SpeechMiner Administration Guide

Configuring SpeechMiner

5/19/2026

Configuring SpeechMiner

This topic explains how to configure SpeechMiner after it is installed. SMConfig is used to perform the majority of the SpeechMiner configuration. For information about installing SMConfig, see Installing the Components.

SMConfig is a Windows application that can be installed on any machine on your network. Once installed it can be used to configure the entire SpeechMiner system.

The following sections describe the steps that you must perform before you can begin working with SMConfig:

Permissions

Required Permissions

- The user account from which SMConfig is opened must have read, write, and modify permissions on the local installation folder and files.
- For most of the configuration changes you can perform using SMConfig, you will need Administrator privileges on the current machine or on other machines. For each configuration task described below, the required permissions are listed. If you are running SMConfig as a non-administrator user, and errors are generated during the configuration process, make sure that you have the right permissions for the task.
- The web application user used to connect to the database must have db_datareader and db_datawriter roles.
- In Windows Vista and later versions of Windows, if **User Access Control** is enabled, SMConfig will automatically require you to run it with administrator privileges. If **User Access Control** is disabled, it is recommended to manually run SMConfig with administrator privileges. To do this, right-click the **SMConfig** icon, and then select **Run as administrator**.

For more information on the permissions required for the other SpeechMiner components, see Configuring Permissions.

Database Connection

Encrypting the Connection to the Database

The connection between SMConfig and the database can be encrypted to ensure that confidential data cannot be intercepted and viewed by unauthorized people. This option is configured by the system administrator on the SQL database server. Three encryption settings are defined there:

- Always use encryption
- Never use encryption
- Use encryption when the user requests it

If the latter setting is implemented in your system, you can choose to use an encrypted connection when you log into SMConfig. If the database server is configured to always encrypt or not to encrypt at all, you cannot change this option when you log into SMConfig, and selecting one of the options has no affect.

Starting SMConfig

Starting SMConfig

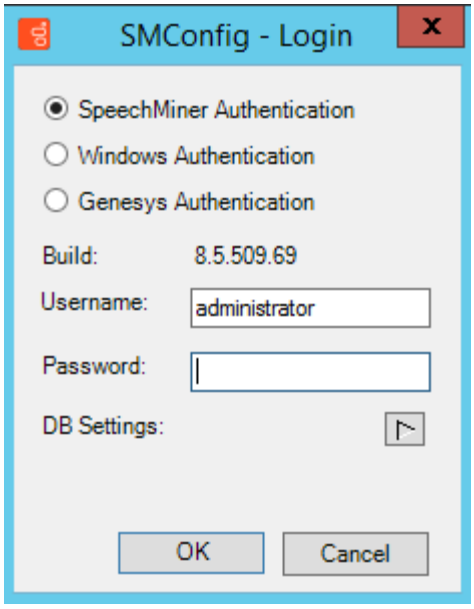
SMConfig can be run on any machine in your system in which it is installed. During installation, an SMConfig icon is placed on the desktop of the machine.

You can log into SMConfig in one of the following ways:

- Using a SpeechMiner user account
- Using the Windows account you used to log onto the PC
- Using a Genesys user account and connecting to a Genesys configuration server for confirmation

To open SMConfig:

