Network Requirements for Q-Interactive Assess

Q-interactive®

Snapshot

This guide will help you ensure that your network environment is optimized so the Q-Interactive Assess application is able to share information between the client and practitioner devices. While Assess does not require an active WiFi connection, the network must have the correct communication protocols enabled for the devices to discover each other automatically via Apple's Bonjour technology. Included in this document is an overview of the networking requirements needed for Bonjour to function properly.

For detailed information about Bonjour, see Apple's Support documentation.

Local Network

Assess uses a direct connection method to communicate through the local network. In environments with multiple wireless nodes, node-to-node communication must be enabled.

Your devices must be on the same VLAN or subnet within the network to connect. Apple's Bonjour technology cannot cross subnets/VLANs natively. If you require your devices to be on different subnets, then a Bonjour Gateway may be needed for your network. While some network hardware has this functionality built in, others may require a third-party solution.

A Bonjour Gateway allows Bonjour to cross subnets/VLANs so your devices can communicate. **Aerohive** and **Cisco** are two such developers of Bonjour Gateways.

Multicast

Your local network must be allowed to run Bonjour and mDNS (multicast DNS). Multicast must also be enabled, but multicast drop should be disabled.

The Bonjour protocol consists of service announcements and service queries that allow devices to ask for and advertise specific applications. DNS-SD (Domain Name System – Service Discovery) over a multicast link is used to query the local network for registered services. Each query or advertisement is sent to the Bonjour multicast address for delivery to all clients on the subnet.

Apple's Bonjour protocol relies on mDNS operating at UDP port 5353 and sends to these reserved group addresses:

- IPv4 Group Address - 224.0.0.251
- IPv6 Group Address - FF02::FB

The addresses used by the Bonjour protocol are link-local multicast addresses and thus are only forwarded locally. **Routers cannot use multicast routing to redirect traffic because the time to live (TTL) is set to one, and link-local multicast is meant to stay local.**

For a full list of TCP and UDP ports used by Apple software products, see Apple's Support documentation.

Multicast Groups

Some networks may use a multicast group to manage multicast traffic. When multicast is enabled, all multicast traffic will flow to all connected clients in a subnet. By using a multicast group to limit the number of clients receiving the multicast data, you can reduce the overall workload being placed on the network.

Using groups is typically not required, but it can be helpful if there are many Bonjour devices on the network. When creating multicast groups, there are three important factors to consider:

When creating multicast groups, there are three important factors to consider:

1. Multicast groups must include the subnets or VLANs where Assess devices are connected.
2. All Assess devices must be members of the multicast group..
3. If using multicast groups, then IGMP Snooping must be enabled on your network to allow your devices to listen to the multicast group. This allows your devices to see the multicast group traffic without affecting the rest of your network.

Detailed information about multicast groups and IGMP Snooping can be found **here**.

Bonjour Protocol Security

To mitigate risks associated with Apple's Bonjour protocol, Q-interactive utilizes an internal, secret passcode to establish a secure connection between devices. To further improve security, network administrators may choose to implement segmentation, access controls, and/or traffic filtering to restrict Bonjour usage to only necessary services.

To secure a network to allow only the specific service for Q-interactive while blocking others, follow these general steps:

1. Identify the Required Bonjour Service
   - Each Bonjour service has a unique Service Type. Q-interactive's service name is _assess2._tcp.
2. Implement VLANs & Segmentation
   - Create a separate VLAN for devices that need to use the Bonjour service.
   - Use a Bonjour Gateway or mDNS Repeater (if required) to bridge service discovery between VLANs while blocking other services.
3. Control mDNS Traffic with Firewall Rules
   - Allow only mDNS (UDP port 5353) traffic for the specific service and block others.
   - Example rule:
     - **Allow** UDP 5353 traffic for _assess2._tcp
     - **Deny** all other mDNS traffic

4. Use Access Control Lists (ACLs)

- Configure ACLs to allow only devices that need the service to send or receive mDNS packets for that service.
- Example ACL (on a managed switch or router):
  - **Permit** mDNS traffic for _assess2._tcp
  - **Deny** all other mDNS broadcasts

5. Configure Network Discovery Controls

- If your network equipment supports mDNS Snooping, enable it to filter out unwanted Bonjour traffic
- Disable Bonjour/mDNS services on devices that don't need them to reduce network congestion.

6. Use Mobile Device Management (MDM) or Endpoint Controls

- Use MDM policies to allow only the required Bonjour service on devices.
- Restrict unwanted Bonjour activity such as AirPlay, File Sharing, or other Bonjour services through device configuration profiles.

7. Monitor & Log mDNS Traffic

- Use network monitoring tools to verify only the allowed service is advertised.
- Set up alerts for unauthorized Bonjour services appearing on the network.

By isolating, filtering, and/or restricting Bonjour traffic, you can secure your network while allowing intended services, such as Q-interactive.

Using all the information contained in this guide, you should be able to ensure that any network is optimally configured for Q-Interactive Assess.

For answers to specific questions or more advanced configuration details, contact your network hardware manufacturer.

800-627-7271 | PearsonAssessments.com

Pearson