OPEN HP WEB JETADMIN REQUIRED PORTS IN THE WINDOWS FIREWALL AND PORTS DIAGRAM

CONTENTS

INTRODUCTION

HP Web Jetadmin listens continuously on several ports and uses other ports for specific functionality. The firewall that you are using might block the connection and prevent HP Web Jetadmin from communicating with the network. Instead of adding firewall rules for these ports one at a time, create a batch file that opens all of the ports that HP Web Jetadmin requires for the Windows Firewall at one time. The batch file applies to Windows Firewall. For other firewall applications, contact the vendor about creating a batch file. Finally, the Ports Diagram shows which ports are needed for different actions. These ports are also described in the Install and Setup Guide.

CAUTION: You must remove any conflicting rules before the firewall allows HP Web Jetadmin to communicate with the network.

CREATE A BATCH FILE

1. Open Notepad or a similar text editor that has the appropriate create and edit permissions.
2. Copy the following commands into a text document.

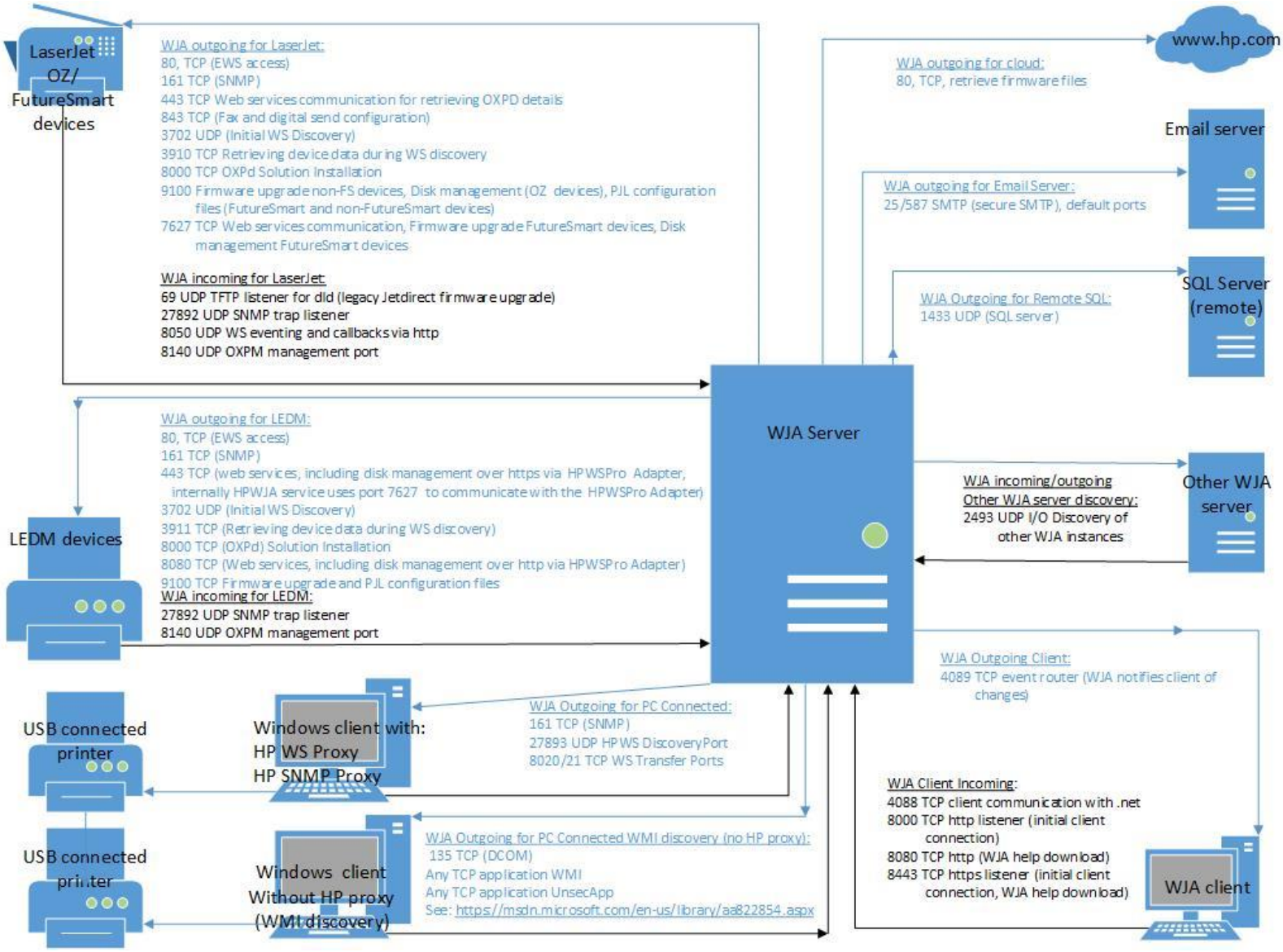
   Note: You can use other names for the firewall rules. The following is only an example for the Windows firewall. If you are using another firewall, the following commands might not work and you must manually update the firewall.

```
netsh advfirewall firewall add rule name="HP WJA TFTP port 69" dir=in action=allow protocol=UDP localport=69
netsh advfirewall firewall add rule name="HP WJA Remote Control Panel of EWS" dir=out action=allow protocol=TCP localport=80
netsh advfirewall firewall add rule name="HP WJA SNMP" dir=out action=allow protocol=UDP localport=161
netsh advfirewall firewall add rule name="HP WJA Discovery: SLP Listen" dir=in action=allow protocol=UDP localport=427
netsh advfirewall firewall add rule name="HP WJA https" dir=out action=allow protocol=TCP localport=443
netsh advfirewall firewall add rule name="HP WJA fax/scan configuration" dir=out action=allow protocol=TCP localport=843
netsh advfirewall firewall add rule name="HP WJA Remote SQL server" dir=in action=allow protocol=UDP localport=1433
netsh advfirewall firewall add rule name="HP WJA Remote SQL server" dir=out action=allow protocol=UDP localport=1433
netsh advfirewall firewall add rule name="HP WJA Discovery: other HP WJA servers" dir=in action=allow protocol=UDP localport=2493
netsh advfirewall firewall add rule name="HP WJA Discovery: other HP WJA servers" dir=out action=allow protocol=UDP localport=2493
