NetSupport

NetSupport DNA

Product Manual

Version 4.80

Manual COPYRIGHT (C) 2020 NetSupport Ltd. All rights reserved.

The Information in this document is subject to change without notice. NetSupport Ltd. reserves the right to revise this document and to make changes from time to time in the content hereof without obligation to notify any person or persons of such revisions or changes.

The software described in this document is supplied under a licence agreement and is protected by international copyright laws. You may copy it only for the purpose of backup and use it only as described in the Licence agreement.

Any implied warranties including any warranties of merchantability or fitness for a particular purpose are limited to the terms of the express warranties set out in the licence agreement.

Program COPYRIGHT (C) 2020 NetSupport Ltd. All rights reserved.

Trademarks

NetSupport and NetSupport DNA are registered trademarks of NetSupport Ltd.

Windows, Windows XP, Vista, Windows 7, Windows 8/8.1 and Windows 10 are trademarks of Microsoft Corporation.

Other products, trademarks or registered trademarks are the property of their respective owners.

Software Licence Agreement

Please read this agreement before using your copy of NetSupport Software. This is a legal agreement between you and NetSupport Ltd. If you do not wish to be bound by the terms of this licence agreement you must not load, activate or use the software.

TERM: Subject to termination under Termination Clause below the licence shall be perpetual.

GRANT OF LICENSE: Subject to the payment of the applicable license fees, and subject to your abidance by the terms and conditions of this agreement, NetSupport Ltd hereby grants to you a non-exclusive, non-transferable right to use one copy of the specified version of the software which you have acquired.

USE: The software is licensed with volume use terms specified in the applicable order acknowledgement, product invoice, license certificate or product packaging. You may make, install and use as many additional copies of the software on the number of devices as the terms specify. You must have a reasonable mechanism in place to ensure that the number of devices on which the software has been installed does not exceed the number of licenses you have obtained.

SERVER USE: To the extent that the applicable order acknowledgement, product invoice, product packaging or license certificate sets forth, you may use the software on a device or on a Server within a multi-user or networked environment ("Server Use"). A separate license is required for each device or "seat" that may connect to the software at any time, regardless of whether such licensed devices or seats are connected to the software concurrently, or are actually using the software at any particular time. Your use of software or hardware that reduces the number of devices or seats that connect to and use the software directly or simultaneously (e.g., "multiplexing" or "pooling" software or hardware) does not reduce the number of licenses required. Specifically, you must have that number of licenses that would equal the number of distinct inputs to the multiplexing or pooling software or hardware "front end"). If the number of devices or seats that can connect to the software can exceed the number of licenses you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the software does not exceed the use limits specified for the license you have obtained.

COPYRIGHT: This software is protected by international copyright laws. You may copy it only for backup purposes. The software is licensed to you, but not sold to you.

RESTRICTIONS: Neither you nor any reseller may rent, lease, sell licensed copies [on approval], or otherwise transfer the right to use this software to another person, except that you may sell or give away your original copy, as long as you do not keep any copies. The software may not be modified, disassembled or reverse engineered except with the prior written consent of NetSupport Ltd.

LIMITED WARRANTY: NetSupport Ltd warrants that the software will perform substantially in accordance with the accompanying documentation for a period of ninety (90) days from the date of purchase. NetSupport's entire liability and your exclusive remedy shall be either a) the replacement of the defective software or b) return of the price paid. This remedy shall be at NetSupport's option and subject to proof of purchase from an authorised source.

Any implied warranties including any warranties of quality or fitness for a particular purpose are limited to the terms of the express warranties. NetSupport Ltd. Shall not in any event be liable for loss of profits, data or information of any kind or for special, incidental, consequential, indirect or other similar damages arising from any breach of these warranties or use of the software even if they have been advised of the possibility of such damages. Some countries do not allow the limitation or exclusion of incidental or consequential damages, so

the above limitation or exclusion may not apply to you. This warranty does not affect your statutory rights, and you may have other rights that vary from country to country. In any event NetSupport's maximum liability shall not exceed the price paid by the end-user / licensee.

TERMINATION: You may terminate this licence and this Agreement at any time by destroying the program and its documentation, together with any copies in any form.

NetSupport Ltd. may terminate this licence forthwith by notice in writing to you if you commit any serious breach of any term of this licence and (in the case of a breach capable of being remedied) shall have failed within 30 days after receipt of a request in writing from NetSupport Ltd. so to do, to remedy the breach (such request to contain a warning of NetSupport's intention to terminate). Upon termination you will destroy or return to NetSupport Ltd the original and all copies of the software and will confirm in writing to NetSupport Ltd that this has been done.

SUPPORT: If you have a problem with the installation of the software you should in the first instance contact your supplier. You can separately purchase support and maintenance which will also cover the supply of enhancements and upgrades.

GOVERNING LAW: This agreement shall be governed by the laws of England.

Contents

WELCOME TO NETSUPPORT DNA 12
Features 14
NetSupport DNA Packs 27
INSTALLATION 28
System Requirements 28
Planning an Installation 29
Starting the Installation 32
NetSupport Licence Agreement 32
Select Setup Type 33
Custom setup 34
SQL Server Installation 36
Setting up the Server 37
Web Server Database setup 39
Inter Component Communications 40
Select Enterprise Type 41
Existing Installation 42
Using the NetSupport DNA Database Wizard 43
Install and set up database for use 44
Set up NetSupport DNA user for accessing the database 45
Set up admin users for accessing the NetSupport DNA Server 46
Register a Licence 47
Reset System Admin Password 48
Gateway Settings 49
Mobile Connection Settings 51
Installing via Active Directory 53
Advanced Option - Command Line Installation 54
Installing NetSupport DNA Agent on Mac Systems 56
NetSupport Browser for iOS 57
NetSupport DNA Browser for Android 59
NetSupport DNA Chrome Agent 61
NetSupport DNA Gateway 62
Gateway Server (Local) Configurator 63

Gateway Agent (Remote) Configurator 64
SNMP Server Configuration 66
Gateway Status 68
Upgrading from Existing NetSupport DNA Versions 69
NetSupport DNA Mobile Console 70
GETTING STARTED 71
Running the Console 71
The Console Window 72
Create Additional Console Users 77
Create or Edit Console Operator Logins 78
Secure Mode 80
Create or Edit Console Roles 82
Discovery and Deploy 84
Agent Discovery and Deploy Tool 85
Deploy Options Dialog 87
Deploying on Windows XP 89
Deploying on Windows Vista 90
Automatic Agent Discovery 91
Managing discovered computers 92
Device Discovery 94
Display Sections 95
Integration with Active Directory 97
Create a department 99
Change the Properties of a department 101
Adding Agents to departments 103
Dynamic Groups 105
Dynamic Groups Editor 108
NetSupport DNA Configuration 111
Profiles 111
Assigning Profiles 113
Configure Component Settings 115
Agent 116
Logon Control 117

Internet Metering 119
Hardware Inventory 121
User Details 122
Application Metering 123
Print Monitor 124
USB Device Control 125
Title Blocking 126
Software Distribution 129
Explorer 130
Software Inventory 131
Alerting 133
Report Concern 135
Phrase Monitoring 137
Acceptable Use Policy 139
Remote Control 140
Risk Analysis 142
Energy Monitor 143
SNMP Configuration Settings 145
SNMP Monitor Settings 146
SNMP Alert Settings 146
SNMP History Settings 147
Console Preferences 148
General 150
User Interface 152
Active Directory Settings 153
Email Settings 154
Auto Discovery 155
Audit 156
File Locations 157
NetSupport DNA Cloud Console 158
Manage Web Concern 160
USING NETSUPPORT DNA 161
Console Window – Summary/Home Screen 161
Efficiency View 162

Explorer 164
Spotlight 169
User Details 172
Request/Edit User Details 175
Bind User Dialog 177
Custom User Details 178
Custom Fields Editor – Controls 180
Activity Monitoring 184
Hardware Inventory 187
Gather Inventory Data For Remote Users or Non Scanned Devices 190
Add Non Standard Hardware 190
Create a new PC 191
Import a Standalone/Remote device 192
Add Hardware Peripherals 194
Additional Devices 196
Contract Manager 198
Software Inventory 200
Installed Programs Manager 204
Merge Installed Programs 205
Edit Installed Programs 207
Installed Programs Licence Management 208
Application Groups 210
Edit Application Group 211
Merge Application Groups 213
USB Device Control 214
Registering USB Devices 217
USB Device Details 218
eSafety 220
Safeguarding Roles 221
Managing Safeguarding Administrators and Users 222
Add or Edit Safeguarding Administrators and Users 223
Phrase Monitoring 225
Keywords and Phrases Database List 229

Create or Edit Keywords and Phrases 231
Importing/Exporting Keywords and Phrases 232
Review Triggered Phrases 235
Application Ignore Lists 239
URL Ignore Lists 240
Phrase Cloud 242
Concerns 244
Safeguarding Resources 247
Reporting a Concern 249
Reporting a Concern via a Website 250
Adding Notes to a Concern 254
Archiving Concerns 255
Risk Analysis 256
At Risk Application Lists 259
At Risk URL Lists 260
Alerting 262
PC Alerts 264
Alert Manager 266
NetSupport DNA Alert Wizard 267
Group Definitions 268
NetSupport DNA Server/Console Alerts 269
Active Alerts 270
Review Active PC Alerts 272
Closing Alerts 274
History Window 275
Energy Monitor 277
Energy Costs 280
Internet Metering 281
Internet Restrictions 284
Using the Spotlight feature to assign URLs to an Approved or Restricted list 288
Application Metering 290
Application Restrictions 293
Block applications by Window Title 295

Print Monitor 297
Configure Print Costs 299
Software Distribution 301
Create Software Distribution Packages 304
Create New Package 305
Distribute a Package 307
Scheduling a Package 310
Advertise a Package 311
Request a Package 312
Import a Package 313
Software Distribution Warehouse 314
NetSupport DNA Application Packager 316
NetSupport DNA Application Packager - Script Builder 320
SNMP Monitor 324
SNMP Alert 326
SNMP Alert Configuration 328
Creating a New Alert 329
SNMP History 330
NetSupport DNA Reporting and Analysis Tools 332
Query Tool 335
Create a Query 336
Edit an existing Query 343
Run a Query 344
Scheduled Queries 346
Finding PCs, Users and Devices 348
Bookmarks 351
Acceptable Use Policies 353
Audit Log 357
Vault 358
Manage User Accounts 360
Locate a User 362
Chatting to Agents 363
Remote Control 364

Send a Message 367
Agent Status 368
Creating QR Code labels 370
Database Maintenance 371
NetSupport DNA Agent Window 386
CONTACT US 388
INDEX 389

WELCOME TO NETSUPPORT DNA

Education
Optimised for the easy management of a school or campus-wide IT infrastructure, NetSupport DNA provides a complete toolbox of features to support the effective management of school, staff and student technology. The solution is built with ease of installation and ease of use at the heart of each and every feature.

Save time with proactive warning alerts of issues across the network - from server failure, low disk space, unauthorised software installs, through to licence compliance and student help requests. Generate reports automatically and routinely for the Senior Leadership Team and use the supporting mobile apps to ensure key data is accessible for IT staff from wherever they are.

Reduce IT costs by identifying hardware that can either be redeployed or upgraded rather than replaced; tracking software licence deployment and, critically, licence usage - thereby avoiding costly renewals for software no longer needed; monitoring print usage across the school; energy monitoring and deployment of a power management policy in relevant areas of the school.

Deliver a safer environment by monitoring and controlling internet use with approved and restricted URL lists. Stay alerted to any safeguarding issues with keyword monitoring and enable students to report concerns directly to trusted staff. Control access to content with endpoint security across the school; deliver user acceptance policies; monitor students in the classroom, and much more.

Corporate
A complete ITAM solution for the effective management of the enterprise. NetSupport DNA delivers a full suite of features to help support the management and maintenance of IT assets.

NetSupport DNA is designed to be easy to install and with ease of use at the heart of each feature. NetSupport DNA has the flexibility to scale with your business needs – from a single SME through to larger multi-site implementations – without breaking the IT budget.

Save time with proactive warning alerts of issues across the network - from server failure, low disk space, unauthorised software installs, through to licence compliance and user help requests; with reports automatically and routinely generated for management; and by using the

supporting mobile apps to ensure key data is accessible for IT staff from wherever they are.

Reduce IT costs by identifying hardware that can either be redeployed or upgraded rather than replaced; tracking software licence deployment and, critically, licence usage - thereby avoiding costly renewals for software no longer needed; by monitoring print usage across the enterprise and with energy monitoring and deployment of a power management policy to relevant areas of the company.

Add security by preventing access to unauthorised websites; limiting use of key applications to only authorised users; by helping protect company data with profiled memory stick access; delivering user acceptance policies; and sending security alerts for any unauthorised activity such as hardware removal, antivirus services being stopped and more.

Features

Ease of Installation
NetSupport DNA is designed to deliver a complete suite of IT administration features without the associated expensive hardware purchase, implementation and training costs of alternative solutions.

After installation of the server module (used to manage and add information to the DNA database), the deployment tool provided will automatically discover and install the DNA client on targeted devices. The DNA console (installed by the IT technician) provides full DNA system control, rich on-screen information and real-time reporting.

A typical 50-user PC evaluation can be up and running within 30 minutes. An additional gateway component is included as standard for linking multiple remote sites and SQL Server Express is also included so it can be used for evaluation. DNA will link with Active Directory (including single sign-on) and includes the ability to profile department access and administrative features by console user.

Device Auto-discovery
Receive notifications of any new devices that join the network and choose whether to deploy an agent automatically.

Once NetSupport DNA is installed and operational in your enterprise, it will constantly monitor the network and identify any new devices that join, providing the option to automatically deploy an agent for future management.

Hardware Inventory
NetSupport DNA provides one of the most comprehensive and detailed Hardware Inventory modules available on the market today. A wealth of information is gathered from each device, from CPU and BIOS types to network, video and storage information.

Inventory reports are displayed either for a single PC; a selected department; condition-based "Dynamic Groups"; or for the full enterprise.

Contracts options are also provided to record both leases and maintenance contracts associated with any devices and peripherals, including supplier details, contract term dates and costs.

Hardware Inventory updates are configured to run at different time intervals throughout the day or at start-up and can be refreshed instantly

on demand. A stand-alone inventory component is available to run on non-networked or mobile devices and in addition, high value peripherals can also be associated and recorded against a device.

Efficiency View
The unique dashboard highlights at a glance how school technology is being used and the areas where efficiency can be improved to create cost- and time-saving benefits, e.g. highlighting which PCs are least effectively used (and therefore can be redeployed) or which apps are the least used (and therefore may not need renewing).

SNMP Device Discovery
The SNMP Discovery view allows NetSupport DNA to be configured to scan a range of network addresses and report on any appropriate devices discovered, such as printers and access points. These items can then be stored within DNA and real-time data (such as ink or toner levels) can be monitored from the console.

The SNMP module includes both discovery of - and then active monitoring of - any selected SNMP devices; tracking statistics and a history for any data set on a given device over time, such as data traffic on each interface of a network switch. The module also includes a dedicated alerting component, supporting dozens of customisable alerts which can be created and triggered if any tracked data meets a specific criteria. Alerts can be sent automatically to designated console users or pre-defined email accounts. Custom query based reports and views can also be created to reflect all gathered data.

Software Inventory and Licensing
The Software module is designed to help organisations manage licence compliance and reduce software overspend by accurately reporting installed software and proactively identifying PCs with software that has no or low usage.

A detailed summary of all programs and applications installed on each PC is provided, including Windows 8 and 10 store apps. NetSupport DNA can display the information for a selected PC, a department or a custom group and features an extensive module for assigning and tracking licence use. The NetSupport DNA Software Licence module supports the ongoing management of all software licences for each department – recording suppliers, purchase and invoice details, department or cost centre allocation and the tracking of maintenance contracts as well as storing PDF copies of any supporting documents.

A file scan option is also included and can be used to identify files of a certain type installed locally on devices. This could be used to ensure work documents are not being stored locally and missing company backup routines.

The 'Search facility' added makes it easier to find programs or applications you are looking for, and the install date of hotfixes is now shown in a devices Software Inventory – helping to highlight which devices have received updates.

Software Application Metering
The Application Metering module reports on all applications used on each PC or server, detailing the time the application was started and finished, as well as the actual time it was active.

Monitoring application use ensures software licences are assigned to the right users and aren't renewed for users without matching application activity, thus enabling cost savings.

Application usage can also be restricted for users or departments, either fully or just by time of day. Lists of approved and restricted applications, together with times when restrictions apply, can be created and enforced centrally.

In addition to restricting by their specific name, applications can also be blocked or restricted by their window's title, helping technicians to add a broader layer of security while maintaining productivity.

Application Metering enables the business to monitor and report current licence use levels for all installed applications and ensure that application usage complies with corporate policy. Reports can be presented by PC or logged-on user.

Internet Metering
From online collaboration and cloud-based solutions to social media and beyond, access to the internet is constant. To ensure the successful use of staff time, the effective use of company bandwidth and to support a safe environment, it is essential that companies don't just have an internet safety policy in place, but also the right tools to enforce it.

The Internet Metering module provides a detailed summary of all internet activity on each PC by a user, including start and finish times for each URL visited and the active time spent on a page. Results can be reviewed either by activity on a specific device or for a user, no matter where they

worked. Naturally, the key to supporting an effective policy is to provide effective controls. With NetSupport DNA, internet usage can be fully managed; lists of approved and restricted URLs and/or sub-URLs can be applied to profiles. Once applied, NetSupport DNA can allow unrestricted access to all websites, restricted access to certain websites that have been marked as approved by the company or by blocking access to specific sites marked as inappropriate.
In addition to restricting by their specific name, Apps and Games can now be blocked or restricted by their window's title, helping technicians to add a broader layer of security while maintaining productivity.

Access can also be controlled by time of day, perhaps only allowing access to approved gaming or social media sites at lunchtime and outside of working hours.

Enterprise Alerting
NetSupport DNA features an extremely powerful Alerting module that prompts the system to automatically notify operators when any number of changes occurs across the enterprise. Building on the DNA philosophy, the system is designed to be simple to initiate and any number of custom alerts can be added.

There are three types of alert: Server, Console and PC. Server alerts identify any changes within the data gathered by NetSupport DNA across the overall enterprise, including alerts for things like new PCs added, changes in hardware, a new application installed/removed and so on. Console alerts identify changes relating to the NetSupport DNA Console, such as the DNA licence limit being exceeded, an Operator added or deleted and a DNA update installed. PC alerts identify real-time changes or conditions that occur on a specific PC, such as CPU utilisation exceeding XX% for XX minutes, free disk space falling below XX%, when a key service stops (e.g. AntiVirus service or IIS on a server), print spooler alerts, security alerts (e.g. failed login attempts) and much more. As part of a SIEM (Security Information and Event Management) strategy, the PC event log can also be monitored with alerts triggered for errors, warnings or selected audit outcomes.

Alert notifications can be directed to specified email recipients and/or active console users (on a per alert basis, so the nature of the alert may dictate which operators are notified). In addition, outstanding alerts are identified against matching PCs on the main company hierarchy tree view. Actions can be added when creating a PC alert, allowing you to choose what happens when an alert is triggered. The available actions are: capture screenshot, record screen and run application. Once alerts

have been identified, notes can be added by an operator and PC alerts can be reviewed and shared or a permanent record saved for later review. A full history of PC alerts is accessible from the History feature.

Software Distribution
NetSupport DNA provides a multi-delivery option for Software Distribution.

A software distribution package is created by either applying parameters to a collection of files or folders or by using the DNA application packager - recording the user prompts, keystrokes and mouse clicks that are used during a test installation, and then automating these on a live deployment to bypass the need for operator intervention.

Once created, the application package can be automatically "pushed" to the target PCs for deployment or, alternatively, it can be "published". Once published, a user can check to see which applications are available for their PC, based on their departmental membership, and "pull" these on demand.

NetSupport DNA includes a Scheduling feature, allowing packages to be deployed on a specific date and time - usually out of core office hours when network traffic is at its lowest.

With remote deployments, the need to minimise network traffic congestion becomes a priority. In this case, NetSupport DNA allows a client PC, ideally local to the target machines, to be nominated as a distribution point. When the software is deployed, rather than being sent to each remote PC directly, it is just sent to the designated PC which then acts as a relay and re-distributes it to its local PCs.

Energy Monitoring and Power Management
The Energy Monitoring module provides a simple and concise high-level summary of potential energy wastage across an organisation by computer systems that are left powered on out of business hours.

NetSupport DNA checks to verify the powered-on state of all computers and its local monitoring component keeps an accurate record of each time a computer is powered on, off or hibernates. Once it knows the times of day each computer was operational, an average (and customisable) "power consumption per device" calculation is used, facilitating a baseline energy usage calculation for all computers.

With this information to hand, Power Management policies can now be set. Selected PCs can be set to automatically power off at a specified time at the end of each day and then power back on – all at once, or in stages – the next morning. In addition, "inactivity policies" can be applied, allowing rules to be applied for systems to sleep, log out or power down if they have been inactive over a period of time.

Endpoint Security
NetSupport DNA provides a simple and effective solution for managing the use of USB memory sticks to help maintain the security of the network. The use of memory sticks can be controlled across the entire enterprise or, just for specific departments and usage, can be set to allow full access, block all access, allow read-only or prevent applications being run from a memory stick. Alternatively, individual memory sticks can be "authorised" in NetSupport DNA - for the current day, a week or indefinitely - and the use of sticks in the enterprise can also be limited to only those authorised.

A program administrator can connect a memory stick to their local PC and then authorise its use within the DNA console for either a given department or a specific user. Users who connect an unauthorised memory stick to their PC can also request remote authorisation where appropriate. Not only does NetSupport DNA identify both removable (memory stick) and portable (mobile phone, tablet, camera) storage devices, it also provides similar usage controls over CD / DVD devices (including USB and virtual). It also detects whether volumes on hard drives/USB drives are encrypted (BitLocker).

Real-time Monitoring (Explorer Mode)
Gain a real-time summary of all your PCs using Explorer mode. Selected PCs can be viewed in three formats – Icon, Details or Thumbnail view – and these can be refreshed at time intervals of your choice, e.g. every five or ten seconds and so on.

In the Thumbnail view, the PC screens (including multiple monitors) are visible and give a visual overview of current activity. The thumbnails size can be changed to suit the operator's needs. For selected departments (i.e. finance or teachers), privacy modes can be set so the thumbnail is blurred. Displaying the selected PCs as icons is another useful option for viewing large numbers of PCs at a glance and simply highlights OS platforms and any with active notifications.

Drilling down further, the Details view displays all of the selected PC's details in a list with any active notifications highlighted, allowing for easy

identification of PCs that may need immediate attention. This view also provides a visual summary of all active policies applied to each PC and PC performance data such as real-time network traffic, CPU and memory use for each PC and free disk space. In addition, by right clicking on any PC an operator can launch on-the-fly PC-specific features such as power on/off, chat, remote control, send messages and more. The notification filter can be used across all three display modes to highlight the PCs with any active notifications within the chosen time period.

Explorer mode is available from the Users Tree view, enabling Technicians to see data at user level – for example, which profile has been assigned to them.

Technicians can also use the handy Spotlight feature to help them see more details about a selected PC (e.g. any applications, services, websites and processes in use), all in a single glance.

eSafety
NetSupport DNA, together with its optional classroom management module, provides a range of features to support a school-wide eSafety policy. Within DNA, this includes both Internet Monitoring and restrictions to prevent access to inappropriate websites; disabling webcams on classroom devices; controlling access to content on memory sticks; triggering Alerts when violations occur – through to the enforcement of acceptable usage policies.

Safeguarding
NetSupport DNA's Keyword and Phrase Monitoring feature provides insight into and alerts from any activity by a student that might suggest they are engaged in activity that would place them at risk. The details/context of triggered words can be reviewed, with the results (available as a log, screenshot of the screen, webcam image of the user, or a screen recording, according to severity level and which of these the school activates – features are not available for devices used at home), forwarded to a colleague to follow up on, if required. The data captured is securely stored on the school network (LAN) and only designated safeguarding leads can access the information.

A full explanation and definition of each keyword is also given to help staff understand the potential risk to the student, plus the new contextual intelligence-based risk index creates a numerical risk index score for each event based on sophisticated contextual AI risk analysis. This allows staff to view high-risk events and vulnerable students with ease. Staff can also see the broader context of a student's activity from a detailed summary

of their internet and application use (which can also be controlled) that is available for any selected period of time. Age appropriate internet controls can also be added using the Profiles. In addition, vulnerable students can be flagged and tracked as an extra layer of support, and a 'history of concerns' is available for each student.

The Azure-hosted safeguarding Cloud Console stores local data to allow Safeguarding Leads to view triggered safeguarding keywords, new contextual intelligence-based risk alerts, reported concerns by a student and the trending topics word cloud on the go. The new cloud module also includes a smartphone-optimised user interface to allow safeguarding staff to quickly search for a specific student and review any recent alerts or concerns.

Safeguarding needs to be proactive too and so NetSupport DNA enables Students to access online support resources – covering topics such as FGM, drug addiction, grooming and bullying – all from the NetSupport DNA safeguarding icon on their PC. Students can also report their concerns in confidence to a trusted member of staff via the Report a Concern option. (Available via the DNA Agent installed on school devices or, out of hours, via a website.) Students share their problem by sending a message, screenshots or documents to a member of staff they trust, then NetSupport DNA will track the concern, any notes made, and even alert a Safeguarding Administrator if the intended member of staff has not responded within a certain amount of time. Concerns can be re-assigned to another Safeguarding Lead if, for example, the member of staff was on holiday. Teachers can also do the same in situations where they are verbally told of a student's concern. They can log the concern via the 'Add concern' button on the safeguarding ribbon.

Note: These features are only available in the Education Edition of NetSupport DNA.

Vault

NetSupport DNA contains a Vault component, allowing secure storage of serial numbers, passwords or any other confidential IT data. Access to the vault can be restricted to specific console users and activity can be recorded against the central DNA audit trail.

System Audit

NetSupport DNA includes a powerful Audit component, tracking all selected console activity by staff. The Audit feature records changes to

policies or settings; when entries are added/ deleted or where rights are changed for any user.

User Management
NetSupport DNA provides a range of features to locate and manage users within a networked environment. In addition to key user data (name, telephone etc), DNA provides the customer with the ability to tailor the data to be gathered and collated from each user, including tracking of user acceptance forms. DNA also keeps a history of changes to the data entered in User Data. Changes to Custom User Details are recorded, including the following fields: Employee Number, Location, Asset Tag and Owner.

Activity Monitoring
NetSupport DNA now provides a single time-based summary of all activity by a specific user, PC or department. Presented in a chronological view, it shows technicians what time the logon session began and ended, as well as what applications were used and when, plus internet usage – over a set time period. Activity can be viewed in a graphical timeline or text-based grid view. This time-saving feature means that technicians now don't have to look at each area separately and can instead see all the information at a glance in one location. For example, it can highlight the user and time when an application is run on a specific PC.

Profiles
To provide maximum flexibility and to help save time, NetSupport DNA allows you to create multiple profiles for different groups of devices or users (e.g. department level), each with its specific component settings. This means dedicated settings (such as internet access, print metering and much more) can be applied to specific departments, e.g. Marketing (may need access to social media).

Logon Control
In addition to preventing staff logging in on multiple devices, when required, a user can be authorised to log on to multiple PCs at once (between 1 and 5). A useful feature for roaming staff or technicians who may have several devices.

Locate a User
NetSupport DNA allows anyone with a DNA Agent installed on their machine (if the feature is enabled) to locate another logged-on user and then send them a message. This may be useful for staff members that do not have the NetSupport DNA Console installed but need to find and contact other users in the company.

Bookmarks
NetSupport DNA allows you to create and place bookmarks within the PCs, Users and Devices Tree views. This may be useful if you have a large or complex Tree structure, as it allows you to quickly navigate to the place you want to work with.

Custom Images
To help find users/items in the Hierarchy Tree view easily, you can apply custom images to departments, dynamic groups, PCs and Users.

Other supporting tools include real-time chat and enterprise messaging, a real-time system status view for all devices, as well as a range of system admin features.

Enforce Acceptable Use Policies
Acceptable Use Policies (AUP) form an integral part of the key information security policies used by most organisations. It is common practice for new staff to sign an AUP before using company resources for the first time or to confirm they have read any changes to such a policy whenever it is updated.

NetSupport DNA provides a flexible module to support the delivery and tracking of AUPs across an organisation. Policies can be applied to specific devices or users for display each time any user logs on or for one-time display and acknowledgement. Multiple policies can be created, allowing you to have one policy that appears only once for selected users (for example, teachers) and another policy that appears every time for other users (for example, students). Full tracking and exception reporting is also provided.

Print Monitoring
NetSupport DNA includes a high-level Print Monitoring feature. Individual printers across the enterprise are automatically identified and, from the central console view, costs for printing (black and white, colour and so on) can be assigned either globally or against each different printer. Where required, printers can also be excluded from the view. A full overview of printing activities and indicative costs across the enterprise is provided by NetSupport DNA.

Enterprise Reporting
NetSupport DNA provides both on-screen and print-optimised reporting. The on-screen reports/views are provided with supporting bar and pie charts and "live" drill down capabilities on all key summary data. As well as reporting on individual devices, users and departments, NetSupport

DNA also features dynamic groups. These are user-defined and are added to the main company tree. A dynamic group could, for example, be to identify which PCs are upgradeable and such a group would be created automatically from those that match the required criteria – such as "all PCs with more than 'XX' Gb RAM, 'XX' Gb free disk space and XX processor type" and so on.

Print optimised reports are designed for management reporting and can be scheduled for creation and output to a specified file location automatically. All reports include the option to print or export to PDF, DOC and XLS.

NetSupport also supports custom views for all data; the Query Tool provides users with an easy interface for defining custom views. The query tool uses a simple drag and drop field picker, supported with conditions and sum-based features.

Mobile Inventory
Provided as a supporting tool for NetSupport DNA, the Inventory app can be downloaded free from the Google Play and Apple app stores. The DNA mobile app allows a Technician, when away from their desk, to search for and view a detailed Hardware and Software Inventory for any PC on the company network. The mobile app also includes a QR code scanner to help instantly identify any PC, either from an on-screen QR code displayed by DNA or from a label fixed to the device. NetSupport DNA also provides a QR code label creation facility, including support for custom details. Histories of all hardware changes as well as any software installs or removals are also shown on the app.

In addition to the Inventory and History views, the NetSupport DNA mobile app also highlights any new PC alerts that have triggered across the network. Finally, the app also provides an option to launch a Remote Control session on any selected PC directly from the smartphone or tablet – ideal for both remote support and quick access for a technician back to their own desktop PC.

Remote Control
NetSupport DNA (Education Edition) includes powerful Remote Control and monitoring features as standard. Everything from screen viewing to transferring files and more is included in the component. To further aid remote device management, school technicians can launch PowerShell and Remote Command Prompt sessions, edit the Registry of a remote PC and login/logout remote machines.

To facilitate central IT support across multi-site environments, the inbuilt DNA gateway component allows you to deliver seamless and secure Remote Control to Agent machines no matter what their location.

Corporate users have the option to integrate a copy of NetSupport's award-winning Remote Control solution NetSupport Manager, providing access to workstations and servers across your enterprise, both locally and remotely when off-site or mobile.

Classroom Management (optional)
NetSupport is recognised globally as being the leader in classroom management and orchestration software. NetSupport School is the award winning classroom solution delivering a complete range of monitoring, testing, collaboration and orchestration tools for any classroom environment.

NetSupport School helps teachers and trainers improve the efficiency of ICT teaching by delivering a suite of tailored features developed with teachers, for teachers. Teachers and assistants can instruct students centrally to all their own devices; help maintain student focus by monitoring and controlling the use of apps, websites, printers and more; support student learning using unique digital journals; utilise the unique student toolbar to highlight lesson objectives and expected outcomes; and deliver targeted student and peer assessment with a unique Question and Answer module, surveys or pre-prepared tests.

In addition, NetSupport School features a monitoring app for teaching assistants to use in the classroom.

ServiceDesk (optional)
Designed to integrate with NetSupport DNA or operate as a standalone solution, NetSupport ServiceDesk ticks all the boxes as a fully functioning ITIL-compliant IT Service Management (ITSM) tool, supporting the key areas of ITIL's best practice framework – Incident, Problem, Change and Service Level Management. Used with NetSupport DNA and our remote access solution, NetSupport Manager, support teams have a complete network management toolkit.

NetSupport ServiceDesk can be accessed through a web browser by any user from their desktop or mobile device and allows for the customisation of many key features within the solution. From operator functionality to the creation of specific data entry fields, it can be tailored to fit seamlessly into your organisation.

Powerful and customisable workflow rules help ensure delivery of an efficient and timely service in line with agreed service levels, automated email processing helps deliver further time savings and, with NetSupport ServiceDesk's customer-friendly self-service portal, users are able to search for answers before even logging a support request.

NetSupport DNA Packs

For complete flexibility and value for money, NetSupport DNA can be purchased, either as a stand-alone solution or combined with one of our complementary corporate or education solutions:

Pack A
NetSupport DNA (all components as standard).

Pack B *(Education Edition)*
NetSupport DNA plus NetSupport School.

For further information on NetSupport School, please visit www.netsupportschool.com.

Pack C *(Corporate Edition)*
NetSupport DNA plus NetSupport Manager.

For further information on NetSupport Manager, please visit www.netsupportmanager.com.

INSTALLATION

System Requirements

NetSupport DNA Server
Minimum hardware: Single – Dual Core 2.00 GHz CPU 8 Gb RAM or higher.*
Free space required: 20 Gb (dependent on number of Agents supported).
Windows Server 2008 R2 or above (best practice).
Windows 7, Windows 8.1 and Windows 10.

Databases supported: SQL Server 2008 or later. If no version of SQL Server exists on the target system, when installing the DNA Server, you will be prompted to either install SQL Server (SQL Server 2012 Express is included in the NetSupport DNA setup file) or to specify the address of an existing SQL Server.

*Refer to our website www.netsupportsoftware.com/support for recommendations based on installed Agent base.

Optional Server modules (SNMP Discovery, Remote Gateways, Web Server)
Windows 7 or higher.
Windows Server 2008 or higher.

NetSupport DNA Cloud Server
Windows 10.
Windows Server 2008 R2 and above.

NetSupport DNA Management Console
Free space required: 392 MB
Windows 7 or higher.
Windows Server 2008 R2 or higher.

Note: The Console can be installed on multiple machines.

NetSupport DNA Mobile Console apps
Android 4.03 or higher.
iOS 9.3 or higher.

NetSupport DNA Agent (client)
Free space required: 108 MB
Windows Vista or higher.
Windows Server 2008 or higher.

Mac OS X 10.8 or higher.
iOS 9.3 or higher.
Chrome OS.
Android 5.01 or higher.

Note: Terminal Server environments are only supported for the following components: Application Metering, Acceptable Use Policies, User Details, Print Monitoring, Internet Metering and eSafety.

Inventory only Agent
Windows XP SP3.
Windows Mobile 8 or later.

Planning an Installation

Before commencing an installation, consider which components are required. NetSupport DNA consists of eight main components:

1. NetSupport DNA Server
2. NetSupport DNA Console
3. NetSupport DNA SNMP Server
4. NetSupport DNA Web Server
5. NetSupport DNA Agent
6. NetSupport DNA Application Packager
7. NetSupport DNA Server Gateway
8. NetSupport DNA Agent Gateway

NetSupport DNA Server
The machine on which the server software is installed and the database is stored is called the NetSupport DNA Server.

An additional SQL Server needs to be installed to enable the NetSupport DNA Server to operate its database. The SQL Server works with the NetSupport DNA Server by effectively storing and retrieving the data that the DNA database collects, as required.

NetSupport DNA comes with an SQL Server available, which can be automatically installed. Alternatively, you can use an existing SQL Server, by entering the server's login details. The SQL Server may run either on the same computer as the NetSupport DNA Server or on another networked computer.

Note: For further information, see SQL Server Installation.

NetSupport DNA SNMP Server
The SNMP Server is the component that allows you to monitor and configure SNMP-enabled Devices, such as printers and access points. The SNMP Server will need to have network access direct to the SNMP Devices. You will need to enter the DNS name or IP address of your NetSupport DNA Server.

Note: You can use the Gateway to communicate with the Devices.

NetSupport DNA Web Server
The Web Server is installed on a Windows machine. This allows the NetSupport DNA mobile app to connect to NetSupport DNA.

NetSupport DNA Console
The Console is the main interface for executing commands and is generally installed on an administrator's machine. An administrator executes a command and the gathered data is extracted from the NetSupport DNA database which resides on the server. Console users are provided with administrator rights. The installation prompts for an initial Console user logon to be created, but additional Console users can be added depending on your requirements.

Notes:
- The Console can be installed on multiple machines.
- A cloud-based Console is available in the Education Edition of NetSupport DNA, enabling Console Operators to view data away from the main DNA Console in a browser.

NetSupport DNA Agent (Client)
The machine on which the Agent software is installed is called the NetSupport DNA Agent. The Agent is the end-user machine where data is collected from.

NetSupport DNA Local (Server) Gateway
The NetSupport DNA Gateway provides a means of connecting remote Agents to the NetSupport DNA Server. The Local Gateway communicates with the central NetSupport DNA Server. The Local Gateway must be installed separately from other NetSupport DNA components.

Note: If a DNA Server Gateway is installed on the same machine as a NetSupport Connectivity Server (NCS), remote control functionality over the DNA Gateway will not be available. (Applies to Education installations only).

NetSupport DNA Remote (Agent) Gateway
The Remote Gateway acts as a proxy server for the remote NetSupport DNA Agents, allowing them to communicate with the NetSupport DNA Server. The Remote Gateway can only be installed with the NetSupport DNA Agent.

Notes:
- There can be multiple Remote Gateways (one installed at each remote site) but only one Local (central) Gateway.
- The NetSupport DNA Console must be on the same network as the NetSupport DNA Server to be able to pick up Gateway Agents.

NetSupport DNA Application Packager
The NetSupport DNA Application Packager complements the Software Distribution feature and allows users to record and playback "low complexity" product installers.

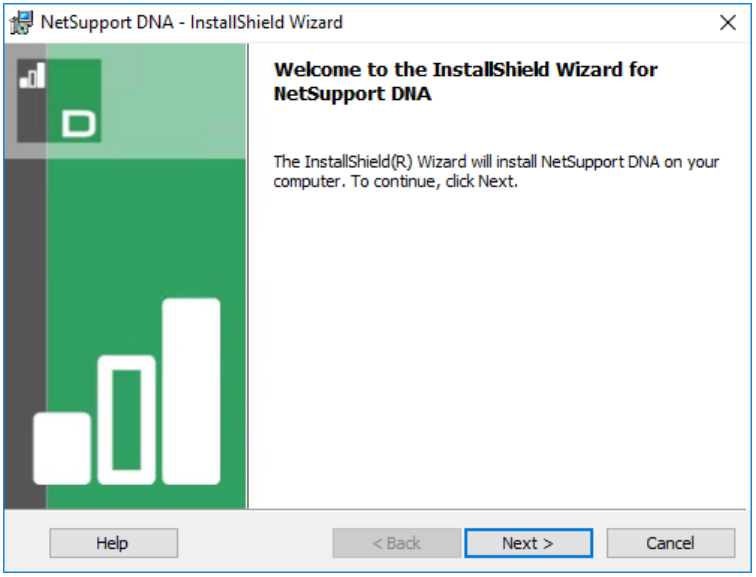
Note: It is recommended that NetSupport DNA Servers, Agent Gateway and Server Gateway components are installed on machines that have a resolvable DNS name and that DNS names are used throughout the configuration of Agents and consoles. If this is not possible, it is highly recommended that fixed IP addresses are assigned to any machine running the NetSupport DNA Server, Gateway Agent or Gateway Server components.

Starting the Installation

Download your copy of NetSupport DNA from
www.netsupportdna.com/downloads.asp

Click the appropriate language from the menu and select the option to install NetSupport DNA.

The NetSupport DNA installation will start displaying a Welcome screen.



Click **Next** to continue.

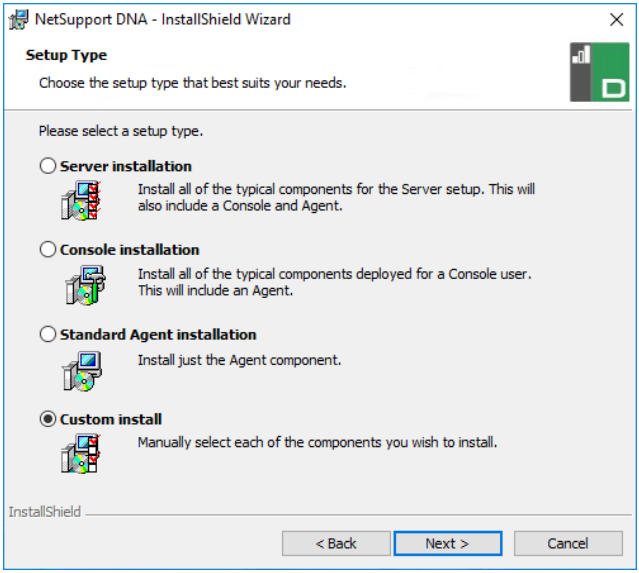
NetSupport Licence Agreement

The NetSupport Licence Agreement will be displayed. Please read the Licence Agreement carefully and select 'I accept the terms of the Licence Agreement' and click **Next** to continue.

If you reject the Licence Agreement, ('I do not accept the terms of the Licence Agreement') click **Cancel**. NetSupport DNA will not be installed and you will be directed to exit from the install program.

Select Setup Type

Choose the setup type to install on the workstation.



Server installation
Installs the NetSupport DNA Server, Console and Agent components.

Console installation
Installs the DNA Console and Agent components.

Standard Agent (Client) installation
Installs just the Agent component.

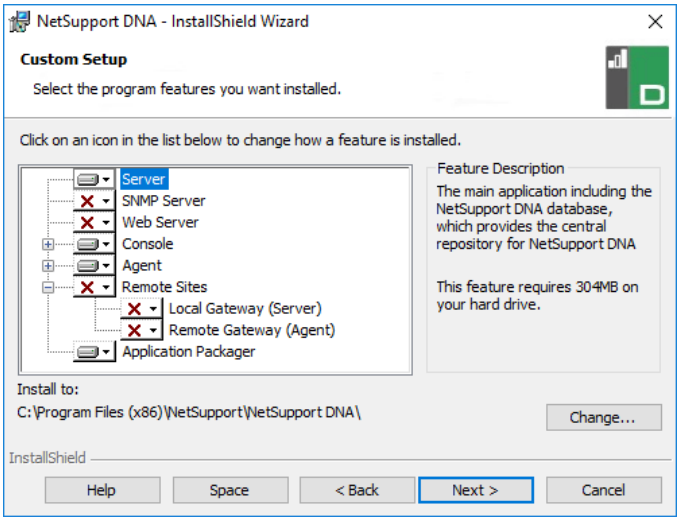
Custom installation
Allows you to pick and choose which components to install on the workstation.

Click **Next** to continue.

Custom setup

Decide which NetSupport DNA components to install.

Note: This screen will only appear if you selected **Custom Install** in the Select Setup Type dialog.



Server

The machine on which the server software is installed and the database is stored is called the NetSupport DNA Server.

An available SQL-based Server is required on which to install the NetSupport DNA database. This server provides all of the functionality of NetSupport DNA. It contains the repositories where all the collected data resides.

SNMP Server

The SNMP Server allows you to monitor and configure SNMP-enabled devices.

Note: If performing an SNMP Server-only install, you will need to enter the location of the NetSupport DNA Server or Remote Gateway.

Web Server
The Web Server is installed on a Windows machine. This allows the NetSupport DNA mobile app to connect to NetSupport DNA.
An available SQL-based Server containing the NetSupport DNA database is required.

Console
The NetSupport DNA Console is the main interface for executing commands and is generally installed on an administrator's machine. An administrator executes a command and the gathered data is extracted from the NetSupport DNA database which resides on the server.

If performing a Console-only install, you will need to enter the location of the server that will be used to connect to Agents.

Agent (Client)
The Agent component should be installed on end-user machines across your network. The server polls Agent machines at regular intervals, gathering and holding system information in the NetSupport DNA database.

If performing an Agent-only install, you will need to enter the location of the server that will be used to connect to Agents.

Note: NetSupport DNA provides a Discovery and Deploy tool, which is a convenient facility that remotely deploys NetSupport DNA Agents to Windows PCs.

Internet Restrictions
Enables you to use the internet blocking facility. By default, this is included when installing the Agent component.

Remote Sites

NetSupport DNA Local (Server) Gateway
The NetSupport DNA Gateway provides a means of connecting remote Agents to the NetSupport DNA Server. The Local Gateway communicates with the central NetSupport DNA Server. The Local Gateway must be installed separately from other NetSupport DNA components.

Note: If a DNA Server Gateway is installed on the same machine as a NetSupport Connectivity Server (NCS), remote control functionality over the DNA Gateway will not be available. (Applies to Education installations only).

NetSupport DNA Remote (Agent) Gateway
The Remote Gateway acts as a proxy server for the remote NetSupport DNA Agents, allowing them to communicate with the NetSupport DNA Server. The Remote Gateway can only be installed with the NetSupport DNA Agent.

Notes:
- There can be multiple Remote Gateways (one installed at each remote site) but only one Local (central) Gateway.
- The NetSupport DNA Console must be on the same network as the NetSupport DNA Server to be able to pick up Gateway Agents.

Application Packager
The NetSupport DNA Application Packager complements the Software Distribution feature and is a utility that can be used to record and playback "low complexity" product installers.

By default, NetSupport DNA will be installed in the folder C:\Program Files\NetSupport\NetSupport DNA.

Select **Next** to continue.

SQL Server Installation

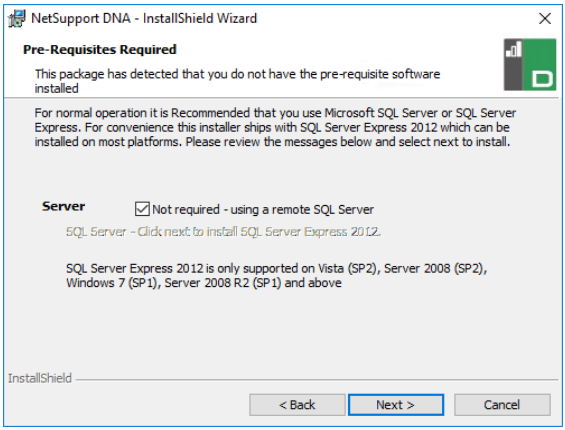
The SQL Server that you plan to use for the NetSupport DNA database can be installed on either the same computer as the NetSupport DNA Server, or a remote computer.

For supported operating systems, the NetSupport DNA installer can, if required, install and configure Microsoft SQL Server Express 2012 as part of the installation process.

Note: If you are using a remote SQL Server, please click here for further information on how to configure Microsoft SQL Server Express for use with NetSupport DNA.

Select **Next** to configure a Microsoft SQL Server.

Note: If you choose to install the SQL Server Express 2012 within NetSupport DNA, you will be directed to the Console User Setup screen.

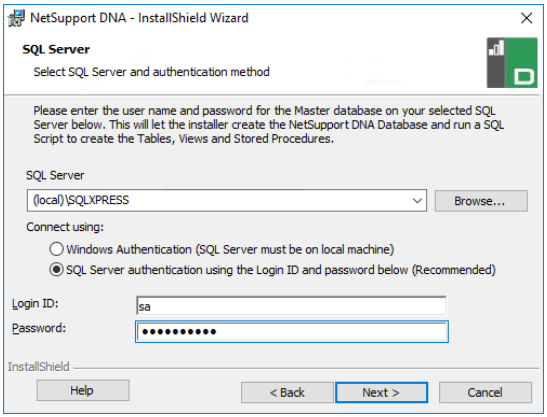


Setting up the Server

Select the SQL Server to install to from the drop-down list or click **Browse** to see a full list of SQL Servers.

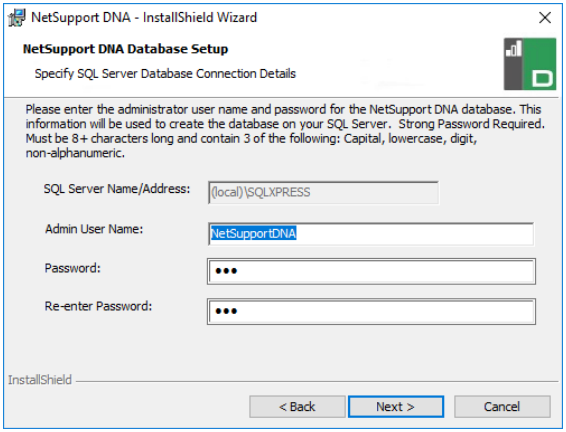
Choose the appropriate verification method: SQL or Windows. If SQL, enter the user name and password of your master database.

Note: This dialog will only appear if the server feature is being installed and you are using a remote SQL Server.



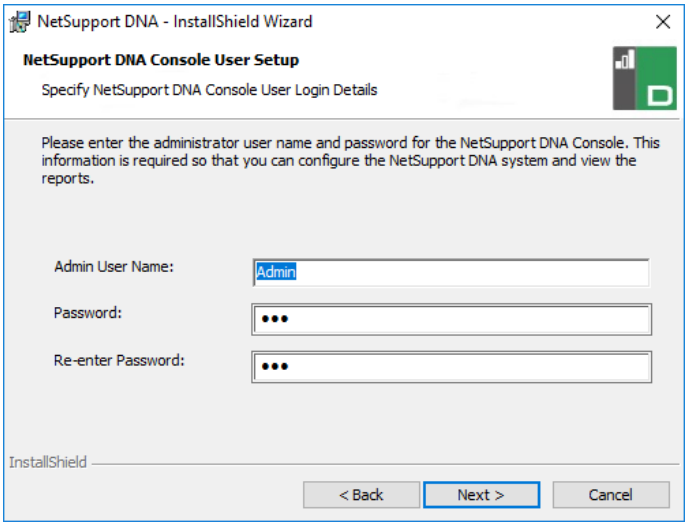
Click **Next**.

Enter the name and password to be used for the NetSupport DNA database and click **Next**.



Enter the user name and password to be used to access the NetSupport DNA Console once installed. Additional Console Operator logins can be created after installation.

Note: This dialog will only appear if the Server feature is being installed.

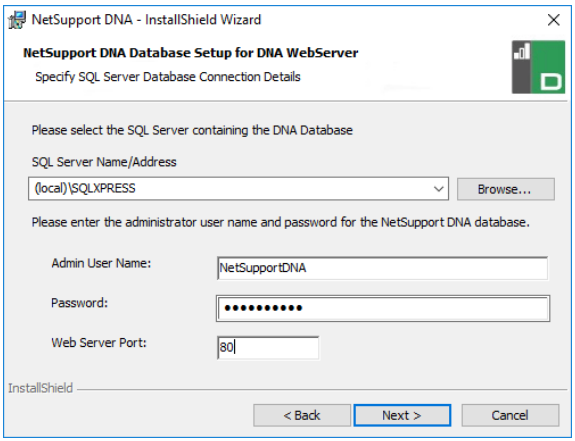


Web Server Database setup

The NetSupport DNA Web Server requires the address of the SQL Server that contains the NetSupport DNA Database. You will also need to provide the user name and password that the NetSupport DNA Server uses to connect to the database.

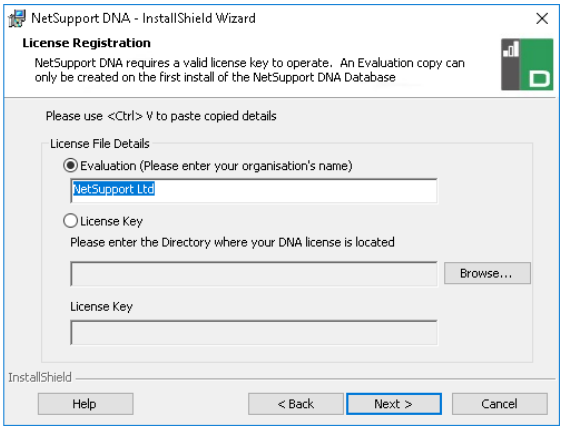
You can also configure the port the Web Server listens for connections on. By default, this is port 80. If you change the port number for the Web Server, you need to ensure that this is added to the end of the Server address used when logging onto the Mobile Console.

Note: This screen will only appear if you are installing the Web Server.



Note: If you do not know the user name or password, run the NetSupport DNA Database wizard on the machine running the NetSupport DNA Server. You can change the user name and password and enter the new details into the installer dialog. You will need to have the user name and password for the administrator of the SQL Server to make this change.

Select **Evaluation** and enter your organisation's name or enter the licence details you have been provided with. You will need to enter the directory where you have saved the NetSupport DNA licence file and enter the licence key number. The licence number is case sensitive. The NetSupport DNA standard evaluation licence runs for a period of 30 days and allows for a maximum of 50 users.

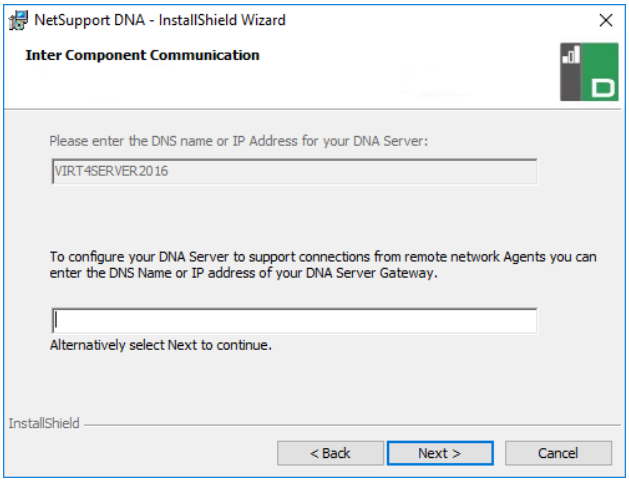


Note: If you are upgrading an existing installation, you will only have the option to enter the licence key details. If you have previously been using an evaluation licence and wish to continue with the evaluation, you will need to manually uninstall the software before installing the updated version. Before continuing with the upgrade, we recommend that you create a backup of your database. Please refer to our website, www.netsupportsoftware.com/support, for full instructions.

Click **Next**.

Inter Component Communications

If you are installing the NetSupport DNA Console, Agent, SNMP Server or Local Gateway, you will be required to enter the DNS name or IP address for the NetSupport DNA Server.



Note: If the DNS name or the IP address cannot be found, you will not be able to continue with the installation.

If you are installing the Remote Gateway, you will need to enter the DNS name or IP address for the Local Gateway. You will also have the option to enter this when installing the NetSupport DNA Server.

Click **Next** to continue.

Select Enterprise Type

NetSupport DNA is available in two versions: corporate and education. Each version features a wealth of components tailored to its intended sector. Businesses and educational institutions alike will benefit from the flexibility the product offers – whether they are focusing the management of multiple users across an enterprise (software distribution, alerting and licence management) or ensuring campus-wide cost savings (print monitoring, energy monitoring and power management).

Select your enterprise type and click **Next**.

Sufficient information has been provided to commence the installation. If you need to review any of the settings, click **Back**; to start the installation, click **Install**. To quit the installation, click **Cancel**.

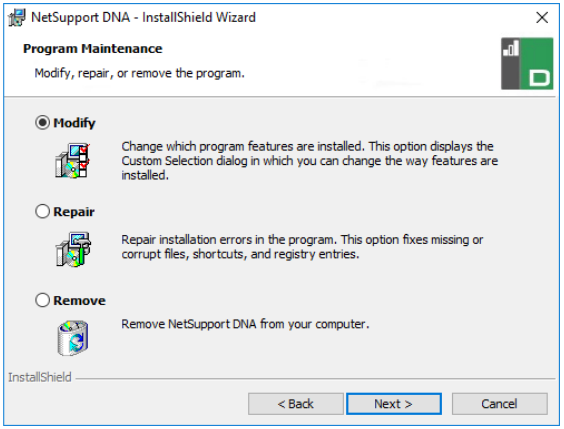
The final screen confirms that the installation has been successful. If you have installed the NetSupport DNA Console, you will have the option to launch this.

Notes:

- When installing the Console and/or Server, it is recommended that you use the latest SQL Native Client. This can be downloaded from www.microsoft.com/en-us/download/details.aspx?id=50402.
- After installation, a convenient utility can be run should you need to update your database, console or upgrade from an evaluation licence to a full licence. See: Using the NetSupport DNA Database Wizard.

Existing Installation

This screen will appear if a copy of NetSupport DNA has already been installed on a workstation.



Modify

Enables you to change the NetSupport DNA components that are currently installed.

Repair

Reinstalls all the program features installed by the previous setup and repairs any installation errors in the program.

Remove

This option removes all installed features.

Select the required option and click **Next**.

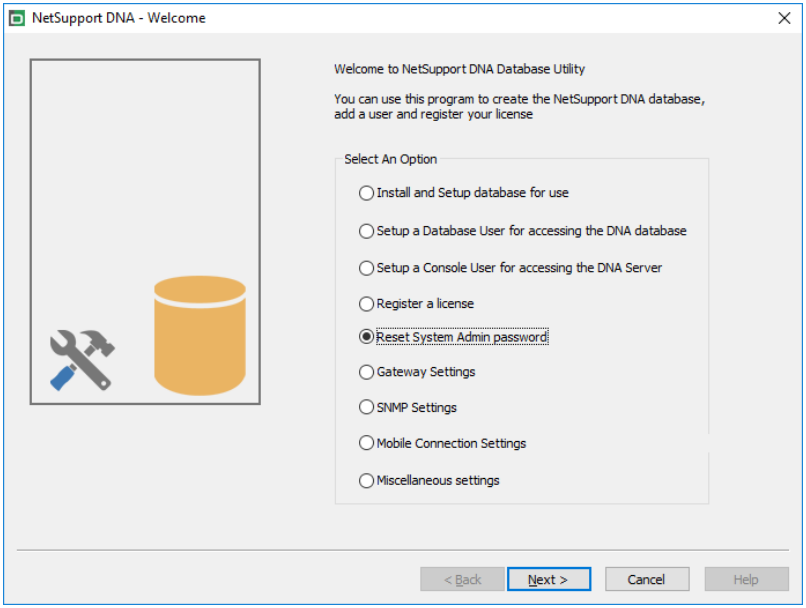
Using the NetSupport DNA Database Wizard

The NetSupport DNA Database wizard is a convenient utility that can be run after installation should you need to change any of your NetSupport DNA settings.

The wizard can be used to create the NetSupport DNA database; add database users; add console users; update licence details; reset the system admin password; add NetSupport DNA Gateway settings; set SNMP settings; set mobile connection settings; and set miscellaneous settings such as SQL Server address, timeout for queries and force AD authentication.

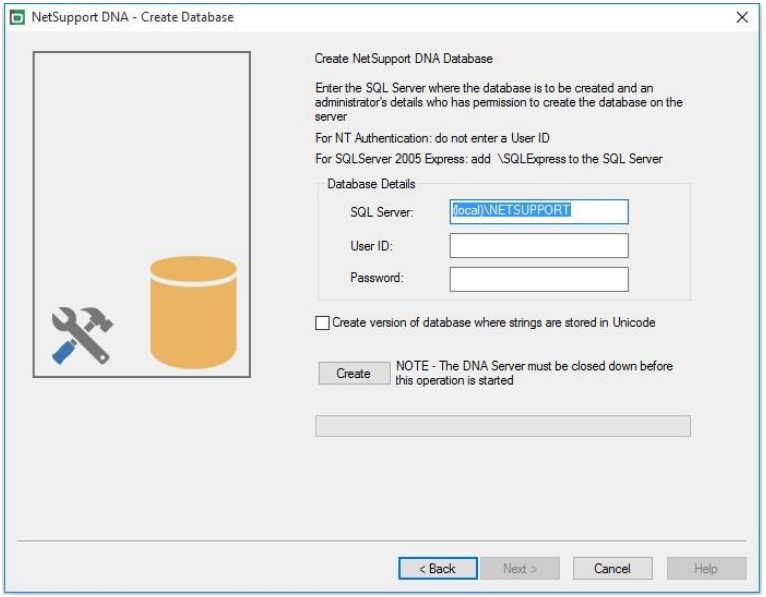
During installation, the NetSupport DNA Database wizard is copied to the Server folder of the NetSupport DNA program directory. The default location is c:\Program Files\NetSupport\NetSupport DNA\Server\DNADBWizard.

Note: For the changes to take effect, the Server service will need restarting.



Install and set up database for use

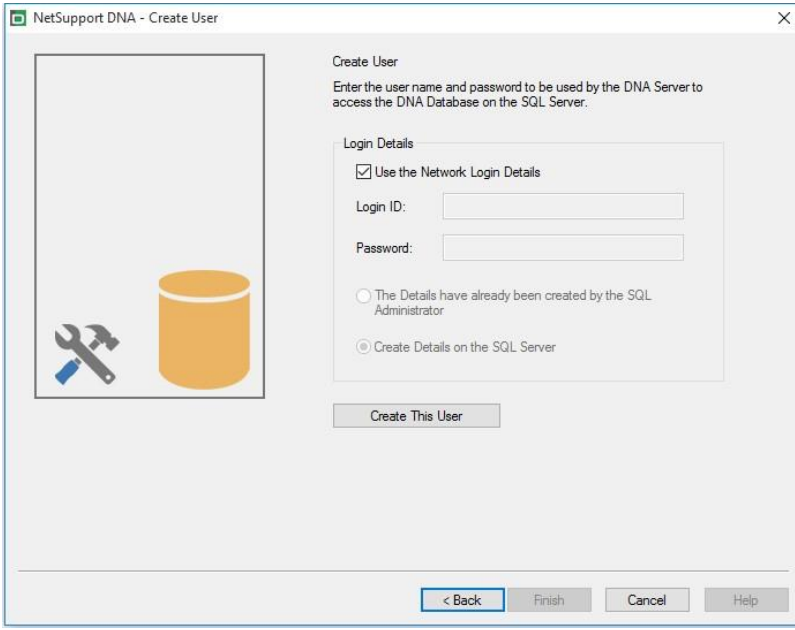
Enter the address/name of the SQL Server where the NetSupport DNA Database is to be created and the administrator logon details.



Set up NetSupport DNA user for accessing the database

This dialog enables you to create/change the user name and password used to access the NetSupport DNA Database on the Server. If using the existing access details, check that the details have already been created by the SQL administrator.

Note: It is preferable not to use an existing administrator login as this could compromise the security of other databases on the SQL server.

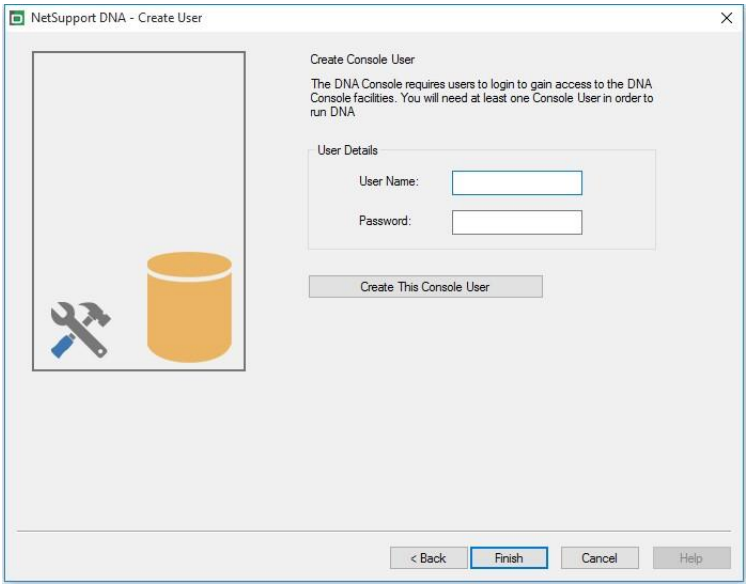


Set up admin users for accessing the NetSupport DNA Server

If there was a problem creating the Console user during installation, this option within the Database wizard can be used to create new Console users. Console users are provided with admin rights.

Notes:

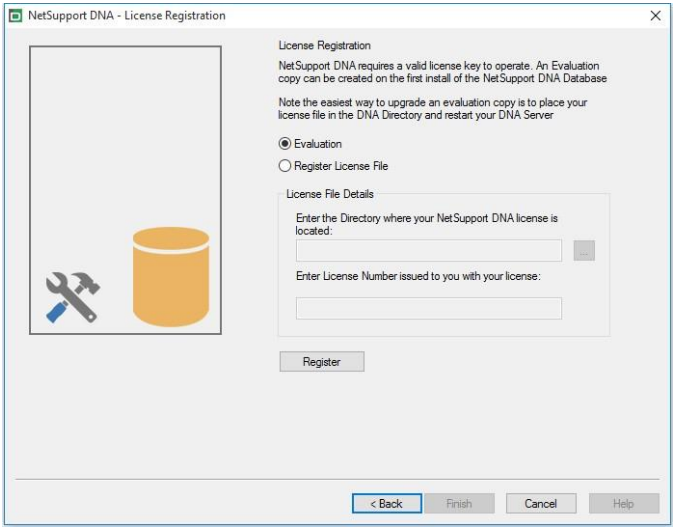
- Admin user rights are required for this operation. You will be prompted to enter the appropriate user name and password when you click **Create User**.
- Additional Console users can also be created via the Console program itself.



Register a Licence

The Database wizard enables you to update your NetSupport DNA licence details, for example, when switching from an evaluation licence to a full sale copy.

Note: Admin user rights are required for this operation. You will be prompted to enter the appropriate user name and password when you click **Registe**r.



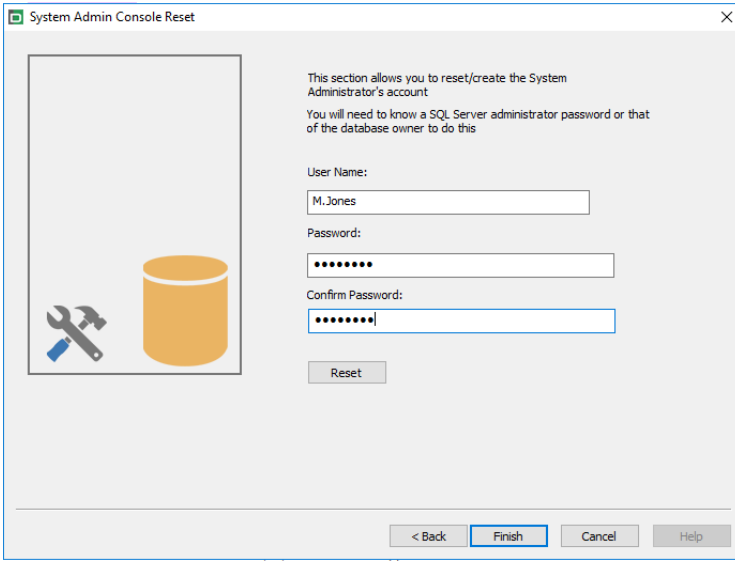
To register a full licence, copy the licence file supplied by NetSupport to an appropriate folder and enter the location into the Registration dialog.

Enter your licence number - the details are case sensitive. Click **Register** to update the licence.

Note: A key element in the day-to-day operation of NetSupport DNA is the frequency that the Server polls Agent machines to gather data for each of the main components (evaluation default = 10 minutes). However, if you have a large Agent base, the number and frequency of connections can place an unwanted overhead on performance. To counter this, when activating a 'sale' copy, NetSupport DNA will determine whether a more appropriate connection interval is required, based on the number of user licences being registered. Post-installation, a Console Operator can manually adjust the interval for each component if required.

