Cochlear®
Hear now. And always

Custom Sound® Pro
software

Custom Sound®
Version 7.1
Installation Guide

Contents

Product information

Product name: Custom Sound®
Version: 7.1

This guide refers to the product by its trade name, Custom Sound Pro.

About this guide

This guide will help you install and run the Custom Sound® Pro software. It contains the technical description of the Custom Sound Pro software and will help you ensure that your system meets the requirements to run the software and provide you with security practices for hardening your system and network. For information on how to use Custom Sound Pro software, please see the Custom Sound Pro software User Guide or view the documentation in the application by pressing F1.

Custom Sound Pro software can be installed by the clinician or local IT administrator.

Symbols used in this guide

Note

Important information or advice

System requirements

	Minimum system requirements	Recommended system requirements
Operating system	Windows® 10 (64-bit) Version 2004 or Windows 11 21H2 (Note: 32-bit versions of Windows 10 are not supported)	Windows 11 22H2 or later (Note: Windows Home version not recommended)
Processor	6th Generation Intel® Core™ i5 Processor i5 6400/AMD Ryzen 5 2600	9th Intel Core i5 9500 Processor/ AMD Ryzen 5 3600 or faster
RAM	8 GB of DDR3 or higher	16 GB DDR4 RAM
Hard drive	Solid State hard drive with 10 GB of available space	HDD 10 GB Free Solid State NVMe PCIe
Screen resolution	1920 x 1080	1920 x 1080
Screen size (for tablet use)	12 inches or higher	12 inches or higher
USB port	2 x USB A ports	2 x USB A ports
Wireless	Bluetooth® 4.0 required for Cochlear™ Wireless Programming Pod	Bluetooth 5.0, or higher, required for Cochlear Wireless Programming Pod
SQL Server®	SQL Server 2019	SQL Server 2022

To participate in Remote Assist sessions the computer system running the Custom Sound Pro software will also need the following:

Video	Integrated laptop camera or USB 2.0 video camera
Voice	Compatible microphone and speakers, headset with microphone, or equivalent device
Network	A stable internet connection

It is important to keep the Windows® operating system up to date. The computer or tablet must be capable of receiving Windows updates.

Any computer system connected to the Cochlear™ system, when used in programming mode, should meet FCC 47CFR Part 15 Class B and CISPR22 Class B emissions requirements. Consult the documentation provided by the computer system manufacturer to ensure compliance, prior to connecting any Cochlear device.

Security considerations

Medical device security is a shared responsibility between medical device manufacturers and health care facilities. Custom Sound Pro software includes a number of built-in features that can help protect the integrity of information such as:

- Removal of patient-identifiable details from records when anonymously exported from the Cochlear database
- Validation checks within the Cochlear database to maintain data integrity
- A backup utility for the Cochlear database
- Encryption of CDX files that are exported from Custom Sound Pro software
- Code signing of installer executables
- User names and passwords to control access to Custom Sound Pro software

To help reduce the risk of unauthorised access to Custom Sound Pro software it is best practice to implement an IT security policy within the healthcare facility that considers the following items:

- Windows operating systems including the latest security updates from Microsoft®
- Anti-virus software including the latest updates available from the vendor with regular scanning of hard disk
- Scanning of USB storage devices for malware or viruses before connecting to the computer running Custom Sound Pro software
- Firewalls to protect computers running Custom Sound Pro software that are accessible to the Internet
- A password policy that requires strong passwords that are changed regularly and are applied to user accounts on computers where Custom Sound Pro software is installed and network-connected computers where the Cochlear database is installed
- Locking computers when unattended
- Regular backups of the Cochlear database

Cochlear also suggests following the recommendations from the **Security practices** section of the ***Custom Sound Pro software- Installation Guide***.

Pre-installation

Prior to installing the Custom Sound Pro software on your computer, there are some decisions and tasks that can be completed to ensure a successful installation and setup.

During the installation, you will be required to choose between a standalone setup and connecting Custom Sound Pro software to a network database. If you choose a standalone installation the installer will install SQL Server® 2022 Express on the local computer. If your clinic uses a network database, careful planning is required to ensure that all computers with Custom Sound Pro software can connect to the database.

Before beginning the install

It is highly recommended that you review the following and use it as a basis for preparing your system for the installation.

- Check that the target Laptop or Desktop meets the recommended system requirements shown in the System Requirements above.
- When installing or upgrading the Custom Sound Pro software, the computer may need to be restarted. Ensure you close any applications before installing the software.
- You must have administrator rights to install or update the software. If you do not have administrator rights, contact your IT department.

  Administrator is a Microsoft Windows security setting that enables restricted access to create, delete, and modify files, folders, and settings on the computer. Administrative rights are granted by administrators to users which allow them to create, delete, and modify items and settings.

  If your computer is not managed by a central IT organisation or network administrator, you most likely have “Administrator” rights as most privately purchased computers come standard with the rights set for individual users. If you do operate under an IT organisation (e.g., in a school or hospital setting) contact your IT department to determine if you are an administrator of your computer.
- You must have access to create a folder in the root directory of your system.
- Backup the current database if upgrading an existing installation.
  - If the installation uses a network database, ask the clinic IT administrator to take a database backup before installation.
  - For standalone installation save a backup of the local database using the Cochlear database manager as described later in *Back up or restore a database.*

For a standalone installation

Local databases cannot be created if the drive is compressed.

Ensure the local drive where you plan to install the Custom Sound Pro software is not compressed.

This can be done by right-clicking on the drive in Windows Explorer and selecting Properties.

If the drive is compressed, please contact the clinician / local IT administrator.

For a network database installation

Take note of database credentials (user name and password) for the network database.

Before beginning the installation ensure you can access the network database with current credentials.

Also, ask the clinic IT administrator to take a database backup of the network database before installation.

Note: Installing or upgrading to a new version of the Custom Sound Pro software may require a database upgrade. If your clinic uses a network database, the following steps are required to ensure that all computers with Custom Sound Pro software can connect to the database:

- Close all Custom Sound Pro software clients.
- Upgrade the clinical database instance.
- Upgrade all Custom Sound Pro software clients.

Please check release notes before installing to see if a database upgrade is required.

Installation

Once all the appropriate pre-installation steps have been completed, proceed with the installation. The following instructions may vary based on the type of environment being installed or upgraded.

The Custom Sound Pro software installation process has been enhanced and installation information will display on the screens throughout the entire install to help guide you through the installation or upgrade process.

If you receive any error messages during the installation recheck the requirements section. You may contact Cochlear at any time for assistance with the installation process.

Prerequisites

If you are upgrading from a previous version of the Custom Sound Pro software, make sure you have backed up the database as directed in the pre-installation section.

Run the installer

Follow the onscreen instructions provided by the software installer.

During the installation you will need to make several choices:

- **Licensing agreement -** The licensing agreement needs to be accepted to continue the installation process. If you do not accept the licensing agreement, no changes will be made to your current version of installed software.
- **Help improve the Custom Sound Experience -** You will be provided with two options to provide different types of feedback to Cochlear. Choosing Yes to the first option will assist Cochlear in making better products. This allows for information on all actions, for example, which buttons and features (no values) are used during a fitting session to be sent back to Cochlear. This feedback is completely anonymised, and no clinic or recipient-specific information is sent back to Cochlear.

  Choosing the option to register the software after it is installed, the software registration information will be sent back to Cochlear when the installation is complete or saved on the desktop for sending at a later time.

