User Guide

Copyright 2021

Contents

Overview

BACPro™ provides unrestricted live monitoring, analysis of offline captures, and comprehensive reporting. Every day, millions of BACnet® messages are sent over your network to the devices that comprise your building control system. Adding to the complexity, the network is often shared by devices from different vendors that do not always work together seamlessly. When problems occur, it often takes a BACnet expert hours or days to review network capture files, understand the causes, and then pinpoint the problematic device or workstation. BACPro cuts through the complexity and saves you time by providing non-stop analysis of every BACnet packet on your network—and then highlights the problem areas.

Modes of Operation

BACPro has two modes of operation: live monitoring, and offline capture file processing.

Live Monitoring

BACPro is a live 24/7 network-monitoring tool that listens to every packet to and from your building automation workstation and then reports any discovered anomalies. BACPro can also send you SMS messages when it finds severe anomalies such as duplicate BBMDs, and device, workstation, and network failures.

Offline Capture File Processing

BACPro can import any BACnet IPv4, IPv6, or MSTP capture file and report issues it finds in the capture. Large captures containing at least an hour's worth of data work best. While BACPro can process any size file, those with less than an hour’s worth of data might not accurately analyze the network’s health. BACPro stores all analyzed information in a SQL database, and it also can generate a comprehensive report for each capture file you import.

Licensing

BACPro has two licensing models.

Online Monitoring

For online monitoring, the license is for a single computer to monitor all traffic to and from a building operator workstation. If your site has multiple workstations then you will need a license for each of them. A license is keyed to a computer.

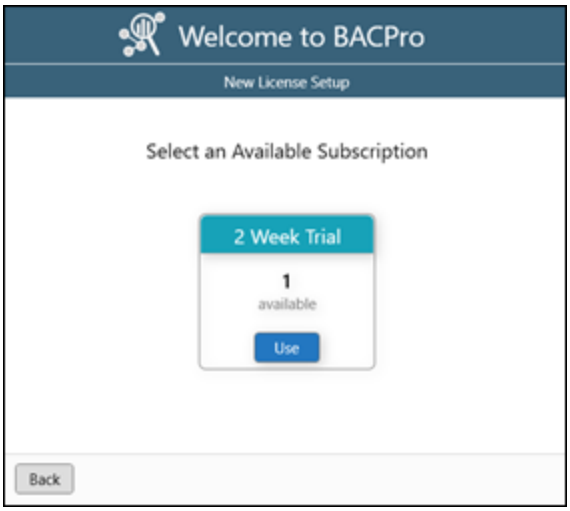
Offline Capture Analysis

For offline capture analysis, the license is intended for a single computer and single user. For example, a technician to use on his laptop. If you have multiple technicians that troubleshoot BACnet issues, please purchase a license for each user.

Getting Started

Once BACPro is installed, you need to set up the license—either a two-week trial license, or your paid subscription license. In the New License Setup dialog box, enter the email address and password you created at bacprotool.com.

After signing in, choose the license type you set up on the website. If you do not have an internet connection, you must choose the Switch to Manual Setup button, and follow the steps to generate your license. The following dialog box shows a 2 Week Trial license. If you paid for a license, it also shows up here. Once you have a valid license, you can import captures or set up a live connection.



Types of Anomalies

BACPro monitors your network for over 30 different types of network problems, which are assigned a severity rating based. Ratings are sometimes open for interpretation. For example, a low hop count could indicate a circular network—a high configuration issue. However, if the initial hop count is set incorrectly, this could be a false positive—and therefore a low network issue.

Severity Rating	**Meaning**
Info	A network issue with very low impact. **Examples:** ● A device with several UDP retries. ● A new device was found on the network
Low	A network issue with low impact, mostly isolated to a device. **Examples:** ● A device that is overloaded or that needs a longer APDU timeout. ● A device with unexpected error codes.
Medium	A network issue with medium impact. Can affect more than just a single device. **Examples:** ● Large amounts of COV or Event traffic ● A router reporting an error.
High	A network issue with high impact to the workstation or network. **Examples:** ● A workstation may not be able to communicate with devices. ● A router might have failed. ● A configuration error that could lead to communication problems until addressed. ● A network with BBMD configuration issues.
Critical	A network issue with severe impact to the system **Examples:** ● A workstation or network shows no communication. ● A configuration issue that must be addressed immediately.