1. On the desktop of the computer, double-click the **SMConfig** icon. The **SMConfig - Login** dialog box appears.

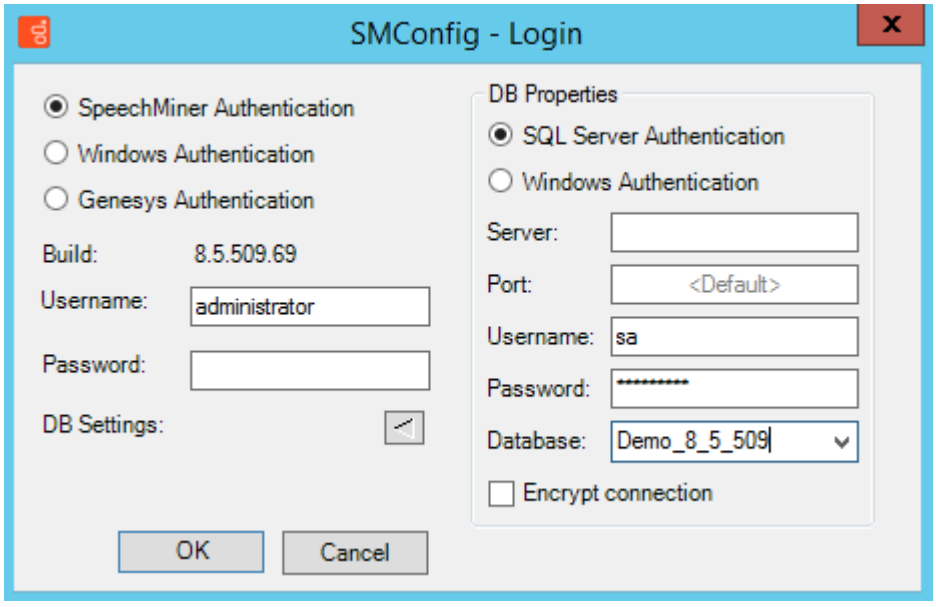


2. Select the type of user account you want to use to log into SpeechMiner:
   - **SpeechMiner Authentication:** Use the username: administrator and the password: Enterprise.
   - **Windows Authentication:** Use the username and password you used to log into Windows.
   - **Genesys Authentication:** Use a Genesys username and password.
3. In the **Username** and **Password** fields, type your username and password.

> **Important**
>
> If you are logging in using Windows Authentication, your username and password are inserted automatically, and the username is in the form `domain\username`.

4. If this is the first time you are opening SMConfig on this computer, or if you want to change the existing database settings, click the **DB Settings** arrow. The **Login** dialog box expands and displays the database settings.

> **Important**
>
> If you do not need to set or modify the database settings, skip this and the next step.



5. Fill in the fields as follows:

Field	Description
SQL Server Authentication / Windows Authentication	Select SQL Server Authentication if the username and password for accessing the database are managed on the SQL server. SelectWindows Authentication if you log into the database using the same username and password you used to log into Windows. **Note:** If you are not sure which option to choose, consult your system administrator.
Server	The name of the database server **Note:** If the database is a named instance on the server, enter both the server name and the instance name, in the format `server_name\instance_name`.
Port	The port to use to connect to the database server

Field	Description
	Note: This should normally be left as `<default>`, even if the database is a named instance.
Username	The username to use to connect to the database **Note:** This field is not available when Windows Authentication is selected. In this case, the username is automatically taken from the username used to log into Windows.
Password	The password to use to connect to the database **Note:** This field is not available when **Windows Authentication** is selected. In this case, the password is automatically taken from the username used to log into Windows.
Database	The name of the database
Encrypt connection	If encrypting the connection to the database is optional in your system, select this option to activate encryption. **Note:** If encryption is always turned on in your system, selecting or clearing this option will have no effect. If encryption is always turned off in your system, selecting this option will prevent SMConfig from connecting to the database server and you will not be able to log in. In this case, an error message stating, `Could not connect to database. Please check database settings`, will appear when you click **OK**.

