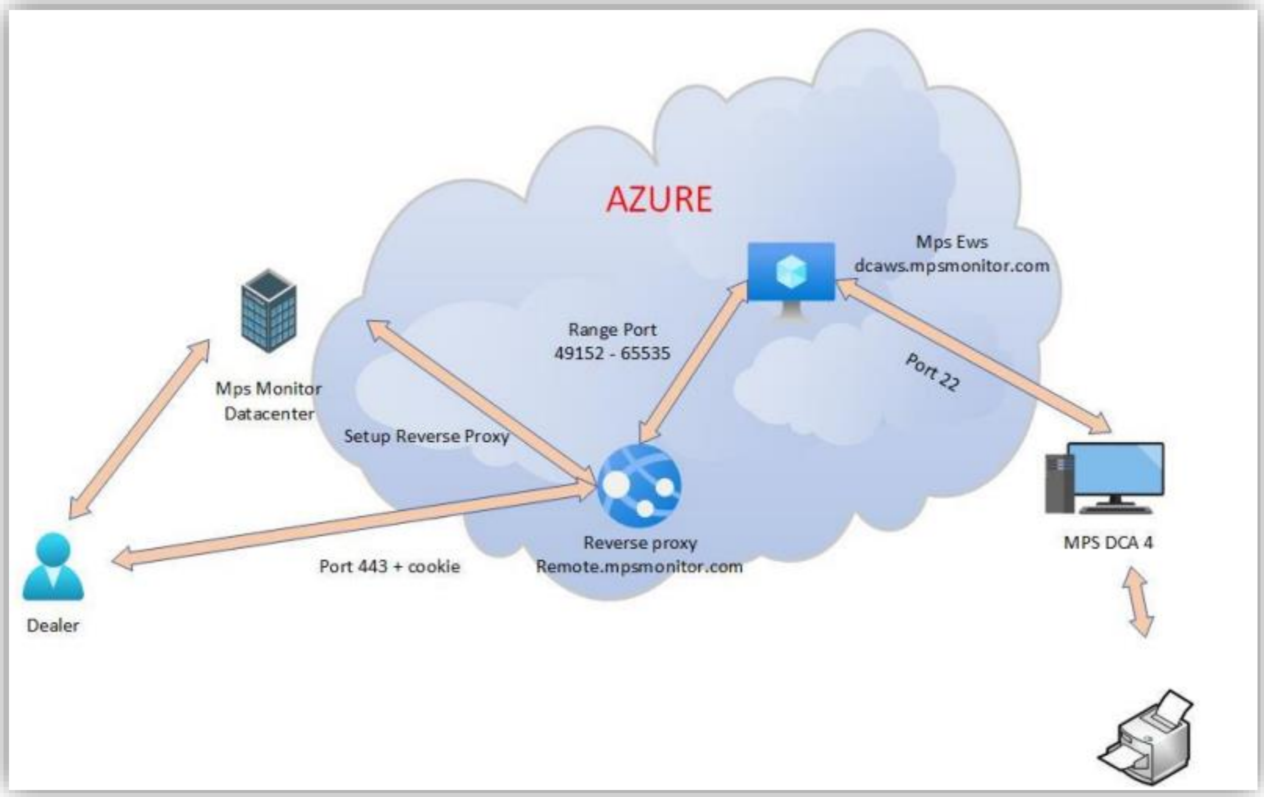
KDFM eXplorer

DEVICE WEB ACCESS

Device Web Access process description DCA 4 allows a user with adequate permissions to connect to the Printers' internal Web Server using the feature called "Device Web Access", which has the following technical specifications and security features:

1. DCA4 receives a Device Web Access connection command from the KDFM eXplorer Portal and verifies that the request is for a managed printer, then creates a Reverse SSH Tunneling.
2. The Reverse SSH Tunneling is based on SSH protocol and it is created from the Web Service Printer Port (typically 80 or 443, or other that can be configured) to a remote SSH server (port 22 / SSH) that can be reached through different domain URLs belonging to the root domain https://*.mpsmonitor.com.
3. Using the SSH protocol the system implements a public-key based authentication and encrypts connections between the printer and the KDFM eXplorer SSH server endpoints.
4. The server-side connection is created as a new tunnel at every connection request, and terminated after every session, with a maximum duration of 10 minutes. The security keys are unique for each installation, and every new tunnel uses a different session ID to avoid session reusing.
5. A complex authentication methodology is implemented to ensure that all the parties involved into each SSH tunnel are legitimate and have the authority to open and maintain the connection.
6. A number of verifications on the device are performed before opening the tunnel to ensure that the target device corresponds to the one on which the connection has been requested. If any of these verification fails, the tunnel is not open.
7. Device Web Access connection is restricted only to selected user profiles and can be activated only by users with strong authentication to the KDFM eXplorer Portal (Two-Factor Authentication or Single Sign-On via Active Directory). This prevents unauthorized or malicious usage of the Device Web Access feature in case of credentials theft.
8. All the web activities performed within Device Web Access are logged on the SSH Server. Customers can access the logs to check the usage of this function by other users.
9. Device Web Access can be disabled on each customer by the user in the KDFM eXplorer Portal, or directly from the DCA 4 local User Interface, by the customer itself. If the function is disabled in the DCA User Interface, it cannot be re-enabled from the Portal, thus ensuring that each customer has the ability to disable this function locally from the system where the DCA 4 is installed.

April 2022



Process description

STEP 1
The dealer connected on kdfmportal.katun.com clicks on the desired printer and requests the DWA to a particular Device.

STEP 2
The portal generates a “Session id” that will be used between the various components to recognize the connection.

STEP 3
The portal sends a command to the DCA to open the connection by passing the following parameters:
- IP Address and Mac Address of the printer
- The Printer web interface port (80 or 443) of the printer that should be forwarded
- The session id to connect
- The SSH parameters
- Other printer’s details like Serial Number, Make and Model

Now the user can work on the printer

STEP 4
The DCA received the command:
1. Verify that the Printer data are equal to the data in its local database and check that it is really a printer.
2. Uses the Windows ssh.exe command and opens an SSH tunnel on dcaws.mpsmonitor.com outbound on port 22
3. Notify the portal that the tunnel is active

STEP 5
The portal connects to remote.mpsmonitor.com using a cookie that contains the Session Id so the Reverse Proxy can forward the requests to the correct forwarded port on the SSH server.
Now the user can work on the printer