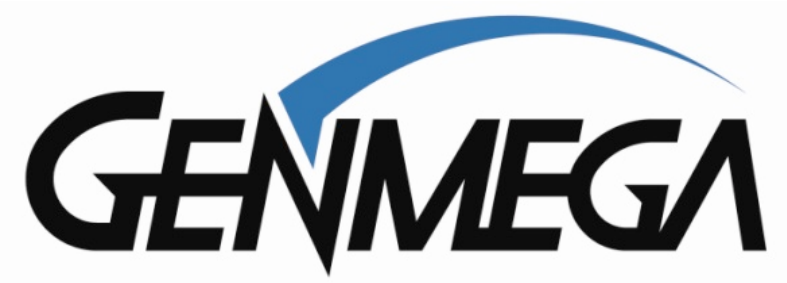


GenRMS Professional V2.7.1

Security Updates

2024

GenRMS Pro V2.7.1 Security Update

In order to increase security within GenRMS Pro and to prevent unauthorized remote access – this release (V2.7.1) contains the following new features.

1. **Default Password**

The RMS Client password can no longer be left at 'default'. If the RMS Server application detects the default password – it will require you to change the password before the Client application will run.

2. **'2FA' Two-Factor Authentication**

This option will require any new login to obtain a code generated by RMS. This is sent you via the email address used for RMS notifications.

3. **Auto-Block**

This function will automatically block any remote IP address that fails login to RMS after X number of attempts. Any remote connection is logged and can be unblocked from the GenRMS Server application.

4. **Local Access Only**

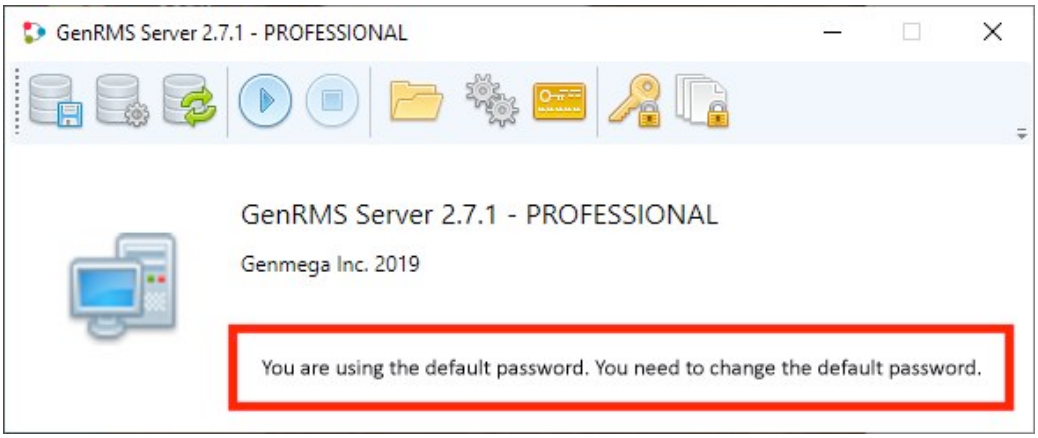
If you are only using RMS from the RMS Server PC, enabling this function will block any outside connection with the RMS Client.

5. **Alert for ATMs with the default RMS Password**

ATMs within your RMS application – which have the default RMS password can be color coded for easy identification.

