

alemba
SERVICE MANAGER



Server Console Guide
Version 1.0



Table of Contents

About this guide	3
Intended Audience	3
Copyright	3
Standards and Conventions	3
Version Details	4
Introduction	5
Accessing the Server Console	6
Creating a new system	7
Creating a new virtual directory	11
Configuring an existing system	13
Configuring general ASM System settings	14
Configuring the database connection	14
Configuring general server settings	16
Configuring diagnostics	18
Enabling a virus check	19
Server Console system tasks	20
System Setup tasks	20
Copying the original files to the ASM System directory	20
Parsing custom query files	20
Running custom PowerShell scripts	20
Configuring system properties	20
Archiving system data	21
Importing and exporting workflows	23
Customizing the server console view	23
Other actions	23
Further Information	24
Product Information and Online Support	24
Technical Support	24
Comments and Feedback	24



About this guide

This document describes how to use the Server Console to create and configure one or more ASM Systems, as well as carry out server console system tasks on each system.

Intended Audience

This guide is written for system administrators responsible for installing Alemba Service Manager™.

Copyright

Copyright © 2019 Alemba Limited. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Alemba® and Alemba Service Manager™ are trademarks of Alemba Ltd. All other marks and names mentioned herein may be trademarks of their respective companies.

You may not copy or disclose this document without prior written consent of Alemba Ltd. Alemba Ltd retains the right to change this document or related product specifications and descriptions, at any time, without notice. Alemba Ltd makes no warranty for the use of this document and assumes no responsibility for any errors that may appear in the document, nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.alemba.com.

Standards and Conventions

The following standards and conventions are used throughout the guide:

	Prerequisites, including security rights and access you may need prior to completing the task. Prerequisites are also highlighted in a shaded box.
	Information related to the current topic that may be of particular interest/significance. Notes are also highlighted in a shaded box.
	Warnings. These are also highlighted in a shaded box.
Field name	Fields are highlighted in bold text.



Version Details

Version No	Date updated	Notes
1.0	17 June 2019	Initial document for the ASM v10.0 release.



Introduction

You can use the ASM Server Console application to create, rename, delete and configure your ASM Systems. You can also use the Server Console to perform a range of tasks, such as archiving calls, and importing/exporting workflow templates.

The following topics will take you through how to access the server console, and create and maintain your system.

- **Accessing the Server Console**
- **Creating a new system**
- **Configuring your systems**
- **Server Console system tasks**



Accessing the Server Console

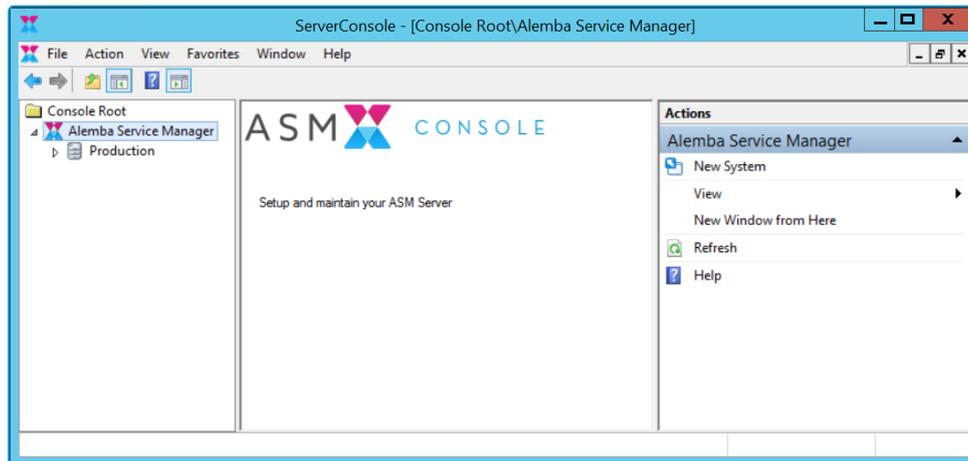
To launch the Server Console:

- From the **Start** menu, select the Server Console.

The Server Console window appears.

