REDCap technical guide

Contents

[Azure environment 1](#_Toc89265903)

[Azure resources 1](#_Toc89265904)

[1. Web App 1](#_Toc89265905)

[2. MySQL database server 2](#_Toc89265906)

[3. SMTP server 2](#_Toc89265907)

[PHP configuration 2](#_Toc89265908)

[Gmail account 3](#_Toc89265909)

[Troubleshooting 3](#_Toc89265910)

[REDCap 4](#_Toc89265911)

[Software 4](#_Toc89265912)

[Configuration 4](#_Toc89265913)

[Authentication 4](#_Toc89265914)

[Admin account 4](#_Toc89265915)

[Hooks (custom functionality) 4](#_Toc89265916)

[Overview 4](#_Toc89265917)

[Configuration 5](#_Toc89265918)

[SEIFA, region, and ARIA assignment 5](#_Toc89265919)

[Updating REDCap 5](#_Toc89265920)

[Easy upgrade 5](#_Toc89265921)

[Incorrect table structure 5](#_Toc89265922)

[Fixing upgrade failures 5](#_Toc89265923)

# Azure environment

# Azure resources

## Web App

## MySQL database server

## SMTP relay

REDCap requires an email server to function properly. Specifically, for our purposes, it needs to send emails in order for user accounts to be validated, and for passwords to be reset periodically.

An email server was not configured when REDCap was first installed. Russell did not know how to configure an SMTP server. All of the instructions and advice I found on the REDCap Community forum and elsewhere referenced the use of SendGrid. SendGrid is an SMTP (email server) which can be installed and configured in an Azure resource group. Unfortunately, it turned out that due to the nature of the Azure subscription (apparently because SendGrid is a SaaS resource), we would have needed assistance – and probably the assignment of administrator privileges – by the Department of the Premier and Cabinet. This was an unattractive prospect, so I decided to make a further attempt at configuring the SMTP settings in PHP while utilising a different SMTP server. After many hours of trawling StackOverflow, testing, and troubleshooting, I got it working. Below is a summary of the configuration details in the form of instructions (should they have to be repeated in the future).

### PHP configuration

REDCap uses PHP to send emails. Here we have to configure PHP to use our desired SMTP settings, so PHP can successfully send emails when requested.

1. First, install Sendmail on the web server. Sendmail is an application that allows you to [send emails from a Windows machine](https://php.tutorials24x7.com/blog/how-to-use-sendmail-on-windows-to-send-email-using-php) without installing an email server.

Download Sendmail from [this Github repository](https://github.com/sendmail-tls1-2/main), unzip it and load the contents into C:\home\site\repository\sendmail on the Web App using Kudu.

1. Now we configure Sendmail with our SMTP settings. In Kudu, open the sendmail.ini file that you just uploaded and modify it with the following values:

smtp\_server=smtp.gmail.com

smtp\_port=465

auth\_username=cdsircredcap@gmail.com

auth\_password=Cdsirc01!

These are the settings for the Gmail account that was created for this purpose (details below). This allows us to use Gmail’s email server instead of using SendGrid or installing and configuring our own email server (no thanks!).

1. Next, we need to configure PHP to use Sendmail to send emails. Everything else is handled by Sendmail with the settings above. Azure does not allow you to modify source code in most directories (including Program Files), so instead of modifying the php.ini file directly, we have to tell PHP to look for additional configuration settings.

To do so, add a PHP\_INI\_SCAN\_DIR app setting to the Web App by running the [following command](https://docs.microsoft.com/en-in/azure/app-service/configure-language-php?pivots=platform-windows) in the Cloud Shell (Bash):

az webapp config appsettings set --name DfE-REDCap --resource-group CDSIRC-REDcap-RG01 --settings PHP\_INI\_SCAN\_DIR="C:\home\site\ini"

You can confirm that this was successful in Azure Portal. Navigate to the App Service (DfE-REDCap), then to the ‘Configuration’ page under Settings. You should see the above application setting (PHP\_INI\_SCAN\_DIR) listed.

1. Now, using Kudu, navigate to C:\home\site and create the ini folder we referenced above. Inside C:\home\site\ini, create a file called settings.ini and include in it the following line:

sendmail\_path = C:/home/site/repository/sendmail/sendmail.exe

Thanks to the app setting we created in the previous step, PHP will scan this folder and include this setting when it runs. PHP will then invoke sendmail.exe, which includes our SMTP settings, when the mail function is called by REDCap. Great success!

### Gmail account

A Gmail account was created for the purpose of sending emails from REDCap.

The email address is: cdsircredcap@gmail.com

The password is: Cdsirc01!

The recovery email address is: educationcdsirc@sa.gov.au

Note that to send emails from REDCap (e.g., when creating user accounts), the associated email account (cdsircredcap@gmail.com) needs to allow external app connections. The account will automatically disable this feature after some period of disuse. To re-enable this:

1. Login to the account
2. Navigate to ‘Manage your Google Account’ under the gear icon
3. Go to the Security tab
4. Enable ‘Less secure app access’

REDCap should now be able to send emails again.

### Troubleshooting

Some issues can be troubleshooted using PHP itself. To run PHP commands in the Kudu Console, create a PHP file containing your PHP code and run php <filename> in the console.

To check the PHP SMTP settings you can run the phpinfo() command. phpinfo(INFO\_GENERAL) will output basic configuration info, including where (or whether) PHP is searching for additional configuration settings.

You may also want to send a test email. This can be performed by running the following code in a PHP file:

<?php

$from = "cdsircredcap@gmail.com";

$to = "<recipient\_email>";

$subject = "Hello Sendmail";

$message = "This is an test email to test Sendmail. Please do not block my account.";

$headers = [ "From: $from" ];

mail( $to, $subject, $message, implode( '\r\n', $headers ) );

Just replace <recipient\_email> with your own email address.

