Automation Studio Security & Architecture Overview

Reference Guide

Release: Advanced Process Automation 7.6

Document Revision: 7.6-A0
Distribution Status: Published
Publication Date: December 2021

For assistance, contact your local supplier or nearest NICE Customer Service Center:

EMEA Region (Europe, Middle East, Africa)
Tel: +972-9-775-3800
Fax: +972-9-775-3000
email: support@nice.com

APAC Region (Asia/Pacific)
Tel: +852-8338-9818
Fax: +852-2802-1800
email: support.apac@nice.com

North America
Tel: 1-800-663-5601
Fax: +201-356-2197
email: na_sales@nice.com

International Headquarters-Israel
Tel: +972-9-775-3100
Fax: +972-9-775-3070
email: info@nice.com

The Americas Region (North, Central, South America)
Tel: 1-800-6423-611
Fax: +720-264-4012
email: support.americas@nice.com

Israel
Tel: 09-775-3333
Fax: 09-775-3000
email: support@nice.com

France
Tel: +33-(0)1-41-38-5000
Fax: +33-(0)1-41-38-5001

Hong-Kong
Tel: +852-2598-3838
Fax: +852-2802-1800

United Kingdom
Tel: +44-8707-22-4000
Fax: +44-8707-22-4500

Germany
Tel: +49-(0)-69-97177-0
Fax: +49-(0)-69-97177-200

NICE invites you to join the **NICE User Group (NUG)**.

Visit the NUG Website at www.niceusergroup.org and follow the instructions.

All queries, comments, and suggestions are welcome! Please email: nicebooks@nice.com

For more information about NICE, visit www.nice.com

CONTENTS

[This page intentionally left blank]

Automation Studio Security Overview

These sections describe NICE's commitment to security as a knowledge-based firm, as well as the APA and Automation Studio architecture and security.

Automation Studio Commitment to Security

NICE is a knowledge-based firm, and as such, its success is dependent on its ability to leverage information and information systems to the firm's best interest and prevent any mishaps.

NICE's management considers its information to be a strategic asset. As such, information security aims to protect its confidentiality, integrity and availability. These goals are met by aligning security procedures with business needs.

The level of information security embedded in NICE's information systems, and the degree to which information security procedures are upheld by employees, subcontractors and suppliers are of utmost importance to NICE's stability and ability to achieve its business objectives.

Customers and business partners see NICE as a respected and reliable provider that can be fully trusted with their confidential information.

Information Security Management Certification

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) within the context of the organization. It also includes requirements for the assessment and treatment of information security risks, tailored to the needs of the organization.[1] The standard is designed to ensure the selection of adequate and proportionate security controls; it is the only such standard currently in existence.

NICE first achieved ISO/IEC 27001 compliance in April 2007 and has continued to receive regular audits since then. The standard requires NICE to ensure a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving our information security management system. We believe our compliance helps us to protect our information assets and gives additional confidence to businesses and individuals we do business with—especially our customers, on whose behalf we often manage information. Accreditation helps to assure them that their information is properly protected.

Of course, ISO/IEC 27001 compliance also holds benefits for NICE, too. It independently demonstrates that:

- Our internal controls meet corporate governance and business continuity requirements.
- All applicable laws and regulations are observed in order to protect company information.

[1] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

- Any company risks are properly identified, assessed and managed, and formalizes information security processes, procedures, and documentation.
- The security of all customer, partner, and employee information is paramount.

ISO27001 Certificate

CERTIFICATE

This is to certify that the Information Security Management System of

NICE LTD AND SUBSIDIARIES

22 Zarchin St. , Ra'anana , Israel

Has been assessed and complies with the requirements of :

ISO/IEC 27001:2013

The Information Security Management System is Applicable to IT Operations Department Related to: Develop products and solutions as well as provide professional services for Contact Center & Trading Floor Management, , Law Enforcement & Criminal Justice Management, and Financial Crime and Fraud Management.

