Silhouette®

Wound + Skin Assessment

Silhouette v4.23

Installation Guide

aranzmedical

This document has been prepared by ARANZ Medical Limited for its customers. The content of this document is confidential. It may be reproduced only with written permission from ARANZ Medical Limited. Specifications contained herein are subject to change, and these changes will be reported in subsequent revisions or editions. The device described in this document cannot substitute for the knowledge, skill, and experience of the competent medical personnel who are its intended users. Its use as such a substitute is prohibited.

Copyright © 2018-2026 ARANZ Medical Limited

All rights reserved. Unauthorized use, reproduction, or disclosure is prohibited. Patents pending. No patent liability is assumed with respect to the use of the information contained herein. While every precaution has been taken in the preparation of this user's guide, ARANZ Medical assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from use of the information contained herein.

CE 0123

ARANZ Medical Limited
Tel +64-3-374 6120
Fax +64-3-374 6130
www.aranzmedical.com

Postal Address:
ARANZ Medical
PO Box 3894
Christchurch 8140
New Zealand

Delivery Address:
ARANZ Medical
47 Hereford Street
Christchurch 8013
New Zealand

To report a serious incident involving an ARANZ Medical Silhouette product, please contact your local representative using the information provided below. When reporting an incident please provide detailed information about the incident, including the device model, lot number or software version, and a description of the event. Reports must be filed in a timely manner in accordance with the reporting requirements specified by the competent authorities in your country.

EC REP

European (EC) Authorised Representative

mdi Europa GmbH
Langenhagener Str. 71
30855 Langenhagen
Germany
Phone +49 (0)511 39089530
werner.sander@mdi-europa.com

US REP

FDA Authorised Representative

MDI Consultants
55 Northern Blvd
Great Neck, NY 11021
Phone +1 (516) 482 9001
alan@mdiconsultants.com

AU REP

Australian Representative

KD&A Pty Ltd
Suite 13, 67 Wanganella Street
Balgowlah NSW 2093
Australia
Phone +61 411 101 392
kdent@kdas.com.au

ARANZ Medical Limited documentation often refers to hardware or software products by their trade names. In most, if not all, cases these designations are claimed as trademarks or registered trademarks of their respective companies. The trade names are used here for identification purposes only.

Document Number: 2018-00262 Rev25.0

Reference: 7d454bf41a7b597457d64799cac4abb21f82e277

Contents

Introduction ... **1**

Notation Convention ... 1

SilhouetteCentral Installation ... **2**

Pre-Installation Planning ... 3

Server Prerequisites and Dependencies ... 5

Add the Web Server role to Microsoft Windows Server (Internet Information Services IIS) ... 5

Update .NET Framework 4 ... 5

Add ASP.NET Core 10.0 Runtime ... 6

Add VC++ Runtime ... 6

Preparing a SQL Server Database ... 7

SilhouetteCentral Dashboard Feature ... 7

Preparing a SQL Server Synchronization Instance ... 8

SilhouetteCentral Web Application Installation ... 9

Configure IIS to Serve the SilhouetteCentral Web Application ... 9

SilhouetteTokenService Web Application Installation ... 11

Configure IIS to Serve the SilhouetteTokenService Web Application ... 11

SilhouetteCentral Initial Configuration Wizard ... 13

SilhouetteTokenService Web Application Configuration ... 15

Database Connection String ... 15

Logo ... 16

Local Silhouette Users ... 16

Logging ... 19

SAML2 Configuration ... 19

Advanced SilhouetteCentral Web Application Configuration ... 23

Patient Assessment Data File Location ... 23

SilhouetteConnect Synchronization Related Settings ... 23

Temporary Storage ... 24

System Events, Email, and Integration Event Application Settings ... 24

Assessment Data Export Related Settings ... 25

File clean up schedule ... 25

Inactive SSO User Expiry ... 25

Purge orphaned documents on SilhouetteCentral ... 25

Dashboard Feature ... 26

Login and Reset Default User Passwords ... 27

Configure Fundamental System Settings ... 28

IIS Configuration Recommendations ... 29

Strict Transport Security (HSTS) ... 29

Copyright © 2018-2026 ARANZ Medical Limited

SilhouetteCentral Maintenance **30**
SilhouetteCentral Backup 30
SilhouetteCentral Database Maintenance 30
SilhouetteCentral Upgrade 31
Versions 32
SilhouetteConnect Installation and Initial Configuration **37**
SilhouetteConnect Pre-Installation Planning 38
Pre-requisites for installing SilhouetteConnect on Windows 11 39
Installing SilhouetteConnect 40
Installing SilhouetteConnect Synced Mode 41
Installing SilhouetteConnect Standalone 42
SilhouetteConnect Setup Screen 43
SilhouetteStar 2 Firewall Rules and Networking 45
Upgrading SilhouetteConnect 45
Uninstalling SilhouetteConnect 46
SilhouetteConnect File Storage and Backup 47
Standalone Mode Storage and Backup 47
Sync Mode Storage and Backup 48
SilhouetteConnect Archive and Backup Data Retention 49
Licensing **50**
Licensing SilhouetteCentral or SilhouetteConnect 50
Licensing SilhouetteTokenService 50
System Configuration **51**
Single Sign On with an External Authentication Provider 52
Example: Configuring Silhouette SSO Integration with AD FS 52
Configure the SilhouetteTokenService 53
Add Silhouette as a Relying Party Trust to the AD FS Server 53
Map Authentication Provider Claims to Silhouette Role and Clinical Data Access 56
Disable Silhouette Local User Login 57
Emergency Access During an Identity Provider Outage 57
Machine Settings File **59**
SilhouetteCentral Testing **60**
Verify Basic SilhouetteCentral Operation with Local Silhouette Users 61
1: Login/Logout with a Silhouette Local User account 61
2: Verify Help and About page is accessible 61
Verify SilhouetteConnect Sync 62
1: Login to SilhouetteConnect and perform a sync 62
Verify Single Sign On with an External Authentication Provider 63
1: Login with an external authentication provider user account 63

Copyright © 2018-2026 ARANZ Medical Limited

2: Verify Allow Local Login (Silhouette Local users) is disabled 63
3: Verify an external authentication provider has been disabled 64
Troubleshooting **65**
SilhouetteTokenService Troubleshooting 66
SilhouetteCentral Troubleshooting 67
SilhouetteConnect Troubleshooting 68
Problems when starting SilhouetteConnect 68
Problems when logging in 68
Problems when syncing 68
Appendices **70**
Appendix A: IIS Configuration 71
Configure IIS using the IIS Management Console 71
Configure IIS via Windows PowerShell 71
IIS and File System Permissions 73
Appendix B: SQL Server Configuration 74
Installing SQL Server 74
Creating a SilhouetteCentral Database 75
Creating a Database using SQL Server Management Studio 75
Creating a Database using Windows PowerShell 75
Appendix C: AD FS Custom Filter Rule Example 77
Rule 1 - Issue non-group claims 77
Rule 2 - Add groups to claims 77
Rule 3 - Issue a filtered set of group claims 78

Copyright © 2018-2026 ARANZ Medical Limited

Introduction

This Installation and Configuration Guide focuses on the pre-planning, installation, and initial configuration of the Silhouette™ system.

The intended audience for this guide includes Project Managers, Systems Administrators, and IT Personnel.

Other useful sources of help:

- For general usage of the Silhouette system, refer to the Silhouette Clinical User's Guide or the Silhouette Administration User's Guide.
- The Silhouette Administration User's Guide contains a system description with information on the system components, the system security, and the optional features.
- For the latest system requirements and operating conditions refer to the www.aranzmedical.com web site. If you need the system requirements for a specific Silhouette version, please contact ARANZ support with your request.

This guide is applicable to following versions of Silhouette Components:

- SilhouetteCentral version 4.23.
- SilhouetteConnect version 4.23.

Notation Convention

Throughout this guide, screen, menu, and field names in SilhouetteCentral are displayed in a **bold font**. A series of actions are shown as follows:

Admin > Organization > Settings

which means to select the **Settings** option in the **Organization** menu in the SilhouetteCentral **Admin** section.

Copyright © 2018-2026 ARANZ Medical Limited

SilhouetteCentral Installation

This section describes the installation and initial configuration of SilhouetteCentral, including the SilhouetteTokenService.

A very high-level view of the process is provided here:

- Do the pre-installation planning and preparation.
  - See the Pre-Installation Planning topic.
- Prepare the web server and database.
  - See the Server Prerequisites and Dependencies topic.
  - See the Preparing a SQL Server Database topic.
  - See the Preparing a SQL Server Synchronization Instance topic.
- Install the SilhouetteCentral and SilhouetteTokenService Web Applications.
  - See the SilhouetteCentral Web Application Installation topic.
  - See the SilhouetteTokenService Web Application Installation topic.
- Configure the Web Applications.
  - See the SilhouetteCentral Initial Configuration Wizard topic.
  - See the SilhouetteTokenService Web Application Configuration topic.
  - See the Advanced SilhouetteCentral Web Application Configuration topic.
- Do the initial login and set the system wide parameters.
  - See the Login and Reset Default User Passwords topic.
  - See the Configure Fundamental System Settings topic.

A number of tests and checks are listed in the topic SilhouetteCentral Testing to help confirm that the system is installed and configured correctly.

Copyright © 2018-2026 ARANZ Medical Limited

Pre-Installation Planning

The following pre-installation steps should be performed before commencing the installation of SilhouetteCentral:

1	Review the Silhouette CTEULA and Terms of Use, see the ARANZ Medical website (https://www.aranzmedical.com/silhouette-legal/). Installing and using SilhouetteCentral means that you accept these conditions.	☐
2	The SilhouetteCentral is a web application using Microsoft .NET v4 framework and Microsoft .NET runtime and is designed to be served by Microsoft Internet Information Services (IIS) on the Microsoft Windows Server operating system. Patient demographic and assessment data is stored in a Microsoft SQL Server database, while images are stored outside of the database on the file system. Review the latest system requirements and operating conditions from www.aranzmedical.com to ensure the targeted installation platforms and networks are adequate.	☐
3	Plan the network location and network firewall configurations for SilhouetteCentral, considering where users will need to access the system from (e.g. nurses may need to use the system from patient's homes or remote clinics).	☐
4	Define the desired URL of the SilhouetteCentral website. The recommended setup for running the main SilhouetteCentral web application and the SilhouetteTokenService is one website with two sub virtual directories. This means that there is one URL required with one SSL certificate. It also means that there is always a path component in the URL. e.g. http://<sub-domain>.<domain name>/<path>/. The path for the main SilhouetteCentral application is typically deployed as *silhouette* and the path for the SilhouetteTokenService application is typically deployed as *silhouettetoken*. The path component of the URL is case sensitive and the consistent use of lower case helps reduce configuration errors later.	☐
5	Plan how SSL certificates will be managed to allow HTTPS to be used. HTTPS communication is required to encrypt data between SilhouetteCentral and the other Silhouette system components. HTTPS communication is also required for the use of SSO with external authentication providers. HTTPS is required for the use of SilhouetteLite or SilhouetteMobile with SilhouetteCentral. These apps do not support unencrypted HTTP connections to SilhouetteCentral.	☐
6	The encryption requirements for the server file system and the database are understood and any required keys and recovery mechanisms are prepared. The SQL Server connection certificates are trusted on the server, or the use of SQL Server fallback encryption (self-signed certificate) are approved.	☐
7	The service account required to run the SilhouetteCentral and SilhouetteTokenService Web Applications have been created and credentials are available. It is not possible to use the IIS DefaultApplicationPool identity if you wish to use Windows Authentication to access SQL Server instance hosted on a different machine than the web server. If planning to use the use the IIS DefaultApplicationPool identity, SQL Server access will be through SQL Authentication mode.	☐

Copyright © 2018-2026 ARANZ Medical Limited

8	Gather the details of the SQL server to host the Silhouette database, including: • SQL Server name • Database name • SQL Server Authentication details (Authentication mode + SQL Server Login credentials)	☐
9	Backup requirements for clinical data stored within Silhouette are understood and backup systems are prepared.	☐
10	The SMTP server details are known. SilhouetteCentral requires SMTP server access to send password reset emails or assessment emails. The details required are listed below and can be entered after installation if required. • SMTP Host • SMTP Port • Use SSL • Sender Email Address • User Name • Password	☐
11	Enable network access to allow the Silhouette automatic licensing process to work. SilhouetteCentral must be able to reach the following URLs: • https://www.silhouettecentral.com/licensing/LicenseDownload.ashx • https://www.silhouettecentral.com/licensing/SilhouetteCentralLicenseService.asmx • https://europe.silhouettecentral.com/licensing/LicenseDownload.ashx • https://europe.silhouettecentral.com/licensing/SilhouetteCentralLicenseService.asmx A generic rule to allow access to https://*.silhouettecentral.com/licensing/ is recommended to allow for any changes in the licensing. If access to these destinations is not enabled the licensing process can be completed offline.	☐
12	Silhouette users and their system access is determined.	☐

Aside from the technical installation considerations, to gain the most out of Silhouette, it is recommended that there is time spent planning how different users are going to use the different components of the system. A demonstration or trial of the system maybe appropriate in some cases to assist with this planning.

The Silhouette system is a powerful tool enabling wound data capture at the point of care, which can assist in the achievement of great clinical results. Spending time defining what data you want to collect can help achieve the desired results, while optimizing workflow for clinical staff.

Copyright © 2018-2026 ARANZ Medical Limited

Server Prerequisites and Dependencies

The items listed in this section form some of the dependencies required to run SilhouetteCentral.

It is not intended that this guide offer complete installation instructions for these components as each have their own complete guides. This guide provides instructions on required configuration options.

Standard configuration and security hardening of these dependencies are not included in this guide.

Add the Web Server role to Microsoft Windows Server (Internet Information Services IIS)

Prior to the installation of SilhouetteCentral you must ensure the server you are installing onto has Internet Information Server (IIS) installed and configured. IIS is an optional component of the Microsoft Windows operating system.

IIS has many optional features. Silhouette requires the following IIS feature set as a minimum:

- Web Server > Common HTTP Features > Static Content (Web-Static-Content)
- Web Server > Application Development > Application Initialization (Web-AppInit)
- Web Server > Application Development > ASP.NET 4.7[1] (Web-Asp-Net45)
- Web Server > Application Development > WebSocket Protocol (Web-WebSockets)
- Management Tools > IIS Management Console (Web-Mgmt-Console)

Follow the instructions for adding features to IIS for your version of Microsoft Windows Server.



The names of the features in brackets above are the feature names used when installing via PowerShell. For example:

```
Import-Module ServerManager

Add-WindowsFeature `
 -Name Web-Static-Content,Web-ASP-Net45,Web-Mgmt-Console, `
 Web-AppInit,Web-WebSockets
```

Installing using the PowerShell cmdlet to add features includes just the features listed; it does not include all components selected by default when installing using the Server Manager UI. For example, the components Web-Dir-Browsing, Web-Http-Errors, Web-Http-Logging and Web-Stat-Compression are selected by default when installing using the Server Manager UI.

Update .NET Framework 4

The SilhouetteCentral web application uses Microsoft .NET Framework v4.8, which must be installed on the server in addition to IIS. If .NET v4.8 is not already installed, .NET can be downloaded from https://dotnet.microsoft.com/. In some circumstances a reboot of the server may be required during or after the installation.

[1]The actual ASP.NET version number listed in the feature name is server version dependent and does not change when later .NET Framework 4.x versions are installed.

Copyright © 2018-2026 ARANZ Medical Limited

Refer to Microsoft's website for "How to: Determine which .NET Framework versions are installed?" to determine which versions of the .NET Framework are installed.

Windows updates can occasionally cause problems with installed .NET frameworks. Microsoft offer a "Microsoft .NET Framework Repair Tool" that detects and repairs frequently occurring .NET Framework issues. This repair tool should be run if SilhouetteCentral reports non-Silhouette related errors when trying to start.

Add ASP.NET Core 10.0 Runtime

The SilhouetteTokenService component of Silhouette uses the ASP.NET Core 10.0 Runtime. A hosting bundle is available which includes both the ASP.NET Core Runtime and IIS runtime support (ASP.NET Core Module v2) and it is recommended to install the hosting bundle.

Add VC++ Runtime

The SilhouetteCentral website requires that VC++ v14 runtime is installed (the version supported by Visual Studio 2015, 2017, 2019, and 2022) to show the *Help and About* page. Server environments often already have the required runtime, however, the installer can be downloaded directly from Microsoft if required, see https://aka.ms/vs/17/release/vc_redist.x64.exe.

Copyright © 2018-2026 ARANZ Medical Limited

Preparing a SQL Server Database

SilhouetteCentral stores all patient demographic and assessment data in a MS SQL Server database. The SilhouetteCentral and SilhouetteTokenService web applications both use the same database.

Typically, deployments use a database provisioned on existing dedicated database servers. However, deployments can be hosted with MS SQL Server running on the same server as the web applications if existing infrastructure is not available, see Appendix B: SQL Server Configuration. If choosing to run SQL Server and the website on the same server, the server needs to be sized appropriately for both systems to run well.

Before preparing the SQL Server database it is necessary to know the authentication mode and identities the SilhouetteCentral and SilhouetteTokenService web applications will be using to connect to the SQL Server. If the authentication mode is to be Windows Authentication, it is helpful to have already setup the identities before completing the SQL Server database setup.

If the IIS Application Pools are going to use the default ApplicationPoolIdentity with SQL Server Windows Authentication mode (only possible if the SQL Server instance is on the same server as IIS), create the Application Pools in IIS before attempting the setup.