The Server Console window has three panes:

- The left pane displays the folder structure within the Console Root folder. From the main Alemba Service Manager™ node you can create a new ASM System. Each system you add is listed below the main node.
- The middle pane displays details of the selected system, or items within the selected node.
- The right pane displays the tasks and actions you can perform, based on the current node or folder.





Creating a new system

You can create and configure a new ASM System using the **New System Wizard**.



Before you start

- Ensure your ASM System environment meets the minimum technical requirements and is configured correctly. For more information, see the **Prerequisites checklist** in the online help.
- Ensure you have correctly installed and configured Alemba Service Manager™. For more information, see **Installing Alemba Service Manager™** in the online help.
- Using a database management tool such as MS SQL Server Management Studio, your database administrator must:
 - Set up a new SQL Server database
 - Make the database user the owner of the dbo database schema, with a sysadmin server-level role
If you cannot use sysadmin, you must use the following database-level roles instead:
 - db_owner
 - db_datawriter
 - db_datareader
- Obtain the database credentials (either the Login ID and password, or Windows Authentication) from your database administrator.

We highly recommend that before you use Windows authentication, you review the implications with Alemba Support.



Alemba® does not support Oracle databases for ASM.



If you are configuring an existing system, see [page 13](#).

To create a new system:

1. Using Server Console, in the left pane, under **Console Root**, right-click **Alemba Service Manager™**, then select **New System** on the shortcut menu.

The New System Wizard appears.

2. Supply the following information:



System Name Type a name for the system. Each system name must begin with an alphabetic letter. By default, the first system name is System1.

 You can use the following in the system name:
alphanumeric characters, spaces, commas, semi-colons and apostrophes. You cannot use double quotes.

System Path Browse to where you want to store the system and its sub-folders. By default, the system directory name is the same as the system name. If required, you can edit it. Use ASCII characters for the system directory name.

 You can specify a path that does not yet exist.

Default Self Service Portal Select the checkbox to set this system as the default on the server. Self Service Portal will access the default system.

3. Select **Next**.

If you specified a System Path that does not yet exist, the Server Console prompts you to confirm that you want to create this system, otherwise continue to configuring the database (step 5).

4. Select **Yes** to proceed with creating the system.

Selecting **No** will cancel this operation.

The **SQL Server DB Details** window appears.

5. Configure the ASM database using the following information:

DB Server Type the name of the SQL server that contains the database.

DB Name Type the database name.

DB Login ID If you are **not** using Windows Authentication, type the database Login ID. The default Login ID is **sa**.

 This is the login for the database, not for Alemba Service Manager™.

DB Password If you are **not** using Windows Authentication, type the database password.



DB NT Auth Select the checkbox to authenticate the database login against the user's network login. Administrators logging into the database must use Windows Authentication details (i.e. the network login and password).

DB SSL Select the checkbox to enable SSL encrypted communication between the ASM System and the database. Ensure that SSL is configured on the selected SQL Server.

 We highly recommend that you discuss enabling SSL with your Account Manager before using this option.

Encrypt in Registry This checkbox is selected by default. It offers additional database security by encrypting the database login ID, password and connection string when these are stored in the registry.

 This option encrypts the database password only, not the password for any Alemba Service Manager™ person record login IDs.

6. Select **Advanced** to set the following advanced options:

Set Concat NULL Yields NULL OFF on every connection Select the checkbox to allow SQL statements to return data. You can configure this option at the session-level or the database-level. Because the default configuration at the database-level is ON, you must select this box to override the database-level configuration where SQL statements are to return data. Clear the checkbox if the Concat NULL Yields is set to OFF at the database-level (for example, to improve performance).

Maximum Connection Pool Size If required, type the size of the client connection pool. The default number of connections is 100, represented by the value 0.

 If this limit is exceeded, errors will occur. Errors are recorded in the event log.

Additional Connection String Properties If required, you can modify the behavior of the Alemba Service Manager™ connection to the database server for more complex SQL Server connections. For example if you have connection pooling, you may need to specify extra information. Type the relevant connection string.

7. Select **OK** to apply the advanced options.

Selecting Cancel will close the dialog box without saving your changes.