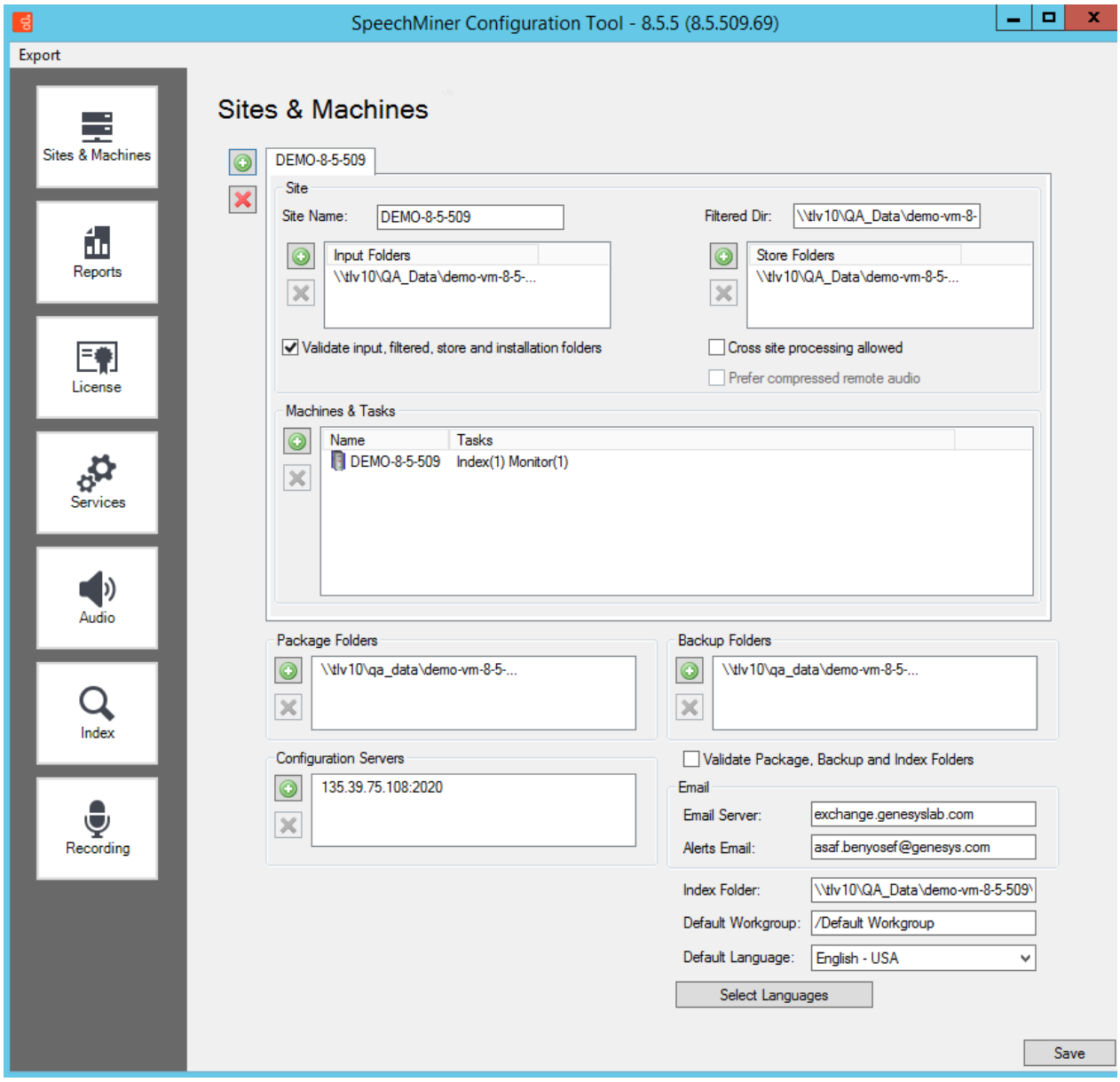
6. Enter the name of the server and the port to use to verify the user information, as follows:
   - Server—Enter the name of the configuration server.

- Port—The port to use to connect to the configuration server in order to verify the user information.

After setting or updating the configuration server host and port in SMConfig (either in the Login window, or in the Sites and Machines panel), the IIS should be restarted.

7. Click **OK**. You are logged into the system, and the **SpeechMiner Configuration Tool** (SMConfig) window opens with the first screen, **Sites and Machines**, displayed.

> **Important**
>
> If a user attempts to log into SMConfig with Genesys Authentication, before defining the Configuration Server in the **Sites and Machines** tab, an error occurs.



The SMConfig interface contains panels (**Sites and Machines**, **Reports**, etc.) in which various categories of configuration settings can be accessed.

To open a panel:

- On the left side of the window, select the icon of the panel. The panel opens on the right side of the window.