- **Contact Information -** Mandatory fields of the contact information need to be completed even if both options in the previous screen are not selected. This information is used to identify stand-alone installations on PCs as well as pre-populating the software registration form.
- **Setup option -** During the installation, you will be required to choose between a standalone setup and connecting Custom Sound Pro software to a network database. If you choose a standalone installation the installer will create a database on the local computer. If you choose to connect to a network database, you will have the option of entering the database connection details now or setting them using the Cochlear database Manager after installation.
- **Database connection -** When connecting to a network database you will need to select a database server and instance from a drop-down menu and select an authentication mode to use to connect to the database instance.
    - **Windows authentication -** selecting this option will use the current user account Windows credentials to access the selected database server. You will also be asked to choose a database name from a drop-down on the server that you want to connect to.

       **Note:** you will need to ensure that the current Windows user credentials have the correct permissions to access the selected network server.
    - **SQL Server authentication -** selecting this option you will need to provide the SQL Server user name and password for the selected SQL Server instance.

       **Note:** you may need your IT administrator to provide the details for the SQL Server access credentials.
- **Complete installation -** At the end of the installation process application icons will have been saved to your desktop, and the Custom Sound Pro software will have been added to your start menu.

Upgrading

Run the installer. During the installation, the installer will detect if you have an older version of the Custom Sound Pro software installed on your computer and you may be able to upgrade from the existing version. Upgrading from a previous version will keep the existing setup option (standalone or networked). However, please be aware that you may be required to update the existing local or network database. If your clinic uses a network database, careful planning is required to ensure that all computers with Custom Sound Pro software can connect to the database. Please check release notes before installing to see if a database upgrade is required.

Additional setup options

Additional setup options are accessible from the initial screen of the installer.

When installing a new database on a network, choose the **Cochlear Database** option and run this setup from the selected networked PC or Server.

When upgrading the Custom Sound Pro software to a networked database, choose the **Cochlear Database Manager** option.

Post installation

After completing the installation of the Custom Sound Pro software, you should review the following post-installation tasks and, if necessary, perform the tasks that are applicable to your system.

Run the application

Running the application allows you to check that the install has been successfully completed and that Custom Sound Pro software is able to connect to the database correctly.

To run Custom Sound Pro software:

1. Double click on the Custom Sound Pro software icon that can be found on the desktop, or in the Windows menu under Cochlear.
2. Follow the log in prompts and enter the application.
3. If connecting to an **existing database**, you should see existing patients in the **Patient List**. If the patient list appears empty, there may be an issue with the database connection.

   If connecting to a **new database**, the patient list will appear empty.
4. Connect a programming pod and a sound processor to the computer and check that both are visible in the status bar in the software.

Regional options

Some features or products are only available in Custom Sound Pro software by activating a regional option. Regional options are activated using the Research and Regional Options Manager. Option information is specified in regional options files (*.cofx).

Note:

- The **Change Research and Regional Options** menu option is greyed out and not available when a session is open. Before activating a regional option, you need an authorisation key for the option you want to activate.

To activate regional options while running the application:

1. Click **Tools > Change Research and Regional Options** in the Menu bar.

   The Research and Regional Options Manager wizard displays.
2. Click the **Activate options** option button.
3. Click **Next**.
4. Click **Browse** and select the relevant regional options file (*.cofx).
5. Click **Open**.
6. Type the authorization key for the option.
7. Click **Next**.
8. Read the conditions and select the **I Accept** checkbox.
9. Click **Activate Options**.
10. Click **Close** to close the Research and Regional Options Manager.

The selected regional option is activated.

Additional security and setup options

Set clinician password

Cochlear recommends setting passwords for clinician accounts created in the Custom Sound Pro software. For instructions on how to setup a clinician password please see the topic *Set or change clinician's login password* in the Custom Sound Pro software help.

Network port access for Remote Assist

The Custom Sound Pro software requires access through any firewall for the following network ports, port 80 and port 443, to allow the full use of the Remote Assist feature.

Cochlear Account Administration Tool (CAAT)

The Cochlear Account Administration Tool (CAAT) is an optional user authentication system based on Microsoft® Active Directory®. Clinician accounts can be set up for Custom Sound Pro software and any other tool that uses Custom Sound Pro software authentication. When configured, the clinician will not be required to log in to Custom Sound Pro software.

Note: You must install a regional key to access CAAT.

Set up Microsoft Active Directory groups

Set up Microsoft Active Directory groups that will be linked to Custom Sound clinician accounts.

Task steps:

1. Create a group called **GLOBAL_custom_sound_administrators.**
2. Add Custom Sound Pro software administrators to the group.
3. Create a group called **GLOBAL_custom_sound_users**.
4. Add all authorised Custom Sound users to the group.

Result:

- The GLOBAL_custom_sound_administrators and GLOBAL_custom_sound_users groups are created.

Link Active Directory and Custom Sound Pro software user accounts

Use CAAT to link members of the GLOBAL_custom_sound_users group to clinician accounts in the Custom Sound database.

Note: You must be an administrator in the GLOBAL_custom_sound_administrators Active Directory group to link Active Directory and Custom Sound Pro software user accounts.

Task steps:

1. Open the **Cochlear Account Administration Tool** from the **Start** menu.
2. Select the **Link** tab.
3. Select the **Domain username** from the **Choose Cochlear software user list**.
4. Select the corresponding Custom Sound Pro software clinician account from the **Cochlear clinician database entry** list.
5. Click the **Link** button.

Result:

- The Domain username is now linked to the new Custom Sound Pro software clinician account.

Unlink Active Directory and Custom Sound Pro software user accounts

Use CAAT to unlink GLOBAL_custom_sound_users and Custom Sound Pro software clinician accounts.

Note: You must be an administrator in the GLOBAL_custom_sound_administrators Active Directory group to unlink Active Directory and Custom Sound Pro software user accounts.

Task steps:

1. Open the **Cochlear Account Administration Tool** from the Start menu.
2. Select the **Processed** tab.
3. Select the Domain username from the Choose Cochlear software user list.
4. Click the **Unlink** button.

Result:

- The link between the Domain username and the Custom Sound clinician account is removed.

Create a new clinician account

Use CAAT to set up a new clinician account and link it to their domain account.

Task steps:

1. Open the **Cochlear Account Administration Tool** from the **Start** menu.
2. Select the **Domain username** from the **Choose Cochlear software user** list.
3. Select the **New clinician database entry** checkbox above the **Cochlear clinician database entry** list.
4. Click the **Link** button.

Result:

The selected domain user details are read from the domain server and a new clinician record is created in the Cochlear database. The Domain user is linked to the new Custom Sound Pro software clinician account.

Troubleshoot CAAT

The following table provides troubleshooting procedures for messages that you may receive following CAAT setup.

Message	Possible cause	Resolution
No Active Directory domain controller found.	• CAAT has been installed and the domain has not been set up. • The user attempts to open CAAT and they are not connected to their work VPN/domain.	• Clinic administrator needs to sign in to the domain.
Create Active Directory user group. This will affect all Cochlear software users.	• The user is connected to the domain but the required Active Directory groups have not been set up.	• Set up the required Active Directory groups. • For more information about Active Directory groups see Set up Microsoft Active Directory groups.
Unauthorised Windows user	• The user attempts to open CAAT but they have not been added to the administrator Active Directory group.	• Add the user to the GLOBAL_custom_sound_administrators group.
Account not found	• The user has not been added to the domain user group. • The domain user has not been added linked to their Custom Sound clinician account.	• Add the user to the GLOBAL_custom_sound_users group. • Link the domain user account to the Custom Sound clinician account.

