Install and upgrade FAQ

Find an FAQ for installing and upgrading Relais version 2020.x.

Do we still run an application server with the 2020 version?
Yes, you still need to run an application server with Relais 2020.

How long can we continue to run 2016 and 2019 versions?
Changes incorporated in v2020.1 will mandate that ALL hosted customers migrate to v2020.1.

Customers utilizing RapidILL will need to do so on or before mid-May 2020 in order to avoid service disruptions with the RapidILL service, as the current production Relais Windows applications do not contain support for TLS 1.2. Also, as of mid-May, access to the RapidILL API will require support for TLS 1.2., and v2020.1 will address this issue.

For customers not using RapidILL interoperability, the current host post-to-web environment will not be maintained past August 31, 2020. There are security concerns with the existing hosted post-to-web functionality, so the new Post-to-Web development included within v2020.1 and Portal 3.1 have been completed to address this issue.

Will there be challenges with the hosted site having been upgraded to 2020 but are still using the 2016 or 2019 versions?
Yes.

Customers utilizing RapidILL will need to update their hosted site on or before mid-May 2020 in order to avoid service disruptions with the RapidILL service, as the current production Relais Windows applications do not contain support for TLS 1.2. Also, as of mid-May, access to the RapidILL API will require support for TLS 1.2., and v2020.1 will address this issue.

For customers not using RapidILL interoperability, the current host post-to-web environment will not be maintained past August 31, 2020. There are security concerns with the existing hosted post-to-web functionality, so the new Post-to-Web development included within v2020.1 and Portal 3.1 have been completed to address this issue.
What should I do if I receive indications that the Relais applications cannot find the required ODBC entry, even though administrator credentials have been entered on the staff workstation, and the CreateODBC.exe utility complete successfully?

In this situation Windows has determined that the user running this utility does not have sufficient privileges to allow the CreateODBC.exe utility to complete successfully. This issue only occurs when running the CreateODBC.exe utility on Windows Vista and higher.

The user data sources are stored on the HKEY_CURRENT_USER tree in the Windows registry.

If someone with Administrator rights has entered their credentials into this prompt, the CreateODBC.exe utility completes successfully but the ODBC setting is created under that user's profile and not the user that is currently logged into the staff workstation.

The Relais ODBC entry must appear under the “User DSN” tab in the Windows “ODBC data Source Administrator”.  

Printed: Fri, 24 Sep 2021 22:37:04 GMT
Temporarily add the user's account into the windows local administrators group. This ensures the user in question has sufficient privileges to allow the CreateODBC.exe utility to add the required entries into the HKEY_CURRENT_USER tree under their profile in the windows registry.

Once this is done you can remove the user account from the windows local administrators group.

**How do I configure for an encrypted connection in 2020.x?**

Starting in Relais 2016.x, the build no longer contains the SQL Native Client driver due to security concerns expressed about including potentially outdated versions of the driver. By removing this component from the build, if the default Windows SQL Server driver is used to create the windows ODBC connection, users will not be able to set the "UseEncryption" option equal to "Yes" in the Relais Windows client. To configure your system to allow for encrypted connections the following must be done:

1. **Install** the third party “Microsoft® ODBC Driver 13.1 for SQL Server” driver.
   

2. **Run** the CreateODBC.exe Utility and select the “ODBC Driver 13.1 for SQL Server” from the list of approved drivers:
Note: Any version of the Native SQL server driver will work in this scenario. The root issue is that the default Windows “SQL Server” driver does not support the encryption of the database correction.