

IT/Network Troubleshooting

Each customer and hospital IT department can implement their own unique security and firewall policies that can impact .decimal's software. This guide provides some general troubleshooting steps to help IT departments ensure they are not blocking or interfering with .decimal software and the HTTPS requests to .decimal's servers that are required to install, authenticate, and place device orders.

Traffic Architecture

.decimal's applications communicate via HTTPS to our server resources. The diagram below demonstrates how our HTTPS traffic flows through each piece of infrastructure and identifies common failure points:



Notes

- 1 .decimal client software is provided by .decimal and installed on your network computers.
- 2 The customer's local PC in which the .decimal client software is installed. This may include local Antivirus or software firewalls that can hinder and impede .decimal software and traffic if not configured correctly.
- 3 The customer's unique security and firewall configuration. This may include any number of network firewalls, web security appliances, proxies, etc. .decimal client software traffic passes through your facilities IT security devices, which can impede and hinder that HTTPS communication. Each device within your facility's network security suite that .decimal's traffic flows through should have an exception for each required .decimal url/port.
- 4 .decimal HTTPS traffic can have multiple destinations depending on the software being installed. Refer to the software's Network and System Requirements document provided by .decimal Staff. At a minimum the URL `direct.dotdecimal.com` (64.128.252.104) port 443 is always used.
- 5 .decimal's internet firewall. We do not blacklist or filter our own HTTPS traffic.
- 6 .decimal's server infrastructure within our network. Our servers accept your HTTPS traffic as received from .decimal's client software after it exits your network security devices.

Common Issues and Resolutions

1. Blocking or filtering the required .decimal urls or ports:

- .decimal applications require specific urls(or IPs) and ports to be unblocked and unimpeded in order to authenticate and place orders to .decimal's servers. Refer to the System and

Network Requirements document provided by .decimal staff. At a minimum the url `direct.dotdecimal.com` (64.128.252.104) port 443 is always used.

2. Proxies / Web Security Appliance (WSA):

- Some WSAs will attempt to decrypt and inspect our HTTPS traffic. Some customers have needed to include an exception in this network security device as this can impact and cause our encrypted and authenticated HTTPS traffic to encounter errors while in transit between the client software installed at the clinical facility and .decimal's servers.

Troubleshooting Steps

The following steps may help when troubleshooting network security and IT issues for your facility.

1. Compatibility Checker

Running the compatibility checker will ensure that all required .decimal IP addresses and ports are not being blocked.



Note:

The Compatibility Checker only ensures that the primary .decimal IPs and ports are not being completely blocked or blacklisted. Additional network security devices may impede or be filtering the HTTPS traffic. If .decimal software continues to encounter problems, please ensure other network security appliances and devices are not filtering or impeding .decimal's HTTPS traffic.



Notes

1 Connectivity Tests

The connectivity tests will test each of the following:

1. **Direct URL** (<https://direct.dotdecimal.com>): Test access to the decimal Direct site.
2. **Update URL** (<https://update.dotdecimal.com>): Test access to the decimal Update server for installing and updating p.d 5.3.
 - o This test is required for p.d 5.3 only. Other software and versions of p.d can ignore the results of this test.
3. **Direct API** (<https://direct.dotdecimal.com/api>): Test access and traffic to the decimal Direct API.

If any test above fails, then a required URL/Port is being blocked. Refer to the System and Network Requirements document provided by decimal staff. You may also refer to the .decimal client app network requirements for each application's latest network requirements (please ensure you have the correct application and app version). For failing tests, the "Error Info" link will provide details about why the test failed.

Test Limitations: Connectivity tests attempt to replicate the HTTPS traffic and connectivity to decimal remote resources that client .decimal applications will need to function. If security software/hardware further limit traffic based on software or implement other access rules, the compatibility checker may still show passing tests even though the .decimal client software encounters issues.

Please refer to Proxies / Web Security Appliance (WSA) for further details.

2 Advanced Tests

1. Legacy Login Test

- o This test allows users of p.d 5.3 to further diagnose network or login issues to .decimal servers.
- o **Users using this test must have a "legacy" username that is NOT an email address.** Users of the decimal Launcher and .decimal applications installed by the Launcher (e.g.: p.d 5.4, eRT, Bolus Designer, etc) will be unable to use this test.
- o This test simulates a p.d 5.3 login to the Direct API and will use the resulting login token to attempt and execute a HTTPS GET request to get the logged in user information.

2. Guest/Unrestricted Network

This option is advised if your network IT has whitelisted and unblocked .decimal's urls and ports but you still encounter issues using .decimal's software and communicating to .decimal's servers.

1. Attempt to download and install the .decimal client software on a device (e.g.: a laptop) not connected to your main cooperate network (e.g.: a guest WiFi network or smart phone hotspot) that has absolutely zero security or firewall blocking, filtering, or packet inspection.
2. Attempt to login to the .decimal client software
3. Confirm you are able to download, install, login, and use the .decimal software on an unrestricted device on an unrestricted internet connection. This ensures no security, firewall, or packet inspection security policies are interfering with your HTTPS connection and traffic to .decimal servers.

1. **Conclusion:** If Step #3 passes, then there is still security policies in place on your main

facility network impeding .decimal HTTPS traffic.

From:

<http://apps.dotdecimal.com/> - **decimal App Documentation**

Permanent link:

http://apps.dotdecimal.com/doku.php?id=support:it_troubleshooting&rev=1637184461

Last update: **2021/11/17 21:27**