Reset System Admin Password

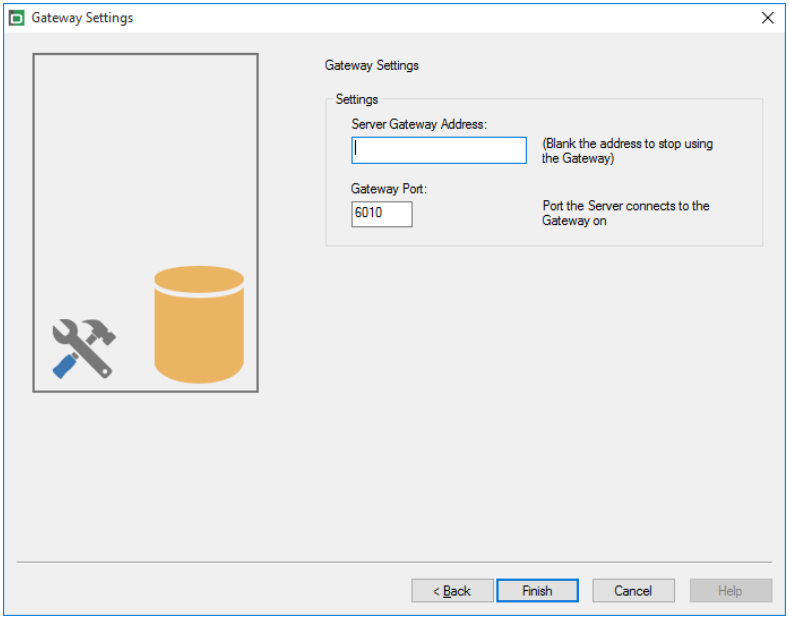
This option allows you to reset the password for the system administrator. To reset this, you will need to know the admin password for the SQL Server.



Enter the system admin user name and new password and click **Reset**. You will then be prompted to enter the details for the SQL Server, user ID (if required) and SQL Server admin password, click **OK**. The password for the system admin will be reset.

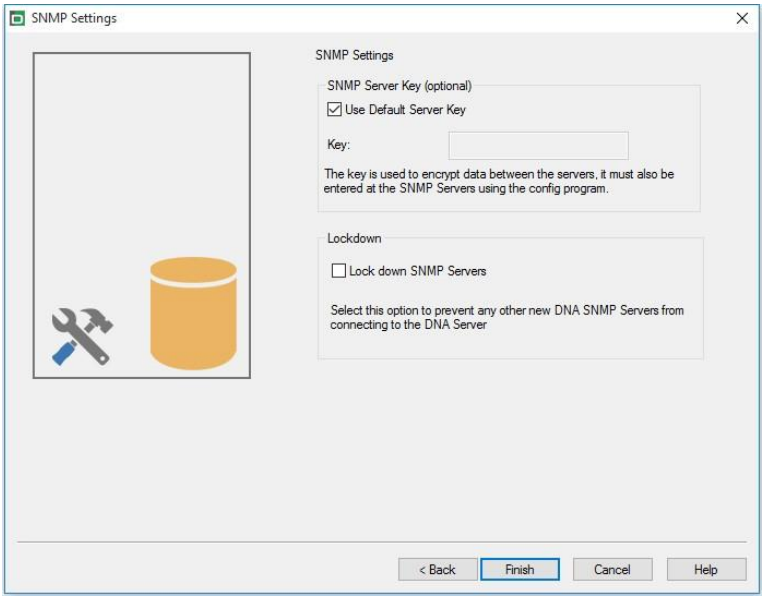
Gateway Settings

To start using the NetSupport DNA Gateway, enter the IP address for the Server Gateway. By default, the Gateway port is 6010. Alternatively, to stop using the NetSupport DNA Gateway, remove the Gateway address.



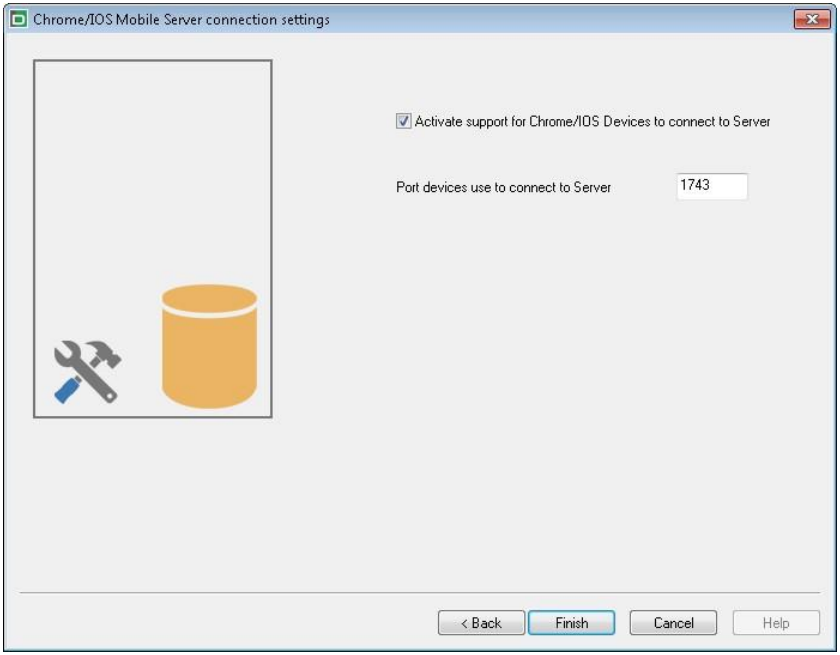
SNMP Settings

This dialog allows you to set an SNMP server key. This is used to encrypt data between servers and must also be set at the SNMP server. You can also lock down the SNMP servers, preventing any other SNMP servers from connecting to the DNA server.



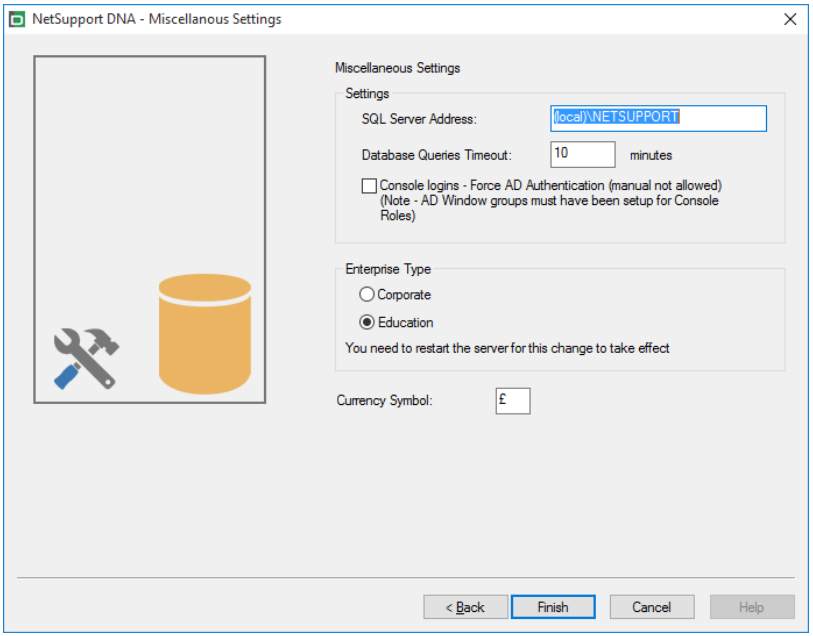
Mobile Connection Settings

By default, NetSupport DNA allows Chrome and iOS devices to connect to the Server, but this can be disabled from here. The port that devices use to connect to the Server is 1743.



Miscellaneous Settings

From this dialog, you can change various NetSupport DNA settings such as the IP address of the SQL Server, database queries timeout, force AD authentication, select the enterprise type and select the currency to be used.



By default, the database queries timeout is set to 10 minutes; you can amend this by entering the required value.

If you have assigned an Active Directory Windows group to a Console role, you can force AD authentication. The user will not be able to access the NetSupport DNA Console unless they are authenticated in Active Directory.

NetSupport DNA is available in two versions: corporate and education. Select the required enterprise type.

NetSupport DNA sets the currency from the system locale of the machine the DNA Server is located on. To change the currency used in the database, enter the required currency symbol here.

Installing via Active Directory

NetSupport DNA allows you to install Agents using Active Directory Group Policy Software Deployment.

In order to install using Active Directory, you will need to locate the DNA.ini and Agent.msi file.

The DNA.ini is stored in the following folder on the NetSupport DNA Console machine:

32bit C:\Program Files\NetSupport\NetSupport DNA\Console
64bit C:\Program Files (x86)\NetSupport\NetSupport DNA\Console

The Agent.msi is available from the downloads area:
www.netsupportdna.com/downloads.asp

For full instructions on how to configure an Active Directory deployment, please visit our Knowledge Base and refer to product article **Installing the NetSupport DNA Agent via Active Directory Group Policy software deployment**.

Advanced Option - Command Line Installation

NetSupport DNA allows administrators to install the Console, Agent, Application Packager and the Remote and Local Gateways from the command line using the MSI installers supplied. In addition, the Console, Agent and Application Packager can be installed via Active Directory.

To carry out installation from the command line

1. Place the appropriate MSI installation file into the same folder as the configuration file on the target machine, or an accessible share.
2. Edit the INI file to set the appropriate settings for your installation, e.g. ServerAddress=, InstallDir=
3. On the target machine, execute the installation according to the following examples:

To install the NetSupport DNA Agent

msiexec.exe /qb /i "NetSupport DNA 470 Agent.msi"

To control which local users NetSupport DNA Console is installed for

msiexec.exe /qb /i "NetSupport DNA 470 console.msi" ALLUSERS=2

ALLUSERS=””	Installs the package for the current user only.
ALLUSERS=1	Installs the package for all local users.
ALLUSERS=2	Checks if the current user has administrative privileges. If so, the package will install for all users, otherwise, it will only install for the current user. **Not supported for NetSupport DNA MSI installers.**

There is a sample DNA.INI file that is created in your Console installation directory. This allows you to customise various parameters for the MSI installation.

Agent and Console options

[All]

InstallDir=	Leave blank for default installation directory, also applies to Application Packager installs.
ServerAddress=	IP address or, preferably, DNS name of the NetSupport DNA Server.

Agent only options

[Agent]

EnableLSP=	1 = install the NetSupport LSP, 0 = do not install
RemoveUninstallOption=	1 = does not appear in Add/Remove programs

Installation via Active Directory (AD)

There are no special considerations for installation of NetSupport DNA using Active Directory.

1. Place the NetSupport DNA MSI and INI file in a share on your AD server which is accessible to your computers/users.
2. Create or edit a Group Policy object (GPO) that affects the users or computers you wish to install NetSupport DNA for.
3. Create a new AD Software Installation Package under either Computer Configuration or User Configuration as appropriate.
4. Assign or publish the package.

For further information on Active Directory software installation, please refer to Microsoft Help resources:
http://support.microsoft.com/kb/816102

Installing NetSupport DNA Agent on Mac Systems

A NetSupport DNA Agent can be installed on Mac systems, allowing you to effectively manage your Mac machines.

Note: The NetSupport DNA Mac Agent supports Mac OS X 10.8 and above.

1. The NetSupport DNA Agent is provided as a standard Mac OS X .DMG file. This is available from the downloads area on our website.
2. To mount the drive image, copy to the hard drive and double click. The mounted drive image will be available on the desktop.
3. The installer will automatically run - follow the on-screen instructions.

Features supported on Mac Agents:

- Gather a full hardware and software inventory from the Agent machine.
- Automatically notify operators of any hardware and software alerts.
- A detailed summary of all internet activity.
- A summary of all applications used.
- Real-time monitoring of Agent machines in icon, details or thumbnail view.
- A single time-based summary of all activity presented in a chronological view.
- Remote control Agent machines, allowing Operators to remotely troubleshoot and perform administrative tasks.
- Agents can report a concern.*
- Monitor keywords and phrases.*

* These features are only available in the Education Edition of NetSupport DNA.

NetSupport Browser for iOS

NetSupport DNA provides a mobile Browser app for iOS tablets and smartphones that supports NetSupport 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 NetSupport DNA Server and is then available for reporting within the NetSupport DNA Console.

The app also supports NetSupport School's core classroom management tools, enabling real-time student interaction and support during a lesson. For more information on NetSupport School, click here.

The NetSupport Browser app can be downloaded from the Apple App Store on iOS 9.3 or higher devices.

For information on how to centrally configure and deploy the NetSupport Browser, please click here.

Standard browser navigation features - including bookmarks, add tabs (with the option to set a default Home Page), internet history, plus the option to change the default search engine - are also included.

Note: By default, the port that devices use is 1743. This can be changed in the NetSupport DNA Database wizard.

Supported features:

- **Real-time Monitoring** - An Operator or teacher via the Console can view a real-time summary of all devices. Selected devices can be viewed either in a detailed list view or via real-time thumbnails of each device screen.
- **Internet Metering** - A summary of internet activity via the app 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** (Education Edition) - This tool helps schools protect students from being exposed to inappropriate online content. It alerts staff 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, radicalisation, child sexual exploitation - and much more.

- **Safeguarding Resources** (Education Edition) - The Safeguarding Resources icon, displayed on the Browser app's toolbar, gives students instant access to a list of appropriate online support resources.
- **Report a Concern** (Education Edition) **-** Students can report concerns directly and discreetly to nominated school staff.
- **Hardware Inventory** - When the DNA Browser is launched on a device, an inventory is dynamically sent to the NetSupport 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.
- **Collect roaming data**– If devices are used away from the network, the app can be configured to record activity in the background with the stored data collected by the central DNA Server once re-connected.

NetSupport DNA Browser for Android

NetSupport DNA provides a mobile Browser app for Android tablets and smartphones, allowing you to gather key system inventory details and monitor online activity. The data collected is dynamically sent to your local NetSupport DNA Server and is then available for reporting within the NetSupport DNA Management Console.

The NetSupport DNA Browser for Android app can be downloaded from the Google Play store on Android 5.01 and above devices.

Standard browser navigation features - including bookmarks, add tabs (with the option to set a default Home Page), internet history, plus the option to change the default search engine - are also included.

Note: It is recommended that a suitable third-party MDM solution is used to enable central deployment and lockdown of the app and its configuration.

Supported features:

- **Real-time Monitoring** - An Operator can view a real-time summary of all devices. Selected devices can be viewed either in a detailed list view or via real-time thumbnails of each device screen.
- **Internet Metering** - A summary of internet activity via the app 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** (Education Edition) – This tool helps schools protect students from being exposed to inappropriate online content. It alerts staff 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, radicalisation, Child Sexual Exploitation - and much more.
- **Safeguarding Report a Concern** (Education Edition) - Students can report concerns directly and discreetly to nominated school staff.
- **Safeguarding Resources** (Education Edition) - The Safeguarding Resources icon, displayed on the Browser apps toolbar, gives students instant access to a list of appropriate online support resources.
- **Hardware Inventory** - When the NetSupport DNA Browser is launched on a device, a full inventory of the device is dynamically

sent to the NetSupport DNA Server for subsequent viewing in the Console.

- **Software Inventory** - When the NetSupport DNA Browser is launched on a device, a full inventory of the installed programs on the device is dynamically sent to the NetSupport DNA Server for subsequent viewing in the Console.
- **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.
- **Chat** – Console Operators can launch a two-way chat session with any number of selected users.
- **Message** – Console Operators can broadcast a one-way notification to selected users.

NetSupport DNA Chrome Agent

The NetSupport DNA Agent extension for Chrome OS supports NetSupport DNA's core desktop management capabilities. When launched within a Chrome Browser, it will interrogate the device to gather key system inventory details and monitor online activity. The data collected is dynamically sent to your local NetSupport DNA Server and is then available for reporting within the NetSupport DNA Management Console.

The NetSupport DNA Chrome Agent extension can be downloaded from the Chrome Web Store.

For information on how to centrally configure and deploy the NetSupport DNA Agent Extension for Google Chrome, please click here.

Note: By default, the port that devices use is 1743. This can be changed in the NetSupport DNA Database wizard.

Supported features:

- Gather a full hardware inventory from the Agent machine.
- Real-time monitoring of Agent machines in icon, details or thumbnail view.
- Agents can report a concern.*
- Monitor keywords and phrases.*
- A detailed view of all internet activity.
- Console Operators can see a chronological view of device activity for a selected time period.
- Real-time alerts enable Console Operators to immediately identify any user who has attempted to access a restricted website or triggered a Safeguarding keyword.

* Only available in the Education Edition of NetSupport DNA.

NetSupport DNA Gateway

The NetSupport DNA Gateway provides a stable and secure method for locating and connecting to Agents on remote networks securely via the internet. Multiple remote locations can communicate data back to a central location with the use of the included Remote and Local Gateway components.

NetSupport DNA Local (Server) Gateway
The NetSupport DNA Gateway provides a means of connecting remote Agents to the NetSupport DNA Server. The Local Gateway communicates with the central NetSupport DNA Server. The Local Gateway must be installed separately from other NetSupport DNA components.

Note: If a DNA Server Gateway is installed on the same machine as a NetSupport Connectivity Server (NCS), remote control functionality over the DNA Gateway will not be available. (Applies to Education installations only).

NetSupport DNA Remote (Agent) Gateway
The Remote Gateway acts as a proxy server for the remote NetSupport DNA Agents, allowing them to communicate with the NetSupport DNA Server. The Remote Gateway can only be installed with the NetSupport DNA Agent.

Notes:
- There can be multiple Remote Gateways (one installed at each remote site) but only one Local (central) Gateway.
- The NetSupport DNA Console must be on the same network as the NetSupport DNA Server to be able to pick up Gateway Agents.
- Gateway installation

The Gateway components can only be installed on Windows XP SP3 or higher machines.

When performing a NetSupport DNA Installation, select the required Gateway components to install from the Custom Setup Screen. When installing the Local Gateway, you will be required to enter the IP address of the NetSupport DNA Server. The IP address of the Local Gateway needs to be entered when installing the Remote Gateway.

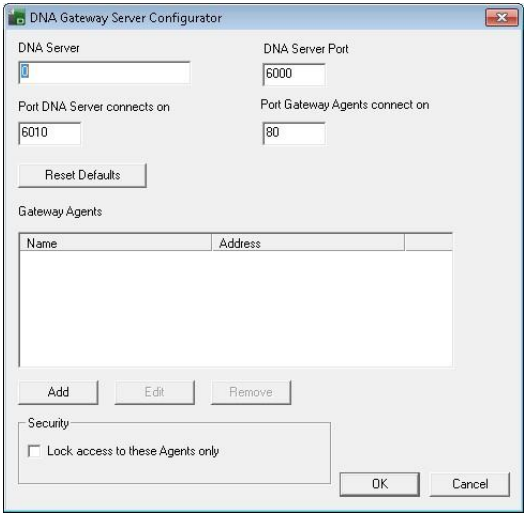
Note: To use the NetSupport DNA Gateway, the IP address of the Local Gateway will need to be entered in the NetSupport DNA server. This can be done during installation or in the NetSupport DNA Database wizard after installation.

You can configure the parameters for the Local and Remote Gateway in the Server (Server) Gateway Configurator and the Agent (Remote) Gateway Configurator.

The current status of the Remote Gateways and connected NetSupport DNA Agents can be viewed in the Gateway Status dialog. Select the Tools tab and click the **Gateway Status** icon.

Gateway Server (Local) Configurator

The Gateway Server Configurator allows you to configure the parameters for the Server Gateway (Local Gateway). During installation, the Gateway Server Configurator is copied to the Gateway folder of the NetSupport DNA program directory c:\Program Files\NetSupport\ NetSupport DNA\Gateway\DNAGatewayConfigS.exe.



DNA Server
The IP address of the NetSupport DNA Server.

DNA Server Port
NetSupport's default Server port number is 6000.

Port DNA Server connects on
The default port that the NetSupport DNA Server connects to the Server Gateway is 6010.

Port Gateway Agents connect on
NetSupport's default port that the Server Gateway and Agent Gateway communicate on is 80.

Reset Defaults
Returns all port settings back to the default values.

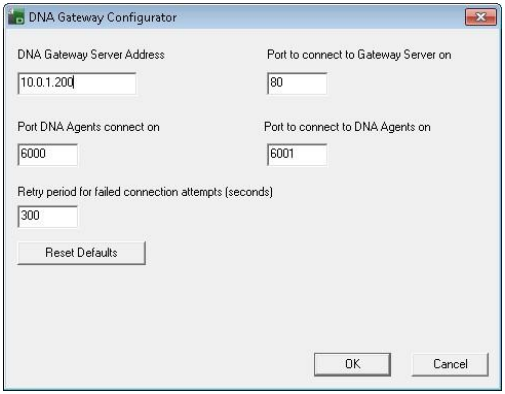
Gateway Agents
Any Gateway Agents that have been found by the Server Gateway will be listed. You can add, edit and remove Agents by clicking the appropriate button.

Security
Selecting **Lock access to these Agents only** allows you to control which remote machines can connect to your Server Gateway.

Note: You can configure the IP address of the Server Gateway in the NetSupport DNA Database wizard.

Gateway Agent (Remote) Configurator

The Gateway Agent configurator allows you to configure the parameters for the Agent Gateway (Remote Gateway). During installation, the Gateway Agent Configurator is copied to the Gateway folder of the NetSupport DNA program directory c:\Program files\NetSupport\ NetSupport DNA\Gateway\DNAGatewayConfigC.exe.



DNA Gateway Server Address
The IP address of the Server Gateway.

Port to connect to Gateway Server on
NetSupport's default port that the Server Gateway and Agent Gateway communicate on is 80.

Port NetSupport DNA Agents connect on
NetSupport's default port that NetSupport DNA Agents use to connect to the Agent Gateway is 6000.

Port to connect to NetSupport DNA Agents on
NetSupport's default port that the Agents Gateway uses to connect to the NetSupport DNA Agents is 6001.

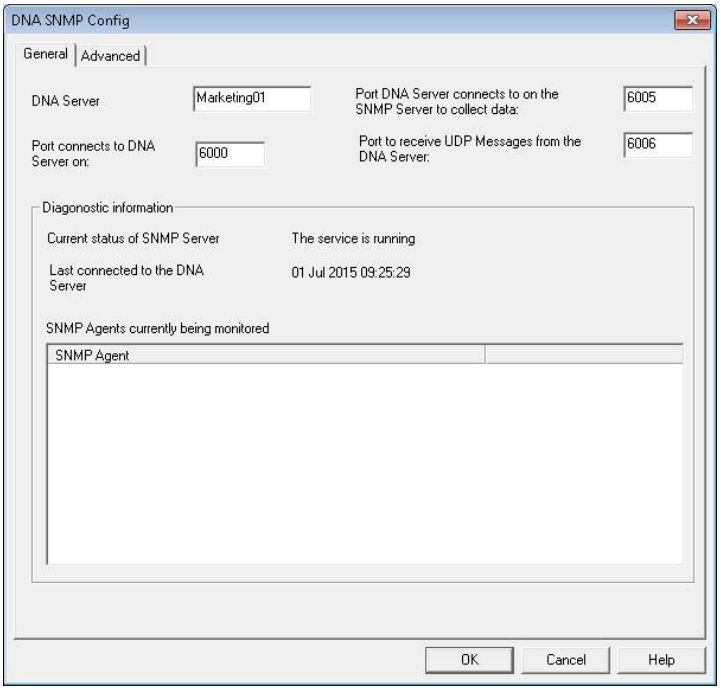
Retry period for failed connection attempts (seconds)
By default, the retry period for failed connections will be 300 seconds, enter a different value if required.

Click **Reset Defaults** to return all settings back to the default values.

Note: You can configure the IP address of the Server Gateway in the NetSupport DNA Database wizard.

SNMP Server Configuration

The SNMP Server Configurator allows you to configure the parameters for the SNMP Server. During installation, the SNMP Server Configurator is copied to the SNMP Server folder of the NetSupport DNA program directory c:\Program Files\NetSupport\NetSupport DNA\SNMPServer\ DNASNMPConfig.exe.



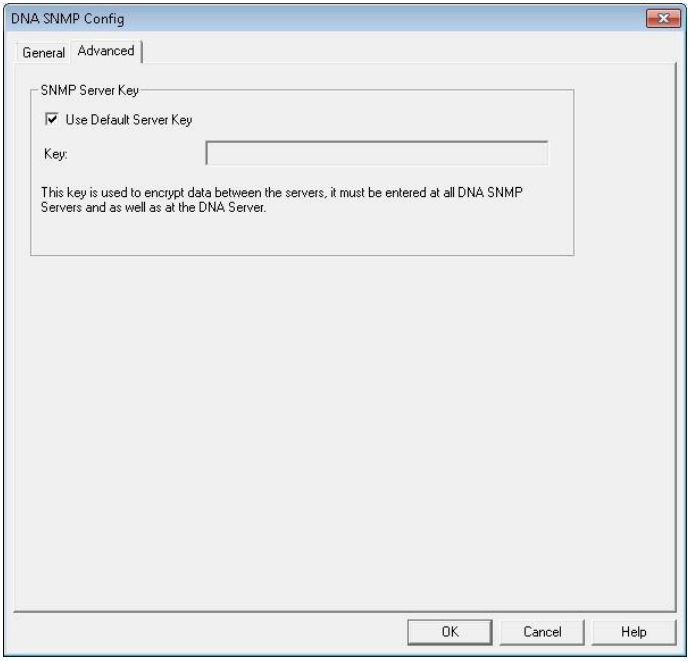
DNA Server
The DNS address of the NetSupport DNA Server.

Port DNA Server connects to on the SNMP Server to collect data
NetSupport's default port that the NetSupport DNA Server uses to connect to the SNMP Server to collect data is 6005.

Port connects to DNA Server on
NetSupport's default port that NetSupport DNA Devices use to connect to the NetSupport DNA Server is 6000.

Port to receive UDP Messages from the DNA Server
NetSupport's default port that is used to receive messages from the NetSupport DNA Server is 6006.

Diagnostic information
Provides information on the current status of the SNMP Server, the last connection time and the SNMP Devices currently being monitored.



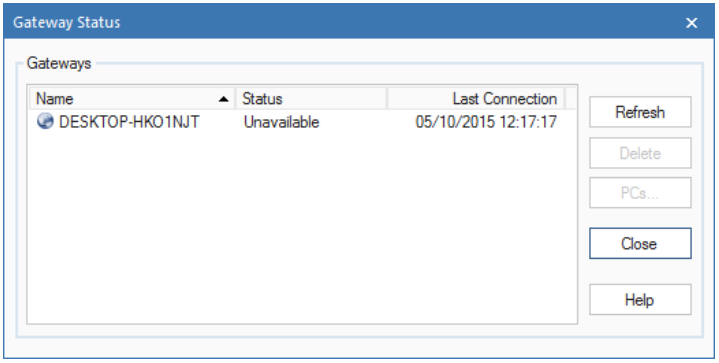
Use Default Server Key
Allows you to set an SNMP server key. This is used to encrypt data between servers and must be set at the SNMP server and NetSupport DNA Server.

Note: You can set a server key in the NetSupport DNA Database wizard.

Gateway Status

The Gateway Status dialog allows you to check the current status of your Remote Gateways. You can also view the NetSupport DNA Agents connected to the Remote Gateways.

1. Select the Tools tab and click the **Gateway Status** icon.
2. The Gateway Status dialog will appear.



3. Your Remote Gateways will be listed. From here, you can see the name, current connection status of **OK** or **Unavailable** and the last connection time.
4. To view the Agents connected to a Gateway, select the required Gateway and click **PCs**.
5. Disconnected Remote Gateways can be deleted from this dialog. Select the required Gateway and click **Delete**.

Click **Refresh** to update the information. By default, the Gateway status is updated every ten minutes.

Note: If the Local Gateway is restarted, it can take the Agent Gateway five minutes to reconnect, unless the Remote Gateway is restarted.

Upgrading from Existing NetSupport DNA Versions

If you are upgrading to the latest version of NetSupport DNA from a previous version of NetSupport DNA (NetSupport DNA 2.70 and above), you can install the new version from the NetSupport DNA Installer.

Note: If you are upgrading from a NetSupport DNA version before NetSupport DNA 2.70, please refer to our website www.netsupportsoftware.com/support for instructions.

1. Run the new NetSupport DNA setup.exe on the PC where the NetSupport DNA Server is located.
2. Follow the on screen instructions. The previous NetSupport DNA version will be removed and the latest version of NetSupport DNA will be installed. All previous NetSupport DNA settings will be kept.
3. Consoles and Agents will be updated to the new version the next time they connect to the Server.

NetSupport DNA Mobile Console

The DNA Mobile Console app allows a technician, when away from their desk, to search for and view a detailed Hardware and Software Inventory for any PC on the company network. The Mobile Console app also includes a QR code scanner to help instantly identify any machine, either from an on-screen QR code displayed in the DNA Agent window, or from a label fixed to the device. NetSupport DNA also provides a QR code label creation facility, including support for custom details. Histories of all hardware changes as well as any software installs or removals are also shown on the app.

In addition to the Inventory and History views, the NetSupport DNA Mobile app also highlights any new PC alerts that have triggered across the network.

The NetSupport DNA Mobile Console app can be downloaded for free from the Google Play and Apple app stores.

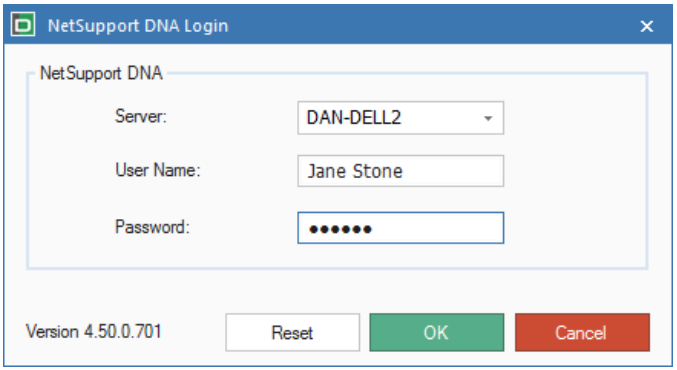
For further information on how to install and configure, click here.

GETTING STARTED

Running the Console

After installation, Administrators (Console Users) can load the NetSupport DNA Console and start interrogating the database.

1. Select {Start}{Programs}{NetSupport DNA}{NetSupport DNA Console}.
2. The Console Login dialog will appear.



3. Confirm that the specified Server address/name is correct. If not, you can manually enter the details. Enter the Console user name and password.
4. Click **OK**.
5. The main NetSupport DNA Console screen will appear.

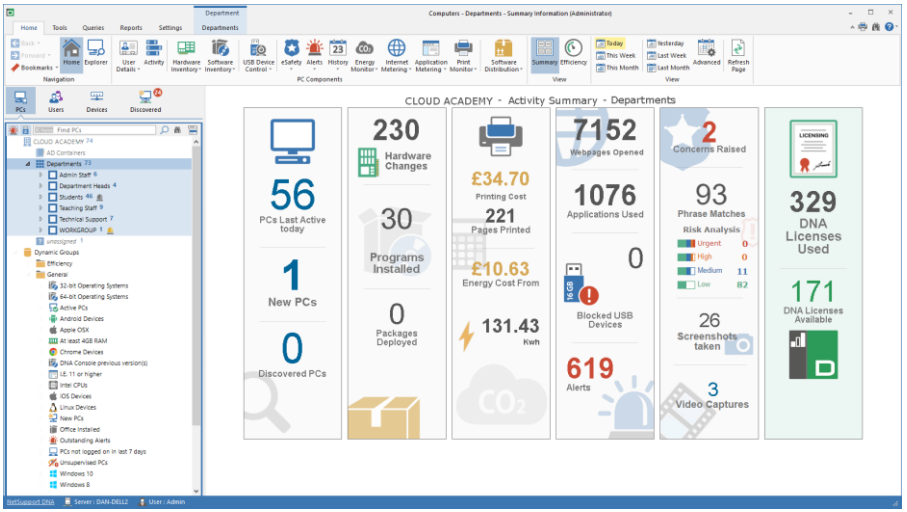
Note: If Secure Mode is enabled, the console user has three attempts to log in before their account is locked out. An Administrator will need to unlock the account, unless the console user has an email address and the email settings have been configured; then a reset option will be available, sending a temporary password by email. The console user will be required to change this password the next time they log in.

The Console Window

The Console Window is the primary interface for accessing the wealth of options provided by NetSupport DNA. A convenient Tree view enables you to quickly display data for a given PC, User, Device or Discovered PC.

When you first log into the Console, a summary screen will be displayed, providing an overview of each of NetSupport DNA's main components. This view can be switched to Efficiency View which provides a dashboard highlighting at a glance how technology is being used and the areas where efficiency can be improved to create cost- and time-saving benefits.

Note: If more than one Console Operator is logged in, only one of them will have access to alter NetSupport DNA's configuration settings. The other Operators will be advised they have read-only access.



Ribbon/Toolbar

The ribbon provides access to all NetSupport DNA's tools, components and configuration utilities and is organised into five main tabs:

1. **Home**
   Provides access to NetSupport DNA's components. Some components have a drop-down menu to access functions relating to it. These functions are also available in the ribbon when a component is active.

2. **Tools**
   Provides access to NetSupport DNA's tools.

3. **Queries**
   The Query Tool enables you to create customised reports based on specific criteria. Once created, the queries can be associated with the appropriate NetSupport DNA component for ease of retrieval on an on-going basis.

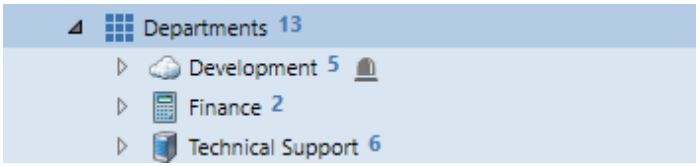
4. **Reports**
   NetSupport DNA provides a variety of pre-defined print-optimised management reports powered by the Crystal Reports engine. Reports can be printed or exported in a variety of formats.

5. **Settings**
   Provides access to profiles, where component settings can be configured and assigned to specific users, Active Directory groups, PCs or departments. Console Preferences can be accessed from here and Operators can be added and have roles assigned to them. And specific to the DNA Education Edition, you can activate the Cloud-based safeguarding console, designed to help Safeguarding Leads access safeguarding alerts on the go and configure the Report Concerns via a website facility.

Notes:
- When an item or user is selected in the Tree view, an additional tab will be displayed in the ribbon. This tab provides quick access to functions available for the selected item.
- The functions displayed in each tab will vary, depending on the Tree view that you are in.

The ribbon can be minimised by clicking ^ at the top right of the Console.

Hierarchy Tree view
The Tree view lists all dynamically-found NetSupport DNA Agents. By default, the Tree will reflect the structure of your workgroup/domain, but you can customise it to suit individual requirements, for example, grouping Agents by geographical location or department. To further highlight items in the Tree view, you can apply custom images to departments, dynamic groups, PCs and Users.



To apply a custom image to a PC or User, select it in the Tree view, right click and select **Properties**. The Properties dialog will appear. Click and browse to the required image, this will now be displayed in the Tree.

Notes:

- NetSupport's integration with Active Directory allows you to view the Hierarchy Tree as per your Active Directory structure. To view PCs in their Active Directory Containers, see **Console Preferences - Active Directory Settings**, you can hide the AD Containers in the Tree view, if required.
- Bookmarks can be added to the PCs, Users and Devices Tree view, allowing you to quickly navigate to a required location.
- By default, only the first 100 items will be displayed in a department in the Tree view. To view all items, click **More**.

The Tree view can be switched between the following options:

- **PCs**
- **Users**
- **Devices**
- **Discovered**

At the top of the Tree view, a search tool is provided that allows you to identify and locate Agents within it. This is not available for the Discovered Tree view.

The **PCs** Tree view displays PCs and data for the PC owner who has been associated with that PC. The PC owner can be changed in the Bind Users dialog. Non-standard items can be added in the PCs Tree.

Note: By default, mobile Agents will appear in the Tree view in an unassigned department. These Agents can be moved to an appropriate department - see Adding Agents to Departments.

The **Users** Tree view displays logged on users and only shows data relevant to them and not the PC. Only the User Details, Activity, USB Device Control, eSafety*, Internet Metering, Application Metering and

Print Monitor components are available when the Users Tree view is selected.

The **Devices** Tree view displays details of any SNMP Agents.

Note: You can customise how Agents are displayed in the above Tree views. Click  and select a display name from the list.

The **Discovered** Tree view will display any computers that were not found at start-up. You can configure NetSupport DNA to scan the network to look for any machines that do not have an Agent installed. Once discovered, you will be able to view a basic Hardware Inventory for the machine and have the option to deploy an Agent to it.

Note: The Discovered Tree view can be hidden, if required. Select the Settings tab and click the **General** icon. The DNA Configuration dialog will appear: click the **General** option under Console Preferences and deselect **Show Discovered PC tree**.

In addition, you can create Dynamic Groups enabling you to quickly identify Agents matching specific criteria. A typical Dynamic Group might be "all PCs running Windows 10". A selection of efficiency and general dynamic groups are provided.

The Tree view can be filtered to only show PCs/Users/Devices that match a Dynamic Group query. Select the required Dynamic Group in the Tree, right-click and select **Apply as Filter**. A filter bar will be displayed at the top of the Tree view showing what Dynamic Group filter has been applied. To remove the filter, click **Clear**.

Information window

The information window displays the data that has been gathered for each of NetSupport DNA's main components. For ease of navigation, icons identifying each component are displayed in all tabs except in the Tools and Settings tab.

A variety of views and filters are available for each component, allowing you to customise the content and format the data displayed in the information window.

The Status bar displays a link to the NetSupport DNA website, the Server the Console is connected to, the user currently signed into the Console and, if cloud* access has been enabled, whether data is being

synchronised to the cloud. When viewing reports, you can switch between layouts and a zoom slider is available. The status bar can be enabled/disabled in the Tools tab.

* The eSafety component and cloud are only available in the Education Edition of NetSupport DNA.

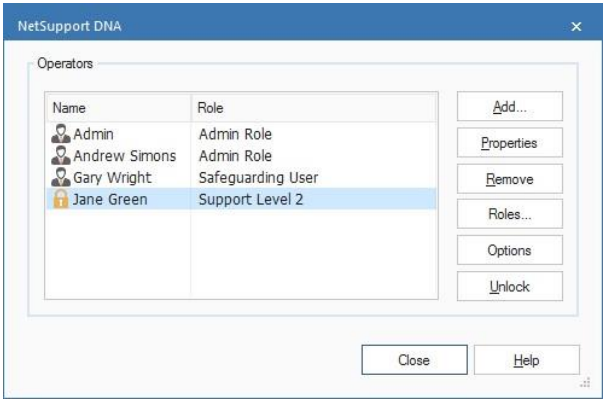
Create Additional Console Users

Additional Console logins can be created. Each user is assigned *Administrator* or *Operator* rights, enabling you to restrict functionality for certain Console users. An Operator will need to be assigned a role. A role allows you to define the access rights for users, enabling you to quickly allocate the same rights to multiple users. Multiple roles can be created.

To increase Console security, Secure Mode can be enabled. This forces Console Operators to use complex passwords. You can specify what complex passwords must consist of, along with the option to disable Operator accounts after three unsuccessful login attempts.

Note: In the Education Edition of NetSupport DNA, Console users can be created when adding contacts in the eSafety feature. These users will have a safeguarding role assigned to them and can only be edited or deleted in the Configure Safeguarding Users dialog.

1. In the Settings tab, select the **Operators** icon. The Console Operators dialog will appear.

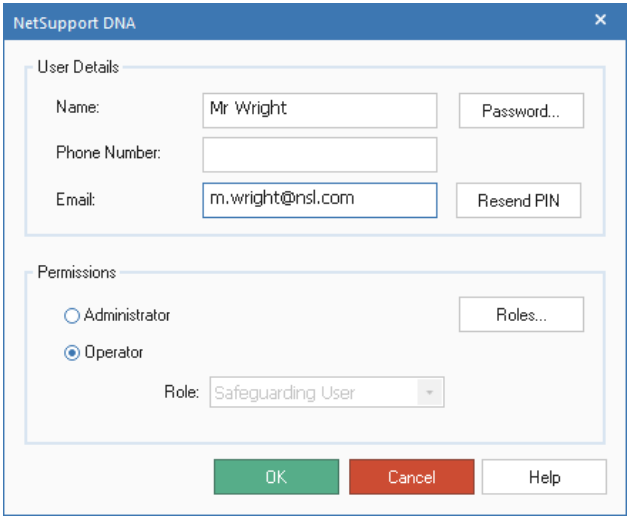


2. To create new Operator logins and assign the appropriate role, click **Add.** To edit an existing user, select the name and click **Properties**. To create or edit roles, click **Roles**.
3. To enable Secure Mode and decide the required level for complex passwords, click **Options**.
4. To remove an item, select the name and click **Remove**.
5. Operator accounts that have been disabled can be unlocked from here. Select the locked Operator, click **Unlock** and reset the password (the Operator can change this the next time they log in).

Note: Only one Console Operator will have access to alter the configuration settings in the case that more than one Operator is logged in at the same time.

Create or Edit Console Operator Logins

This dialog is used to create additional or edit existing Console Operator logins.



1. Enter the user's name. This will also act as the login name, along with their contact number and email address.

   Note: A unique email address must be entered for the console Operator.

2. To change the password for existing Operators, click **Password**. (This will only appear when editing existing Operators).

   Note: When setting a password, you have the option to insist the user changes this to one of their own choosing the first time they log on (you can notify the user by email that they are required to make the change). Operators can be forced to use complex passwords by enabling Secure Mode.

3. If an Operator has not received a PIN (required when logging into the Cloud Console* for the first time), you can send it from here. Click **Send PIN**/**Resend PIN** (these options will only appear if the Cloud Console is enabled and the Operator role has access to the cloud).

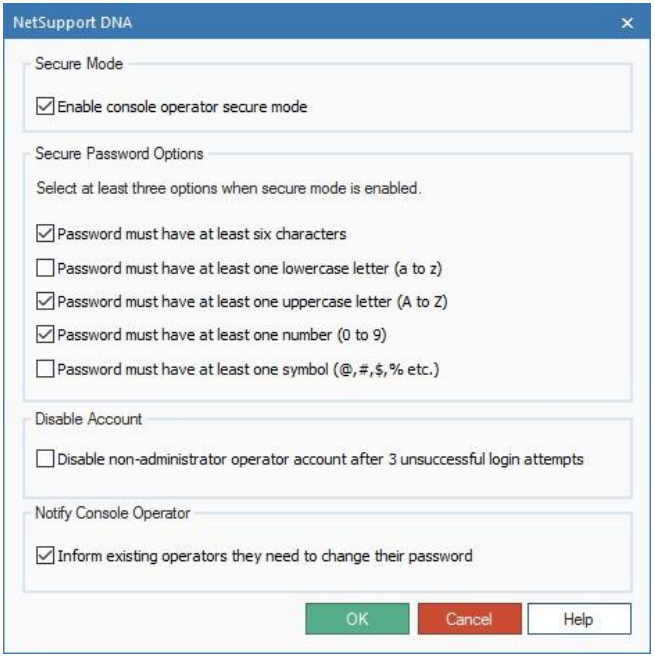
4. You can assign full administrator rights (the remaining fields will not be available) or choose the level of access by selecting **Operator**. Select the Role to be assigned to the Operator, to create a new Role, click **Roles**.
5. Click **OK** when you are finished. You will be prompted to register a password for the new user.

* The Cloud Console is only available in the Education Edition of NetSupport DNA.

Secure Mode

Secure Mode forces Console Operators to use complex passwords increasing the security of the DNA Console. When this option is enabled, the logged on Administrator must change their password immediately and other users the next time they log into the Console.

1. In the Settings tab, select the **Operators** icon.
2. From the Console Operator dialog, click **Options**.
3. The Secure Mode dialog will appear.



Secure Mode
Enable Secure Mode for all Console Operators.

Secure Password Options
Select which options to include when creating complex passwords. At least three options must be chosen.

Disable Account
This option will disable non-administrator accounts if the password has been unsuccessfully entered three times.

Notify Console Operator
Console Operators will be notified by email that they need to change to a secure password the next time they log in.

Note: The email settings must be configured before email notifications can be sent.

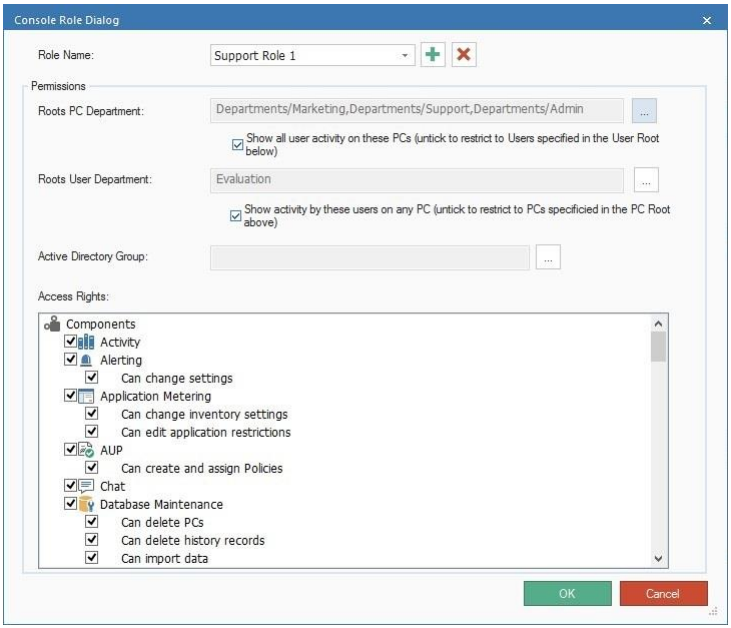
Create or Edit Console Roles

This dialog is used to create new and edit existing roles. A role allows you to define the access rights to be assigned to Operators. Once a role has been created, it can be easily assigned to multiple Operators.

Note: Administrators will automatically have full access and be assigned the Admin role.

1. From the Operators dialog, click **Roles**. The Console Roles dialog will appear.
2. Click  to create a new role. Enter the name for the role and choose between **Read-only Operator** and **Administrator Operator**. You can take a copy of an existing role, select **Copy of Role** and then choose the role to copy from the drop-down list.

   Note: By default, a Read-only Operator will have the admin access rights deselected and the Administrator Operator will have all the access rights selected.



3. To allow greater control over Operator roles and what areas Operators have access to, you can select the levels of the Tree view that the Operator can see and work with when they log on (department or Active Directory container) by clicking . This can be set for the PCs Tree and the Users Tree. By default, you will be able to see all user activity on PCs and all activity by users on any PC for your root departments. For example, if you have the Support department selected in your Roots PC department and a user not from that department logs into a Support PC, you will be able to see that activity. Clear the relevant check box to restrict access to PCs and users in the root department.
4. If the configuration settings have been set to Active Directory containers, this will set the level which the Operator can access.
5. An Active Directory Windows Group can be assigned to the role by clicking . If the user is a member of the Active Directory Group, they will be pre-authenticated to access the Console without needing to login.

   Note: If the user is taken out of the Active Directory Group, they can still access the Console by logging in with their user name and password. You can force Active Directory authentication in the NetSupport DNA Database Wizard. The user will not be able to access the Console unless they are authenticated in Active Directory.

6. Select the required access rights.
7. To remove a Role, select the required Role and click .
8. Click **OK** when you are finished, the Role can now be assigned to an Operator.

Note: In the Education Edition of NetSupport DNA, two safeguarding roles will be available. These relate to the eSafety feature. The safeguarding roles can only be assigned when you are adding eSafety contacts. See Safeguarding Roles for further information.

Discovery and Deploy

The NetSupport DNA Agent Discovery and Deploy utility provides network administrators with the facility to install the NetSupport DNA Agent on multiple computers without the need to visit the machines individually.

Within the NetSupport DNA Agent Discovery and Deploy utility, you have the ability to deploy the NetSupport DNA Agent using an IP address range, the existing Windows network or Active Directory. All of these methods allow you to pick and choose which computers you want to deploy to.

Note: NetSupport DNA provides an Automatic Agent Discovery tool, allowing you to automatically find machines that do not already have a NetSupport DNA Agent installed.

The NetSupport DNA Agent Discovery and Deploy utility can be used to deploy the NetSupport DNA Agent to computers running the following operating systems:

- Windows XP
- Windows 2003
- Windows Vista
- Windows Server 2008/2008r2
- Windows 7
- Windows 8/8.1
- Windows Server 2012
- Windows 10

Note: Due to operating system limitations, the NetSupport DNA Discovery and Deploy utility does not work with Windows XP Home, Windows Vista Home Premium or Windows 7 Starter/Home edition.

How does NetSupport DNA Deploy work?
Once the Deploy options have been configured, the NetSupport DNA Agent Discovery and Deploy utility works by connecting to the target computer using File and Print Sharing.

This method requires access to the target computer's Admin$ share and will need to connect as a user with local administrator access (user details may be requested).

Once authenticated, the NetSupport DNA Agent package files are copied to the following folder on the remote PC using the connection to the Admin$ share:

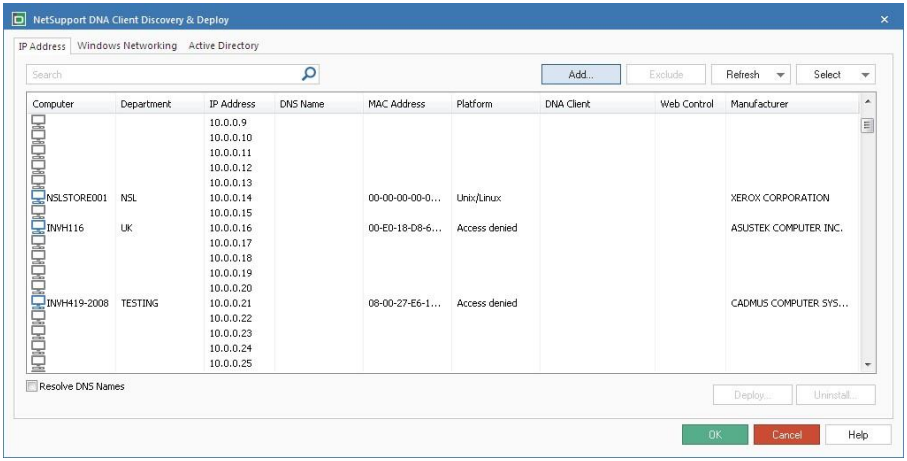
C:\Windows\pcirdist.tmp\

Finally, once the files have been sent to the target PC, the Agent installer file is executed using the Remote Procedure Calls (RPC) Service.

What are the requirements?
In order to successfully deploy the NetSupport DNA Agent component to your target PCs, the following items are required:

- File and Print Sharing must be enabled on the target PC.
- The Sharing and Security for local accounts policy must be set to {Classic} on the target PC.
- The user account used to connect to the target PC must have local administrator permissions on the target PC.
- Network discovery must be enabled on Windows Vista/7 target PCs.
- UAC Remote Restrictions must be disabled for target PCs running Windows Vista and Windows 7 in a workgroup environment.

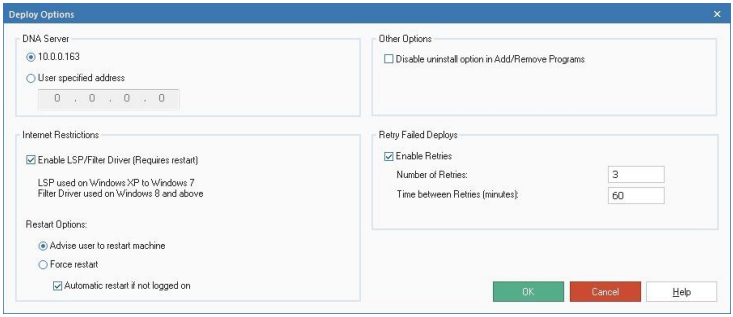
Agent Discovery and Deploy Tool



1. In the Tools tab, click the **Discovery and Deploy** icon.
2. Choose the method for finding machines: by IP address, Windows Networking or Active Directory.
3. Click **Add**.

4. If searching by IP address, enter the address range or select from a previous IP address range entry (the last ten entries are saved). Select the network groups if using Windows Networking or select the PCs to include if using Active Directory.
5. Click **OK** to find matching machines.
6. To help identify the PCs to be included or excluded from the deployment, the list can be sorted by clicking on any of the column headings. You can quickly locate a particular PC by typing in the search box.
7. If required, you can further refine the list by removing machines that you do not want to include in the deployment. For example, 'invalid' Agents or those that are identified as already having a current NetSupport DNA Agent installed. Click **Select** and choose the appropriate task from the drop-down list. Click **Exclude** to remove the highlighted items.
8. From the PCs that remain, select the ones to deploy to. To include all machines, click **Select** – **All Agents** or highlight items individually using Shift-Click, Ctrl-Click.
9. Click **Deploy** when ready.
10. As the PCs may be in use at the time of the deployment, you can send a prompt to users before you commence. Click **Options**. The Deploy Options dialog will appear.
11. Click **Start**.
12. To deploy a remote uninstall to remove the NetSupport DNA Agent, click **Uninstall**.

Deploy Options Dialog



DNA Server

Confirm the address of the NetSupport DNA Server.

Internet Restrictions

In order to make use of the internet blocking features of NetSupport DNA, it is recommended that LSP/Filter Driver is enabled.

In these circumstances, the Agent machine will need restarting in order to complete the installation. Consider if the machines are in use before making your selection.

Restart Options

Advise user to restart machine
Gives the user the opportunity to restart the PC when they want to.

Force Restart
An immediate restart is forced, without any prompting.

Automatic restart if not logged on
This option can be included along with any of the above restart options.

Other Options

Disables the uninstall option in Add/Remove Programs. This ensures the user is unable to remove the NetSupport DNA Agent.

Retry Failed Deploys

Indicate if the deployment should be automatically retried in the event of a failure. Specify the number of retry attempts and the interval between.

Click **OK** to commence the deployment.

Note: If deploying to more than 100 machines simultaneously, a warning will be displayed. There are potential overheads attached to deploying to large numbers of PCs so you may prefer to do the deployment in stages.

Deploying on Windows XP

To enable you to deploy NetSupport DNA Agent on Windows XP Professional, you need access to the Admin$ share on the remote machine in order to transfer the package to be deployed.

By default, there is no access allowed to Admin$ share.

To enable network access:

1. In Administrative Tools, select Local Security Policy.
2. Select {Security Settings}{Local Policies}{Security Options}
3. Select {Network access: Sharing and security model for local accounts}
4. Alter the setting for this policy to {Classic – local users authenticate as themselves}

The Admin$ share will now be available and you can deploy as normal.

Windows Firewall will by default block all network activity produced by NetSupport DNA. To enable NetSupport DNA to function correctly, we have provided a utility that will configure Windows Firewall.

To enable NetSupport DNA in the Windows Firewall Configuration

1. Download the ICFCONFIG.EXE File (link at www.netsupportsoftware.com/support/)
2. Run this utility on a machine with NetSupport DNA installed, using the following command

   ICFCONFIG -e DNA

3. This will create all the required entries in the Windows Firewall Configuration to allow NetSupport DNA to function correctly.

The ICFCONFIG utility can also be used to remove a NetSupport product from the Windows Firewall Configuration. See our website at www.netsupportsoftware.com/support for all the ICFCONFIG Command line options.

Deploying on Windows Vista

Due to increased security restrictions in Windows Vista, the deploy function cannot be used to deploy to Windows Vista PCs that are not part of a Domain.

When deploying to a Windows Vista PC within a Domain, the Console User must be either logged onto the Domain or enter the user credentials when prompted of a Domain Account that has Local Administrator rights to the target PC.

Note: The Deploy Prompt user option is not supported on Windows Vista.

Automatic Agent Discovery

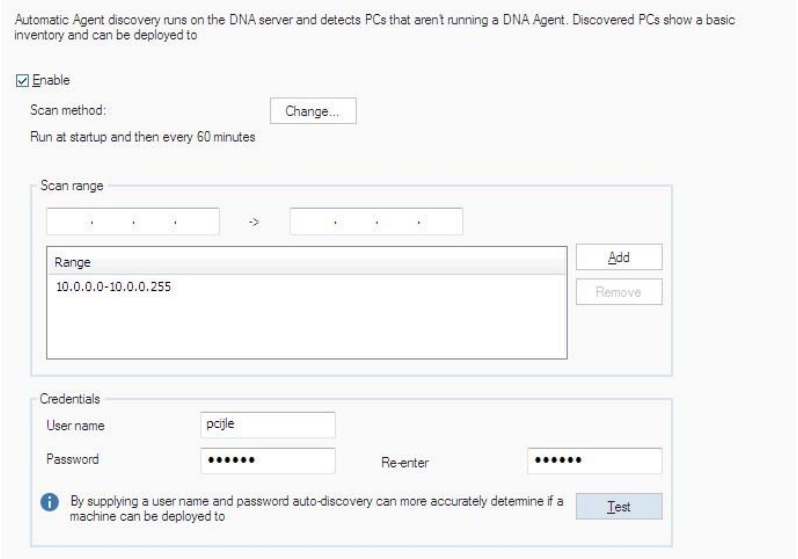
NetSupport DNA allows you to automatically discover machines across your network, even if they have not got a DNA Agent installed. Scan ranges can be created, allowing you to automatically scan as many IP address ranges as needed. Once the Agent has been located, a basic Hardware Inventory can be viewed and a DNA Agent can be deployed (to Windows machines) if required.

Setting up a scan range

1. In the Discovered Tree view, click the **Configure** icon.

   Note: If automatic discovery has not yet been enabled, a header will be displayed in the information window advising this. You can access the configuration settings here.

2. The Automatic Discovery settings will appear.



3. Select **Enable** and enter the required IP address ranges to scan.
4. Entering domain credentials allows NetSupport DNA to determine if a machine can have a DNA Agent deployed to it.
5. Click **OK**.
6. Discovered computers will be listed in the Discovered Tree view.

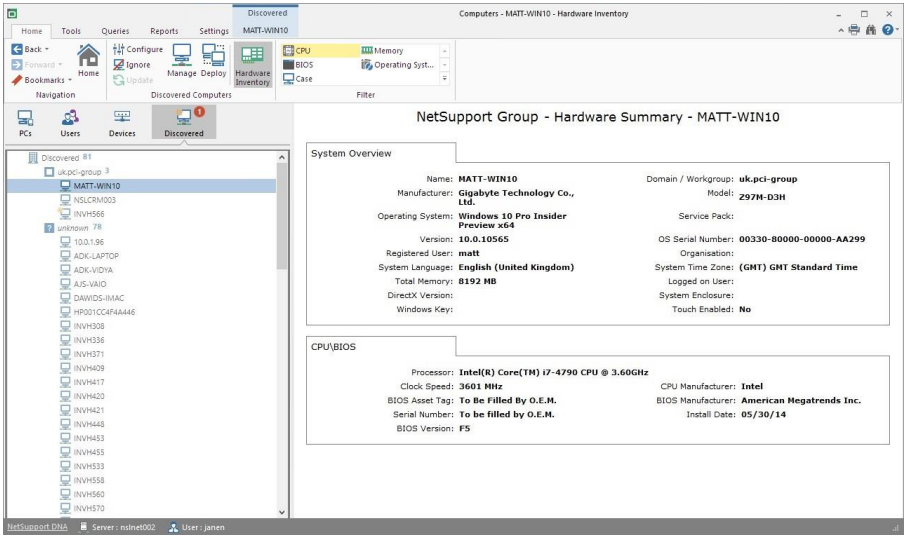
Managing discovered computers

NetSupport DNA will discover new computers on the network even if they do not currently have the NetSupport DNA Agent installed.

Newly discovered computers, irrespective of type, will be listed in the Discovered Tree view. However, where NetSupport DNA cannot determine what type of computer it is, they will be listed separately in the 'Unknown' list and the operator can manually update the properties as required.

If domain credentials have been supplied when searching for new computers, NetSupport DNA will provide a basic hardware inventory prior to the appropriate NetSupport DNA Agent being installed.

By default, when NetSupport DNA discovers a new computer, a popup will appear notifying you of this. This can be disabled in the Console Preferences - General options.

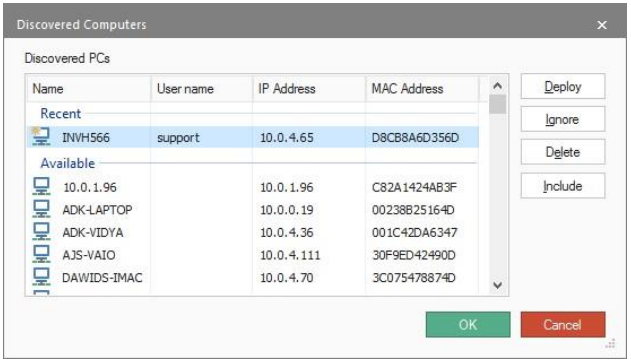


From the Discovered list, you can choose to deploy the NetSupport DNA Agent to the required computers.

Note: The NetSupport DNA Agent can only be deployed to Windows machines.

Computers that you don't wish to deploy an Agent to can be ignored and will be removed from the list. They will still be displayed in the Discovered Computers dialog. From here, you will be able to make them available again in the Discovered Tree view, if required.

1. In the Discovered Tree view, click the **Manage** icon.
2. The Discovered Computers dialog will appear.



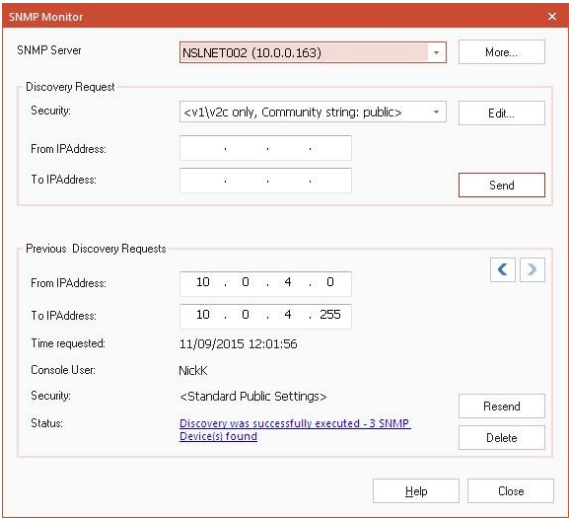
3. All discovered computers will be listed.
4. Any computers that have been ignored can be included again in the Discovered Tree view.

Device Discovery

The SNMP Discovery allows NetSupport DNA to be configured to scan a range of network addresses and report on any appropriate devices discovered, such as printers and access points. These items can then be stored within DNA and real-time data (such as ink or toner levels) can be monitored from the console.

Note: You must ensure that SNMP is enabled on the device for NetSupport DNA to be able to discover it.

1. In the Devices Tree view, click **Device Discovery**.
2. The SNMP Monitor dialog will appear.



3. Select the required NetSupport DNA SNMP Server to use from the drop-down list. Click **More** to see the Server details and any Devices that have been discovered by the Server.
4. Enter the IP address range that you wish to scan Devices on and set the level of security to use. By default, the standard level of security will use a 'public' community string and will not scan for SNMP v3 Devices. To create a new set of security settings, click **Edit**.
5. Click **Send to discover Devices**.

Note: Depending on the IP address range entered, this could take some time to return discovered Devices.

6. The status of the discovery request will be displayed. You can scroll through previous requests using the  icons.

Note: Clicking on the status will display a dialog showing the discovery results.

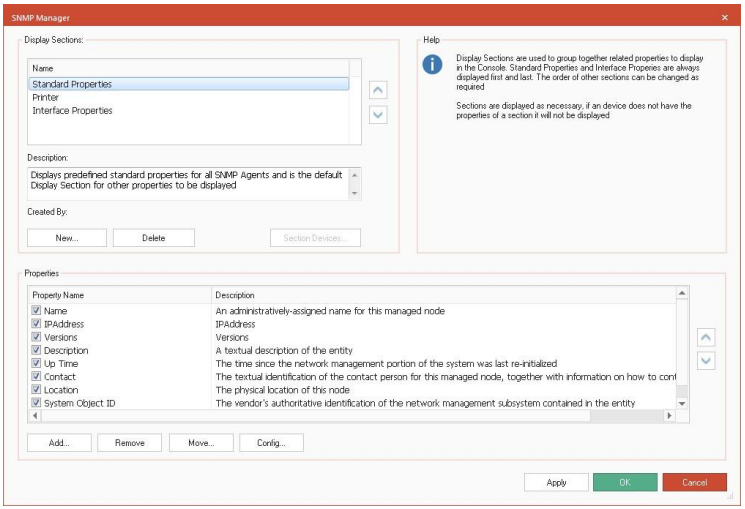
7. The scan request can be resent if required, click **Resend**.

Display Sections

In the NetSupport DNA Console, related SNMP properties are grouped together into display sections. This dialog allows you to manage and create display sections and the properties within these.

By default, there are three sections: Standard Properties, Printer and Interface Properties.

Note: The Console will only show a section if the Device returns any properties from it.



To create a new display section, select **New** and enter a name and description for the new section.

You can see which Devices are returning properties for a section. Select the required section and click **Section Devices**.

The properties in each section will be listed. To change the order that they are displayed in, click the  icons. To edit the property configuration, click **Config**. The property status summary will be displayed. To edit a property, select the required property and click **Edit**.

Properties can be moved from one section to another. Select the required property, click **Move** and select the section to move the property to.

Note: You are unable to move pre-set properties from the Standard or Interface Properties sections.

To add new properties, click **Add**.

Note: For information about OID properties, please visit our Knowledge Base and refer to product article **NetSupport DNA SNMP support**.

Integration with Active Directory

NetSupport DNA integrates with Active Directory, enabling you to configure the PCs and users within the NetSupport DNA Console to mirror their relative position within the Active Directory container structure. Changes made within the AD structure are automatically reflected within NetSupport DNA. User information can also be retrieved from Active Directory.

NetSupport supplies a ready-made administrative template, **NetSupportDNA.ADM**, containing the configurable options. When you install NetSupport DNA, the template is copied to the NetSupport DNA program folder. In turn, you will need to copy this to the folder containing any existing ADM templates.

The NetSupportDNA.ADM template allows you to configure the following policy settings for NetSupport DNA: port connection parameters, NetSupport DNA Server address properties and NetSupport DNA user data binding.

NetSupport DNA provides the ability for users to automatically logon to the NetSupport DNA Console without the need to sign in, based on their membership of a Windows group. When creating a Console Role, you can assign an Active Directory Windows group to the Role, enabling the user to be authenticated based on their membership.

Note: The NetSupport DNA Agent can be deployed using Active Directory. See Installing via Active Directory for further information.

Active Directory Tree view

By default, NetSupport DNA displays the standard departmental Tree view. If you are working with Active Directory, it may be useful to have PCs and users displayed in the same Tree structure.

Note: The Active Directory containers folder will be displayed by default in the Tree. This can be hidden if required.

1. Click the **General** icon in the Settings tab.
2. The DNA Configuration dialog will appear, select the Active Directory settings option.
3. Select **Layout PCs in their AD Containers rather than departments where applicable**.

4. Agents will be moved to the relevant AD container to reflect their position in the structure.

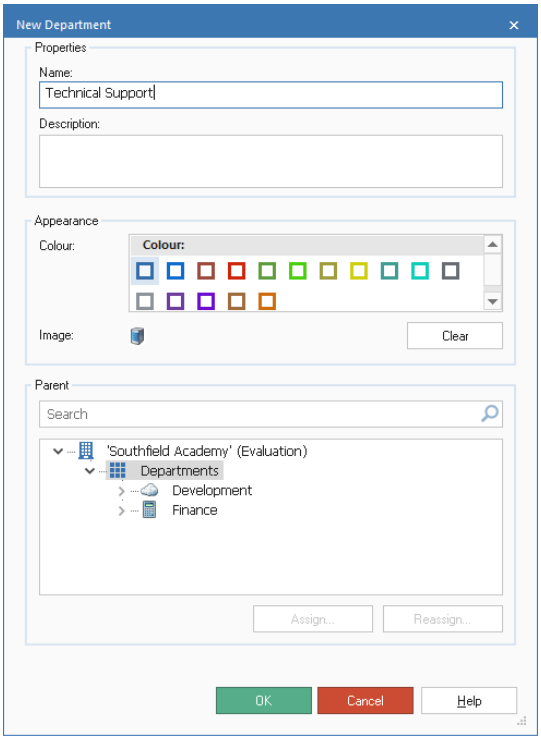
Note: When Agents are moved to their Active Directory Containers, any previous department settings may not apply to the Active Directory container. Please review the component and Agent settings to ensure you have the correct settings applied.