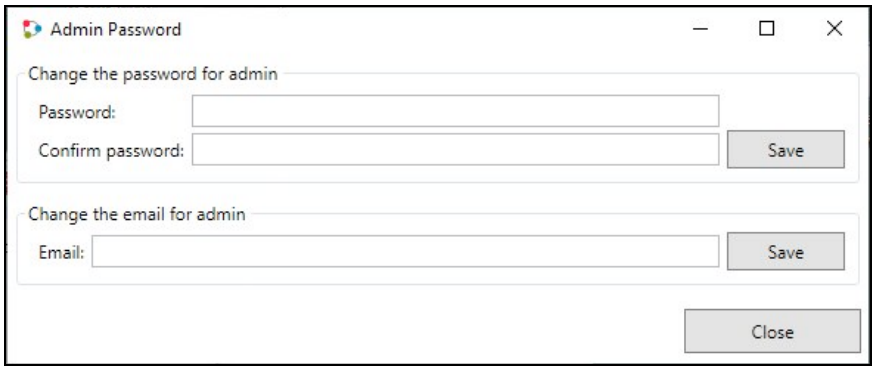
Default Password

When you run the GenRMS Server application, it checks that the password has not been left at default.



If you see the warning message above, then you must change you RMS Password before the service will start.

Click the 'Key' icon on the right to access the password tools.



Enter your new RMS Password (this is the password entered when you run the RMS Client application) and then confirm.

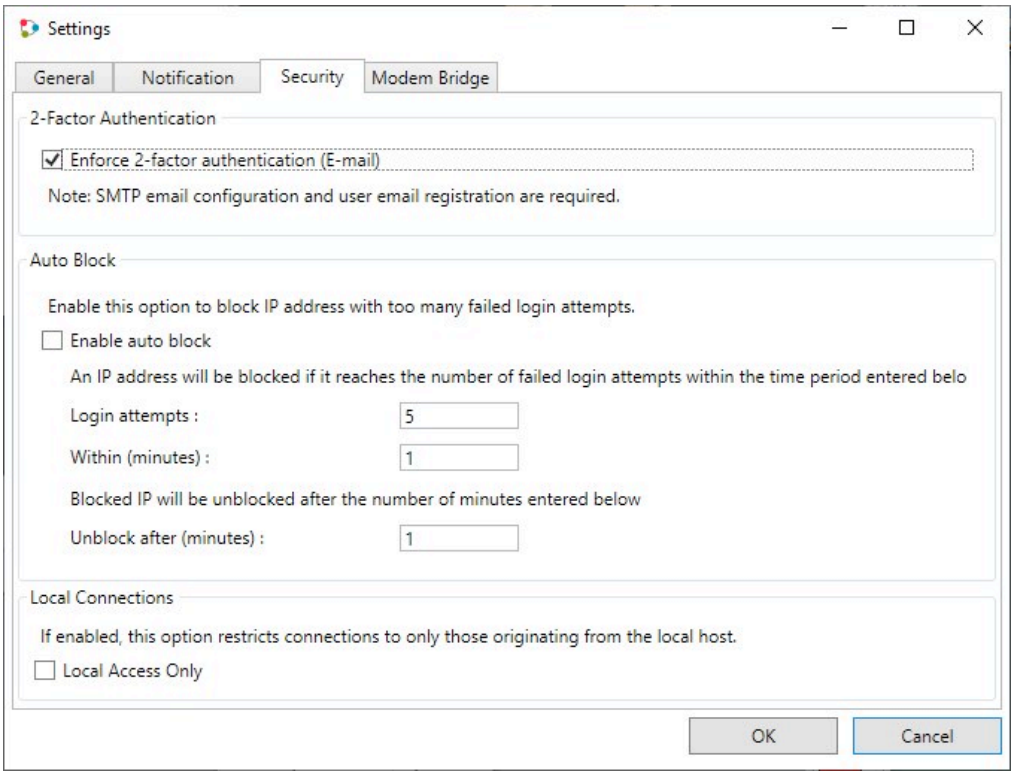
Note if you forget your RMS Client Password – you can reset it from this screen.

The 'Change email for admin' field is where 2FA (two-factor authentication) emails are sent to obtain a login code. If you don't have an email account setup within RMS for notifications, then this function will not work.

