Centrally configuring and deploying the DNA iOS Browser

The DNA Browser app for iOS tablets and smartphones is for use with DNA (version 4.50 and above), a single, low-cost solution delivering IT Asset Management, Classroom Instruction, Internet Safety and more – with dedicated versions available for schools and corporate enterprises.
The Browser app supports DNA's core desktop management capabilities. When launched, it will interrogate the iOS device to gather key system inventory details and monitor online activity. The data collected is dynamically sent to your local DNA Server and is then available for reporting within the DNA Management Console.

Currently supported features:

Real-time Monitoring - View a real-time summary of all iOS devices either in a detailed list view or via real-time thumbnails of each device screen.

Internet Metering - A summary of Internet activity via the Browser is recorded, including start and finish times for each URL visited and the active time spent on a page.

Internet Restrictions - Internet usage can be fully managed with the enforcement of approved and restricted website lists.

Safeguarding Keyword Monitoring – Staff are alerted when students type or search for any terms that match with those in the DNA keyword database, providing safeguarding and internet safety indicators for self-harm, bullying, radicalization, child sexual exploitation - and much more.

Safeguarding Report a Concern - Students can report concerns directly and discreetly to nominated school staff.

Safeguarding Resources - The Safeguarding Resources icon, displayed on the Browser's toolbar, gives students instant access to a list of appropriate online support resources.

Hardware Inventory - When the Browser is launched, an inventory is dynamically sent to the DNA Server.

Enterprise Alerting - Real-time alerts enable Console operators to immediately identify any user who has attempted to access a restricted website or triggered a Safeguarding keyword.

Activity - Console operators can see a chronological view of device activity for a selected time period, websites visited and triggered Safeguarding phrases.

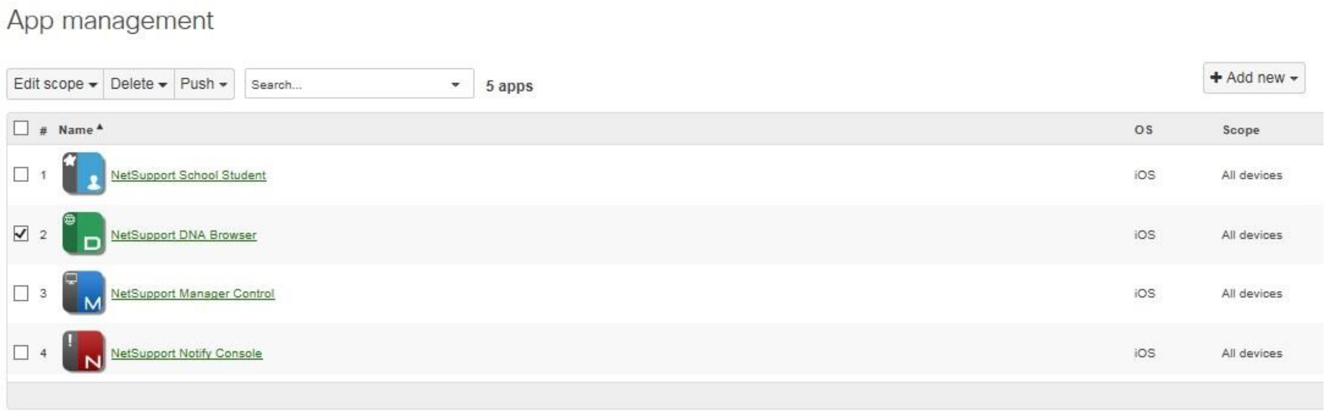
This document will outline how to centrally configure and push-out the relevant DNA settings to your managed iOS devices.

Assumptions made:

- Your iOS devices are already enrolled and centrally managed using an appropriate Mobile Device Management (MDM) solution.
- The additional components needed to complete your DNA installation - DNA Server and Management Console - are already in place. However, if this is a new installation please refer to the DNA Manual for help.