You need to obtain the required connection details to access the database. These details include:

- SQL Server Instance name, i.e. serverName\instanceName.
- Authentication method (Windows Authentication or SQL Server). If the authentication method selected is "SQL Server," you need the associated username and password.
- Database name, e.g. silhouette.
- Confirmation that the SQL Server uses encrypted connections with a well-known (or organizationally trusted) CA or that the use of SQL Server fallback encryption (self-signed certificate) is approved.

Your Database Administrator (DBA) should be able to create the database and provide these details to you.

The database principal or principals used by the SilhouetteCentral and SilhouetteTokenService IIS Application Pools must be allocated the database ownership role for the database. If the applications use different identities, grant access to both. If they use the same custom service account, or use ApplicationPoolIdentity to reach a remote SQL Server as the IIS server's domain computer account, grant that shared principal once. See Appendix B: SQL Server Configuration for examples. The database can be created empty and the Silhouette applications populate it during the installation procedure.

SilhouetteCentral Dashboard Feature

When the optional Dashboard feature is licensed in SilhouetteCentral then you will require a second login/user account that the dashboard engine will use to connect to the database. This login must use "SQL Server" authentication, so you will need the associated username and password.

The user account should then be assigned to the 'rpt_reader' role, and no others. Note that this role will only exist after SilhouetteCentral has run its initial database upgrade.

The connection string used by the dashboard service will need to be set in the settings file for SilhouetteCentral. See the Dashboard Feature section in SilhouetteCentral Web Application Configuration

Copyright © 2018-2026 ARANZ Medical Limited

Preparing a SQL Server Synchronization Instance

If SilhouetteConnect is being supported, then SilhouetteCentral will need access to a MS SQL Server Express LocalDB 2022 instance to be used for the Synchronization process.

The synchronization instance must be a MS SQL Server LocalDB that is compatible with the version used in SilhouetteConnect. The version of MS SQL Server LocalDB used for the synchronization instance can be updated as long as both the version distributed with SilhouetteConnect and the version on SilhouetteCentral remain compatible.

Copyright © 2018-2026 ARANZ Medical Limited

SilhouetteCentral Web Application Installation

The following steps install the SilhouetteCentral web application on IIS.

1. Create the folder you want to serve the web application from. The web application stores a number of files (including images, logs, templates) in a directory under the web application folder. You may want to set the web application physical path storage location to allow for data growth, encryption, and backup requirements.
2. Grant Read and Execute rights to the built-in group IIS_IUSRS on the folder if not already inherited.
3. Unzip the supplied SilhouetteCentral archive into the folder.
4. Setup IIS to serve this folder as a Web Application, see Configure IIS to Serve the SilhouetteCentral Web Application below.
5. Grant Modify rights to the IIS Application Pool Identity on the 'Files' sub-folder.

If upgrading an existing SilhouetteCentral installation, check the instructions in the SilhouetteCentral Upgrade section.

These instructions setup SilhouetteCentral as virtual directories in an IIS website. The configuration of the root website should also be considered, either to route requests to a default site or to provide a relative webpage and to apply or modify HTTP headers, e.g. X-Frame-Options = SAMEORIGIN.

Configure IIS to Serve the SilhouetteCentral Web Application

The table shown here provides the short list of configuration values that need to be set when deploying the SilhouetteCentral web application. The configuration items listed with 'No' in the Required Value column of the table are free to be adjusted according to the system design.

Configuration Item	Value	Required Value?
IIS - Web Site - Physical Path	%SystemDrive%\inetpub\wwwroot	No
IIS - Web Site - Preload Enabled	True	Yes
IIS - Application Pool - Name	SilhouetteCentral	No
IIS - Application Pool - .NET CLR version	.NET CLR Version v4.0.30319	Yes
IIS - Application Pool - Managed pipeline mode	Integrated	Yes
IIS - Application Pool - Start Mode	AlwaysRunning	Yes
IIS - Application Pool - Identity	ApplicationPoolIdentity	No
IIS - Application Pool - Idle Time-out (minutes)	180	No
IIS - Application Pool - Load User Profile	True	Yes
IIS - Web Application - Physical Path	c:\inetpub\wwwroot\silhouette	No

Copyright © 2018-2026 ARANZ Medical Limited

Configuration Item	Value	Required Value?
IIS - Web Application - Alias	silhouette	No
IIS - Web Application - Application Pool	SilhouetteCentral	No
IIS - Web Application - Preload Enabled	True	Yes

The Web Site Bindings configuration is required but is not mentioned above. Set up the web site HTTPS binding with an appropriate SSL certificate as standard IIS configuration.

The above table of configuration items offers a good set of recommended values, however there may be reasons to deviate from the recommendations in specific scenarios. The following table lists recommendations and considerations important to the SilhouetteCentral web application operation.

Configuration Item(s)	**Recommendation or Considerations**
IIS - Application Pool - Identity	If using Windows Authentication for MS SQL Database connections, you will not be able to use the ApplicationPoolIdentity unless the MS SQL server is operating on the same server as the web server.
IIS - Application Pool - Idle Time-out (minutes)	The default IIS Application Pool Idle Timeout is 20 minutes. It is recommended extending this to be longer than a typical wound assessment at a bedside to ensure responsiveness and robust SilhouetteStar 2 operation.
IIS - Web Application - Physical Path	The web application stores a number of files (including images, logs, templates) in a directory under the web application. You may want to set the web application physical path storage location to allow for data growth, encryption, and backup requirements. If you set this to a directory outside of the website directory, ensure you grant read & execute rights to the IIS_IUSRS built in windows group.
IIS - Web Application - Alias	Use a lower case value. Using a lower case value helps to avoid configuration errors at a later stage.

Some general guidance on configuring IIS is included in Appendix A: IIS Configuration.

Copyright © 2018-2026 ARANZ Medical Limited

SilhouetteTokenService Web Application Installation

The SilhouetteTokenService web application is introduced as a component of SilhouetteCentral in Silhouette v4.11. The following steps install the SilhouetteTokenService web application on IIS.

1. Create the folder you want to serve the web application from. The web application stores a number of files (including logs) in a directory under the web application folder. You may want to set the web application physical path storage location to allow for data growth, encryption, and backup requirements.
2. Grant Read and Execute rights to the built-in group IIS_IUSRS on the folder if not already inherited.
3. Unzip the supplied SilhouetteTokenService archive into the folder.
4. Setup IIS to serve this folder as a Web Application, see Configure IIS to Serve the SilhouetteTokenService Web Application below.
5. Create a sub directory in the folder named Files and grant modify rights on the folder to the Application Pool Identity.



The SilhouetteTokenService component must be the same version as the SilhouetteCentral component and you should be supplied archives for both components at the same time.

Configure IIS to Serve the SilhouetteTokenService Web Application

The table shown here provides the short list of configuration values that need to be set when deploying the SilhouetteTokenService web application. The configuration items listed with 'No' in the Required Value column of the table are free to be adjusted according to the system design.

Configuration Item	Value	Required Value?
IIS - Web Site - Physical Path	%SystemDrive%\inetpub\wwwroot	No
IIS - Web Site - Preload Enabled	True	Yes
IIS - Application Pool - Name	SilhouetteToken	No
IIS - Application Pool - .NET CLR version	No Managed Code	Yes
IIS - Application Pool - Managed pipeline mode	Integrated	Yes
IIS - Application Pool - Start Mode	AlwaysRunning	Yes
IIS - Application Pool - Identity	ApplicationPoolIdentity	No
IIS - Application Pool - Idle Time-out (minutes)	180	No
IIS - Application Pool - Load User Profile	True	Yes
IIS - Web Application - Physical Path	c:\inetpub\wwwroot\silhouettetoken	No
IIS - Web Application - Alias	silhouettetoken	No
IIS - Web Application - Application Pool	SilhouetteToken	No
IIS - Web Application - Preload Enabled	True	Yes

Copyright © 2018-2026 ARANZ Medical Limited

The above table of configuration items offers a good set of recommended values, however there may be reasons to deviate from the recommendations in specific scenarios. The following table lists recommendations and considerations important to the SilhouetteTokenService web application operation.

Configuration Item(s)	Recommendation or Considerations
IIS - Application Pool - Identity	Typically use the same setting as used for the SilhouetteCentral web application component.
IIS - Application Pool - Idle Time-out (minutes)	The default IIS Application Pool Idle Timeout is 20 minutes. It is recommended extending this to reduce the number of application restarts during idle periods.
IIS - Web Application - Physical Path	Typically set this to a directory in a similar location as the SilhouetteCentral web application component. Do not set it as a sub directory of the SilhouetteCentral web application as this causes nested web config files and can create errors. The SilhouetteTokenService web application stores a number of files (including logs) in a directory under the web application folder. You may want to set the web application physical path location to allow for data growth, encryption, and backup requirements. If you set this to a directory outside of the website directory, ensure you grant read & execute rights to the IIS_IUSRS built in windows group.
IIS - Web Application - Alias	Use a lower case value. Using a lower case value helps to avoid configuration errors at a later stage.

Some general guidance on configuring IIS is included in Appendix A: IIS Configuration.

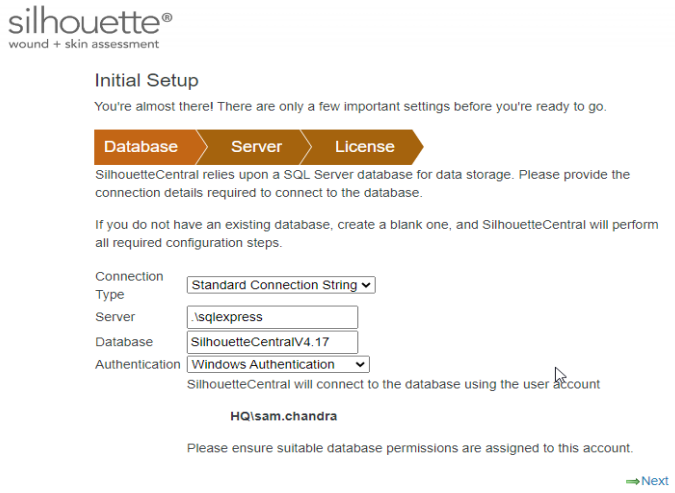
Copyright © 2018-2026 ARANZ Medical Limited

SilhouetteCentral Initial Configuration Wizard

After you have completed the install process, you need to perform some additional setup. The setup automatically runs the first time you visit the SilhouetteCentral website. To run the wizard

1. Launch a Web Browser
2. Navigate to https://<domainname>/silhouette/ (or the location you installed the application to).

This wizard configures the basic settings required for SilhouetteCentral to run correctly.

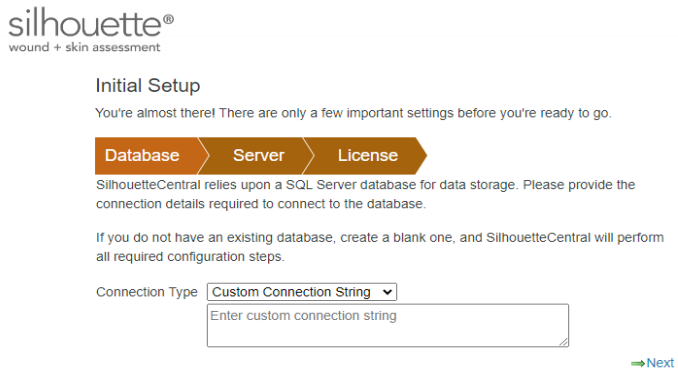


Step 1 - Database

Enter the connection details to the SQL Server instance and database that Silhouette uses. The database entered here must already exist and it should be a new blank database, see Preparing a SQL Server Database instructions.

Do not use space characters in the Server string as it will cause the database setup to fail.

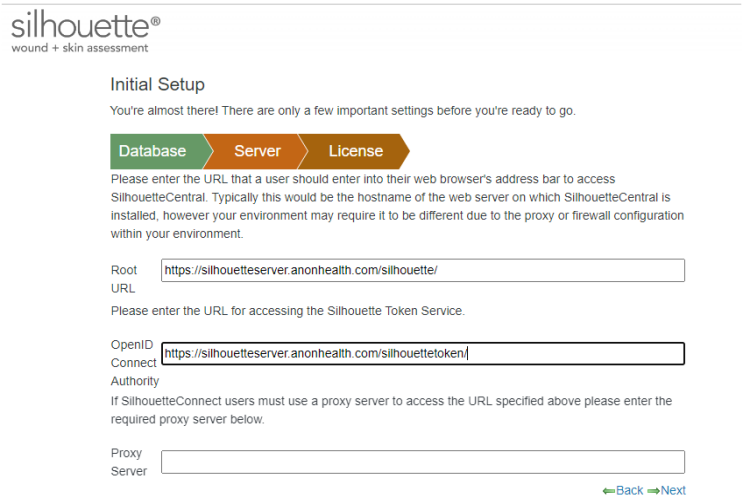
The account used to authenticate must have database owner permissions.



It is expected that the SQL Server connection certificate will already be trusted by the server. If the use of SQL Server fallback encryption (self-signed certificates) is approved then you will need to add the appropriate properties to the connection string manually, see the help topic Advanced SilhouetteCentral Web Application Configuration.

If you require an option not available with the standard connection string settings, choose "Custom Connection String" from the connection type dropdown and input your connection string in the text area.

Copyright © 2018-2026 ARANZ Medical Limited



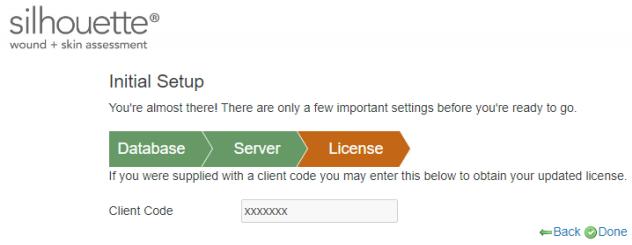
Step 2 - Server

The **Root URL** is the URL of the SilhouetteCentral instance, e.g. https://<domainname>/silhouette.

The Root URL must be a resolvable hostname on your network, preferably with SSL certificates and HTTPS bindings already in-place.

Failure to enter the correct value for the Root URL causes a SilhouetteStar 2 Wi-Fi connection failure and possibly a user login failure.

The **OpenID Connect Authority** is the URL of the SilhouetteTokenService, e.g. https://<domain>/silhouettetoken. The value is case sensitive and the path must be the same case as the SilhouetteTokenService Web Application virtual path in IIS.



Step 3 - License

Enter your client code here. SilhouetteCentral attempts to contact the license server and download the required license file for SilhouetteCentral.

Leave this blank in order to proceed using a trial license.

This step may complete automatically, depending on how you obtained your SilhouetteCentral installation files.

Step 4 - Finish configuration of SilhouetteTokenService

At this point in the setup wizard it is complete and you may receive an error or you will see a screen asking you to restart AppPools.

Finish setting up the SilhouetteTokenService web application and then restart both the SilhouetteCentral and SilhouetteTokenService application pools.

Copyright © 2018-2026 ARANZ Medical Limited

SilhouetteTokenService Web Application Configuration

The configuration of the SilhouetteTokenService web application is completed through configuration files on the server. You must have privileged user access to the server to edit this configuration.

In the SilhouetteTokenService Web Application folder there is a file named 'appsettings.json' containing default settings and should not be modified. Settings are overridden by including a second production appsettings file called 'appsettings.Production.json'. The json files are text format files following the JSON format specified in RFC8259 and can be edited by any standard text editor, e.g. Notepad.

The only mandatory setting to include in the production appsettings file is the database connection string. Other settings will be included based on your needs. Not all settings are listed in this chapter, only those you are likely to need.

A very basic appsettings.Production.json file looks like:

```
{
	"ConnectionStrings": {
		"sts": "Data Source=.;Initial Catalog=silhouette;Integrated Security=true"
	}
}
```

The convention used in this chapter when referring to members within the JSON file is to use a dotted notation (the chain of JSON member names separated by periods (.). For example, the connection string above can be referred to as ConnectionStrings.sts.

Where the property is part of an array, the members are included in square brackets.

Changes to the appsettings are only applied when the associated application pool is recycled.

Database Connection String

The database connection string is a required setting and should be configured to connect to the SilhouetteCentral database.

```
{
	"ConnectionStrings": {
		"sts": "Data Source=.;Initial Catalog=silhouette;Integrated Security=true"
	}
}
```

Member Name	Value
ConnectionStrings.sts	A MS SQL Server connection string.

Copyright © 2018-2026 ARANZ Medical Limited

Member Name	Value
	Note that the example above does not include the encryption properties. The SilhouetteTokenService forces the connection encryption property to 'Mandatory'. The preference should be that the connection is encrypted with a trusted certificate. If the use of SQL Server fallback encryption (self-signed certificate) is approved then adding the `TrustServerCertificate=true` property to the connection string is necessary.

Once the SilhouetteCentral Initial Configuration Wizard is completed then the database connection string can be copied from the SilhouetteCentral web application MachineSettings.xml file.

Logo

If a logo is uploaded in the SilhouetteCentral initial configuration wizard, you can set the SilhouetteTokenService to display the same logo on the login pages.

```
{
	"Configuration": {
		"CustomerLogoUrl": "/silhouette/api/v4/customfile/customerlogo"
	}
}
```

Member Name	Value
Configuration.CustomerLogoUrl	The website path to the customer logo. This URL must be a reference to an image file on the same website as the SilhouetteTokenService. This is typically a path to the SilhouetteCentral API that contains the logo set in the SilhouetteCentral initial configuration wizard. For example: `/silhouette/api/v4/customfile/customerlogo` Note that the v4 in the URL example refers to the version of API. v4 API was introduced in Silhouette v4.15.

