Tech20140613-1-2

Security Options for Cellwatch iBMU

This application note is intended for anyone planning to install the Cellwatch iBMU onto a corporate network. It should be read by installers and network administrators. The iBMU comes in an unsecured form. The revision state of Windows cannot be guaranteed to be up to date, as the iBMU may have been manufactured several months before final site installation and commissioning. As with most commercial systems there is no virus protection provided on the Cellwatch iBMU.

NETWORK PORTS

There are two network ports available on the iBMU. One service port configured as a static IP and one network port configured as a dynamic IP. Settings are configured for the iBMU to obtain an IP address as soon as it is plugged into an Ethernet network.

Cellwatch is designed to be remotely accessible in order to streamline the interactions with the software and simplify the retrieval of battery data. There are several hardware and software options for interfacing with the iBMU. The most common method is using a keyboard, monitor, and mouse and the primary alternative is Windows Remote Desktop.
This means there are many ways to secure the iBMU while still maintaining the ease of access for the user. The data protocols and port specifications for Cellwatch and supporting software are detailed below.

USER ACCOUNT

There are two user accounts on the iBMU. These accounts are labeled “Cellwatch” and “Recovery”. Both have passwords that are the iBMU’s serial number. The Cellwatch account’s password can be changed, but we highly recommend not changing the Recovery account’s password. Upon startup, the password will have to be entered in order to login into the account. Cellwatch 5 runs as a Windows service and does not require a user to be logged in to start scanning. In the event of a power failure, the iBMU will be able to return to normal scanning mode automatically.

Putting the iBMU on a Domain may change operating system settings and prevent Cellwatch from performing normally. System level changes and domain settings limit Technical Support’s ability to help troubleshoot issues on the system.

Cellwatch

Available data output ports

Modbus: TCP/IP port 502

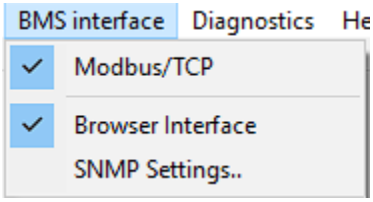
Browser Interface: TCP/IP port 80 (HTTP)

Browser interface can be protected by a username and password. Username: “cellwatch” Password: “deafcat”. To enable the log in requirements, open the Cellwatch.ini file and enter “1” for the Authorization needed field.

[HTTP]

Authorization needed=1

Restricting ports: All available data output ports can be disabled in the running software. Go to the menu option at the top: “BMS Interface”. Uncheck “Modbus TCP/IP” and “Browser Interface”. The password “deafcat” is required to make changes to the BMS options.



Remote Connection

The iBMU can be connected to remotely over Windows Remote Desktop. To remote into the iBMU, place it on a local network using the Dynamic port or connect directly with a network cable to the Service port. The Dynamic port will take the address given to it by the network, while the service port will stay at the default service static IP address.

Default service static IP address: 192.168.0.128
The service port will always be accessible at the 128 address above. When using a network cable, place the laptop’s IP address on the same address range of 192.168.0.xxx to remote into the iBMU.

Username: cellwatch
Password: iBMU serial number

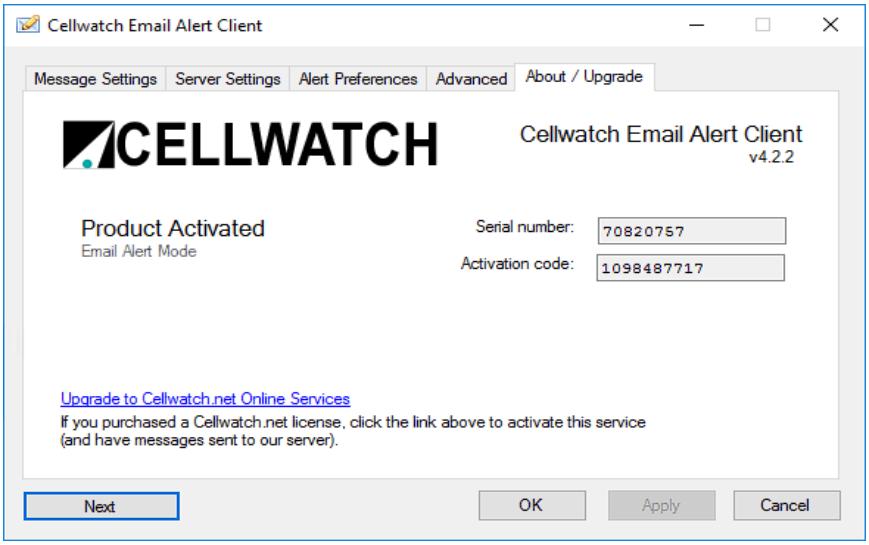
Windows Remote Desktop: TCP/IP port 3389