For further information on how to configure Active Directory policies, refer to www.netsupportsoftware.com/support/.

Create a department

The Tree view is highly configurable, enabling you to customise your NetSupport DNA setup to mirror your organisation's structure. Your own custom images can be applied to further highlight the department in the Tree view. Departments can be manually added and Agents moved between departments as required.

1. In the Tree view, select Departments or an existing department name.
2. Right-click and select **New department**.
3. The New department dialog will appear.



4. Enter the department name and a suitable description.
5. The appearance of the department in the Tree view can be customised. A colour can be applied to the department and a custom image can be assigned to it. Click  to browse for the required image.

6. Decide at which level of the Tree view to insert the department by selecting the parent. To search for a parent department, enter the name or partial name of the department and click . The first matching item in the Tree view will be displayed along with the number of matches found. You can scroll through these using the arrows. Click  to clear the search.
7. Click **OK**.

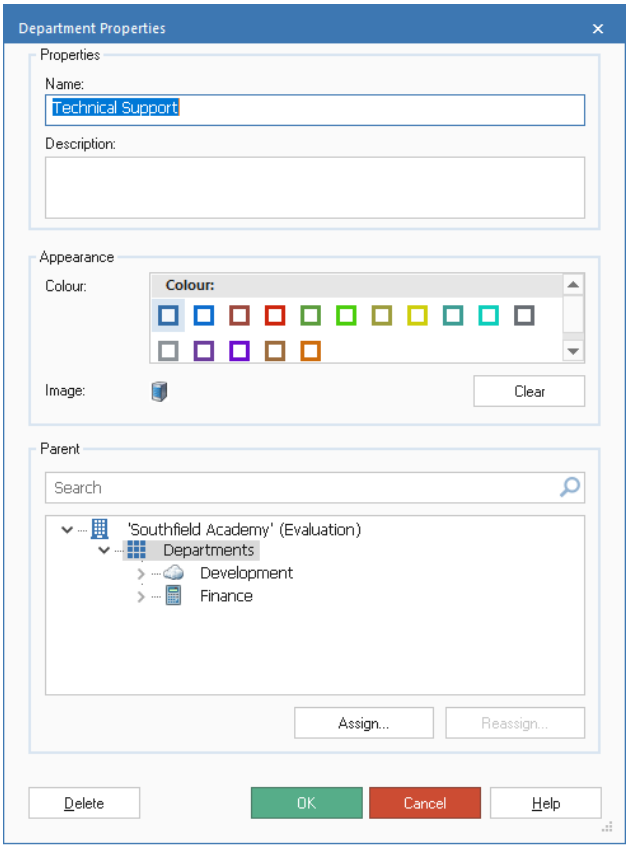
Note: The **Assign**/**Reassign** options are only active when editing the properties of an existing department.

Change the Properties of a department

This dialog can be used to:

- Change the general properties of a department.
- Change the appearance of the department in the Tree.
- Associate a department with a new parent in the Tree.
- Delete a department.
- Move Agent PCs between departments.

1. Select the required department in the Tree view.
2. Right-click and select **Properties**.



Properties

The department name and description can be changed if required.

Appearance
The colour assigned to the department can be changed and, if a custom image has been added, this can be edited (click on the image and select a new one) or deleted (click **Clear**). If there is no image, one can be added by clicking .

Parent
The department can be moved within the Tree view by clicking on a new Parent. To search for a parent department, enter the name or partial name of the department and click . The first matching item in the Tree view will be displayed along with the number of matches found. You can scroll through these using the arrows. Click  to clear the search.

Assign
Enables you to add Agents to the current department.

Reassign
Allows you to move Agents from the current department.

Note: Only Administrators are able to create departments or move PCs between departments.

Delete
The selected department can be deleted from the Tree view as long as there are no Agents currently associated with it.

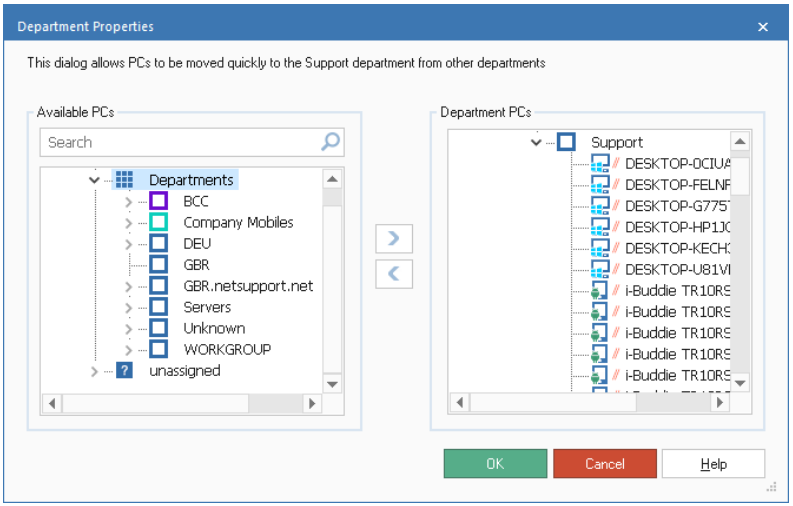
Adding Agents to departments

When a NetSupport DNA Agent is installed, it is dynamically added to the appropriate domain in the Console Tree view. However, Console Operators can customise the Tree view to include additional departments and move Agents between these areas.

An individual Agent can be moved by simply dragging and dropping the required PC between departments in the Tree view. Alternatively, the User Details can be edited. Right-click on the required Agent in the Tree view, select **Edit Details** and update the department field.

Multiple Agents can be easily moved using the **Assign/Reassign** facility.

1. In the Tree view, right-click on the required department. The one you are moving Agents to or from.
2. Select **Properties**. The current properties for the selected department will be displayed.
3. Click **Assign** or **Reassign** depending on whether you are moving Agent PCs to or from the department.



4. From the Available PCs list, select the PC to move and click . Repeat for any additional PCs that you wish to move.

Note: To search for an item in the Tree view, enter the name or partial name of the PC in the search box and click . The first matching item in the Tree view will be displayed along with the number of matches found. You can scroll through these using the arrows. Click  to clear the search.

5. If you have moved the Agent PC in error, click  to reassign it to the original department.
6. Click **OK** when finished.

Dynamic Groups

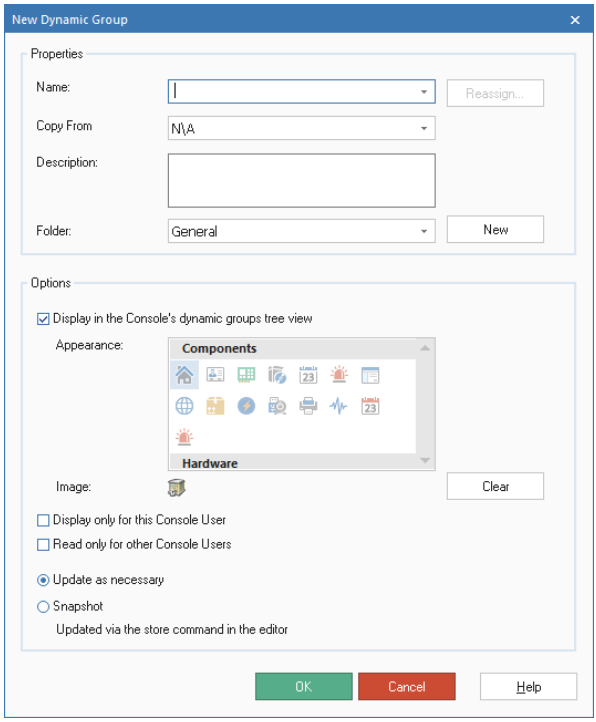
This facility provides a quick and easy method for grouping Agents based on specific conditions. Typical uses could be to identify users that are running out-of-date hardware or software.

NetSupport DNA provides a selection of predefined efficiency and general dynamic groups. Dynamic groups relating to Efficiency view are stored in an Efficiency folder and all others are stored in a General folder in the Tree view. New folders can be created by right-clicking on Dynamic Groups and selecting **New folder** – or when creating a new dynamic group. Enter the required name and click **OK**.

Note: The Tree view can be filtered to only show PCs/Users/Devices that match a dynamic group query. Select the required dynamic group in the Tree, right-click and select **Apply as Filter**. A filter bar will be displayed at the top of the Tree view showing what dynamic group filter has been applied. To remove the filter, click **Clear**.

To create a new dynamic group

1. In the Tree view, right-click on Dynamic Groups and select **New Dynamic Group**.
2. The New Dynamic Group dialog will appear.



3. Enter a name and description for the new group.
4. You can copy an existing dynamic group (the conditions from the original will be applied to the new dynamic group). Select the required dynamic group from the **Copy From** drop-down list.
5. Select the folder the dynamic group is to be located in from the **Folder** drop-down list. To create a new folder, click **New**, enter a name for the group and click **OK**.
6. Select any applicable options:

   Display in the Console's dynamic groups tree view

   If this is to be a one-off search for a particular group of PCs, you can choose not to add the group to the Tree view.

   Appearance

   If the new group is being displayed in the Tree view, select the required icon that will be associated with it. A selection of images is provided. Alternatively, you can use a custom image.

Image
To assign your own custom image to the new group, click  and browse for the required image.

Display only for this Console User
Select this option if you want the new group only to be visible to this Console User.

Read only for other Console Users
If you want other Console Users to be able to view the new group, but not alter it, you can make the group read-only.

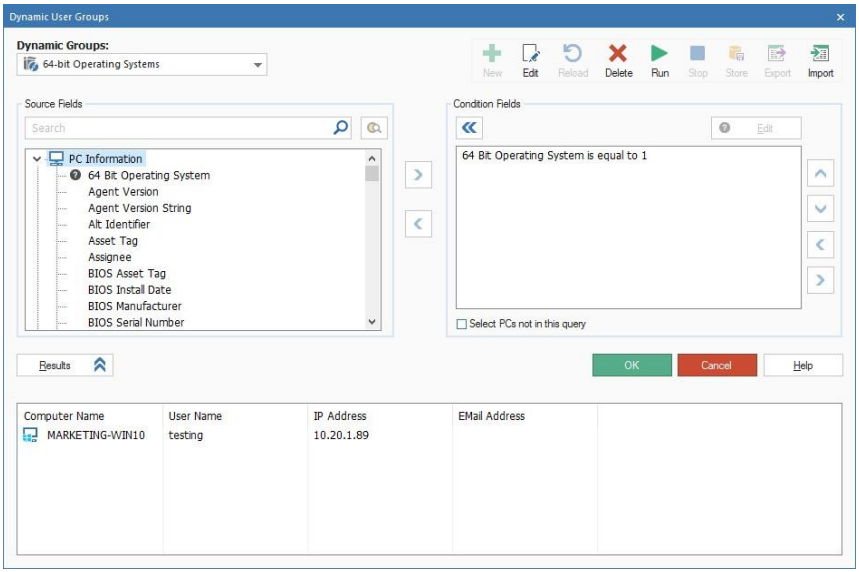
Update as necessary
Enable this option if you want any new Agent PCs that match the criteria to be automatically added to the group.

Snapshot (Updated via the store command in the editor)
Rather than automatically add new PCs to the group, you can take a snapshot at a given time. You can then update the Agent list as and when required using the **Store** option in the Dynamic User Groups editor.

7. To assign the group to a different Console User, click **Reassign**. This is only available when you are editing the properties of an existing dynamic group.
8. Click **OK**. The Dynamic User Groups editor dialog will appear, enabling you to create the conditions that will determine which Agents are selected for the group.

Dynamic Groups Editor

The Dynamic Group Editor dialog is primarily used to create the condition that determines which Agents are included in a Dynamic Group. You can edit the properties of an existing group, create new groups, run the output from here and import and export dynamic groups.



1. The dialog can be launched when creating a new group or editing an existing item.
   Or
   Right-click on the Dynamic Group name in the Tree view and select **Properties**.
2. The dialog will indicate which group is loaded. You can select another group from the drop-down list.

   The following options are available:

   New
   Create a new Dynamic Group.

   Edit
   Change the properties of an existing Dynamic Group.

Reload
Reloads the stored version of the group's properties, if you want to ignore any changes you have made. The option is not available once the results have been run.

Delete
Delete the currently loaded Dynamic Group.

Run
Run the results of the currently-loaded group. Items matching the specified condition will be listed in the Results window. You can hide/un-hide the output by clicking the **Results** button.

Stop
Cancel running the results.

Store
If, when entering the general properties for the group, you elected to create a snapshot (meaning that any new Agents matching the criteria are not automatically added to the group) clicking **Store** will update the Agent list.

Export
Exports the dynamic group to an .XML file.

Note: You can only export user-defined dynamic groups.

Import
Allows you to import a dynamic group.

Note: You cannot import dynamic groups that have been exported using Database Maintenance.

Specifying the condition fields

1. From the Source Fields Tree, select the field(s) on which to base the condition. Click  to move each item in turn to the Condition Fields window. You can view the current values for the field by clicking .
2. The Condition Editor will appear. Multiple conditions can be applied. Click **OK**.
3. Click **Run** to retrieve the results. The Dynamic Group will be listed in the Console Tree view along with those Agents matching the condition.

Note: There may be occasions when you quickly want to view PCs that do not meet the specified condition. In the above example, the condition highlights Agents that have 64-bit operating systems but, when planning major rollouts, you might equally want to reverse that and display those that don't have this operating system. Check **Select PCs not in this query** to enable this option and click **Run** to display the results.

NetSupport DNA Configuration

Profiles

To provide maximum flexibility, NetSupport DNA allows you to create multiple profiles for different groups of devices or users, each with its specific component settings. The profile can be assigned at user, Active Directory group, PC and department level. A default profile is provided that applies to all Agents that do not already have a profile assigned to them. This profile cannot be removed, but the settings can be changed.

Notes:

- Profiles assigned at user level will override a profile that has been applied at any other level.
- You can see which profile Agents have assigned to them in Explorer mode, details view and also when an Agent is selected in the Tree view in the PC or User tab that appears.
- Console Preferences can be accessed from the **General** icon in the Settings tab.
- If you are upgrading from version 4.40, any previous department settings will be imported and a profile containing these will be created.

Create a new profile

1. In the Settings tab, click the **Create new profile** icon.
2. The Add Profile dialog will appear.

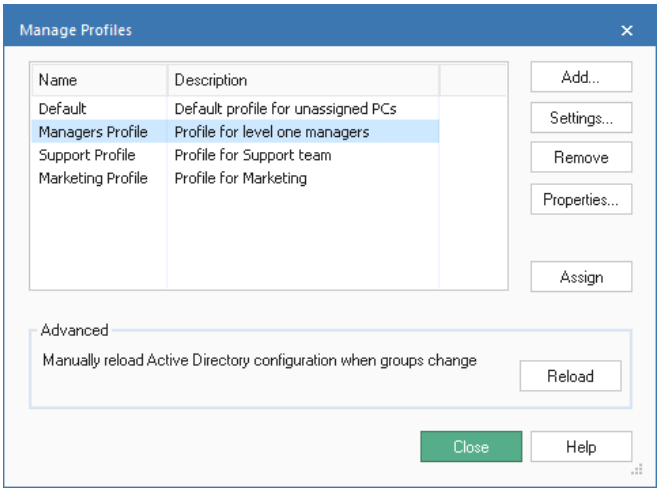


3. Enter the name and description for the profile. You can copy an existing profile by selecting the relevant one from the drop-down list.
4. Click **OK**.
5. The Settings dialog will appear. Configure the required component settings and click **Save**.
6. The Profile Assignment dialog will appear.

7. The profile can be assigned to users, an Active Directory group, PCs and departments. Click **Assign** next to the relevant area and a Tree will appear, allowing you to select who to assign the profile to.
8. The new profile will be listed in the Manage Profiles dialog.
9. Click **Close**.

Manage existing profiles

1. In the Settings tab, click the **Manage existing profiles** icon.
2. The Manage Profiles dialog will appear, listing existing profiles. Select the profile you want to manage.



3. To change the properties of a profile, click **Properties** and make the required changes to the name and description.
4. To amend the settings for a profile, click **Settings**.
5. To change who the profile is assigned to, click **Assign**.
6. Click **Reload** to manually reload the Active Directory configuration when groups have changed.
7. To remove a profile, click **Remove**.

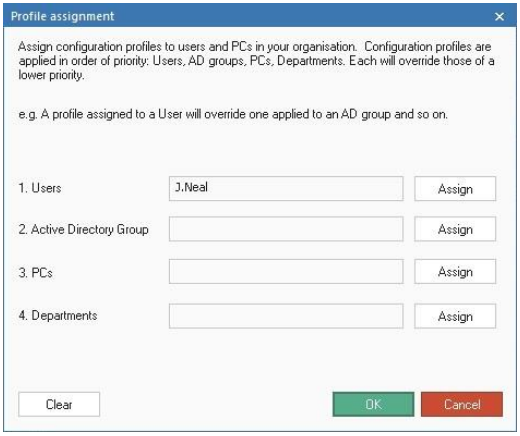
Note: A profile can only be deleted if there is nothing assigned to it. To clear the assignments for a profile, click **Assign** and then **Clear**.

Assigning Profiles

This dialog allows you to assign a profile to the required users and PCs in your organisation. The following hierarchy is used when assigning profiles:

Users	The profile is assigned to a Windows logged on user.
Active Directory Group	The profile is assigned to users contained within Active Directory Groups. When assigning a profile to an Active Directory Group, it will only be applied to users who are a member of that Active Directory Group and not: contacts, services accounts, computers, distribution groups or other objects. Profiles will not be applied to members of groups who have that group as their Primary Group.
PCs	The profile is assigned to a PC.
Departments	The profile is assigned to a department and the PCs within that department will inherit this profile.

Note: Users that have not been assigned a profile at user or Activity Directory level will inherit the profile of the department they belong to (if a profile has been assigned to the department).



Click **Assign** next to the relevant area and a Tree will appear, allowing you to select who to assign the profile to.

To clear all assignments for the profile, click **Clear**.

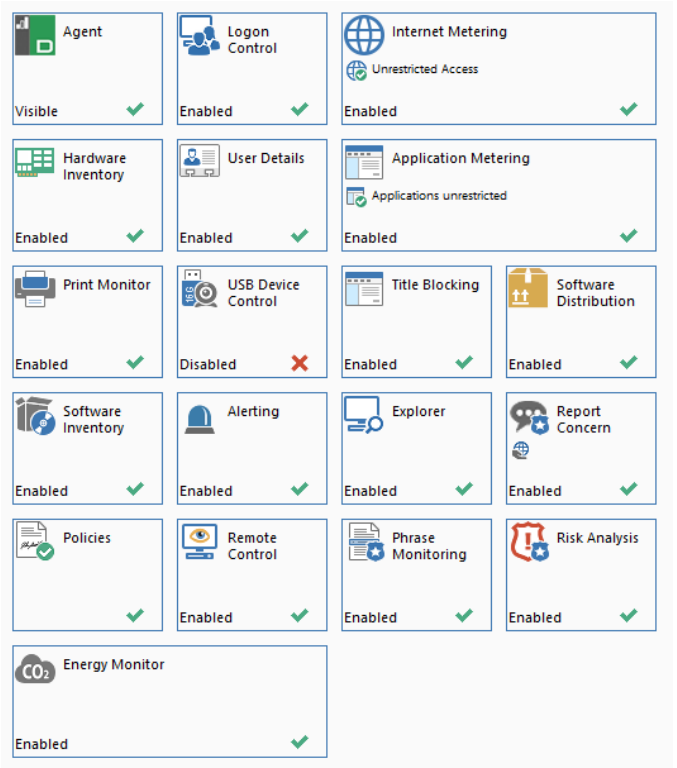
Configure Component Settings

The NetSupport DNA Configurator allows Administrators/Console Operators to apply specific settings (which can be assigned at user, Active Directory group, PC or department level), to each of NetSupport DNA's primary features. For example, the frequency at which Inventory data is collected can be set at an individual department level or you may want to block specific users from accessing certain websites.

The NetSupport DNA Configuration settings are accessed when creating or managing profiles.

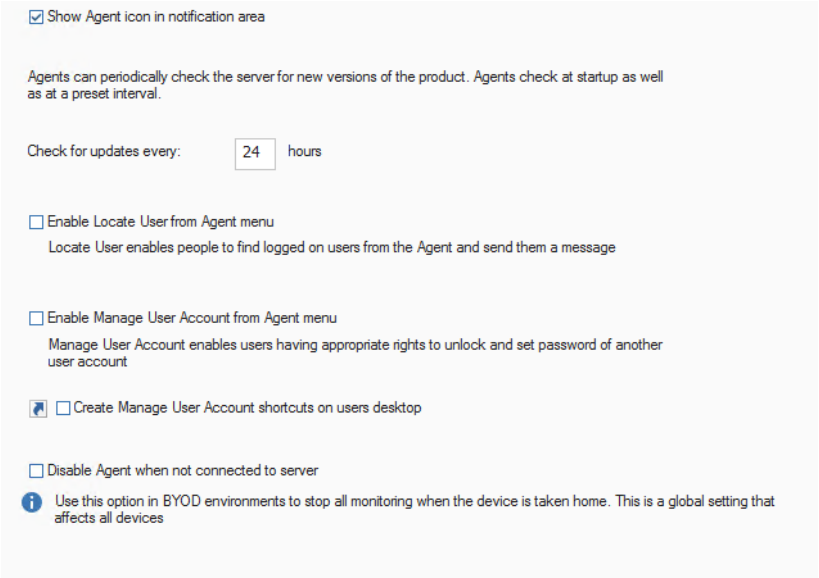
Notes:

- Console Preferences can be accessed from the **General** icon in the Settings tab.
- SNMP component settings are available from the Devices Tree view; select the Settings tab and click **General**.



An overview of the settings for each component will be displayed, allowing you to see which components are currently enabled. A yellow indicator will be displayed when changes have been made but not saved. Clicking on an icon will take you to the settings for that area. Click **Save** to save any changes. You will be asked how you want these settings to apply to the department. To revert to the default settings, click **Reset**.

Agent



Show Agent icon in notification area
When enabled, the Agent icon will appear in the taskbar at the Agent PC.

Check for updates every *xx* hours
Each time a NetSupport DNA Agent service starts, it will automatically check the server for updated components. While Agents are active, you can also set the frequency at which they continue to poll the server. For example, if you have a large network, you might want to reduce the number of instances where Agents check for updates to one or two times a day. Alternatively, when updates are available, you may need Agents to check more regularly.

Enable Locate User from Agent menu
Allows Agents to search for and locate other logged on users and send them a message.

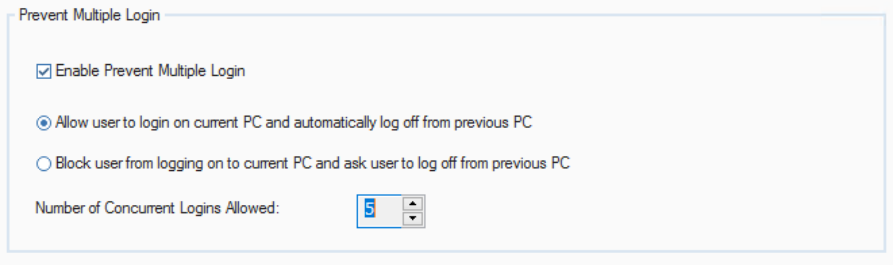
Enable Manage User Account from Agent menu
Agents will be able to access the Manage User Account feature from the Agent menu. From here, they can unlock and set passwords of another user account (if they have appropriate rights).

> **Create Manage User Account shortcuts on users' desktops**
> A shortcut to the Manage User Account feature will be created on users' desktops.

Disable Agent when not connected to server
When the Agent cannot connect to the DNA Server or Agent Gateway, it will be disabled and no monitoring data will be collected. This may be useful if you do not want monitoring data collected from the Agent if the device is taken home.

Notes:
- This is a global setting that applies to all devices.
- This option is not supported on Terminal Services.

Logon Control

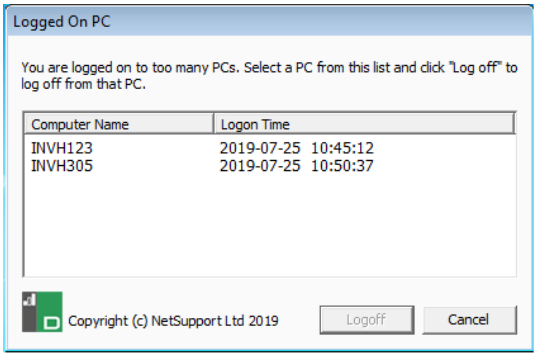


Prevent Multiple Login
There may be occasions when a user needs to be logged into more than one PC at the same time. NetSupport DNA allows you the flexibility to set the number of concurrent logins allowed for a single user up to a maximum of 5 machines.

Note: This feature is only supported for domain Windows accounts and it will not be available for Terminal services/RDP sessions.

Enable Prevent Multiple Login
When enabled, you can choose how multiple concurrent logins are handled:

Allow user to login on current PC and automatically log off from previous PC
If the user attempts to exceed the specified number of concurrent PC logins, they will be prompted to select one of the other PCs to log off. If a number more than 1 hasn't been specified, the second login will be allowed but the first PC will be automatically logged off.



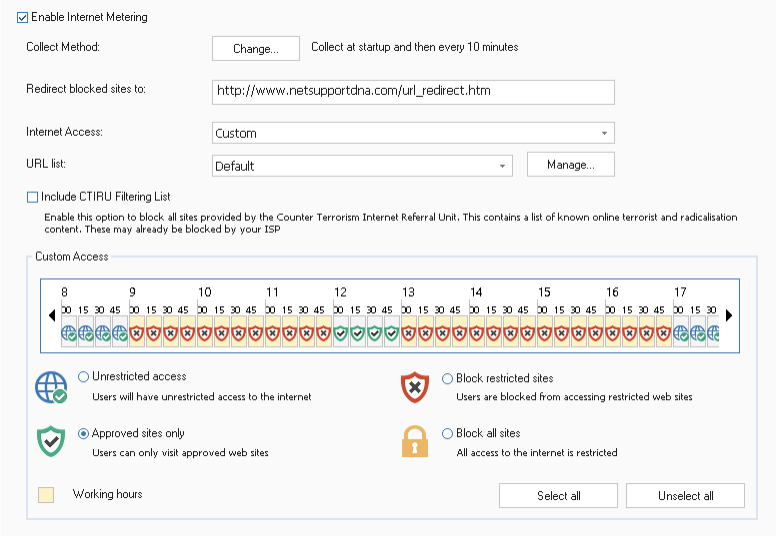
Note: The user will be logged out of the chosen PC even if the machine is locked and any unsaved work will be lost.

Block user from logging on to current PC and ask to log off from previous PC
In this scenario, if the user attempts to exceed the specified number of concurrent PC logins, they will need to manually log off one of the other PCs before continuing.

Number of Concurrent Logins Allowed
You can set this to a maximum of 5 concurrent network logins for a single user. If a person attempts to login, with the same credentials, to one more machine than the specified limit a warning, as above, will appear.

Internet Metering

Internet Metering enables Operators to monitor and restrict Agents' internet usage. You can switch metering on or off and restrict access to designated sites.



Enable Internet Metering
Clear this box to switch Internet Metering off.

Collect Method:
By default, Internet Metering will collect data when the NetSupport DNA Agent starts up and then every ten minutes. Click **Change** to amend the settings and set custom collect times.

Note: We recommend a more reasonable collect data time interval of 30 minutes as a guideline to balance the accuracy of data displayed against an increase in the network traffic from the DNA Agent machines.

Redirect Blocked Sites to xxxxxxx
Enter the URL you wish Agents to be redirected to if they attempt to visit a blocked site.

Internet Access
As well as monitoring internet usage, you also have the option of preventing Agents from visiting certain sites. Select the required level of access from the drop-down list: you can choose to have unrestricted access, block access all the time, restrict or block access during office hours or out of office hours. Selecting **Custom** enables you to customise the access to suit your own requirements.

URL List
A URL list (a list of approved and/or restricted websites) can be assigned to a profile. Select the required list from the drop-down menu. To create or manage lists, click **Manage**.

Note: For the list to be activated, the internet access level must be set to one of the 'restrict internet' access options, or, if using custom access, the 'approved sites' or block 'restricted sites' enabled.

Include CTIRU Filtering List
The CTIRU Filtering list is a list of known online terrorist and radicalisation websites provided by the Counter Terrorism Internet Referral Unit. This option will automatically block access to these websites (if they are not already blocked by your ISP). You will be notified that access to a restricted website has been attempted in Internet Metering (the website address will be obfuscated) and an alert will be raised.

Custom Access

Unrestricted access
Agents will be able to access any website.

Approved sites only
When enabled, Agents will only be able to visit websites included in the Approved list.

Block restricted sites
When enabled, Agents will not be able to visit websites included in the Restricted list.

Block all sites
When enabled, Agents will not be able to visit any websites.

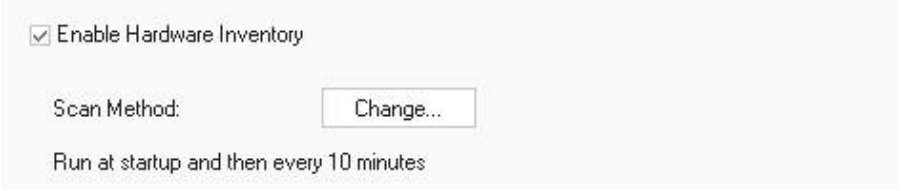
You can restrict Agents' internet access at specific times during the day. Select the required restriction and, using the arrows, scroll to the desired time frame and click on the segment to apply the relevant icon.

Note: By default, access will be unrestricted.

The current office working hours will be shaded yellow. These can be amended to suit your organisation in the Console Preferences - General settings.

Click **Select all** to apply the selected restriction across the whole day or **Unselect all** to revert back to unrestricted access.

Hardware Inventory



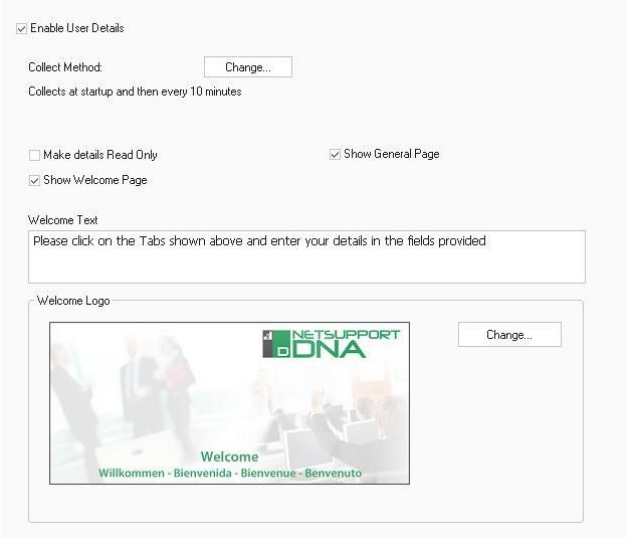
Enable Hardware Inventory
Deselect to prevent Hardware Inventory from running.

Scan Method
By default, Hardware Inventory will run when the NetSupport DNA Agent starts up and then every ten minutes. Click **Change** to amend the settings and set custom scan times.

Note: We recommend a more reasonable run time interval of 1440 minutes as a guideline to balance the accuracy of data displayed against an increase in the network traffic from the DNA Agent machines.

User Details

Agent and asset information can be updated using the User Details dialog.



The default settings for the dialog can be adjusted as follows:

Enable User Details
If this check box is cleared, the facility for Agents to access the User Details dialog is disabled at their machine. Console operators can still open the dialog at Agent machines.

Collect Method:
By default, User Details will collect data when the NetSupport DNA Agent starts up and then every ten minutes. Click **Change** to amend the settings and set custom collect times.

Make details Read Only
If checked, Agents can view the User Details but cannot enter information.

Show Welcome Page
By default, the User Details dialog contains two pages (tabs), **Welcome** and **General**. Operators can also add custom pages, if required. Un-check this box to hide the Welcome page.

Show General Page
Un-check this box to hide the General page.

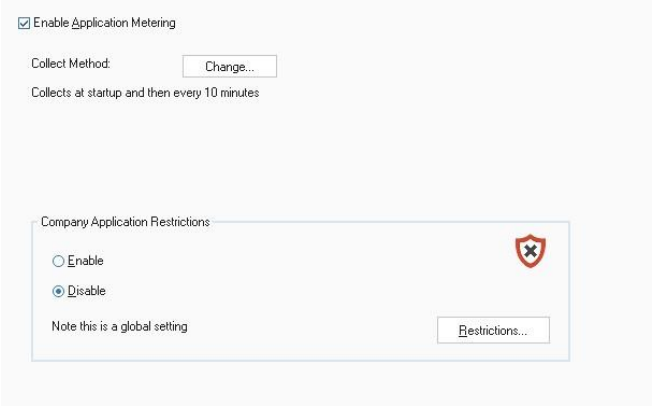
Welcome Text
If the Welcome page is displayed, you can add a customised message/prompt.

Welcome Logo
The default image that appears on the Welcome page can be replaced with a bitmap of your choosing. As the file is not remotely downloaded to Agent machines when requesting User Details, it must exist on the Agents machine in the specified folder or the Agents NetSupport DNA component folder.

Click **Change** and browse for the required file.

Application Metering

Application Metering enables Operators to monitor and restrict Agents' application usage. You can switch metering on or off and restrict access to designated applications.



Enable Application Metering
Un-check this box to switch Application Metering off.

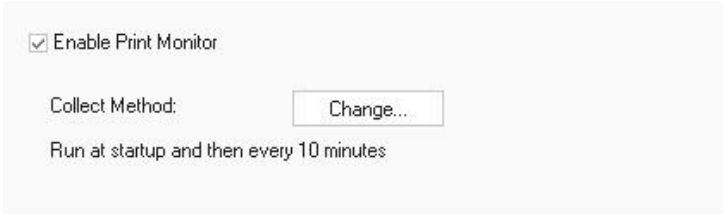
Collect Method:
By default, Application Metering will collect data when the NetSupport DNA Agent starts up and then every ten minutes. Click **Change** to amend the settings and set custom collect times.

Note: We recommend a more reasonable collect data time interval of 30 minutes as a guideline to balance the accuracy of data displayed against an increase in the network traffic from the DNA Agent machines.

Company Application Restrictions
Click **Restrictions** to create an approved and/or restricted list of applications and choose whether to enable or disable the restrictions.

Note: This setting will apply across the whole company.

Print Monitor



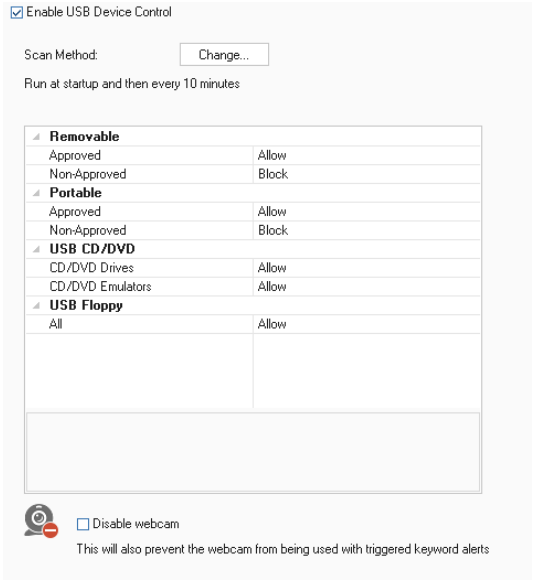
Enable Print Monitor
Clear this check box to disable Print Monitor.

Collect Method:
By default, Print Monitor will collect data when the NetSupport DNA Agent starts up and then every ten minutes. Click **Change** to amend the settings and set custom collect times.

Note: We recommend a more reasonable collect data time interval of 30 minutes as a guideline to balance the accuracy of data displayed against an increase in the network traffic from the DNA Agent machines.

USB Device Control

The use of USB devices can be controlled and, from here, you can set the state for approved and non-approved devices depending on type.



Enable USB Device Control
Select this check box to enable USB Device Control.

Scan Method
By default, USB Device Control will run when the NetSupport DNA Agent starts up and then every ten minutes. Click **Change** to amend the settings and set custom scan times.

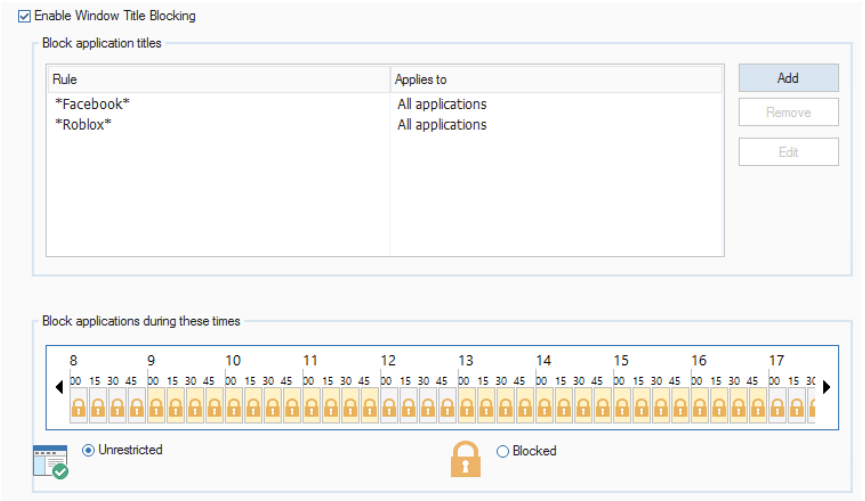
You can set the access level for the approved and non-approved devices depending on device type. The current level of access will be displayed. To change this, select the required device type and from the drop-down list choose the level of access. Access can be set to allow full access, block all access, allow read-only or prevent applications being run.

Disable webcam
Select this option to prevent users from using webcams.

Title Blocking

In addition to restricting websites and applications by their specific name, apps, websites and games can also be blocked by window title.

Rules are created, which can include a wildcard character, to indicate which page title(s) the blocking should apply to and for added flexibility, you have the option to create custom lists that include or exclude certain applications within a specified group. You can also choose the time periods when the rules apply.

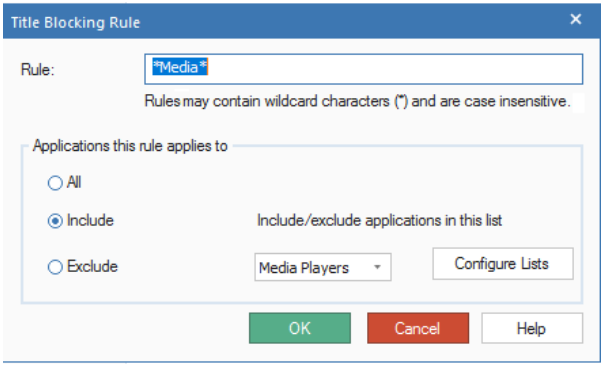


Enable Window Title Blocking
Clear this check box to turn Window title blocking off.

Note: Application Metering must be enabled for this feature to function.

Click **Add** to create a new rule (title name).

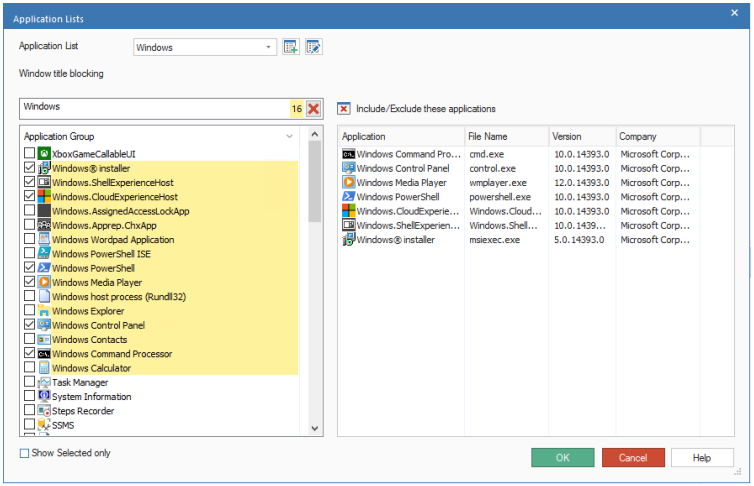
Add a Title Blocking Rule
Enter the title/rule for the application that you wish to block (case insensitive). You can include a wildcard character to ensure variations of the Window title are included.



This rule can apply to all matching applications or you can create customised lists that you can choose to include or exclude the rule from. Select **Include** or **Exclude** to activate the lists, select the required list from the drop-down menu or click **Configure Lists** to create a new list.

Configure Application lists

To create or edit a Title Blocking Application list:



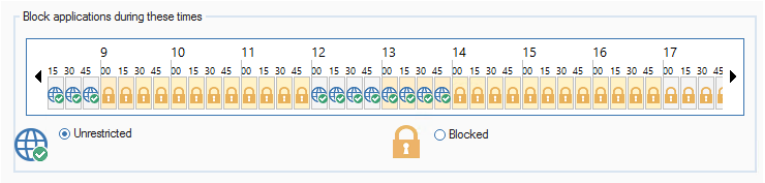
Application list

Use the **Add** or **Edit** icons to create a new list or change the properties of an existing list. Give the list a suitable name.

Window title blocking

1. Start typing the name of the application or Application Group that you want to include in the list. All matching items will be highlighted.
2. Select the required apps to confirm you want to include them in the list.
3. Click **OK** when complete. You will return to the Title Blocking Rule dialog.
4. Click **OK** to return to the Title Blocking settings dialog.

You can choose when to apply the restriction/blocking. Select the required icon (**Unrestricted** or **Blocked**) and, using the arrows, scroll to the desired time frame and click on the segment to apply.

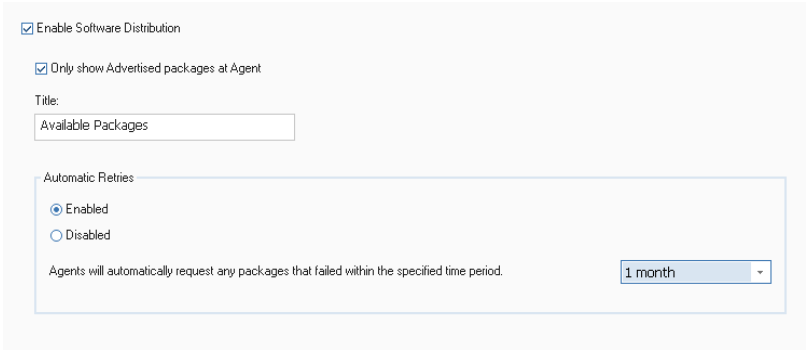


Note: By default, access will be blocked.

The current office working hours will be shaded yellow. These can be amended to suit your organisation in the Console Preferences - General settings.

Software Distribution

The Software Distribution settings primarily determine whether the Request Package facility is available at Agent machines.



Enable Software Distribution

Clear this check box to disable the Request Package facility at Agent machines.

Only show Advertised packages at Agent

The Request Package facility enables Agents to install packages that have been advertised by the Console operator. These will be listed in a dialog for the Agent to select from. Although Agents can only install advertised packages, you can display a full list of packages for the Agents to view by un-checking this box.

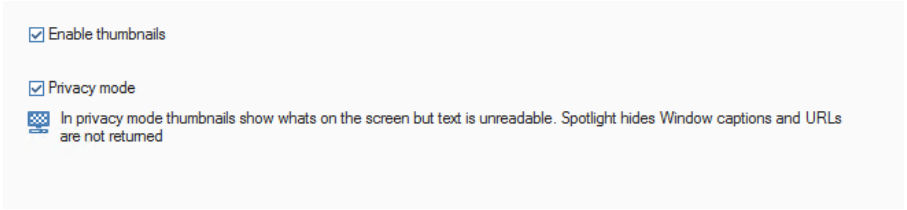
Title

You can display a customised title on the Package dialog that appears at Agent PCs.

Automatic Retries

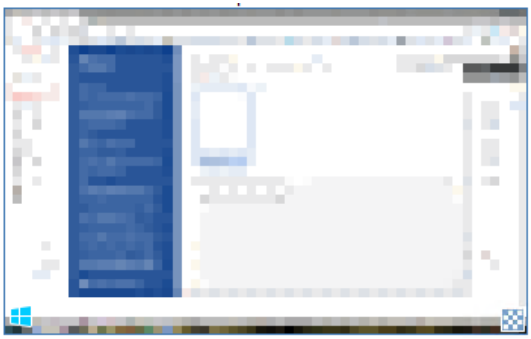
You can turn on/off the Automatic Retry option allowing you to redistribute any failed packages. The time period for failed packages to still be available for Agents to request automatically can be specified (from 1 day to 6 months). Select the required time period from the drop-down list.

Explorer



Enable thumbnails
Clear this check box to disable thumbnail view in Explorer.

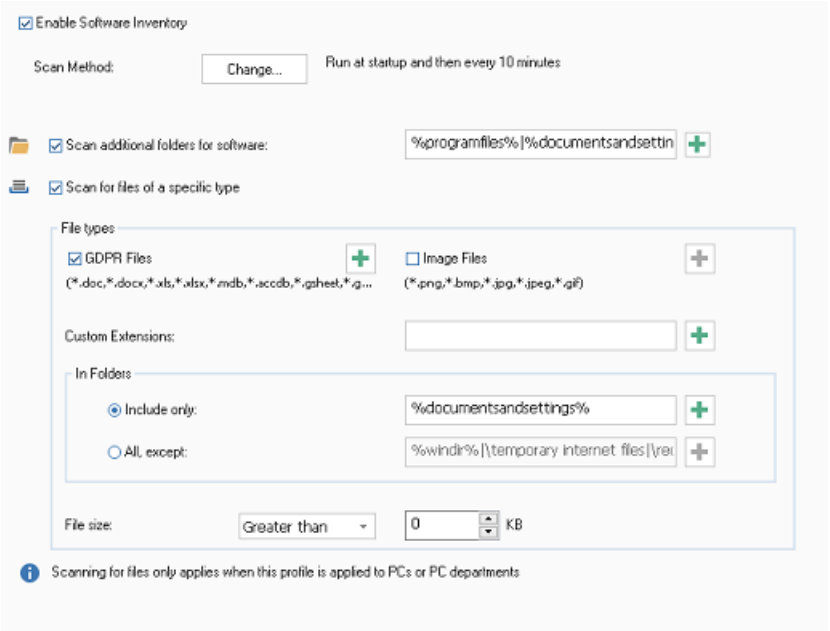
Privacy mode
If enabled, still allows you to view the Agent thumbnails, but the text will be pixelated to make it unreadable.



In addition, when viewing a selected Agent in Spotlight mode, the Window titles of any currently running applications will be masked and URLs will not be displayed.

Software Inventory

By default, the Software Inventory tool scans common locations, for example, program files, searching for the .exe files installed at each Agent PC. However, you can expand the search to include additional folders and file types.



Enable Software Inventory
Deselect to prevent Software Inventory from running.

Scan Method
By default, Software Inventory will run when the NetSupport DNA Agent starts up and then every ten minutes. Click **Change** to amend the settings and set custom scan times.

Note: We recommend a more reasonable run time interval of 1440 minutes as a guideline to balance the accuracy of data displayed against an increase in the network traffic from the DNA Agent machines.

Scan additional folders
Enables you to specify folders which may not be included by default when compiling the Software Inventory.

Scan for files of a specific type
Enables you to scan for specific types of files and allows you to specify custom extensions.

File types

GDPR Files
You can choose whether to include GDPR files in the scan, allowing you to quickly see where potential GDPR files are located. By default, .doc, .docx, .xls and .xlsx file extensions are scanned for. To include different file types, click  .

Image Files
Choose whether to include image files in the scan. By default, .png, .bmp, .jpg, .jpeg and .gif file extensions are scanned for. To include different file types, click  .

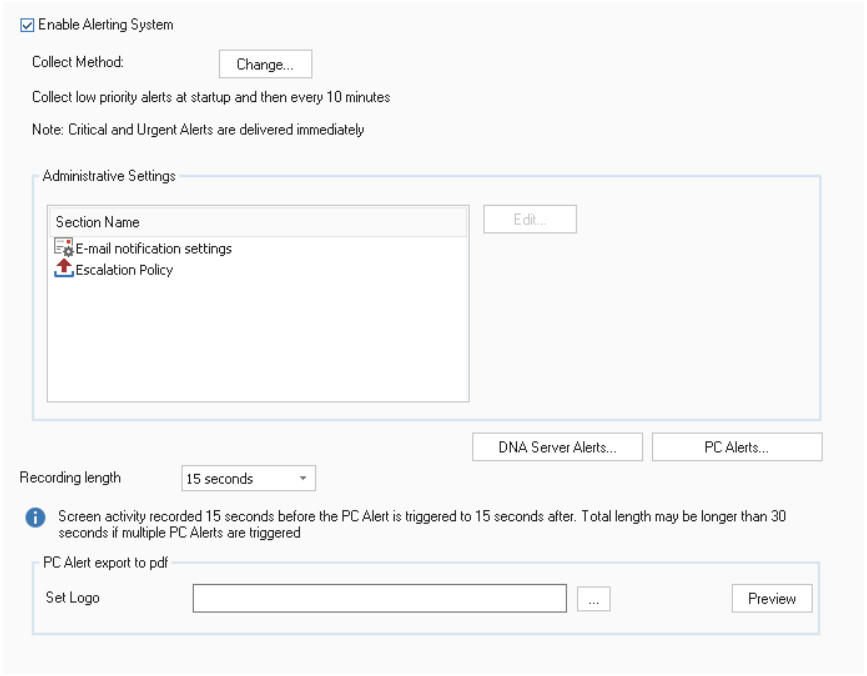
Custom Extension
If required, specify the extension of any additional file types. Click  and select the file types from the list or add your own.

In Folders
Indicate which folders should be included or excluded.

File Size
Specify a minimum or maximum file size.

Alerting

The email notification settings need to be configured from here before you can send an alert notification by email.



Enable Alerting System
Un-check this box to switch Alerting off.

Collect Method:
By default, Alerting will collect low priority alerts when the NetSupport DNA Agent starts up and then every ten minutes. Click **Change** to amend the settings and set custom collect times.

Note: Critical and urgent alerts are sent to the server immediately.

Administrative Settings

You can configure the settings for the NetSupport DNA Alerting System by clicking **Edit**.

Email Notification Settings

Allows you to specify an email address for an Administrator to be notified of any unanswered critical alerts and whether to be notified when an alert is closed.

Administrator Notification
Enter the email address of the Administrator to be notified of all unanswered alerts.

Send email Notification on Close
If required, an email notification can be sent when an alert is closed.

Note: When inputting the above values into the settings dialog, press **Enter** to accept these values.

Escalation Policy

Allows you to amend the specified times for Operators to deal with alerts before they are escalated to the next level. Once they have been escalated to critical for the specified time, the Administrator will be notified by email.

Selecting **NetSupport DNA Server Alerts** or **PC Alerts** enables you to create or edit alerts.

Recording length
If a PC Alert action is set to 'record screen', the screen recording length can be set here. By default, the recording length will be set to fifteen seconds (fifteen seconds before and after the PC Alert has been triggered). Select the required time from the drop-down menu.

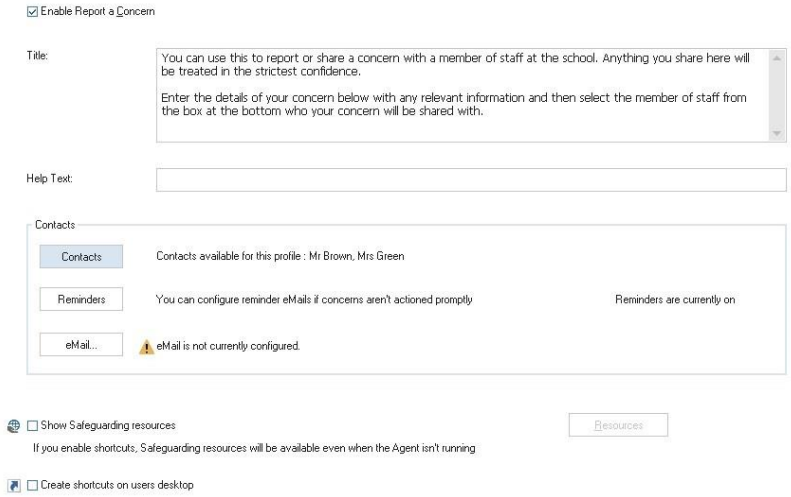
PC Alert export to PDF

When a PC Alert has been triggered, you can export the details to a PDF file. From here, you can customise the PDF with your organisation's branding by adding a logo.

Note: You can specify the folder to export the PDF to in File Location settings.

Set Logo
Click ... to select an image file. BMP, JPG and PNG files are supported and the maximum file size is 5MB. Click **Preview** to see how the logo will be displayed in the PDF.

Report Concern



Note: These settings will only be available in the Education Edition of NetSupport DNA.

Enable Report a Concern
Select this check box to allow students to be able to report concerns.

Title
You can customise the text that is displayed in the Report a Concern dialog by overtyping the existing text.

Help Text
Allows you to add a line of help text to the Report a Concern dialog. For example, you may want to include an external phone number or email address that students can contact if they wish to speak to someone outside of the school.

Contacts

Before students can report a concern, contacts (staff members who can receive concerns) need to be defined. Click **Contacts** to create new contacts, edit existing contacts and choose which contacts should be available for this profile.

If concerns are not actioned within four hours, a reminder email will be sent. This option is enabled by default. Click **Reminders** to disable or alter the reminder interval.

Note: NetSupport DNA will only scan for concerns during the defined working hours. The working hours can be amended to suit your requirements in the Console Preferences - General settings.

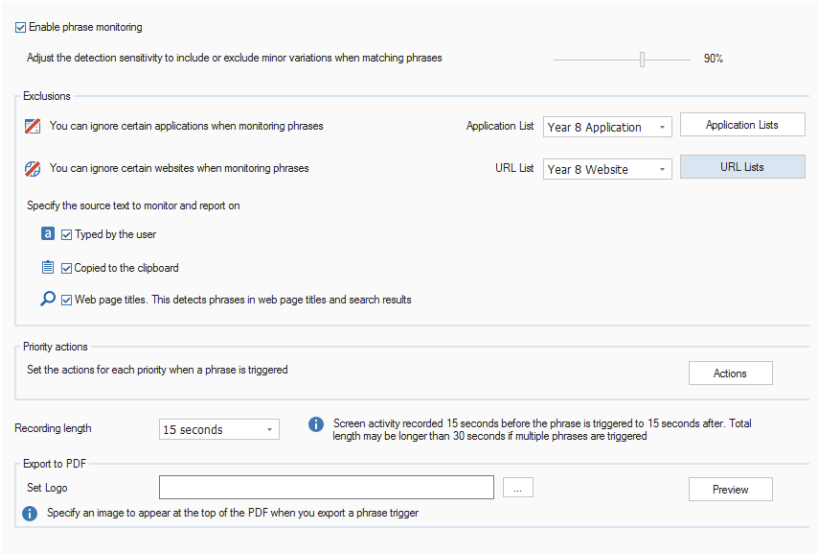
For contacts to receive an email notification when a concern is raised, you must configure the email settings. Click **eMail**.

Show safeguarding resources
Selecting this option will enable a link to a list of safeguarding resources (websites and helplines), which will be available to students from the NetSupport DNA Agent menu and when they report a concern. When you first enable this option, you will be asked to set your region to ensure a list of relevant resources is displayed. To add or edit the list, click **Resources**.

Create shortcuts on users' desktops
Shortcuts to report a concern and safeguarding resources (if enabled) will be created on student desktops.

Note: The safeguarding resources shortcut will be available even when the NetSupport DNA Agent is not running.

Phrase Monitoring



Enable phrase monitoring
Clear this check box to disable the phrase monitoring feature.

When matching keywords, you can adjust the accuracy level to determine how accurately words must be typed by the student before they are reported. By default, this level is set at 90%, allowing for minor misspellings to be taken into account when matching.

If the accuracy is set to 100%, this would require the student to type the keyword exactly for it to be matched. The lower the percentage, the more likely the term (or words similar to the term) will be flagged as inappropriate.

Exclusions

Certain applications and websites can be ignored when monitoring keywords and phrases.

Application List
To create a new Application list, click **Application Lists** and select which applications to ignore. Once the list has been created, select it from the drop-down menu. All applications in the Application list will be ignored for phrase matching.

URL List
To create a URL list, click **URL Lists** and select which websites to ignore. Once the list has been created, select it from the drop-down menu. Websites in the URL list will be ignored when monitoring phrases.

Source text
Decide what type of text to monitor and report on: text typed by the user, text copied to the clipboard and text in web page titles.

Priority actions

When a phrase is triggered, the action taken will depend on the priority level set. By default, all priority levels will record usage in the eSafety information window (unless the priority is set to off); medium and above levels will also generate an alert; a high level will additionally take a screen shot at the student and send an email notifying users that a phrase has been triggered, and an urgent level will take a screen recording at the student who has triggered the phrase.

Notes:
- The email settings must be configured before email notifications can be sent. Users can be set up to receive email notifications for triggered phrases in the Safeguarding User dialog.
- An image of the student who has triggered the phrase can be captured, if the student machine has an active webcam. By default, this action is turned off, but can be applied to any of the priority levels. A webcam image will not be taken if the webcam is currently in use on the student machine or if the webcam has been disabled in the USB Device Control settings.

To customise what actions are taken for each priority level, click **Actions**.

Recording length
The screen recording length for an urgent priority level can be set here. By default, the recording length will be set to fifteen seconds (fifteen seconds before and after the phrase has been triggered). Select the required time from the drop-down menu.

Export to PDF

When a phrase has been triggered, you can export the details to a PDF file. From here, you can customise the PDF with your school branding by adding a logo.

Note: You can specify the folder to export the PDF to in File Location settings.

Set Logo

Click ... to select an image file. BMP, JPG and PNG files are supported and the maximum file size is 5MB. Click **Preview** to see how the logo will be displayed in the PDF.

Note: These settings will only be available in the Education Edition of NetSupport DNA.

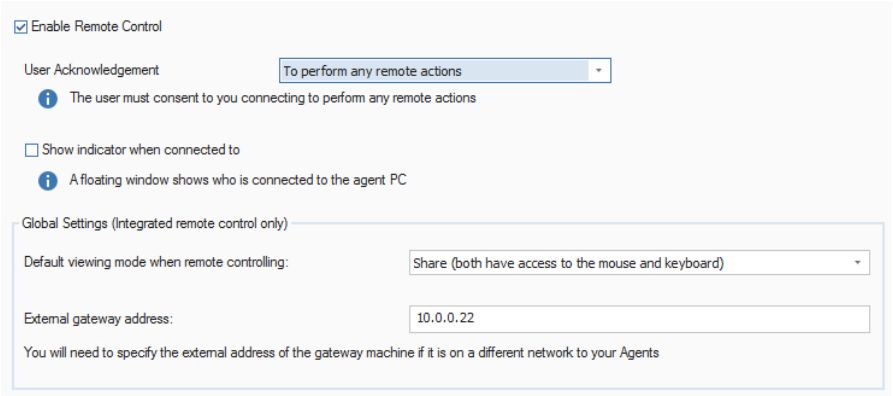
Acceptable Use Policy



Enable
Clear this check box to disable the Acceptable Use Policy feature.

Manage
Allows you to create, view and manage Acceptable Use Policies. Click **Manage**.

Remote Control



Enable Remote Control
Clear this check box to disable the remote control feature.

User Acknowledgement
When user acknowledgement is enabled the remote user (Agent) has to consent (by acknowledging a message) before remote actions and/or viewing of their screen can take place. Select the required option from the drop-down list:

None
You can connect to and perform any remote action without the user's consent.

To view remote screen
You can connect to and perform remote actions, such as File Transfer, launch a remote command prompt, but the user must consent before you are able to view their screen.

To perform any remote actions
The user must consent before any remote action can be performed.

Show indicator when connected to
When a remote control session is active, the Agent will be able to see who is connected to them.

Global Settings (Integrated remote control only)

Default viewing mode when remote controlling
From the drop-down list, select the viewing mode when remote controlling Agents. By default, this is set to Share mode.

Share
Both the Console Operator and the Agent will be able to enter keystrokes and mouse movements.

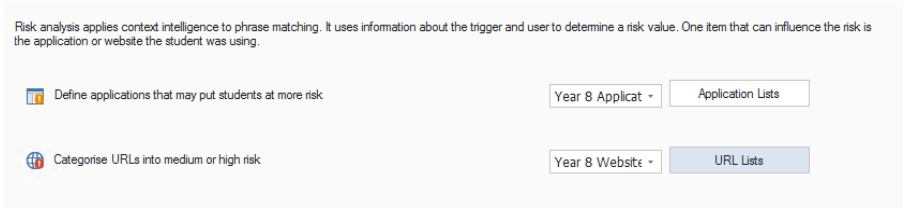
Watch
Only the Agent will be able to enter keystrokes and mouse movements. The Console Operator's mouse and keyboard will be disabled.

Control
Only the Console Operator will be able to enter keystrokes and mouse movements. The user at the Agent will be locked out.

External gateway address
If any of the Agent machines you want to remote control are located on remote networks, you need to enter your external (public) gateway address to enable the integrated remote control features at these devices.

Note: These settings will only be available in the Education Edition of NetSupport DNA.

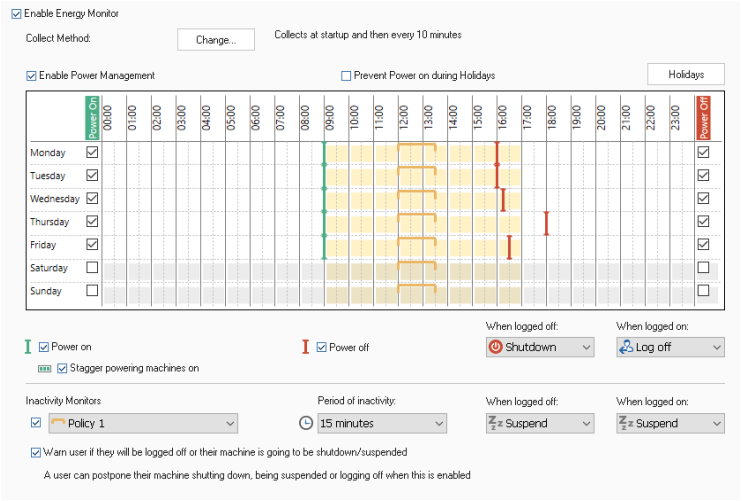
Risk Analysis



Define applications that may put students at more risk
You can select which applications are going to be classed as a higher risk. These applications can be added to an Application list and multiple lists can be created, allowing you to have different lists for different profiles. Click **Application Lists**.

Categorise URLs into medium or high risk
URL lists can be created, allowing you to specify whether websites are medium or high risk. Multiple lists can be created, allowing you to have different lists for different profiles. Click **URL Lists**.

Energy Monitor



Enable Energy Monitor
Clear this check box to prevent Energy Monitor from running.

Collect Method:
By default, Energy Monitor will collect data when the NetSupport DNA Agent starts up and then every ten minutes. Click **Change** to amend the settings and set custom collect times.

Enable Power Management
Select this option to enable the power management function. A power management schedule will be displayed.

Note: Yellow shaded areas show the organisation's working hours. Working hours are set in Console Preferences - General settings.

Prevent power on during holidays
This option will exclude any holiday dates that have been set from the power on schedule. To set your holiday periods, click **Holidays**.

Power On
Select this option to enable the power on function. Choose the days to power on machines. To adjust the time to power on machines, slide the green bar to the required time slot.

Stagger powering machines on
This option will stagger the machines powering on, instead of powering them on all at once.

Power off
Select this option to enable the power off function. Choose the days to power off the machines. To adjust the time to power off the machines, slide the red bar to the required time slot.

You can decide what action is taken when a user is logged on or off when power off is enabled; do nothing, shut down, suspend, lock or log off (when logged on).

Note: The schedule power off function is unavailable for machines with a Server operating system, a DNA Server installed, an SNMP Server installed, a Web Server installed or a DNA Remote (Agent) Gateway installed.

Inactivity Monitors
Two inactivity policies can be set up, allowing you to create rules as to what action is taken when a machine is inactive for a specified period of time. When a policy is enabled, a marker will be displayed. You can resize this and drag to the time period you want the policy to apply for.

Warn user if they will be logged off or their machine is going to be shut down/suspended
This option will warn a user that they will be logged out of their machine or it is due to be shut down or suspended. The user then has the option to postpone this action for fifteen, thirty or sixty minutes.

Note: The user will be able to see if a power management schedule has been set and postpone the action in the NetSupport DNA Agent window.

Click **Save** to save any changes. To revert to the default settings, click **Reset**.

Click **Close** to exit the dialog (any unsaved changes will be lost) or click  to go back to the main menu.

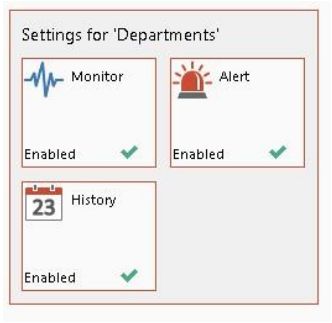
SNMP Configuration Settings

The NetSupport DNA SNMP Configurator allows Administrators/Console Operators to apply specific settings, at company or department level, to each of the SNMP primary features.

To access the NetSupport DNA Configuration menu, highlight the department or company in the Devices Tree view that the settings should apply to, right-click and select Settings – or, in the Settings tab, click the **General** icon. You can also access the individual component settings from the component icon drop-down list.

Notes:

- These settings will only appear when you are in the Devices Tree View.
- Console Preferences can also be accessed from this dialog.

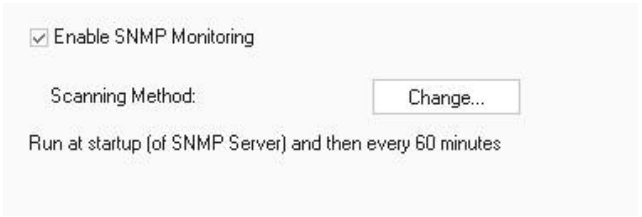


An overview of the settings for each component will be displayed, allowing you to see which components are currently enabled. A yellow star will be displayed when changes have been made to a component but not saved.

Clicking on an icon will take you to the settings for that area.

Click **Save** to save any changes. You will be asked how you want these settings to apply to the department. The **Reset** button will delete all department settings and revert to the default settings or parent settings.

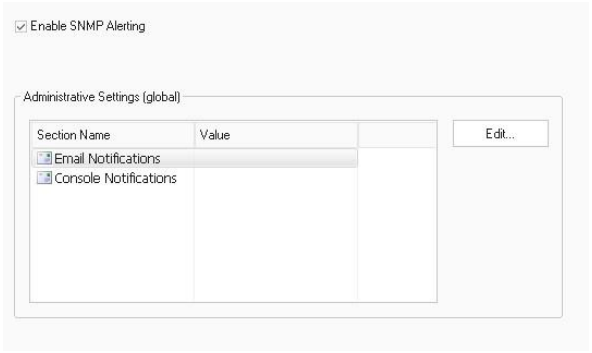
SNMP Monitor Settings



Enable SNMP Monitoring
Clear this check box to disable SNMP Monitoring.

Scanning Method
By default, SNMP Monitoring will run when the SNMP Server starts up and then every sixty minutes. Click **Change** to amend the settings and set custom scan times.

SNMP Alert Settings



Enable SNMP Alerting
Clear this check box to switch Alerting off.

Administrative Settings
You can configure the settings for the NetSupport DNA SNMP Alerting system by clicking **Edit**.

Email Notifications
Allows you to specify an email address for an Administrator/Operator to be notified when an SNMP alert becomes active.

Note: Multiple email addresses can be added. They must be separated by a semicolon.

Console Notifications
Select which Console users should receive Console notifications.

SNMP History Settings



Enable SNMP History
Clear this check box to disable SNMP History.

Click **Save** to save any changes. You will be asked how you want these settings to apply to the department. The **Reset** button will delete all department settings and revert to the default settings or parent settings.

