



BACnet® Troubleshooting Simplified

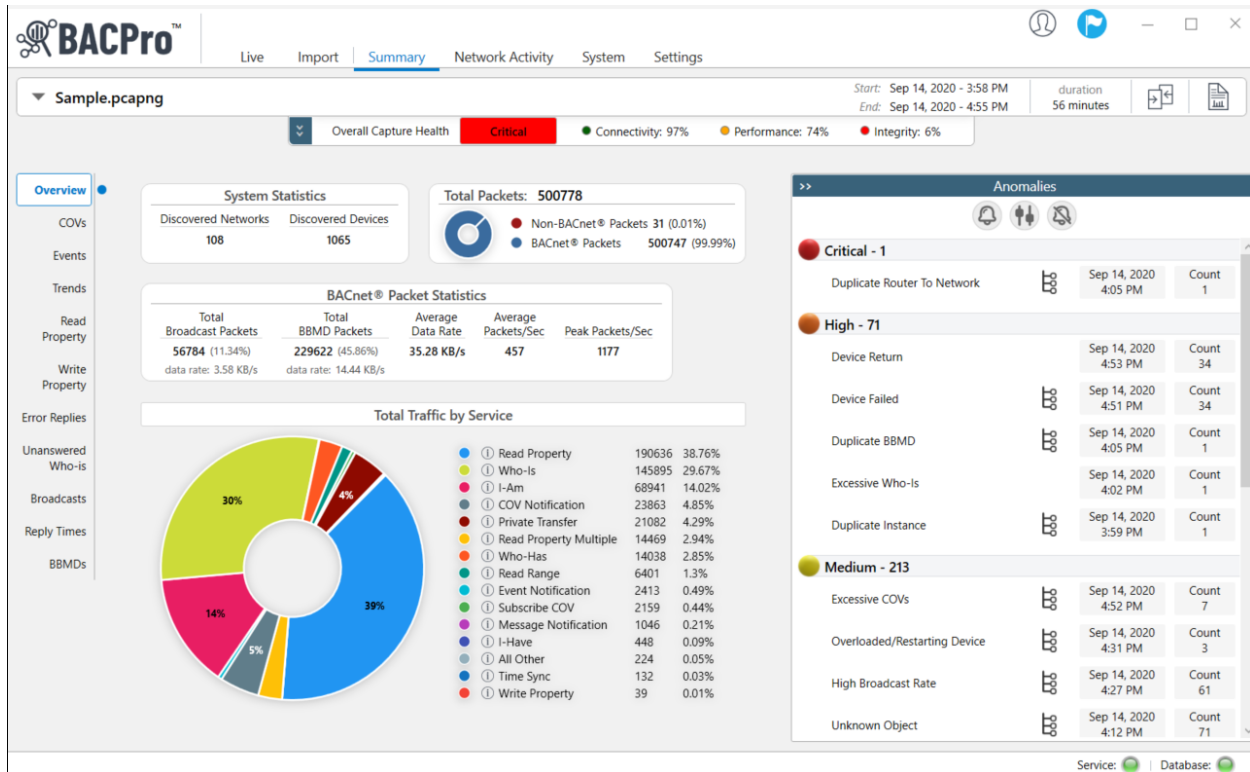
User Guide

Contents

- 1. Overview 4**
- 2. Operating Modes..... 4**
 - 2.1 Live Network Monitoring 4
 - 2.2 Offline Capture File Processing 5
 - 2.3 Continuous File Processing 5
- 3. Licensing..... 5**
 - 3.1 Online Monitoring 5
 - 3.2 Offline Capture Analysis..... 5
- 4. Getting Started 5**
- 5. Anomaly Severity Ratings and Types 7**
- 6. Health Scores..... 13**
- 7. Reports 16**
 - 7.1 Daily Report..... 16
 - 7.2 Network Report..... 16
 - 7.3 Summary Report..... 16
 - 7.4 Audit Report 16
- 8. Notifications 17**
 - 8.1 SMS 17
 - 8.2 Email 17
- 9. About the Database..... 18**
- 10. Capture Comparison..... 19**
- 11. BACPro User Interface 22**
 - 11.1 Tour Guide..... 22
 - 11.2 Live Tab 23
 - 11.3 Import Tab..... 31
 - 11.4 Summary Tab 33
 - 11.5 Network Activity Tab 36
 - 11.6 System Tab 39
 - 11.7 Settings Tab..... 41
- 12. Suppressing False Positives 46**

13. Reset Daily Anomalies	48
14. Reused Networks and Instance Numbers	48
15. BACnet Secure Connect	49
16. Troubleshooting	49
16.1 Service and Database Lights Are Green	49
16.2 Service Light Is Red	49
16.3 Database Light Is Red.....	50
16.4 Full Database Reset	50
16.5 Log Files.....	51
16.6 Reports Fail to Create the PDF File	51
16.7 No Folders When Selecting Import.....	51
16.8 SMTP Error When Using Outlook	52
Appendix A: FAQ.....	54
Appendix B: Release Notes	56

1. 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 can take 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 continuous analysis of every BACnet packet on your network—and then highlights the problem areas.

2. Operating Modes

BACPro has three operating modes: live monitoring, offline capture file processing, and Wireshark continuous file processing.

2.1 Live Network 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.

2.2 Offline Capture File Processing

BACPro can import any BACnet IPv4, IPv6, unencrypted BACnet SC, ARCNET, 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.

2.3 Continuous File Processing

Continuous file processing using Wireshark is a good option for a job site that does not have BACPro installed on the same computer as the building control workstation. You can install Wireshark on the workstation and have it write capture data to a file share directory that BACPro can also access. BACPro will monitor the directory and process those files like a live connection would, but with a small delay since Wireshark writes files at a user-defined rate. For additional information, see *Section 11.1*.

3. Licensing

BACPro has two licensing models: online monitoring, and offline capture analysis.

3.1 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, you will need a license for each of them. A license is keyed to a computer.

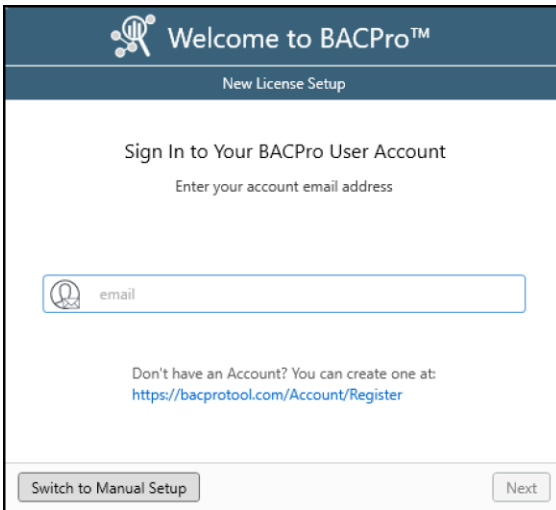
3.2 Offline Capture Analysis

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 who troubleshoot BACnet issues, please purchase a license for each user.

4. Getting Started

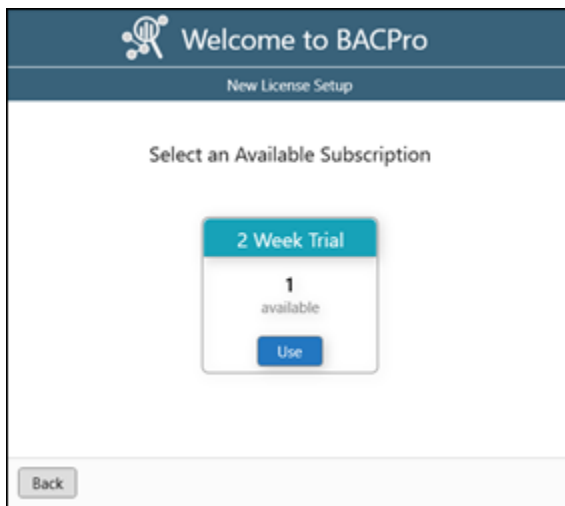
Once BACPro is installed, you need to set up the license—either a two-week trial license, or your paid subscription license.

1. In the **New License Setup** dialog box, enter the email address you created at bacprotool.com, and then click **Next**.



2. Enter the password you created at bacprotool.com, and then click **Sign In**.

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 displays here. Once you have a valid license, you can import captures or set up a live connection.



5. Anomaly Severity Ratings and Types

BACPro monitors your network for approximately 65 different types of network problems, which are assigned a severity rating. 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 indicate a false positive—and therefore a low network issue.

Anomaly Severity Ratings	
Severity Rating	Meaning
Info	A network issue with a very low impact: <ul style="list-style-type: none"> • A device with several UDP retries. • A new device was found on the network
Low	A network issue with a low impact, mostly isolated to a device: <ul style="list-style-type: none"> • A device that is overloaded or that needs a longer APDU timeout. • A device with unexpected error codes.
Medium	A network issue with a medium impact. Can affect more than just a single device: <ul style="list-style-type: none"> • Substantial amounts of COV or Event traffic • A router reporting an error.
High	A network issue with a high impact to the workstation or network: <ul style="list-style-type: none"> • 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 a severe impact to the system: <ul style="list-style-type: none"> • A workstation or network shows no communication. • A configuration issue that must be addressed immediately.

Anomaly Types		
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.
Reused Network Number	Info	A reused network number was found but appears to be on an isolated network. This is not flagged as a critical problem as long as no devices are being talked to by both of the routers.

Anomaly Types		
Type	Severity	Description
Reused Instance Number	Info	A reused instance number was found but appears to be on an isolated network. This is not flagged as a problem as long as no other devices are being talked to by both of them.
Device Database Downloaded	Info	A device had its database downloaded. If this occurs repeatedly, it might mean that the device is cold starting due to internal errors.
Firmware Revision Changed	Info	A device is reporting an updated firmware revision. If there is unexpected behavior, it could be related to a firmware change.
UTC Offset Changed	Info	A device's UTC Offset was changed, which could affect scheduled items in the device.
Daily Decrease in Connectivity	Info	The daily average for a live capture falls by 5 percent. Notifications are supported. Percentages can be configured the Settings tab > Anomalies menu.
Daily Decrease in Performance	Info	The daily average for a live capture falls by 5 percent. Notifications are supported. Percentages can be configured in the Settings tab > Anomalies menu.
Daily Decrease in Integrity	Info	The daily average for a live capture falls by 5 percent. Notifications are supported. Percentages can be configured the Settings tab > Anomalies menu.
Questionable Trend Data Date	Info	A device is reporting a time stamp for trend data before the year 2000 or in the future. This can indicate that the internal clock is inaccurate. Incorrect dates can cause problems for applications like metering that rely on trend data.
Off-Node Trending	Info	A device is trending a property on another device. This can be ok if the remote device does not support trend logs, but it will generate more network traffic. Whenever possible, limit off-node trending and use local trend logs instead.
Duplicate Time Master	Info	If two different servers set the time on the same device, the time can jump around and possibly cause scheduling problems.
Suppressed Failed Router	Info	A device failed but is suppressed because of maintenance or other expected failure.
Suppressed Return Device	Info	A device returned but is suppressed because of maintenance or other expected failure.
Suppressed Duplicate Router	Info	A duplicate router to network was found and suppressed because there are more than one isolated networks on the same UDP port.
Suppressed Duplicate Instance	Info	A duplicate Instance was found and suppressed because there are more than one isolated networks on the same UDP port.
Suppressed Failed Device	Info	An unresponsive router was found and suppressed because of maintenance or other expected failure.

Anomaly Types		
Type	Severity	Description
Short Capture	Info	There is less than 10 minutes of capture data. It may show some issues, but it is not long enough for a meaningful health score. We recommend using 30 minutes or more of data.
Invalid Packet	Info	There was a problem decoding this packet. It may be invalid, proprietary, or a mistake in decoding logic.
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.
MSTP Scanning too high	Low	The highest MSTP address should have the max device address set to itself to prevent unnecessary polling for master packets on the network
MSTP Nonconsecutive nodes	Low	MSTP devices should start at 0 and be addressed consecutively to minimize 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.
Value Out of Range	Low	A value out of range error usually indicates a write failed. A piece of equipment might not be controlled correctly. Check Schedules, Command Objects, or Programs for invalid values.
Error Reading Object List	Low	During discovery of devices on a network, a device has returned an error reading the object list. The device must answer the request.
Unreachable Destination	Low	A packet was sent to an unreachable destination. This can be a misconfigured BBMD address/port, or the remote node has failed. Look at the contained packet's destination address and verify that it is correct.
Questionable Time Sync	Low	A TimeSync request is setting the time to a value that is a minute or more off from the computer clock where this capture was taken. Verify that the time is correct at the device where the request originated.
Object List read error	Low	A device has returned an error reading the object list. This could cause problems with discovery operations.
Timeout Error	Medium	A timeout error or abort code was returned for a request. A device might need a longer APDU timeout.
Unknown Object	Medium	An unknown object error indicates an inconsistency problem between a field device and a workstation. For example, a write property might be trying to command an object that is not in the device.
Invalid Data Type	Medium	An invalid data type error usually indicates a write failed. For example, a write property might be sending an enum data type instead of unsigned for a multistate object.

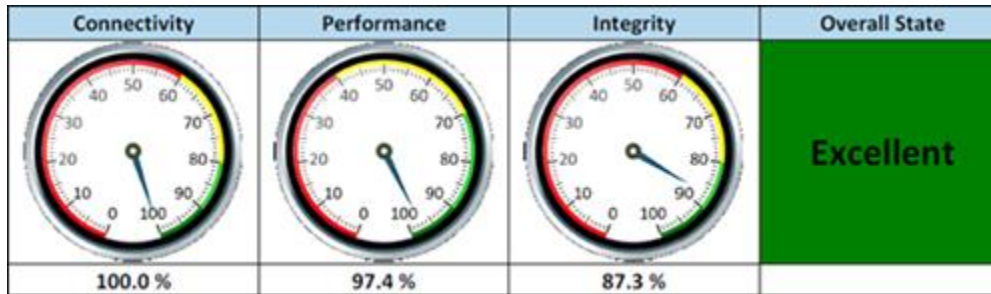
Unresponsive Device	Medium	There are devices sending Who-is repeatedly looking for a node that is not answering I-am. This is a common problem with Notification Classes having a recipient that is not on the network anymore. This leads to extra broadcast traffic on the network and causes devices with limited processing power to have to handle these broadcast requests. Clean up notification class recipient lists so that only active devices are 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 Broadcast Rate	Medium	A high rate of broadcasts puts a burden on all devices that must process the messages. Reduce COV broadcasts, remove failed node scans to non-existent devices, and fix failed devices to improve the health of the network. Those in this list had several of the same type in a minute.
High COV Rate	Medium	A device is sending COVs too frequently. Any COV rate of more than 30 per minute 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.
High WP Rate	Medium	A device receives 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, 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.
Device Restarting	Medium	A device has failed to answer requests and was considered failed by other nodes. It quickly answers a Who-is with an I-am. The device could be warm-starting or overloaded.
Excessive Error Replies	Medium	More than 20 percent of all requests return error replies. Investigate if some of these errors are avoidable.
High Text Message Rate	Medium	A device sends more than 20 text messages a minute. This may need attention.
Excessive Global Who-Is Router	Medium	A global Who-Is Router generates broadcast traffic from every router on the network. Devices in this anomaly list are sending more than 3 Who-Is requests in a 60-minute period. This should be a rare occurrence on a network.
Unknown Node Failed	Medium	Unresponsive devices are those that do not answer a targeted who-is. They could be failed or they could be caused by misconfigured objects like notification classes. Those in this list have not answered at least 3 Who-Is requests.
Large Network Number	Medium	There are more than 150 networks detected. Many devices have a fixed network table size and will generate more traffic when the table size is exceeded. We recommend having less than 150 networks.
Excessive Error Reply	Medium	More than 20 percent of requests have error replies. See the error summary table for which devices are contributing to this and if the errors are avoidable.
Duplicate Instance	High	Two devices are reporting the same instance number to a device. 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/Returned	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. A device has returned from failure.
Global Who-Is	High	A device sends excessive Global Who-is requests, which are used periodically to discover devices. BACPro flags them if there is more than 3 every 60 minutes. They cause all devices on the network to answer I-am and can overload devices that need to process all the broadcast communications.