Local Silhouette Users

The AccountSecurity section of the configuration sets the parameters for Local Silhouette User accounts and the associated password and account lockout rules.

Copyright © 2018-2026 ARANZ Medical Limited

```
"AccountSecurity": {
	"AllowLocalLogin": true,
	"ForgottenPasswordEmail": {
		"Enabled": false,
		"RequestExpirationMinutes": 60
	},
	"Passwords": {
		"ExpirationEnabled": false,
		"ExpirationDays": 14,
		"MinLength": 3,
		"MaxLength": 20,
		"MustContainAlphaAndNumeric": false,
		"MustNotMatchUser": false,
		"HistoryCount": 0
	},
	"Lockout": {
		"Enabled": false,
		"AfterFailedLogonCount": 6,
		"CheckIntervalMinutes": 10
	}
}
```

Member Name	Value
AccountSecurity.AllowLocalLogin	Set to true by default. Setting to false disables the ability to login for all Silhouette Local User accounts, including default ARANZ Support and Admin users. Only set to false if there is an external identity provider configured.
AccountSecurity.ForgottenPasswordEmail.Enabled	Set to true to enable the use of the password reset emails.
AccountSecurity.ForgottenPasswordEmail.RequestExpirationMinutes	Use this setting to set how long a password reset link is valid for. The minimum setting is 10 minutes. The maximum setting is 1440 minutes (24 hours).
AccountSecurity.Passwords.ExpirationEnabled	Set to false by default. Setting to true means that passwords will expire for Silhouette Local User accounts.
AccountSecurity.Passwords.ExpirationDays	This value is only considered if the password expiration is enabled. The number of days Silhouette Local User account passwords will last before the user is asked to change it. The default value is 14 and it can be set between 1 and 365 days.

Copyright © 2018-2026 ARANZ Medical Limited

Member Name	Value
AccountSecurity.Passwords.MinLength	The default value is 3 and the value can be set between 3 and the MaxLength setting. Sets the minimum length for Silhouette Local User account passwords.
AccountSecurity.Passwords.MaxLength	The default value is 20 and the value can be set between the MinLength and 50. Sets the maximum length for Silhouette Local User account passwords.
AccountSecurity.Passwords.MustContainAlphaAndNumeric	The default value is false. Set to true to require Silhouette Local User account passwords to have both at least one alphabetical character and one numeric character.
AccountSecurity.Passwords.MustNotMatchUser	The default value is false. Set to true if Silhouette Local User account passwords must be different to the accounts User Name.
AccountSecurity.Passwords.HistoryCount	The default value is 0 and the maximum value is 9. Sets the number of old Silhouette Local User account passwords that are remembered. When setting a new password, the user cannot select a password in the remembered history.
AccountSecurity.Lockout.Enabled	The default value is false. Set to true to enable Silhouette Local User account lockout if there are too many failed login attempts.
AccountSecurity.Lockout.AfterFailedLogonCount	The default value is 6. Sets the number of failed login attempts the user gets before their Silhouette Local User account is locked.
AccountSecurity.Lockout.CheckIntervalMinutes	The default value is 10. Sets the period (in minutes) which failed login attempts must occur within for the Silhouette Local User account to be locked out.

Copyright © 2018-2026 ARANZ Medical Limited

The AccountSecurity.Password settings also have paired settings in the SilhouetteCentral Organizational Settings which need to configured the same as these SilhouetteTokenService settings for robust operation.

Logging

The SilhouetteTokenService uses the Serilog logging library. Some of the logging configuration is exposed and is able to be set. Not all configuration is included in the table below.

```
"Serilog": {
	"MinimumLevel": {
		"Default": "Information"
	},
	"WriteTo": [
		{
			"Name": "File",
			"Args": {
				"path": "Files/Logs/TokenServiceLog.txt",
				"retainedFileCountLimit": "90"
			}
		}
	]
}
```

Member Name	Value
Serilog.MinimumLevel.Default	The default value is "Information". Set to "Debug" to increase the level of logging for setup and debugging the configuration. This can be useful when setting up SAML2 integration. Production systems should not leave "Debug" level logging on under normal operating conditions.
Serilog.WriteTo[.Name="File"].Args.path	The default value is "Files/Logs/TokenServiceLog.txt". Set to an alternative log file output path. The SilhouetteTokenService application pool must have Write and Modify access to this path.
Serilog.WriteTo [.Name="File"].Args.retainedFileCountLimit	The default value is 90. Sets the number of rolled log files that kept.

SAML2 Configuration

The Saml2 configuration section allows SSO with an external authentication provider. This configuration is only applied if there is a valid license for the SSO Integration optional feature.

```
"Saml2": {
	"Enabled": true,
	"AuthenticationSchemes": [
		{
			"Scheme": "Saml2",
			"DisplayName": "Work ID",
			"Metadata": "https://<domain name>/<path>/Saml2",
			"ModulePath": "",
			"IdentityProviders": [
```

Copyright © 2018-2026 ARANZ Medical Limited

```
                        {
                            "EntityId": "http://example.com/adfs/services/trust",
                            "Metadata": "https://example.com/FederationMetadata/2007-
                            06/FederationMetadata.xml",
                            "LoadMetadata": true
                        }
                    ],
                    "ClaimTypes": {
                        "FirstName":
                        "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname",
                        "LastName":
                        "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname",
                        "Email":
                        "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress",
                        "Group": "http://schemas.xmlsoap.org/claims/Group"
                    }
                }
            ]
        }
```

Member Name	Value
Saml2.Enabled	Set to true to allow sign-on with an external identity provider. If this value is set to true, at least one Saml2.AuthenticationScheme configuration object must be provided. Setting this value to false disables user login using external identity providers, leaving the provider configuration and user records in the Silhouette database. The default value is false.
Saml2.AuthenticationSchemes[].Scheme	An identifier for the authentication scheme. Typically set this value to "Saml2" unless multiple authentication schemes are being defined. Removing or changing an authentication scheme, removes the ability to login using that identity provider and removes user records and provider claim to Silhouette group mapping configuration.
Saml2.AuthenticationSchemes[].DisplayName	Set to a value that is reasonably short and meaningful to users logging in. The descriptive name used in the Silhouette UI. Some of the places it can be shown are: • The login screen has a button "Login with <DisplayName>" if there are multiple login options for users. • The authentication provider claims section on the Groups admin screen when mapping group claims to Silhouette groups. • The authentication provider for a user account on the Users admin screen. • Shows in Silhouette Login Attempt logs.
Saml2.AuthenticationSchemes[].Metadata	Sets the Entity ID URI of the authentication scheme. The external Identity Provider will need to know this value. This value is typically the case sensitive SilhouetteTokenService Web Application URL plus the Scheme identifier. For example: `https://private.example.com/silhouettetoken/Saml2`

Copyright © 2018-2026 ARANZ Medical Limited

Member Name	Value
Saml2.AuthenticationSchemes[].ModulePath	Set to an empty string ("") unless there are more than one authentication schemes being configured. If set to an empty string the default value of Saml2 is used. This value explicitly sets where the SilhouetteTokenService hosts the various Saml2 endpoints, including the metadata and the Assertion Consumer services. Once set, the Saml2 relying party (RP) metadata can be downloaded from: `https://<domain name>/<SilhouetteTokenService path>/<ModulePath>` The metadata downloaded from the metadata URL contains the Entity Id and the Assertion Consumer Services endpoints and can be used to configure a SAML2 Identity Provider (IdP).
Saml2.AuthenticationSchemes[].IdentityProviders	This value is an array of objects describing identity providers that use this scheme. Silhouette expects a single identity provider object in this array. The identity provider object typically contains three members: • EntityId - The entity id URI of the identity provider. • Metadata - The URL where the metadata XML document for the identity provider can be found. The metadata XML contains the rest of the configuration that is required for the SilhouetteTokenService to operate. The SilhouetteTokenService must be able to connect to this URL. • LoadMetadata - set to true to load the configuration from the provided metadata URL when the SilhouetteTokenService restarts. `{ "EntityId": "http://example.com/adfs/services/trust", "Metadata": "https://example.com/FederationMetadata/2007-06/FederationMetadata.xml", "LoadMetadata": true }`
Saml2.AuthenticationSchemes[].ClaimTypes	The ClaimTypes is an object that sets how the SilhouetteTokenService uses claims provided by the Identity Provider. The ClaimTypes object expects four members: • FirstName - specifies the URI of the claim to display as the users First Name. • LastName - specifies the URI of the claim to display as the users Last Name. • Email - specifies the URI of the claim Silhouette uses as the Email Address for the account. • Group - specifies the URI of the claim Silhouette uses to map to Silhouette group membership. The typical configuration is listed here. `{ "FirstName": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname", "LastName": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname", "Email": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress",`

Copyright © 2018-2026 ARANZ Medical Limited

Member Name	Value
	"Group": "http://schemas.xmlsoap.org/claims/Group" } The claim type used for the User Name field (main account identifier) in Silhouette is not included in the ClaimTypes configuration. It uses either the JWT 'sub' claim or the Name ID (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier) claim.

Copyright © 2018-2026 ARANZ Medical Limited

Advanced SilhouetteCentral Web Application Configuration

There are a number of web application settings available in the <Main Application Directory>\Files\Settings\machinesettings.xml file. In most installations there is no need to adjust the Web Application settings.

Any adjustments to the MachineSettings file should be made with care and by first taking a copy of the original settings. If an invalid file or invalid settings are detected, the initial SilhouetteCentral setup wizard is displayed when accessing the web site.

Changes to the application settings in the machinesettings.xml are only applied when the associated SilhouetteCentral application pool is recycled.

Patient Assessment Data File Location

By default, SilhouetteCentral stores patient images and report files in the Files\Data folder under the main web application folder. The location of this Data folder may be altered by updating the DataDirectory property in the MachineSettings configuration file. This allows the data to be stored in a different location to the SilhouetteCentral application files. This can be either a local directory or a UNC file share.

Before changing this setting, consider moving the entire web application folder using IIS configuration.

As an example updating the setting within machinesettings.xml as follows would store patient images and reports in the D:\Silhouette\Data folder.

```
<DataDirectory>D:/Silhouette/Data</DataDirectory>
```



Changing this setting does not transfer any existing images and reports to the new location. To change this setting:

1. Stop the SilhouetteCentral application pool,
2. Move the contents of the existing folder to the new location,
3. Update the DataDirectory setting, and
4. Restart the SilhouetteCentral application pool.

SilhouetteConnect Synchronization Related Settings

Synchronization Database Configuration

The connection string used by SilhouetteCentral to connect to the synchronization SQL Server instance can be customized in the MachineSettings configuration file.

```
<SilhouetteConnectDatabaseInstanceConnectionString>Data Source=.\Silhouette;Integrated
Security=SSPI;</SilhouetteConnectDatabaseInstanceConnectionString>
```

Note that the example above assumes that the SQL Server is set to force encryption on and that the SilhouetteCentral server is already configured to trust the CA used for the encryption certificate. If SQL Server fallback encryption (self-signed certificates) are being used then the properties `Encrypt=True;TrustServerCertificate=True` can be added to the connection string.

Number of days to keep SilhouetteConnect databases

SilhouetteCentral keeps an archived copy of the SilhouetteConnect database when it is uploaded during a synchronization. The SilhouetteConnect database copies are only kept for 10 days by default and are then deleted. The number of days the databases are kept can be customized in the MachineSettings configuration file with a minimum of 1 day.

Copyright © 2018-2026 ARANZ Medical Limited

```
<DaysToKeepArchivedConnectDatabases>10</DaysToKeepArchivedConnectDatabases>
```

Temporary Storage



Modifying the temporary storage directories doesn't move or clean up the old directory. Clean up must be done manually.



The Email Attachment and Data Export temporary storage contains patient information. Ensure these directories are adequately protected against unauthorized access.

Email Attachment Storage

If emails are configured to be sent with attached PDF reports, these reports are generated and stored on the file system.

```
<EmailAttachmentsDirectory>~/Files/Data/EmailAttachments</EmailAttachmentsDirectory>
```

Data exports file location

This setting tells where on the file setting to create and store data exports before they are downloaded.

```
<DefaultAssessmentExportDirectory>~/Files/Data/Exports</DefaultAssessmentExportDirectory>
```

System Events, Email, and Integration Event Application Settings

When using the automatic assessment email or the integration event features there are a number of settings that can be adjusted in the MachineSettings configuration file.

System Event Queue Processing

The following settings allow the period of the System Event processing job and how many system events will be processed in one go. If the email log shows that the system event job is commonly taking more than 30 seconds to run, you should consider reducing the batch size. The batch size given in the configuration is per system event type (assessment create and assessment update).

```
<ProcessAssessmentSystemEventsCronSchedule>* * * * *</ProcessAssessmentSystemEventsCronSchedule>

<ProcessAssessmentSystemEventsBatchSize>1000</ProcessAssessmentSystemEventsBatchSize>
```

Email Queue Processing

The email queue processing settings allow you to control how many emails will be attempted in any one period (the period is set by the System Event Queue Processing settings) and how many emails are sent concurrently. These settings may need to be adjusted to fit within sending limits of the SMTP service being used.

```
<ProcessEmailQueueMaximumNumberOfEmailsToSendPerJob>20</ProcessEmailQueueMaximumNumberOfEmailsToSendPerJo
b>

<ProcessEmailQueueMaximumNumberOfEmailsToSendConcurrently>5</ProcessEmailQueueMaximumNumberOfEmailsToSend
Concurrently>
```

The maximum age for an email in the queue is also adjustable. Any emails still pending after they have been in the queue for more than the maximum age are not sent.

```
<ProcessEmailQueueMaximumAgeOfEmailsInDays>10</ProcessEmailQueueMaximumAgeOfEmailsInDays>
```

Copyright © 2018-2026 ARANZ Medical Limited

Integration Event Queue Processing

The integration event queue processing settings allow you to control how many pending integration events are forwarded to the integration engine in any given period (the period is set by the System Event Queue Processing settings). Typically, the sending of integration events causes more traffic to SilhouetteCentral as the integration engine gets report content and data.

```
<ProcessIntegrationQueueMaximumNumberOfEventsToSendPerJob>25</ProcessIntegrationQueueMaximumNumberOfEvent
sToSendPerJob>
```

Purging System Events and Email Queue

The system event queue and email queue are stored in the database. Silhouette has a daily job that removes old emails and system events. The configuration can be adjusted if there is a reason to keep data for longer.

```
<PurgeEmailAndSystemEventsIsEnabled>true</PurgeEmailAndSystemEventsIsEnabled>
```

```
<PurgeEmailAndSystemEventsCronSchedule>0 1 * * *</PurgeEmailAndSystemEventsCronSchedule>
```

```
<PurgeEmailAndSystemEventsBatchSize>500</PurgeEmailAndSystemEventsBatchSize>
```

The minimum age of an item to be purged can be set from 35 to 400 days. Setting a value outside of this range causes the default of 35 days to be used.

```
<PurgeEmailAndSystemEventsMinimumAgeInDays>35</PurgeEmailAndSystemEventsMinimumAgeInDays>
```

Assessment Data Export Related Settings

Days to keep data exports

This setting controls how long Silhouette keeps data exports after they are created. Valid settings are from 1 to 7 days. Any non-valid setting will cause the default of 3 to be used.

```
<MaximumAgeOfExportedDataInDays>3</MaximumAgeOfExportedDataInDays>
```

File clean up schedule

The file clean up schedule controls when the job which cleans up Synchronized SilhouetteConnect databases and expired data exports is run.

```
<CleanUpFilesCronSchedule>0 0 * * *</CleanUpFilesCronSchedule>
```

Inactive SSO User Expiry

Single-Sign-On (SSO) user records are created in the system as they sign-in (JIT provisioning). Silhouette expires (deletes) these JIT provisioned records if the user does not use the system for a number of days based on the following settings. Valid expiry days setting is from 32 to 365 days. Any non-valid setting will cause the default of 90 to be used.

```
<InactiveUserExpirationDays>90</InactiveUserExpirationDays>
```

```
<DeleteInactiveUserCronSchedule>30 1 * * *</DeleteInactiveUserCronSchedule>
```

The minimum expiry of 32 days is chosen to prevent conflicts with the SilhouetteConnect Maximum Offline Session Time (hrs) as deleting a user account in SilhouetteCentral that is still being used in SilhouetteConnect may cause unnecessary synchronization errors.

Purge orphaned documents on SilhouetteCentral

Documents that are uploaded but never linked to a note (therefore inaccessible in SIlhouette) can be automatically deleted after a configurable amount of time.

Copyright © 2018-2026 ARANZ Medical Limited

One situation to be aware of is partial uploads from Connect where a file upload could be successful but the assessment sync fails. The handle this issue, the number of days setting (PurgeOrphanedDocumentsDaysToKeepFiles) should be set sufficiently long to allow the user to perform a second sync of the assessment.

```
<PurgeOrphanedDocumentsIsEnabled>true</PurgeOrphanedDocumentsIsEnabled>
<PurgeOrphanedDocumentsCronSchedule>5 0 * * *</PurgeOrphanedDocumentsCronSchedule>
<PurgeOrphanedDocumentsDaysToKeepFiles>10</PurgeOrphanedDocumentsDaysToKeepFiles>
```

Dashboard Feature

The dashboard feature of SilhouetteCentral uses a separate connection to access the database. This setting needs to be configured before the dashboards will work.

```
<DashboardConnectionString>...</DashboardConnectionString>
```

Copyright © 2018-2026 ARANZ Medical Limited

Login and Reset Default User Passwords

SilhouetteCentral has a default administrator user, which can be used to bootstrap the installation:

- User Name: admin
- Default Password: aranz

Steps to complete:

1. Open your web browser and navigate to the SilhouetteCentral web application URL.
2. Login with the 'admin' user and the default password. You will be asked to reset the password for the account.
3. Login with the 'admin' account and your new password.
4. Using the Admin -> Users section in SilhouetteCentral, create a new user account for yourself in the Admin group.
5. Using the Admin -> Users section in SilhouetteCentral, reset the password for the default aranz user account. In some deployments this account password will have already been reset and this step can be skipped.
6. Once you have created admin accounts for your admin users, disable the default admin user account by editing it and setting the status to disabled.