Click **Close** to exit the dialog or click  to go back to the main menu.

Console Preferences

Console Preferences are global settings that apply across the whole of the NetSupport DNA Console.

Note: NetSupport DNA's component settings are configured through profiles.

There are seven types of settings that Operators can configure in the Console Preferences dialog:

1. **General**

   Configure the general settings that apply across the NetSupport DNA Console, define when NetSupport DNA checks for available updates and set the working hours and holiday periods for your organisation.

2. **User Interface**

   Allows you to customise what is viewed in the Hierarchy Tree view.

3. **Active Directory Settings**

   Allows you to configure the NetSupport DNA components based on the Active Directory containers, rather than departments.

4. **Email Settings**

   Allows you to set up the email settings for notifications to be delivered.

5. **Auto Discovery**

   Allows you to enable the automatic Agent discovery feature.

6. **Audit**

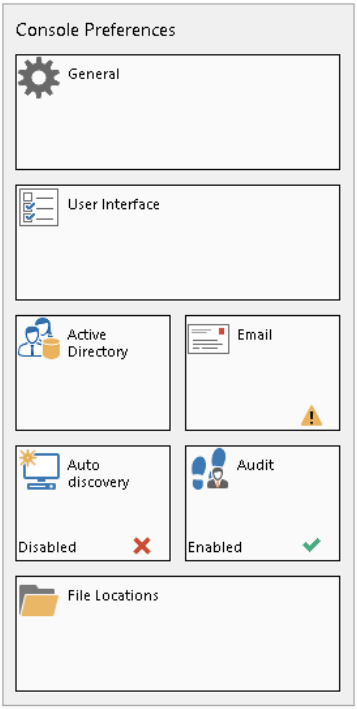
   Allows you to configure the settings for the NetSupport DNA Audit Log.

   Note: Audit will not be available when Console Preferences are accessed from the Users, Devices or Discovered Tree.

7. **File Locations**

   Allows you to specify where PDFs are exported to for PC Alerts and eSafety* triggered phrases.

To access the Console Preferences, select the Settings tab and click the **General** icon.



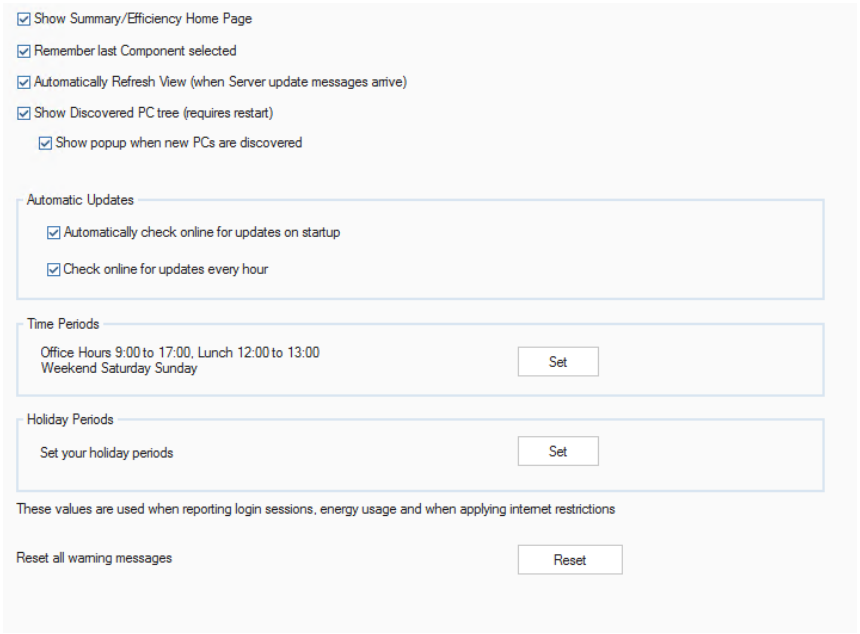
Clicking on an icon will take you to the settings for that area.

Note: A yellow star will be displayed when changes have been made but not saved.

Click **Save** to save any changes.

*eSafety is only available in the Education Edition of NetSupport DNA.

General



Show Summary/Efficiency Home Page
This option allows you to hide/display the summary/efficiency screen.

Remember last Component Selected
If checked, the NetSupport DNA Console will remember the last component that was selected when you exit. When you next enter the NetSupport DNA Console, you will be taken straight to that component.

Automatically Refresh View (when Server update messages arrive)
When enabled, NetSupport DNA will advise you that there are new updates available (an indicator will appear on the **Refresh Page** icon in the ribbon), allowing you refresh the view at the next convenient opportunity.

Show Discovered PC tree (requires restart)
This option allows you to hide/display the Discovered PC Tree view in the Console.

Show popup when new PCs are discovered
If the Discovered Tree view is displayed, you can choose whether to be notified of any new PCs that are discovered.

Automatic Updates

By default, NetSupport DNA automatically checks for any available updates. If any are found, a header bar will be displayed in the Console window. You can view the updates and download them from here.

Automatically check online for updates on startup
NetSupport DNA will automatically check for any updates each time the Console starts.

Check online for updates every hour
NetSupport DNA will check for updates every hour.

Time Periods

The working days and hours that are used when reporting login sessions and energy usage, when applying internet restrictions and when determining if a phrase* has been triggered in or out of lesson times can be customised to suit your organisation. Click **Set** to specify the working hours, lunch period and weekend.

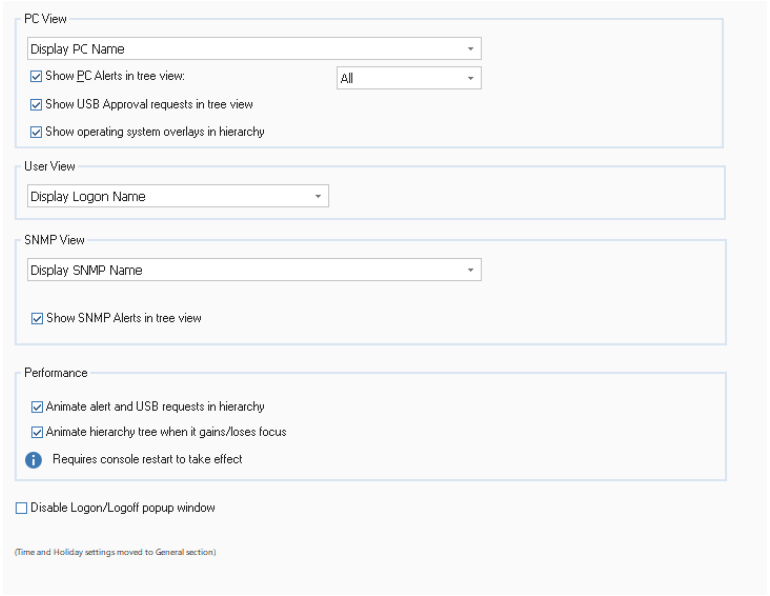
Holiday Periods

NetSupport DNA allows you to set holiday periods. These dates can then be excluded from the power on schedule in Energy Monitoring settings, so machines are not powered on. Click **Set** to specify the dates.

Reset all warning messages
When a warning message appears in the Console, you can choose not to display it again. Selecting this option will reset all warning messages, so they will now be displayed.

* Only available in the Education Edition of NetSupport DNA.

User Interface



PC View

Choose how to display the Agents in the PCs Tree view.

Show PC Alerts in tree view
Allows you to turn on/off the icon that is displayed at the Agent level in the Tree view when an alert is raised. From the drop-down list, select whether to turn off all alert icons, PC or Server alerts.

Show USB Approval requests in tree view
Allows you to show/hide USB approval requests in the PCs Tree view.

Show operating system overlays in hierarchy
Shows/hides the operating system icon overlay on the Agents in the PCs Tree view.

User View

Choose how to display the Agents in the Users Tree view.

SNMP View

Choose how to display the devices in the Devices Tree view.

Show SNMP Alerts in tree view
Allows you to turn on/off the icon that is displayed in the Devices Tree view when an alert is raised.

Performance

Animate alert and USB requests in hierarchy
By default, the alert and USB request icons displayed in the hierarchy Tree view are animated. To turn this off, clear this check box.

Animate hierarchy tree when it gains/loses focus
By default, a highlighted item in the Tree view will be in focus and other items will be faded. This can be turned off, so all items always remain in focus.

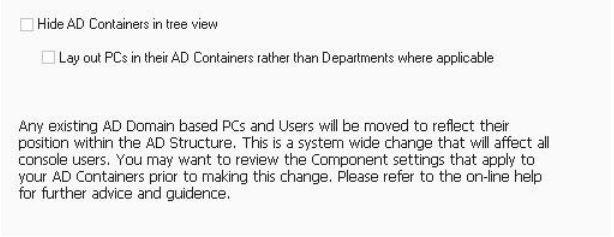
Note: For these settings to take effect, the NetSupport DNA Console will need to be restarted.

Disable Logon/Logoff popup window

Every time another user logs in or out of the NetSupport DNA Console, a popup message is displayed, selecting this option will disable this message.

Active Directory Settings

By default, NetSupport DNA displays the standard departmental Tree view. If you are working with Active Directory, it may be useful to have PCs and users displayed in the same Tree structure.



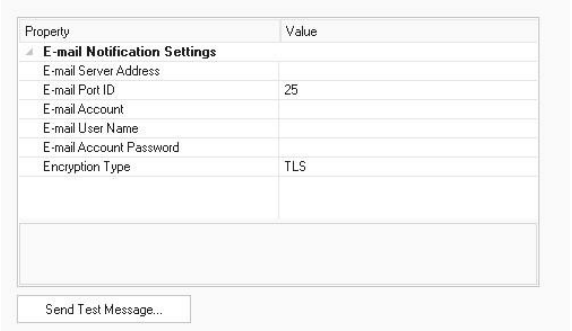
Hide AD Containers in tree view
The AD Containers folder will be displayed by default in the Tree view, regardless of whether you are using them. Checking this option will hide the AD Containers in the Tree.

Lay out PCs in their AD Containers rather than departments where applicable
Checking this option will move Agents to the relevant AD Container to reflect their position within the structure.

Note: Any changes to the structure will need to be made through Active Directory; NetSupport DNA will then pick up these changes.

When Agents are moved to their Active Directory Containers, any previous department settings may not apply to the Active Directory Container. Please review the component and Agent settings to ensure you have the correct settings applied.

Email Settings



Email Notification Settings

Allows you to configure the email settings for notifications to be sent to Operators.

Email Server Address
Enter the email server address that you wish to use.

Email Port ID
Enter the email server TCP/IP port number.

Email Account
Enter the email address that all notification emails will be sent from.

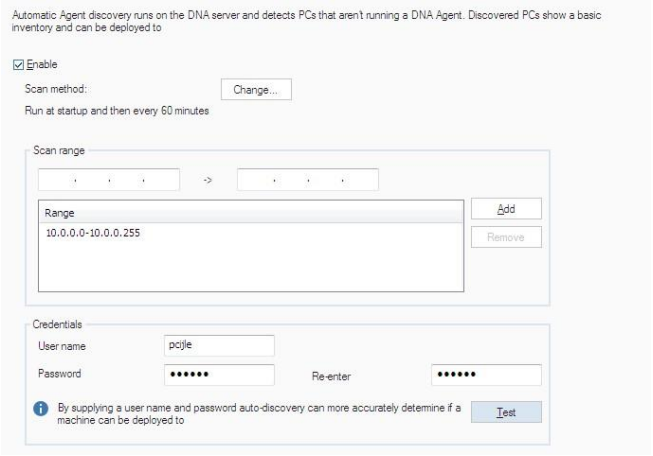
Email User Name
Enter the logon name of the above email account.

Email Account Password
Enter the password for the email account.

Encryption Type
Select the encryption type from the drop-down list: SSL, TSL or SMTP.

Send Test Message
Allows you to send a test message. Enter the email address to send the test to.

Auto Discovery



Enable
Select this option to enable automatic discovery.

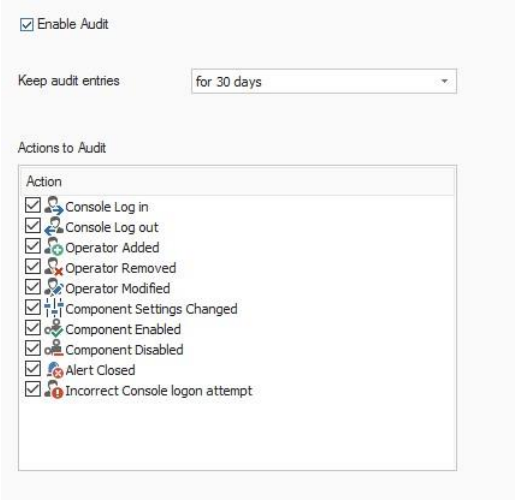
Scan method
By default, automatic discovery will run at start up and then every sixty minutes. Click **Change** to amend the settings and set custom scan times.

Scan range
Enter the required IP address range to scan and click **Add** to include it in the list.

Credentials
You can enter a user name and password, allowing you to determine if a machine can have a DNA Agent deployed to it.

Test
Allows you to test the credentials that you have entered.

Audit



Enable Audit
Clear this check box to disable the Audit Log.

Keep audit entries
Decide how long to keep audit entries for: thirty days, sixty days, ninety days or indefinitely.

Actions to Audit
The actions that can be audited are listed. Deselect any actions that you do not want to be recorded.

File Locations



PC Alert export to PDF

When a PC Alert has been raised, you can export the details to a PDF file. From here, you can specify the default folder that the PDF is exported to.

Set export folder

Click ... to specify the folder that the PDF is exported to.

eSafety Phrase export to PDF

When a phrase has been triggered, you can export the details to a PDF file. From here, you can specify the default folder that the PDF is exported to.

Set export folder

Click ... to specify the folder that the PDF is exported to.

Note: This option will only appear in the Education Edition of NetSupport DNA.

Click **Save** to save any changes. Click **Close** to exit the dialog or click to go back to the main menu.

NetSupport DNA Cloud Console

In addition to the main Windows Console, NetSupport DNA offers a cloud-based safeguarding console for use when away from the local network, enabling Console Operators to access data from any device. A smartphone-optimised user interface allows safeguarding staff to quickly search for a specific student and review any recent alerts or concerns.

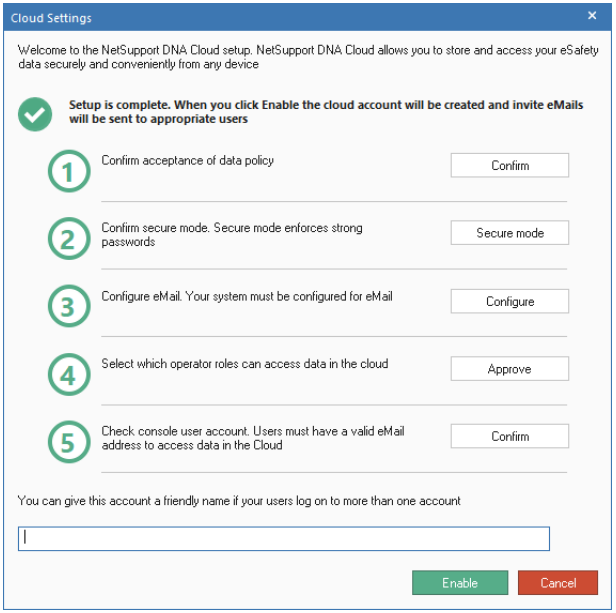
Notes:

- Only available in the Education Edition of NetSupport DNA.
- Only eSafety components, Phrase Monitoring, Report a Concern and Risk Analysis are enabled in this version of the DNA Cloud Console.
- The Cloud Console must also be enabled if you want to use the Report a Concern via website facility.

Enable access to the Cloud Console

1. In the Settings tab, click the Cloud Settings icon in the ribbon.
   Or
   If displayed, click **Setup** on the green header bar in the Console.
2. The Cloud settings dialog will be displayed. This takes you through the required steps to set up cloud access.

Note: When a step is completed it will turn green.



Step 1
Click **Confirm** to accept the cloud user policy. Read the policy and select **I have read and agree to this policy** and click **OK**.

Step 2
We recommend that Secure Mode is enabled as it forces Console Operators to use complex passwords which increases security when using the cloud. Click **Secure Mode**.

Step 3
The email settings for NetSupport DNA must be configured before you can proceed. Click **Configure**.

Step 4
You must choose which Operator roles will have access to the cloud, click **Approve**. A list of available roles will be displayed, select the required roles to have cloud access. To create a new role, click **Roles**.

Note: By default, the system administrator will always have access to the cloud.

Step 5
If you have not set up email addresses for your users, you will need to do this before cloud access can be enabled. Click **Confirm**. A list of available users that have a role assigned to them with cloud access enabled will be displayed. Enter a valid email address and click **OK**.

Note: This is the email address users will use to log into the Cloud Console.

3. If required, you can enter a name for the cloud account. This may be useful if users have access to more than one account.
4. Once all steps are green, click **Enable**.
5. An account will be created in Microsoft Azure and your data synchronised with the cloud. Users will receive an email invitation, enabling them to log into the Cloud Console. The status of the cloud is displayed on the Status bar and you can click here to access the Cloud Console.

Note: For security reasons, the first time you log in (or existing operators change email address) you will need to enter a PIN to verify who you are. You can manually send or resend a PIN (which will be included in the email invitation) via email when editing Console Operators.

To disable access to the Cloud Console, click **Disable** in the Cloud Settings dialog. All data stored in the cloud will be deleted.

Manage Web Concern

As well as providing vulnerable students with the option to report their concerns via a DNA Agent enabled device, you can also provide a custom Report a Concern link on a website, your school's site for example, for use out of school hours or when the student doesn't have access to an Agent machine.

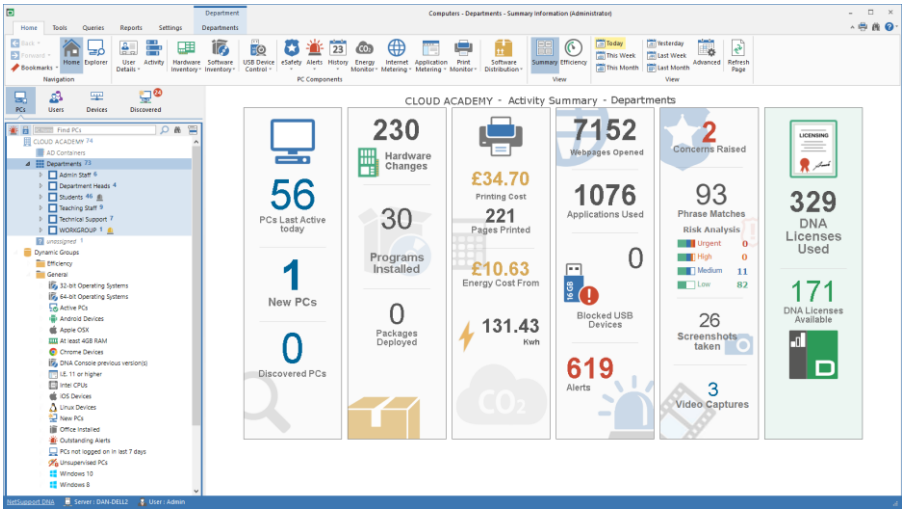
Notes:

- Only available in the Education Edition of NetSupport DNA.
- The NetSupport DNA Cloud Console must be enabled before you can use this feature.

For instructions on how to configure and implement this feature, please refer to the topic 'Reporting a Concern via a Website' in the eSafety section of this manual.

USING NETSUPPORT DNA

Console Window – Summary/Home Screen



The Summary screen presents an overview of the main NetSupport DNA features. From here, you can quickly jump to the actual information window for that component by clicking on the relevant icon. You are also provided with a summary of your NetSupport DNA licences and clicking here will display your full licence information.

As with all NetSupport DNA components, the data can be viewed at company, department, AD container, Dynamic Group or Agent level by simply selecting the required option in the Tree view.

The data can be viewed for a specified period. To switch between different time periods, click the appropriate icon in the View section of the ribbon. Clicking **Advanced** allows you to apply a customised date/time filter.

You can view the Summary screen by clicking the **Home** icon in the ribbon.

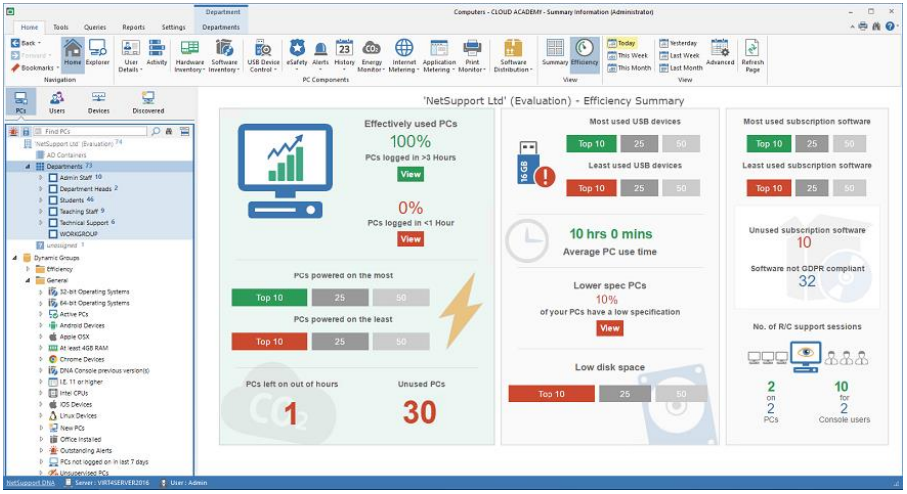
Note: By default, the Summary screen will be displayed, if you have been viewing Efficiency View, click the **Summary** icon in the ribbon.

You have the option to hide the Summary screen: select the Settings tab and click the **General** icon. The DNA Configuration dialog will appear: click the **General** option under Console Preferences and deselect **Show Summary/Efficiency Home Page**.

Efficiency View

NetSupport DNA allows you to see at a glance how efficiently hardware and software is being used across your organisation. Efficiency View provides a visual dashboard highlighting key areas of efficiency data, such as how many PCs were left on 'out of hours', the number of unused PCs, PCs with the lowest spec and disk space, the most and least used USB devices and applications and more. Clicking on the relevant icon in the dashboard allows you to identify the relevant PCs and manage issues such as retiring unused PCs, ensuring PCs are turned off overnight and upgrading lower spec PCs.

1. Click the **Home** icon in the ribbon and then click **Efficiency**.
2. The Efficiency view dashboard will appear.



The data can be viewed for a specified period. To switch between different time periods, click the appropriate icon in the View section of the ribbon. Clicking **Advanced** allows you to apply a customised date filter.

Clicking an icon in the dashboard will take you to the appropriate dynamic group in the Efficiency folder in the Tree view, allowing you to view the

PCs in the relevant component (or a dialog will appear displaying the required data).

Note: The remote control support sessions data will not be displayed if the Audit Log has been turned off or the remote control component disabled. When using the date filter, data may not show as expected if what you are trying to view is past the audit entries cut off date. For example, audit entries are kept for 30 days and you set the date filter to last month.

For NetSupport DNA to know what applications are classed as subscription software, you need to assign them to the Subscription Software category in the Application Manager.

1. Select the **Software Inventory** icon in the ribbon.
2. Click the **Software Inventory** icon drop-down arrow and select {Application Manager} from the menu.
   Or
   Click the **Application Manager** icon in the Software Inventory group.
3. The Software Manager dialog will appear. Select the Applications tab.
4. A list of applications will be displayed, select the required application and click **Edit**.
5. In the Application Categories section, click **Assign**.
6. Select **Subscription Software** and click **OK**.
7. Click **OK**.
8. Repeat the process for any other applications and click **OK** when finished.
9. The applications will now be classed as subscription software.

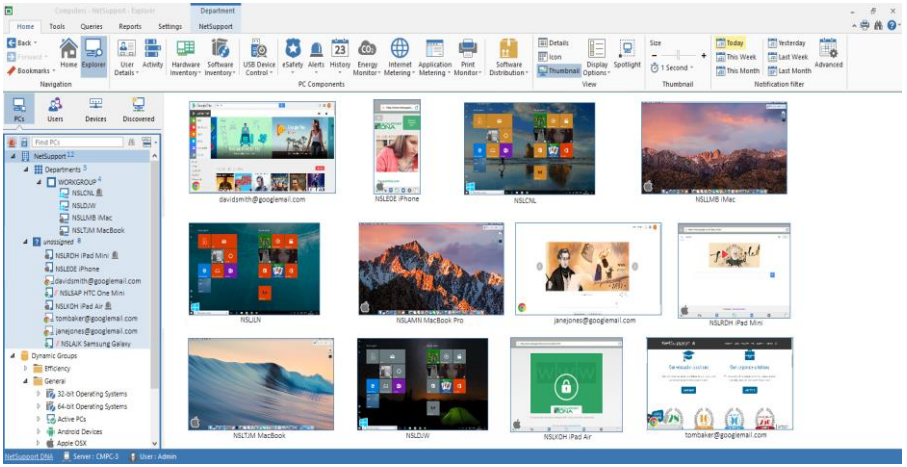
Explorer

Explorer mode provides a real-time overview of all PCs and users on the network, highlighting those that have current notifications, ensuring operators can identify and resolve issues quickly. Any active policies will be displayed, along with the assigned profile, performance data and much more. The data view can be presented as Icons, Details or Thumbnails (where the PC screens are visible). Privacy modes can be set to pixelate thumbnails, providing data protection and confidentiality.

The Spotlight feature offers a similar service to Task Manager providing a quick and easy method for viewing and managing currently running processes and services at a selected Agent PC but with the added benefit of also allowing you to interact with open applications and websites.

1. Click the **Explorer** icon in the ribbon. The Explorer window will appear.

Note: If the component icons are not visible, click the Home tab.



You can switch the Tree view between PCs and Users. The PCs Tree view displays PCs and the PC owner who is associated with the PC. The Users Tree view displays logged on users.

In the Tree view, select the level at which you want to view the Agents: company, department, AD container, Dynamic Group or individual Agent.

The information window will display the selected Agents. Right-clicking on an Agent allows you to select from a range of available features. For example, you can send a message, start a chat session, power on machines etc.

Notes:

- A remote control session can be opened by double clicking an Agent. Ensure the **Double click PC in Explorer to remote control** option is enabled. Select the Tools tab, followed by **Configure Remote Control**. This feature will only be available in the Education Edition of NetSupport DNA or, if in the Corporate Edition, you have NetSupport Manager or a third-party remote control application installed.
- If any of the Agent machines you want to remote control are located on remote networks, you need to enter your external (public) gateway address into the Remote Control Configuration settings to enable the integrated remote control features at these devices.

Notifications are displayed when an Agent has triggered a phrase*, raised an alert and requested USB device approval. By default, Agents will be highlighted when they have a notification. To turn this off, select **Display Options** in the ribbon and clear the option **Highlight PCs with notifications**.

* Only available in the Education Edition of NetSupport DNA.

Notification data can be viewed for a specified period. To switch between different time periods, click the appropriate icon in the Notification Filter section of the ribbon. Clicking **Advanced** allows you to apply a customised date/time filter.

The working hours shown can be amended to suit your organisation in the DNA Configuration dialog. See Console Preferences - General for further information.

If the Agent is running on a laptop or mobile device, the wireless status and battery power level are displayed when in details or thumbnail view.

Note: To hide the department icons in the information window, select **Display Options** in the ribbon and clear the **Show departments** option.

In the Users Tree view, you can choose only to show users that are currently logged on; click the **Logged On** icon in the ribbon.

Agents can be displayed in three modes:

Details
A detailed view of Agents will be listed in the information window. The Agent computer/user name, department, IP address*, last connected time*, last logged on user*, the assigned profile and operating system* will be displayed, along with any notifications, active policies (power on and off schedule, inactivity policies, web and application restrictions, USB, CD, webcam, thumbnail and privacy mode policies), performance data (CPU usage, memory usage, network usage - bytes received/sent and free disk space) and battery and wireless indicators.

* These columns are not displayed in the Users Tree.

Notes:
- To customise the columns that are displayed, select **Display Options** in the ribbon and select which columns to display in the PC/User Columns section.
- Performance data can be highlighted once it reaches a specified limit, allowing you to easily see Agents with high CPU, memory or network usage. Select **Display Options** in the ribbon and under Performance Data move the highlight slider to the required level.

Icon
Displays an icon for each Agent. The operating system the Agent is running and any active notifications will also be displayed.

Thumbnail
A thumbnail view of Agent screens is displayed. If an Agent is running multiple monitors, you will be able to switch the view between each monitor. If you have an Agent selected in the Tree view, both monitors will be displayed as a thumbnail. In the Users Tree view, if a user is logged on to more than one machine, a thumbnail of each machine will be displayed. Icons will be displayed next to the Agent showing which Agents have thumbnails disabled and if they are in privacy mode.

Notes:
- Thumbnail view can be disabled in the DNA Configuration - Explorer settings.
- You can choose to only display Agents that thumbnails can be retrieved for. Select **Display Options** in the ribbon and then select the option **Only show devices that support thumbnails**.

Customise thumbnail size
Agent thumbnails can be resized to suit personal preferences.

1. Use the size slider in the ribbon to select the required size.
   Or
   Click the + or - icons in the ribbon.

Changing the thumbnail refresh rate
Depending on how closely you want to monitor Agent activity, you can adjust the frequency at which the thumbnails are refreshed.

1. Select the  drop-down menu in the ribbon.
2. Select the required time interval from the available options.

Privacy mode
When viewing Agent thumbnails, the text displayed can be pixelated to make it unreadable.

1. Select the Settings tab.
2. Click **Create new profile** to create a new profile with this setting enabled or click **Manage existing profiles** to enable Privacy mode in an existing profile.
3. In the NetSupport DNA Configuration dialog, select the **Explorer** option.
4. Select **Privacy Mode**.

Queries
Select the Queries tab to display the Queries window.

NetSupport DNA's Query tool enables you to interrogate the database for records matching specified criteria. Queries specific to the component currently being viewed will be listed, enabling fast retrieval of the results.

Click the **Add Query** icon on the ribbon to create a new query or click the **Edit Query** icon in the ribbon to edit an existing item in the list.

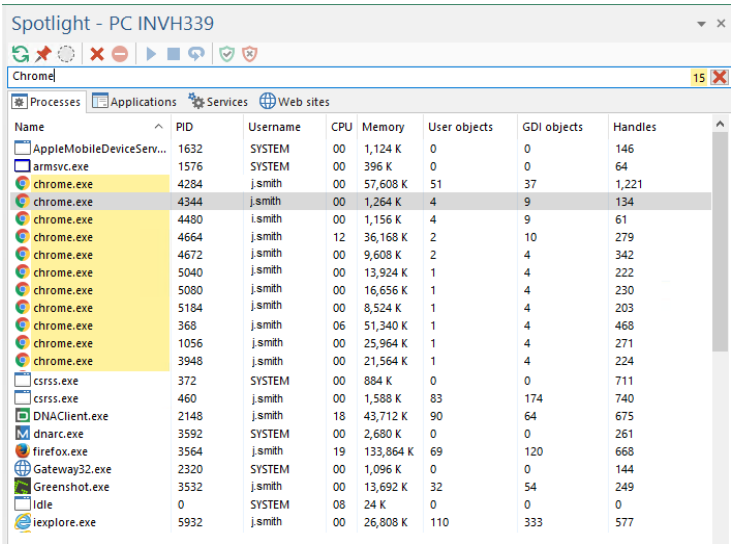
Reports
Select the Reports tab to display the Reports window.

A number of pre-defined management reports, powered by the Crystal Reports engine, are attached to each component. Select the required report from the drop-down list. The results will be listed in the information window. These can be exported if required.

Spotlight

The Spotlight feature within Explorer mode provides a similar service to Task Manager. It offers a quick and easy method for viewing and managing currently running processes and services at a selected Agent PC but with the added benefit of also allowing you to interact with open applications and websites.

1. Click the **Explorer** icon in the ribbon.
2. In the View section of the ribbon, click **Spotlight**. The Spotlight pane will appear in the information window. The Spotlight pane can be 'docked' or 'floating'. Click the down arrow at the top right of the pane or right click in a blank area and select the preferred option. If you move away from Explorer mode, the Spotlight pane will remain visible.
3. If an Agent machine has not already been selected in the Tree view or information window, you will be prompted to select one.
4. Once selected, the currently running processes, applications, services and active website will refresh. Click the tabs to see the current state of each of the four options.



Name	PID	Username	CPU	Memory	User objects	GDI objects	Handles
AppleMobileDeviceServ...	1632	SYSTEM	00	1,124 K	0	0	146
armsvc.exe	1576	SYSTEM	00	396 K	0	0	64
chrome.exe	4284	j.smith	00	57,608 K	51	37	1,221
chrome.exe	4344	j.smith	00	1,264 K	4	9	134
chrome.exe	4480	i.smith	00	1,156 K	4	9	61
chrome.exe	4664	j.smith	12	36,168 K	2	10	279
chrome.exe	4672	j.smith	00	9,608 K	2	4	342
chrome.exe	5040	j.smith	00	13,924 K	1	4	222
chrome.exe	5080	j.smith	00	16,656 K	1	4	230
chrome.exe	5184	j.smith	00	8,524 K	1	4	203
chrome.exe	368	j.smith	06	51,340 K	1	4	468
chrome.exe	1056	j.smith	00	25,964 K	1	4	271
chrome.exe	3948	j.smith	00	21,564 K	1	4	224
csrss.exe	372	SYSTEM	00	884 K	0	0	711
csrss.exe	460	j.smith	00	1,588 K	83	174	740
DNAClient.exe	2148	j.smith	18	43,712 K	90	64	675
dnarc.exe	3592	SYSTEM	00	2,680 K	0	0	261
firefox.exe	3564	j.smith	19	133,864 K	69	120	668
Gateway32.exe	2320	SYSTEM	00	1,096 K	0	0	144
Greenshot.exe	3532	j.smith	00	13,692 K	32	54	249
Idle	0	SYSTEM	08	24 K	0	0	0
iexplore.exe	5932	j.smith	00	26,808 K	110	333	577

Note: The Spotlight Pane title bar will indicate if Explorer Privacy mode is currently active. This will disable certain Spotlight features as detailed below.

Search bar



The search bar enables you to quickly identify specific items within each list. Simply enter the required criteria and matching items will be highlighted. The bar will indicate how many matched items there are.

Toolbar

The toolbar icons perform as follows:

	Refresh list(s)	Asks the selected Agent PC to re-send the data for each tab.
	Pins the selected PC	Retains the currently displayed information on screen while you navigate to other PCs to perform different tasks. You will need to un-pin the current PC before being able to view the data for another machine.
	Clear the current PC	This clears the Spotlight pane whether a PC pinned or not. It does not close the pane. This is useful to remove a pinned PC and also to clear the pane if you move away from Explorer mode.
	Close process or application	Applies to the Process and Applications tabs, closes the selected process or application.
	Block application	Applies to the Applications tab, allows you to quickly add the selected applications Window title to a blocked list. The Add Application Block dialog will appear allowing you to edit the displayed title if required and select a profile to add the item to. **Note:** If Privacy mode is active, the application titles will be masked and the option to block will be disabled.

	Start service	Applies to the Services tab, starts the selected service.
	Stop service	Applies to the Services tab, stops the selected service.
	Restart service	Applies to the Services tab, restarts the selected service.
	Approve URL	Applies to the Websites tab, adds the selected URL to an approved websites list. The Add Website dialog will appear allowing you to edit the URL details if required and choose a URL list to add the item to. **Note:** If Privacy mode is active, this option will be disabled and URLs will not be displayed.
	Restrict URL	Applies to the Websites tab, adds the selected URL to a restricted websites list. The Add Website dialog will appear allowing you to edit the URL details if required and choose a URL list to add the item to. **Note:** If Privacy mode is active, this option will be disabled and URLs will not be displayed.

Note: As well as the toolbar icons, you can also perform the actions by right-clicking on an item in each of the lists.

User Details

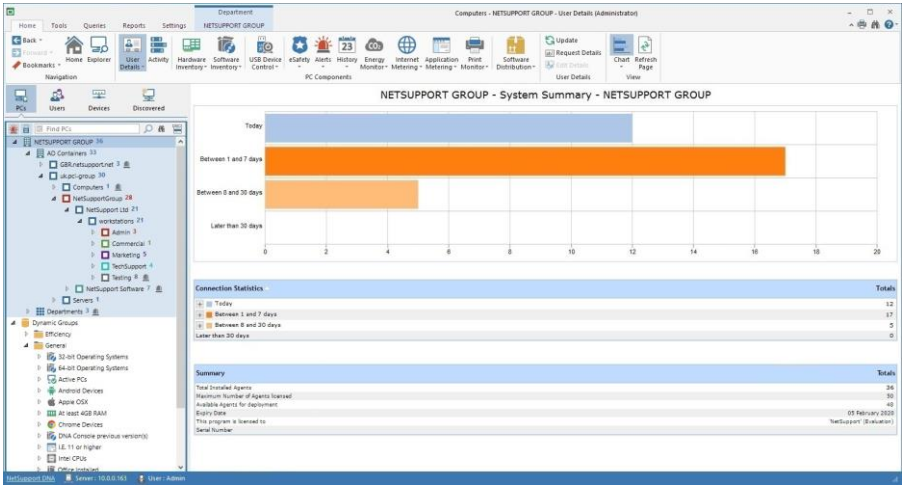
NetSupport DNA provides a range of features to locate and manage users within a networked environment. Agents have the facility to amend their details at any time or Console Operators can request updates. In addition to key user data (name, telephone etc), DNA provides the customer with the ability to tailor the data to be gathered and collated from each user, including tracking of user acceptance forms. DNA also keeps a history of changes to the data entered in User Data.

Note: User information can be retrieved from Active Directory. If the information is available, the name, company, email address, mobile, pager, telephone number and location will be taken and displayed in the Users Details dialog. Any changes will need to be made via Active Directory and NetSupport DNA will automatically pick these up.

NetSupport DNA also allows you to manage Active Directory accounts and see user accounts that have been disabled or locked, giving you the chance to quickly unlock or reset them as required.

1. Click the **User Details** icon in the ribbon. The User details window will appear.

   Note: If the component icons are not visible, click the Home tab.



You can switch the Tree view between PCs and Users. The PCs Tree view displays data for PCs and the PC owner who is associated to the PC. The Users Tree view displays data for logged on users and does not show any data relating to PCs.

When NetSupport DNA connects to a PC, the logged on user will automatically become the PC owner unless they already own another PC. If this is incorrect, you can reassign to the correct user in the Bind User dialog.

Note: A PC can only have one PC owner, whereas a user can own more than one PC. You can assign PCs to users in the Edit User Details dialog.

In the Tree view, select the level at which you want to view the information: company, department, AD Container, Dynamic Group or individual Agent.

The information window will display a breakdown for each selected item in graph and list format. To view the graph in a different format, click the **Chart** icon drop-down arrow on the ribbon and select the appropriate format. To print the active view, click the  icon at the top of the Console.

Note: Clicking the **Chart** icon in the ribbon will hide/show the graph.

Connection statistics detailing the PC name, PC owner, department and last connection will be listed for every NetSupport DNA Agent and can be viewed for the company as a whole, department or a Dynamic Group. A summary of your NetSupport DNA licence details is also displayed when viewing at company or department level.

When the data is viewed at Agent level, you can switch between **General** (PC owner, asset and maintenance information) and **Login Sessions** (PC logon information). Click the appropriate icon in the User Details ribbon or click the **User Details** drop-down icon and select {Display - General/Login Sessions}.

In the Users Tree view, all Agent logon sessions for the selected time period will be displayed. The working hours shown can be amended to suit your organisation in the Console Preferences dialog. See **Console Preferences - General** for further information.

Switching to the Users Tree view shows all Agent logon sessions for the selected time period. To switch between different time periods, click the appropriate icon in the Filter section of the ribbon. Clicking **Advanced** allows you to apply a customised date/time filter. Listed descriptions can be expanded to provide an individual Agent breakdown for each item. The working hours shown can be amended to suit your organisation in the DNA Configuration dialog. See **Console Preferences - General** for further information.

Active Directory user accounts can be managed, allowing you to unlock accounts, enable or disable accounts and reset passwords. Right click an Agent in the Users Tree and select **Manage User Accounts**.

In the Education Edition of NetSupport DNA, you have the option to mark Agents (students) as vulnerable. This allows Safeguarding users to easily identify and support vulnerable students. A student can be marked as vulnerable in the Edit User dialog, or by right-clicking on the student in the Users Tree and selecting **Vulnerable Student**. The student will then be displayed in the appropriate dynamic group in the Users Tree view.

Note: The date/time format displayed in the Console is taken from the machine where the NetSupport DNA Server is installed. To change the format in the Console, you will need to change the system date/time format on this machine. For further information, please contact our Support team www.netsupportsoftware.com/support.

Queries
Select the Queries tab to display the Queries window.

NetSupport DNA's Query tool enables you to interrogate the database for records matching specified criteria. Queries specific to the component currently being viewed will be listed, enabling fast retrieval of the results.

Click the **Add Query** icon in the ribbon to create a new query or click the **Edit Query** icon in the ribbon to edit an existing item in the list.

Reports
Select the Reports tab to display the Reports window.

A number of pre-defined management reports, powered by the Crystal Reports engine, are attached to each component. Select the required report from the drop-down list. The results will be listed in the information window. These can be exported if required.

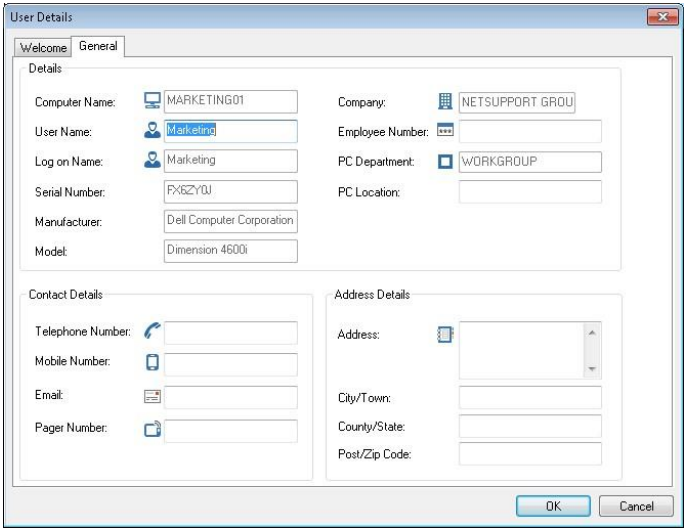
A quick refresh facility enables you to update data outside of the specified frequency. This can be useful for targeting particular Agents or departments. Right-click on the required item in the Tree view and select **Update** or click **Update** in the User Details menu or ribbon.

Request/Edit User Details

User and associated asset details can be updated by the Agents themselves or by Console Operators with appropriate rights.

The **Request Details** option enables Console Operators to remotely launch the User Details dialog at Agent PCs.

1. With the User Details tab selected, highlight an Agent, department, AD container or the company in the PCs Tree view.
2. Right click and select **Request Details**.
   Or
   Click on the **User Details** icon drop-down arrow and select {Request Details} from the menu.
   Or
   Click the **Request Details** icon in the User Details group.
3. The User Details dialog will appear at the selected machines, enabling Agents to add or update their information.



When launched at Agent PCs, a Welcome page is displayed by default. This can contain customisable messages/prompts or it can be disabled using the User Details Settings option. See NetSupport DNA Settings for more information.

At the Agent
An Agent can update its own user and asset details.

1. Right click on the NetSupport DNA Agent icon in the taskbar and select **Edit User Details**.
2. The User Details dialog will appear.

Edit user details
Console Operators with appropriate rights can edit individual Agents information from both the PCs and the Users Tree view.

Note: When editing User details from the User Tree view, only User information is shown. The asset details will not be displayed.

Edit user details from the PCs Tree view
1. Select an Agent in the PCs Tree view.
2. Right click and select **Edit Details**.
   Or
   Click on the **User Details** icon drop-down arrow and select {Edit Details} from the menu.
   Or
   Click the **Edit Details** icon in the User Details group.
3. The User Details dialog will appear.
4. From here you can edit the general details of the Agent and its asset details, as well as view any leasing or maintenance information.

Note: Each PC has a PC owner associated with it. If this is incorrect, you can change the PC owner in the Bind Users dialog. A PC can only have one PC owner.

Edit user details from the Users Tree view
1. Select an Agent in the Users Tree view.
2. Right click and select **Edit User Details**.
   Or
   Click on the **User Details** icon drop-down arrow and select {Edit Details} from the menu.
   Or
   Click the **Edit Details** icon in the User Details group.

3. The User Details dialog will appear.
4. From here you can edit the general details of the Agent. Any PCs that the User owns will be displayed. Click  to add/remove PCs. Users can own more than one PC.

Note: In the Education Edition of NetSupport DNA, you can choose to identify vulnerable students. Select the **Mark this student as vulnerable** option (this option will only appear when editing user details from the Users Tree). Vulnerable students will then be displayed in a Vulnerable Students dynamic group. The dynamic group list in the Tree will need to be refreshed for this to appear.

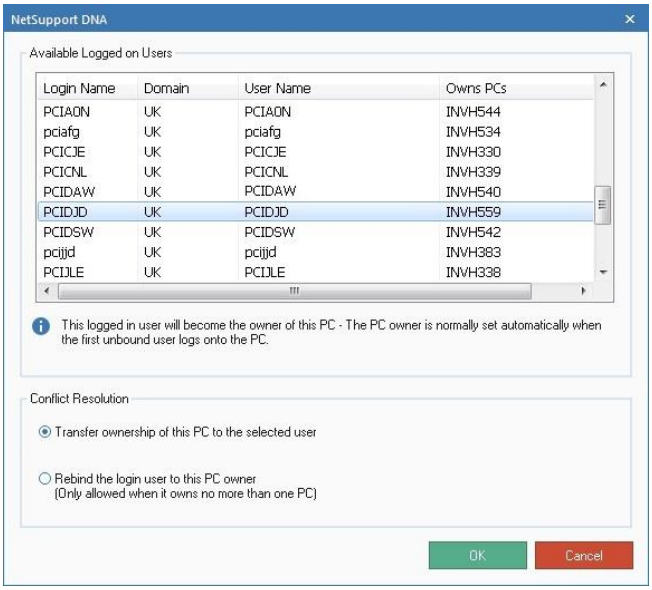
Bind User Dialog

When NetSupport DNA connects to an Agent PC, it will automatically bind the logged on user as the PC owner, as long as the user does not own any other PCs. There may be circumstances when the user bound to the PC is incorrect, in which case, you can change the PC owner using the Bind Users dialog.

There are two ways of reassigning the PC owner. **Transfer ownership**: this method changes the PC owner to the selected logged on user and takes on all the user details of the new user, any previous user data for this PC will be deleted. **Rebind the login user**: this method rebinds the logged on user to own this PC but keeps the user details already associated with the PC, only the user login details will be changed. This method is only allowed when the logged on user does not own more than one PC.

Note: You can also bind a PC with a user from the Edit User details dialog in the Users Tree view.

1. Select the required PC in the PCs Tree view.
2. Right-click and select **Change PC Owner**.
   Or
   Click on the **User Details** icon drop-down arrow and select {Change PC Owner} from the menu.
3. The Bind Users dialog will appear.



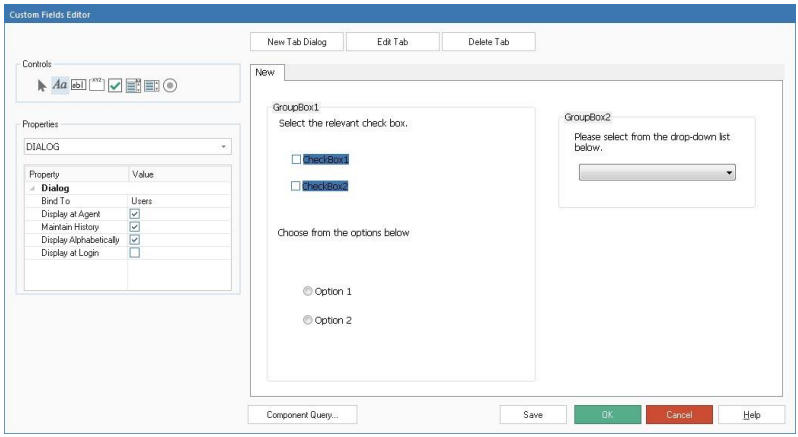
4. The available login names will be displayed along with any PCs that are already owned (you need to scroll right to see this).
5. Select the login name you wish to transfer ownership to and select the required resolution.
6. Click **OK**.

Custom User Details

By default, a range of user and asset information is dynamically recorded. The data can be updated using the Request User Details and Edit User Details options.

If you find that the default pages do not fully cover your requirements, additional customised tabs can be created.

1. In the Tools tab, click the **Custom Users Details** icon.
   Or
   Click the **User Details** icon drop-down arrow and select {Custom User Details} from the menu.
2. The **Custom Fields Editor** will appear, enabling you to create any number of custom tabs.



3. Click **New Tab Dialog** to create a new page and enter a suitable name. To save time, the content of an existing tab can be copied should fields of a similar nature be required. (**Edit Tab** enables you to change the name of an existing page.) Click **OK**.



4. Enter the properties for the tab.



5. Decide whether information contained in the new tab should be bound to the logged on user or the physical PC, when viewing the User Details dialog.

6. You can hide the tab from users should you only want Console Operators to update the information. Un-check the **Display at Agent** field to exclude the tab when launching the User Details dialog at Agent PCs.
7. **Maintain History**. If checked, a record of any changes to the user/asset data on this page is maintained. Operators can view the changes by selecting the **History** icon in the ribbon.
8. The order of the fields will be displayed alphabetically in the Console view. Un-check **Display alphabetically** to control the order of the fields.
9. Constructing the page involves adding the appropriate controls. Select a **control** and drag and drop it into the required position on the page.
10. Enter the properties and associated values for each control.
11. Store the new page at any stage by clicking **Save**.
12. Click **OK** when the page is complete.

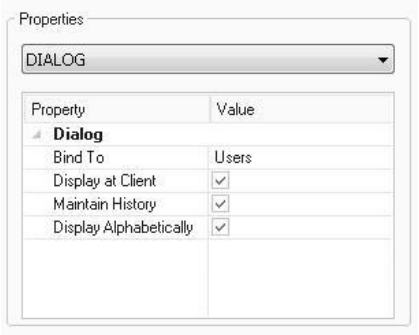
Component Query
Click this option to create a ready-made report containing the fields on the page. Use the Query Tool to load, edit and run the output.

Custom Fields Editor – Controls

A customised user/asset details tab can include a variety of controls/input fields.



Select the required control, drag and drop into the required position on the page and enter the associated properties.



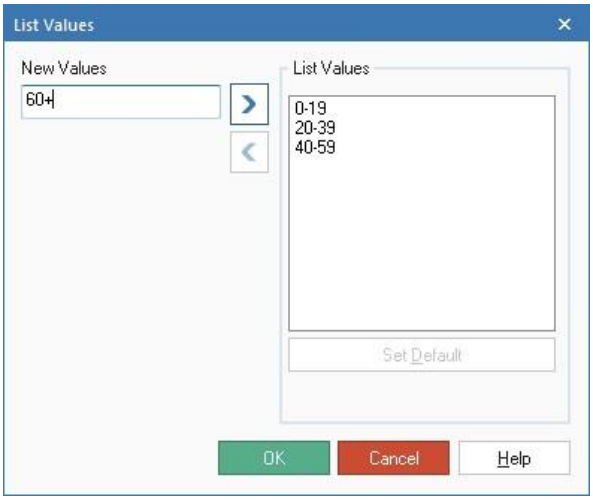
Button	Purpose	Properties
	Used to reposition/resize items on the page.	
	Enables you to add the text descriptions for each input field. The descriptions are displayed on the tab as a guide to users when updating their details but are not shown in the User Details information window at the Console.	The control will be assigned a sequential name: Text 1, Text 2 etc. To enter the required field description, amend the control properties. In the properties window, two items will be listed: the Name of the control and the Text value currently assigned. Replace the text value with your own wording.
	Creates a text box for users to enter free text. For input purposes, you would generally include a text description control adjacent to the box. The User Details information window at the Console can have descriptive text added.	In the properties window, this control is assigned the name Edit 1, Edit 2 etc. This description will appear on the User Details information window unless you change the properties. Change the value for the **Name** property to the wording of your choice. **Disable at Agent** and **Blank at Agent** can be used to 'hide' the field from users, meaning that only Operators can update the details. To allow text to be input on more than one line, check **Multiline**. To determine the order of display fields in the Console click **Field Order**. Click , the Field Order dialog will appear.
	Creates a group box. This is useful for partitioning the input form into obvious categories, allowing you to draw a box around a group of fields and apply a category heading.	Drop the control into the required position and use the sizing handles to expand the box to the required size. To add a suitable description, change the value of the text property.
	Creates a check box. This control would generally be used in multiples, offering users a choice of responses. For example, 18-35, 36-50 etc.	The control will be assigned a sequential name: Check Box 1, Check Box 2 etc. To change the name on the input form, amend the **Text** value property. To change the description on the User Details window, change the **Name** value property. The field can be disabled at the Agent if required. To determine the order of display fields in the Console, click **Field Order**. Click , the Field Order dialog will appear.

	Offers users a choice of responses in a drop-down list. You would generally include a text description control adjacent to the box.	To add descriptive text to the User Details window, amend the **Name** value property. The field can be disabled or blanked at the Agent if required. To enter the values for the drop-down list, click in the list values property. Click , the List Values dialog will appear. To determine the order of display fields in the Console, click **Field Order**. Click , the Field Order dialog will appear.
	Creates a list box. A list of values is provided for the user to select the appropriate response. You would generally include a text description control adjacent to the box.	To add descriptive text to the User Details window, amend the **Name** value property. The field can be disabled or blanked at the Agent if required. To enter the values, click on the list values property. Click , the List Values dialog will appear. To determine the order of display fields in the Console, click **Field Order**. Click , the Field Order dialog will appear.
	Creates a radio button. Similar to check boxes, they offer users a choice of responses, but only one button can be selected. Only the highlighted choice is recorded on the User Details window.	As there must be multiple choices, two options are added by default. To change the text descriptions, amend the **Radio Buttons** property by clicking in the list values field. Click , the Radio button List Values dialog will appear. Use the dialog to add the required number of options and associated descriptions. The field can be disabled and blanked at the Agent if required. To determine the order of display fields in the Console, click **Field Order**. Click , the Field Order dialog will appear.

Note: When changing the field order of controls, ensure the **Display alphabetically** is un-checked.

List Values Dialog

When creating customised User Details tabs, this dialog enables you to list the choices for a drop-down list field and the radio buttons.



1. Enter the new value and click  to add it to the List Values window. Repeat for each of the other choices.
2. One of the values can be selected as the default entry for the field. Select the item and click **Set Default**. If no default is assigned, the field will be empty when the user views it.

   Note: When entering values for the radio buttons, you must set a default.

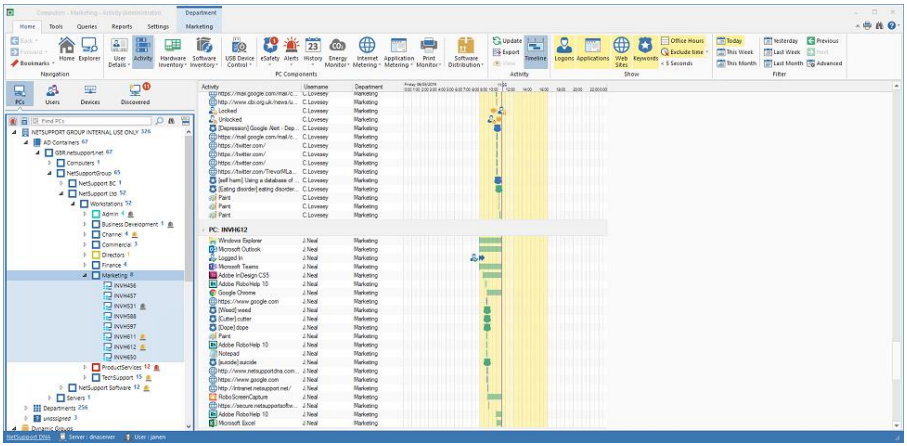
3. Click **OK** when complete.

Activity Monitoring

The Activity component provides a single chronological view of Agent logon sessions, application usage, internet usage and any eSafety* triggered phrases for a given user, PC or department over a specified period of time. You can choose which information to view and also exclude applications that are not relevant, allowing you to customise the data displayed. Activity can be viewed in a graphical timeline or text-based grid view.

1. Click the **Activity** icon in the ribbon. The Activity window will appear.

Note: If the component icons are not visible, click the Home tab.



You can switch the Tree view between PCs and Users. The PCs Tree view displays a breakdown of activity by PC and the Users Tree view shows activity by user.

In the Tree view, select the level at which you want to view the information: company, department, AD container, Dynamic Group or individual Agent.

You can view data for a specified period. To switch between different time periods, click the appropriate icon in the Filter section of the ribbon. Clicking **Advanced** allows you to apply a customised date/time filter. The working hours shown can be amended to suit your organisation in the DNA Configuration dialog. See Console Preferences - General for further information.

Note: You can only view a maximum of 31 days of activity.

By default, activity is displayed in a timeline. To toggle between the timeline and text-based grid view, click the **Timeline** icon in the ribbon.

To customise the data displayed in the information window, click the appropriate icon in the Show section of the ribbon (if the icon is shaded yellow the activity is displayed).

There may be certain applications or websites that you do not need to view - these can be excluded from the activity list. Select the required application/website in the list, right-click and select **Hide from Activity and Application/Internet Metering**. The application or website will be removed from the activity list and also in Application/Internet Metering.

Notes:

- To add a hidden application back to the list, click the **Software Inventory/Application Metering** icon drop-down arrow and select {Application Manager} from the menu, select the Applications tab, find the required application in the list, click **Edit** and then select **Show in Application Metering views**.
- Application and website visits less than a specified time can be ignored. Select the Exclude time drop-down icon in the ribbon and choose the required time period to exclude. Visits below this time will no longer be displayed.

When viewing activity in the timeline, the start and end times for items will be represented by a horizontal bar (websites = blue, applications = green), user logins/logouts are shown as a single event and when an eSafety* phrase is triggered, a shield representing the risk index score will be displayed. The office working hours will be shaded yellow and the current time is highlighted by a purple line. Websites and triggered eSafety* phrases can be viewed from here; select the occurrence in the timeline and click the **View** icon in the ribbon. You can zoom in and out of the timeline by pressing CTRL and scrolling the mouse wheel.

You can zoom in and out of the timeline by pressing CTRL and scrolling the mouse wheel.

The current activity data can be exported to a .CSV file; click the **Export** icon in the ribbon.

A quick refresh facility enables you to update data outside of the standard frequency. This can be useful for targeting particular Agents or departments. Click **Update** in the ribbon.

Note: The date/time format displayed in the Console is taken from the machine where the NetSupport DNA Server is installed. To change the format in the Console, you will need to change the system date/time format on this machine. For further information, please contact our Support team www.netsupportsoftware.com/support.

Queries
Select the Queries tab to display the Queries window.

NetSupport DNA's Query tool enables you to interrogate the database for records matching specified criteria. Queries specific to the component currently being viewed will be listed, enabling fast retrieval of the results.

Click the **Add Query** icon on the ribbon to create a new query or click the **Edit Query** icon in the ribbon to edit an existing item in the list.

Reports
Select the Reports tab to display the Reports window.

A number of pre-defined management reports, powered by the Crystal Reports engine, are attached to each component. Select the required report from the drop-down list. The results will be listed in the information window. These can be exported if required.

* The eSafety component is only available in the Education Edition of NetSupport DNA.

Hardware Inventory

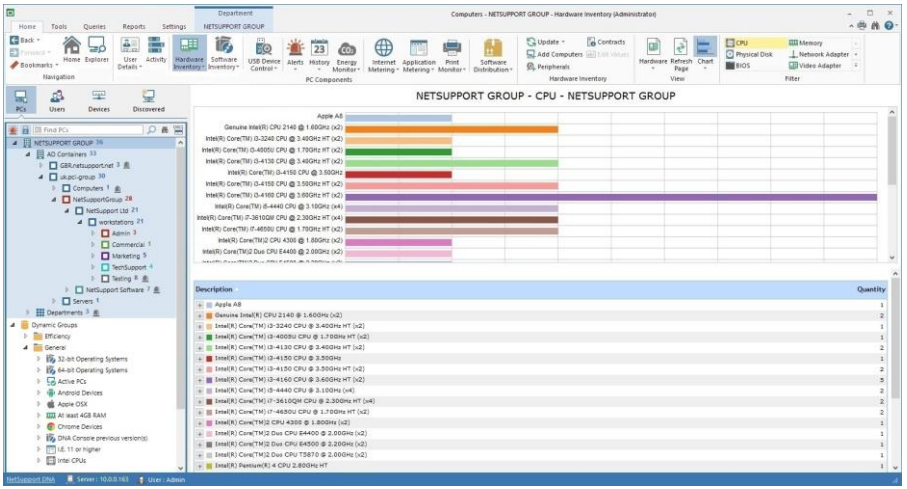
NetSupport DNA provides a comprehensive and detailed Hardware Inventory. A wealth of information is gathered from each device, from CPU and BIOS types to network, video and storage information.

Inventory reports are displayed either for a single PC, a selected department, condition-based "Dynamic Groups" or for the full enterprise. A Contracts module is also provided to record both leases and maintenance contracts associated with any devices and peripherals, including supplier details, contract term dates and costs.

Hardware Inventory updates are configured to run at different time intervals throughout the day or at start-up and can be refreshed instantly on demand. A standalone inventory component is available to run on non-networked or mobile devices and in addition, high value peripherals can also be associated and recorded against a device.

1. Click the **Hardware Inventory** icon in the ribbon. The Hardware Inventory window will appear.

Note: If the component icons are not visible, click the Home tab.



In the PCs Tree view, select the level at which you want to view the Hardware information: company, department, AD Container, Dynamic Group or individual Agent.

Note: A focused Hardware Inventory will be displayed for PCs in the Discovered Tree view.

The information window will display a breakdown for each selected item in graph and list format. To view the graph in a different format, click the **Chart** icon drop-down arrow on the ribbon and select the appropriate format. To print the active view, click the  icon at the top of the Console.

Note: Clicking the **Chart** icon in the ribbon will hide/show the graph.

You can switch between which hardware component is displayed by clicking on the appropriate icon in the Filter section of the ribbon.

The listed descriptions can be expanded to provide an individual Agent breakdown for each item; these can be exported or printed if required. When viewing at Agent level in the Tree view, a complete Hardware Inventory for that PC is displayed. Any values that are not displayed or are incorrect can be edited. Click the **Hardware Inventory** drop-down arrow and select {Edit Values} from the menu or select the **Edit Values** icon in the ribbon.

To view any leasing or maintenance contracts that have been associated with devices, click the **Hardware Inventory** drop-down list and select {Display - Contracts} icon or click the **Contracts** icon in the Hardware Inventory section of the ribbon.

The frequency at which the server collects data can be adjusted using the NetSupport DNA settings option.

A quick refresh facility is available if you know the Inventory for a particular Agent or department is out of date. Right-click on the required item in the Tree view and select **Update** or click **Update** in the Hardware Inventory drop-down menu or ribbon.

If an error message relating to the 16-bit MS-DOS subsystem appears, please refer to the NetSupport Technical Support website www.netsupportsoftware.com/support for further guidance.

Queries
Select the Queries tab to display the Queries window.

NetSupport DNA's Query tool enables you to interrogate the database for records matching specified criteria. Queries specific to the component currently being viewed will be listed, enabling fast retrieval of the results.

Click the **Add Query** icon in the ribbon to create a new query or click the **Edit Query** icon in the ribbon to edit an existing item in the list.

Reports
Select the Reports tab to display the Reports window.

A number of pre-defined management reports, powered by the Crystal Reports engine, are attached to each component. Select the required report from the drop-down list. The results will be listed in the information window. These can be exported if required.

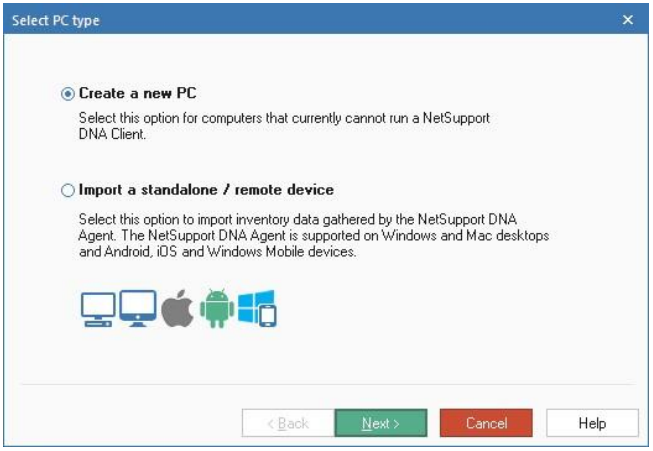
Gather Inventory Data For Remote Users or Non Scanned Devices

In order to maintain accurate asset information, it is vital that all user, hardware and software related data is recorded. Whilst the NetSupport DNA Server will dynamically retrieve information from those machines that have an Agent installed, you will probably have instances where items cannot be found. You may have users in remote offices that aren't attached to the network and you will probably purchase peripheral equipment such as routers, webcams etc.

To ensure this information is known, NetSupport DNA provides you with the tools to gather data for remote/standalone PCs and to log details of peripheral devices.

Add Non Standard Hardware

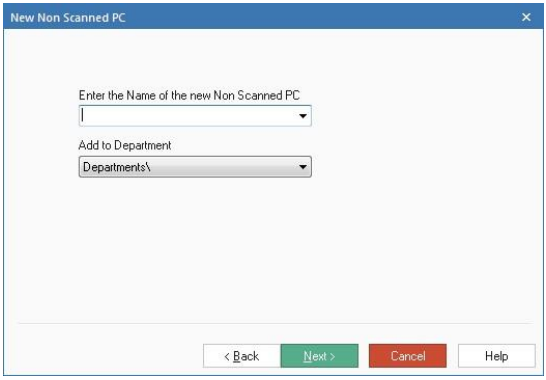
1. Click the **Hardware Inventory** icon drop-down arrow and select {Add Computers} from the menu.
   Or
   Click the **Add Computers** icon in the Hardware Inventory group.
2. Choose one of the two available options and click **Next**.



Create a new PC

Select this option to associate a non-scanned item of hardware/peripheral device with a department.

Adding non-scanned devices
Enter the name of the PC/device to be added and select the department to associate the item with.



Click **Next**.

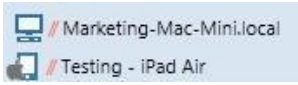
Before the new item is added to the Tree view, select one of the following options:

Add Hardware Peripherals to a PC
You can simply add the new hardware to the Tree as a standalone item, or you can associate additional equipment with it, thus creating a 'mini' hardware inventory page for the device.

Create more PCs
Enables you to repeat the process for other non-scanned items.

Finish
Adds the new item to the Tree view and returns you to the Hardware Inventory window.

Non-standard items are easily identified in the Tree view, each being prefixed with //.



Import a Standalone/Remote device

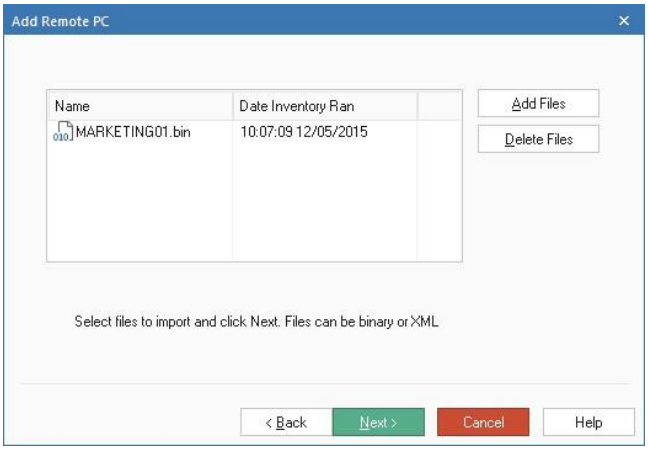
Select this option to add inventory data for a remote or standalone device.

