I1

Field Guide: Integration and Infrastructure

IMPL.

ebms

nimblex

Contents

1 Infrastructure and Integration

This document gives some guidance around the Infrastructure (Servers etc.), Information Technology (IT) and Integration needs of an implementation.

Matters where you may need to consult your IT department have been highlighted with an orange tip like this.

2 Infrastructure

You will need to address only one of these sub-sections, dependant upon your selected hosting model.

2.1 Public Cloud, and Private Cloud

A public cloud system is a pure SaaS (Software as a Service) delivered application that runs on (in this case) eBMS common server infrastructure.

A private cloud system is a SaaS-delivered application running on servers dedicated to a single client. eBMS makes use of Microsoft Azure for our Private Cloud servers.

For implementations on the cloud, you are unlikely to need significant IT involvement, as the system is web-based and compatible with typical Office and email tools.

You may need IT to be involved in integration-related tasks (See 3 Integration). For integration in a private cloud environment, it is suggested that may want to have a VPN set up between the Private cloud and your site, also requiring IT participation.

2.2 On-Premises

An on-premises implementation is installed on equipment owned and managed by the client, usually located on your site or in your data-center.

You and your IT department will be responsible for the provisioning of all the required server environments and providing eBMS with appropriate access to these environments for installation, support and upgrades. IT will also be involved in setting up an email account (or providing SMTP relay information) for email notifications from the system.

2.2.1 Server Setup

Please refer to 2.3.2 Server Configuration Options.

2.2.2 Remote Access

eBMS requires remote access to the related server environments at a minimum for the time duration required to install the Nimblex application. We are comfortable with a wide range of VPNs and remote access tools. Generally, we make use of Remote Desktop to work on the actual servers. We may also require access for support purposes and to install security patches and upgrades. At your option, this may be a permanent arrangement or provided on an as-required basis.

2.2.3 Database

The Nimblex platform runs as an IIS (Internet Information Server) application and a Windows Service. To access the required backend database, you will need either an SQL account or an AD service account. For setup, it is advisable to give this account full control over the application's databases.

A typical on-premises install requires two databases – a book-keeping database called ‘shared’ and an application database.

2.2.4 Dependencies

Nimblex makes use of a third-party application called Wkhtmltopdf, which converts HTML content to PDF format. This will be provided by eBMS and needs to be installed on the application server.

2.2.5 Email Notifications

The Nimblex platform can be set up to send emails to users. To do this, you will need to supply SMTP outgoing information. This may be an email server, username and password, or it may be an SMTP relay.

The following information is needed:

Setting	Explanation
Host	The IP Address or DNS name of an SMTP server
Port	The incoming port of the SMTP server
Username	User account to authenticate against the SMTP server (not required when using an SMTP relay)
Password	User account to authenticate against the SMTP server (not required when using an SMTP relay)
Auth Mode	SSLTLS, Basic or None
Display Name	Appears in the **From** field of emails sent out
From Address	Appears in the **From** field of emails sent out

2.3 Nimblex Technical Requirements

This whole section will require IT input.

This section describes what hardware and software are required to run Nimblex in an on-premises arrangement. For Public and Private cloud hosting you can skip this section.

2.3.1 Operating System Requirements

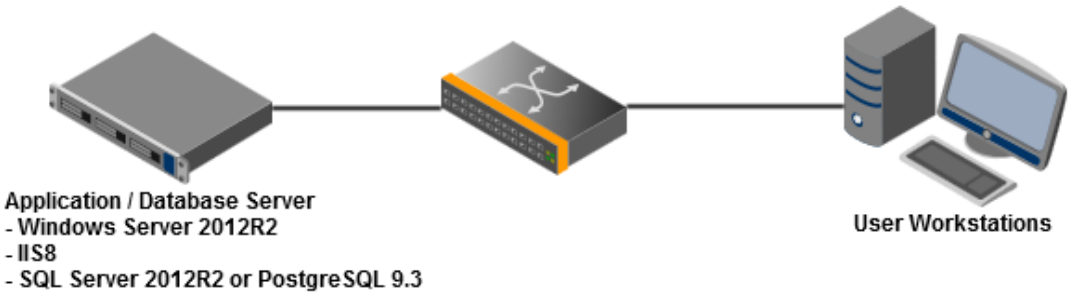
The Nimblex application will reside on any server running Windows 2016 Web Edition (or higher year / edition).