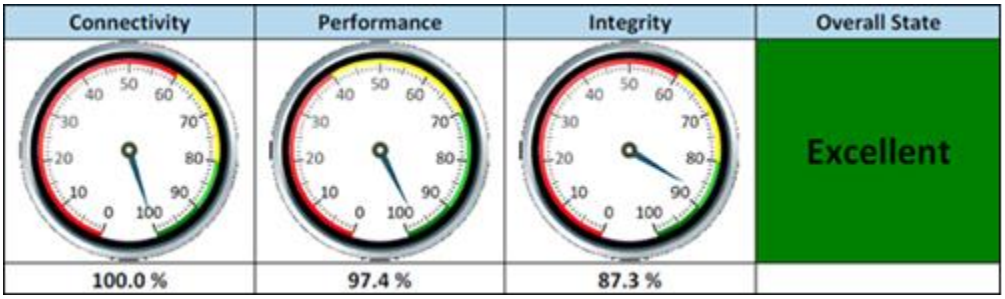
Type	Severity	Description
Excessive Retries	Info	A device is not answering a request within the APDU timeout, causing the request to be sent again. This can happen normally with UDP, but when it happens often it could mean the device needs a longer APDU timeout or is too overloaded to respond to requests. BACPro will flag a device that has more than 20 retries per day.
New Device on Network	Info	A new device was found on the network. If an I-am is found for a device that was not previously known, it will be brought to your attention. Hopefully, it was expected.
Packet Never Answered	Low	This is similar to a retry, but the device did not answer the retry either. If this happens often, it means the APDU timeout is too short or the device is too busy to answer requests. Try setting a longer APDU timeout.
High Number of Networks	Low	Many devices have a fixed size router table. If there are more networks than the size of the table they will send out extra who-is-router to network messages. 150 is a common max networks table size.
MSTP Scanning too high	Low	The highest MSTP address should have the max device address set to itself to prevent unnecessary poll for master packets on the network
MSTP Nonconsecutive nodes	Low	MSTP devices should start at 0 and be addressed consecutively. This minimizes unnecessary poll for master packets on the network
MSTP Master Poll Frequency	Low	MSTP devices should set the frequency to poll for master above every 50 token passes.
Timeout Error	Medium	A timeout error or abort code was returned for a request. A device might need a longer APDU timeout.
Unknown Failed Node	Medium	There are devices sending Who-is repeatedly looking for a node that is not answering I-am. This is a common problem with Notification Classes having a recipient that is not on the network anymore. This leads to extra broadcast traffic on the network and causes devices with limited processing power to have to handle these broadcast requests. Clean up notification class recipient lists to have only active devices on the network.
Reject Message to Network	Medium	A router has rejected a message that it could not forward or that was not formatted correctly. If this is happening constantly, then investigate the source device of the message.
Router Busy Message	Medium	A router has returned an error code indicating it was too busy to send a message. If this happens frequently, investigate what type of traffic is being sent to the router. It could be excessive polling, COVs, or broadcasts.
High COV Rate	Medium	A device is sending COVs too frequently. Any COV rate of more than one-per second for the same property will be flagged. High COV traffic puts a burden on the recipient to process the traffic and can negatively impact the overall network.

Type	Severity	Description
High WP Rate	Medium	A device is receiving Write Properties too frequently for the same property. This will be flagged if there are more than 10 writes for the same property in a minute. High write traffic might indicate poor control logic. Excessive commanding on some types of equipment can cause wear and tear and shortens its life.
High RP Rate	Medium	A device is sending Read Properties too frequently for the same property. This is flagged if there are more than 10 reads per minute. This is usually too much workstation polling. Try adjusting polling rates. This excessive traffic can overload the target device, reducing its ability to function.
High Alarm Rate	Medium	A device is sending alarms too frequently. This is flagged if there are more than 10 alarms in a minute for the same object. This can be caused by not using alarm dead bands or time delay values correctly. High alarm traffic leads to workstations having too many nuisance alarms, possibly causing operators to miss more important alarms.
Preempted by Higher Priority Task	Medium	A device has returned the error code Preempted by Higher Priority Task, indicating the device is overloaded or busy. If it happens often, it should be investigated.
Out of Memory	Medium	A device has returned the Out of Memory error code. The device might be overloaded and should be investigated. It may have too many trend logs or other objects that can consume memory. It might also be receiving too much traffic and cannot queue it up for processing.
Incorrect Password	Medium	A device has returned an error code indicating an invalid password. This could be a misconfigured workstation trying to do a backup.
Buffer Overflow	Medium	A device has returned an error code indicating a buffer overflow. This usually indicates that a device cannot allocate enough memory to respond or queue a request.
Excessive Error Replies	Medium	More than 20 percent of all requests are returning error replies. Investigate if some of these errors are avoidable.
Duplicate Instance	High	Two devices are reporting the same instance number. This is a configuration error that must be corrected. Instance numbers must be unique for devices to communicate properly and receive traffic that is intended for them.
Node Failed / Return	High	A device that was communicating previously has stopped communicating. It could be a temporary communication issue, or it could be more serious if the device has stopped working. It should be investigated. BACpro can send SMS messages for devices that have failed for longer than 10 minutes.
Global Who-Is	High	A device is sending excessive Global Who-is requests, which are used periodically to discover devices. BACPro flags them if there is more than 1 every 30 minutes. They cause all devices on the network to answer I-am and can overload devices that need to process all the broadcast communications.