This utility enables you to import the Hardware/Software Inventory for 'standalone' PCs that cannot be found dynamically by NetSupport DNA.

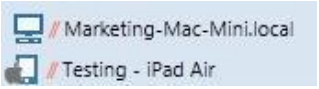
Obtaining inventory data from Windows machines
The file DNAInv.exe (installed in the NetSupport DNA program folder) is run at the remote PC which in turn creates a BIN file containing the Inventory data. The Operator imports the BIN file into NetSupport DNA and the User, along with their associated Hardware and Software Inventory data is added to the Console.

1. Copy the file **DNAInv.exe** from c:\program_files\netsupport \netsupport_dna\dna\console\ and send/email/transport it to the required user(s).
2. Run the file at the required machines. The Inventory data is recorded in a new file '**machine_name.BIN**' which should be returned to the operator/administrator.
3. Upon receipt, the operator should copy the BIN file to a suitable location ready to import the recorded Inventory data.

Importing the data
1. Click the **Hardware Inventory** icon drop-down arrow and select {Add Computers} from the menu.
   Or
   Click the **Add Computers** icon in the Hardware Inventory group.
2. The Select PC Type dialog will appear. Select **Import a Standalone/ Remote PC** and click **Next**.
3. The Add Remote PC dialog will appear.



4. Click **Add Files** and browse for the BIN files. As you select each file, they will be added to the dialog.
5. Click **Next**. The Inventories for each displayed machine will be imported and the User details added to the Tree view.

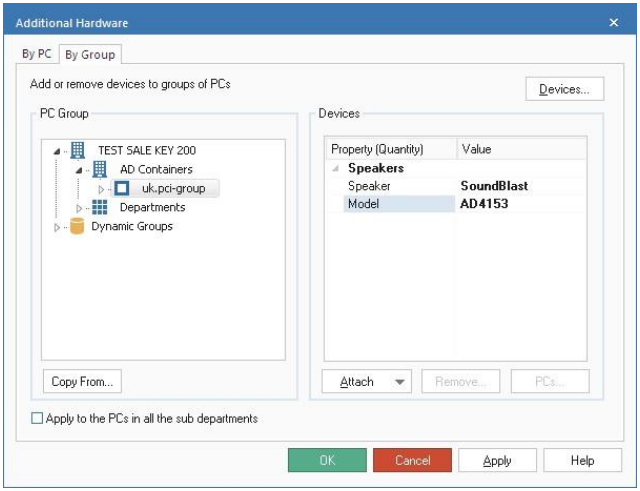


6. Click **Finish** to end the process or to import another Inventory click **Create another PC**. If required, you can also add peripheral hardware items to the new record.

Add Hardware Peripherals

All peripheral/non-scanned hardware needs to be recorded in order to maintain an accurate asset log. NetSupport DNA enables you to manually associate details of these components with their respective 'owners'. Devices can be associated to individual PCs or to groups.

1. You can add a peripheral device when creating a new 'non-scanned' hardware record.
   Or
   To associate the device with an existing item in the Tree view, ensure the hardware component is selected and right click on an Agent, department, AD container, dynamic group or the company and select **Peripherals**.
   Or
   Click the **Hardware** icon drop-down arrow and select {Peripherals - Add} from the menu.
   Or
   Click the **Peripherals** icon in the Hardware Inventory group.



Add peripherals by PC

1. Select the By PC tab and in the Tree view, select the PC to associate the hardware with.
2. Click **Devices** to create a new device. Once created, the device will be displayed in the **Attach** drop-down list. Select the required device from the list to associate with the PC.

3. Enter the device values (for example, the specific make/model of the device) that will be listed on the Hardware Inventory.
4. Click **Apply**.
5. Devices can be copied from one PC to another; click **Copy From** and select the PC to take the data from. All devices attached to that PC will be copied over.
6. You can add further devices by repeating the process or click **OK** when complete. To remove an item currently attached, select the required device and click **Remove**.

Add peripherals by group

1. Select the By Group tab and in the Tree view, select the department or Dynamic Group to associate the hardware with.

   Note: You can include all Agents within the selected department by checking **Apply to the PCs in all the sub departments**.

2. Click **Devices** to create a new device. Once created, the device will be displayed in the **Attach** drop-down list. Select the required device from the list to associate with the PC.
3. Enter the device values (for example, the specific make/model of the device) that will be listed on the Hardware Inventory.
4. Click **Apply**.
5. Devices can be copied from one group to another; click **Copy From** and select the group to take the data from. All devices attached to that group will be copied over.
6. You can add further devices by repeating the process or click **OK** when complete.

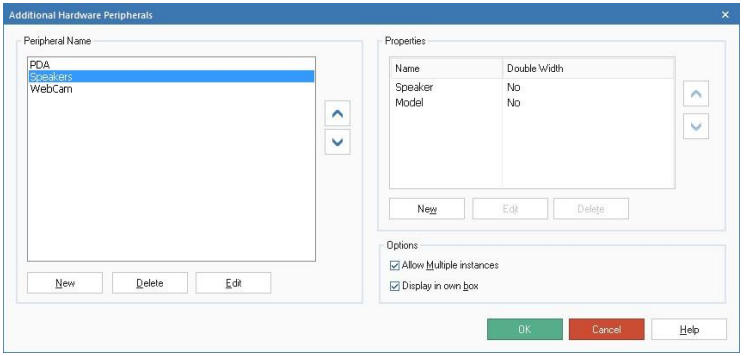
   Note: To view which PCs have been associated with a device, select the required device and click **PCs**.

7. To remove a device, click **Remove**, select the group that the device is to be removed from and then select the required device, click **OK**. The device will be removed from all PCs in the selected group.

Additional Devices

Use this dialog to compile a register of non-scanned hardware devices along with their associated properties. Listed items can then be associated with Agents or non-scanned peripheral equipment.

1. You can create a new device when adding peripheral equipment to an existing record in the Tree view.
   Or
   You can prepare a list of devices in advance, click the **Hardware Inventory** icon drop-down arrow and select {Peripheral Management} from the menu. These can then be attached at a later date.



Peripheral Name

New
Click **New** to add a device to the list. The list can be sorted by clicking the arrows.

Edit
Change the name of an item in the list.

Delete
Removes the device from the list and from any hardware inventories that it may appear on.

Options

Allow Multiple instances
If checked, enables you to associate multiple instances of the device with a user's inventory. For example, two digital cameras but with different make/model numbers.

Display in own box
If checked, each instance of the device will be listed in a new box on the hardware inventory page. However, if there are multiple instances of the same device, you may prefer to group them together in the same box.

Properties

You can edit the properties of the new item and associate additional items with the device dependant on how much related information you need to record.

New
Associates additional items with the primary device. Click **New** and enter the device name. Depending on how much information will be entered, you can provide a double width field. Click **OK**.



Use the arrow keys to arrange the devices into the order you want them displayed on the inventory page.

Edit
Enables you to edit the properties of a device.

Delete
Removes a device from the list and from any inventories that it may be attached to.

When all details are entered, click **OK**.

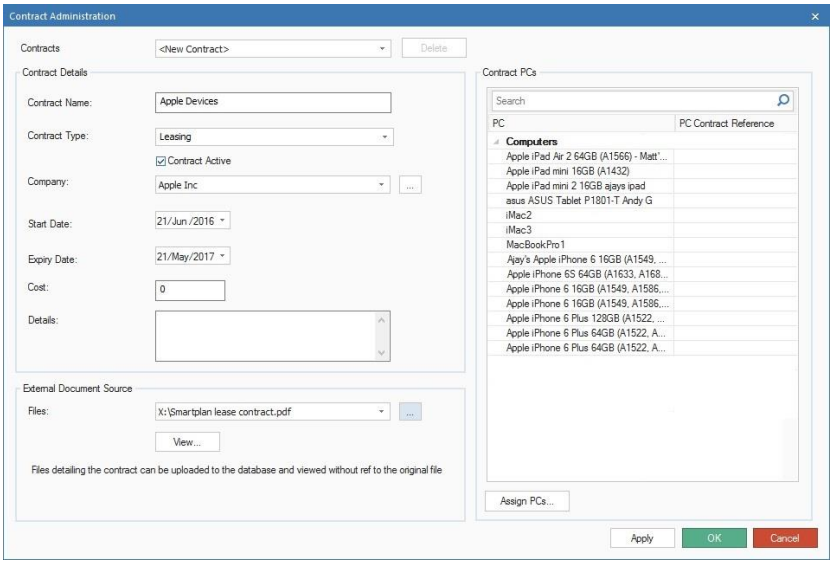
Contract Manager

NetSupport DNA allows you to record leasing/maintenance contracts associated with any devices and peripherals. Once a contract has been created, it can be assigned to any number of devices. Documents relating to the leasing/maintenance contract can be attached, allowing you to keep all information relating to the contract in one place. The contract information is then displayed for the device in the User Details dialog and the Hardware Inventory information window.

Note: If you are upgrading from a previous version of NetSupport DNA and have associated leasing/maintenance details with PCs, these details will be transferred over and displayed in the Contracts field. You will need to assign these to the appropriate PCs.

Adding a new contract

1. Click on the **Hardware Inventory** icon drop-down arrow and select {Contracts} from the menu.
2. The Contract Manager dialog will appear. Existing contracts can be viewed by selecting them from the **Contracts** drop-down list.



3. Enter the name for the contract.
4. Select the contract type from the drop-down list - **Leasing** or **Maintenance** - and choose whether the contract is active.

5. Supplier details can be associated with the contract. To create a new company record, click  in the **Contracts Details** section. The Companies dialog will appear, allowing you to enter the details for the company. Existing companies can be selected from the **Company** drop-down list.
6. Enter the start and expiry dates, cost and any other information relating to the contract.
7. To attach files to the contract (PDFs, emails, Word documents, etc.), click  in the **External Document Source** section. The External Documents dialog will appear, allowing you to browse and add files. You can see which files are already attached to the record by clicking the arrow to view the drop-down menu list.
8. To associate PCs with this contract, click **Assign PCs** and, from the Tree view, select the required devices.

   Note: You can quickly search for devices by typing in the Search box and clicking  .
9. Click **Apply** to save this record.

Note: To delete a contract record, select the required contract from the **Contracts** drop-down list and click **Delete**.

Software Inventory

The Software Module is designed to help organisations manage licence compliance and reduce software overspend by accurately reporting installed software and proactively identifying PCs with software that has no or low usage.

A detailed summary of all programs and applications installed on each PC is provided, including Windows 8 and 10 store apps. NetSupport DNA can display the information for a selected PC, a department or a custom group and features an extensive module for assigning and tracking licence use. The NetSupport DNA software licence module supports the ongoing management of all software licences for each department – recording suppliers, purchase and invoice details, department or cost centre allocation and the tracking of maintenance contracts as well as storing PDF copies of any supporting documents.

The data can be viewed in the information window in a variety of formats:

Programs
Provides a list of installed programs as displayed in the Agents Add/Remove programs dialog. Licence levels can be managed in the Program Manager dialog.

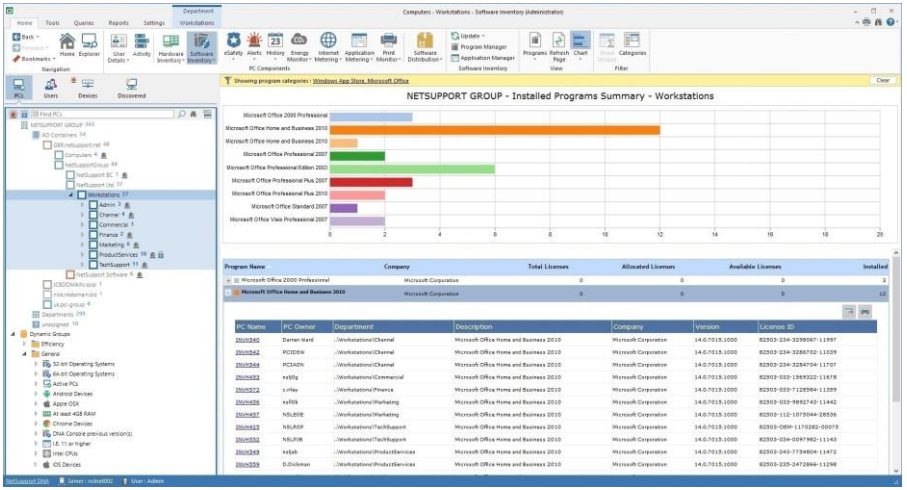
Applications
Provides a much more detailed view of applications installed by displaying all executable files that have been found on each PC.

Files
Allows you to extend the search to include additional file types (such as GDPR files), if required.

Hotfixes
Provides you with a list of hotfixes that have been installed on each PC.

1. Click the **Software Inventory** icon in the ribbon. The Software Inventory window will appear.

   Note: If the component icons are not visible click the Home tab.



In the Tree view, select the level at which you want to view the displayed data: company, department, AD Container, Dynamic Group or individual Agent.

You can toggle between Programs, Applications, Files and Hotfixes by clicking the Software Inventory drop-down arrow and selecting {Display - Programs/Applications/Files/Hotfixes} or clicking the appropriate icon in the ribbon.

A breakdown of the data will be displayed in graph and list format for the selected company or department. To view the graph in a different format, click the **Chart** icon drop-down arrow on the ribbon and select the appropriate format. To print the active view, click the  icon at the top of the Console.

Note: Clicking the **Chart** icon in the ribbon will hide/show the graph.

Software Inventory enables you to easily monitor licence usage and highlight any potential licensing issues. The number of licences purchased for each program can be logged using the Program Manager dialog and detailed license information is displayed when viewing **Programs**. Each description can be expanded to provide details of Agent PCs that have the application installed.

Note: Licence information will only show in the **Applications** view if the application group has been assigned to the installed Program in the Edit Application Group dialog.

When viewing applications, the application list can be refined if you find that multiple entries for the same software are being recorded. For example, different versions of the same product. For example, different versions of the same product. Using the Application Groups option, you can merge items into a single record. In these circumstances, the 'quantity' totals may not appear to provide a true reflection of how many PCs are running certain applications, as Agents that have more than one item in the merged group will be counted as multiple entries. In order to provide a unique figure, click the **Show Unique** icon in the ribbon.

Note: Installed Programs can also be merged using the Programs Manager. Programs that have been merged will display as the 'Merged Group' at company and department levels in the hierarchy but show as the original program at PC level.

A useful way of viewing specific programs and applications and limiting the amount of data displayed is to group 'similar' items together into categories. See Application Groups or Installed Programs Manager for more information. To display a category, click the **Categories** icon, select the required group to view and click **OK**. The information window will display data just for that category. A yellow header will be displayed advising what category you are viewing; you can switch categories and clear categories from here.

By default, NetSupport DNA scans Agents' PCs for executables but you can include additional file types (such as GDPR files, image files and custom file extensions), if required. Use the NetSupport DNA Software Inventory settings option to specify which other files should be included in the search. The results can be viewed by clicking the **Files** icon in the Software Inventory ribbon.

When viewing files, you can filter what types of files are displayed in the information window. Select the Types icon in the ribbon and select the file types to display from the list. You can quickly include/exclude GDPR and image files by selecting the appropriate option. Click **OK**. A yellow header will be displayed advising what file types you are viewing. Click **Clear** to revert back to all file types.

Note: File types will only appear in the File Types list if they have been configured in the Software Inventory settings.

The frequency at which the server collects data can be adjusted using the NetSupport DNA settings option.

A quick refresh facility is available if you know the Inventory for a particular Agent or department is out of date. Right-click on the required item in the Tree view and select **Update** or click **Update** in the Software Inventory drop-down menu or ribbon.

Queries
Select the Queries tab to display the Queries window.

NetSupport DNA's Query tool enables you to interrogate the database for records matching specified criteria. Queries specific to the component currently being viewed will be listed, enabling fast retrieval of the results.

Click the **Add Query** icon in the ribbon to create a new query or click the **Edit Query** icon in the ribbon to edit an existing item in the list.

Reports
Select the Reports tab to display the Reports window.

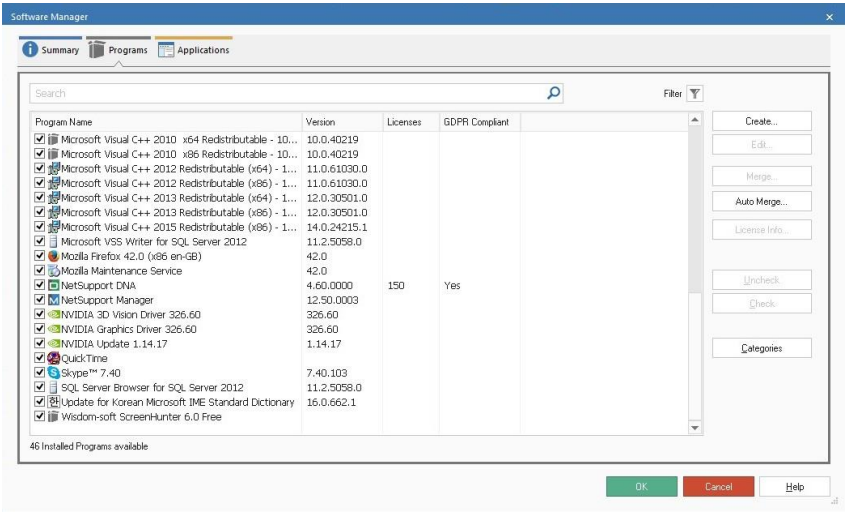
A number of pre-defined management reports, powered by the Crystal Reports engine, are attached to each component. Select the required report from the drop-down list. The results will be listed in the information window, these can be exported if required.

Installed Programs Manager

This dialog displays the installed programs discovered from the Programs and Features list on Agents' PCs. You can customise the content to make the list more manageable. From here, you can decide what options are included in the inventory, merge multiple versions of the same software into one record and manage licence levels.

1. Click the **Software Inventory** icon drop-down arrow and select {Programs Manager} from the menu.
   Or
   Click the **Programs Manager** icon in the Software Inventory group.
2. The Software Manager dialog will appear. Select the Programs tab.
3. The installed programs will be displayed, along with the number of licences held (if recorded) and if the program is GDPR compliant. The check box alongside each program indicates if it is included in inventories or not.

Note: You can mark a program as GDPR compliant in the Program Details dialog.



You can quickly locate a particular program by typing in the search box.

To make the list more manageable, you can filter the programs that are displayed. Click  and the Installed Program Filter dialog will appear. From here, you can choose what program groups are to be displayed.

Program categories can be created, enabling you to group similar programs. The Software Inventory window allows you to display programs by group rather than listing 'all' items, making it easier to track specific records.

If an installed program is not listed, you can create a new program and link it to the relevant application group by clicking **Create**.

Note: If the required installed program is not displayed, ensure that the PC with the software program installed has connected to the DNA Server.

Multiple versions of the same product can be merged into a new installed program group. Select the required items, using Shift-Click or Ctrl-Click, and click **Merge**. To unmerge programs, select the required group and click **Edit**.

Note: You can automatically merge programs which have similar names. Click **Auto Merge** and a dialog will appear. To merge existing installed programs, click **Auto Merge Now**. By default, new programs will be automatically merged. To switch this off, uncheck **Activate Auto Merge**.

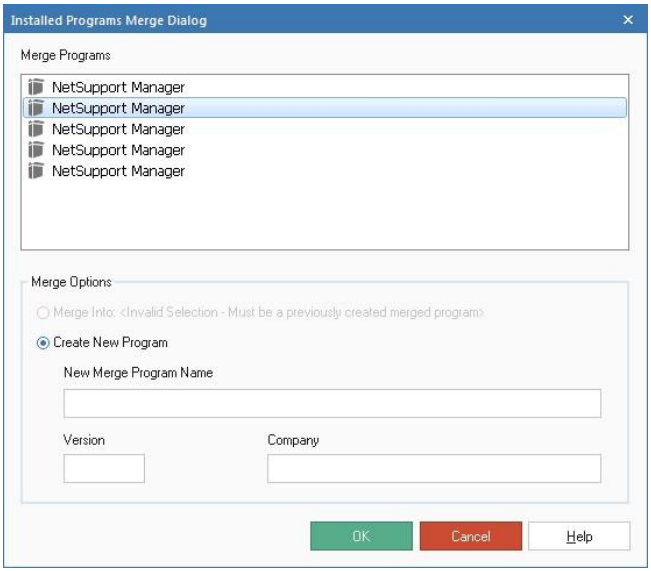
To manage the licence information for a program, select the required program and click **Licence Info**.

If you are upgrading from a previous version of NetSupport DNA (below version 3.00) and you have licences allocated against Application Groups, the Convert Licences wizard will appear, allowing you to assign your licences to the new Installed Programs dialog.

Merge Installed Programs

This dialog enables you to merge multiple versions of the product into a single group - ideal for tracking different versions of the same software. The programs that you are merging will be displayed.

Note: Programs should only be merged if they are effectively the same product, i.e. NetSupport Manager 10.01 and NetSupport Manager 10.02. The merged installed programs will be treated as the same product for licensing purposes. Grouping together different products will give unpredictable results and may adversely affect licensing.



Merge Options

Merge into 'xxxxxxxxxxx'
The new program will be merged into a previously created merged group. Click the appropriate name from the list to select.

Create New Program
Alternatively, enter a new name for the group.

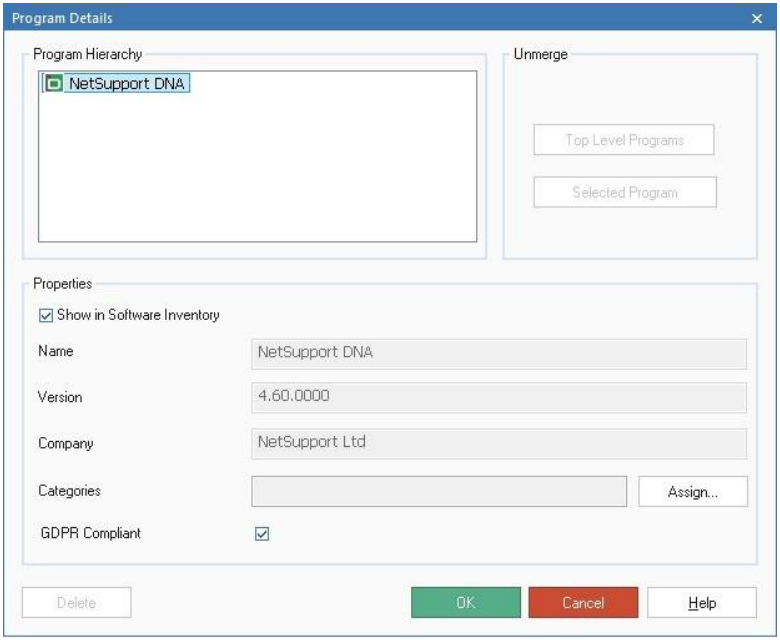
Version
Enter the version for the program if required.

Company
Enter the company name if required.

Click **OK** to create the new group. The programs can be un-merged at a later date if required.

Edit Installed Programs

This dialog displays the properties of an installed program. If the item is a merged group, all programs in the group will be listed. Installed programs that have been merged can be separated here if required.



Unmerge

Top Level Programs
All programs in the group will be unmerged.

Selected Program
The selected program will be separated from the group.

Note: Licences will be returned to the original program when the group is unmerged. Any licences allocated to the group after it was merged will need to be manually reallocated to the correct installed program.

Properties

Displays the properties for the program. The name, version and company details can only be edited for a merged group.

Show in Software Inventory
Enables you to limit the number of items listed in Software inventories. If un-checked, the program will be removed from the list of displayed items.

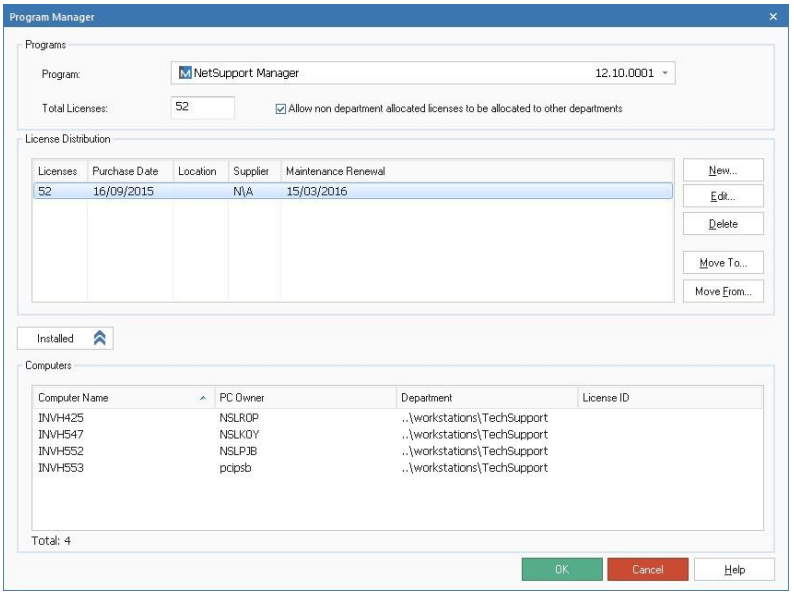
Categories
Allows you to assign the program to a category. Click **Assign** and the Program Categories dialog will appear.

GDPR Compliant
Allows you to confirm if the program is GDPR compliant.

Installed Programs Licence Management

NetSupport DNA allows you to record licence information against each installed program. Full licence information such as purchase details, third-party details and maintenance details can be recorded in the Licence Information dialog. Licences can also be allocated to departments. Any licences not allocated will be available for all departments that have not already been allocated licences.

Note: To stop unallocated licences from being allocated to other departments, uncheck **Allow non department allocated licences to be allocated to other departments**.



To record licence information against a program, select the required program from the Program drop-down list. Click **New.** The Licence Details dialog will appear: enter the required details. To amend licence information, select the current record and click **Edit**.

If you have recorded the licence information against the incorrect application, you can move the licence information to the correct application. Click **Move To** and select the correct application from the list to transfer the licence information to a different program. Click **Move From** to transfer licence information from another application.

Click **Installed** to view details of where the licences are installed.

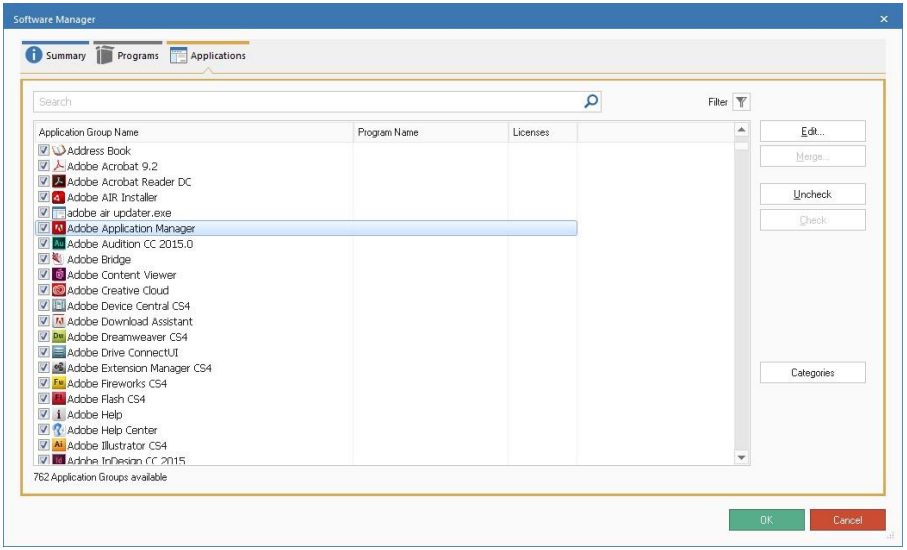
Application Groups

Although Software Applications will include all scanned applications by default, you can customise the content to make the list more manageable. The Application Groups option enables you to pick and choose which items are included in the inventory and merge multiple versions of the same software into one record.

The groups can also be accessed in the Application Metering option.

1. Click the **Software Inventory** icon drop-down arrow and select {Application Manager} from the menu.
   Or
   Click the **Application Manager** icon in the Software Inventory group.
2. The Software Manager dialog will appear. Select the Applications tab.
3. Applications found on all Agent PCs will be listed and, if recorded, the number of licences held. The check box alongside each application indicates if it is included in inventories or not.

Note: The licence information will only be displayed if the application has been assigned to the Installed Program in the Edit Application Group dialog and the licence information has been set up in the Installed Program Manager.



You can quickly locate a particular application by typing in the search box.

To make the list more manageable, you can filter the applications that are displayed. Click ; the Applications Group Filter dialog will appear. From here, you can choose what groups are to be displayed.

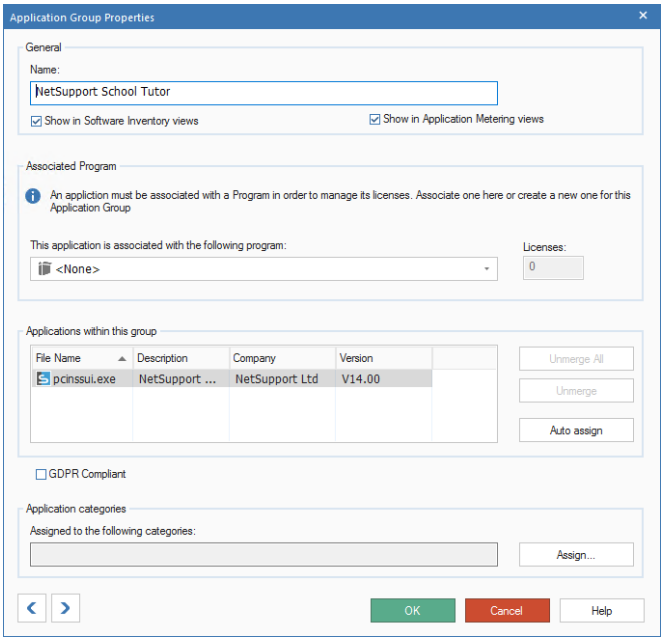
Application group categories can be created, enabling you to group similar applications. The Software Inventory and Application Metering windows allow you to display applications by group rather than listing 'all' items, making it easier to track specific records. Click **Categories**.

To change the properties of an application, select the item in the list and click **Edit**.

Multiple applications can be merged to make a new Application Group. Select the required items, using Shift-Click or Ctrl-Click, and click **Merge**.

Edit Application Group

This dialog enables you to edit the properties of an Application Group.



General

Name
Displays the name of the selected application. You can change the listed description for any item, if required.

Show in Software Inventory views
Enables you to limit the number of items listed in Software inventories. If un-checked, the application will be removed from the list of displayed items.

Show in Application Metering views
If un-checked, the application will be removed from the Application Metering and Activity information window.

Associated Program

Enables you to link the application with the installed program entry, allowing any licence information to be displayed. Licences can be managed in the Installed Programs Manager.

Note: The application must be linked with the installed program for the licences to be displayed.

Applications within this group
Displays any other applications that are included with this group.

Unmerge/ Unmerge All
Applications that have been merged can be separated if required.

Auto assign
Allows you to create descriptions/keywords that, if matched, will automatically add an application to this group.

GDPR Compliant
Allows you to confirm if the application is GDPR compliant.

Application categories

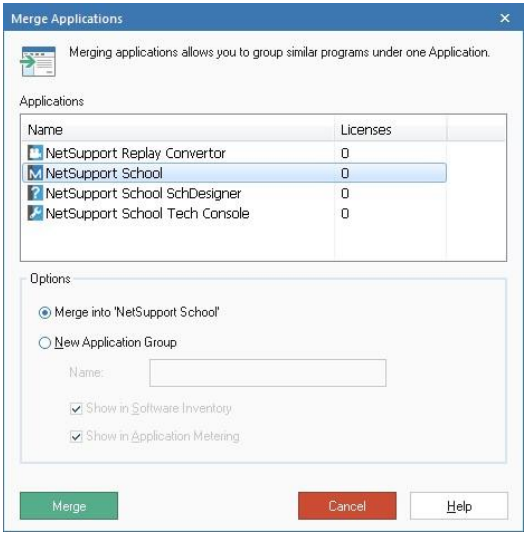
Allows you to assign the application to a category. Click **Assign**; the Application Group Categories dialog will appear.

Note: For an application to appear as subscription software in Efficiency View, you need to assign it to the Subscription Software category

Use  to scroll backwards or forwards through each item displayed in the Applications Groups dialog.

Merge Application Groups

This dialog enables you to merge multiple applications into a single group. Ideal for tracking different versions of the same software.



Merge into 'xxxxxxxxxxx'
The new application group can be allocated the name of one of the listed items. Click the appropriate application from the list to select.

New Application Group
Alternatively, enter a new name for the group.

Show in Software Inventory
If un-checked, the new application group will not be listed in the Software Inventory.

Show in Application Metering
If un-checked, the application group will be removed from the Application Metering Information window.

Click **Merge** to create the new group. The applications can be un-merged at a later date if required.

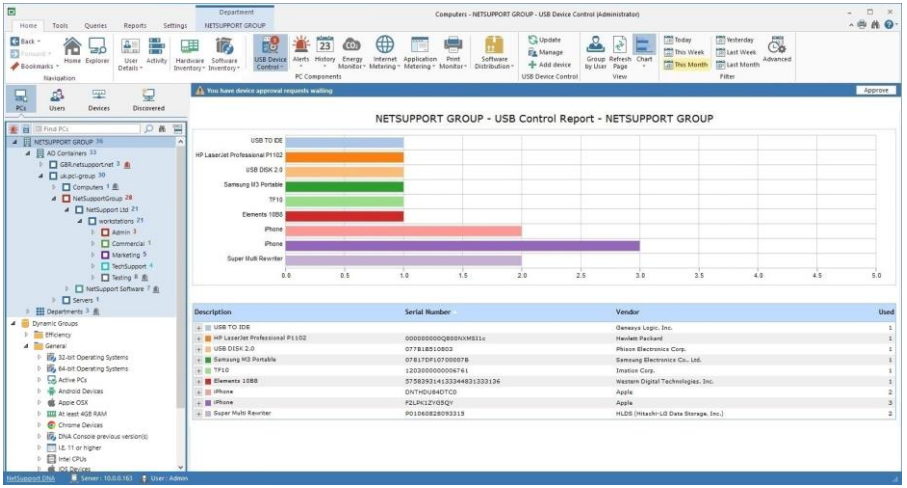
USB Device Control

NetSupport DNA provides a simple and effective solution for managing the use of USB memory sticks to help maintain the security of the network. The use of memory sticks can be controlled across the entire enterprise or, just for specific departments and usage, can be set to allow full access, block all access, allow read-only or prevent applications being run from a memory stick. Alternatively, individual memory sticks can be "authorised" in NetSupport DNA and the use of sticks in the enterprise can also be limited to only those authorised.

A program administrator can connect a memory stick to their local PC and then authorise its use within the DNA console for either a given department or a specific user. When authorising for a user, the approval can be restricted for a limited amount of time. Users who connect an unauthorised memory stick to their PC can also request remote authorisation where appropriate. Not only does NetSupport DNA identify both removable (memory stick) and portable (mobile phone, tablet, camera) storage devices, it also provides similar usage controls over CD/DVD devices (including USB and virtual).

1. Click on the **USB Device Control** icon in the ribbon. The USB Device Control window will appear.

Note: If the component icons are not visible, click the Home tab.



In the Tree view, select the level at which you want to view the data: company, department, AD container, Dynamic Group or individual Agent.

The information window will display a breakdown for each selected item in graph and list format. To view the graph in a different format, click the **Chart** icon drop-down arrow on the ribbon and select the appropriate format. To print the active view, click the icon at the top of the Console.

Note: Clicking the **Chart** icon in the ribbon will hide/show the graph.

You can view data for a specified period. To switch between different time periods, click the appropriate icon in the Filter section of the ribbon. Clicking **Advanced** allows you to apply a customised date/time filter. Listed descriptions can be expanded to provide an individual Agent breakdown for each item.

The working hours shown can be amended to suit your organisation in the DNA Configuration dialog. See Console Preferences - General for further information.

Selecting **Group by User** allows you to view device usage based on Agents' user IDs and not the PC. This option will not be available in the Users tree view.

Selecting **Group by PC** allows you to view device usage based on the PC details and not the Agent user's details when in the Users tree view. This option will not be available in the PCs tree view.

Note: By default, USB Device Control is disabled. You can enable this in the DNA Configuration - USB Device Control settings and also preset the level of access for different types of devices.

When an Agent inserts a device into their machine, they will be asked if they want to register the device. The Console Operator will then be notified that an approval request is required; a notification icon will be displayed at the top of the **USB Device Control** icon and in the information window. You can then manage the approval requests.





Note: USB device requests will also be displayed in the Tree view. You can toggle these on/off by clicking .

Devices can be registered and approved for departments or users before they are given to users. Click the **USB Device Control** icon drop-down arrow and select {Add Device} or click the **Add Device** icon in the ribbon. Insert the device to be registered. The USB Device Details dialog will appear, allowing you to register the device.

The frequency at which the server scans for devices can be adjusted using the NetSupport DNA settings option.

Queries
Select the Queries tab to display the Queries window.

NetSupport DNA's Query tool enables you to interrogate the database for records matching specified criteria. Queries specific to the component currently being viewed will be listed, enabling fast retrieval of the results.

Click the **Add Query** icon on the ribbon to create a new query or click the **Edit Query** icon in the ribbon to edit an existing item in the list.

Reports
Select the Reports tab to display the Reports window.

A number of pre-defined management reports, powered by the Crystal Reports engine, are attached to each component. Select the required report from the drop-down list. The results will be listed in the information window. These can be exported if required.

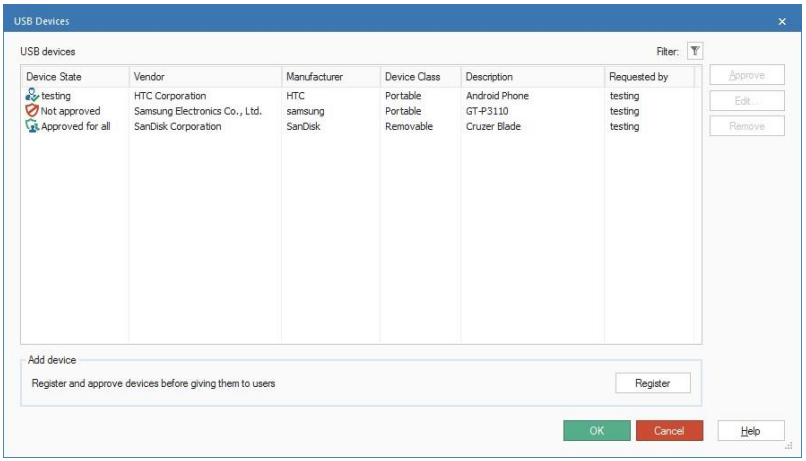
Registering USB Devices

When USB Device Control is enabled and an Agent inserts a USB device into their machine, if it has not already been pre-approved, the Agent will be advised that the device is blocked and asked if they want to request access for it. Console Operators will be notified of any approval requests in the Console.

To manage approval requests

1. Click the **USB Device Control** icon drop-down arrow and select {Manage}.
   Or
   Click the **Manage** icon in the ribbon.
   Or
   In the approval notification in the information window, click **Approve**.
2. The USB Devices dialog will appear. A list of all USB devices will be displayed showing the device state and details.

Note: You can filter the USB devices that are displayed by clicking the **Filter** icon and selecting what device state you want to see.



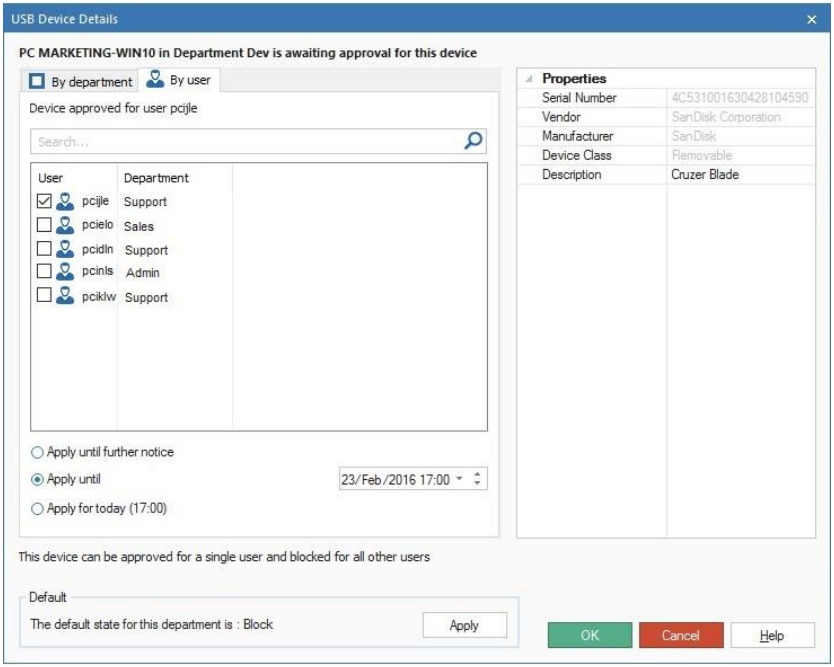
3. Select the device that is waiting for authorisation and click **Approve** to authorise the request.
4. To edit existing devices, click **Edit**.
5. To remove a device, click **Remove**.

Add USB device
USB devices can be pre-approved before they are given to users.

1. Click the **USB Device Control** icon drop-down arrow and select {Add Device}.
   Or
   Click the **Add Device** icon in the ribbon.
   Or
   Click **Register** from the Manage Device dialog.
2. Insert the USB device into a port to register it.
3. The USB Device Details dialog will appear, allowing you to authorise the device for departments or individual users.

USB Device Details

This dialog allows you to approve USB devices for departments or individual users.



The properties for the device you are approving will be displayed. The description can be amended by overtyping in the description field.

Select the By department tab and check which departments this device is to be approved for - or, to authorise for individual users, select the By user tab and check the users to approve the device for. Uncheck departments or users that you do not want the device to be approved for.

You can quickly search for users by typing in the Search box and clicking  . When approving by user, you have the option to apply the approval until further notice or restrict the approval for a limited amount of time.

The default state for the current department will be displayed. To apply this for the current device, click **Apply**.

eSafety

NetSupport DNA helps enhance your school's safeguarding policy with the Keyword and Phrase Monitoring feature, which provides insight into and alerts from any activity by a student that might suggest the child is engaged in activity that would place them at risk. Each time a phrase is triggered, a risk analysis is performed and a risk index score allocated, allowing safeguarding staff to easily see which triggered phrases pose the highest risk. Additionally, the "Report a Concern" feature allows students to report concerns, via a DNA Agent machine or website*, directly and discreetly to nominated school staff. They are alerted instantly, allowing them to track the concern and record any follow-up actions directly from within NetSupport DNA.

Note: The eSafety feature is only available in the Education Edition of NetSupport DNA.

1. Click the **eSafety** icon in the ribbon.

   Note: If the component icons are not visible, click the Home tab.

There are three modes available within eSafety:

Phrase Monitoring

Report a Concern

Risk Analysis

To switch between Phrase Monitoring, Report a Concern and Risk Analysis mode, click the **Phrases**, **Concerns** or **Risk Analysis** icon in the ribbon.

Notes:

- eSafety data can also be viewed in the Cloud Console, which allows safeguarding staff to access the data on any device when away from the local network.
- * Before your nominated Safeguarding Users can receive student concerns reported via the website option, the Cloud Console must be enabled.

Safeguarding Roles

NetSupport DNA provides two predefined safeguarding roles: Safeguarding Administrator, which allows the user full access to the eSafety functions; and Safeguarding User, which allows the user to see and manage concerns assigned to them and view any phrases that have been triggered. Access to concerns is restricted to safeguarding roles, preventing other console users from them.

Notes:

- The safeguarding roles will only allow access to the User Details, Activity, Internet Metering and eSafety components.
- These roles can only be assigned in the Safeguarding User dialog, not when you are creating a Console Operator.
- A Safeguarding Administrator does not have access to the eSafety settings.

Assigning safeguarding roles

1. Click the **eSafety** icon in the ribbon.
2. Select the **eSafety** icon drop-down list and select {Safeguarding Users}.
   Or
   Click the **Safeguarding Users** icon in the ribbon.
3. Click **Add** to create a new contact.
4. The Safeguarding User dialog will be displayed.
5. Select **Create new Console User**, select the required role from the drop-down list and click **Create**.

   Note: You can assign the contact to an existing console user. Select **Associated Console User** and then select a console user from the drop-down list. The console user will also need to have the eSafety access rights enabled in their console role to be able to access the eSafety functions.

Restricting access

Once you have created a Safeguarding Administrator, access can then be restricted so other console users are unable to manage contacts.

1. Click the **eSafety** icon in the ribbon.
2. Select the **eSafety** icon drop-down list and select {Safeguarding Users}.
   Or
   Click the **Safeguarding Users** icon in the ribbon.
3. The Configure Safeguarding Users dialog will be displayed.
4. Select the **Restrict access to Safeguarding Admin users** option.

Note: Only a Safeguarding Administrator can enable this restriction.

Managing Safeguarding Administrators and Users

This dialog displays the users that have been created for students to report a concern to and that can respond to triggered phrases. From here, you can add new, edit existing users and select which users are available when defining profiles.

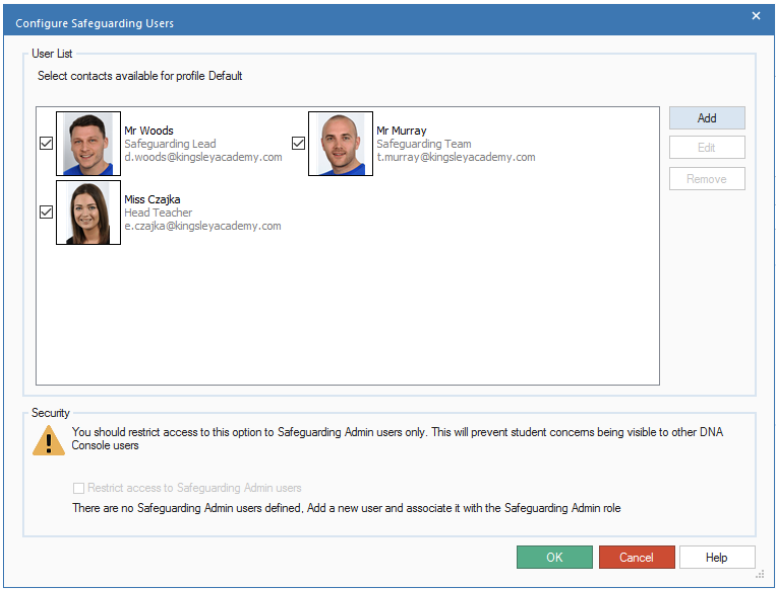
Notes:

- This dialog will only be available if Report a Concern has been enabled in the DNA Configuration - Report Concern settings.
- When accessing this dialog from the Report Concern settings, you will be selecting the users available for the current profile. This allows you to assign a different list of users to each profile.

1. Click the **eSafety** icon in the ribbon.
2. Select the **eSafety** icon drop-down list and select {Safeguarding Users}.

   Or

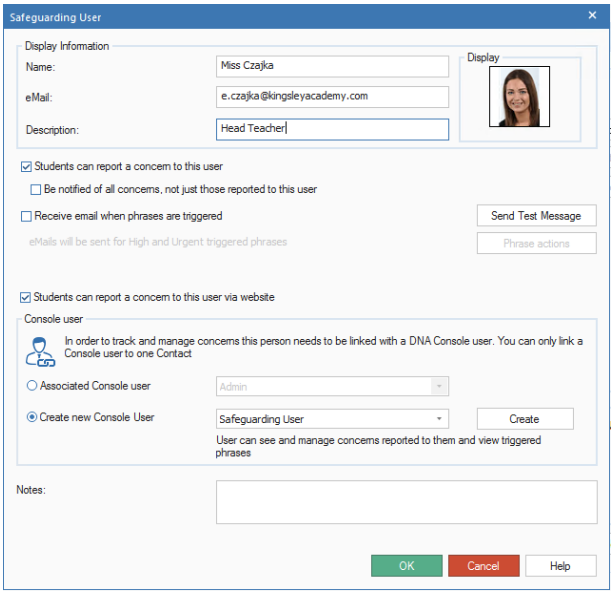
   Click **Safeguarding Users** icon in the ribbon.
3. The Configure Safeguarding Users dialog will appear.



4. Any existing users will be listed.
5. To add a new user, click **Add**.
6. To edit an existing user, click **Edit**.
7. To delete a user, click **Remove**.
8. You can define which users are available when selecting contacts for profiles. Users that are ticked will be available for selection by all profiles. If you do not want a user to be available, clear the tick and that user will no longer appear when accessing this dialog from the Report Concern settings.
9. Access to this area can be restricted to Safeguarding Administrators only, preventing other Console users from managing them. Select **Restrict access to Safeguarding Admin users**. This option can only be enabled if the current logged on user is a Safeguarding Administrator.

Add or Edit Safeguarding Administrators and Users

This dialog allows you to create new users that students can report a concern to and that can respond to triggered phrases, as well as edit existing users.



1. Enter the name, email address and description for the user.
2. Clicking on the display image allows you to add a photo or picture to be associated with the user.

3. Clear the **Students can report a concern to this user** check box if you do not want students to be able to report a concern to the user.
4. You can allow a Safeguarding User to be notified of all reported concerns – select **Be notified of all concerns, not just those reported to this user**. This option is not available for Safeguarding Administrators as, by default, they see all concerns.
5. The user can be sent an email when a monitored phrase is triggered: select **Receive email when phrases are triggered**. By default, emails are sent for high priority and urgent triggered phrases - click **Phrase Actions** to change this. To send a test email to the user, click **Send Test Message**. The email settings must be configured before you can send a test.
6. If you also want this user to receive student concerns that have been reported via a website, select **Students can report a concern to this user via a website**.

   Note: The NetSupport DNA Cloud Console must be activated in order to use this method.

7. The new user will need to be associated with a Console user. Select an existing one from the drop-down list or select **Create new Console User** to create a new Console user. There are two roles to create a Console user from: Safeguarding Administrator, which allows the user full access to the eSafety functions; and Safeguarding User, which allows the user to see and manage concerns assigned to them and view triggered phrases.

   Note: When associating with an existing console user, you need to ensure their console role has sufficient eSafety rights to view concerns. Otherwise, you will need to create a new Console user.

8. If you are creating a new console user, click **Create** and enter a password for the user. By default, the console user will be prompted to change this password the first time they log on and be notified of the password update by email. Clear these options if they are not required and click **OK**.
9. Include any relevant notes.
10. Click **OK**.

Phrase Monitoring

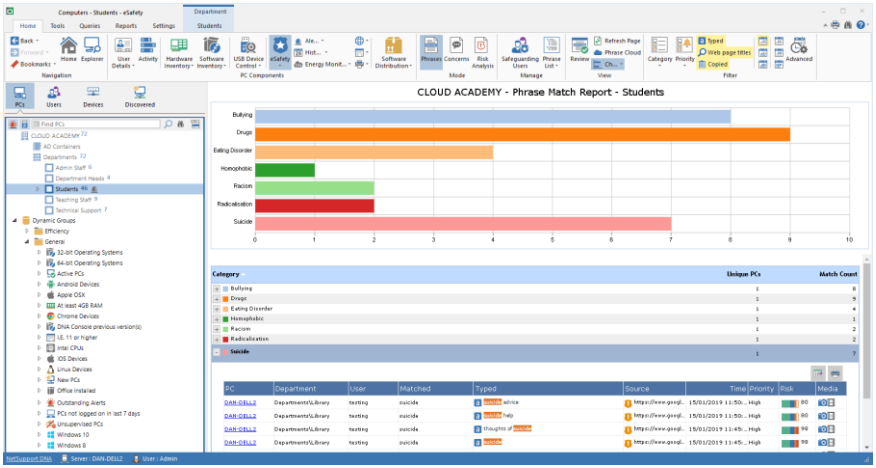
NetSupport DNA's Keyword and Phrase Monitoring feature provides insight into and alerts from any activity by a student that might suggest they are engaged in activity that would place them at risk. Using a database of pre-supplied safeguarding keywords and phrases covering a range of topics from self-harm, bullying and racism through to risks of radicalisation, NetSupport DNA is your eyes and ears, monitoring the school network. The details/context of triggered words can be reviewed, with the results (available as a log, screenshot of the screen, webcam image of the user, or a screen recording, according to severity level and which of these the school activates – features are not available for devices used at home), forwarded to a colleague to follow up on, if required. Each time a phrase is triggered, a risk analysis is performed and a risk index score allocated, allowing safeguarding staff to see which triggered phrases pose the highest risk. An innovative word cloud highlights trending topics across the school to help you put incidents into a broader context.

Note: Students can be marked as vulnerable, allowing Safeguarding Users to easily identify and provide support to them. You can mark students as vulnerable when editing user details or by right-clicking the Agent in the Users Tree view. They will then be displayed in the appropriate dynamic group in the Users Tree view.

1. Click the **eSafety** icon in the ribbon.

   Note: If the component icons are not visible, click the Home tab.

2. Select the **Phrases** icon in the ribbon.



In the Tree view, select the level at which you want to view the metering data: company, department, AD container, Dynamic Group or individual Agent.

The information window will display a breakdown for each selected item in graph and list format. To view the graph in a different format, click the **Chart** icon drop-down arrow on the ribbon and select the appropriate format. To print the active view, click the  icon at the top of the Console.

Note: Clicking the **Chart** icon in the ribbon will hide/show the graph.

When a student types a keyword or phrase that is matched in the database, you will be notified in the information window and, depending on the priority level, an alert will be raised, an email will be sent notifying users that a phrase has been triggered and a screen shot or screen recording will be taken. You can customise what actions are taken for each priority level in the Phrase Monitoring settings (different actions can be set for each profile) or when adding or modifying a phrase.

Notes:

- A single image of the student who has triggered the phrase can be captured, if the student machine has an active webcam. By default, this action is turned off, but can be applied to any of the priority levels. This may be useful if a high-risk phrase (such as a suicide term) has been triggered on a communal school PC and there is no other way of knowing who was sitting at the PC. A webcam image will not be taken if the webcam is currently in use on the student machine or if the webcam has been disabled in the USB Device Control settings.
- For email notifications to be sent, the email settings must be configured. Users can be set up to receive email notifications for triggered phrases, ensure the Receive email when phrases are triggered option in the Safeguarding User dialog is selected.
- For an alert to be raised, the 'eSafety key phrase triggered' alert must be enabled in Alerting.

An accuracy level can be set to determine how accurately words must be typed by the student before they are flagged as a potential cause for concern. You can customise this level in the DNA Configuration – Phrase Monitoring settings depending on how closely you want words to be matched.

You can view data for a specified period. To switch between different time periods, click the appropriate icon in the Filter section of the ribbon. Clicking **Advanced** allows you to apply a customised date/time filter. Listed descriptions can be expanded to provide an individual Agent breakdown for each item.

The working hours shown can be amended to suit your organisation in the DNA Configuration dialog. See Console Preferences - General for further information.

Note: To view an associated screen shot, screen recording or webcam image, click the appropriate media icon next to the individual Agent record in the detailed list view.

A useful way of targeting specific keywords and phrases (and limiting the amount of data displayed), is to view certain categories, priority levels and types of source text. To select which categories are displayed, click the **Category** icon, select the required group to view and click **OK**. To hide the data for a priority level, click the **Priority** icon, clear the relevant check box and click **OK**. To hide data for a source text type, click the required source type to clear the yellow shading. The information window will now only display data for the selected categories, priority levels and source text types.

Note: You can choose not to monitor certain source text types in the DNA Configuration - Phrase Monitoring settings.

There may be applications and websites that you do not want to trigger a keyword match from, in which case, you can choose to ignore certain applications and websites. Application and URL Ignore lists can be created containing a list of applications/websites to ignore when monitoring phrases and these can be applied in the Phrase Monitoring settings.

You can review the phrases triggered by clicking **Review** in the ribbon. An overview of the phrase, who has triggered it and what has been typed to trigger it, along with details of the risk index score will be displayed, along with any screen shots, screen recordings and webcam images. From here, you can print, save, email, export to PDF and, if a screen shot, recording or webcam image is attached, see a history of who has viewed it. If the triggered phrase is deemed to be a false match, it can be marked as a false alarm and it will no longer appear in the information window.

Note: Triggered phrases that have been marked as a false alarm can still be viewed by clicking the **Category** icon in the ribbon and selecting **Show False alarms**. When reviewing false alarms in the Review Triggered Phrase dialog, you will be able to see any notes that have been added and also remove the triggered phrase from the false alarm category.

NetSupport DNA provides a keyword database of matching words and phrases that may indicate dangerous or inappropriate activity. These can be added to, to keep up with current trends. To manage and add new keywords and phrases, click the **Phrase List** icon in the Manage section of the ribbon.

NetSupport DNA provides a selection of phrases in various languages. You can include these in Phrase Monitoring by selecting the languages to include from the Language files drop-down list in the Keywords and Phrases database list.

A phrase cloud provides a visual representation for the most frequently used phrases or keywords matched for a given period of time.

Triggered phrases can be removed from the database using the Database Maintenance utility. You also have the option just to remove associated screenshots and recordings and leave the triggered phrases in the database.

Note: You can view all triggered phrases by risk instead of by phrase category by clicking **Risk Analysis** in the ribbon.

Queries
Select the Queries tab to display the Queries window.
NetSupport DNA's Query tool enables you to interrogate the database for records matching specified criteria. Queries specific to the component currently being viewed will be listed, enabling fast retrieval of the results.

Click the **Add Query** icon on the ribbon to create a new query or click the **Edit Query** icon in the ribbon to edit an existing item in the list.

Reports
Select the Reports tab to display the Reports window.

A number of pre-defined management reports, powered by the Crystal Reports engine, is attached to each component. Select the required

report from the drop-down list. The results will be listed in the information window. These can be exported if required.

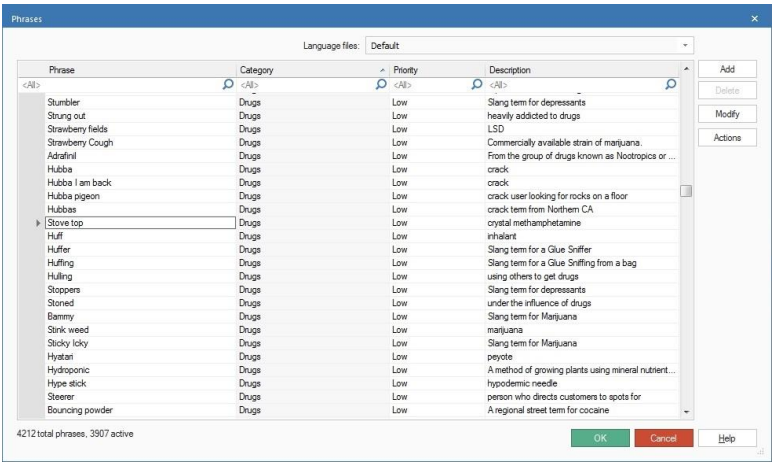
Keywords and Phrases Database List

NetSupport DNA provides a database of pre-defined keywords and phrases. To keep up with current trends, you can add your own terms to this. Keywords can be assigned to categories and you can set the priority level depending on how closely you want to monitor that term. All priority levels will record usage in the eSafety information window (unless the priority is set to off). By default, medium and above levels will also generate an alert; a high level will additionally take a screen shot at the student and send an email notifying users that a phrase has been triggered, and an urgent level will take a screen recording at the student who has triggered the phrase.

Notes:

- User-defined keywords can be imported or exported to a .CSV file.
- The email settings must be configured before email notifications can be sent. Users can be set up to receive email notifications for triggered phrases in the Safeguarding User dialog.
- The screen recording length for an urgent priority level can be set in the Phrase Monitoring settings.

1. Click the **eSafety** icon in the ribbon and select the **Phrases** icon.
2. Select the **eSafety** icon drop-down list and select {Manage Keywords and Phrases}.
   Or
   Click the **Phrase List** icon in the Manage section of the ribbon.
3. The Phrases dialog will appear.



4. A list of pre-defined and user-defined keywords and phrases will be listed. The category the phrase belongs to will be displayed, along with the current priority level, a description and the language of the phrase (if you have selected more than one language file). The total number of phrases in the database, along with the number that are active will be listed at the bottom of the window.
5. You can filter the data displayed or search for certain keywords by typing in the search boxes at the top of each column.
6. To monitor additional languages, select the **Language files** drop-down list and choose the required language(s).
7. You can modify the category, priority or description for individual items in the list itself. To modify multiple items, select the required phrases and click **Modify**.

Note: You can only change the priority for predefined phrases.

8. To add a new phrase, click **Add** and enter the required information for the phrase.
9. To delete a phrase, select the required phrase and click **Delete**.

Note: You can only delete user-defined phrases.

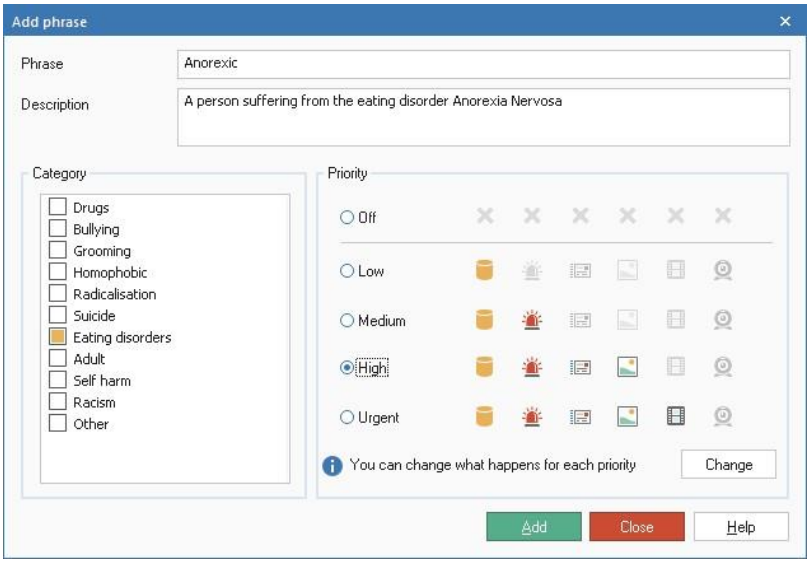
10. The action taken for each priority can be customised by clicking **Actions**.

Note: Different actions can be set for each profile in the Phrase Monitoring settings.

We are always happy to receive any comments you may have regarding the phrases included, please email the safeguarding team at safeguarding@netsupportsoftware.com.

Create or Edit Keywords and Phrases

This dialog is used to create new or edit existing keywords and phrases.



1. Enter the keyword or phrase that you wish to monitor and a description for this.
2. Choose which category the phrase applies to and set the priority level.

   Note: The actions to be taken for each priority will be displayed. Click **Change** to customise these. Different actions can be set for each profile in the Phrase Monitoring settings.

3. Click **Add** to add the phrase to the user-defined list.

Note: When editing predefined terms, you will only be able to change the priority level and the actions taken.

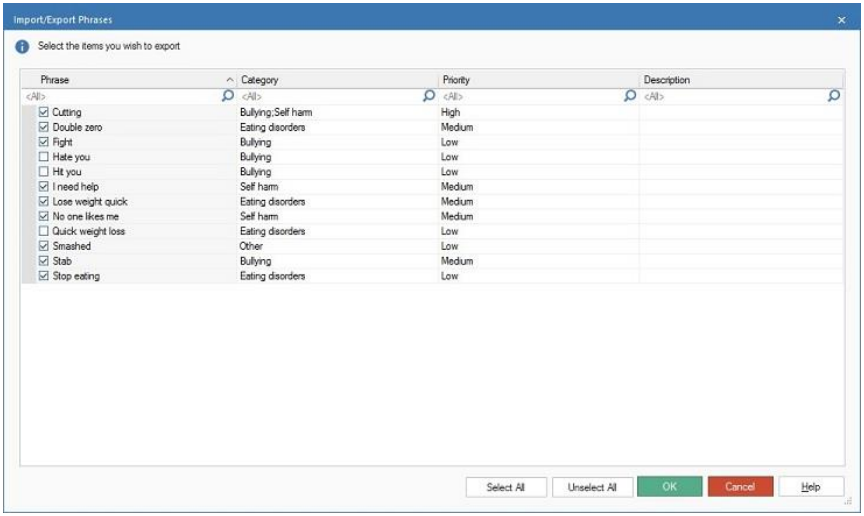
Importing/Exporting Keywords and Phrases

NetSupport DNA allows you to import and export keywords and phrases to or from a .CSV file.

Note: Only user-defined keywords can be imported or exported.

Exporting phrases

1. Click the **eSafety** icon in the ribbon and select the **Phrases** icon.
2. Select the **eSafety** icon drop-down list and select {Export}.
   Or
   Click the **Export** icon in the ribbon.
3. The Import/Export Phrases dialog will appear.



4. A list of user-defined phrases that are available for export will be displayed.
5. Ensure the phrases that you want to export are ticked and click **OK**.

   Note: To select all the listed phrases, click **Select all**.
6. Enter a name and location for the .CSV file.
7. Click **Save**.

Importing phrases

Only .CSV files can be imported. The file must be in the format of phrase name, category, priority and description.

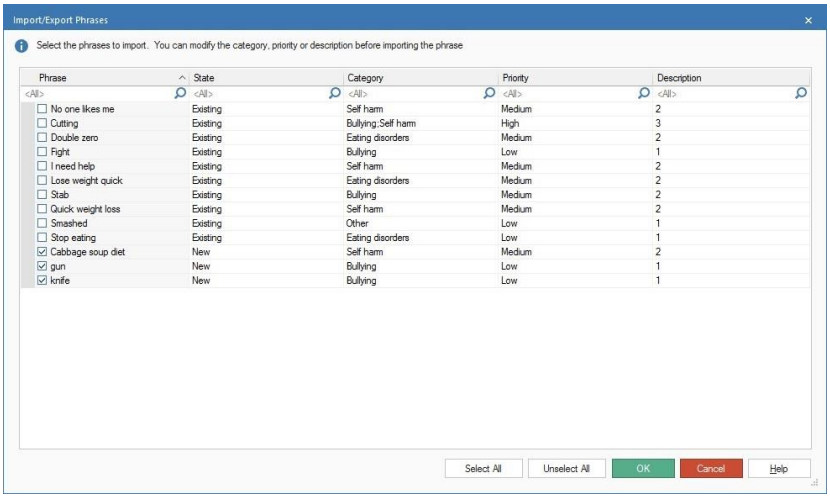
A	B	C	D
Phrase Name	Category	Priority	Description
Test phrase	256	2	This is a test phrase.

The phrase category and priority must be a numeric value. A list of the values are:

Category	Value	Priority	Value
Drugs	1	Off	0
Bullying	4	Low	1
Grooming	8	Medium	2
Homophobic	32	High	3
Radicalisation	64	Urgent	4
Suicide	128		
Eating disorders	256		
Adult	512		
Self harm	1024		
Racism	2048		
Other	4096		

Note: Please ensure that the .CSV file is closed before you import. If the file is open, it will not be imported.

1. Click the **eSafety** icon in the ribbon and select the **Phrases** icon.
2. Select the **eSafety** icon drop-down list and select {Import}.
   Or
   Click the **Import** icon in the ribbon.
3. Select the .CSV to import and click **Open**.
4. The phrases will be displayed in the Import/Export Phrases dialog.



5. From here, you can modify the category, priority and description by clicking in the relevant field.
6. Ensure the phrases that you want to import are ticked. To select all the listed phrases, click **Select all**.

