agilepoint

Security Guide

AgilePoint-Hosted Environments

AgilePoint NX v9.0, Software Update 1

January 16, 2026

Contents

Legal Statements and Policies 13

Scope of the Document 15

Abbreviations, Terminology and Definitions 16

Security and Governance 18

- Regulatory Compliance 18
- AgilePoint's Information Security Management System (ISMS) 19
- Corporate Information Security Objectives 20
- Overview of Information Security 20
- Remote Access to AgilePoint's Network 21
- Risk Management 22
  - Risk Assessment 22
  - Risk Analysis 22
  - Risk Assessment Process 23
  - Risk Treatment 23

IT Infrastructure, Data Center and Cloud Security 25

- Data Center Security 26
  - AgilePoint NX OnDemand (Public Cloud) 26
  - AgilePoint NX PrivateCloud 28
- Network Security 29

IP Whitelisting 30
Firewall Management 30
Logging and Auditing of Logs 31
Monitoring 32
Product Level 32
Infrastructure Level 33
Alerting and Reporting 33
SIEM and MDR Implementation 35
Access to IT Infrastructure 36
AgilePoint NX Private Cloud 37
AgilePoint NX Public Cloud 37
AgilePoint Office Premises 37
Protection from Malware, Viruses, and Hackers 38
Data Backup 38
RPO and RTO 38
Key features of AWS Backup 39
AWS Backup 40
AgilePoint NX Public Cloud 40
AgilePoint NX Private Cloud 41
Business Continuity - Disaster Recovery 42
AgilePoint NX Public Cloud 43
AgilePoint NX Private Cloud 43
Capacity Planning and Demand Forecasting 44

Initial Capacity Planning 44
Post Installation Capacity Management – AgilePoint NX Private Cloud 45
Post Installation Capacity Management – AgilePoint NX Public Cloud 45
Bandwidth monitoring 45
Malware Protection 46
Vulnerability Assessment and Penetration Testing (VAPT) 46
File Integrity Monitoring 47
Golden Image and Hardening 47
Software Updates and Security Patches 48
The Shared Responsibility Model 48
Security in Operations 50
Third Party Software and Open-Source Libraries 50
Software OEM Vendors 50
Open-Source Libraries and Packages 51
Software Development Life Cycle (SDLC) 52
Software Development Principles 52
Product Development 54
Change Management 54
Product Testing 55
Release Management 55
Product Packaging 56
Virus and Malware Scan 57
Vulnerability Scanning and Penetration Testing 57

Customers Service Management and Engagement 58
Customer Queries 58
Incident Management and Reporting 58
Product Download and Support Service 59
Web Meetings 59
Customer Locations 60
Customer Data Protection 60
AgilePoint Employee Access to Customer Data 60
Employees Handling Confidential Information 61
Handling a Security Breach 61
Secure Document Management System 62
License Key 62
Data at Rest 63
Data in Transit 63
Community 63
Privacy 64
Data Retention and Customers Offboarding 64
AgilePoint's Partners 65
Vendor Management 65
External Contractors 65
Employee On-Boarding and Exit 65
Security at Product Level 67
Architecture of the Product 67

Secure Architecture Approach 67
Access Tokens 69
Identity Management - User Level 70
Multiple Authentication Providers 75
Anonymous User for Electronic Forms 76
Anonymous Users for Web Pages 78
Identity Management - System Level 79
Layers - 3 Tier View 79
Internal System Level Identity Management 80
External System Level Identity Management 81
AgilePoint's REST APIs 87
Identity Management - SharePoint 87
On-premises SharePoint Identity Management 88
SharePoint for Microsoft 365 Identity Management 88
Administration 88
AgilePoint Service Account and System Account 89
Tenant Administrator 89
Administrators Role 89
AgilePoint User Management 89
AgilePoint Group Management 90
AgilePoint Role Management 90
Access Management 91
Role Based Access Controls (RBACs) 91

Permission Groups 91
Analytics Permissions 92
Webhooks 92
Session Management 93
Excel File Import to Data Entity 94
Excel File Import to eForm 95
Custom Actions Framework 95
Add Document to an Activity 96
Mobile App Configuration – QR code 96
Announcements and Maintenance Notifications 97
Data Sources 98
Cookies 99
Logging Services 100
Audit 101
Ensuring Application Integrity During Collaborative App Development 108
Enhanced Data Governance in Data Entity 109
Open Standards 110
AI Security and Governance 111
Introduction 111
Ethics 113
AI System Design and Ethical Operation 113
Bias Prevention 113
Transparency in Ethical Considerations 113

Ethical Framework and Scope 114
Auditing and Fair Decision-Making 114
Security 114
Protection from Cyber Threats 114
Pre-Deployment Security Testing 114
Employee Security Training 115
Data Protection 115
Data Protection Measures 115
Retention and Disposal Policies 115
Preventing Sensitive Data Exposure 115
Global Compliance 116
Breach Detection and Response 116
Privacy 116
User Privacy Assurance 116
Surveillance Concerns 116
Balancing Data Collection and Privacy 116
Personal Data Analysis Policies 117
Stakeholders 117
Impact on Stakeholder Trust 117
Addressing Ethical Dilemmas 117
Staying Abreast of Regulations 117
Compliance 117
Ensuring Regulatory Compliance 117

Internal Compliance Reporting 118
Project Execution 118
Project Management Methodology 118
Risk Management in AI Projects 118
Quality Assurance 119
Quality Control Measures 119
Accuracy and Reliability of AI Outputs 119
Adherence to Standards 120
Regulatory Adherence 120
Keeping Pace with Regulations 120
International Compliance Standards 120
PIIs and Sensitive Data 120
Alignment with Data Protection Laws 120
Risk Management 121
Risk Assessment and Management 121
Protocol for Compliance Breaches 121
Third-Party Vendors 121
Evaluation and Monitoring of Third-Party Compliance 121
Vendor Expectations and Requirements 121
Employee Training 122
Training Programs on Compliance 122
Measuring Training Effectiveness 122
Reporting Mechanisms 122

Internal and External Reporting 122
Continuous Monitoring 123
Ongoing Compliance Tools 123
Portfolio Management 123
Preventing Performance Bottlenecks 123
Architecture 123
Data Transmission, Processing and Storage 124
AI Control Tower 133
Secure Integration and Data Handling 133
Configurable AI Engagement 134
Audit and Access Control 134
Third-Party Trusted AI Service Provider's Legal Text 135
AgilePoint NX on Third-Party App Stores 136
iOS App 136
Privacy 136
Permissions 136
Data Storage and Management 137
Data Transmission 137
Malware and Antivirus 138
Advertisement and Tracking 138
Android App 138
Privacy 138
Permissions 138

Data Storage and Management 140
Data Transmission 140
Malware and Antivirus 140
Certification 141
Advertisement and Tracking 141
Android App Stores in China 141
Salesforce App 142
Sign-In Credentials 142
Permissions 142
Data Storage 142
Malware and Antivirus 142
Code Security Scan 143
SharePoint for Microsoft 365 App 143
Permissions 143
Data Storage 145
Outlook Task Manager App 146
Privacy 146
Permissions 146
Data Storage 146
Data Transmission 147
AgilePoint NX Connector for Power Automate 147
Privacy 148
Permissions 148

Data Storage 148
Data Transmission 149
AgilePoint NX Activity for UiPath 149
Privacy 149
Permissions 150
Data Storage 150
Data Transmission 150
Contact Us 151

Legal Statements and Policies

This section provides legal statements and general policies for AgilePoint software and documentation.

Disclaimer of Warranty

AgilePoint, Inc. makes no representations or warranties, either express or implied, by or with respect to anything in this document, and shall not be liable for any implied warranties of merchantability or fitness for a particular purpose or for any indirect, special or consequential damages.

Copyright and Trademarks

Government Rights Legend

Use, duplication or disclosure by the U.S. Government is subject to restrictions set forth in the applicable license agreement and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013(c)(1)(ii) (Oct 1988), FAR 12.212(a) (1995), FAR 52.227-19, or FAR 52.227-14, as applicable.

Virus-Free Software Policy

AgilePoint recognizes that viruses are a significant security consideration for our customers. AgilePoint takes the following measures to make sure our software is free of viruses upon delivery:

- AgilePoint is built on top of Microsoft .NET framework. The pre-compiled executable is a.NET Common Language Runtime (CLR) application, not a native machine binary. As far as is known at this time, there are no viruses that infect .NET CLR executables.
- The virtual environment for the product packaging process in is fully isolated and protected, and anti-virus software is installed and running during packaging.
- The compiled and packaged software files are scanned by virus scanning software before they are released. An official disclosure document regarding the findings from our virus scanning activities is available upon request.

External Links in Documentation

AgilePoint, Inc. user resources, such as Product Documentation and community forums, sometimes include links or URLs that AgilePoint does not control. Third-party web sites are referenced for convenience only. AgilePoint has no control over these external web sites, so we cannot make any representations about their accuracy or guarantee their security, such as the potential presence of malware. You assume any and all risks associated with visiting non-AgilePoint URLs.

Scope of the Document

This guide provides the most current information on the security of AgilePoint NX architecture, customer data, privacy, operations, and cloud security. The details noted within this document provide transparency into how AgilePoint protects its employees and its customers. While this document does disclose some details about tools and approaches currently in use, it does not convey a binding contract between AgilePoint and the reader. AgilePoint continually evaluates its product solutions against emerging security threats and trends and may change policies or tools without announcement.

This document focusses on AgilePoint NX deployments that are hosted by AgilePoint. Unless otherwise stated, the security features would typically apply to both AgilePoint hosted public cloud environment, which uses a shared infrastructure and AgilePoint hosted dedicated cloud environment, which uses a dedicated infrastructure for each client.

Abbreviations, Terminology and Definitions

- **AgilePoint** – Refers to AgilePoint, Inc., a Delaware registered company with company number 3611708. The headquarters is at 1916 Old Middlefield Way, Suite B, Mountain View, CA 94043, USA.
- **The AgilePoint Ecosystem** – The AgilePoint ecosystem consists of hundreds of AgilePoint product deployments, app store, developer collaboration systems such as forums, online helpdesks, 24X7 support, knowledge base, several hours of how-to HD videos, ticketing systems, blogs, developer networks and partner networks for rapid solution development.
- **AgilePoint Product or Platform** – Primarily refers to AgilePoint NX Digital Business Platform, a True Low-Code/No-Code Rapid Application Development (RAD) platform. Using the platform, one can build and deploy various types of apps such as mobile apps, electronic-form based apps, process-based apps, intranet web pages, SharePoint apps, Salesforce apps, dashboards, reports and more. As a unified platform it enables discovery, design, modelling, implementation, collaboration, testing, version control, deployment, execution, monitoring, optimization, reporting, logging, management, audit, AI assistance, and more.
- **Deployment** – Customers can choose cloud-based deployments, on-premise deployments or go for a customized deployment based on the business needs.
- **Tenancy** – The cloud-based deployments are available as a Single-Tenant and as a Multi-Tenant Platform. In a Single-Tenant system, the AgilePoint NX server serves a single customer. A multi-Tenant system, allows more than one customer to execute their apps in their private space.

- **AgilePoint NX Private Cloud** – It is a Cloud Service Hosted by AgilePoint and is a single tenant system. Each cloud instance is dedicated to one client. Hence it can also be called AgilePoint NX Dedicated Cloud.

- **AgilePoint NX Public Cloud** – It is Cloud Service Hosted by AgilePoint and is a multi-tenant system. It is also referred to as AgilePoint NX OnDemand, since this mode of setup is readily available.

- **AgilePoint NX Cloud Services** – Jointly refers to the Public Cloud and Private Clouds hosted by AgilePoint.

- **Cloud Infrastructure Provider** – AgilePoint hosts its cloud using data center infrastructure provided by Amazon Web Services (AWS) and Microsoft Azure. AgilePoint is not a Cloud Infrastructure Provider and it does not own any own data centers.

- **Users of AgilePoint NX** – The most generic way to classify the users of the AgilePoint NX platform is based on user functional background. For more details, please refer to the chapter on the product.

    - **End Users** – The business users or just the users who access the app to fulfill their authorized functions.

    - **Administrators** – Are responsible for ensuring that the platform is smoothly running and take care of day-to-day operations, administrative activities, management of various technical aspects of the system and provisioning of systems if applicable.
    - **Developers** – Design, develop, test and deploy various types of business applications.

Security and Governance

AgilePoint is committed to protecting its employees, customers, partners, vendors, and the companies' data from illegal, or damaging actions by individuals, either knowingly or unknowingly. AgilePoint's Internet, intranet, and extranet hosted systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Internet browsing, social media, mobile apps, cloud-based services, and FTP are the property of AgilePoint. These systems are used only for business purposes serving the interests of the company, and of AgilePoint's customers in the course of normal operations.

Security measures at AgilePoint are guided by industry standards and regulations, such as, but not limited to ISO 27001, HIPAA, PCI DSS, NIST 800, GDPR, SOC 2, CPRA and more.

Regulatory Compliance

AgilePoint is built on strong security and data privacy foundations. Infrastructure, Operational and Platform security are the key components that AgilePoint engineers used as design pillars from Day 1. We combine built-in safeguards with administrative controls to protect our customers data. AgilePoint has ensured that it qualifies with all the required compliance programs. Listed below are some of the completed compliance programs:

- SOC 2 Type 2 and SOC 3 Type 2
- ISO 27001, ISO 27017 and ISO 27018
- GDPR
- EU-US Data Privacy Framework
- FIPS

AgilePoint's Information Security Management System (ISMS)

The ISMS covers guidelines to develop Information Security controls which cover standards, practices, procedures, guidelines and organizational structures. These controls are established to ensure that the specific security objectives of the organization are met. The scope of the ISMS covers the organization as a whole, or in certain cases parts of the organization, covering the relevant assets, systems, applications, services, networks and technology. AgilePoint's ISMS continuously pursues the implementation of actions addressing the effectiveness of the three basic components of data security.

The Three Tenets of Data Security

Confidentiality	•To guarantee that only duly authorized persons can access data and systems.
Integrity	•To guarantee the accuracy of information and systems against alteration, loss or destruction, whether accidental or fraudulent.
Availability	•To guarantee that the information and systems can be used in the required manner and at the required time.

Each year, AgilePoint seeks to establish and review its Information Security objectives and ensure the objectives are communicated. Appropriate resources are allocated to meet its Information Security objectives and that a process is in place to measure and improve its objectives. Each quarter, the status/metrics of these objectives is presented. Objectives are reviewed if there are major changes to the business.

The ISMS is designed to address the major risks that are identified to the information security of AgilePoint. In identifying, assessing, and managing these risks there are several options open to the organization according to its appetite for risk. In general terms, the organization's appetite for risk is defined as Low.

Corporate Information Security Objectives

AgilePoint is committed to ensuring its people, process, information and technologies are secured in line with best practices. AgilePoint is committed to ensuring the availability, integrity and confidentiality of its clients' data, employee information. To do this successfully, AgilePoint has defined five key objectives for information security.

- **Objective 1** – Conformance with ISO 27001 Standards.
- **Objective 2** – Deliver regular security awareness and education to staff.
- **Objective 3** – Continuous improvement of Logging, Monitoring and Incident Response practices.
- **Objective 4** – Continuous Improvement of the Security of its Cloud Infrastructure.
- **Objective 5** – Maintain uptime as per the customer agreements for production environments.

Overview of Information Security

AgilePoint employees understand that Information Security is the responsibility of everyone at work. AgilePoint's working environment incorporates employees in multiple offices and remote locations. All software services use either Single Sign-On (SSO) and/or Multi-Factor authentication (MFA). Information systems are encrypted, hosted in secure environments and backed up. The regional offices connect to the US office via site-to-site VPN. All systems have secure baselines configurations and are joined to the Active Directory. New machines undergo offline virus scan before joining to AD. Continuous vulnerability scanning is enabled on all assets. Hardware and software resources are tracked using asset management tools.

Access to locations, information and programs is based on the theory of least privileged and zero-trust. Granting of access to software or systems requires a change management request and management approval. Disabled or inactive accounts are removed immediately, unless management authorizes to retain that same for 90 days. All projects are managed through issue tracking and project management software Jira. All change requests, incidents and support requests are executed through service desk.

Group Policy Object (GPO) setting for all machines ensure all workstations have anti-malware, firewall, drive encryption and are password protected. Unapproved software cannot be installed. Access to buildings, software products and repositories is monitored and logged. Policies and procedures covering information security, acceptable usage, confidential information are reviewed and acknowledged by all employees on an annual basis. Human Resources has standardized practices for onboarding and offboarding employees. Vendor security reviews and vendor onboarding procedures are in place. Data is encrypted, inventoried and restricted based on business need. Customer hosted instances are secured and monitored. All employees are annually trained in security awareness, tested with phishing exercises and their device security is managed using tools such Microsoft InTune and access restricted by SSO/MFA. Product development follows a secure SDLC regiment that incorporates secure coding practices, security testing and vulnerability scanning.

Remote Access to AgilePoint’s Network

Remote access to AgilePoint's corporate network, applications and cloud services is essential to promoting efficient productivity. Whether the access is from a remote office or while traveling, all employees need to follow corporate security mandates. AgilePoint’s networks, devices and services can only be used for AgilePoint business. Accessing the corporate Internet or using AgilePoint device(s) for outside business interests is forbidden and monitored. Remote access is always secured over a VPN. AgilePoint provides the employee with mobile device(s) and service for business use only. AgilePoint permits its employee to use their personal devices(s) only if the employee has signed an agreement to allow Mobile Device Management (MDM) to be installed on the device(s) and abides by the MDM settings.

While using an AgilePoint-owned computer to remotely connect to AgilePoint's corporate network or services, users are not allowed to connect to the remote host over a public WIFI (e.g., airport or restaurant). Use of external resources to conduct AgilePoint business must be approved in advance by the Chief Information Security Officer (CISO) and the employee's manager. All systems that that connect to the AgilePoint's networks have up-to-date anti-virus software installed. Bring Your Own Device (BYOD) equipment used to connect to AgilePoint's networks must meet the guidelines of the Information Security Policy.

Risk Management

AgilePoint follows standardized Risk Assessment Methodology in its day-to-day activities to prevent the loss, corruption, deletion, disclosure, or non-availability of its information assets.

Risk Assessment

The Information Technology Risk Assessment is one of the key steps in the execution of AgilePoint's information security program. Using this assessment, AgilePoint gets to know of the types of risk and information it should protect, the level to which such protection should be implemented, and the costs in terms of financial costs and operational constraints which AgilePoint now believes to be appropriate to reduce the risks to acceptable levels.

Risk Analysis

AgilePoint has based its risk analysis process on the guidance published by ISO 27001.

1. **Scope of the Analysis** – All confidential information that AgilePoint creates, receives, maintains, or transmits must be included in the risk analysis.

2. **Data Collection** – Defined methods for data collection of assets with confidential information.

3. **Identify and Document Potential Threats and Vulnerabilities** – Develop a critical analysis of the vulnerabilities and likelihood of threats.
4. **Assess Current Security Measures** – Look for potential weak points.
5. **Determine the Likelihood of Threat Occurrence** – Perform a risk analysis across the network.
6. **Determine the Potential Impact of Threat Occurrence** – What happens if an attack occurs.
7. **Establish a Threat Matrix** – What are the vulnerable points in the network.
8. **Determine the Level of Risk** – Perform a risk analysis on all data collected.
9. **Finalize Documentation** – A summary to address the risks exposed in this analysis.

Risk Assessment Process

AgilePoint's risk assessment process is implemented by the CISO. The first step in risk assessment is the identification of all assets which may affect confidentiality, integrity and availability of information in the organization. The next step is to identify all threats and vulnerabilities associated with each asset. Every asset may be associated with several threats, and every threat may be associated with several vulnerabilities. For each risk, a risk owner has to be identified – the person or organizational unit responsible for each risk. The consequences for each combination of threats and vulnerabilities for an individual asset if such a risk materializes is determined. Finally, consequences for each asset and the likelihood of each risk are put together to determine the risk value.

Risk Treatment

The outcome of the risk management process is one of the four:

1. **Risk Reduction** – Reduce the risk by applying the necessary remedial measures.

2. **Risk Transfer** – Transfer the risks to a third party – e.g. by purchasing an insurance policy or signing a contract with suppliers or partners.

3. **Risk Avoidance** – Avoiding the risk by discontinuing a business activity that causes such risk.

4. **Risk Acceptance** – Accept the risk – this option is allowed only if the selection of other risk treatment options would cost more than the potential impact should such risk materialize.

IT Infrastructure, Data Center and Cloud Security

Customers can choose to deploy AgilePoint NX from the following types of deployment approaches.

Type of Deployment	IT Infrastructure	Hosting of NX	Data
On-premises at Customer Location and/or Customer's Private Cloud	Owned by customer.	Managed by Customer Administrator.	Owned by Customer.
AgilePoint NX Private Cloud	Managed by cloud service provider - AWS, Azure, or others.	Managed by AgilePoint Administrator.	Owned by Customer.
AgilePoint NX OnDemand (Public Cloud)	Managed by cloud service provider - AWS or Azure.	Managed by AgilePoint Administrator.	Owned by Customer.

The responsibility of security, monitoring, responding to alerts, and the access to infrastructure varies as per the hosting model. This document focuses only on cloud deployments managed by AgilePoint. This is shown in rows 2 and 3 of the above table. Please note that AgilePoint does not host any production software system in its office premises. An AgilePoint-hosted cloud environment offers the following from an infrastructure perspective:

- Firewall and other various network security features

- Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)
- File Integrity Monitoring (FIM)
- Antivirus and other malware protection
- Physical access controls
- Logical access controls
- Audit logging mechanisms
- Backups and disaster management
- Monitoring, alerting and reporting

It is important to note that not every feature listed above is available in NX OnDemand multi-tenant public cloud. Also, some of the features that are listed above are paid add-ons in NX dedicated cloud hosted by AgilePoint. These features are specifically requested by customers to meet regulatory compliances such as HIPAA, PCI DSS and more.

Data Center Security

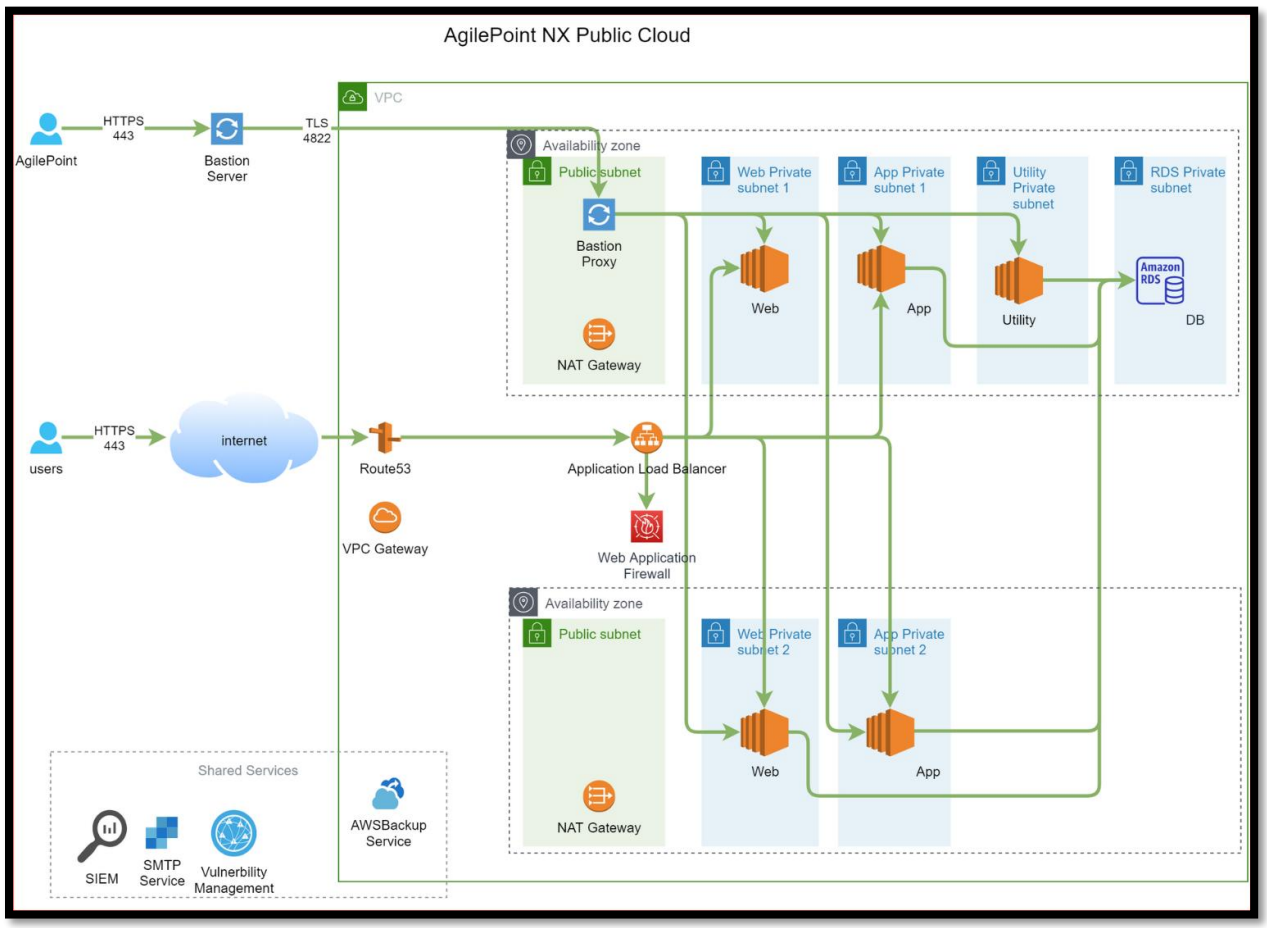
Depending on the type of deployment, the security needs, administration activities, management, and day-to-day operation may vary.

AgilePoint NX OnDemand (Public Cloud)

AgilePoint NX cloud-based deployments are hosted on cloud infrastructure providers AWS and Azure. These service providers provide high levels of physical and network security, along with hosting provider vendor diversity. Though the hardware is shared between customers, each customer still gets their own dedicated database with complete data isolation from other customers for highest level of data privacy.

- **AWS** – At the time this document was created, AWS was available in 36 geographic regions and 114 availability zones around the world. Key points about AWS deployments:
    - AgilePoint has implemented Amazon Virtual Private Cloud (VPC) (https://aws.amazon.com/vpc/) and use web application firewall capabilities of AWS WAF (https://aws.amazon.com/waf/). AWS cloud infrastructure comes with many security features. For more information, refer to https://aws.amazon.com/security/.
    - AgilePoint supports data centers in us-east-1 (north Virginia), us-west-1 (north California), and ap-southeast-1 (Singapore). Each region functions as both primary and disaster region.
    - Customers in Europe can choose the data center in Frankfurt. Moving forward, AgilePoint could have more locations, if customers have a specific region needs.
    - Encryption is applied for data in transit with TLS 1.2 across all servers.
    - Connectivity options are available to enable private or dedicated connections from the customer's office or from the customer's on-premises environment.

Network Diagram of Multi-Tenant Public Cloud



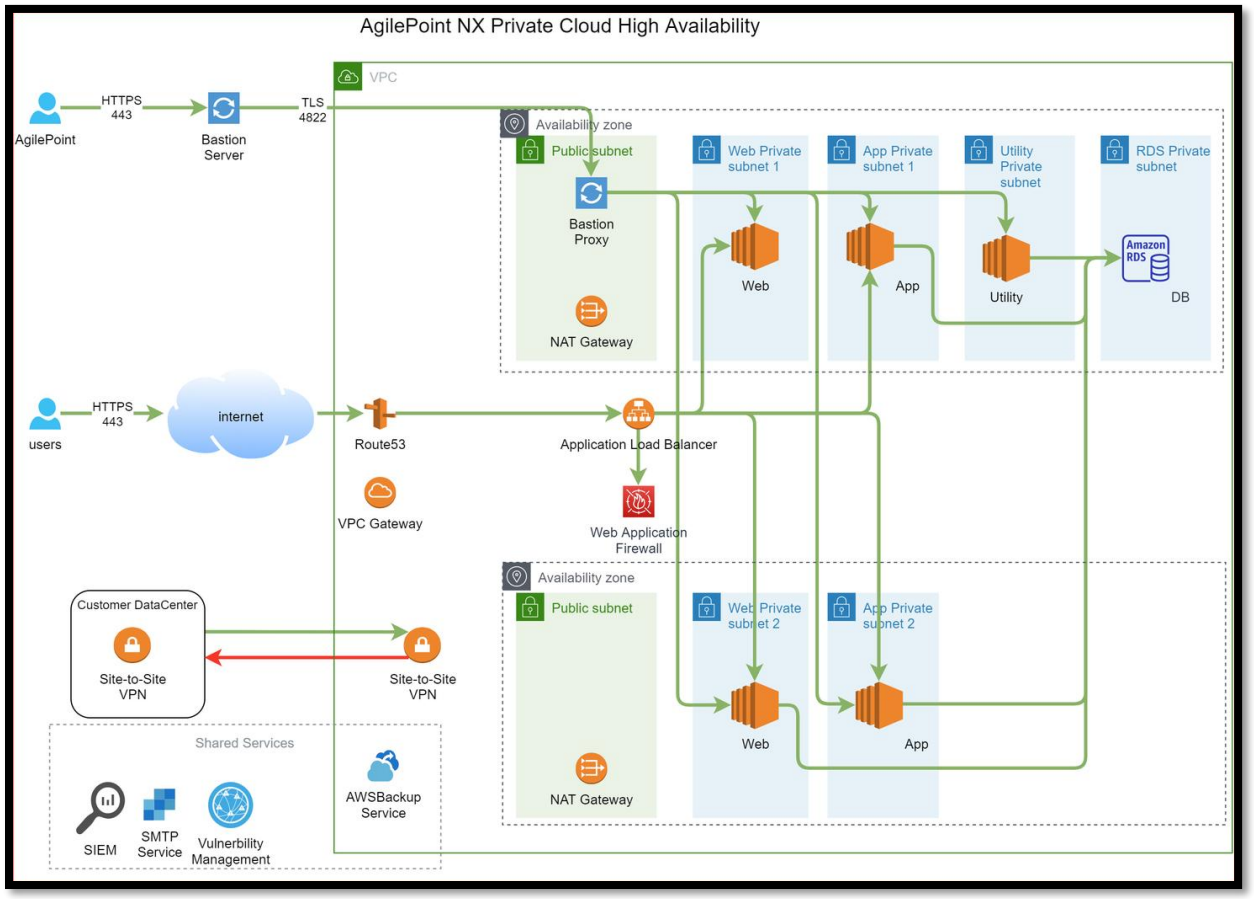
AWS and Azure provide advanced facilities such as power, security, and networking with a guaranteed minimal 99.95% to full 100% uptime, along with N+1 redundancy of power, Heating, Ventilation and Air Conditioning (HVAC), and network redundancy. Access to these sites is highly restricted, both physically and electronically, via public (Internet) and private (intranet) networks. The physical, environmental, and infrastructure security plans, including business continuity, are maintained by audited security program including SOC 2 and ISO 27001.

