# nVision axence® Overview of module functionalities

| FEATURES AVAILABLE FOR EACH MODULE | | NETWORK | INVENTORY | USERS | HELPDESK | DATAGUARD | SMARTTIME |
|---|---|---|---|---|---|---|---|
| **GENERAL** | **ADMINCENTER** | | | | | | |
| • Windows Agent | • displaying nVision data in a web browser with widgets | • network scanning: device and TCP/IP service detection | • IT Asset Management: centralized asset management for IT department | • full user management based on groups and security policies | • creating and processing tickets through a web interface or via email | • information on devices currently connected to a a specific computer | • working time statistics: activity start and end time, time spent at the computer, and time away from the computer |
| • protecting the Agent from being uninstalled | • responsive widgets; widget grid size management | • interactive network maps, user/ branch maps, smart maps | • comprehensive asset tracking: detailed records of asset actions, customizable statuses and fields, and protocol generating | • blocking of running applications | • absence planning in assigning tickets | • list of all devices connected to computers on the network | • detailed statistics on the working time at the computer and work history in a graphical view: list of desktop applications and visited websites |
| • diagnostic toolkit Axence net-Tools | • automatic dashboard refresh | • TCP/IP services: response time and correctness, statistics of packets received/lost (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL, etc.) | • view of assets, applications, documents, licenses for individual users or separate view by assets assigned to devices | • monitoring of e-mail messages (headers) - anti-phishing | • selecting the approver | • audit (history) of connections and operations performed on mobile devices, network shares and local drives | • user-visible personal activity statistics |
| • event/action alerts | • light and dark mode dashboards | • WMI counters: CPU load, memory usage, disk usage, network transfer, etc. | • bulk editing of properties e.g. status | • detailed working time: activity start and end time, breaks | • creating ticket approval flows based on the category assigned to the ticket | • monitoring file operations in directories on the system drive | • group and member activity statistics visible to the group manager |
| • alerts (desktop, e-mail, SMS) and corrective actions (starting the program, restarting the computer, etc.) | • sharing read-only dashboards | • Windows performance: service status change (start, stop, restart), event log entries | • simultaneous assignment of a document to multiple assets | • applications used: active and inactive | • sending automatic notifications to a person who accepts the ticket | • monitoring file operations from network assets shared by devices not supported by the Agent, e.g. Synology, Qnap arrays, etc. | • subordinate activity statistics visible to the superior |
| • alarm notifications sent via MS Teams and Slack messengers | • managing administrators' permissions to AdminCenter functionality | • SNMP v1/2/3 counters (e.g. network transfer, temperature, humidity, supply voltage, toner level, etc.) | • access permissions for administrators to asset types, licenses, and documents within departments | • visited websites tracking: titles, addresses, visits, and length | • software repository: creating a list of secure applications for self-installation by the user | • managing access rights (read, write, execute) for devices, computers, and users | • user screenshot monitoring for managers and administrators |
| • alarm notifications sent via smsapi.com | • widgets for the Network module: performance counters, alerts, and TCP/IP service responses | • MIB file compiler | • Software Asset Management: comprehensive system for application and license management, including license usage identification | • print audits: printer, user, computer, printing costs | • managing Service Level Agreement metrics (SLA) | • central configuration: setting rules for the entire network, groups, and users of Active Directory | • categorizing applications and websites (e.g., office applications, instant messengers, entertainment); a predefined list of editable categories |
| • OAuth 2.0 support for e-mails and SMS messages | • widgets for the Inventory module: hardware configuration changes and application configuration changes for Agent-enabled devices; alerts for assets | • support for SNMP traps | • unified license management: accounting for all license types, including cloud-based licenses | • remote desktop preview (read-only access) | • automated ticket assignment based on predefined conditions | • integration of user and group database with Active Directory | • adding exceptions by the group administrator to designate certain applications within the group as productive |
| • user hierarchy management (inc. AD import) | • widgets for the Users module: printouts statistics, application usage statistics, bandwidth usage, web activity | | • license billing by user, device, serial number, or based on the installed application version | • screenshots: user work history captured screen by screen | • ticket category and priority management with HelpDesk | • automatically setting a user a default monitoring and security policy | |
| • reports (for the device, departments, selected map, or the entire network) | | | • hardware and software inventory audit | • website blocking | • real-time ticket updates and advanced search functionality | • automatically giving the user a default monitoring and security policy | |
| • simultaneous use of more than one administrator; Admin access log | | | • insight into the licenses assigned to a user working on multiple devices | • a registry of blockage violations aggregating information on attempted access to blocked websites, running banned applications, and downloading files with forbidden extensions. | • configuration of ticket visibility rules and automated actions triggered by specific conditions in the ticketing system | | |
| • managing the permissions of multiple administrators | | | | | • restrict ticket creating by selected user groups to certain categories only | | |
| • group management: creating, assigning users | | | | | • advanced ticket report system | | |
| | | | | | • comments and attachments in tickets; adding custom fields | | |
| | | | | | • internal chat system with file transfer functionality | | |