8. Select **Test Connect** to test that the information you entered enables you to connect to the server and database.

A message appears to verify if the connection is successful or has failed. If it fails, you can use the detailed error message to diagnose any problems.

If you are using an existing database, the database schema is detailed, but if you are using a blank database, the database schema is not defined.

9. Select **Next**.
10. In the **Enter New Licence Key** field, specify the licence key.

If required, you can load the licence key from a Server Manager License File (*.lic). Select **Load From File** to browse to the file and **Open** it.

11. Select **Decode** to see the licence details.



Licences control the number of analysts that can access the system. Contact your Alemba® Account Manager to increase the number of analysts on your licence.

12. Select **Next**.

If you support customers using multiple languages, you can set up one or more ASM Systems to point at a single Unicode database, and if required, choose a different default language for each ASM System.

Unicode databases can use a greatly extended character set and can display multiple languages on the same window. However, you must properly configure the databases to take advantage of the Unicode features.



Ideally, you should set up the Unicode database when the database is empty. **Do not** select the **Create as a Unicode Schema** without consulting Alemba® Professional Services. Alemba® can upgrade existing non-Unicode databases to support Unicode, but this is a complex process that requires specialist consulting work.

13. If required and after you have received consultation, select the **Create as a Unicode Schema** check box.
14. Select **Next** to create the ASM database using the settings you specified.
This may take several minutes.
15. On the **Website** window, select an existing IIS **Website** from the dropdown list.
The default selection is Default Web Site.
16. Select the **Virtual Directory** that points to the physical location of the ASM System files.



You may need to create a new virtual directory. For more information, see [page 11](#).

 If you do not specify a virtual directory, you can continue to create your system, but you will need to add a website before completing the configuration in order to avoid errors.

 Ensure that your virtual directory is configured correctly, otherwise you will have difficulties running and upgrading your system, and using Chat. This is particularly important if you have multiple systems.

17. If required, change the default Mail Message Access **MMA URL** to a different virtual directory, or a different URL on another server, or to a load balancer.

By default, the MMA URL points to the current server, using the following format:
`http://machinename/Virtual Directory/Core.aspx`.

 If you are using a qualified domain name for the Self Service Portal, specify the qualified domain name in the **MMA URL** field. This way, all the pages on the Self Service Portal will use the qualified domain name, rather than the name of the server/virtual directory.

18. If required, change the **Chat Virtual Directory**.

 When you create a new virtual directory, the **Chat Virtual Directory** field automatically populates with a path that exists within the selected virtual directory. We highly recommend that you use this default setting.

19. Select **Next**.

Currently, English is the only available language. This is automatically selected.

20. Select **Next** to update the database.

After all the files are copied and your system is configured, the process completes.

 You can make changes to the system properties and configure it further, changing general settings such as the default date format and currency, setting up diagnostics and enabling a virus check. For more information, see [page 13](#).

Creating a new virtual directory

Using the Server Console **New System** wizard, when you specify the **Website** properties for your system, you may need to create a new virtual directory.

To create a new virtual directory:

1. On the **Website** page, select **Create**.

The New Virtual Directory dialog box appears.



2. Type a name for the new virtual directory.
3. If you want to use SSL encryption between the client and the server, select the **Use SSL** check box.



The term SSL refers to encryption protocols supported by IIS. This security is configured in IIS. Alemba Service Manager™ will work with any protocol supported by the client and/or server.



If your virtual directory uses SSL, start the address with **https** when logging in.

4. Select **OK** to create the virtual directory.

The MMA URL and Chat Virtual Directory automatically populate.



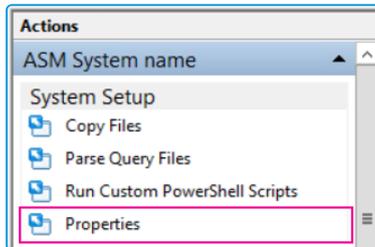
When you create a new virtual directory, Alemba Service Manager™ will also create a new application pool in IIS.



Configuring an existing system

To configure and update an existing system properties:

1. Using Server Console, select the system you want to configure, then select **Properties** in the right-hand **Actions** panel.