According to Statement of Applicability: 11.8.2021

Initial Approval:	18/06/2007		
Certification Decision:	23/12/2021		
Valid Until:	23/12/2024	Certificate No.:	78236

SII-QCD assumes no liability to any party other than the client, and then only in accordance with the agreed upon Certification Agreement. This certificate's validity is subject to the organization maintaining their system in accordance with SII-QCD requirements for system certification. The continued validity may be verified via scanning the code with a smartphone, or via website www.sii.org.il. This certificate remains the property of SII-QCD.

Dr. Gilad Golub
CEO

R.N 520036872

Avital Weinberg
Director, Quality & Certification Division

THE STANDARDS INSTITUTION OF ISRAEL

The standards Institution of Israel
42 Chaim Levanon St,
Tel-Aviv 6997701

Page 1 of 3

Our Vision: To Enhance Both Global Competitiveness of our Services, with our Uncompromised Quality and Integrity

SDLC Framework

NICE APA is developed according to the security development lifecycle (SDLC) methodology. SDLC ensures that all features are designed, developed and tested according to the industry's best practices on security. This applies to both on-premises and hosted solutions.

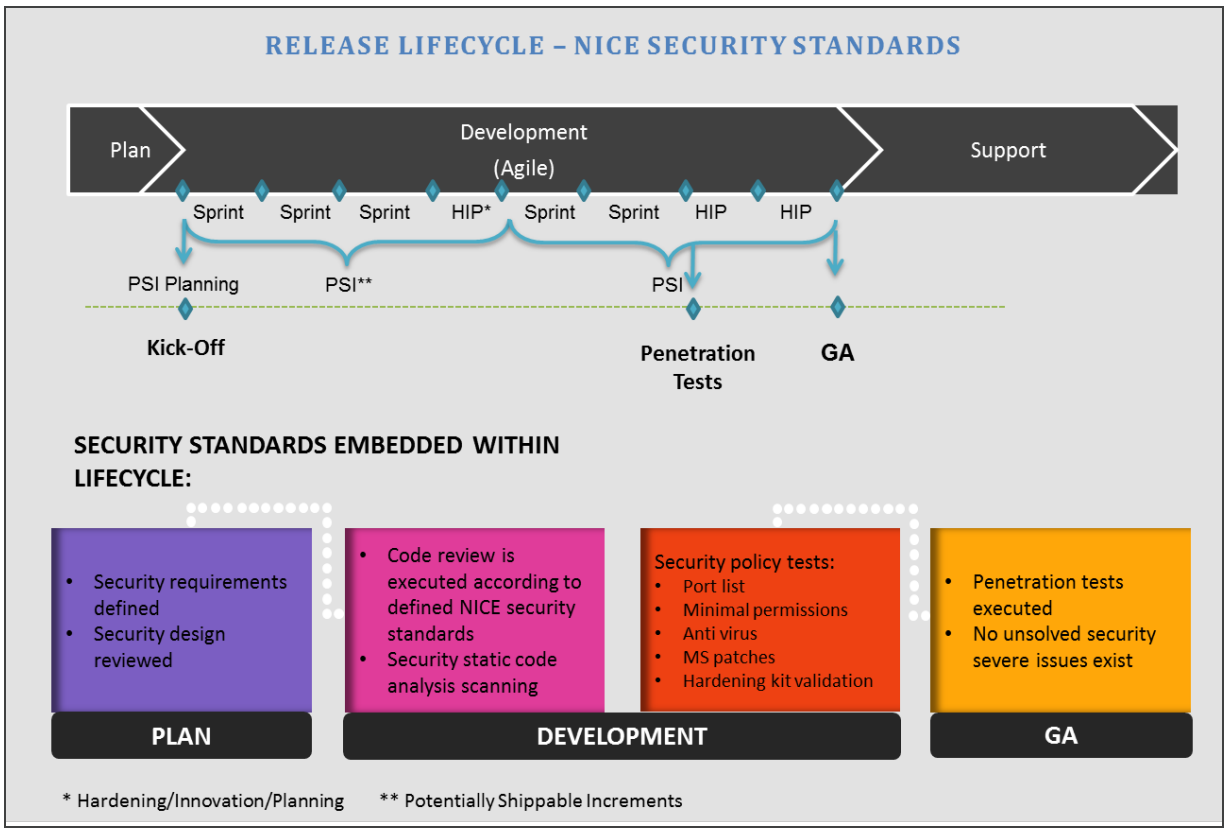


Figure 2: NICE Release Lifecycle

Development Security Standards - Ongoing Activities

Security Training:

- Periodically train R&D and QA on common security vulnerabilities and secure coding practices (OWASP TOP 10, CWE/SANS TOP 25).

