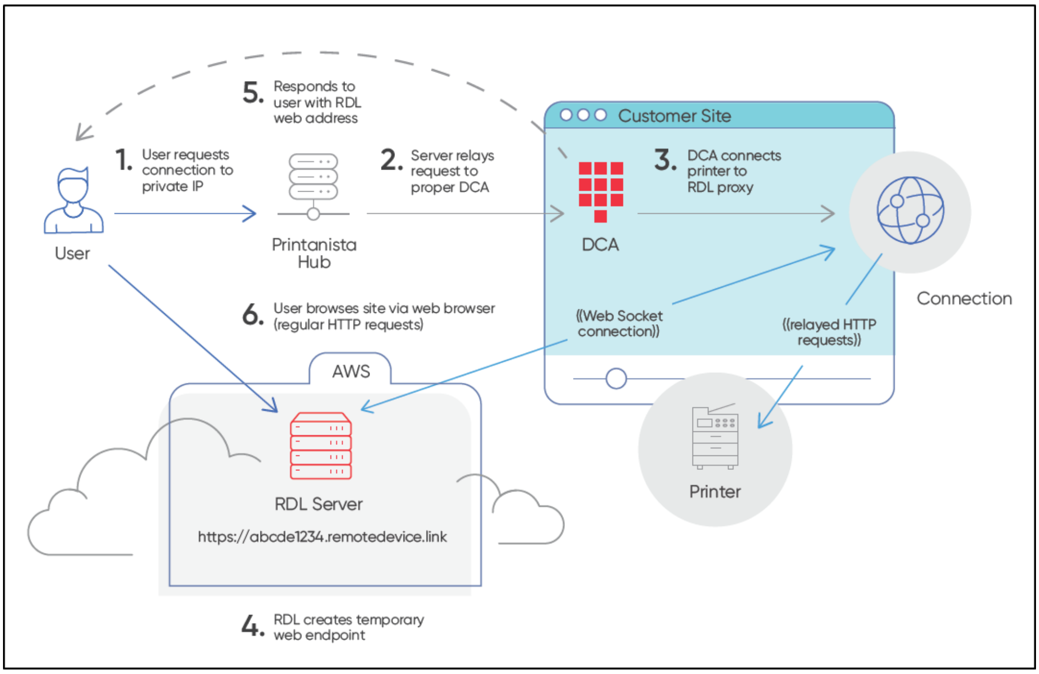
KDFM Printanista

Remote Device Link - RDL


5. Responds to user with RDL web address
1. User requests connection to private IP
2. Server relays request to proper DCA
Customer Site
3. DCA connects printer to RDL proxy
User
Printanista Hub
DCA
Connection
6. User browses site via web browser (regular HTTP requests)
((Web Socket connection))
((relayed HTTP requests))
AWS
RDL Server
https://abcde1234.remotedevice.link
Printer
4. RDL creates temporary web endpoint

System Overview – Remote Device Link (RDL)

Remote Device Link (RDL) is a service allowing a remote end-user to access an HTTP endpoint on a private LAN. There are 4 major components to it:
1. The **end-user** accessing the device
2. The **Remote Device Link server**, on public internet (via https://*.remotedevice.link URL)
3. The **RDL client** (embedded in the DCA), running on the private LAN
4. The **HTTP endpoint** (printer) being accessed (running on the private LAN)

Security: Ports and SSL (Secure Sockets Layer)
The public-facing path for RDL is always an https:// URL on port 443, regardless of the endpoint port and/or SSL status.

Enablement and Permissions
1. Global enablement option per dealer instance
2. Local enablement for each end-customer account
3. Permissions are required for a user to be able to access the feature

Auditing Capabilities
1. KDFM Printanista local auditing of each session details
    a. Printanista Hub Administration reports for Remote Device Link (RDL) Auditing
2. Remote Device Link (RDL) AWS (Amazon Web Services) cloud logging of all session details.

Remote Device Link (RDL) Security
Security of Remote Device Link (RDL) was a key concern when developing this tool.

Authorization:

- User must have permission from within KDFM Printanista to access Remote Device Link (RDL) feature on the specific account
- The Data Collection Agent (DCA) will only accept Remote Device Link (RDL) requests from KDFM Printanista server which is mutually authenticated
- The Data Collection Agent (DCA) only establishes Remote Device Link (RDL) connection to known and currently monitored print devices within the Data Collection Agents (DCA) discovery IP range(s).
- Each individual web request must be to the same IP – The Data Collection Agent (DCA) will not follow redirects

Connection Security:

- All connections to and from the Remote Device Link (RDL) and Printanista Hub servers are encrypted using standard TLS 1.2 (Transport Layer Security)
- Each connection is given a unique domain name which uses a 19-character (96-bit) random alpha/numeric combination
- Each request requires a 160-bit security token, stored as a browser cookie, and only set at the very start of the session secured by TLS encryption
- The Data Collection Agent (DCA) may establish a non-encrypted HTTP connection to the print device across the local network, but supports TLS 1.2 if the device does