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.
Excessive Who-is	High	Who-is traffic on the network exceeds 30 percent. This is likely misconfigured notification classes looking for nodes that are no longer present.
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. A network has returned from failure. Traffic on the local network has returned.
Workstation Failure/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. A workstation return from failure has been detected.
Duplicate Router to Network	Critical	Two routers that answer I-am Router to Network for the same network number to a single device is a severe configuration error. A device should only know 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 could be bad wiring, duplicate nodes, or noise.
MSTP data CRC errors	Critical	The data portion of the MSTP packet is failing CRC checks. This could be bad wiring, wrong packet length, duplicate nodes, or noise.

6. 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 <i>Good</i> 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. Therefore, the score on the screen may vary from the score shown in a report.

The Integrity score is affected by the anomaly types in the following table. There is a penalty per occurrence of an anomaly, up to a maximum penalty amount.

How the Integrity Score Is Affected		
Type	Penalty per Occurrence	Maximum Penalty
MSTP Scanning too high	5%	10%
MSTP Nonconsecutive nodes	5%	5%
MSTP Master Poll Frequency	5%	5%
Timeout Error	.05%	15%
Unknown Failed Node	.50%	5%
Reject Message to Network	1%	10%
High Broadcast Rate	0.1%	25%
High COV Rate	0.1%	10%
High WP Rate	0.1%	10%
High RP Rate	0.1%	10%
High Alarm Rate	0.1%	10%
Preempted by Higher Priority Task	0.1%	10%
Value Out of Range	.10%	5%
Out of Memory	1%	5%
Unknown Object	.1%	5%
Invalid Data Type	.1%	5%
Incorrect Password	1%	5%
Buffer Overflow	1%	5%
Excessive Error Replies	5%	5%
Duplicate Instance	5%	40%
Unreachable Destination	.5%	5%
Global Who-Is	1%	15%
Low Hop Count / Circular Network	5%	40%
Duplicate MAC address	5%	40%
Duplicate BBMD	10%	40%
Failed Router	5%	20%
Excessive Broadcasts	15%	15%

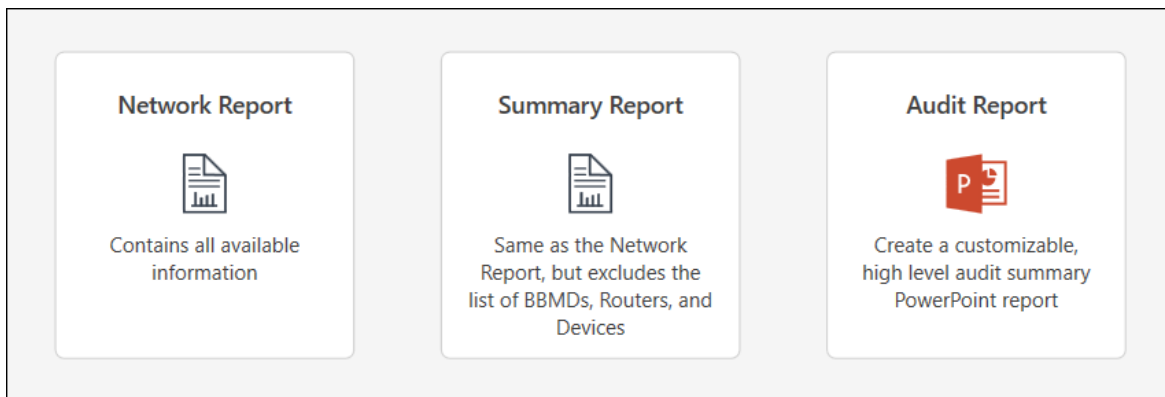
How the Integrity Score Is Affected		
Type	Penalty per Occurrence	Maximum Penalty
Excessive Who-is	10-30%	30%
Complete Network Failure/Return	40%	40%
Workstation Failure or Return	40%	40%
Duplicate Router to Network	10%	60%
MSTP header CRC errors	60%	60%
MSTP data CRC errors	20%	60%

7. Reports

BACPro automatically provides a daily report (a Summary Report) for live monitoring while also allowing you to manually generate additional reports for any capture. For the on-demand reports, you can choose whether you want a full Network Report, a shorter Summary Report, or a high-level Audit Report created in PowerPoint.



Sometimes the instance number displays as Unknown. This means there were no packets in the capture that provided the instance number to BACPro. The address of the device is always known.



7.1 Daily Report

Creates a PDF

The Daily Report covers the previous 24 hours of traffic for live connections, and contains health scores, traffic summaries, and a list of devices. It also shows all anomalies found and provides guidance about how to correct them. For live monitoring, the report is placed in the `\DailyReports` directory where BACPro is installed. You can turn off the daily report feature in the Settings tab of the application.

7.2 Network Report

Creates a PDF

The Network Report contains all available information in the capture.

7.3 Summary Report

Creates a PDF

The Summary Report is a shorter version of the Network Report—it excludes the list of BBMDs, Routers, and Devices while still showing all the issues for the day.

7.4 Audit Report

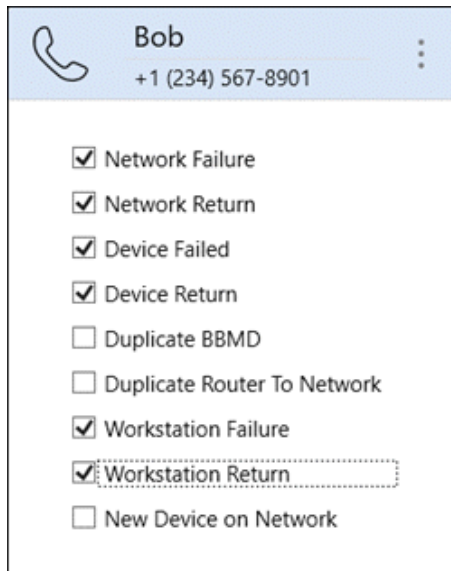
Creates a PowerPoint Presentation

The Audit Report allows you to create a customizable, high-level report in PowerPoint.

8. Notifications

BACPro can send SMS and email notifications for many high and critical anomalies (Settings > Notifications). To receive messages, 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 notifications for it until the next day. You can configure which anomalies to send to which recipient, as shown below. For the device failure notification, BACPro sends a 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.

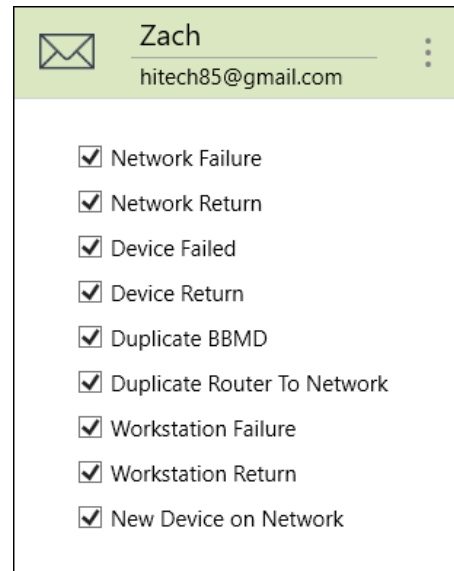
SMS Notification Recipient



Bob
+1 (234) 567-8901

- Network Failure
- Network Return
- Device Failed
- Device Return
- Duplicate BBMD
- Duplicate Router To Network
- Workstation Failure
- Workstation Return
- New Device on Network

Email Notification Recipient



Zach
hitech85@gmail.com

- Network Failure
- Network Return
- Device Failed
- Device Return
- Duplicate BBMD
- Duplicate Router To Network
- Workstation Failure
- Workstation Return
- New Device on Network

8.1 SMS

SMS 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.

8.2 Email

If internet access is available, you can send daily reports and email notifications by using the BACPro Mail Server, or you can configure an SMTP mail server if internet access is not available.

9. About the 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 for each live connection. The UI can quickly switch between databases you are viewing. Even if your site only forwards packets to perform offline imports, you need a SQL database for every BACPro installation. If needed, you can configure a remote database from the Settings tab.

BACPro supports both Windows and SQL Server Authentication. When selecting SQL Server Authentication, you can require SQL server user credentials every time BACPro is started.

Windows Authentication	SQL Authentication
<p>Database Connection</p> <p>Status: Connected</p> <p>Server Name: localhost\SQLEXPRESS</p> <p>Authentication: Windows Authentication</p> <p><input type="button" value="Configure"/></p>	<p>Database Connection</p> <p>Status: Connected</p> <p>Server Name: ██████████</p> <p>Authentication: SQL Authentication (Credentials Required at Startup)</p> <p>User Name: BP_User</p> <p><input type="button" value="Configure"/></p>

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 many capture files, you can delete older ones to create more space. For live connections, BACPro keeps two weeks of data by default, and at midnight each night purges data older than the specified period. You can modify the period from the Settings tab. If you have the full SQL version, then space is not limited.

10. Capture Comparison

You can select a maximum of three captures for side-by-side comparison. Reasons to compare captures include:

- Finding and correcting issues found during a site audit, and then comparing the original capture with a new capture to see if you have improved your customer's network.
- Creating captures of the same job at regular intervals to see how the site has changed.

You can find the Compare icon in the following BACPro tabs: Live, Import, Summary, Network Activity, and System.

The following example from the Summary tab shows two captures selected for comparison:

The screenshot displays the BACPro Summary tab interface. At the top, the capture name 'Sample_2.pcapng' is highlighted with a red box, and a red arrow points to a 'Compare' icon in the top right corner. Below the capture name, the overall capture health is shown as 'Critical' with a red bar. The interface includes various statistics and charts, such as 'System Statistics' (108 Discovered Networks, 1065 Discovered Devices), 'BACnet® Packet Statistics' (Total Broadcast Packets: 56784, Total BBMD Packets: 229622), and 'Total Traffic by Service' (a donut chart showing 30%, 14%, and 39% segments). On the right, an 'Anomalies' panel lists several critical and high-priority events. At the bottom, a dark grey bar titled 'Captures Selected to be Compared (2/3)' contains two capture selection boxes: 'capture: Sample_1.pcapng' and 'capture: Sample_2.pcapng'. A red arrow points from the 'Compare' icon in the top right to the 'Compare' button in this bottom bar. A 'Cancel' button is also present.

Magnified View

This magnified view shows the 'Captures Selected to be Compared (2/3)' bar in detail. It features two white boxes with blue 'X' close buttons. The first box contains the text 'capture: Sample_1.pcapng' and the second box contains 'capture: Sample_2.pcapng'. To the right of these boxes are two buttons: a blue 'Compare' button and a grey 'Cancel' button.

Capture Comparison		
Note: Compared captures are listed from oldest to newest based on the end time.		
	Sample_1.pcapng	Sample_2.pcapng
Start Time	Sep 14, 2020 - 3:58 PM	Nov 03, 2020 - 9:58 AM
End Time	Sep 14, 2020 - 4:55 PM	Nov 03, 2020 - 10:55 AM
Duration	56 minutes	56 minutes
Health Data		
Health	● Critical	● Good
Connectivity	97%	97%
Performance	74%	82% ↑
Integrity	6%	72% ↑
System Data		
Network Count	108	109 ↑
Device Count	1064	1066 ↑
Networks - New	-	Network: 7772 Address: 10.167.7.72
Networks - Removed	-	none
Devices - New	-	All devices under Network: 7772 Net=8200 - 5 - 47808
Devices - Removed	-	Net=0 - 10.160.25.37 - 47808
Anomalies <small>(click anomaly for details)</small>		
Critical	Duplicate Router To Network (1)	<u>Removed</u> Duplicate Router To Network (1)
High	Device Failed (34) Device Return (34) Duplicate BBMD (1) Duplicate Instance (1) Excessive Who-Is (1)	Device Failed (34) Device Return (32) ↓ Excessive Who-Is (1) <u>Removed</u> Duplicate BBMD (1) Duplicate Instance (1)

Capture comparison continued on next page . . .

Capture comparison continued from previous page . . .

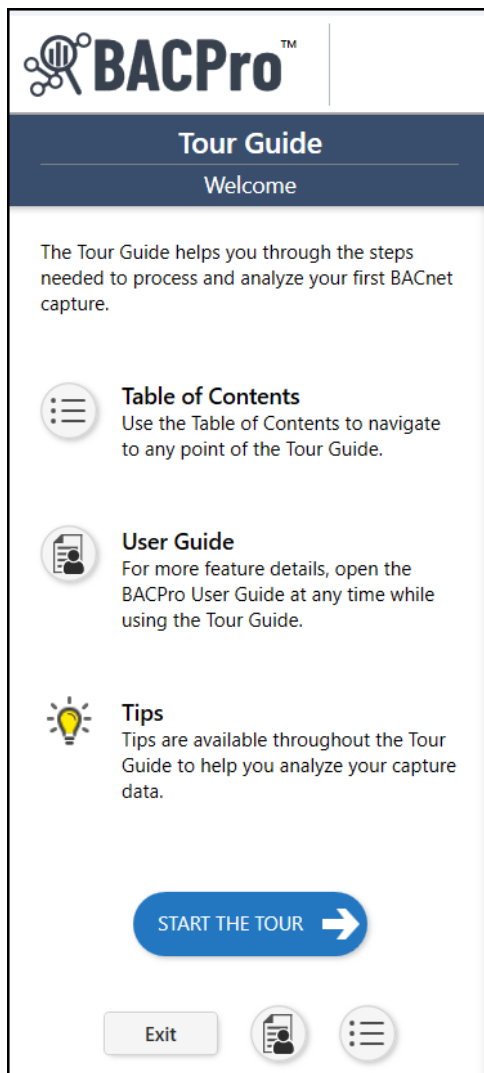
Medium	Excessive COVs (7) Excessive Events (3) High Broadcast Rate (35) High Text Message Rate (1) Incorrect Password Error (1) Overloaded/Restarting Device (3) Timeout Error (30) Unknown Object (9) Unresponsive Device (33)	Excessive COVs (6) ↓ Excessive Events (2) ↓ High Broadcast Rate (34) ↓ High Text Message Rate (1) Incorrect Password Error (1) Overloaded/Restarting Device (3) Timeout Error (29) ↓ Unknown Object (8) ↓ Unresponsive Device (32) ↓ New Preempted By Higher Priority Task (1) Reject Message to Network (1)
Low	Unanswered Request (55)	Unanswered Request (62) ↑
Information	Retries (198)	Retries (195) ↓
Network Traffic		
COV Notification	4.85% (23863)	4.85% (23498)
Event Notification	0.49% (2413)	0.5% (2405) ↑
I-Am	14.02% (68941)	14.06% (68109) ↑
I-Have	0.09% (448)	0.09% (442)
Message Notification	0.21% (1046)	0.22% (1046) ↑
Private Transfer	4.29% (21082)	4.3% (20830) ↑
Read Property	38.76% (190606)	38.7% (187486) ↓
Read Property Multiple	2.94% (14468)	2.93% (14208) ↓
Read Range	1.3% (6401)	1.3% (6285)
Subscribe COV	0.44% (2159)	0.44% (2127)
Time Sync	0.03% (132)	0.03% (131)
Who-Has	2.85% (14038)	2.86% (13864) ↑
Who-Is	29.67% (145895)	29.67% (143714)
Write Property	0.01% (39)	0.01% (39)
All Other	0.05% (224)	0.05% (222)

11. BACPro User Interface

The BACPro User Interface consists of six tabs (views) that are intuitive and easy to use—Live, Import, Summary, Network Activity, System, and Settings—as well as an innovative Tour Guide to help you process and analyze your first BACnet capture.