Type	Severity	Description
Low Hop Count / Circular Network	High	A hop represents a packet passing through a router or gateway on the way to its destination. Low hop count could indicate a circular network, a severe configuration error. It could also be a device that does not start with 255 as the hop count. These should be investigated to make sure there is no circular network.
Duplicate MAC address	High	More than one device is reporting the same MAC address. This is a configuration error that must be corrected. The MAC address must be unique on the network to ensure the device receives all expected traffic.
Duplicate BBMD	High	More than one BBMD is defined on a network segment. This is a configuration error that must be corrected. It leads to excessive traffic on the network. BACpro can send you an SMS message when this happens.
Failed Router	High	A router that does not answer I-Am Router to Network will keep all devices on that network from being seen by the client that is looking for that network.
Excessive Broadcasts	High	Traffic on the network exceeds 30 percent. This puts a burden on every device that must process these messages.
Complete Network Failure/Return	Critical	Traffic on the local network has fallen by 95 percent or more for over a minute. This needs to be investigated immediately. BACpro can send you an SMS message when this happens. It can send an SMS message on return as well.
Workstation Failure or Return	Critical	Traffic from a workstation has fallen by 95 percent or more for a minute. This needs to be investigated immediately. It can be a failure of a driver or process on the workstation, or a restart. BACpro can send you an SMS message when this happens.
Duplicate Router to Network	Critical	Two routers that answer I-am Router to Network for the same network number is a severe configuration error. There should be only one router per network. This must be fixed. BACpro can send you an SMS message when this happens.
MSTP header CRC errors	Critical	The header portion of the MSTP packet is failing CRC checks. This can be bad wiring, duplicate nodes, or noise.
MSTP data CRC errors	Critical	The data portion of the MSTP packet is failing CRC checks. This can be bad wiring, wrong packet length, duplicate nodes, or noise.

Health Scores

BACPro provides three health scores and an overall state-of-the-network rating.



Connectivity	A measure of all devices that are communicating correctly. This means they answer requests and answer I-am to a Who-Is. If there is a who-Is to a device that has never talked on the network, it is counted as not connected, but could also be a configuration error.
Performance	A rating based on how fast devices answer requests. The faster a device answers the better the score. IP devices must answer within 200 ms on average to get the highest score and MSTP devices within 400 ms. The network report shows the average reply time for every device. For a MSTP capture, performance is also a measure of average token pass time. There is also a penalty for high broadcast rate or error replies.
Integrity	A score that starts at 100% and decreases in accordance with the severity of each anomaly discovered on the network. These are the most important issues to address. Examples of integrity issues are misconfigured BBMDs, duplicate addresses, duplicate routers, excessive broadcasts, and router errors.
Overall State	The overall state rating is a weighted average of the above three values. Integrity is weighted highest, then connectivity, then performance. A rating below *Good* should be investigated and corrected to keep your network working well. The overall ratings are Excellent, Good, Fair, Poor, and Critical.

These values are calculated once every minute. When you run a network report, the report shows values based on the average of all values from the past 24 hours for live mode, and for the entire capture file for offline mode. This is why the score on the screen may vary from the score shown in a report.

Network Report and Daily Report

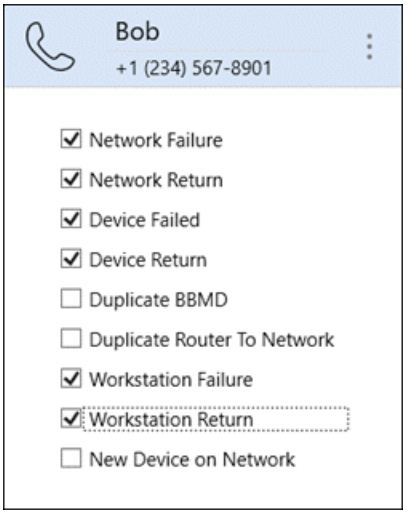
On request, BACPro can generate a comprehensive report for each imported capture. However, BACPro automatically provides a daily report covering the previous 24 hours of traffic for live connections. The report is placed in the same directory as the capture file that was imported. For live monitoring, the report is placed in the *DailyReports* directory where BACPro is installed. The report contains health scores, traffic summaries, and a list of devices. It also shows all anomalies found and provides guidance about how to correct them. The daily report does not contain the full list of devices and networks—it is a shorter report showing all the issues for the day. You can turn off the daily report feature in the Settings tab of the application.

