Eidola Application Note #1

Quick set up and test of an EiPi™

IDmachines LLC
1264 Beacon St. #5
Brookline, MA 02446
eidola@idmachines.com
+1 617.201.4809

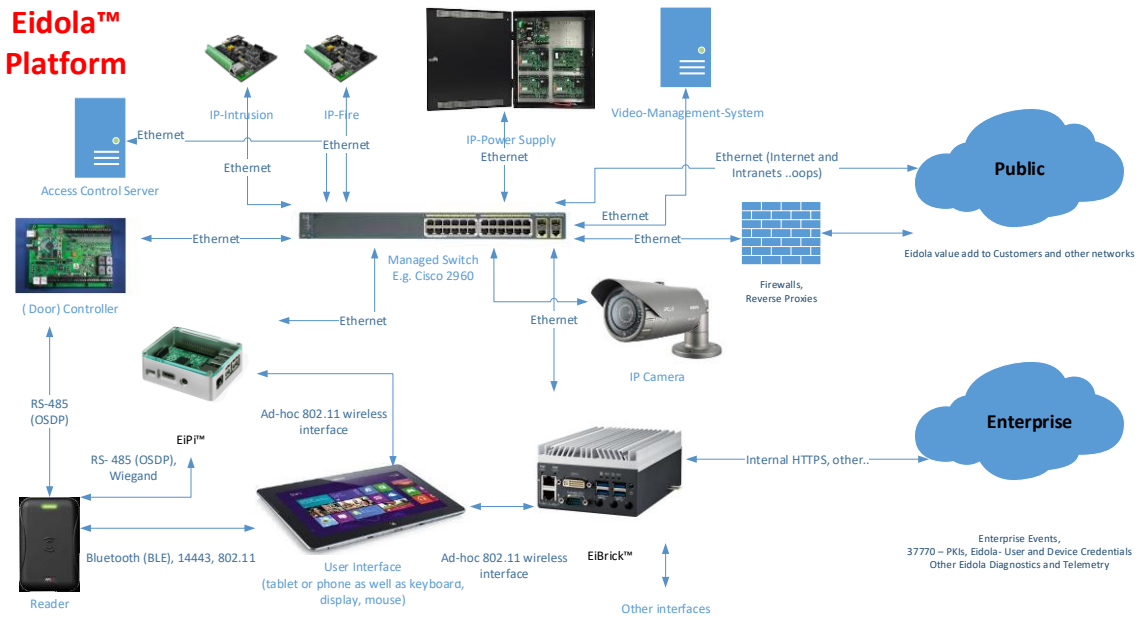
Introduction to Eidola

The Eidola platform consists of a set of tools to help manage the lifecycle of networked devices, in particular security systems and their related components. The primary tools consist of network and infrastructure services and diagnostics that help configure, integrate, certify and maintain security systems. These are combined with requirements and guidance IDmachines has produced, sometimes in concert with manufacturers to provide hardened configurations of security systems. The Eidola™ baseline diagnostics provide you with a set of tools that creates a foundation for the delivery of high-assurance security systems. Eidola puts you and your organization in a position to address, meet and profit from the challenges of networked physical security systems, IoT and the connected world we all live in.

Basic Steps

The goal here is to quickly allow you to see how Eidola tools interact with security systems and components. We often provide an EiPi™ as a demo unit so you can become familiar with how to integrate the Eidola platform into your services. At it's heart Eidola provides you with information about security systems and devices. We want you to exercise the tools and begin to collect information and put in place processes that improve you security services in a number of way.

So, let's plug an EiPi into a security system network, along with a laptop. We will open up shell (command line), ssh (for secure file transfer) and browser interfaces to the EiPi, run some tests and look at the results. The following is a rough drawing showing an EiPi (and EiBrick) plugged into a switch (Cisco in this case).



Not trying to do any OSDP reader connections yet…. See Eidola Application Note #5 and #6 for Open Supervised Device Protocol toolkit getting started.

Basic steps here:

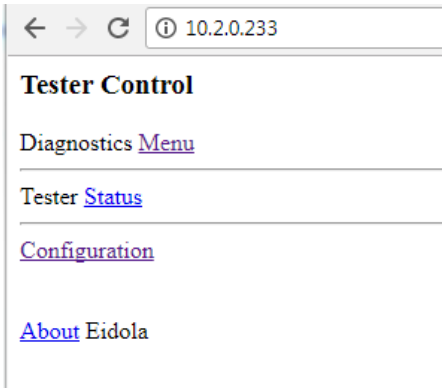
1. Plug in the EiPi
    a. Put power to device with micro USD and 5v 2.4A wall wart supplier or equivalent.
        i. When operating normally a red LED with an occasional green flash on the solid
        ii. The power cord shipped with the EiPi has a switch
    b. Connect EiPi to managed switch with RJ-45 CAT cable
        i. Normal is orange and green lights when a network connection is established
    c. Connect long-range wireless antenna (optional).