AgilePoint NX PrivateCloud

In this mode of deployment, while the security points described earlier still hold good, each customer gets their own dedicated virtual machines and databases in AWS or Azure. Customers get to choose the infrastructure provider, which is either

AWS or Azure. AgilePoint provides the cloud hosting to the customer, and also manages the same on behalf of the customer. The customer may opt to connect to their internal systems hosted within their firewall using a site-to-site VPN or other secure channels.

Network Diagram of Dedicated Cloud



Network Security

AgilePoint's product infrastructure is built with Internet-scale security protections in mind. The network security protections stop unauthorized network access both, to and from within the infrastructure. Our security measures use enterprise-grade routing and network access control lists. Network-level access control lists are implemented in AWS VPC security groups, which applies port-level and address-level protections to all the server instances in the infrastructure.

The security controls implement a fine-grained control for network traffic from a public network as well as between the internal server instances. The network restrictions define a many-tiered approach to ensure that only the appropriate types of devices can communicate. Changes in the network security model are controlled by standard change control processes, which is actively monitored. All the existing network control rules and changes are regularly evaluated for security risk. For AgilePoint instances that run on AWS, AWS Security Group firewall is used for network protection. For more information, refer to https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

To protect against any attack in AWS, AgilePoint leverages AWS Web Application Firewall (WAF) (https://aws.amazon.com/waf/). The AWS website states:

> AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application. New rules can be deployed within minutes, letting you respond quickly to changing traffic patterns.

IP Whitelisting

IP whitelisting is a security feature used for limiting access to trusted users. IP whitelist is a list of trusted IP addresses or IP ranges from where customer can access the network. In case of Dedicated Cloud hosted by AgilePoint, customer can provide AgilePoint with whitelisted IP addresses. This whitelisted IP addresses typically covers the IP addresses of customer’s office premise and other customer’s networks.

Firewall Management

Firewalls have implicit deny-all rules. Firewall rule sets are configured to permit authorized inbound and outbound traffic by their IP addresses to the trusted environments. Inbound Internet traffic is limited to restricted IP addresses within

the Demilitarized Zone (DMZ) within the cardholder environment in case of PCI DSS compliant network.

Anti-spoofing measures are implemented to detect and block forged sourced IP addresses from entering the network. Firewall rule sets are documented and reviewed regularly and sign-off is recorded in a ticket. Changes are made to the configuration of the firewall and the firewall rule sets after a review of the impact of the changes are performed by relevant stakeholders. Firewall changes are tested for both security vulnerabilities and functionality in a test environment prior to being placed into the production environment.

Stateful inspection firewalls are in use, with Network Address Translation (NAT) in place to prevent IP masquerading. Only those ports and services which are required for business purposes are enabled. The firewalls explicitly deny inbound and outbound traffic using any other ports and services. Only those protocols which are required for business purposes are enabled. The firewalls explicitly deny inbound and outbound traffic using any other protocols. The access to the firewall is restricted to the Cloud VTC team. All laptops and desktops which connect to AgilePoint network also have local firewall enabled.

Logging and Auditing of Logs

AgilePoint has implemented CloudTrail on AWS to log, monitor and retain account activity related to actions across AWS infrastructure. CloudTrail captures event history of AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. In addition, CloudTrail is used to detect unusual activity AWS accounts. Continuous Logging and Monitoring is also enabled on our Azure Infrastructure. AgilePoint has engaged a well-established 24/7 Managed Detection and Response (MDR) provider for 24/7 Security Monitoring services of its IT Asset Infrastructure.

In addition, all the generated logs are regularly audited. The logs from VPN connections, all OS (windows desktop and server side), logs from network devices, logs related to disaster management and apps that are part of the infrastructure. This process is subject to external audit as part of ISO compliance.

Monitoring

AgilePoint has invested heavily on automated monitoring, alerting, and response technologies as hundreds of our customers run mission-critical business apps on cloud. The infrastructure is instrumented to alert security engineers and administrators for potential issues. Monitoring is enabled at 2 levels.

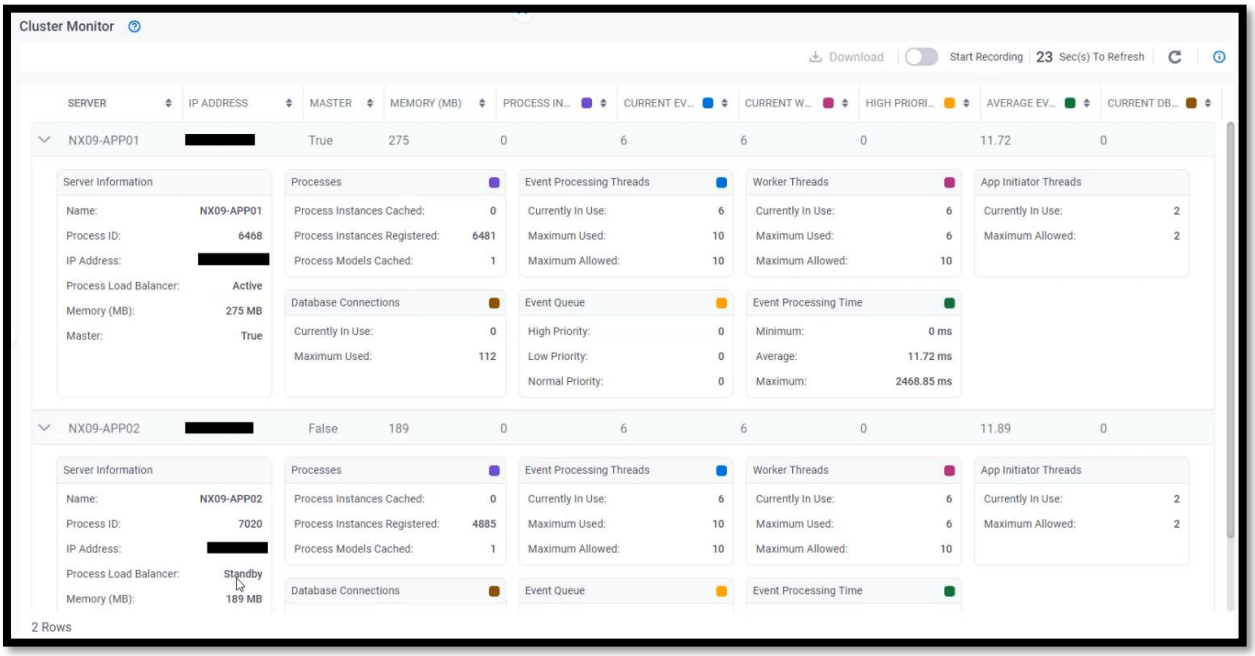
- Product level
- Infrastructure level

Product Level

AgilePoint's IT team and Customer Support team monitor the AgilePoint Server, infrastructure components, and the apps. AgilePoint NX provides the system administrator with advance monitoring capabilities of NX app via System Monitor, Performance monitor and Cluster Monitor.

- The System Monitor screen provides details of the system health which includes performance overview for thread usage, database connections usage, average event processing time, user count, license information, app overview, email notification overview etc.
- The Performance monitor screen displays real time statistics for event thread usage (system activity threads), working thread (human activity threads) usage, and database connections. AgilePoint NX extensively logs various concerned activities and actions going at the server level, including but not limited to, the end points, storage, CPU, RAM utilization, and many other details.
- Cluster monitor is a web-based administrator screen to monitor all the instances of AgilePoint NX server, within the same cluster providing key statistical information of all the nodes in the cluster. This includes information about the server node, memory utilization, processes and threads, average event execution time, database connections and more. The administrator can record the performance of the entire cluster for a given time period and download the same for further analysis.

Webbased In-built Cluster Monitoring



Infrastructure Level

All the logs and events of various infrastructure components are continuously monitored in real time. AgilePoint uses Site24x7 (https://www.site24x7.com/) to monitor any changes to infrastructure and the infrastructure health. AgilePoint has defined triggers for many parameters that are monitored (CPU, memory, services, disk space, database memory, database CPU, disk I/O, and more).

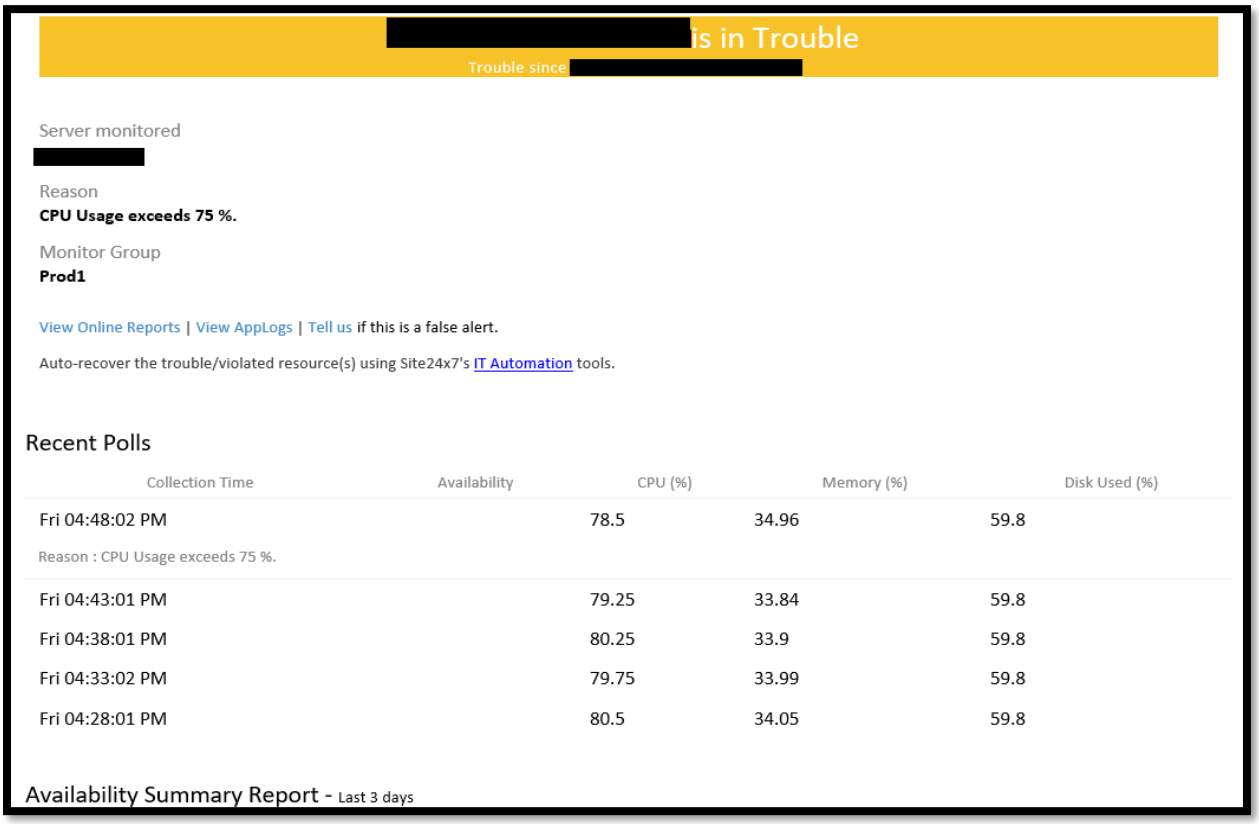
Alerting and Reporting

The onset of any unexpected or unplanned event, error rates, application attack, abuse scenarios or anomaly results in the appropriate teams taking rapid actions and neutralizing the threat. When any anomaly occurs, AgilePoint's security engineers, administrators, and concerned response teams are immediately notified. The concerned teams investigate the alerts, analyze the situation, and take appropriate actions. Automated triggers are designed into the system to immediately respond to predefined situations. This ensures that the system protects itself against a wide variety of undesirable situations. Traffic blocking,

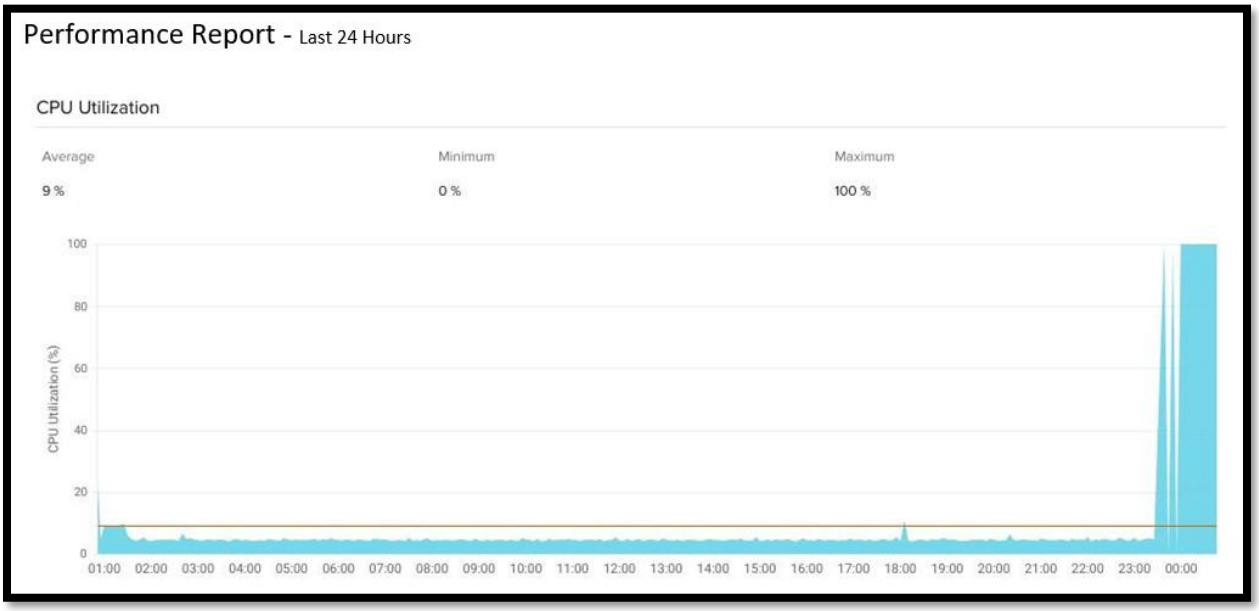
quarantine, process termination, and other protective functions kick in at pre-defined thresholds to ensure that the system protects itself against a wide variety of undesirable situations.

Reports are scheduled to reach the concerned teams, as per our security policy, at regular intervals. Shown below are examples of 2 reports. The first is a near-time email alert, alerting the concerned teams of the CPU utilization rate going over a predefined threshold (85%). The second email, a daily report, shows the timeline view of the CPU utilization over a period of 24 hours.

Screenshot from an Alert



An Alert Showing CPU Utilization Hit 100%



SIEM and MDR Implementation

Managed Detection and Response (MDR) solutions identify active threats across an organization and then respond to eliminate, investigate, or contain them. It assists in rapid incident response to eliminate threats and implement remediation actions. It combines tools, technologies, procedures, and methodologies used to provide full cybersecurity lifecycle. SIEM (Security information and event management) provides real-time analysis of security alerts generated by applications and network hardware. AgilePoint has implemented Alert Logic for its SIEM/MDR.

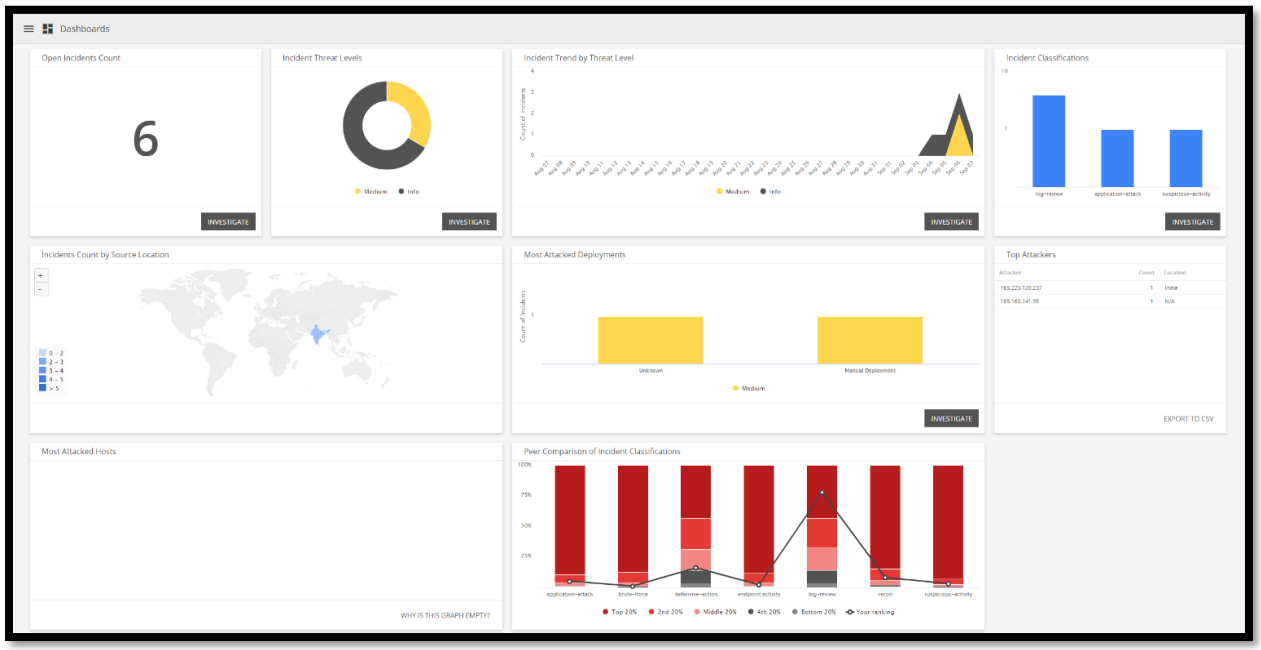
The following security features are covered:

- Asset discovery
- Vulnerability scanning
- Cloud security configuration checks
- Extended Endpoint Protection

- Threat Risk Index (TRI)
- Threat visibility
- File Integrity Monitoring (FIM)
- Web Log Analytics (WLA)
- Log management, storage, and search
- Compliance readiness

AgilePoint has installed network Intrusion Detection System (IDS) in AWS and Azure, for incident detection and generation, log collection, and log analytics to provide information on active threats in our environments.

SIEM and MDR Implementation



Access to IT Infrastructure

AgilePoint NX instances are hosted on AWS and Azure. AgilePoint's IT team manages the cloud hosting from our corporate offices. The following sections explain how the access to the IT infrastructure is kept secure.

AgilePoint NX Private Cloud

Though the AgilePoint NX installations are managed by AgilePoint IT team, AgilePoint's Support, Product, and Services teams are not given access to the customer's data and apps. Customers must create a dedicated support account if AgilePoint's Support team must troubleshoot any issue in their environment. Only authorized AgilePoint employees from the Support, Product, or Services team are allowed to access the environment using authorized browser-based session, after approval from the customer. Direct network connection to the customer's tenants, even though SSH and similar protocols, is prohibited.

AgilePoint NX Public Cloud

Access to the multi-tenant, public cloud environment works exactly as access to dedicated cloud hosted by AgilePoint. In a multi-tenant environment, one customer cannot access the data and apps of another customer.

AgilePoint Office Premises

AgilePoint ensures that the premises from where AgilePoint NX Cloud Services is accessed are secure. AgilePoint's offices employ alarms of all ingress and egress point and sensitive areas. External people without permission cannot enter. Only employees with active security badges can access the building or sensitive areas where they have been given permission.

AgilePoint has implemented zoning in the office space. Employees can access only those areas to which they have access rights, based on roles. For access to infrastructure components, servers, and similar services, access is minimized to only those individuals whose jobs require it. All employee access to office building and sensitive areas are validated by an internal approval process.

AgilePoint does not have any component of the cloud services running from any of its offices.

The office premise is under constant security surveillance and is regularly inspected by reputed independent external agencies. These agencies review electricals, power systems, annunciator, alarm systems, detectors and various other security features

inside the office perimeter and submit a security report. The security reports are reviewed by external auditor as part of the ISO 27001 process.

Protection from Malware, Viruses, and Hackers

AgilePoint takes all steps to ensure its IT systems are not compromised. System owners (PCs, Macs, laptops, desktops, workstations, and VMs) cannot install unauthorized software. Internal audits are conducted every quarter to ensure compliance. The Internet connectivity is monitored for threats by viruses in systems and firewall at corporate level. Except IT team, no one in the organization can alter the firewall and antivirus settings. AgilePoint has deployed antivirus on all of its VMs in its network.

Emails are scanned for malware and phishing attempts. Awareness programs are run at the corporate level. AgilePoint enforces online internal assessments on security and governance. All employees have to take and pass the tests. Email and other collaboration software's use 2-factor authentication. All systems have brute-force login prevention mechanism. Multi-Factor Authentication (MFA) is now mandatory for all accounts.

Data Backup

AgilePoint NX OnDemand (public cloud) provides industry standard backup plans that meets the business needs of most customers.

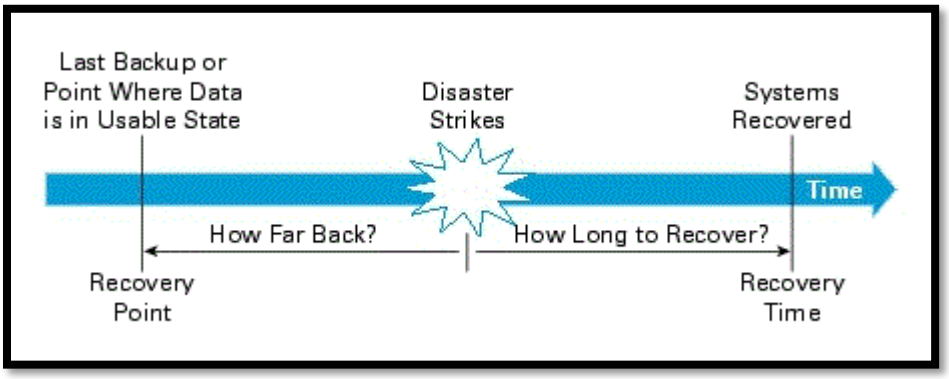
RPO and RTO

Minimizing downtime and data loss is measured in terms of 2 concepts:

- **Recovery time objective (RTO)** – The time it takes after a disruption to restore a business process to its service level, as defined by the operational level agreement (OLA).

- **Recovery point objective (RPO)** – The acceptable amount of data loss measured in time.

RPO and RTO



In order to avoid unacceptable consequences associated with a break in business continuity, it is very important to decide an acceptable RTO and RPO based on the impact to the business when systems are unavailable.

Key features of AWS Backup

AgilePoint uses AWS Backup (https://aws.amazon.com/backup/) leverages the native snapshot capability of AWS to create and manage snapshots, thus enabling fast backup and recovery process. It is used to back up the following backup targets:

- EC2 instances (including some or all of the instance's EBS volumes)
- Amazon Relational Database Service (RDS) databases

Some of the key features are:

- **Cloud Native** – AWS Backup is a dedicated backup, recovery and DR solution for AWS, not an add-on for an "on-premise" backup solution.
- **Encryption** – AWS Backup leverage AWS KMS encrypting all backups in backup vault.

- **Deployment** – AWS Backup uses the native snapshot capability of AWS and does not require any agents to be installed.
- **Recovery** – AWS Backup does not backup to an S3 repository, but creates and manages snapshots in the snapshots section of the account/region. This enables faster backup and recovery to support shorter RPO/ RTO.
- **Extensible** – AWS Backup supports cross-region backups.

AWS Backup

As discussed earlier, each AWS region supported by AgilePoint functions as both primary and disaster recovery region. Example, if the deployment primary region is us-east-1 then us-west-1 is the Disaster Recovery region and vice versa. The AWS Backup schedule is published in the table below. All backups are replicated to the disaster recovery region. For data security, AgilePoint maintains 2 copies of each backup in 2 different regions at all time.

AgilePoint NX Public Cloud

Differential backups are performed at midnight, local server time. The data sets are stored on a distributed file storage facility such as Amazon's S3 and the data is replicated across different region. 2 copies of the backup are maintained. The backup is encrypted and is protected through access-controlled restrictions. The backups are stored for a period of 7 days. Backups have a size restriction based on the service agreement. Backup is done for all the environments (such as development and production) that exist in the system. AgilePoint leverages AWS or Azure cloud services for hosting, backup, recovery, and transportation.

	Non-Production Environment		**Production Environment**	
	Single Region	**Cross Region**	**Single Region**	**Cross Region**
RPO	<=24 Hours	<=24 Hours	<=24 Hours	<=24 Hours

	Non-Production Environment		Production Environment	
	Single Region	**Cross Region**	**Single Region**	**Cross Region**
RTO	24 Hours	24 Hours	> 4 Hours	< 4 Hours
Data Retention	7 Days	7 Days	14 Days	14 Days

Note: All values in Table #2 are indicative and are subject to change based on business decisions. Please contact sales for more information.

AgilePoint NX Private Cloud

In this hosting option, customers can opt for more frequent backups, as a paid add-on, with the RPO that best suits the customer's business needs. For mission critical business apps, customers choose the minimum possible RPO, as agreed between AgilePoint and customers. Apart from this, the number of backups stored and the retention period of the backups is customized based on the customer's business continuity policy.

The table below provides indicative RPO and RTO for AgilePoint NX Private Cloud.

	Non-Production Environment		Production Environment	
	Single Region	**Cross Region**	**Single Region**	**Cross Region**
RPO	24 Hours	24 Hours	<=1 Hours	<= 24 Hours <= 12 Hours (paid) <= 6 Hours (paid)

	Non-Production Environment		Production Environment	
	Single Region	**Cross Region**	**Single Region**	**Cross Region**
				<= 4 hours (paid)
RTO	24 Hours	24 Hours	≤ 4 Hours	≤ 4 Hours
Data Retention	7 Days 14 Days (paid)	7 Days 14 Days (paid)	7 Days 14 Days (paid)	7 Days 14 Days (paid)

> **Note**: All values in Table #3 are indicative and are subject to change based on business decisions. Please contact sales for more information.

AgilePoint can provide additional features (based on sales agreement) such as Public IP address, Extra bandwidth for large sized backups as agreed with customers, Database encryption, Encryption for data in transit, Automatic process archival for completed process instances within agreed number of days after completion, Different backup tiers (back up every 4/6/12/24/etc.), configurable data retention period and regions where the data is stored.

> **Note:** AgilePoint disaster recovery plan does not cover site-to-site VPN. Site-to-site VPN changes on customer network so it is outside AgilePoint's control.

Business Continuity - Disaster Recovery

AgilePoint's Information Security Management System (ISMS) Compliance Committee has enforced and regularly reviews its comprehensive disaster recovery and backup plan policies and processes along with the execution of the DR processes. A formal risk assessment is regularly undertaken to determine the requirements of its disaster recovery plan. AgilePoint’s disaster recovery plan covers all essential and critical infrastructure elements, systems and networks, in

accordance with key business activities. The disaster recovery plan is periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed. AgilePoint employees are imparted training and are fully aware of the disaster recovery plan and their respective roles. The disaster recovery plan is kept up to date to consider changing circumstances. Hosted customer data is backed up on a regular basis and readily accessible for recovery. Corporate data is backed up on a regular basis and readily accessible for recovery.

AgilePoint's Business Continuity Plan provides for events such as network outage, power outage, physical damage to infrastructure, fire, flooding, human error, natural disaster, planned upgrades, and more. Our recovery processes are validated continuously through regular maintenance and support processes. AgilePoint has invested time and resources to plan and prepare, to train employees, and to document the disaster management processes. AgilePoint has a detailed Disaster Recovery and Backup Policy and Procedure to provide for effective recovery from disasters. This policy primarily relies on infrastructure redundancy, data replication, and backups. Annually, the DR drills are performed by AgilePoint Cloud-infra team. DR exercise reports are shared with the compliance auditors.

The DR requirement for dedicated cloud hosted by AgilePoint varies among different customers. This is handled on a case-by-case basis, based on AgilePoint's agreements with specific customers.

AgilePoint NX Public Cloud

The planned DR setup consists of 1 primary site and 1 backup site. The backup site is a replica of the primary site and includes HA (optional). The typical RTO (subject to change) = 2 hours + [data in GB] * 0.167 hours. The planned DR procedure includes drills to ensure that the system is sane. The drills do not impact the service. A drill is performed once in a year. The drill report can be shared upon request. Only AgilePoint IT can initiate the drill.

AgilePoint NX Private Cloud

This hosting option has all the benefits of a OnDemand (public cloud) deployment, plus customers have an additional option to tailor the DR procedures as per their

corporate business continuity policies, based on the mutually agreed contractual clause. As a paid add-on, customers can choose the location of the primary and the DR site, both of which can be either on Azure or on AWS.

In the upcoming DR implementation plan, the switch-over will be manually triggered. When the production site is available again, the switch back is initiated manually. The DR mode that is available is Active/Passive from backup.

Capacity Planning and Demand Forecasting

Availability and uptime are important aspects of business continuity and AgilePoint ensures that proper capacity planning and management is done to ensure that the infrastructure on which AgilePoint apps run, do not collapse due to the workload. AgilePoint takes full ownership of capacity planning on all its hosted environments. The goal is to avert adverse impact on the business operations which could arise due to lack of resources or poor planning.

Initial Capacity Planning

The installation team will adjust the customer's deployment with attention paid to:

- **Processing capacity** – Number of CPUs needed to support normal operations.
- **Database storage** – Determine customer's data storage policy, including archiving (i.e. offline for future purposes). Planned growth is also considered at the time of installation.
- **Security overhead** – If security monitoring or reporting software is deployed, then the servers and data usage that security services consume need to be added to the capacity planning criteria.

Post Installation Capacity Management – AgilePoint NX Private Cloud

The IT team continuously monitors the system utilization. When readings indicate that capacity needs to be expanded to maintain SLA levels, a ticket is opened by IT in the Service Desk to upgrade the architecture. The Customer Success Management Department (CSM) receives a notice when the Service Desk ticket is opened. CSM then contacts the customer to discuss for approval, planning, execution and closure.

Post Installation Capacity Management – AgilePoint NX Public Cloud

The Public Cloud is a multi-tenant deployment that shares the same hardware, but each customer receives a separate dedicated database that is isolated from other customers. To maintain a balance between costs and performance, AgilePoint's IT Department monitors the consumption of resources by each customer entity in the Public Cloud. Being a shared resource, overutilization by a single customer can affect performance for all customers.

When set thresholds are crossed, IT opens a ticket in Service Desk to address the issue with the customer. The customer has the choice of reducing resource consumption or moving to a Private Cloud deployment with fewer restrictions. In addition, as the customer accounts grow in the Public Cloud, IT periodically adjusts to higher "normal" system loads.

Bandwidth monitoring

Bandwidth is provided by the cloud provider. Bandwidth monitoring is part of capacity management's effort to reduce the impact on the customers' traffic and ensure availability and responsiveness.