It requires ASP.net and the .NET Framework 4.7 to be installed.

2.3.2 Server Configuration Options

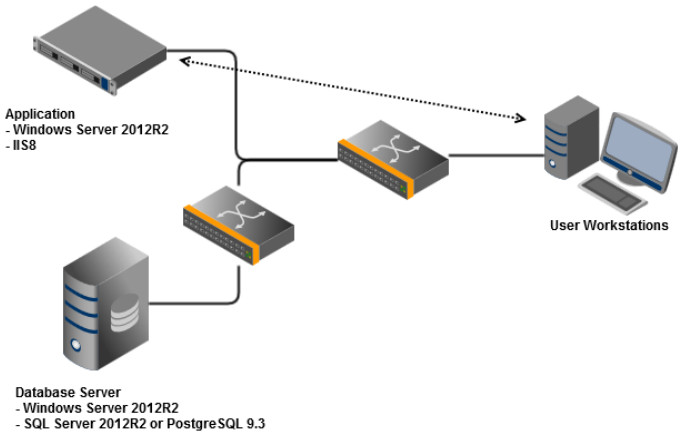
There are several configurations of servers that can work. The most common are 1) single 'big' server, or 2) separate app and database server. Alternatively, you can locate your database on a shared database server that is used for other applications as well.

2.3.2.1 (Option 1) Single Server



Configuration	Application Server	
Joint Application and Database Server	x64, 2.0 GHz Dual Core Processor 4GB RAM Minimum of 10 GB HDD space	**Note:** This specification is for a single instance of the platform, hosts with multiple tenants may require more RAM and processing power, depending on load.

2.3.2.2 (Option 2) Split Database and Application Servers



Configuration	Application Server	
Application Server *For hosting database separately*	x64, 2.0 GHz Dual Core Processor 4GB RAM Minimum of 10 GB HDD space	**Note:** This specification is for a single instance of the platform, hosts with multiple tenants may require more RAM and processing power, depending on load.
Database Option 1: Database Server (Microsoft SQL Server)	x64, 2.0 GHz Dual Core Processor 4GB RAM Minimum of 10 GB HDD space	Typically allow about 2GB RAM for SQL Server to use. SQL Server does not hard limit the memory usage, so a buffer is required. This may be a shared database environment. **Note:** This specification is for a single instance of the platform, hosts with multiple tenants may require more RAM and processing power, depending on load.
Database Option 2: Database Server (PostgreSQL)	x64, 2.0 GHz Dual Core Processor 4GB RAM Minimum of 10 GB HDD space	Typically allow about 500 MB RAM for Postgres to use. This may be a shared database environment. **Note:** This specification is for a single instance of the platform, hosts with multiple tenants may require more RAM and processing power, depending on load.
Microsoft Azure Application and Database Server	Either: 2 vCPU 7GB RAM or 4 vCPU 14GB RAM 128GB Premium SSD	DS2v2 or DS3v2, with image: Windows Server 2016 and SQL Server Web Edition

2.3.3 Hardware Requirements

For an installation of Nimblex, you will need at least an application server and a database server, OR a joint Application/Database server.

2.3.3.1 (Option 3) Shared Database Servers

Nimblex will happily co-exist in a shared database server environment, but it is difficult for us to give exact processor requirements due to the unknown (to us) requirements of other applications using the database. Note also that should performance issues arise may prove more difficult to isolate and resolve in a shared database environment.