11.1 Tour Guide

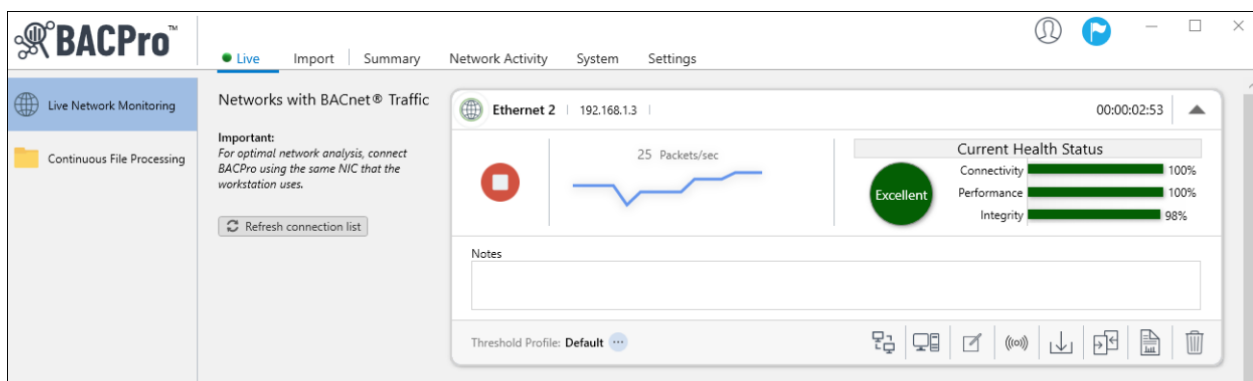
To start processing and analyzing a BACnet capture, click the Tour Guide icon in the upper-right corner of BACPro, and then click **Start the Tour**.



11.2 Live Tab

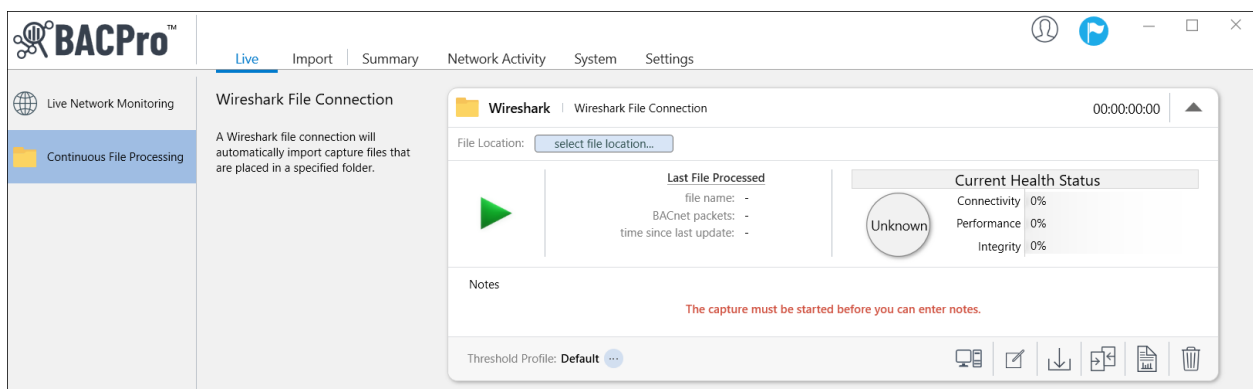
For live network monitoring, BACPro listens on the same IP address and port (uses the same network interface card) as the workstation so that it can see all traffic to and from the workstation. This provides optimal network analysis. If BACPro is not on the same computer or same NIC, it cannot see this traffic. This is not a requirement for offline continuous file processing. 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, and then moves BACnet networks to the top of the list. You can still connect to any other network, however, even if BACPro does not initially identify it as a BACnet network.

11.2.1 Live Network Monitoring



In live network monitoring mode, BACPro generates standard *.pcapng* or *.pcap* 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. Since this can use a lot of disk space (large networks generate approximately 4 GB of data per day), we do not recommend keeping them for longer periods.

11.2.2 Continuous File Processing



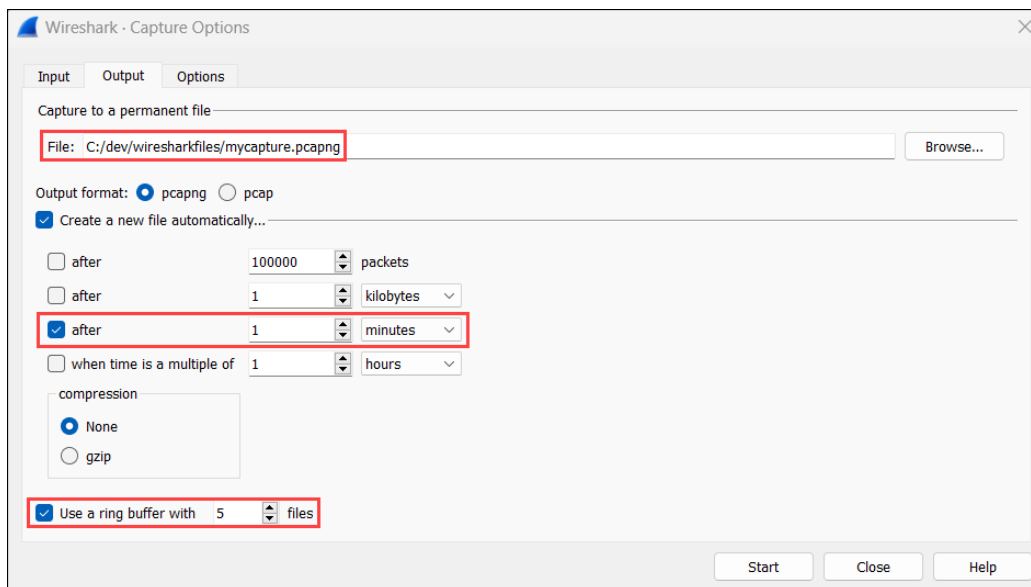
Continuous file processing is a good option for a job site that does not have BACPro installed on the same computer as the building control workstation. You can install Wireshark on the workstation and have it write capture data to a file share directory that BACPro can also access. BACPro will monitor the

directory and process the files like a live connection would, but with a small delay since Wireshark writes files at a user-defined rate (every 20 – 60 seconds will keep files from becoming too large and ensure that they are imported into BACPro frequently).

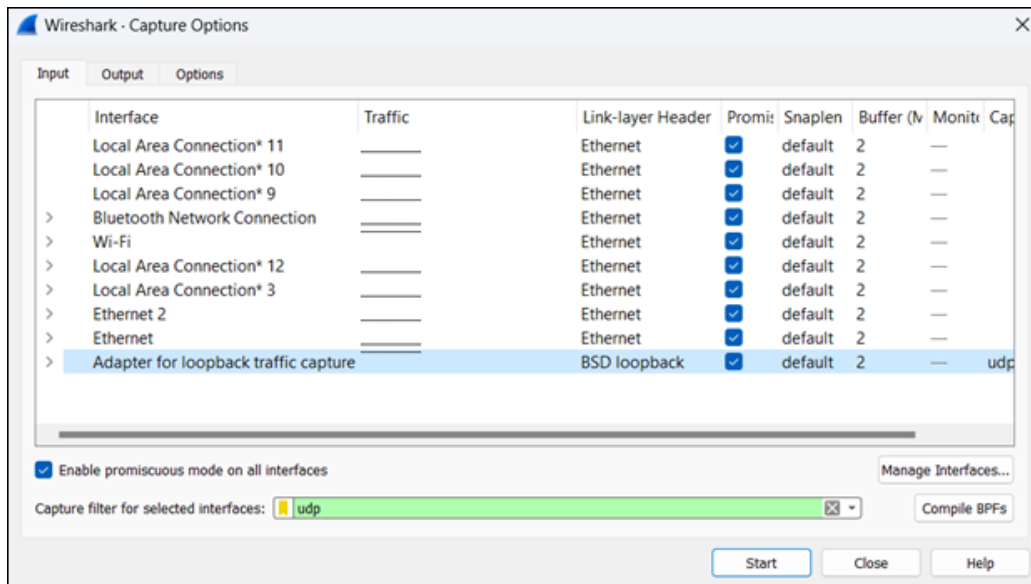
BACPro can process any *.pcapng* or *.pcap* files added to the directory you have setup. We recommend using Wireshark or Tshark (a command line version of Wireshark) or any tool or vendor system that can export *.pcapng*, or *.pcap* files to a specific location. Both Wireshark and Tshark can be setup to delete old files. However, Tshark can also be setup with third-party software such as NNMS or AlwaysUp to run as a service so that it automatically restarts data collection after a reboot.

To use Wireshark, do the following:

1. Open Wireshark.
2. From the **Capture** menu, select **Options**.
3. In the **Output** tab, set the directory you want to write the files to and provide a file name ending in *.pcapng*, or *.pcap*.
4. Check **Create a new file automatically**, and select a range of **20 – 60 seconds**.
5. Set the ring buffer to **5** files.



- On the **Input** tab, set a filter such as **udp** to reduce the amount of traffic written.



- Click **Start**.

To use Tshark, complete the following steps:

- Add Wireshark to your computer's path statement, or provide the full path when you create a batch file.
- Run **Tshark -D** to see the list of NIC IDs, which will look similar to the following example:
\Device\NPF_{A95DAAF9-B5B1-49CB-8B85-57D6FC5814E4} (Ethernet)
- Create a **.bat** file and enter the following command in the file:
Tshark -i \Device\NPF_{my NIC ID here} -f udp -b interval:30 -b files:5 -w c:\mypath\myfile.pcapng
- (Optional)* Setup your Tshark batch file to run as a service by using the instructions provided with NNMS or AlwaysUp.
- Test your batch file to ensure that it writes files where you specify and that memory is not growing on the process over time.

In BACPro, complete the following steps:

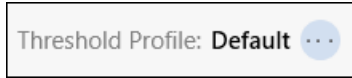
- Select the Wireshark live connection.
- Press the **select file location** button and choose a directory that Wireshark will write capture files to.
- Press **Start Data Capture**.
- Once the live Wireshark capture starts, you can view, analyze, and run a report on the data in the Summary, Network Activity, and System views.

11.2.3 Additional Live Capture Features

Additional features are available from the Live Connection Menu.



Anomaly Threshold Profile



You can change the anomaly threshold profile anytime for live captures, even if the live capture is running.

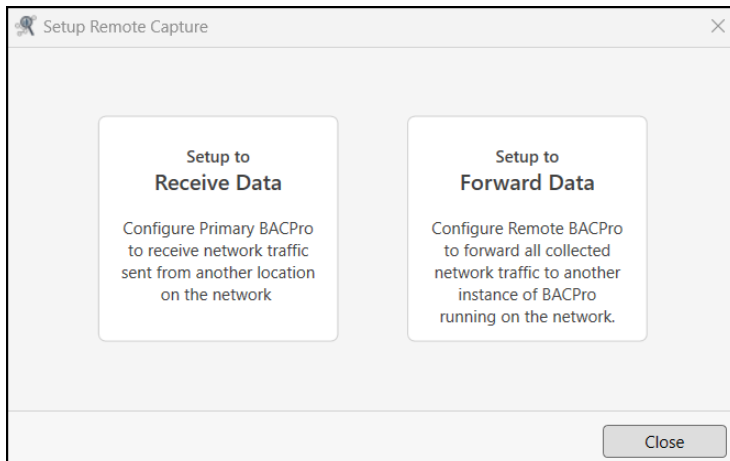
Setup Remote Connection



Does not apply to Wireshark Continuous File Processing

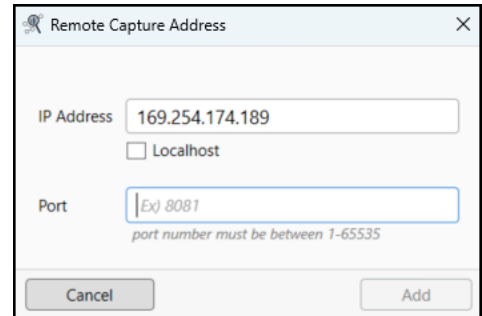
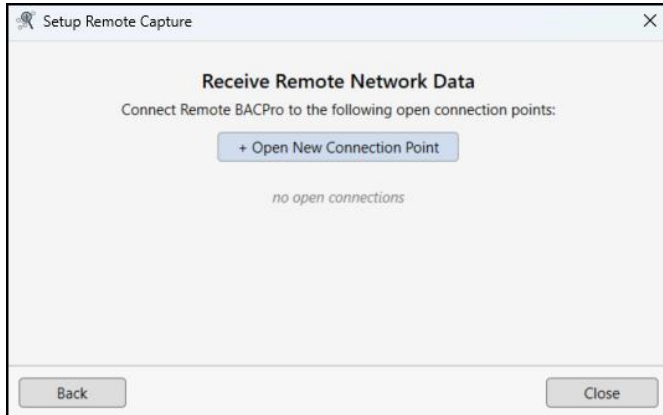
For distributed systems with two or more computers, each with their own BACnet network, you can send all the live capture traffic from a Remote BACPro installation to the computer designated as the Primary BACpro. A BACPro license/subscription is required for each computer in the system, and each computer needs SQL installed for local imports. The Primary BACPro, however, contains the capture database, which allows you to generate one report for all BACPro installations in the system. From the Live tab, expand your network adapter, and then press the **Setup Remote Capture** button.

Select one of the following options, and then complete the information in the corresponding dialog box.

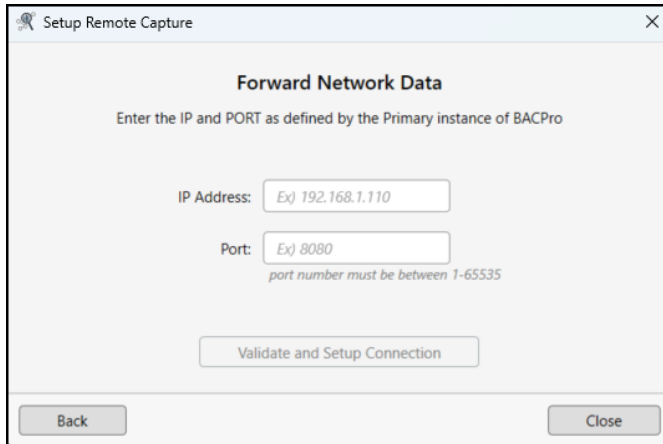


In the following dialog boxes, the specified TCP port needs to be open for incoming traffic on the Primary BACPro, and also open for outgoing traffic on the Remote BACPro. The Remote BACpro will not display any data in Summary mode.

Setup to Receive Data



Setup to Forward Data



Set Workstation



BACPro automatically tries to determine the network workstation by selecting the node that communicates the most. If BACPro selects the wrong node, or you are getting false-positive workstation failure anomalies, you can set the correct workstation node or disable the Workstation Failure anomaly check by selecting the Set Workstation button. You can then provide the workstation network number, the IP address, and the UDP port. If this node stops communicating for more than one minute, BACPro generates a workstation failure alarm.

Configure Workstation

BACPro tries to determine the Workstation on the network, which can take up to 3 minutes after a Live capture is started. If the Workstation is not defined correctly, you will receive incorrect Workstation anomalies.

