CONNX TECHNICAL SPECIFICATIONS

FOR CONNX V6.6

ConnX Pty Ltd
Level 8
303 Coronation Drive
MILTON QLD

PO Box 1122
MILTON QLD 4064
AUSTRALIA

Ph: 1300 CONNXHR
1300 266 694
Intl: +61 7 3368 2623
Web: www.connx.com.au

Ref: ConnX Technical Specifications V6.6.docx

TABLE OF CONTENTS

1.0 CONNX TECHNICAL SPECIFICATIONS

ConnX is a web-based HR and employee self-service program which can be installed in a variety of technical environments. Users access ConnX via a web browser. This document aims to advise you on supported environments and considerations you should make when determining the correct environment.

1.1 Overview

The ConnX program has several core server-based components and other optional components.

The core components are:

- A Microsoft SQL Server for the ConnX database(s)
- A Microsoft IIS server for the ConnX web application(s)
- A Microsoft Windows Service which performs background tasks
- Microsoft .NET Framework 4.8 (supplied by ConnX)
- Microsoft .NET Core 6 Runtime & Hosting Bundle (v6.0.32) (supplied by ConnX)
- Microsoft IIS URL Rewrite Module 2 (supplied by ConnX)
- IIS configuration for the ConnX Background Worker
- An interface to send email to the mail server (SMTP Server settings)

Depending on your requirements and optional add-on modules, you may also require:

- Microsoft OLE DB Driver for SQL Server Setup installed on the IIS server (supplied by ConnX)
- Integration or interface to your payroll system
- Additional Windows Services to support other features such as further ConnX modules and integration with other applications.
- Additional configuration to support Single Sign On or Same Sign On
- Additional mailbox and firewall rule changes to enable secure connections external to the domain.
- Reconfiguration of firewalls and an SSL certificate (not supplied by ConnX) for external or mobile access.

- Additional IIS configuration for the ConnX Web Service
- Crystal Reports runtime installed on the IIS server (supplied by ConnX)
- If sending emails via SendGrid, configuration of your domain to allow access to SendGrid.

1.2 Key Questions to Determine Your Correct Environment

Determining the correct environment for your installation depends on several elements, including:

- Do you have a current server environment to support ConnX?
- Which modules of ConnX your organisation is purchasing.
- Do you want your users to be able to access ConnX from outside the network?
- The server your current payroll system is installed on.
- Do you wish to integrate with an external application?

1.3 ConnX Security Overview

Please refer to the ConnX Security Overview document for more information about the security aspects that are provided as part of the ConnX suite and additional optional security aspects that you should consider if you are installing ConnX within your own server environment or hosting ConnX via a hosting partner.

The latest version of the ConnX Security Overview document is available via the following link:

http://www.connx.com.au/files/ConnX Security Overview.pdf

1.4 Authentication

By default, ConnX is configured so that users have their own username and password which is maintained directly in ConnX. Depending on your ConnX installation and configuration you can configure either Single Sign On, Same Sign On or SAML 2.0 authentication. This can be further enhanced by applying two-factor authentication to any of these primary authentication methods.

