IT user access form - quick guide

Version:	0.1
Issued:	20th February 2019
Author:	Jon Rolph

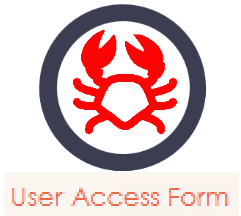
Document Control

Date	*Ver*	*Change Description*	*Author*
20/02/2019	0.1	Initial document created	Jon Rolph

Contents

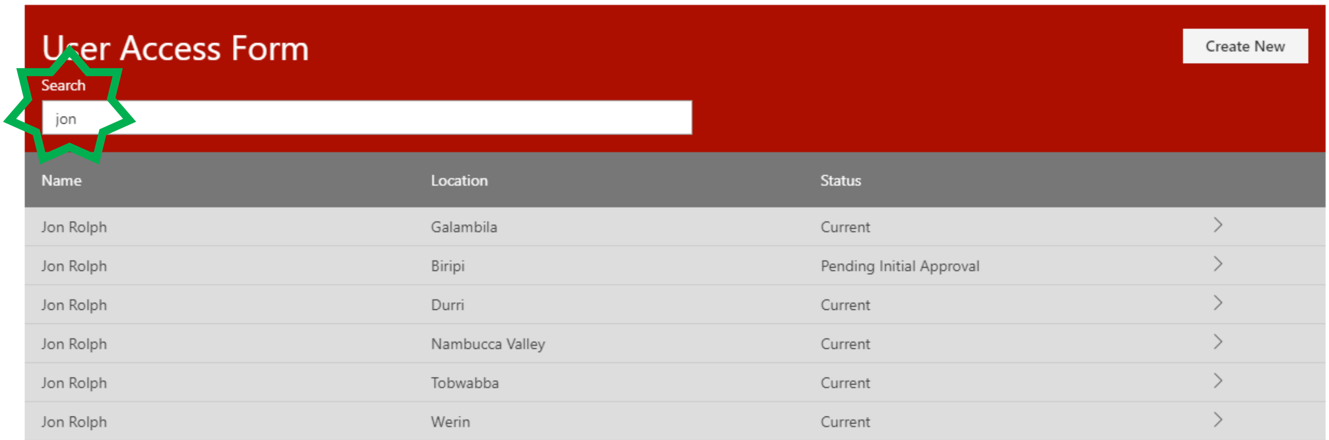
Step 1: Open the system

Select the “User Access Form” from the main page of your intranet site. The icon used to identify the form is below.



Step 2: Find the record

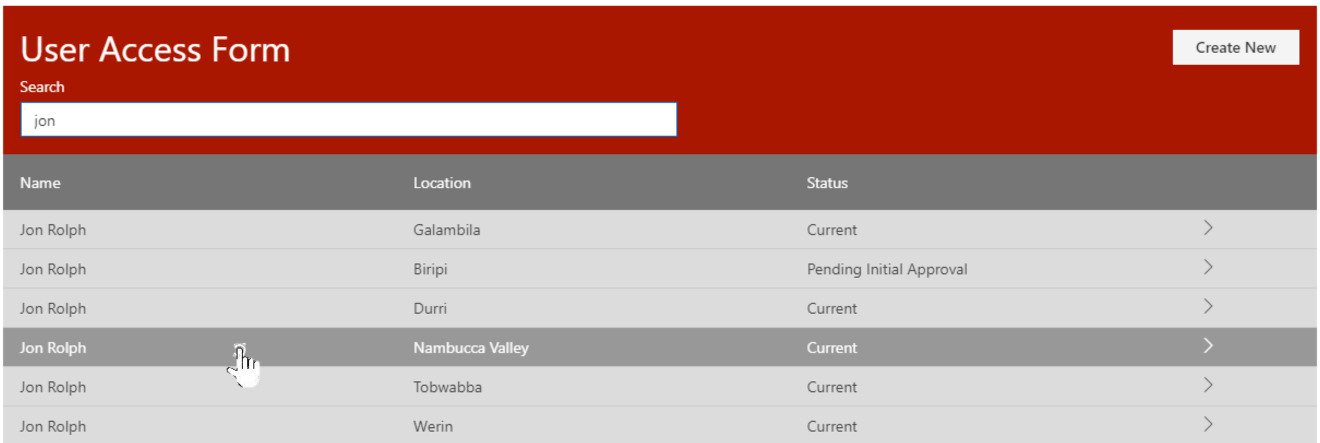
If you cannot see the person you are looking for in the screen, at the top of the page start typing the name in the Search field (you can use their first or last name).