We recommend allowing the database at least 1GB of RAM

3 Integration

3.1 Standard Integrations

Standard integrations are intrinsic to the Nimblex application, so will not incur additional ongoing costs. If you need eBMS services for implementation, this is a billable service, so please let us know at the sales stage if possible.

Standard Integrations are discussed below:

3.1.1 Active Directory Integration

Most organisations make use of Microsoft's Active Directory to manage accounts and computers within their network. The Nimblex platform can be configured to integrate seamlessly with Active Directory, allowing user accounts to be managed from Active Directory and/or to allow users to sign on with their network accounts.

Each Organisation manages their AD differently, you will need your IT departments' advice around how best to link your AD to Nimblex. This may include: where are the users? are there any groups set up that roughly mirror your Nimblex needs? what information is in AD for each user?

The following information is needed to set up the link:

Setting	Explanation
AD Controller Address	Optional when joined to a domain this will be autodetected
Username	Username of a service account used to access AD for synchronisation
Password	Password of a service account used to access AD for synchronisation
Domain Name	E.g. ebms.com.au
Target Group	*Only applies when 'Group' is selected* A user group for which all members will be synchronised
Search Container	*Only applies when 'BaseAndFilter' is selected* The full distinguished name of an OU to search. This may be the root of the Domain.
Search Filter	*Only applies when 'BaseAndFilter' is selected* A filter to apply when searching for accounts to synchronise. E.g. (objectClass=user)
How to Derive DisplayName?	How the system will generate a Display Name for each user: DisplayName, FirstLast, LastFirst, LastCommaFirst, DontDerive

Time of day to Synch	Defaults to midnight. Daily at this time of day the system will perform a full synchronisation pass.
Scheduled synchronisation enabled?	When not enabled users will not be synchronised and will need to be manually managed. (Not recommended)
Use Active Directory for authenticating users?	When enabled passwords will be checked against AD – otherwise Nimblex native passwords will be used.

To enable Windows Integrated Authentication the following criteria must be met:

- The server must be joined to the AD Domain
- Windows Integrated Authentication must be turned on for the website (and no others)
- Your users' internet browser must be configured with the address to the system in the list of Intranet sites (or otherwise recognise that it is an intranet side – I.e. sometimes this will 'just work' with a non-domain-qualified host name)

3.1.2 SAML2 Integration (ADFS, Azure AD, Others)

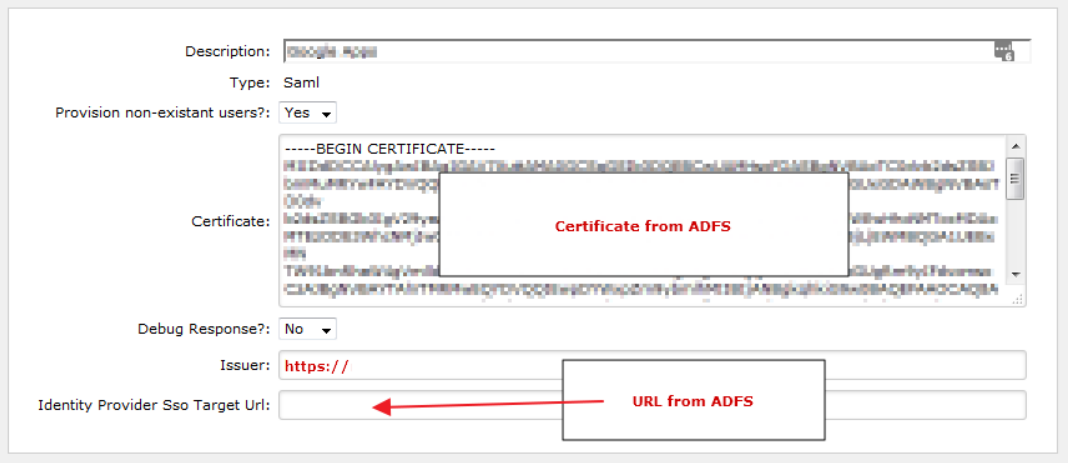
Nimblex SAML2.0 Integration allows for SSO (Single Sign On) with various SAML2.0 Identity Providers, including but not limited to:

- Active Directory Federation Services
- Azure Active Directory (see: https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/nimblex-tutorial)
- Google's G Suite

Your IT department will need to register the Nimblex application with your SAML 'Identity Provider' and share some information with the eBMS implementation team.

