefore it is recommended to generate reports in nVision Console installed on the desktop version of Windows or in a web browser on a desktop system.

For details see:

<http://blogs.technet.com/b/plitpromicrosoftcom/archive/2010/04/30/internet-explorer-enhanced-security-configuration.aspx>

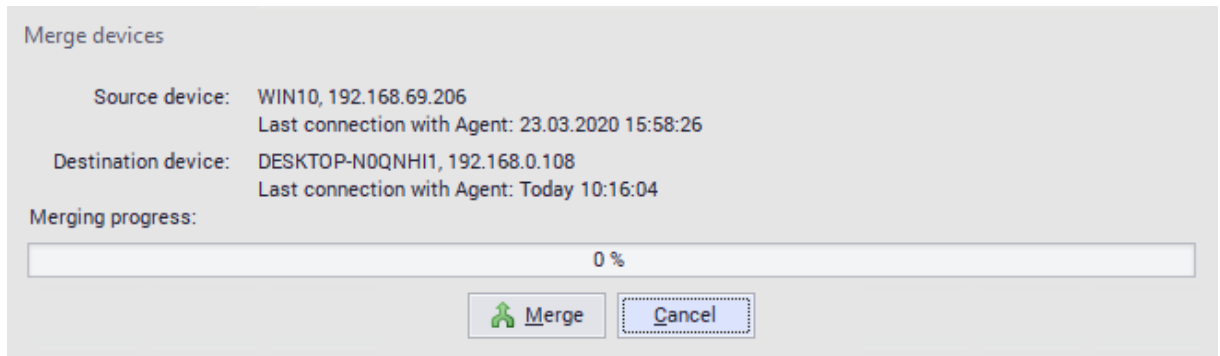
[http://technet.microsoft.com/en-us/library/dd883248\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd883248(v=ws.10).aspx)



17.9 Hosts merging

To merge hosts with Agents:

1. In the **Hosts / Agents** view, select hosts to be merged.
2. Right-click and select the **Agent / Merge hosts** option. The **Merge hosts** window will open.
3. To start the merging process, press **Merge** button. The old host will be removed from the map.



17.10 How “Uninstall nVision Agent” option works

The Agent will be uninstalled after receiving uninstallation command during connection with the nVision Server.

If the Agent is not connected with the nVision Server (e.g. the Agent was temporarily disabled or the machine where the Agent is installed is not running), uninstallation will proceed during the next connection with the nVision Server.

17.11 Installing Agent through WMI

To install nVision Agent remotely with the use of WMI, perform the following steps on the destination machine:

1. open the command line with administrator rights and run **WmiEnable.exe** (available in nVision installation folder)
2. make sure that “**File and Printer Sharing**” is enabled in Windows:
 - o **Windows 7 and 8:** *Control Panel / Network and Sharing Center / Advanced sharing settings* (option on the left side of the dialog box);
 - o **Windows Vista:** *Control Panel / Network and Sharing Center;*
 - o **Windows XP:** *Control Panel / Windows Firewall / Exceptions;*
3. check the properties of the machine in nVision to make sure that the Windows logon data test is passed successfully

17.12 Launching SNMP in Linux system

How to run SNMP in Linux system (on the example of openSUSE distribution):

1. Install **net-snmp** packages (with dependencies)
2. Open ports **161 TCP** and **161 UDP** in the firewall
3. Open command line, enter:

```
su -
```

followed by the root user password

4. Run **gedit** from the command line and edit the **/etc/snmp/snmpd.conf** file
5. To have access to the entire SNMP tree for reading, enter:

```
view systemonly included . 1
```

```
r o c o m m u n i t y p u b l i c d e f a u l t
```

and save such modified file

6. If you want SNMP service to start during each system boot, enter in the command line:

```
ch k c o n f i g s n m p d o n
```

7. Now run SNMP service by entering in the command line:

```
s e r v i c e s n m p d s t a r t
```

When the above procedure has been performed, open **Credentials** tab in the properties window of selected host in nVision, select **SNMP manageable host** option and click **OK**. Then, when a device information window is opened, it is possible to view SNMP counters tree in the **SNMP** tab.

