CONNX SECURITY OVERVIEW

ConnX is a web-based application that can be installed in a variety of technical environments.

The purpose of this document is to advise you on the security aspects provided as part of the ConnX suite and additional optional security aspects you should consider if you are installing ConnX within your own server environment (either on-premise or private cloud) or hosting ConnX via a hosting partner.

IT security is constantly evolving and changing. As such, we at ConnX Pty Ltd are always refining and updating our security practices.

Related Information

This document should be read in conjunction with the ConnX Technical Specification document for a complete understanding of the environments, systems, and security aspects.

Please refer to http://connx.com.au/privacy for more information about our privacy policy.

This document was last reviewed in March 2024.

THE CONNX SUITE

ConnX has multiple software components, namely:

1. Main ConnX solution including:
    a. ASP.NET web application;
    b. Microsoft SQL Server database; and
    c. A Windows Service for scheduled background tasks.
2. Optional ConnX Careers module.
3. Optional 3rd party products such as Crystal Reports and Yellowfin BI, which are embedded as modules within the main ConnX solution.
4. Optional 3rd party products integrated to the main ConnX solution, namely Onboard Centre, requiring ConnX Web Service component for full integration.

5. Additional components for integration between ConnX and SEEK.com.au.

This document specifically discusses the situation where the main ConnX solution is installed within your own server environment (either on-premise or private cloud) or you are hosting ConnX via a hosting partner.

The ConnX Careers and Onboard Centre modules are only offered as cloud solutions.

CONNX DIRECT INVOLVEMENT IN SECURING YOUR INFORMATION

This document details how ConnX Pty Ltd secures the ConnX application on behalf of clients. The design and development of the ConnX application and database are controlled by us. As such, ConnX manages the following items:

1. Application Security (e.g., login and passwords)
2. Database Security (e.g., encryption of data at rest)
3. Application Penetration testing
4. Data Breaches

1.0 APPLICATION SECURITY

1.1 Login Security and Passwords

- All users are required to login to ConnX with a username and password.
- If configured by you, password complexity rules for "strong passwords" are easily enforced.
- Employees must be "activated" before they can login. Activation can be by either the System Administrator, HR Administrator, or Manager, depending on how you configure your instance of ConnX.
- If configured by you, an email can be sent to a user as part of the activation process with a strong temporary password. The user must create their own password when they first login to ConnX.
- ConnX has an inactivity timeout setting of 20 minutes by default, with a warning message shown after 19 minutes. Inactivity after this time will automatically logout the current user. You can change this timeout duration to be shorter or longer depending on your requirements.

1.2 Single Sign On / Same Sign On (SSO)

Available for clients with on-premise installations, ConnX can be configured by you for Single Sign On or Same Sign On.

Single Sign On bypasses the login page and logs the user in with the same credentials they used to login to Active Directory.

Same Sign On shows the Login page in ConnX but authenticates the user against Active Directory instead of their ConnX username/password.

SSO is only available for on-premise installations of ConnX. In both cases, ConnX is authenticating user credentials to Active Directory to obtain a 'pass' (successful username/password combination) or 'fail' only and not using any other components of Active Directory.

1.3 SAML 2.0

Available for all clients, SAML 2.0 login authentication is available if you have a cloud based SAML identity provided such as Azure Active Directory or others like it.

You must configure ConnX and your SAML Identity Provider for this feature to be enabled.

1.4 Two Factor Authentication (2FA)

Available for all clients, 2FA login authentication is available via a Time-based One-time Password (TOTP) process via an authenticator app (e.g., Microsoft Authenticator). 2FA applies to both the desktop and mobile login screens.

You must enable this feature within your ConnX system if you wish to use it. 2FA can be applied to individual user accounts that you select.

1.5 Security Groups and Permissions

- There are seven primary security groups, as shown below:

1. System Administrator
2. Restricted System Administrator
3. HR Administrator
4. Restricted HR Administrator
5. Manager
6. Supervisor
7. Employee

- The following modules of ConnX also have additional security: Recruitment; Learning & Education; Performance Reviews; Work Health & Safety; Reports Manager; and Business Intelligence.
- There are many settings within the ConnX system to restrict access to information within the Supervisor, Manager, and other "restricted" security groups.

1.6 Email (SMTP Server)

You can configure Email within ConnX to be sent over Transport Layer Security (TLS) through the ConnX "Use SMTP Authentication" option. Typically, this uses an SMTP server that is within your control and configuration.

1.7 Email (via SendGrid Email Transaction Service)

You can configure Email within ConnX to be sent using the SendGrid email service (sendgrid.com). SendGrid is a trusted and reliable provider of email services globally. Emails will be sent via a SendGrid account created and maintained by ConnX Pty Ltd. However, you are able to configure your own custom email domain to personalise your emails for your organisation. SendGrid have their own security protocols and policies, which can be found at sendgrid.com/policies/security/

1.8 ConnX Modules

Please refer to the ConnX Technical Specifications for more information about the following modules:

- Mobile
- Business Intelligence
- Careers
- Onboard Centre
- Timecard with Award Interpretation
- Web Services
- Recruitment

1.9 Careers and Onboard Centre Modules

These modules are cloud hosted only.