SAML2.0 is purely an SSO solution so does not synchronise the full user list from system to system but can be configured to provision user accounts on-demand (I.e. when the user successfully identifies themselves). Alternatively, Administrators can create users manually, or via the JSON API.

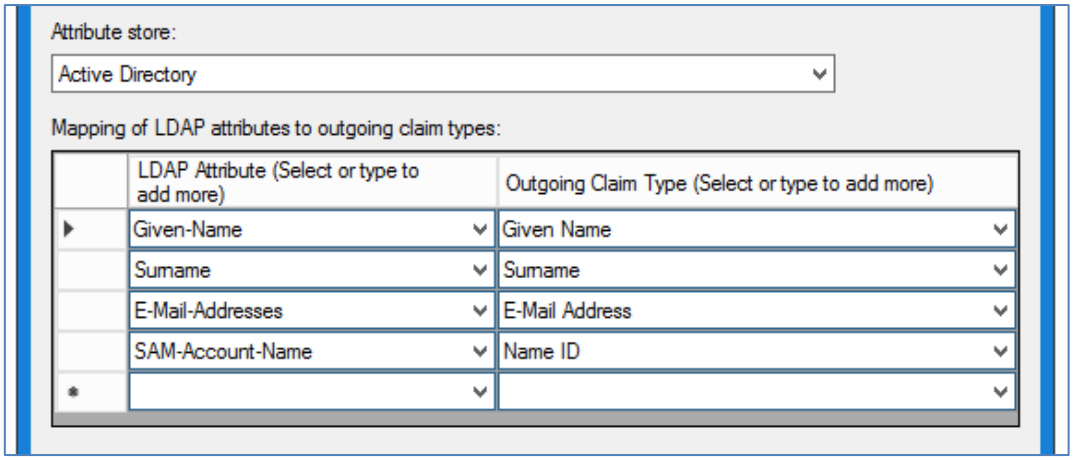
*Note: This does **not** need to be on the same network or joined to the same domain (Unlike AD SSO)*



eBMS will provide:

Setting	Value
SSO service URL (reply URL based on system URL)	https://systemurl.com.au/SamlReply.aspx
Identifier (system url)	https://systemurl.com.au

These are the default claims expected:



Settings needed from the Identity Provider (These can be extracted from IDP metadata):

Setting	Description
Verification certificate	Export of the certificate used by ADFS to sign tokens, which Nimblex will use to verify the source of SAML messages. (PEM format required)
Identity Provider SSO target URL	ADFS login URL (Reachable from client machine)

3.1.3 Sending Emails

For Cloud environments, eBMS will manage this. You can at your option provide us with your SMTP information if you wish to use your own email infrastructure (And therefore control the address that is used).

For on-premises installs you will need to provide your SMTP information as per (2.2.5 Email Notifications);

3.1.4 Receiving Emails

The Nimblex platform can be configured to capture emails sent to a specific email address. **Note** that you will need to provide your defined mailbox, as eBMS does not currently offer mailboxes as a service.

To do this, POP3 settings for an email inbox need to be supplied.

It is strongly advised that you not use an email account that is also used for another purpose, as this will almost certainly interfere with the required functionality.

The following information is needed:

Setting	Explanation
Host	The IP Address or DNS name of a POP3 server
Port	The listening port of the POP3 server (TLS: 995)
Username	User account to authenticate against the POP3 server
Password	User account to authenticate against the POP3 server
Use TLS?	Secure vs plaintext – recommend 'Yes'
Validate Certificate?	Optional security function – generally recommend turning this on, but if your mail server does not have a correct SSL certificate this will fail.