Every Windows machine comes with Remote Desktop and the versions are backwards compatible across Windows versions. Close the session using the X on the window.

KVM over IP (optional)

To remove an iBMU from the local network but still be able to remotely access it, a KVM over IP can be used. The hardware uses video out/USB connections to the back of the iBMU. The key commands and video signal can be sent over the local network. This allows a remote user to interact with the iBMU without being able to send or receive data. There is no risk to the local network as the VGA, HDMI, and USBe ports can't move data packets other than the hardware commands.

Email Alert



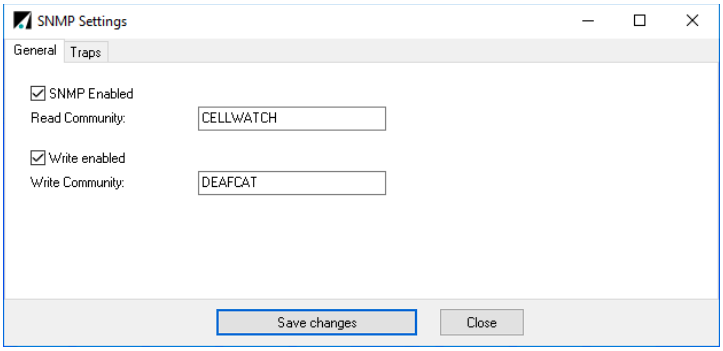
Email Alert can be configured to use the desired port for the site's SMTP server. IP address and port preference can be changed under the "Server Settings" tab in the Email Alert client settings window.

Default SMTP port: 25
Default secure port: 587

SNMP

Ports: 161, 162 (Traps)

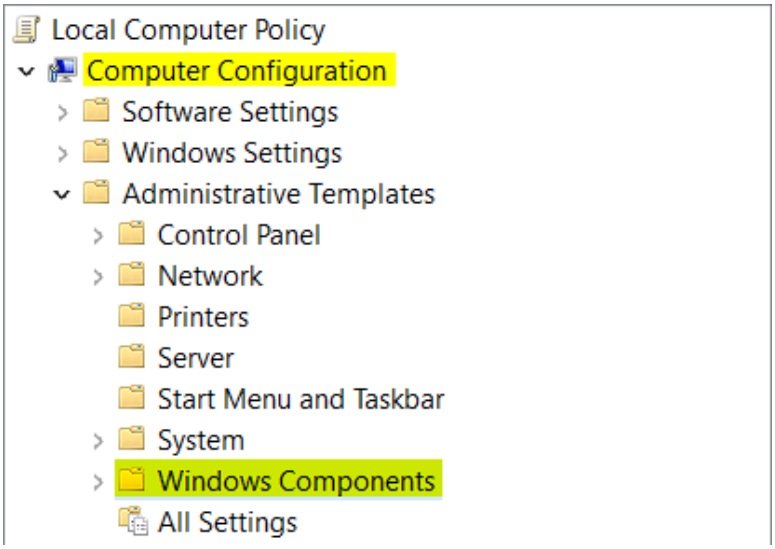
Cellwatch 5 now has the SNMP settings integrated into the software which transmits the Cellwatch data over SNMPv1 protocol. The data is protected using the SNMP read and write communities. Traps can also be sent to recipient IP addresses.