Centrally deploying the DNA Browser app to your managed iOS Devices

1. Login to your MDM tool and add the 'NetSupport DNA Browser' app to your list of managed iOS apps.



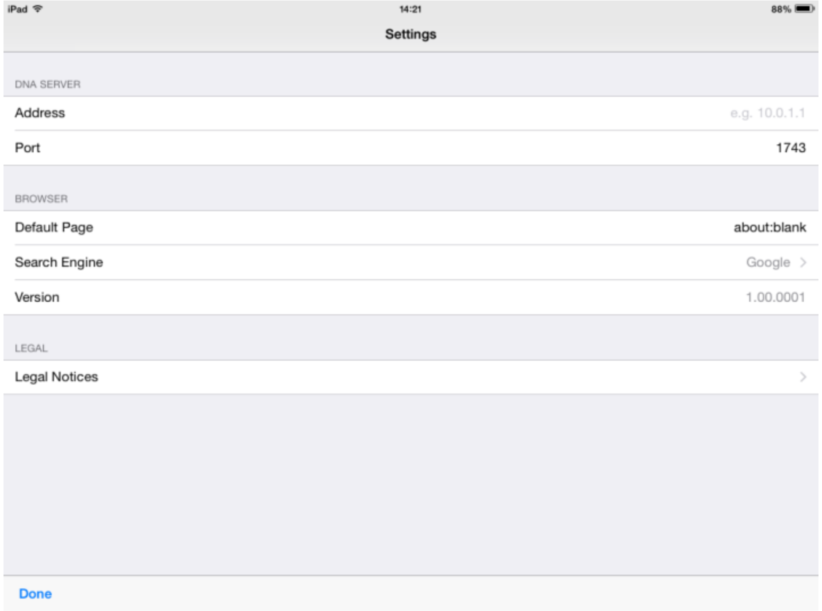
App management

Edit scope ▾ | Delete ▾ | Push ▾ | Search... ▾ | 5 apps | ✚ Add new ▾

☐	#	Name ▴	OS	Scope
☐	1	NetSupport School Student	iOS	All devices
☑	2	NetSupport DNA Browser	iOS	All devices
☐	3	NetSupport Manager Control	iOS	All devices
☐	4	NetSupport Notify Console	iOS	All devices

2. Push the app out to the required iOS tablets and smartphones

3. Launch the app on a device to confirm the installation has worked correctly. Click ⚙ on the DNA Browser toolbar to view the app settings



iPad 14:21 88%

Settings

DNA SERVER

Address	e.g. 10.0.1.1
Port	1743

BROWSER

Default Page	about:blank
Search Engine	Google ›
Version	1.00.0001

LEGAL

Legal Notices ›

Done

Initially, the DNA Server Address is blank. To initiate a connection between each iOS device and your local DNA Server for reporting and monitoring purposes, the Server's IP Address should be entered here. DNA's default communication Port, 1743, can be changed if required.

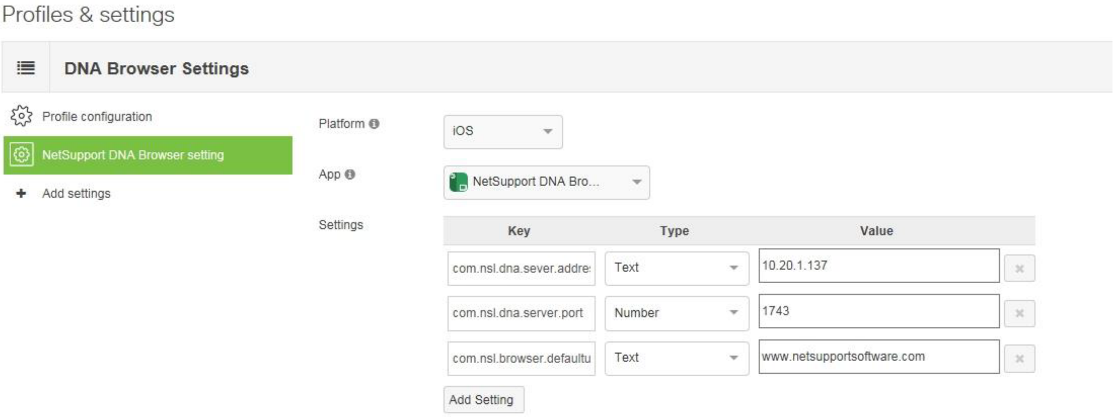
For convenience and to ensure app configurations are secure, it is recommended that you deploy the required DNA Server settings via your MDM tool.

Centrally deploying the DNA Server settings

Once deployed, an app may still require a specific set of parameters or keys before becoming operational. As explained above, in the case of devices running the DNA Browser app, they do not become available for monitoring and reporting within the DNA Management Console until your local DNA Server Address and Port have been configured in the apps Settings page.

MDM tools allow you to create profiles containing the required settings/keys and, for security, because the profile has been centrally deployed to devices using an MDM, the settings are locked.

Many MDM tools will provide a graphical interface, like below, in which to enter the keys, others will require you to create a text file in Plist format containing the exact instructions.



Profiles & settings

DNA Browser Settings

Profile configuration

NetSupport DNA Browser setting

+ Add settings

Platform: iOS

App: NetSupport DNA Bro...

Settings

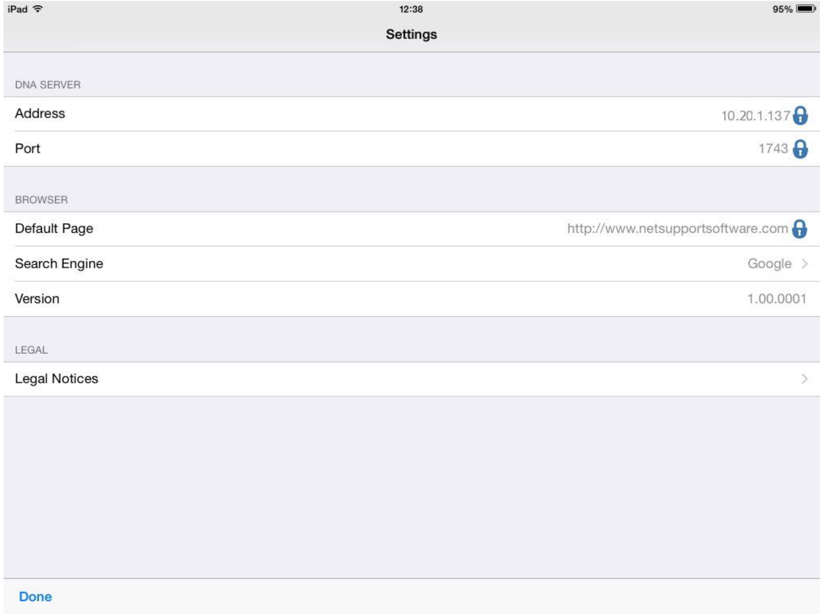
Key	Type	Value
com.nsl.dna.sever.addre:	Text	10.20.1.137
com.nsl.dna.server.port	Number	1743
com.nsl.browser.defaultu	Text	www.netsupportsoftware.com