Excessive Global Who-Is	Severity: High	A global who-is generates broadcast traffic from every device on the network. These should be very rare on a network. Any device in this list is sending more than 1 in a 30 minute period.
Time	Instance	Source MAC address
12/18/2020, 9:22:36 AM	-1	192.168.1.110 - 47808

Sometimes the instance number is **-1**. This means there were no packets in the capture that provided BACPro the instance number. The address of the device is always known.

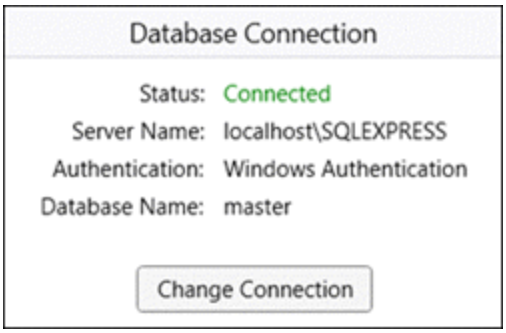
SMS Notifications

BACPro can send SMS notifications for many high and critical anomalies. To receive them, BACPro must have internet access. BACPro can send a maximum of 20 notifications per day per type. If the same type of issue keeps recurring, BACPro stops sending SMS notifications for it until the next day. You can configure which anomalies to send to which recipient. For the device failure notification, BACPro sends an SMS notification only if the device has been failed for 10 minutes or more. This avoids nuisance messages if a device restarts or fails to answer only a few requests. Notifications are sent using Twilio™, the cost of which is included in your subscription. The notifications originate from phone number (256) 743-8671. This is not a voice line—it is only for sending texts, so BACPro will not receive any texts back from it. The network is monitored, and SMS notifications are sent by the background windows service, so the application does not need to be running.



Database

BACPro uses a SQL Express™ database to store all configuration and analytic data. BACPro also creates a separate database for each PCAP file that is imported and also for each live connection. The UI can quickly switch between databases you are viewing data for. We recommend using SQL Express on the same computer where BACPro is installed for the best performance. However, if needed, you can configure a remote database from the Settings tab. BACPro supports only Windows Authentication mode for the database.



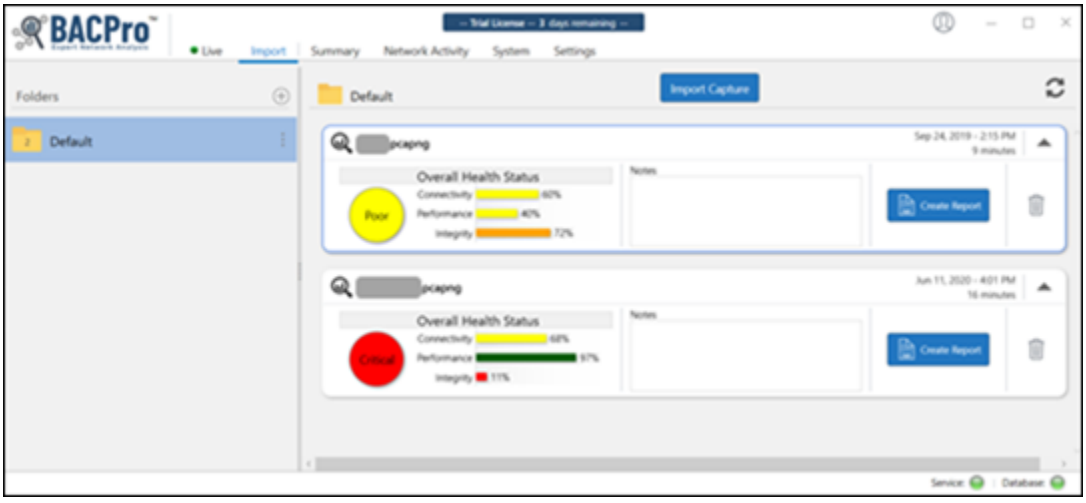
The free version of SQL Express can store a maximum of 10 GB of data. It is unlikely BACpro will need that much space. If you are importing a large number of capture files, you can delete older ones to create more space. For live connections, BACpro keeps two weeks of data by default. At midnight each night, BACpro purges data older than the specified period, which you can modify from the Settings tab. If you have the full SQL version, then space is not limited.

Live Mode

On startup, BACPro creates a list of all network interfaces that it finds. It listens to each network for a few seconds and tries to identify which networks currently have BACnet traffic. It moves BACnet networks to the top of the list. However, you can still connect to any other network, even if BACPro does not initially identify it as a BACnet network.