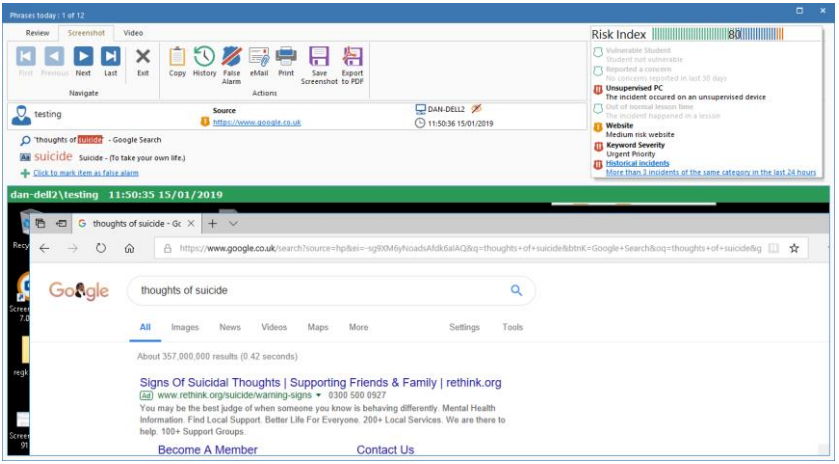
Note: If the phrase is already in the database, the state will show as existing. These phrases can still be imported.

7. Click **OK**.

Review Triggered Phrases

You can review phrases that have been triggered and perform a variety of functions.

1. Select the time period you want to review triggered phrases for by clicking the appropriate icon in the Filter section of the ribbon.
2. Click the **Review** icon in the ribbon.
3. The Review triggered phrases will be displayed.



4. Scroll through the triggered phrases by using the forward and back arrows.
5. A Review tab is displayed for all phrases, providing an overview of the phrase, who has triggered it, what has been typed to trigger it and the risk index score (along with the factors used to calculate the score, which allows you to see if further action needs to be taken). These details can be copied to the clipboard by clicking the **Copy** icon. Phrases marked as "high" priority will have a Screenshot tab, allowing you to view the screen shot taken when the phrase was triggered and those marked as "urgent" priority will also include Video tab, allowing you to view a screen recording of the event.

Note: A Webcam tab will appear if you have enabled the webcam action for a priority level (this is turned off by default and can be enabled when customising the actions taken). The Webcam tab will display a single image taken from an active webcam at the student machine, allowing you to easily identify the person who has typed the keyword. This may be useful if a high-risk phrase (such as a suicide term) has been triggered on a communal school PC and there is no other way of knowing who was sitting at the PC.

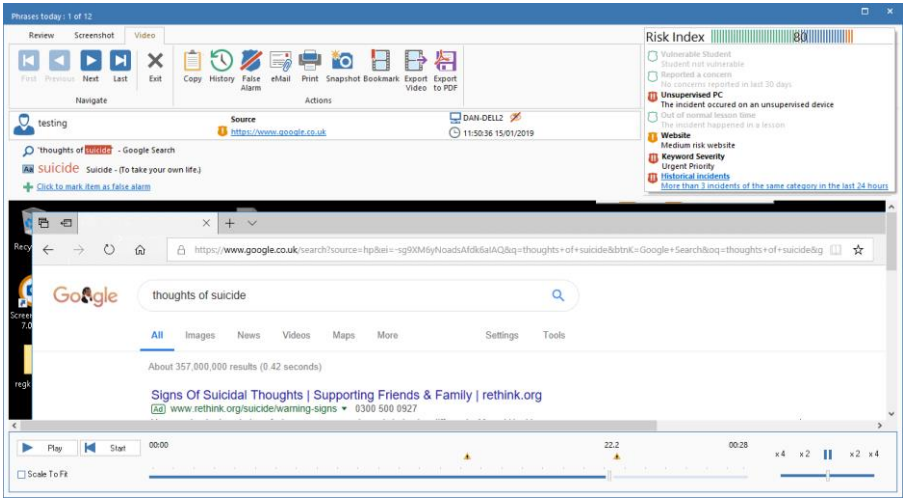
6. You can print or email a copy of the triggered phrase by clicking the appropriate icon. To see a history of who has viewed a screen shot, video recording or webcam image, click **History**. The triggered phrase details can be exported to a PDF by clicking **Export to PDF**.

Note: You can specify the default folder the PDF is exported to in the File Location settings and customise the PDF with your school branding in the Phrase Monitoring settings.

7. If the triggered phrase is deemed to be a false match, it can be marked as a false alarm and it will no longer appear in the main information window. To mark an individual item as a false alarm, select **Click to mark item as false alarm**, enter a note (a drop-down list of previous entries will appear, or you can type your own) and press **Enter**. To mark multiple items as false, click **False Alarm** for the required triggered phrases and click **Exit**. A dialog will appear asking you to confirm these phrases are false matches and you can add a note for these items.

Note: Triggered phrases that have been marked as a false alarm can still be viewed by clicking the **Category** icon in the ribbon and selecting **Show false alarms**. When reviewing false alarms in the Review Triggered Phrase dialog, you will be able to see any notes that have been added, the Console user that marked it as a false alarm and the date and time. To remove the triggered phrase from the false alarm category, click **False Alarm** and click **Exit**.

To view a screen recording



When viewing a screen recording, playback controls will be displayed, allowing you to watch what happened at the Agent when the phrase was triggered.

A timeline shows where in the recording the phrase has been triggered and if any bookmarks have been added. You can use the slider to move to the required position. Click **Play**, to start the recording - by default, this will begin from where the phrase was triggered (clicking **Start** will take you to the beginning of the recording). You can fast forward and rewind the recording by clicking on the slider in the far right of the dialog. When you release the slider, the recording will pause at that location. Select **Scale to fit** to show the whole of the student screen in the display area.

Bookmarks can be added, allowing you to highlight areas of interest in the recording. Ensure you are at the required location in the timeline and click **Bookmark**. Enter a description for the bookmark, a list of bookmarks can be displayed by clicking and you can remove bookmarks from here. Click **OK**.

Note: A snapshot of the recording can be saved. Click **Snapshot**, enter a name for the screen shot, select the type of file to save as and click **Save**.

A screen recording can be converted to a video file, allowing it to be played outside of the DNA Console on a range of media players. It can be converted to WMV and AVI formats. Click **Export Video** and the Replay File Conversion wizard will guide you through the conversion process.

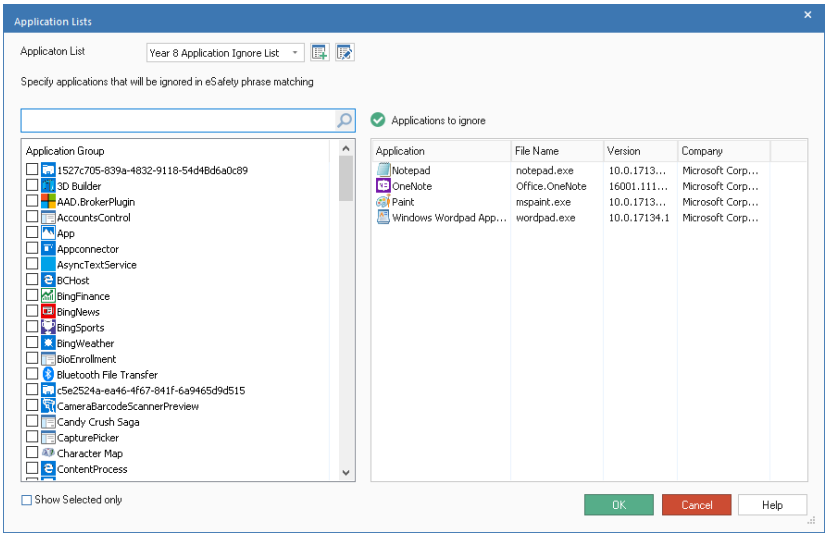
Note: By default, the screen recording length is fifteen seconds (fifteen seconds before and after the phrase has been triggered). This can be customised in the Phrase Monitoring settings.

Application Ignore Lists

When monitoring keywords and phrases there may be applications that you do not want to trigger a keyword match from, in which case, you can choose to ignore certain applications. Application lists can be created, allowing you to have a list of applications that are ignored when monitoring phrases. Multiple lists can be created, allowing you to assign different lists to different profiles.

Creating and applying an Application list

1. In the Settings tab, select **Manage Existing Profiles**.
2. Select the required profile from the list and click **Settings**.
3. Select **Phrase Monitoring**.
4. The Phrase Monitoring settings will be displayed.
5. Click **Application Lists**.
6. The Application Lists dialog will appear.



7. To create a new Application list, click . Enter a name for the list and, if required, a description. You can copy an existing list by selecting it from the 'Copy from' drop-down list. Click **OK**. To edit an existing list, click  .
8. A list of applications will be displayed. Select the applications to include in the Application list.
9. Click **OK**.

10. Select the required Application list from the Application List drop-down menu.
11. Click **Save** to apply the changes.

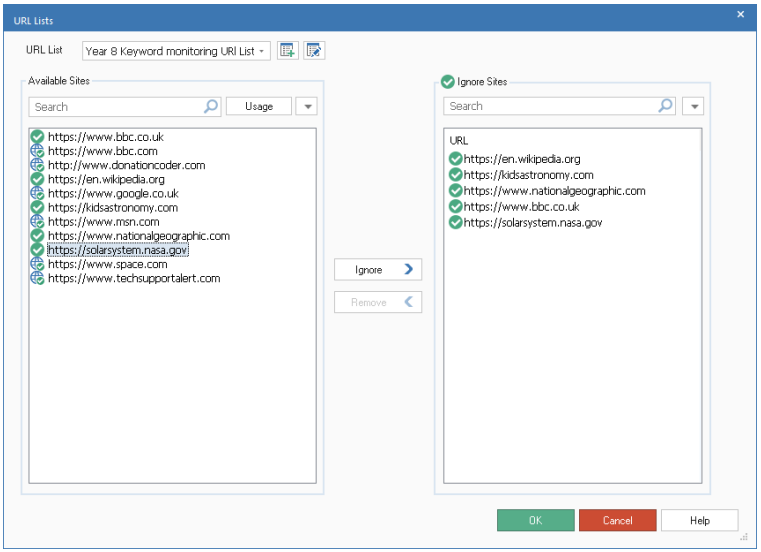
URL Ignore Lists

When monitoring keywords and phrases there may be websites that you wish to ignore. A URL list can be created, allowing you to ignore any phrase matches from websites that are included in the list. Multiple lists can be created, allowing you to assign different URL lists to different profiles.

Note: Internet restriction URL lists containing approved or restricted websites can also be created, allowing you to control the websites visited by Agents.

Creating and applying a URL list

1. In the Settings tab, select **Manage Existing Profiles**.
2. Select the required profile from the list and click **Settings**.
3. Select **Phrase Monitoring**.
4. The Phrase Monitoring settings will be displayed.
5. Click **URL Lists**.
6. The URL Lists dialog will appear. Websites already visited by Agents will be listed automatically in the Available Sites list and the default URL list will be displayed.



7. To create a new URL list, click . The URL List dialog will appear. Enter a name for the list and, if required, a description. You can copy an existing list by selecting it from the 'Copy from' drop-down list.

   Note: An internet restrictions list can be copied, URLs in the Approved Sites list will be added to the Ignore Sites list.

   Click **OK**. To edit an existing list, click .
8. To add an existing URL to the Ignore Sites list, select the URL in the Available Sites list and click **Ignore**, or drag and drop the URL into the list.
9. To add a new website to the list, click in the Ignore Sites list, select **Add URL** and enter the required details. The new website will appear in Ignore Sites list and will also be automatically added to the Available Sites list. To delete URLs, click and select **Delete URL**.
10. Once the required URLs have been added to the Ignore Sites list, click **OK**.
11. Select the required URL list from the URL List drop-down menu.
12. Click **Save** to apply the changes.

To view full website usage data, select the required website in the Available Sites list and click the Usage button. The Website Usage dialog appears, showing which users have accessed the website and how many times they have visited. Clicking a user will display a full breakdown of when and how long the user accessed the website for.

Phrase Cloud

The phrase cloud provides a visual representation of all triggered phrases, highlighting trending topics across the school. By clicking on any word in the cloud, you can see details of which students have typed it and the application used.

1. Click the **eSafety** icon in the ribbon and select the **Phrases** icon.

   Note: You can also view the phrase cloud by risk; click the **Risk Analysis** icon.

2. Click the **Phrase Cloud** icon in the ribbon.

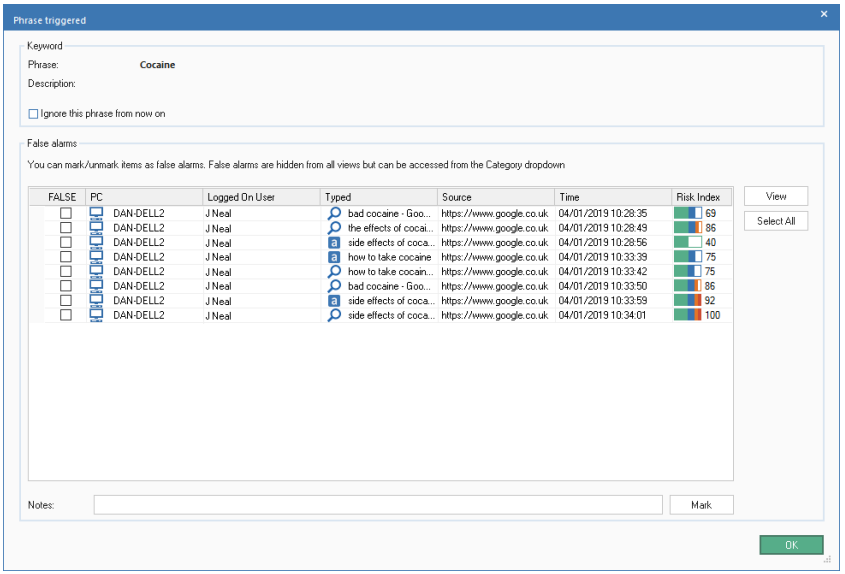


You can limit the amount of data that is displayed by viewing certain categories, priority levels and types of source text. To select which categories are displayed, click the **Category** icon, ensure the required groups to view are selected and click **OK**. To hide the data for a priority level, click the **Priority** icon, clear the relevant check boxes and click **OK**. To hide data for a source text type, click the required source type to clear the yellow shading. The phrase cloud will now only display data for the selected categories, priority levels and source text types.

The phrase cloud can be viewed in a single colour, or the phrases can be coloured according to their priority level, allowing you to see at a glance phrases that pose a greater risk. Right-click in the phrase cloud, select **Colour** and choose the required option.

Viewing usage

1. Click on a word in the phrase cloud.
   Or
   Right-click on a word and select **View Usage**.
2. The Phrase Triggered dialog will appear.



3. A list of users who have triggered the phrase, what was typed and where and the risk index score will be displayed. From here, you can choose to ignore the phrase from now on, so it will no longer appear in the phrase cloud or information window. To view full details of a triggered phrase, highlight the required occurrence and click **View**.
4. A triggered item can be marked as a false alarm; these instances will not be reported in the information window but are still stored. Select the required item, you can select all occurrences by clicking **Select All.** A note can be added, allowing you to include a reason why the triggered phrase has been marked as a false alarm. Click **Mark**. False alarms can be viewed by clicking the **Category** icon in the ribbon and selecting **Show false alarms**.

Note: An image of the phrase cloud can be saved. Right-click in the phrase cloud and select **Save As**.

Concerns

A student who feels vulnerable can report a concern, via the DNA Agent component installed on school devices or a web link, to someone trusted at the school. Once a concern is reported and the appropriate member of staff is notified, it can then be tracked and an ongoing audit log of any subsequent activities undertaken as a result.

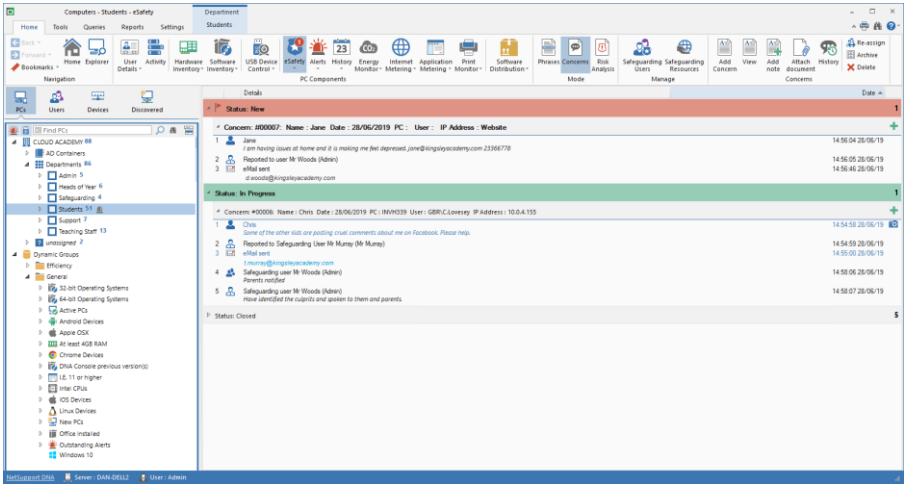
Notes:

- By default, Report a Concern is disabled. You can enable this in the DNA Configuration - eSafety settings.
- Students can be marked as vulnerable, allowing Safeguarding Users to easily identify and provide support to them. You can mark students as vulnerable when editing user details. They will then be displayed in the appropriate dynamic group in the Users Tree view.

1. Click the **eSafety** icon in the ribbon.

   Note: If the component icons are not visible, click the Home tab.

2. Select the **Concerns** icon in the ribbon.



Before students can report a concern, contacts need to be defined, allowing students to select who to send the concern to. Click **Safeguarding Users** in the Manage section of the ribbon.

There may be occasions when a student verbally reports a concern directly to a teacher. In these cases, the teacher can add a concern from within the DNA Console allowing it to be tracked alongside other

concerns. Click **Add Concern** in the ribbon, enter the information the student provided and assign it to the appropriate safeguarding contact.

When a student reports a concern, you have the option to include links to safeguarding resources (websites and helplines), providing students with alternative support mechanisms. To display this, you need to enable the **Show safeguarding resources** option in the DNA Configuration - Report Concern settings. To change your region, add or edit the list of support websites, click **Safeguarding Resources** in the Manage section of the ribbon.

Once a student has raised a concern, a notification icon will be displayed at the top of the **eSafety** icon and the new concern will be displayed in the information window. The staff member who the concern was reported to will receive an email advising them that a concern has been raised and to log into the NetSupport DNA Console to view it.

Notes:

- To send notifications by email, you must ensure you have configured the email settings in the NetSupport DNA Email settings and defined an email address for the staff member in the Safeguarding User dialog.
- A header bar will be displayed in the Phrase Monitoring information window advising when new concerns have been raised; click **View** to switch to Concerns mode.

Access to view current concerns is restricted to Safeguarding Roles only. To enable a Console user to view concerns, you will need to link them to an eSafety contact.

Concerns will be listed by their status (new, in progress, closed or archived).

Each concern will be headed with the user/student and PC details if known. If the concern was reported via a DNA Agent the IP address of the device used will be listed. Alternatively, it will show website if the student reported the concern using your own custom website button.

If there is a screen shot attached to a concern, a camera image will be displayed next to it. Clicking this will show the image. From here, you can print, save, email and see a history of who has viewed the screen shot. To view an individual concern, select the required concern and click **View**.

Notes can be added to a concern to show what progress has been made. These are displayed in chronological order. Each note has an image to indicate its type. To add a note, select the required concern and click **Notes** or click .

Documents containing information relevant to the concern can be added. Select the required concern and click **Attach document**. Select a file and click **Open**. The file will be added to the concern. To view a document that has been attached to a concern, click .

Note: Students can also attach supporting documents and screenshots when raising a concern. (Only available when reporting the concern using the DNA Agent.)

If concerns are not actioned within a pre-defined period of time, a reminder email will be sent. Reminders can be configured in the DNA Configuration - Report Concern settings.

A history of all concerns a student has raised can be viewed. Select a concern for the student you wish to view and click **History**. The Concern History dialog will be displayed, allowing you to see in calendar format all concerns the student has raised by day, week or month. Safeguarding Users will only be able to view concerns that have been assigned to them, unless they are authorised to view all concerns.

There may be times when a concern needs to be reassigned to a different Safeguarding User. Select the concern to be reassigned and click **Re-assign**. The Re-assign Concern dialog will appear, showing a list of available Safeguarding Users. Select the required user and click **Re-assign**. Both the existing and new user will be notified of the change via email.

Note: Only Safeguarding Administrators can reassign concerns.

Concerns can be archived once they have been dealt with. Archived concerns are still visible for audit purposes but it will no longer be possible to add to them.

There may be occasions where concerns need to be deleted, for example, if they have been reported in error or if they are over a certain age. Select the required concern to delete and click **Delete**. You can delete this concern, all concerns for the selected user, all concerns raised before a specific date or all archived concerns.

Note: Before concerns can be deleted, a second Safeguarding Administrator will need to authorise this. You will be prompted to choose a Safeguarding Administrator from the list and they will need to enter their password. If you only have one Safeguarding Administrator, you will need to create another one before you can delete concerns.

Safeguarding Resources

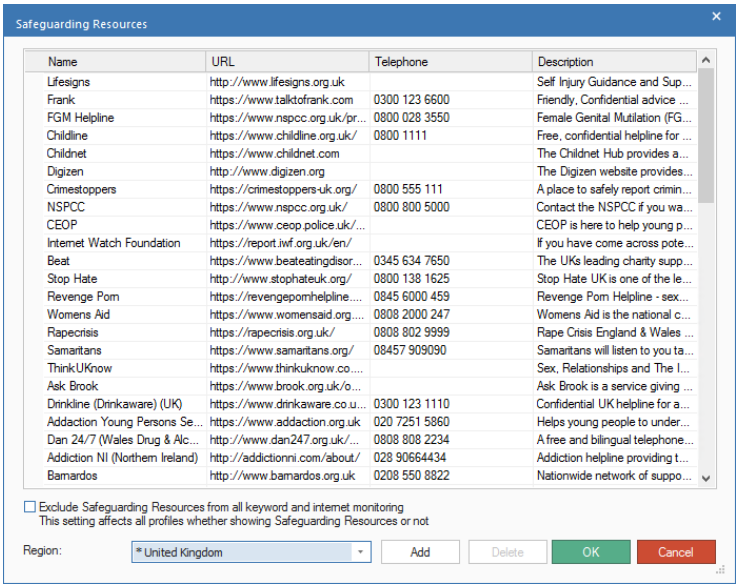
A link to safeguarding resources can be made available to students when they report a concern - from the NetSupport DNA Agent menu and also from a desktop icon. This link will provide the students with details of support websites and helplines that they can use if they would rather speak to someone outside of the school.

Notes:

- This feature can be enabled in the Report Concern settings; select **Show safeguarding resources**.
- A Safeguarding Resources icon can be displayed on student desktops. Select **Create shortcuts on users' desktops** in the Report Concern settings. This icon will also be available when the NetSupport DNA Agent is not running.

To add or edit resources

1. Click the **eSafety** icon in the ribbon and select the **Concerns** icon.
2. Select the **eSafety** icon drop-down menu and select {Safeguarding Resources}.
   Or
   Click the **Safeguarding Resources** icon in the ribbon.
3. The Safeguarding Resources dialog will appear.



4. A list of default resources will be provided. Select the region from the drop-down list to display these for your country.
5. You can exclude these URLs from being reported in Internet Metering or anything typed in them from being matched in Phrase Monitoring. Click **Exclude Safeguarding Resources from all keyword and internet monitoring**.

Note: This is a global setting and will apply to all profiles, even if safeguarding resources is disabled.

6. To add a new item, click **Add** and enter the required details.
7. To edit a current item, click on the required field and overtype the information.
8. To delete an item, select the required item and click **Delete**.
9. Click **OK**.

Reporting a Concern

Student concerns can be reported directly to a selected staff member via the DNA Agent installed on school devices or via a custom website link.

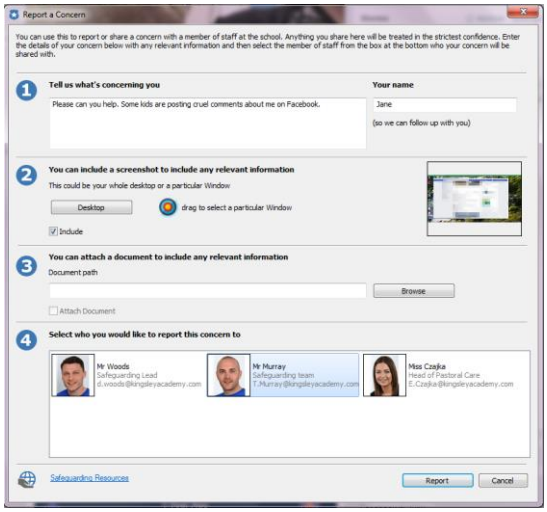
Notes:

- By default, Report a Concern is disabled. You can enable this in the DNA Configuration – Report Concern settings and create contacts to report the concern to from here.
- Concerns can also be raised from within the NetSupport DNA Console. This may be useful if a student verbally raises a concern with a teacher. The teacher is then able to manually log the concern and assign it to the appropriate staff member, allowing it to be tracked.

Reporting a concern via the DNA Agent

1. Right-click the NetSupport DNA icon in the taskbar and select {Report a Concern}.
   Or
   Click the icon in the taskbar.
   Or
   Click the **Report a Concern** desktop icon.

   Note: For the desktop icon to be displayed, you will need to enable the **Create shortcuts on users' desktop** option in the DNA Configuration - Report Concern settings.
2. The Report a Concern dialog will be displayed.



3. From here, the student can enter all the information regarding the concern, along with their name.

Notes:

- Students are limited to 512 characters when entering their text.
- The current logged on user name will be reported when a concern is raised.

4. Click **Desktop** to include a screen shot of the whole desktop or, to include a screen shot of an individual window, drag the  icon to the required window.
5. A document can be attached to the concern, allowing any additional information to be included. Click **Browse** to select the required file and click **Open**.
6. A list of staff members to report the concern to will be displayed and the student can choose who to send the concern to.
7. A link to safeguarding resources can be made available to students, providing them with alternative support mechanisms. This option needs to be enabled in the DNA Configuration - Report Concern Settings.
8. Click **Report**.
9. The concern will be reported to the appropriate staff member.

Reporting a Concern via a Website

During the school day the Report a Concern option installed on school devices is available to students via the DNA Agent component. However, for added flexibility, you can also offer students the same facility for out-of-hours use or when they don't have access to an Agent device via a custom-made Report a Concern button and form that you create and embed on a website of your choosing, the school website for example.

A handy wizard in the DNA Console helps you create an HTML snippet containing the required code.

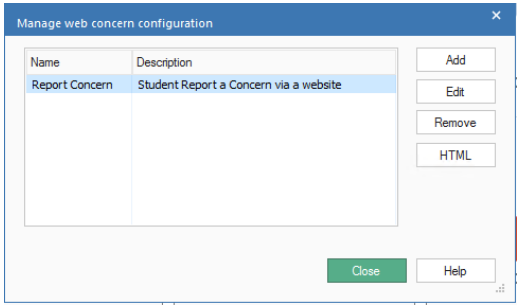
Notes:

- To use this method for reporting a concern, the DNA Cloud Console must be enabled.
- Ensure the appropriate Safeguarding User accounts are configured to receive concerns reported via the web.

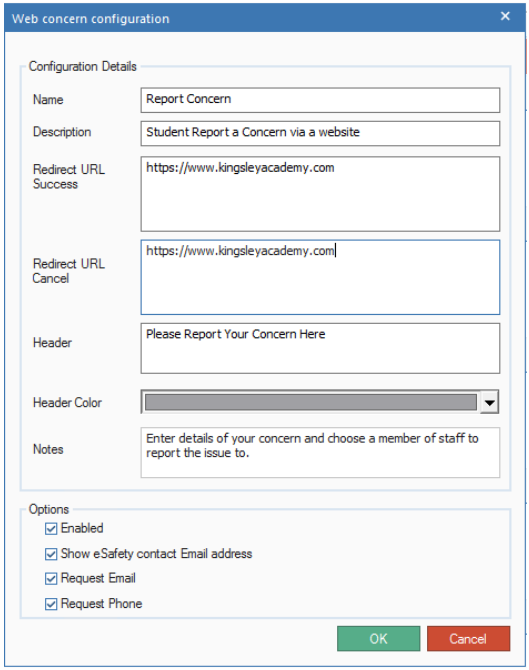
Manage web concerns

1. Select the Settings tab in the DNA Console.

2. Click the **Manage Web Concerns** icon. The Manage web concern configuration dialog will appear.



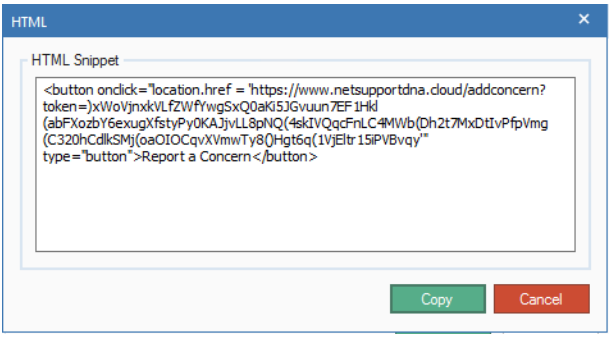
3. A useful wizard is provided to help you build the required elements of the Report a Concern button and form and in turn compile the HTML snippet that will need to be copied into your chosen website page. Click **Add**. The Web concern configuration wizard will appear.



- Enter a suitable name and description to identify each configuration (HTML snippet) you create. These are the details that appear in the Manage web concern configuration dialog.

- Specify a redirect URL for use when the student has successfully reported a concern. Ensure this is the full URL, including http(s)//.
- Specify a redirect URL for instances where the student cancels the request. Ensure this is the full URL, including http(s)//.
- Enter a header message that should appear at the top of the web page.
- Choose a header colour.
- A default note that will appear on the web page is supplied but you can enter your own custom message/instruction if required.
- **Options:**
  - By default, the Report Concern form will always be enabled. If disabled, a message will appear when students try to access the form.
  - The form will show the Safeguarding staff members (eSafety contacts) who the student can send their concern to. You can choose whether to include the person's email address on the form.
  - You can add a field to the form that asks the student to enter their email address.
  - You can also request the student's phone number.

4. Click **OK** when you have completed the wizard. You will return to the **Manage web concern configuration** dialog.
5. Click **HTML** to view the code that has been created. You can edit the text description that will appear on the Report a Concern button if required.



6. Click **Copy** to select the HTML snippet, decide which page on your website you wish to place the Report a Concern button and embed the HTML into the source code for the required web page. You can further customise the code at this stage to suit individual needs if required. For example, editing the text that will appear on the Report a Concern button.

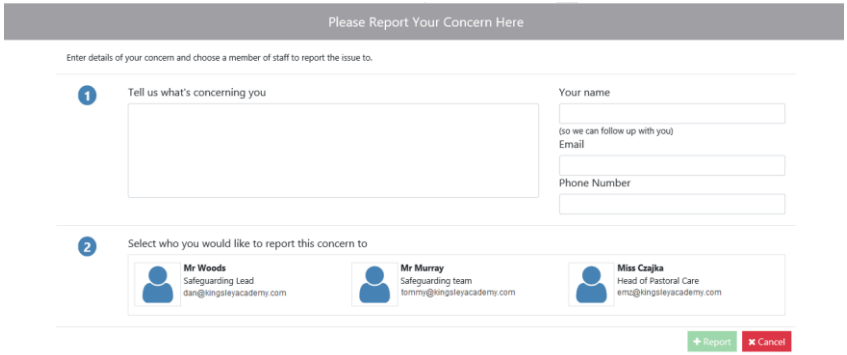
Testing the form

If you want to test the form before adding to your website, follow these steps:

1. Open Notepad or similar and paste the copied HTML. Save the file with a suitable name and ensure you add .HTML as the extension.
2. Run the HTML file and in the first instance, you will see the **Report a Concern** button.



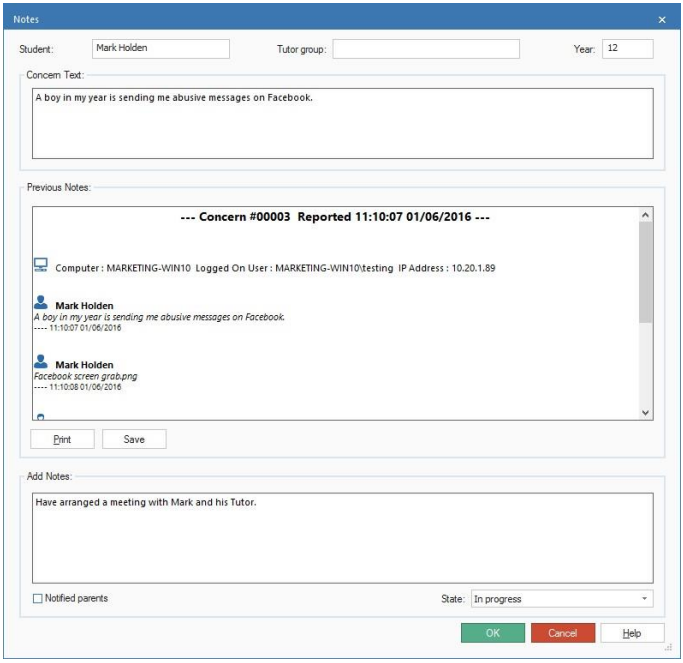
3. Click the button and the main form will open. Complete the form, select a Safeguarding User and click **Report**. Sign in to your NetSupport DNA Console where you should now be able to view the reported concern in the eSafety component. Confirm that the redirect URL worked correctly and that a new concern assigned email was received by the nominated Safeguarding User.



Note: Photos associated with your Safeguarding Users cannot currently be displayed using the website option.

Adding Notes to a Concern

This dialog is used to add notes to a concern.

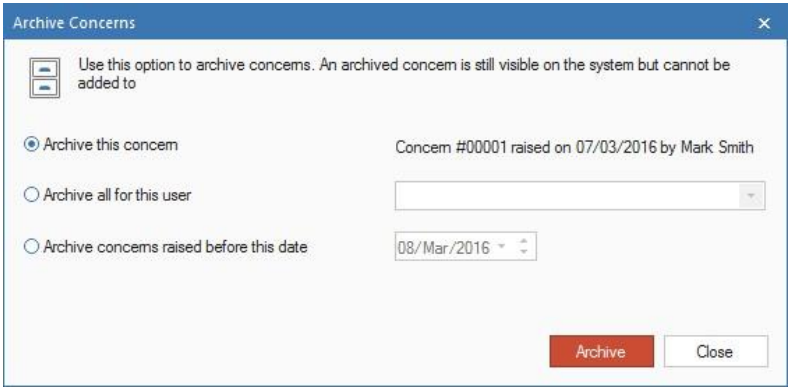


1. A full history of notes relating to the concern will be displayed. This can be printed or saved to .RTF.
2. The student name, tutor group and year of the student that the concern relates to can be added, if required.
3. Enter your notes in the **Add Notes** box.
4. The state of the concern can be changed by choosing the appropriate option from the drop-down list.
5. If the student's parents have been notified of the issue, you can select the **Notified parents** option to advise of this.
6. Click **OK**.
7. Your note will be added to the concern.

Archiving Concerns

Once a concern has been dealt, with it can be archived. Archived concerns are still visible for audit purposes but it will no longer be possible to add to them.

1. Select the concern to archive and click **Archive**.
2. The Archive Concerns dialog will be displayed.



3. You can archive just this concern, all concerns for a user (select the user from the drop-down list) or all concerns before a specific date.
4. Click **Archive**.

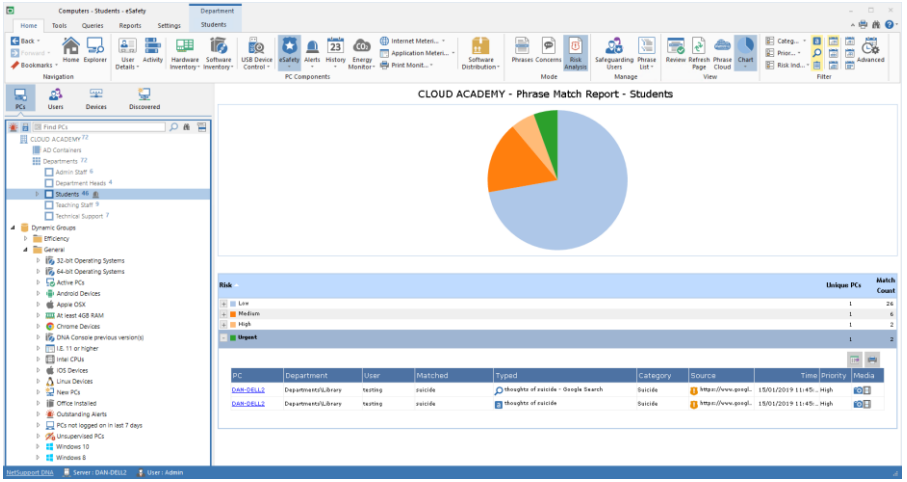
Risk Analysis

NetSupport DNA contains a contextual intelligence-based risk index which automatically flags high-risk events and vulnerable students. It assesses the context and history of a student's activities – from the devices used, time of day, and websites visited (including previous alerts they may have triggered) – and, from this information, creates a numerical risk index score. A high-risk index could result if a student has repeatedly researched a safeguarding topic (e.g. suicide) out of hours, in an unmonitored setting such as the library. A lower index rating could result from a student searching a lower risk keyword in a local application during school hours that may have been used for curriculum topics.

1. Click the **eSafety** icon in the ribbon.

   Note: If the component icons are not visible, click the Home tab.

2. Select the **Risk Analysis** icon in the ribbon.



In the Tree view, select the level at which you want to view the metering data: company, department, AD container, Dynamic Group or individual Agent.

The information window will display a breakdown for each selected item in graph and list format. To view the graph in a different format, click the **Chart** icon drop-down arrow on the ribbon and select the appropriate format. To print the active view, click the  icon at the top of the Console.

Note: Clicking the **Chart** icon in the ribbon will hide/show the graph.

You can view data for a specified period. To switch between different time periods, click the appropriate icon in the Filter section of the ribbon. Clicking **Advanced** allows you to apply a customised date/time filter.

Data is displayed according to the risk the triggered phrase poses (low, medium, high and urgent). Listed descriptions can be expanded to provide an individual Agent breakdown for each item.

A useful way of targeting specific keywords and phrases (and limiting the amount of data displayed), is to view certain categories, priority levels, risks and types of source text. To select which categories are displayed, click the **Category** icon, select the required group to view and click **OK**. To hide the data for a priority level, click the **Priority** icon, clear the relevant check box and click **OK**. To hide data for a risk index type, click the **Risk Index** icon, clear the relevant check box and click **OK**. To hide data for a source text type, click the required source type to clear the yellow shading. The information window will now only display data for the selected categories, priority levels, risks and source text types.

To view an associated screen shot, screen recording or webcam image, click the appropriate media icon next to the individual Agent record in the detailed list view.

Full details of each triggered phrase can be viewed; click **Review**. From here, you can see who triggered the phrase, along with the factors which make up the risk index score, allowing you to see if further action is required. You can print, save, email, export to PDF and, if a screen shot, recording or webcam image is attached, see a history of who has viewed it.

'At Risk' Application and URL lists can be created, containing applications and websites that are considered a higher risk to students. Multiple lists can be created, allowing different lists to be assigned to different profiles.

Note: Any phrases triggered out of lesson time will be classed as a higher risk. You can amend the lesson hours to suit your school in the DNA Configuration dialog. See Console Preferences - General for further information.

Define unsupervised PCs
PCs located in an unmonitored environment, such as the library, may be considered more of a risk than those in the classroom. You can specify which PCs across your network are unsupervised and any phrases triggered on them will have a higher risk index.

1. Select an Agent, department or dynamic group in the PCs Tree view.
2. Right click and select **PC supervision**.
3. Click **Unsupervised** and click **OK**.
4. The PCs will be displayed in the Unsupervised PCs dynamic group in the Tree view.

Queries
Select the Queries tab to display the Queries window.

NetSupport DNA's Query tool enables you to interrogate the database for records matching specified criteria. Queries specific to the component currently being viewed will be listed, enabling fast retrieval of the results.

Click the **Add Query** icon on the ribbon to create a new query or click the **Edit Query** icon in the ribbon to edit an existing item in the list.

Reports
Select the Reports tab to display the Reports window.

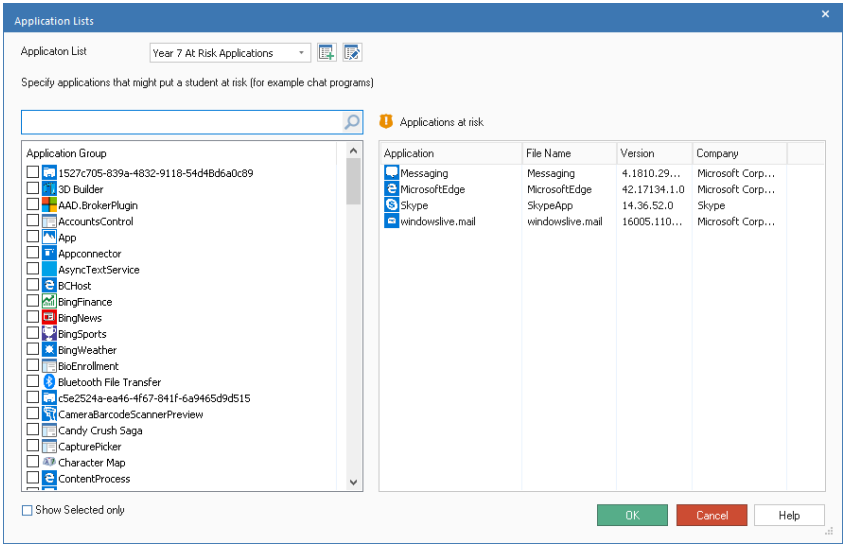
A number of pre-defined management reports, powered by the Crystal Reports engine, is attached to each component. Select the required report from the drop-down list. The results will be listed in the information window. These can be exported if required.

At Risk Application Lists

At Risk Application lists can be created, allowing you to define applications that may put students at more risk. For example, phrase matches in Skype may be considered a higher risk than those triggered using Microsoft Word. Multiple lists can be created, allowing you to assign different lists to different profiles.

Creating and applying an Application list

1. In the Settings tab, select **Manage Existing Profiles**.
2. Select the required profile from the list and click **Settings**.
3. Select **Risk Analysis**.
4. The Risk Analysis settings will be displayed.
5. Click **Application Lists**.
6. The Application Lists dialog will appear.



7. To create a new Application list, click . Enter a name for the list and, if required, a description. You can copy an existing list by selecting it from the 'Copy from' drop-down list. Click **OK**. To edit an existing list, click .
8. A list of applications will be displayed. Select the applications to include in the Application list.
9. Click **OK**.
10. Select the required Application list from the drop-down menu.
11. Click **Save** to apply the changes.

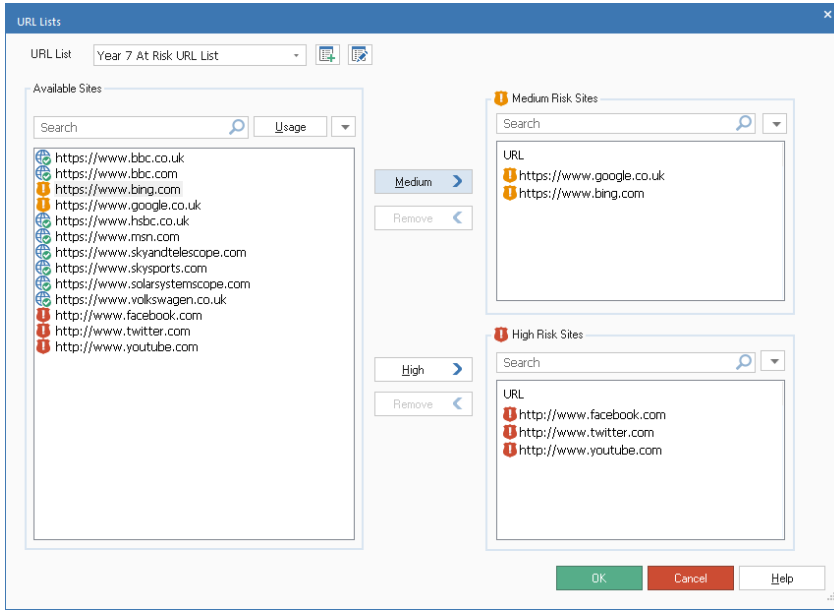
At Risk URL Lists

At Risk URL lists can be created, allowing you to define websites that pose a medium or high risk for students. Multiple lists can be created, allowing you to assign different lists to different profiles.

Note: Internet restrictions URL lists containing approved or restricted websites can also be created, allowing you to control the websites visited by users.

Creating and applying a URL list

1. In the Settings tab, select **Manage Existing Profiles**.
2. Select the required profile from the list and click **Settings**.
3. Select **Risk Analysis**.
4. The Risk Analysis settings will be displayed.
5. Click **URL Lists**.
6. The URL Lists dialog will appear. Websites already visited by Agents will be listed automatically in the Available Sites list and the default URL list will be displayed.



7. To create a new URL list, click . The URL List dialog will appear. Enter a name for the list and, if required, a description. You can copy an existing list by selecting it from the 'Copy from' drop-down list.

Note: An internet restrictions list can be copied, URLs in the Approved Sites list will be added to the Medium Risk Sites list and URLs in the Restricted Sites list will be added to the High Risk Sites list.

Click **OK**. To edit an existing list, click .

8. To add an existing URL to the Medium or High Risk Sites list, select the URL in the Available Sites list and click **Medium** or **High**, or drag and drop the URL into the required list.
9. To add a new website to the list, click in the Medium or High Risk Sites list, select **Add URL** and enter the required details. The new website will appear in the appropriate Sites list and will also be automatically added to the Available Sites list. To delete URLs, click and select **Delete URL**.
10. Once the required URLs have been added, click **OK**.
11. Select the required URL list from the drop-down menu.
12. Click **Save** to apply the changes.

To view full website usage data, select the required website in the Available Sites list and click the Usage button. The Website Usage dialog appears, showing which users have accessed the website and how many times they have visited. Clicking a user will display a full breakdown of when and how long the user accessed the website for.

Alerting

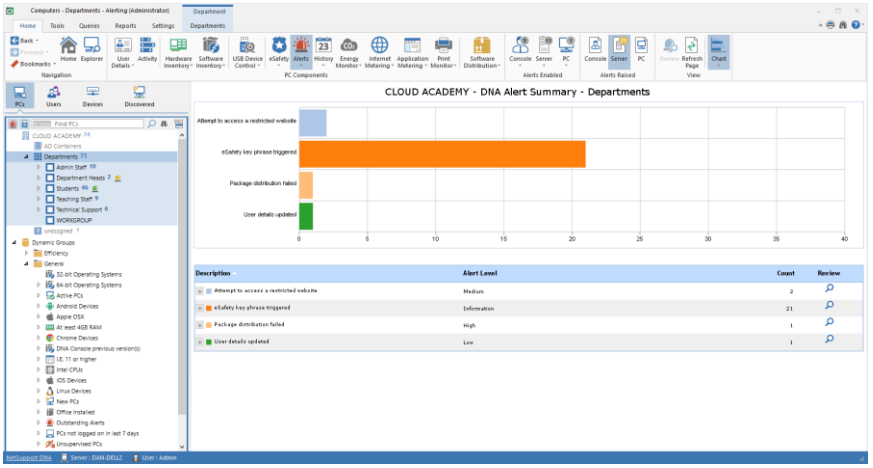
NetSupport DNA features an extremely powerful Alerting module that prompts the system to automatically notify Operators when any number of changes occurs across the enterprise. There are three types of alerting options that you are able to define alerts for: Server alerts, Console alerts and PC alerts. Server alerts identify any changes within the data gathered by the NetSupport DNA Server across the overall enterprise, including alerts for things like new PCs added, changes in hardware, a new application installed/removed and so on. Console alerts identify changes relating to the NetSupport DNA Console, such as the DNA licence limit being exceeded, an Operator added or deleted and a DNA update installed. PC alerts identify real-time changes or conditions that occur on a specific PC, such as CPU utilisation exceeding XX% for XX minutes, free disk space falling below XX%, when a key service stops (e.g. AntiVirus service or IIS on a server), print spooler alerts, security alerts (e.g. failed login attempts) and much more.

Alert notifications can be directed to specified email recipients and/or active Console users (on a per alert basis, so the nature of the alert may dictate which Operators are notified).

Note: NetSupport DNA also provides SNMP alerts, which identify any changes to SNMP device properties.

1. Click on the **Alerts** icon in the ribbon. The Alerts window will appear.

   Note: If the component icons are not visible, click the Home tab.



In the Tree view, select the level at which you want to view the displayed: data, company, department, AD Container, Dynamic Group or individual Agent.

You can toggle between PC, Server and Console alerts by clicking the **Alerts** icon drop-down list and selecting {Display - Server Alerts/Console Alerts/PC Alerts} or clicking the appropriate icon in the Alerts Raised section of the ribbon.

The information window will display a breakdown for each selected item in graph and list format. The listed descriptions can be expanded to provide an individual Agent breakdown for each item; these can be exported or printed if required. To view the graph in a different format, click the **Chart** icon drop-down arrow on the ribbon and select the appropriate format. To print the active view, click the  icon at the top of the Console.

Note: Clicking the **Chart** icon in the ribbon will hide/show the graph.

To configure and create alerts, click the **Console**/**Server**/**PC** icon in the Alerts Enabled section of the ribbon. You can see which alerts are currently running by selecting the drop-down list under the required icon.

Note: Clicking an icon here allows you to create or configure alerts.

Outstanding alerts are identified against matching PCs on the main company Tree view. Once alerts have been identified, you can view the details in the information window by clicking . The alert can be closed if required and notes can be added to PC alerts. When a PC alert has been closed, the details will still be accessible from the History feature.

Note: You can show/hide alerts in the Tree view by clicking .

An action can be added to a PC alert, allowing you to choose what happens when an alert is triggered. The actions available are: capture screenshot (this can be attached to the email that is sent when the alert is activated), record screen and run application. These are added in the DNA Alert wizard. When an alert has been raised, you can review this by selecting the **PC** icon in the Alerts Raised section of the ribbon and clicking **Review**. An overview of the alert and who has activated it will be displayed, along with any screen shots and screen recordings. From here, you can print, save, email, export to PDF and, if a screen shot or recording is attached, see a history of who has viewed it.

Queries
Select the Queries tab to display the Queries window.

NetSupport DNA's Query tool enables you to interrogate the database for records matching specified criteria. Queries specific to the component currently being viewed will be listed, enabling fast retrieval of the results. Click the **Add Query** icon in the ribbon to create a new query or click the **Edit Query** icon in the ribbon to edit an existing item in the list.

Reports
Select the Reports tab to display the Reports window.

A number of pre-defined management reports, powered by the Crystal Reports engine, are attached to each component. Select the required report from the drop-down list. The results will be listed in the information window. These can be exported if required.

Notes:
- The date/time format displayed in the Console is taken from the machine where the NetSupport DNA Server is installed. To change the format in the Console, you will need to change the system date/time format on this machine. For further information, visit www.netsupportsoftware.com/support.
- The frequency at which the server collects data can be adjusted using the NetSupport DNA Settings option. This will not be applicable for critical, urgent or high alerts, the data for these alerts will be sent to the server immediately.

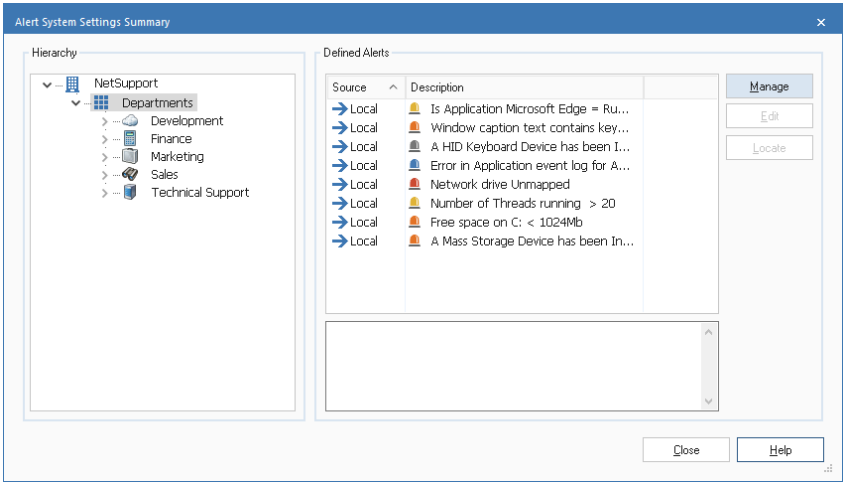
PC Alerts

PC Alerts give Operators the ability to identify changes that occur on a specific PC. There are a number of pre-defined alerts that the Operator can choose to set up, for example, disk space alerts, security alerts etc. The Operator then specifies the conditions for the alert, who should be notified and any actions to be taken when the alert is triggered. Once the alert is active at the Console, you can review the full details of it and save a permanent record for later review.

1. With the Alerts icon selected, highlight a company, department or AD container.
2. Right-click and select **PC Alerts**.
   Or
   Click the **Alerts** icon drop-down arrow and select {PC Alerts} from the menu.

Or
Click the **PC Alerts** icon in the Alerts Enabled section of the ribbon.

3. The Alert System Settings Summary dialog will appear.



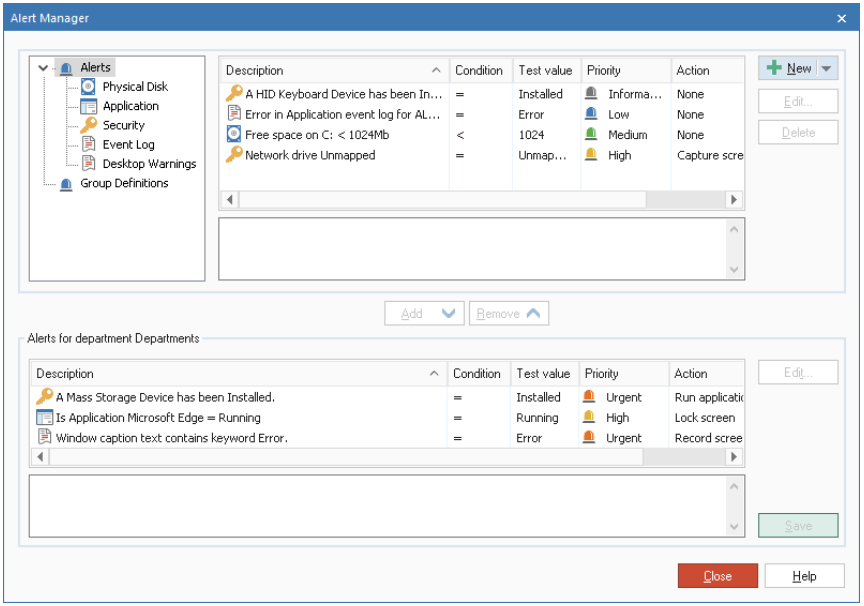
4. Select the required level in the Hierarchy; a description of any existing alerts will be displayed. Alerts identified at the source level as local alerts were originally created at that level, inherited alerts have had been passed down from the company or department above.
5. Select **Manage** and the Alert Manager dialog will appear, allowing you to create a new alert, edit or delete an existing alert.
6. To alter the properties of an existing alert, click **Edit**. You cannot directly edit an inherited alert, only a local alert. To change an inherited alert to a local alert, select the required alert and click **Locate**.

Alert Manager

This dialog enables you to create new alerts, edit the properties for existing alerts and allocate alerts at company or department level.

1. In the Tree view, select whether you want to create an alert or set up group definitions.

Note: Group definitions are a collection of alerts that can be applied to a company or department.

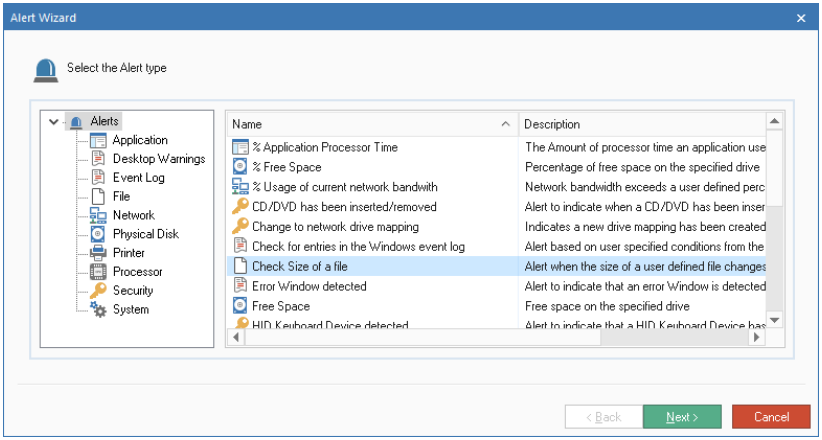


2. Click **New** to create a new alert or group definitions.
   Or
   Click **Edit** to alter the properties of an existing alert.
   Or
   Click **Delete** to remove an alert that is no longer needed.
3. Once an alert has been created, a description of this will appear. To activate an alert, you will need to include this in the current department. Add or remove alerts by using the appropriate buttons.
4. Once you are happy with the changes, click **Save** and then **Close**.

Note: If you are editing an alert that is currently active, not all fields can be amended. To alter the main properties of an alert, you must first deactivate this.

NetSupport DNA Alert Wizard

The NetSupport DNA Alert wizard guides you through the process of setting up a PC Alert. You can customise the properties by entering your own condition parameters.



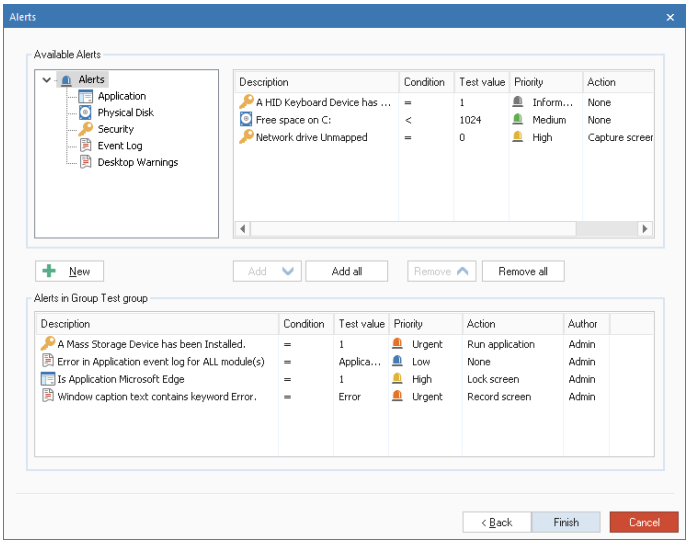
1. Choose from the selection of pre-defined alerts. Once you have decided on an alert, highlight and click **Next**.
2. Enter the required properties, decide on a priority level for the alert and select the action to be taken when the alert is raised. Select **Advanced** for further options to configure.
3. Click **Next**. A list of Console Operators will appear. Select the Operator to be contacted in the event the alert is raised. Using the appropriate buttons, you can add or remove Operators to be notified.
4. Decide how the Operator will be informed once the alert is raised. Select either Console message or email notification.
5. Click **Finish**. A description of the alert will now be displayed in the Alert Manager dialog.

Note: To send notifications by email, you must ensure you have configured the email settings in the NetSupport DNA Alerting System Settings and defined an email address for the Operator in the Console Operators dialog.

Group Definitions

A group definition allows you to set up a collection of alerts that can be applied to a company or department.

1. In the Alert Management System dialog, select **Group Definitions** from the Tree view and click **New**.
2. The Group Definitions Details dialog will appear. Enter a name and a description for the group. Click **Next**.
3. All alerts previously created will be listed. Navigate using the Tree view to highlight an alert to include in the profile.

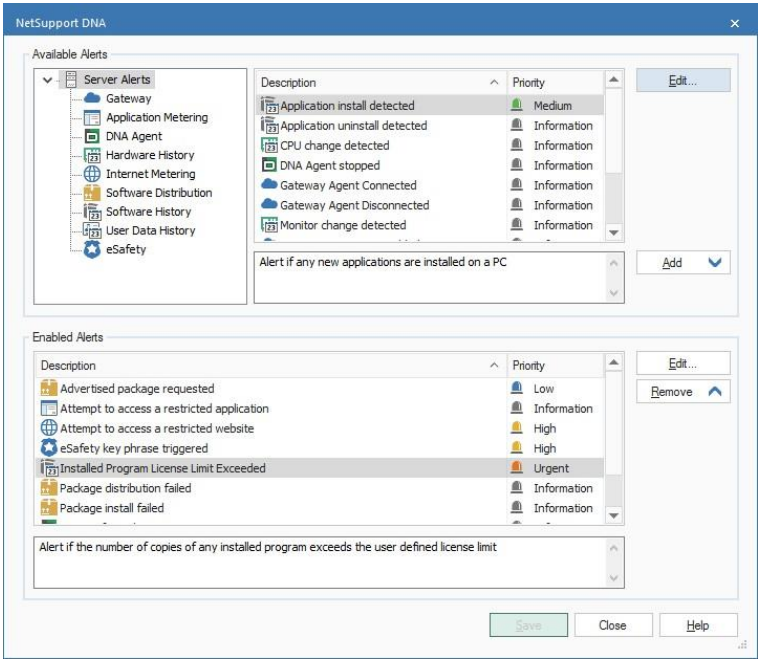


4. To create a new alert, click **New**. The Alert wizard will appear. Once the alert has been created, it will be included in this dialog.
5. Using the appropriate buttons, you can include or remove alerts from the current group.
6. Click **Finish**. The group will now appear in the Alert Manager dialog. You can activate this by adding it to the current department.

NetSupport DNA Server/Console Alerts

Server alerts enable Operators to identify changes in the data gathered by NetSupport DNA Server across the company as a whole. DNA Server alerts are alerts for individual PCs, for example, if a user attempts to access a restricted website. Console alerts identify changes relating to the NetSupport DNA Console. Alerts that don't relate to individual PCs will fall under Console alerts, for example, if a new Operator is added.

1. Click the **Alerts** icon drop-down arrow and select {Server/Console Alerts} from the menu.
   Or
   Click the **Server/Console Alerts** icon in the Alerts Enabled section of the ribbon.
2. The Server/Console Alerts dialog will appear.



3. A selection of pre-defined alerts will appear in the Available Alerts list. Any active alerts will be listed in the Enabled Alerts list. Use the appropriate buttons to remove or add alerts to the Enabled Alerts list.
4. You can alter the priority level of the alert and the notification contact (only for Server alerts) details by selecting **Edit**.
5. Once all changes are complete, click **Save** and **Close**.

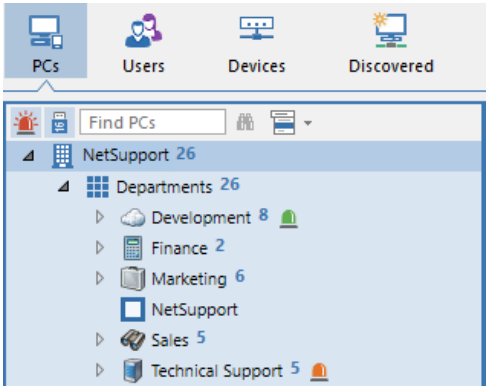
Active Alerts

Once an alert has become active, the Operator is notified by either a Console message or email notification, depending on the method that was selected when the alert was created.

Note: The **Alerts** icon on the ribbon will turn red if there are any outstanding alerts.

Console message notification

When an alert is raised, the Operator is notified with an appropriate identifier being displayed next to the company, department or Agent level in the Tree view (depending on which level is open). The Operator can view full details of the alert in the information window.



Note: You can show/hide alerts in the Tree view by clicking .

Operators will be informed of critical, urgent and high Server and PC alerts with a notification window 'sliding up' on the right-hand side of the PC taskbar. This ensures the Operators are notified immediately, no matter what section of the NetSupport DNA Console they are viewing.

The notification window will display which alert has been activated. Clicking the notification window will take the Operator directly to the Alerts component, where the full details will be displayed.

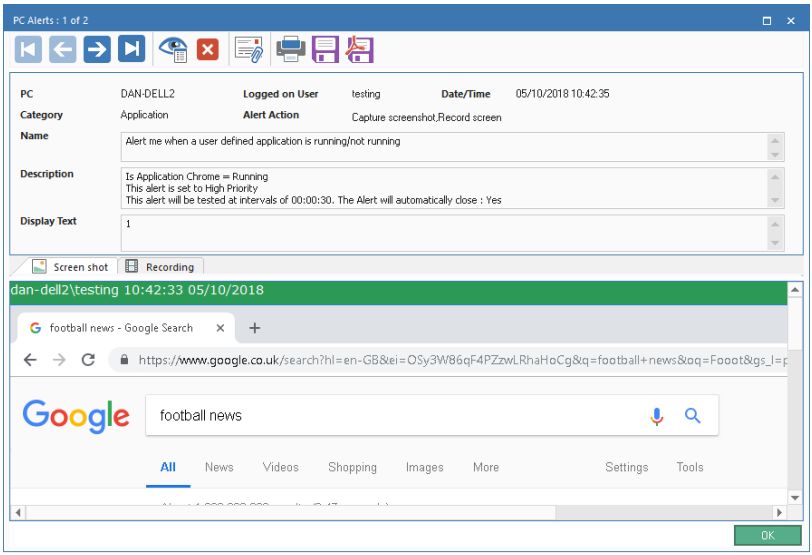
Email notification
Once the alert becomes active, an email will be sent to the relevant Operator, advising them that an alert has been raised. The email will include the priority level of the alert, date and time the alert was raised, details of the system and user and how long it has been active for.

The alert will also be displayed in the information window. From here, you can view the full details and close the alert by clicking . PC alerts can be reviewed and a permanent record of it saved on file.

Review Active PC Alerts

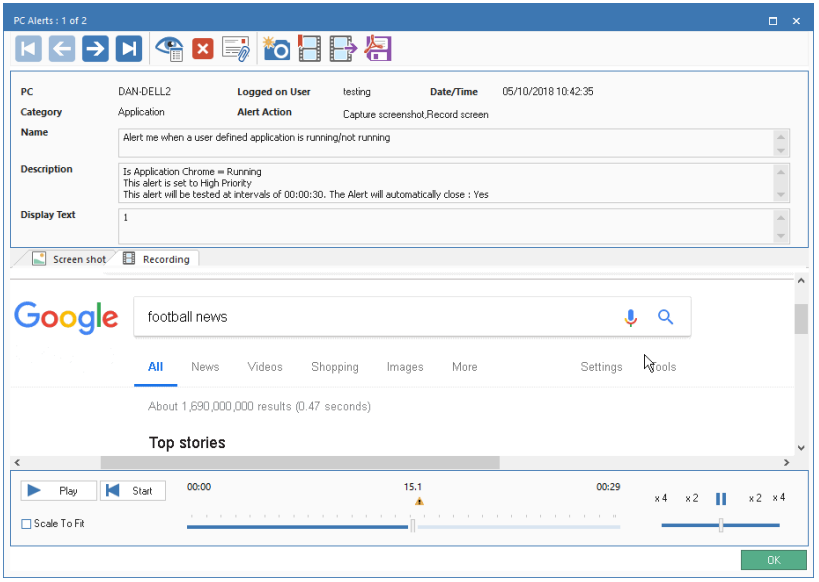
PC Alerts that have been raised can be reviewed and shared from here.

1. Select the **PC** icon in the Alerts Raised section of the ribbon.
2. Click the **Review** icon in the ribbon.
3. The PC Alerts dialog will be displayed.



4. Scroll through the active alerts using the forward and back arrows.
5. An overview of the alert and who has activated it will be displayed. Alerts with an action set to capture screen shot, will include a screen shot and those with an action set to record screen will include a screen recording.
6. You can print, save, email and, if a screen shot or recording is attached, see a history of who has viewed it.
7. The alert details can be exported to a PDF by clicking . You can specify the default folder the PDF is exported to in the File Location settings and customise the PDF with your organisation's branding in the Alerting settings.
8. To close an alert, click  and then click **OK**. A Close Alerts dialog will appear. A description of why you are closing the alert can be added. Click **Yes**. A history of all closed PC alerts is provided in the History component.