Make sure you remember the user name and password you set for the admin and aranz user accounts. If you lose all your passwords to the system you will need to contact ARANZ Medical Support for assistance and have privileged access to the database.



The default ARANZ Support user in the system, with the user name aranz, has special access for setting advanced features (see the System Configuration topic). These features need assistance from the ARANZ Medical support team to ensure that they are used correctly.

Copyright © 2018-2026 ARANZ Medical Limited

Configure Fundamental System Settings

It is recommended to set the following settings as part of the initial deployment. Details for setting these configuration items are included in the Administration User's Guide.

- Configure information people will see who navigate or open Silhouette, before they are authenticated:
  - System Identification.
  - Login Banner.
- Configure options controlling authenticated session behavior:
  - Hide App Idle Timeout (pattern hiding).
  - SilhouetteCentral idle session termination.
  - SilhouetteConnect offline session functionality.

Copyright © 2018-2026 ARANZ Medical Limited

IIS Configuration Recommendations

ARANZ Medical recommends including the following configuration options for IIS.

Strict Transport Security (HSTS)

Enabling Strict Transport Security response header in IIS. This opt-in security enhancement ensures that all content will be sent over HTTPS.



NOTE: Read carefully how this header works before using it. If the HSTS header is misconfigured or if there is a problem with the SSL/TLS certificate being used, legitimate users might be unable to access the website. For example, if the HSTS header is set to a very long duration and the SSL/TLS certificate expires or is revoked, legitimate users might be unable to access the website until the HSTS header duration has expired.

Copyright © 2018-2026 ARANZ Medical Limited

SilhouetteCentral Maintenance

This section describes the basic maintenance tasks for the SilhouetteCentral system. Topics covered are:

- SilhouetteCentral Backup
- SilhouetteCentral Database Maintenance
- SilhouetteCentral Upgrade

SilhouetteCentral Backup

On completing the installation of SilhouetteCentral a backup plan and procedure should be put in place. The following items should be included in your backup plan to ensure no data is lost in the event of a hardware or software failure:

1. Backups of the SilhouetteCentral database and copying of the backup files to a secure backup location. Backups may be scheduled using SQL Agent or a Windows Scheduled Task.
2. The Files sub-folder in the SilhouetteCentral web application folder. This folder contains all of the assessment images, reports, license, logs, and configuration files.
3. The SilhouetteTokenService web application folder. This folder contains the licenses, data protection keys, logs, and configuration files.

SilhouetteCentral Database Maintenance

SilhouetteCentral does not purge deleted data or old audit records from the database. Removing data from the database after a period of time is a manual maintenance task. The following categories of data can be considered for removal after a retention period has expired.

- Deleted clinical data, including associated audit records.
- View logs.
- Login attempt logs.

If purging data from the Silhouette database, there are a few things to be aware of:

- Do not purge audit records for active patients as this can prevent the patient record being shown in the audit log review facility in SilhouetteCentral.
- Login attempt log records must be kept long enough to support the inactive SSO user expiry time, see Advanced SilhouetteCentral Web Application Configuration.

Copyright © 2018-2026 ARANZ Medical Limited

SilhouetteCentral Upgrade

To upgrade SilhouetteCentral, both the SilhouetteCentral and the SilhouetteTokenService web applications need to be upgraded.



When upgrading from a version prior to v4.11, follow the install instructions for the SilhouetteTokenService. If the SilhouetteConnect web application is installed in the root of the web site, contact ARANZ Medical Support for assistance moving it into a virtual path.

It is advised to take a backup or ensure the latest backup is good before attempting the upgrade.

When upgrading SilhouetteCentral, ensure that the corresponding Silhouette client software (e.g. SilhouetteConnect) is updated to compatible versions as well.

The upgrade procedure is:

1. Ensure HTTPS is enabled and the systems RootURL setting is configured with the correct HTTPS URL.
2. Extract the contents of both the SilhouetteCentral and SilhouetteTokenService ZIP files.
3. Using IIS manager, stop both the SilhouetteCentral and SilhouetteTokenService Application Pools.
4. Delete everything from the SilhouetteCentral web application folder except the "Files" sub-folder (the "Files" folder contains all of the configuration and images to be upgraded).
5. Delete everything from the SilhouetteTokenService web application folder except the "Files" sub-folder and the appsettings.Production.json configuration file.
6. Move the newly extracted SilhouetteCentral files into the SilhouetteCentral web application directory.
7. Move the newly extracted SilhouetteTokenService files into the SilhouetteTokenService web application directory.
8. Check the database compatibility level of the database. If it is not at the latest available version then it should be updated.
9. Start the SilhouetteTokenService and SilhouetteCentral application pools.
10. Browse to the SilhouetteCentral website to allow the upgrade to complete. Once you see the start page of SilhouetteCentral the upgrade has completed.
11. Test the upgrade to confirm operation.

After installation, it is possible a "database is upgrading" screen is displayed as the existing database content is upgraded. At various stages of the database upgrade you may be prompted for some inputs.

The SilhouetteCentral web application is not accessible to any users while the database is upgrading.

After the database upgrade completes, you may be placed part way through the configuration wizard as described in previous sections of this guide. If this occurs, it means that the new version requires additional configuration (or options).

Specify the settings as required and click **Next** to complete the wizard (the wizard is automatically populated with all originally specified information).

After an upgrade which changes the major version number (e.g. v3 to v4) then the system settings should be reviewed for desired configuration, e.g. users, groups, units, notes definitions, etc.

Copyright © 2018-2026 ARANZ Medical Limited

Versions

The method specified above can be used to upgrade SilhouetteCentral from any version greater than v3.10. The following notes are provided as there are some versions where additional care must be taken.

From v3.x

To v4.x

Upgrading from v3.x to v4.x is a major upgrade and the following points need consideration. If you have any queries or concerns please contact ARANZ Medical Limited before upgrading, at: support@aranzmedical.com

- For versions prior to v3.10 of the software, it is recommended that a customer support representative be contacted to assist with this process.
- Tissue Type Classification feature is not available in v4.23. Any tissue type outlines need to be segregated in the data before upgrading.
- The storage format of the image captured date is converted based on the Default Timezone specified in the Organization Settings. As such, you should verify that the Default Timezone setting is correct prior to starting the upgrade. If an adjustment has to be made, sync the change to all SilhouetteConnect devices before proceeding with the upgrade.

  The automatic upgrade process assumes that all image capture dates are from a single timezone. If data should be split into multiple timezones this needs to be performed by a customer support representative.

- Data consistency issues may cause upgrades to fail. These data consistency issues must be fixed before an upgrade can complete.
- The v3 integration component SilhouetteLink is replaced in v4 with NextGen Connect (formerly Mirth Connect). Not all integrations can be supported in v4 but reconfiguration is required.
- LDAP Sync is replaced with SSO integration. LDAP sync'd user accounts in v3 will be disabled on upgrade.
- Once upgraded review the user groups and permissions granted as the permissions model has changed significantly.

From pre-v4.3

To v4.3+

Upgrading to v4.3, or beyond, requires that a synchronization instance of SQL Server be available on SilhouetteCentral to support the SilhouetteConnect synchronization process. The synchronization instance of SQL Server needs read and write access to the appropriate files\mdfcreation directory.

Ensure that all SilhouetteConnect installations sync before upgrading as upgrading SilhouetteConnect no longer supports migrating data from versions prior to v4.3.

Copyright © 2018-2026 ARANZ Medical Limited

It is also recommended to modify the SilhouetteCentral web site configuration in IIS to set Preload Enabled to True and to set the Application Pool Start Mode property to Always Running. The optional IIS Application Initialization feature is required to enable these properties.

See the following topics for more details:

- Server Prerequisites and Dependencies
- Preparing a SQL Server Database.
- SilhouetteCentral Web Application Installation.

From pre-v4.4

To v4.4+

Upgrading to v4.4, or beyond, changes the way assessment dates are stored. Assessment creation dates are changed to record the local time plus an offset from UTC, as well as recording the time zone name of where they were created.

The time zone database used by Silhouette is the IANA time zone database. Information on the IANA time zone database can be found on the website https://www.iana.org/time-zones.

During the upgrade to v4.4, the upgrade will ask you to select an appropriate time zone to use for historical assessments. Selecting the correct time zone is important as the offset from UTC applied is dependent on any seasonal clock changes for that time zone.

The upgrade will ask you to specify a time zone per unit configured in Silhouette. The upgrade assumes is that the patients seen in different time zones will be in different units. If that is not the case for your system, contact ARANZ Medical for support while upgrading.

From pre-v4.6

To v4.6+

Version 4.6 reintroduces the concept of Wound State which was part of version 3 Silhouette but had previously been missing from the version 4 product.

If you are upgrading from a v3 Silhouette, the wound state records will be upgraded. These upgraded entries will appear as wound state changes on the relevant patient and wound time lines. The time given to the wound state records is 00:00 (midnight), in some case if a wound was healed on the same day as an assessment was completed for that wound then the healed state will show earlier than the assessment on the time line.

All wounds created in previous v4 versions of Silhouette are given an Open state based on the creation date and time of the wound.

This wound state upgrade requires the time zone mappings mentioned above in the v4.4 upgrade. If the time zone to unit mappings are not present, or are incomplete, then you will be asked to specify them during the upgrade of SilhouetteCentral.

Version 4.6 wound state also allows you to update the current wound state as part of a wound assessment. When upgrading any assessments will have a blank associated wound state record.

To v4.8+

v4.8 upgrade removes previous blockers upgrading v3 systems, specifically systems with multiple patient identifiers and with duplicate wound indexes can now be upgraded. v3 systems with these properties should be directly upgraded to v4.8 without any intermediary steps.

Copyright © 2018-2026 ARANZ Medical Limited

When upgrading v3 systems with Multiple Patient Identifiers, you will be asked to identify a single identifier for use within Silhouette during the upgrade process. All other identifiers will be migrated to standard note fields as part of the patient details.

In some rare cases this upgrade can leave some patient records without patient identifiers to display within Silhouette. Contact ARANZ Medical support if you require some data migration other than that provided by the standard upgrade script.

To v4.9+

v4.9 introduces the concept of a wound baseline date. The wound baseline date is used to identify the wound baseline measurement when calculating area reduction. The upgrade sets the baseline date for wounds created in v3 based on the baseline assessment date from v3, otherwise the baseline assessment date is set the same as the wound open date.

Area reduction was previously shown in Silhouette v3. when upgrading from v3, the area reduction values seen pre-upgrade vs post upgrade may change slightly as the calculation has been modified to remove the rounding errors from the display of area reduction.

v4.9 re-introduces the persistent note feature that was available in v3, but does not include support for persistent conditional expression. The v3 to v4.9 upgrade will keep notes that were persistent in v3, however all upgraded notes should be reviewed for their applicability.

To v4.11+

v4.11 introduces the SilhouetteTokenService as a separately installed Web Application using .NET Core 3.1 runtime. When upgrading to v4.11 you will need to follow the upgrade instructions for SilhouetteCentral and the installation instructions for the SilhouetteTokenService provided in this manual.

Once updated to v4.11, you will need to be operating with a HTTPS binding on SilhouetteCentral. This may require updating the RootURL in SilhouetteCentral and the SyncURL in the associated SilhouetteConnect installations.

During the SilhouetteCentral upgrade, you will be asked to enter the OIDC Authority. Enter the URL for the new SilhouetteTokenService web application, e.g. https://<domain>/silhouettetoken.

v4.11 enables integration of Silhouette with an external identity provider using the SSO SAML 2.0 protocol. Silhouette v3 had a similar feature through direct LDAP queries to an external user directory. There is no upgrade of the v3 identity integration to the v4.11 identity integration. The v4.11 upgrade will disable any external user accounts previously sync'ed using LDAP and the SSO feature can be configured.

To v4.12+

v4.12 changed the database engine for sync'ed SilhouetteConnect deployments. Upgrading a v4.11 or earlier SilhouetteConnect deployment that is set to synchronize to SilhouetteCentral will move data (database and images) from the common application data folders in Windows (typically c:\programdata\) to the users local appdata folder (typically c:\users\<profile>\appdata\local\). The upgrade moves the data for the first user to start SilhouetteConnect. Subsequent users logging in to Windows and starting SilhouetteConnect will start with a blank database and be asked to synchronize when they initially login.

Copyright © 2018-2026 ARANZ Medical Limited

To v4.13+

v4.13 split the User “Groups” into “User Roles” and “Clinical Data Access”. On upgrade, an “All Access” Clinical Data Access group is created which has access to all Units. Any user that previously belonged to a Group that had access to “All and future units” is assigned to this “All Access” Clinical Data Access group. For any other Group, a new Clinical Data Access group is created with the same name as the original Group, and the same Unit access.

A Role is created for each existing Group which will have the same permissions and same name as the previous Group. All users that were assigned to the Group are assigned to the new Role after upgrade.

After the upgrade has completed every user in the system should be assigned to one User Role and one Clinical Data Access Group and have equivalent permissions and patient access to earlier Silhouette versions.

The Can Manage Users and Groups permission pre-v4.13 has been split into separate permissions:

- Can Manage Roles
- Can Manage Clinical Data Access
- Can Manage Email Lists
- Can Manage Clinical Users

The Can Manage Clinical Users permission has additional options to control which user records can be managed and which roles can be assigned to users. These additional settings allow for site admins to manage users at their own site. Best effort assignments are made when upgrading a Silhouette system which uses the site admin configuration. However, it is unlikely that site admin roles will have appropriate assignable roles configuration or that site admin user accounts have correctly assigned clinical access groups. Review these parts of the configuration carefully on upgrade.

If the system is using the Single Sign On feature of Silhouette 4.11/4.12 then the Authentication Provider Claims are not migrated to the new Clinical Access Groups. Each Clinical Access Group will have to have the appropriate claims configured after the upgrade has completed. The “User Roles” should have the same Authentication Provider Claims as the Groups in the previous version

To v4.15+

v4.15 updates the version of .NET used by the SilhouetteTokenService web application from .NET Core 3.1 to .NET 6.0. Once the upgrade is complete the old .NET Core 3.1 runtime is no longer needed by Silhouette.

v4.15 updates the API version number from v3 to v4:

- If you have referenced this API version number (eg in the SilhouetteTokenService configuration file for the customer logo path) then this will need to be updated.
- If you are using the Silhouette integration interface then the integration configuration will need to be updated to the new API version.

The integration interface definitions have also been changed to be compatible with the new Assessment Definition Versioning feature, so all these will need to be updated.

To v4.17+

v4.17 changes the SilhouetteConnect syncing instance to use SQL Server LocalDb 2022

Copyright © 2018-2026 ARANZ Medical Limited

	rather than SQL Server Express. Once the upgrade to v4.17 is complete the old SQL Express syncing instance is no longer required and can be uninstalled.
To v4.18+	During the upgrade, existing dashboard files are moved to the database. Once the upgrade to v4.18 is complete, this folder and its content can be removed: <Main Application Directory>\Files\Dashboards\ v4.18 can be configured to send email alerts for expiring authentication certificates for Silhouette Surface Modeling Service. Alerts are disabled on upgrade but can be enabled, and recipients set in the configuration section.
To v4.20+	v4.20 updates the version of the .NET used by the SilhouetteTokenService web application from .NET 6.0 to .NET 8.0. Once the upgrade is complete the old .NET 6.0 runtime is no longer needed by Silhouette. The email generator has been updated and is now stricter on the template HTML syntax. If SilhouetteCentral uses any custom "Welcome Email" templates with invalid HTML syntax, then these will be archived and replaced with the default template. The archived templates can be retrieved from the email templates folder, or via ARANZ Medical Support. Other custom email templates should be verified after the upgrade to ensure they are still working (eg. assessment creation email templates). If SilhouetteCentral has the optional Dashboard feature licensed, and the system uses either the Progress Note or Messages feature, then prior to upgrade it should be verified that the syncing of patient data to the Dashboard database has completed.
To v4.22+	From v4.22, SilhouetteConnect Standalone upgrade from v3.x to v4 is no longer supported. Please contact ARANZ Medical support for upgrade assistance.
To v4.23+	v4.23 updates the version of the .NET used by the SilhouetteTokenService web application from .NET 8.0 to .NET 10.0. Once the upgrade is complete the old .NET 8.0 runtime is no longer needed by Silhouette. From v4.23, SilhouetteCentral no longer supports direct upgrades from v3.x systems that use multiple patient identifiers. Please contact ARANZ Medical support for assistance. Version 4.23 introduces Handlebars templates for PDF reports and emails. For PDF reports, the previous template format is called Format 1 (XML), and the new format is called Format 2 (HBS). The standard templates for both Assessment Reports and Progress Note Reports now use Format 2 (HBS). Customized Progress Note Report templates must be updated to Format 2 (HBS) as part of the upgrade. Customized Assessment Report templates in Format 1 (XML) will continue to function, but cannot be included in Progress Note Reports. All default email templates now use Handlebars. The previous email template format is deprecated, and customized email templates must be updated to Handlebars as part of the upgrade. For assistance with updating templates, contact ARANZ Medical Support.