Do not check for Workstation
This option will prevent the 'Workstation Failure' anomaly from being flagged.

-- Workstation has not been defined --

Workstation Network #

Workstation IP Address

Workstation Port

Customize Device Names



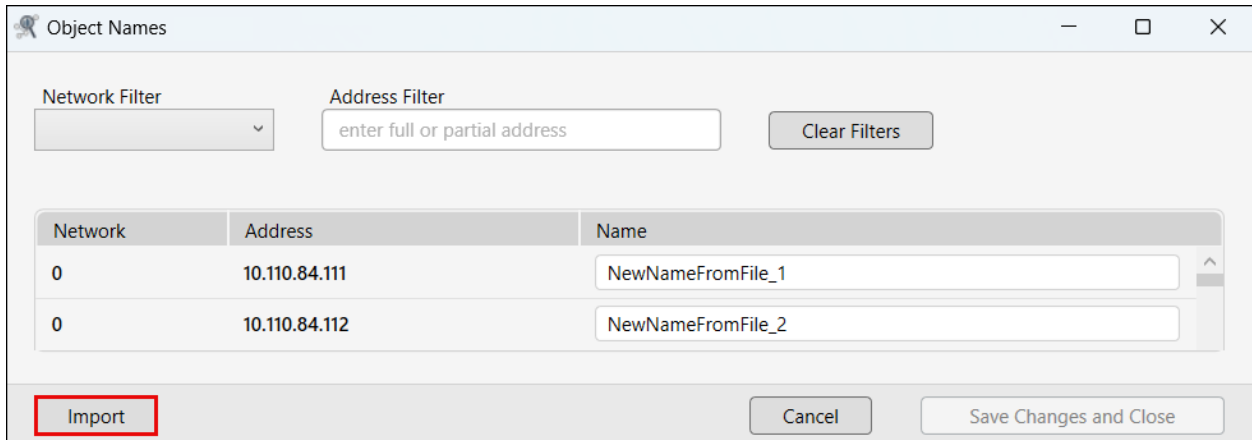
You can add custom names to devices in the network to help you quickly identify them.

Object Names

Network Filter: Address Filter:

Network	Address	Name
3	100.0.0.0	<input type="text" value="Unique Device Name"/>
3	101.0.0.0	<input type="text" value="BACnetDev_101"/>
3	102.0.0.0	<input type="text" value="BACnetDev_102"/>
3	103.0.0.0	<input type="text" value="BACnetDev_103"/>
3	104.0.0.0	<input type="text" value="BACnetDev_104"/>

You can also import object names from a .csv or .txt file.



Send Who-Is Broadcast



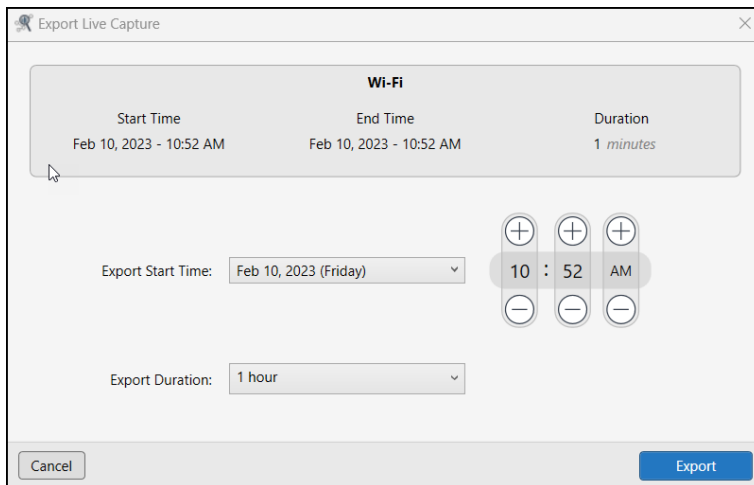
Does not apply to Wireshark Continuous File Processing

Sending a Who-Is broadcast can help BACPro discover all the devices on the network. To avoid unnecessary network traffic, use this feature sparingly.

Export Live Capture Data



BACPro saves all capture data in one-minute capture files, but it can also consolidate them into a larger file for analysis in Wireshark. Pressing the Export Live Capture Data button opens the Export Live Capture dialog box, where you can select an export start time and duration to merge files into a single capture file.



Compare



You can select a maximum of three captures for side-by-side comparison. Comparing captures can help you find and correct issues found during a site audit. You can then compare the original capture with a new capture to see if you have improved your customer's network. You can also create captures of the same job at regular intervals to see how the site has changed. For more information, see *Section 10*.

Create Report



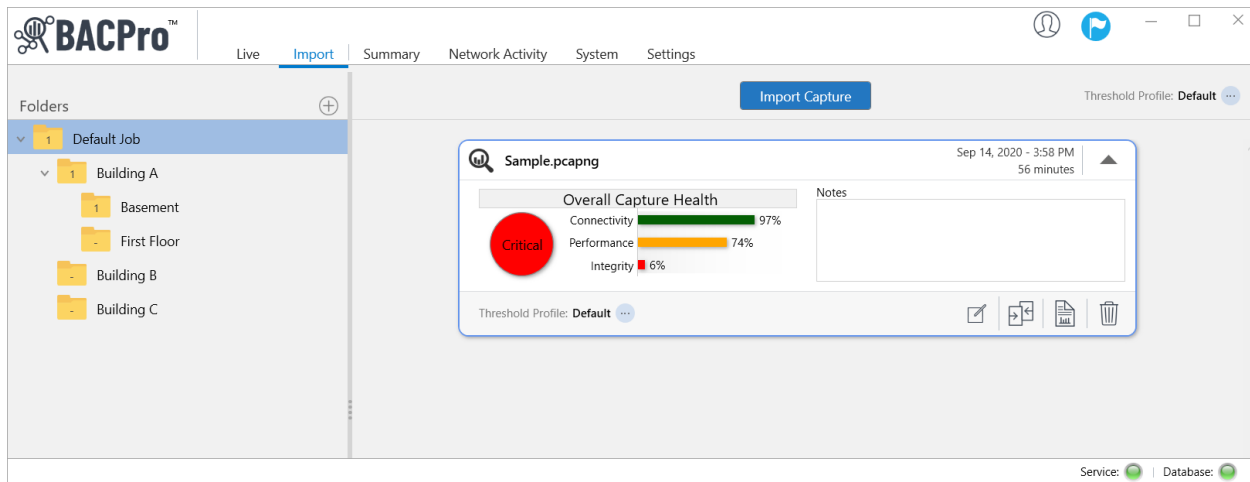
BACPro automatically provides a daily report (a Summary Report) for live monitoring while also allowing you to manually generate additional reports for any capture. For the on-demand reports, you can choose whether you want a full Network Report, a shorter Summary Report, or a high-level Audit Report created in PowerPoint. For more information, see *Section 7*.

Delete Capture



You can delete one or multiple captures.

11.3 Import Tab



In the Import tab, you can import an unlimited number of network capture files. The multi-level folder feature allows you to create a folder hierarchy for your site and import captures directly into any selected folder. Once captures are imported, you can move them individually from one folder to another by dragging them from the capture viewing area. To simultaneously move all captures to a different folder, you can right-click a folder and select Move all Captures.

After an import completes, you can generate a report using the Create Report button, 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 Notes field, you can enter pertinent text to save with the import and display with a report.

11.3.1 Anomaly Threshold Profile

The anomaly threshold profile selected at the folder level is the profile used when new captures are imported. You can change the threshold profile for a capture after it is imported, but if you do, you must reimport the capture.

11.3.2 MSTP Imports

BACPro can also 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.

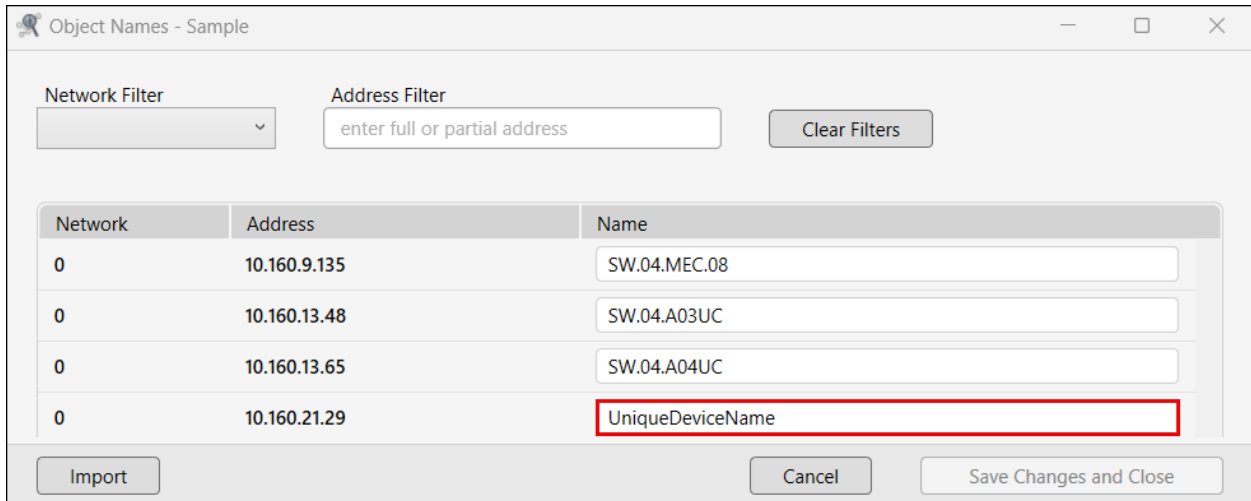
The standard deviation of the token cycle time is a measure of the variance in the token cycle times. The larger the value, the less predictable the performance of the network. A value larger than 500 ms reduces the performance score.

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 un-fails a device when it replies again. BACPro is looking for file extension .cap for MSTP files.

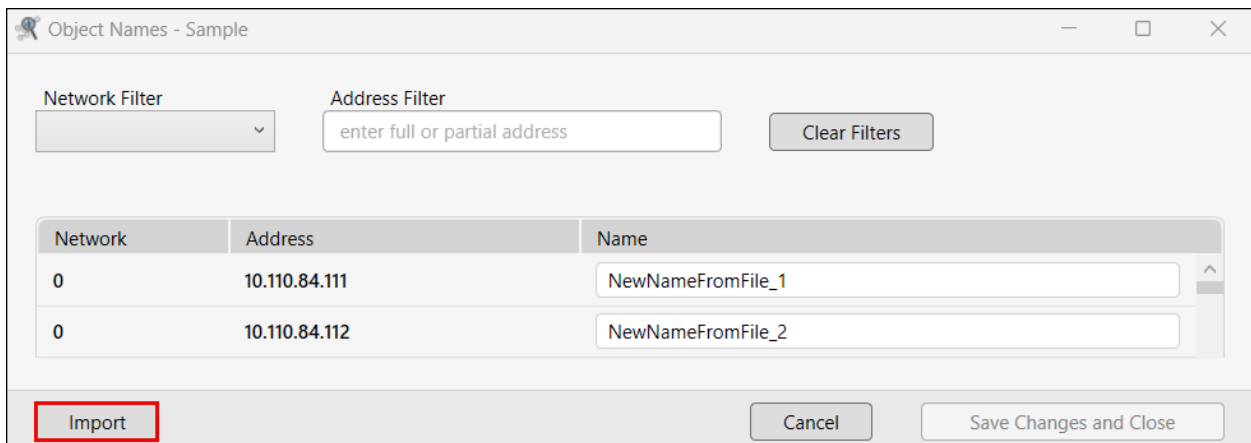
Customize Device Names



You can add custom names to devices in the network to help you quickly identify them.



You can also import object names from a .csv or .txt file.



11.4 Summary Tab

The screenshot displays the BACPro Summary tab for a capture named 'Sample.pcapng'. The interface includes a navigation menu on the left with options like Overview, COVs, Events, Trends, Read Property, Write Property, Error Replies, Unanswered Who-is, Broadcasts, Reply Times, and BBMDs. The main area is divided into several sections:

- System Statistics:** Shows 108 Discovered Networks and 1065 Discovered Devices.
- Total Packets:** 500778 total, with 31 (0.01%) Non-BACnet Packets and 500747 (99.99%) BACnet Packets.
- BACnet® Packet Statistics:**

Total Broadcast Packets	Total BBMD Packets	Average Data Rate	Average Packets/Sec	Peak Packets/Sec
56784 (11.34%)	229622 (45.86%)	35.28 KB/s	457	1177
- Total Traffic by Service:** A donut chart showing the distribution of traffic across various services, with Read Property being the largest at 39%.
- Anomalies:** A list of detected issues sorted by severity:
 - Critical - 1:** Duplicate Router To Network (Sep 14, 2020 4:05 PM, Count 1).
 - High - 71:** Device Return (34), Device Failed (34), Duplicate BBMD (1), Excessive Who-is (1), Duplicate Instance (1).
 - Medium - 213:** Excessive COVs (7), Overloaded/Restarting Device (3), High Broadcast Rate (61), Unknown Object (71).

At the bottom right, there are status indicators for Service (green) and Database (green).

The Summary tab 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 click the shark fin icon to view the packet directly in Wireshark®.

The 'Anomaly Details' window shows the following information for a 'Device Failed' event with a severity of High:

A device failure has been detected. It is not answering a Who-is or poll for master but was communicating previously.

Time	Instance	MAC Address	Type	Comment
9/14/2020 4:03:11 PM	70307	Net=0 - 10.160.32.75 - 47808	Failure	
9/14/2020 4:04:32 PM	7162	Net=7100 - 62 - 47808	Failure	
9/14/2020 4:05:11 PM	9209	Net=9200 - 9 - 47808	Failure	
9/14/2020 4:05:37 PM	70307	Net=0 - 10.160.32.75 - 47808	Failure	
9/14/2020 4:05:41 PM	7160	Net=7100 - 60 - 47808	Failure	
9/14/2020 4:08:55 PM	70307	Net=0 - 10.160.32.75 - 47808	Failure	
9/14/2020 4:09:11 PM	7162	Net=7100 - 62 - 47808	Failure	
9/14/2020 4:09:36 PM	7161	Net=7100 - 61 - 47808	Failure	
9/14/2020 4:12:03 PM	70307	Net=0 - 10.160.32.75 - 47808	Failure	
9/14/2020 4:14:24 PM	70307	Net=0 - 10.160.32.75 - 47808	Failure	

Associated Packet 1

```

P General Information
P Frame 65027: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
P Ethernet II, Src: Cisco_15:16:41 (e4:c7:22:15:16:41), Dst: VMware_8a:d5:67 (00:50:56:8a:d5:67)
P Internet Protocol Version 4, Src: 10.160.25.24, Dst: 10.110.84.111
P User Datagram Protocol, Src Port: 47808, Dst Port: 47808
P BACnet Virtual Link Control
P Building Automation and Control Network NPDU
P Building Automation and Control Network APDU
  
```

A 'Close' button is located at the bottom right of the window.

On a live monitoring system, some anomalies have a “mark as fixed” link that you can click as you correct issues that BACPro found. Once you click “mark as fixed,” BACPro removes the penalty from the integrity score for that day. If the error is detected again the next day, the anomaly returns, letting you know it was not fixed.

Excessive Events						Severity
High Event traffic puts a burden on workstations or devices that must process each message. Try adjusting alarm limits or deadband values. These have more than 10 events in a minute.						
Time	Source Instance	Object ID	Source Address	Destination Address	Fixed	
4/1/2021 8:20:42 PM	1016	BinaryValue - 1	Net=444 - 248.3.0.0 - 47809	Net=0 - 192.168.1.110 - 47808	mark as fixed	
4/1/2021 8:20:42 PM	1017	BinaryValue - 1	Net=444 - 249.3.0.0 - 47809	Net=0 - 192.168.1.110 - 47808	mark as fixed	

On the left side of the Summary tab, you can view objects generating COVs, Events, Trend collections, Read Properties, Write Properties, Broadcasts, and BBMDs. A drop-down menu is available in the title bar that allows you to select the number of viewable objects or to export data to a CSV file.