‘2FA’ Two Factor Authentication

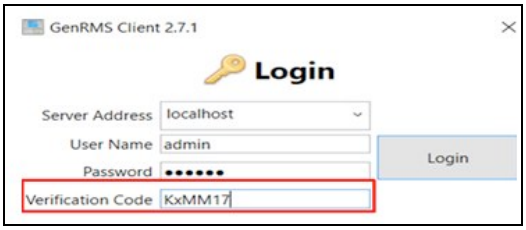
Click on the ‘Gears’ icon to enter the RMS Setting Menu

With the Settings window, click on the Security tab.

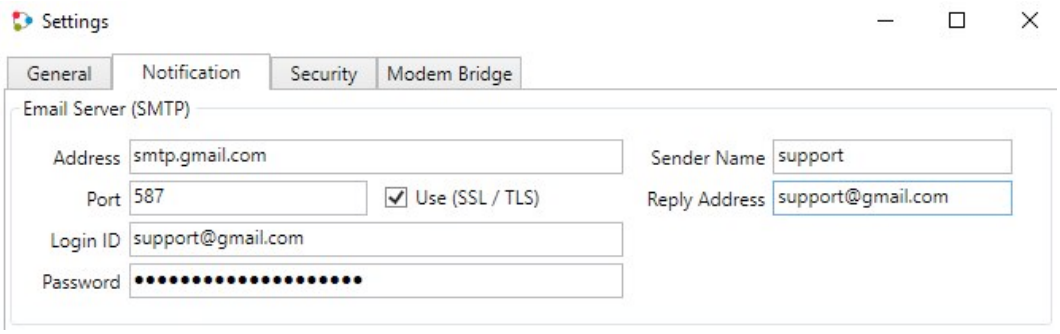


Click on the checkbox at the top for ‘Enforce 2-factor authentication (Email)’

This will require each new RMS Client login (remote or local) to enter a one time passcode (Verification Code) sent via email to the admin account – in addition to the RMS Client Password.



Before this 2-factor authentication will work, you must have setup an email address / account in the Notification tab.



Note: If you're using Gmail as your notification account – you'll need to first enable 2FA within your Google account. Log into your Google account and search for 'App Password' – this will generate an 'app specific' password on your screen.

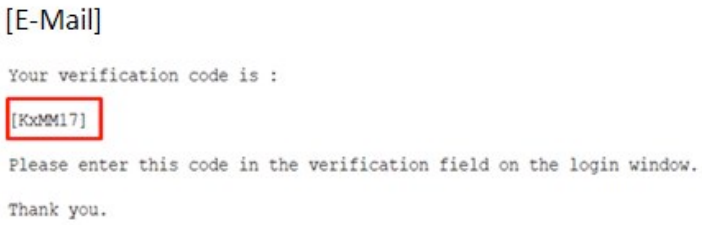
Create a name for the 'app' – for example 'genrms-notification' (you can name it whatever you want) and then a long password will be generated on the screen.

Cut and paste that new password into the Notification password field above – do not enter your gmail password, it will not work.

This article from Google explains this process:

how-to-create-app-passwords-gmail

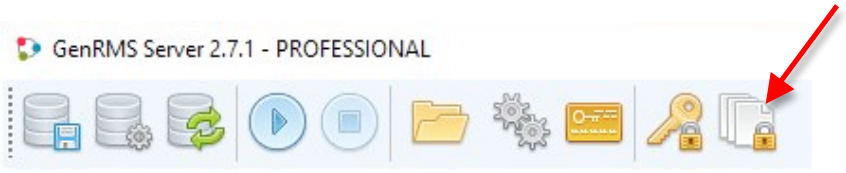
Once this process has been enabled and the email account is properly configured, as you log into the GenRMS Client application, you'll see a notice that a verification code has been sent to the notification email address:



Enter the verification code into the GenRMS Client window (do not include the brackets [ ]) Once successfully entered – the login has been verified and will continue.