In live capture mode, BACpro generates network capture files for your network and stores them in the *\CaptureFiles* directory. It creates a new file every minute and puts only BACnet packets in the file. BACpro keeps all files for one week by default, and since this can use a lot of disk space, it is not recommended to keep more. Nevertheless, you can change this default in the Settings tab. These files are standard .pcap files, which can also be viewed in various network sniffing tools.

Importing Files



With BACPro, you can import an unlimited number of network capture files, and you can organize your captures in individual folders or place them all in a single folder. After the import completes, just press the Create Report button to generate the Network Report, or you can switch to the Summary tab to view anomalies. Each import is stored in its own database. When you are finished with a capture, you can delete it, and it will be removed from the database. A summary of the network health is displayed after the import completes. In the Description field, you can enter pertinent text to save with the import.

MSTP Imports

BACPro can analyze MSTP capture files for many common problems. The ideal configuration has consecutively numbered device addresses starting at 0. You should set the max masters property to the highest node on the network to reduce polling for masters. CRC errors indicate a serious problem with the network that must be fixed. CRC errors can be caused by improper wiring, duplicate addresses, or electrical noise.

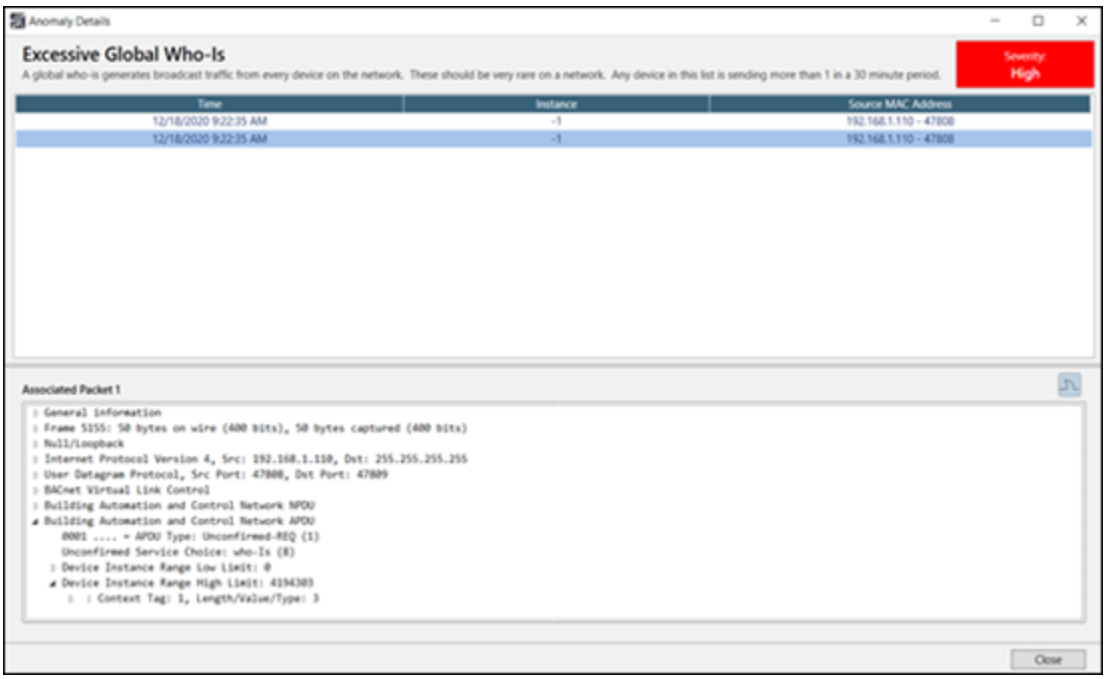
BACPro calculates the average token cycle time. Acceptable average cycle times depend on the number of devices. On average, cycle times less than 20 ms per device are considered excellent. Values of 20 – 160 ms reduce the performance score, and anything more than 160 ms per device is not performing well.

The standard deviation of the token cycle time is a measure of the variance in the token cycle times. The larger the value, the less predictable the performance of the network. A value larger than 500 ms reduces the performance score.

BACPro also monitors every token pass. A token not delivered to the same node as the previous token cycle will be counted as a Token Interruption, usually caused by a device that is too busy or failed. BACPro fails a device if it does not answer 3 Poll For Masters in a row, and then unfails a device when it replies again. BACpro is looking for file extension .cap for MSTP files.