You can also:

- View Chatty Devices and click on them to see more detail.
- View all the Reply Times, Error Replies, and Unanswered Who-Is communications on the network. These Views can help you remove excessive traffic on the network.
Note: BACPro starts tracking only when 5 occurrences of a service type exist. For example, if there are only 4 COVs for Point A, BACPro does not keep the point in the database.
- Export table data to a CSV file by right-clicking in the table and selecting **Export to CSV**.

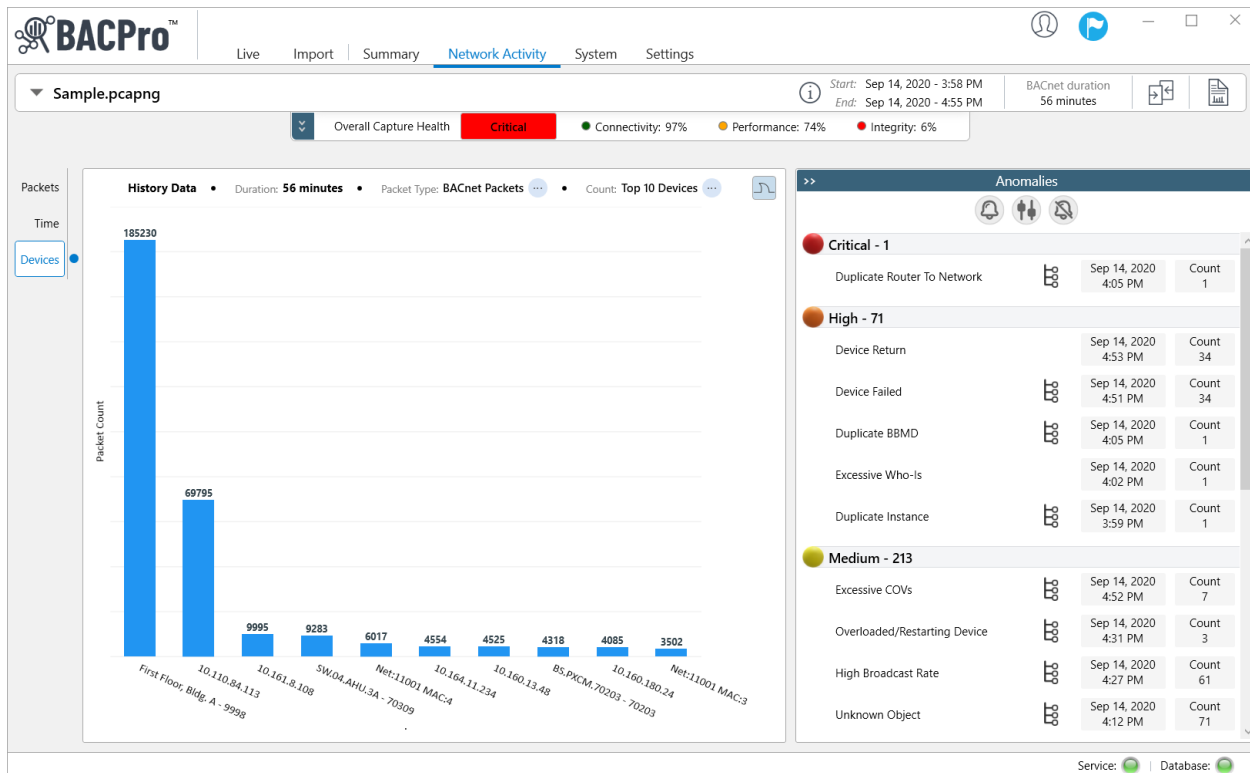
Overview	Chatty Devices Click row to see more details										
	Instance	Address	COV (Objects)	Event (Objects)	Trend (Objects)	Reads (Objects)	Writes (Objects)	Errors	Broadcasts	Anomalies	Total
COVs	71001	10.160.180.24	0	0	86	0	0	0	3	3	92
Events	9998	10.110.84.111	0	0	0	33	0	1	25	7	66
Trends	70121	10.161.8.108	36	0	0	0	0	0	1	2	39
Read Property	70201	10.160.21.40	2	0	0	20	0	0	2	0	24
Write Property	70120	10.160.13.48	4	0	0	14	0	0	1	2	21
Write Property	71002	10.160.180.25	0	0	13	0	0	0	3	3	19
Error Replies	701212	addr: 52 - net: 121	4	0	0	10	0	0	0	0	14
Error Replies	701213	addr: 53 - net: 121	4	0	0	10	0	0	0	0	14
Unanswered Who-is	70309	10.160.25.37 SW.04.AHU.3A	0	2	1	4	0	0	3	4	14
Broadcasts	70104	10.164.11.234	8	0	0	3	0	0	1	1	13
Broadcasts	701214	addr: 54 - net: 121	5	0	0	0	0	0	3	0	8
Reply Times	70307	10.160.32.75	0	0	0	0	0	1	7	0	8
BBMDs	10200	10.160.27.92	0	0	0	0	0	0	4	3	7
Chatty Devices	70101	10.161.52.31	0	0	0	0	0	2	3	2	7
Chatty Devices	710011	addr: 1 - net: 11001	6	0	0	0	0	0	0	0	6
Chatty Devices	70123	10.161.8.109	2	0	0	0	0	1	1	2	6

11.4.1 Tool Tips for Error Replies

You can view tool tips for Error Replies by hovering over a row. If an anomaly is associated with the error, BACPro displays that as well.

Write Property Error Replies ● Unanswered Who-is Broadcasts	0	10.240.58.232 POL908_FF7352	Error	Unknown Property	33	<div style="border: 1px solid black; padding: 5px;"> <p style="text-align: center;">Error : Timeout</p> <hr/> <p style="text-align: center;">Associated Anomaly: Timeout Error</p> <hr/> <p>Potential Problems</p> <ul style="list-style-type: none"> • A device did not answer a request in the allotted APDU time. <p>Suggested Solution</p> <ul style="list-style-type: none"> • Try increasing the APDU timeout value for the device. </div>
	0	10.167.6.78 N143_IP_Gateway_BACnet_KNX	Error	Unknown Property	23	
	0	10.110.84.113	Error	Timeout	18	
	35679	0.0.0.1.139.98	Error	Unknown Object	16	
	0	10.160.25.26 SW.04.A03UC	Error	Unknown Property	14	

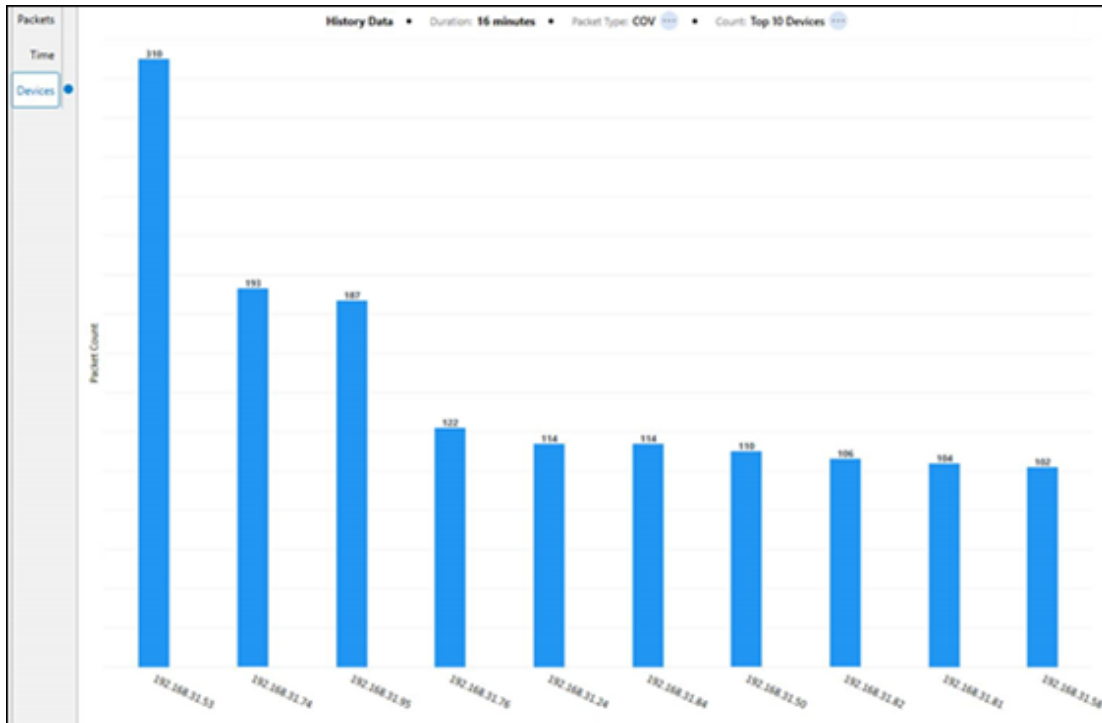
11.5 Network Activity Tab



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 (*see next page*).

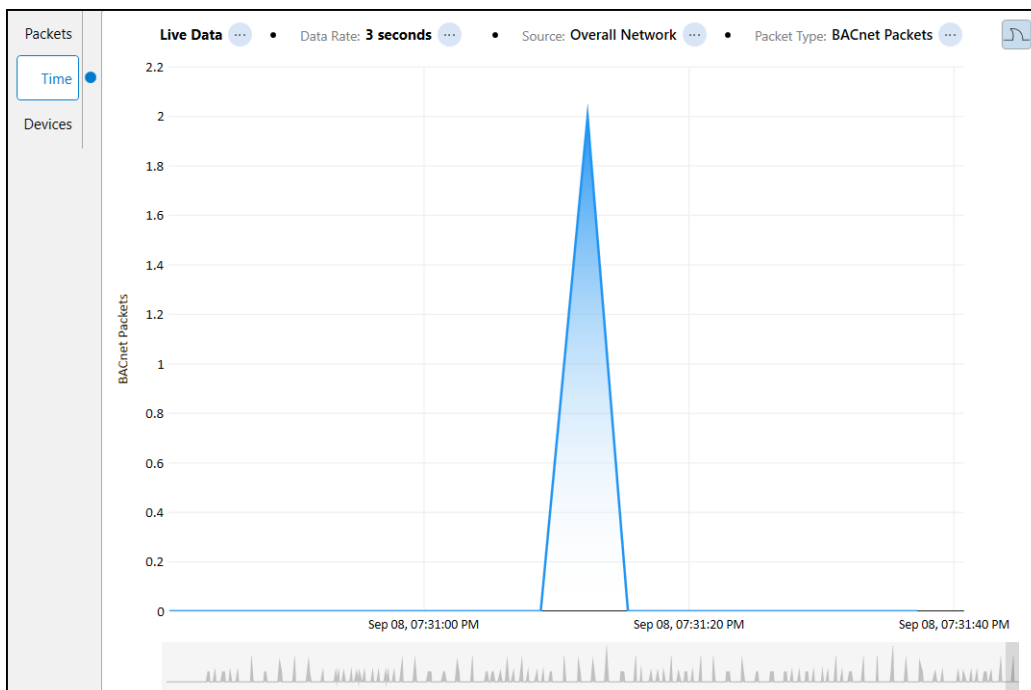
The graphs display the Device name and Instance number if found in the capture file. Otherwise, the address of the device displays.

Top 10 Devices Sending COVs

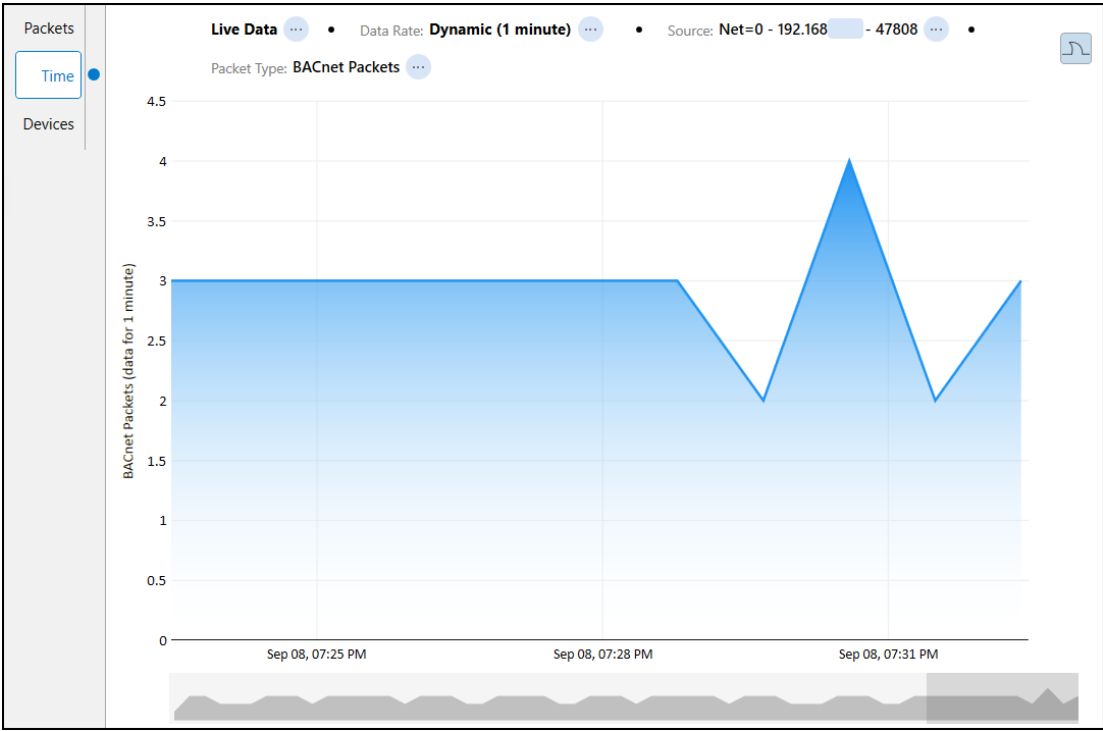


11.5.1 Data Rates

For live system monitoring, BACPro records overall network traffic every 3 seconds. The values displayed in the following graph represent all the data recorded during the time period.



When a single device is selected, the data rate is dynamic: BACPro determines and records the rate once every 1 – 30 minutes per device based on the number of devices in the system. The values displayed in the following graph represent all the data recorded during the time period.



11.6 System Tab

The screenshot displays the BACPro System tab interface. At the top, there are navigation tabs: Live, Import, Summary, Network Activity, System (selected), and Settings. Below the navigation, there's a status bar showing 'Overall Capture Health' as Critical, with Connectivity at 97%, Performance at 74%, and Integrity at 6%. A search bar and a 'Select Anomaly...' dropdown are also present. The main area features a tree view of networks and devices. A table lists devices for Network 1001 (10.160.180.24) with columns for Instance, Name, Address, Avg Reply Time, and Vendor id. The Node Details panel on the right shows statistics for an active device (Instance: 1100101, Address: 1, Port: 47808).

Instance	Name	Address	Avg Reply Time	Vendor id
1100101		1	336.66	Unknown
1100102		2	373.85	Unknown
1100103		3	400.87	Unknown
1100104		4	427.47	Unknown
1100105		5	462.44	Unknown
1100106		6	502.29	Unknown
1100107		7	554.18	Unknown
1100108		8	572.64	Unknown
1100109		9	218.8	Unknown
1100110		10	324.05	Unknown
1100111		11	297.16	Unknown
1100112		12	363.25	Unknown
1100113		13	403.67	Unknown
1100114		14	444.16	Unknown
1100115		15	606.69	Unknown

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 update dynamically—showing a red or green icon.

