Symphia NowForce

Security Information Note

For all versions

August 09, 2022

Introduction

In recent years, advancements in technology have changed the way we think about security and cloud-based solutions. While on-premise solutions have been the standard for data security and privacy, cloud-based solutions have rapidly closed the gap, ensuring your data stored on-premise or in the cloud, is always secure and protected using the latest tools available.

Symphia NowForce's cloud-based environment encompasses multiple state-of-the-art security tools and implements best practices to accommodate Information Security and Privacy concerns. Cognyte has devoted extensive resources to ensuring security and privacy concerns drives every part of our development process as well as keeping our cloud infrastructure networks and services protected.

In this document we will review how Symphia NowForce cloud service is protecting your data and privacy. Additional information is available in the links below:

- Symphia NowForce's Information Security and Privacy practices: https://intercom.help/nowforce/en/articles/62902-nowforce-security-controls
- Information about AWS security controls: https://aws.amazon.com/security
- Presentation deck with more details can be received upon request.

ISO Certification

As part of our commitment to information security, Cognyte implements globally certified security controls ISO 27001:2013 and ISO 27799:2016, the global benchmarks for managing information security.

For more information, see Cognyte ISO Certificates.

Data and Privacy Policies

Cognyte has clear and transparent Data Processing Agreements and Privacy Policies, for more information see:

- Cognyte Global Privacy Policy
- Data Processing Agreement

Security Controls

This section describes the Symphia NowForce security controls implemented for all NowForce Mobile App customers.

Security Control Processes

- Routine Antivirus scans (the antivirus is constantly updated).
- Amazon Web Application Firewall (WAF) - Protects from DDoS and XSS attacks.
- Continuous security updates to patch known vulnerabilities of operating systems and third-party software.

Application Security

Cognyte follows industry-standards of software development best practices and has implemented the following:

- All of our development employees are trained with Microsoft SDL practices.
- Routine vulnerability assessment and penetration testing of all software under development.
- Static code analysis is routinely undertaken.

Data Control

Your data is always protected, whether when you're sending data or when the data is stored. Data encryption is provided as standard in-transit and at-rest.

- Data-in-transit encryption - SSL/TLS encryption 1.2 for all communications.
- Data-at-rest encryption - Based on state-of-the-art encryption algorithms (available for SaaS customers).

Access Control

Privileged access to all systems is controlled and monitored. User access to data and systems is carefully managed and controlled, based on the least privilege settings.

Controls include:

- Cognyte administrators use multi-factor authentication for access to the cloud production environments.
- Access to NowForce API uses OAuth 2.0 authentication.
- Customer access control management.

Enabled as default:

- Unique credentials
- Login audit
- Mobile device unique ID (allow blocking/disabling of unauthorized users)

Optional configuration (per customer):

- Strong passwords enforcement
- Multi-Factor Authentication (MFA)
- OAuth 2.0
- IP Range lock
- Single device login

Privacy Controls

Privacy controls enable the organization to oversee which information is being captured and where. The customer organization is the "data controller" and decides on the collected data. Cognyte is the "data processor".

Data collection

Depending on the organization's policy and requirements, the following data can be collected:

- Incident related data (forms data, text, video, voice, images etc.)
- Location data is managed and controlled by the customer.
  - Customer administrator can select if and under which cases the location of the mobile device is shared (role based).
  - User location sharing status is transparent to the user on his mobile application. A user can turn off location sharing settings, or change the mobile application to offline mode.

Data retention

Data retention on behalf of client organizations includes:

- Routine location - up to 3 months.
- Personal data, incident information and location - can be deleted on request.
- Deletion of retained data is done when the SaaS period ends (data is available upon customer request).

Frequently Asked Security Questions for Symphia NowForce

Data Collection and Retention

Q: Is Symphia NowForce ISO certified?

A: Yes. Symphia NowForce has a ISO 27001 certificate, you can view the certificate here.

Q: Is Symphia NowForce GDPR compliant?

A: Symphia NowForce adheres to GDPR guidelines including data privacy measures, user privacy rights and access rights to the system, but does not have an official GDPR compliance certificate.

Q: Where is Symphia NowForce SaaS client data stored?

A: Client data is stored in three locations: MS SQL data is stored on AWS; Mongo data is stored on Atlas and raw data is stored on AWS S3.

Q: How are Symphia NowForce's WebAPI logs monitored?

A: AWS CloudWatch is used for logging and monitoring of WebAPI logs.

Security Controls

Q: Does Symphia NowForce utilize validation on XML and XSL imports, or make use of a white list input?

A: We use WAF with XSS policies to prevent malicious XML inputs; in addition, the Symphia NowForce API utilizes XML and with an enforced white list input.

Q. How is Symphia NowForce protected against SQL Inject attacks?

A: We use WAF with relevant policies and use Veracode to scan our code for threats.

Q: What measures are in place to prevent cross-site scripting (XSS) attacks?

A: Symphia NowForce makes use of WAF with relevant up to date policies. In addition, an external company runs annual penetration tests including testing for XSS vulnerabilities.

Application Security

Q: What security analysis is run during development of Symphia NowForce products?

A: We use Veracode to run Penetration Static Code Analysis during the development process of every version of our product.

Q Are the outcomes of routine penetration tests and vulnerability scans documented?

A: Yes, reports of testing is managed internally, and can be requested from the Customer Success team.

Q:Does Symphia NowForce use any RFC (RFC6749, RFC6750, etc) for authentication?

A: Yes, RFC 6749 is the core OAuth 2.0 framework which is used by NowForce for authentication.

Access Control

Q: What user authentication measures are used by the Symphia NowForce API?

A:OAuth 2.0 is used.

Q:Are all connection attempts monitored?

A: Yes, these are logged and stored.

Data Control

Q: What encryption is used for secure communication?

A: Data-in-transit encryption uses SSL/TLS 1.2 and data-at-rest encryption is used to encrypt all DB data.

Q: What encryption is used for secure communications between Symphia NowForce and third-parties?

A: We use OAuth 2.0 for authentication, and SSL /TLS 1.2 for all communications between the Symphia NowForce API and third-parties.

Q: Do we utilize data obfuscation for data transfer?

A: No, we make use of TLS as the encryption mechanism for secure communications. The encryption provided by the TLS is more robust than data obfuscation, providing better protection, confidentiality and data integrity.