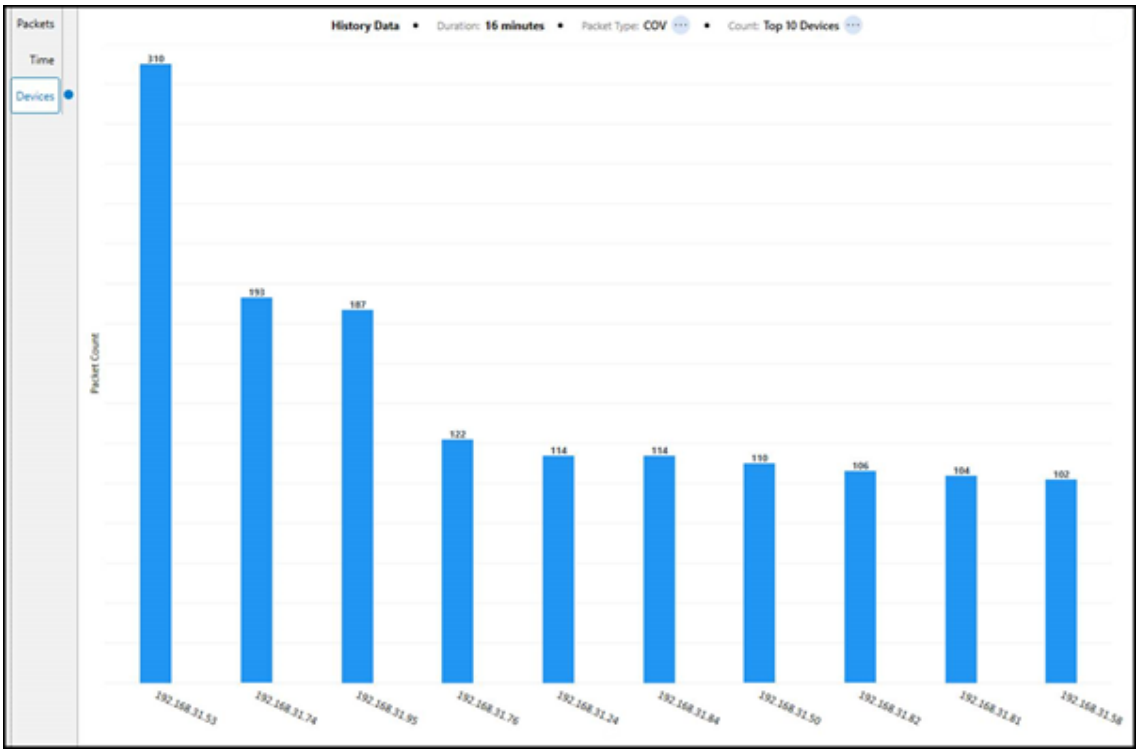
Summary Tab

The Summary screen provides the best overview of your system. The Anomaly section shows all discovered issues sorted by severity, and an instance count for each issue. Clicking an anomaly provides additional information, such as which device and network packets are involved in determining the anomaly. You can press the shark fin icon to view the packet directly in Wireshark®



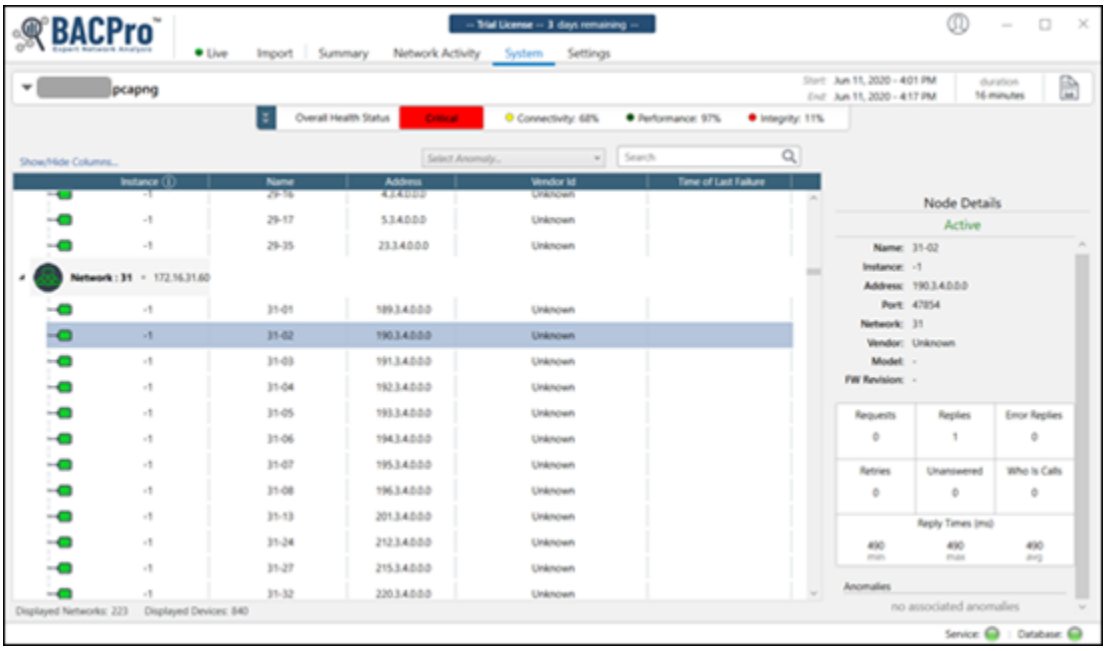
Network Activity Tab

The Network Activity tab displays real time graphs of your live network, or summary graphs of capture files. You can control the columns on the graph and switch between views of packet counts, time, and specific devices. For example, you can display a graph of the top 10 devices sending COVs.