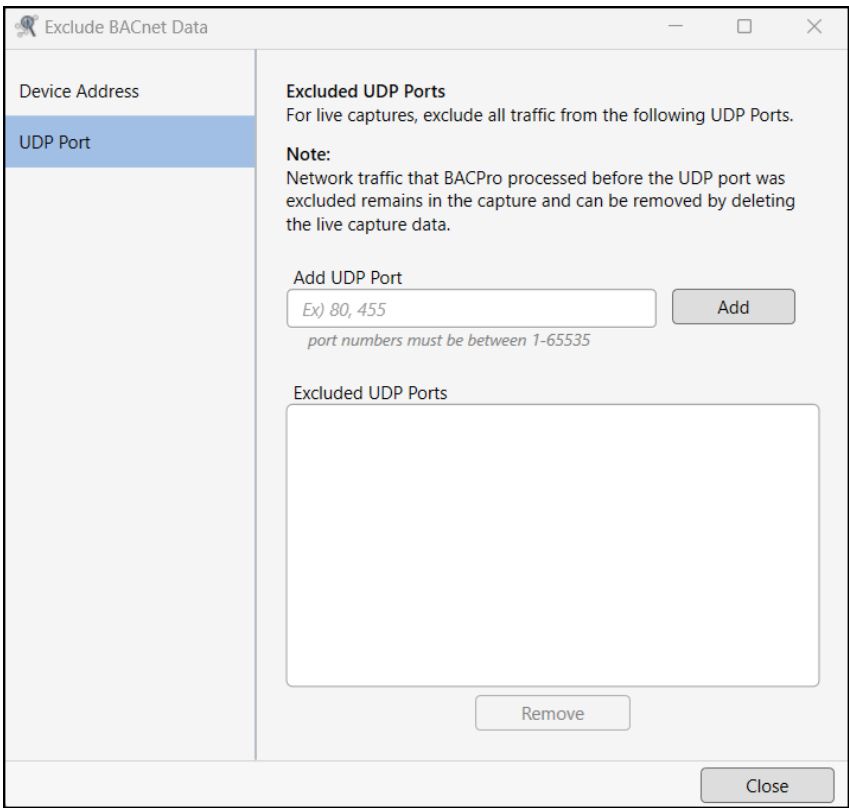
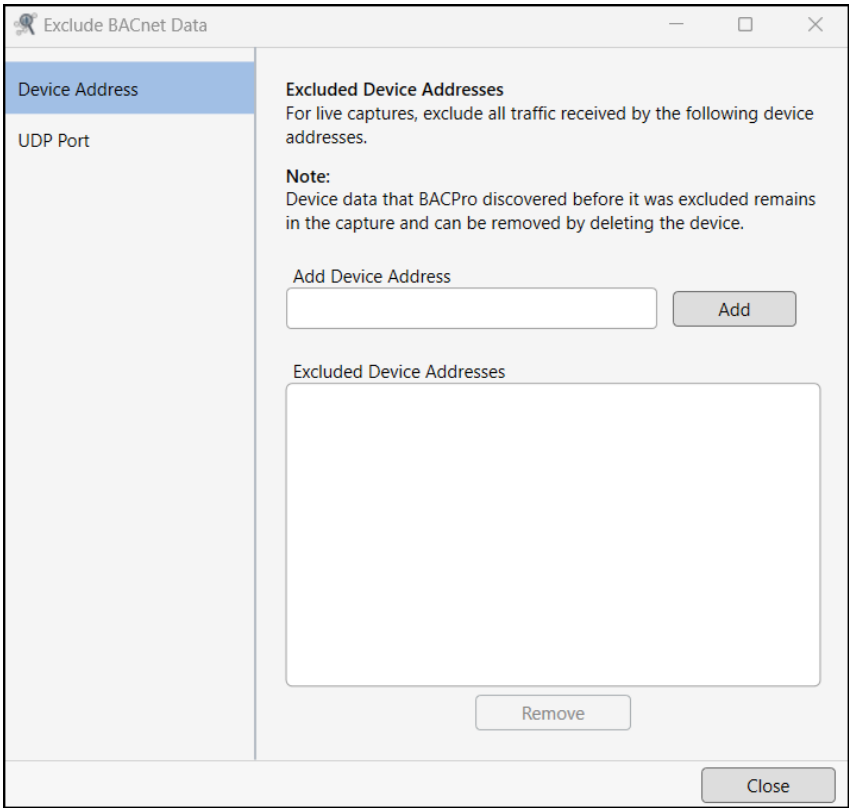
You can also:

- 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 opens Wireshark and applies a filter that matches what the graph displays.
- Export data to a .CSV file by right-clicking in the table and selecting 'Export to CSV.'
- Delete a BACnet device from a live capture database.

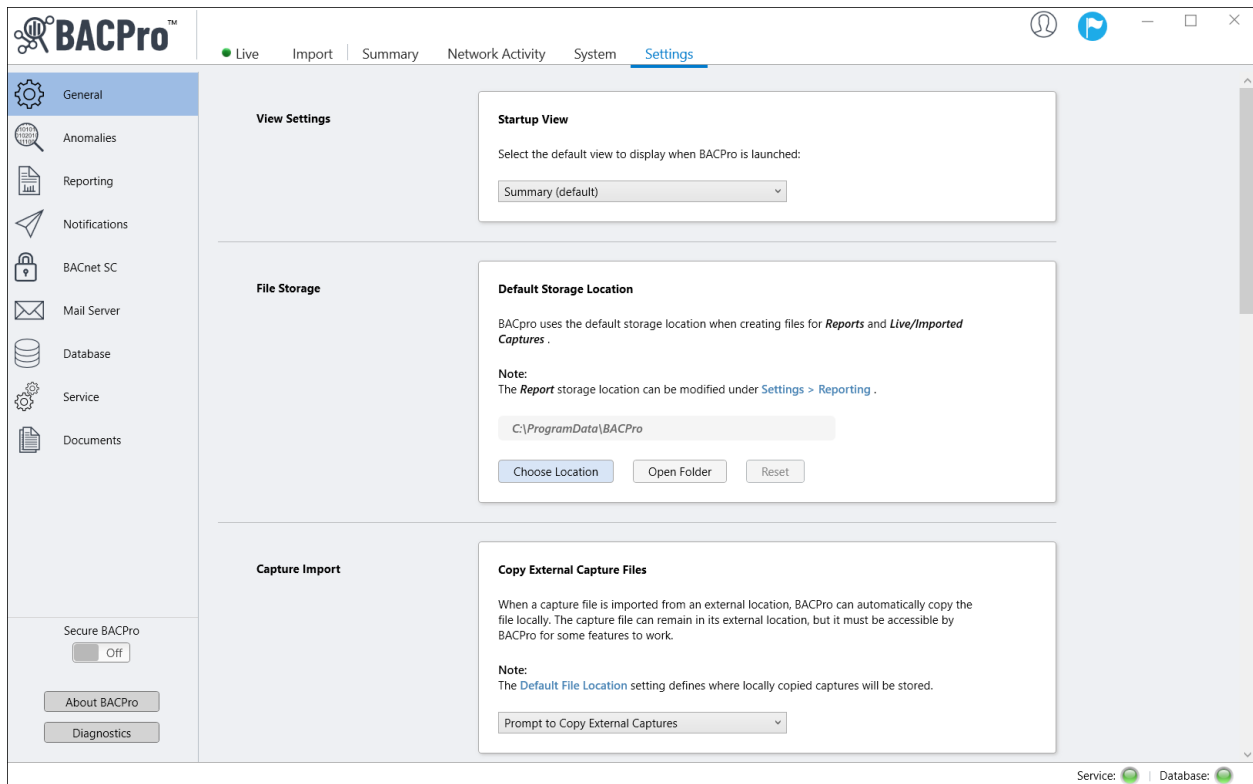
The screenshot shows the Node Details panel for a failed device. The status is 'Failed' with a red trash icon. Fields include Name: BACnetDev_104, Instance: 104, Address: 104.0.0.0, Port: 47809, and Network: 3. A 'Remove Device' button is visible.

- Exclude device addresses and UDP ports so that BACPro ignores them during live captures.

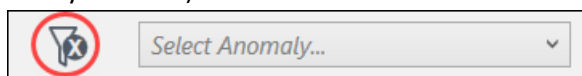
The screenshot shows the 'Select Anomaly...' dropdown menu with a red circle and slash over the shark fin icon.



11.7 Settings Tab

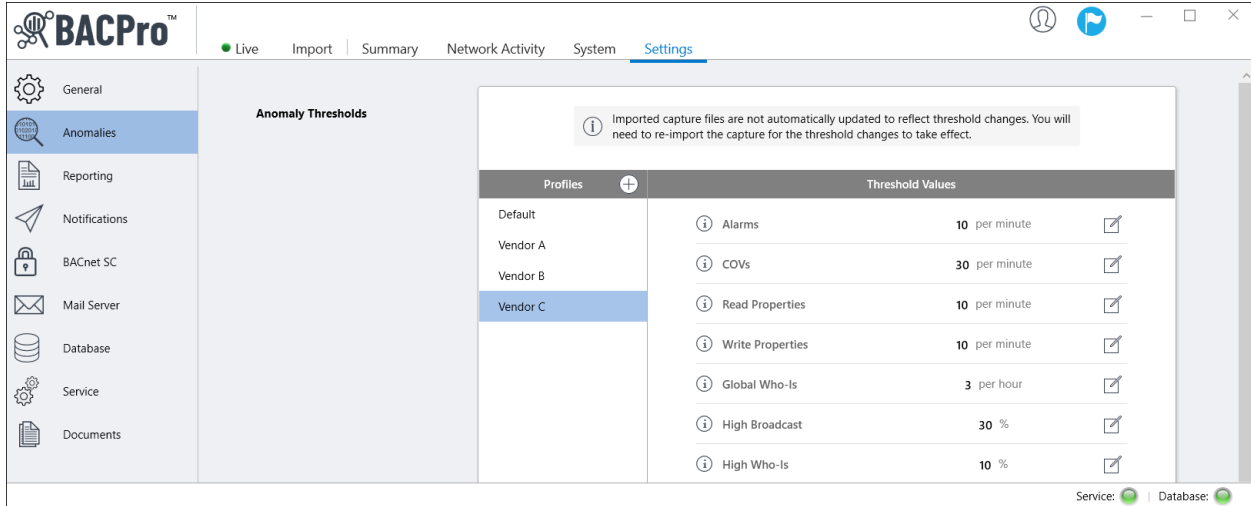


The Settings tab allows you to configure the database, SMS notifications, and a mail server to receive daily reports and email notifications. You can also choose how long to keep live capture files and data in the database. If you have low hop count anomalies on your system, they can be false positives. 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. Additionally, you can exclude device addresses and UDP ports so that BACPro ignores them during live captures (you can also do this from the System tab).



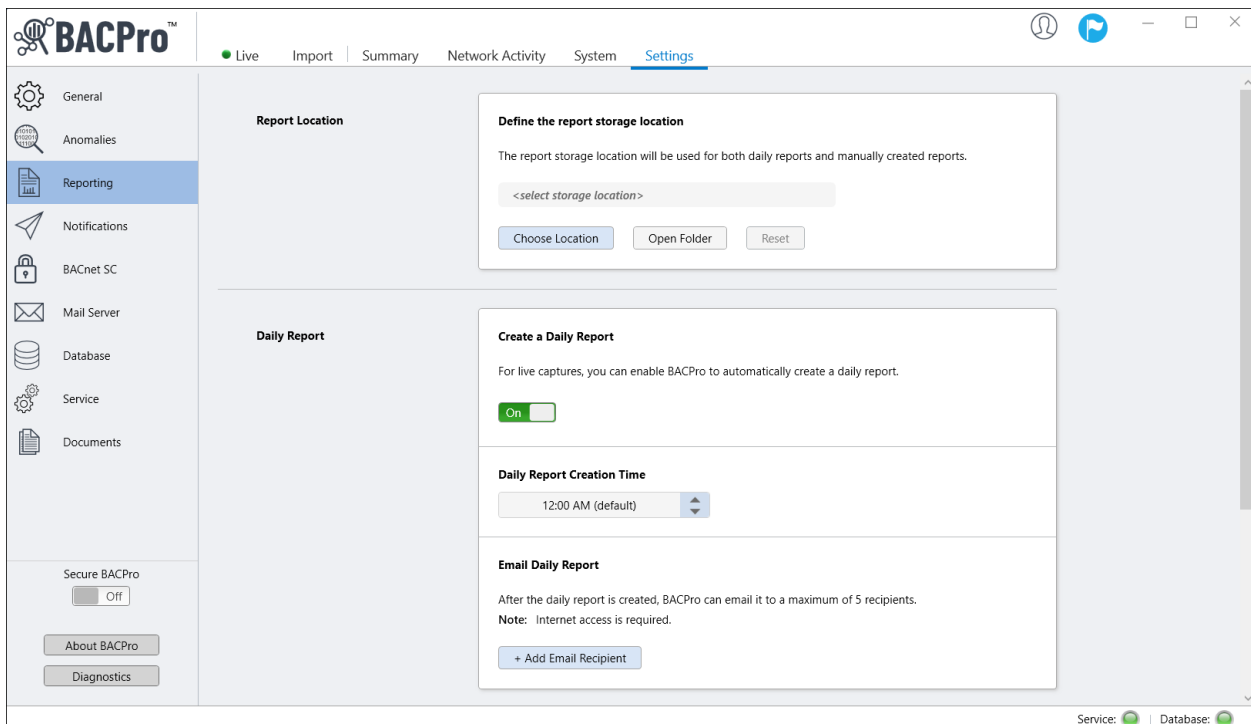
11.7.1 Anomaly Thresholds

From the Anomalies menu, you can adjust the thresholds for excessive traffic or high broadcasts for both live and imported captures. While the default values are usually sufficient, you can also add profiles for custom settings.



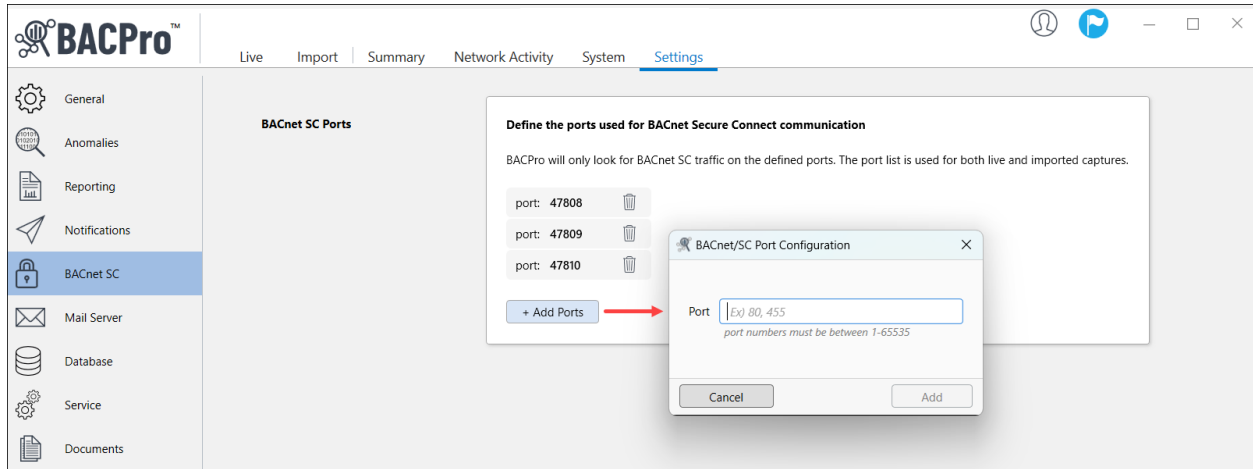
11.7.2 Reporting Options

From the Reporting menu, you can enable BACPro to automatically run a daily report and select where the file is stored. With internet connectivity where you installed BACPro, you can email the report to a maximum of five recipients. You can also replace the BACPro logo with your company logo. All of these features can be used as part of an audit package you provide your customers.