Bandwidth can be impacted by:

- Cloud provider’s SLA violations
- Overutilization by a single customer (only in Multi-Tenant Public Cloud)
- Unexpected growth in app usage
- Unexpected cloud service provider outage

When automated alerts are sent to IT to indicate bandwidth congestion, IT will open a ticket in Service Desk To notify CSM and IT. CSM and IT will collaborate to determine the best method to meet the system requirements. This may include conferring with the cloud provider and/or the customer(s) to discuss possible upgrades or remediation.

Malware Protection

This section is applicable to both NX on-demand (multi-tenant public cloud) and NX private cloud - dedicated cloud hosted by AgilePoint. Antivirus systems are deployed on all system components. The antivirus systems are kept up to date and run periodic scans. The antivirus systems cannot be tampered with or altered except for limited times by an authorized user on a case-by-case basis.

Vulnerability Assessment and Penetration Testing (VAPT)

AgilePoint performs VAPT testing as part of the SDLC testing cycle which is part of its ISO 27001/SOC II compliance. AgilePoint engages with an independent third-party vendor to perform penetration testing on the hosted cloud system. Customer may perform own testing by coordinating with AgilePoint's Cloud Operations team. Arrangements such as whitelisting of IP addresses will be facilitated.

One of the vulnerability Management tools used by AgilePoint is Tenable, which helps in identifying, categorizing, and prioritizing vulnerabilities across the assets (Windows/Linux). It provides scanning capabilities to discover compliance policy

violations (CIS Benchmark). The reporting capabilities allow the security team to prioritize the remediation process.

File Integrity Monitoring

File integrity monitoring is a paid add-on that is provided in the dedicated cloud hosted by AgilePoint. Compliances such as PCI DSS and HIPAA require a file integrity monitoring system deployed on the infrastructure components. Customer can define processes with AgilePoint's Cloud Operations team to manage alerts.

Golden Image and Hardening

Golden image is a process of building a pre-configured image for the infrastructure deployment. A golden image will have the functionality, security, and settings applied. AgilePoint uses AWS EC2 Image Builder (https://aws.amazon.com/image-builder/). AgilePoint Golden images are built with DOD STIG Standard. STIGs are the configuration standards for DOD [information assurance, or IA] and IA-enabled devices/system. The STIGs contain technical guidance to 'lock down' information systems/software that might otherwise be vulnerable to a malicious computer attack.

In additional to the DOD STIG standard, AgilePoint scan all systems with CIS standard and apply certain CIS recommended standard configuration. Post deployment of the VM, the infra team goes through the Windows 2022 Server hardening checklist that updates that the settings and configurations related to:

- Up to date with patches and hotfixes
- UAC hardening
- Network security configurations
- Securing Registry configurations
- Audit policy settings
- Anti-virus and anti-malware configurations

- Windows services configurations
- NTP settings and many more

Software Updates and Security Patches

AgilePoint updates the cloud environment with the latest software and security patches soon after they become available. The security patches are applied at 2 levels:

- The operating system and other infrastructure service (for example, Microsoft IIS) level.
- AgilePoint NX itself.

The Shared Responsibility Model

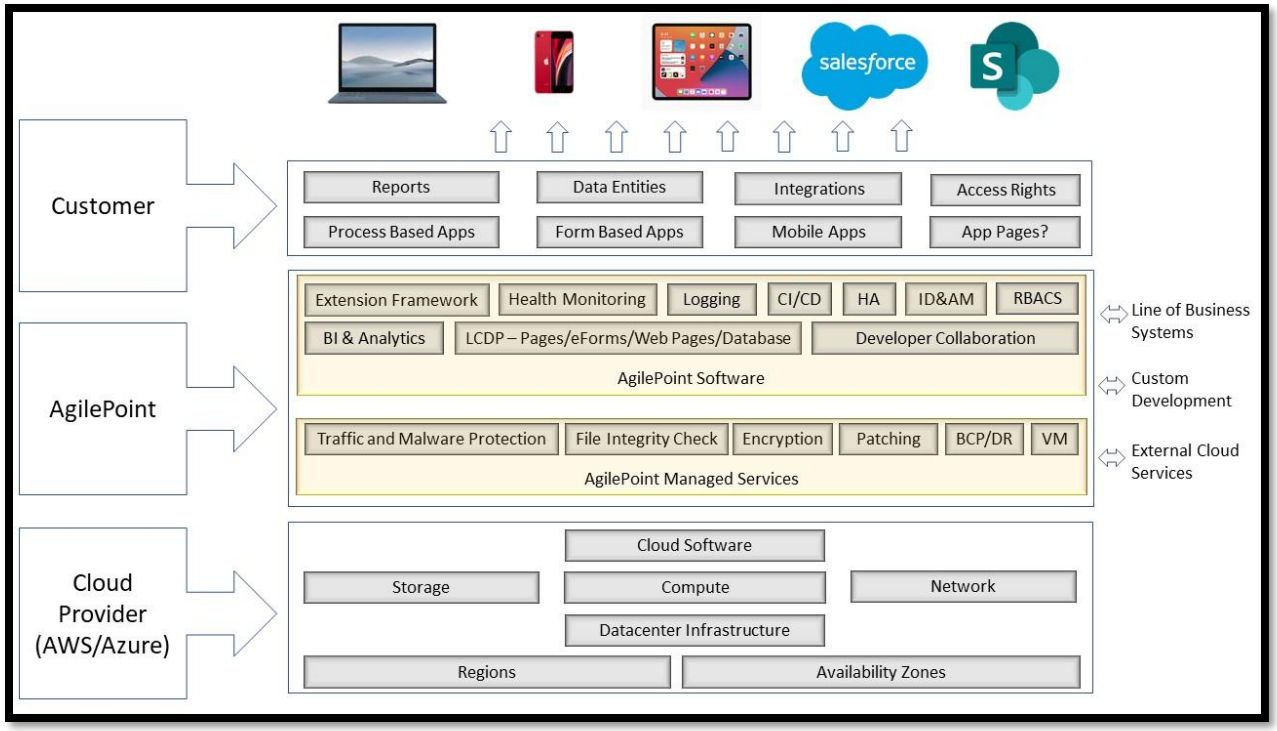
Compliance and Security is a shared responsibility between AgilePoint and the customer. The idea of the 'shared responsibility model' is to provide clear clarity on which aspects are owned by AgilePoint and which are owned by the customer. The responsibility in AgilePoint hosted private cloud, is trifurcated amongst the cloud provider (AWS and Azure), AgilePoint and the customer.

Responsibility of the cloud provider: The cloud provider is responsible for protecting the infrastructure elements of the data center/cloud offering. This includes the hardware, the facilities where the hardware is located, the cloud management software, power management, networking and more.

Responsibility of AgilePoint: From an infrastructure perspective, based on the license, AgilePoint will manage file integrity monitoring, firewall (network security, intrusion detection and intrusion prevention), logging, encryption along with the VM in high-availability configuration. The backups along with disaster recovery, based

on the agreement will be managed by AgilePoint. The Low-code rapid application development platform comes in-built with health monitoring, identity and access management and logging services.

The Shared Responsibility Model – AgilePoint Hosted Private and OnDemand Cloud



Responsibility of the customer: The customer is responsible for the apps and the data.

Security in Operations

AgilePoint incorporates the latest tools to secure its networks and data. AgilePoint maintains a secure environment in its product development, network operations, and business practices. The standards of ISO 27001 and SOC 2 guide the day-to-day operations and security protocols are adhered to by all employees.

AgilePoint provides all employees with required security training and a variety of secure communication tools. Various methods to probe and test the security of its networks and personnel are employed on a continual basis. These probes are unannounced with failures resulting in additional employee training. All tools, software, and hardware used by employees are company issued, configured, and monitored by AgilePoint. Additionally, it employs a variety of global internal communication strategies to ensure employees clearly understand their roles and responsibilities and receive important updates promptly. These strategies include orientation and training programs for new hires, regular management meetings to discuss business performance, security and other matters, and digital channels such as online collaboration, email, and information posted on company intranet.

Third Party Software and Open-Source Libraries

As part of the secure software development lifecycle, AgilePoint product engineering team uses externally developed software and libraries. The external fall into one of the two categories:

- Software OEM vendors.
- Open-source libraries.

Software OEM Vendors

AgilePoint performs the below mentioned detailed and through evaluations, which typically last at least a couple of months.

Vendor’s Profile

Through checks are carried out to ensure that the software that is meant to be procured is from a reputed company. Wide adoption of the software from the vendor is another important criterion. The vendor should have implemented various regulatory compliance programs such as ISO 27001, GDPR, etc.

Software’s capability

The product engineering team creates a check list encompassing functional needs, non-functional need and security needs. The software is tested for vulnerability via manual testing and DAST/VAPT tools. Before procurement, the vendor has to disclose all known vulnerabilities, if it exists along with the plan to fix the same. During integration testing (before the actual procurement) if a vulnerability is discovered, the same is discussed with vendor. The contract with the vendor would explicitly mention that the know and un-known vulnerabilities along with the security needs have to be fixed on a mutually agreeably timelines, based on the severity of the issue.

Open-Source Libraries and Packages

AgilePoint uses trusted and well know libraries such as NuGet and GitHub. NuGet is a package manager designed to enable developers to share reusable code. It is a software-plus-service solution whose client app is free and open-source. GitHub is one of the largest repositories of openly collaborated software projects.

Various checks are done by the developer, including:

- Using packages from a trusted owner.
- Analyzing the source code, both manually and via SAST.
- Running DAST and VAPT tools on the build.
- Verifying the security details of the package/library on the concerned product page.

During each release, if a security patch is available for any of the libraries in use, then the concerned libraries are patched and the same is documented in the product release approval certificate.

Software Development Life Cycle (SDLC)

AgilePoint has a mature and standardized software development process. Security is part of all the aspects, including requirements management, software development, and software package delivery to customers.

Software Development Principles

As stated in its ISO 27001 mandate, the following ten principles are in place as part of product development.

1. Product Engineering's SDLC is based on ISO 27001 security policy, which acts as a founding principle. The corporate security policies are AgilePoint's commitment for physical and information security. The policy identifies security goals such as confidentiality, integrity, availability, accountability, and assurance and these goals guide the procedures, standards and controls used in SDLC design.

2. **Security is an integral part of system design** - AgilePoint understands that it is both difficult and costly to implement security measures properly and successfully after a change request has been implemented. So, it is integrated fully into the system life-cycle process, at each stage. This includes Security assessment before feature development, understanding the resulting security requirements from customer's perspective, code reviews, usage of third-party tools to scan for security issues and security testing post change implementation.

3. **Continuous training** - Developers are mentored and trained to write secure software. Senior team members ensure that developers are adequately trained in the development of secure software before developing the system.

This includes application of engineering disciplines to design, development, configuration control, and integration and unit testing.

4. **Data protection is paramount** - The system is designed to protect both data in transit and data under process. System engineers, architects, and security experts implement security measures to preserve, the integrity, confidentiality, and availability of data.

5. **Third part products for security** - Product team uses industry-best-in-the-class third party systems to ensure security, as oppose to using homegrown tools. This includes, SonarQube for source code vulnerability scanning, Zap scanner for checking run time vulnerability. SonarQube and Zap scanner are the most widely used open source tools in the world.

6. **Use open standards** - The entire product stack is built using open technologies and implement open protocols. These include, but is not limited to, .NET framework, HTML5, CSS, JS, REST APIs, and HTTP/S. This improves interoperability with browsers, devices and external services.

7. **Plan for any class of attack** - Product development is done keeping in mind that the attack can originate from any type of source (internal or external), might require physical or digital access, proximity, malicious code can be injected either during development, packaging, deployment or execution. Please refer to AgilePoint NX Security Guide for more details.

8. **Make system resilient** - Ensure that the business continuity is maintained. Product team has developed disaster recovery procedures to ensure appropriate availability. Please refer to AgilePoint NX Security Guide for more details.

9. **Isolate systems** - The product development, testing and production systems are kept isolated from one another. Dev team checks-in code to TFS and this code goes to build system. Only release team has access to this. Once the build is available, the QA team performs testing on their individual laptops. The dev team cannot access release systems and QA laptops. The QA team cannot access release systems and dev laptops. This is due to physical isolation. The production systems hosted by customers in their data centers cannot be accesses by anyone from AgilePoint. Only customer can access these. The production systems that are hosted by AgilePoint can be accessed only by certain individuals such as the IT team when the system

needs to be upgraded. Customer's prior approval is always obtained before accessing. Please refer to AgilePoint NX Security Guide for more details.

10. **Minimize the system elements to be trusted** - The security measures cover people, operations, and technology. These measures include physical isolation, role-based access controls, dedicated teams for UI, development, product management, release, testing and support, formal processes for each activity, usage of technology components such as GIT, JIRA, ZenDesk, which are popularly used globally for software development.

Product Development

The source code is versioned controlled in GitLab https://about.gitlab.com/. It is secure and cannot be accessed by unauthorized users. The permission for each component is based on roles and teams. For example, the Apple iOS mobile app team cannot modify the source code for components in the AgilePoint NX Portal. Only the team leads and architects have file delete permissions.

The source code undergoes 2 rounds of reviews, apart from review of the design documentation for all big-ticket items. After the reviews, check-in approval is provided to the software developer. The testing team executes test cases as discussed next. Only IT Admin has permission for granting permission to developers. The product development environment is different from product testing environment.

Change Management

AgilePoint uses Atlassian Jira for program and project management. This covers change management, issue tracking, bug tracking, sprint management, release management and task allocation as part of product development lifecycle. All check-ins to GitLab have a corresponding Jira ticket. Change requests that originate from outside of the product team, such as those from customers or prospects, are first logged on to ZenDesk ticketing system either by the product support team or by the customer. A corresponding Jira ticket is created against each accepted ZenDesk ticket to ensure requirements traceability. At the end of the product release cycle, the changes are documented in the official release notes.

Product Testing

Each feature, apart from unit testing by the developer, is tested by independent QC teams. The dedicated QC activities generally consists of:

1. Functional testing
2. Third-Party integration testing
3. Automation testing
4. Accessibility testing covering Section 508 by the United States Access-Board, WCAG by W3.org and EN 301 549 by the ETSI, EU
5. End-to-end use case testing
6. Security testing – DAST
7. Security testing – SAST
8. Performance/Stress testing
9. Mobile security scan
10. Anti-virus and malware scan
11. AI testing
12. Patching third-party libraries to latest stable version

At the end of the security cycle, the person in the role of Chief Security Officer signs-off the security cycle.

Release Management

The product release process is managed by a dedicated release management team. Apart from this team, no one else in the organization has access to the build servers. The release management team is not involved in any other product development or support related activities. Release management releases 4 types of software packages, which are shown in this table.

Name	Purpose	Frequency
Major Release	Major features, bug fixes, and cumulative fixes from previous releases.	Once every 2 years.
Software Update	Major features, bug fixes, and cumulative fixes from previous releases. The difference between Software Update and Major Releases is that usually Software Update do not include new UI components or major UI changes.	Every six to nine months.
Cumulative Update	Bug fixes, security patches, and performance enhancements.	Every 2 to 3 months.
Emergency custom fix	Specific fixes.	As Required.

Software release packages must be approved by the AgilePoint NX Product Department head and CTO. No one else is authorized to make request for a product release. The release management team creates a new branch for making the release, called the release branch, once all the source code has been checked in. The build package is generated only from this branch, which is tamper-proof.

Product Packaging

The virtual environment for the product packaging process is fully isolated and protected. Antivirus software is installed and is running during packaging. The packaging is done on an access restricted AWS cloud environment, managed by the dedicated release management team. The build output is made available through a secure document transfer server. The secure storage allows users to only download the package. The build package (generated from the build output), is digitally signed and is hosted via the AgilePoint Product Download Manager.

The release history is version controlled. Traceability is maintained. For apps, the build team uploads the apps to the respective app stores, as shown below. The upload is done as per the process provided by the respective app store.

- Apple iTunes store.
- Google Play Store and other Android app stores in China.
- Salesforce AppExchange.
- Microsoft AppSource for SharePoint for Microsoft 365 and the Outlook desktop client plugin.

Virus and Malware Scan

The compiled and packaged software files are scanned by a variety of anti-malware software services before they are made available for customers download. An official disclosure document regarding the findings from our virus scanning activities is available upon request. To date no malware has been ever found in AgilePoint's software. Please read AgilePoint's virus free policy.

Vulnerability Scanning and Penetration Testing

AgilePoint uses vulnerability scanning tools to eliminate any security issues during the security cycle, part of the SDLC testing cycle. The OWASP top 10 and SANS 25 are eliminated during coding phase itself. The runtime check of the security vulnerability is done via the OWASP ZAP (https://www.zaproxy.org/) scanner tool and all issues with high and medium priority are remediated as per AgilePoint policy. The ZAP scanner reports are made available upon request.

Customers Service Management and Engagement

The procedure described below is for security involved in incidences only. For general support procedures please refer to AgilePoint's Governance Guide.

AgilePoint customers service is provided via the Support Portal, which is based on the Zendesk platform. Zendesk's servers are hosted at Tier IV or III+, SSAE-16, PCI DSS, or ISO 27001 compliant facilities. All information exchanged between AgilePoint and customers during the resolution of customers issue is through the Support Portal. To know more, please click here https://www.zendesk.com/in/trust-center/.

Customer Queries

Customers can securely raise their product queries in Support Portal. The information stored there is secure. Customers cannot view another customer's queries and information. Support team does not circulate information of customers. Communication is done via Support Portal, as per the support agreement.

Incident Management and Reporting

AgilePoint’s incident response plan is defined in its incident response policy. The Incident Response Plan provides a well-defined, organized approach for handling any potential threat as well as taking appropriate action when the source of the intrusion or incident at a third party is traced back to the organization. This Plan also identifies and describes the roles and responsibilities of the Incident Response Team (IRT) members. The IRT is responsible for putting the plan into action.

The Incident Response Team provides a quick, effective and orderly response to computer related incidents, such as virus infections, hacker attempts and break-ins, improper disclosure of confidential information to others, system service interruptions, breach of personal information, and other events with serious information security implications. AgilePoint’s Incident Response Team’s mission is to prevent a loss of profits, public confidence or information assets by providing an

immediate, effective and skillful response to any unexpected event involving computer information systems, networks or databases. AgilePoint’s Incident Response Team is authorized to take appropriate steps deemed necessary to contain, mitigate or resolve the incident. The Team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and reporting findings to management and the appropriate authorities as necessary. The Chief Information Security Officer (CISO) coordinates these investigations.

The IRT consists of CISO, IT, SOC Team, Operations team, Legal and heads of business/regions (if needed). AgilePoint's networks and cloud installations are monitored 24x7. Unusual network activity or breach attempts results in the activation of the Incidence Response Team. This team, along with the customer's service operations team, reviews the data and if the attempts have compromised the customer's data, the customer is notified. All incidences are reviewed by the ISMS Compliance Committee to determine if modifications to procedures or technology must be updated.

Product Download and Support Service

The Product Support team creates a download session for customers and shares the download link in the support ticket. The link expires after 24 hrs. Product Support will call only office numbers, not private numbers. It does not make direct calls to personal numbers, unless specifically instructed.

Web Meetings

When the Support team engages with customers on web, calls are not recorded. If screensharing is involved, the team views the environment, as bound by NDA signed between both the parties. Any information acquired is only shared with authorized AgilePoint employees. If there is a need to record a specific scenario (for example, as an input to the development team), prior approval is needed. The recorded information is posted over the secure support ticket. The customer can look at it anytime. Product installations services can be done via web meetings based on the customer's request.

Customer Locations

When AgilePoint consultants go to customers site, they are bound by the customer's IT and security policies. Product installation and upgrades are completed based on access granted by the customer, and they are carried out in the presence of a customer representative. At the customer's site, if there is a need to enter a specific credential into the system, the customer types in credentials. AgilePoint's consultant will never ask for this information.

Customer Data Protection

AgilePoint defines 2 types of customers data:

- **Customer's information** – Information about the customer pertains to agreed services, invoices, and contact information. This information is encrypted, with access limited to only those who need the same in order to perform their authorized work. Customer information is never shared, sold, or loaned to third parties.
- **Customer's data** – Data gets securely accumulated on the customer's tenant, during the day-to-day operations. When a customer hires AgilePoint Professional Services, access to the relevant data is limited to the authorized engineers. All accesses use a specific account created to the customer's AgilePoint NX instance and the access is terminated when the work is complete.

AgilePoint does not use the customer's production data in development, testing environment, or for product training purpose.

AgilePoint Employee Access to Customer Data

AgilePoint employees do not have access to the customer's data. If a need arises to debug an AgilePoint NX instance, a request is sent to the customer's tenant admin

to collect logs and upload to a secure location. The link to access the logs is then provided by the tenant admin to a designated support personnel, via a Support ticket. The credentials that are used for product development and testing cannot be used for logging into any production environment.

Employees Handling Confidential Information

Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secured in their work area at the end of the day or when they are away from their work area. Computers get auto-locked after five minutes of inactivity. All proprietary or confidential information are removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday. The file cabinets are always closed and locked, when not in use. Employees ensure that the printouts containing proprietary or confidential information are immediately removed from the printer. These documents are shredded in the official shredder bins. All portable computing devices such as laptops and tablets are kept locked inside of the office. Official tablets and cell phones have lock screens and requiring authentication (passcode or biometric).

Handling a Security Breach

Handling of a security breach is discussed from both customer's perspective and from AgilePoint's perspective. If identity-related information gets compromised from the customer's side, customers are advised to immediately contact AgilePoint Customer Support team. The team will rapidly investigate, neutralize the threat and resolve the issue based on the situation.

If AgilePoint's system were to be compromised, AgilePoint would activate its Incident Reporting Process and Procedures. Some highlights from the plan are:

- Initiate the Security Response Team.
- The Chief Information Security Officer (CISO) will notify the proper authorities.

- The Security Team would notify the affected customers of the breach.
- Work with customers to restore the system. If required, the existing Virtual Machines can be permanently deleted and new VMs can be instantiated using the database backup.
- Perform a root cause analysis to determine why the breach took place in the first place. Based on this, AgilePoint will ensure that the breach will not take place in future.
- Compile all the details on the threat into an Incident Response Report.

To date, AgilePoint's cloud installations have never been compromised.

Secure Document Management System

AgilePoint stores all its confidential information in AgilePoint's Document Management System (DMS). Examples of confidential information include the customer's documentation, proposals, RFPs, RFQs, RFIs, and other documents from customers or pursuits. A definition of confidential information and how it is to be handled are set forth in AgilePoint's Confidential Information Policy. Access to the documents in the DMS are restricted to those with a must access said documents. Non AgilePoint employees do not have access to the DMS.

License Key

Customers can request a license key by contacting the Customer Support team. The license key is tied to the serial number of the hard disk drive. For installation on a VM, the key is tied to the serial number of the virtual disk or the domain name of the customer. This ensures that if someone steals the key from the customer's site, the product activation will fail on a different hard disk or virtual disk. Customers must activate the license through a secure link. Some organizations have policies that prevent software from contacting anything outside the firewall. In

this scenario an offline method to validate the license key can be provided. This same policy is also applicable at the time of license renewal.

Data at Rest

Any third-party system's credentials that are stored in the NX database as part of connection strings, is encrypted using Rijndael algorithm and can only be resolved by AgilePoint Server.

In AgilePoint-hosted cloud environments, we provide encryption of data at rest using disk level encryption of data. For, AgilePoint-hosted private cloud environments, we provide an additional add-on feature of requesting database level encryption using the SQL Server 2019 and later encryption feature, which uses Transparent Data Encryption (TDE).

Data in Transit

All the data transfer in AgilePoint hosted cloud environments are encrypted by TLS 1.2 encryption cipher.

Community

The general public can access AgilePoint's public forum on our Support Portal. Content can be posted only by registered users. AgilePoint's terms and conditions prohibit the posting of sensitive information or identifiable information such as email IDs, mobile numbers, or similar information. The Community Forums are monitored and moderated by an AgilePoint employees.

Privacy

AgilePoint values your privacy when you provide certain personal information to the Company and is committed to ensuring that your privacy is protected. AgilePoint's Privacy Policy summarizes and governs what personal information we may collect by which you can be identified when using this website, and how we might use this information. This policy also describes other important topics relating to information privacy.

AgilePoint has separate Privacy Policies for its website, AgilePoint NX Platform, and its Mobile App. The policies are available online on the AgilePoint website.

- Privacy Policy (Website)
- Platform Privacy Policy
- Mobile App Privacy Policy
- GDPR Policy Statement

Data Retention and Customers Offboarding

If customers decide to part ways with AgilePoint, AgilePoint does not retain any customer data. Typically, the data is immediately deleted based on customers request but if customers wish to retain data, it can be done for a maximum of 90 days before it is permanently deleted. If customers were to request for their data (process models, database, etc.) the same can be arranged. For OnDemand (public cloud) hosting, customers tenants are unrecoverable and permanently deleted. For Dedicated Cloud hosting, AgilePoint will permanently close the Private Cloud and the VMs in the Private Cloud will be unrecoverable and permanently deleted. In either case, the entire backup of the customer's data will also be permanently erased. The offboarding process ensures that the customer's data is irrecoverably pruned. AgilePoint does not have access to any of the digital keys.

AgilePoint's Partners

AgilePoint's partners are held to the same security, privacy, and data retention policies that AgilePoint adheres to.

Vendor Management

AgilePoint runs a vendor management program to ensure that appropriate security and privacy controls are in place. The program includes inventorying, tracking, and reviewing the security programs of the vendors who work for us. All vendors receive an annual "Vendor Security Survey" report from AgilePoint. The surveys are required and subject to audit by AgilePoint. This is reviewed by the CISO to verify compliance. Appropriate safeguards are assessed relative to the service being provided and the type of data being exchanged.

External Contractors

External contractors are limited to only those AgilePoint systems that are required in the performance of their contract. If they receive an AgilePoint email, the external contractor must follow the guidelines detailed in AgilePoint's Information Security Policy. External contractors do not ever have access to AgilePoint's customer data.

Employee On-Boarding and Exit

As a condition for employment, prospective employees must submit to:

- A 50-state criminal background check
- Verification of industry references

- A credit inquiry
- Validation of higher education attendance

All employees sign the NDAs as part of their on-boarding process and undergo security training. Employee onboarding in offices in other regions adhere to the concerned government regulations.

Employee separation process is governed by the strict employee exit policy which is designed to enhance business continuity and minimize the potential for fraud, deception, and security lapses.

Security at Product Level

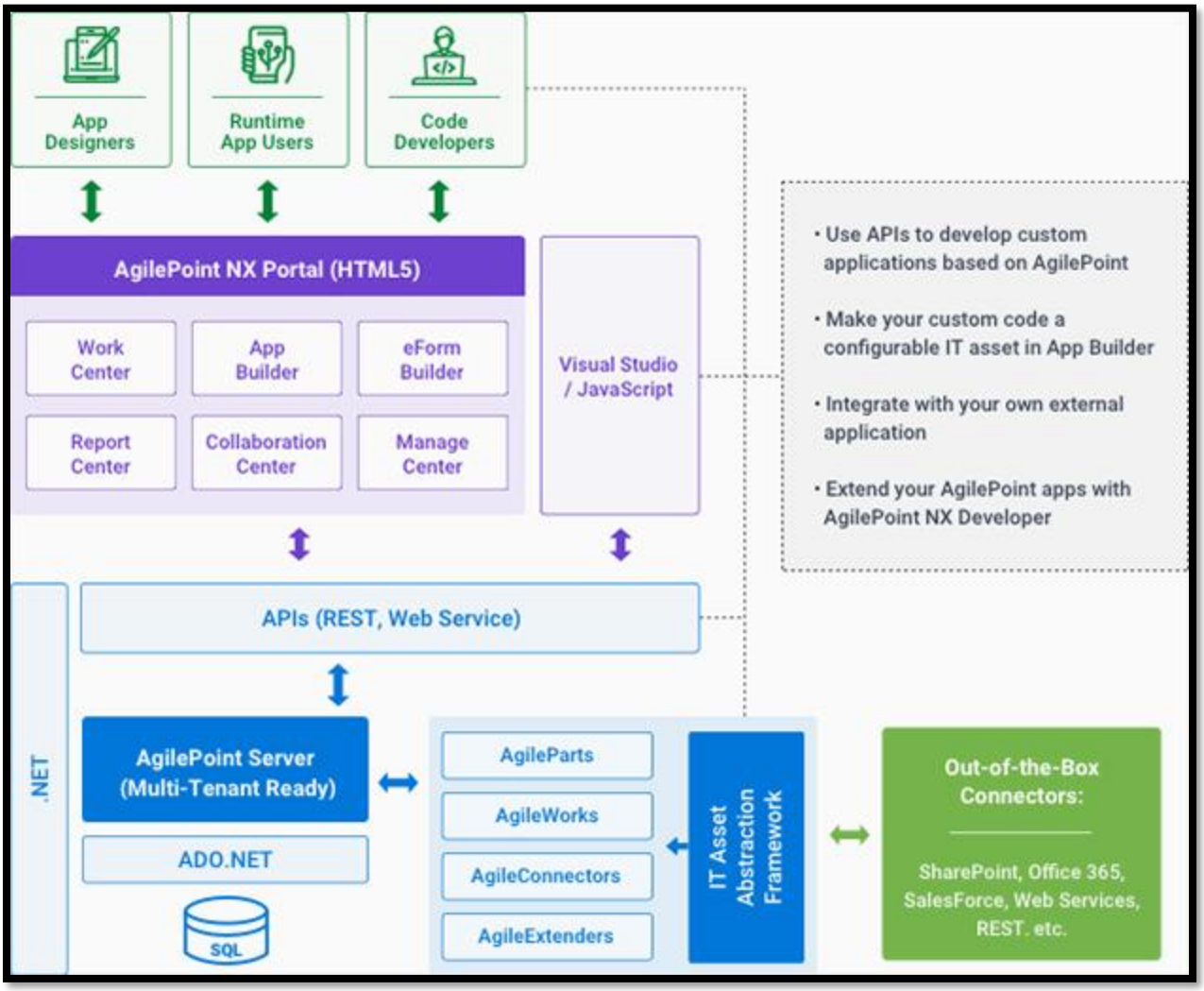
Security is built into every phase of the product development lifecycle and into every feature of the product.

Architecture of the Product

Secure Architecture Approach

The architecture of AgilePoint's security framework is built upon several key pillars that ensure robust, scalable, and efficient operations while maintaining strict security and compliance. Drawing inspiration from industry best practices, the design emphasizes Security and Data Integrity, where stringent access controls, encryption, and secure communication protocols protect sensitive data at all times. Reliability and Resilience are achieved through continuous monitoring, fault-tolerant designs, and comprehensive audit logging, ensuring that the system can gracefully handle failures and recover quickly. Performance Efficiency is embedded in the architecture by optimizing processes for speed and resource utilization, ensuring rapid response times without compromising security. Finally, Operational Excellence is maintained through a clear governance framework that includes automated monitoring, regular assessments, and ongoing improvements, allowing administrators and privileged users to maintain strict oversight and control over process flows. This multi-faceted approach creates a secure, agile, and efficient environment that is capable of adapting to evolving business needs and threat landscapes.