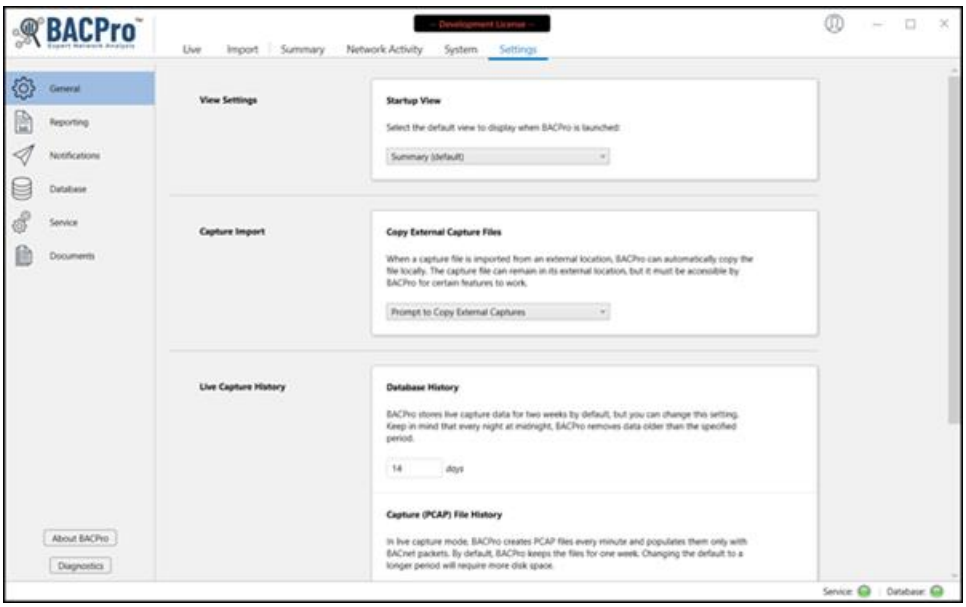
For live system monitoring, you can control the update display rate. The default is every 3 seconds. The graphs display the Device name and Instance number if found in the capture file. Otherwise, the address of the device displays.

System Tab



The System tab shows a hierarchy of all the BACnet® networks and devices found on the live network or capture file. Selecting a device shows several statistics for it in the Node Details section. On a live system, device failures dynamically update—showing a red or green icon. You can also filter the tree by anomaly type—for example, all devices with the excessive COV anomaly. At the top of some graphs, you will see a shark fin icon. Pressing this takes you to Wireshark and applies a filter that matches what the graph displayed.

Settings Tab



The Settings tab is where you configure SMS notifications and the database. You can also choose how long to keep live capture files and data in the database. If you have low hop count anomalies on your system, they can be false positives. If you determine that they are, you can disable this check on the live system so that it does not affect the health score. It remains enabled for processing offline capture files.

Troubleshooting

BACpro has three main components: the user interface, a windows service, and a database. When you open BACPro, the user interface displays the status of the windows service and database in the lower-right corner.

Service and Database Are Green

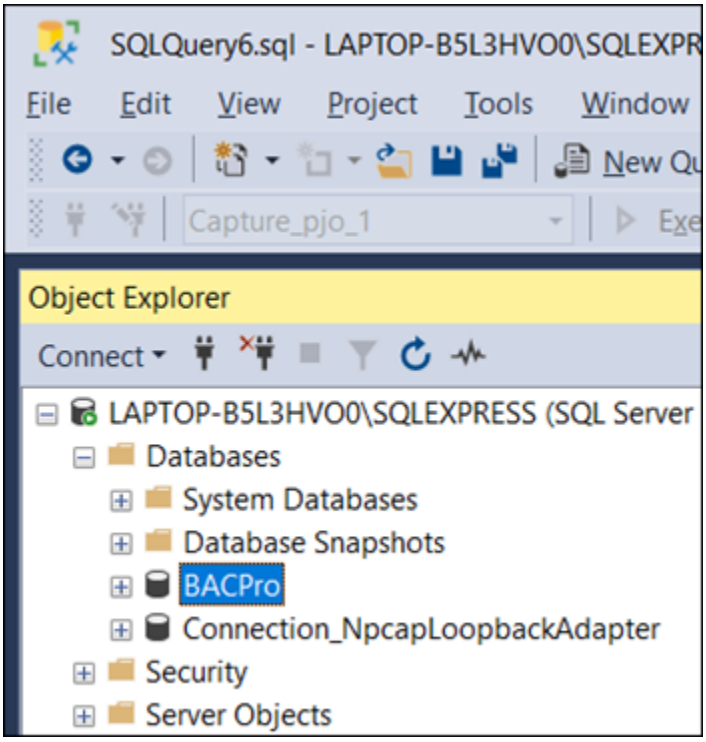
If both are green, everything is communicating correctly. The windows service must run under a user account that has access to the database.

