Technical Overview

Security and Hardware Features: Agilent Connected Instrument Device (CID) for OpenLab CDS

Authors

Alok Mishra,
Sunil Rehman,
Mike Kicinski,
Edison X Cerda
Agilent Technologies, Inc.

Abstract

The Agilent Connected Instrument Device (CID) solution and the CID Hub offers a new deployment model for client-server configurations running OpenLab CDS AICs. The solutions delivers an IoT device with pre-installed software & drivers (i.e. CID) and a SaaS-based multitenant web application (i.e. CID Hub) that centralizes the deployment, management, and troubleshooting of the AICs in the client-server configuration. Additionally, the solution includes security features that simplify IT management workflows and offer resiliency & redundancy benefits for instrument control and data acquisition.

The Agilent Connected Instrument Device (CID) for Agilent OpenLab CDS is an instrument control device that allows analytical instruments to be controlled by the OpenLab CDS clients, and can be managed remotely. The CDS clients access the device over the customer's intranet to operate the instruments controlled by the device.

This technical overview addresses the security measures built into the CID in support of both its operation of instruments under control of a CDS client and its remote (cloud) management and deployment features.

Network deployment diagram

The CID is a component of a client-server OpenLab CDS deployment. It is functionally equivalent to the Agilent OpenLab Analytical Instrument Controller (AIC). Rather than installing software on a Microsoft Windows PC, the CID is a turnkey Internet of Things (IoT) device that can be managed remotely and deployed using an Agilent-hosted cloud-based CID Hub. Figure 1 shows a distributed OpenLab CDS deployment including both a CID and an AIC. Although CIDs and AICs have many similarities, only CIDs have the connectivity features that make it visible and accessible in the Agilent CID Hub.

As shown in Figure 1, CIDs have two network interfaces: one connected to the corporate Wide Area Network (WAN) and CID Management Hub (via the internet), the other connected to a private lab/instrument Local Area Network (LAN) or directly to an instrument.

A detailed network connectivity diagram including components and interfaces described in subsequent sections of this document is described here.

Outgoing endpoints

The following URL(s) will need to be whitelisted in the local network for CIDs to be able to connect to the CID Hub:

1. ***.cid.agilent.com**
   - Registration APIs are used by CIDs to communicate with the Hub and query for its configuration and settings information. CIDs also update their status on the Hub using these APIs.
   - IoT commands and tasks issued to CIDs from the Hub webpages (like "install a driver") are sent to the corresponding CID via the Agilent AWS IoT core service. CIDs connect to the IoT Core Service to look for messages.