Login / Verification Code Logs:

Click on the ‘log’ icon – far right of the tool bar

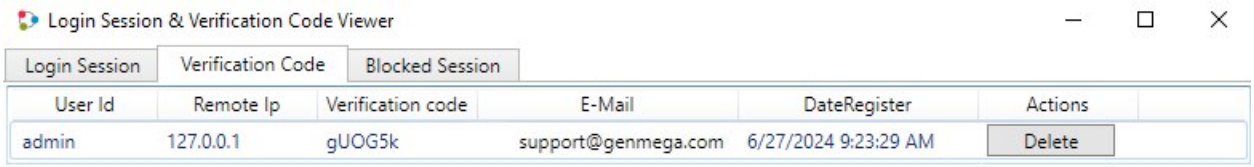


This log screen will show any attempted login attempts, as well as any verification codes issued to specific remote logins – by IP address.

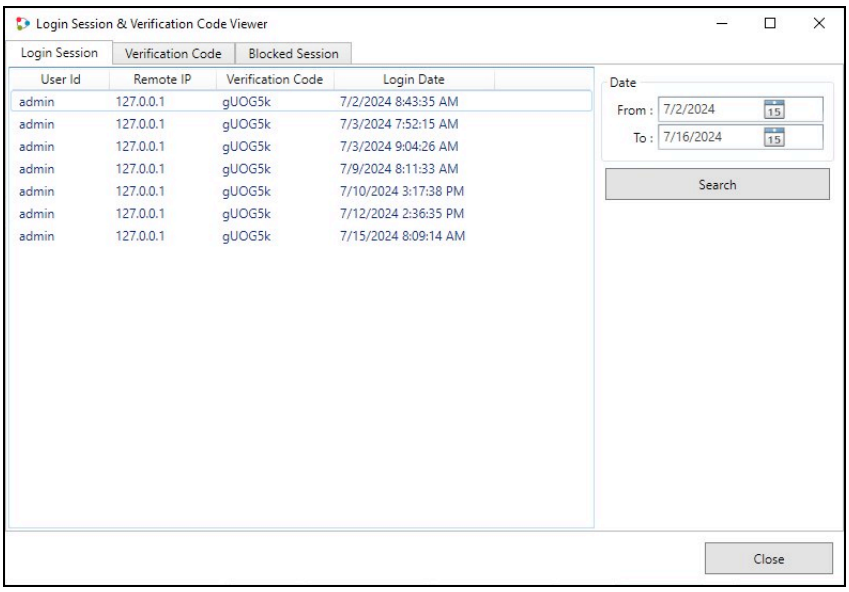
Below you can see a login, with the verification code from a remote user.

If this is an approved login, then there’s nothing else to do – if you want to terminate access for this remote user, use the [Delete] button to remove the code and user.

This will require a new verification code, if that same user needs to reconnect.