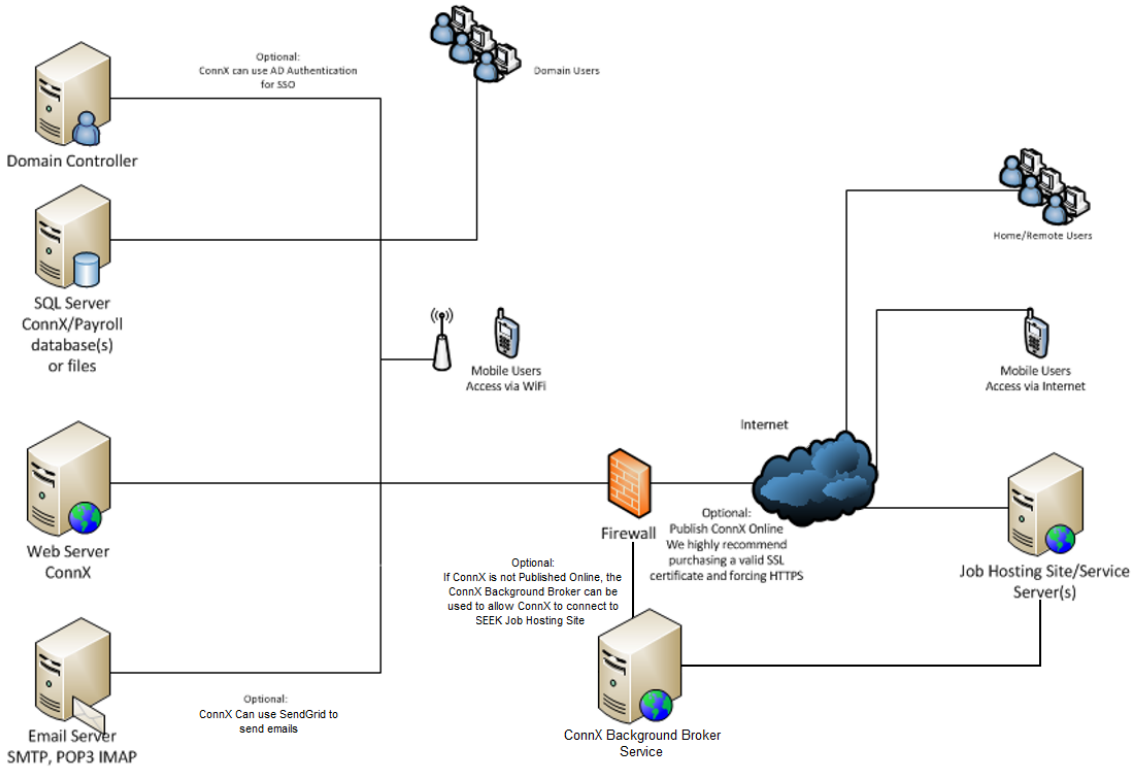
1.4.1 ConnX Background Worker

The ConnX Background Worker is a software communication layer between the user interface and background processes. The ConnX Background Worker is a mandatory core component of the ConnX solution and if it is not operational you might find that many features will not work as expected.

2.0 POSSIBLE ENVIRONMENT CONFIGURATIONS

2.1 ConnX on a Domain or Private Cloud

In this scenario, ConnX is installed into an existing network environment either onsite or in an existing private cloud. The following diagram shows how ConnX may interact with the other elements of your current environment.



2.1.1 Determining Single or Multiple Servers for Web (IIS) and SQL

You would be more likely to have SQL and Web on separate servers in the following conditions:

- You already have an SQL Server with other databases.
- You want to publish ConnX to the Internet.
- You want to keep your databases separate from the IIS server for greater security.