2. Set-up other device for communication, typically laptop or tablet.
    a. Connect laptop to managed switch.[1]
    b. Connect laptop to EiPi ad hoc wireless network. An SSID in the Eidola-Tester-xxx format should appear where xxx is number on EiPi label for its shipping fixed IP address (10.2.0.xxx) (configurable later).
    c. Connect tablet to EiPi ad hoc wireless network.

3. Connect Laptop, Table or Phone to EiPi
    a. Open a browser https://10.2.0.xxx (wired if set up for 10.2.0.xxx network) or https://10.2.2.1 (to get screen below)[2] (see Appendix A which includes defaults username and password)
    b. Open a shell session with PuTTy (for example) to same address (alternately you can connect a USB keyboard and monitor via HDMI port)
    c. Open a WinSCP (or other SFTP) connection to same address.

[1] First time through it is suggested that you set up a small test network. However, if you want to plug the device directly into an existing network you will need to set the appropriate network parameters for the EiPi™ and laptop. Alternately setting up a 10.2.0.xxx or 192.168.1.xxx e.g. network with a switch and devices (door controllers, camera, workstations) is a good way to get started.

[2] Particularly with demo units you will get a number of warnings due to the fact that certificates have not been loaded. Depending on the browser you will need to e.g. in Chrome go to advanced at bottom of screen and create a security exception. Security of the devices on production networks is something we take seriously. Certificate management is covered in Eidola Application Note #7.



4. Configure (confirm) EiPi Setting w/Browser
    a. Select Configuration
    b. Eidola Device Mode (infrastructure or stand-among) (shipped default in Preset 1 for EiPi and 2 for EiBrick)
    c. No need to touch these now.
    d. Click on parameters in Manage diagnostic parameters as shown below.

