Network Protection

The Agilent CrossLab Connect Remote Advisor Enterprise Manager is hosted in the Amazon Web Services (AWS) computing cloud environment, and leverages the AWS Virtual Private Cloud (VPC), subnet, and security group services to isolate the application from the Internet and other networks.

AWS provides full data center infrastructure with controls, procedures, and services to support the operations of highly available, durable, and secure enterprise applications. Only required and appropriate network connection ingress/egress is allowed. All network communications are encrypted to ensure point-to-point data security. The primary ingress is by way of HTTPS on port 443 for most of the services. Additional ingress is allowed from specific Agilent data center IP addresses to the Enterprise Manager on port 5439. Data is pulled for utilization by the Agilent Laboratory Business Intelligence (LBI) and Asset Portal applications.
Network Communications and Access Control

The Enterprise Manager is accessed by the Lab Manager Gateway, Laboratory Business Intelligence and Asset Portal data collection, and the Agilent Customer Service agents to access appropriate Enterprise Manager resources.

Lab Manager Gateway

Lab Manager Gateways initiate all communications between the Gateway and the Enterprise Manager. All communications are via encrypted HTTPS. Additional security assigns each Gateway a Gateway/Customer account. The Gateway account and access credentials are created at the time the Gateway is installed and configured to communicate with the Enterprise Manager.

Gateways must provide access credentials with each request to the Enterprise Manager. Any request attempts that are not encrypted or do not have correct credentials will be blocked. AWS Identity and Access Management (IAM) services are used to allow or deny account access.

Firewall filters for the Gateway to communicate to the Enterprise must be open for the Gateway to communicate to these URLs.

- **https://firehose.us-east-1.amazonaws.com**
  Send instrument monitoring, event, utilization, and audit log data to the Enterprise
- **https://kinesis.us-east-1.amazonaws.com**
  Send Remote Assist requests to the Enterprise
- **https://s3.amazonaws.com**
  Send copies of System, Data Transfer Service, and Remote Advisor Log Files to the Enterprise
- **https://raemanager.agilent.com**
  Used during Gateway registration to activate a new Gateway
- **https://apigateway.us-east-1.amazonaws.com**
  AWS URL used internally in AWS API calls through Enterprise Manager specific custom API Gateway URL below
- **https://62eben3s9g.execute-api.us-east-1.amazonaws.com**
  Used for HTTP requests for Software Content Updates and Messages sent from the Gateway to the Enterprise such as instrument log file request retrieval

Outbound Port: HTTPS Port 443

Agilent CrossLab Connect LBI and Asset Portal

The Agilent CrossLab Connect LBI and Asset Portal applications reside in the Agilent Data Center. LBI and Asset Portal process the data collected by the Enterprise Manager for inventory, utilization, and troubleshooting reports.

Data transfer requests from LBI and Asset Portal are from specific IP addresses within the Agilent Data Center to the Enterprise Manager database. Authorization credentials are also required to setup the connection. The Enterprise Manager network only allows database requests from the specified Agilent IP addresses meeting specific authorization credentials. Only encrypted SSL connections are accepted. All connection requests from other IP addresses and any session requests without the correct credentials are blocked.

Agilent Customer Service User Access

Authorized Agilent Customer Service agents access the Enterprise Manager web user interface. Call center agents use the Enterprise Manager for remote instrument diagnostics. User access is limited to Agilent personnel. The web user interface operates only over encrypted HTTPS connections limited to TLS 1.2 protocol and associated secure ciphers.

Agilent IT Security Scans and Tests

The Agilent Software Design Life Cycle requires that the Agilent IT Security team execute security tests against the application and provide an approved passing result prior to the application going into service. The Agilent IT Security team operates independently of the application development team to provide separation of duties and accountability.

Software source file vulnerability scans are performed in accordance with the Agilent Software Design Life Cycle (SDLC) to ensure that all coding meets industry accepted security practices.

Network Penetration tests are performed against the deployed application to ensure there are no network or protocol vulnerabilities. The scans identify known industry vulnerabilities like cross-site scripting, HTML tag injection, formula injection and Open Redirection. Any identified vulnerabilities are remediated and must pass subsequent tests prior to pushing the application into production service.

Penetration tests are performed regularly in accordance with the Agilent Penetration Test Security Standard.
Role Separation of Duties and Least Privilege Permissions

Agilent follows separation of duties and least privilege policies to limit access to systems and data to appropriate levels of access required to perform a job.

Data Storage

Data that is processed by RA Enterprise Manager is stored in secure AWS databases and AWS S3 storage. Daily data backups are maintained for 30 days.

References

See the following references for more information about AWS data center and services compliance and security.

- AWS Cloud Security
  https://aws.amazon.com/security/
- AWS Compliance
  https://aws.amazon.com/compliance/
- AWS Data Centers
- AWS Shared Responsibility Model
  https://aws.amazon.com/compliance/shared-responsibility-model/
- What is Amazon VPC?

NOTE: The above reference links were valid at the time of publication.