netsh advfirewall firewall add rule name="HP WJA Discovery: WS Discovery" dir=out action=allow protocol=UDP localport=3702
netsh advfirewall firewall add rule name="HP WJA Print Request status" dir=out action=allow protocol=TCP localport=3910
netsh advfirewall firewall add rule name="HP WJA Printer Status" dir=out action=allow protocol=TCP localport=3911
netsh advfirewall firewall add rule name="HP WJA client communication" dir=in action=allow protocol=TCP localport=4088
netsh advfirewall firewall add rule name="HP WJA client" dir=in action=allow protocol=TCP localport=4089
netsh advfirewall firewall add rule name="HP WJA Web Services" dir=out action=allow protocol=TCP localport=7627
netsh advfirewall firewall add rule name="HP WJA Discovery Listen" dir=out action=allow protocol=UDP localport=8000
netsh advfirewall firewall add rule name="HP WJA client UI and WJA Help (http)" dir=in action=allow protocol=TCP localport=8000
netsh advfirewall firewall add rule name="HP WJA Pro Adapter" dir=out action=allow protocol=TCP localport=8080
netsh advfirewall firewall add rule name="HP WJA Device communication: WS eventing" dir=in action=allow protocol=TCP localport=8050
netsh advfirewall firewall add rule name="HP WJA OXPm Web Services (http)" dir=in action=allow protocol=TCP localport=8140
netsh advfirewall firewall add rule name="HP WJA OXPm Web Services (https)" dir=in action=allow protocol=TCP localport=8143
netsh advfirewall firewall add rule name="HP WJA Client UI and WJA help (https)" dir=in action=allow protocol=TCP localport=8443
netsh advfirewall firewall add rule name="HP WJA file transfer to printers" dir=out action=allow protocol=TCP localport=9100
netsh advfirewall firewall add rule name="HP WJA SNMP Trap Listener" dir=in action=allow protocol=UDP localport=27892
netsh advfirewall firewall add rule name="HP WJA Communication with WS Proxy Agent" dir=in action=allow protocol=UDP localport=27893
netsh advfirewall firewall add rule name="HP WJA Communication with remote SQL server" dir=out action=allow protocol=TCP localport=59113
netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
```

   Note: The last rule is only required for discovering PC-connected devices when no HP proxy server is installed.

3. Save the text document with a name such as firewall_changes.bat.
4. To execute the changes, double-click the file.

PORTS DIAGRAM



c05337591EN, Rev. 4, July 2017