

8872 Security Bulletin

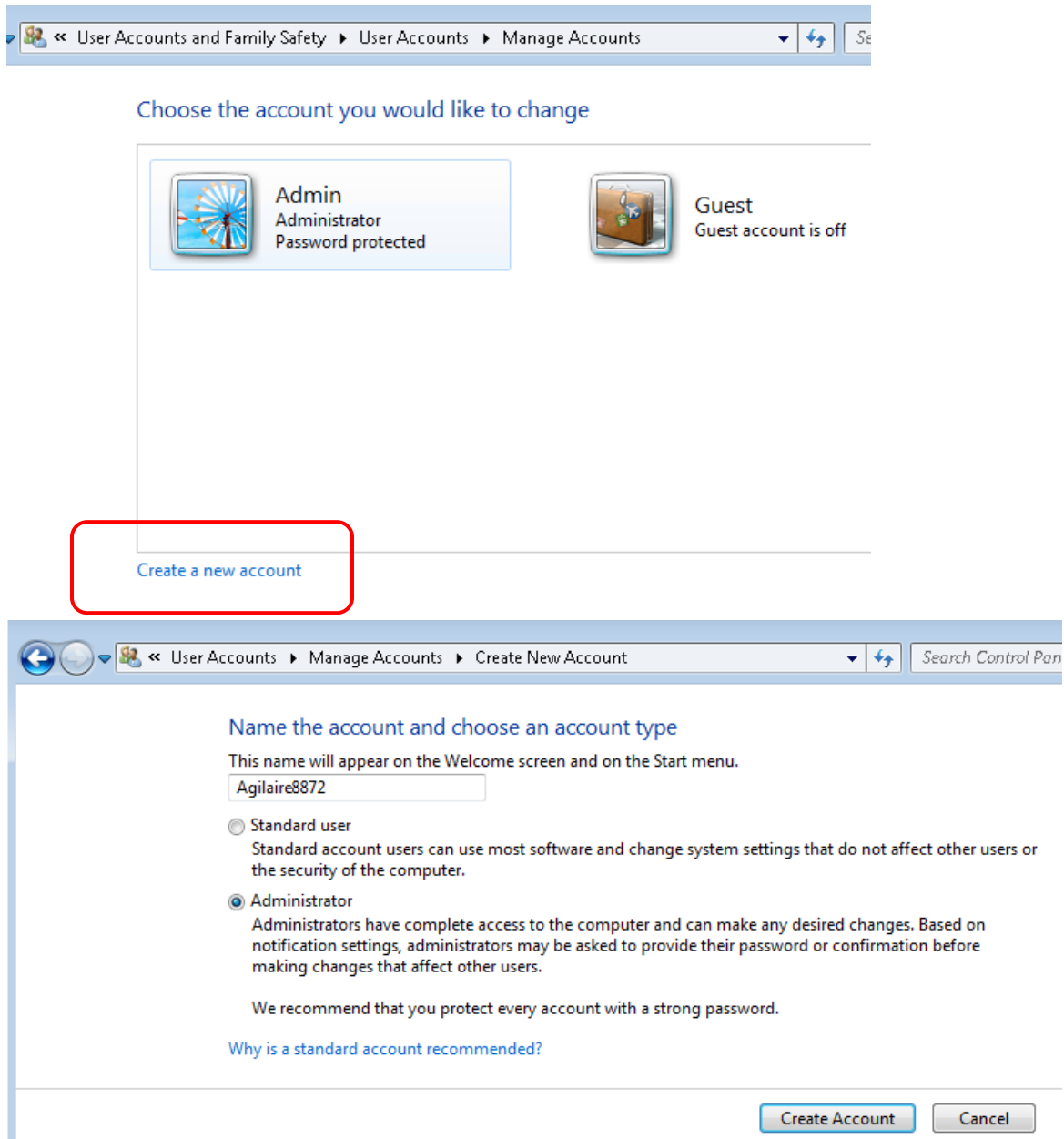
04/13/2021

To improve system security of 8872s deployed behind public facing IP addresses (cellular modems, etc.) Agilaire has the following recommendations for customers to review and implement as appropriate on their 8872 loggers.

Windows Accounts

1. Change the default 'admin' Windows account password
AND / OR
2. Create a new Windows user account with a name OTHER than 'admin' and set it up as an administrator role and set a 'strong' password.

Windows 7



The image shows two screenshots from a Windows 7 system. The top screenshot is the 'User Accounts and Family Safety' control panel window, specifically the 'Manage Accounts' section. It displays two accounts: 'Admin' (Administrator, Password protected) and 'Guest' (Guest account is off). A red box highlights the 'Create a new account' link at the bottom. The bottom screenshot is the 'Create New Account' wizard. It prompts the user to 'Name the account and choose an account type'. The name 'Agilaire8872' is entered in the text box. The 'Administrator' radio button is selected. The 'Standard user' option is also visible. At the bottom, there are 'Create Account' and 'Cancel' buttons.