Manage auto-updates

If you have clinic administrator permission, you can manage the auto-update preferences for Custom Sound Pro software.

Task steps:

1. Click on **Tools > My Clinic** in the Menu bar.

   The My Clinic window displays a list of registered clinicians.
2. Click the **Edit Clinic Details** link.

   The Clinic Details window General tab displays.
3. Select the **Auto Update** tab.
4. Select one of the auto-update options from the Preferences.
   - Automatically download but ask me to install update on application close.
   - Notify me of updates. I will choose when to download and install the update.
   - Do not download or install update.

   The OK button becomes active as soon as a change has been made.
5. Click **OK** to save the changes and close the Clinic Details window.

Result:

- The auto-update preferences are modified.

Cochlear Database Manager

A database is automatically created, or the application is configured to connect to a network database when Custom Sound is first installed. The database is shared across Custom Sound Pro software and Custom Sound EP software and contains the records for all patients created in either application. The Cochlear Database Manager allows you to manage databases and to select the database you want to connect to.

The Cochlear Database Manager contains the following tabs:

- **Connections:** displays the list of connections to existing databases. When you log on to Custom Sound Pro software or Custom Sound EP software, the software connects to the database specified by the current connection. The connection that is currently in use is indicated by a **Check** symbol  .
- **Databases:** displays the list of existing databases. The Databases tab allows you to connect to the database server, create new databases and manage existing databases.

Create or edit a connection

The Cochlear Database Manager allows you to create a new connection to an existing database, and to edit or delete existing connections.

Task steps:

1. Navigate to the Windows **Start** menu.
2. Open the Cochlear Database Manager from the Windows Start menu.
3. Click **Add** in the **Connections** tab.

   The Add Connection window displays. Mandatory boxes are indicated by a **Required** symbol .
4. Type a name for the connection in the **Connection Name** box.
5. Type the name of the server on which the database resides in the **Server\Instance Name** box.
6. If a password is required to log on to the database server, select the **Use a Specific Username and Password** option button and type the username and password in the appropriate boxes.

   Otherwise, retain the **Use Windows Integrated Security** option button.
7. Select the database you wish to connect to from the **Database** drop-down list.
8. To adjust the amount of time that Custom Sound Pro software or Custom Sound EP software will wait for a response from the database server, type the number of seconds in the **Connection Timeout** box.
9. Click **OK**.
10. To select the new connection as the default, right-click on the connection and select **Set as Active Connection**.

    The connection is marked with a **Check** symbol .

Result:

- The connection is added to the Connections list.

To edit a connection, right-click on the connection and select **Edit Connection**. Edit the existing details as required, and click **OK**.

To delete a connection, right-click on the connection, select **Delete Connection** and click **Yes** to confirm the deletion. Deleting a connection does not delete the database it connects to.

Connect to a server

In order to create or manage databases, you must first connect to the server on which the databases reside.

Task steps:

1. Navigate to the Windows **Start** menu.
2. Open the Cochlear Database Manager from the Cochlear folder, under the Windows Start menu.
3. Click the **Databases** tab in the Cochlear Database Manager.
4. Click **Connect**.

   The Connect window displays.
5. Type the name of the server on which the databases reside in the **Server\Instance Name** box, or retain the default setting.
6. Retain the **Use Windows Integrated Security** option button.

   Alternatively, select the **Use a Specific Username and Password** option button and type the username and password for the database server in the appropriate boxes.
7. Click **OK** to save the changes and close the Connect window.

   The databases that exist on the server display in the Database list.

Result:

- Cochlear Database Manager is now connected to the server.

Once the connection to the server has been established, the Cochlear Database Manager allows you to:

- Create a new database
- Upgrade a database
- Back up or restore a database
- Delete a database

Create a database

The Cochlear Database Manager allows you to create a new database as desired. By default, a connection to the new database is automatically created, but is not selected as the default connection.

Task steps:

1. Navigate to the Windows **Start** menu.
2. Open the Cochlear Database Manager from the Cochlear folder, under the Windows Start menu.
3. Click **Create** in the **Databases** tab.

   The Create Database window displays.
4. Type a name for the database in the **Database** box.
5. Type the clinic and clinician names in the appropriate boxes.

   The clinician name is used to automatically create a clinician with clinic administrator rights in Custom Sound Pro software.
6. Type a name for the connection in the **Connection Name** box.
7. Retain the **Use Windows Integrated Security** option button.

   Alternatively, select the **Use a Specific Username and Password** option button and type the username and password for the database server in the appropriate boxes.
8. Click **Create**.

   The database displays in the Database list, and a connection is created in the **Connections** tab.

Result:

- The new database is created.

If you do not wish to automatically create a new connection when the database is created, clear the **Create a New Connection for This Database** check box.

Upgrade a database

An existing database may need to be upgraded when a new version of the Custom Sound Pro software is released. By default, the Cochlear™ Database Manager backs up the existing database prior to performing the upgrade.

Task steps:

1. Navigate to the Windows **Start** menu.
2. Open the Cochlear Database Manager from the Cochlear folder, under the Windows Start menu.
3. Select the database in the Database list.
4. Click **Upgrade**.
5. Type a file location and filename for the backup file, or retain the default file path.
6. Click **Upgrade**.

Result:

- The database is upgraded.

If you do not wish to back up the database prior to upgrading, clear the **Backup the Database Before Upgrading** check box.

Note: When you upgrade the Custom Sound Pro software from 2.0 or later, the installer provides the option to upgrade the database. When the upgrade option in the installer is selected, the Custom Sound Pro software database that is currently in use is upgraded. Any additional databases or databases created using an earlier version of the software can be upgraded using the Cochlear Database Manager.

Back up or restore a database

The Cochlear Database Manager allows you to back up a database to an external file. A database can be restored from a previous backup if required.

To back up a database:

Task steps:

1. Navigate to the Windows **Start** menu.
2. Open the Cochlear Database Manager from the Cochlear folder, under the Windows Start menu.
3. Select the database in the Database list.
4. Click **Backup**.

   Alternatively, right-click on the database and click **Backup**.
5. Type a file location and filename for the backup file, or retain the default file path.
6. Click **Backup**.

Result:

- A backup of the database is saved to the specified location.

To restore a database:

Task steps:

1. Click **Restore** in the **Databases** tab.
2. Type a new name for the database in the **Database** box.
3. Type the file path of the file you wish to restore in the **Backup File** box.

   Alternatively, click **Browse**, navigate to the desired file, and click **OK**.
4. Click **Restore**.

Result:

- The restored database displays in the Database list.

Delete a database

Databases that are no longer required can be deleted from the Database list. A deleted database cannot be restored. A database can only be restored from a backup file, and it is recommended you back up the database prior to deletion.

Task steps:

1. Navigate to the Windows **Start** menu.
2. Open the Cochlear Database Manager from the Cochlear folder, under the Windows Start menu.
3. Select the database you wish to delete in the Database list.
4. Click **Delete**.

   Alternatively, right-click on the database and select **Delete Database**.
5. Click **Yes** to confirm the deletion.

Result:

- The selected database is no longer available.

Security practices

This section provides reference and general guiding principles around securing the clinical database and related infrastructure. It focuses on general principles around database management in Microsoft SQL Server with a special focus on security features and how to defend the Cochlear clinical database against cyber-attacks.

Because the clinical database is nearly always network-accessible, a security threat to any component within, or a portion of, the network infrastructure is also a threat to the clinical database. Any attack impacting a clinic or hospital workstation can threaten the clinical database. This means that clinical database security must extend beyond the confines of the clinical database.