Planning Phase:

- Define security requirements according to the development scope.
- Perform security design reviews on new features to ensure that they meet security standards.

Development Phase:

- Execute static code analysis periodically using Micro Focus Fortify (former software division of Hewlett Packard Enterprise), a leading industry security tool.
- Third parties scanning and licensing using BlackDuck, a leading industry security tool.
- Code review according to defined security guidelines.

- Conduct testing on hardened environments.
- Complete penetration tests.
- Fix all critical and high issues before GA.

GA Phase:

- Certify MS security patches on an ongoing basis.
- Certify leading vendor anti-virus tools on an ongoing basis.

Security Vulnerability Policy for NICE APA

Security vulnerability in the APA product can be discovered in one of the following ways:

- NICE Penetration Tests are executed by an external third party. The third party issues a statement to NICE that the product was tested and classifies any potential vulnerabilities. NICE is committed to fixing any vulnerabilities tagged as **Critical** or **High**.
- Vulnerability that is disclosed by NVD (National Vulnerability Database) https://nvd.nist.gov/home.cfm
- Customer feedback

The vulnerabilities can be classified by NICE as Critical, High, Medium or Low. Public CVEs are classified by the NVD CVSS Severity V2 model and by the role within the NICE product.

NICE will address the vulnerabilities according to the following table and under the assumption that the fix does not break the product functionality/architecture.

VULNERABILITY LEVEL	NICE APA POLICY
Critical	Fix, Hardening or Mitigation Plan will be provided for the current release.
High	Fix, Hardening, Mitigation Plan will be provided for the current release.
Medium	Fix, Hardening or Mitigation Plan will be provided for the next release (in the next 12 months).
Low	Items that are considered as part of NICE long term roadmap.

Corporate Practices

Security Policies and Standards

The Global Information Security Policy expresses NICE management's commitment to implementing information security policy and processes as part of the overall business processes reflected in the organizational and technological aspects of the firm. The policy outlines the principal guidelines by which information security is managed and applies to all NICE employees, temporary employees, and subcontractors. This is a global policy that applies to all NICE sites and subsidiaries.

All security policies and standards are published and accessible to employees, contractors, and relevant external parties.

Periodic Reviews

Policies and standards are reviewed annually, as well as in the event of significant changes to organizational environment, business circumstances, legal conditions, or the technical environment to ensure continuing adequacy and effectiveness.

Segregation of Duties

Tasks involved in critical business processes must be performed by separate individuals. Responsibilities of programmers, system administrators and database administrators must not overlap, unless authorized by the data owner. Duties and responsibilities shall be assigned systematically to a number of individuals to ensure that effective checks and balances exist. Such controls keep a single individual from subverting a critical process. Key duties include authorizing, approving and recording transactions, issuing and receiving assets and reviewing or auditing transactions.

Segregation of duties should be maintained between the following functions:

- Data entry
- Computer operation
- Network management
- System administration
- Systems development and maintenance
- Change management