Copyright © 2018-2026 ARANZ Medical Limited

SilhouetteConnect Installation and Initial Configuration

This section of the manual describes the installation of SilhouetteConnect, the PC Client software. The Silhouette Administrator's Guide has information on configuration options set within the application.

Topics covered in this section are:

- SilhouetteConnect Pre-Installation Planning
- Pre-requisites for installing SilhouetteConnect on Windows 11
- Installing SilhouetteConnect
- SilhouetteConnect Setup Screen
- SilhouetteStar 2 Firewall Rules and Networking
- Upgrading SilhouetteConnect
- Uninstalling SilhouetteConnect
- SilhouetteConnect File Storage and Backup

Copyright © 2018-2026 ARANZ Medical Limited

SilhouetteConnect Pre-Installation Planning

The following pre-installation steps should be performed before commencing the installation of SilhouetteConnect:

1	Prior to installation ensure the SilhouetteConnect dependency installer package step has been completed. This link can be found in the welcome email or the About page, if it is enabled for viewing in Silhouette Central. Contact an Administrator if you have trouble finding the link.	☐
2	Review the Silhouette CTEULA and Terms of Use, see the ARANZ Medical website (https://www.aranzmedical.com/silhouette-legal/).	☐
3	Determine if you require the Standalone mode or the Synchronized mode installer. ARANZ Medical support can help determine the right installer for your application.	☐
4	The SilhouetteConnect application uses the Microsoft .NET framework and either the MS SQL Server Express 2022 or MS SQL Server LocalDb database depending on the mode of operation. The installer package distributed by ARANZ Medical limited includes the appropriate .NET framework and MS SQL Server installers.	☐
5	SilhouetteConnect stores patient data in both the SQL Server database and in the PC file system. Ensure that BitLocker disk encryption or similar technology is enabled and recovery mechanisms are in place.	☐
6	Ensure SilhouetteStar devices are allowed to utilize the USB port (any group policy or port access restrictions).	☐
7	If SilhouetteStar 2 is being used with SilhouetteConnect the device uses IP over USB using the Microsoft RNDIS protocol. Ensure the requirements listed in the SilhouetteStar 2 Firewall Rules and Networking topic are met to allow connection.	☐
8	If the SilhouetteConnect is to be Synchronized mode, ensure that the PC has network access to SilhouetteCentral.	☐
9	Determine any backup requirements for the data on the PC. In synchronizing mode, regular synchronization to SilhouetteCentral provides a good backup of data.	☐
10	Enable network access to allow the Silhouette automatic licensing process to work. SilhouetteConnect must be able to reach the following URLs: • https://www.silhouettecentral.com/licensing/LicenseDownload.ashx • https://www.silhouettecentral.com/licensing/SilhouetteConnectLicenseService.asmx • https://europe.silhouettecentral.com/licensing/LicenseDownload.ashx • https://europe.silhouettecentral.com/licensing/SilhouetteConnectLicenseService.asmx A generic rule to allow access to https://*.silhouettecentral.com/licensing/ is recommended to allow for any changes in the licensing. If access to these destinations is not enabled the licensing process can be completed offline.	☐
11	If running Windows 11, ensure that you will not have issues running SQL Server Windows 11 Installation	☐

Copyright © 2018-2026 ARANZ Medical Limited

Pre-requisites for installing SilhouetteConnect on Windows 11

SQL Server Issues on Windows 11

SilhouetteConnect uses Microsoft SQL Server, which can have can have issues running on Windows 11 when the disk sector size is greater than 4 KB. In this case the installation of SQL Server may fail, or the Database Engine Service will not be able to start due to the unsupported file system. This can occur for both SQL Server Express (SilhouetteConnect Standalone mode) and LocalDB (SilhouetteConnect Synced mode). This issue is only likely to occur if using an NVMe drive.

You can confirm whether you may encounter this specific issue by:

1. Running the command from an administrator command prompt: `fsutil fsinfo sectorinfo C:`
2. Look for the value `PhysicalBytesPerSectorForAtomicity`, returned in bytes. A value of 4096 indicates a sector storage size of 4 KB.
3. If `PhysicalBytesPerSectorForAtomicity` is showing a value greater than 4096, you will need to apply one of the resolutions in the Microsoft troubleshooting article https://docs.microsoft.com/en-us/troubleshoot/sql/admin/troubleshoot-os-4kb-disk-sector-size prior to installing SilhouetteConnect.

If you have already installed SilhouetteConnect before encountering this issue, you may need to uninstall SQL Server before applying a fix.

Copyright © 2018-2026 ARANZ Medical Limited

Installing SilhouetteConnect

SilhouetteConnect has a different install process depending on whether it is installed in Standalone or in Synced Mode.

- Synced Mode
- Standalone Mode

To install SilhouetteConnect using an unattended software distribution tool contact ARANZ Medical Support.

Copyright © 2018-2026 ARANZ Medical Limited

Installing SilhouetteConnect Synced Mode

The installer for SilhouetteConnect is split into two parts

- SilhouetteConnect application installer. This does not require administrator permissions to be able to install, but is only available in the help and about page in SilhouetteCentral
- SilhouetteConnect dependency bundle. This includes SilhouetteStar drivers, as well as the database engine used by SilhouetteConnect. This requires administrator permissions to install.



If SilhouetteConnect is being upgraded from 4.20 or earlier, then the first step of the installation process is to manually uninstall the existing SilhouetteConnect application. It is recommend to ensure SilhouetteConnect has synced all data to SilhouetteCentral prior to performing the upgrade.

Download the installers from SilhouetteCentral

Both the SilhouetteConnect and the SilhouetteConnect dependency installation packages can be downloaded from an instance of SilhouetteCentral by using a web browser to navigate to https://<SilhouetteCentral URL>/about

When the SilhouetteConnect installer is downloaded from a SilhouetteCentral instance, it includes a *CustomProperties.xml* file, which bootstraps the installation of SilhouetteConnect with the initial configuration.

Once the installation files are obtained:

1. Navigate to the folder that contains the installation files.
2. If you are needing to install the SilhouetteConnect dependency bundle, then this should be installed first:
    1. Double click the **SilhouetteDriverInstallerBundle.exe** to start the installation process.
    2. Follow the on screen instructions to select the drivers and dependencies you need for the SilhouetteConnect install.
3. Install the SilhouetteConnect application:
    1. Double click the **SilhouetteConnect.exe** file to start the installation process.
    2. Follow the on-screen instructions, which includes the acceptance of the Silhouette CTEULA and Terms of Use, see the ARANZ Medical website (https://www.aranzmedical.com/silhouette-legal/).

The SilhouetteConnect install file may be prevented from running by the Windows SmartScreen filter. In order to run the setup, click on the **More Info** link, and then on the **Run anyway** button.

Once the installation is complete, launch SilhouetteConnect by double-clicking on the icon created on your desktop or by selecting SilhouetteConnect from the **All Programs** menu. The first run of SilhouetteConnect will upgrade (see Upgrading SilhouetteConnect) any existing installation data or show the SilhouetteConnect Setup Screen if necessary.

Copyright © 2018-2026 ARANZ Medical Limited

Installing SilhouetteConnect Standalone

The installer package for SilhouetteConnect Standalone comes with required third party installers. The installer package can be obtained from ARANZ Medical support or from your instance of SilhouetteCentral. The recommended best practice is to have the installation file on your local machine to perform the installation.

Once the installation files are obtained:

1. Navigate to the folder that contains the installation files.
2. Double click the **setup.exe** file to start the installation process.
3. The install requires admin permissions to install.
4. Follow the on-screen instructions, which includes the acceptance of the Silhouette CTEULA and Terms of Use, see the ARANZ Medical website (https://www.aranzmedical.com/silhouette-legal/).

Running the **setup.exe** file rather than the **SilhouetteConnect.msi** installer first checks for and installs the required pre-requisites. You can use the **SilhouetteConnect.msi** directly if you are confident the pre-requisites (typically .NET framework and MS SQL instance are already installed).

The SilhouetteConnect install file may be prevented from running by the Windows SmartScreen filter. In order to run the setup, click on the **More Info** link, and then on the **Run anyway** button.

The installer includes the drivers for SilhouetteStar, as well as, any necessary SilhouetteStar 2 software patches. These drivers are installed per USB port when a SilhouetteStar is connected to the computer.

The included SilhouetteStar 2 software patches allow the firmware in a SilhouetteStar 2 to be upgraded or downgraded to the latest compatible version when it is connected to SilhouetteConnect. See the Clinical User's Guide for information on connecting a SilhouetteStar and getting started with Silhouette.

Once the installation is complete, launch SilhouetteConnect by double-clicking on the icon created on your desktop or by selecting SilhouetteConnect from the **All Programs** menu. The first run of SilhouetteConnect will upgrade (see Upgrading SilhouetteConnect) any existing installation data or show the SilhouetteConnect Setup Screen if necessary.

The SilhouetteConnect dependency bundle should not be installed when installing SilhouetteConnect Standalone.

Copyright © 2018-2026 ARANZ Medical Limited

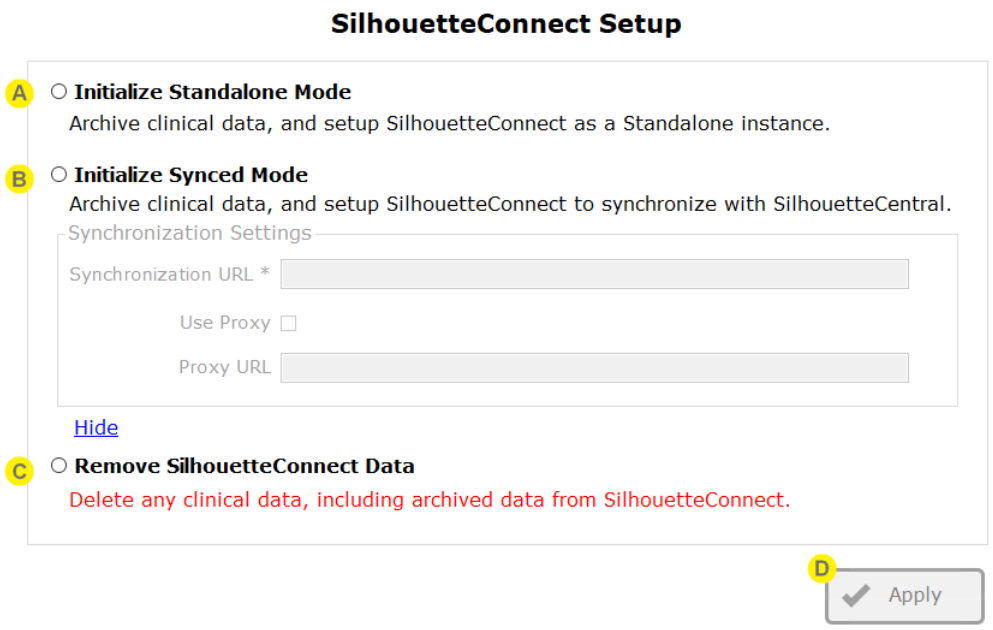
SilhouetteConnect Setup Screen

When SilhouetteConnect is first run a SilhouetteConnect Setup screen will be shown unless the application was automatically configured with a *CustomProperties.xml* file during installation.

The SilhouetteConnect Setup screen allows you to initialize the SilhouetteConnect operation mode, choosing between Standalone or Synced mode.

To force the SilhouetteConnect Setup screen to show you run the **SilhouetteConnect.exe** with the `--setup` command line parameter, e.g. run the following command from the Run dialog or the command line:

```
C:\Program Files (x86)\ARANZ Medical
Limited\SilhouetteConnect\SilhouetteConnect.exe --setup
```



A Choose **Initialize Standalone Mode** to start SilhouetteConnect in Standalone mode. This creates an empty SilhouetteConnect Standalone database with default settings.

If there is already data in the SilhouetteConnect program data folders it is moved to a data archive folder before initializing the new system. See the help topic SilhouetteConnect File Storage and Backup for further information.

When initializing as Standalone mode it is expected that the named SQL Server Express instance is already configured. If the SilhouetteConnect Synchronized mode installer package was used to do the initial installation, the SQL Server Express instance will not be there and the initialization will fail. Run the **setup.exe** from the Standalone installer package to setup the SQL Server Express instance as required.

B Choose **Initialize Synced Mode** and set the Synchronization Settings to start SilhouetteConnect in Synchronized mode.

Set the **Synchronization URL** to the URL of the SilhouetteCentral instance to sync to, typically something like:

```
https://www.silhouettecentral.com/<instanceName>/serviceview
.asmx
```

Copyright © 2018-2026 ARANZ Medical Limited

The serviceview.asmx part of the path will be appended to the URL if it is not entered. The application will try the URL once you press the **Apply** button and determine if SilhouetteCentral is responding.

If there is any data already saved in either the current users Synchronized mode data folder or the mode data folder, that data is moved to a data archive folder before re-initializing the application, see the help topic SilhouetteConnect File Storage and Backup for further information. Other PC users will have their data archived the next time they start SilhouetteConnect, if the Sync URL has changed since they last used the application.

C Choose **Remove SilhouetteConnect Data** to remove all the current users synced data and any PC wide standalone data and data archives.

This option also removes organizational settings and resets any Synchronization Settings.

It does not remove the log files, machine specific settings or preferences or SilhouetteStar 2 software patches.

> The **Remove SilhouetteConnect Data** action can not be undone. Make sure any data you wish to keep is backed up before you select this option, see SilhouetteConnect File Storage and Backup.

D Select the **Apply** button to execute the selected initialization / re-initialization option.

To exit the setup screen without making any changes to the configuration or the existing data then close the application using the close window button at the top right of the application window.

Copyright © 2018-2026 ARANZ Medical Limited

SilhouetteStar 2 Firewall Rules and Networking

The SilhouetteStar 2 in wired mode uses RNDIS drivers to communicate. This means that when the SilhouetteStar 2 is connected to a computer using the USB cable, the device is seen as a IP Network interface with an Ethernet device appearing in the networking section of windows.

The IP Network interface gets assigned a known IPv4 address by the SilhouetteStar 2. By default this address is a link-local address, 169.254.0.2. The addresses used can be changed, see the Administration User's Guide for details.

The SilhouetteConnect installer inserts firewall rules into the default Windows firewall to allow the SilhouetteStar 2 to connect to the computer on TCP port 9874. If a firewall other than the default Windows firewall is being used, the user must manually add a firewall rule to allow connections on TCP port 9874 for all network profiles (domain, public, and private PCs).

The SilhouetteStar 2 appears to the computer as a wired network with no internet access.

Some third party network management software can offer network adapter switching features, either turning off Wi-Fi if there is a wired connection present or not allowing a wired connection if also using a Mobile connection. Care must taken to determine the correct compatibility and configuration to allow both a network connection and a SilhouetteStar 2 connection.

Upgrading SilhouetteConnect

If the computer has, or has had, a previous version of SilhouetteConnect installed, then the installer will upgrade the instance and will not replace the previous data or settings. To remove the clinical data and SilhouetteConnect settings from a computer see the uninstall instructions.



Upgrading from a version prior to v4.3 is not supported.

When upgrading a Standalone SilhouetteConnect to v4.4 or beyond, then when you first start SilhouetteConnect you will be asked to select which time zone your historical assessments were captured in. You will be asked to select a time zone per unit, however, for a Standalone SilhouetteConnect it is expect that all time zone selections are the same. SilhouetteCentral Upgrade for more details on why the time zone mapping is requested.

If you are upgrading a Synchronized SilhouetteConnect, it is required that you obtain the specific installer from your SilhouetteCentral instance, via `https://<SilhouetteCentral URL>/install`. This installer contains specific information to ensure that the data in SilhouetteConnect is upgraded in the same way as the data in SilhouetteCentral.

SilhouetteConnect v4.6 and beyond reintroduces wound state recording in Silhouette. See SilhouetteCentral Upgrade for details on how existing wounds are updated to include state information during the upgrade.

SilhouetteConnect v4.12 and beyond changes where data is stored on the PC, from a global (all user) shared location to a per-user location, see SilhouetteConnect File Storage and Backup. The first user to run SilhouetteConnect will have any previous data moved to their user profile.

Standalone SilhouetteConnect v4.17 now uses SQL Server Express 2022 by default, however the upgrade process does not automatically upgrade the previously installed SQL Server instance. The SQL Server Express instance will need to be upgraded manually from 2014 to 2022 as per Microsoft's documentation. This does not affect Synchronized SilhouetteConnect.

When upgrading Synchronized SilhouetteConnect from v4.20 or earlier to v4.21 or later, then the old version of SilhouetteConnect must be manually uninstalled prior to installing the new version of SilhouetteConnect.

In v4.21 of Sychronized SilhouetteConnect, the installer is split into two components. Both the SilhouetteConnect dependency bundle and the SilhouetteConnect application installer must be run - see Installing SilhouetteConnect.

Copyright © 2018-2026 ARANZ Medical Limited

Uninstalling SilhouetteConnect

Should you need to uninstall SilhouetteConnect, this can be done via **Programs and Features**, which is accessible via the **Control Panel**. Please ensure that you have first backed up all information to SilhouetteCentral or an alternative location, see SilhouetteConnect File Storage and Backup.

Uninstalling SilhouetteConnect removes the application software, but leaves all clinical data on your machine.