When evaluating clinical database security consider each of the following areas:

Physical security: Whether your database server is on premise or in a cloud data centre, it must be located within a secure environment.

Administrative and network access controls: Only the minimum number of users should have access to the database, and their permissions should be restricted to the minimum levels necessary for them to do their jobs. Likewise, network access should be limited to the minimum level of permissions necessary.

End user account and workstation security: Always be aware of who is accessing the clinical database and when and how the data is being used. Data monitoring solutions can alert you if data activities are unusual or appear risky. All user devices connecting to the network housing the clinical database should be physically secure (in the hands of the right user only) and subject to security controls at all times.

Database software security: Always use the latest version of your database management software, and apply all patches as soon as they are issued.

Backup security: All backups, copies, or images of the clinical database must be subject to the same (or equally stringent) security controls as the clinical database itself.

Auditing: Record all log-ins to the clinical database server and operating system, and log all operations performed on sensitive data as well. Clinical database security standard audits should be performed regularly.

Securing the clinical database environment

As part of your hardening process, assess the deployed software infrastructure that supports your clinical database system and verify that it meets the manufacturer's recommendations and hardening guidelines.

Software infrastructure elements to consider include operating system components, supporting software, and database software. Address security concerns in these and other components according to the manufacturer's recommendations and other relevant security protocols.

General clinical database environment considerations

Installation decisions

Before installing your clinical database environment it is important that you consider the following installation decisions.

- **CPU:** CPU power and speed are required for optimal SQL Server function. When a clinic or hospital want to use data encryption technology TDE (transparent data encryption) a faster and more powerful CPU is recommended.
- **Memory:** SQL Server runs mostly from memory and requires considerable server memory. You will need more memory depending on how large the Microsoft SQL Server COCHLEAR instance, and if it has the online transaction processing (OLTP) feature enabled.
- **Disk:** SSDs (solid state disks) are faster for I/O operations. Data files and the internal database of SQL Server should be put on SSDs to improve SQL Server performance.
- **Disk Tools**: Using disk testing tools like SQLIO and SQLIPSIM to check the performance and the requirements of the hardware in the clinical database environment.
- **Operating System:** Microsoft recommends Windows Server environment for server operating system. We recommend using the latest version of Windows Server.
- **MS SQL Server Edition**: Enterprise version of Microsoft SQL Server allows an IT administrator to configure all the features and is the recommend version among available editions.

Installing and configuring Windows Server

Note: This section uses Microsoft Windows Server 2016 as a reference here for installation and configuration. Windows Server system platform and the minimum requirements can be found at the Microsoft website.

Windows Server Requirements

(https://docs.microsoft.com/en-us/windows-server/get-started/system-requirements)

Cochlear recommends the following requirements when installing and configuring Windows Server:

- 2 GB of memory is the minimum recommended for clinical database services to run smoothly.
- A Windows Domain is strongly recommended for security and management reasons.

  We recommend first installing the domain and then Active Directory domain services.

  Active Directory domain services provide secure structure hierarchical data search for objects such as users, computers and printers. If Active Directory domain services and domain controller are not installed then it is recommended to install Active Directory domain services before installing clinical database system.
- Install a DNS domain name service using the server manager application.
- It is not recommended to install the clinical database server onto a domain controller server. We recommend having different computers for your domain controller and your clinical database server.
- Microsoft SQL Server installation requires .net framework 3.5 to be installed as a prerequisite. Install Microsoft .NET framework 3.5 using server manager, if not already installed.

Service account security

Microsoft Windows has a managed service account and a virtual server account. It is good practice to use service accounts in a SQL Server environment instead of direct user accounts or share accounts. A service account is a user account that is created explicitly to provide a security context for services running on Windows Server operating systems. Service accounts should ideally be set with minimum privileges.

Some practices that we recommend are:

- Use a network server account or a specific domain user account instead of share accounts because shared accounts pose a security risk.
- Use SQL Server configuration manager to manage any updates to change service accounts. If using a user or domain account, change passwords at regular intervals as a best practice.
- Microsoft SQL Server can use credentials to execute jobs so that you do not have to change or update the SQL Server agent service account privileges. Depending on the job or task you can create different credentials so that you will not have to give excessive privileges to a task.
- If a user needs to execute a job that requires a different level of credential, then it's a good idea to create a proxy account for that job. The use of proxy accounts is a secure way to do certain operations.

For more information on service account security please view the link below or contact your Microsoft vendor.

- ***Service Accounts***

  (https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/service-accounts)

Password policy

When developing or implementing a password policy for your organisation Cochlear recommends the following guidance:

- Passwords are mandatory.
- Password complexity is enforced.
- Password minimum length is 8 characters for user accounts, 12 characters for privileged accounts and 20 characters for service or integration accounts.
- Do not use credentials that are hard-coded, default, easily-guessed, easily compromised (i.e., passwords which are the same for each device; unchangeable; can persist as default; difficult to change; and vulnerable to public disclosure).
- Limit public access to passwords used for privileged device access.
- Systems that have the capability to store passwords have the following functionality:
    - Stored passwords are encrypted, not in clear text
    - Or stored as hashes after hashing the password with a salt. Salt should be long, random and generated using a Cryptographically Secure Pseudo-Random Number Generator (CSPRNG). The salt needs to be unique per-user per-password. Every time a user creates an account or changes their password, the password should be hashed using a new random salt.
    - Protect password files by restricting access.
- Passwords and credentials are protected during transmission implementing secure protocols: - encrypt data-in-transit.
- Passwords and credentials are not included in emails, user guides or instructions for use.

Patching and compliance

It is best practice to apply a hotfix, Windows update and service packs promptly to ensure that a system is up to date with the latest security fixes.

Patching and Windows Updates best practices are:

1. Maintain the currency of software, including all libraries and components, by installing the latest versions and relevant security patches.
2. Enable security-related product upgrade and patching.
3. Ensure that the manufacturer has the means to notify you of the content and reason for new versions and whether it will impact the security or safety.
4. Test all updates before they are applied to the system.

Before applying any updates, it is a good idea to check if new versions or patches have any recorded know issues which may affect the business continuity of your environment. Updating and using the latest versions of both the Windows operating system and the SQL Server are also recommended. Keep in mind before changing operating systems or database server to test the changes beforehand in a testing or staging environment.

SQL Server 2008 R2 has achieved Common Criteria compliance. This Common Criteria compliance allows security auditing and helps administrators to share industry compliance such as HIPAA or FIPS 140-2/3 and represents the outcome of the efforts to develop criteria for evaluation of the security.

Common criteria is a computer security certification that assures that the process of specification, implementation and evaluation of a computer security product like Microsoft SQL Server has been conducted in a rigorous, standard and repeatable manner.

For more information on Common Criteria Compliance please view the link below or contact your Microsoft vendor.

- ***Common Criteria Compliance Enabled Server Configuration***

  (https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/common-criteria-compliance-enabled-server-configuration-option?view=sql-server-ver15)

Securing Microsoft Windows workstations

Workstations are often targeted by using malicious websites, emails, or removable media in an attempt to extract sensitive information. Hardening workstations is an important part of reducing this risk.

Contact your Microsoft vendor or cyber security professionals in your country or region for guidance about hardening practices for Microsoft products.

- ***Windows 10 Enterprise Security***

  (https://docs.microsoft.com/en-us/windows/security/)

Securing Microsoft SQL Server

It is recommended that you verify that your Microsoft SQL Server database meets security guidelines as established by Microsoft.