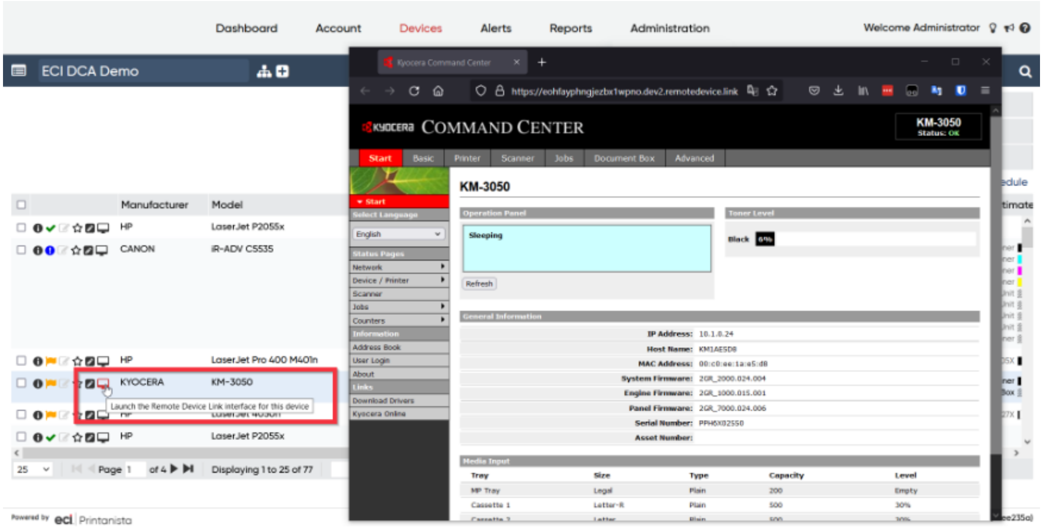
Session Time Limits:

- Each individual Remote Device Link (RDL) session times out after 20 minutes of inactivity by default with an absolute maximum of 2 hours.

Implications

The connection between the DCA and KDFM Printanista is protected by authentication keys that are DCA installation specific, and the connection requires a valid trusted SSL certificate to use over a TLS connection.

All traffic transiting from the DCA to the internet is encrypted. However, the DCA can talk to the device in the local network over plain HTTP connections if the device does not support secure connections.



	Manufacturer	Model
□	HP	LaserJet P2055x
□	CANON	iR-ADV C5535
□	HP	LaserJet Pro 400 M401n
□	KYOCERA	KM-3050
□	HP	LaserJet 4050n
□	HP	LaserJet P2055x

Launch the Remote Device Link interface for this device

25 Page 1 of 4 Displaying 1 to 25 of 77

https://eohfayphngjezbx1wpno.dev2.remotedevice.link

KM-3050
Status: OK

KM-3050

Operation Panel: Sleeping

Toner Level: Black 6%

General Information

IP Address: 10.1.0.24
Host Name: KM1AE5D8
MAC Address: 00:c0:ee:1a:e5:d8
System Firmware: 2GR_2000.024.004
Engine Firmware: 2GR_1000.015.001
Panel Firmware: 2GR_7000.024.006
Serial Number: PPH6X02550
Asset Number:

Media Input

Tray	Size	Type	Capacity	Level
MP Tray	Legal	Plain	200	Empty
Cassette 1	Letter-R	Plain	500	30%
Cassette 2	Letter	Plain	500	30%

FAQs

- *Which brands of equipment will Remote Device Link (RDL) monitoring work with? What are the requirements for it to work?*

  All brands with an embedded webpage are discovered by ECI DCA. The information on the embedded webpages will vary by manufacturer and model. Local devices will not show the embedded webpage.

- *Are there added security concerns with Remote Device Link (RDL)?*

  A secure channel is opened between the device on the local customer network and an operator located outside of that network. RDL will only report back devices discovered and actively monitored through ECI DCA. A message appears indicating device connection is not supported through the DCA

- *Remote Device Link (RDL) seems a bit slow, why is this?*

  This can be expected as the connection needs to be tunneled through our cloud services. However, the main influencing factor is how quickly the devices respond to Web User Interface (UI) requests. We have seen devices responding in tenths of seconds to the first connection attempts, to being influenced by current usage or resources available for the User Interface (UI).

- W*hat features are available with Remote Device Link (RDL)?*

  Any options the OEM provides access to through the embedded webpage are accessible through Remote Device Link (RDL).

- *Can the Remote Device Link (RDL) feature be turned off?*

  Yes, there is the ability to switch this feature off per account. It is also possible to turn this feature off per user, allowing you to block a user’s access to Remote Device Link (RDL).