To remove SilhouetteConnect data you can use the SilhouetteConnect Setup screen before you uninstall the application, see the help topic SilhouetteConnect Setup Screen, or you can remove clinical data manually from a device by:

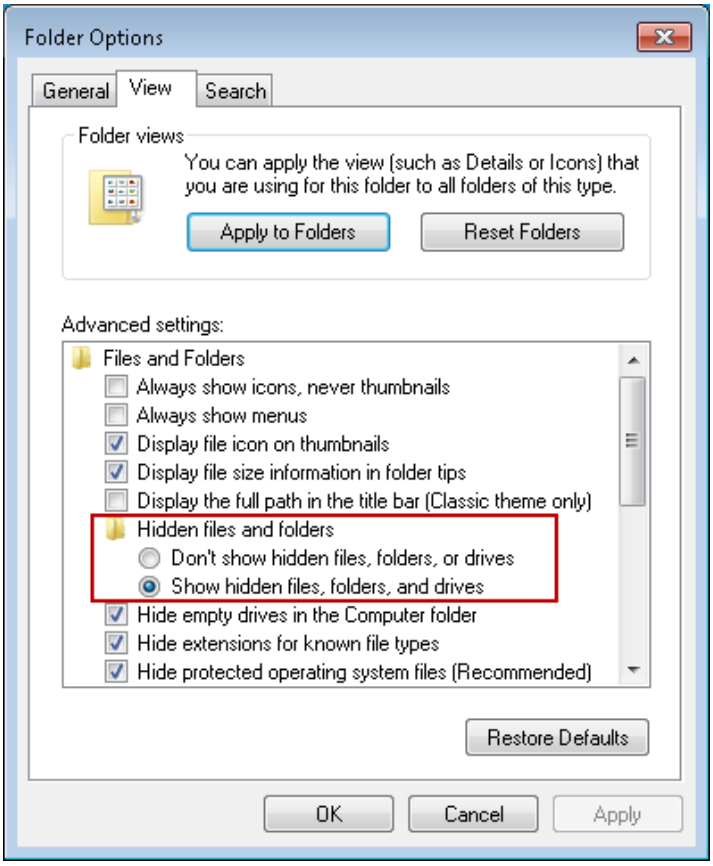
1. Remove the database used by Silhouette by opening a command prompt and running the one of the commands:

   (Standalone mode) `sqlcmd.exe -S .\SILHOUETTE -Q "DROP DATABASE Silhouette"`

   (Synchronized mode) `sqllocaldb d SilhouetteConnect`

2. Delete the folder '`%programdata%\ARANZ Medical Limited\SilhouetteConnect`' from your computer.
3. For Synchronized mode installations, delete the '`%localappdata%\ARANZ Medical Limited\SilhouetteConnect`' folders from each user profile on the computer.

Note that the '`C:\ProgramData`' folder is typically hidden. Hidden folders can be shown by selecting the **Show hidden files, folders, and drives** folder option:



Copyright © 2018-2026 ARANZ Medical Limited

SilhouetteConnect File Storage and Backup

The data storage location on the file system depends on the operation mode (Synchronized or Standalone) of SilhouetteConnect.

Standalone Mode Storage and Backup

SilhouetteConnect, in Standalone mode, creates and uses the following files or directories:

- `%programdata%\ARANZ Medical Limited\SilhouetteConnect\Settings\` - Directory that contains settings files controlling the operation of SilhouetteConnect. Typically the settings that need to be set in these files are configured by options in the install process, in the setup screens or from within the Silhouette application.

  There are some settings that can be changed in the `MachineSettings.xml` file within this directory to control the behavior of SilhouetteConnect. Before changing this file it is best to check with ARANZ Medical support.

  - `MaximumAgeOfExportedDataInDays` - Controls how long export data is stored within the application data directories. The default is 3 days and the valid range is 1 to 7 days.
  - `MaximumAgeOfOldInstanceDataInDays` - Controls how long old instance data archives are kept. The default is 31 days and the valid range is 0 to 365 days.
  - `Star1CableEnabled` - Enables or disables the SilhouetteStar 1 cable adapter. Valid values are "true" or "false".
  - Other settings are available to control the database connection and the instance of the ARANZ Medical licensing server used for licensing.

- `%programdata%\ARANZ Medical Limited\SilhouetteConnect\SilhouetteConnect.lic` - The license file for SilhouetteConnect allows it to run on the PC for the appropriate license period.
- `%programdata%\ARANZ Medical Limited\SilhouetteConnect\Logs\` - Directory that contains application log files for SilhouetteConnect. ARANZ Support Limited may ask you to provide these log files if you are having problems with the application.
- `%programdata%\ARANZ Medical Limited\SilhouetteConnect\CabInstalls\` - Directory that contains the SilhouetteStar 2 software patch files that are compatible with the running version of SilhouetteConnect.
- `%programdata%\ARANZ Medical Limited\SilhouetteConnect\Data\` - Directory that contains the clinical data stored on the system. This is kept in a PC wide area (available to all PC users) of the file system to allow multiple Windows users to share data on the same Standalone installation. The `data` directory contains the physical database files for the MS SQL Express database instance and sub-directories for the captured images and periodic database backups.
  - The database for Standalone SilhouetteConnect is stored in a named MS SQL Express instance (typically named SILHOUETTE).

Copyright © 2018-2026 ARANZ Medical Limited

  - Periodic backups (weekly and daily) are taken of the database and kept in the `Backup` sub-directory.
  - If you wish to backup data from the PC to a remote file system, backup the `Backup` and `Sdr` sub-directories.

- `%programdata%\ARANZ Medical Limited\SilhouetteConnect\Data_<n>\` - If the SilhouetteConnect installation has been re-initialized at any point in time, any previous data is archived by appending a sequential number to the end of the `data` folder, before initializing a new `data` folder.
- `%programdata%\ARANZ Medical Limited\SilhouetteConnect\CefCache\` - The `CefCache` folder holds some of the per-device remembered preferences for SilhouetteConnect operation (like tracing stylus use).

A manual backup of the SQL Express database can be taken by running the following command on the command line:

```
sqlcmd -S .\SILHOUETTE -Q "backup database [Silhouette] to disk='%programdata%\ARANZ Medical
Limited\SilhouetteConnect\Data\Backup\Silhouette.bak'"
```

Contact ARANZ Medical Support for details on how to restore from backups if necessary.



Always take a backup of the database to move or re-locate the Silhouette database, rather than moving the raw ldf and mdf data files.

Sync Mode Storage and Backup

SilhouetteConnect in sync mode creates and uses the following files or directories:

- `%localappdata%\ARANZ Medical Limited\SilhouetteConnect\Settings\` - Directory that contains settings files controlling the operation of SilhouetteConnect. Typically the settings that need to be set in these files are configured by options in the install process, in the setup screens or from within the Silhouette application.
  There are some settings that can be changed in the `MachineSettings.xml` file within this directory to control the behavior of SilhouetteConnect. Before changing this file it is best to check with ARANZ Medical support.
  - `MaximumAgeOfExportedDataInDays` - Controls how long export data is stored within the application data directories. The default is 3 days and the valid range is 1 to 7 days.
  - `MaximumAgeOfOldInstanceDataInDays` - Controls how long old instance data archives are kept. The default is 31 days and the valid range is 0 to 365 days.
  - `Star1CableEnabled` - Enables or disables the SilhouetteStar 1 cable adapter. Valid values are "true" or "false".
  - Other settings are available to control the database connection, the database version, and the instance of the ARANZ Medical licensing server used for licensing.
- `%localappdata%\ARANZ Medical Limited\SilhouetteConnect\SilhouetteConnect.lic` - The license file for SilhouetteConnect allows it to run on the PC for the appropriate license period.
- `%localappdata%\ARANZ Medical Limited\SilhouetteConnect\Logs\` - Contains application log files for SilhouetteConnect. ARANZ Support Limited may ask you to provide these log files if you are having problems with the application.

Copyright © 2018-2026 ARANZ Medical Limited

- `%localappdata%\ARANZ Medical Limited\SilhouetteConnect\CabInstalls\` - Contains the SilhouetteStar 2 software patch files that are compatible with the running version of SilhouetteConnect.
- `%localappdata%\ARANZ Medical Limited\SilhouetteConnect\Data\` - Contains the clinical data stored on the system. This is kept in a per-user area of the file system. Each Windows user syncs their own data from the SilhouetteCentral instance, however all users sync to the same instance. The `data` directory contains the physical database files for the MS SQL LocalDb database instance and sub-directories for the captured images and periodic database backups.
  - The database for Syncing SilhouetteConnect is stored in a named MS SQL LocalDB instance (typically named SilhouetteConnect).
  - Periodic backups (weekly and daily) are taken of the database and kept in the `Backup` sub-directory.
- `%localappdata%\ARANZ Medical Limited\SilhouetteConnect\CefCache\` - The `CefCache` folder holds some of the per-device remembered preferences for SilhouetteConnect operation (like tracing stylus use).
- `%localappdata%\ARANZ Medical Limited\SilhouetteConnect\Data_<n>\` - If the SilhouetteConnect installation has been re-initialized at any point in time, any previous data is archived by appending a sequential number to the end of the `data` folder, before initializing a new `data` folder.
  - The data for the user performing the re-initialization is archived when they do the re-initialization.
  - The data for the other users is only archived when those users login to the PC and start SilhouetteConnect, and only if the sync URL has actually changed since their last use.

When using SilhouetteConnect in Synchronized mode, then backing up the data from the local PC is not necessary as data is backed up in SilhouetteCentral when a sync is performed.

SilhouetteConnect Archive and Backup Data Retention

Each time a user logs in to SilhouetteConnect the age of the SilhouetteConnect data archives, stored in the `Data_<n>` folders, is checked and they are deleted if they are older than the `MachineSetting MaximumAgeOfOldInstanceDataInDays`, which is 31 days.

Adding a key `MaximumAgeOfOldInstanceDataInDays` in the `MachineSettings.xml` setup file allows you to control how long data is archived in the data archive folders (`Data_<n>` folders). The default retention for old instance data is 31 days and the valid settings range from 0 to 365 days.

SilhouetteConnect database backups are controlled by Organizational Settings within the admin part of the application. See the Administration User's Guide for more details.

Copyright © 2018-2026 ARANZ Medical Limited

Licensing

The **Admin > License** screen allows you to update the license for the current Silhouette component. For example, the **License** screen in SilhouetteCentral shows details about the licensing of SilhouetteCentral and the **License** screen in SilhouetteConnect shows details about the licensing for that install of SilhouetteConnect. The following license details are displayed:

1. **Client Code**: The client code the product is licensed against. If there is no client code in the text box, the Silhouette instance is unlicensed, and operating in a trial mode.
2. **Created**: The creation date of your license.
3. **Expires**: This is the expiry date of your license. If you have purchased a perpetual license, 'Never' is displayed.
4. **Features**: Any optional software features that have been licensed are listed here.

Licensing SilhouetteCentral or SilhouetteConnect

Underneath the license details there is a **Check for Update** section that provides an **Update** button. To license Silhouette for the first time, enter your client code and select the **Update** button. To subsequently update your license, for example if you have purchased additional features or extended your warranty, it is only necessary to select the **Update** button.

In order for the automatic license update process to function, access to the Internet is required. If there is no Internet access, instructions on obtaining the license file manually are provided after the **Update** button is pressed.

Licensing SilhouetteTokenService

The SilhouetteTokenService only requires a license file if you are enabling optional features, i.e. SSO Integration. The SilhouetteTokenService doesn't support automatic license file retrieval as described for SilhouetteCentral.

To obtain a license file for the SilhouetteTokenService, supply the server details to ARANZ Medical Support. The server details are the same details required to obtain the SilhouetteCentral license.

To install the license file, rename it to SilhouetteTokenService.lic and place it in the directory (you may need to create the License directory first):

```
<SilhouetteTokenService Web Application Directory>\Files\License\
```

Copyright © 2018-2026 ARANZ Medical Limited

System Configuration

Silhouette can be configured to match clinical needs. Configuration of users, groups, units, and SilhouetteStar 2 settings can be performed via the admin interface. For details please see the Silhouette Administrator's User Guide.

In SilhouetteConnect, some of the configuration available depends on the mode SilhouetteConnect is operating in. For example, if SilhouetteConnect is operating in Synchronized mode then the configuration is mostly contained in SilhouetteCentral.

Copyright © 2018-2026 ARANZ Medical Limited

Single Sign On with an External Authentication Provider

Configuration of SSO feature needs to be coordinated with the configuration of the authentication/identity provider.

The high-level tasks to configure the external authentication provider are:

1. Add the SSO Integration optional feature to the SilhouetteTokenService license.
2. Configure the SilhouetteTokenService with the authentication provider details, see SilhouetteTokenService Web Application Configuration.
3. Provide the SilhouetteTokenService connection information to the authentication provider, including:
    1. Entity ID.
    2. Assertion consumer service endpoints.
    3. Claim mapping requirements.
4. Map Authentication Provider Claims to Silhouette Role and Clinical Data Access groups in SilhouetteCentral administration screens, see the Administration User's Guide.
5. Test SSO integration, see Verify Single Sign On with an External Authentication Provider.
6. Optionally disable Silhouette Local User login, see SilhouetteTokenService Web Application Configuration.

Example: Configuring Silhouette SSO Integration with AD FS

The configuration of Active Directory Federation Services (AD FS) is outside the scope of this documentation and it is recommended that you follow the AD FS configuration manuals. The example offered in these manuals are to provide some context and clarity to assist with the Silhouette configuration.

This example assumes you have the following items in place and are simply adding Silhouette as a Relying Party (RP) into AD FS:

- An AD FS server is in place with an Attribute Store and Claims Provider Trust configured.
- The AD FS Entity ID is `http://adfs.anonhealth.aranz.nz/adfs/services/trust`.
- The AD FS Metadata URL is `https://adfs.anonhealth.aranz.nz/FederationMetadata/2007-06/FederationMetadata.xml`.
- Active Directory (AD) has groups 'SILHOUETTE Vendor Support' , 'SILHOUETTE Admin', 'SILHOUETTE Clinical'.
- AD has users configured with membership in each of the above AD groups.
- The SilhouetteTokenService website is available at `https://anonhealth.aranz.nz/silhouettetoken`.
- The SilhouetteTokenService is already licensed with the optional feature SSO Integration.
- SilhouetteCentral has groups 'ARANZ Medical Support', 'Admin', 'Default' configured.

Copyright © 2018-2026 ARANZ Medical Limited

Configure the SilhouetteTokenService

Edit the SilhouetteTokenService appSettings.production.json file to include the following Saml2 configuration.

```
"Saml2": {
  "Enabled": true,
  "AuthenticationSchemes": [
    {
      "Scheme": "Saml2",
      "DisplayName": "ADFS",
    A "Metadata": "https://anonhealth.aranz.nz/silhouettetoken/Saml2",
      "ModulePath": "",
      "IdentityProviders": [
        {
      B "EntityId": "http://adfs.anonhealth.aranz.nz/adfs/services/trust",
        "Metadata": "https://adfs.anonhealth.aranz.nz/FederationMetadata/2007-06/FederationMetadata.xml",
        "LoadMetadata": true
        }
      ],
      "ClaimTypes": {
        "FirstName": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname",
        "LastName": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname",
        "Email": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress",
        "Group": "http://schemas.xmlsoap.org/claims/Group"
      }
    }
  ]
}
```

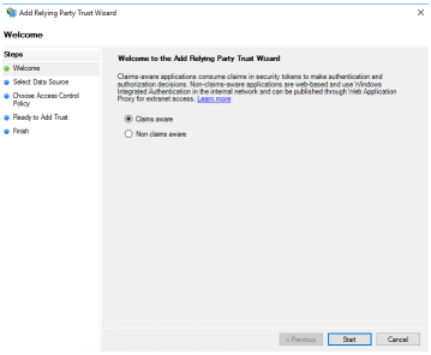
A — The URL where the SilhouetteTokenService Saml2 metadata is available.

B — Entity ID and Metadata URL of the AD FS server.

Stop and start the SilhouetteTokenService to apply the configuration.

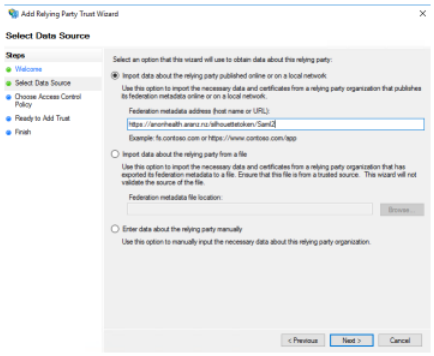
Add Silhouette as a Relying Party Trust to the AD FS Server

Using the AD FS Management interface, select the Add Relying Party Trust action.



SilhouetteTokenService is a Claims aware RP. Select Claims aware and press the Start button.

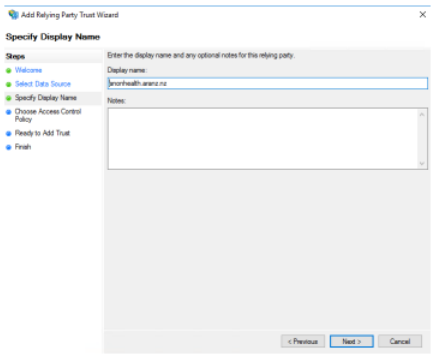
Copyright © 2018-2026 ARANZ Medical Limited



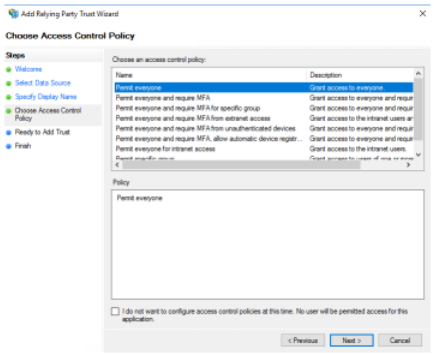
If the SilhouetteTokenService metadata URL is published at a location where the AD FS system can access it, enter the metadata URL in the 'Import data about the relying party published online or on a local network' text box.

