

August 2019

NOTICE TO EMPLOYERS & PENSION PROVIDERS

Renewing your Revenue Online Service (ROS) digital certificate

ROS uses digital certificates for customer authentication purposes. They provide a high level of security.

One of the security features is that ROS digital certificates currently have a maximum lifespan of 2 years and have in-built expiry dates from the date of issue; which means that they must be renewed at least every two years. The renewal reminder process includes the following:

- the option to renew a certificate appears 3 months before the certificate is due to expire, and
- reminder emails are sent to the ROS administrator before a certificate lapses. You should ensure that your ROS contact email address is up to date so that you receive these emails.

Some 130k digital certificates are due to be renewed over the next 6 months, with the majority of them required to be renewed in September, October and November. It is important to renew your ROS digital certificate when you are prompted to do so, in order to ensure continued secure access to ROS and so that you can meet your filing, paying and reporting obligations.

What happens if a ROS certificate is not renewed on time

- The certificate expires and all access to ROS is lost.
- If the expired certificate is the main ROS Administrator certificate, any sub-users will also be unable to log on to ROS.
- If the expired certificate or one of the sub-user certificates is being used in a payroll package to communicate directly with ROS, this access or communication will be unavailable.

How to renew your ROS digital certificate

To renew your certificate, please follow these steps:

- Login to ROS - the certificate renewal screen will appear.
- Enter your 'Old Password' (this is the one you have been using to log into ROS up to now).

- Create a 'New Password' - this will be your new login password. Your new password may not contain your certificate name. Note your new password.
- Retype your new password at 'Confirm Password'.
- Click 'Renew Now'.
- Follow the on-screen prompts to **save** your renewed certificate.

A new digital certificate will be created in your web browser. Your certificate will have the same name as the old certificate, but it will have the new password that you have just entered.

Why it is important to 'save' your digital certificate

When the digital certificate is renewed, it is important to securely save it. Older copies of the certificate made before renewal are no longer valid for ROS.

If the renewed certificate is used in a payroll package, the payroll package will need access to the newly saved certificate.

A digital certificate is a computer file. If you do not save your certificate in a permanent folder or file path that you can locate again, it is possible that the certificate will be stored only in temporary storage. Some computer operating systems or browsers automatically clear temporary storage after a period of time, and your certificate could be deleted from that temporary storage.

Certificates in direct reporting payroll software packages

If your certificate is used by a direct reporting payroll package, the payroll package may need to be updated to use the renewed certificate. Users should ensure that they follow the payroll package instructions to select or apply the newly saved, renewed certificate. After renewing and saving the certificate, employers should test that the payroll package can communicate with ROS successfully.

Further information on ROS digital certificates can be found on the Revenue website in Online services support / ROS Help.

Maura Conneely
Personal Division
Revenue Commissioners