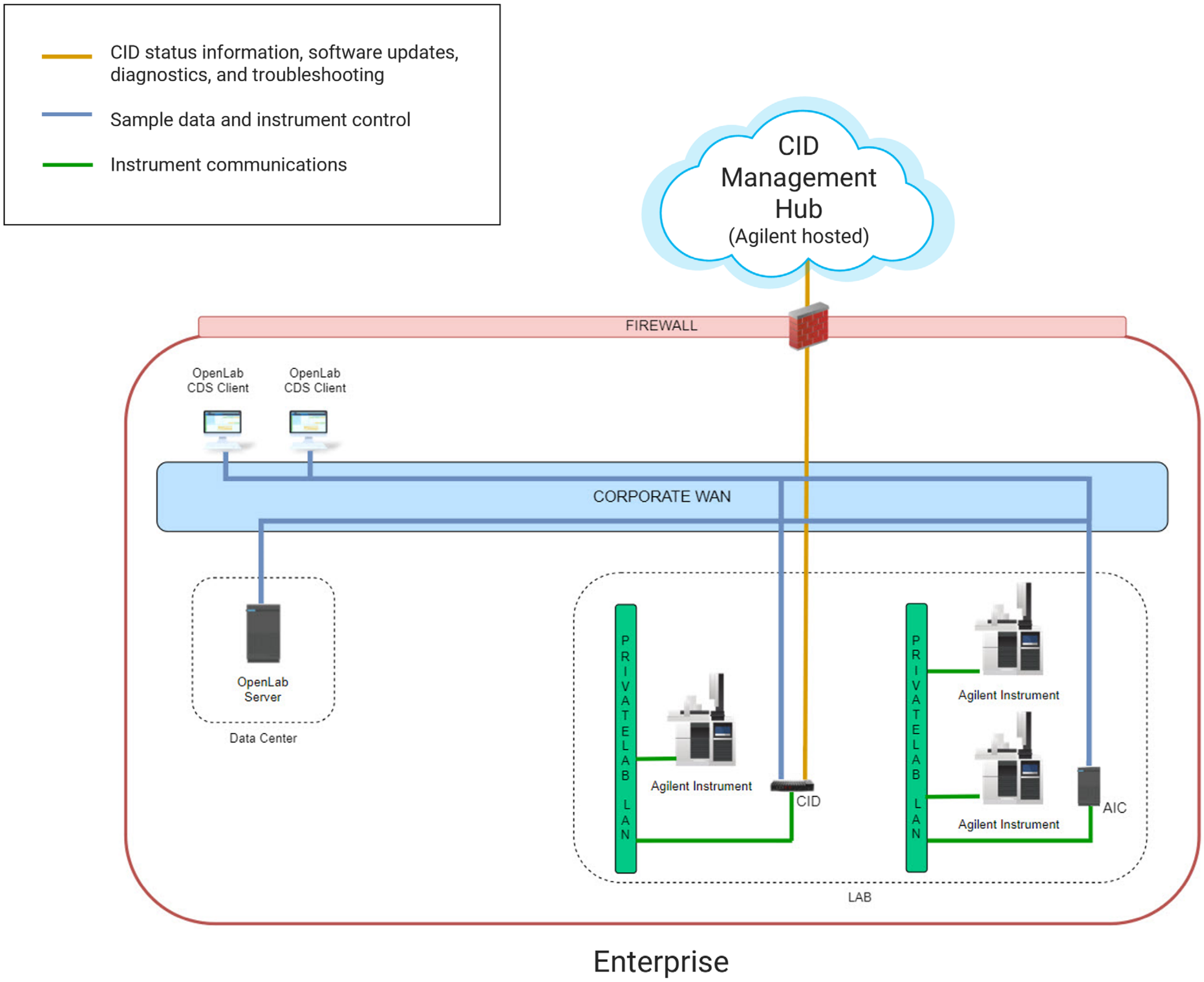

Figure 1. Network Deployment Diagram

- The Agilent AWS S3 bucket stores installation files and release notes related to CDS, drivers, and both Microsoft Windows and Linux updates.

2. **Data.tunneling.iot.*AWS_REGION*.amazonaws.com, i.e.** Data.tunneling.iot.us-west-2.amazonaws.com
   - Secure tunneling proxy service to establish bidirectional communication to CID over a secure connection that is managed by AWS IoT.
   - AWS_REGION can be found at https://hub.cid.agilent.com/health under the IOT section.

Operational interfaces

All incoming and outgoing connections to the CID from CDS clients are on TCP port 443 and are standard HTTPs or Secure Web Socket (WSS) connections. These are shown as dashed black lines in Figure 2. These are the same operational interfaces exposed by an AIC running in Windows, but the CID is not a Windows PC. Instead, the CID is an IoT device that natively runs a version of Linux. A network scan of the CID shows only a single (Linux) IP address with only port 443 open. CDS client connections are served by an embedded Windows virtual machine (VM) that does not have an IP address visible to the corporate WAN. The CID Reverse