Saving Changes

Saving the Changes in SMConfig

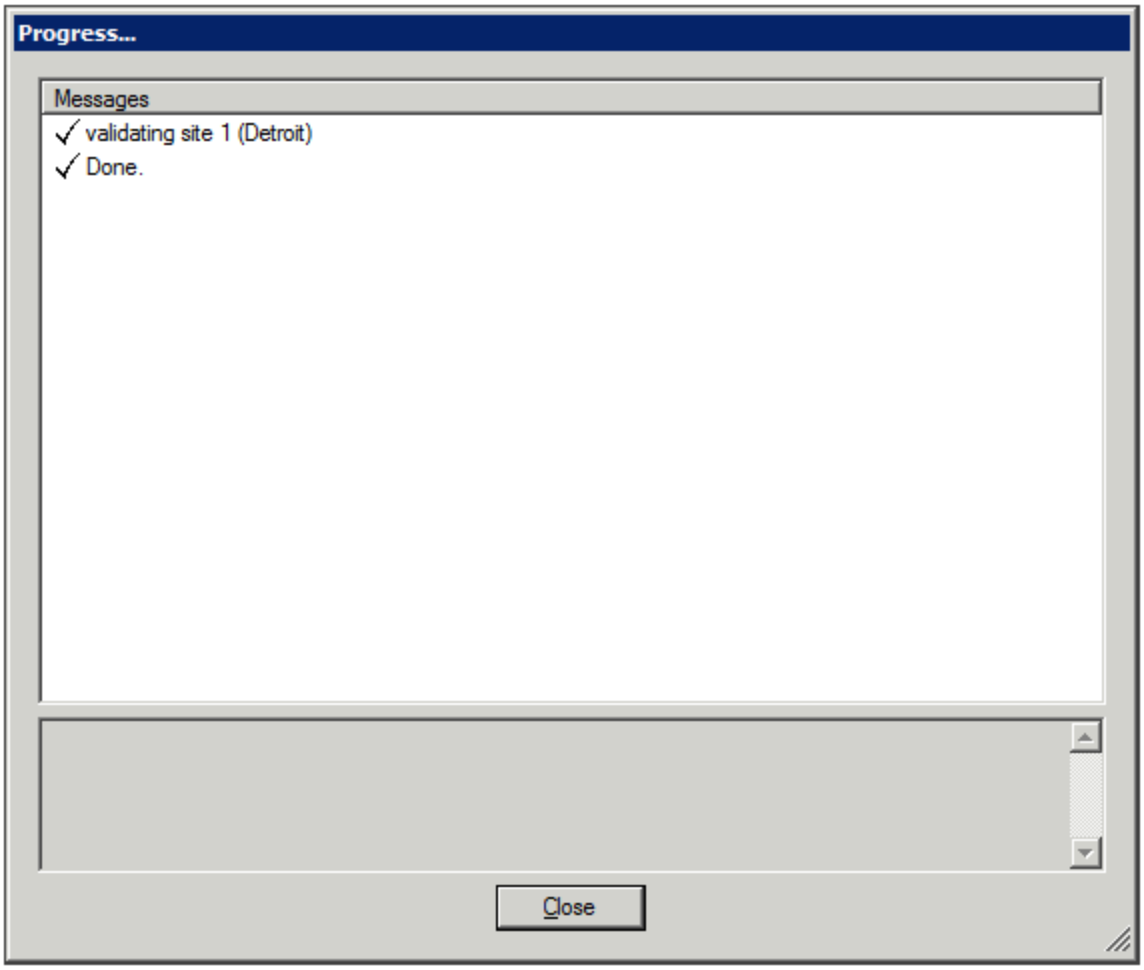
Changes you make in one panel of SMConfig are saved temporarily if you open a different panel. Nonetheless, you must click **Save** in each panel to save the settings in that panel.

