

FEATURES AVAILABLE FOR EACH MODULE		NETWORK	INVENTORY	USERS	HELPDESK	DATAGUARD	SMARTTIME
GENERAL	ADMINCENTER						
<ul style="list-style-type: none"> • Windows Agent • protecting the Agent from being uninstalled • diagnostic toolkit Axence net-Tools • event/action alerts • alerts (desktop, e-mail, SMS) and corrective actions (starting the program, restarting the computer, etc.) • alarm notifications sent via MS Teams and Slack messengers • alarm notifications sent via sm-sapi.com • OAuth 2.0 support for e-mails and SMS messages • user hierarchy management (inc. AD import) • reports (for the device, departments, selected map, or the entire network) • simultaneous use of more than one administrator; Admin access log • managing the permissions of multiple administrators • group management: creating, assigning users 	<ul style="list-style-type: none"> • displaying nVision data in a web browser with widgets • responsive widgets; widget grid size management • automatic dashboard refresh • light and dark mode dashboards • sharing read-only dashboards • managing administrators' permissions to AdminCenter functionality • widgets for the Network module: performance counters, alerts, and TCP/IP service responses • widgets for the Inventory module: hardware configuration changes and application configuration changes for Agent-enabled devices; alerts for assets • widgets for the Users module: printouts statistics, application usage statistics, bandwidth usage, web activity 	<ul style="list-style-type: none"> • network scanning: device and TCP/IP service detection • interactive network maps, user/branch maps, smart maps • TCP/IP services: response time and correctness, statistics of packets received/lost (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL, etc.) • WMI counters: CPU load, memory usage, disk usage, network transfer, etc. • Windows performance: service status change (start, stop, restart), event log entries • SNMP v1/2/3 counters (e.g. network transfer, temperature, humidity, supply voltage, toner level, etc.) • MIB file compiler • support for SNMP traps 	<ul style="list-style-type: none"> • IT Asset Management: centralized asset management for IT department • comprehensive asset tracking: detailed records of asset actions, customizable statuses and fields, and protocol generating • view of assets, applications, documents, licenses for individual users or separate view by assets assigned to devices • simultaneous assignment of a document to multiple assets • Software Asset Management: comprehensive system for application and license management, including license usage identification • unified license management: accounting for all license types, including cloud-based licenses • license billing by user, device, serial number, or based on the installed application version • hardware and software inventory audit • insight into the licenses assigned to a user working on multiple devices 	<ul style="list-style-type: none"> • full user management based on groups and security policies • blocking of running applications • monitoring of e-mail messages (headers) - anti-phishing • detailed working time: activity start and end time, breaks • applications used: active and inactive • visited websites tracking: titles, addresses, visits, and length • print audits: printer, user, computer, printing costs • remote desktop preview (read-only access) • screenshots: user work history captured screen by screen • website blocking • integration with security lists, including CERT, to block access to malicious websites 	<ul style="list-style-type: none"> • creating and processing tickets through a web interface or via email • absence planning in assigning tickets • selecting the approver • creating ticket approval flows based on the category assigned to the ticket • sending automatic notifications to a person who accepts the ticket • software repository: creating a list of secure applications for self-installation by the user • managing Service Level Agreement metrics (SLA) • automated ticket assignment based on predefined conditions • ticket category and priority management with HelpDesk • real-time ticket updates and advanced search functionality • configuration of ticket visibility rules and automated actions triggered by specific conditions in the ticketing system • advanced ticket report system 	<ul style="list-style-type: none"> • information on devices currently connected to a specific computer • list of all devices connected to computers on the network • audit (history) of connections and operations performed on mobile devices, network shares and local drives • monitoring file operations in directories on the system drive • managing access rights (read, write, execute) for devices, computers, and users • central configuration: setting rules for the entire network, groups, and users of Active Directory • automatically setting a user a default monitoring and security policy • automatically giving the user a default monitoring and security policy 	<ul style="list-style-type: none"> • working time statistics: activity start and end time, time spent at the computer, and time away from the computer • detailed statistics on the working time at the computer and work history in a graphical view: list of desktop applications and visited websites • user-visible personal activity statistics • group and member activity statistics visible to the group manager • subordinate activity statistics visible to the superior • user screenshot monitoring for managers and administrators • categorizing applications and websites (e.g., office applications, instant messengers, entertainment); a predefined list of editable categories • adding exceptions by the group administrator to designate certain applications within the group as productive