Service Is Red

If the service is red, verify that the BACProService is running in the Windows Services app. It should be set to automatic and running under a user account with access to SQL.

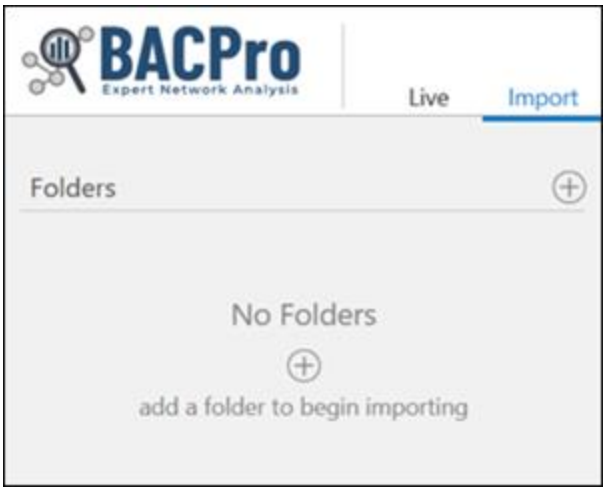
Database Is Red

If the database is red, you can download SSMS (SQL Server Management Studio) from the internet. Once it is installed and running, you will see a BACPro database and databases for your live connection or imported captures. If the database becomes corrupted, you can delete the BACPro database, and it will be recreated if you reboot or restart the BACProService.



No Folders when Selecting Import

When you try to import a wireshark capture, you may encounter a message indicating No Folders are available. This may be a result of the logged-on windows user not having SysAdmin rights in SQL. The user can be assigned SysAdmin rights in SQL using SSMS (SQL Server Management Studio).



If a report is not getting created or an import will not complete, you can refer to the BACProService.txt log file in the installation directory. It contains issues detected by BACPro. For example, if the same report is created twice, you could get a "file exists" error on the second report, such as the following:

8/16/2020 8:57:19 PM combit.ListLabel25.LL_Exporting_Exception: An error occurred during export (e.g. no access rights to destination path, file to be exported already exists and is write-protected).

If a capture file will not import for you, or you believe something is not reported correctly, email it to us at the following address, and we will debug it:

support@bacprotool.com

FAQ

Does BACPro work on a virtual computer?

Yes, you can install BACPro on a virtual computer. Many building workstations run in these environments.

Why do I sometimes see -1 for the Instance number?

BACPro can only show Instance numbers if it sees a packet on the wire that contains the Instance number. This is usually an I-am. Until the tool learns the Instance number it will show -1.

If I use live monitoring, can I import a capture at the same time?

Yes, you can import captures even when live monitoring. All imported captures create their own database. The live capture runs in parallel.

If my building control system has multiple workstations, do I need multiple copies of BACPro to do live monitoring?

Yes, BACPro watches a single workstation. You will need a copy for each one. You can contact us about a volume discount.

Does BACPro work with a BACnet/SC (Secure Connect) network?

Not currently. A BACnet/SC network uses encryption to keep any tool from viewing network traffic. The tradeoff for using Secure Connect is a loss in the ability to troubleshoot the network.

How much disk space is needed for BACPro?

Disk space is used to keep all network traffic for the period you have configured in the settings. By default, this is 7 days. It is recommended to have at least 20 GB of free space. Some space is also used for imported capture files and network reports.

Why does BACPro have to be installed on the same computer as the building automation workstation?

For live monitoring, BACPro listens on the same IP address and port as the workstation so that it can see all traffic to and from the workstation. If it is not on the same computer, it cannot see this traffic. This is not a requirement for offline file capture processing.

Why does the Norton/Symantec™ Virus scanner detect that BACProService.exe contains the Heur.AdvML.B virus?

Norton™ uses a heuristic algorithm that generates many false positives. We have asked them to whitelist our windows service. You can just exclude the BACPro installation directory from your scan. We are not aware of any other virus scanners flagging the service.

If I have an idea about how to improve BACPro, what should I do?

We would like to hear your ideas about making improvements to BACPro. Visit our website at https://bacprotool.com and send us a message from the *Support > Contact Us* menu.