11.7.3 BACnet SC

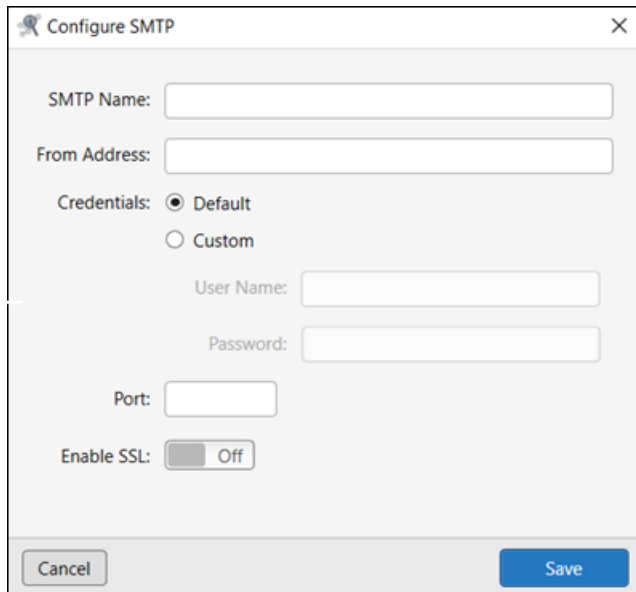
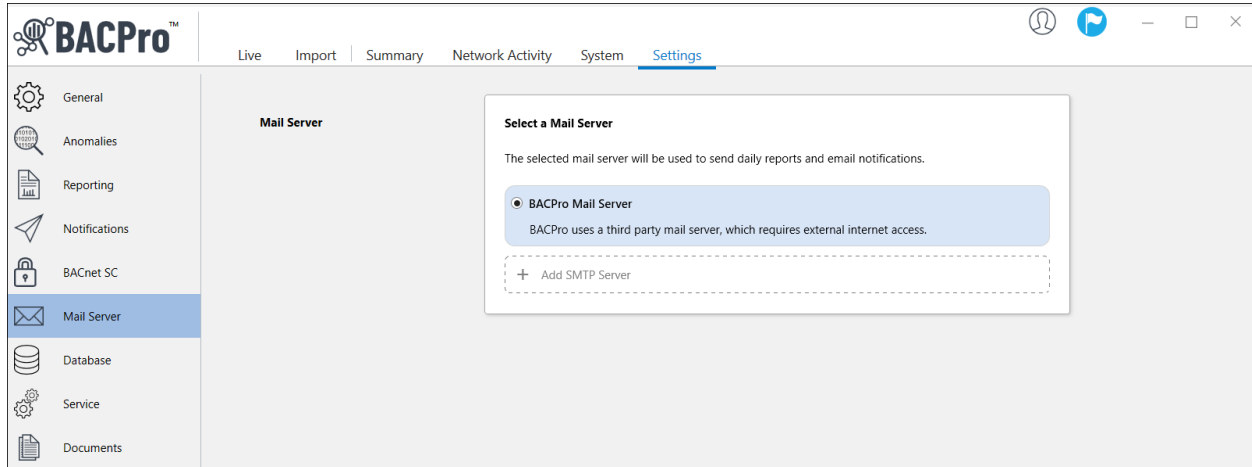
From the BACnet SC menu, you can define the ports used for BACnet SC (Secure Connect) communication. The port list is used for both live and imported captures.



11.7.4 Mail Server Options

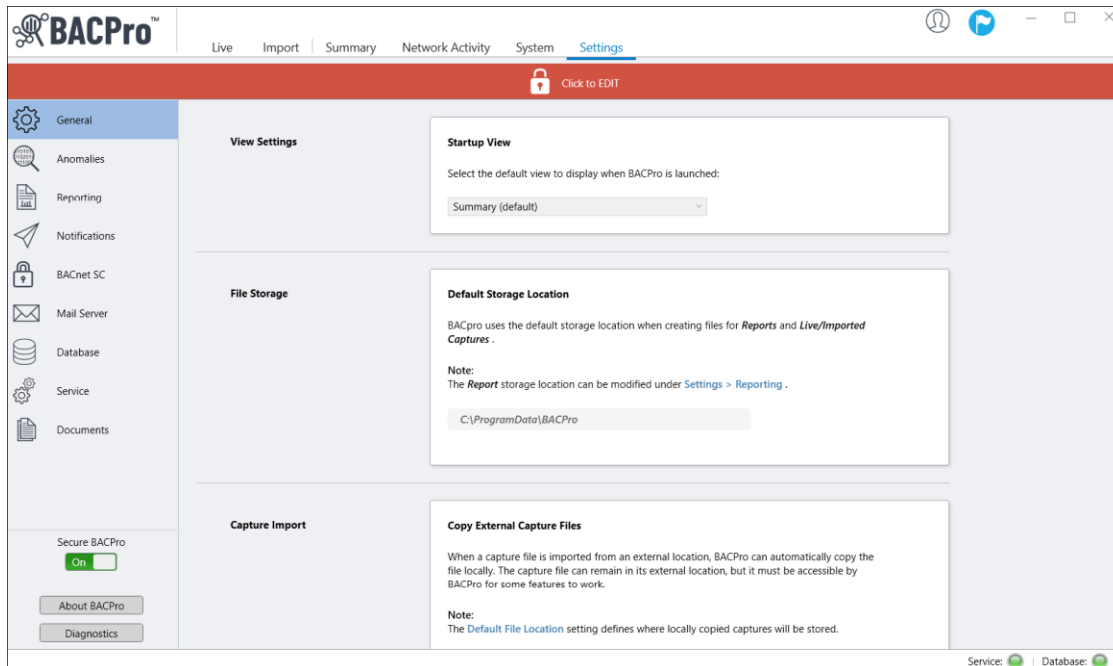
From the Mail Server menu, you can select a mail server for sending daily reports and email notifications. The BACPro Mail Server uses a third-party mail server and requires internet access. Sites without internet access can configure and use an SMTP mail server instead.

Note: When configuring SMTP using an Outlook account as the “From Address,” you need to use a verified account. See “SMTP Error When Using Outlook” in the Troubleshooting section for more information.

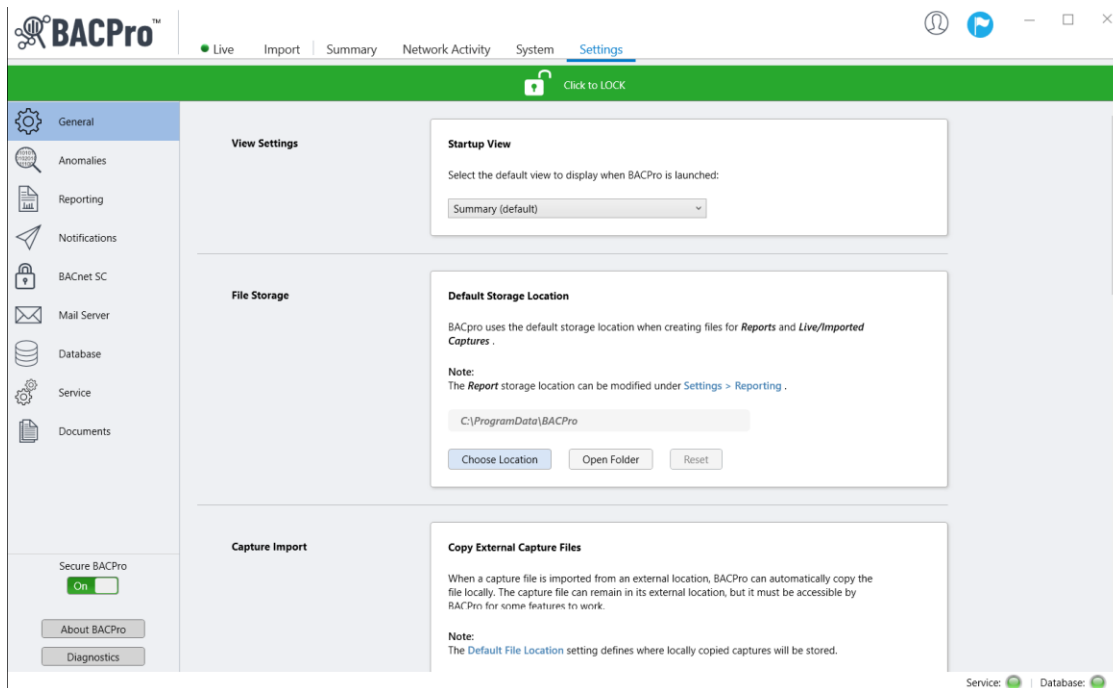


11.7.5 Secure BACPro

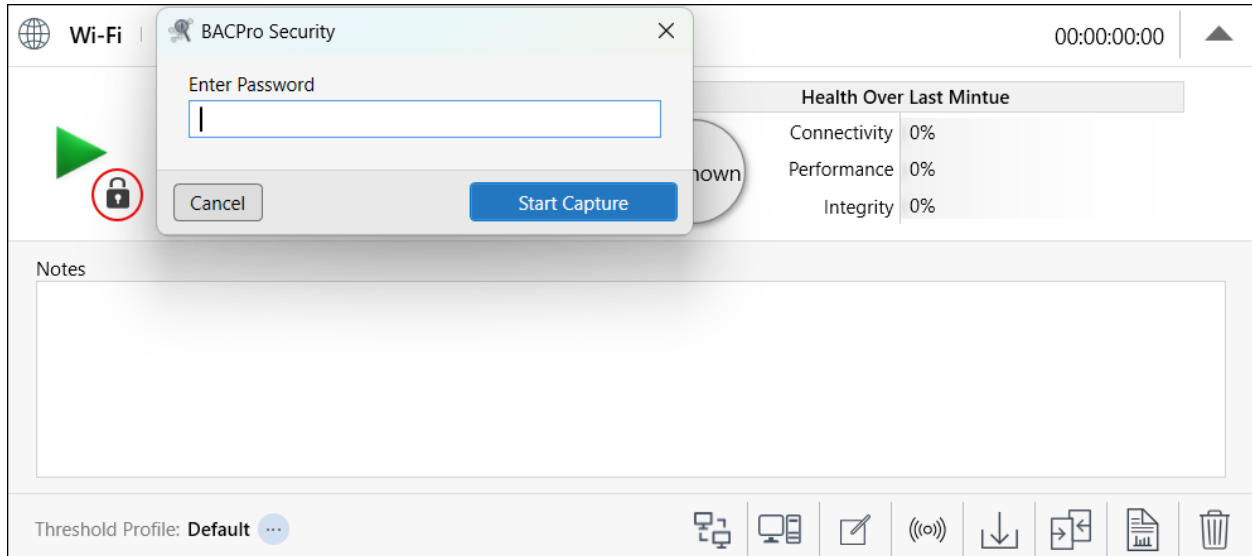
The Secure BACPro button allows you to lock all settings and require a password to edit them. When Secure Settings is turned on, a locked icon appears in a banner on the Settings tab.



Once you enter your password to edit the settings, an unlocked icon appears in a banner on the Settings tab.



Secure BACPro also locks live captures and prevents them from being started or stopped without entering a password.

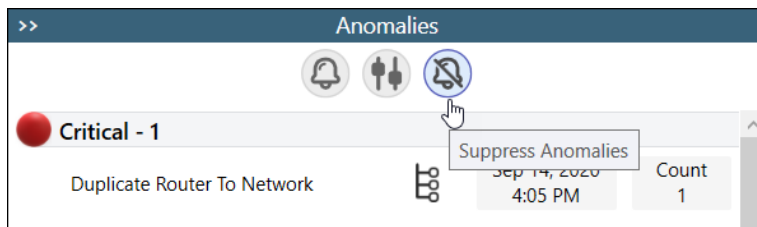


12. Suppressing False Positives

Some types of errors display as a false positive based on certain types of configurations. For example, a duplicate instance number might be reported, but if your workstation has two different isolated BACnet networks on the same network segment and same UDP port, this is not a configuration error. BACPro does try to resolve this, but if you find a false positive, you have a way to suppress it. Low hop count is another anomaly that is often a false positive because many vendors do not start the hop count at 255 per the BACnet specification.

The Suppress Anomalies button at the top of the Anomalies window opens the Suppressed Anomalies Manager, where you can add or remove items from the Suppressed Anomalies list.

Note: After adding or removing items from the list, you must reimport the capture file to update the integrity score.



Suppressed Anomaly Manager

Recommendation:
When two or more isolated BACnet networks are connected to the same workstation, you should suppress duplicate instance and network anomalies so they do not adversely affect the integrity health score.

Suppressed Anomalies

Anomaly Type	Id
Suppressed Duplicate Router	Network: 101
Suppressed Duplicate Instance	Instance: 101218

Remove Add

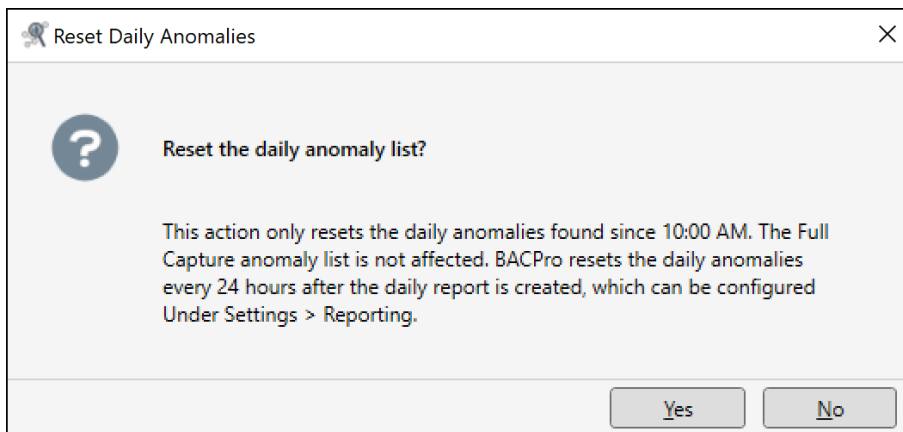
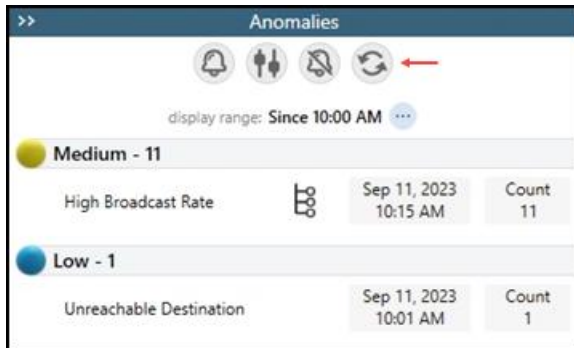
Important:
For accurate health scores, you need to reimport the capture file after an item is added to or removed from the Suppressed Anomalies list.

Reimport Capture Close

13. Reset Daily Anomalies

The Reset Daily Anomalies feature is for live captures only and is based on the 24-hour display range set for the Daily Report (Settings > Reporting).

In the Anomalies window, selecting the Reset Daily Anomalies button opens a dialog box and asks if you want to reset all daily anomalies. The Full Capture anomaly list is not affected.