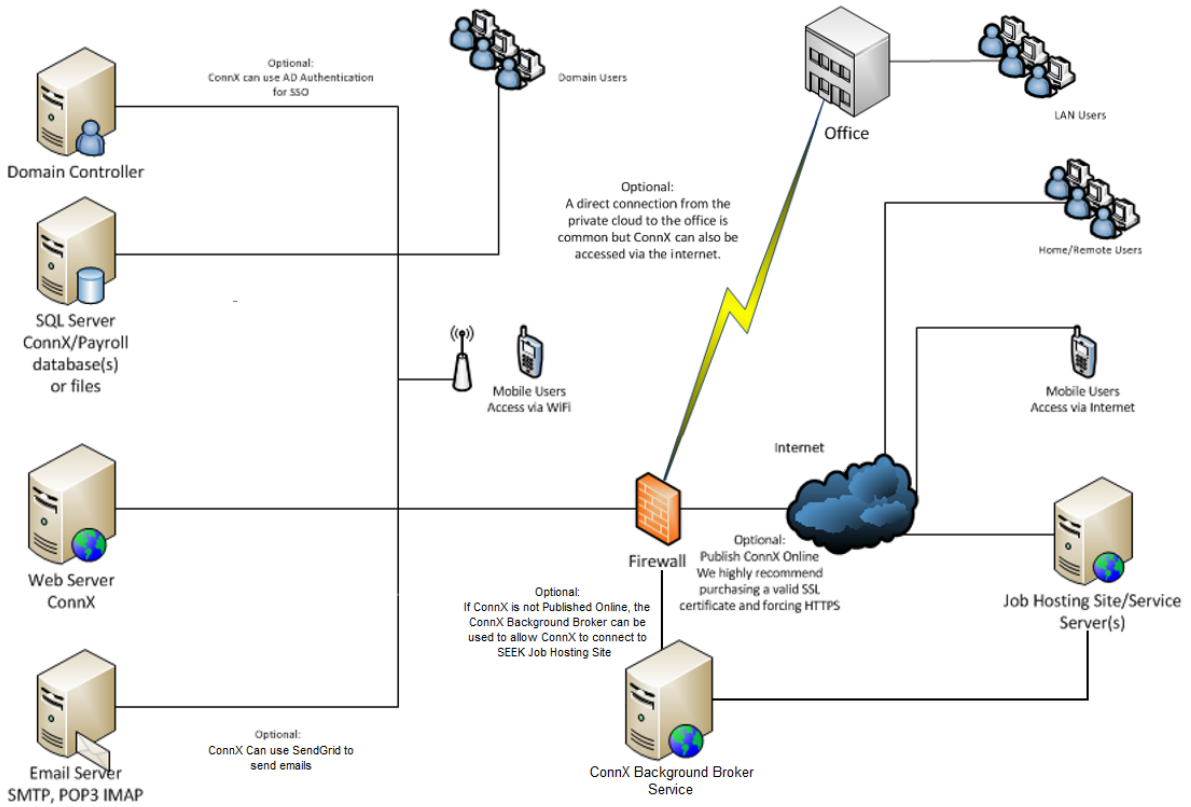
You are more likely to have SQL and Web on the same server in the following conditions:

- It is a new setup, and you want to keep it separate from all other servers.

- You do not have many servers and want to keep it that way.
- Users only get access to ConnX on a LAN.

2.2 Hosted SaaS or Hybrid Cloud

In this scenario, ConnX is installed into a hybrid cloud or hosted SaaS environment. The following diagram shows how ConnX may interact with the server and user elements. Please note that there may be some limitations to the functionality of Single Sign On authentication which requires access to an Active Directory server.



2.2.1 Determining if You Want ConnX in a SaaS or Hybrid Cloud Environment

ConnX is most likely to be hosted in a SaaS or hybrid cloud environment in the following conditions:

- You have remote staff that require access to ConnX from non-company locations.
- You want to publish ConnX to the internet, but not from your network.

- You do not want to worry about updating, maintaining, or implementing security for your ConnX/payroll server(s) operating systems.
- You do not want your IT staff to have access to the ConnX/payroll server(s).

3.0 CONNX MODULES AND OPTIONAL CONFIGURATION

Additional modules or features of ConnX may affect the configuration of the server environment.

3.1 Single Sign On

Single Sign On, meaning no username or password is required to access pages in ConnX, requires the IIS server to have a "link" to the Active Directory. Users accessing ConnX on the same domain as the IIS server will not be prompted for a username/password, and users accessing ConnX from outside the domain are prompted for a username/password via the browser.

NOTE

This option will only be available if your ConnX IIS Server has access to your domain.

3.2 Same Sign On

Same Sign On means the user is prompted to enter a username and password and enters their Active Directory credentials to access pages in ConnX. The ConnX IIS server must be on the same domain and requires access to a domain controller to be able to use Same Sign On for authentication.

NOTE

This option will only be available if your ConnX IIS Server has access to your domain.

3.3 Security Assertion Markup Language (SAML)

SAML is becoming the preferred method of authenticating to multiple applications without the need of multiple usernames and passwords. ConnX supports SAML 2.0.

NOTE

SAML 2.0 also means that your ConnX IIS Server does not need to be on the same domain as your domain controller.

The ConnX IIS Server will need https access to your SAML identity provider though.

All ConnX clients have the option to use this feature.

3.4 Two Factor Authentication (2FA)

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. There is no technical configuration required, only enabling and configuring the feature within ConnX itself.

