8872 Security Bulletin UPDATE

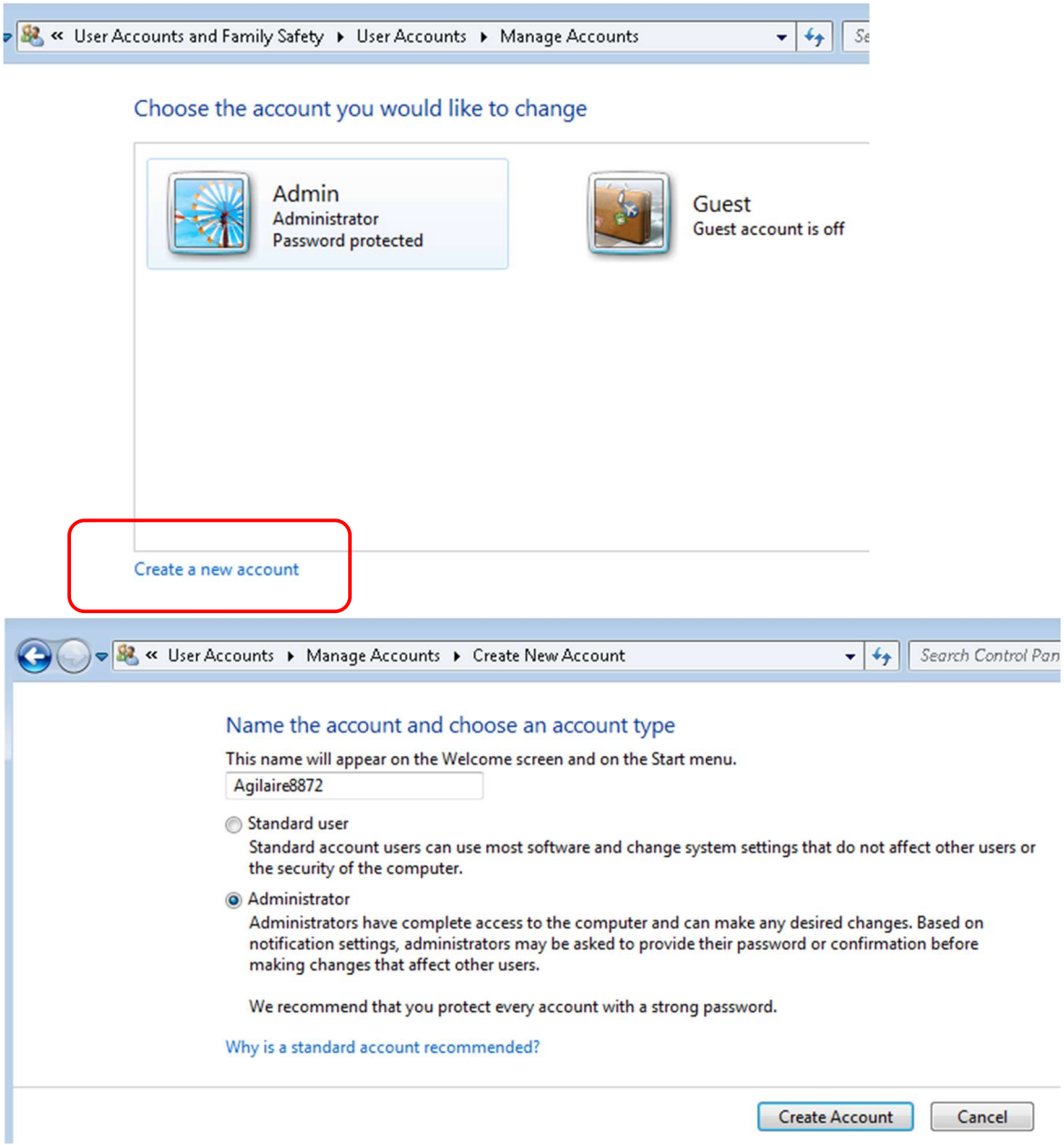
07/27/2022

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

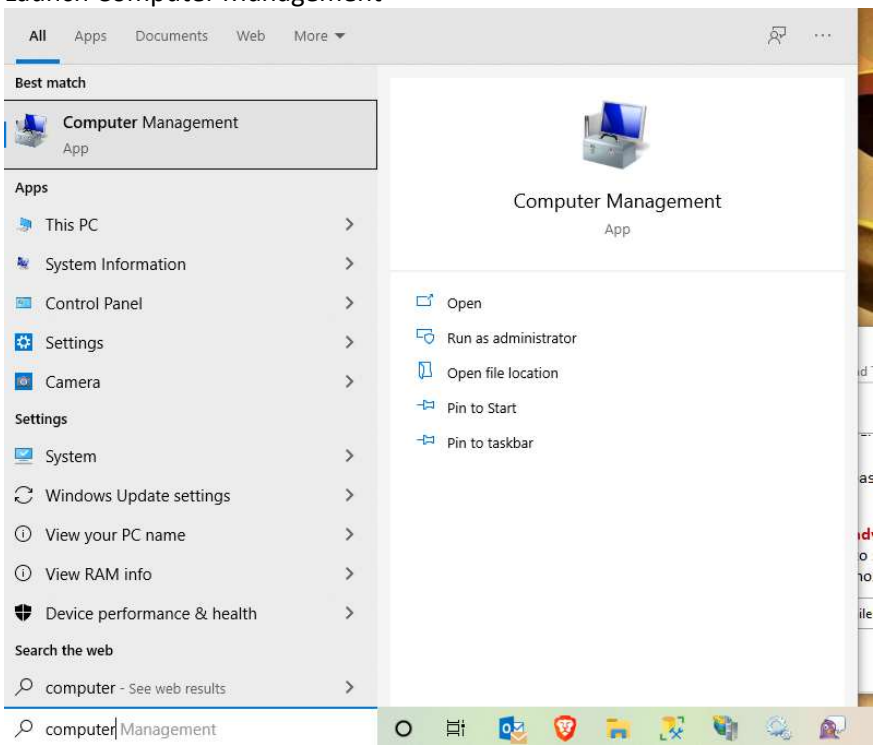
1. Change the default 'admin' Windows account password
2. Create a new Windows user account with a name OTHER than 'admin' and set it up as an administrator role and set a 'strong' password.