Especially interesting system information can be found in branch:

```
. i s o . o r g . d o d . i n t e r n e t . m g r t . m i b - 2 . h o s t
```

```
O I D : . 1 . 3 . 6 . 1 . 2 . 1 . 2 5
```

17.13 Monitoring multiple locations in nVision

There are a few ways to monitor several locations in nVision:

1. One installation of nVision Server and monitoring of devices in remote locations connected with the head office with use of VPN
2. One installation of nVision Server and monitoring of devices (in particular, sending data from nVision Agents) through the Internet
3. Independent installations of nVision Servers in remote locations:
 - o no central database (each nVision Server has an independent database)
 - o Agents accept configuration changes and new versions only from one nVision Server (Master Atlas)
 - o access to nVision Servers with nVision Console in LAN, with RDP in WAN or with a Web browser (nVision Web Access)

The **Users** tab allows the creation of user accounts and to assign each user to one of the three roles. It is described in detail in chapter Types of user roles.

17.14 Moving nVision to another machine

To move nVision to another machine, perform the following steps:

1. Use the **Tools / Agents / Propagate new Atlas address** menu option to propagate new Atlas address to Agents.
2. In the **Agents** view, in the **Last connection time** column, make sure all Agents have received new Atlas address (Agents' connection time should be later than the time when the new address was propagated).

3. Copy the installer file **nVisionSetup.exe** from the **<nVision>\Sources** folder (it will be required in the further part of the procedure).
4. Make sure the amount of free disk space on the target machine is twice larger than the size of the **<nVision>\Database** folder.
5. [Make a full backup](#)⁶³⁰¹ of the Atlas using the **DBBackup** tool, which is located in the **<nVision>\Backups** folder.
6. Uninstall nVision.
7. Install nVision on the new machine using the file downloaded in step 3).
8. Copy full backup made in step 5) to the target machine.
9. [Restore full Atlas backup](#)⁶³⁰¹ using the **DBRestore** tool.
10. Start nVision.
11. Go to the main nVision settings. Then, in the service configuration tab, change the HelpDesk IP address to the address of the new nVision server.

17.15 Not all users have been imported from Active Directory

The default value of **MaxPageSize** parameter (maximum page size supported for LDAP response) in Windows is 1000 records. If there are more users and groups in the Active Directory, then increase the **MaxPageSize** value in the LDAP protocol configuration.

For details see:

<http://support.microsoft.com/kb/315071>

17.16 OFFLINE inventory scanner parameters

The nVision offline scanner executable file can be run with following parameters:

`silent`

program does not display the window reporting its operation

`directory`

program results are saved in the specific path

`runonce`

if many files with previous scanning results are detected, the program will terminate immediately.

Example:

```
nVision_Invent oryScanner . exe - silent - runonce - directory " c : \ "
```

17.17 Ports used by nVision

The following ports should be open for incoming connections on the machines where nVision Server is installed:

nVision Server:

- 4434 – diagnostic information
- 4436 – permanent connection (socket) of the Agent
- 8080 – Web Access
- 8081 – API server
- 162 – SNMP trap.

nVision Agent:

- 4433 – diagnostic information

Machine from which the data from counters / services / Windows event log will be collected:

- 135, 139, 445, 593 – WMI

Windows Firewall is automatically configured during the installation of nVision Server and nVision Agent.

You need to configure firewalls from other producers on your own – for examples, see:

- [Eset Antivirus](#)
- [Kaspersky Antivirus](#)
- [AVG Internet Security](#)

17.18 Printouts monitoring

A locally installed Agent collects information about printouts from the printers installed as local ones only. In the case of printers configured as network devices, the Agent must be installed in the system on which the printer is provided. If the Agent will not be used for other purposes there, the Agent profile can be configured so as to only collect information about printouts.