NOTE

All ConnX clients have the option to use this feature.

3.5 Document Storage

A variety of documents can be stored within the ConnX solution.

We recommend these documents be stored within a secondary SQL database however, everything can be stored in the primary ConnX database if desired.

Some documents can still be stored on the file system if desired.

To configure documents to be stored in the database, you need a folder for temporary documents and a user account that has modify permissions for that folder.

3.6 Sending Email

3.6.1 SMTP Server - Unauthenticated email (internal email server)

ConnX requires access to an SMTP Server to send email. The unauthenticated email set is usually used if you have your own email server internally on your domain. To utilise this configuration your Email Server must have "relay" enabled from the ConnX IIS Server if you are sending emails external to your domain.

3.6.2 SMTP Server - Authenticated email (Internal, Microsoft 365, G Suite etc.)

The authenticated email configuration can be used for an internal email server but is generally used with Microsoft 365, G Suite or other external email providers.

If you are using authenticated email one of the following will be required, to authenticate against the server sending emails.

- Internal domain will require a full AD user account.
- Microsoft 365 an E3 account or G Suite it will be a basic account.
- Microsoft 365 accounts will need basic authentication enabled on the tenancy to work. If the account was created after 30/06/2021 a ticket to Microsoft support may be required to enable this feature.

NOTE

Depending on modules in use and configuration selections up to three (3) additional email accounts may be required.

3.6.3 SendGrid

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. Details for DNS record updates are created and provided during the configuration setup process within ConnX.

This interface is achieved using the standard SendGrid API. Port 443 must be open to enable the HTTPS protocol.

The SendGrid integration requires access to https://api.sendgrid.com/v3/

3.7 Payroll Integration

3.7.1 For MicrOpay Payroll

Integration between ConnX and MicrOpay payroll requires:

- SQL Databases to be either on the same SQL instance or linked SQL Servers.
- File Transfers for the import of transaction records from ConnX to MicrOpay.
- MicrOpay Service (supplied by Micropay) to be installed and able to connect to all MicrOpay databases and the ConnX database.

3.7.2 For HR3 Payroll

Integration between ConnX and HR3 payroll requires:

- SQL Databases to be either on the same SQL Server or linked SQL Servers.
- File Transfers for the import of transaction records from ConnX to HR3pay.
- HR3 Web Services component (supplied by HR3) installed and configured.

3.7.3 For other payroll systems

A file-based import/export is used. These files can either be uploaded to and download from a static folder on the ConnX IIS Server, or a ConnX Admin user can upload/download them to the ConnX applicaton via their PC.

3.7.4 Additional payroll vendor components/modules

Payroll integration may rely on the payroll software vendor installing additional software. You should check with the payroll vendor on any additional requirements.

3.8 SAP Litmos

SAP Litmos is a popular Learning Management System used by many organisations. ConnX has the ability to interface with Litmos and allows ConnX to register employees into your Litmos system and also active (and de-active) their Litmos accounts as necessary.

This interface is achieved using the standard Litmos API. Port 443 must be open to enable the HTTPS protocol.

3.9 Recruitment Module

The ConnX Recruitment module can automatically post jobs to external job boards (such as SEEK) and automatically accept applications from candidates back into ConnX. To support these features additional configuration is required on the servers, including:

- Firewall configured to allow ConnX access to send data to various job sites via the internet (this depends on where you publish your job ads).
- Relay enabled on the email server from the ConnX IIS Server (ConnX may be configured to reply to candidates via email automatically, and the recruitment team can correspond via email to candidates within ConnX, so emails are sent externally to your domain).
- There may be other requirements based on interactions with other related systems (e.g., ConnX Careers, SEEK etc) which are outlined below.

3.9.1 ConnX Careers

ConnX Careers provides the job advertising from ConnX viewable from your website. ConnX Careers is hosted only on connxcareers.com and typically configured as https://YourCompany.connxcareers.com. ConnX Careers will be styled and themed to appear like it is part of your website.

To use ConnX Careers successfully, you need to:

1. Provide a link from your website to ConnX Careers so users of your website can view and apply for jobs.
2. Open a port on the firewall so ConnX can communicate to ConnXCareers.com.

