



IT Primer for Q™

Q™ FAQ's

What is Q™?

Q™ is a new delivery channel for relevant, ongoing training reinforcement and communications with sales, customer service and other customer-facing employees. Q™ provides frequent reinforcement, coaching and measurement to dramatically improve retention and application of new information and change.

Q™ is a hosted application - is Q™ entirely web-based?

No, there is a small client program that is loaded on each employee's computer. The purpose of the client application is to notify and launch daily reinforcement exercises. The client application takes about 1 minute to install and is available for download over the internet – if employee lacks permission to install the application, the installation program can be provided to company IT Staff for internal distribution.

How is the install packaged?

The installation package for the Q™ client is available in two formats. One is an executable file (qsetup.exe). The other is a standard Windows installer file (q.msi).

Can the Q™ client installation be automated?

Yes. Typically, the Windows installer file (q.msi) is used with automated tools to push the client to the users' desktops. In most cases, the automated push should install the client in the context of the logged in Windows user (as opposed to the System account). This is because the installation launches a background process at the end, which needs to run under the user's context.

What support does the Q™ client have for proxy server environments?

Q™ will operate in a web proxy environment, and supports authentication with the proxy server.

Does the Q™ client make any DNS calls?

Yes. The client makes DNS calls when connecting to www.count5q.com and www.oddcast.com.

Does the Q™ client require any special IP ports to be opened in the firewall?

No. The client communicates with the Q™ servers using the standard HTTPS protocol and port.

Does the Q™ client run as a service?

No. The Q™ client launches a background process automatically on system start-up via the "run" key under the Local Machine section in the Windows registry.

What personal employee information does Q™ store?

Q™ stores each employee's name and email address on the Q™ server. Q™ also makes a record on the Q™ server of each person's participation with reinforcement activities and answers to applicable questions.

Does Q™ access or store any customer/prospect information or require integration with or access systems that house customer/prospect information?

No.

What are the system requirements for the Q™ client?

- *OS - Windows 2000, XP, Vista. All latest critical patches and service packs required.*
- *Browser - Microsoft Internet Explorer 6.0 or higher.*
- *CPU - Pentium III, 600MHz minimum*
- *Estimated RAM Utilization for Q™ Client - 10 MB*
- *Hard Disk - 10 MB available for Q client software.*
- *Monitor - 800 x 600 pixel resolution minimum.*

Q™ Application Architecture and Security

Architecture:

Server: ASP.Net, Web Services, C#, MS SQL Server, MS SQL Reporting Services

Client: C++, MFC

Details:

- **Installation** - The Q client is installed using an InstallShield setup package. This package is a Windows MSI installation, optionally packaged in a setup.exe file. Depending on how the installation file is configured, the user can choose the installation directory (defaults to c:\Program Files\Count5\Q), and all files are copied to that directory. This includes Microsoft .dll's for MFC and standard C and C++ libraries.
- **Startup** - Once installed, the Q client launches a background process automatically on system start-up via the "run" key under the Local Machine section in the Windows registry. This process uses a task-tray icon to indicate client status, and allow the user to sign in, sign out, and launch the full client user interface. The process polls the Q server at a configurable time interval (defaults to 60 minutes) to determine whether the user is required at that time to conduct a reinforcement exercise. If the user chooses to run an exercise, the client launches a Microsoft Internet Explorer window which is used to present the exercise.
- **Login** – The first time the Q client runs on the PC, the background process prompts the user for an ID (email address) and password. After successfully logging in to Q, the client stores these values in the registry (encrypted), so the user does not have to login manually to Q every time the user logs in to Windows. The server can be configured to lock out users who attempt to login with invalid credentials a certain number of times.
- **Server Communications** - All communications between the client (background process and full UI) and server use industry standard SOAP/XML over HTTPS protocols. The IE window uses HTML over HTTPS to communicate to the server.
- **Other** - The client requires access to the registry in order to create the following two registry keys plus sub-keys: HKLM\Software\Count5 and HKCU\Software\Count5

Encryption:

All Q™ clients are configured to communicate with the Q™ server using industry-standard Secure Sockets Layer (SSL) encryption. This is the technology used by all major internet sites to secure e-commerce transactions. By using SSL, network traffic is safe from unauthorized 3rd party inspection. Reinforcement exercises viewed in the browser also use SSL via HTTPS.

Authorization:

Access to the Q™ server application (web service) is restricted to users with the Q™ Client and proper credentials (ID and password). No user can connect to the Q™ server without the Q™ client and a proper ID/password. Customer maintains full control of administrative permissions and active user credentials. The same ID/password is required to view the reinforcement exercises in the browser.

Upgrades:

Server software upgrades and patches are transparent to the end users. Client upgrades and patches can be installed two ways: 1) the new client can be pushed to end user desktops using in-house tools, or 2) the client can perform an "auto-upgrade" which downloads the new client from the server, and installs it without need for end-user intervention. The auto-upgrade download process uses Microsoft's Background Intelligent Transfer Service (BITS). Most upgrades and patches affect only the small subset of users that have administrative privileges.

Data Center Security & Reliability

The Network:

The data center has high-bandwidth private transport network connections. The local fiber connectivity is redundant with three fiber rings with dual entry points from Optical Carrier-12 (OC-12) hardware.

The data center has demonstrated 99.999% network availability, which means that the network will be down no more than 5 minutes a year — as close to perfect as you can get. The SQL Database is backed up daily.

The data center is **SAS 70, type II** compliant.

Security Details:

The data center is monitored for all aspects of operational security, and environmental conditions. It is equipped with state-of-the-art security and environmental monitoring systems. These systems include Card Readers, PINs, Biometrics, Multiple Sensors for intrusion detection, and environmental sensors.

There is also an on-site network operations center (NOC) that is staffed 24 hours a day, 7 days a week with network operations personnel. The NOC monitors the entire network for efficiency, congestion, and network errors. NOC technicians can re-route traffic and respond to any alarms that might occur.

Uninterruptible Power:

The data center is engineered with a redundant, uninterruptible power system and backup generator to deliver seamless power. In the event of a commercial power failure, the isolated UPS system will provide immediate backup power until the diesel generators take over the load and continue operation of the center. Each generator has a fuel tank capable of running for a minimum of 48 hours at full capacity. Service agreements from local fuel vendors guarantee priority refueling in the case of long-term power outages.

Redundant HVAC:

The redundant HVAC system keeps the average temperature in the Data Center at 70 degrees F (+/- 2), ensuring a consistent operating atmosphere for all servers. Additional sensors detect variations in humidity and keep the average humidity at 50% (+/-3).