Cochlear recommends that you:

- Review the recommendations in the appropriate Microsoft SQL Server hardening and securing best practice guidelines.
- Review all Microsoft security bulletins regarding your installed version of Microsoft SQL Server.
- Enable transparent data encryption (TDE) to ensure database files, backup files and tempdb files cannot be attached and read without proper certificates decrypting database files. Not enabling TDE allows for an attacker to take the physical media and restore or attach the database to read/alter contents. See

  https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-ver16#enable-tde

Not following the hardening recommendations might result in exposure to known security vulnerabilities from insecure components on your Microsoft SQL Server version.

Contact your Microsoft vendor for guidance about hardening practices for Microsoft products.

Note: This section uses SQL Server 2014 as a reference for installation, configuration, hardening and policy management considerations. SQL Server 2019 is the minimum supported version for Custom Sound Pro software. However it is recommended to use latest SQL Server versions and patches as suggested by Microsoft. Contact your Microsoft vendor for more guidance.

Microsoft SQL Server installation considerations

The minimum supported version Microsoft SQL Server for Custom Sound Pro software is Microsoft SQL Server 2019. We recommend using the 'Enterprise' edition.

SQL Server installation preparations

Before installing Microsoft SQL Server:

- Refer to Microsoft SQL Server Security documentation from the SQL Server Installation Center for configurations for secure implementation.
- We recommend creating or using a separate Windows Server administrator user account for the SQL Server installation.
- If Active directory services are implemented (recommended), add a new user account using Server Manager.

SQL Server installation

During the installation of Microsoft SQL Server:

- Check '**Use Microsoft updates to check for updates (recommended)**' option.
- It is not recommended select '**All features with Defaults**' from security point of view.
  Only install what is required and revisit to install or uninstall other components when required.
- It is recommended to select Windows authentication mode. Avoid mixed mode to prevent brute force attack on the SQL Server. For security, Windows authentication only is an acceptable authentication mode for clinics or hospitals.

For more information please view the link below or contact your Microsoft vendor.

- ***Security Considerations for a SQL Server Installation***

  (https://docs.microsoft.com/en-us/sql/sql-server/install/security-considerations-for-a-sql-server-installation?view=sql-server-ver15)

Microsoft SQL Server hardening considerations

The clinical database (Microsoft SQL Server application) relies on data. Data is a typical target for hackers and therefore clinical data is at risk of being compromised either accidentally or intentionally.

A clinic or hospital IT administrator can minimise these risks by hardening SQL Server through reducing its surface area and other security measures.

For more general information on SQL Server network configuration please view the link below or contact your Microsoft vendor.

- ***Server Network Configuration***

  (https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/server-network-configuration?view=sql-server-ver15)

Surface area reduction

Surface area is seen as the pathways which can be exploited to gain access or elevate privilege on a SQL Server. Surface area reduction uses service reduction techniques to prevent unauthorised access or unauthorised elevated privileges.

Surface area reduction can be further explained as:

- Limiting avenues for potential attacks.
- Stopping or disabling unused services.
- Using the least privileges approach.

We have identified several services that can be disabled or removed to support service area reduction.

Analysis Service: The Analysis Services (SSAS) are not required and can be uninstalled or deselected during installation.

Integration Services: The Integration Services are not required and can be uninstalled or deselected during installation.

Reporting Services: 'Reporting Services – Native' and 'Reporting services – SharePoint' and its extension, if required, should be installed on a different server and not on the server with the clinical database engine. Installing SQL Server Reporting services (SSRS) on the same server as the database engine allows a vulnerability in the secret layer to be exploited by hackers to take control of the server.

VSS Writer: The service SQL Server VSS Writer provides the interface to back up and restore Microsoft SQL Server through the Windows VSS infrastructure service. It should be enabled only when it is being actively used. If you are not using third-party application to create SQL backups there is no need to run this service.

SQL Server Browser: Keeping this browser service disabled will remove the redirect as an attack vector. However, there is a trade-off. If you disable this you cannot use dynamic ports or SQL Server Dedicated Admin Connection (DAC). This is a service for database administrators to create a dedicated and straight connection.

Static and dynamic port configurations

We can define the ports as an endpoint. This will bind the port to a particular application or service for communication purposes. When SQL Server is installed, it configures default ports for its services. Each client application uses the combination of IP addresses and port number to connect to SQL Server.

There are two kinds of ports used in SQL Server:

Static Port: A static port, once set, is always bound to a service or application and does not change due to a service or system restart.

Dynamic Port: You can configure SQL Server to use a dynamic port. If you use dynamic port allocation, you specify port number zero in the network configuration. Once SQL Service restarts, it requests a free port number from the operating system and assigns that port to SQL Server. Once the operating system allocates a dynamic port to SQL Server, that port number is written to the Windows registry. SQL Server Browser service gives back the port number of a specific instance. An application can connect to SQL Server using that dynamic port.

 **Note:** SQL Browser service is essential for the named instances with dynamic port allocation. It should be in a running state for applications to query and receive the port details.

 **Note:** You should change the SQL Server Port configuration using the SQL Server Configuration Manager only.

For more information on setting static or dynamic ports please view the links below or contact your Microsoft vendor.

- ***TCP/IP Properties (IP Addresses Tab)***

  (https://docs.microsoft.com/en-us/sql/tools/configuration-manager/tcp-ip-properties-ip-addresses-tab?view=sql-server-ver15)

- ***Configure a Server to Listen on a Specific TCP Port***

  (https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-a-server-to-listen-on-a-specific-tcp-port?view=sql-server-ver15)

Updating firewall settings for static or dynamic port access

Firewall systems help prevent unauthorised access to computer resources. If a firewall is not correctly configured, connections to the SQL Server might be blocked.

To access your clinical database instance through a firewall, you must configure the firewall on the computer that is running SQL Server. The firewall is a component of Microsoft Windows. If you are using a third-party firewall or if there is anti-virus software installed, make sure those settings are properly configured to accept connections to the SQL Server.

For more information on how to configure Windows Firewall please view the link below or contact your Microsoft vendor. If you are using a third-party firewall or anti-virus software, please consult their corresponding documentation.

- ***Configure a Windows Firewall for Database Engine Access***

  (https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-a-windows-firewall-for-database-engine-access?view=sql-server-ver15)

Extend Protection with Channel and Service bindings

Both Channel and Service binding completes the configuration for extended protection.

Channel binding addresses both luring and spoofing attacks. However, it incurs a larger runtime cost because it requires encryption of all the session traffic. Service binding addresses luring attacks by requiring a client to send a signed service principal name (SPN) of the SQL Server service that the client intends to connect to.

For more information on Extended Protection and Channel and Service bindings please view the links below or contact your Microsoft vendor.

- ***Connect to the Database Engine Using Extended Protection***

  (https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/connect-to-the-database-engine-using-extended-protection?view=sql-server-ver15)

- ***Enable encrypted connections to the Database Engine***

  (https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-ver15)

Hiding SQL Server instance

The SQL Server Browser Service enables client applications to browse for a server and helps clients to distinguish between multiple instances of the database engine on the same computer. This allows attackers to identify the service to attack. You can hide the SQL Server instance in your clinical database to prevent clients from locating the instance through SQL Server Browser service.

For more information on how to hide your clinical database instance please view the link below or contact your Microsoft vendor.

- ***Hide an Instance of SQL Server Database Engine***

  (https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/hide-an-instance-of-sql-server-database-engine?view=sql-server-ver15)

Policy management considerations

Policy based management allows the clinic or hospital IT administrator to monitor the best practices in SQL Server database engine.