ConnX will push jobs to your ConnX Careers site via the ConnX Careers web service.

Applicants are retrieved by the ConnX Automated Process Service from ConnX Careers on a set interval. Port 443 must be open so that ConnX can use the HTTPS protocol.

3.9.2 SEEK

SEEK is a well-known job site within Australia. ConnX interfaces with SEEK to send vacancies to be published on the SEEK job site and also to receive data from applicants who apply on the SEEK website.

The SEEK API is a solution involving an API over HTTPS and webhook notifications. The API is used to send and retrieve data to/from SEEK. Webhook notifications are used so that SEEK can tell ConnX when an event has occurred on its site (e.g., an applicant has applied) so that ConnX can action that event if needed (e.g., retrieve the applicant's details).

Requirements:

- Port 443 must be open to enable the HTTPS protocol.
- Multiple SEEK URLs may need to be allow-listed (see section below for details)
- SEEK JavaScript file may need to be allow-listed (see section below for details)
- ConnX Background Worker will need to be public facing on the internet and under HTTPS in order to receive webhook notifications from SEEK. If this is not possible, then you have the option of using the ConnX Cloud Communication Broker as discussed below.
    - Communication Broker URL may need to be allow-listed (see section below for details)
    - Port 443 must be open so that ConnX can use the HTTPS protocol.

3.9.3 Broadbean

Broadbean is a separate system used to interface with many job boards all over Australia and the world. Broadbean can be set up within ConnX to advertise vacancies automatically to several job boards at the same time.

To use Broadbean with ConnX, you must have:

1. the ConnX Recruitment module

2. a ConnX Careers account

3. a Broadbean account

ConnX will push jobs to your Broadbean account via the Broadbean website, but the Vacancy must first be advertised on ConnX Careers. Port 443 must be open to enable the HTTPS protocol.

ConnX receives applicant data either from the job board via email or directly from ConnX Careers if you want to add additional features such as screening questions.

3.9.4 ConnX Cloud Communication Broker (optional)

The ConnX Cloud Communication Broker is a service offered by ConnX Pty Ltd for clients that have ConnX installed on their servers (called 'on premise') who do not have ConnX available and secure on the internet. If you do not have ConnX Recruitment, you do not need to worry about this.

When a candidate applies for a job on SEEK directly, SEEK now needs to tell ConnX that a candidate has applied, so that ConnX can retrieve the application. SEEK sends this information via a webhook notification. If your ConnX system is not on the internet or properly secure, SEEK cannot communicate directly to your ConnX system for this function, because a webhook notification will not work under this situation. This is what the ConnX Cloud Communication Broker is for. SEEK will send the *notice* of an application to the Communication Broker, and ConnX will retrieve this notice from the Communication Broker rather than from SEEK. The Communication Broker is acting as a middle-man to receive notices from SEEK, and pass them onto your ConnX system. Note that there is no applicant or vacancy information transferred to or stored in the Communication Broker database.

Requirements:

- Communication Broker URL may need to be allow-listed (see section below for details)
- Port 443 must be open so that ConnX can use the HTTPS protocol.

3.10 Onboard Centre

Onboard Centre is an onboarding solution, which is only available as a cloud solution. Whereas ConnX is available most typically as an on-premise solution but also available via ConnX's partner hosted environments.

Where ConnX is on premise

Where ConnX is installed on premise (meaning installed on servers within your control), you may need to adjust your firewall rules to allow seamless integration.

Where partners host ConnX

Where ConnX is hosted with a partner provider, ConnX and the partner manages the integration between ConnX and Onboard Centre.

ConnX to Onboard Centre integration

In ConnX, users will create a 'new starter' with basic details and trigger the onboarding process to the cloud. ConnX IIS server requires outgoing access to the Onboard Centre web service located on the Onboard Centre server. ConnX communicates to Onboard Centre over HTTPS/SSL only.