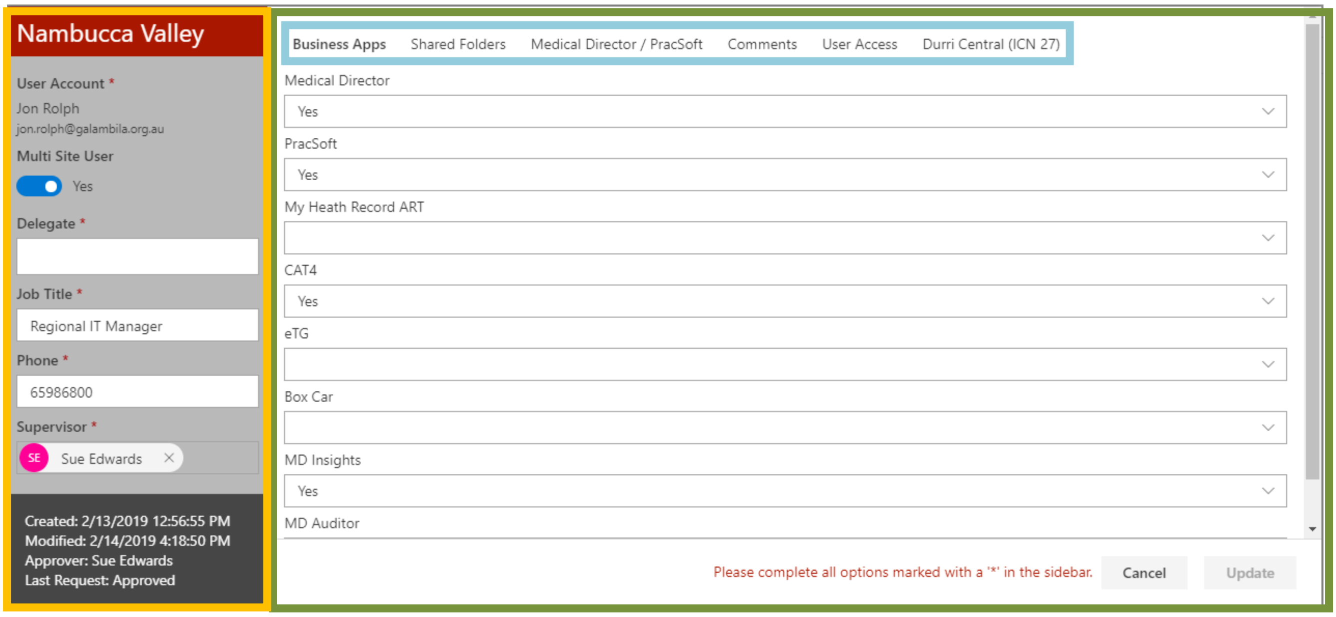
You will see an entry for each location if a user has access to more than one.

Step 3: Select the Record

Click on the record you want to open.



Step 4: Review/Update details



Yellow - The sidebar containing the personal details of the user
Green - The main window contains a number of tabs (in blue) that represent different aspects of the user's access.

Step 4a: Review / amend personal details

Within the personal details the information that can be updated is:

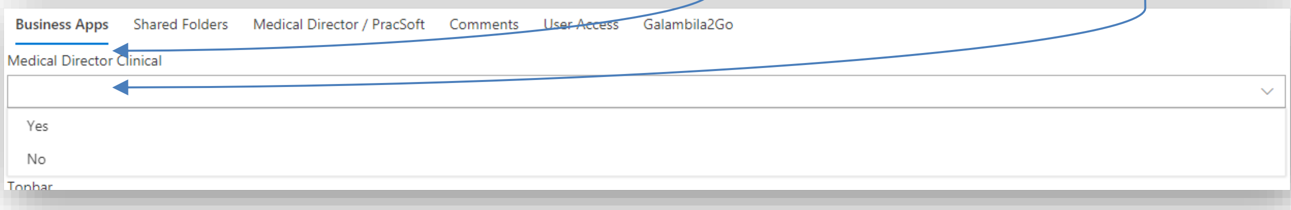
1. The Supervisor of the employee
2. The employees phone number & Job Title
3. The Delegate to approve any changes to the details. This is initially blank but must be chosen before updates can be processed.
4. Multi Site user indicator which is set if a user will work at multiple sites (e.g. a visiting specialist) and use the same logon name and password for all.

In addition to this the employees name and email address are shown at the top of the section and the dates when the account was created and last modified, along with the name of the Delegate who approved the change, is shown at the bottom on the section.

Step 4b: Review / amend remaining details for the user

Whilst the exact details to be entered are different for each organisation, reflecting the different applications used by each, the method of doing this is common to all.