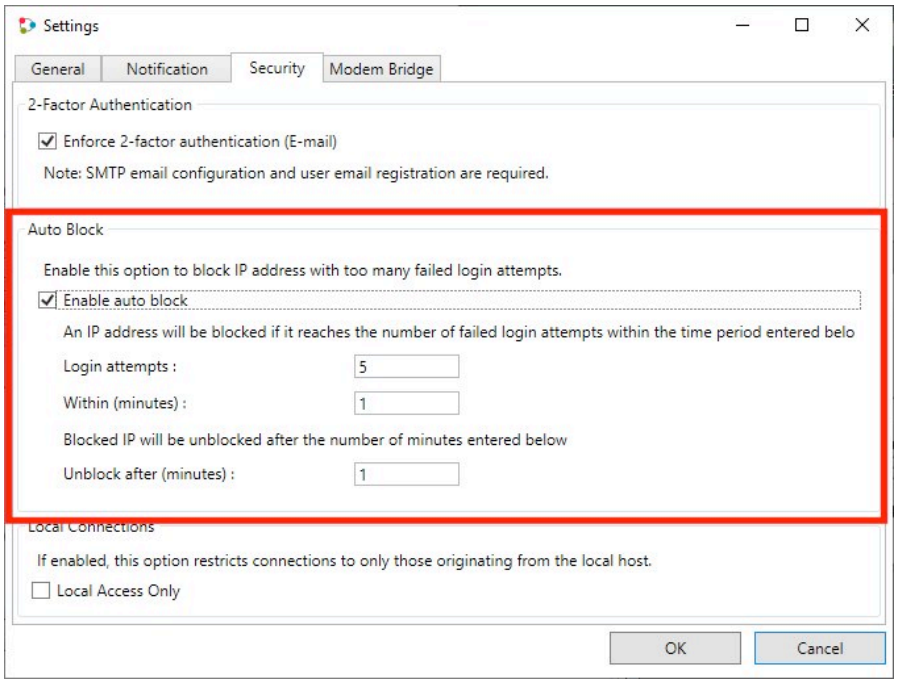


The ‘Login Session’ tab shows the IP address of any login to RMS – including locally at the RMS PC – along with the date and time of the login.



Auto Block

Auto block provides tools to limit remote login attempts. When you enable this function from the menu below – any attempted remote login to your RMS will be blocked, based on the settings below.



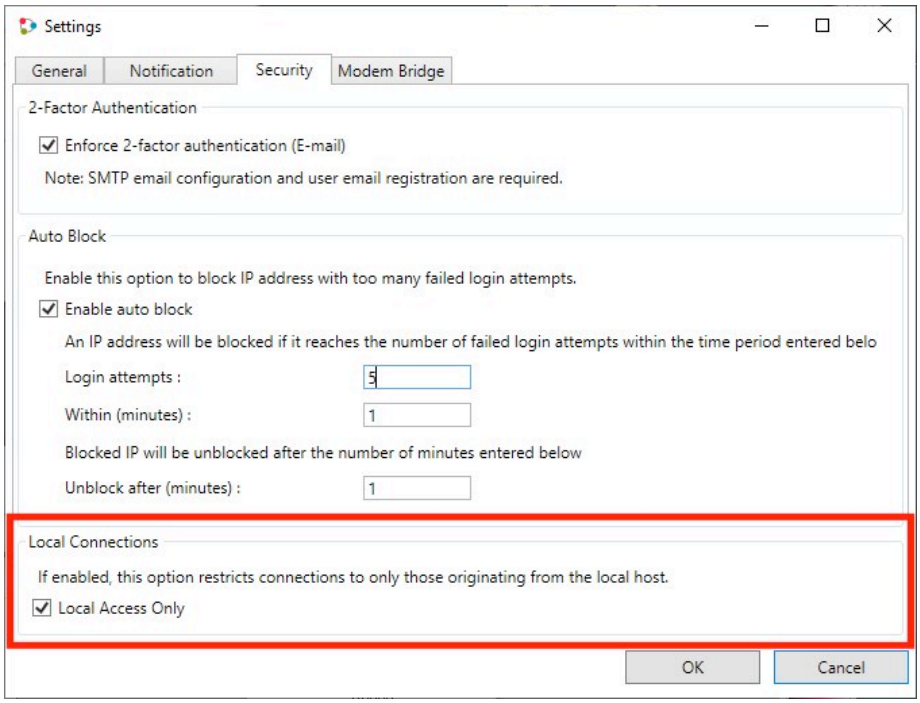
RMS will block an incoming IP address after X number of attempts within the specified time period selected above. These blocked attempts will also be stored in the logging screen.

Blocked addresses are found in the 'Blocked Session' tab – listed by IP address and last attempted date / time.

If an authorized user is accidentally blocked, you can manually 'unblock' them by clicking the [UnBlock] button next to the entry.

