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.

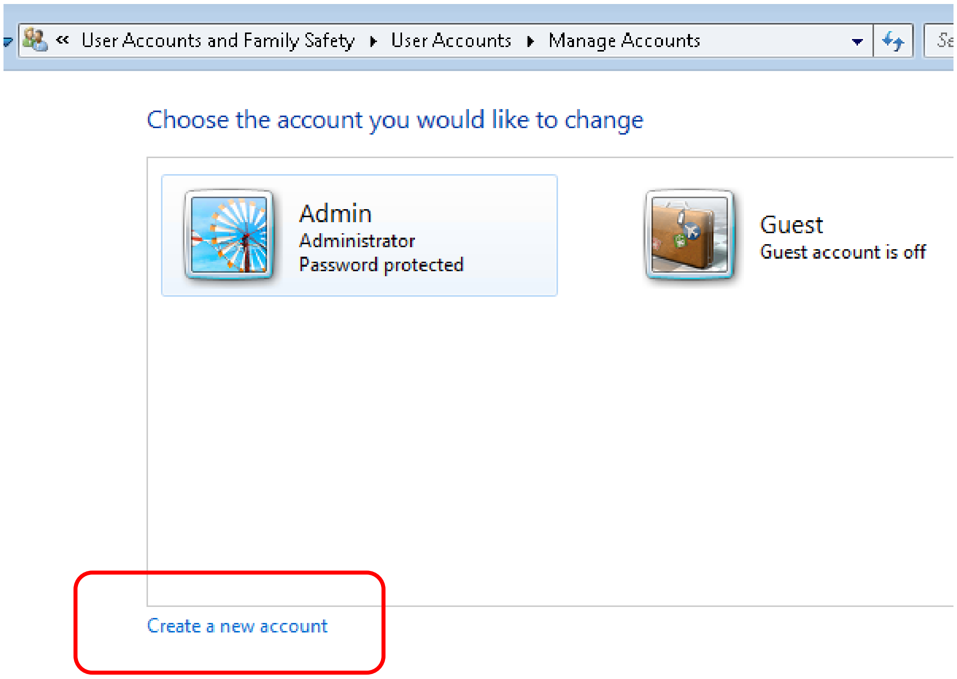
Windows Accounts

1. Change the default 'admin' Windows account password

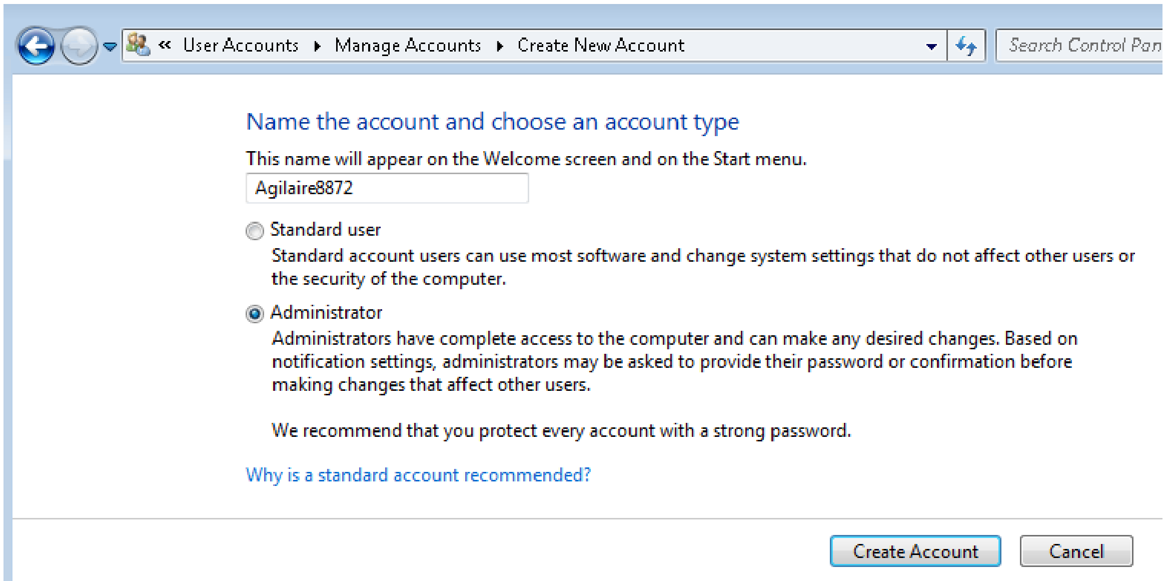
AND / OR

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


« User Accounts and Family Safety ▸ User Accounts ▸ Manage Accounts
Se

Choose the account you would like to change



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