Additional security is therefore required from ConnX, which includes:

- Data sovereignty – all data is held in Australia;
- Data transmission encryption – all data is encrypted in transmission under HTTPS. This is the only transmission protocol enabled on the server;
- Data access – only appropriately qualified ConnX personnel with a need to access data on the server are provided access. ConnX does not sub-contract these services;
- Process for accessing data – access to all production databases is only performed after approval from the Client Services Director. All access is logged;
- Data backups & access to backups – a differential backup is performed hourly during working hours and a complete backup is performed nightly. Access to all backups is restricted to only those that need it;
- Data breaches – please refer to the Data Breaches section below for more information.
- Software upgrades/updates – ConnX follows a strict process of performing software upgrades, which includes complete separation of development, quality assurance, user acceptance testing, pre-production, and production environments.

1.10 ConnX Cloud Communication Broker

This service is optional and is used by clients who cannot create a webhook subscription with SEEK directly from their own environments.

This service is cloud hosted only and follows all the same principles as Careers and Onboard Centre above.

2.0 DATABASE SECURITY

2.1 Database Authentication/Authorisation

ConnX uses a Microsoft SQL Server database. If you have ConnX installed on-premise, you may configure the SQL Server and database to restrict access only to required users. If you have ConnX in a cloud hosted environment, authorisation to the ConnX database will be managed by the cloud provider.

2.2 Data Encryption

Sensitive data in the database is automatically encrypted, so even if access to the database was achieved, the data cannot be read or interpreted.

This sensitive data includes:

- Tax file numbers;
- Pay advices;
- Payment summaries;
- Bank account details;
- Passwords; and
- Rates of pay (if configured by you).

2.3 Auditing

If configured by you, many of the database tables can be audited for changes. The change, date/time, and the user who made the change are all recorded and held for a duration that is set by you.

3.0 PENETRATION TESTING

On each major upgrade, ConnX Pty Ltd engages a 3rd party security specialist organisation to perform a series of up-to-date security tests and report their findings.

All tests are performed 'black box' as a public profile accessing the various ConnX sites.

ConnX always makes sure that the solution meets our security policy before we release to clients.

You may request our latest security certificate by contacting our Support team.

4.0 DATA BREACHES

ConnX Pty Ltd is bound to comply with Australian Privacy Principles (APPs). The APPs include when and how to address real and potential data breaches, and ConnX follows the practices that are set out in these documents.

YOUR INVOLVEMENT IN SECURING YOUR INFORMATION

Security of the server, network, and devices that access ConnX are your responsibility. We strongly recommend that you discuss your specific security requirements with your IT department and/or hosting provider.

The following sections outline some of the items you may wish to consider as part of the security review of your server and network.

1.0 DATA TRANSMISSION SECURITY

Data can be encrypted in transmission under SSL/TLS. This is done on the server by yourself (if installed on your own server environment) or your hosting partner. We strongly recommend that you use SSL/TLS to encrypt data in transmission.

2.0 SERVER AND ENVIRONMENT SECURITY

ConnX is an ASP.NET application that runs on Internet Information Server (IIS). IIS has two standard security features that can benefit ConnX security. Both are optional.

1. Directory Security – Domain Authentication

   Used to only permit users who are currently members of the Windows Domain to access and run ConnX (i.e., currently logged on to the network).

2. Secure Sockets Layer (SSL)/ Transport Layer Security (TLS)

   Used to encrypt the page sent by the server to the client. Requires a valid certificate for encryption that must be installed on the web server.

2.1 Server Hardening

ConnX has included some foundational server hardening via HTTP response headers at the website level, e.g., the prevention of cross-site scripting.

3.0 ADDITIONAL RECOMMENDED ITEMS

- Apply IIS server hardening techniques, such as:
    - Additional hardening for your HTTP response headers;
    - Block any ports not required by the server or ConnX; and
    - Keep your IIS server behind a firewall.
- Run the ASP.NET worker process using a Domain service account.
- Configure Employee Documents in a separate Documents Database with encryption.
- Configure email sending to use authentication.
- Configure a robots.txt to stop search engine crawlers from indexing your ConnX site and prevent it from appearing in search engine results.

Document Revision History

Date	Author	Section	Description of Change
1/05/2018	GS	All	Published
18/09/2018	RW	All	Update site security
16/04/2019	RW	All	General review
22/01/2020	BK	All	General review
24/09/2020	NK	All	General review
11/03/2021	NK	All	General Review/Update to include SAML
13/07/2021	NK	All	General Review
09/02/2022	NK	All	General Review

25/05/2022	NK	All	General Review
29/03/2023	BK	All	General Review and addition of 2FA
26/04/2023	JD	All	General Review
28/03/2024	BK	All	General Review