17.19 Silent installation and uninstallation of nVision Agent

To install the Agent without user interaction, use the following command on the selected machine:

```
nvagent i nst al l . exe / ver ysi l ent / nVi si onon: ADRES_I P_nVi si on
```

or

```
msi exec. exe / i nvagent i nst al l . msi / qn
```

To uninstall the Agent without user interaction, mark selected machines in nVision Console, and then right-click and select the **Agent / Uninstall** options from the context menu

or use the following command on the selected machine:

```
uni ns000.exe /verysiilent /password=AGENTS_PASSWORD
```

17.20 Updating and archival versions of nVision

Technical issues to be taken into consideration while updating nVision:

1. Installation of nVision Server on Windows XP is no longer possible – minimum required system for nVision Server is Windows Vista or Server 2008 or newer, for nVision Console and nVision Agent minimum required system is Windows XP SP3 or newer.
2. Updating of nVision (or restoration from backup) **to version 7** is possible only from nVision (or its backup) of the latest build of version **6 (6.5.4.14214)**.
3. After updating nVision to the latest version 6, **run the program at least once (open Atlas)**, then close nVision and perform the database repair to verify the database before updating.
4. Atlas import can be performed only in the local console.
5. The software must be run first from the local console in order to set the administrator's password.
6. You can install nVision Console on another machine using the same **nVisionSetup.exe** file downloaded for nVision 7 update - after executing this file selection of installation type will be available: nVision Server+Console or nVision Console.
7. Updating of nVision to version 7.5 is possible only from nVision of the latest build of **version 7.1 (7.1.3.15872)**. Because of database rewriting this process can take longer time.
8. Because of database engine change after updating nVision to version 7.5 backup settings will be reset so the best is to check it and adjust it according to your needs.
9. Because of database engine change restoring database from backup in nVision 7.5 is possible only from backup created also in nVision 7.5.
10. To update nVision **to version 8.2**, you should first install the latest **version of nVision 7 (7.6.2.17769)**.
11. Updating of nVision to **version 9** is possible only from nVision of the latest build of **nVision 8.2 (8.2.1.20202)** or nVision **8.6 (8.6.0.22469)**.
12. Direct update to **nVision 10** is possible since nVision 8.6. Before updating to version 10, read carefully the document concerning [technical issues of migration to version 10](#).
13. Updating nVision to version 11 and 12 is possible by updating **nVision 8.2 (8.2.1.20202)** or newer.

Archival nVision installation files can be downloaded from the following sources:

- [nVision 6 \(6.5.4.14214\)](#)
- [nVision 7.1 \(7.1.3.15872\)](#)
- [nVision 7 \(7.6.2.17769\)](#)
- [nVision 8.2 \(8.2.1.20202\)](#)
- [nVision 8.6 \(8.6.0.22469\)](#)
- [nVision 9 \(9.3.4.25361\)](#)

- [nVision 10 \(10.5.3.27614\)](#)
- [nVision 11 \(11.9.1.29555\)](#)
- [nVision 12 \(12.5.3.31064\)](#)

17.21 Virtual machines

If you want to detect virtual machines in the network, you can create smart maps defining filters:

Primary MAC address / starts with / <type the first three octets from the list below>

If, on the other hand, you want the network scanner/rescanner not to detect virtual machines (e.g. due to exceeded limit of devices allowed by the license), add the first three octets from the following list, each followed by an asterisk, to the ignored addresses list (in the Atlas properties).