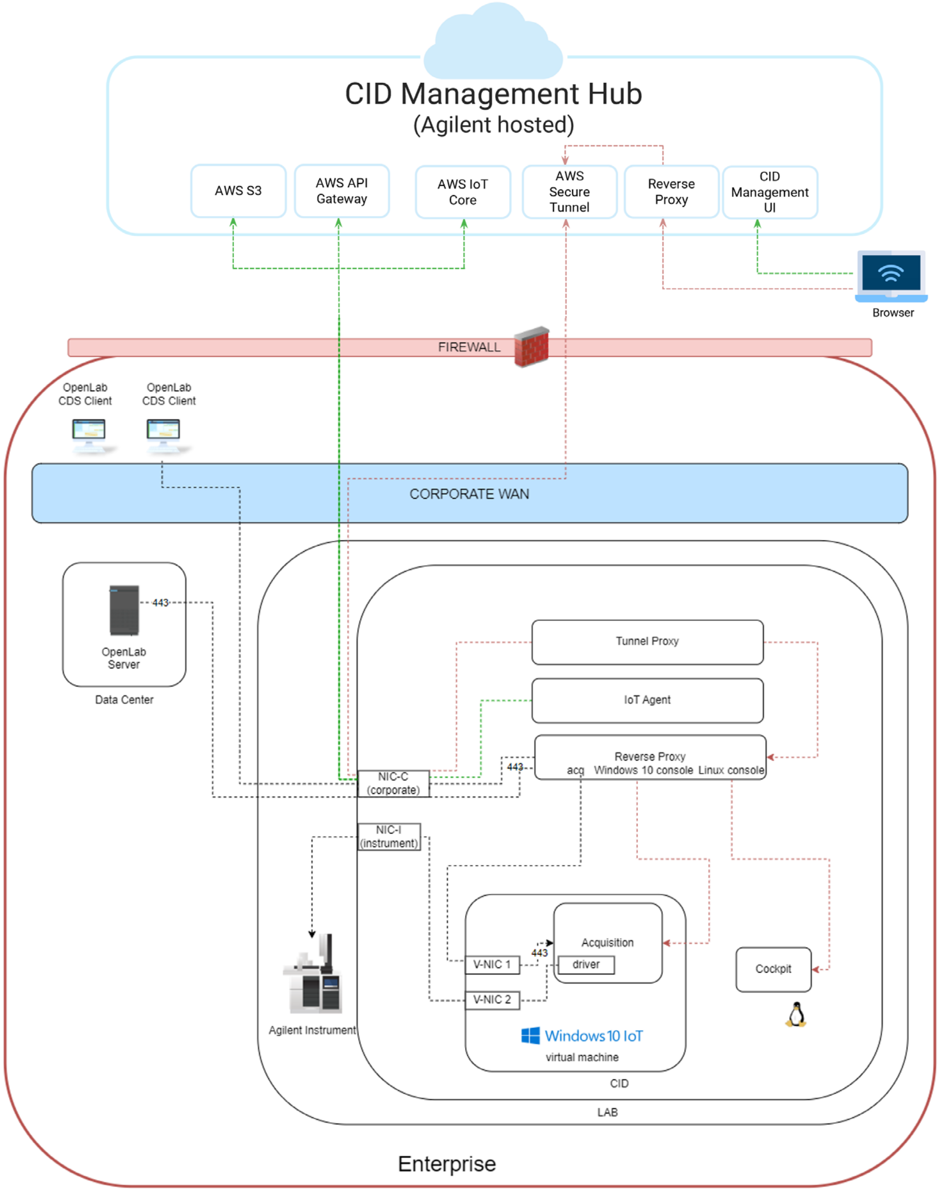

Figure 2. Network Connectivity Diagram

Proxy component (shown in Figure 1) acts as a firewall, shielding the Windows VM from all incoming network traffic except connections from CDS clients. Outbound network connections from the CID to the backend CDS components use a reverse proxy mechanism which makes the source IP address for these connections be the IP address of the Linux system. The operating system (OS) for the Windows VM is Windows 10 IoT Enterprise LTSC, which is Microsoft's OS for IoT appliances that do not require domain policies, and where no Windows updates are required to be managed by IT. This can be centrally handled by the Agilent CID Hub Management system. Running the Windows system as a VM that does not have an IP address visible to the corporate network adds a layer of protection.

Network connections from the Windows VM to instruments use a separate virtual network interface card (V-NIC) in the Windows VM which is passed through the Linux OS to the instrument network. This arrangement directly exposes the Windows VM's IP address for this network to instruments, but this network interface is meant to be either directly connected to an instrument or to an instrument network that has no external exposure (i.e. no internet access).

Connected Instrument Device (CID) Hub for OpenLab CDS

Agilent CID Hub is a multitenant cloud web application where each tenant has a separate and isolated account. Users log into their account on the website to manage CIDs and additional users. Agilent CID support personnel have only view access to CIDs in the account. Logins to the account are authenticated using AWS's Cognito service.

The CID Hub website also registers and activates CID devices. When a CID connects to the internet for the first time, it attempts to register with the CID Hub using REST APIs. As part of the registration process, a unique X.509 IoT device certificate is generated and downloaded to the device. This certificate is then used to connect to the CID Hub, which uses the AWS IoT infrastructure. Only standard HTTPs and Secure Web Socket outbound connections are made from the CID to the CID Management hub. If the corporate firewall restricts outbound connections to these endpoints, the CID will not be able to connect, and will not be able to be managed using the CID Hub. All connections from the device to the Hub are TLS encrypted. Please refer to the section on outgoing endpoints for additional information. CIDs do not require any inbound communication from the CID Hub and are not exposed to the internet.

This IoT connection from the CID to the CID Hub is not necessary for using CDS (i.e., instrument control, running samples, etc.). The IoT connection is required for managing CIDs from the CID Hub. These connections are shown as green dashed lines in Figure 2.

