White Paper

DSS 5 – Bidirectional Communication between the DSS Server and Devices

Date Written: 10/31/2014

Digital Sending Software 5

Bi-directional Communication between DSS Server and Devices

Whitepaper

Table of Contents

Introduction

DSS 5 servers require bi-directional (Bidi) communication between the server and managed devices for most DSS functions to operate properly. In this context communication means that one endpoint of the communication (either the DSS server or the device) can initiate a TCP-IP communication with the other endpoint. For example, if the DSS server initiates a communication with a device and the device is able to answer during the same communication session this does not prove bi-directional communication, this would only be considered uni-directional communication from the DSS Server to the Device. For the communication to be bi-directional the device would also have to be able to initiate a communication session with the DSS Server.

DSS servers communicate with FutureSmart devices over TCP port 7627. DSS servers communicate with pre-FutureSmart devices over port 1783.

Symptoms of Bidi Problems

If communication between the DSS server and the device are blocked in both directions the administrator will get an “unable to communicate” error when trying to add the device, or while performing a Status update to an already bound device.

It is possible for a device to be added to DSS with only uni-directional communication enabled from the DSS server to the device. If this is the case there will be problems encountered with job processing later when end users try to send jobs from the devices. Jobs will fail. There can be others errors as well, such as the auto-completion of email addresses will fail.

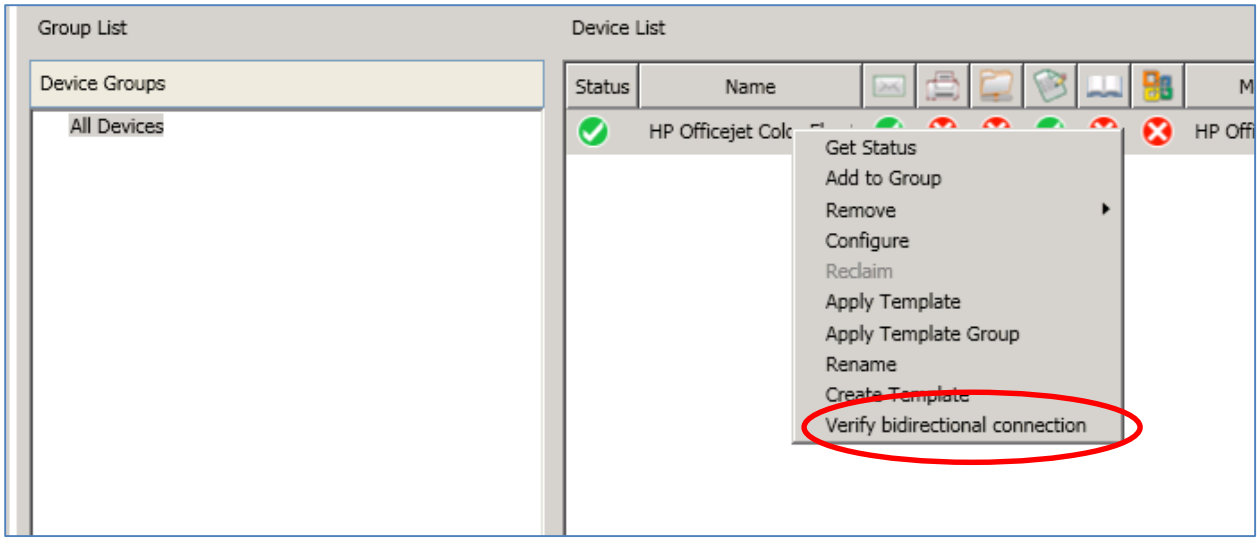
Testing

Starting with DSS 5.01.02 the automated and manual testing of bidi communication has been implemented and/or improved from past versions. The available tests change depending on device type: FutureSmart or pre-FutureSmart.

FutureSmart Devices

Automated testing has been added to the system for testing bidi communication with FutureSmart devices. Every time the DSS service is started, DSS will do a bidi test with the first FutureSmart device added to DSS. The test will wait up to 1 minute for the device to do its part to initiate a conversation with the DSS server, if that conversation is not started within 1 minute the test fails and the administrator is informed of the failure. If the test passes it typically will not add more than 5 seconds to the device add process.

A manual test has also been added that can be run on FutureSmart devices. This is to cover the scenario where the administrator feels bidi communication may be an issue after the system has done its single automated test. To run the test, from the Device Configuration tab of the Configuration Utility, right click on the device to be tested. In the menu that opens select the “Verify bidirectional connection” item.



If a bidi test fails there will be a message presented to the user on the DSS server display, as well as an error entered into the DSS log which can be viewed on the log tab of the DSS service in the Configuration Utility.

Pre-FutureSmart Devices

Every pre-FutureSmart had an automatic bidi test done when it is added to DSS. This has always been the case with DSS 5 but the reporting was poor. If the test fails now an error is entered into the DSS log which can be viewed on the log tab of the DSS service in the Configuration Utility.

Possible Causes of Bidi Problems and Debugging Tips

There are two primary known causes for bidi problems:

- Blocked TCP ports in the communication channel
- Errors on the device validating the DSS certificate

Blocked TCP Ports:

The most common cause of communication problems are blocked ports somewhere in the infrastructure. This is most common with FS devices since port 7627 is a well-known port for web services communication. It is also possible for port 1783 to be blocked, but since this is not a widely used port it is less common.

It is very common in today's security conscious world that IT administrators block ports by default and only open what they need. When opening these ports for DSS use the administrator must know that they have to be opened bi-directionally and not just out from the DSS server. The most common problem occurs with port 7627 open from the DSS server out, but closed from the outside world into the DSS server.

The ports can be blocked in many places in the infrastructure. Many times there will be a firewall on the DSS server itself which will block the ports, but port blocking can also occur on other network devices such as routers and switches.

If it is suspected that a port is blocked it can be very useful to use a network capture utility like Wireshark to analyze network traffic. With the capture utility capturing packets at the DSS server, initiate a job from the device and capture the traffic. If no packets are seen at the network interface that originate from the device then the port is being blocked in the network infrastructure and not on the DSS server itself. But, if the traffic is blocked on the DSS server then what will be seen is an initial packet coming in from the device that is repeated every 3 seconds for about 30 seconds. This is because the packet sent from the device to start a communication with the DSS service reaches the network adaptor, but the firewall prevents it from getting to the DSS service so the service never acknowledges the incoming packet. The device, not getting an acknowledgement, will retry every 3 seconds until it gives up after 30 seconds.

Errors in Certificate Validation

This section applies only to FutureSmart devices. FutureSmart devices communicate with DSS using a SSL/ TLS secure channel which requires an exchange of certificates between the device and the DSS server. The certificate that the DSS server gives to the device is a self-signed certificate with a date range that starts when the DSS instance was installed.

Starting in FutureSmart firmware from November 2014 the FutureSmart devices have server certificate validation enabled by default. This means that when an external server gives the device a certificate for SSL/TLS communication the device checks the certificate to make sure it is valid.
The most common certificate validation error we have seen is due to date checking. The DSS server's certificate has a valid start date from when DSS was installed and an end date way in the future (more than 20 years). If the device has an incorrectly set date, one that is outside of the range for valid dates for the DSS server's certificate, then certificate validation will fail. When certificate validation fails the device is unable to initiate communication with the DSS server.

The FutureSmart devices will log any certificate validation failures in the device's event log. If jobs are failing the manual bidi test should be run. If it fails, the event log of the device should be checked for certificate validation errors. The error code to look for is 44.A0.A1.