## FEATURES AVAILABLE FOR EACH MODULE

| GENERAL | ADMINCENTER | NETWORK | INVENTORY | USERS | HELPDESK | DATAGUARD | SMARTTIME |
|---|---|---|---|---|---|---|---|
| • context menu with the possibility of defining your own tools<br><br>• Admin access log: sending events to external Syslog collector<br><br>• global search engine in nVision console: search for objects (e.g.: devices,users, assets), and Program interface elements (e.g. options)<br><br>• logging the Agent uninstalled in the console<br><br>• multifactor authentication (MFA)<br><br>• enhanced password policy<br><br>• encrypted synchronization with Active Directory with LDAPS (Secure LDAP) | • widgets for the HelpDesk module: ticket handling statistics, list of recent unresolved tickets, list of oldest unresolved tickets, last 10 tickets with breached SLA metrics, 10 upcoming SLA metrics<br><br>• widgets for the DataGuard module: recently connected external media, recent file operations<br><br>• widgets for the SmartTime module: group productivity; unproductive time statistics | • routers and switches: port mapping; device-to-switch connectivity information<br><br>• Syslog message support<br><br>• support for AES, DES, and 3DES encryption for the SNMPv3 protocol<br><br>• applying performance counters to devices based on templates<br><br>• monitoring and managing VMware virtual machines | • remote access to the file manager with the possibility of deleting user files<br><br>• information about hardware configuration and registry entries, files, and .zip archives on the workstation<br><br>• detailed hardware configuration information for a specific workstation<br><br>• management of software installations/ deinstallations based on the MSI package manager<br><br>• alarms: software installations and hardware asset changes<br><br>• archiving and comparing audits<br><br>• Mobile Inventory Assistant for Android: asset search, label scanning, asset addition and editing, service action addition, label printingt<br><br>• template-based document generator<br><br>• auto-numbering of added assets and documents according to the defined auto-numbering sequence<br><br>• history of a specific software license's usage<br><br>• S.M.A.R.T. data readout from NVMe drives | • alerts for incidents collected in the registry of violations<br><br>• integration with security lists, including CERT, to block access to malicious websites<br><br>• GDPR compliant: assigning configuration, permissions and accesses to a specific user, regardless of device<br><br>• computer forensics: detailed activity and user metrics<br><br>• process blocking based on .EXE file path<br><br>• web filtering and application blocking rules: revised mechanism for creating, managing, and grouping rules<br><br>• web filtering and application blocking rules: creating, grouping, duplicating between groups of users<br><br>• detecting and preventing suspicious user activity, including the use of jigglers<br><br>• support for using the wildcard character „*" in exclusion filters for TCP/IP stack integrations | • simultaneous administrators work with announcements<br><br>• mandatory read confirmation option for announcements to users/computers<br><br>• viewing of notification history in the Agent<br><br>• remote access to computers with mouse/keyboard locking<br><br>• simultaneous remote access by several administrators to the same Agent. Full support for terminal sessions<br><br>• ability to select the displayed screen during remote access<br><br>• user database integrated with Active Directory<br><br>• remote file distribution and executing tasks (e.g. remote software installation); two-way file exchange<br><br>• knowledge base with integrated search engine and multimedia support<br><br>• remote access to file manager and user file deletion functionality<br><br>• Windows local user account management<br><br>• processing tickets in anonymous mode<br><br>• notification category descriptions with GDPR clause inclusion<br><br>• dark mode in the ticketing system and chat<br><br>• remote registry editing on computers with the nVision Agent<br><br>• users's name cards in ticket view<br><br>• exportable list of tickets<br><br>• drafting and archiving announcements | • deleting non-existing/ disposed data carriers (e.g. flash drives)<br><br>• trusted device attribute<br><br>• user metrics displaying current settings for a specific employee.<br><br>• integration with Windows Defender: managing embedded antivirus software settings, alerting about detected issues, and providing scan results<br><br>• detecting antivirus software other than Windows Defender<br><br>• integration with Windows BitLocker: reading TPM module status and volume encryption<br><br>• remote disk encryption using BitLocker<br><br>• integration with Windows Firewall: enabling/disabling firewall for specific connection types, creating traffic rules, and reading firewall status on workstations. | • productivity classification of desktop applications and websites as productive, neutral, or unproductive; assigning productivity exceptions for specific groups of users<br><br>• productivity metrics: time spent on productive activity, productivity calculated as a percentage based on working time statistics<br><br>• defining the productivity threshold and the unproductivity limit; email notifications for managers<br><br>• list of contacts within the organization<br><br>• private time feature: ability to disable activity analysis in SmartTime when using a company computer for personal use<br><br>• dark mode in the productivity app<br><br>• separation of productivity indicators for subgroups within the main group, reporting to the selected manager<br><br>• limiting available contacts |

BACK