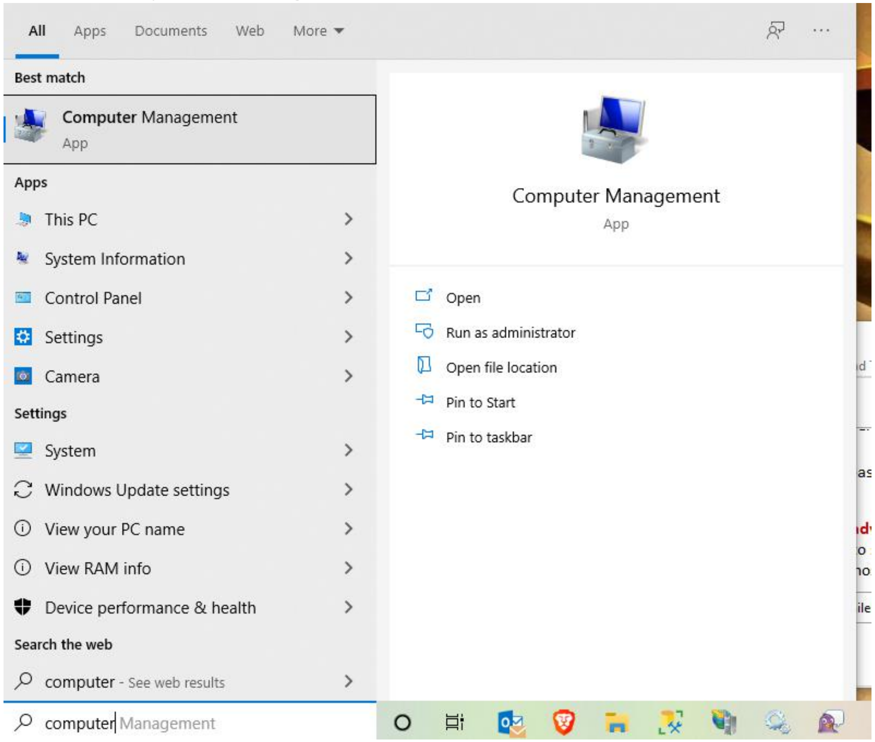
Administrators have complete access to the computer and can make any desired changes. Based on notification settings, administrators may be asked to provide their password or confirmation before making changes that affect other users.

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

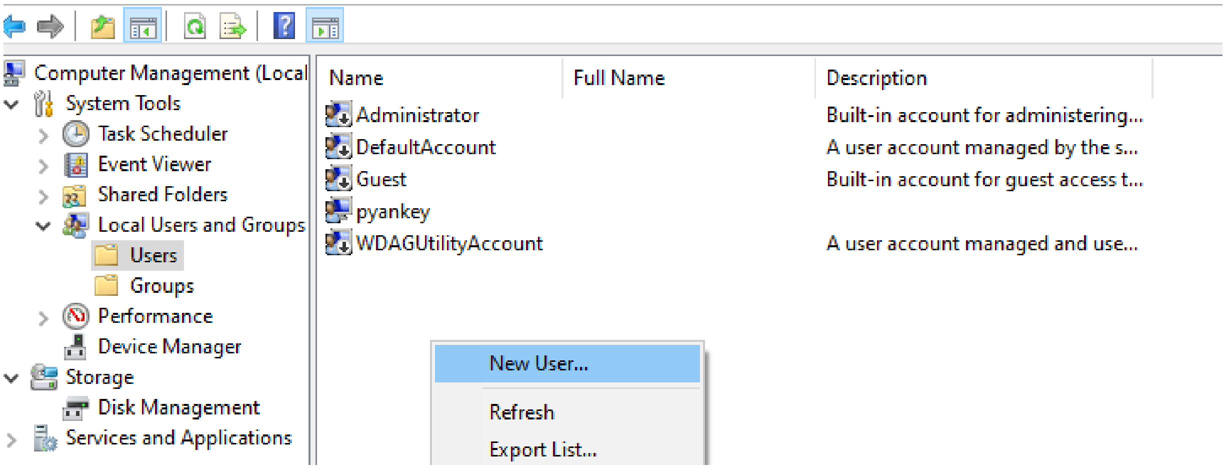
Why is a standard account recommended?