Best practices for the SQL Server Database Engine policy management considerations includes:

1. Select a facet
2. Create a condition
3. Create a policy
4. Give a target to the policy

The end result of the policy created will use the facets, conditions, policies and apply them to the target. SQL Server provides a set of policy list and policy files which can be imported and used as a best practice solution. You can then evaluate your targets for example, the database instance, instance objects or the database objects.

We recommend that, in addition to any policies required by your clinic or hospital, you create policies to manage the following:

XP Command Shell: XP command shell service can potentially be dangerous from a security perspective. It has the same privilege level as the SQL Server Service. This means users with access can run system level commands via the shell. If by chance a hacker gains access to the system, they can run arbitrary commands on the server. They can even create new security policy to look for changes of configuration or disable security policies, leaving the system vulnerable.

Log in Creation Prevention: SQL Server can use Windows password policy mechanisms. The password policy applies to SQL Server authentication and database users with password. We recommend clinic or hospital IT administrators use policy based management to strengthen security around clinical database management and usage.

For more information on policy management please view the links below or contact your Microsoft vendor.

- ***Administer Servers by Using Policy-Based Management***

  (https://docs.microsoft.com/en-us/sql/relational-databases/policy-based-management/administer-servers-by-using-policy-based-management?view=sql-server-ver15)

- ***Monitor and Enforce Best Practices by Using Policy-Based Management***

  (https://docs.microsoft.com/en-us/sql/relational-databases/policy-based-management/monitor-and-enforce-best-practices-by-using-policy-based-management?view=sql-server-ver15)

- ***Create a New Policy-Based Management Condition***

  (https://docs.microsoft.com/en-us/sql/relational-databases/policy-based-management/create-a-new-policy-based-management-condition?view=sql-server-ver15)

- ***xp_cmdshell Server configuration option***

  (https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/xp-cmdshell-server-configuration-option?view=sql-server-ver15)

- ***Password Policy***

  (https://docs.microsoft.com/en-us/sql/relational-databases/security/password-policy?view=sql-server-ver15)

SQL assistant tools

This section describes some tools and best practices policy sets available that can be used to make clinical database environment safe and secure.

SQL vulnerability assessment tool

The SQL vulnerability assessment tool can help you discover, track, and remediate potential database vulnerabilities. You can use it to proactively improve your database security. This vulnerability assessment tool is available in SQL Server Management Studio (SSMS) for SQL Server 2012 or later.

Please refer to this Microsoft article below for more information about this tool usage and baseline security setting for your clinical database.

- ***Vulnerability assessment for SQL Server***

  (https://docs.microsoft.com/en-us/sql/relational-databases/security/sql-vulnerability-assessment?view=sql-server-ver15)

Belarc Advisor - BelSecure

The BelSecure software automatically performs a vulnerability assessment of your IT systems, checking security policies, configuration settings and discovering other information about the host such as anti-virus status, application versions, security patches, user accounts and more. Policy settings are then automatically compared with consensus benchmarks from NIST (Windows 10 DISA STIG), which allow IT administrators to automatically determine the security status of their IT assets in advance of an attack.

Please refer to BelSecure product link for more details.

- ***PRODUCTS : BelSecure***

  (https://www.belarc.com/products_belsecure)

SQL Server agent's service documentation

This document from Microsoft provides the best practices for setting up your accounts to run SQL Server services. It provides detailed information about the limitations of some common tasks and information about using local system accounts or SQL Service “this account” to run a service.

- ***Select an Account for the SQL Server Agent Service***

  (https://docs.microsoft.com/en-us/sql/ssms/agent/select-an-account-for-the-sql-server-agent-service?view=sql-server-ver15)

Decommission and disposal

This section contains information on how to safely decommission and dispose of the Custom Sound Pro software and includes, safe guarding personal and health-related data in connection with security and privacy.

To safely decommission the Custom Sound Pro software:

1. Back up the clinical database.
2. Remove the instance of the clinical database.
3. Uninstall the Custom Sound Pro software.
4. (Optional) Uninstall Microsoft SQL Server .

For more information on how to perform each of these tasks, please see the section below.

Back up database

To back up the clinical database, please use the Backup function of the Cochlear Database Manager. See the section ***Back up or restore a database*** in this Installation Guide for instruction on how to do this. If you no longer have access to the Cochlear Database Manager you can also perform a backup using the SQL Server Management Studio.

For more information on how to do this, please view the link below or contact your Microsoft vendor.

- ***Quickstart: Backup and restore a SQL Server database on-premises***

  (https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/quickstart-backup-restore-database?view=sql-server-ver15)

Remove the instance of the clinical database

To remove the clinical database, please use the Delete function of the Cochlear Database Manager. See the section ***Delete a database*** in this Installation Guide for instruction on how to do this. If you no longer have access to the Cochlear Database Manager you can also remove a database instance using the SQL Server Utility.

For more information on how to do this, please view the link below or contact your Microsoft vendor.

- ***Remove an Instance of SQL Server from the SQL Server Utility***

  (https://docs.microsoft.com/en-us/sql/relational-databases/manage/remove-an-instance-of-sql-server-from-the-sql-server-utility?view=sql-server-ver15)

Uninstall Custom Sound Pro software

If the Custom Sound Pro software is no longer required, you can uninstall the software using the uninstall tool.

To uninstall the Custom Sound Pro software:

1. Navigate to **Settings** from the Windows Start menu and then choose **Apps**.
2. Select **Custom Sound (Version)**. For example, Custom Sound 7.1.
3. Select **Uninstall**.
4. Follow the uninstallation wizard to remove the software.

Custom Sound Pro software will be uninstalled.

Remove Microsoft SQL Server

If your clinical database instance is being hosted on a shared database server then you will not want to remove Microsoft SQL Server. But, if the clinical database is hosted alone or SQL Server is no longer required, you can uninstall Microsoft SQL Server.

For more information on how to use the SQL Server Utility, please view the link below or contact your Microsoft vendor.

- ***Uninstall an Existing Instance of SQL Server (Setup)***

  (https://docs.microsoft.com/en-us/sql/sql-server/install/uninstall-an-existing-instance-of-sql-server-setup?view=sql-server-ver15&tabs=Windows10)

Other information

This section contains other technical information for the Custom Sound Pro software.

Ranges and precision

Range: Ranges for values, where applicable, are displayed within the user interface of Custom Sound Pro software.

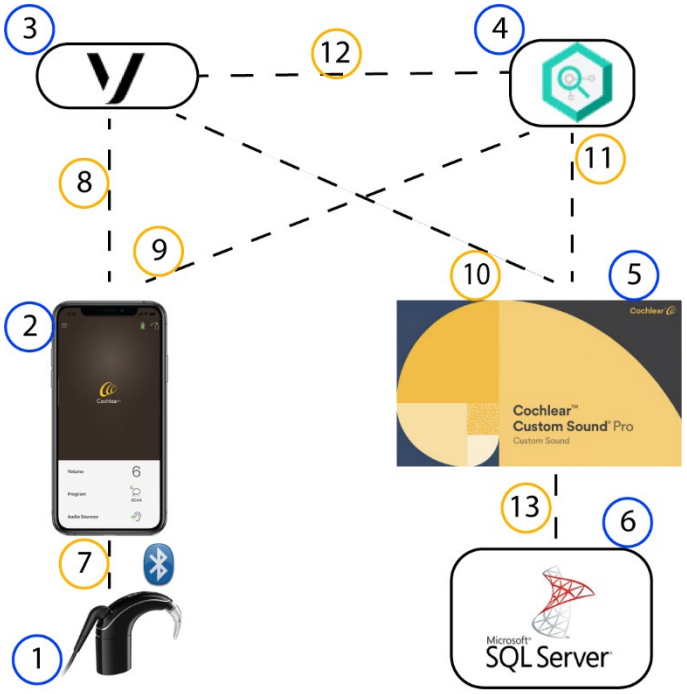
Precision: The precision (rounding) values for the following measurements are shown below.