Architecture of AgilePoint NX



The AgilePoint NX Portal is a software component that displays other AgilePoint NX components, such as Process Builder and Manage Center. The Portal enables authentication to AgilePoint NX and provides the overall navigation. AgilePoint NX Developer is a AgilePoint NX software component that lets users create custom assets, such as activities, AgileConnectors and AgilePoint NX web applications. AgilePoint NX Developer is an extension for Microsoft Visual Studio. WCF is a Microsoft framework for building service-oriented applications.

AgilePoint NX offers a full set of REST APIs, and can integrate with RESTful services directly from an application with out-of-the-box activities. AgilePoint Server is a software engine that runs AgilePoint NX apps behind the scenes. AgilePoint NX uses

several databases to store data. For more information on this, please refer to System Requirements for AgilePoint Server in the product documentation site. The Abstraction Extension Framework lets one extend the AgilePoint NX.

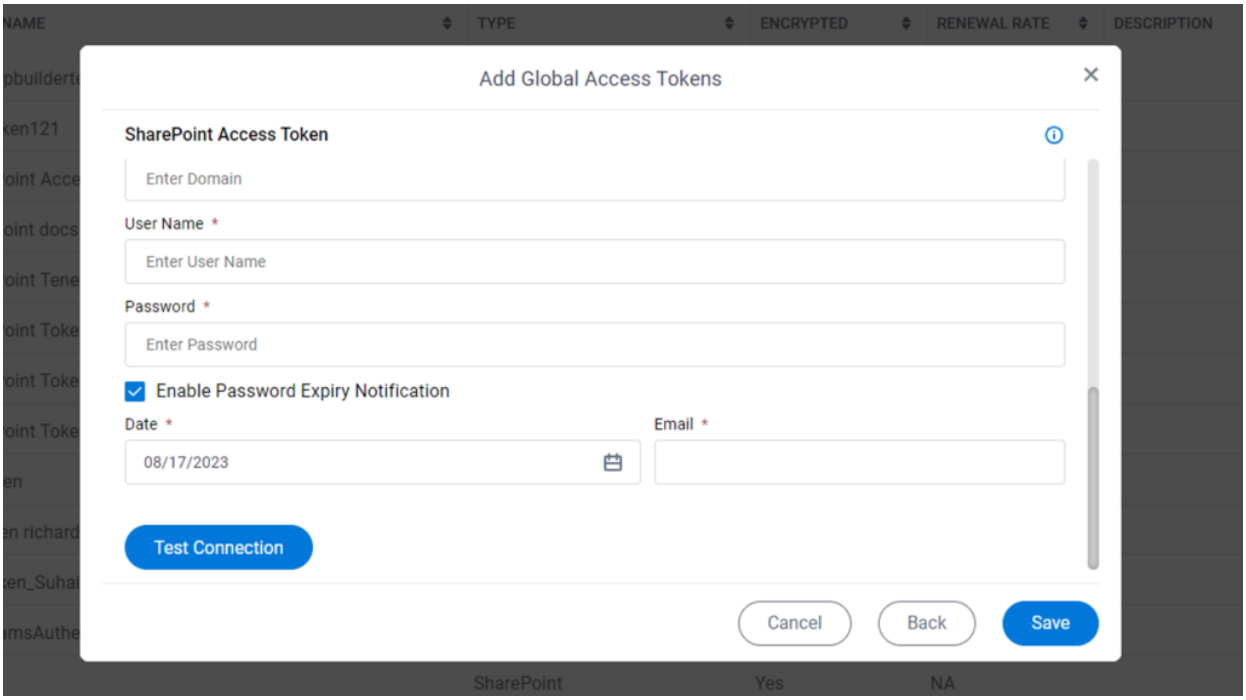
Access Tokens

An access token is a secure object that stores an endpoint (usually a URL) and authentication credentials to connect to a service or technology. Once an access token is created, application designers can simply select and reuse it, rather than entering the credentials each time they are needed. The administrator can configure the access rights of a token at the global level or at app level. Global level access tokens can still be restricted for certain roles and users. For more information about the security for access token credentials, refer to the section, External System Level Identity Management.

As an enhanced security measure, when the user wants to edit the access token, they are prompted to revalidate the access token password or secret key to ensure the user who is editing the token is an authorized user.

Majority of the third-party systems support OAuth2 based authentication and implement auto-refresh of the token enabled as per the OAuth2 specification, which makes sure tokens are auto recycled at regular interval without any human intervention. A handful of systems still work using basic authentication (username and password). Token expiry would prevent the exchange of information between AgilePoint NX apps and the third-party system, resulting in app downtime. AgilePoint NX comes with a built-in alerting mechanism. Once password expiration date and email has been configured, AgilePoint NX system will start sending a reminder notification 15 days before the password expiration date to the email address configured and copy will be sent to system admin or tenant administrator.

Configure Token Expiry Notification



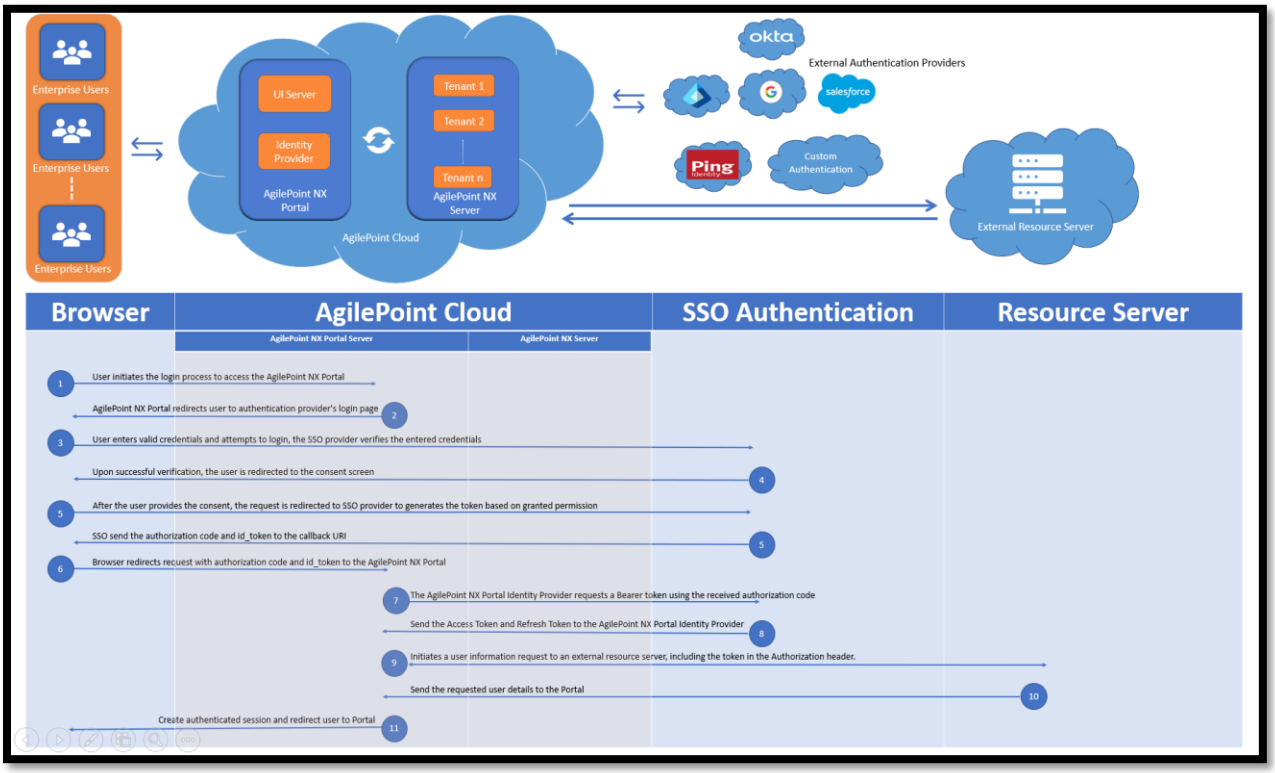
Identity Management - User Level

AgilePoint NX supports a concept of "Bring Your Own Identity," where customers can bring their existing identity providers of their choice to authenticate a user. AgilePoint NX performs user authorization to determine the access rights of the user post authentication. AgilePoint NX does not store any end user passwords in its databases.

Third-party authentication providers help clients maintain user profile and password compliance through industry standard identity providers while also meeting the Single Sign-On (SSO) needs of their enterprises. When a user signs in to the AgilePoint NX Portal using third-party credentials, the request is directed to the associated authentication provider portal. The user follows the third-party sign in process, which approves access, and then redirects to the NX Portal with corresponding OAuth 2.0 access token. Every authenticated user is registered as an AgilePoint user and gets a basic profile in AgilePoint, even if they use an external

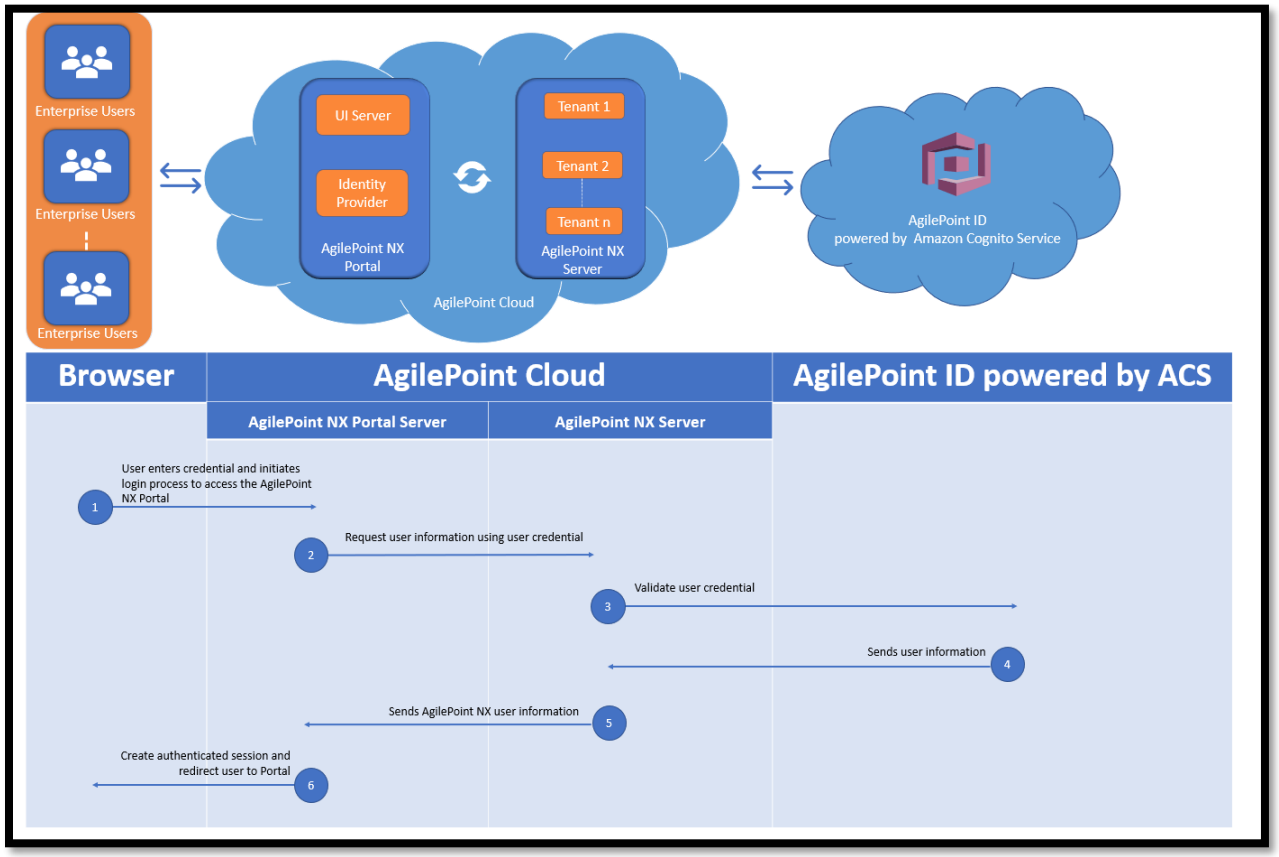
authentication provider. AgilePoint user profile controls operations such as task assignments and emails.

Authentication in AgilePoint NX Using Third-Party Authentication Providers



Some AgilePoint customers opt for an AgilePoint ID in which the users are maintained by an AgilePoint managed AWS Cognito service. The AgilePoint ID based authentication is available only for OnDemand (public cloud) deployments.

AgilePoint ID Provided by AgilePoint in Public Cloud



Authentication Name	Purpose	Supported In	Authentication Type/Protocol
AgilePoint ID	Enables native AgilePoint authentication.	AgilePoint NX OnDemand (Multi-Tenant Public Cloud)	Basic*
Active Directory	Enables AgilePoint authentication using Active Directory.	AgilePoint NX On Premises AgilePoint NX Private Cloud - Dedicated Cloud Hosted by AgilePoint	Basic*

Authentication Name	Purpose	Supported In	Authentication Type/Protocol
ADFS	Enables ADFS account authentication.	AgilePoint NX On Premises AgilePoint NX Private Cloud - Dedicated Cloud Hosted by AgilePoint	OAuth 2.0
Salesforce	Enables Salesforce account authentication.	AgilePoint NX OnDemand (Multi-Tenant Public Cloud) AgilePoint NX On Premises AgilePoint NX Private Cloud - Dedicated Cloud Hosted by AgilePoint	OpenID Connect
Microsoft Azure Active Directory	Enables Microsoft Azure Active Directory account authentication.	AgilePoint NX OnDemand (Multi-Tenant Public Cloud) AgilePoint NX OnPremises AgilePoint NX Private Cloud - Dedicated Cloud Hosted by AgilePoint	OpenID Connect
Google Workspace	Enables Google Workspace authentication.	AgilePoint NX OnDemand (Multi-Tenant Public Cloud) ilePoint NX OnPremises AgilePoint NX Private Cloud - Dedicated Cloud Hosted by AgilePoint	OAuth 2.0

Authentication Name	Purpose	Supported In	Authentication Type/Protocol
Okta	Enables Okta account authentication.	AgilePoint NX OnPremises AgilePoint NX Private Cloud - Dedicated Cloud Hosted by AgilePoint	OpenID Connect
IdentityServer4	Enables Identity Server4 account authentication.	AgilePoint NX OnPremises AgilePoint NX Private Cloud - Dedicated Cloud Hosted by AgilePoint	OpenID Connect
CA SiteMinder	Enables SiteMinder account authentication.	AgilePoint NX OnPremises AgilePoint NX Private Cloud - Dedicated Cloud Hosted by AgilePoint	None**
PingFederate	For identity management, SSO and API security.	AgilePoint NX OnPremises AgilePoint NX Private Cloud - Dedicated Cloud Hosted by AgilePoint	OpenID Connect
Amazon Cognito	Enables Amazon Cognito account authentication.	AgilePoint NX OnPremises AgilePoint NX Private Cloud - Dedicated Cloud Hosted by AgilePoint	OpenID Connect

*Even though it is using basic authentication, we have a special mechanism of securing the authorization header by passing a secured JWT token instead of passing user credentials as Base64 format.

**SiteMinder provides a custom mechanism where once user authenticates against SiteMinder, an access ticket is issued which is automatically passed along with any

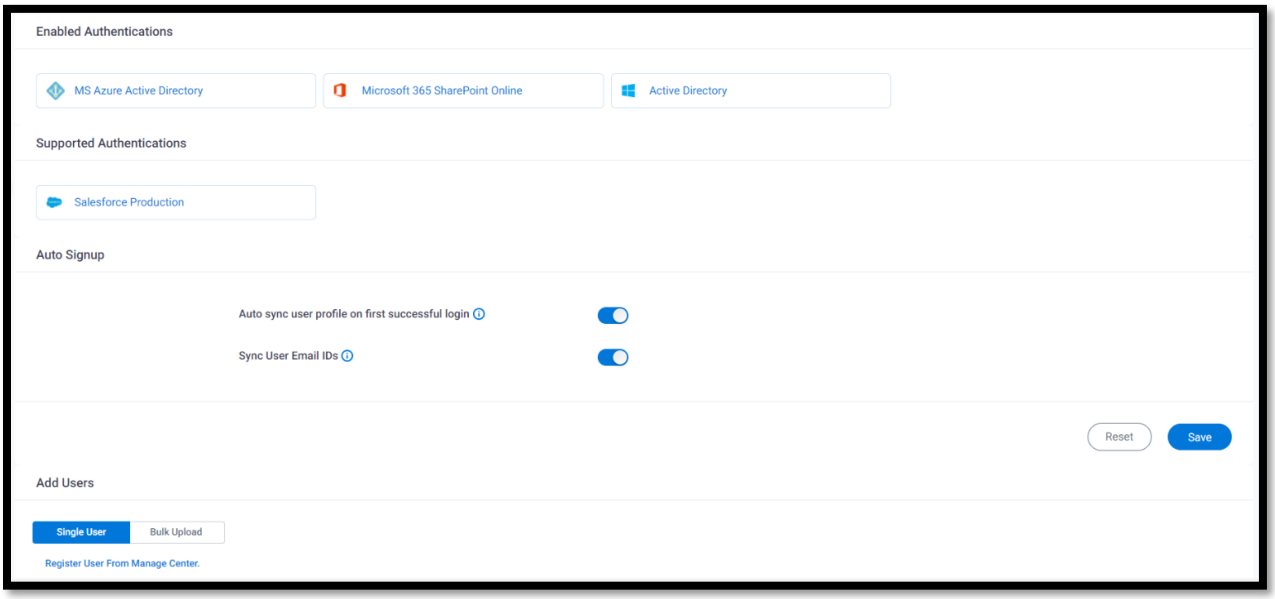
request made from that browser. This security is handled by SiteMinder automatically.

Information needed (client ID and secrets) for external authentication such as Microsoft Azure Active Directory, Salesforce, etc. are stored in web.yaml. The access to the file is limited only to the AgilePoint System Account, which manages the AgilePoint Server instance.

Multiple Authentication Providers

AgilePoint NX supports onboarding multiple authentication providers in parallel, on the same tenant. Business scenarios such as merger of enterprises, acquisition of a firm or onboarding teams from a different geographic region are the typical reasons why customers end up with multiple authentication providers. Based on the license agreement, AgilePoint will enable two or more authentication providers in modes of deployment.

Authentication Providers in AgilePoint NX

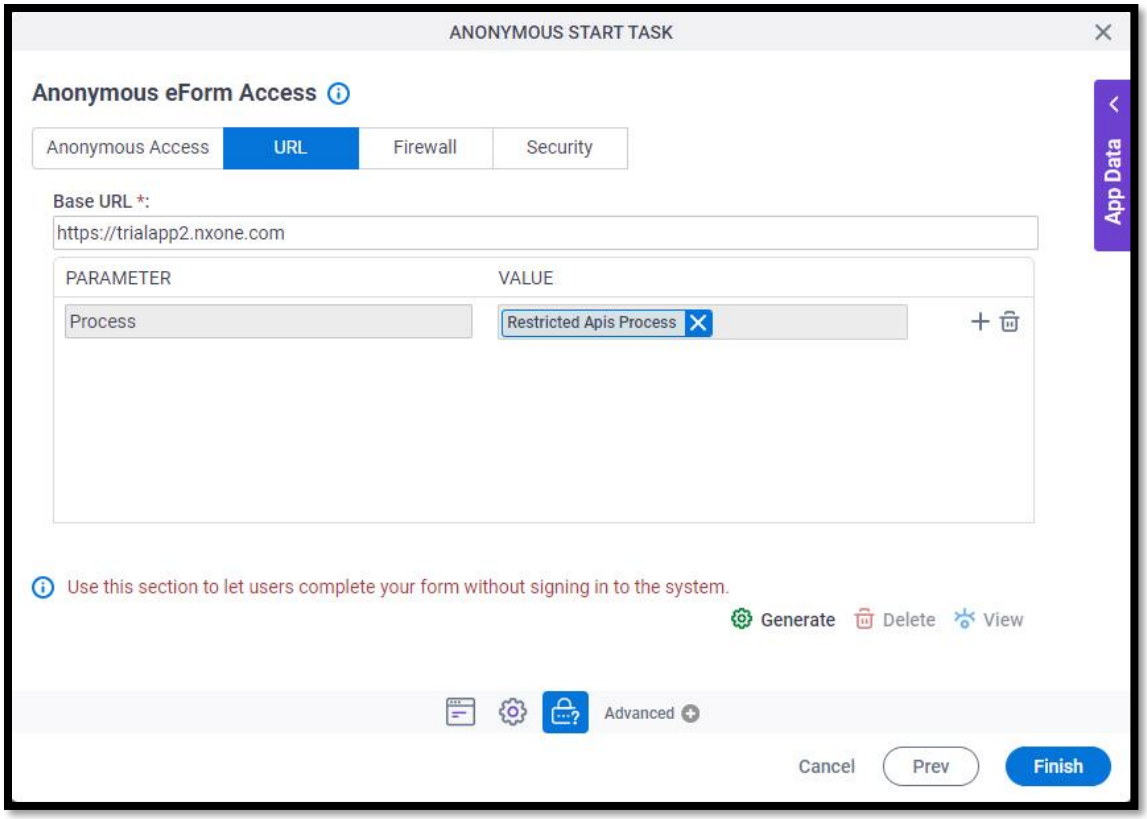


Anonymous User for Electronic Forms

AgilePoint NX supports anonymous, or unauthenticated, users for public-facing apps where the runtime app user is not registered in the AgilePoint system and can access the app without authenticating to the system. The link for an anonymous page carries an encrypted access code to securely give access to a public facing app. This link, which contains an encrypted access code, is unique to each form. Therefore, a runtime app user can only access the specified form using the link and cannot cross the application security boundary. The anonymous form cannot be accessed by a user who has login.

The following security features are made available to the anonymous form designer.

- **Token** – Depending on the business needs, a single app might require one or more, different access tokens. The designer can select a different local or global access token for each anonymous form.
- **URL** – This configuration allows developer to specify AgilePoint NX Portal instance URL. One can also specify a different proxy or external URL to expose the form externally.



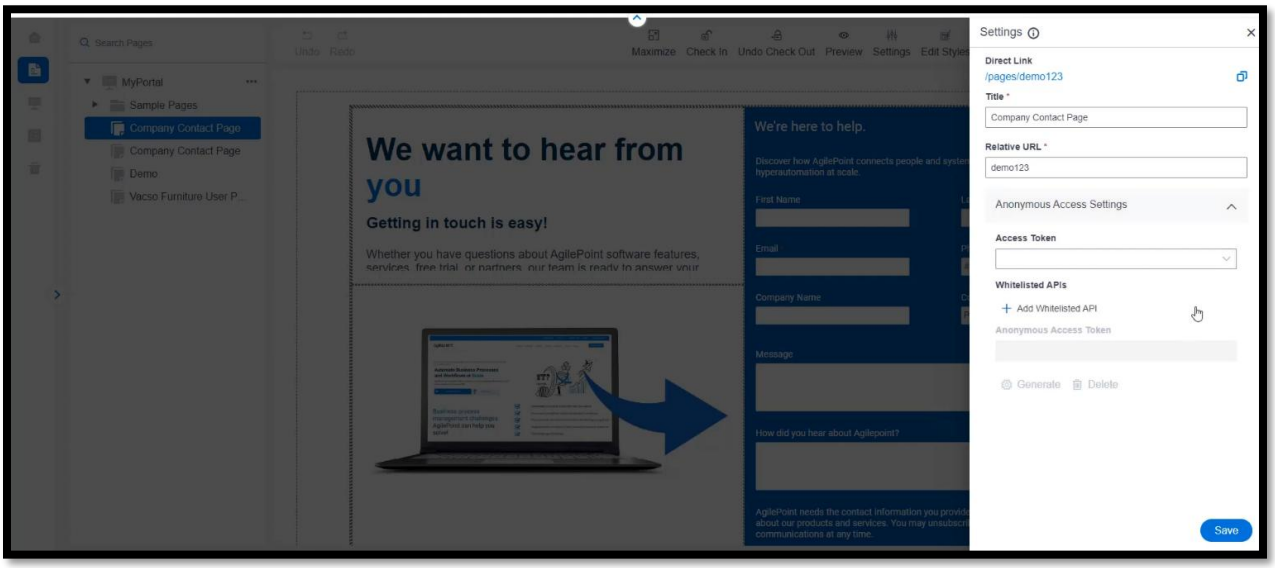
- **IP filtering** – Allows the enterprise to specify a list of IP address ranges (from IP and to IP). Access to the anonymous from outside of the whitelisted IP addresses is blocked.
- **Restrict APIs** – Prevents unauthorized access by allowing only APIs from the whitelist to make API calls to or from the anonymous form. If an API is not on the whitelist and a call is attempted against the anonymous form, an error message is thrown.
- **Restrict System Tokens** – This setting allows the developer to block the form developer from using a token which he/she is not supposed to use.
- **Time Out** – The anonymous form will expire after the specified timeout.
- **Two Factor Authentication** – AgilePoint NX Anonymous forms supports 2FA. A 6-digit access code is emailed to the targeted user when he/she clicks the task form link. The user must enter that 6-digit code before he/she can open the task form.

Anonymous Users for Web Pages

AgilePoint NX supports anonymous web pages which has led to adoption of use cases such as event registration page, webinar pages, customer feedback pages and more, which are backed by eForms, integration and workflows. The key security features are as follows:

- By default, this feature is disabled. It has to be explicitly enabled.
- For an eForm to be embedded, the same has to be anonymous. Regular eForms cannot be embedded in the anonymous pages.
- Only the APIs that are explicitly whitelisted can be consumed when the page is viewed in anonymous mode. So, if the page needs to access an AgilePoint API via a custom JavaScript to fetch data from a Data Entity or call a Server API, these have to be explicitly whitelisted.

Anonymous Pages



Identity Management - System Level

This section describes system level identity management at 2 levels:

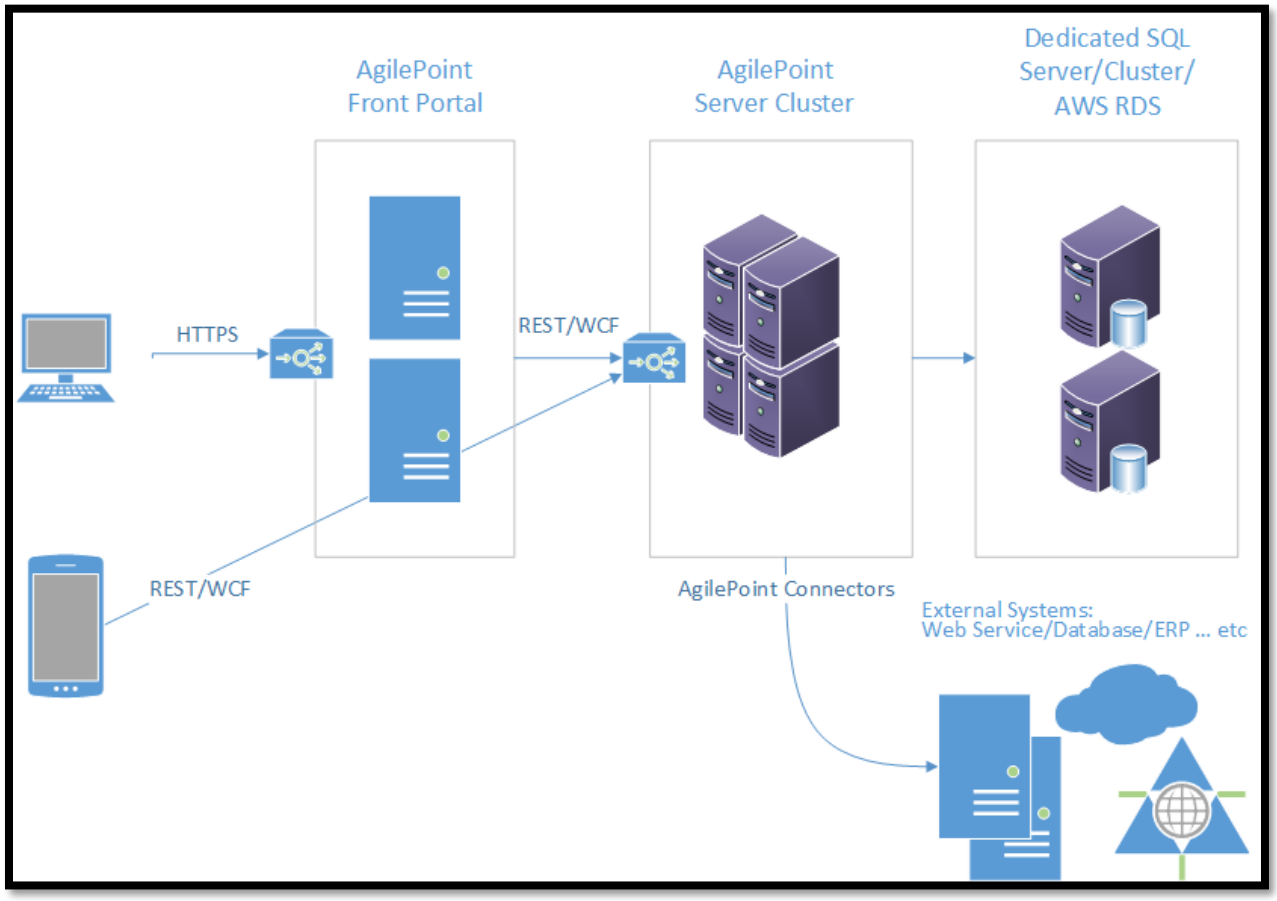
- **Internal** – Identity management between the internal modules of AgilePoint NX.
- **External** – Identity management between AgilePoint NX and external systems.

Layers - 3 Tier View

An AgilePoint NX instance can be logically viewed to be composed of 3 layers:

- Front End App Server (Presentation Layer or the Business Layer) – This consists of the AgilePoint Portal and its components. Runtime app users can access the runtime app (sometimes called a business application) here.
- AgilePoint Servers (Business Logic Layer) – This is the heart of the NX. The workflow engine and the form engine sit here. Communication with the external systems happen from this layer.
- Database Server (Data Layer) – In most small- to medium-scale AgilePoint implementations, the database resides on a database server that serves other apps. However, this can be a dedicated server, and it often is in enterprise implementations. Active/passive failover is recommended.

Logical View of AgilePoint NX Architecture



Each layer can be independently installed on a different physical or virtual machine and managed separately.

Internal System Level Identity Management

Communication between an AgilePoint Sever and an AgilePoint database is a server-to-server call. AgilePoint supports SQL authentication and Windows authentication. The sign-in credentials are stored in a config file which is only accessible to the AgilePoint System Account and is encrypted. Communication between the AgilePoint Server and the AgilePoint NX Portal is also a server-to-server call, which takes place only during authentication of a user. The service account credentials used to call the authentication API are stored in config file in

encrypted format and this is not an end user credential. In order to send and receive emails, the AgilePoint Server connects to an SMTP server using Microsoft Exchange, IMAP, POP3, Exchange Web Services, and Microsoft 365.