14. Reused Networks and Instance Numbers

Reusing a Network number or Instance on a BACnet network is a serious configuration error. There are some circumstances where this is not a problem. If you have a workstation that has more than one BACnet stack, each communicating with its own isolated network, then you can reuse both instances and network numbers. BACPro will detect this configuration and will put the reused Network numbers and Instance numbers in an "Info" severity anomaly. These will not affect the integrity score and are there only to let you know that it happened. If BACPro detects communication between both duplicates and another device, it will create the Critical or High anomaly for those.

15. BACnet Secure Connect

Many vendors offer BACnet Secure Connect (BACnet/SC) devices, which means communication between devices will be encrypted. For BACPro to analyze the capture files, you must first decrypt them. Vendors need to provide a diagnostic mode in which their devices can export capture data in an unencrypted format.

Current BACPro Limitations of BACnet/SC support:

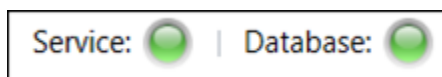
- Traffic must first be decrypted in the capture file
- IPv4 traffic only
- Wireshark does not support BACnet/SC (navigation to Wireshark for BACnet/SC packets does not work)
- Detection of failed BACnet/SC nodes and broken WebSockets

16. 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.

16.1 Service and Database Lights Are Green

If both the Service and Database lights are green, everything is communicating correctly. The Windows service must run under a user account with administrative access to the SQL database and Windows system.



16.2 Service Light Is Red

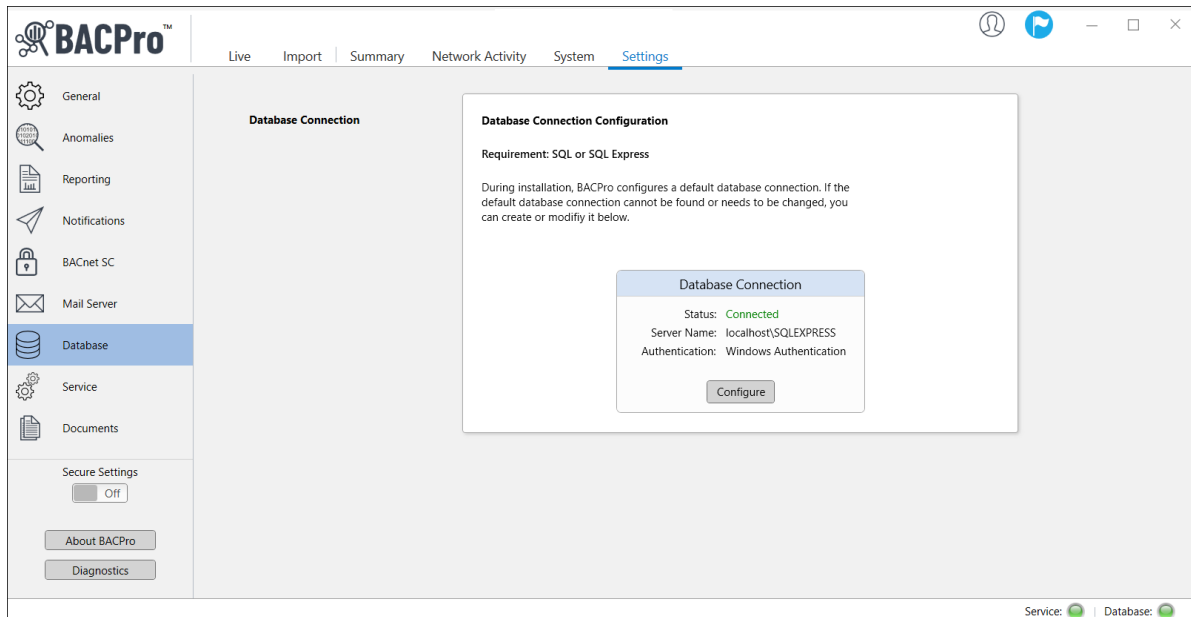
If the Service light is red, make sure the **BACProService** is running. It should be set to automatic and running under a user account with admin access to the SQL database and Windows system.



16.3 Database Light Is Red

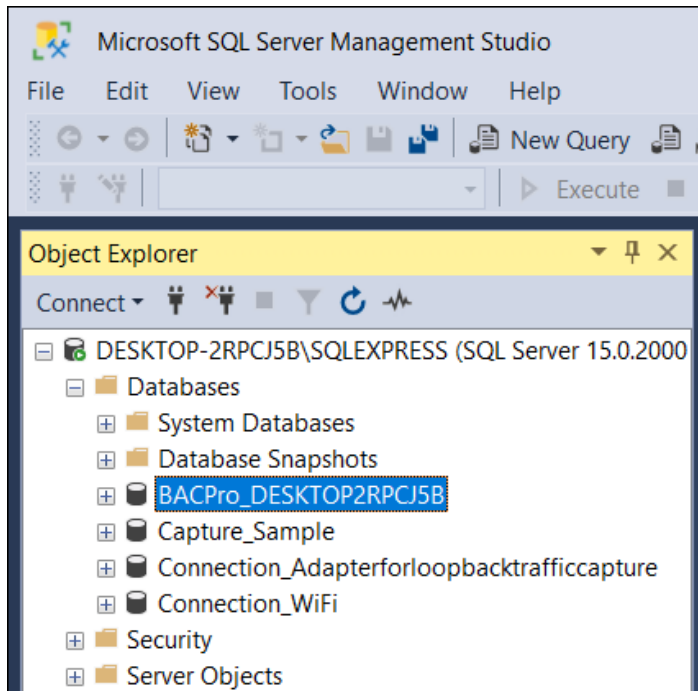
If the Database light is red, do the following:

1. Select **Settings > Database**.
2. Click **Configure**, and then select the correct version of SQL in the list.
3. Click **Validate** to make sure BACPro has admin access to SQL.
4. Click **Connect**, and the database light should turn green.
5. Make sure the **BACProService** is running under a user account with admin access to the SQL database and Windows system.



16.4 Full Database Reset

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 once you reboot your computer or restart the BACProService.



16.5 Log Files

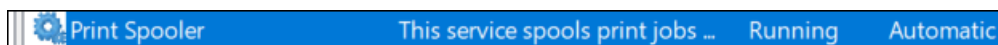
BACPro has two log files located in the OS `[Drive]:\ProgramData\BACPro` directory. Problems in the user interface are logged to `BACPro_[WindowsUserName].txt`. Problems in the Windows service are logged to `BACProService.txt`. To review the logs:

1. From the **Settings** tab, click **Diagnostics**.
2. In the **Log** tab, click **BACPro Log** and **BACPro Service Log**.

If you are unable to resolve the issue after reviewing the logs, you can send the files to support@bacprotool.com, and we will help you get BACPro working correctly again.

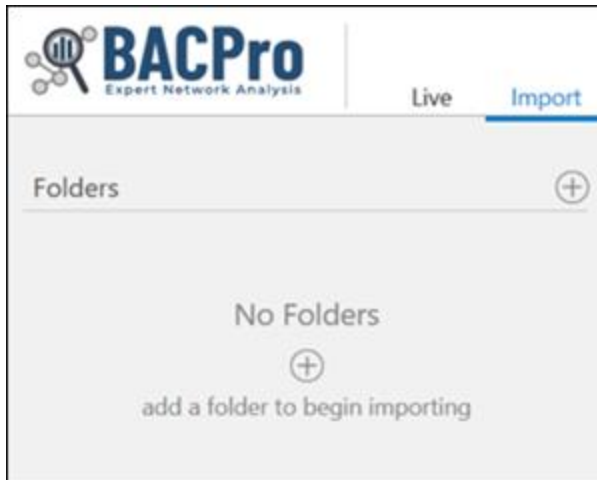
16.6 Reports Fail to Create the PDF File

The report engine uses the Windows Print Spooler service to render the report. Make sure it is running.



16.7 No Folders When Selecting Import

When you try to import a wireshark capture, you may encounter a message indicating that 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 being 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

16.8 SMTP Error When Using Outlook

You have configured the “From Address” field using Outlook as your SMTP server, and you receive the following error message:

“Failed to process message due to a permanent exception”

This is Microsoft’s way of letting you know that you have sent too many emails in the allotted period. They will send an email giving you options to fix the problem. Click the **verifying your account** link.

What do you need to do?

You can wait a day to send your message, or you may be able to increase the limit by [verifying your account](#). Verifying your account helps you enjoy Outlook.com with fewer interruptions and limitations.

Thanks,

The Outlook.com Team

Enter your phone number, and then click **Submit**. Within a few minutes, you should be able to use the account again without error messages.



Enter your mobile number to verify your account

We'll send a verification code in a text message. This helps us eliminate spam – we won't give out your number. The code will expire in about 10 minutes.

Country code

Phone number

[Send code](#)

Appendix A: FAQ

Does BACPro work on a virtual computer?

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

Does BACPro talk to my BACnet devices?

No, BACPro listens to all traffic and looks for problems by analyzing packets. It does not join the network or talk to devices. However, BACPro can broadcast a global Who-Is to discover devices on the network.

Why do I sometimes see Unknown 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 or COV. Until BACPro learns the Instance number, it will show Unknown.

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 monitors 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?

Yes, but you must decrypt the traffic before importing it. Most vendors have a device diagnostic that saves capture data without encryption.

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.

For live monitoring, 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 (uses the same network interface card) as the workstation so that it can see all traffic to and from the workstation. This provides optimal network analysis. If it is not on the same computer or same NIC, 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.

Appendix B: Release Notes

Version	Enhancements
3.20	<ul style="list-style-type: none"> - Added Chatty Devices as an Audit Report option - Added security for live captures to prevent them from being started or stopped without entering a password.
3.19	<ul style="list-style-type: none"> - Added Chatty Devices table to highlight devices causing the most network traffic
3.18	<ul style="list-style-type: none"> - New anomaly type: Duplicate Time Master
3.17	<ul style="list-style-type: none"> - Added support for importing object names from a file - Added additional examples for the Failed Router anomaly - Added support for Schneider export - Updated the EULA
3.16	<ul style="list-style-type: none"> - Added a menu item to reset Live capture network traffic counts in the Summary view network traffic tables - Fixed an issue where the YABE browser was adding a new device every time it was run - Provide a warning if Npcap is installed in admin only mode - Added the ability to delete an unused network in system view
3.15	<ul style="list-style-type: none"> - Defined the default storage location for reports and live/imported capture files - Added Customize Device Names feature for imported capture files
3.14	<ul style="list-style-type: none"> - New anomaly type: Excessive Global Who-Is Router - Added Customize Device Names feature for live captures - Added performance enhancements for Remote Capture
3.13	<ul style="list-style-type: none"> - New anomaly type: Off-Node Trending - Move all captures simultaneously between folders in the Import tab - Updated OSS software components - Fixed a false positive with trend data dates
3.12	<ul style="list-style-type: none"> - Added Exclude UDP Ports feature for live captures - New anomaly type: Questionable Time Sync Anomaly - New anomaly type: Questionable Trend Data Date Anomaly
3.11	<ul style="list-style-type: none"> - Added Tour Guide, an interactive feature that shows the steps needed to process and analyze a BACnet capture - Added Exclude Device feature for live captures - Added filters showing previous hours of anomalies for live captures
3.10	<ul style="list-style-type: none"> - Added button to purge live anomaly list and recalculate health score - New anomaly type: Unreachable Destination - Decode captures that used port mirroring (ERSPAN encapsulation) - Look for BACnet on non-standard UDP ports as low as 10000
3.9	<ul style="list-style-type: none"> - Added top 20 broadcasts to report

	<ul style="list-style-type: none"> - Fix export anomalies as .csv
3.8	<ul style="list-style-type: none"> - Look for BACnet traffic higher than UDP port 49000 - Minor enhancements to report, show column headers on each page
3.7	<ul style="list-style-type: none"> - Added Wireshark Continuous File Processing feature, a live connection type that monitors a directory Wireshark writes files to
3.6.1	<ul style="list-style-type: none"> - Bug fixes: correct health scores in report from imported captures
3.6.0	<ul style="list-style-type: none"> - New anomaly type: Daily Decrease in Connectivity - New anomaly type: Daily Decrease in Performance - New anomaly type: Daily Decrease in Integrity - Tool tips for Error Replies - Improved startup speed - Can edit how long a device is failed before SMS is sent
3.5.0	<ul style="list-style-type: none"> - New anomaly type: UTC Offset Changed - Remote Capture feature provides one report for multiple BACPro installations.
3.4.0	<ul style="list-style-type: none"> - Updated Report Engine / Windows 11 official support - Support decoding VLAN wrapped BACnet packets
3.3.0	<ul style="list-style-type: none"> - Added Delete multiple captures at once feature - Minor bug fixes
3.2.0	<ul style="list-style-type: none"> - Allow anomaly suppression on Failed routers and devices - Minor bug fixes
3.1.0	<ul style="list-style-type: none"> - Compare Capture feature shows the differences between 2 or 3 captures - New anomaly type: Error Reading Object List - Upgrade Installation will no longer ask for service account and password - Reduced frequency of data stored in SQL database. The data rate scales with the number of devices - Added Port filter for BACnet SC. BACPro only looks for SC on ports you list - Added customizable threshold for Network Failure. You can specify how many minutes of silence before an anomaly is created
3.0.0	<ul style="list-style-type: none"> - New anomaly type: High Text Message Rate - New anomaly type: Firmware Revision Changed - Delete a BACnet device from a live capture database - Send global Who-Is Broadcast for live connections - Set workstation address to prevent false-positive failed workstation anomalies. - SQL database names now contain computer name so you can have many BACPro copies writing to the same SQL database - Moved log files, capture files, and reports to the operating system \ProgramData\BACPro directory - SQL databases created in SQL default location - Run BACPro from an RDP session

	<ul style="list-style-type: none"> - Lock BACPro settings with a password - Added Object List count to statistics we collect - Fixed an issue with duplicate instances on Network 0
2.5.0	<ul style="list-style-type: none"> - Disable the Workstation Failure or Return anomaly - Added median reply time to reply times table - Added data rate statistics for BBMD and Broadcast traffic to report - Use TLS 1.2 for SMTP mail messages
2.3.0	<ul style="list-style-type: none"> - Support for anomaly threshold profiles
2.2.0	<ul style="list-style-type: none"> - Ability to create a customizable, high-level Audit Report in PowerPoint
2.0.0	<ul style="list-style-type: none"> - Added decoding of BACnet SC unencrypted capture files - Added export to .CSV file in System view
1.2.3	<ul style="list-style-type: none"> - SMTP mail server support for sending daily reports and email notifications - Multi-level (nested) folders available for capture imports
1.2.1	<ul style="list-style-type: none"> - Export live captures data to a single .pcapng file given a start time and period - New anomaly type: Device Database Downloaded - Import MSTP files if their timestamps occur before 1970. Issue with some 3rd party capture tools that do not fill in date time correctly
1.1.9	<ul style="list-style-type: none"> - Email a Daily Report to a maximum of 5 recipients - Select a daily report creation time - Specify the storage location for reports - Set a site name that is used in emails and SMS messages - Improvements for daily database cleanup - Fix second packet display in the duplicate MAC anomaly
1.1.8	<ul style="list-style-type: none"> - New anomaly type: Device Restarting - Allow SQL username and passwords to connect to the database - Notes from a capture are now displayed in the reports
1.1.7	<ul style="list-style-type: none"> - Internal release, database writing improvements
1.1.6	<ul style="list-style-type: none"> - Added export to .CSV file from tables in Summary view - Minor fixes
1.1.5	<ul style="list-style-type: none"> - Added support for Branch license