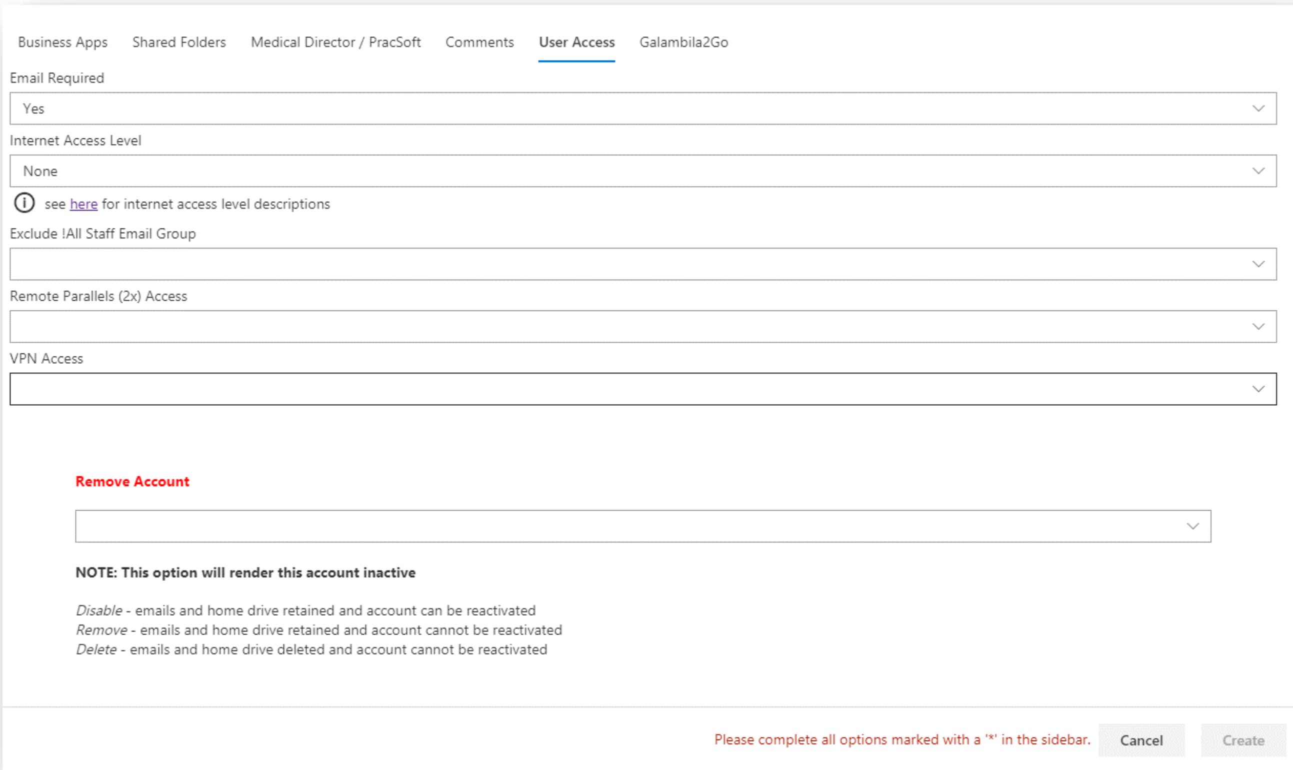
For each option that you want to update, click on the rectangle below the name and select “Yes” to add access or “No” to remove it.



Don’t forget that sometimes a change in role means that some existing access is no longer needed and should be removed.

Step 4c: Complete the User Access tab

The “User Access” tab requires some explanation and is common to all organisations. I will therefore provide more detail on filling in this element of the form:



Each entry is outlined below:

- Email Required: For some account (e.g. visiting specialists) there is no benefit in having an email account.
- Internet Access Level: Ensuring that staff have only the level of internet access they need for their role, and no more, is a way of minimising the risk of malware infection through compromised

web sites. There are six levels of access (other than no access) supported. Pick the most appropriate one from the list:

None: No internet access is provided

Base: Access to the most common types of web site and suitable for most users

Shop: As Base PLUS shopping web sites

Social: As Shop PLUS social media web sites

Stream: As Social PLUS streaming media web sites

Email: As Stream PLUS web based email (often used for Registrars or visiting specialists)
Note: Access to work email via the Office 365 web site does not require this

Skype: As Email PLUS web based video conferencing

The following link will take you to a detailed list of the types of site available to each level: http://itrams.org.au/resources/FortiClient%20Groups%20%40%2008.07.2016.pdf

- Exclude !All Staff Email Group: Each organisation has a public group that will send emails to all staff. Some account, such as visiting specialists, Board members, etc. would generally be excluded from this group so they do not receive such emails.
- Remote Parallels (2x) Access: Parallels, formally called 2x, is the system through which most shared applications are accessed. To protect our confidential information access to such systems is prohibited from anywhere physically outside the organisations without special permission. Selecting this option will give such permission.
  Note: This option required the use of a 2 factor authentication, which will be provided by the IT Helpdesk.
- VPN Access: The VPN (Virtual Private Network) client is a way of securely connecting to some IT services when working remotely, via an IT@RAMS provided computer. The services that will be accessible via a VPN connection are; Network drives, Printers and Parallels delivered applications (e.g. Medical Director, Communicare, Best Practice, etc.).
- Remove Account: When a user leaves the organisation it is highly recommended that something is done as soon as possible regarding their access. A decision needs to be made about what to do with their accounts and data. Three options are available:
  1. Disable: Emails and home drive are retained and the account is temporarily made inaccessible but can be reactivated if needed.
  2. Remove: Emails and home drive are retained but the account is deleted and cannot be reactivated.
  3. Delete: Emails, home drive and account are all deleted and cannot be recovered.

Step 4: Submit the request for approval

Once the form is complete reviewing the account details select "Update" from any tab to submit any changes for approval by the Delegate. If you do not want to save the changes, or you have not made any, select "Cancel"