Value	Precision
Impedance	two decimal places
T-NRT	nearest integer
Current Levels (T & C)	nearest integer
Dynamic Range	nearest integer
Frequency	nearest integer
Gain	nearest integer
Battery health	nearest integer
Data viewer	nearest integer (hours)
Stimulation rate	nearest 100 Hz

Network Specifications

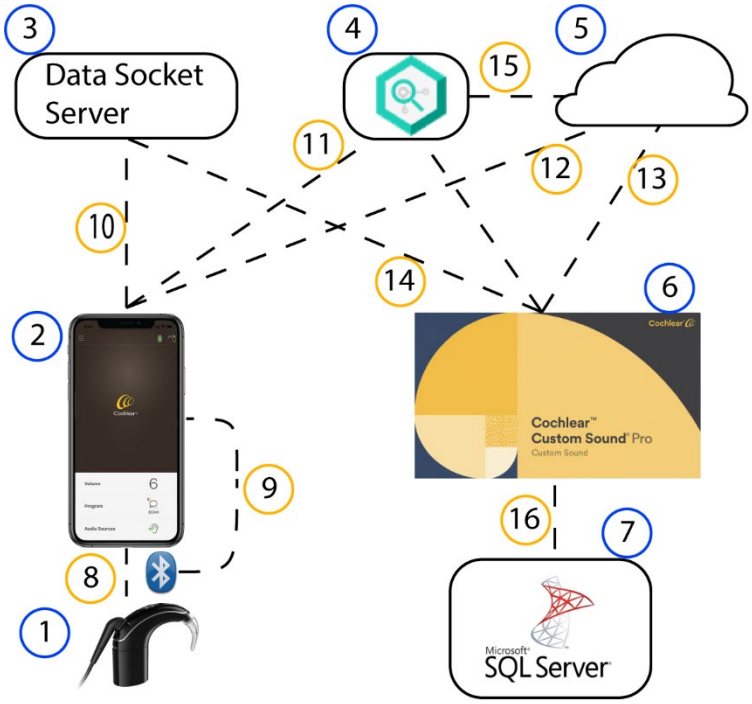
The following diagrams show the flow of information between the Custom Sound Pro software and other software applications when using the Remote Assist feature. These diagrams show the flow of information to a Remote Assist chat and video session and a data session where the clinician is making changes to the MAPs or processor settings remotely. Each diagram shows a description of the services or applications connected as well as the specification of the connection type.

Custom Sound Pro software with Remote Assist - Video and chat information flow



Key	Description
1	Sound processor
2	Nucleus® Smart App on a compatible iOS or Android device using the screen, camera and microphone of the device.
3	Vonage Video API (Application Programming Interface) cloud
4	Atlas Services API
5	Custom Sound Pro software
6	Microsoft SQL Server database
7	BLE audio control between the iOS or Android device and the sound processor
8	Web RTC (Web real-time communication) audio visual stream between Nucleus Smart App and Vonage
9	HTTPS AV session setup
10	Web RTC (Web real-time communication) audio visual stream between Custom Sound Pro software and Vonage
11	HTTPS audio visual session setup between Custom Sound Pro software and Atlas Services API
12	HTTPS audio visual session setup between Vonage and Atlas Services API
13	TCP/IP

Custom Sound Pro software with Remote Assist - Data information flow



Key	Description
1	Sound processor
2	Nucleus Smart App on a compatible iOS or Android device using the screen, camera and microphone of the device.
3	WebSockets API Gateway
4	Atlas Services API (Application Programming Interface)
5	CIM/SFDC (Cloud Information Model/Salesforce Dot Com)
6	Custom Sound Pro software
7	Microsoft SQL Server database
8	BLE (Bluetooth Low Energy) audio control between the iOS or Android device and the sound processor
9	SPAPI (Sound Processor Application Programming Interface) over BLE
10	SPAPI over secure WebSocket over TCP
11	HTTPS authentication authorisation between Nucleus Smart App and Atlas Services API
12	HTTPS authentication
13	HTTPS authentication
14	SPAPI over secure WebSocket over TCP
15	HTTPS authentication
16	TCP/IP

Custom Sound Pro software with Cochlear Cloud intraoperative data import

The following diagram shows the flow of information between the Custom Sound Pro software and the Cochlear Cloud when importing intraoperative data. The diagram shows a description of the services or applications connected as well as the specification of the connection type.

Key	Description
1	Microsoft SQL Server database
2	Custom Sound Pro software
3	Cochlear Cloud
4	TCP/IP
5	HTTPS

Configuration

After Nucleus SmartNav has been installed on an iPad, Nucleus SmartNav and Custom Sound® Pro software must be configured using the settings below if the iPad will be connected to:

- the Wi-Fi network of an organisation
- the local network of a clinic. This includes clinic workstations that are using Custom Sound Pro software.

Requirements	Nucleus SmartNav and Custom Sound Pro software
Firewall Settings on HTTPS port 443 TLS/SSL interception for the following fully qualified domain names (FQDNs) will need to be disabled or permitted for iPads with Nucleus SmartNav installed and clinic workstations using Custom Sound® Pro software.)	**myCochlear™ Professional Portal**
	FQDN: https://atlas-couch.mycochlear.com FQDN: https://secure.mycochlear.com FQDN: https://clinician-portal.mycochlear.com
	Authentication for SmartNav services
	FQDN: https://customsoundpro-api.cochlear.link FQDN: https://atlas-api.cochlear.link FQDN: https://www.cochlear.com FQDN: https://cochlear.force.com FQDN: https://id.cochlear.com
	Enable functionality for majority of application functions For example, firmware updates, secure cloud data transfer initiation
	FQDN: https://smartnav-api.cochlear.link Custom Sound update URL: https://csds-api.cochlear.link Redirect URL for Custom Sound update: https://d25fud42317hnc.cloudfront.net
	End destination of secure cloud data transfer Completes secure cloud data transfer
	FQDN: https://intraoperative-file-service-prd-upload-bucket.s3.eu-west-1.amazonaws.com
	Secure session data import communication
	FQDN: https://data-socket-server.cochlear.link
	Enables functionality to check upon launch of app for newer app versions and notify user
	FQDN: https://discovery.cochlear.link

Requirements	Nucleus SmartNav and Custom Sound Pro software
Port settings (Basic)	80 and 443 (HTTP and HTTPS)
USB ports	Apple® Lightning® to USB adapter (for USB data transfer only)
Camera (Optional)	For scanning implant details from data codes on the implant packaging
Notifications (Optional)	To inform users of actions required
Bluetooth® (Required)	To enable connectivity between the Cochlear Surgical Processor and Nucleus SmartNav
Secure Cloud Data Transfer (Intraoperative data)	To ensure cloud data transfer is available, ensure the following are allowed and open outbound port 443 on the iPad. After a user authenticates using Professional Account credentials in Custom Sound Pro software, data download can be initiated.
	Data import to Custom Sound Pro software:
	FQDN: https://customsoundpro-api.cochlear.link
	Data upload to Cochlear Cloud from SmartNav:
	FQDN: https://intraoperative-file-service-prd-upload-bucket.s3.eu-west-1.amazonaws.com
	Baseline functionality that enables data upload to Cochlear Cloud:
	FQDN: https://smartnav-api.cochlear.link
	Enable user login to initiate Cochlear Cloud data upload / download:
	FQDN: https://atlas-api.cochlear.link
Proxy Settings (If a proxy server is utilised)	Transparent proxy or it must be configured in the browser for HTTPS connections

Note: Information provided is correct as of date of publication but is subject to change without notice.