Alternatively, the metadata can be imported from a file by navigating to the SilhouetteTokenService metadata URL in a web browser to retrieve the file, which can then be provided to the AD FS system. Once copied the file location can be entered in the 'Import data about the relying party from a file' text box.

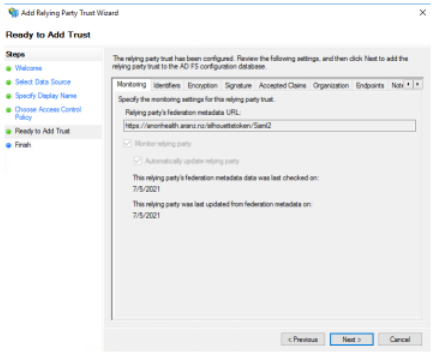
The information entered at this point is case sensitive. If downloading and supplying the metadata file, use the correct case in the URL for downloading the metadata.



Choose a display name for the RP and press the Next button.



Select the appropriate access control policy and select the Next button.

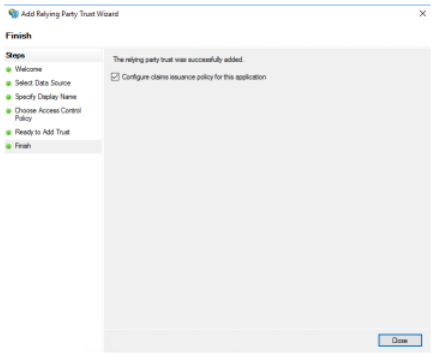


The next step in the wizard shows the RP configuration for review.

SilhouetteTokenService EntityId is shown on the Identifiers tab and the SAML Assertion Consumer Endpoints are listed in the Endpoints tab.

Select the Next button.

Copyright © 2018-2026 ARANZ Medical Limited

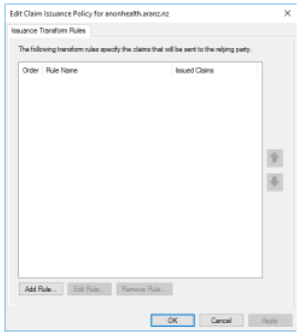


If the RP configuration was successful, you can either move on to configure claims issuance policy or close the wizard.

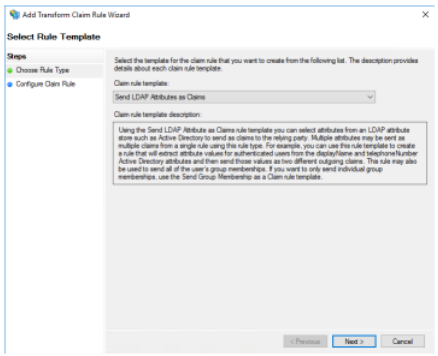
The next step is to setup claim issuance policy to issue claims about the identity to Silhouette. Most of the data about the identity comes as a claim.

An claim issuance policy for an RP can have multiple rules of different types and can have filters applied to the information shared (e.g. only issue group claims that start with Silhouette). This example a simple example of sending LDAP Attributes as Claims.

To edit the claim issuance policy for an RP, select the RP and choose the Edit Claim Issuance Policy action.

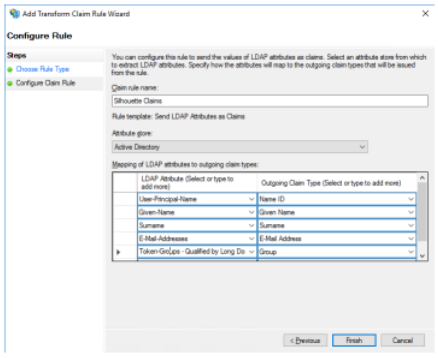


Select the Add Rule... Button.



Select the Rule Type. This example shows sending LDAP attributes as Claims.

Select the Next button.



Give the claim rule a name.

Select the Attribute Store which has been previously configured.

Map LDAP attributes to outgoing claims.

- The left hand attributes are the LDAP attributes to read from the attribute store.
- The right hand column are the names of the claim types that will be sent to Silhouette. These claim types should include the Name ID and all of the ClaimTypes in the SilhouetteTokenService

Copyright © 2018-2026 ARANZ Medical Limited

configuration. Only the Name of the claim is shown here. The AD FS Management console also includes a list of Claim Descriptions which includes the full description of how the Name maps to the full Claim Type (e.g. Name ID = http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier)

Once completed, select Finish and then Apply.

The screenshot shows the LDAP attribute Token Groups - Qualified by Long Domain Names being used as the group identifier. There are a number of options giving slight different information. As by way of an example, the membership to an group 'SILHOUETTE Admin' in the domain med.anonhealth.aranz.nz:

- *Token Groups - Unqualified Names* = SILHOUETTE Admin
- *Token Groups - Qualified by Domain Name* = med\SILHOUETTE Admin
- *Token Groups - Qualified by Long Domain Name* = med.anonhealth.aranz.nz\SILHOUETTE Admin
- *Is-Member-Of-DL* = CN=SILHOUETTE Admin,OU=Wound Care Roles,OU=Clinical,DC=med,DC=anonhealth,DC=aranz,DC=nz

You can also send a custom claim string for a precise group membership using a different type of claim issuance rule.

If users have a lot of group memberships and are using long domain name or Is-Member-Of-DL mapping, the login may fail with HTTP Bad Request - request headers too long errors. In this case it is also possible to apply filters to the group memberships that are sent, only sending those relevant to Silhouette. An example of filtering claims is provided in Appendix C: AD FS Custom Filter Rule Example.

Map Authentication Provider Claims to Silhouette Role and Clinical Data Access

When all the above AD FS configuration done successfully, there is a **Login with ADFS** button on the Silhouette login page. Using that button shows the ADFS login page and users can login with their anonhealth.aranz.nz ID. However, when they do login all they see is a webpage that reports Access Denied until they are part of a AD group that is sent to a claim in AD FS, which is in turn then mapped to a Silhouette Role and/or Cinical Data Access Group.

To map an authentication provider claim to a Silhouette Role or Clinical Data Access Group:

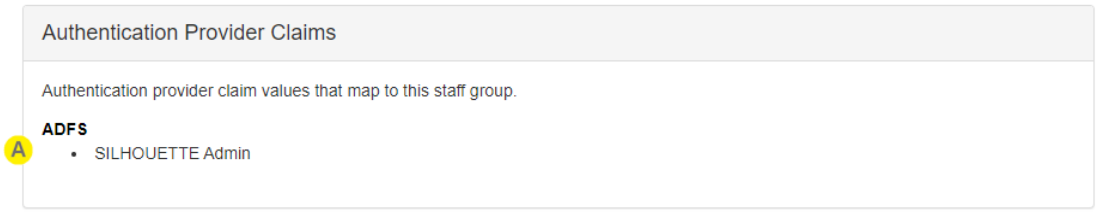
1. Login to SilhouetteCentral as a Local Silhouette User with Can Manage Roles and Can Manage Clinical Data Access permissions.
2. Navigate to **Admin > Clinical Data Access** or **Admin > Roles** and select the Group or Role you wish to apply mapping to.
3. Select **Edit**, add the Authentication Provider Claim mapping for the appropriate Authentication Provider by inserting the exact string you expect to receive in the group claim value and **Save**.
4. Repeat for each Silhouette Role and Clinical Data Access group, mapping the appropriate claim.

Copyright © 2018-2026 ARANZ Medical Limited

5. Once complete, you can logout and then attempt to login through the **Login with ADFS** button on the login page and you will be granted access to the system according to your mapped Authentication Provider Claims.
6. Use the procedure in Verify Single Sign On with an External Authentication Provider to check the mappings and access.

A user account in AD may be a member of lots of groups and can be assigned to multiple Silhouette roles and Clinical Data Access groups.

The administration 'Export Clinical Users' feature can be helpful to review the actual permissions that a user has.



A An example of the claim SILHOUETTE Admin from the ADFS Authentication Provider mapped to the Silhouette Group called Admin.

Disable Silhouette Local User Login

Once SSO integration is complete and you have all user accounts (include ARANZ Medical support and system admin) accounts managed in the external directory, you can disable Silhouette Local User login, see SilhouetteTokenService Web Application Configuration.

Once Silhouette Local User login is disabled, the Silhouette login page is skipped and users will only see the external login provider page.

Use the test listed in Verify Single Sign On with an External Authentication Provider to verify Silhouette Local User login is disabled.

Emergency Access During an Identity Provider Outage

If the external identity provider becomes unavailable and local login is disabled, a server administrator can temporarily re-enable Silhouette Local User login. This procedure requires privileged access to the SilhouetteCentral application server and IIS; it does not require access to SilhouetteCentral.

Enabling local login does not create, enable, unlock, or reset the password of a local account. Before disabling local login, confirm that an enabled local administrator account exists and that its credentials are available for emergency use.

Do not remove the `Saml2.AuthenticationSchemes` configuration to work around a temporary outage. Removing an authentication scheme removes its external user records and its authentication-provider claim mappings from Silhouette.

1. Sign in to the SilhouetteCentral application server using an account that can edit the SilhouetteTokenService configuration and recycle its IIS application pool.

Copyright © 2018-2026 ARANZ Medical Limited

2. Open the SilhouetteTokenService Web Application folder and make a backup copy of `appsettings.Production.json`. Do not modify `appsettings.json`.
3. Open `appsettings.Production.json` in a text editor.
4. In the `AccountSecurity` section, change `AllowLocalLogin` to `true`. If the setting is not present, add it to the section while preserving valid JSON syntax.

```
{
	"AccountSecurity": {
		"AllowLocalLogin": true
	}
}
```

5. Save the file, then recycle the SilhouetteTokenService IIS application pool to apply the change.
6. Navigate to SilhouetteCentral and select **Login**. The local username and password fields are displayed alongside any available external-provider options.
7. Sign in using an existing enabled Silhouette Local User account with the permissions required for the emergency work.

After the identity provider is available again, verify that SSO login is working. If local login was disabled before the outage, change `AccountSecurity.AllowLocalLogin` back to `false`, save the file, and recycle the SilhouetteTokenService application pool again.

Copyright © 2018-2026 ARANZ Medical Limited

Machine Settings File

The file contains a list of settings that does not need modification in general. The only setting that needs modification is the SilhouetteStar 1 cable adapter enable setting. This is only useful if you are using the specific cable adapter for the SilhouetteStar 1.

```
<Star1CableEnabled>true</Star1CableEnabled>
```

By default this field is set to **True**, it can however, be manually edited and changed to **False**. When this field is set to **False** prior to an upgrade, it will retain the setting post-upgrade

The location of the file is dependent on the type of SilhouetteConnect installed on the machine, for

- **Standalone SilhouetteConnect** the file is usually located in *%ProgramData%\ARANZ Medical Limited\SilhouetteConnect\Settings*
- **Synced SilhouetteConnect** the usual location is *%localappdata%\ARANZ Medical Limited\SilhouetteConnect\Settings*

Copyright © 2018-2026 ARANZ Medical Limited

SilhouetteCentral Testing

This section describes how to test the SilhouetteCentral installation and configuration is working as expected. You may want to perform these tests after the initial installation and after any subsequent changes to the configuration.

Not all tests are relevant to every SilhouetteCentral installation. Choose the tests that match your configuration.

- Verify Basic SilhouetteCentral Operation with Local Silhouette Users
- Verify SilhouetteConnect Sync
- Verify Single Sign On with an External Authentication Provider

Copyright © 2018-2026 ARANZ Medical Limited

Verify Basic SilhouetteCentral Operation with Local Silhouette Users

The tests listed here can be used to confirm the deployment of the SilhouetteCentral system has completed successfully and is working with Local Silhouette Users.

1: Login/Logout with a Silhouette Local User account

Use this procedure to check the SilhouetteTokenService is correctly configured with `AccountSecurity.AllowLocalLogin` set to `true`. Use this test on initial deployment or if the configuration is changed.

1. Navigate to the SilhouetteCentral web application URL. You see the SilhouetteCentral unauthenticated user landing page with a Login button.
2. Select **Login**. You are presented with a SilhouetteCentral login which includes Username and Password text entry boxes.
3. Enter an invalid username and password and select **Login**. The login is rejected.
4. Enter a valid username and password and select Login. The SilhouetteCentral web application loads and you can navigate in the application.
5. Select **Logout** from the application menu. The user is logged out and is returned to the SilhouetteCentral unauthenticated user landing page. Pressing the back button on the browser does not take you back into the SilhouetteCentral application.

2: Verify Help and About page is accessible

Use this procedure to verify that the help and about page is accessible and that the required VC++ runtime is working.

1. Access the SilhouetteCentral website and use the **Help and About** link on the unauthenticated landing page or from the application menu when logged in.
2. Check that the help and about page loads and shows the UDI data matrix and the expected software version beside the REF icon.

Copyright © 2018-2026 ARANZ Medical Limited

Verify SilhouetteConnect Sync

The tests listed here can be used to confirm the deployment of SilhouetteConnect in Synchronized mode with SilhouetteCentral.

Select the appropriate procedures for your configuration.

1: Login to SilhouetteConnect and perform a sync

Use this procedure to check the Silhouette system is setup and is capable of syncing data between SilhouetteConnect and SilhouetteCentral.

1. Open the SilhouetteConnect application on you PC. You see the SilhouetteConnect unauthenticated user landing page with a Login button.
2. Select **Login**. Your default web browser will open a new tab.
3. If you see the Silhouette login page, complete the login.
4. The web browser may show a pop-up message asking for your approval to use SilhouetteConnect to open a link. Grant your permission.
5. SilhouetteConnect might ask you to perform a sync, if so do perform the sync.
6. You see the main SilhouetteConnect application, with your username in the top right.
7. Select **Sync** from the application menu. The sync completes successfully.

Copyright © 2018-2026 ARANZ Medical Limited

Verify Single Sign On with an External Authentication Provider

The tests listed here can be used to confirm the deployment of the SilhouetteCentral system configured with Single Sign On (SSO) using an external authentication provider (e.g. ADFS).

Tests are also provided to confirm operation on various configuration changes relating to SSO, including when an external authentication provider has been disabled or when Silhouette Local User logins are disabled.

Select the appropriate procedures for your configuration.

1: Login with an external authentication provider user account

Use this procedure to check the Silhouette system and external authentication provider are correctly configured. The use of this procedure proves the following:

- The SilhouetteTokenService is configured with `Saml2.Enabled` set to `true`.
- The SilhouetteTokenService is configured a valid `Saml2.AuthenticationSchemes` configuration.
- The SilhouetteCentral Group configuration has correctly mapped Authentication Provider Claims.

1. Navigate to the SilhouetteCentral web application URL. You see the SilhouetteCentral unauthenticated user landing page with a Login button.
2. Select **Login**.
3. If you see the Silhouette login page, there is a **Login with <displayName>** button to initiate the login with the authentication provider. Select the **Login with <displayName>** button.
4. If you see the authentication provider login page, proceed with the login.
5. You are logged in to the SilhouetteCentral application and can navigate to view your user profile under **Admin > Profile** or **Admin > Users**.

If possible, have someone assigned to each of the Silhouette groups login to check that all authentication provider mapping is correct.

2: Verify Allow Local Login (Silhouette Local users) is disabled

Use this procedure to check the SilhouetteTokenService is correctly configured with `AccountSecurity.AllowLocalLogin` set to `false`.

1. Navigate to the SilhouetteCentral web application URL. You see the SilhouetteCentral unauthenticated user landing page with a Login button.
2. Select **Login**. You are not presented with a Silhouette login page with Username and Password text entry boxes. You are either:
    1. Presented with a Silhouette login page with buttons to select between external authentication providers.
    2. Presented with a login page from the external authentication provider.
    3. Logged in to the SilhouetteCentral app automatically based on an active session established with the external authentication provider.

Copyright © 2018-2026 ARANZ Medical Limited

3: Verify an external authentication provider has been disabled

Use this procedure to check an external authentication provider configuration has been disabled. The use of this procedure proves the SilhouetteTokenService configuration has had a `Saml2.AuthenticationSchemes` successfully removed.

1. Navigate to the SilhouetteCentral web application URL. You see the SilhouetteCentral unauthenticated user landing page with a Login button.
2. Select **Login**.
3. You see the Silhouette login page and there is no **Login with <displayName>** button.
4. Proceed to login as a Local Silhouette User with Can Manage Clinical Users permission.
5. Navigate to Admin -> Users. Review the list of users to confirm there are no longer any user records listed for the removed authentication scheme.

Copyright © 2018-2026 ARANZ Medical Limited

Troubleshooting

This section describes how to troubleshoot problems which can be encountered on initial installation or upgrade of SilhouetteCentral, SilhouetteTokenService, and SilhouetteConnect.

Use the following order when troubleshooting a Silhouette system:

1. Make sure the SilhouetteTokenService is operational, see SilhouetteTokenService Troubleshooting.
2. Make sure SilhouetteCentral is operational, see SilhouetteCentral Troubleshooting.
3. Make sure SilhouetteConnect is operational and sync is possible, see SilhouetteConnect Troubleshooting.