Onboard Centre to ConnX integration

In Onboard Centre, users will accept their employment agreement and complete a questionnaire including tax, banking and superannuation details. These details are passed from Onboard Centre to ConnX via the ConnX Web Service (CWS). The ConnX web service must be installed on a server with access to the ConnX SQL database; typically this will be the same IIS server that ConnX is installed on. The integration is initiated from Onboard Centre to the ConnX IIS server, so firewall rules must be configured to allow this incoming connection. We strongly recommend the ConnX web service is configured to run under HTTPS/SSL. It is the clients' responsibility to purchase and configure the SSL certificate on the ConnX IIS server.

3.11 Reports Manager Module

The Reports Manager module requires:

- Crystal Reports Runtime 13 (64 bit) to be installed on the IIS server (supplied by ConnX)
- Microsoft OLE DB Driver for SQL Server Setup installed on the IIS server (supplied by ConnX)

3.12 Mobile Module

The ConnX Mobile module is not a smart phone application (i.e., users do not download it from a 'store').

ConnX Mobile consists of pages within the ConnX web application which have been optimised to run on smartphones. To use ConnX Mobile, the user must have access to the ConnX web application on the smart phone's browser. You will need to consider how your smartphone users will get access to the ConnX mobile pages of the ConnX web application, such as publishing ConnX on the internet, VPN applications, or port forwarding. ConnX Pty Ltd does not provide configuration assistance or helpdesk for the configuration of the technical accessibility of the ConnX Mobile module.

For best use of the mobile module, ConnX should be published to the internet. For security reasons SSL certificates are recommended and you should consider ensuring ConnX denies automatic indexing by search engines so that it does not show up on search results.

3.13 ConnX Web Service

The ConnX Web Service gives ConnX the ability to interact with other 3rd party applications through a Web Service API. For installation of the Web Service, you will need to have a Windows Server with IIS enabled, typically the same server that is hosting ConnX. The IIS server will need to have access to the SQL Server where the ConnX database is installed as well as any requirements that your 3rd party application needs to be able to interact with it. The ConnX Web Service does not need to be installed on the same IIS server as the ConnX application itself. If the 3rd party applications are "cloud-based" or hosted, then you may need to open ports on the firewall to allow access from the 3rd party application to the ConnX Web Service.

ConnX Web Service requires that the WebDAV module within IIS is not installed on the server.

3.14 Timecard with Award Interpretation Module

The ConnX Timecard module requires additional processing capacity for your IIS and SQL servers. The resourcing required will be determined by the number of employees and devices in the configuration.

3.14.1 With Clocking Devices

Third party software that manages the configuration and working of your clocking devices is required to be installed.

If ConnX is in a cloud environment or hosted externally the Clocking Service will need to connect to an FTP Server.

3.15 Other Modules

The following ConnX modules do not require any additional software or configuration of your servers:

- Learning and Education
- Performance Reviews
- Roles and Positions
- Timesheets
- Variations
- Work Health & Safety
- Workforce Planning

4.0 MINIMUM HARDWARE REQUIREMENTS

ConnX will need a Windows Server with SQL Server and Internet Information Services (IIS). These can be on the same or separate servers depending on your needs or environment.

NOTE

The following hardware specifications take into consideration the recommended hardware specification of Windows Server 2012 system requirements. Please consider your operating systems hardware specifications when making your decision.

4.1 IIS and SQL on the Same Server

- Microsoft Windows Server 2016, 2019, 2022
- Microsoft SQL Server 2016, 2017, 2019, 2022 and Express versions
- Microsoft Internet Information Services (IIS)
- Microsoft Internet Information Services (IIS) – Application Initialization feature
- Microsoft .NET Framework 4.8
- Microsoft .NET Core 6 Runtime & Hosting Bundle(v6.0.32)
- Microsoft C++ 2017 Runtime (x86)
- Microsoft C++ 2010 Runtime (x86) (if using Recruitment module)
- IIS URL Rewrite Module 2
- 4 cores allocated or Quad core CPU
- 8 GB RAM
- HDD 80GB or greater
- Initial space for the application files of approximately 1000 Mb
- Initial space for the database is approximately 1000 Mb

The space used by both the database and files varies depending on the planned usage for document storage and auditing (i.e., the number of tables and history of changes) by the ConnX administrators.