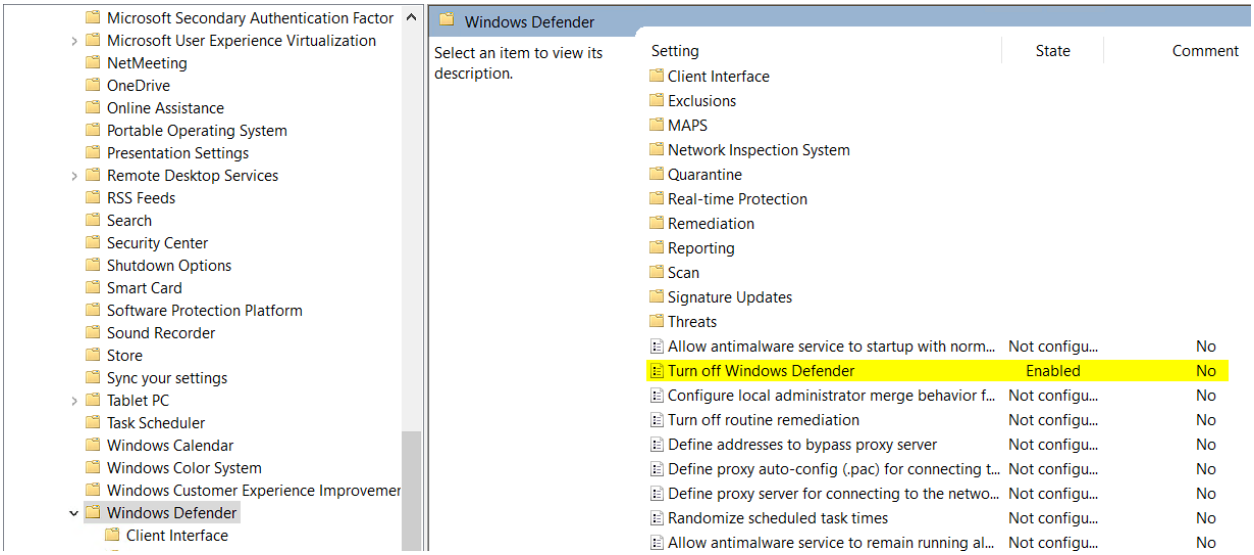
Antivirus Software

By default, Windows Defender is disabled. You will need to edit the group policy in order to enable Window Defender.

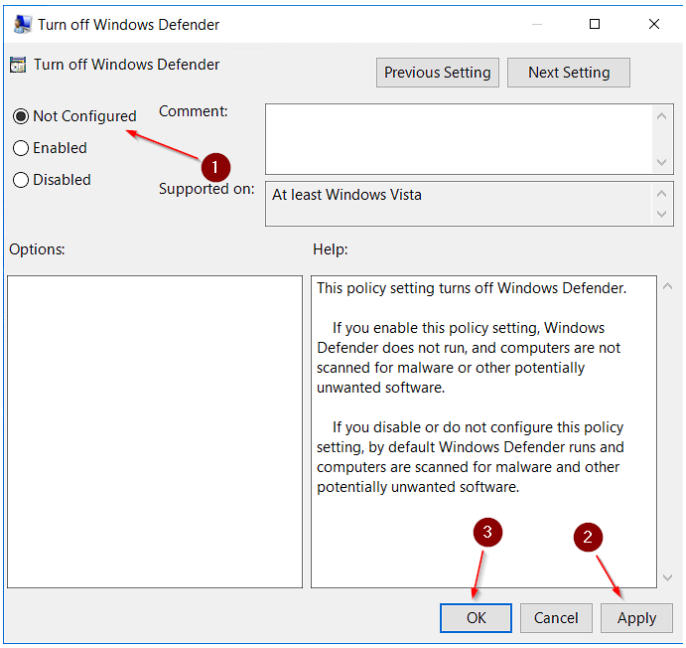
Open the start menu in the lower left corner and search for “Edit Group Policy”. Under the Computer Configuration line, select “Administrative Templates”. Double click on “Windows Components”.



Scroll down to “Windows Defender” and double click. In the window to the left, there will be a line that says “Turn off Windows Defender” is enabled.



Right click and select “Edit”. You will select “Not Configured”, hit apply, and then OK.



This allows Windows Defender to be on. Open “Update & Security” under Windows settings. In there, you will find the Windows Defender settings. Turn Windows Defender on and start a scan. Once completed, review any suspicious files found and close the window. The iBMU is now protected.