Local Access Only

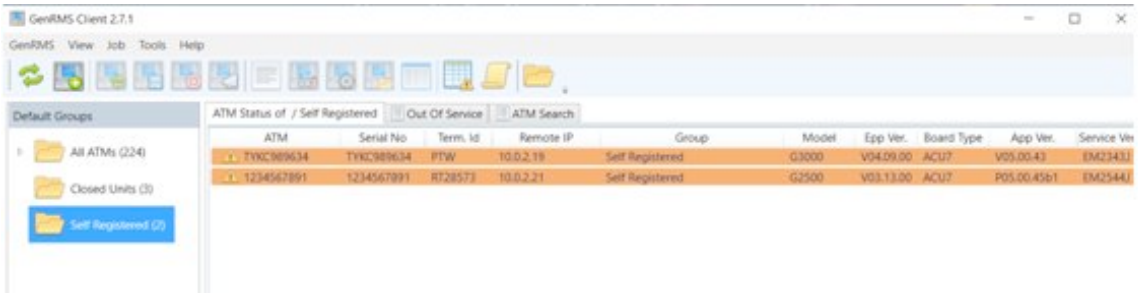
If you log into your RMS PC within your office – and you're not using a remote connection to RMS via IP address – then you can now disable any remote access by selecting the option below:



Enabling this option will restrict all RMS Client access – except from the RMS PC directly.

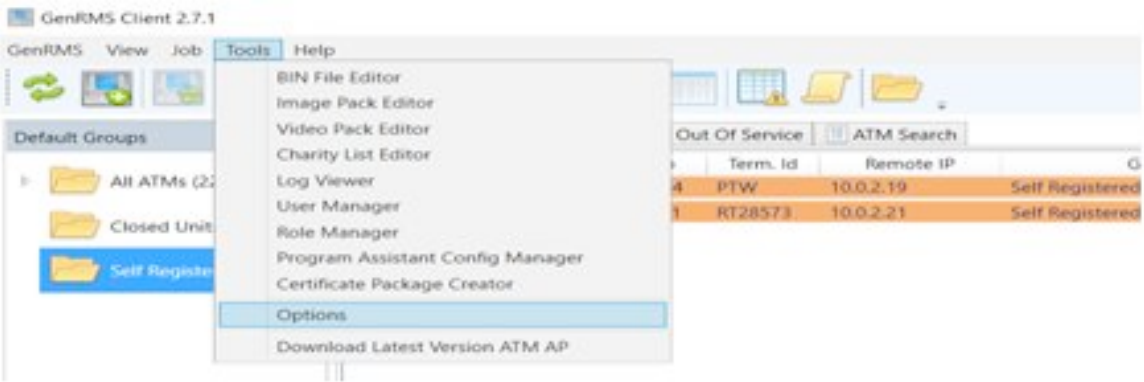
Alerts for default ATM RMS Password

This new version will highlight all ATMs in your RMS Client window, which have been left at the default RMS Password (333333). ATMs where the RMS password has not been changed, will show highlighted in Orange:

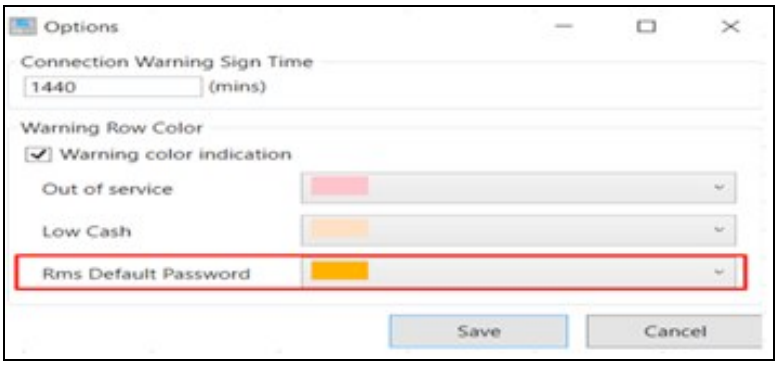


You can change the color code – or turn it off within the 'Options' menu.

From the RMS Client screen, click 'Tools' – then 'Options'



Within this menu, you can select color codes.



If you don't want to see the color codes, just select 'white' to match the default background.