NOTE

Additional server resources will be required depending on the number of modules used and number of employees. Contact the ConnX Technical Support team for recommendations.

4.2 IIS and SQL on Separate Servers

4.2.1 IIS Server

- Microsoft Windows Server 2016, 2019, 2022
- Microsoft Internet Information Services (IIS)
- Microsoft Internet Information Services (IIS) – Application Initialization feature
- Microsoft .NET Framework 4.8
- Microsoft .NET Core 6(v6.0.32) Runtime & Hosting Bundle
- IIS URL Rewrite Module 2
- 4 cores allocated or Quad core CPU
- 8GB of RAM
- HDD 40GB or greater
- Initial space for the application files of approximately 1000 MB
- Microsoft C++ 2017 Runtime (x86)

4.2.2 SQL Server

- Microsoft Windows Server 2016, 2019, 2022
- Microsoft SQL Server, 2016, 2017, 2019, 2022 and Express versions
- 4 cores allocated or Quad core CPU
- 8GB of RAM
- HDD 40GB or greater
- Initial space for the database is approximately 500 MB (average database size after several years of use is between 1000-5000 MB)

The space used by both the database and files varies depending on the planned usage for document storage and auditing (i.e., the number of tables and history of changes) by the ConnX administrators.

4.2.3 Microsoft SQL Server Express

Please note that Microsoft SQL Server Express has limitations on performance, features, and database size. Refer to Microsoft's latest SQL Express version and details via the following link:

https://learn.microsoft.com/en-us/sql/sql-server/editions-and-components-of-sql-server-2022?view=sql-server-ver16#scale-limits

4.3 Web Browsers

ConnX is known to operate in the following web browsers:

Desktop:

- Google Chrome (Windows and macOS)
- Microsoft Edge Chromium (Windows and macOS)*
- Mozilla Firefox (Windows and macOS)
- Apple Safari (macOS only)

Mobile Phone:

- Apple Safari on iOS15 and above
- Google Chrome on Android 10 and above

* Please note that running Microsoft Edge in Internet Explorer mode ("IE mode") is not supported.

ConnX Pty Ltd checks compatibility with the latest version of the above web browsers at the release of each version. Older devices and browsers are not tested with the latest versions of the ConnX application. All browsers are tested without any add-in or browser plug-ins or extensions installed.

5.0 ALLOW-LISTING

Because ConnX integrates with many systems, you may need to arrange allow-listing of several items into your environment. The following table provides details however please be aware that these details can and do change from time to time and should be regularly reviewed.

5.1 URLs and IP Ranges

ConnX Careers	
URL	connxcareers.com
ConnX Onboard Centre (Production)	
IP Address/IP Range	13.210.172.120
ConnX Onboard Centre (Sandbox)	
IP Address/IP Range	13.210.160.163
ConnX SFTP Service	
IP Address/IP Range	ap-southeast-2 ec2 AWS IP ranges (AWS IP ranges are subject to change without notice)
Ports	22
ConnX Cloud Communication Broker	
URL	https://broker.connxcloud.com
SendGrid	
IP Address/IP Range	159.183.125.95
Ports	25, 587, 2525
URL	https://api.sendgrid.com/v3/
SEEK API	

URL	https://auth.seek.com https://graphql.seek.com https://seekcdn.com/hirer/indirect-posting/product-selection-panel/seek.js https://integration.seek.com https://www.seek.com.au
Broadbean	
IP Address/IP Range	46.254.116.1-128 or 46.254.116.0/25 83.223.97.130 through to 83.223.97.254 208.82.5.0/24 (208.82.5.1 - 208.82.5.254)
Email Domains	@broadbean.com @broadbean.net
SAP Litmos	
AU Hosted SAP Litmos IP range	13.210.199.173 13.211.7.120 54.66.138.67 3.106.70.147 13.238.220.144 18.184.123.31 18.185.58.96
New Relic	
IP Address/IP Range	50.31.164.0/24 162.247.240.0/22 185.221.84.0/22
URL	https://collector.newrelic.com

5.2 JavaScript Files

ConnX Recruitment	
URL	https://seekcdn.com/hirer/indirect-posting/product-selection-panel/seek.js
URL	https://cdn.jsdelivr.net/gh/linways/table-to-excel@v1.0.4/dist/tableToExcel.min.js
URL	https://js-agent.newrelic.com/nr-892.min.js

5.3 Content Security Policy (CSP)

To enhance security, some ConnX clients have implemented Content Security Policy (CSP) by modifying the web.config file or configuring it through Internet Information Services (IIS). CSP acts as an extra layer of protection by restricting the execution of certain scripts on web pages.