0003FF

Virtual PC

<http://blogs.technet.com/b/medv/archive/2011/01/24/how-to-manage-vm-mac-addresses-with-the-globalimagedata-xml-file-in-med-v-v1.aspx>

000569

VMware

<http://technet.microsoft.com/en-us/library/jj590655.aspx>

00155D

Hyper-V

<http://technet.microsoft.com/en-us/library/jj590655.aspx>

080027

VirtualBox

<https://forums.virtualbox.org/viewtopic.php?f=1&t=26295>

Index

- A -

A 117, 636
Access log 8
Actions 47, 604, 605, 606, 612, 613
ActionsCustom alert messages 613
ActionsDefining properties 606
ActionsManaging 606
ActionsNotification 47
ActionsSetup 612
ActionsTypes 605
Agent installation 115, 117
Agent installationActive Directory 115
Agent installationManual 117
Agent installationMSI installer 115
Agent installationRemote anti-virus software management console 117
Agents 45, 114, 115, 117, 118, 119, 125, 130, 132, 166, 173, 477, 636
AgentsAdvanced configuration 45
AgentsArchive 118
AgentsArchiving 118
AgentsBasic information 114
AgentsFile distribution 477
AgentsGUID 45
AgentsID 45
AgentsInstallation 115, 117
AgentsIntroduction 114
AgentsLarge number 45
AgentsPassword 118
AgentsPrintouts 173
AgentsProfile management 119
AgentsSetting 125
AgentsTroubleshooting 636
AgentsUninstallation 118
AgentsUser activity monitoring 166
AgentsView 132
AgentsWeb filtering profile 130
AI 588
Alerts 60, 63, 335, 336, 586, 587, 591, 592, 615
AlertsConcepts 586
AlertsConnection of a mobile de 336
AlertsDataGuard 335, 336
AlertsDisabling 588
AlertsEscalation 592
AlertsEvent log 615
AlertsFile operation on a mobile device 336
AlertsFiltering inherited alarms 588

AlertsInherited 591
AlertsManaging 588
AlertsManaging overview 587
AlertsOverview 586
AlertsPerformance counters 63
AlertsServices 60
Atlas 82
AtlasOverview 82
Audit 174, 339, 624
AuditDataGuard 339
AuditPrintouts 174
AuditWeb Access 624
Audyt
 Inwentaryzacja sprzetu 246, 248
Axence account 9, 10, 12, 14, 15
Axence accountActivation 15
Axence accountLog in 12
Axence accountManage 14
Axence accountRegistration 10

- B -

Backup 630
Backup copy 630
BackupAutomatic backup 630
BackupProfiles 630
Blocking access to websites 130, 169
Blocking access to websitesTroubleshooting 130
Blocking applications 167
Browser 620

- C -

Configuration 22, 27
ConfigurationPorts 22
Console 23
ConsoleInstallation 23
Counters 28, 61
CountersEnabling monitoring on Windows XP 28
CountersRequirements 28

- D -

D 327
Database 631
DatabaseProblems 631
DataGuard 316, 317, 319, 320, 321, 323, 324, 325, 326, 329, 331, 335, 336, 339, 343, 344
DataGuardAccess log 329
DataGuardAccess rights 316, 317, 320, 325
DataGuardActive Directory users 327

DataGuardAlerts 335, 336
 DataGuardAudit 339
 DataGuardCategories 316
 DataGuardConnected devices 331
 DataGuardConnected devices 323
 DataGuardDevice 320
 DataGuardDevice n 324
 DataGuardInherited rights 319
 DataGuardIntroduction 316
 DataGuardManagement 321
 DataGuardManaging access rights 316, 325, 326
 DataGuardQuick help 339, 343
 DataGuardTrustees 325, 326
 DataGuardTypical scenario 339
 DataGuardUSB devices 343, 344
 Departments 105, 106, 107
 DepartmentsAdding devices 106
 DepartmentsManaging 105
 DepartmentsReports 107
 DepartmentsStructure 105
 DHCP 166

- E -

Events 593, 595, 597, 604
 EventsDefining properties 597
 EventsManaging 595
 EventsOverview 593
 EventsRising, falling and reset thresholds 604
 EventsThresholds 604
 EventsTypes 593