Alternatively, right-click the system, then select **Properties** in the shortcut menu.

The System Properties window appears, with a selection of tabs relating to different system settings.

2. Make your changes:
 - For system settings, see [page 14](#).
 - For database settings, see [page 14](#).
 - For general ASM-related server settings, see [page 16](#).
 - For diagnostics settings, see [page 18](#).
 - For virus checker settings, see [page 19](#).
3. Select **OK** to save your changes and exit the System Properties window.
4. Exit Server Console.

A confirmation box appears.

5. Select **Yes** to save your settings and exit Server Console.

The application server cache automatically clears and refreshes. This may cause some slight performance delays.



You must restart the polling and IIS services for changes to the System Properties window to take effect.



Configuring general ASM System settings

1. On the System Properties **General** tab, you can change the following information:

System Name Type a name for the system. Each system name must begin with an alphabetic letter. By default, the first system name is System1.

 You can use the following in the system name:
alphanumeric characters, spaces, commas, semi-colons and apostrophes. You cannot use double quotes.

System Path Browse to where you want to store the system and its sub-folders. By default, the system directory name is the same as the system name. If required, you can edit it. Use ASCII characters for the system directory name.

 You can specify a path that does not yet exist.

Default Self Service Portal Select the checkbox to set this system as the default on the server. Self Service Portal will access the default system.

2. Select **Apply** to save your changes.

Configuring the database connection

1. On the System Properties **Database** tab, you can configure the following database settings:

DB Server Type the name of the SQL server that contains the database.

DB Name Type the database name.

DB Login ID If you are **not** using Windows Authentication, type the database Login ID. The default Login ID is **sa**.

 This is the login for the database, not for Alemba Service Manager™.

DB Password If you are **not** using Windows Authentication, type the database password.

DB NT Auth Select the checkbox to authenticate the database login against the user's network login. Administrators logging into the database must use Windows Authentication details (i.e. the network login and password).



DB SSL Select the checkbox to enable SSL encrypted communication between the ASM System and the database. Ensure that SSL is configured on the selected SQL Server.

 We highly recommend that you discuss enabling SSL with your Account Manager before using this option.

Encrypt in Registry This checkbox is selected by default. It offers additional database security by encrypting the database login ID, password and connection string when these are stored in the registry.

 This option encrypts the database password only, not the password for any Alemba Service Manager™ person record login IDs.

2. Select the **Licence** tab to change your license details.

If required, you can load the licence key from a Server Manager License File (*.lic). Select **Load From File** to browse to the file and **Open** it.

 Licences control the number of analysts that can access the system. Contact your Alemba® Account Manager to increase the number of analysts on your licence.

3. Select **Decode** to view what your license provides.
4. Select the **Website** tab to configure the system virtual directory and MMA settings.

You may need to create a new virtual directory. For more information, see [page 13](#).

 Ensure that your virtual directory is configured correctly, otherwise you will have difficulties running and upgrading your system, and using Chat. This is particularly important if you have multiple systems.

By default, the MMA URL points to the current server, using the following format:
http://machinename/Virtual Directory/Core.aspx.

 If you are using a qualified domain name for the Self Service Portal, specify the qualified domain name in the **MMA URL** field. This way, all the pages on the Self Service Portal will use the qualified domain name, rather than the name of the server/virtual directory.

 When you create a new virtual directory, the **Chat Virtual Directory** field automatically populates with a path that exists within the selected virtual directory. We highly recommend that you use this default setting.

5. Select **Apply** to save your changes.



Configuring general server settings

1. On the System Properties **Settings** tab, you can change the following server settings:

Session Time Out

If required, adjust the idle time limit for an Alemba Service Manager™ client browser session before the connection with the server times out. The default setting is 120 minutes. There is no maximum time limit.

The system timeout applies to both named and concurrent analysts who are logged into the system and idle. Named analysts are included in system timeouts so that lost sessions are not held open, leaving calls in a locked state.

 We do not recommend that you disable the session time out by setting the time to zero. Disabling the session time out may lead to calls that are left open for an extended period of time, and may lead to performance issues.