Windows 10

Launch Computer Management

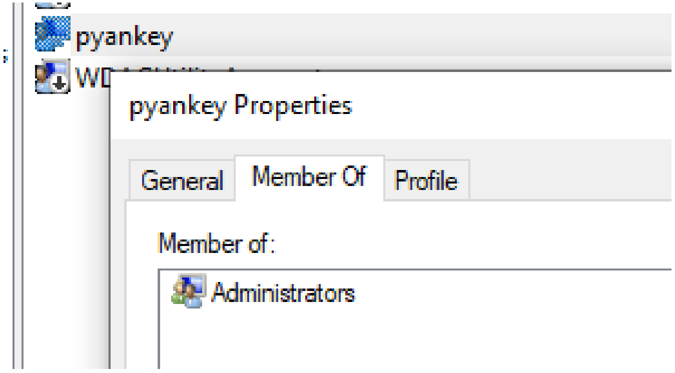


Drill down to Users folder, right click and select New User



Name	Full Name	Description
Administrator		Built-in account for administering...
DefaultAccount		A user account managed by the s...
Guest		Built-in account for guest access t...
pyankey		
WDAGUtilityAccount		A user account managed and use...

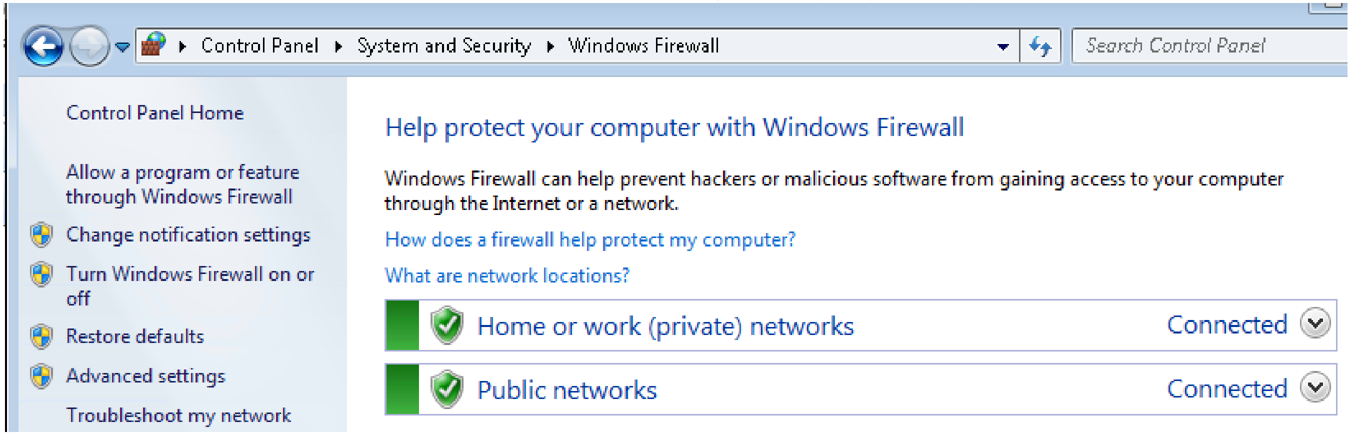
Right click the new user, select Properties, and add to Administrators on the Member Of tab



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).