- F -

FAQ 23, 42, 60, 63, 70, 71, 74, 77, 130, 167, 169, 324, 344, 477, 631, 636, 642, 643, 644, 645, 646, 647, 648, 649, 650
 File distribution 477
 Files 477
 FilesDistribution 477
 FilesExecute 477
 Frequent 647
 Frequently 648
 Frequently Asked Questions 645
 Frequently Asked Questions 23, 42, 60, 63, 70, 71, 74, 77, 130, 167, 169, 324, 344, 477, 631, 636, 642, 643, 644, 645, 646, 647, 648, 649, 650
 Frequently Asked Questions Cloning disk with Agent 642
 Frequently Asked QuestionsAgent installation with Active Directory 636

Frequently Asked QuestionsAgent uninstallation 645
 Frequently Asked QuestionsAntivirus software 642
 Frequently Asked QuestionsAudit 643
 Frequently Asked QuestionsDownloading the list of users from Active Directory 647
 Frequently Asked QuestionsDuplicated hosts 643
 Frequently Asked QuestionsInstalling Agent on laptop 642
 Frequently Asked QuestionsInstalling Agent through WMI 645
 Frequently Asked QuestionsInventory scanner 647
 Frequently Asked QuestionsLinux - SNMP 645
 Frequently Asked QuestionsMonitoring multiple locations 646
 Frequently Asked QuestionsMoving nVision Server 646
 Frequently Asked QuestionsPorts 648
 Frequently Asked QuestionsUpdating 649
 Frequently Asked QuestionsVirtual machines 650
 Frequently Asked QuestionsWindows Server reports 643
 Functionality 2

- G -

GSM devices 47

- H -

HelpDesk 349, 350, 356, 358, 360, 361, 363, 375, 377, 382, 417, 422, 424, 427, 440, 447, 456, 457, 458, 473, 477, 484
 HelpDeskAbsence plan 456
 HelpDeskActivity list 422
 HelpDeskActivity reports 440
 HelpDeskAutomations 458
 HelpDeskCategories 363
 HelpDeskChat 377
 HelpDeskClosed ticket reports 427
 HelpDeskConfiguration 349
 HelpDeskFile distribution 477
 HelpDeskHTTPS 350
 HelpDeskInterface 375
 HelpDeskKnowledge base 417
 HelpDeskMessages 473
 HelpDeskPriorities 361
 HelpDeskProcessed ticket reports 447
 HelpDeskRemote command execution 484
 HelpDeskReports 424
 HelpDeskSettings 356
 HelpDeskTicket processing 358

HelpDeskTrouble ticket assignment 457
 HelpDeskTrouble ticket database 382
 HelpDeskUsers 360
 Host 82
 Hosts 50, 55, 82, 98, 99, 101, 644
 HostsAdding a new host 55
 HostsInfo window 82
 HostsManaging 101
 HostsMerging 644
 HostsOverview 98
 HostsStatus 50
 HostsVisualization 99

- I -

Import skanów inwentaryzacji 307
 Inherited alerts 591
 Introduction 2
 Inwentaryzacja
 Aplikacje 254
 Audyt sprzętu 246, 248
 Informacje systemowe 250, 253
 Programy 254
 Skany 307
 Sprzet 246
 Inwentaryzacja programów
 Ustawienia 254
 Wprowadzenie 254
 Inwentaryzacja sprzętu
 Audyt 246, 248
 Historia 249
 Ustawienia 246
 Wprowadzenie 246

- L -

Limitations 20

- M -

Map layout 92
 Map layoutCreating 92
 Map layoutLayout assistant 92
 Maps 82, 90, 91, 92, 96
 MapsCreating objects 92
 MapsLayout 92
 MapsLocking 92
 MapsManaging 91
 MapsObject precedence 92
 MapsObjects 91
 MapsProperties of static objects 96

