ImageQuest Data Protection Recommendations

Data at Rest – Server

Document files are stored in the file share and accessed by the IQ application server. SQL server is used to store document metadata and other properties of the IQ system. For data at rest encryption, we recommend a volume encryption solution like Microsoft BitLocker. It is recommended that all volumes on the IQ application server and SQL server are encrypted, so that any temp files generated by the application also fall into BitLocker protection. We recommend sensitive data not be stored as document metadata attributes.

Data at Rest – Client

ImageQuest clients download and store document files on disk so they can be displayed or opened by the native viewer. These documents are temporary and cleaned up periodically by the IQ client. If protection of this content is required, we recommend applying BitLocker or similar technology on the IQ client machines.

NOTE: the user can choose to save local copies or export data elsewhere that may not be protected by BitLocker. If this is a concern, we suggest looking into the “view-only” permission and if that would work with your specific file types and business process.

Data in Transit – Server to Client

Document content is transferred between IQ server and IQ desktop client. ImageQuest version 15 includes TLS security for this data transit. Attribute metadata transferred between IQ client and SQL server is not currently encrypted. We recommend metadata not contain any secure information.

Data in Transit – Network Scan Device to Server

Network scanner devices typically scan documents into a network share. We recommend enabling SMB 3.0 encryption on the server to protect the data from scanner device to IQ server. It is recommended that BitLocker be used on this share to protect the data once received.

Multi-Factor Authentication

We recommend ImageQuest be configured for single sign-on, so that authentication is handled by Windows. If multi-factor authentication is required, we recommend that a multi-factor authentication server be configured at the domain level.