The AgilePoint NX Portal database consists of a master database and a tenant database. All tenant-based connection strings, which are needed to communicate between the NX Portal web application and the NX Portal database, are stored securely in the master database and are not accessible to anyone except the AgilePoint System Account.

The AgilePoint Server authorizes the calls of its services to run processes and execute apps using the authorization header passed from the user's browser to AgilePoint Server. AgilePoint supports both basic and bearer tokens as part of authentication headers. The credentials in the config files are encrypted using the Rijndael algorithm. We highly recommend using JWT tokens instead of basic authentication from a security perspective. AgilePoint supports tokens even for Active Directory authentication.

External System Level Identity Management

Information exchanges between AgilePoint systems and external systems are secured using access tokens.

The credentials listed in the table below are stored in encrypted format in an AgilePoint NX database and only the AgilePoint Server can read and decrypt it. These are not transmitted to end user browsers nor are they exposed via any API.

Integration Name	Type of Service	Authentication Details	Encrypted
Microsoft SQL Server	Database	Basic/Windows	Yes
.NET Proxy	Web services	Basic/Anonymous	Yes

Integration Name	Type of Service	Authentication Details	Encrypted
Active Directory	Active Directory Service	Basic/JSON Web Token (JWT)	Yes
Adobe Sign	HTTPS	OAuth 2.0	Yes
AgilePoint NX	HTTP/HTTPS	Basic	Yes
AWS	HTTPS	OAuth 2.0	Yes
Anonymous Form	HTTP/HTTPS	Basic	Yes
Microsoft Azure Bot Service	HTTPS	OAuth 2.0	Yes
Bing Maps	HTTP	API Key	Yes
Bitly	HTTPS	OAuth 2.0	Yes
Box	HTTPS	OAuth 2.0	Yes
Blue Prism	HTTP/HTTPS	Windows	Yes
External Database	Database	Basic/Windows	Yes
DocuSign	HTTP	Basic + API Key	Yes
Dropbox	HTTPS	OAuth 2.0	Yes
Exchange Server	HTTPS	Basic/OAuth 2.0	Yes
FTP	HTTP	Basic	Yes
Facebook	HTTPS	OAuth 2.0	Yes
Google Maps	HTTPS	API Key	Yes
Google Drive	HTTPS	OAuth 2.0	Yes
LinkedIn	HTTPS	OAuth 2.0	Yes

Integration Name	Type of Service	Authentication Details	Encrypted
Microsoft Dynamics 365	HTTPS	Basic	Yes
Microsoft Azure IoT	HTTPS	OAuth 2.0	Yes
Microsoft Azure Machine Learning	HTTPS	API Key	Yes
Microsoft Cognitive Services	HTTPS	API Key	Yes
Microsoft Teams	HTTPS	OAuth 2.0	Yes
MongoDB	Database	Basic	Yes
NetSuite	HTTP/HTTPS	Basic/ OAuth 2.0	Yes
OData Services	HTTP/HTTPS	Basic	Yes
Microsoft 365 (Non-SharePoint)	HTTPS	OAuth 2.0	Yes
OneDrive	HTTPS	OAuth 2.0	Yes
PayPal	HTTPS	OAuth 2.0	Yes
Microsoft Power BI	HTTPS	OAuth 2.0	Yes
Rest Services	HTTP/HTTPS	Basic/OAuth 2.0	Yes
Redox	HTTPS	OAuth 2.0	Yes
SAP	HTTP	Basic	Yes
SFTP	HTTP/HTTPS	Basic	Yes
Salesforce	HTTPS	OAuth 2.0	Yes
Sertifi	HTTPS	API Key	Yes

Integration Name	Type of Service	Authentication Details	Encrypted
SharePoint	HTTPS	Basic/Forms/OAuth 2.0/ADFS	Yes
Skype for Business	HTTPS	Basic	Yes
Slack	HTTPS	OAuth 2.0	Yes
Trello	HTTPS	Key and Token	Yes
Twilio	HTTPS	Account SID and Auth Token	Yes
UiPath	HTTPS	Basic	Yes
WCF Services	HTTP/HTTPS	Basic/Anonymous	Yes
SOAP	HTTP	Basic/Anonymous	Yes
Microsoft Azure Active Directory	HTTPS	OAuth 2.0	Yes
WordPress	HTTP/HTTPS	Basic	Yes
Yammer	HTTPS	OAuth 2.0	Yes
Zendesk	HTTPS	Basic	Yes
Zoho CRM	HTTPS	Basic	Yes
Zoom	HTTPS	OAuth 2.0	Yes
Ethereum	HTTPS	Private Key	Yes
Jira	HTTPS	OAuth 2.0	Yes
Oracle DB	Database	Basic	Yes
ServiceNow	HTTPS	OAuth 2.0	Yes

Integration Name	Type of Service	Authentication Details	Encrypted
PowerAutomate	HTTPS	OAuth 2.0	Yes
MS Dataverse	HTTPS	OAuth 2.0	Yes
Generic OAuth 2 Token	HTTPS	OAuth 2.0	Yes
AWS Cognito Authentication	HTTPS	OIDC	Yes
Teams	HTTPS	OAuth 2.0	Yes
Snowflake	HTTPS	OAuth 2.0	Yes
HubSpot CRM	HTTPS	OAuth 2.0	Yes
PostgreSQL	Database	Basic/Windows	Yes
GitHub	HTTPS	OAuth 2.0	Yes
Google AI	HTTPS	OAuth 2.0	Yes
Mailchimp	HTTPS	OAuth 2.0	Yes
Okta	HTTPS	OAuth 2.0	Yes
SendGrid	HTTPS	API Key	Yes
Asana	HTTPS	OAuth 2.0	Yes
Google Sheets	HTTPS	OAuth 2.0	Yes
Azure Service Bus	HTTPS	OAuth 2.0/Shared Access Signature	Yes
Amazon SageMaker	HTTPS	Access Key/ IAM Role	Yes
Abbyy Vantage	HTTPS	OAuth 2.0	Yes

Integration Name	Type of Service	Authentication Details	Encrypted
AWS Redshift	HTTPS	OAuth 2.0	Yes
AWS Lambda	HTTPS	OAuth 2.0	Yes
Azure Functions	HTTPS	OAuth 2.0	Yes
gRPC	HTTP/HTTPS	Basic/OAuth 2.0	Yes
Stripe	HTTPS	API Key	Yes
OpenAI	HTTPS	API Key	Yes
AWS S3	HTTPS	Access Key/IAM Role	Yes
Elastic Search	HTTP/HTTPS	API Key/Basic/Anonymous	Yes
Azure Blob Storage	HTTPS	OAuth 2.0/Shared Access Signature/Access Key	Yes
Kafka	HTTP/HTTPS	Basic/Anonymous	Yes
Google Translation	HTTPS	OAuth 2.0/Service Account	Yes
Amazon SNS	HTTPS	Access key/ IAM Role	Yes
Google Cloud Storage	HTTPS	OAuth 2.0	Yes
MS Azure Machine Learning	HTTPS	API Key	Yes
Microsoft Planner	HTTPS	OAuth 2.0	Yes
Mindee	HTTPS	API Key	Yes
Monday.com	HTTPS	API Key	Yes

Integration Name	Type of Service	Authentication Details	Encrypted
NVIDIA NIM	HTTPS	API Key	Yes
Neo4j	HTTPS	Basic	Yes

AgilePoint's REST APIs

AgilePoint Server enables third-party software integrations by exposing RESTful APIs. AgilePoint provides 3 categories of RESTful APIs:

- Tenant administration
- Managing data that is stored in NX
- Making calls to the workflow engine in AgilePoint Server.

Third party apps must use encrypted access tokens in order to integrate with AgilePoint NX. We highly recommend using OAuth 2.0 authentication or JWT Token based authentication instead of Basic authentication. For your data security, AgilePoint strongly recommends using SSL (https) for all communication with the AgilePoint REST API. To know more about the APIs, please refer to the REST API documentation.

Identity Management - SharePoint

AgilePoint NX can be deployed on both to on-premises SharePoint and SharePoint for Microsoft 365.

On-premises SharePoint Identity Management

SharePoint On-Premises stores service account credentials in an encrypted format in the AgilePoint Settings list in SharePoint. On-premises SharePoint authenticates against Active Directory or ADFS. The credentials are encrypted using the Rijndael algorithm.

SharePoint for Microsoft 365 Identity Management

SharePoint for Microsoft 365 integration does not store a service account identity. AgilePoint NX SharePoint for Microsoft 365 app authenticates users and apps against the Microsoft Azure Active Directory.

Administration

AgilePoint NX provides different types of administrators based on the type of deployment.

- OnDemand (public cloud) Deployment has 3 types of administrator roles: AgilePoint System Account, Tenant Administrator, and Administrator.
- AgilePoint-Hosted Dedicated Cloud has 2 administrator roles: AgilePoint System Account and Administrator.

For a complete list of administrator types and their permissions, refer to the following article in the AgilePoint NX documentation:

- Administrator Types

AgilePoint Service Account and System Account

The AgilePoint Service Account is the master, "headless" administrator account for the AgilePoint NX system. When AgilePoint Server is installed, the AgilePoint Service Account is given the same credentials as the AgilePoint System Administrator, which is called the System Account. The System Account is managed by the master, human administrator for the AgilePoint system.

Tenant Administrator

Tenant Administrator is a special role that can only be assigned to one AgilePoint user in a multi-tenant environment. In an NX OnDemand (multi-tenant public cloud), the tenant administrator is the user who signs up for the tenant.

Administrators Role

Administrator is the main administrator role for the AgilePoint NX Portal.

AgilePoint User Management

AgilePoint NX has its own user management system. To access AgilePoint NX, users must be a registered user within the system. Usernames can be in Domain\username format or username@abc.com (UPN) format based on the type of user authentication. Users can be synchronized from Active Directory, Microsoft Azure Active Directory, Salesforce, SharePoint, database, or other sources. As part of the user profile, the details collected are Full Name, User Name, Email Address, Department, Title, Manager, Language, Phone Number, Yammer ID, Chatter ID, and Skype for Business ID, if applicable.

For complete documentation about creating and managing users in AgilePoint NX, refer to the following articles in the AgilePoint NX documentation:

- Users – How to create and manage users in AgilePoint NX.

- Runtime App Users – A list of end user types in AgilePoint NX and their associated permissions.

AgilePoint Group Management

AgilePoint NX allows you to create a group within a system to assign tasks or send emails to recipients that directly point to a group. Groups must have a group lead. Groups can be synchronized with external LDAP where enterprises create and manage groups according to their security policies.

For complete documentation about creating and managing users in AgilePoint NX, refer to the following articles in the AgilePoint NX documentation:

- Groups – How to create and manage groups in AgilePoint NX.

AgilePoint Role Management

AgilePoint NX has a granular role-based access control system that provides an access control mechanism with more than 200 access rights controlling every action users can perform within AgilePoint. Roles can consist of users or groups. AgilePoint NX depends on external systems for authentication but has its own role-based authorization mechanism.

For complete documentation of the default roles in AgilePoint NX and their access rights, refer to the following articles in the AgilePoint NX documentation:

- Default Roles – A full list of the default roles and their access rights.
- Access Rights – A full list of all available access rights.
- Roles – How to configure roles and access rights.

Access Management

AgilePoint has built an extensive set of controls to facilitate access to meet its customer's security access needs and support their compliance activities. Once a user is authenticated against the user identity store of choice, AgilePoint authorizes the user to determine their permissions within the AgilePoint system. AgilePoint NX provides a very granular and layered permission control system. Enterprises can control access to almost every feature of the AgilePoint Portal and Server. This includes, users, groups, roles, apps, modules, reports, pages, entities, and more.

Role Based Access Controls (RBACs)

The administrator can provide just-in-time access to users or groups based on the need. AgilePoint NX provides granular controls to roles with 100+ platform level permissions. AgilePoint NX allows enterprises to build their own governance model by creating roles based on business needs and set access rights to each role. AgilePoint NX implements detailed rights schemes to access APIs and platform components. The table below shows the access provided to each of the default roles.

For complete documentation of the default roles in AgilePoint NX and their access rights, refer to the following articles in the AgilePoint NX documentation:

- Default Roles – A full list of the default roles and their access rights.
- Access Rights – A full list of all available access rights.
- Roles – How to configure roles and access rights.

Permission Groups

Permission groups allow you to configure targeted access control for specific elements within AgilePoint NX. Permission groups can be configured for apps, entities in Data Entities, and custom pages in Page Builder. When they are configured, permission groups take priority over RBACs for determining access controls.

For complete documentation on permission groups, refer to the following articles in the AgilePoint NX documentation:

- Permission Groups – A complete list of permission groups and their associated permissions.
- Permission Groups, Roles, and Task Participants – Detailed documentation for configuring permission groups. This section also provides documentation on some roles and other types of users that have impacts on permissions when permission groups are enabled. For example, some roles are still applicable, and runtime app users are handled differently for various parts of the AgilePoint NX system.

Analytics Permissions

The AgilePoint NX analytics module stands as a full-fledged BI and reporting product on its own. Permission controls are available across all aspects of the product. Listed below are the granular actions that can be managed by the analytics permission's framework.

For information about Analytics roles and permissions, refer to the following articles in the Analytics documentation:

- Roles Setup
- Permissions Setup

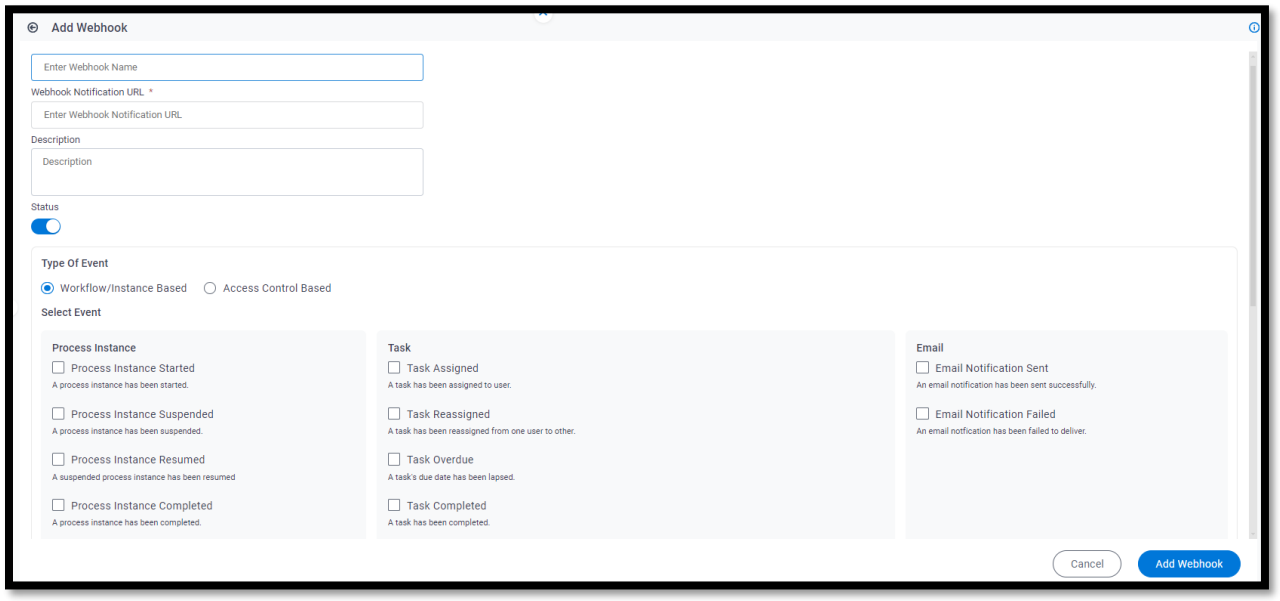
Webhooks

The AgilePoint Server provides event subscription to third-party software by exposing webhooks. AgilePoint provides 6 categories of webhooks:

- Process Instance
- Task
- Email

- User
- Group
- Roles

Webhooks in AgilePoint NX

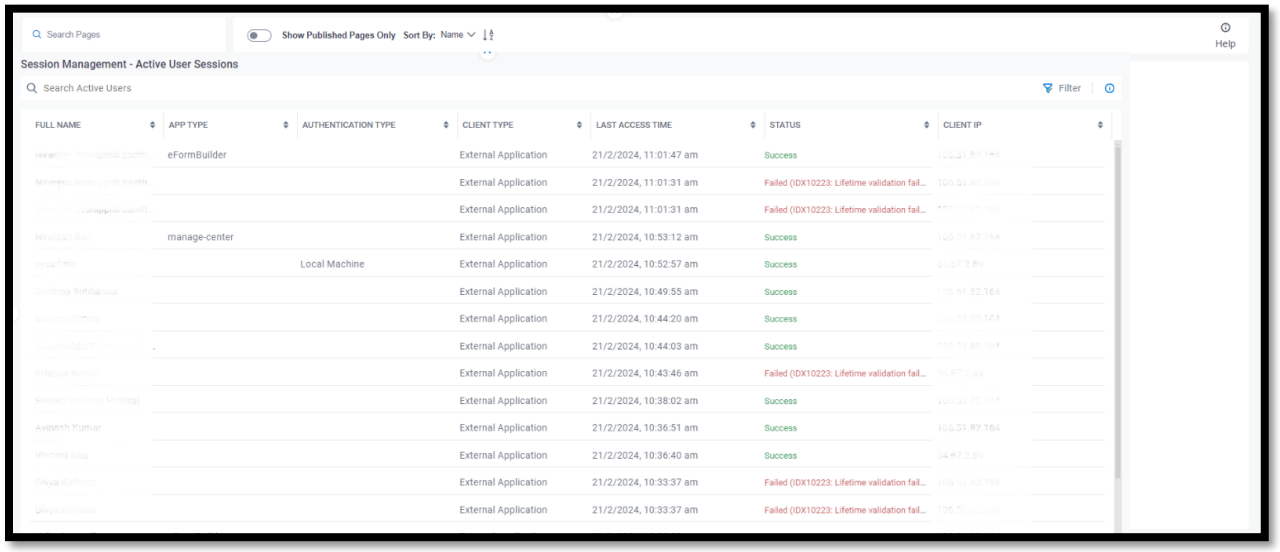


Third-party applications and services must use encrypted access token in order to integrate with AgilePoint NX. For data security, AgilePoint strongly recommends using SSL (https) for all communication with the AgilePoint REST API.

Session Management

Session Management functionality lets the system administrator monitor and protect the concerned AgilePoint NX tenant by reviewing active sessions. A session is established after authentication and the user can work on the system as long as the session is active. The admin can view live details of the calls, both incoming and outgoing. If a call were to fail, the admin can view the details to figure out the cause.

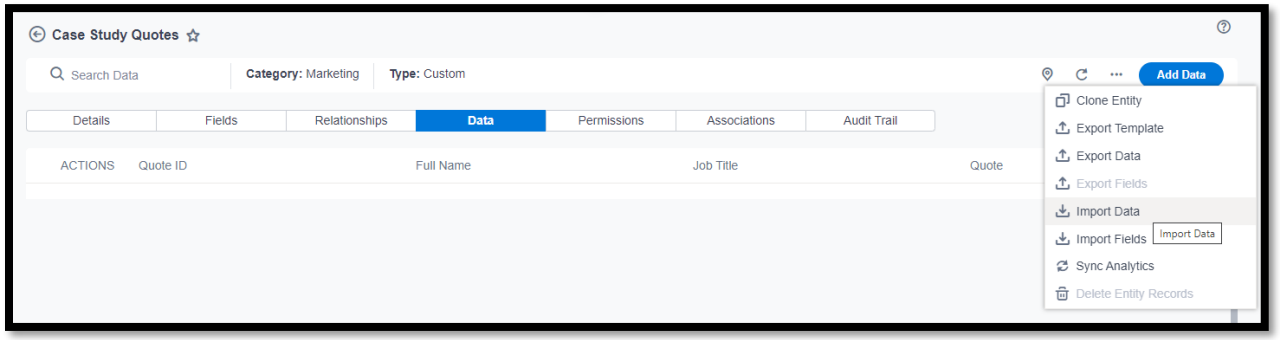
Session Management



Excel File Import to Data Entity

On AgilePoint NX, authorized user can easily import data from an Excel file into a data entity. AgilePoint NX does not store or transfer during the data transfer process. The data is extracted on the user interface side. The data entity engine parses through the data to ensure data integrity before the actual import. The data is transmitted via SSL connection and is encrypted. The details of the import can be viewed on a row-by-row basis, if the audit log is enabled for the entity.

Excel Data Import



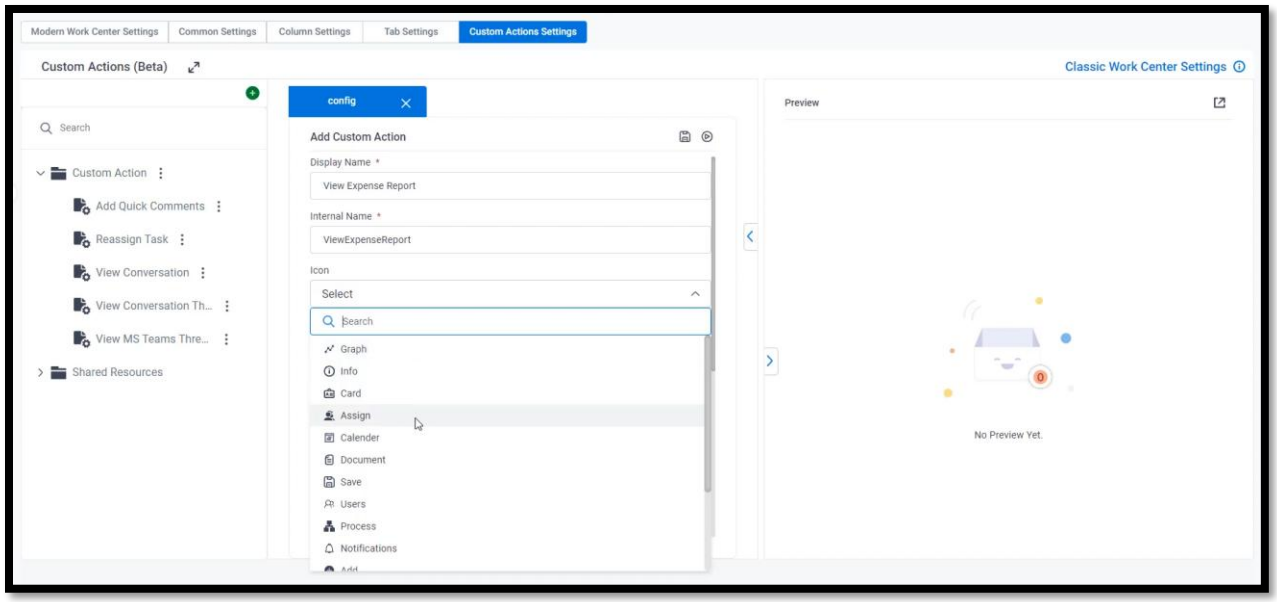
Excel File Import to eForm

AgilePoint NX allows end users to directly upload Excel and CSV files directly into sub-form control and/or data grid control on the eForms page. The content that is read from the Excel or the CSV files is not stored it anywhere in the AgilePoint NX (system/database). The file content is converted into string format and then sent back as JSON format to display on the page. For larger files, you should consider alternatives like using process model to read rows from Excel and map back to underlying system directly. The same API is used for Excel import into Data Entity, eForms and Process model.

Custom Actions Framework

Custom Actions Framework allows developers to customize the Modern Work Center. Custom actions involve the usage of HTML, CSS, JS by authorized users. This newly inserted HTML, CSS and JS code will execute in the Modern Work Center tasks and process pages. Any access API to the AgilePoint server can be called, but all API calls are secured and authorization check is done on the backend server code as well. Custom actions configuration is available in the settings module.

Custom Actions Framework in Modern Work Center



Add Document to an Activity

All activities in the process designer allow the developer to upload web links and documents. These links/documents become part of the applications assets and can be seen in the folder structure of the app. This is extremely useful in case new app designers join the team and can know what was the logic associate with that particular step in the process. The document upload supports most of the commonly used formats such as PDF, JPEG, GIF, Word, Excel and more. These files inherit the access restrictions defined on the app.

When the app designer exports the application from one environment to another, the associated documents are also included in the export package. The concerned developers have to keep in mind the number of files along with the corresponding file size, to ensure that the package size does not become very large. At run time, these files and links can be accessed from the process viewer.

Authorized users can import the files for attachments. AgilePoint NX stores the files in the Application Resources folder of the app and the file content gets stored in the Database. App Builder parses through the data to ensure data integrity before the actual import. The data is transmitted via SSL connection and is encrypted. The imported file can be downloaded by the authorized user in design time or in Process Monitor's activity details in runtime.

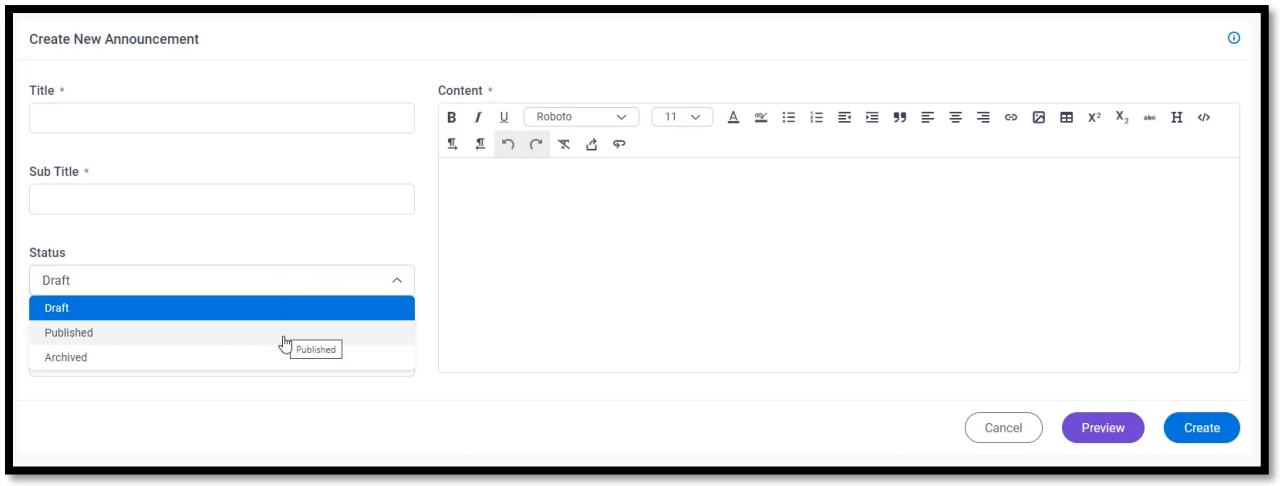
Mobile App Configuration – QR code

A QR code is generated to configure the companion mobile application, available in Google Play Store and Apple iTunes Store. This QR code is visible under user profile and settings page, meaning unauthorized user cannot have access to the QR code generated. The QR code is generated dynamically on the fly, when a user accesses the above-mentioned page. This dynamically generated QR code is not be saved in the database. The generated QR code does not contain any confidential information such as password. It only stores the configuration required for the user to set up companion Android/iOS app, publicly available in the corresponding app store.

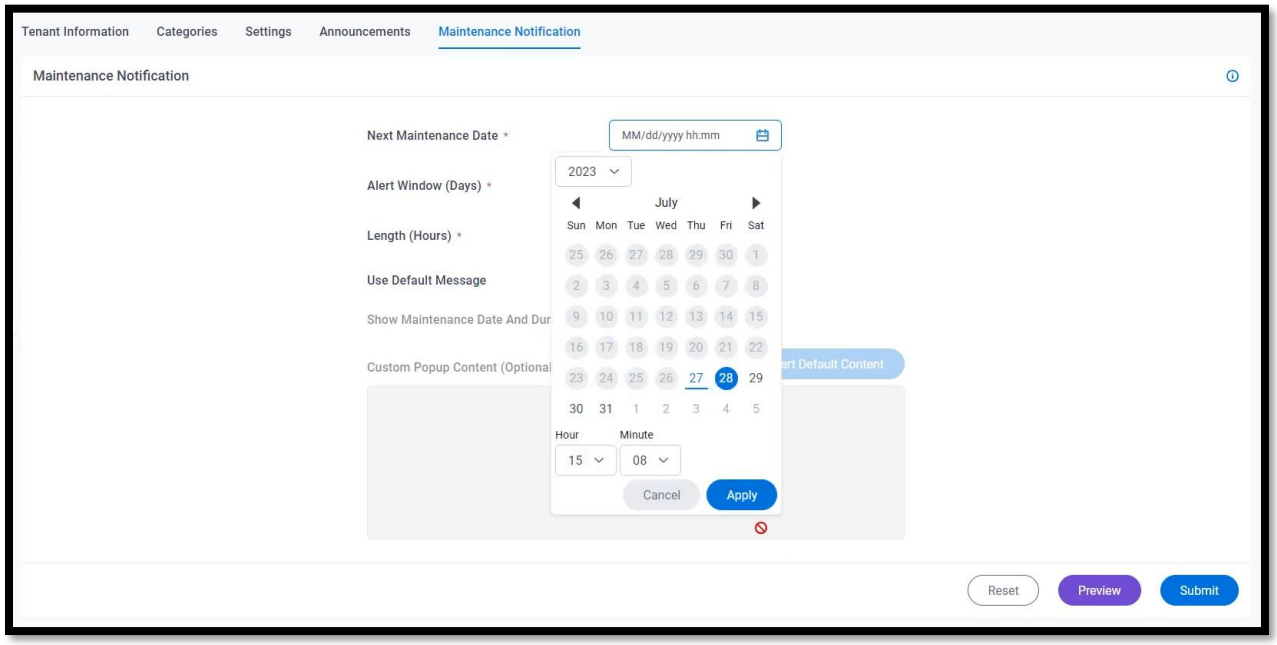
Announcements and Maintenance Notifications

AgilePoint NX provides a facility for the Tenant Administrator to make in-portal announcements. and to provide maintenance notifications to all users of the concerned tenant. For customers who are on OnDemand (public cloud) - shared tenant, the announcements, and notifications are managed by AgilePoint's IT team. For a dedicated cloud hosted by AgilePoint, the announcements, and notifications are managed by the customer's designated administrator. Past announcements are available for audit.

Announcements



Maintenance Notifications



Data Sources

AgilePoint NX securely connects to external data sources only through secured access tokens. (More information about Access Tokens is in Section 6.2). Users cannot access data sources from the browser; access to data sources are available only through the server using the corresponding access tokens. AgilePoint NX supports a concept of primary and secondary data sources.

Primary Data Source - This is the primary data repository used in your app. When a user submits a form or a process updates a data as part of logic, the data is directly saved in the primary data source mapped with the process or eForm. The following data sources are currently supported:

- MySQL
- MS SQL Server
- SharePoint
- Salesforce

- AgilePoint Data Entities
- Excel
- Oracle

Application metadata is stored in AgilePoint's internal database, which is different than the app data stored in the data source. The application developer must explicitly map the fields in the data sources with the app's variables in order to read from and write into the data source, using the schema mapper. The schema mapper ensures that the data integrity of the data source's data. If the application developer wants to store a copy of the app's data locally also, then they must explicitly enable this feature in each process. Please refer to the AgilePoint NX Product Documentation for further details on data sources.