- Security administration
- Security audit

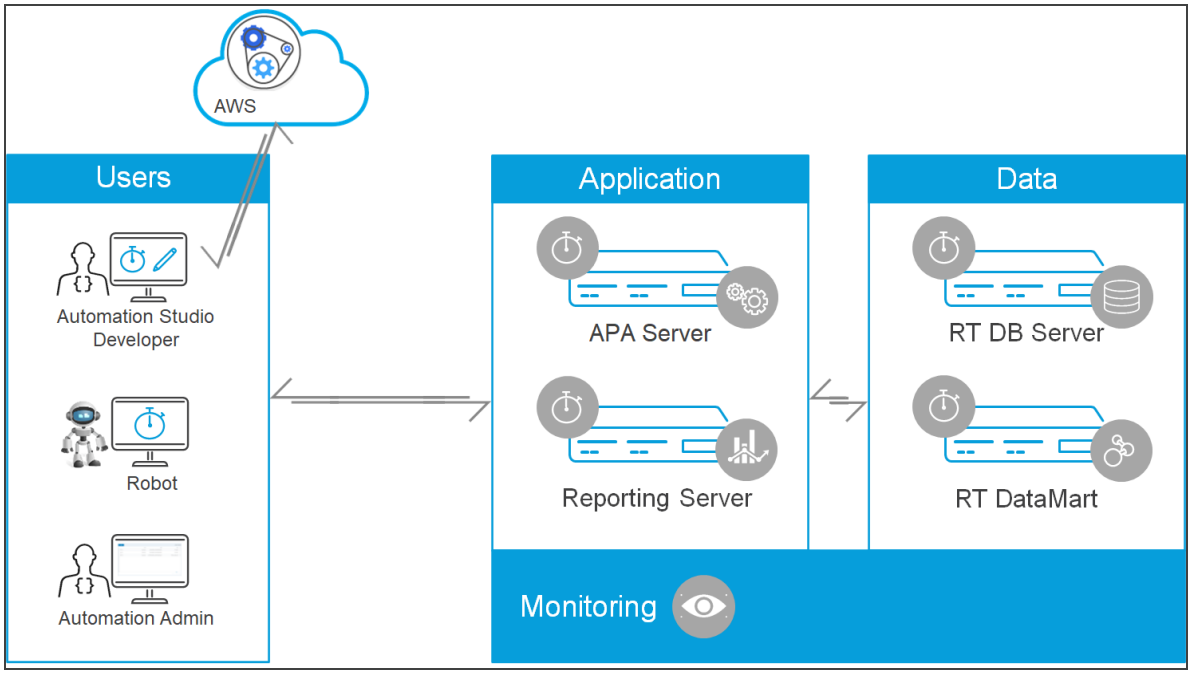
Qualified and continuous supervision is to be provided to ensure that internal control objectives are achieved. This standard requires supervisors to continuously review and approve the assigned work of their staff as well as provide the necessary guidance and training to ensure that errors, waste, and wrongful acts are minimized and that specific management directives are followed.

Automation Studio Architecture and Security

The following topics provide details about the architecture and security of Automation Studio.

Automation Studio and APA Infrastructure Components

The following diagram describes the Automation Studio and APA tiers at a high level.



There are several types of users:

- **Automation Studio Developer:** The developer using the new APA development tool to create and manage automations.
- **Real-Time Robot:** A Real-Time Client that resides on an unattended station and executes automation based on requests that are scheduled in the Automation Portal or sent to the APA server via an API and pulled by the robots.
- **Automation Admins:** Users accessing the Automation Portal to monitor and control.

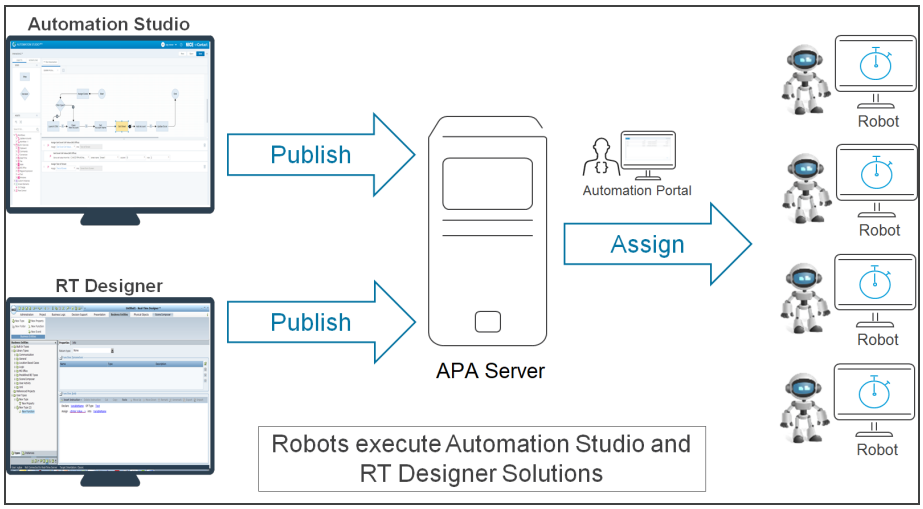
The following components reside in the data center:

- **APA server:** Hosts the APA server applications, connects to the clients, collects client statuses and data, and stores the data in the RT Database. A load balancer can be used to support several servers in a APA server cluster.