Risks of software and network

Cochlear wishes to advise that running the Custom Sound Pro software with a networked database or using the Remote Assist feature (which requires internet access) could cause potential risks to patients, software users or third-parties. We recommend you perform your own evaluation to identify, analyse, evaluate and control these risks.

Changes to your network could introduce additional risks.

These changes include:

- Changes to the network configuration.
- Introducing new network hardware or software.
- Updating or upgrading network hardware or software.

Cochlear identified the following situations that may result from network failure. These should be communicated to the patient prior to a session.

- If the Remote Assist session ends with unsaved adjustments made by the clinician, those changes will revert to their previous state when the patient's sound processor restarts.
- If there is an interruption in communication that causes uncomfortable stimulation, the patient should remove the coil, cable and sound processor as soon as communication through Remote Assist stops or they experience uncomfortable stimulation.

Troubleshooting

Issue	Resolution
You have an issue during installation with access rights to the local computer or the installation fails to run.	To clear this issue, try the following steps: 1. Before attempting to install again: • Sign in as an Administrator or an account with administrator rights. • Empty the TEMP folder. (To open the TEMP folder, type %TEMP% in the address bar of Windows Explorer and press Enter). • Disable the anti-virus software. Make sure windows defender is disabled. 2. Try to install again: • Run the Custom Sound Pro software installer previously downloaded.
Custom Sound Pro software is blocked by anti-virus software when running it after installation.	Add Custom Sound Pro software to the allowed list of any anti-virus software installed on the local computer. For more information on how to do this, consult the help or support documentation for your anti-virus software.

Issue	Resolution
You get a pop-up during the installation process that some dependencies failed to install. For example, Microsoft .NET framework.	To clear this issue, try the following steps: 1. Before attempting to install again: • Sign in as an Administrator or an account with administrator rights. • Empty the TEMP folder. (To open the TEMP folder, type %TEMP% in the address bar of Windows Explorer and press Enter). • Disable the anti-virus software. Make sure windows defender is disabled. 2. Update windows • Run the windows '***Check for updates***' command. • Restart your system once the updates have been installed. 3. Try to install again: • Run the Custom Sound Pro software installer previously downloaded.
You get a message during installation that SQL Server has not installed correctly or that there is an issue accessing or creating the database.	For standalone installations, try the following steps: 1. Before attempting to install again: • Sign in as an Administrator or an account with administrator rights. • Empty the TEMP folder. (To open the TEMP folder, type %TEMP% in the address bar of Windows Explorer and press Enter). • Disable the anti-virus software. Make sure windows defender is disabled. 2. Update windows • Run the windows '***Check for updates***' command. • Restart your system once the updates have been installed. 3. Try to install again: • Run the Custom Sound Pro software installer previously downloaded.

Issue	Resolution
	For network installations, try the following steps: 1. Before attempting to install again: • Sign in as an Administrator or an account with administrator rights. • Empty the TEMP folder. (To open the TEMP folder, type %TEMP% in the address bar of Windows Explorer and press Enter). • Disable the anti-virus software. Make sure windows defender is disabled. 2. Update windows • Run the windows '***Check for updates***' command. • Restart your system once the updates have been installed. 3. Check the connection to the Server • Run ***CMD*** (as admin): ***PING <server ip address>*** to check that the client is able to connect to the server and that the server is running. 4. Try to install again: • Run the Custom Sound Pro software installer previously downloaded.

Notes

AU **Cochlear Ltd** (ABN 96 002 618 073)
1 University Avenue, Macquarie University, NSW 2109, Australia
Tel: +61 2 9428 6555

EC REP DE **Cochlear Deutschland GmbH & Co. KG**
Mailänder Straße 4 a, 30539 Hannover, Germany
Tel: +49 511 542 770

CH REP CH **Cochlear AG**
Peter Merian-Weg 4, 4052 Basel, Switzerland
Tel: +41 61 205 8204

US **Cochlear Americas**
10350 Park Meadows Drive, Lone Tree, CO 80124, USA
Tel: +1 (800) 523 5798

CA **Cochlear Canada Inc**
2500-120 Adelaide Street West, Toronto, ON M5H 1T1, Canada
Tel: +1 (800) 523 5798

GB **UK Responsible Person: Cochlear Europe Ltd**
6 Dashwood Lang Road, Bourne Business Park, Addlestone,
Surrey KT15 2HJ, United Kingdom
Tel: +44 1932 26 3400

BE **Cochlear Benelux NV**
Schaliënhoevedreef 20 i, B-2800 Mechelen, Belgium
Tel: +32 15 79 55 11

FR **Cochlear France S.A.S.**
135 Route de Saint-Simon, 31035 Toulouse, France
Tel: +33 5 34 63 85 85 (International) or 0805 200 016 (National)

IT **Cochlear Italia S.r.l.**
Via Trattati Comunitari Europei 1957-2007 n.17,
40127 Bologna (BO), Italy
Tel: +39 051 601 53 11

SE **Cochlear Nordic AB**
Konstruktionsvägen 14, 435 33 Mölnlycke, Sweden
Tel +46 31 335 14 61

www.cochlear.com

TR **Cochlear Tıbbi Cihazlar ve Sağlık Hizmetleri Ltd. Şti.**
Küçükbakkalköy Mah, Defne Sok, Büyükhanlı Plaza No:3 Kat:3
Daire: 9-10-11-12, 34750, Ataşehir, İstanbul, Türkiye
Tel: +90 216 538 5900

HK **Cochlear (HK) Limited**
Room 1404-1406, 14/F, Leighton Centre, 77 Leighton Road,
Causeway Bay, Hong Kong
Tel: +852 2530 5773

KR **Cochlear Korea Ltd**
2nd Floor, Yongsan Centreville Asterium, 25,
Hangang-daero 30 gil, Yongsan-gu, Seoul, Korea (04386)
Tel: +82 2 533 4450

CN **Cochlear Medical Device (Beijing) Co., Ltd**
Unit 2608-2617, 26th Floor, No.9 Building, No.91 Jianguo Road,
Chaoyang District, Beijing 100022, P.R. China
Tel: +86 10 5909 7800

IN **Cochlear Medical Device Company India Pvt. Ltd.**
Ground Floor, Platina Building, Plot No C-59, G-Block,
Bandra Kurla Complex, Bandra (E), Mumbai – 400 051, India
Tel: +91 22 6112 1111

JP **株式会社日本コクレア(Nihon Cochlear Co Ltd)**
〒113-0033 東京都文京区本郷2-3-7 お茶の水元町ビル
Tel: +81 3 3817 0241

AE **Cochlear Middle East FZ-LLC**
Dubai Healthcare City, Al Razi Building 64, Block A, Ground Floor,
Offices IR1 and IR2, Dubai, United Arab Emirates
Tel: +971 4 818 4400

PA **Cochlear Latinoamérica S.A.**
International Business Park, Building 3835, Office 403,
Panama Pacifico, Panama
Tel: +507 830 6220

NZ **Cochlear NZ Limited**
Level 4, Takapuna Towers, 19-21 Como St, Takapuna,
Auckland 0622, New Zealand
Tel: + 64 9 914 1983

D2008088-V2 2025-03