Secondary Data Source - Even though your app is configured to primarily store data in the primary data source automatically, there might be app requirements where as part of application logic you might have to push the data to a secondary data source like a document repository, data repository, digital signature providers, and so on. These are supporting systems for your app. Secondary data source follows the same security principles that are applicable to primary data sources.

In addition to the primary data sources listed above, AgilePoint apps can connect to 120+ secondary data sources using secured access tokens. Please refer to the section on External System Level Identity Management for a comprehensive list of secondary data sources supported by AgilePoint NX.

Cookies

AgilePoint NX creates the cookies listed below. AgilePoint does not track users' behavior. If the encrypted cookie is tampered with, then the system will reject the cookie, and the requested action will fail.

Cookie Name	Purpose	Notes	Encrypted
.NX.PORTAL.V2	The session cookie for NX Portal.	The name is configurable through the NX Portal configuration.	Yes
AP_Auth	The session cookie for client-side modules.	Created on the fly and is automatically deleted when the window is closed.	No
AP_Version	Used by the client-side modules to control clearing of cache between product releases. It carries only the release version and date	Created when user logs in and is deleted when user logs out.	No
RequestVerificationToken	To prevent CSRF (Cross Site Request Forgery).	Created when user accesses a page in the NX Portal from a form and is deleted when user logs out.	Yes

Logging Services

AgilePoint NX writes module wise logs. AgilePoint Server, AgilePoint Cluster Server Manager, SharePoint Connector, and Active Directory Sync all provide an option to write separate log files. Log files store different types of data, including, but not limited to, failure messages, exceptions, user authentication, and session

information. Location of the log files can be customized. Only the System Account Administrator can access the log files.
The details of the information logged by AgilePoint NX are:

- **Error** – Exception and critical operation failure message would be logged under error log files.
- **Warning** – Logs those messages which are not critical, but it would good to get resolved.
- **Info** – Logs message which would help to trace the regular flow of the operation including server start and stop.
- **Debug** – Stores log line which has been written for troubleshooting any issue or temporary log lines which can be removed once feature becomes stable.

Audit

Detailed information is available for auditors on various types of actions in NX, such as app file versioning, runtime activity execution, task monitoring, events from AgilePoint Server, change in app data (process and form) and more. The system records events and actions about both the system and users.

The following user actions are logged:

- **App Builder (application designer) actions** – Across the app design lifecycle.
- **Runtime app user actions** – Interactions with the app at runtime (sometimes called a business application).
- **System Administrator actions** – Maintenance and administrative activities are recorded.

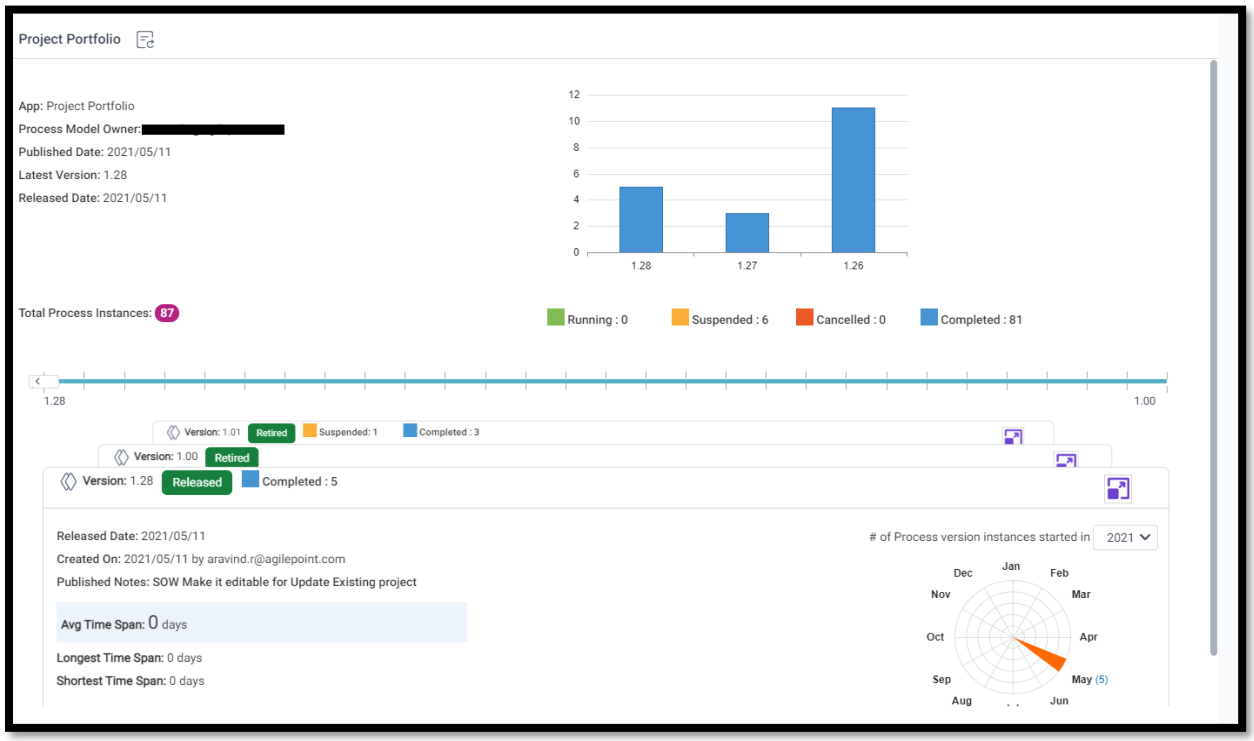
Auditors can get detailed historical and live information at the application level:

- **At design time** – History of operations that include editing, check-in, check-out, save, publish, export, import, delete, API integrations, and rollback.

- **At Runtime** – History of executions, process initiation requests, API integrations, and user activities.
- **For app components** – Processes, eForms, tasks, API calls, and notifications.

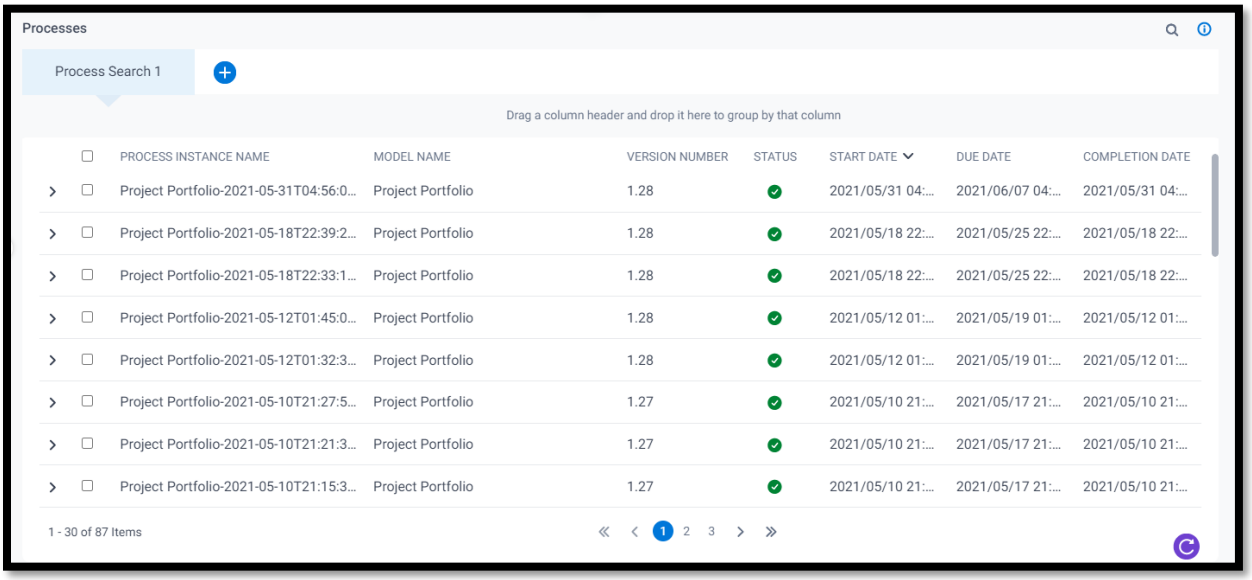
Authorized users can view the change history log of the app at each process level. As shown below, for each process, the number of live instances in each version can be viewed using the version slider bar at the bottom of the screen.

App Change History



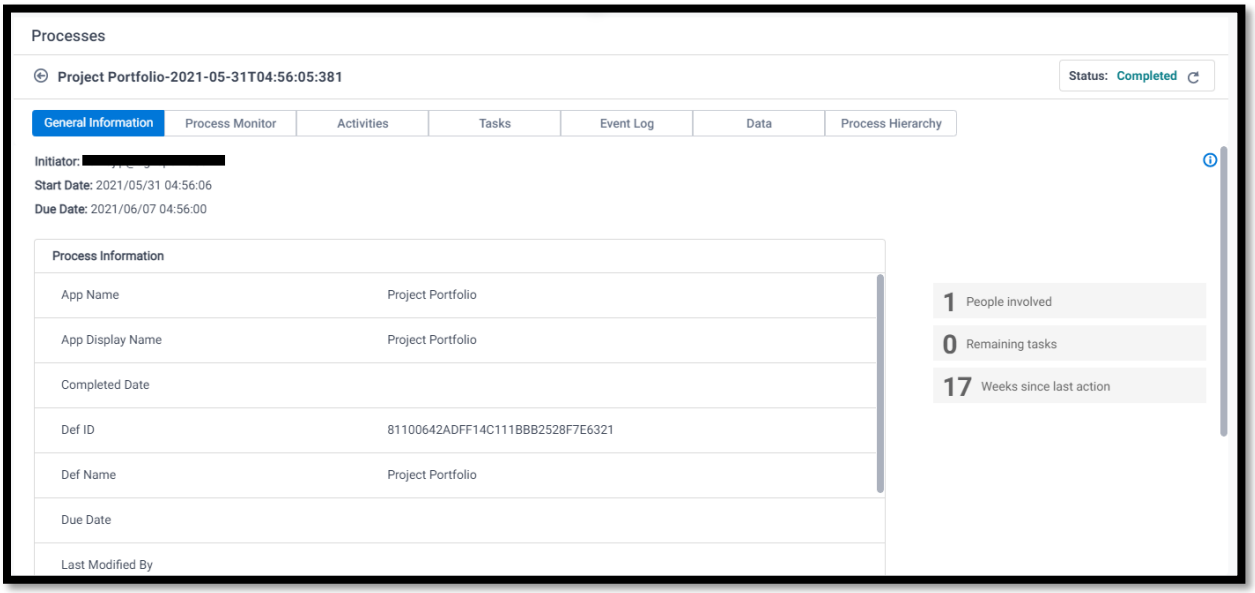
Authorized users can access the detailed history of each process instance of any selected version of the process of any selected app in the system. The process instance may show as Completed, In Progress, Suspended, or Cancelled status. In the screenshot below, the user is viewing all instances of a process for a selected app.

List of All Process Instances in a Selected App



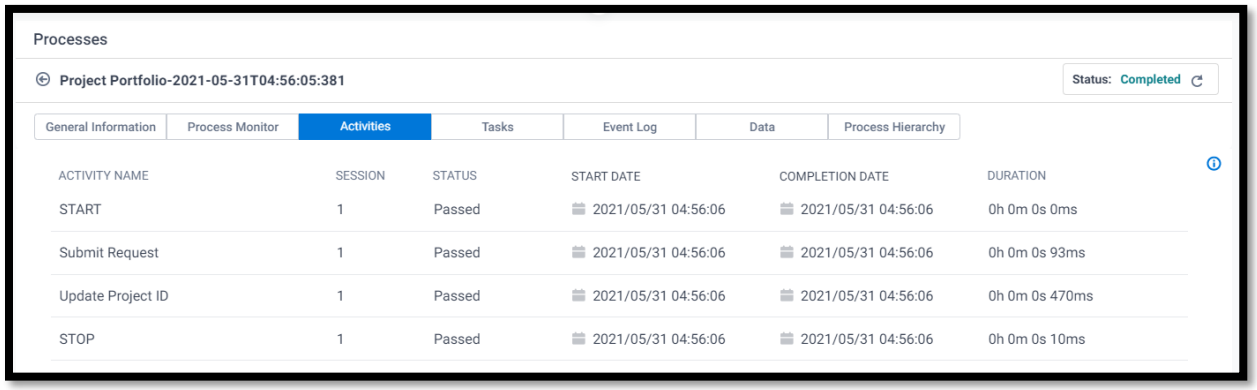
For a given process, the authorized user can now view many data points under the General Information tab. This includes the parent app's details, the number of users involved in the process instance, pending tasks of the process instance, and time since last action in the process.

Audit Logs for All Actions



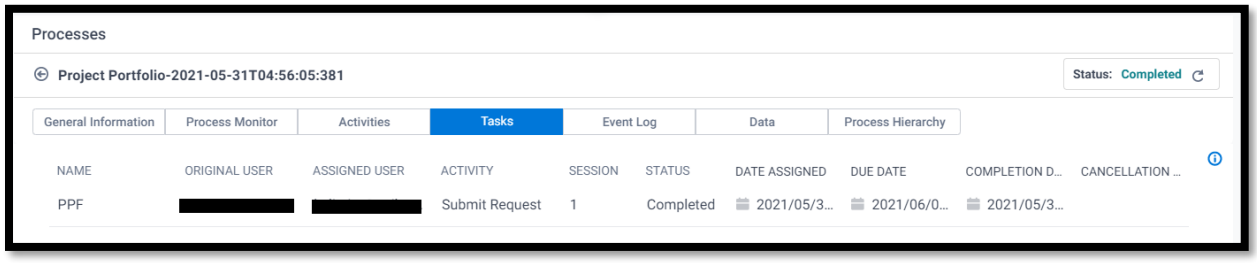
The authorized user can view information of all the activity instances of the selected process instance. This includes the name of the activity instance, number of times the activity was executed, the start and end date-time of the activity and the status of the execution.

Audit Logs for Activity Execution



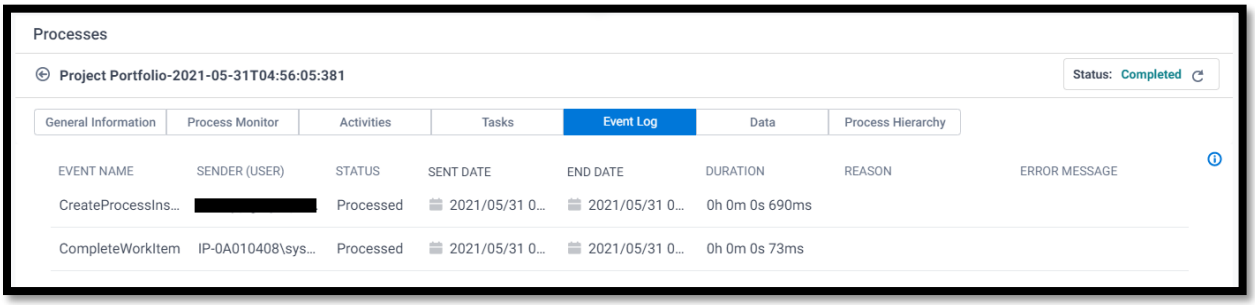
Many processes have tasks that users must complete. The authorized user can view the name of the task, the user who executed it, the user who was originally assigned, the number of times the activity was executed, and the date-time of creation and completion.

Audit Logs for Task Monitoring



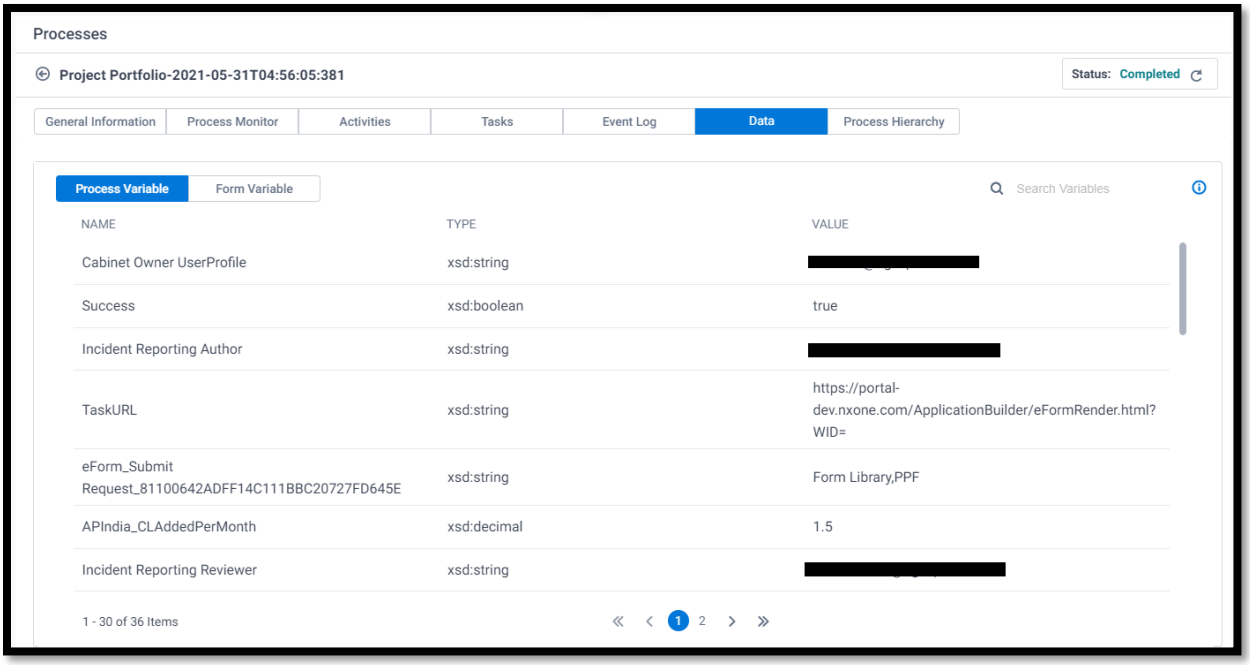
Authorized users can view details of various events related to the specified process instance. This includes the type of event, the user associated with the event, the status of the event, and the event start and end date-time.

Audit Logs for Engine Events



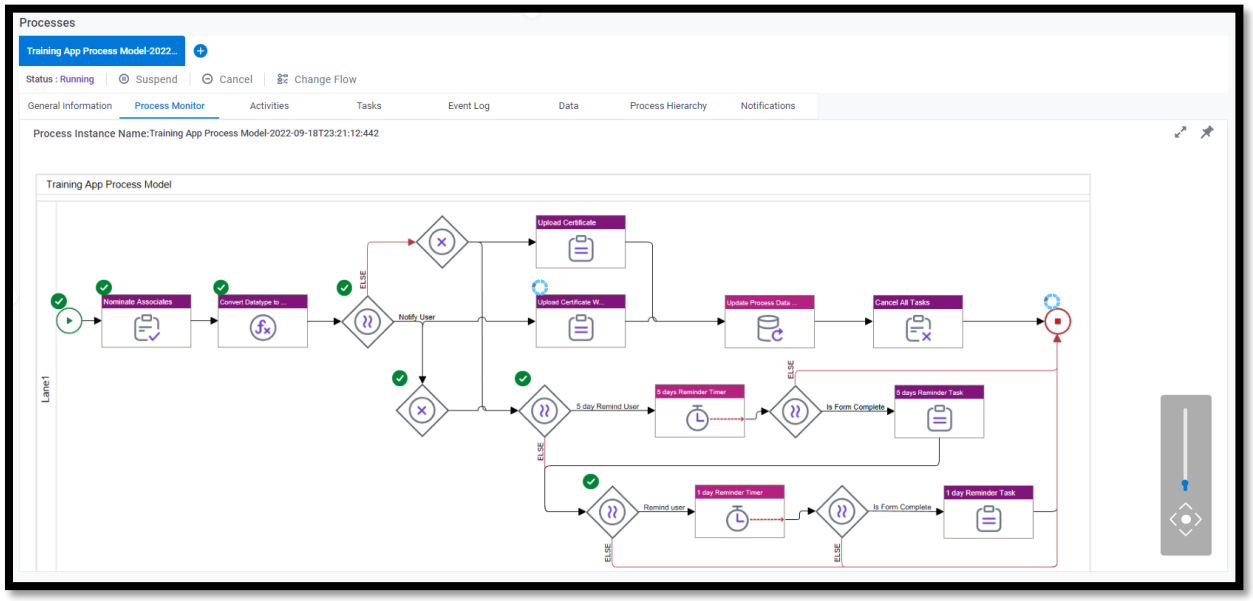
For each process instance, the authorized user can view the data of all the variables. The variables cover both the variables that are part of the process instance and the variables that are part of the eForm.

Auditing the Values Stored in the Variables



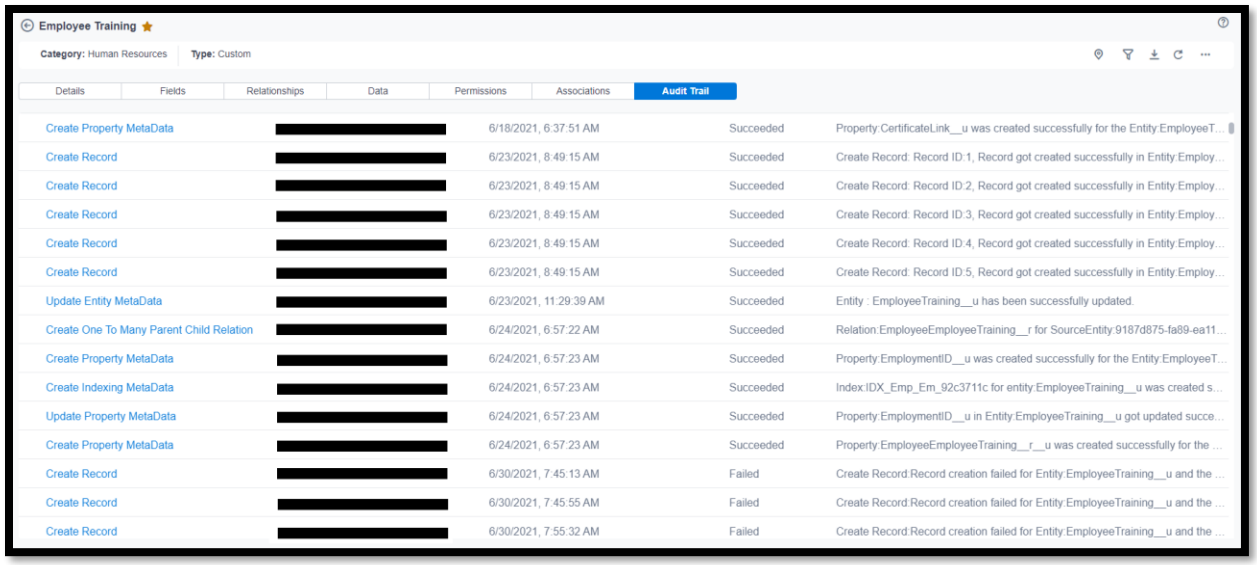
The authorized user can also graphically audit a live or a past process instance.

Graphical Audit Logs for Workflow Execution



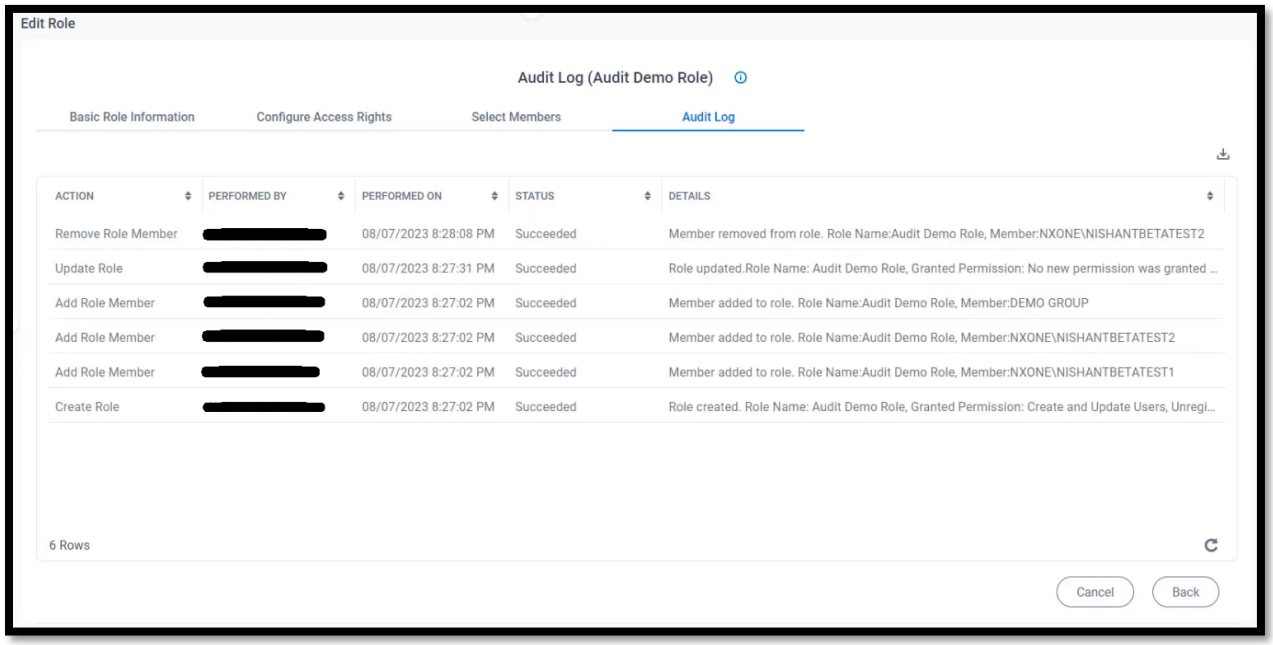
The Data Entity module provides an option to the user to selectively enable or disable audit trail on individual entity. Enabling audit on data entity, provides history of user actions in the data.

A Data Entity Audit Log

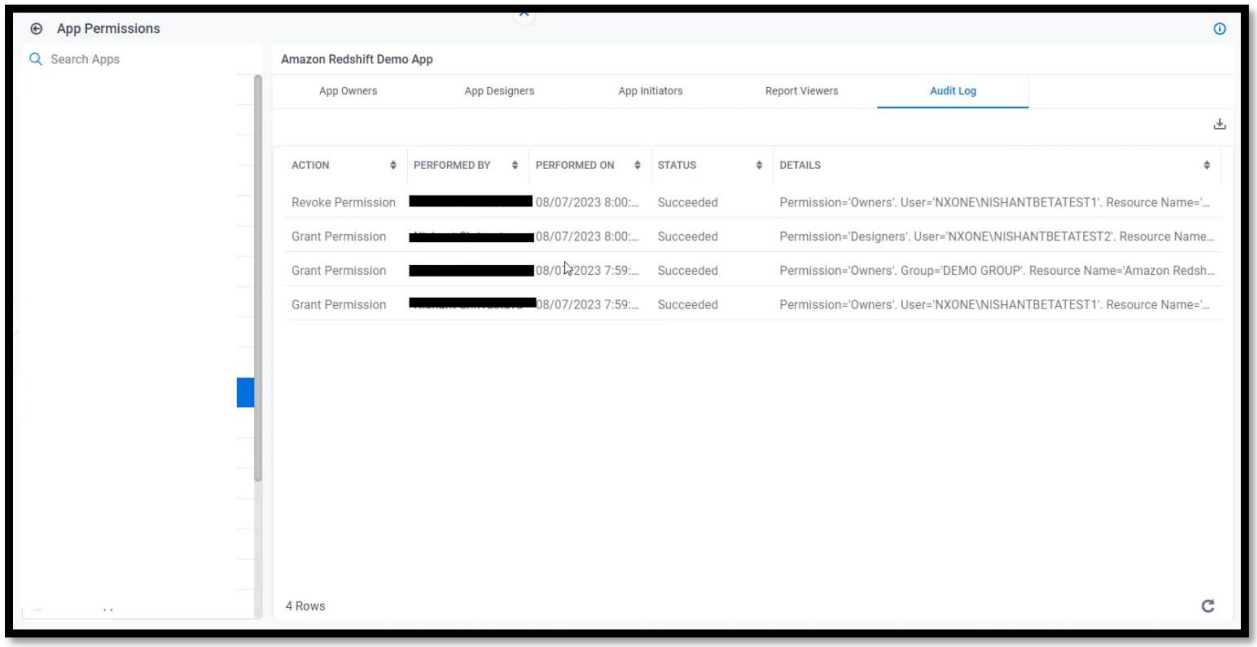


AgilePoint NX also comes with security audit logs. These audit screens display all changes to Groups, Roles, Pages, Entities and Application related permissions, whether done by a user or through the API. It is available for all deployment options. It tracks whether the action failed, or was completed successfully.

Audit Logs for Roles



Audit Logs for Apps



Ensuring Application Integrity During Collaborative App Development

When application development requires a larger team, the team may choose to enable the collaborative development feature in the Settings module. The AgilePoint NX platform ensures that the integrity of the app is ensured application development lifecycle. If a Process were to be locked for editing by one user, the following are blocked for the remaining app developers:

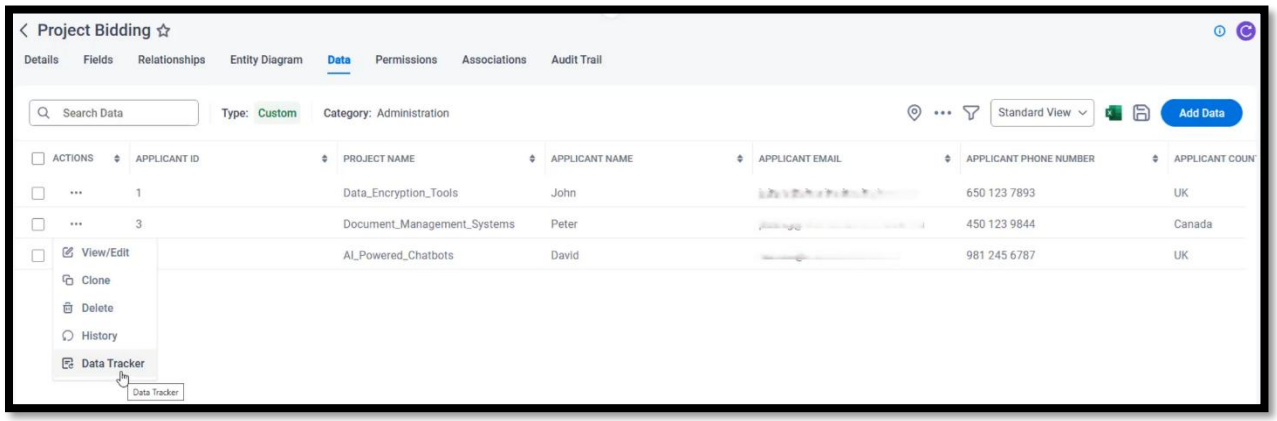
- Changing the process data model
- Edit of its library
- Creating/Editing Data Sources

If an eForm were to be locked for editing, the following are blocked for the remaining app developers:

- Adding new controls
- Promoting a control to the library
- Mapping of a data source
- Edit DataGrid/ListView configuration

Enhanced Data Governance in Data Entity

Data governance is crucial for enterprise customers, and AgilePoint has made this a top priority. With Data Tracking, authorized users can now enable this on selected fields within an entity to view a full history of recorded changes at the individual row level. The authorized user sees exactly what the old values were and what they've been changed to.