Choose the account you would like to change

Admin
Administrator
Password protected

Guest
Guest account is off

Create a new account

Name the account and choose an account type

This name will appear on the Welcome screen and on the Start menu.

Agilaire8872

Standard user
Standard account users can use most software and change system settings that do not affect other users or the security of the computer.

Administrator
Administrators have complete access to the computer and can make any desired changes. Based on notification settings, administrators may be asked to provide their password or confirmation before making changes that affect other users.

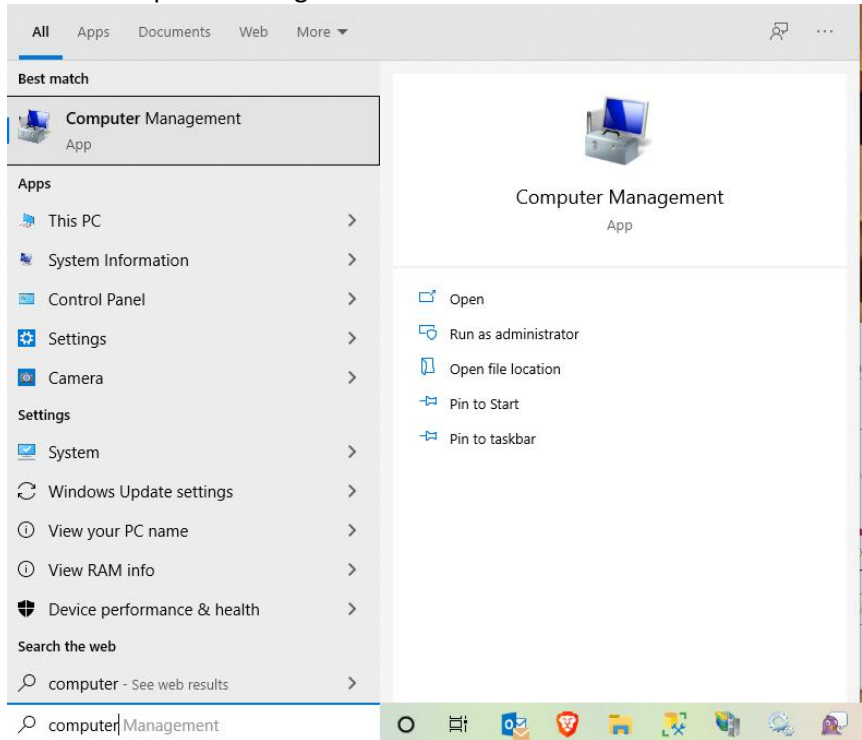
We recommend that you protect every account with a strong password.

[Why is a standard account recommended?](#)