Control Panel ▸ System and Security ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

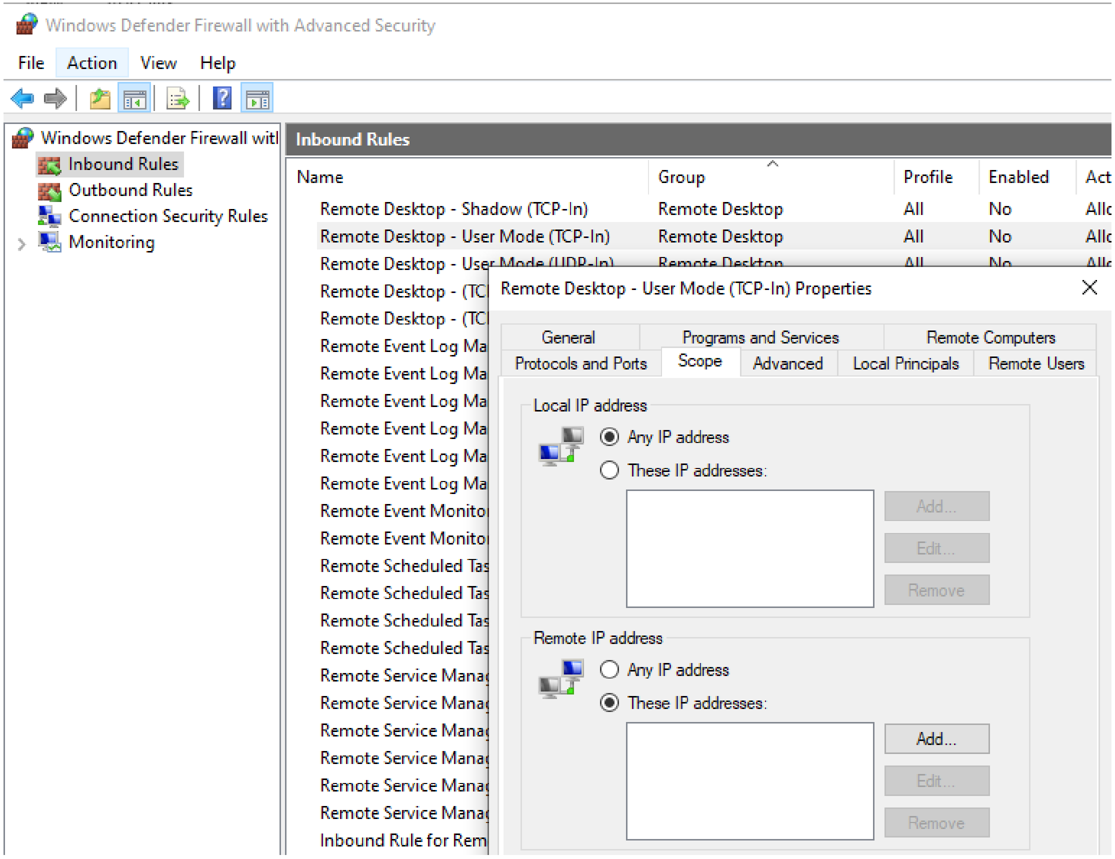
How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks — Connected

Public networks — Connected

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.


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall wit
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

Inbound Rules

Name	Group	Profile	Enabled	Act
Remote Desktop - Shadow (TCP-In)	Remote Desktop	All	No	Allo
Remote Desktop - User Mode (TCP-In)	Remote Desktop	All	No	Allo
Remote Desktop - User Mode (UDP-In)	Remote Desktop	All	No	Allo
Remote Desktop - (TC				
Remote Desktop - (TC				
Remote Event Log Ma				
Remote Event Log Ma				
Remote Event Log Ma				
Remote Event Log Ma				
Remote Event Log Ma				
Remote Event Log Ma				
Remote Event Monito				
Remote Event Monito				
Remote Scheduled Tas				
Remote Scheduled Tas				
Remote Scheduled Tas				
Remote Scheduled Tas				
Remote Service Mana				
Remote Service Mana				
Remote Service Mana				
Remote Service Mana				
Remote Service Mana				
Remote Service Mana				
Inbound Rule for Rem				

Remote Desktop - User Mode (TCP-In) Properties

Local IP address
● Any IP address
○ These IP addresses:

Remote IP address
○ Any IP address
● These IP addresses:

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).