MapsTools 92
 MapsTypes 90
 MapsWorking with 92
 MIB file compiler 70
 Mobile phone configuration 47
 Modules 2, 3
 Monitor 62
 Monitors 130
 Monitorin 67
 Monitoring 55, 56, 57, 61, 66, 68, 166
 Monitoring e-mails 130
 Monitoring mail and 66
 Monitoring mail and web server 66
 Monitoring mail and web serverDefining counter properties 67
 Monitoring mail and web serverOverview 66
 Monitoring performance 61, 62, 63, 64
 Monitoring performanceCounter properties 64
 Monitoring performanceCounter types 62
 Monitoring routers and switches 68, 69
 Monitoring routers and switchesNetwork traffic 69
 Monitoring routers and switchesOverview 68
 Monitoring routers and switchesSwitch ports 68
 Monitoring services 57, 59
 Monitoring servicesManaging 59
 Monitoring servicesOverview 57, 61
 MonitoringConcepts 56
 MonitoringDHCP address assigned computers 166
 MonitoringMail server 66
 MonitoringNetwork interfaces 68
 MonitoringNetwork traffic 68
 MonitoringOverview 55
 MonitoringPerformance of the system and the device 61
 MonitoringPOP3 server 66
 MonitoringRouters 68
 MonitoringServices 57
 MonitoringSMTP server 66
 MonitoringSwitches 68
 MonitoringTCP/IP services 57
 MonitoringURL 66
 MonitoringUser activity 166
 MonitoringWeb p 66
 MonitoringWeb page load time 66
 MonitoringWeb server 66
 MonitoringWindows services 61

- N -

Network discover 51
 Network discovering 50
 Network discoveringIntroduction 51

Network discovery 53
 Network discovery Network discovery wizard 53
 Network monitor 50
 Network monitoring 50
 Network monitoringHost status 50

- O -

Options 42

- P -

Performanc 63
 Performance 45, 64
 Performance c 61
 Performance counter 62, 63
 Performance counterCreating a counter on many hosts at once 63
 Performance counters 64
 Performance countersAlerts 63
 Performance countersOverview 61
 Performance counterTypes 62
 Performance monitoringC 63
 Performance monitoringManaging 62
 Ports 22
 Printouts 173, 174, 175, 177, 648
 PrintoutsAudit 174
 PrintoutsIntroduction 173
 PrintoutsPrinter grouping 177
 PrintoutsPrinting costs 175
 PrintoutsTroubleshooting 648

- R -

Remote access 486
 Remote accessRequirements 486
 Remote console 8
 Remote waking up of the device 77
 Report a problem 46
 Reports 45, 560, 562, 569, 579
 ReportsCreating new reports 560
 ReportsIntroduction 560
 ReportsPerformance 45
 ReportsSegment types for host rep 562
 ReportsSegment types for map reports 569
 ReportsSegment types for user reports 579
 Requirements 20, 486
 RequirementsRem 486

- S -

S.M.A.R.T. 253
 Services 60
 ServicesAlerts 60
 Skany inwentaryzacji 307
 SmartMaps 107, 108, 109
 SmartMapsCreating 109
 SmartMapsFilters 107, 108
 SNMP trap 71
 Styles 101, 102, 104
 StylesDefining 102
 StylesManaging 104
 StylesOverview 101
 Syslog 74
 Syslog server 74
 System requirements 20

- T -

Thresholds 604

- U -

User activity moni 166
 User activity monitoring 115, 166, 167, 171, 172, 173
 User activity monitoringActive time 167
 User activity monitoringAgent installation 115
 User activity monitoringBandwidth usage 166
 User activity monitoringE-mails 172
 User activity monitoringGeneral 167
 User activity monitoringIntroduction 166
 User activity monitoringPrintouts 173
 User activity monitoringRequirements 166
 User activity monitoringScreenshots 171
 User activity monitoringUsed applications 167
 User activity monitoringVisited web pages 166, 167
 Users 621
 UsersWeb Access 621

- V -

Versions 3
 View 132
 ViewAgents 132

- W -

Wake On LAN 77
Web Access 620, 621, 623, 624
Web AccessAudit 624
Web AccessUsers 621
Web AccessWindow layout 623
WMI 477
WMI - problem 28
WMIFile distribution 477