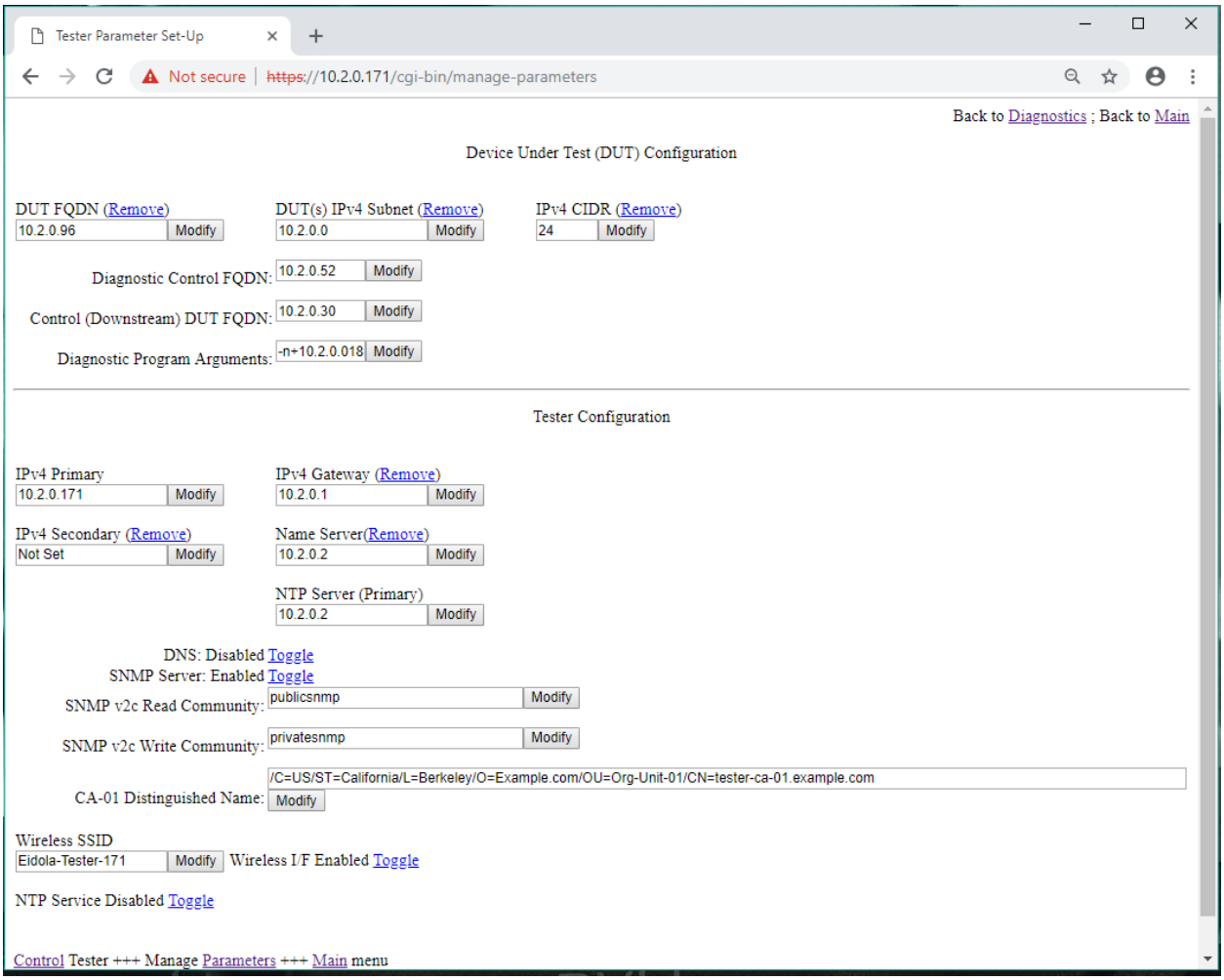
Manage diagnostic parameters

Preset Configurations

Load Preset No. 1 (Static IP eth0 10.2.0.209 server-209.example.com)
Load Preset No. 2 (Static IP eth0 10.2.0.2 etc. full stand-alone services ns-1.example.com)
Load Preset No. 3 (DHCP lease on ethernet, wireless at 10.2.2.1, no network services)
Load Preset No. 4 (Static IP eth0 192.168.0.209, wireless at 10.2.2.1, no network services)
Load Preset No. 9 (Special Services)

