NIST SP 800-171

	Security Requirements	Relevant Genian NAC Functionality
1. ACCESS CONTROL		
Basic Security Requirements		
1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Network Access Control ● Correlates access info (Device, User, IP/MAC, Switch Port, SSID) ● Provides role-based/context based access control ● Integrates with user databases (AD, CSV, CRM, ERP systems)
1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	
Derived Security Requirements		
1.3	Control the flow of CUI in accordance with approved authorizations.	Information flow can be controlled by classifying groups for network assets and users. Each group will have its own access permission (Network segment, Services, and Time-based) to appropriate network resources
1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Allows network access only to authorized users/groups (Based on roles and duties of users) For example: ● Web server administrators - allows access to a specific service port of the web server they manage ● Security officers - allows access to IT security products ● Network Admins - allows access to specific service ports of the managed network devices
1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Supports Least-privileged user account (LUA) ● Network segment, Services, and Time-based
1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.	See 1.5
1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	Logs all activities (Devices, users, connections, compliance status changes, etc.) as part of the audit trail

		Detects any status changes against compliance policies in real time
1.8	Limit unsuccessful logon attempts.	Agent-based control: ● Controls Windows login configuration ● Checks Windows password protection and strength
1.9	Provide privacy and security notices consistent with applicable CUI rules.	
1.10	Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	
1.11	Terminate (automatically) a user session after a defined condition.	Agent-based control: ● Terminates processes ● Controls network interfaces ● Controls Windows screenlocks
1.12	Monitor and control remote access sessions.	Manages devices and users accessing through VPN
1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	
1.14	Route remote access via managed access control points.	See 1.12
1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	See 1.12
1.16	Authorize wireless access prior to allowing such connections.	Provides Built-in RADIUS, AD integration
1.17	Protect wireless access using authentication and encryption.	Secures Wireless Access: ● User Authentication via 802.1x/EAP and RADIUS (Built-in RADIUS and AD integration) ● AES and TKIP encryption provided
1.18	Control connection of mobile devices.	● Identifies and classifies all mobile device platforms automatically in real time. ● Allows access through AAA process
1.19	Encrypt CUI on mobile devices.	
1.20	Verify and control/limit connections to and use of external information systems.	Supports custom integration using Syslog, SQL, LDAP, and Restful API
1.21	Limit use of organizational portable storage devices on external information systems.	Agent-based control: ● Controls peripheral devices including USB devices

1.22	Control information posted or processed on publicly accessible information systems.	
2. AWARENESS AND TRAINING		
Basic Security Requirements		
2.1	Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.	
2.2	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	
Derived Security Requirements		
2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	
3. AUDIT AND ACCOUNTABILITY		
Basic Security Requirements		
3.1	Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	Logs all activities (Devices, users, connections, compliance status, etc.) as part of the audit trail powered by Elastic search Detects any status changes against compliance policies in real time
3.2	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	See 3.1
Derived Security Requirements		
3.3	Review and update audited events.	See 3.1
3.4	Alert in the event of an audit process failure.	Provides various notification methods: Captive portal service, PC Alert, Email notification, SNS, and more
3.5	Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	Refer to 3.1

3.6	Provide audit reduction and report generation to support on-demand analysis and reporting.	Provides reporting service (xls format) and personalized dashboards using over 120 custom widgets
3.7	Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	Time settings provided for each Network Sensor
3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.	
3.9	Limit management of audit functionality to a subset of privileged users.	Provides Role-based Administrator privileges
4. CONFIGURATION MANAGEMENT		
1	Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	Agent-based control: ● Checks all installed hardware, software information including business context such as EOL, EOS ● Checks Windows Updates, Antivirus ● Maintains baseline configuration of Windows devices
2	Establish and enforce security configuration settings for information technology products employed in organizational information systems.	Agent-based control: ● Windows configuration management
3	Track, review, approve/disapprove, and audit changes to information systems.	See 3.1
4	Analyze the security impact of changes prior to implementation.	
5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.	Network Access Control for all IP enabled devices in the network. See 3.1
6	Employ the principle of least functionality by configuring the information system to provide only essential capabilities.	

7	Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.	Agent-based control: ● Controls File Folder Sharing ● Controls ARP Spoofing ● Controls DNS ● Controls External devices access ● Controls Network Interfaces (Wired, Wireless) ● Controls Installed SW (Chat, P2P, etc.) ● Installs/uninstalls Programs ● Manages Files ● Controls Windows web browser options ● Controls Windows configuration/ Process ● Controls Windows screenlock ● Controls Power options
8	Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or denyall, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	Enforces install and uninstall blacklist/whitelisting-based applications
9	Control and monitor user-installed software.	
5. IDENTIFICATION AND AUTHENTICATION		
1	Identify information system users, processes acting on behalf of users, or devices.	Supports standards-based authentication, such as Active Directory, RADIUS, 802.1X and integration with external user databases (Oracle, MySQL, MSSQL, CSV). Provides most accurate device platform intelligence to identify device information without using Agent
2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	Refer to 5.1
3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	Supports two-factor authentication
4	Employ replay-resistant authentication mechanisms for network access to privileged and non privileged accounts.	
5	Prevent reuse of identifiers for a defined period.	
6	Disable identifiers after a defined period of inactivity.	Detects inactive devices/users for a certain period of time and control them.

