QRadar Support

Help and case escalations

Support workflow

QRadar Users

Case Opened

1. Case is opened. Description, severity, and current contact number provided.

Waiting on IBM

2. Initial contact is made. QRadar Support might request additional information, schedule a live session, or ask for logs or an export.

Waiting on Customer

3. Status is set to 'Waiting on Customer' for feedback.

Waiting on IBM

4. Problem determination is in progress with QRadar Support.

Severity Increase

5. User increases severity:

- Add an updated contact number.
- Include any relevant new information.

Waiting on IBM

6. Problem determination is in progress with QRadar Support.

Duty Manager

7. User requests a duty manager for assistance.

- Ensure you leave a contact number.
- Provide a description of the problem or changes that impact your business when you request the duty manager.
- Any user can request a duty manager to escalate a support issue or case.

IBM Security

v1.0

Global: http://ibm.com/planetwide
U.S.A/Canada: 1-800-426-7378
Mexico: 01-800-0032500
U.K.: 03705 500 900
France: 33 810 631 213
Germany: 0800 5 253553
Italy: 800-820-094

India: 1 800 425 6666
Brazil: 0800-728-7378
Japan: 0120-34-0000
China: 8008101818-5200
Russia: 7-800-200-6300
South Africa: 0860 700 777
U.A.E: 8004704

Open a case - https://ibm.com/mysupport
Support 101 - https://community.ibm.com/qradar/support
Customer forums - https://ibm.biz/qradarforums
Learning Services - https://ibm.biz/learnqradar
Software list - https://ibm.biz/qradarsoftware
Firmware list - https://ibm.biz/qradarfirmware
QRadar Open Mics - https://ibm.biz/qradaropenmic

QRadar Support Cases 101

v1.0

For all QRadar Support cases include:

1. A detailed description of the issue.
2. Impact statement of how the problem effects your business.
3. Hours you are available to work the issue.
4. Your phone number/email to confirm our records are up to date.
5. List any alternate contacts if you are unavailable or out of the office.
6. Is this a production system?

Case details that reduce the time to resolution

- What are the symptoms of the issue?
- What version of the product are you using (7.3.1.xxxxxxxxx)?
- What is the approximate time the issue first occurred?
- What steps did you take to reproduce the issue?
- What changes were made to the system before the issue occurred?
- What steps you have attempted to resolve the issue?
- Would a screen capture help explain your case to QRadar Support?

Parsing must gather information

Submit this information

1. The version of the device support module (DSM).
2. Add a filter for 'Event is Unparsed' is 'True':
   (Log Activity > Add Filter > Event is Unparsed = True)
3. Export the events to an XML file:
   (Log Activity > Actions > Export to XML > Full Export (All Columns)
4. Provide the name of the device sending events.
5. Provide the software/firmware version for the device.
6. Provide logs from your QRadar appliance:
   (Admin > System & License Management > Actions > Collect log files)

Log source configuration issues

Submit this information

1. Verify events are received by the log source.
   For TCP Syslog, type:
   tcpdump -s 0 -A host Device_Address and port 514 or 6514
   For UDP Syslog, type:
   tcpdump -s 0 -A host Device_Address and udp port 514
2. Provide logs from your QRadar appliance:
   (Admin > System & License Management > Actions > Collect log files)
3. Provide a screen capture of the log source configuration:
   (Admin > Log Sources > Double Click your log source)

WinCollect must gather information

Submit this information

1. Zip and attach these folders to your case:
   C:/Program Files/IBM/WinCollect/logs
   C:/Program Files/IBM/WinCollect/config
2. Managed WinCollect tools (/opt/qradar/support):
   WinCollectHealthCheck.sh
   WinCollectDeploymentSummary.sh
3. Agent tools: (C:/Program Files/IBM/WinCollect/bin)
   WinCollectPing.exe

Install and upgrade issues

Submit this information

1. Collect logs from the Console
   (Admin > System & License Management > Actions > Collect log files)
2. Is IMM or a remote management interface available?
3. Is this a fresh install or an upgrade?
4. Is this a high-availability appliance pair?
5. List any error messages from the installer in your case description.

https://ibm.com/mysupport