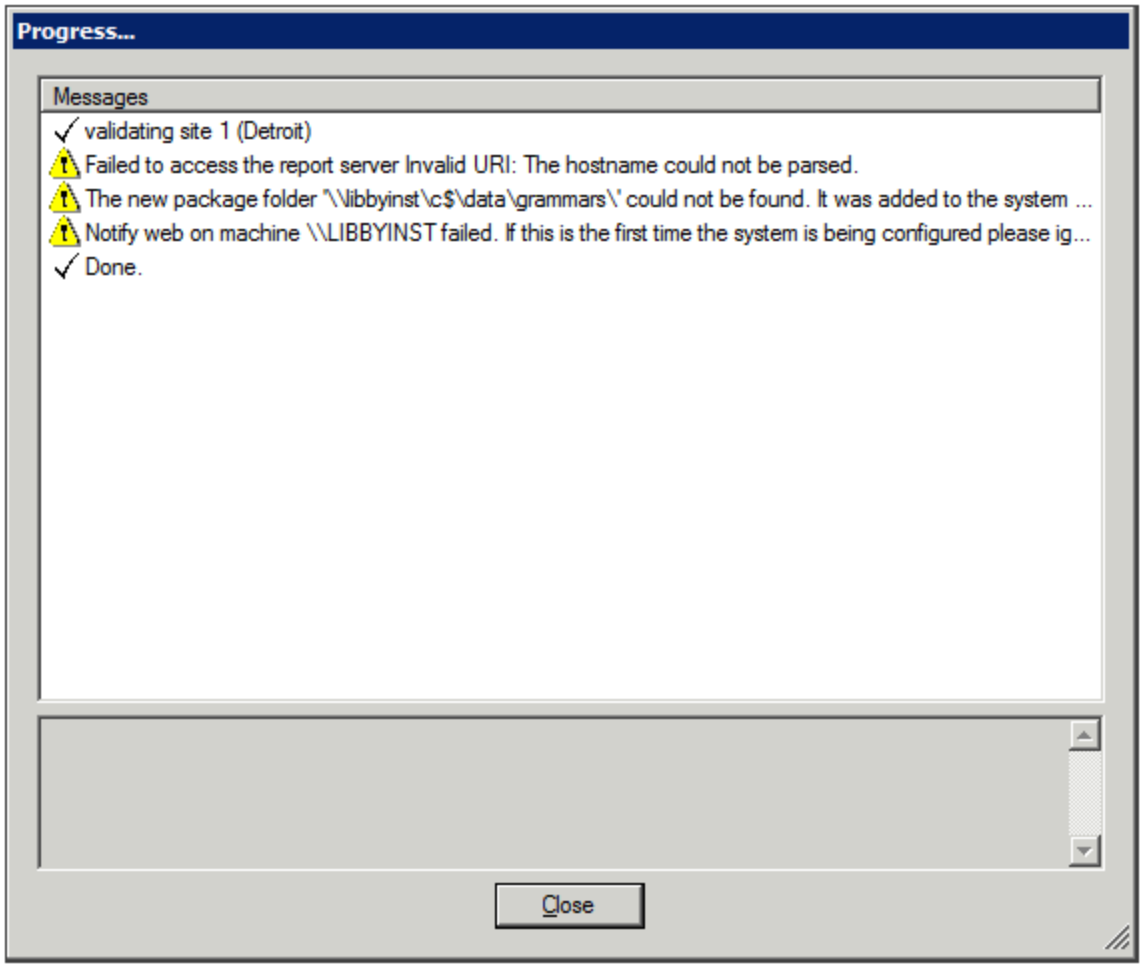
After you click **Save**, before the settings are actually saved, some settings go through a validation process. Validation ensures that the locations specified for folders and files exist and can be accessed, and checks that certain important parameters are configured properly. Certain key settings are always validated when Save is selected; you can choose to have the system validate certain others if you wish.