Window Virtual Machine Console

The CID Hub supports the ability for users to access the Windows console of the embedded Windows virtual machine for troubleshooting purposes and in cases when CDS failover is required. Users can access the Windows desktop of the virtual machine by logging in using the user ID and password provided on the CID Hub. The password for this user is automatically recycled once per day (this process is executed only if the CID is connected to the CID Hub).

When a user is within the same network as the CID, they can access the Windows console from the CID Hub via the local network, using a web browser. They can also access it by typing the following URL into a browser: https://CID-FQDN-or-ip-address/aic-windows-desktop. To log into Windows, the user still needs to retrieve the Windows user ID and password from the Hub and to enter it in the Windows login dialog box.

When a user is not within the same network as the CID, the CID Hub provides access to the Windows console via IoT tunneling. Once the IoT tunnel is active, the user can access the Windows console of the embedded Windows VM after logging in with the local Windows username and password.

If Agilent support needs to access the Windows console, they initiate a request from the CID Hub which then needs to be explicitly approved or rejected by an authorized user in your account. Agilent support can access the Windows console only when approved by an authorized user.

Only authorized users as mentioned above are allowed to initiate and access the console, which is only accessible while they remain logged in and on the CID page (CID from which the session is initiated) on the CID management hub. These IoT connections are shown as red dashed lines in Figure 2. These connections are Secure Web Socket connections established from the CID to the CID Hub. Technical details about AWS Secure Tunneling are available at https://docs.aws.amazon.com/iot/latest/developerguide/secure-tunneling.html. Users can see if IoT connections are active from the CID Hub, and can terminate any active connection.

Linux Cockpit

Linux Cockpit (https://cockpit-project.org/) is a web-based management interface to the Linux OS of the CID, and is provided for troubleshooting purposes. This interface can be accessed only by administrators in your account. Agilent support can also access it after initiating a request from the CID Hub and getting approval from an administrator in your account. Linux Cockpit also requires a user ID and password, which is provided on the CID Hub. This password also is recycled once per day.

When an administrator is within the same network as the CID, they can access Linux Cockpit from the CID Hub via the local network using a web browser. They can also access it by typing the following URL into a browser: https://CID-FQDN-or-ip-address/ac-cockpit. To log in, the administrator still needs to retrieve the user ID and password from the Hub and use it to log into Cockpit.

When the administrator is not within the same network as the CID, the CID Hub provides access to Linux Cockpit via IoT tunneling. Once the IoT tunnel is active, the administrator can access the Linux Cockpit after logging in with the user ID and password retrieved from the CID Hub.

Only authorized users as mentioned above are allowed to initiate and access Linux cockpit, which is only accessible while they remain logged in and on the CID page (CID from which the session is initiated) on the CID management hub.

Connected Instrument Device (CID) Hub Health Page

The CID Hub Health page is a network connectivity and performance assessment tool and is accessible at https://hub.cid.agilent.com/health. This tool attempts to connect to the CID hub and reports if connections are "OK" or there are any connectivity issues. It also measures network performance and reports whether or not the performance is acceptable.

Connected Instrument Device (CID) Hardware

The CID hardware is an IoT device that comes ready for instrument connectivity with pre-installed Operating System (OS) and OpenLab CDS software. For more details, contact your local Agilent sales representative.

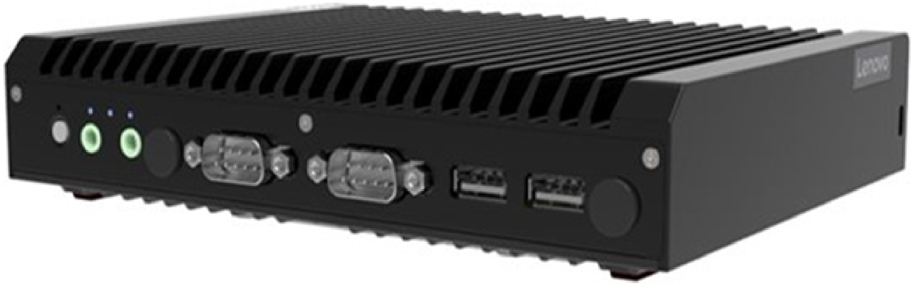

Figure 3. Agilent Connected Instrument Device (CID) for OpenLab CDS physical hardware configuration.
Note: Actual device may appear different than the image shown.

DE36839239

This information is subject to change without notice.

Printed in the USA, May 24, 2024
5994-7490EN

Agilent
Trusted Answers