3.2 Plugin Integrations

These are some integrations which require an additional plugin service (with associated costs), but do not require custom development.

Plugin	Description
DocuSign	Using our DocuSign integration, you can send documents for signing via email. Read more: https://getnimblex.com/services/docusign/
QIN	QIN is a mobile app allowing recording of data and submission of forms from your mobile device, without an ongoing internet connection. https://getnimblex.com/solutions/nimblex-qin-mobility-solution/

3.3 Custom Integrations

Custom integrations will require substantial input from your IT department. It is a good idea to involve them early, as Integration implementation can be some of the most time-consuming work in your application implementation.

Custom integrations are those that are not native to the Nimblex application. There are several ways to achieve this integration, detailed in sub-headings in this section.

Section	Type
0	By **Reference**
3.3.2	External party accessing **Nimblex API**
3.3.3	Accessing a **3rd party API**
0	Scheduled import from **file**
3.3.5	Accessing a 3rd party **database** directly

Each option has its advantages and disadvantages. From hard-earned experience, we have learnt that it is challenging to find a one size fits all approach, so we look to partner with clients to implement integration that suits their needs.

When implementing a custom integration, eBMS will prepare an Integration specification that details each point of contact between the two systems.

3.3.1 By Reference

This is the simplest type of integration, where you enter a reference number within Nimblex relating to a record in another system. If the other system is web-based, you could enter a hyperlink instead – allowing your user to create the link and subsequently to be navigated directly to the record. Our 'editable hyperlink' control allows you to drag a drop a link from an email or website directly into the system.

Depending on requirements and complexity, this may be included as part of the configuration budget of your project, and not as an additional itemised cost.

3.3.2 Accessing a 3rd party API

Nimblex can make requests against RESTful (and other HTTP-based) APIs using built-in configuration tools to push or pull data between two different systems.

This requires knowledge of the other system and will likely require obtaining information, documentation and even software from another Vendor to do. Managing this third party is the obligation of our client and will not be built into the price of your implementation project (As the effort required is impossible to predict).

Please provide:

- Documentation for the 3rd Party API – ideally include information about which endpoints that will need to be used;
- Access details for your non-production environment;
- Contact information for 3rd Party API / application support.

3.3.3 External party accessing Nimblex API

Nimblex has a comprehensive RESTful API that can be accessed by other parties. The standard public cloud API is limited to allow basic experimentation, and in order to use the API in a live system you will need to involve eBMS. As our systems are configured to suit the client, the usage of the API will vary and will generally require input from your implementation team.

For documentation: https://nimblex.help/nimblex-university/developers-portal/

3.3.4 Scheduled import from file

File-based integration is a very basic form of integration. This has the benefit that it is generally very reliable, and very straightforward to set up without having to know about the internals of either system. As a simpler option, it often comes with a lower price tag.

A common scenario is: on an hourly or daily basis we import data from a csv file generated by another system or output our data in a format to be pulled into another system.

You will need to arrange:

- A shared folder accessible to Nimblex;
- The extraction of the required data to this folder, on whatever schedule required;
- Provide to eBMS specific and exact field information for each column in the file, and where you would like this data to be used.

3.3.5 Accessing a 3rd party database directly

The direct route: to and from the database, is often a cost-effective way of accessing data in another system on a real-time basis.

In situations where no API exists or to spare the cost of accessing resources from multiple vendors, we can link straight into the database of other software to provide synchronisation.

We strongly recommend that this be a read-only integration, as modifying data directly in another applications' database can lead to unexpected situations in the application – and result in errors.

Please provide:

- Information about the source database:
    - Host information (IP address/ name)
    - Type of database
    - Credentials
- Access to a non-production database

For further information, please contact:
info@ebms.com.au | 1300 721 159 | 03 9958 0000