To view a screen recording



When viewing a screen recording, playback controls will be displayed, allowing you to watch what happened at the Agent when the alert was triggered.

A timeline shows where in the recording the alert has been triggered and if any bookmarks have been added. You can use the slider to move to the required position. Click **Play**, to start the recording - by default, this will begin from where the alert was triggered (clicking **Start** will take you to the beginning of the recording). You can fast forward and rewind the recording by clicking on the slider in the far right of the dialog. When you release the slider, the recording will pause at that location. Select **Scale to fit** to show the whole of the student screen in the display area.

Bookmarks can be added, allowing you to highlight areas of interest in the recording. Ensure you are at the required location in the timeline and click . Enter a description for the bookmark and click **OK**.

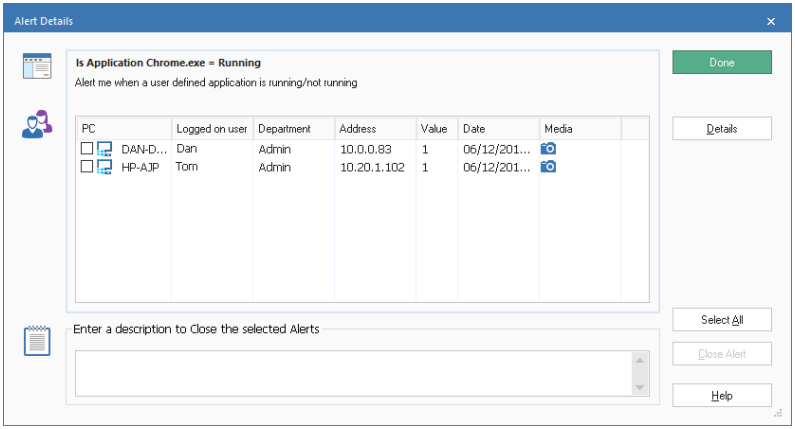
Note: A snapshot of the recording can be saved. Click , enter a name for the screen shot, select the type of file to save as and click **Save**.

A screen recording can be converted to a video file, allowing it to be played outside of the DNA Console on a range of media players. It can be converted to WMV and AVI formats. Click  and the Replay File Conversion wizard will guide you through the conversion process.

Note: By default, the screen recording length is fifteen seconds (fifteen seconds before and after the alert has been triggered). This can be customised in the Alerting settings.

Closing Alerts

Once the alert is identified, the Operator can close the alert by clicking  in the information window. The following dialog will appear.



Details of the alert will be displayed, with a list of PCs/users that the alert is outstanding for. Full details of PC alerts and any associated media can be viewed and shared by clicking **Details** (PC alerts can also be closed when reviewing the full details).

If more than one PC has triggered the alert, select the required PCs to close the alert for, if required, enter a description and click **Close Alert** to close the alert. You do not need to enter a description to close DNA Server or Console alerts. The alert will now disappear from the Alerts information window. There will be full history details of all PC alerts provided in the History component.

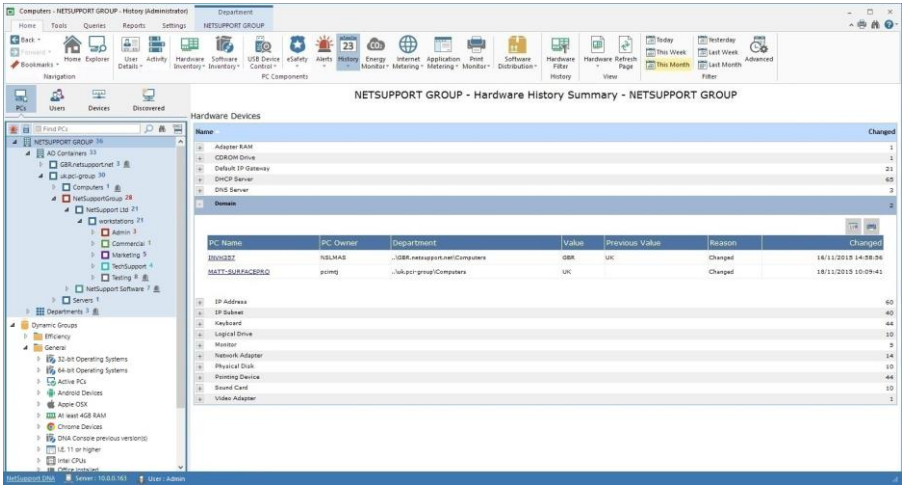
History Window

The History option enables you to track changes that have been made to an Agent's Hardware Inventory, Software Inventory, User Details and also view the Alerting and Console logon history.

Each time NetSupport DNA gathers data, it compares the current details against information already held on the server and, if there are any differences, they are recorded in the history.

1. Click the **History** icon in the ribbon. The History Summary window will appear.

Note: If the component icons are not visible, click the Home tab.



You can view the history at company, department, AD Container, Dynamic Group or individual Agent. Select the required level in the Tree view.

To switch between views, click the **History** icon drop-down list and select {Display – Hardware/Software/User Data/Alerting/Console Logon History} or click the appropriate icon in the ribbon.

You can view data for a specified period. To switch between different time periods, click the appropriate icon in the Filter section of the ribbon. Clicking **Advanced** allows you to apply a customised date/time filter. Listed descriptions can be expanded to provide an individual Agent breakdown for each item. The working hours shown can be amended to

suit your organisation in the DNA Configuration dialog. See **Console Preferences - General** for further information.

The date/time format displayed in the Console is taken from the machine where the NetSupport DNA Server is installed. To change the format in the Console, you will need to change the system date/time format on this machine. For further information, visit www.netsupportsoftware.com/support.

Note: There may be hardware changes that are recorded which you do not wish to track. You can disable items from being displayed in the Console and delete existing data for items that have been de-selected. Click the **History** icon drop-down arrow and select {Hardware Filter} from the menu or click the **Hardware Filter** icon in the ribbon.

Queries
Select the Queries tab to display the Queries window.

NetSupport DNA's Query tool enables you to interrogate the database for records matching specified criteria. Queries specific to the component currently being viewed will be listed, enabling fast retrieval of the results.

Click the **Add Query** icon in the ribbon to create a new query or click the **Edit Query** icon in the ribbon to edit an existing item in the list.

Reports
Select the Reports tab to display the Reports window.

A number of pre-defined management reports, powered by the Crystal Reports engine, are attached to each component. Select the required report from the drop-down list. The results will be listed in the information window. These can be exported if required.

Energy Monitor

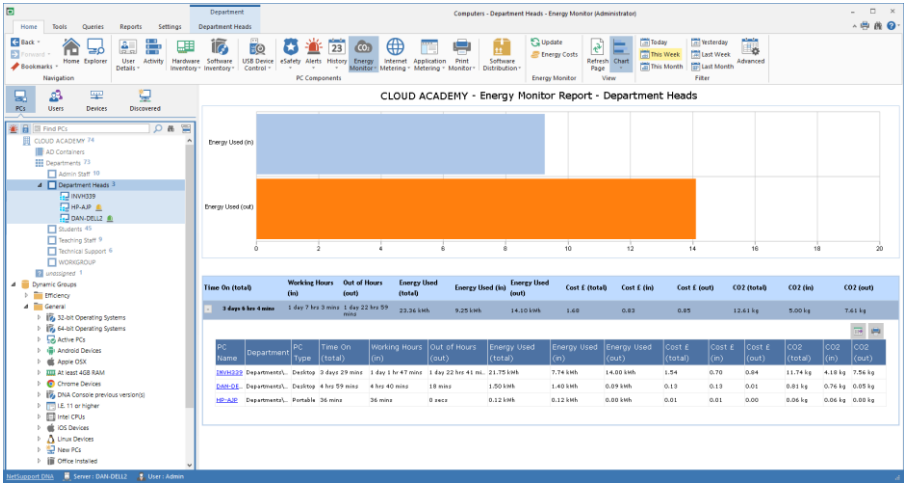
The Energy Monitoring module provides a simple and concise high-level summary of potential energy wastage across an organisation by computer systems that are left powered on out of business hours.

NetSupport DNA checks to verify the powered-on state of all computers and its local monitoring component keeps an accurate record of each time a computer is powered on, off or hibernates. Once it knows the times of day each computer was operational, an average (and customisable) "power consumption per device" calculation is used, facilitating a baseline energy usage calculation for all computers.

With this information to hand, computers in selected departments can be set to automatically power off at a specified time at the end of each day and then power back on the next morning.

1. Click the **Energy Monitor** icon. The Energy Monitor window will appear.

Note: If the component icons are not visible, click the Home tab.



In the Tree view, select the level at which you want to view the data, company: department, AD Container, Dynamic Group or individual Agent.

The total time powered on, energy usage, cost and CO2 emissions, both in and out of working hours is displayed in a graph and a list format. To view the graph in a different format, click the **Chart** icon drop-down arrow on the ribbon and select the appropriate format. To print the active view, click the  icon at the top of the Console.

Note: Clicking the **Chart** icon in the ribbon will hide/show the graph.

You can view data for a specified period. To switch between different time periods, click the appropriate icon in the Filter section of the ribbon. Clicking **Advanced** allows you to apply a customised date/time filter. Listed descriptions can be expanded to provide an individual Agent breakdown for each item. The working hours shown can be amended to suit your organisation in the DNA Configuration dialog. See **Console Preferences - General** for further information.

The values used for power usage, energy costs and CO2 emissions can be customised. Click the **Energy Monitor** icon drop-down list and select {Energy Costs} or click the **Energy Costs** icon in the ribbon.

A power management schedule can be set to automatically power on and off machines on selected days and specific times. You can also set what action is taken if a user is still logged on to a machine when it is time to power off. Inactivity policies can be created, allowing you to choose what happens when a machine has been inactive for a specified period of time: for example, you can set a machine to shut down if there has been no activity for thirty minutes between 17:00 and 19:00. A power management schedule can be created in the NetSupport DNA - Energy Monitor settings.

Holiday periods can be defined, so machines are excluded from the power on schedule for these dates. You can specify holiday periods in Console Preferences - General. The **Prevent power on during holidays** option then needs to be enabled in NetSupport DNA - Energy Monitor settings.

Note: Agent machines can be powered on or off by right-clicking the required level in the Tree and selecting {Power Management - Power On/Power Off}.

A quick refresh facility enables you to update data outside of the specified frequency. This can be useful for targeting particular Agents or departments. Right-click on the required item in the Tree view and select **Update** or click **Update** in the Energy Monitor drop-down menu or group.

Queries
Select the Queries tab to display the Queries window.

NetSupport DNA's Query tool enables you to interrogate the database for records matching specified criteria. Queries specific to the component currently being viewed will be listed, enabling fast retrieval of the results.

Click the **Add Query** icon in the ribbon to create a new query, click the **Edit Query** icon in the ribbon to edit an existing item in the list.

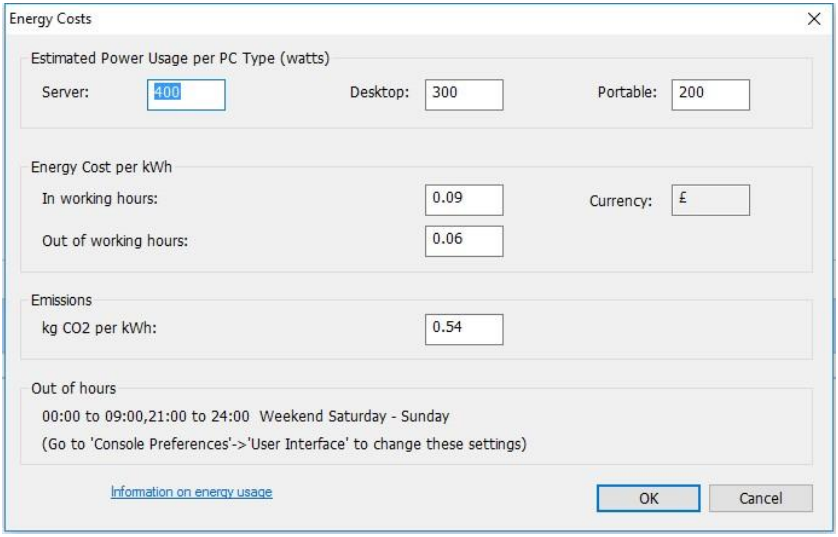
Reports
Select the Reports tab to display the Reports window.

A number of pre-defined management reports, powered by the Crystal Reports engine, are attached to each component. Select the required report from the drop-down list. The results will be listed in the information window. These can be exported if required.

Note: The frequency at which the Server collects data can be adjusted using the NetSupport DNA settings option.

Energy Costs

The values required to calculate the power consumption, cost and CO2 emissions in the Energy Monitor component can be set here.



Estimated Power Usage per PC Type (watts)
The estimated power usage for each PC type can be specified here.

Energy Cost per kWh
Enter the energy cost per kWh. You can enter the values for both in and out of working hours. The currency symbol shows the currency being used. This can be changed in the DNA Database wizard - Miscellaneous settings.

Emissions
By default, the emissions value is set to 0.54kg of CO2 per kWh.

Out of hours
The office working hours and days will be displayed. These can be amended to suit your organisation in the Console Preferences - General settings.

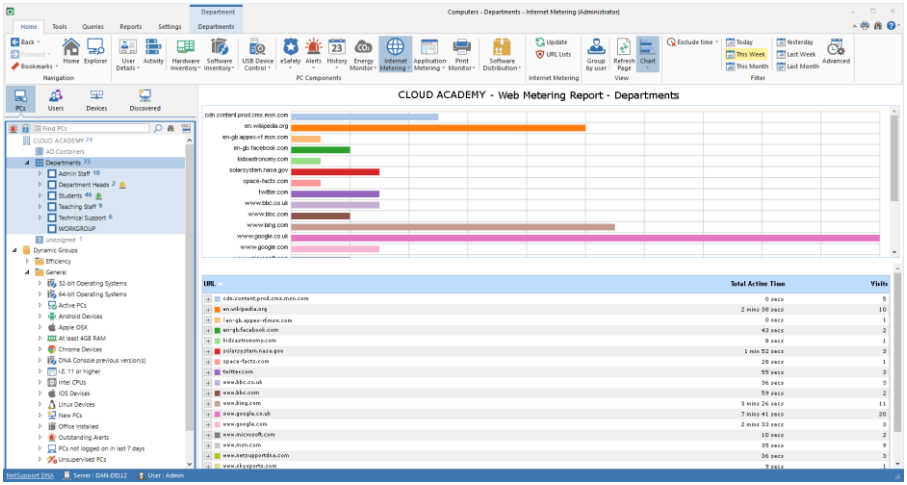
Internet Metering

The Internet Metering module provides a detailed summary of all internet activity on each PC by a user, including start and finish times for each URL visited and the active time spent on a page. Results can be reviewed either by activity on a specific device or for a user, no matter where they worked. Naturally, the key to supporting an effective policy is to provide effective controls. With NetSupport DNA, internet usage can be fully managed - and lists of approved and restricted URLs and/or sub-URLs (including the Counter Terrorism Internet Referral Unit list) can be applied centrally, plus multiple approved/restricted URL lists which can be assigned to specific profiles. This means dedicated internet settings can be applied to specific departments. Once applied, NetSupport DNA can allow unrestricted access to all websites, restricted access to certain websites that have been marked as approved by the company or by blocking access to specific sites marked as inappropriate.

Access can also be controlled by time of day, perhaps only allowing access to approved gaming or social media sites at lunchtime and outside of working hours.

1. Click the **Internet Metering** icon in the ribbon. The Internet Metering window will appear.

Note: If the component icons are not visible, click the Home tab.



You can switch the Tree view between PCs and Users. The PCs Tree view displays data for the PC owner who is associated to a PC and the Users Tree view displays data for logged on users.

In the Tree view, select the level at which you want to view the metering data: company, department, AD Container, Dynamic Group or individual Agent.

The information window will display a breakdown for each selected item in graph and list format. To view the graph in a different format, click the **Chart** icon drop-down arrow on the ribbon and select the appropriate format. To print the active view, click the  icon at the top of the Console.

Note: Clicking the **Chart** icon in the ribbon will hide/show the graph.

You can view data for a specified period. To switch between different time periods, click the appropriate icon in the Filter section of the ribbon. Clicking **Advanced** allows you to apply a customised date/time filter. Listed descriptions can be expanded to provide an individual Agent breakdown for each item. Websites that have been active for less than a specified time can be ignored if required.

Note: The working hours shown can be amended to suit your organisation in the DNA Configuration dialog. See Console Preferences - General for further information.

By default, internet usage is displayed by websites accessed. Selecting **Group by User** allows you to view internet usage based on Agents' User ID's and not the PC. This option will not be available in the Users Tree view.

Selecting **Group by PC** allows you to view internet usage based on the PC details and not the Agent Users details when in the Users Tree view. This option will not be available in the PCs Tree view.

Note: By selecting different levels in the Tree view, you can view Agent internet usage on PCs across different levels of the organisation.

A quick refresh facility enables you to update data outside of the specified frequency. This can be useful for targeting particular Agents or departments. Right-click on the required item in the Tree view and select **Update** or click **Update** in the **Internet** icon drop-down menu or ribbon.

The number of reported URLs can be limited by excluding specific websites from the list. For example, if you have an approved list of sites that users can visit you may decide not to include these in the metering stats. See **Internet Restrictions** for more information.

URL lists can be created, allowing you to control the websites visited by Agents. Click the **URL Lists** icon in the ribbon. Once URL lists have been defined, they can be assigned to specific profiles. See Internet Metering settings.

Queries
Select the Queries tab to display the Queries window.

NetSupport DNA's Query tool enables you to interrogate the database for records matching specified criteria. Queries specific to the component currently being viewed will be listed, enabling fast retrieval of the results.

Click the **Add Query** icon in the ribbon to create a new query or click the **Edit Query** icon in the ribbon to edit an existing item in the list.

Reports
Select the Reports tab to display the Reports window.

A number of pre-defined management reports, powered by the Crystal Reports engine, are attached to each component. Select the required report from the drop-down list. The results will be listed in the information window. These can be exported if required.

Notes:

- The frequency at which the server collects data can be adjusted using the NetSupport DNA settings option. This also enables you to activate any restrictions that may apply to internet usage.
- The date/time format displayed in the Console is taken from the machine where the NetSupport DNA Server is installed. To change the format in the Console, you will need to change the system date/time format on this machine. For further information, visit www.netsupportsoftware.com/support.

Internet Restrictions

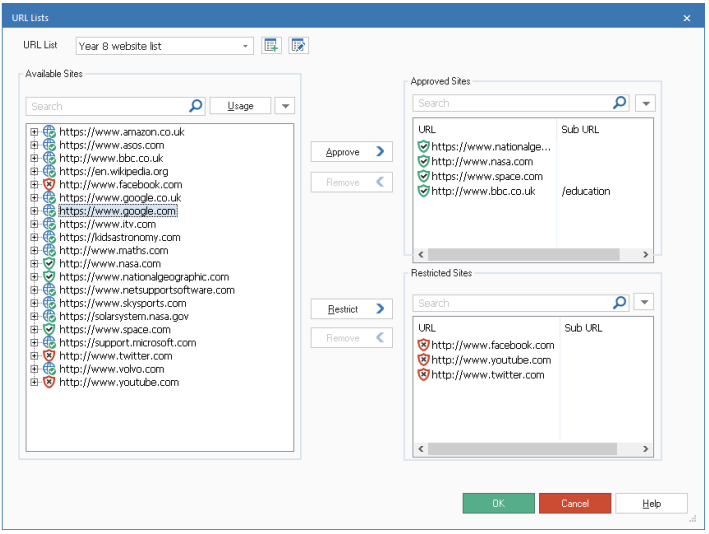
You can control the sites visited by Agents by creating approved and restricted lists. You determine which URLs it is or isn't appropriate for users to visit and then use the Internet Metering settings option to activate either list as required. Multiple lists can be created, allowing you to assign different approved/restricted websites to different profiles.

Sub-URLs can be added under a main URL. This allows you to restrict/approve access to certain areas of a website. For example, allow access to www.bbc.co.uk but restrict access to www.bbc.co.uk/sport.

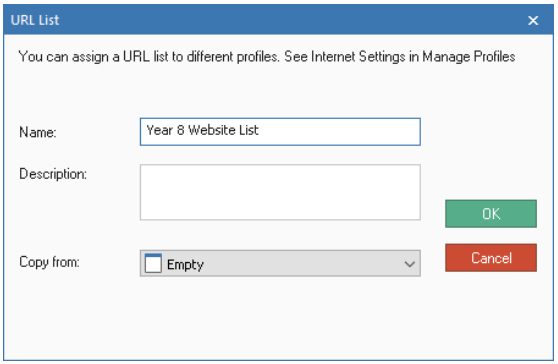
Note: To use the internet blocking facility, you must first ensure that NetSupport DNA's Internet Restrictions are enabled at Agent machines. When installing an Agent, the Internet Restrictions are enabled by default. You can also deploy a NetSupport DNA Agent with Internet Restrictions enabled to the required PCs.

Creating an approved/restricted URL list

1. Click the **Internet Metering** icon drop-down arrow and select {URL Lists} from the menu.
   Or
   Click the **URL Lists** icon in the Internet Metering group.
2. The Internet Metering dialog will appear. Websites already visited by Agents will be listed automatically in the Available Sites list and the default URL list will be displayed.



3. To create a new website list, click . The URL List dialog will appear.



Enter a name for the list and, if required, a description. You can copy an existing list by selecting it from the 'Copy from' drop-down list.

Note: A URL Ignore list or At Risk URL list* can be copied. URLs from these lists will be added to the appropriate Sites list.

Click **OK**. To edit an existing list, click .

4. Ensure the correct list to add the approved/restricted websites to is selected from the drop-down menu.
5. To add an existing URL to the Approved or Restricted Sites list, select the URL in the Available Sites list. You can modify the filter that enforces the URL restriction to fine tune which occurrences of the URL are affected.

   For example:

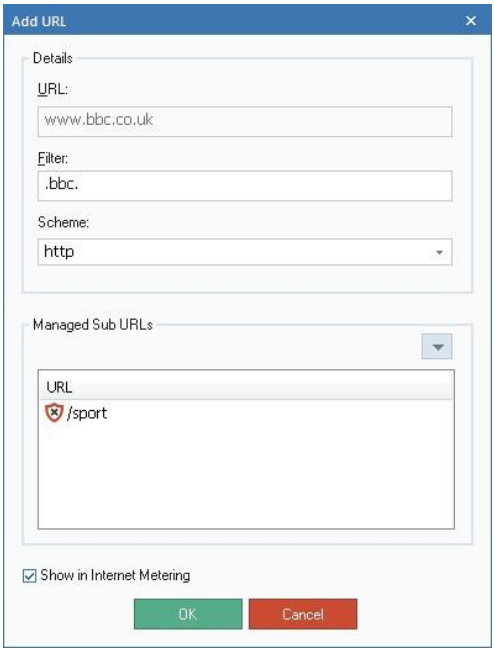
   Entering www.amazon.com as the URL will automatically create a filter of .amazon. This filter will block www.amazon.com and www.amazon.co.uk. However, if you modify the filter to read .amazon.com the internet restriction will not apply to amazon.co.uk.

   For further information, please see our website www.netsupportsoftware.com/support.

6. Click  and select **Edit URL** to edit the filter of a listed item and to indicate if the site should be excluded from being displayed in Internet Metering. Click **OK**.

Note: You can specify a scheme either of HTTP or HTTPS. This does not affect internet restrictions but ensures that hyperlinks displayed in the PC level web metering report link to the correct website.

7. Transfer the selected URL to either the Approved or Restricted Sites list by clicking **Approve** or **Restrict**, or by dragging and dropping the URL into the required category. An appropriate icon will display next to the URL in the Available Sites list showing whether the item is approved or restricted.
8. To add a new site to the Approved or Restricted Sites list, click in the Approved or Restricted Sites list, select **Add URL** and enter the required details. The new website will appear in the appropriate Sites list and will also be automatically added to the Available Sites list. To delete URLs, click and select **Delete URL**.
9. Each URL can have a Sub-URL assigned to it which can be approved or restricted. Select the required URL from the Approved or Restricted list, click and select **Edit URL**. The Edit URL dialog will appear.



10. Click  in the Managed Sub URLs list and select **Add URL**. Enter the Sub-URL and select whether to approve or restrict the URL. Click **OK**. The Sub-URL will be displayed under the appropriate Sites list.
11. Click **OK**.

To view full website usage data, select the required website in the Available Sites list and click the **Usage** button. The Website Usage dialog appears, showing which users have accessed the website and how many times they have visited. Clicking a user will display a full breakdown of when and how long the user accessed the website for.

Note: To exclude URLs from being displayed in the Internet Metering list, click the required URL and un-tick **Show in Internet Metering**. This may be useful, for example, if you do not wish to view URLs that users are approved to use.

Assigning a URL list to a profile
URL lists can be assigned to a profile and activated as and when required in the Internet Metering settings.

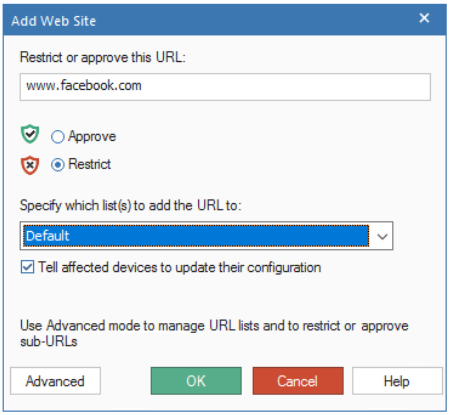
1. In the Settings tab, select **Manage Existing Profiles**.
2. Select the required profile from the list and click **Settings**.
3. Select **Internet Metering**.
4. The Internet Metering settings will be displayed.
5. Select the required URL list from the URL list drop-down menu.
6. For the list to be activated, the internet access level must be set to one of the 'restrict internet access' options. Or, if using custom access, the 'approved sites' or 'block restricted sites' enabled.
7. Click **Save** to apply the changes.

* These are only available in the Education Edition of NetSupport DNA.

Using the Spotlight feature to assign URLs to an Approved or Restricted list

The Spotlight feature, available in Explorer mode, offers a quick and easy method for adding URLs to an approved or restricted list.

1. In the ribbon, select the **Explorer** icon.
2. Select an Agent machine in the information window or in the hierarchy tree.
3. From the View section of the ribbon, select **Spotlight**. The Spotlight window will open and the processes, services, applications and websites currently running at the selected machine will be displayed.
4. Click the Websites tab. The currently open website will appear.
5. Right-click on the website and select **Restrict Website** or **Approve Website**.
6. The Add Website dialog will appear.



Check that the displayed URL is correct and confirm that the URL should be added to the Approved or Restricted URL list as previously selected.

If you have multiple URL lists created for different profiles, select the list that this URL should be added to.

By default, you can update affected machines with the new URL list immediately. If unticked, the changes will apply when the Agent machines restart.

Click **OK**.

The specified URL will be added to the appropriate Approved / Restricted URL list.

Note: You can quickly access the URL Lists dialog by clicking **Advanced.**

Application Metering

The Application Metering module reports on all applications used on each PC or server, detailing the time the application was started and finished, as well as the actual time it was active.

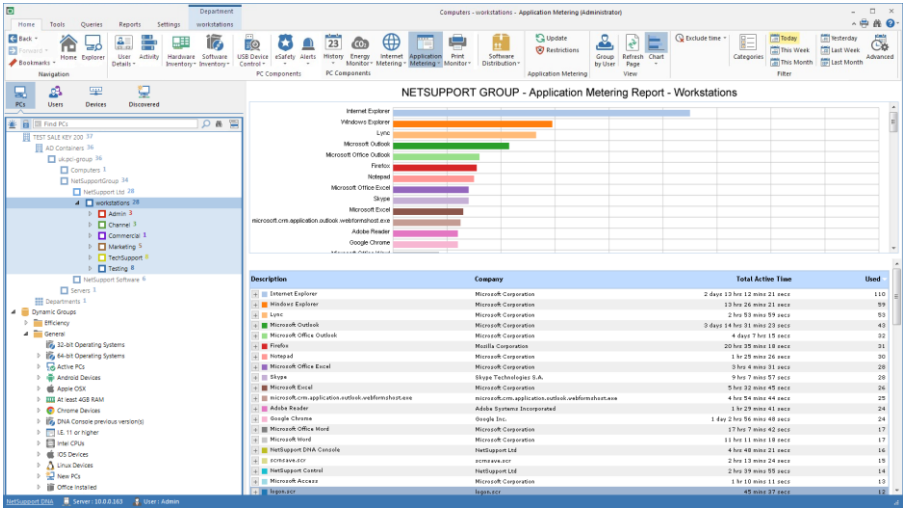
Monitoring application use ensures software licences are assigned to the right users and aren't renewed for users without matching application activity, thus enabling cost savings.

Application usage can also be restricted for users or departments, either fully or just by time of day. Lists of approved and restricted applications, together with times when restrictions apply, can be created and enforced centrally.

Application Metering enables the business to monitor and report current licence use levels for all installed applications and ensure that application usage complies with corporate policy. Reports can be presented by PC or logged-on user.

1. Click on the **Application Metering** icon in the ribbon. The Application Metering window will appear.

Note: If the component icons are not visible, click the Home tab.



You can switch the Tree view between PCs and Users. The PCs Tree view displays data for the PC owner who is associated to a PC and the Users Tree view displays data for logged on users.

In the Tree view, select the level at which you want to view the metering data: company, department, AD Container, Dynamic Group or individual Agent.

The information window will display a breakdown for each selected item in graph and list format. To view the graph in a different format, click the **Chart** icon drop-down arrow on the ribbon and select the appropriate format. To print the active view, click the  icon at the top of the Console.

Note: Clicking the **Chart** icon in the ribbon will hide/show the graph.

You can view data for a specified period. To switch between different time periods, click the appropriate icon in the Filter section of the ribbon. Clicking **Advanced** allows you to apply a customised date/time filter. Listed descriptions can be expanded to provide an individual Agent breakdown for each item. Applications that have been open for less than a specified time can be ignored if required.

Selecting **Group by User** allows you to view application usage based on Agents' User ID's and not the PC. This option will not be available in the Users Tree view.

Selecting **Group by PC** allows you to view application usage based on the PC details and not the Agent Users details when in the Users Tree view. This option will not be available in the PCs Tree view.

Note: By selecting different levels in the Tree view, you can view Agent application usage on PCs across different levels of the organisation.

A useful way of targeting specific application usage and limiting the amount of data displayed is to group 'similar' applications together into categories. For example, to see how much time users spend playing solitaire, you could create a group containing games. See Application Groups for more information. To display a category, click the **Categories** icon, select the required group to view and click **OK**. The information window will display data just for that category. A yellow header will be displayed advising what category you are viewing. You can switch categories and clear categories from here.



A quick refresh facility enables you to update data outside of the specified frequency. This can be useful for targeting particular Agents or departments. Right-click on the required item in the Tree view and select **Update** or click **Update** in the Applications drop-down menu or ribbon.

Queries
Select the Queries tab to display the Queries window.

NetSupport DNA's Query tool enables you to interrogate the database for records matching specified criteria. Queries specific to the component currently being viewed will be listed, enabling fast retrieval of the results.

Click the **Add Query** icon in the ribbon to create a new query or click the **Edit Query** icon in the ribbon to edit an existing item in the list.

Reports
Select the Reports tab to display the Reports window.

A number of pre-defined management reports, powered by the Crystal Reports engine, are attached to each component. Select the required report from the drop-down list. The results will be listed in the information window. These can be exported if required.

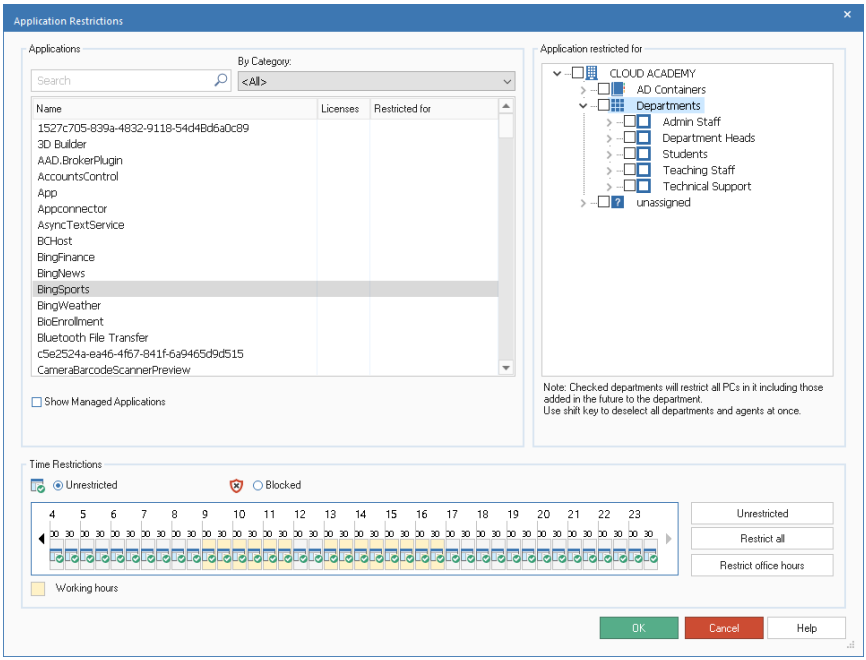
Notes:

- The frequency at which the server collects data can be adjusted using the NetSupport DNA settings option.
- The date/time format displayed in the Console is taken from the machine where the NetSupport DNA Server is installed. To change the format in the Console, you will need to change the system date/time format on this machine. For further information, visit www.netsupportsoftware.com/support.

Application Restrictions

To ensure that application usage complies with your company policies, you can create lists of approved and restricted applications and apply time frames for when the restrictions apply.

1. Click the **Application Metering** icon drop-down arrow and select {Restrictions} from the menu.
   Or
   Click the **Restrictions** icon in the Application Metering group.
2. The Application Restrictions dialog will appear.



A list of all applications is displayed, along with licence details and the number of Agents the application is approved or restricted for.

Note: Licence information will only be displayed if the application group has been linked to the relevant installed program in the Edit Application Group dialog.

Search
You can quickly search for applications by typing in the Search box and clicking .

By Category
To view applications that have been grouped together, select the required category from the drop-down list.

Note: Categories can be created in the Application Groups dialog.

Show Managed Applications
If checked, this option enables you to see at a glance which applications already have restrictions in place and to which users they apply. Any applications that have licence details available will also be displayed.

If unchecked, a full list of scanned applications is shown, enabling you to select an item to apply restrictions to.

To set up restrictions
1. Select the required application in the list. The Application restricted for window will list the Tree view.
2. To restrict certain Agents from using the application, check the required PC in the Tree view. Checking a department will restrict the application for all PCs (including any new PCs added or moved in the future) in that department.
3. You can choose to restrict access at specific times during the day.

   Select 

   and, using the arrows, scroll to the desired time frame and click on the segment to apply the restriction. Select 

   to apply unrestricted access.

4. Clicking **Unrestricted** will allow unrestricted access across the day. Clicking **Restrict all** will restrict all access across the day. Clicking **Restrict office hours** will restrict access just during the working hours.

   Note: The current office working hours will be shaded yellow. These can be amended to suit your organisation in the Console Preferences - General settings.

5. The Applications window will indicate how many Agents have the restriction applied. Click **OK** to save the details.

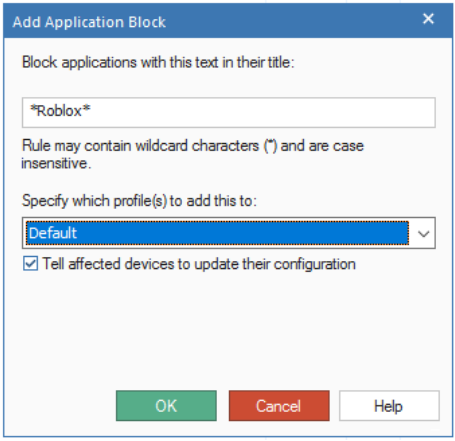
To apply restrictions

1. In the Settings tab, select **Manage Existing Profiles**.
2. Select the required profile from the list and click **Settings**.
3. Select **Application Metering**.
4. The Application Metering settings will be displayed.
5. Under Company Application Restrictions, click **Enable**.
6. Click **Save**.
7. The application restrictions you created will be applied across the organisation.

Block applications by Window Title

As well as blocking applications by name, you can also block based on the app's Window title. The Spotlight feature, available in Explorer mode, offers a quick and easy method for adding a currently running application to the Title Blocking settings:

1. In the ribbon, select **Explorer** icon.
2. Select an Agent machine in the information window or in the hierarchy Tree.
3. From the View section of the ribbon, select **Spotlight**. The Spotlight window will open and the processes, services, applications and websites currently running at the selected machine will be displayed.
4. Click the Applications tab.
5. Right-click on the required application and select **Block**. (You can also close the application if preferred.)
6. The Add Application Block dialog will appear.



7. The Window title of the currently running application will appear. To ensure all applications with a similar title are blocked, you can edit the title and use wildcard characters.
8. From the drop-down list, choose the profile that this restriction should apply to.
9. By default, you can update affected machines with the updated blocked list immediately. If unticked, the changes will apply when the Agent machines restart.
10. Click **OK**.
11. The application will be added to the Title Blocking settings.

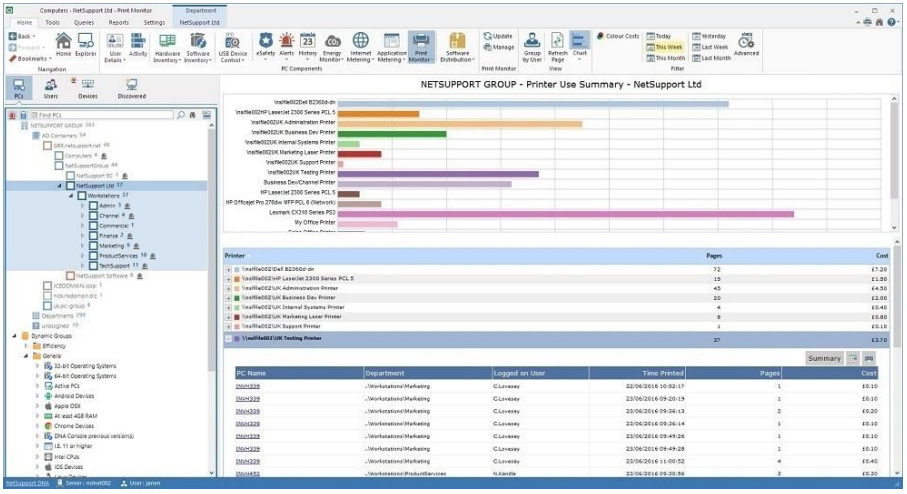
Print Monitor

NetSupport DNA includes a high-level Print Monitoring feature. Individual printers across the enterprise are automatically identified and, from the central console view, costs for printing (black and white, colour and so on) can be assigned either globally or against each different printer. Where required, printers can also be excluded from the view. A full overview of printing activities and indicative costs across the enterprise is provided by NetSupport DNA.

Note: Print monitoring relies on printer notifications returning to the DNA Agent informing it what has been printed. Any printing environment where this is prevented, or where identification of print jobs in notifications has been modified, might give unexpected results. For example, this could happen where authentication to a print server uses credentials other than the user's logged on user name, where printing occurs on servers in a different domain, or where print notifications are blocked by firewalls or proxy servers.

1. Click on the **Print Monitor** icon in the ribbon. The Print Monitor window will appear.

   Note: If the component icons are not visible, click the Home tab.



In the Tree view, select the level at which you want to view the data: company, department, AD container, Dynamic Group or individual Agent.

The information window will display a breakdown for each selected item in graph and list format. To view the graph in a different format, click the **Chart** icon drop-down arrow on the ribbon and select the appropriate format. To print the active view, click the  icon at the top of the Console.

Note: Clicking the **Chart** icon in the ribbon will hide/show the graph.

You can view data for a specified period. To switch between different time periods, click the appropriate icon in the Filter section of the ribbon. Clicking **Advanced** allows you to apply a customised date/time filter. Listed descriptions can be expanded to provide an individual Agent breakdown for each item.

The working hours shown can be amended to suit your organisation in the DNA Configuration dialog. See **Console Preferences - General** for further information.

Selecting **Group by User** allows you to view print usage based on Agents' user ID's and not the PC. This option will not be available in the Users tree view.

Selecting **Group by PC** allows you to view print usage based on the PC details and not the Agent user's details when in the Users tree view. This option will not be available in the PCs tree view.

By default, all types of printing will be listed. You can view just the colour printing costs by clicking **Colour Costs** in the ribbon.

To configure the cost settings of printing, select the **Print Monitor** icon drop-down list and select {Manage} or click the **Manage** icon in the ribbon.

The frequency at which the server collects data can be adjusted using the NetSupport DNA settings option.

A quick refresh facility enables you to update data outside of the specified frequency. This can be useful for targeting particular Agents or departments. Right-click on the required item in the Tree view and select **Update** or click **Update** in the **Print Monitor** icon drop-down menu or ribbon.

Queries
Select the Queries tab to display the Queries window.

NetSupport DNA's Query tool enables you to interrogate the database for records matching specified criteria. Queries specific to the component currently being viewed will be listed, enabling fast retrieval of the results.

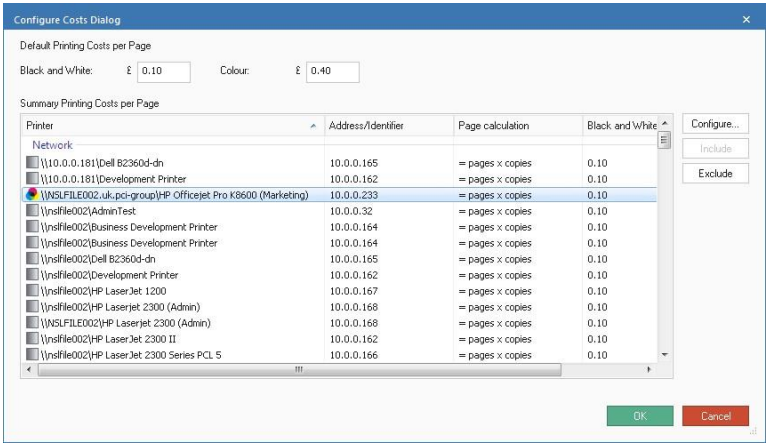
Click the **Add Query** icon on the ribbon to create a new query or click the **Edit Query** icon in the ribbon to edit an existing item in the list.

Reports
Select the Reports tab to display the Reports window.

A number of pre-defined management reports, powered by the Crystal Reports engine, are attached to each component. Select the required report from the drop-down list. The results will be listed in the information window. These can be exported if required.

Configure Print Costs
This dialog displays all printers across the company. From here, you can exclude printers that you don't wish to monitor as well as set up and configure the costs involved in printing.

1. Select the **Print Monitor** icon drop-down list and select {Manage}.
   Or
   Click the **Manage** icon in the ribbon.



A summary of all the printers across the company will be listed, with an identifier showing if it is a black and white or colour printer. By default, all printers will be included for monitoring in the information window. You can choose to exclude printers that you do not wish to monitor by clicking **Exclude**. To exclude all printers with the same name (this may be useful if you want to exclude all instances of Adobe PDF), right-click on the required printer name and select **Exclude all 'xxx'** from the list.

Note: Printers that are excluded will be moved to an "excluded" section at the bottom of the printer list and, from here, they can be included again.

By default, the printing costs per page are set to £0.10 for black and white and £0.40 for colour printing. Overtype this to change the costs. Changing the costs here will change them for all printers. You can change the costs for an individual printer by selecting the printer and clicking **Configure**.

Note: When printing black and white documents on a colour printer, they will be charged at the colour cost, unless the user chooses to print in greyscale.

Software Distribution

NetSupport DNA provides a multi-delivery option for software distribution, enabling timely and cost-effective application deployments across the enterprise. An Operator defines a software package containing a collection of files or folders to be deployed. Once created, the package can be automatically "pushed" to target PCs or "published/advertised" centrally in order for users to access and install on demand. Defined packages can also be "scheduled" to deploy at specific times.

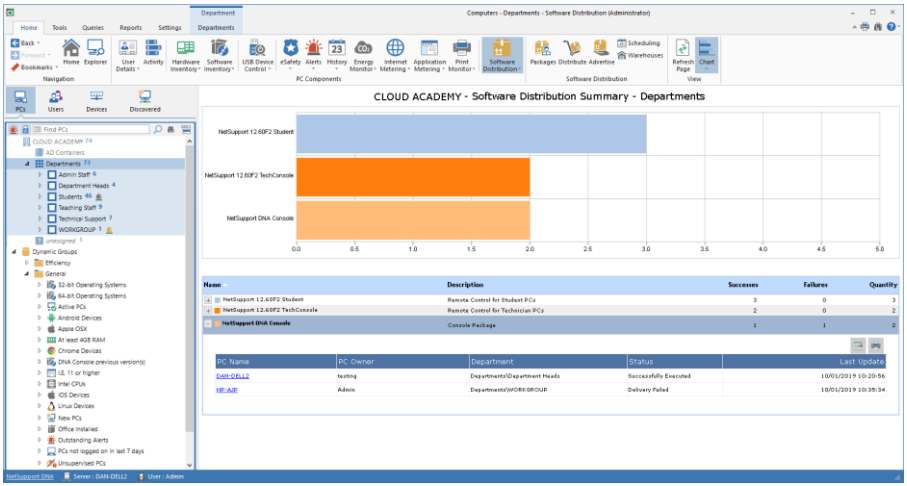
Action parameters can also be included in the package enabling you, for example, to build in any user prompts required during the application install, so that the package can be deployed onto a user's system without intervention.

When planning the deployment, you can utilise NetSupport DNA's Hardware and Software Inventory features to ascertain the current status of the assets within your organisation, to ensure compatibility. Similarly, configured systems can be grouped to ensure the rollout is as efficient as possible.

NetSupport DNA also considers the effect that deploying large packages across the network can have. Network overheads will naturally increase as packages are pushed out to multiple Agent machines from the NetSupport DNA Server. To help ease congestion, you can create a 'distribution warehouse' local to the Agent machines. The package is deployed to the warehouse and nominated Agents are then serviced from this local 'server'.

1. Click on the **Software Distribution** icon in the ribbon. The Software Distribution window will appear.

   Note: If the component icons are not visible, click the Home tab.



In the Tree view, select the level at which you want to view the Distribution data: company, department, AD container, Dynamic Group or individual Agent.

The main information window will display a breakdown of distributed packages for each selected item in graph and list format. To view the graph in a different format, click the **Chart** icon drop-down arrow on the ribbon and select the appropriate format. To print the active view, click the  icon at the top of the Console.

Note: Clicking the **Chart** icon in the ribbon will hide/show the graph**.**

For each listed package, a count of successful or failed distributions is provided. The drill-down lists can be expanded to provide an individual Agent breakdown for each item.

Note: The date/time format displayed in the Console is taken from the machine where the NetSupport DNA Server is installed. To change the format in the Console, you will need to change the system date/time format on this machine. For further information, visit www.netsupportsoftware.com/support.

Queries
Select the Queries tab to display the Queries window.

NetSupport DNA's Query Tool enables you to interrogate the database for records matching specified criteria. Queries specific to the component currently being viewed will be listed, enabling fast retrieval of the results.

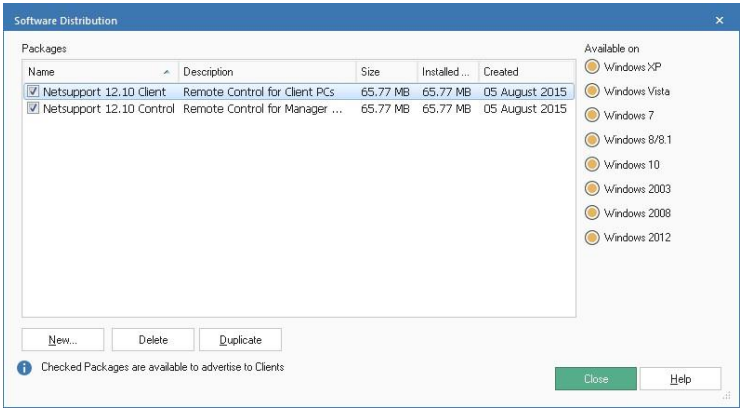
Click the **Add Query** icon on the ribbon to create a new query or click the **Edit Query** icon in the ribbon to edit an existing item in the list.

Reports
Select the Reports tab to display the Reports window.

A number of pre-defined management reports, powered by the Crystal Reports engine, are attached to each component. Select the required report from the drop-down list. The results will be listed in the information window. These can be exported if required.

Create Software Distribution Packages

1. Click the **Software Distribution** icon drop-down arrow and select {Package Administration} from the menu.
   Or
   Click the **Packages** icon in the Software Distribution group.
   Or
   In the Tools tab, click the **Package Administration** icon.
2. The Package Administration dialog will appear. Details of any existing packages are listed. Any that are checked will be advertised at Agent PCs.

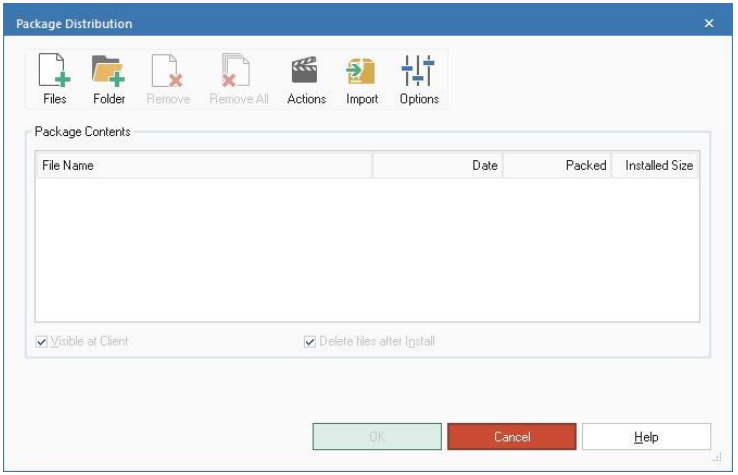


3. Click **New** to create additional packages for distribution.
   Or
   Click **Delete** if a package in the list is no longer required.
   Or
   Click **Duplicate** if you want to clone an existing package. This can be useful if you need to distribute the same package but with some additional parameters included. The amended version will be added to the list.

Available on
Shows the supported operating systems for each individual package. This can be specified when creating a new package.

Create New Package

This dialog enables you to specify the files/folders and additional action parameters to include in the package.



1. Select **Files** or **Folder** and locate the file(s) to be integrated into a package for distribution. The file will appear in the Package Contents list.
2. Highlight the package and click **Actions** to add the required parameters/command line instructions to be run when the distributed package arrives at Agent PCs. A variety of pre-defined parameters are also available, including the **Copy Command** which can be used to copy files, such as images from their source location to the specified target folder. Click **OK**.
3. Click **Options** and decide whether to distribute the package using NetSupport DNA's default admin account or an admin user name and password present on your domain.
4. Select **Visible at Agent** if you would like to make this package available to advertise to Agents (applicable to a department and company only).
5. After installation, the package setup files can be removed from the Agent machine(s). Select **Delete files after install**.
6. Click **OK**.
7. The Test Package dialog will appear. Before storing the package, you can test it to ensure reliability or, if you are happy, click **Save Package**.
8. Enter a name and description for the package. You can also specify which operating systems are supported by the package. All are

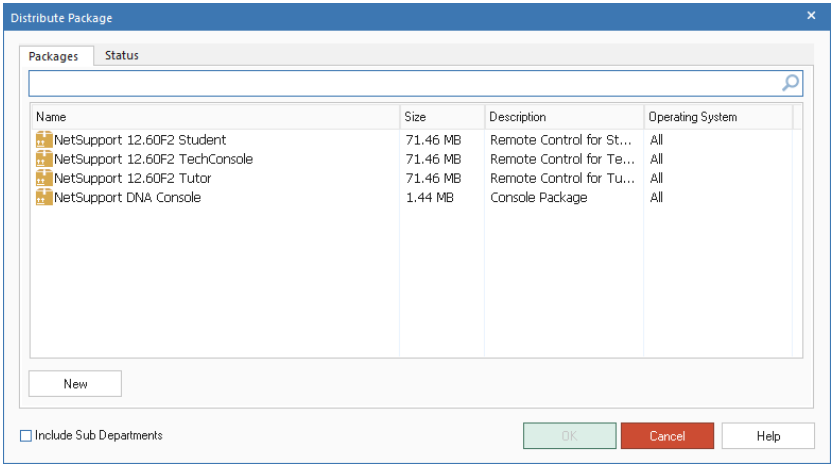
selected by default. Agents that do not match the specified operating systems will be excluded from the distribution. Click **Finish** to confirm. The package will be sent to the server ready for distribution.

The import facility can be used to retrieve packages from the server for editing purposes.

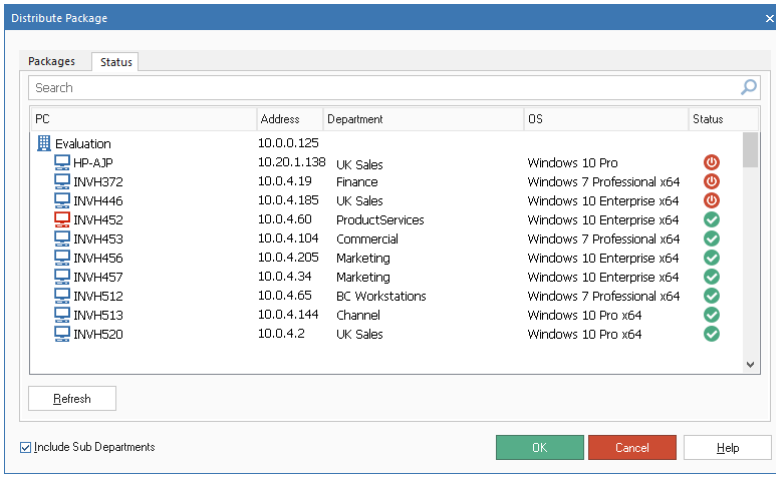
Distribute a Package

Once you have created the required package, it can be deployed to selected Agents.

1. In the Tree view, highlight the Agent, department, AD container, Dynamic Group or company that you wish to distribute the package to.
2. Right-click and select **Distribute**.
   Or
   Click the **Software Distribution** icon drop-down arrow and select {Distribute} from the menu.
   Or
   Click the **Distribute** icon in the Software Distribution group.



3. All packages previously created will be listed. Highlight the required file. If the required package is not available, you can create it from here - click **New**.
4. If distributing to a company, department or AD container, ensure the **Include Sub-departments** box is checked if you wish to include all departments/Agents within that area.
5. Before proceeding, you can check the status of the PCs you are about to distribute to. Select the Status tab to indicate whether the PCs are available (green), not available (red) or logged off (amber).

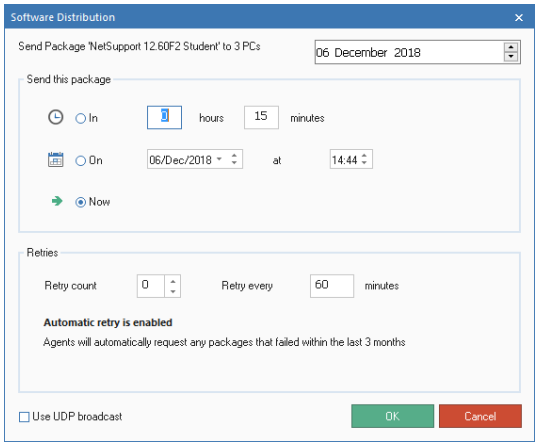


6. Click **OK**. The Schedule Distribution dialog will appear. Indicate whether the package should be deployed immediately or on a specific date/time. Delayed deployments can be viewed on the Schedule Packages dialog. You can enter a number of retry attempts in the event the distribution fails and also set the interval between the attempted retries.

   In addition, an automatic retry facility allows you to handle failed distributions for PCs that are turned off or unavailable when the distribution is sent. You can enable/disable automatic retries and specify the time period that failed packages will still be available for Agents to automatically request using the NetSupport DNA settings option.

   If required, select **Use UDP broadcast** to distribute via the broadcast method.

   Note: If using the broadcast distribution method, PCs must be on the same subnet as the NetSupport DNA Server, otherwise distribution will fail.



7. Click **OK** to distribute the package. The distribution window will display the results.

Note: When creating a package, you can specify what credentials (user name and password) are used when the package is sent to an Agent. If no credentials have been supplied, then NetSupport DNA uses the default 'SYSTEM' credentials (recommended), which allows full access to install MSI installers and alter files local to the Agent. If the package requires specific credentials, for example, to access a network resource, you can enter them.

When sending a package and the Agent has any user logged on:

- The supplied credentials will be used to execute all parts of the package.
- If the credentials are incorrect, the package will not run and NetSupport DNA will report the error.

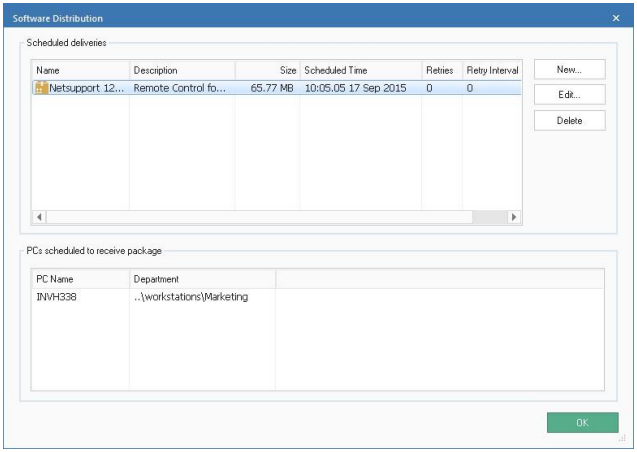
When sending a package and the Agent is logged off:

- The supplied credentials will only be used if access to network resources is required. All other elements of the package will use the default credentials.
- If the credentials are incorrect, the package will not run and NetSupport DNA will not report the error.

Scheduling a Package

When creating a package for distribution, you can schedule the deployment for a specific date or time. This would be useful if you want to distribute files out of office hours. This dialog is used to edit the properties of scheduled distributions or create new schedules.

1. With the Software Distribution component selected, highlight an Agent, department, AD container, Dynamic Group or company in the Tree view.
2. Right-click and select **Scheduling**.
   Or
   Click the **Software Distribution** icon drop-down arrow and select {Scheduling} from the menu.
   Or
   Click the **Scheduling** icon in the Software Distribution group.
3. The Scheduled Packages dialog will appear. Details of any packages that you have scheduled for distribution will appear, along with the names of any Agents associated with the package.

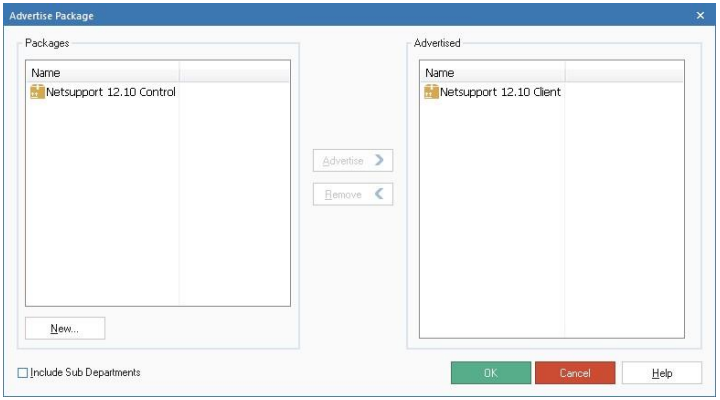


4. Click **New** to create a new distribution schedule.
   Or
   Click **Edit** to amend the distribution details of an existing scheduled package.
   Or
   Click **Delete** if a package in the list no longer needs to be distributed.
5. Click **OK** when you are finished.

Advertise a Package

Advertising, or publishing, a package gives Agents the opportunity to install a package at their convenience. Packages are created in the usual manner but, rather than being deployed immediately, the setup files are held at the server and can be 'pulled' by nominated Agents as required.

1. In the Tree view, highlight the department, AD container or company that you wish to advertise the package to. The action cannot be performed at Agent or Dynamic Group level.
2. Right-click and select **Advertise**.
   Or
   Click the **Software Distribution** icon drop-down arrow and select {Advertise} from the menu.
   Or
   Click the **Advertise** icon in the Software Distribution group.
3. The Advertise Package dialog will appear. All packages that have been created with the **Visible at Agent** option enabled will be listed. To create a new package, click **New**.

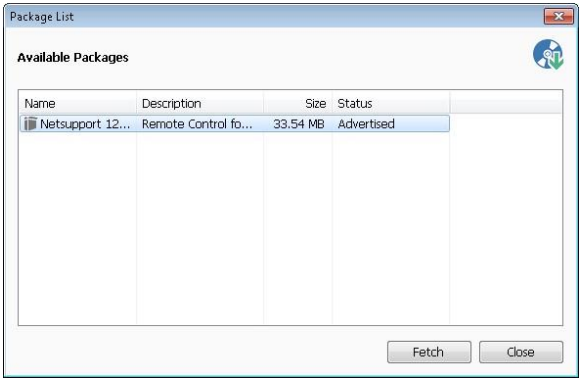


4. Select the required package and click **Advertise** to transfer to the Advertised box.
5. Select **Include Sub Departments** if you wish all departments/Agents below the current level to be included in the distribution.
6. Click **OK**.

Request a Package

Advertised packages can be 'pulled' from the server by Agents using the Request Package tool.

1. At the Agent machine, right-click on the NetSupport DNA icon in the taskbar and select **Request Package**.
2. The Package List dialog will appear, listing all packages available to that Agent.



3. Highlight the required package and click **Fetch**. The application setup files will be executed at the Agent. The status of the package will change to indicate that it has been delivered to the Agent.

Note: Console Operators have the ability to remove an Agent's access to request packages by editing the Software Distribution settings. They can also include 'non' advertised packages in the Package list as shown above, but Agents can only install advertised items.

Import a Package

The Import option enables you to retrieve a stored distribution package from the server with a view to editing the package content.

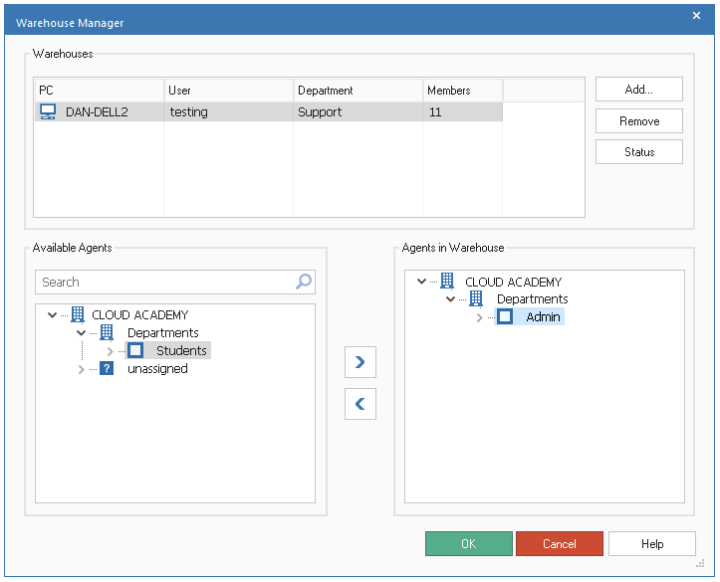
1. Click the **Software Distribution** icon drop-down arrow and select {Package Administration} from the menu.
   Or
   Click the **Packages** icon in the Software Distribution group.
   Or
   In the Tools tab, click the **Package Administration** icon.
2. The Package Administration dialog will appear.
3. Select **New**. The Package Distribution dialog will appear.
4. Select **Import**. Navigate to the Packages folder, c:\program files\netsupport\netsupport dna\server\packages, and choose the required Package. Click **Open**.
5. If required, click **Actions** to include additional parameters.
6. Click **OK**.
7. The Test Package dialog will appear. Before storing the package, you can test it to ensure reliability or, if you are happy, click **Save Package**.
8. Enter a name and description for the package and click **Finish**. The package will be resubmitted to the server ready for distribution.

Software Distribution Warehouse

When planning a large-scale deployment, consider the effect that it will have on your network. Packages being pushed out to multiple Agents across remote networks will naturally have an impact on resources.

To ease congestion, NetSupport DNA enables you to nominate an Agent, ideally local to the target machines, to act as a 'distribution warehouse'. When the package is deployed, rather than the server pushing it to each Agent in turn, it installs at the warehouse Agent, which then distributes it to the remaining targets.

1. Click the **Software Distribution** icon drop-down arrow and select {Warehouses} from the menu.
   Or
   Click the **Warehouses** icon on the Software Distribution group.
2. The Warehouse Manager dialog will appear.



3. Existing warehouse PCs will be listed. Highlight an item to view Agents currently being serviced by the warehouse and details of Agents that are available to be added to it. Click **Status** to display details of packages currently residing in the warehouse.

4. To create a new warehouse, click **Add**. The Select Warehouse dialog will appear, enabling you to assign an Agent machine to host the warehouse.
5. Choose the Agents that will be serviced by the warehouse. From the 'Available Agents' Tree, highlight the required department or Agent(s) and click . To remove an Agent from the warehouse, click .

Note: To search for an item in the Tree view, enter the name or partial name of the PC in the search box and click . The first matching item in the Tree view will be displayed along with the number of matches found. You can scroll through these using the arrows. Click  to clear the search.

6. Click **OK**.

NetSupport DNA Application Packager

The NetSupport DNA Application Packager complements the Software Distribution facility and is ideally suited to situations where the application to be rolled-out does not have its own 'silent' install routine. (If the software to be installed does support silent/automated routines, it is recommended that these are used.) The Application Packager enables Operators to record and playback a third-party installer. All necessary keystrokes and mouse movements are stored in a script which is then played back at Agent PCs without the need for user intervention. NetSupport DNA's Software Distribution option is used to push the stored script out to the required Agent PCs.

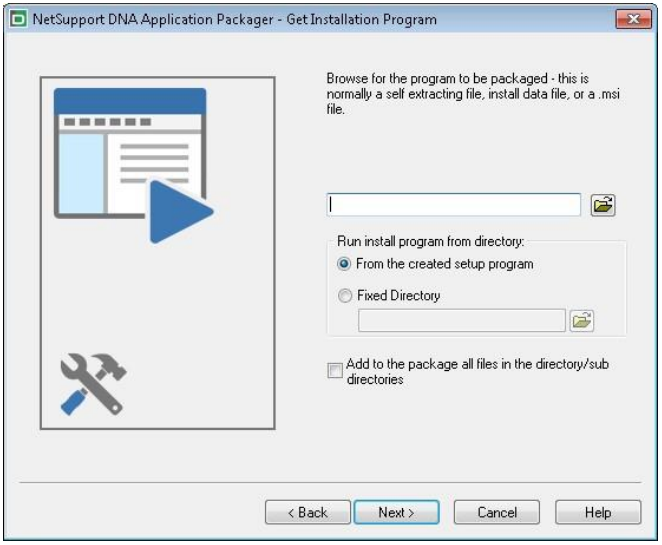
Note: The Application Packager can be used to record and playback "low complexity" product installers. The Application Packager relies on the same sequence of installer screens being presented when running the installation on the target machines. Any unexpected dialogs displayed during playback will result in the installation process being halted.

If required, a Script Editing tool is provided, which enables you to handle certain differences.

1. To load the Application Packager, select {Start}{Programs}{NetSupport DNA}{DNA Application Packager}.
2. The Application Packager Welcome dialog will appear. The Application Packager wizard will guide you through the recording process.
3. Click **Next**.

Get Installation Program

Use this dialog to specify the program to be packaged and the directory to extract the installed setup files to at the Agent PC.