On the access front, a user's permission can be configured to any of the three access scenarios:

- **Entity Owner** - Full permissions for the entity. This includes all other security roles and the ability to manage security roles to other users and groups.

- **Entity Designer** - Add, modify, and delete fields, relationships, and other parts of the entity.
- **Entity Metadata Viewer** - Allows authorized users to view the metadata of the entity, giving your app designers ability to configure form lookups and process activities without needing a designer permission on the underlying data entity.

Open Standards

AgilePoint strongly believes in using open standards to promote interoperability and to ensure security. During the app design, the application developer is not forced to learn any proprietary scripting language. At the runtime, AgilePoint NX communicates with other systems via open standards. The NX user interface is built using open industry standard technologies such as HTML5, CSS3, and JavaScript.

AI Security and Governance

Introduction

AgilePoint NX is a smart platform that helps in operationalize AI, spread across various aspects of the platform, including:

- **AI Control Tower** - These are AI agents that provide centralized, real-time monitoring and analytics feature that leverages artificial intelligence to help organizations oversee, improve governance and optimize their business processes.
- **Generative AI** - This helps design emails, apps, data entities, picklist and eForms from inputs such as images, Excel, PDFs or text input typed on a prompt console through natural language recognition. The table below summarizes some of the GenAI implementation available on the platform.

Sr. No.	Feature Name	Demo Link
1	Intelligent Assistant - AgilePoint Resource for Intelligent Assistant (ARIA)	Click Here
2	Generate Form-Based-App from GenAI Prompt	Click Here
3	Generate Form-Based-App from Image file	Click Here
4	Generate Form-Based-App from PDF file	Click Here 2
5	Generate Form-Based-App from Excel file	Click Here
6	Generate Data Entity	Click Here
7	Generate Picklist	Click Here

Sr. No.	Feature Name	Demo Link
8	Generate Email Text from GenAI Prompt	Click Here
9	Translate Email Text to Other Languages	Click Here
10	Translate Form Text to Other Languages	Click Here
11	GenAI Agents	Click Here
12	Generate Process Based App using GenAI	Click Here
13	Translate Picklist Text to Other Languages	Click Here
14	Generate Master-Detail Data Structures in Forms	Click Here

- **GenAI Agents** - Available as workflow tasks, it takes natural language input and converts this into AgilePoint specific orchestration and automation.
- **ARIA** - The intelligent chatbot is trained on AgilePoint NX platform to engage with developers and end users to provide technical assistance via Natural Language Processing (NLP). It has the knowledge of AgilePoint product and also has the capability to generate code.
- **Smart Lookups** - At run time, based on the request input a Machine Learning (ML) model will get executes and the output data will be fetched, processed, formatted and displayed on the eForms.
- **Translations and localization** - To convert text from one language to another in emails, picklists, and eForms.
- **Third-Party Connectors** - AgilePoint provides a rich portfolio of OOTB popular third-party Machine Learning/Deep Learning (ML/DL) connectors such as Azure, AWS, OpenAI, and NVIDIA that can be used in drag-drop-configure manner.

Ethics

AI System Design and Ethical Operation

AgilePoint ensures that its AI systems are designed and operated ethically by following a comprehensive set of principles. The company employs reinforcement learning from human feedback (RLHF) to guide AI responses toward ethical and responsible behavior, publishes system cards and technical papers to provide transparency regarding model functionality and limitations, and enforces strict usage policies that prevent misuse. Its models are trained solely on technical documentation and how-to videos to mitigate bias, while extensive testing and user feedback continuously refine performance. Data from customer or prospect is never used for training. User controls, such as clear disclaimers and the ability to report issues, along with ongoing investments in research, underscore AgilePoint's commitment to responsible AI deployment.

Bias Prevention

AgilePoint's pretrained model is configured to avoid processing requests that are outside the product's intended scope, thereby preventing the perpetuation of biases or discriminatory outputs. Users are advised to not enter PII and use the model for the purpose of application development only. If users attempt to use AgilePoint's AI for purposes other than what it is meant for, such as asking questions that is not product related, then the output is not guaranteed.

Transparency in Ethical Considerations

The company maintains transparency by openly disclosing details of its base model and the data exposure involved, ensuring that users understand the ethical framework and the minimal post-processing applied—limited solely to parsing structured data from large language model outputs.

Ethical Framework and Scope

AgilePoint's AI is purpose-built exclusively for resolving AgilePoint platform related queries. This focused design prevents the system from engaging in any activities beyond its intended function, thereby simplifying the ethical framework and minimizing potential misuse.

Auditing and Fair Decision-Making

To guarantee that AI decisions remain fair and auditable, AgilePoint publishes details of its base model (https://huggingface.co/Qwen/Qwen2.5-32B-Instruct), which provides a transparent basis for evaluating AI performance and decision-making.

Security

Protection from Cyber Threats

AgilePoint protects its AI systems by isolating them from external networks, restricting human access solely to authorized system administrators (with CTO approval), and limiting API access exclusively to the AgilePoint NX product. These measures collectively minimize exposure to cyber threats.

Pre-Deployment Security Testing

Before any deployment, AgilePoint subjects its AI systems to rigorous security testing through a Secure-SDLC process based on ISO 27001 and SOC 2 standards, along with additional dedicated security tests to ensure robust protection.

Employee Security Training

All employees, particularly programmers, receive comprehensive security training—including mandatory annual sessions—that covers the unique challenges and best practices related to AI technology.

Data Protection

Data Protection Measures

AgilePoint manages the security of data used by its AI systems through multiple layers of protection: data in transit is encrypted, data at rest is access-restricted, and data in use is isolated. Additionally, dynamic application security testing (DAST) is performed to continuously assess the system. AgilePoint does not train models on customer's data. ARIA is solely trained on AgilePoint's documentation and knowledge base to answer AgilePoint related queries. 90 days is the time window after which the user chat history is permanently purged. The chat output is related to AgilePoint documentation. Customer can delete their chats via a self-service. The PDF/Images uploaded for GenAI are not stored. They are discarded once labels and control types are parsed.

Retention and Disposal Policies

The company does not transmit or store any personally identifiable information (PII) in its AI systems. Any stored data is irretrievably purged after a period of 90 days, ensuring strict adherence to data retention policies.

Preventing Sensitive Data Exposure

AgilePoint ensures that its AI systems do not inadvertently expose sensitive data by design. In public cloud deployments, the multi-tenancy architecture of AgilePoint NX confines any data, even if inadvertently submitted, to the originating tenant.

Global Compliance

By adhering to key international standards—such as GDPR, the EU-US Data Privacy Framework, and CCPA—AgilePoint maintains robust data security and regulatory compliance.

Breach Detection and Response

Protocols for detecting and responding to data breaches in AI systems are defined according to the rigorous standards of AgilePoint's ISO 27001 and SOC 2 implementations.

Privacy

User Privacy Assurance

AgilePoint's AI systems are designed to work without the use of personally identifiable or sensitive information, effectively ensuring user privacy at every stage of development and deployment. Users are advised to not enter PII. User can always and selectively delete data from chat history.

Surveillance Concerns

The AI is strictly designed for application development and support purposes, not for surveillance, thereby addressing any potential concerns related to invasive monitoring.

Balancing Data Collection and Privacy

Since AgilePoint's systems do not collect any PII or sensitive data, the balance between necessary data collection and the right to privacy is inherently maintained.

Personal Data Analysis Policies

Policies regarding the analysis of personal data are not applicable, as the AI does not handle any PII or sensitive information.

Stakeholders

Impact on Stakeholder Trust

AgilePoint's AI is developed solely to enable application development, a focused purpose that helps maintain clear expectations and safeguards stakeholder trust.

Addressing Ethical Dilemmas

Since the AI is limited to supporting application development and product support, potential ethical dilemmas are minimized due to its narrowly defined operational scope.

Staying Abreast of Regulations

The CTO and CISO at AgilePoint actively monitor current developments and legislative trends, ensuring that the company remains up to date with evolving AI regulations.

Compliance

Ensuring Regulatory Compliance

AgilePoint's compliance with industry regulations is reinforced by partnering with reputable service providers (such as AWS, Azure, Google, and OpenAI) that meet

strict industry standards. Both its AI offerings and the AgilePoint NX platform operate well within these compliance boundaries.

Internal Compliance Reporting

Compliance reporting is managed internally by encouraging employees to report concerns directly to the CTO, while external issues are tracked through a traceable ticket system managed by product support. This dual approach ensures that all reports are addressed appropriately.

Project Execution

Project Management Methodology

AgilePoint applies the same mature and well-trusted project management methodologies used for the AgilePoint NX platform to its AI implementation projects, ensuring consistency and reliability throughout the project lifecycle.

Risk Management in AI Projects

Risks associated with AI project execution are managed by providing orchestration capabilities that allow customers to control and govern AI deployments. The AI system, being purpose-built for application development on the AgilePoint NX platform, is designed without access to PII or sensitive information, thereby reducing potential risks.

Quality Assurance

Quality Control Measures

A multi-layered quality control framework underpins AgilePoint NX's AI-driven processes. This framework includes rigorous input validation, real-time error monitoring, and comprehensive audit logging to ensure any discrepancies are swiftly identified and addressed. Configurable trigger conditions and action rules empower administrators to fine-tune AI outputs to meet predefined quality standards and business objectives. Additionally, stringent code reviews and dedicated testing cycles for AI components are integral to the process, ensuring that any potential issues are resolved prior to deployment. Security is reinforced through systematic vulnerability assessments, including Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST). Finally, detailed design documents are required to be reviewed and formally approved for each major change, further cementing the framework's role in maintaining system integrity and performance.

Accuracy and Reliability of AI Outputs

To ensure continuous improvement and relevance, AgilePoint employs a rigorous training framework that complements our ongoing model updates. This process begins with domain-specific fine-tuning—leveraging high-quality, curated datasets and transfer learning techniques—to capture the nuances of our industry and specialized tasks. Effective prompt engineering further refines the training process by utilizing structured prompts and contextual examples, while iterative testing and user feedback continually optimize model responses. In addition, data quality is maintained through diligent curation and augmentation with diverse sources such as customer insights and domain-specific literature. Reinforcement learning, incorporating systematic human feedback, plays a pivotal role in aligning AI outputs with real-world requirements. Furthermore, our base model is upgraded or replaced on a regular basis to ensure that the system remains at the forefront of AI advancements, consistently benefiting from the latest developments in AI technology. Finally, continuous monitoring using defined performance metrics and regular security assessments, alongside thorough reviews of design documents for

every major change, ensures that each training cycle enhances both the accuracy and reliability of the AI outputs while adhering to stringent compliance and ethical standards.

Adherence to Standards

AgilePoint adheres to stringent standards, including ISO 27001 and GDPR, to ensure high-quality assurance for its AI systems.

Regulatory Adherence

Keeping Pace with Regulations

AgilePoint's legal team continuously advises leadership and product management on the latest AI regulatory requirements, ensuring that the company's practices evolve in line with emerging standards.

International Compliance Standards

The legal team also ensures that all AI applications comply with existing, evolving, and forthcoming international compliance standards, safeguarding the company's global operations.

PIIs and Sensitive Data

Alignment with Data Protection Laws

AgilePoint's AI systems are designed in strict accordance with data protection laws such as GDPR and CCPA by not collecting any personally identifiable information (PII) or sensitive data, ensuring robust data governance.

Risk Management

Risk Assessment and Management

As a platform provider, AgilePoint enables individual application teams to assess and manage the risks associated with integrating AI into compliance-sensitive areas. The company provides the necessary framework for these assessments without directly handling the application-specific risk.

Protocol for Compliance Breaches

In the event of an AI-related compliance breach, the responsibility for addressing and managing the incident lies with the teams building the applications, with AgilePoint offering the requisite framework for reporting and remediation.

Third-Party Vendors

Evaluation and Monitoring of Third-Party Compliance

AgilePoint evaluates third-party AI components by partnering with globally recognized providers such as Google, AWS, Azure, OpenAI, and Meta, ensuring that these solutions meet stringent industry compliance standards.

Vendor Expectations and Requirements

AgilePoint requires vendors to maintain a strong reputation and hold necessary certifications, with contract terms that mandate proper approvals for any changes. Vendors must demonstrate robust data handling and protection practices in line

with privacy policies and regulations (such as GDPR and CCPA), implement clear data retention and destruction policies, maintain detailed logs for monitoring, and adhere to solid performance, security, and risk management practices. Compliance with local, national, and international regulations—supported by certifications such as ISO 27001/27017/27018, SOC 2 or, SOC 3—is also mandatory, along with clear protocols for data transition upon termination of the partnership.

Employee Training

Training Programs on Compliance

All employees, particularly programmers, participate in general annual security training that covers AI compliance. This ensures that concerned staff members are well-versed in the best practices and regulatory requirements associated with AI.

Measuring Training Effectiveness

The effectiveness of these training programs is evaluated by simulating internal security attacks. Employees who do not demonstrate adequate alertness are required to retake the training, thereby ensuring continuous improvement.

Reporting Mechanisms

Internal and External Reporting

AgilePoint addresses AI compliance issues and escalations on a case-by-case basis. Internally, concerns are escalated to the CTO. Issues that are reported through a traceable ticket system managed by the product support team. The next level of escalation is the product management team and the final level in the escalation matrix is the CTO. This process ensures that all compliance issues receive prompt and appropriate attention.

Continuous Monitoring

Ongoing Compliance Tools

AgilePoint employs both static application security testing (SAST) tools and dynamic application security testing (DAST) tools to support ongoing compliance monitoring, ensuring that the system remains secure and resilient.

Portfolio Management

Preventing Performance Bottlenecks

To ensure that AI-generated applications do not lead to performance bottlenecks, AgilePoint conducts thorough capacity planning before the development of each application, aligning resource allocation with anticipated workloads. Add run time.

Architecture

AgilePoint's abstraction layer architecture is designed for seamless integration with generative AI (GenAI) tools by leveraging a metadata-driven, platform-agnostic, and composable design. A unified metadata layer standardizes data and application logic, allowing GenAI tools to access consistent, process-centric data models. Its codeless composability enables rapid AI deployment without extensive coding, while an adaptive "Automation Fabric" supports dynamic workflows in changing environments. This architecture also enhances collaboration by providing real-time insights, automates data preparation for AI readiness, and incorporates governance features—such as the AI Control Tower—to ensure responsible AI usage. Additionally, the ARIA assistant leverages large language models to offer contextual guidance and streamline complex tasks, creating a synergistic environment between AgilePoint's platform and GenAI tools.

Data Transmission, Processing and Storage

Feature	What's Transmitted	What's Processed	What's Retained/Discarded
AgilePoint's Resource for Intelligent Assistance - ARIA	1. Text input from user. 2. Transmission is end-to-end encrypted. 3. Data goes to ARIA-API and response is transmitted back to ARIA chat console.	1. Plain text is processed in AgilePoint private cloud. 2. The ARIA-API Embedding service is called to vectorize the input. 3. Vectorized input is used to retrieve relevant documents from the vector DB. 4. LLM Service is used to run the inference on the text and the documents. 5. Inference output is post processed	1. Vector service does not retain any information, including logging. 2. LLM does not retain any information. 3. The chatbot's memory preserves the conversion history with configurable auto-delete, managed by AgilePoint admin and the concerned user. 4. This information is not logged in any log file.

Feature	What's Transmitted	What's Processed	What's Retained/Discarded
		before streaming the response to chat console.	
Create Data Entity or Picklist using GenAI	1. Text input from user is transmitted to ARIA-API, which is end-to-end encrypted. 2. Text may be sent to translation API. 3. Text from ARIA-API is transmitted to LLM hosted in AgilePoint private cloud for inference. 4. LLM's response is returned to AgilePoint NX by ARIA-API.	1. Plain text in any single-language supported by AgilePoint. 2. Translation API detects and translates text to English, if the language is not English, for processing. 3. LLM service is used to run the inference on the translated text inside AgilePoint private cloud. 4. The inference output is post-processed and translated back to the detected language	1. The plain text input and post processed output are logged for troubleshooting purpose in the ARIA database. 2. Data is automatically purged after 90 days.

Feature	What's Transmitted	What's Processed	What's Retained/Discarded
		using Translation API, if not in English.	
Generate Form Based App from PDF file	1. File is transmitted to ARIA-API. 2. Data from ARIA-API, is transmitted to OpenAI and is transmitted back. 3. ARIA-API sends response to AgilePoint NX. 4. If PII is included in the uploaded file, then this is transmitted.	1. File is preprocessed to extract the first five pages into equivalent images by ARIA-API. 2. Inference is run by the OpenAI model to extract the required information from the image(s). 3. ARIA-API post processes the inference output and sends it to AgilePoint NX. 4. The system does not understand if the uploaded file contains PII or not.	1. The extracted image(s) is(are) saved in the ARIA database. 2. The PDF file is not saved on the ARIA-API's filesystem or in AgilePoint NX. 3. The ARIA system admin requires CTO's approval to access the database. 4. Data is automatically purged after 90 days.

Feature	What's Transmitted	What's Processed	What's Retained/Discarded
Generate Form based app from prompt	1. Text input from user is transmitted to ARIA-API, which is end-to-end encrypted. 2. Text may be sent to Translation service API. 3. Text from ARIA-API is transmitted to LLM hosted in AgilePoint cloud for inference. 4. LLM's response is returned to AgilePoint NX by ARIA-API.	1. Plain text in any single-language supported by AgilePoint. 2. Translation service API detects and translates text to English, if the language is not English, for processing. 3. LLM service is used to run the inference on the translated text inside AgilePoint cloud. 4. The inference output is post-processed and translated back to the detected language using Translation service, if not in English.	1. The plain text input and Post processed output are logged for troubleshooting purpose in the ARIA database. 2. Data is automatically purged after 90 days.

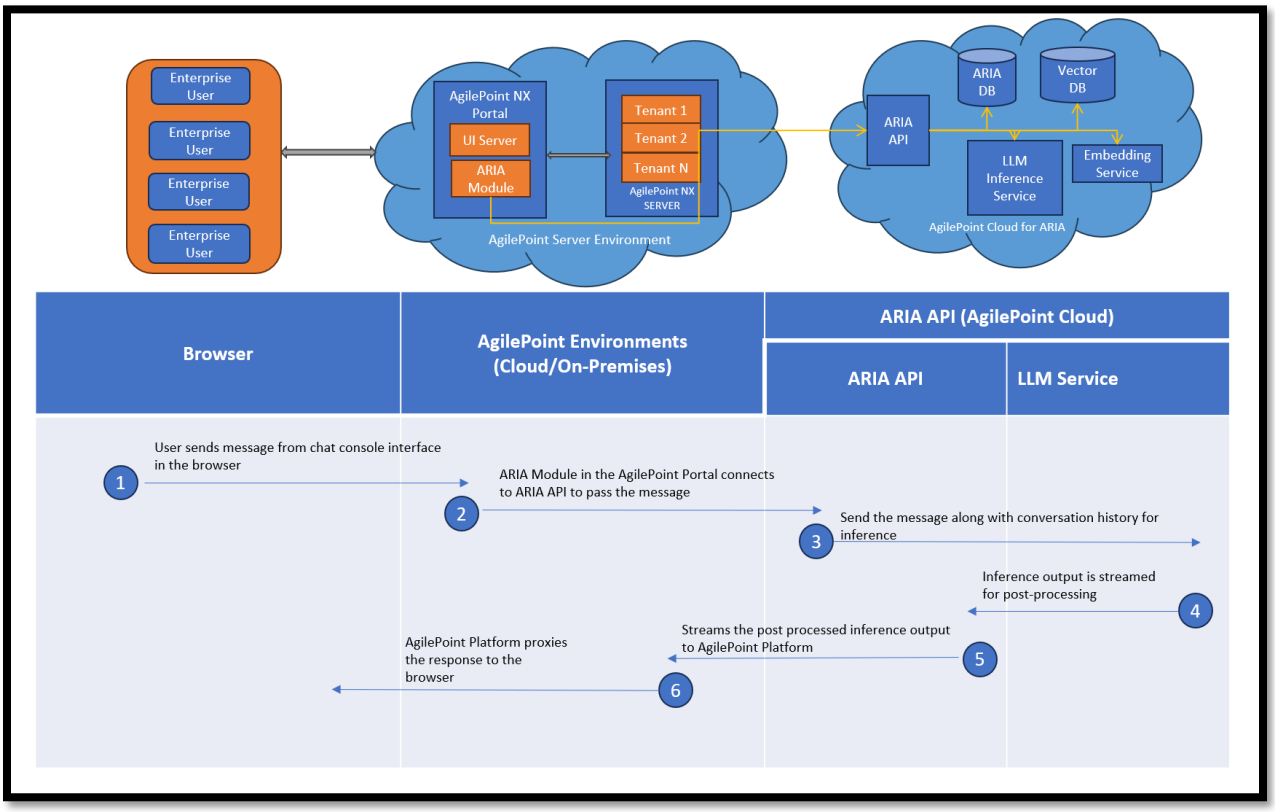
Feature	What's Transmitted	What's Processed	What's Retained/Discarded
Generate Form Based App from Image file	1. File is transmitted to ARIA-API. 2. Data from ARIA-API, is transmitted to OpenAI and is transmitted back. 3. ARIA-API sends response to AgilePoint NX.	1. Inference is run by the OpenAI model to extract the required information from the image(s). 2. ARIA-API post processes the inference output and sends it to AgilePoint NX.	1. The uploaded image is saved in the ARIA database. 2. The file is not saved on the ARIA-API's filesystem or in AgilePoint NX. 3. The ARIA system admin requires CTO's approval to access the database. 4. Data is automatically purged after 90 days.
Generate Form Based App from Excel file	1. No information is transmitted to ARIA API or any LLM.	2. Processing is done on the data fields and its metadata extracted from the Excel file on the AgilePoint server.	1. The uploaded file is not stored anywhere. 2. The data fields and the extracted meta data of the data fields are by itself not stored anywhere.

Feature	What's Transmitted	What's Processed	What's Retained/Discarded
Generate email text using GenAI	1. Text input from user is transmitted to ARIA-API, which is end-to-end encrypted. 2. Text may be sent to language translation service. 3. Text from ARIA-API is transmitted to LLM hosted in AgilePoint cloud for inference. 4. LLM's response is returned to AgilePoint NX by ARIA-API.	1. Plain text in any single-language supported by AgilePoint. 2. Language translation service detects and translates text to English, if the language is not English, for processing. 3. LLM service is used to run the inference on the translated text inside AgilePoint cloud. 4. The inference output is post-processed and translated back to the detected language using language translation	1. The plain text input and post processed output are logged for troubleshooting purpose in the ARIA database. 2. Data is automatically purged after 90 days.

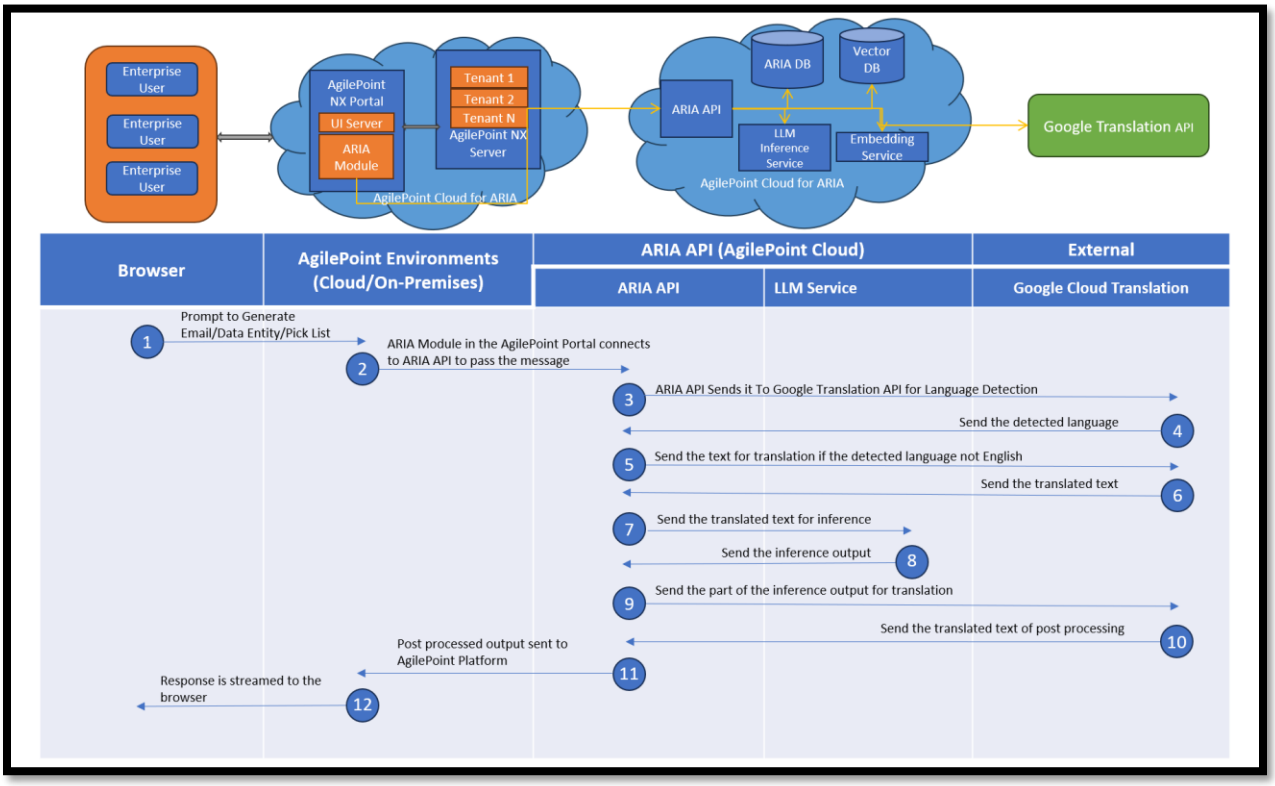
Feature	What's Transmitted	What's Processed	What's Retained/Discarded
		service, if not in English.	
Translate Email or Form Text or Picklist to Other Languages Using GenAI	1. Text only - entered by user. 2. Connection is end-to-end encrypted. 3. Data may be sent to language translation service. 4. Response is transmitted back to the client.	1. Text entered by user goes to ARIA-API. 2. Language translation API is called to detect the language and translate text to requested language. 3. The language translation response is post processed by ARIA-API.	1. The input and output are logged by ARIA-API for troubleshooting purpose in the ARIA system. 2. The ARIA system admin can access the database and needs CTO's approval. 3. Data is automatically purged after 90 days.
Generate Process Based App using GenAI	1. Text only - entered by user is transmitted to ARIA-API. 2. Data from ARIA-API, is transmitted to 3rd party trusted AI service and is transmitted back.	1. 3rd party trusted API runs Inference. 2. ARIA-API post processes the inference output and sends it to AgilePoint NX.	1. The plain text input and Post processed output are logged for troubleshooting purpose in the ARIA database. 2. Data is automatically purged after 90 days.

Feature	What's Transmitted	What's Processed	What's Retained/Discarded
	3. ARIA-API sends response to AgilePoint NX.		3. The ARIA system admin requires CTO's approval to access the database. 4. Data is automatically purged after 90 days.

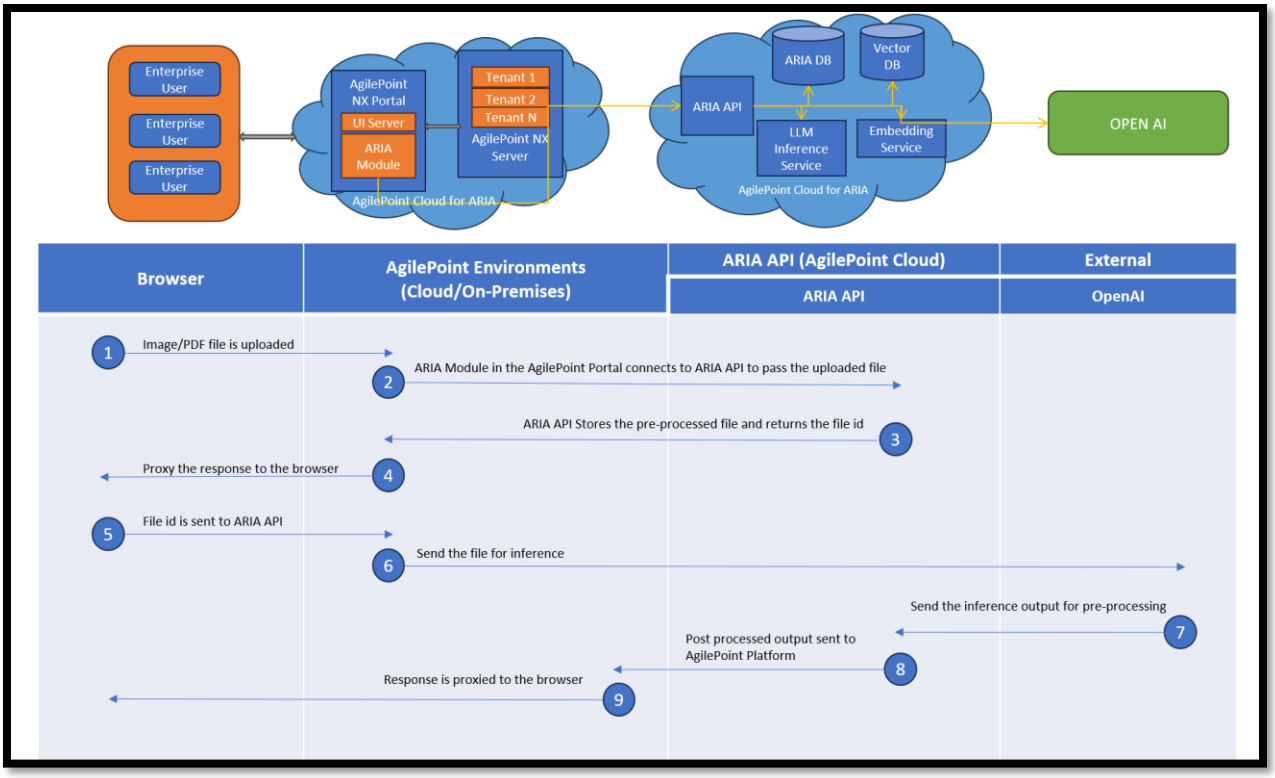
To visually illustrate, three simplified flow diagrams are shared next.



The above flow diagram illustrates the working of ARIA.



The above flow diagram illustrates the flow of translation from one language to another.



The above flow diagram shows the flow involved with GenAI.