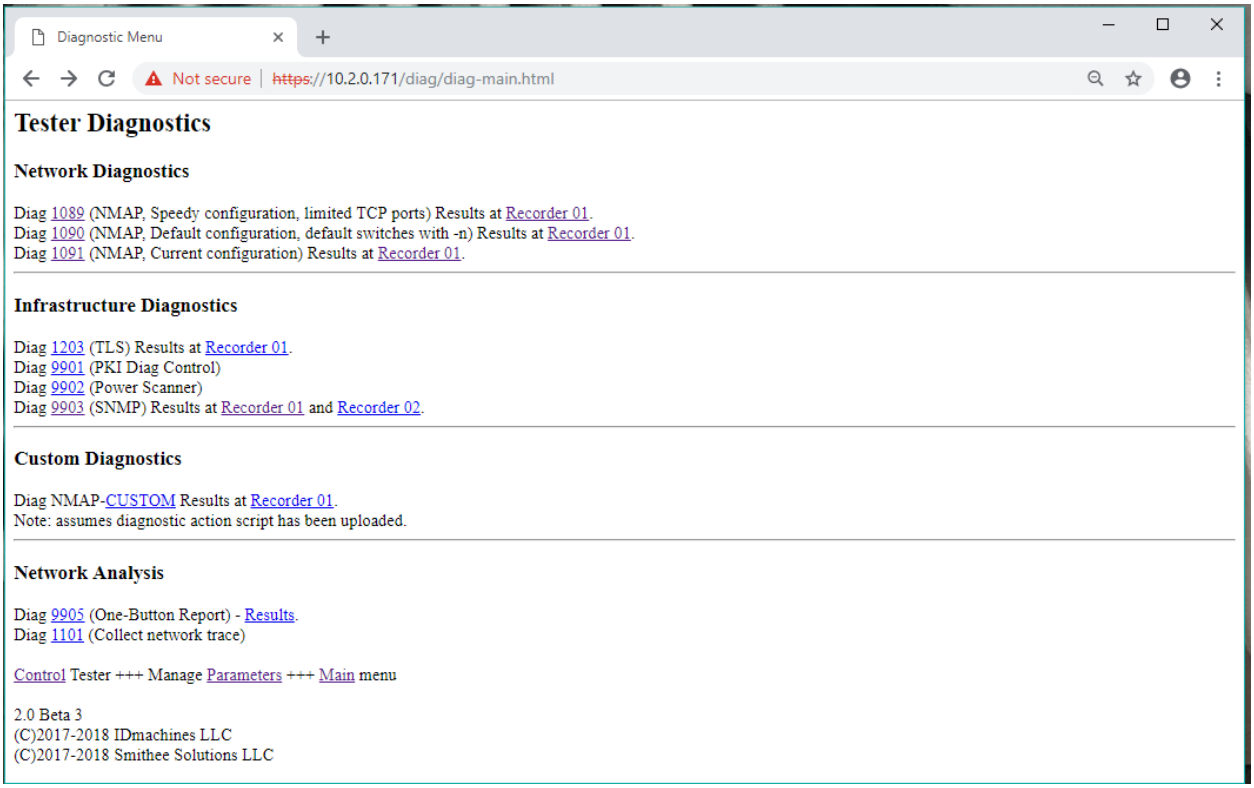
Immediate Commands

Tester Reboot NOW +++ Tester Power-Off NOW +++ Clear SYSLOG NOW +++ Main menu

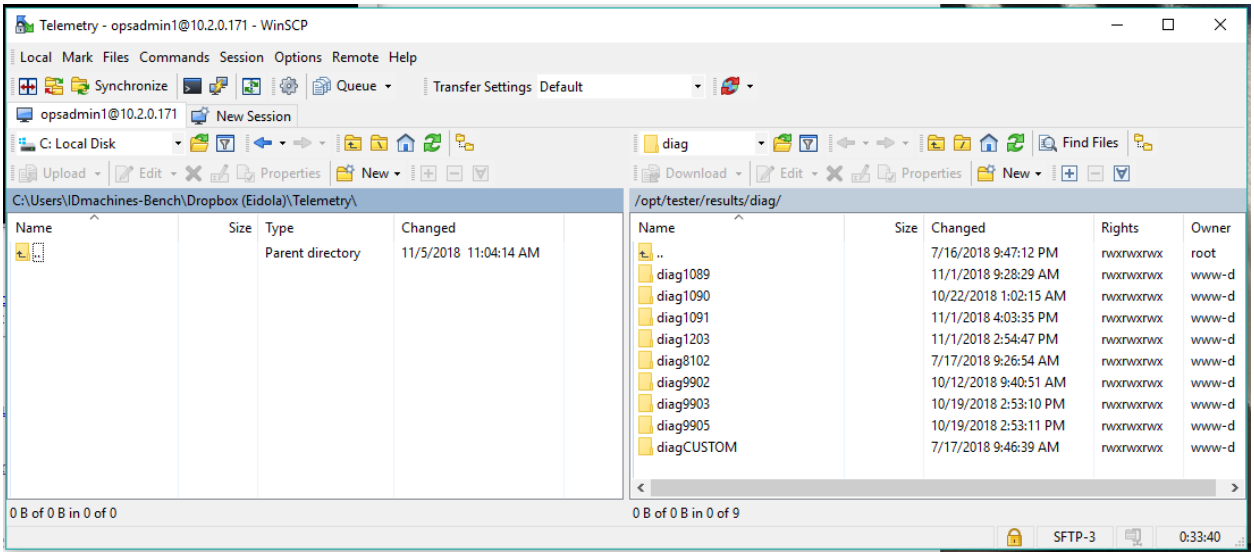


a. Set Device Under Test Target FQDN or IP address
b. Set Network target Subject IPv4 Subnetwork (address range to scan), including CIDR block
c. set device Primary IPv4 address (if necessary)
d. Set gateway, DNS and NTP, these are set to default for a 10.2.0.xxx network.
e. set wireless address name, e.g. Eidola-Tester-171 from default if not already done
f. configure SNMP community strings (these must match the settings on target devices.
g. toggle other network services as necessary, typically these are disabled on first pass with the device in stand-among mode
h. click modify in each case and wait for any changes to take place, in case of IP address change of device reboot is necessary, which can be done from the configuration screen

5. Run Diagnostics (EiDiag) and Export Results



a. From the main menu select diagnostics menu
b. Select an NMAP (among the 3 options) scan, when complete look at results by clicking on Recorder 01, you will now have a record of device addresses, ports, services, status and MAC addresses displayed)
c. Select a device for further testing. Return to the parameter screen and reset (modify) this setting for the Device Under Test (DUT) if necessary.
d. Perform TLS and SNMP test and review results at Recorder in browser. The TLS diagnostic results are at the bottom along with a lot of other info about the security of the network connection, the SNMP diagnostic gives you detailed information about the device (both require the target devices to be set up properly or no to poor results will be returned). For TLS a certificate and HTTPS must be enable and for SNMP it needs to be enabled along with the proper (matching) community string.
e. Open WinSCP or like file transfer tool and navigate to the results directory on the EiPi
    i. /tester/current/results/diag/diagNNNN/ where NNNN is the diagnostic test performed in the case of NMAP is 1091
f. Transfer the results to a local or designated drive (will become part of the device archive), rename file to local convention.