- **Real-Time Database Server (Operational):** Stores the system and user information. Data from the clients is stored in the database (Data Collection and Activity Monitoring).
- **Real-Time Data Mart (Reporting):** The Data Mart is the database that extracts the data from the operational database for reporting and long-term retention.
- **Reporting Server (Cognos):** The Cognos server is used for Advanced Process Automation out-of-the box or customized reporting.
- **Monitoring:** APA server health is monitored by a Prometheus and Grafana monitoring stack.

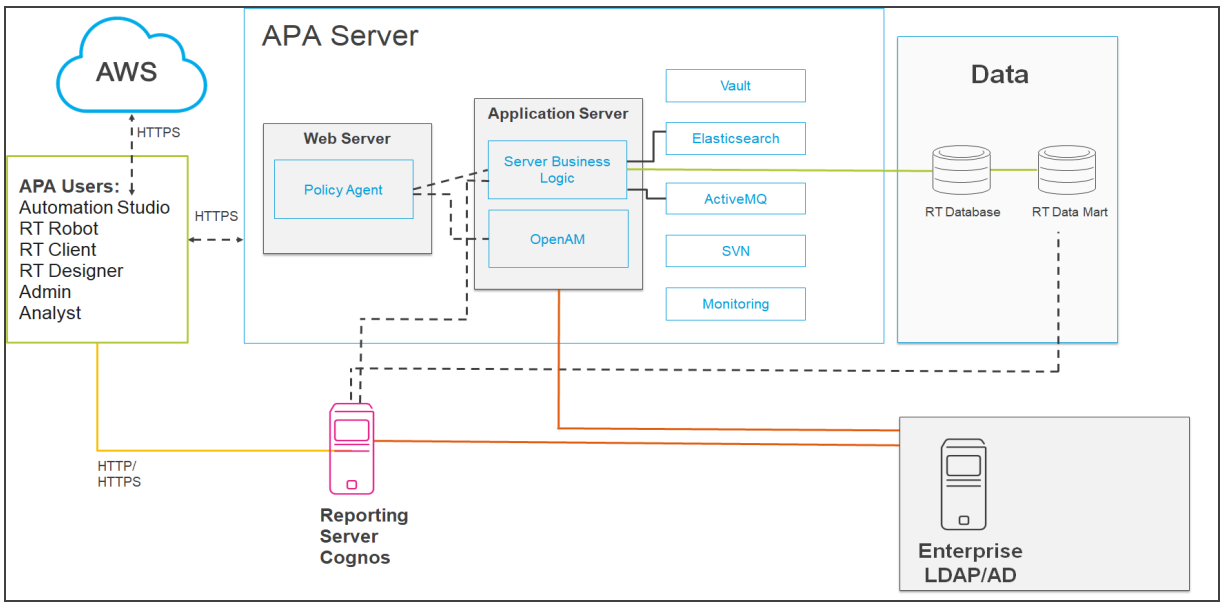
APA and Automation Studio Solution Publishing

Automation Studio solutions are published to the APA server. Automation Studio and RT Designer can run side-by-side, serviced by the same APA server. Unattended solutions created on both Automation Studio and RT Designer can run on the same robots.



APA and Automation Studio Architecture

The following diagram describes the APA high-level architecture.