CSP urls before V6.6

The following URLs need to be added to the allowed list so CSP does not block them for version 6.5 and prior

Section	Url
script-src	https://seekcdn.com/hirer/indirect-posting/product-selection-panel/seek.js
script-src	https://cdn.jsdelivr.net/gh/linways/table-to-excel@v1.0.4/dist/tableToExcel.min.js
script-src	https://js-agent.newrelic.com/nr-892.min.js
script-src	Any other third party url used in welcome widgets e.g. https://feed.surfing-waves.com/js/rss-feed.js

Newly added urls with 6.6

The following URLs need to be added to the allowed list so CSP does not block them for version V6.6

Section	Url
script-src	https://integration.seek.com
style-src	https://integration.seek.com
style-src	https://www.seek.com.au

DOCUMENT REVISION HISTORY

Date	Author	Section	Description of Change
22/04/2015	GS		Version 1 published.
21/07/2015	MR	6.0	Remove references to Microsoft Windows Server 2003, and 2003 R2, and Internet Explorer 7.
8/2/2016	MR	2.1	Added references to the Award Interpretation Module, ConnX Careers, firewall changes, and additional IIS space for the ConnX Web Service.
		5.4, 5.7, 5.8, and 5.9	Added new sections for ConnX Careers. ConnX Web Service, and ConnX Award Interpretation with and without Clocking Devices.
		6.2	Updated the Web Server requirements and supported web browsers.
27/7/2016	NK	1.1, 5.1, and 5.2	Added the IIS URL Rewrite Module 2 as a requirement for ConnX V5.0 SP2.

Date	Author	Section	Description of Change
	NK	4.2	Changed MicrOpay Meridian to Sage MicrOpay.
06/01/2017	NK	4.3.1, 4.3.2, 4.5, 5.0, 5.4	Created section 4.3.2 for Broadbean Created section 4.5 for ConnX BI Removed unsupported Windows and SQL versions. Updated version numbers for browsers.
24/03/2017	NK	4.3.3	Added section about Onboard Centre.
22/09/2017	NK	4.6	Updated pre-requisites for ConnX BI.
03/05/2018	GS	1.3	Added ConnX Security Overview section.
17/09/2019	RW	1.1, 1.2, 2.0, 2.1.1, 2.2, 2.2.1, 3.0, 3.3, 3.12, 3.12.1, 4.0, 4.1, 4.2.1, 4.2.2, 4.4	Revision and updates for ConnX V6.0. Remove references for Microsoft SQL Server 2008 and 2008R2.
22/01/2020	NK	4.0	Remove Windows Server 2008 references.
08/05/2020	BK	4.3	Added Mobile Phone browsers.
04/08/2020	BK	All & 5.0	General review and added section 5.0
18/09/2020	NK	All	General review and update for V6.1 Release.
11/03/2021	NK	All	General review for V6.2 Release
13/07/2021	NK	All	Removed Sage from references to MicrOpay
09/02/2022	NK	All	General Review
17/03/2022	NK	3.5	Microsoft 365 basic authentication

Date	Author	Section	Description of Change
25/05/2022	NK	All	General Review and update for V6.4 Release including new components
22/08/2022	BK	All	General Review and minor updates for V6.4 SP1 Release
10/10/2022	AD	4.0	Remove SQL 2012 and Server 2012 references
29/03/2023	BK	All	General Review and updates for V6.5 Release
28/03/2024	BK	All	General Review and update
09/09/2024	AP	All	General Review and update. Added CSP section. Removed SQL server 2014 as it is not supported.