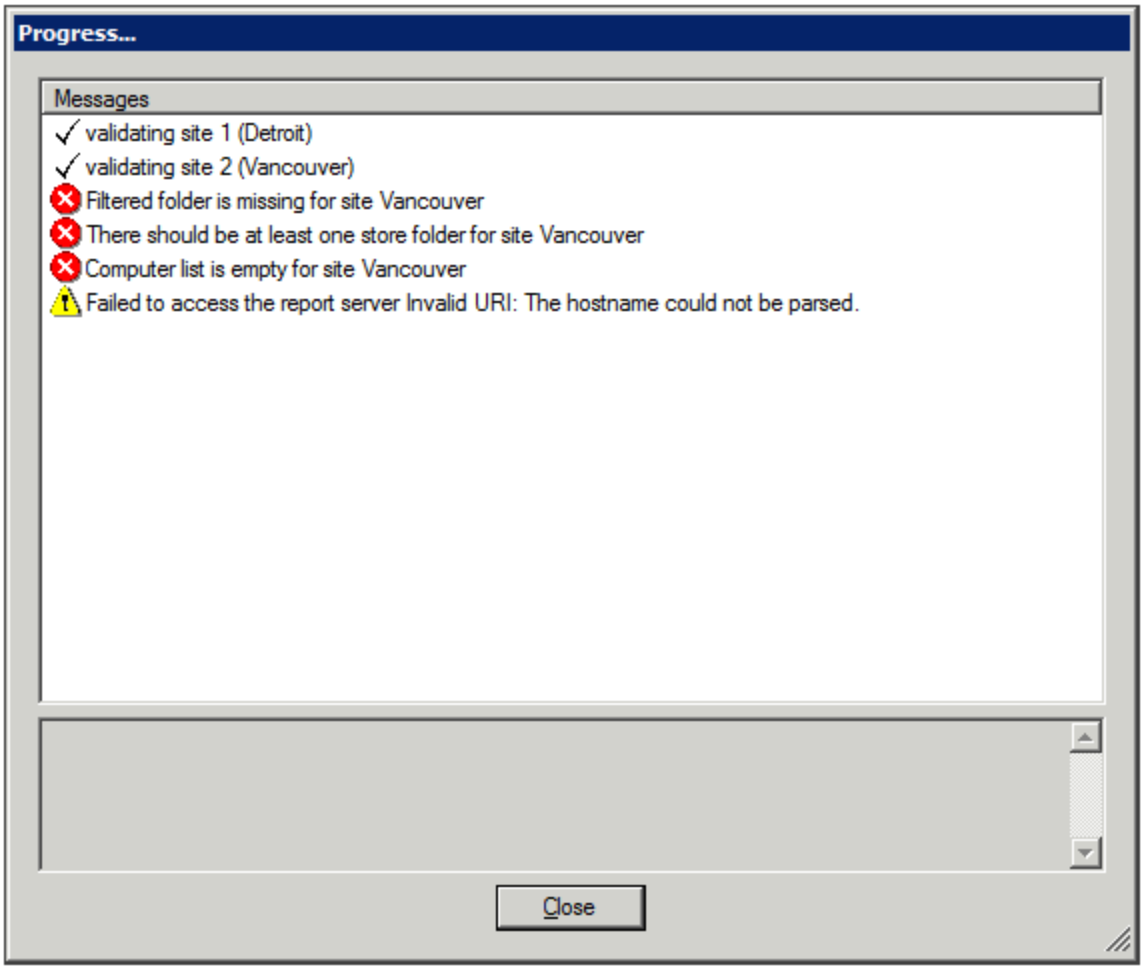
During the validation process, a Progress window is displayed. The window lists the stages of the validation process as they are completed, with an icon indicating the status of each stage.

Icon	Description
	**Success:** Validation of the stage was successful.
	**Warning:** Validation of the stage was successful, but some problematic issues were detected.
	**Failure:** Validation of the stage failed, because of the problems indicated. No changes to the configuration were saved.

When the process is complete, the **Close** button at the bottom of the window becomes active. If validation was successful, the last line of the log says **Done**. If the **Progress** window contains any stages that failed (indicated by ), the entire save process is cancelled. The following screenshots depict examples of each status:

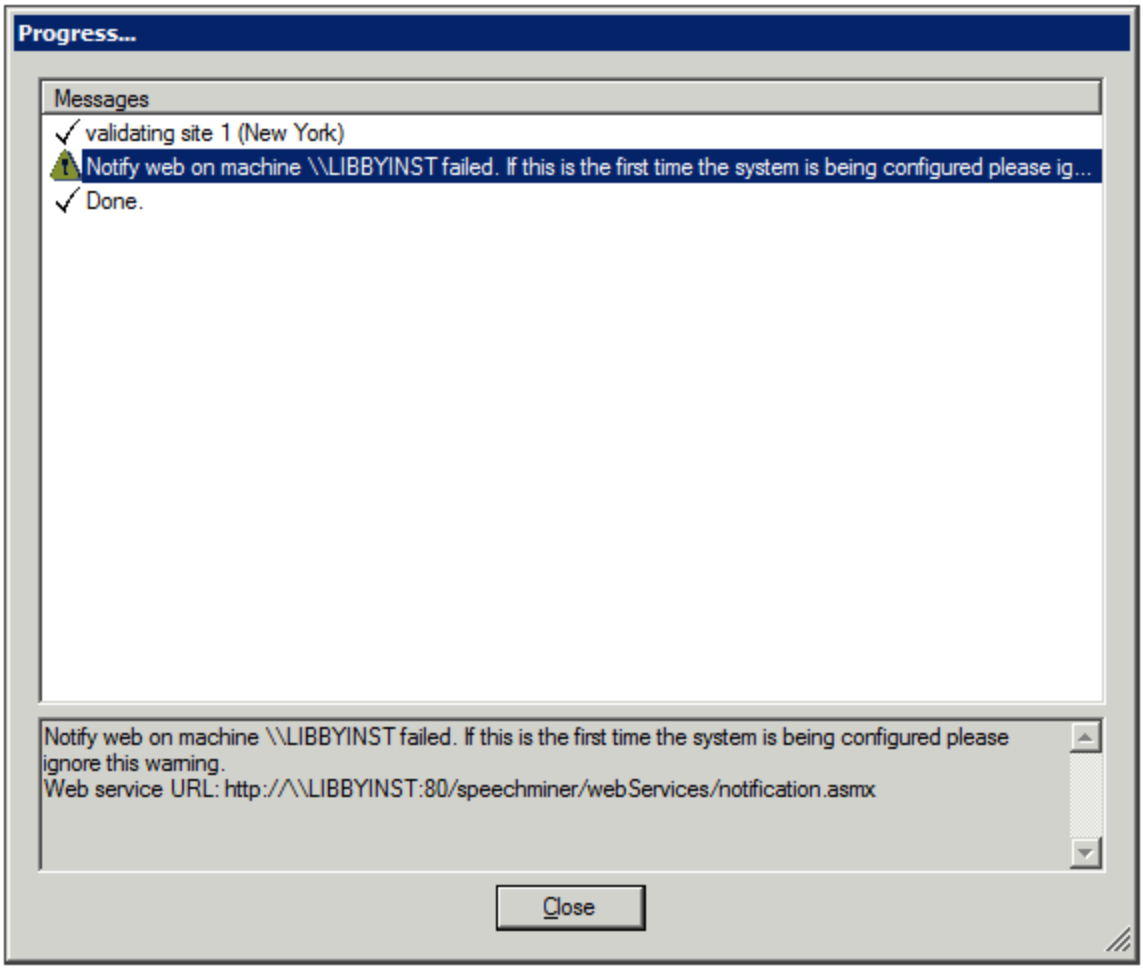

Progress...
Messages
validating site 1 (Detroit)
Done.
Close


Progress...
Messages
validating site 1 (Detroit)
Failed to access the report server Invalid URI: The hostname could not be parsed.
The new package folder '\\libbyinst\c$\data\grammars\' could not be found. It was added to the system ...
Notify web on machine \\LIBBYINST failed. If this is the first time the system is being configured please ig...
Done.
Close

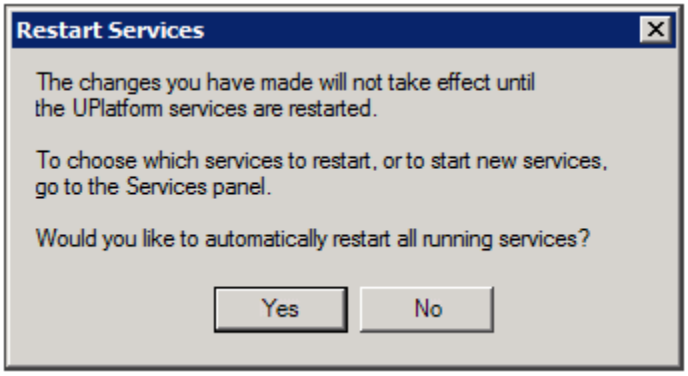


To see details about a warning or failure:

- In the Progress window, select the item. Details are displayed at the bottom of the window.



After the configuration changes are successfully saved, a **Restart Services** message appears.



Select **Yes** to restart all of the services, or **No** if you prefer to restart them later (either after you make additional configuration changes, or manually from the **Services** panel.)

Using SMConfig

This section describes how to use SMConfig to configure the Enterprise.