 If you have configured license corrals, use ASM System Administration to specify a particular session timeout for each license corral.

Self Service Portal Session Time Out

If required, adjust the idle time limit for a Self Service Portal session. The default setting is 120 minutes. There is no maximum time limit.



Server Date Format If required, adjust the default date format used by underlying ASM processes, such as the email polling service. This default does not affect how dates are displayed within the application, where the date format is displayed according to an analyst's browser settings. The default date format is dd/MM/yyyy HH:mm. You can format the date and time as follows:

dd	day
MM	month
yyyy	year
HH	hour
mm	minutes
tt	AM or PM

Currency Symbol If required, adjust the default currency symbol.

Self Service Portal Security Cookie Select the check box to enable a security check that prevents users from accessing another user's browser session. If this check box is selected and a user attempts to access another session by copying the URL for that session to a different browser, the following error message appears: **Invalid Security Cookie**.

2. Select **Apply** to save your changes.



Configuring diagnostics



If you select the check boxes on this tab, the relevant information is stored in the database. If you clear the check boxes, the information is not recorded.

1. On the System Properties **Diagnostics** tab, you can configure the following settings to help you troubleshoot issues that may arise:

- Trace to Debug** Select the check box to enable diagnostics for this system.
- Trace Application** Select the check box to trace all the actions performed by analysts in ASM Core.
If selected, application trace information for this system is sent to DBWin32 (or DBGView).
- Trace Polling** Select the check box to trace all the polling information for this system. If selected, polling trace information for this system is sent to DBWin32 (or DBGView).
- Trace Server Admin** Select the check box to trace all the actions that a system administrator performs on the ASM System using Server Console .
- Query Tracing** Select the check box to capture and save data about each query that is run in the system, including:
- The analyst who ran the query
 - What query it was
 - How long it took to run
 - How many results were returned
 - The SQL statement itself

If selected, the information is logged in the database trace table.

Query Tracing also logs slow running queries as well as logging a warning to the Windows Events log and a row is added to the trace table.

2. If required, select **Extract & Clear** to extract all of the record queries into an XML file and place the file into the System/Diagnostics directory.

Everything is then deleted from the trace table.



Extracting data from the table into XML format can be slow.

3. If required, select **Clear Trace** to delete everything from the trace table.
4. Select **Apply** to save your changes.



Enabling a virus check

Alemba Service Manager™ can interface with a third-party virus checking application in order to scan uploaded files.

If you define a virus checker in the Server Console, the following will occur whenever someone uploads a file in Alemba Service Manager™:

- The file is copied into a temporary location.
- The specified virus checker application runs against the uploaded file.
- Alemba® assumes that if the virus checker finds a virus, it will remove the virus if it is capable of doing so, and will delete any file with an unknown or irremovable virus.
- If ASM finds the file in the temporary location, it will assume the file is clean.
- If ASM cannot find the file in the temporary location, it will assume the file was infected and deleted.

To enable a virus checker:

1. On the System Properties **Virus Check** tab, you can configure the following:

Enabled	Select the check box to turn on virus checking and enable the other fields on this tab.
Application/Script File	Select Browse , then locate and select the virus checking application file. Select Open to insert the path and application into the field.
Command Line Arguments	If required, type any parameters you need to pass to the virus checking application. Check your virus checker documentation for more information on required command line parameters. ASM will run the virus checker in the following order: [Virus checker path] [target file] [command line parameters]

2. Select **Test** to test the virus checking functionality.

The ASM Server Console attempts to create the virus checking directory and run the specified application.

3. Select **Apply** to save your changes.



Server Console system tasks

You can perform a range of tasks using the Server Console. You can access the tasks in the **Actions** pane to the right of the server console window. Tasks are grouped by functional area (that is, System Setup, Database Tasks, and so on).

System Setup tasks

Copying the original files to the ASM System directory

Select **Copy Files** to copy the original files to the System directory.

 This task may overwrite customized files. You should only undertake this task following consultation with Alemba®.