FEATURES AVAILABLE FOR EACH MODULE		 NETWORK	 INVENTORY	 USERS	 HELPDESK	 DATAGUARD	 SMARTTIME
GENERAL	ADMINCENTER						
<ul style="list-style-type: none"> context menu with the possibility of defining your own tools Admin access log: sending events to external Syslog collector global search engine in nVision console: search for objects (e.g.: devices, users, assets), and Program interface elements (e.g. options) logging the Agent uninstalled in the console multifactor authentication (MFA) enhanced password policy 	<ul style="list-style-type: none"> 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 widgets for the DataGuard module: recently connected external media, recent file operations widgets for the SmartTime module: group productivity; unproductive time statistics 	<ul style="list-style-type: none"> routers and switches: port mapping; device-to-switch connectivity information Syslog message support support for AES, DES, and 3DES encryption for the SNMPv3 protocol applying performance counters to devices based on templates monitoring and managing VM-ware virtual machines 	<ul style="list-style-type: none"> remote access to the file manager with the possibility of deleting user files information about hardware configuration and registry entries, files, and .zip archives on the workstation detailed hardware configuration information for a specific workstation management of software installations/ deinstallations based on the MSI package manager alarms: software installations and hardware asset changes archiving and comparing audits Mobile Inventory Assistant for Android: asset search, label scanning, asset addition and editing, service action addition, label printingt template-based document generator auto-numbering of added assets and documents according to the defined auto-numbering sequence history of a specific software license's usage 	<ul style="list-style-type: none"> GDPR compliant: assigning configuration, permissions and accesses to a specific user, regardless of device computer forensics: detailed activity and user metrics process blocking based on .EXE file path web filtering and application blocking rules: revised mechanism for creating, managing, and grouping rules web filtering and application blocking rules: creating, grouping, duplicating between groups of users detecting and preventing suspicious user activity, including the use of jigglers 	<ul style="list-style-type: none"> comments and attachments in tickets; adding custom fields internal chat system with file transfer functionality mandatory read confirmation option for announcements to users/computers viewing of notification history in the Agent remote access to computers with mouse/keyboard locking user database integrated with Active Directory remote file distribution and executing tasks (e.g. remote software installation); two-way file exchange knowledge base with integrated search engine and multimedia support remote access to file manager and user file deletion functionality Windows local user account management processing tickets in anonymous mode notification category descriptions with GDPR clause inclusion dark mode in the ticketing system and chat remote registry editing on computers with the nVision Agent 	<ul style="list-style-type: none"> deleting non-existing/ disposed data carriers (e.g. flash drives) trusted device attribute user metrics displaying current settings for a specific employee. integration with Windows Defender: managing embedded antivirus software settings, alerting about detected issues, and providing scan results detecting antivirus software other than Windows Defender integration with Windows BitLocker: reading TPM module status and volume encryption remote disk encryption using BitLocker integration with Windows Firewall: enabling/disabling firewall for specific connection types, creating traffic rules, and reading firewall status on workstations. 	<ul style="list-style-type: none"> productivity classification of desktop applications and websites as productive, neutral, or unproductive; assigning productivity exceptions for specific groups of users productivity metrics: time spent on productive activity, productivity calculated as a percentage based on working time statistics defining the productivity threshold and the unproductivity limit; email notifications for managers list of contacts within the organization private time feature: ability to disable activity analysis in SmartTime when using a company computer for personal use dark mode in the productivity app separation of productivity indicators for subgroups within the main group, reporting to the selected manager limiting available contacts