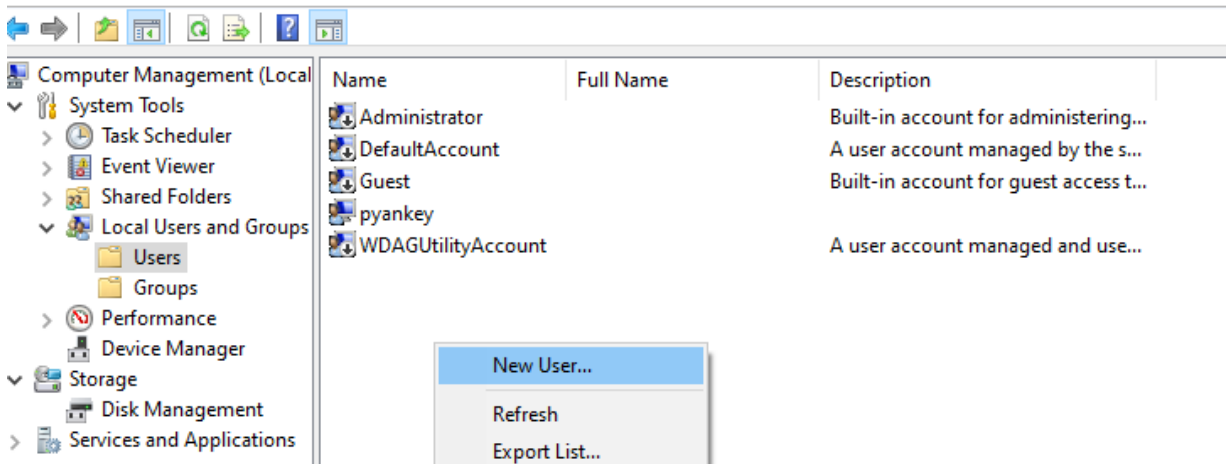
Create Account Cancel

Windows 10

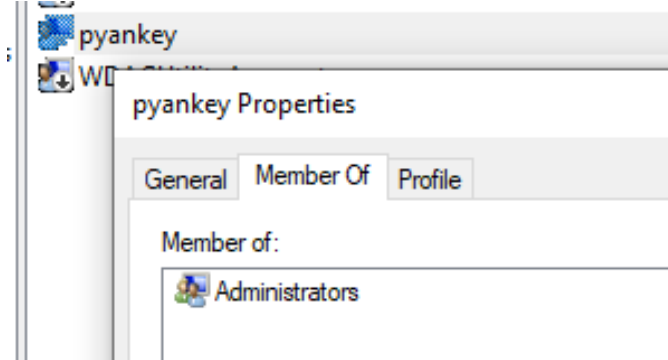
Launch Computer Management



Drill down to Users folder, right click and select New User



Right click the new user, select Properties, and add to Administrators on the Member Of tab



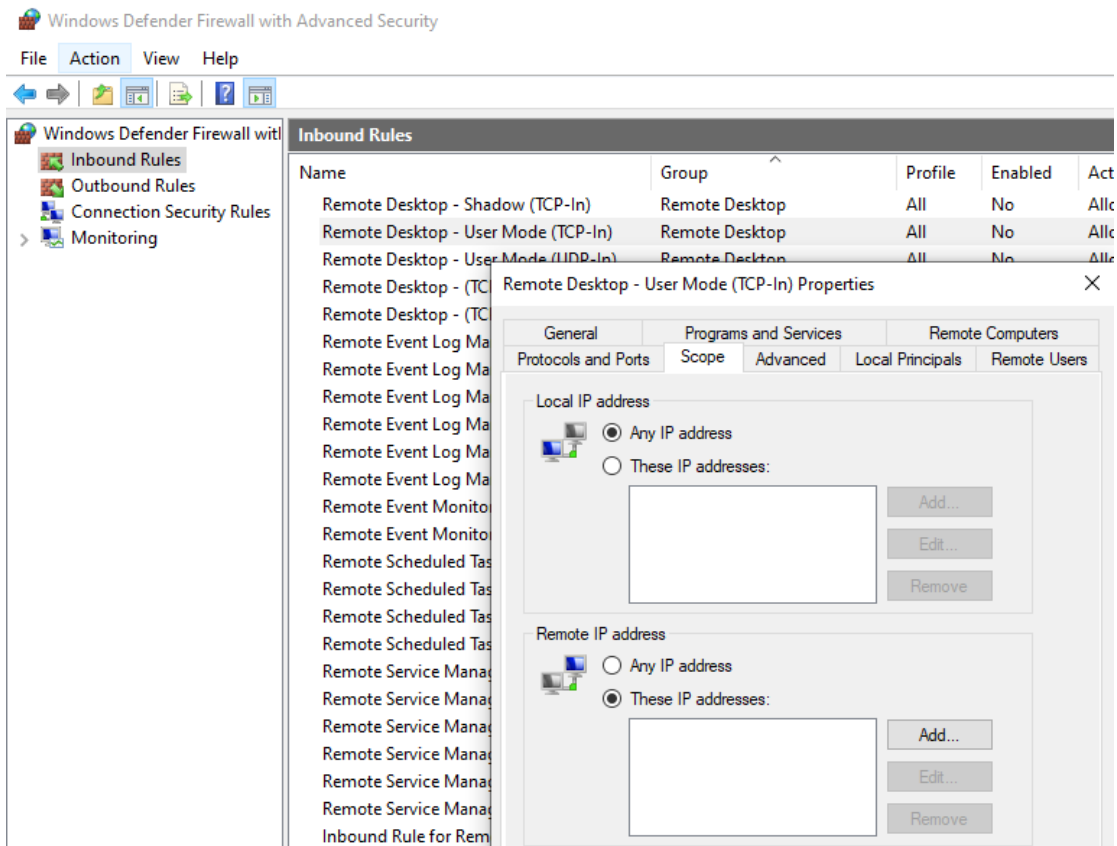
- a. Remove RDP access for default Administrator account
 - i. Run secpol.msc
 - ii. Navigate to Security Settings\Local Policies\User Rights Assignment
 - iii. Double click on 'Deny log on through Remote Desktop Services'
 - iv. Click 'Add User or Group'
 - v. Add the Administrator user then 'OK' and close out of the editor

Firewall

1. Make sure the Windows firewall is enabled (unless using a third party security suite).



2. Set firewall restrictions for Remote Desktop, limit the IPs or IP ranges that can access Remote Desktop using the 'Scope' tab and 'Remote IP Address' option of the rule properties.



Site Router

Use options in your site router to use another port for Remote Desktop (default is 3389) and have the routing send external traffic over the new port to port 3389 on the 8872.

If possible, use IP / IP range restrictions in the router to limit what source traffic can get through to the port. This would apply to both the Remote Desktop port and the SQL port (1433 or 8998 depending on Win 7 or Win 10 8872).