If the configuration settings above were applied correctly, this email should be sent successfully.

If it is not sent, check the crash.txt file in the directory in which you ran the above code, or check the error.log file in C:\home\site\repository\sendmail for error messages.

# REDCap

## Software

## Configuration

## Authentication

Table-based authentication is in use. User accounts can be added using the admin account. Note that the Gmail account’s setting may need to be altered for this to work. See the Gmail account section on the previous page.

### Admin account

The administrator account (CDSIRC-Admin) has elevated privileges and essentially has complete control over the system. For example, it can be used to suspend other user accounts and delete records. This account must be used with caution and should only be used for administration and configuration purposes.

See the Password Log in Objective for login details.

## Hooks (custom functionality)

### Overview

As per the [REDCap Developer Tools documentation](https://dfe-redcap.azurewebsites.net/redcap/redcap_v11.4.0/Plugins/index.php), a hook is a PHP function that is executed in a predetermined location inside REDCap. This location is determined by the specific hook function used; for example, a redcap\_data\_entry\_form hook will be executed when an instrument is accessed.

Other functions – including user-defined functions – can be placed inside a hook in order to modify either the data in or appearance of that form. Functions can be written in PHP, which will be executed by the web server, or in JavaScript, which will be executed by the browser. HTML and CSS can also be implemented.

Because hooks are executed by REDCap itself (on the web server), they can utilise REDCap’s resources, including the database connection to the mySQL backend, and all available PHP constants and functions used by REDCap.

### Configuration

The REDCap Hooks setting points REDCap to the appropriate location to find the hooks file, currently C:\home\site\wwwroot\redcap\hooks\hook\_functions.php. This setting can be found in REDCap under Control Panel -> General Configuration.

Add or modify hook functions in this file to add functionality to REDCap. The file can be modified using Kudu.

### SEIFA, region, and ARIA assignment

The SEIFA, ARIA (Remoteness Area), and SA Government Region fields are automatically updated with the appropriate value based on the record’s year of death and postcode. The information for these fields is stored in nested dictionaries (JavaScript objects). The values are assigned by passing the (census) year and postcode as keys to the appropriate dictionary; the values are returned and passed to the REDCap fields.

The script is executed inside **function** redcap\_data\_entry\_form($project\_id, $record, $instrument, $event\_id, $group\_id, $repeat\_instance){} each time the case\_information instrument is modified (the script is executed inside an if statement).

Note the syntax for accessing or modifying REDCap field values using JavaScript is $('input[name=”<fieldname> “]').val(), passing the field’s name to the name parameter and, if setting the value, passing that value to the val() method.

## Updating REDCap

### Easy upgrade

The Easy Upgrade feature automatically checks for REDCap updates. The update process will not be triggered automatically; a button will appear in the Control Center when an upgrade is available. Clicking this will cause the new version to download to the web server (at C:\home\site\wwwroot\redcap\redcap\_vXX.X.X).

Once downloaded, REDCap will provide an update button which should perform the update automatically. However, it is common for an error to arise following the update, whereby the database table structure is not consistent with REDCap’s expectations. There is an option to automatically apply a fix, but this has not worked I the past.

Instead, copy the SQL script provided by REDCap and run it directly on the database (e.g. using MySQL Workbench). This will fix the table structure and should complete the successful upgrade to the new version of REDCap.

### Restoring to a backup

Both the web server and the database server are configured to automatically perform a backup daily, with a 30-day retention period.

It is important to note that when restoring to a backup, the web server (i.e. REDCap) and the database must be restored independently. The Azure web app (App Service) does have a Backup Database feature, but this cannot be used since the app is configured to disallow public access; the app and database are accessed via the private endpoints. Thus, the Backup Database does not work because it attempts to connect to the database via a public network connection.

If REDCap needs to be restored to a recent backup and the database can remain in its current state, i.e. no changes to the REDCap configuration data or to the table structure have been made since the last web app restore point, then the web app may be able to be restored independently.

However, if the web app reversion requires the database to be restored as well, this will need to be performed separately. Restoration of the database involves generating a new database server; thus, new private endpoints will also need to be generated, and REDCap will need to be pointed to the new database by modifying the database file (C:\home\site\wwwroot\redcap\database.php). Education ICT may need to be involved in the generation of the new endpoints.

### Failed REDCap version upgrade

If a version upgrade fails or otherwise breaks REDCap, a restoration to web app backup may be required. However, note that if the upgrade was executed then the REDCap version was likely changed in the database. If this is the case, REDCap will not function after being restored.

REDCap checks the database for which version to run. If, for example, you have just upgraded from v11.4.0 to v12.0.2, encountered an issue, and then restored the web app the most recent backup, REDCap will attempt unsuccessfully to run a non-existent version 12.0.2. I learned this the hard way.

However, if the table structure hasn’t changed, then the easiest way to remedy this (that doesn’t require restoring the database server as described above) is to modify the REDCap version number in the database by executing the following SQL: UPDATE redcap\_config SET value = 'XX.X.X' WHERE field\_name = 'redcap\_version', replacing XX.X.X with the appropriate version number.

# MySQL

## MySQL Workbench

### Connection issues

The MySQL server does not use SSL. Connection errors will arise if the MySQL client enforces SSL, as is the case in MySQL Workbench 8.0.27. The software was downgraded to version 8.0.26, fixing the issue. An appropriate version of Workbench will have the ‘No’ and ‘If available’ options available in the SSL options menu.

To set or check this, go to the settings for the connection, select the SSL tab, and see the options under the ‘Use SSL’ dropdown.

Remember that you can also connect to the MySQL database using another client, including simply using R or Python.