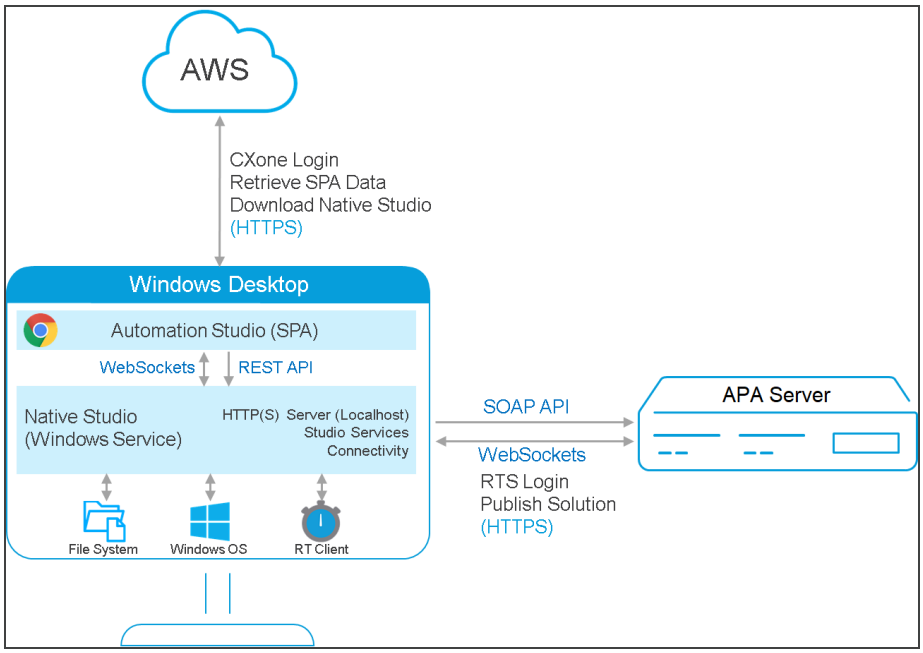
APA Server Main Components

COMPONENTS	DESCRIPTION
Apache Web Server	Web server used for communication with the clients.
Policy Agent	Enforces the access policy to the server.
Application Server Apache Tomcat	Hosts the application: • Gets client status. • Collects data from the clients and stores it in the database. • Imports users into the server. • Manages the solution publishing and assignment to clients.
AM Access Management	Manages the server authentication policy configuration and decisions.
Elasticsearch	Used for the Automation Portal - Robotic Client Control Room and Task Control Room.

COMPONENTS	DESCRIPTION
Active MQ	Message broker used by the Application Server to manage incoming messages queue from the Real-Time Clients.
SVN	Software versioning and revision control that is used for APA solution version control.
Vault	The Vault manages the encryption and decryption of the passwords used in the APA server.

Automation Studio Components and Security

The following diagram describes the Automation Studio architecture and associated security.



AWS Cloud

- Automation Studio users are provisioned using CXone AWS in a customer-specific tenant.
- Automation Studio connects to AWS using HTTPS.
- Users are authenticated against CXone when they log in.

- If a more recent version of the Native Studio is available, this triggers an automatic download of the new version of Native Studio (and RT Client, if required).

> **Important**
> Please note that NO customer data is stored on the AWS Cloud.

Automation Studio User Management

Automation Studio uses CXone for its user management. For details on CXone security, refer to the *CXone System Security Summary* that describes both the general system and the control family implementation comprehensive summary including:

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity

Windows Desktop

- Automation Studio runs as a Single Page Application (SPA) in the browser.

- Automation Studio communicates with Native Studio via WebSockets and a REST API.
- Native Studio runs as a Windows Service and functions as an HTTP(S) Server on the localhost, and provides Automation Studio services and connectivity to the File System, Windows OS and RT Client. The Native Studio to RT Client communication is a process start call (the same as Real-Time Designer to RT Client).

Automation Studio General Security

Automation Studio follows the general APA commitments to security including:

- Information Security Management Certification
- SDLC Framework
- ISO27001 Certificate
- Development Security Standards - Ongoing Activities
- Security Vulnerability Policy for NICE APA
- Corporate Practices

APA Server

- Automation Studio communications with APA server via a SOAP API and WebSockets.
- Automation Studio solutions are published to APA server via HTTPS.

Automation Studio to RT Server Security

Access to the server is enforced by the Policy Agent. A Web Policy Agent is a library installed on the Web Server and configured to be called by the Web Server when a client requests access to a protected resource in a Web Server.

Authorization for Solution Publishing

Authorization is handled by the APA server engine according to the registered users in the Real-Time Database. This means that solution downloading/publishing is available only to authorized users.

General APA Security

For more details on general APA security considerations, see the *APA Security Guide*.