7	Enforce a minimum password complexity and change of characters when new passwords are created.	Agent-based control: ● Manages passwords with a minimum password length of 9 characters, special characters, uppercase letters, past passwords, and the prohibition of repeated characters.
8	Prohibit password reuse for a specified number of generations.	Agent-based control: ● Prohibits the reuse of old passwords ● Specifies the number of allowed uses of the same password
9	Allow temporary password use for system logons with an immediate change to a permanent password.	Agent-based control: ● Allows temporary password use for the first time login and enforces users to change the temporary password on next login
10	Store and transmit only encrypted representation of passwords.	Stores hashed passwords from customer's authentication system into Genian NAC DB Users' passwords are hashed and stored in the Genian NAC database securely
11	Obscure feedback of authentication information.	Provides obscure feedback during the authentication process: ● Displays asterisk symbols when typing in a password ● Provides hint when password is not matched
6. INCIDENT RESPONSE		
1	Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.	
2	Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.	
3	Test the organizational incident response capability.	
7. MAINTENANCE		
1	Perform maintenance on organizational information systems.	

2	Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.	
3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	
4	Check media containing diagnostic and test programs for malicious code before the media are used in the information system.	
5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	
6	Supervise the maintenance activities of maintenance personnel without required access authorization.	
8. MEDIA PROTECTION		
1	Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.	
2	Limit access to CUI on information system media to authorized users.	
3	Sanitize or destroy information system media containing CUI before disposal or release for reuse.	
4	Mark media with necessary CUI markings and distribution limitations.	
5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	
6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	
7	Control the use of removable media on information system components.	Agent-based control: ● Controls removable media access (USB drive, CD, DVD)

8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	Agent-based control: ● Only authorized users can use portable storage devices, such as USB
9	Protect the confidentiality of backup CUI at storage locations.	
9. PERSONNEL SECURITY		
1	Screen individuals prior to authorizing access to information systems containing CUI.	Authorization by various authentication processes: ● MAC-based ● User ID / Custom Inputs / Device information ● Role/context based access
2	Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.	Immediately terminates all access privileges of users no longer working in the organization and controls devices the users used
10. PHYSICAL PROTECTION		
1	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	Provides Role-based access control
2	Protect and monitor the physical facility and support infrastructure for those information systems.	
3	Escort visitors and monitor visitor activity.	Supports BYOD, Guest access
4	Maintain audit logs of physical access.	Refer to 3.1
5	Control and manage physical access devices.	Integrates with ID scanning system
6	Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).	
11. RISK ASSESSMENT		
1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.	
2	Scan for vulnerabilities in the information system and applications periodically and	Agent-based control: ● Checks outdated/missing Windows patches, required software

	when new vulnerabilities affecting the system are identified.	Integrates with vulnerability scanner (e.g. Nessus)
3	Remediate vulnerabilities in accordance with assessments of risk.	Detects non-compliant/compromised devices and fixes them through remediation process Enforces policies to update Windows and applications
12. SECURITY ASSESSMENT		
1	Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.	Performs compliance monitoring in real time
2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.	
3	Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	
13. SYSTEM AND COMMUNICATIONS PROTECTION		
1	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	
2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	
3	Separate user functionality from information system management functionality.	
4	Prevent unauthorized and unintended information transfer via shared system resources.	
5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	
6	Deny network communications traffic by default and allow network communications	

	traffic by exception (i.e., deny all, permit by exception).	
7	Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.	Allows only IP/MAC based communication as designed
8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	
9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	See 1.11
10	Establish and manage cryptographic keys for cryptography employed in the information system.	
11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	
12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	
13	Control and monitor the use of mobile code.	
14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	
15	Protect the authenticity of communications sessions.	
16	Protect the confidentiality of CUI at rest.	
14. SYSTEM AND INFORMATION INTEGRITY		
1	Identify, report, and correct information and information system flaws in a timely manner.	Agent-based control: ● Check the current status of Windows Updates, any required software like Antivirus, Windows setting. ● Manipulate endpoint's system configuration to maintain IT security baseline
2	Provide protection from malicious code at appropriate locations within organizational information systems.	

3	Monitor information system security alerts and advisories and take appropriate actions in response.	
4	Update malicious code protection mechanisms when new releases are available.	
5	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	
6	Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	
7	Identify unauthorized use of the information system.	