Windows 7

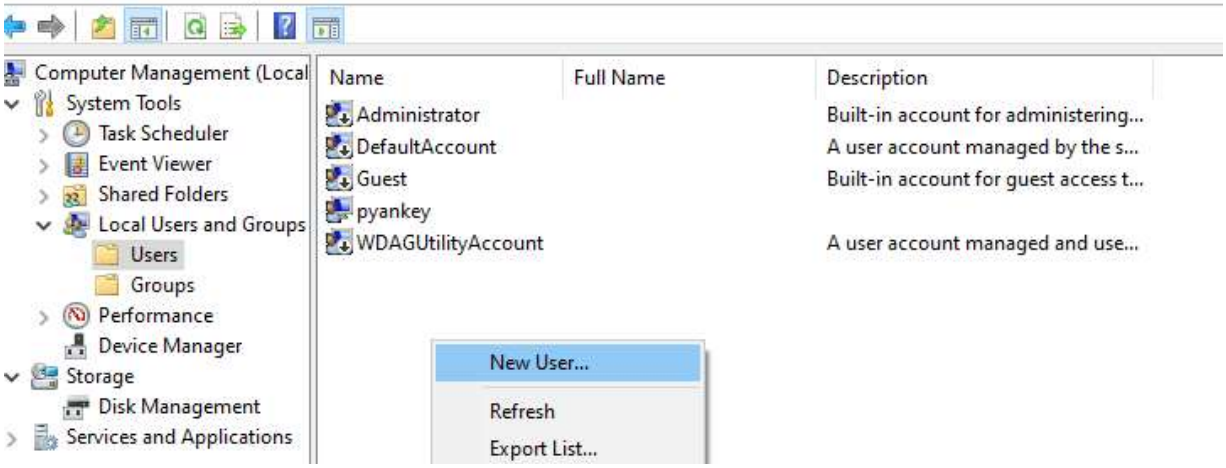


Windows 10

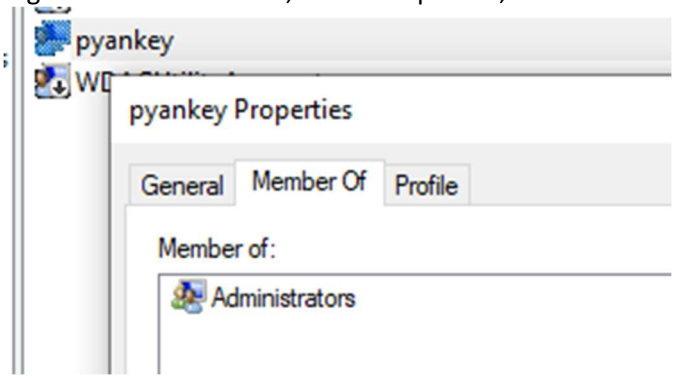
Launch Computer Management



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

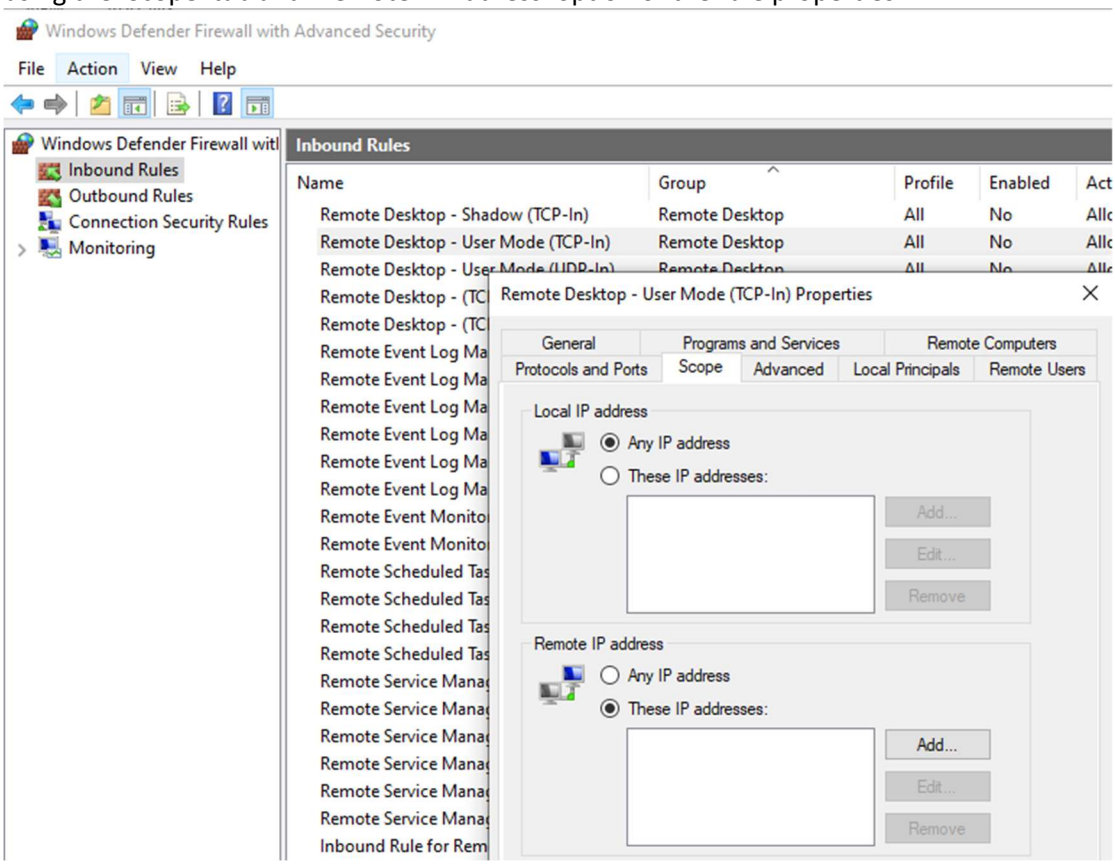


a. Remove RDP access for default Administrator account
    i. Run secpol.msc
    ii. Navigate to Security Settings\Local Policies\User Rights Assignment
    iii. Double click on 'Deny log on through Remote Desktop Services"
    iv. Click 'Add User or Group'
    v. Add the Administrator user then 'OK' 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 ALL ports set up with routing/forwarding on the site router (1433 or 8998 for sync, the port set for RDP, 9881 for polling, 9885 for AV client).

Windows 7

As of January 14, 2020, computers running Windows 7 will still function but Microsoft will no longer provide the following:

- Software updates
- Security updates or fixes

Agilaire strongly recommends customers still running Windows 7 8872s procure a security / malware / virus protection application and apply it to those loggers. This should provide real time protection. Agilaire does NOT support third party applications. We have had personal good experiences with Malware Bytes.

Also, Internet Explorer is out of Microsoft support. Agilaire recommends deleting any IE shortcuts and using a currently supported browser that provides its own security updates. Customers should consider MS Edge, FireFox, Google Chrome.

NOTE to avoid performance issues, the SQL Data directory should be excluded from realtime scanning. The path should be C:\Program Files\Microsoft SQL Server\MSSQL10_50.SQLEXPRESS\MSSQL\DATA (highlighted portion may vary)