Add Setting

The following keys should be used for your DNA Browser app configuration, replacing the example Server Address and, if required, Port, as needed. You can also include an optional key to set a default web page for use when users create additional browser tabs. (If creating a Plist file, you can copy the full instructions below into a suitable editor and save as, for example, *DNABrowserSettings.plist*.)

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>com.nsl.dna.server.address</key><string>10.20.1.137</string>
<key>com.nsl.dna.server.port</key><string>1743</string>
<key>com.nsl.browser.defaulturl</key><string>www.netsupportsoftware.com</string>
</dict>
</plist>
```

Save the configuration and check a device to confirm that the DNA Browser app settings page now shows the required details. Most MDM solutions will push out the settings immediately but there may be a short delay before they are shown in the app.



Settings

DNA SERVER

Address 10.20.1.137

Port 1743

BROWSER

Default Page http://www.netsupportsoftware.com

Search Engine Google

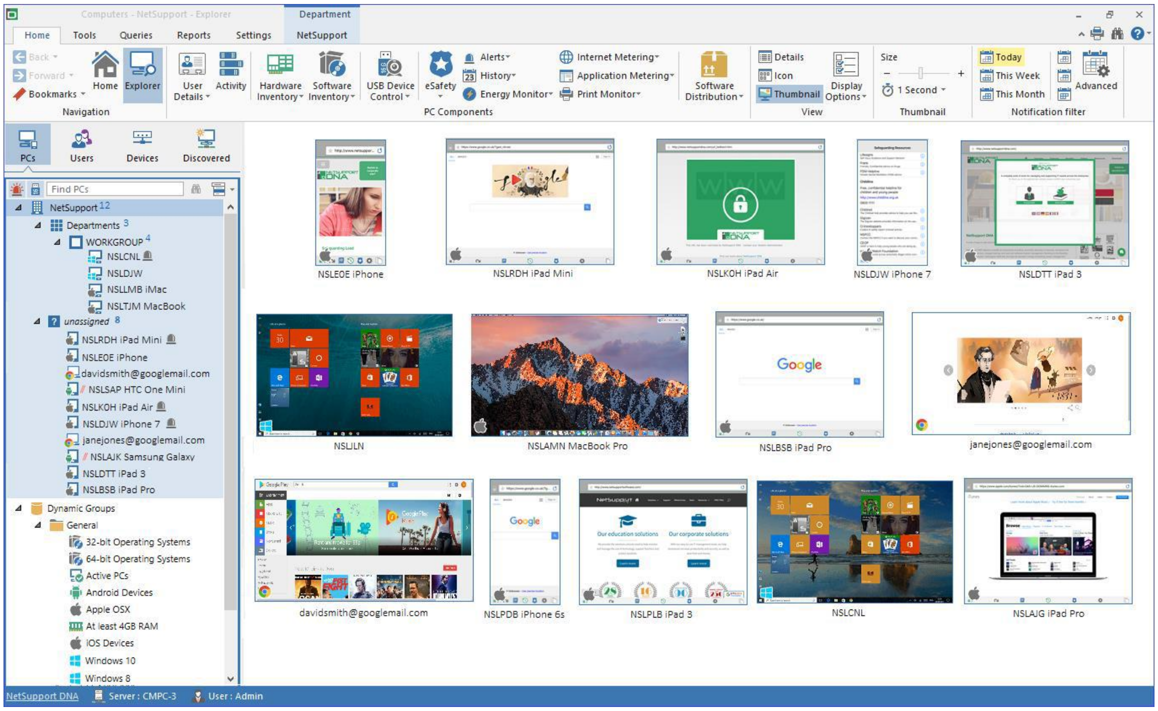
Version 1.00.0001

LEGAL

Legal Notices

Note: To ensure users can only use the DNA app for web browsing, you should also apply appropriate restrictions within your MDM tool to ensure users cannot access or download other browsers, for example removing Safari from devices.

To complete the process, login to your DNA Management Console and confirm that the required iOS Devices are now listed within the hierarchy tree alongside your other DNA Agents.



These instructions should help ensure a smooth deployment of the DNA Browser app for iOS. If you require additional help, our support team will be pleased to answer any questions you may have.