Copyright © 2018-2026 ARANZ Medical Limited

SilhouetteTokenService Troubleshooting

To confirm the SilhouetteTokenService is operational, open a web browser and navigate to the https://<SilhouetteTokenService URL>/.well-known/openid-configuration.

If the service is running, the result will be some plain JSON text.

If an error is reported, follow the troubleshooting steps below to investigate.

1. Check the SilhouetteTokenService Log files for error reports.
2. Check the Application events log in the Windows Event Viewer for any reported errors from the source "IIS AspNetCore Module V2".
3. Check that the SilhouetteTokenService Application Pool Identity has modify rights on the Files sub-folder.

Copyright © 2018-2026 ARANZ Medical Limited

SilhouetteCentral Troubleshooting

To confirm that SilhouetteCentral is running, you can browse to the SilhouetteCentral URL and you should see the SilhouetteCentral unauthenticated landing page (or the SilhouetteCentral app if you already have an active session).

If SilhouetteCentral reports an error, first confirm that the SilhouetteTokenService is operational, see SilhouetteTokenService Troubleshooting. After that, further errors can be investigated by:

1. Check the SilhouetteCentral Log files for error reports.
2. Check the Application events log in the Windows Event Viewer for any reported errors from the source "ASP.NET 4.0.30319.0".
3. Check that the SilhouetteCentral Application Pool Identity has modify rights on the Files sub-folder.

Copyright © 2018-2026 ARANZ Medical Limited

SilhouetteConnect Troubleshooting

The troubleshooting discussed here is focused on the problems that can occur on initial installation or upgrade. The Administration User's Guide and the Clinical User's Guide have additional troubleshooting information for problems that can occur after initial setup.

To confirm that SilhouetteConnect is running successfully in Synchronized mode:

- Open the SilhouetteConnect application.
- Login.
- Perform a sync.

Problems when starting SilhouetteConnect

If SilhouetteConnect reports an error attempting to start, the problem is likely to be localized to the PC. Errors are investigated primarily by checking the SilhouetteConnect log files. However, there can also be some information in the Windows Event Viewer > Application Event Log where there are problems with the SQL Server Database instance.

Some of the causes of issues known to be caused by configuration are:

- Missing dependencies for .NET Framework or the SQL Server Database Instance. To remedy this issue, install the correct dependencies.
- A previous installation of SilhouetteConnect was not tidied up correctly. See the help topic Uninstalling SilhouetteConnect for details on how to correctly clean an installation.
- There are known compatibility issues with SQL Server Database instance and Windows 11 and some disk types, see the help topic Pre-requisites for installing SilhouetteConnect on Windows 11 for details.
- An error message like "URL Reservation is not found. Contact your system administrator." indicates that the SilhouetteConnect dependency bundle needs to be installed. See Installing SilhouetteConnect

Problems when logging in

The expected login flow for a SilhouetteConnect in Synchronized mode, is that the web browser will open to allow you to login. Once the login is completed in the web browser, SilhouetteConnect will load the application and show your name in the top left corner of the screen.

The first step to solve a login issue is to restart SilhouetteConnect as there are a number of unusual cases which can occur on initial launch after install and major configuration changes.

If the web browser does not open, you can manually navigate to the SilhouetteCentral URL to confirm that the PC has the required network connectivity and that both the SilhouetteTokenService and SilhouetteCentral is operational.

Further troubleshooting information can be retrieved from the SilhouetteConnect logs and the SilhouetteTokenService logs.

Problems when syncing

If SilhouetteConnect reports an error when trying to sync with SilhouetteCentral, first confirm that SilhouetteCentral is operational, see the help topic SilhouetteCentral Troubleshooting. After that, further errors can be investigated by:

Copyright © 2018-2026 ARANZ Medical Limited

1. Check the SilhouetteConnect Log files for error reports.
2. Check the SilhouetteCentral Log files for error reports.

Some of the sync errors that are known to be caused by configuration issues are:

- The Sync URL is from an older installation has not been updated to the HTTPS protocol causing an authentication failure when attempting to download the required files from the server. Modify the Sync URL to remedy this issue.
- The identity running the SQL Server Synchronization Instance on the SilhouetteCentral server doesn't have modify rights on the \Files\mdfCreation folder in the SilhouetteCentral Web Application folder. Re-check the SilhouetteCentral configuration to ensure correct rights are granted.

Copyright © 2018-2026 ARANZ Medical Limited

Appendices

 Appendix A: IIS Configuration

 Appendix B: SQL Server Configuration

 Appendix C: AD FS Custom Filter Rule Example

Copyright © 2018-2026 ARANZ Medical Limited

Appendix A: IIS Configuration

This topic provides some guidance for configuring IIS using either the IIS Management Console or the PowerShell WebAdministration module.

Configure IIS using the IIS Management Console

1. Open IIS Manager.
2. Creating a new application pool:
    1. In the Connections pane, right-click the Application Pools node.
    2. Select Add Application Pool.
    3. Give the pool a unique name and set the appropriate settings as per the relevant section of the Installation and Configuration guide.
    4. Click OK.
    5. Right-click on the new Application Pool in the list and select Advanced Settings...
    6. Set any advanced mode settings as per the relevant section of the Installation and Configuration guide, e.g. Start Mode, Application Pool Identity, etc.
    7. Click OK.
3. Adding a web application into IIS:
    1. In the Connections pane, expand the Sites node and then the node representing your website (e.g. Default Web Site).
    2. Either:
        1. Right-click the folder the node representing the folder you created in step 1 and click Convert To Application, or
        2. Right-click the website and select Add Application.
    3. Set the Alias if you need to (the path portion of the URL).
    4. Choose the application pool you want to run the web application.
    5. Set the physical path if you need to (the path on the file system).
    6. Click OK.
    7. Right-click the web application node in IIS and selecting Advanced Settings... to review and set web application settings as per the relevant section of the Installation and Configuration guide.

Configure IIS via Windows PowerShell

The application pool and web application may also be scripted via a PowerShell command prompt. The following example sets up a SilhouetteCentral and SilhouetteTokenService web site:

```
Import-Module WebAdministration

New-WebAppPool -Name Silhouette

Set-ItemProperty -Path IIS:\AppPools\Silhouette `
 -Name "managedRuntimeVersion" -Value "v4.0"
```

Copyright © 2018-2026 ARANZ Medical Limited

```
Set-ItemProperty -Path IIS:\AppPools\Silhouette `
 -Name "startMode" -Value "AlwaysRunning"

Set-ItemProperty -Path IIS:\AppPools\Silhouette `
 -Name "loadUserProfile" -Value "True"

New-WebAppPool -Name SilhouetteToken

Set-ItemProperty -Path IIS:\AppPools\SilhouetteToken `
 -Name "startMode" -Value "AlwaysRunning"

Set-ItemProperty -Path IIS:\AppPools\SilhouetteToken `
 -Name "loadUserProfile" -Value "True"

New-WebApplication -Name silhouette `
 -Site "Default Web Site" `
 -PhysicalPath c:\inetpub\wwwroot\silhouette `
 -ApplicationPool Silhouette

Set-ItemProperty -Path "IIS:\Sites\Default Web Site\silhouette" `
 -Name "preloadEnabled" -Value "True"

New-WebApplication -Name silhouettetoken `
 -Site "Default Web Site" `
 -PhysicalPath c:\inetpub\wwwroot\silhouettetoken `
 -ApplicationPool SilhouetteToken

Set-ItemProperty -Path "IIS:\Sites\Default Web Site\silhouettetoken" `
 -Name "preloadEnabled" -Value "True"
```

Copyright © 2018-2026 ARANZ Medical Limited

IIS and File System Permissions

The identity used by the application pool (by default set to IIS AppPool\Silhouette) requires read and execute permission to all files within the web application folder. By default, IIS automatically add the application pool identity as a member of the local IIS_IUSRS group, which by default has read access to all web applications hosted in the wwwroot folder. If you are not using a sub-folder of the wwwroot folder as the web application physical path, grant read & execute rights to the IIS_IUSRS built in windows group to the folder you are using.

The IIS anonymous authentication user (built in IUSR identity) typically has read access to the web application folder by default through the Users group. If the IUSR identity doesn't have access you will get authentication errors when trying to serve static resources from the web application folder. If you experience this, grant the IUSR account Read & Execute access to the web application folder.

Copyright © 2018-2026 ARANZ Medical Limited

Appendix B: SQL Server Configuration

This help topic covers basic SQL Server setup and configuration suited for use with Silhouette. This guide is offered as a quick start and is not intended to replace the MS SQL Server installation and deployment instructions.

Installing SQL Server

> The use of SQL Server Express Edition is not recommended for production installations due to limitations on database performance, size, and features.

The exact instructions to install SQL Server depend on the SQL Server edition and version. The basic SQL Server 2022 steps are provided below. Review the current Microsoft SQL Server installation instructions and apply your organization's database, security, storage, backup, and high-availability standards.

1. Sign in to Windows using an account authorized to install SQL Server, then run `setup.exe` as an administrator.
2. In SQL Server Installation Center, select **Installation**, then select **New SQL Server stand-alone installation or add features to an existing installation**.
3. Complete the Edition, license terms, and setup-rule pages. Resolve any failed setup rules before continuing.
4. If the Azure Extension for SQL Server page is displayed, select or clear the extension according to your organization's Azure management policy.
5. On the Feature Selection page, select **Database Engine Services**. SQL Server Management Studio (SSMS) is no longer included in SQL Server Setup and must be installed separately.
6. On the Instance Configuration page, choose a default or named instance according to the deployment design. If using a named instance, enter an appropriate name, for example `SQLSILHOUETTE`. Record the instance name for use in the Silhouette connection strings.
7. On the Server Configuration page, configure the SQL Server service accounts, startup types, and collation according to your organization's standards.
8. On the Database Engine Configuration page:
    1. Select **Windows authentication mode** where possible. If the optional SilhouetteCentral Dashboard feature will be used, select **Mixed Mode** because its reporting account uses SQL Server authentication, and specify a strong `sa` password.
    2. Under **Specify SQL Server administrators**, select **Add Current User** and add the appropriate DBA users or groups. SQL Server 2022 does not automatically grant local Windows administrators access to the Database Engine.
    3. Review the Data Directories, TempDB, MaxDOP, and Memory tabs and apply the settings required by your DBA or organizational standards.
9. Complete the Ready to Install and installation-progress pages, then confirm that the Database Engine installation succeeded.
10. Install the current supported release of SSMS on the administration workstation or server if it is not already available.

Copyright © 2018-2026 ARANZ Medical Limited

Creating a SilhouetteCentral Database

Once SQL Server has been installed a blank database must be created to store all clinical assessment data. This can be created in a number of ways including:

- SQL Server Management Studio
- Windows PowerShell

Creating a Database using SQL Server Management Studio

1. Open SSMS and connect to the required Database Engine instance using an account authorized to create databases, logins, and users.
2. In Object Explorer, right-click **Databases**, select **New Database...**, enter `Silhouette` as the database name, then select **OK**.
3. Identify the Windows principal used by each web application to connect to SQL Server. Both SilhouetteCentral and SilhouetteTokenService require access:
   - For the default, separate application pools and a SQL Server instance on the IIS server, use `IIS AppPool\SilhouetteCentral` and `IIS AppPool\SilhouetteToken`.
   - If both application pools use the same custom domain or group managed service account, grant that account access once.
   - If SQL Server is on another server and the application pools use ApplicationPoolIdentity, grant access to the IIS server's domain computer account, for example `DOMAIN\WEBSERVER$`. Both application pools present this account when accessing network resources.
   - If the application pools use separate custom domain identities, grant access to both domain accounts.
4. For each distinct Windows principal identified above:
   1. In Object Explorer, expand the server-level **Security** node, right-click **Logins**, then select **New Login...**.
   2. Enter or search for the Windows principal in **Login name**.
   3. Select the **User Mapping** page, select the **Silhouette** database, then select the **db_owner** database-role membership.
   4. Select **OK**.

Creating a Database using Windows PowerShell

Creation of the SilhouetteCentral database may also be scripted from an elevated PowerShell prompt. The following example requires the `Invoke-Sqlcmd` command from the SqlServer PowerShell module and assumes SQL Server is on the IIS server, the named instance is `SQLSILHOUETTE`, and the web applications use their default, separate application-pool identities:

```
Invoke-Sqlcmd -ServerInstance '.\SQLSILHOUETTE' -Query 'CREATE DATABASE [Silhouette];'

Invoke-Sqlcmd -ServerInstance '.\SQLSILHOUETTE' -Query 'CREATE LOGIN [IIS AppPool\SilhouetteCentral] FROM
WINDOWS WITH DEFAULT_DATABASE=[Silhouette];'

Invoke-Sqlcmd -ServerInstance '.\SQLSILHOUETTE' -Query 'USE [Silhouette]; CREATE USER [IIS
AppPool\SilhouetteCentral] FOR LOGIN [IIS AppPool\SilhouetteCentral]; ALTER ROLE [db_owner] ADD MEMBER
[IIS AppPool\SilhouetteCentral];'
```

Copyright © 2018-2026 ARANZ Medical Limited

```
Invoke-Sqlcmd -ServerInstance '.\SQLSILHOUETTE' -Query 'CREATE LOGIN [IIS AppPool\SilhouetteToken] FROM
WINDOWS WITH DEFAULT_DATABASE=[Silhouette];'

Invoke-Sqlcmd -ServerInstance '.\SQLSILHOUETTE' -Query 'USE [Silhouette]; CREATE USER [IIS
AppPool\SilhouetteToken] FOR LOGIN [IIS AppPool\SilhouetteToken]; ALTER ROLE [db_owner] ADD MEMBER [IIS
AppPool\SilhouetteToken];'
```

Replace the server instance, database name, and Windows principals with the values for the deployment. Grant each distinct principal only once. For a remote SQL Server using ApplicationPoolIdentity, replace both local virtual-account examples with the IIS server's domain computer account. For custom application-pool identities, use the relevant domain or group managed service account or accounts.



The local `IIS AppPool\<pool name>` virtual accounts can be granted SQL Server access only when SQL Server is on the IIS server. Create both application pools before adding these logins. When SQL Server is remote, ApplicationPoolIdentity accesses it as the IIS server's domain computer account; alternatively, configure the application pools to use a custom domain identity. Do not attempt to create an `IIS AppPool\...` login on the remote database server.

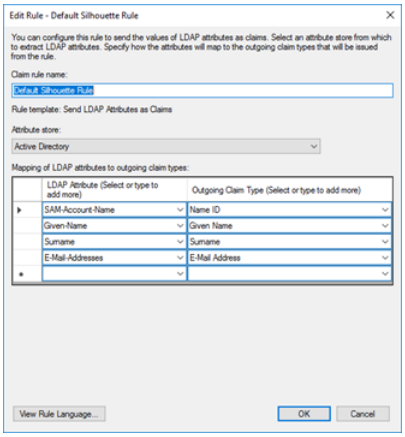
Copyright © 2018-2026 ARANZ Medical Limited

Appendix C: AD FS Custom Filter Rule Example

This help topic provides an example of AD FS custom claim issuance rules that filter a user's group memberships, only issuing group claims that are relevant to Silhouette.

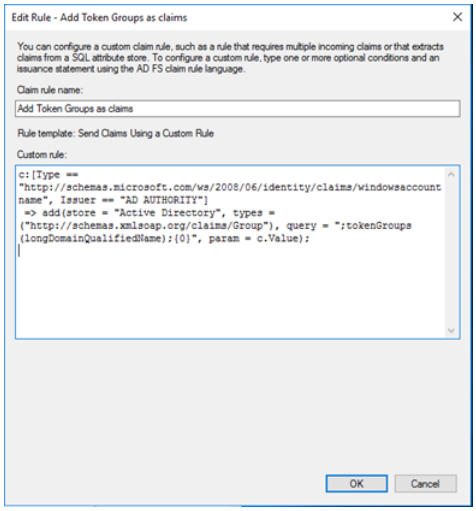
The example uses three issuance claim rules.

Rule 1 - Issue non-group claims



The first rule is created from the Send LDAP Attributes as Claims template. It issues Name Id, Given Name, Surname, and E-Mail Address. Notably it does not issue the Group claims.

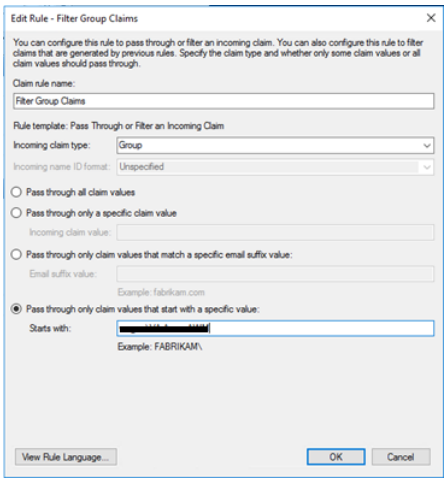
Rule 2 - Add groups to claims



The second rule is a custom rule to add (not issue) group membership into the claim set. The custom rule uses the rule language.

Copyright © 2018-2026 ARANZ Medical Limited

Rule 3 - Issue a filtered set of group claims



The third rule uses the "Pass through or filter an incoming claim rule" template. It filters the claims added in rule two and issues them.

As an example, if all relevant AD groups being with 'SILHOUETTE' then enter 'SILHOUETTE' in the Starts with text box. If Rule 2 is adding 'longDomainQualifiedNames' then the starts with filter needs the long domain included, e.g. domain\SILHOUETTE.

Copyright © 2018-2026 ARANZ Medical Limited