Parsing custom query files

 You must parse the query files after any change to a query file, config-queries.xml, or the database schema, or if you have created a custom query file.

In the Server Console **Actions** pane, select **Parse Query Files** to parse the custom or updated query file.

This process creates a parsed .SQP file in the queries folder for that ASM System. This is a binary file; you cannot use a text editor to read or edit it.

This task:

- Identifies the query files and the order in which they are used by the system.
- Fetches information about the database schema to enforce correct parameter lengths in the queries.
- Writes the queries into a format that is quick to read by the application.

Running custom PowerShell scripts

In the Server Console **Actions** pane, select **Run Custom PowerShell Scripts** to manually run the PowerShell script required to use the Alemba API. When you select this option, the script is automatically selected. Select **Open** to run it.

Configuring system properties

In the Server Console **Actions** pane, select **Properties** to configure your ASM System properties. You can specify a new system name, path, or configure your database connection. For more information, [page 13](#).



Archiving system data

Before you start

We recommend that you archive data outside of database usage peak hours, as it consumes resources, especially if your database is large. If Analysts are taking action on a call during the archive process, an error may occur.

- After calls are archived, you cannot move them back to the standard tables unless you move them manually using SQL commands.

You can reduce the size of your Call Logging and Call History tables by archiving the data. This improves your system performance.

When a call is archived, the following happens:

- All items within the CL_CALL_LOGGING database table, which holds the Call Details, are moved to the table ARCHIVE_CALL_LOGGING.
- All items within the CL_PROBLEM_HISTORY database table, which holds the Call History, are moved to the table ARCHIVE_PROBLEM_HISTORY.
- Any calls, knowledge entries and other entities linked to the archived call are unlinked.
- All other items that are linked to the archived call, such as attachments, are deleted.



You can configure your Analysts' search criteria to include the **Archived Calls** check box and drop-down list. This enables Analysts to search archived calls.

To archive calls:

1. In the Server Console **Actions** pane, select **Archiving > Archive Calls**.
The Archive Wizard window appears.
2. In the **Archive Calls Actioned Until** drop-down, select or type the final date for closed calls you want to archive.



The archiving process uses the **Time Last Actioned** date.

All calls that were closed up to and including this date are archived.

3. If required, select the **Include Experience Base Calls** check box to archive calls that were selected for the Experience Base.



This option is clear by default, since it is assumed that administrators want to keep Experience Base calls separate from the archiving process.

4. Select **Next**.



A confirmation dialog box appears.

5. Select **Yes** to start the archiving process.

This may take a few minutes. After the archiving completes, the wizard confirms its success or failure.



If you receive an error during the archiving process, you should perform the archive again.

6. If required, select **View Log File** to view the log file of the results.
7. Select **Finish** to close the **Archive Calls** window.

If you selected the View Log File check box, the log file opens.



Importing and exporting workflows

You can import and export ASM workflow templates between ASM Systems. This is particularly useful for transferring workflow templates from a test system to a production system, or when best practice templates are provided by Alemba®.

When importing workflow templates, we strongly recommend that the source and target ASM Systems have the same configuration settings. This is especially important when importing partitioned workflow templates. To ensure the templates are ported to the correct partition, the systems must have the same partition settings configured within ASM Core System Administration.

 For more information about Workflow Template Portability, see the **Workflow Template Portability Guide**.

Customizing the server console view

In the Server Console **Actions** pane, select **View > Customise** to change the Server Console display.

On the **Customize View** dialog box, select a check box to display an item, or clear it to hide an item.

Other actions

Using the **Actions** pane, you can also **Delete**, **Rename** and **Refresh** the selected system.



Further Information

Product Information and Online Support

For information about Alemba® products, licensing and services, visit www.alemba.com.

For release notes and software updates, see www.alemba.help.

For product documentation, training materials and videos, see www.alemba.help/help.



You may need to register to access some of these details.

Technical Support

For technical support, visit: www.alemba.com and select the **ASM support** link. You will need to log in to the Alemba® Self Service Portal to contact the Alemba® Service Desk.

Comments and Feedback

If you have any comments or feedback on this documentation, submit it to info@alembagroup.com.