AI Control Tower

The AI Control Tower is a robust, secure activity integrated within the AgilePoint process model to augment workflows with dynamic, predictive, and generative AI capabilities. By seamlessly overlaying custom behavior onto existing processes, the AI Control Tower interacts with third-party AI prediction models—including Amazon SageMaker and Azure Machine Learning—to derive real-time insights and drive automated decisions. Additionally, the AI Control Tower seamlessly handles AI Agent integration and orchestration.

Secure Integration and Data Handling

All communications with external AI prediction and/or generation services occur over HTTPS, ensuring that data in transit is protected against interception and

tampering. The design guarantees that input data is processed entirely in-memory during the prediction and/or generation cycle. This transient processing model minimizes data exposure risks and supports stringent compliance with data security standards.

Configurable AI Engagement

The AI Control Tower is highly configurable, allowing users to define when and how to invoke external prediction or generation models based on specific activity events and conditional logic. Users can tailor the execution flow by setting up trigger conditions that determine the precise moments at which AI predictions should influence process behavior. Depending on the prediction outcomes, the system can automatically reroute flows, dispatch notification emails, or initiate other predefined actions, ensuring that processes remain agile and responsive.

Audit and Access Control

For enhanced security and traceability, all interactions—including input/output data, trigger conditions, action conditions, and any error logs—are meticulously recorded in the Audit Log. Access to these logs is strictly restricted to administrators and privileged users within the Runtime Management section of the Manage Center. This controlled access framework ensures that sensitive operational data is safeguarded while providing necessary transparency for security audits and compliance reviews.

Third-Party Trusted AI Service Provider's Legal Text

Sr. No.	Service	Link
1	Google	https://cloud.google.com/translate/data-usage#:~:text=Will%20the%20text%20I%20send,place%20for%20Google%27s%20Cloud%20Services.
2	OpenAI	https://openai.com/policies/row-terms-of-use/
3	OpenAI	https://openai.com/policies/business-terms/
4	OpenAI	https://openai.com/policies/privacy-policy/
5	Meta	https://www.llama.com/llama3/license/
6	Meta	https://www.llama.com/llama3/use-policy/
7	AWS	https://aws.amazon.com/service-terms/
8	AWS	https://aws.amazon.com/service-terms/#60._Amazon_SageMaker_AI
9	Qwen	https://huggingface.co/Qwen/Qwen2.5-32B-Instruct
10	Qwen	https://huggingface.co/Qwen/Qwen2.5-32B-Instruct/blob/main/LICENSE

AgilePoint NX on Third-Party App Stores

AgilePoint NX is available in the following third-party app stores:

- Apple iTunes store.
- Google Play Store globally and in China, multiple Android stores.
- Salesforce AppExchange.
- Microsoft AppSource for SharePoint for Microsoft 365 and its Chinese counterpart available from the Chinese version of the AppSource.
- Microsoft AppSource for Outlook.
- AgilePoint NX connector in Logic Apps, Power Automate and Power Apps.
- UiPath Marketplace.

These apps connect back to a live AgilePoint NX instance.

iOS App

AgilePoint NX is available in the Apple iTunes Store (https://itunes.apple.com/in/app/agilepoint-nx/id822086525?mt=8).

Privacy

Please read the privacy policy of the app.

Permissions

By default, AgilePoint NX app only checks for network.

- Network access.
- Camera (optional, required only if users use dynamic file upload).
- Location (optional, required only if users' needs map controls in eForms).

Data Storage and Management

The data stored on the mobile device by the app is within the app's sandbox space and managed by the OS. No other app will be able to access this data. The account information is encrypted and is stored in device memory. The security of this data may be compromised if an iOS device is "jailbroken" or "rooted." AgilePoint workflow and eForms related data comes from AgilePoint Server database using an API. Data is not cached in the device unless it is being used in the offline mode.

AgilePoint NX clears sign in data when users sign out, but other app configuration details are retained. When the user uninstalls the app, the offline cache of eForms files and log files are not deleted (not confidential data). AgilePoint eForms definition files are static files that do not have confidential data; however, if you use offline feature for individual apps, you can cache data for the eForms and tasks on the secured sandboxed space of the mobile app. Data being cached would depend on features used in the custom designed app. This is not a feature of the mobile app, but a specific implementation done on the AgilePoint platform by the customer. User-related data is stored in the secured app space.

Data Transmission

The information exchange between the AgilePoint Server and the mobile apps uses HTTPS. All AgilePoint-hosted environments are SSL protected using a TLS compliant certificate. Customers may build apps that need non-AgilePoint Server interactions such as authentication from other secure identity providers (Microsoft Azure Active Directory, Salesforce, G Suite, Okta, etc.). The apps may transmit or receive information, including files, with other external servers. This is not a feature of the mobile app. It is a specific implementation developed on the AgilePoint NX platform by customers.

Malware and Antivirus

The AgilePoint NX app is certified by the Apple iTunes store through AgilePoint's store account. AgilePoint does not use any third-party hosting. The store takes care of reviewing enterprise applications for malware features. AgilePoint has a virus-free policy and scans each release before pushing it to the app store.

Advertisement and Tracking

AgilePoint does not have advertisements (such as Google AdSense) incorporated in any of its products.

Android App

AgilePoint NX is available on the Google Play Store (https://play.google.com/store/apps/details?id=agilepoint.android.mobilebpm).

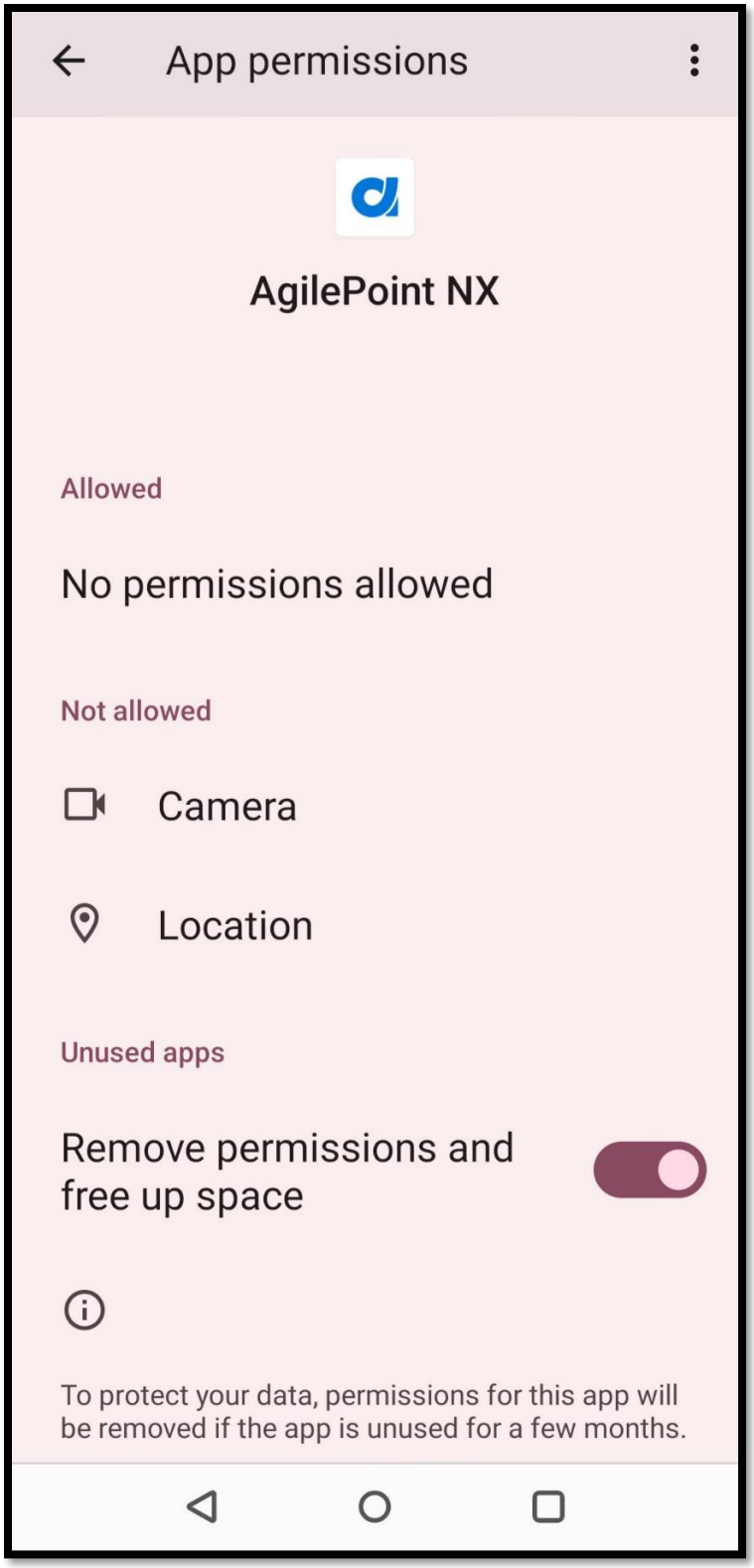
Privacy

Please read the privacy policy of the app.

Permissions

The list of permissions needed by the app is as follows:

- Network access.
- Read and modify the contents of your USB storage.
- Camera (optional, required only if users need to use dynamic file upload).
- Location (optional, required only if users require map controls in eForms).


App permissions
AgilePoint NX
Allowed
No permissions allowed
Not allowed
Camera
Location
Unused apps
Remove permissions and free up space
To protect your data, permissions for this app will be removed if the app is unused for a few months.

Data Storage and Management

The data stored on the mobile app is in a private storage unit. The Android OS protects the mobile app's data. This data will not be visible even on the computer when connected through USB. However, safety cannot be guaranteed if the android OS is rooted.

AgilePoint workflow and eForms-related data comes from an AgilePoint Server database using REST API. AgilePoint NX clears sign in data when users sign out, but other app configuration details will be retained. When the user uninstalls the app, the offline cache of eForms definition files and log files are not deleted (they are not considered confidential data). AgilePoint eForms files are static files. If the customer chooses to use offline feature for individual apps, then the app will cache data for the eForms and tasks on the secured sandboxed space of the mobile app. Data being cached depends on features used in the custom designed app. This is not a feature of the mobile app, but rather a specific implementation on the AgilePoint NX platform by the customer. User related data is stored in the secured app space.

Data Transmission

The information exchange between the AgilePoint Server and the mobile apps is based on HTTPS. All AgilePoint-hosted environments are SSL protected using a TLS compliant certificate. Customers may build apps that need non-AgilePoint Server interactions such as authentication from other secure identity providers (Microsoft Azure Active Directory, Salesforce, G Suite, Okta, etc.). The apps may transmit or receive information, including files, with other external servers. This is not a feature of the mobile app but rather a specific implementation developed on the AgilePoint NX platform by customers.

Malware and Antivirus

The AgilePoint NX app is certified by the Google Play Store through AgilePoint's account. AgilePoint does not use any third-party hosting. The Google Play Store reviews enterprise applications for malware features. AgilePoint has a virus-free policy and scans each release before making it available on the app store.

Certification

Certified by:

- ClassInd - All ages.
- ESRB – Everyone.
- PEGI - PEGI 3.
- USK - All ages.
- IARC Generic - Rated for 3+.
- Google Play Russia - Rated for 3+.
- Google Play South Korea - Rated for 3+.

IARC Certificate ID: 8afb4cad-f503-43fe-ba07-11c3483a0afe

Advertisement and Tracking

AgilePoint NX does not have Advertisements (such as Google AdSense) incorporated in any of its products.

Android App Stores in China

AgilePoint NX Android apps are available in the top android stores, including:

- Xiaomi
- Oppo
- OnePlus

Salesforce App

AgilePoint NX is available on the Salesforce AppExchange (https://appexchange.salesforce.com/appxListingDetail?listingId=a0N3A00000DqDRHUA3).

Sign-In Credentials

The AgilePoint NX Salesforce app works based on SSO. Identity management happens through HTTPS, driven under Salesforce's context. AgilePoint NX can access only the bearer token generated by Salesforce. This means, AgilePoint does not have access to the end user credentials, though the users are using the AgilePoint NX app on Salesforce.

Permissions

To use the apps, the authorized user only requires access to the AgilePoint features such as Work Center and apps. No other additional permissions are required. Access to other Salesforce apps and objects, is a custom development done by customers. It is not a feature of the app created by AgilePoint.

Data Storage

AgilePoint Workflow-related data is stored in the AgilePoint Server database. Any Salesforce entity created or edited by the AgilePoint NX App is part of the Salesforce database. Logs for Salesforce apps are stored in the Salesforce entity.

Malware and Antivirus

The AgilePoint NX app is certified by the Salesforce AppExchange through AgilePoint's store account.

Code Security Scan

AgilePoint performs regular runtime security code scans on its software. This is one of the key requirements to host an app in the Salesforce AppExchange. Apps listed in the Salesforce AppExchange must meet stringent code security scan requirements. For more information about the security scanning process, refer to https://developer.salesforce.com/page/Security_Review. AgilePoint runs the ZAP scanner test (https://security.secure.force.com/security/tools/webapp/zapbrowsersetup) with every release for Work Center, Manage Center and Forms rendering components that are rendered within Salesforce.

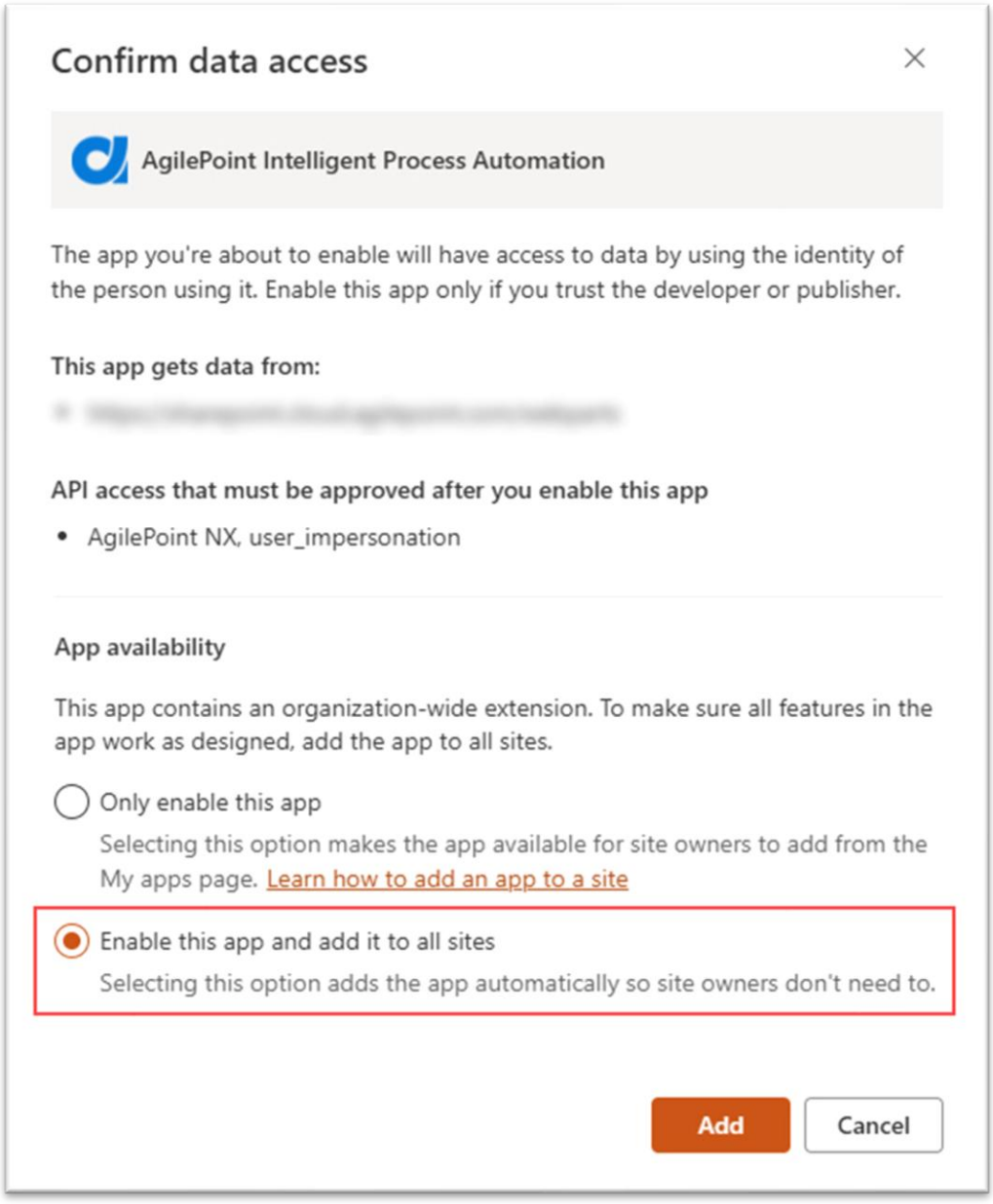
SharePoint for Microsoft 365 App

AgilePoint NX is available on the SharePoint Store (https://appsource.microsoft.com/en-us/product/office/WA200007669?tab=Overview .

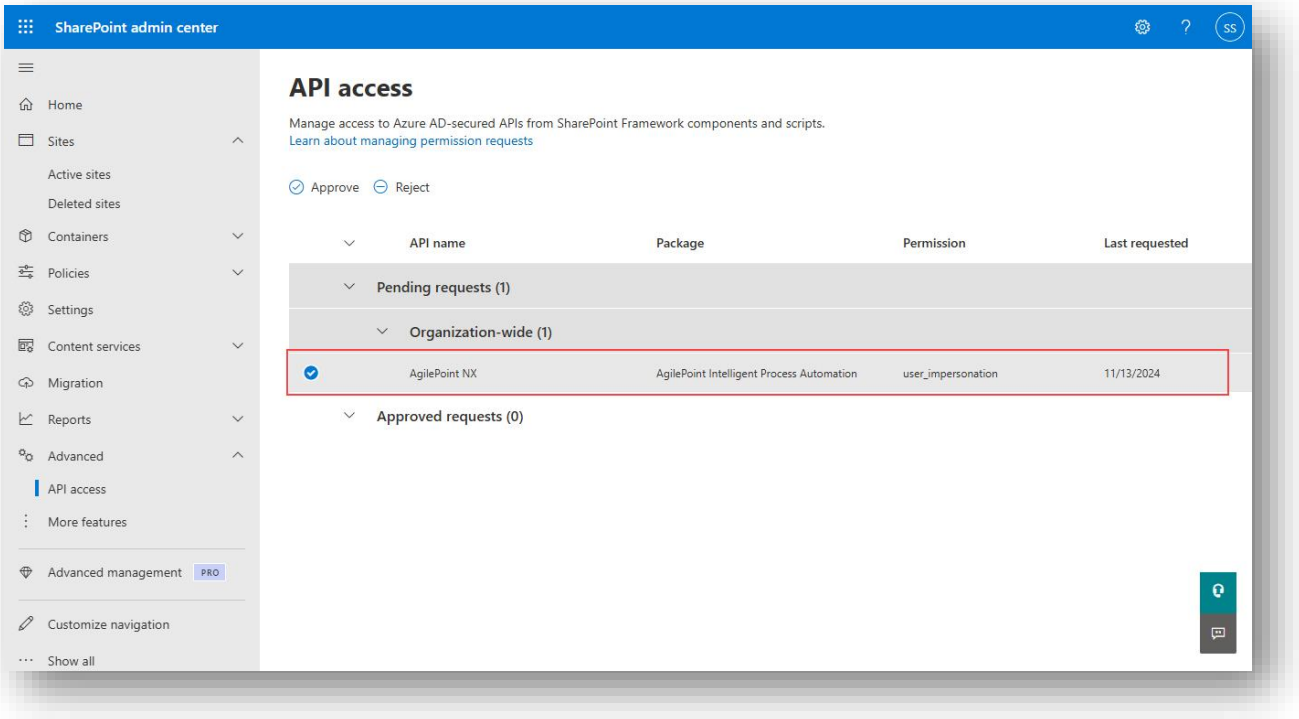
Permissions

AgilePoint NX Microsoft 365 app is a low trust app that is readily available in the SharePoint store. Permission to work at 2 levels:

- To install:
    - To add the AgilePoint Intelligent Process Automation app, one must be signed in to SharePoint as a Global Administrator.



- Approve the API Permission as shown above after enabling app.



- To use:
    - Add Work Center on a page: A user needs the "Edit" permission level, which allows them to actively manage and contribute content on the site, including creating, modifying, and deleting pages.

Data Storage

AgilePoint workflow-related data is stored in the AgilePoint Server database. SharePoint lists that are created or edited by an AgilePoint app reside in SharePoint, not in AgilePoint.

Outlook Task Manager App

AgilePoint NX is available on the Outlook Store (https://appsource.microsoft.com/en-us/product/office/WA104379838?tab=Overview).

Privacy

Please view the privacy policy of the app here.

Permissions

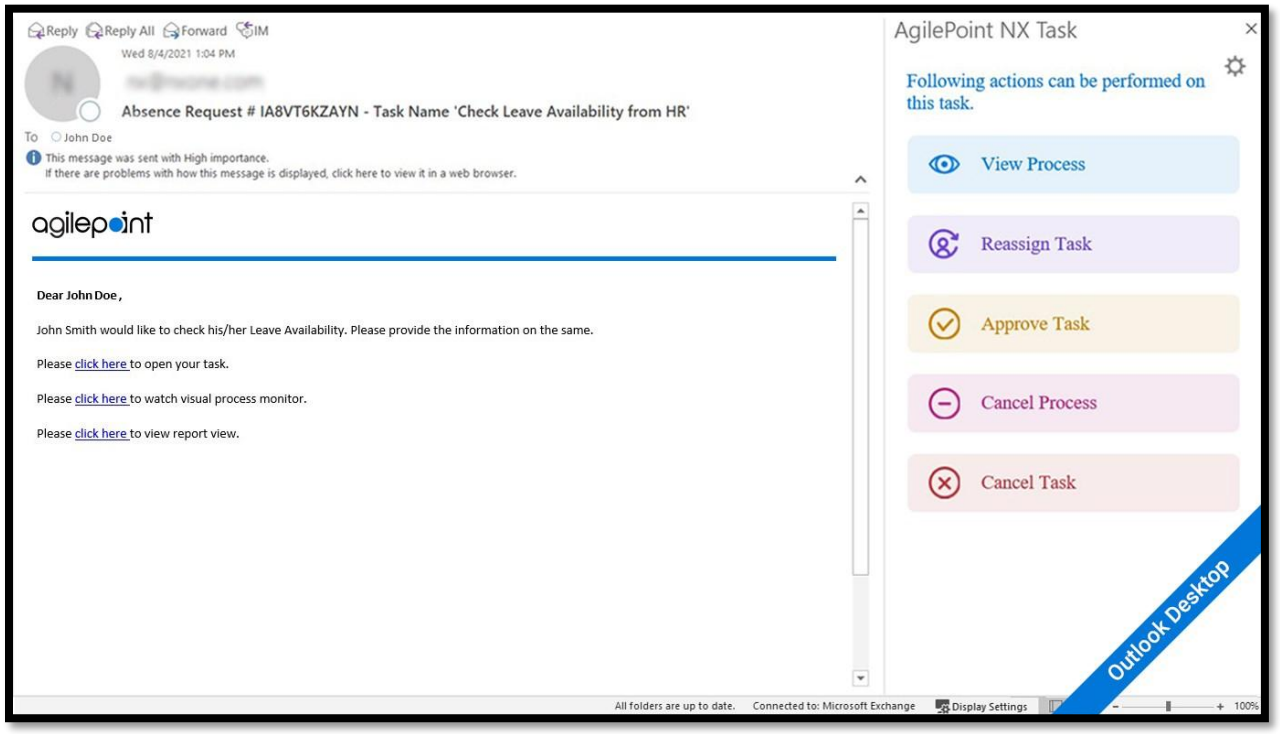
The app has the following permissions:

- It can read or modify the contents of any item in the mailbox and create new items.
- It can access personal information – such as the body, subject, sender, recipients, or attachments – in any message or calendar item.

Data Storage

The app does not have its own database. The data that is shown on the App UI is directly retrieved from AgilePoint Server using the REST API.

AgilePoint NX Task Manager for Outlook



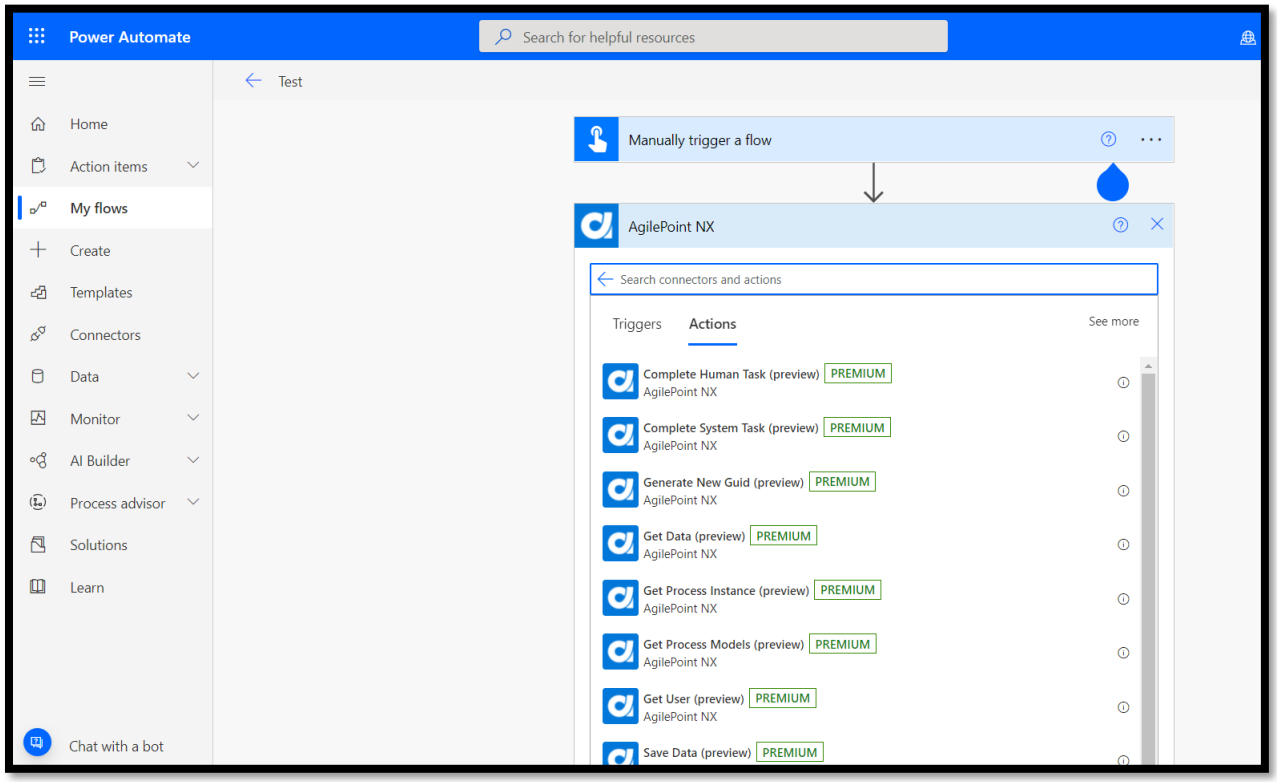
Data Transmission

Information that is transmitted is always to an AgilePoint Server. The Outlook app supports HTTPS. All AgilePoint-hosted environments are SSL protected and use a TLS compliant certificate.

AgilePoint NX Connector for Power Automate

AgilePoint NX is available in Power Automate, Logic Apps and Power Apps (https://docs.microsoft.com/en-us/connectors/agilepointnx/).

AgilePoint NX Connector for Power Automate



Privacy

This connector connects to the AgilePoint NX platform. Please refer to the product's privacy policy for more details.

Permissions

The connector does not need any specific permission. It depends on the permissions assigned to the Power Automate workflow where this connector is used.

Data Storage

The connector does not store any data. It is only a connector.

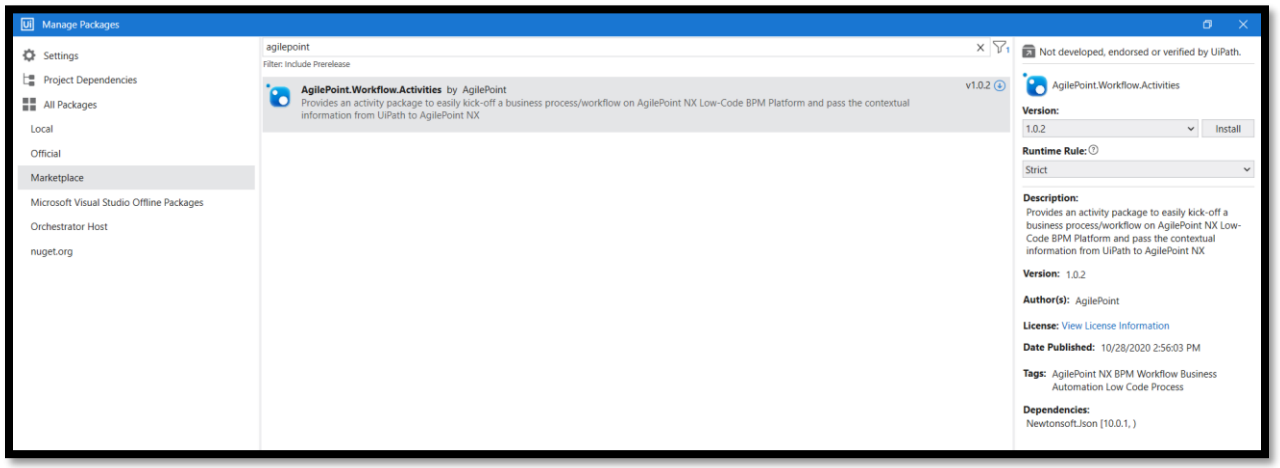
Data Transmission

All AgilePoint-hosted environments are SSL protected and use a TLS compliant certificate. Microsoft Power Apps are also SSL protected. So, all transmitted data is encrypted.

AgilePoint NX Activity for UiPath

AgilePoint NX is available under the name 'AgilePoint - Digital Process Automation Activity' in the UiPath Market Place. It provides an activity package to easily kick-off a business process/workflow on AgilePoint NX Low-Code BPM Platform and pass the contextual information from UiPath to AgilePoint NX. A UiPath developer can download the activity via the UiPath studio.

AgilePoint NX Activity for UiPath



Privacy

This is a custom activity which connects to the AgilePoint NX platform to kick off a business process. The UiPath developer defines what data to pass to AgilePoint NX. Please refer to the product's privacy policy for more details.

Permissions

The custom activity does not need any specific permission on the UiPath side. On AgilePoint NX side, permission to connect and initiate a process is needed.

Data Storage

The data stored on the AgilePoint NX server depends on what contextual data the UiPath workflow designer decides to pass to AgilePoint NX, while kicking off a business process.

Data Transmission

All the AgilePoint-hosted environments are SSL protected and use a TLS compliant certificate. So, all transmitted data to AgilePoint NX is encrypted.

Contact Us

To know more about security at AgilePoint, please feel free to reach us:

- Create a tech support ticket on Helpdesk.
- Email us at support@agilepoint.com.
- Based on your region – Call us.