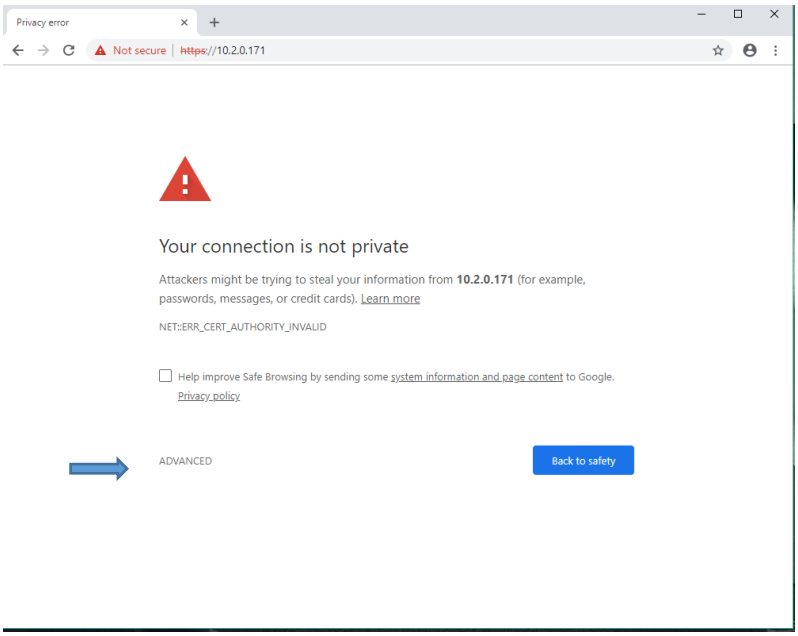
Lots more here, but at this point you have performed all that is needed to create value from the deployment of modern networked physical security systems. You will have collected information (telemetry) from your system, this documents the as-is and also sets you up to complete the optimization of the device (and system) settings. See our YouTube channel if you like and do this while following along.

And by the way, happy to do this along with you on a GoToMeeting, to help you get started!

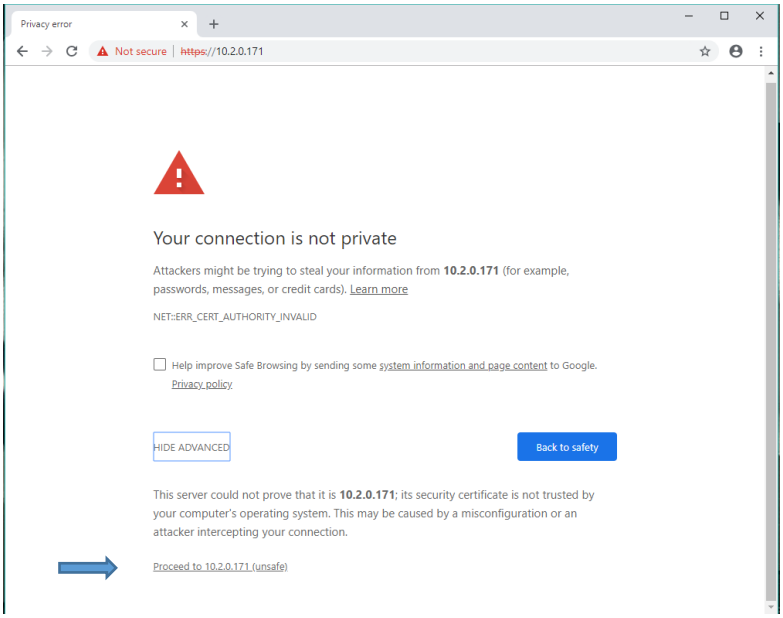
Best from all at the IDmachines team.

Appendix 1. Chrome Security Exception Steps

When you first attempt to open a browser session you will get an exception until you register the Eidola certificate (See Application Note 7 for details). To proceed click advanced (see blue arrow below), this will vary among browsers.



Then click proceed



Proceed to login, default login is opsadmin1 and the pw is Test2012Credz? (yes the ? is a special character and part of the pw…)