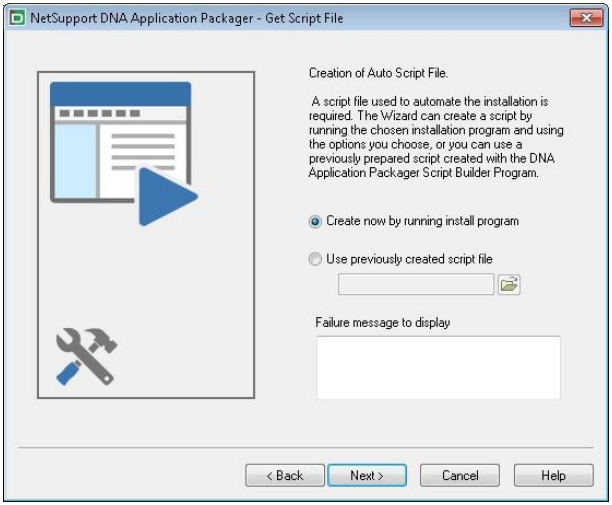


1. Browse to find the required program setup file.
2. Indicate where the installed program should be run from at the Agent machines. When pushed to Agent PCs, the .exe file created by the Application Packager is stored in C:\program files\netsupport\ netsupport dna\Agent\packages. Unless you specify an alternative fixed directory from which to run the setup in future, it will always be accessed from the above setup program directory.
3. Select **Add to the package all files in the directory/sub directories**, if you require these additional files to be available during installation. They will be deleted upon successful installation.
4. Click **Next**.

Get Script File

When the packaged application is pushed to Agent PCs, the actions required to perform the installation are contained in a pre-defined script. The script can be created at this stage by running the installation and having the keyboard/mouse movements recorded or you may have an existing script which contains the procedure.

NetSupport DNA's Application Packager provides a Script Building utility which can be used to manually create and edit script files.



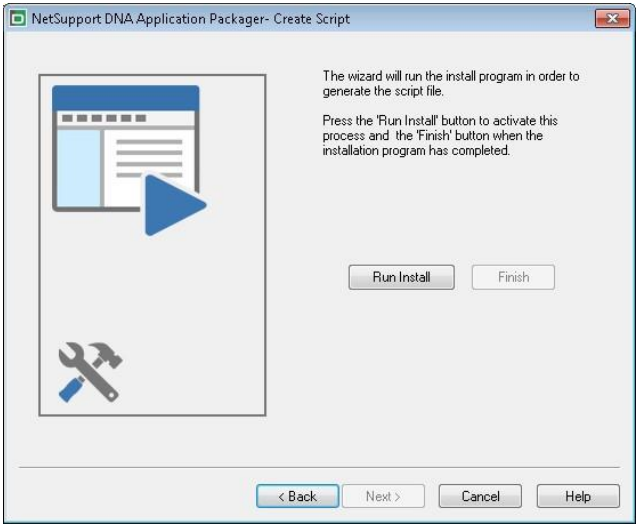
If you are using a previously created script file, browse for the appropriate *.rscrpt file.

Should the install encounter a problem, you can display a custom message. Enter a suitable failure message in the box provided.

Click **Next**.

Create Script

This dialog appears if you have chosen to create the script by running the install program now rather than use a pre-defined *.rscrpt file.



Click **Run Install** to launch the selected programs installer. The installation will take place in real-time at the Operator's machine. As you work through the process, each key depression or mouse movement is recorded and added to the script file. Remember that this is exactly how the installation will run at Agent PCs when it is pushed out. If you inadvertently press a key or select an option by mistake, you can always edit the script before distributing it to Agents.

When the installation is complete, click **Finish**.

Click **Next** to continue.

Additional Files

There may be instances where the specified setup relies on the presence of additional files in order to complete the installation or there may be a number of associated application files that you want to bundle with the setup and make available to users after installation.

Source Directory
Specify the location of the 'additional' install and/or application files and indicate whether the content of any sub-directories should be included.

Target Directory
Identify a target directory at the Agent machines to extract the files to.

Click **Next**.

Build Options

Name to give created program
Decide where to store the package executable in readiness for distribution.

Options

Lock Mouse/Keyboard
While the installation is running, you can lock the Agents' mice and keyboards to ensure users do not interrupt the automated process.

Allow Cancel Script
Enables Agents to interrupt the installation by pressing CTRL-BREAK.

Password Details
These options enable you to password protect the distributed file and customise the dialog that appears at Agent machines.

Click **Next**. The package will now be created.

NetSupport DNA Application Packager - Script Builder

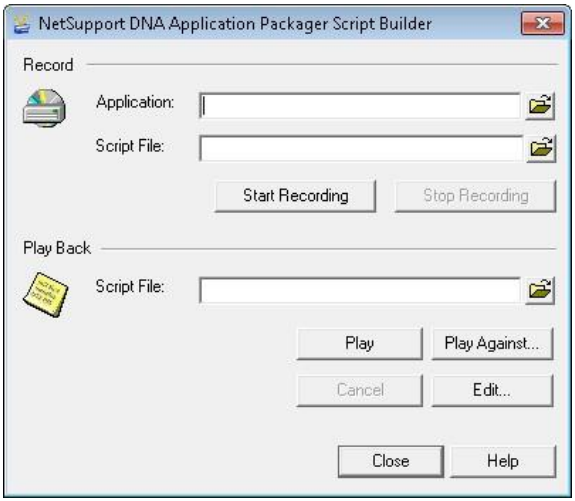
NetSupport DNA's Application Packager gives Operators the ability to record and playback third-party installers and is ideally suited for applications that do not provide a 'silent' install facility. The Application Packager guides Operators through the installation, recording the dialogs that appear and the responses made, the information being stored in a script.

If you are happy with the recorded procedure, it can be pushed out to Agent PCs. However, you may feel that an action recorded at the Operator's machine may not be required when the installation is run at Agent PCs or you may have inadvertently made an incorrect mouse click or key depression.

The Script Builder can be used to edit scripts created in the Application Packager or you can use it to record new scripts.

1. The Script Builder can be loaded from c:\program files\netsupport\netsupport dna\console\

.
2. The Script Builder dialog will appear.



Record New Script

Whilst the Application Packager utility provides a convenient wizard that will guide you through the process of creating the installer script, you can also use the Script Builder to record the required actions.

Application
Specify the location and name of the required applications setup file.

Script File
Specify a location and name for the new script file.

Click **Start Recording** to launch the specified setup file. The chosen applications installer will start and the Script Builder will record the dialogs that appear and the mouse/keyboard movements that the Operator executes. The installation is being performed in real-time at the Operator's machine but, also remember that this is the process that will run at Agent PCs when the script is distributed.

When the installation is complete, click **Stop Recording**.
If you want to review the finished script or make changes in the event that an action was performed incorrectly, click **Edit**.

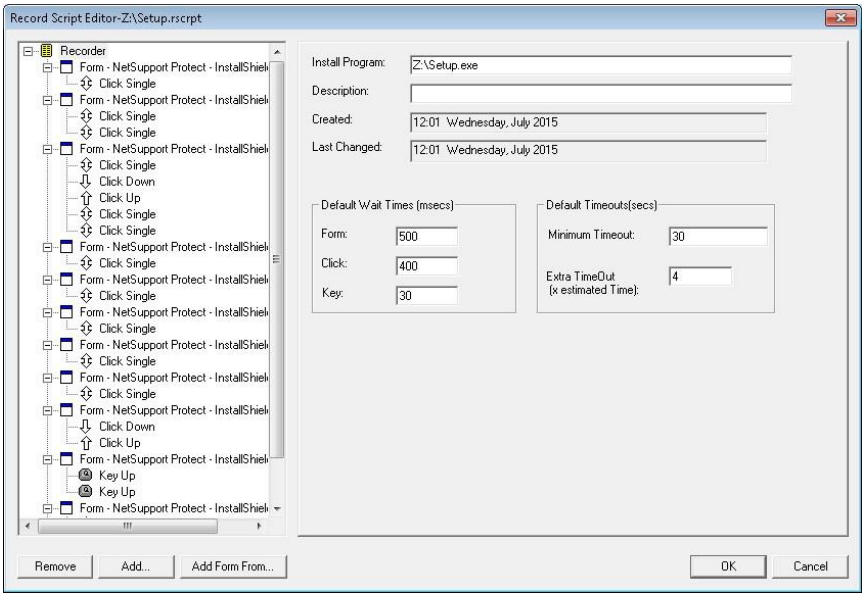
Edit Script

The Script Builder can be used to playback or edit stored installer scripts.

Play Back
Open the stored script (*.rscrpt file). Click **Play** to playback the recorded actions.

You can also test whether an existing script will successfully run against another setup file - for example, an updated version of the application already used. Click **Play Against** and browse for the new setup file.

Playing back the script may identify errors or missing actions. Click **Edit** in order to make changes to the script. The Script Editor will appear.



The left-hand pane of the window lists details of the recorded dialogs (Forms) along with any actions performed, mouse clicks etc. As you highlight each line of the script, the right-hand pane displays associated information.

The sample script above highlights some typical uses of the Editor.

- The Licence Agreement and Licence Information forms appear several times, indicating that the operator revisited these dialogs in order to rectify an error. For the final script to run successfully at Agent machines, the duplicated items need to be deleted by clicking **Remove**.

- While recording the installer, an Existing Installation has been detected at the operator's machine. As this may not be the case when the script runs at Agent PCs, you can indicate that the dialog is optional.

New items can be added to the script if required:

Add
Enables additional actions to be added to a form.

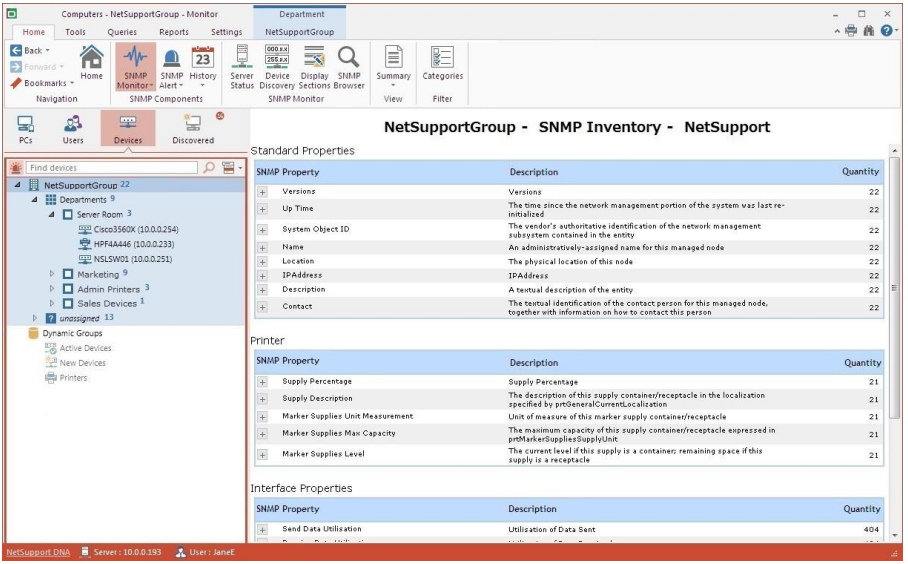
Add Form From
Enables a form to be inserted from another script. Specify the name of the script file and click **Load**. The entire script will be displayed from which you can select the individual form to add.

SNMP Monitor

Once Devices (such as printers and access points) have been discovered, they are stored within NetSupport DNA. The real-time data (such as ink or toner levels) can then be monitored from the console.

1. From the Devices Tree view, click the SNMP Monitor icon in the ribbon. The SNMP Monitor window will appear.

Note: If the component icons are not visible, click the Home tab.



Once the SNMP Devices have been discovered, they will be displayed in the Tree view.

Note: Devices are grouped automatically in the Tree view according to the values held in their location properties.

Select the level at which you want to view the displayed data: company, department, Dynamic Group or individual Device.

The information window will display a breakdown for each selected item in a list format. The SNMP properties are grouped together into display sections. To print the active view, click the  icon at the top of the Console.

Note: You can create and manage display sections and properties; click the **Display Sections** icon in the ribbon.

To limit the amount of data that is displayed in the information window, you can choose just to view certain SNMP categories. To display a category, click the **Categories** icon in the ribbon. Select the required categories to view and click **OK**. The information window will display data just for that category. A yellow header will be displayed advising what category you are viewing; you can switch categories and clear categories from here.

To view any leasing or maintenance contracts that have been associated with Devices, click the **SNMP Monitor** drop-down list and select {Display - Contracts} or click the **Contracts** icon in the ribbon.

To view the status of your SNMP Servers, click the **DNA SNMP Server Status** icon in the ribbon.

The frequency at which the server collects data can be adjusted using the NetSupport DNA settings option.

A quick refresh facility enables you to update data outside of the specified frequency. This can be useful for targeting particular Devices or departments. Right-click on the required item in the Tree view and select **Update** or click **Update** in the **SNMP Monitor** icon drop-down menu or ribbon.

Queries
Select the Queries tab to display the Queries window. NetSupport DNA's Query tool enables you to interrogate the database for records matching specified criteria. Queries specific to the component currently being viewed will be listed, enabling fast retrieval of the results.

Click the **Add Query** icon on the ribbon to create a new query or click the **Edit Query** icon in the ribbon to edit an existing item in the list.

Reports
Select the Reports tab to display the Reports window.

A number of pre-defined management reports, powered by the Crystal Reports engine, are attached to each component. Select the required report from the drop-down list. The results will be listed in the information window. These can be exported if required.

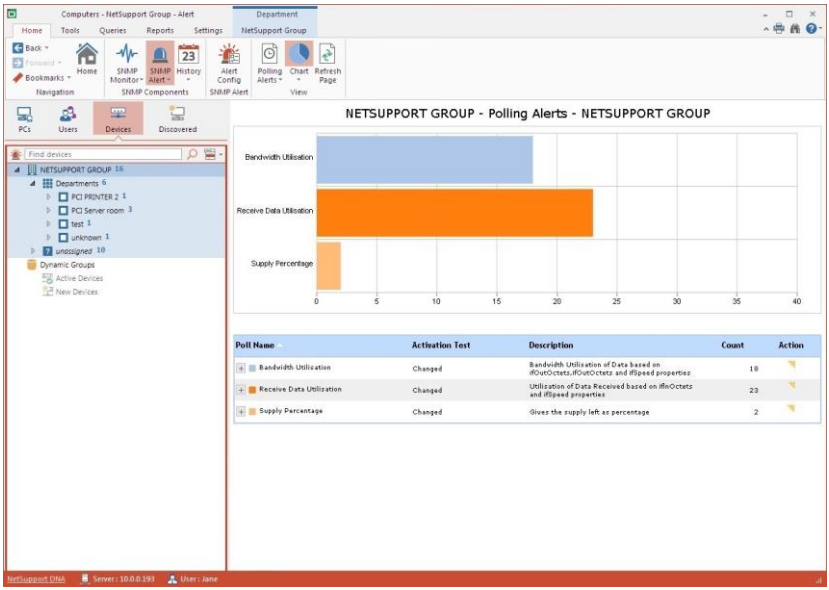
SNMP Alert

NetSupport DNA provides an alerting facility, enabling you to identify changes to the gathered SNMP data. For example, printer toner falling below XX%.

Alert notifications can be directed to specified email recipients and/or active Console users.

1. From the Devices Tree view, click the **SNMP Alert** icon in the ribbon. The SNMP Alert window will appear.

Note: If the component icons are not visible, click the Home tab.



In the Tree view, select the level at which you want to view the displayed data: company, department, Dynamic Group or individual Device.

The information window will display a breakdown for each selected item in graph and list format. Listed descriptions can be expanded to provide an individual Device breakdown for each item. To view the graph in a different format, click the **Chart** icon drop-down arrow on the ribbon and select the appropriate format. To print the active view, click the icon at the top of the Console.

Note: Clicking the **Chart** icon in the ribbon will hide/show the graph.

Outstanding alerts are identified against matching Devices on the main company Tree view. Once alerts have been identified, notes can be added by an Operator. A full history of all alerts is accessible from the History feature.

Note: You can show/hide alerts in the Tree view by clicking .

To configure the properties of an alert, select the **SNMP Alert** icon drop-down list and click **Alert Config**.

Queries
Select the Queries tab to display the Queries window.

NetSupport DNA's Query tool enables you to interrogate the database for records matching specified criteria. Queries specific to the component currently being viewed will be listed, enabling fast retrieval of the results. Click the **Add Query** icon on the ribbon to create a new query or click the **Edit Query** icon in the ribbon to edit an existing item in the list.

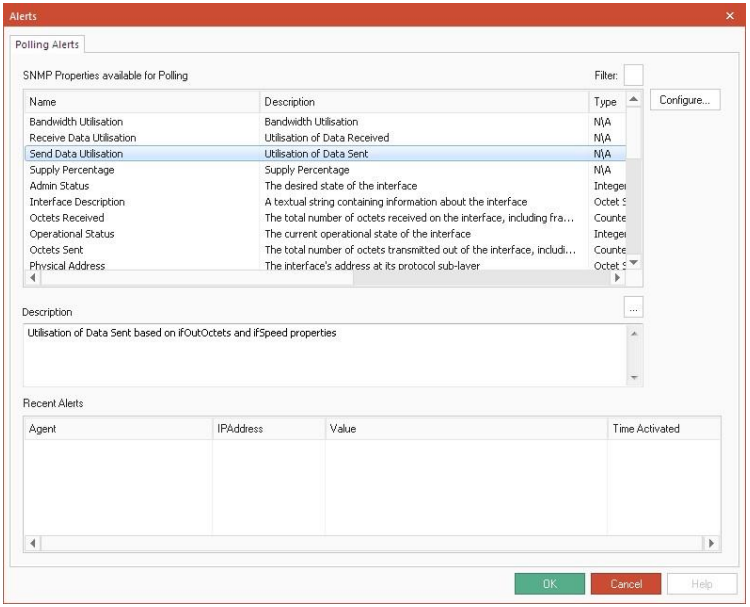
Reports
Select the Reports tab to display the Reports window.

A number of pre-defined management reports, powered by the Crystal Reports engine, are attached to each component. Select the required report from the drop-down list. The results will be listed in the information window. These can be exported if required.

Note: The date/time format displayed in the Console is taken from the machine where the NetSupport DNA Server is installed. To change the format in the Console, you will need to change the system date/time format on this machine. For further information, please contact our Support team www.netsupportsoftware.com/support.

SNMP Alert Configuration

This dialog allows you to see the SNMP properties that are available for alerts.

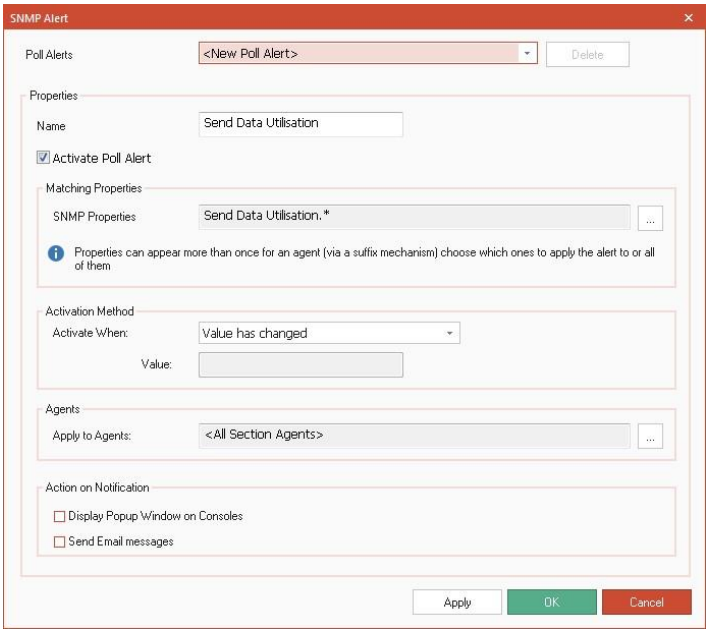


To make the list more manageable, you can filter the properties that are displayed. Click  and the Polling Filter dialog will appear.

To create a new alert or configure existing alerts, select the required SNMP property and click **Configure**.

Details of active alerts will be displayed in the Recent Alerts section.

Creating a New Alert



To create a new alert

1. Select **New Poll Alert** from the Poll Alerts drop-down list.

   Note: A list of existing alerts for the selected property will appear in this drop-down list.

2. A default name will be displayed - amend this if required.
3. Ensure Activate Poll Alert is selected.
4. Select the SNMP properties to apply to the alert. Click ... .
5. Choose in what instance the alert will be activated from the drop-down list and enter the value, if needed.
6. Select the Devices to apply the alert to. Click ... .
7. Decide on the notification method when the alert is active: popup window in the Console and/or email message.

   Note: You can set up the recipients for alerts in the SNMP Alert settings.

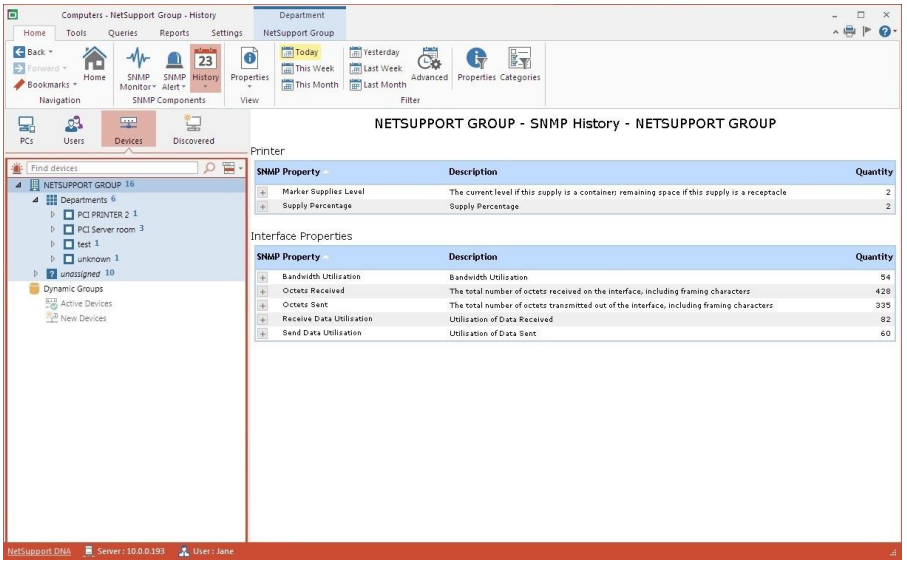
SNMP History

The History option enables you to track changes that have been made to a Device's SNMP Property and also view the Alerting history.

Each time NetSupport DNA gathers data, it compares the current details against information already held on the server and, if there are any differences, they are recorded in the history.

1. From the Devices Tree view, click the **History** icon in the ribbon. The History Summary window will appear.

   Note: If the component icons are not visible, click the Home tab.



You can view the history at company, department, Dynamic Group or Device level. Select the required level in the Tree view.

To switch between views, click the **History** icon drop-down list and select {Display – Properties/Poll Alerts} or click the appropriate icon in the ribbon.

You can view data for a specified period. To switch between different time periods, click the appropriate icon in the Filter section of the ribbon. Clicking **Advanced** allows you to apply a customised date/time filter.

Listed descriptions can be expanded to provide an individual Device breakdown for each item.

The working hours shown can be amended to suit your organisation in the DNA Configuration dialog. See Console Preferences - General for further information.

The date/time format displayed in the Console is taken from the machine where the NetSupport DNA Server is installed. To change the format in the Console, you will need to change the system date/time format on this machine. For further information, please contact our Support team www.netsupportsoftware.com/support.

Note: There may be property changes that are recorded which you do not wish to track. You can disable items from being displayed in the Console and delete existing data for items that have been de-selected. Click the **Properties** icon in the ribbon.

To limit the amount of data that is displayed in the information window, you can choose just to view certain SNMP categories. To display a category, click the **Categories** icon in the ribbon. Select the required categories to view and click **OK**. The information window will display data just for that category. A yellow header will be displayed advising what category you are viewing; you can switch categories and clear categories from here.

Queries
Select the Queries tab to display the Queries window.

NetSupport DNA's Query tool enables you to interrogate the database for records matching specified criteria. Queries specific to the component currently being viewed will be listed, enabling fast retrieval of the results.

Click the **Add Query** icon on the ribbon to create a new query or click the **Edit Query** icon in the ribbon to edit an existing item in the list.

Reports
Select the Reports tab to display the Reports window.

A number of pre-defined management reports, powered by the Crystal Reports engine, are attached to each component. Select the required report from the drop-down list. The results will be listed in the information window. These can be exported if required.

NetSupport DNA Reporting and Analysis Tools

NetSupport DNA provides both on-screen and print optimised reporting.

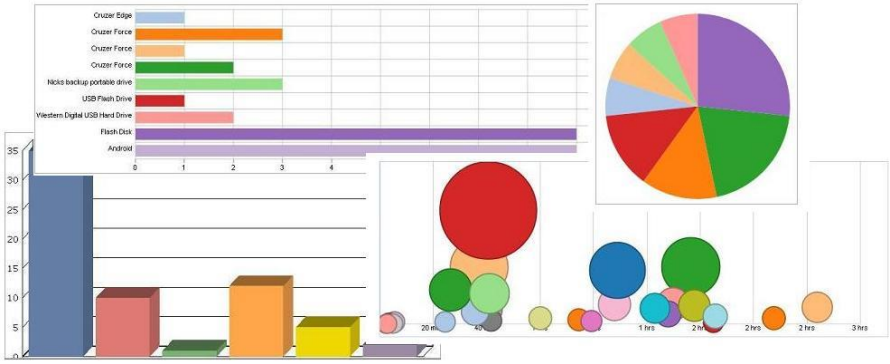
The on-screen reports/views are provided with supporting bar and pie charts and "live" drill down capabilities on all key summary data. As well as reporting on individual devices, users and departments, NetSupport DNA also features dynamic groups. These are user-defined and are added to the main company tree. A dynamic group could, for example, be to identify which PCs are upgradeable and such a group would be created automatically from those that match the required criteria – such as "all PCs with more than 'XX' Gb Ram, 'XX' Gb free disk space and XX processor type" and so on.

Print optimised reports are designed for management reporting and can be scheduled for creation and output to a specified file location automatically. All reports include the option to print or export to PDF, DOC and XLS.

NetSupport also supports custom views for all data; the Query Tool provides users with an easy interface for defining custom views. The query tool uses a simple drag and drop field picker, supported with conditions and sum-based features.

On screen analysis

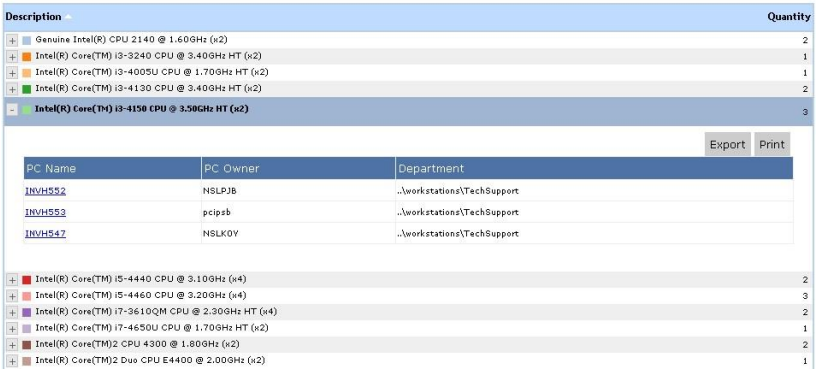
When viewing one of the components, information will be listed for a selected company, department, AD container, Dynamic Group or individual Agent in graph and list format.



The data can be displayed in a variety of graph formats by selecting the appropriate option from the **Chart** icon drop-down menu.

Note: Clicking the **Chart** icon in the ribbon will hide/show the graph.

Below the graph, the same records are presented in a list format. You can expand this information for a more detailed overview by clicking . This will present all individual Agent records.



To print the active view, click the icon at the top of the Console.

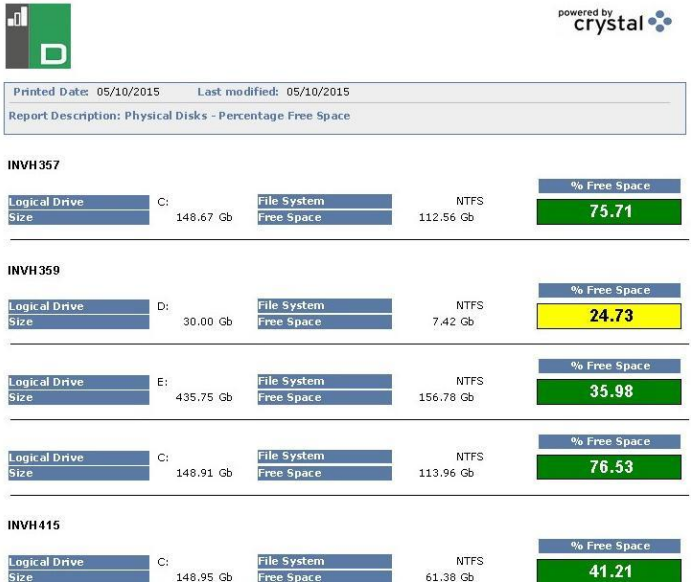
Queries
Select the Queries tab to display the Queries window.

NetSupport DNA's Query tool enables you to interrogate the database for records matching specified criteria. Queries specific to the component currently being viewed will be listed, enabling fast retrieval of the results.

Click the **Add Query** icon in the ribbon to create a new query or click the **Edit Query** icon in the ribbon to edit an existing item in the list.

Reports Window
Select the Reports tab to display the Reports window.

A number of pre-defined management reports, powered by the Crystal Reports engine, are attached to each component. Select the required report from the drop-down list. The results will be listed in the information window.



All available reports are provided with options to export as PDF, DOC, XLS, XML, HTML, CSV and RTF by clicking the **Export** icon in the ribbon.

Scroll through the report pages using the controls in the ribbon.

Note: You can switch between page layouts and zoom in and out of reports using the controls on the Status bar.

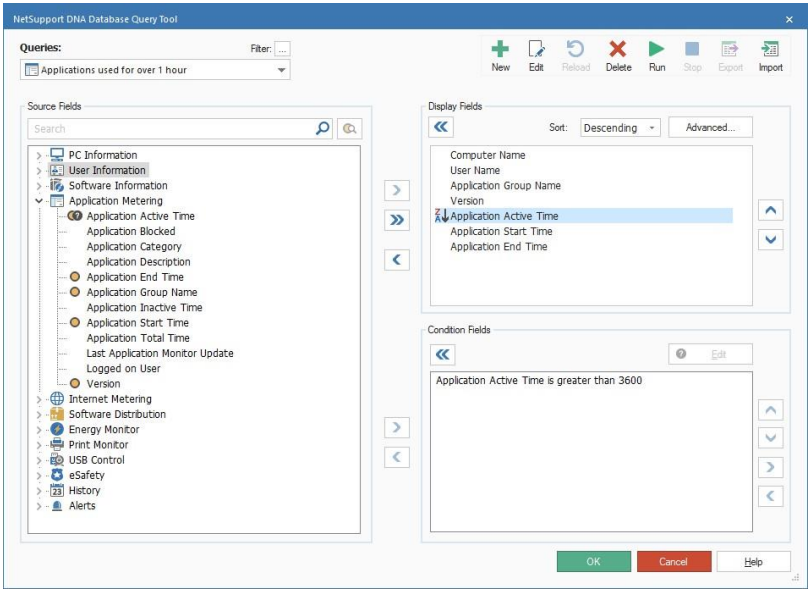
Query Tool

The Query Tool further enhances the reporting options available within NetSupport DNA. While on-screen and pre-defined Crystal Reports provide a wealth of ready-made information, the Query Tool enables you to tailor the output to meet your specific requirements.

Results can be viewed on-screen, printed or exported. Each stored query can be attached to the NetSupport DNA component that it relates to enabling easy on-going retrieval.

1. Click the **Query** icon in the Tools tab. The Query Tool dialog will appear and all existing queries are displayed. From here, you can create, edit, delete, run, import and export queries.

Note: You can filter the number of queries displayed to only those in certain groups. Click ... to specify which query groups to display. You can create query groups and add queries to a group in the Query Properties dialog when creating or editing a query.



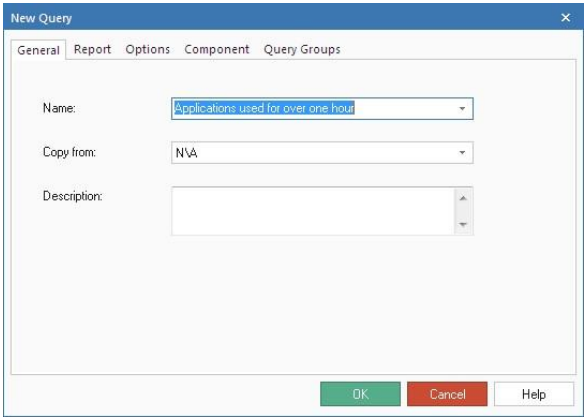
Create a Query

1. From the Query Tool dialog, click **New**.
   Or
   From the Console window, select the Queries tab and choose the appropriate component to attach the query to. Click the **Add Query** icon in the ribbon.

   Note: You will be unable to change the component the query is attached to using this method.

2. The New Query dialog will appear. Enter the properties for a new query.

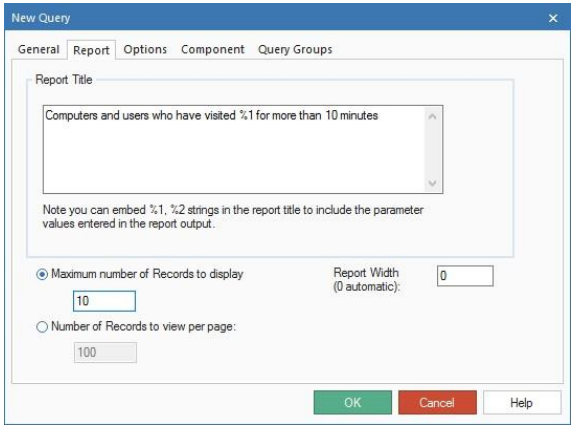
General



Name and Description
Enter a meaningful name and description for the query. The name is added to the drop-down queries list for you to select each time you want to load the report.

Copy from
To save time, the content of an existing query can be copied and used to form the basis of the new report. The fields and any associated criteria can then be edited as required.

Report

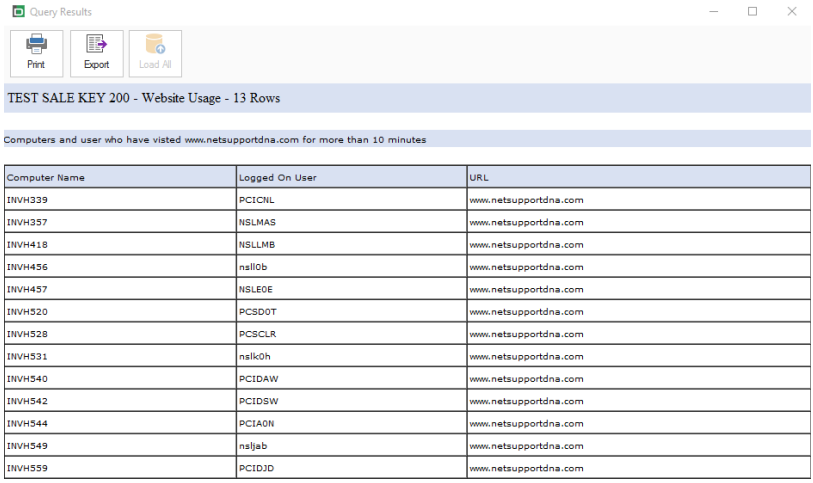


Enter a title for the report; this is what will be included with the final output. For flexibility, you can indicate that a variable condition is required to be input at run time using the format %1, %2 etc.

For example:

Computers and users that have visited %1 for more than 20 minutes.

This will allow you to enter a variable condition (for example, www.netsupportdna.com) when the query is run.



Computer Name	Logged On User	URL
INVH339	PCICNL	www.netsupportdna.com
INVH357	NSLMAS	www.netsupportdna.com
INVH418	NSLLMB	www.netsupportdna.com
INVH456	nsll0b	www.netsupportdna.com
INVH457	NSLE0E	www.netsupportdna.com
INVH520	PCSD0T	www.netsupportdna.com
INVH528	PCSCLR	www.netsupportdna.com
INVH531	nslk0h	www.netsupportdna.com
INVH540	PCIDAW	www.netsupportdna.com
INVH542	PCIDSW	www.netsupportdna.com
INVH544	PCIA0N	www.netsupportdna.com
INVH549	nsljab	www.netsupportdna.com
INVH559	PCIDJD	www.netsupportdna.com

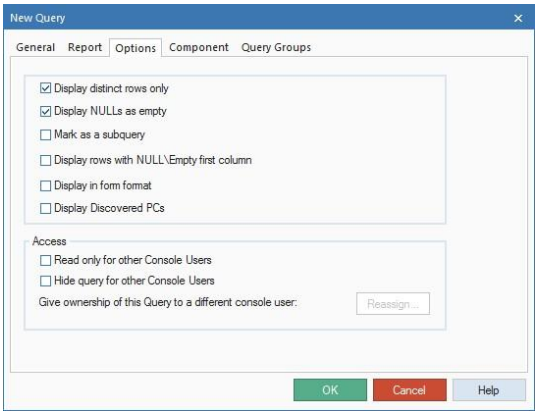
Maximum number of records to display
Specify how many records to display. This may be useful if you want to view the 'top ten' or 'top twenty' records.

Number of records to view per page
Enter how many records should be displayed on each page.

Note: This option cannot be used when **Maximum number of records to display** has been selected.

Report Width
Generally, the output will automatically fit the page, but you can specify a character width should you wish to change the display width.

Options



Display distinct rows only
Check this option to prevent multiple occurrences of the same record being included.

In considering the likely output that the query will generate, decide if you want to exclude duplicate records. All displayed fields must match for the record to be ignored. In the sample output below, although 'Marketing' has visited the same website several times, the inclusion of the active time makes each record distinct. If the active time wasn't included, you probably would only want one instance of each record.

Evaluation - Internet Activity - 7 Rows

URL	User Name	Internet Active Time
www.bbc.co.uk	Marketing	4 secs
www.bbc.co.uk	Marketing	9 secs
www.bbc.co.uk	Marketing	10 secs
www.bbc.co.uk	Marketing	16 secs
www.bbc.co.uk	Marketing	23 secs
www.bbc.co.uk	Marketing	27 secs
www.bbc.co.uk	Marketing	40 secs

Display NULLs as empty
Leave empty fields blank rather than display NULL.

Mark as a subquery
Sub-queries provide a means for running 'opposite' criteria to that specified in an existing query. For example, you may have a query that finds PCs that have had a particular hotfix installed. However, you may equally want to identify which PCs haven't had that hotfix applied.

In the first instance, create the sub-query and specify the required condition. For example, PCs that have had hotfix 12345678 installed.

Secondly, create a new query where the condition will ask for PCs that weren't found in the above example.

Display rows with NULL\Empty first column
If the first column of information for a record is blank, you can choose to ignore that record.

Display in form format
Ideal for queries that produce minimal output, this option enables you to list each record in a form style rather than individual rows.

Evaluation - PC Owner - 2 Rows

PC Owner

Computer Name:	MARKETING01	PC Owner:	Marketing
Logged On User:	Marketing	Logon Domain Name:	Marketing01
Asset Owner:			

Computer Name:	XP-SP3	PC Owner:	testing
Logged On User:	testing	Logon Domain Name:	XP-SP3
Asset Owner:			

Display Discovered PCs
Normally, only users with a NetSupport DNA Agent will be displayed in the query results. Selecting this option will also include discovered PCs.

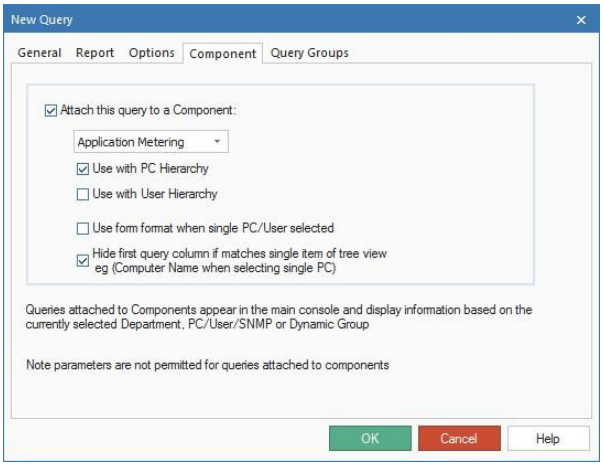
Access

Read-only for other Console Users
Selecting this option will allow other Console users to view the query but not make any amendments.

Hide query for other Console Users
Hides the query from other Console users.

Note: No other users (including Administrators) will be able to change the above two properties a Console user has set. The query can be reassigned to another user to take ownership of the query. Click **Reassign**.

Component



Attach this query to a Component
You can attach the query to the component that it relates to - Application Metering, Internet Metering etc - meaning that the output can be viewed in the relevant information window by selecting the Queries tab.

Note: Because there is no mechanism for entering parameters via the Queries tab, do not attach queries to a component if the title requires a variable. Reports of this nature can only be run from the Query Tool option.

Use with PC Hierarchy
By default, the query will be used with the PCs hierarchy. Clear this option if you do not wish to use the query with the PCs hierarchy.

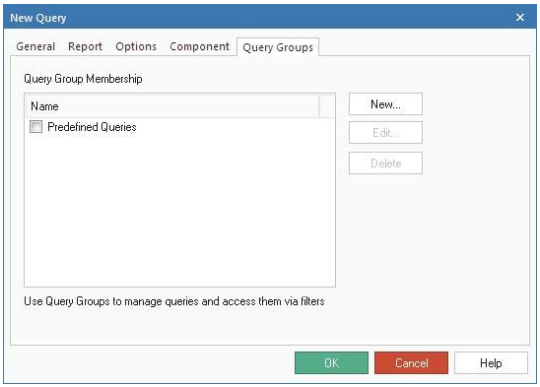
Use with User Hierarchy
Selecting this option allows the query to be used with the Users hierarchy.

Note: This option will only appear for components that are available in the Users hierarchy.

Use form format when single PC/User selected
When running the query from the Console window, you can highlight an individual Agent name in the tree to list records for that User only. In these circumstances, form format can be enabled.

Hide first query column if matches single item of tree view e.g. (computer name when selecting single PC)
If the first column of the query matches an item in the Tree view, then this column will be hidden. For example, if the first column in the query is computer name and you are selecting a single PC in the Tree view - the computer name column will not appear in the query.

Query Groups



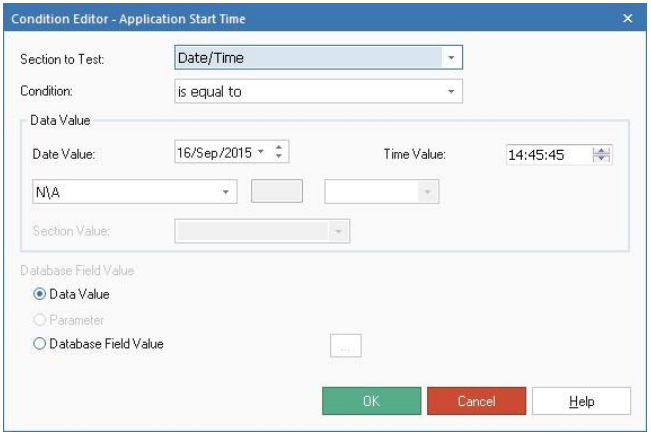
Query groups can be created, allowing you to filter the number of queries displayed in the Query Tool. A default group, Predefined Queries, will list all existing queries. To create a new group, click New and enter a name and description for the new group.

Click **OK** to return to the main Query Tool dialog.

3. From the Source Fields list, select the items to include in the output. You can quickly locate a particular source field by typing in the search box. Click  to transfer each one to the Display Fields window. You can transfer all fields in a particular category by clicking . You can view the current values for the field by clicking .

Note: Double clicking a source field will also add this to the Display Fields window.

4. Arrange the Display Fields into the order you want them to appear in the final output by clicking  and . If you want the output to be sorted by a particular field, select the item and choose the required Sort Criteria from the drop-down list.
5. To customise the displayed fields, click **Advanced**.
6. You can interrogate the database for specific records by adding conditions. Select the source field(s) and click the lower  to transfer to the Condition Fields window. The Condition Editor dialog will appear, allowing you to set the conditions. Click **Edit** to edit an existing condition.



From the drop-down list, select the condition to apply when interrogating the database to find Agents matching the specified criteria. The condition can be compared against an exact data value, a field name or you can enter a custom value.

Notes:
- If trying to identify PCs that were not found in a sub-query, ensure that the 'not in subquery' condition is selected and choose the appropriate sub-query from the available list.
- If you have included a variable condition when creating a query, ensure that the **Parameter Value** field is selected.
- When adding a date field condition, you can filter the query results by date by including a global date filter from **the Data Value** drop-down list.

7. The query will be saved when you run it or click **OK.**

Export a query
1. From the Query Tool, select the required query to export from the drop-down list.
2. Click **Export** and then click **Save**.
3. The selected query will be exported to an .XML file.

Import a query
1. From the Query Tool, click **Import**.
2. Select the file to import and click **Open**.
3. The selected query will be displayed in the Query Tool.

Note: You cannot import queries that have been exported using the Database Maintenance tool.

Edit an existing Query

1. From the Query Tool, select the required query to edit from the drop-down list.
   Or
   Select the Queries tab and choose the relevant component. Select the query to edit from the drop-down list and click **Edit Query**.
2. The related information will appear in the display and condition fields.
3. Add or remove display/condition fields using the appropriate buttons.
4. To edit the query properties, click **Edit**.
5. All changes will be saved when you run a query or click **OK**.

Run a Query

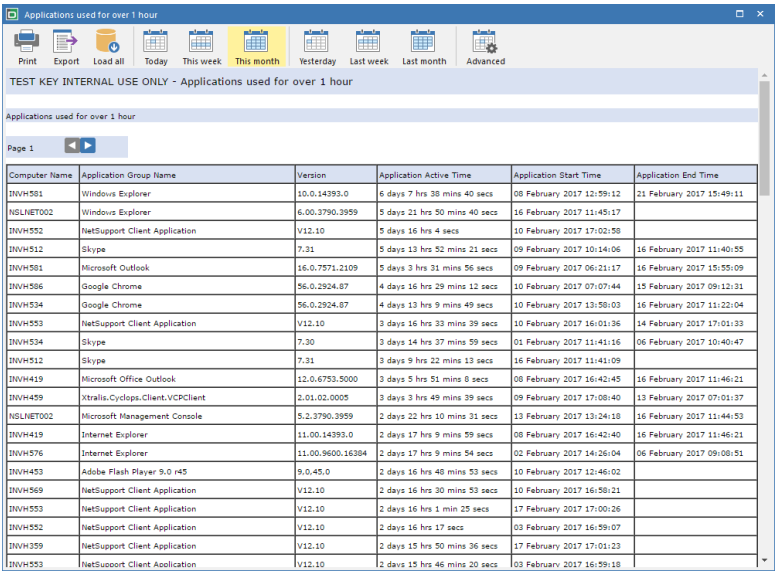
Queries can be run from the main Query Tool dialog or, if attached to a component, from the relevant component tab in the Console window.

Running queries from the Query Tool dialog

1. Select the Tools tab and click the **Query** icon.
2. The Query Tool will be displayed. Select the item to run from the drop-down queries list. If required, you can edit the properties and fields before running the query.
3. Click **Run**.

Note: If you have included a variable condition in the query, you will be prompted to enter the value.

4. The Query Results window will display the output. The number of records displayed per page is determined by the amount specified on the Query Properties dialog, in the **Number of rows to view at once** field. If you would rather display the records in a continuous list, click **Load All**.



Computer Name	Application Group Name	Version	Application Active Time	Application Start Time	Application End Time
INVH581	Windows Explorer	10.0.14393.0	6 days 7 hrs 38 mins 40 secs	08 February 2017 12:59:12	21 February 2017 15:49:11
NSLNET002	Windows Explorer	6.00.3790.3959	5 days 21 hrs 50 mins 40 secs	16 February 2017 11:45:17	
INVH552	NetSupport Client Application	V12.10	5 days 16 hrs 4 secs	10 February 2017 17:02:58	
INVH512	Skype	7.31	5 days 13 hrs 52 mins 21 secs	09 February 2017 10:14:06	16 February 2017 11:40:55
INVH581	Microsoft Outlook	16.0.7571.2109	5 days 3 hrs 31 mins 56 secs	09 February 2017 06:21:17	16 February 2017 15:55:09
INVH586	Google Chrome	56.0.2924.87	4 days 16 hrs 29 mins 12 secs	10 February 2017 07:07:44	15 February 2017 09:12:31
INVH534	Google Chrome	56.0.2924.87	4 days 13 hrs 9 mins 49 secs	10 February 2017 13:58:03	16 February 2017 11:22:04
INVH553	NetSupport Client Application	V12.10	3 days 16 hrs 33 mins 39 secs	10 February 2017 16:01:36	14 February 2017 17:01:33
INVH534	Skype	7.30	3 days 14 hrs 37 mins 59 secs	01 February 2017 11:41:16	06 February 2017 10:40:47
INVH512	Skype	7.31	3 days 9 hrs 22 mins 13 secs	16 February 2017 11:41:09	
INVH419	Microsoft Office Outlook	12.0.6753.5000	3 days 5 hrs 51 mins 8 secs	08 February 2017 16:42:45	16 February 2017 11:46:21
INVH459	Xtralis.Cyclops.Client.VCPClient	2.01.02.0005	3 days 3 hrs 49 mins 39 secs	09 February 2017 17:08:40	13 February 2017 07:01:37
NSLNET002	Microsoft Management Console	5.2.3790.3959	2 days 22 hrs 10 mins 31 secs	13 February 2017 13:24:18	16 February 2017 11:44:53
INVH419	Internet Explorer	11.00.14393.0	2 days 17 hrs 9 mins 59 secs	08 February 2017 16:42:40	16 February 2017 11:46:21
INVH576	Internet Explorer	11.00.9600.16384	2 days 17 hrs 9 mins 54 secs	02 February 2017 14:26:04	06 February 2017 09:08:51
INVH453	Adobe Flash Player 9.0 r45	9,0,45,0	2 days 16 hrs 48 mins 53 secs	10 February 2017 12:46:02	
INVH569	NetSupport Client Application	V12.10	2 days 16 hrs 30 mins 53 secs	10 February 2017 16:58:21	
INVH553	NetSupport Client Application	V12.10	2 days 16 hrs 1 min 25 secs	17 February 2017 17:00:26	
INVH552	NetSupport Client Application	V12.10	2 days 16 hrs 17 secs	03 February 2017 16:59:07	
INVH359	NetSupport Client Application	V12.10	2 days 15 hrs 50 mins 36 secs	17 February 2017 17:01:23	
INVH553	NetSupport Client Application	V12.10	2 days 15 hrs 46 mins 20 secs	03 February 2017 16:59:18	

5. If required, the output can be printed or exported.

Print
By default, only the currently displayed page will be printed. To print all of the output, click **Load All** to display the records in a continuous list.

Export
The output can be exported in XML, HTML or CSV (comma separated values) format. Click **Export** to display the Export Options dialog and select the required format. If using HTML, you can remove images (the NetSupport DNA logo) from the output. This is similar to the print option, where only the currently displayed page will be exported by default. To include all records, check the **All Pages** option. Click **OK** and save the export file to a suitable location.

Running queries from the Console window
When a query has been attached to a component, you can run it directly from the component in the Console window.

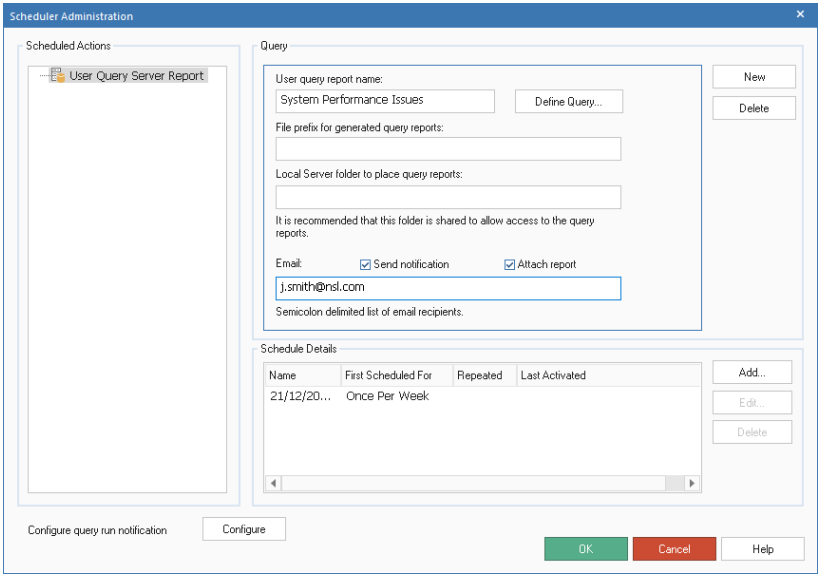
1. Select the Queries tab and choose the appropriate component.
2. The list of attached component queries will appear in a drop-down list.
3. Click on the required query. The output will be displayed in the information window. The results can be refined by clicking on a department or Agent in the Tree. A single Agent can be displayed in form format, if the option has been enabled in the query properties.

Scheduled Queries

The Scheduled Queries tool allows you to create queries and schedule them to run at a specific date/time or at regular intervals. The queries will generate reports, which are stored on the Server PC in HTML and XML formats.

Note: Existing queries cannot be scheduled.

1. In the Tools tab, click the **Schedule Queries** icon.
2. The Scheduler Administration dialog will appear.



3. Click **New**, enter a user query report name and select **Define Query** to create a new query.
4. The New Query dialog will appear. Enter the required properties for the query and click **OK**.

   Note: 'Mark as sub-query', 'read only for other Console users' and 'hide query for other Console users' will not be available. You will also not be able to attach the query to a component when scheduling queries.

5. In the Query Tool, select the source fields to include in the query and add any conditions.
6. Enter a file name for the generated query report (the date/time is automatically appended to the file name).

7. An email can be sent notifying when the report has run; click **Send notification** and enter the required email addresses. To include a copy of the query report, click **Attach report**.
8. Specify a valid directory on the Server PC where the reports will be generated. This directory must already exist and be accessible by the NetSupport DNA Service.
9. To schedule the report, click **Add**. The Scheduled Action times dialog will appear. Select the date and time you want the report to run and if this is to be repeated. Click **OK** to save.
10. Details of the scheduled times will now be displayed in the dialog and can be edited or deleted as required.
11. By default, a Console notification will only be sent if there is an error when running a scheduled query. Click **Configure** to choose to be alerted every time a scheduled query runs and if you want an email notification to be sent.
12. Click **OK** once you are finished.
13. The generated reports will be available in HTML and XML format in the directory specified on the Server PC.

Finding PCs, Users and Devices

NetSupport DNA provides a Find PC/User/SNMP Agent tool, used for identifying and locating Agents within the PCs, Users or Devices Tree views. A pre-defined list of search parameters is provided or you can create your own. A quick search facility is also provided, allowing you to perform a search within the PCs and Users Tree view.

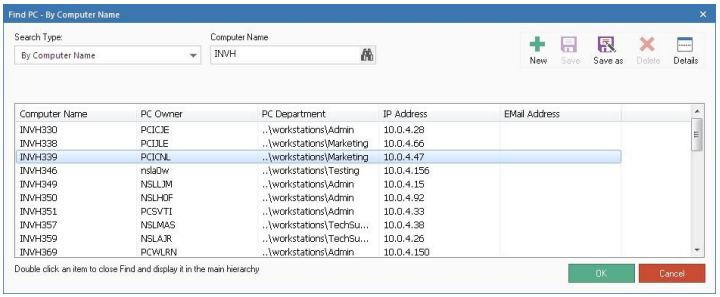
Quick search

You can perform a search within the PCs and Users Tree view from the search bar at the top of the Tree.

1. Enter the name or partial name in the search box and click . The search can be based on PC name, asset tag, BIOS serial number in the PCs Tree or logon name in the Users Tree. To switch between modes, click .
2. The first matching item in the Tree view will be displayed along with the number of matches found. You can scroll through these using the arrows.
3. The search results can be used as a filter in the Tree view, click . A filter bar will be displayed at the top of the Tree view showing what search filter has been applied. When a filter is applied, you can perform a search within this filter. To remove the filter, click **Clear**.
4. Click to clear the search.

Find PC/User/SNMP Agent tool

1. In the search bar at the top of the PCs, Users or Devices Tree view, enter your search terms and click . The Find PC/User/SNMP Agent dialog will appear displaying the results of your search.
   Or
   Click at the top right of the Console to open the Find PC/User/SNMP Agent tool.

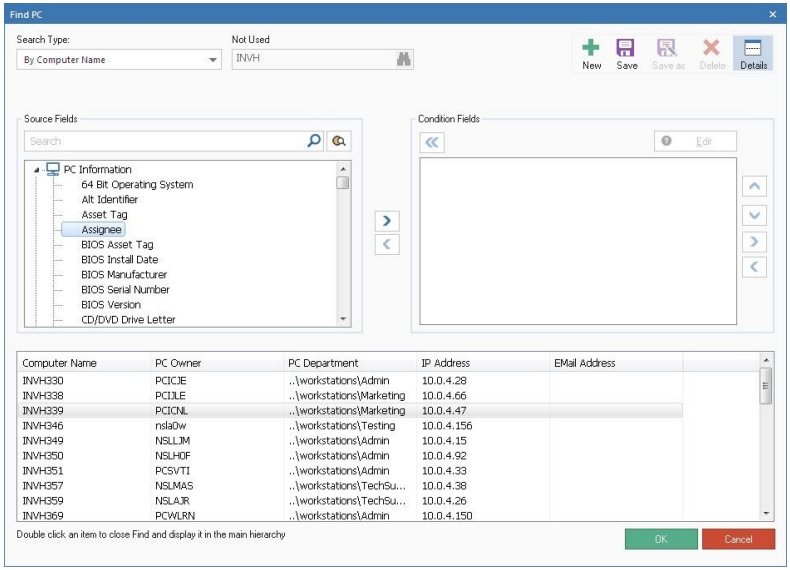


2. To perform a more detailed search, select a pre-defined search type from the drop-down list and then enter an associated value to help narrow the search. Partial information can be entered if unsure of the exact details. For example, if searching by computer name, any computer that starts with "Test".
3. You can include additional search parameters by clicking **Details**.
4. Click .
5. A list of matching Agents will appear.
6. Select the required Agent in the list and click **OK**.
7. The Agent will be located and highlighted in the Tree view.

Create search parameters

If the pre-defined search parameters are limiting, you can create new queries which will be added to the list for future use. For example, to find users who have visited a particular website:

1. From the Find dialog, click **New**.



2. From the Source Fields list, select the items to include. You can quickly locate a particular source field by typing in the search box. Click  to transfer to the Condition Fields window. You can view the current values for the field by clicking .

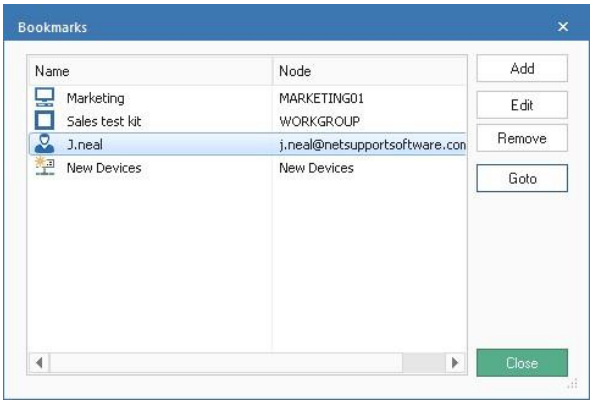
3. The Condition Editor dialog will appear. Enter the required condition; multiple conditions can be selected. Click **Edit** to change an existing condition.
4. Click **Save As** to store the query. Enter a name and click **OK**. The new query will be added to the search type drop-down list.
5. To perform the search, ensure the required query is selected from the drop-down list. Enter the associated parameter and click . Matching Agents will be listed.
6. Select the required Agent in the list and click **OK**.
7. The selected Agent will be located and highlighted in the Tree view.

Bookmarks

NetSupport DNA allows you to create and place bookmarks within the PCs, Users and Devices Tree views. This may be useful if you have a large or complex Tree structure, as it allows you to quickly navigate to the place you want to work with.

Add a bookmark

1. Navigate to where you want to place the bookmark in the Tree view.
2. Click the **Bookmarks** icon in the ribbon.
3. The Bookmarks dialog will appear. Any existing bookmarks will be displayed and you can edit, remove or go to a bookmark from here.



4. Click **Add**, enter a name for the bookmark and click b.
5. The new bookmark will be added.

Note: You can also add a new bookmark by clicking the drop-down arrow on the Bookmarks icon in the ribbon and selecting **Add Bookmark**. Enter the name for the bookmark and click **OK**.

Locate a bookmark

1. Click the **Bookmarks** icon in the ribbon.
2. The Bookmarks dialog will appear. A list of bookmarks will be displayed.
3. Select the required bookmark and click **Goto**.
4. The Tree view will open at the required location.

Or

1. Click the drop-down arrow on the **Bookmarks** icon in the ribbon.
2. A list of bookmarks will appear.

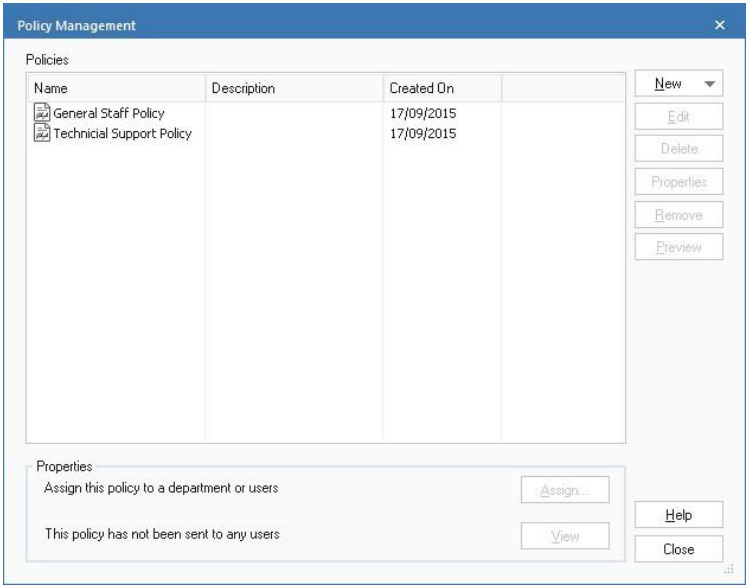
3. Click the required bookmark.
4. The Tree view will open at the required location.

Acceptable Use Policies

Acceptable Use Policies (AUP) form an integral part of the key information security policies used by most organisations. It is common practice for new staff to sign an AUP before using company resources for the first time, or to confirm they have read any changes to such a policy whenever it is updated.

NetSupport DNA provides a flexible module to support the delivery and tracking of AUPs across an organisation. Policies can be applied to specific devices or users for display each time any user logs on or for one-time display and acknowledgement. Multiple policies can be created, allowing you to have one policy that appears only once for selected users (for example, teachers) and another policy that appears every time for other users (for example, students). Full tracking and exception reporting is also provided.

1. In the Tools tab, click the **Manage AUP** icon.
   Or
   Click on the **User Details** icon drop-down arrow and select {Acceptable Use Policies} from the menu.
2. The Policy Management dialog will appear.

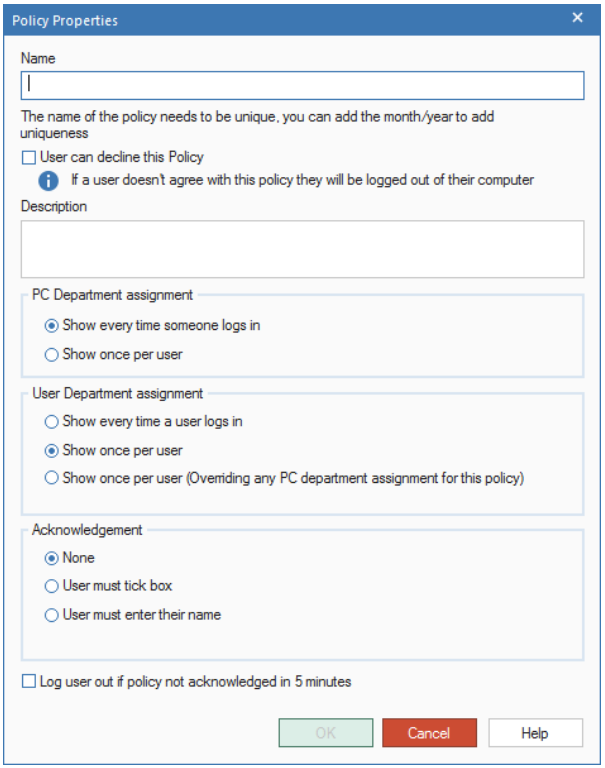


To create a new Acceptable Use Policy

1. Click **New** and select **Blank**.

Note: An example template is provided. You can use or edit this by selecting **New** and then **From Template**.

2. Enter the required text for the policy and click **OK**.
3. The Policy Properties dialog will appear.



Name
Enter a unique name for the policy.

User can decline this Policy
This option allows the user to decline the policy.

Note: The user will be logged out of their computer if they disagree with the policy.

Description
Enter a description for the policy.

PC Department assignment

Show every time someone logs in
The policy will be displayed each time a user logs into their machine.

Show once per user
The policy will only be displayed once per user.

User assignment

Show every time a user logs in
The policy will be displayed each time a user logs in.

Show once per user
The policy will only be displayed once per user.

Show once per user (overriding any PC department assignment for this policy)
If a user has a policy set to show only once and they log into a PC where the policy is set to show every time, the PC department policy will take precedence. Selecting this option allows you to override the PC department setting and only show the policy once per user.

Acknowledgement

None
No acknowledgement is required from the user.

User must tick box
The user must tick a box to acknowledge the policy.

User must enter their name
The user must enter their name to acknowledge the policy.

Log user out if policy not acknowledged in 5 minutes
If the user does not acknowledge the policy within five minutes, they will be logged out of their machine.

4. Click **OK**.
5. The policy will now be listed in the Policy Management dialog.
6. To preview policies before assigning them, click **Preview**.
7. Click **Assign** to assign the policy to departments or users.

8. To assign the policy to departments or users, select the required policy and click **Assign**.

Track user acknowledgements

1. Select the required policy from the list.
2. Click **View**.

   Note: If the policy has not been sent or acknowledged by any users, this option will be unavailable.

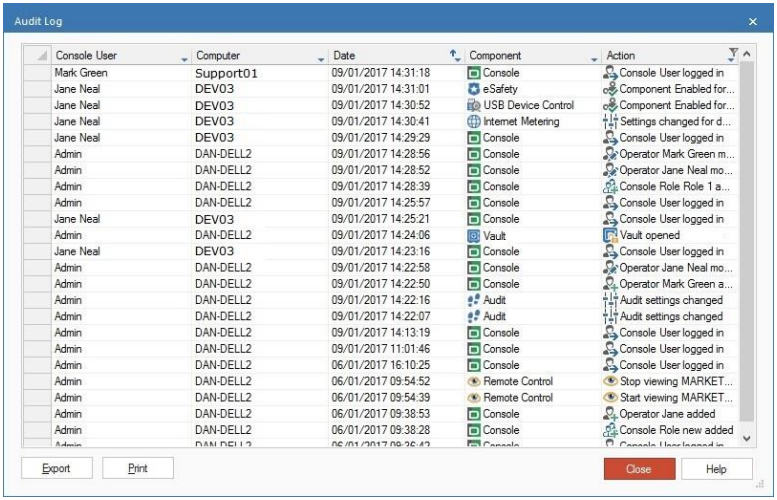
3. The Policy Acknowledgements dialog will appear. From here, you can see the users who have acknowledged the policy, the date and time of the acknowledgement and on which PC it was acknowledged.

Audit Log

NetSupport DNA provides an Audit Log, which allows you to keep track of actions that Console users have taken within the NetSupport DNA Console. Console activities such as, when users have logged in and out of the Console, when components have been enabled or disabled and any changes to the component settings, are recorded.

Note: You can choose which actions are logged in the Console Preferences – Audit settings.

1. In the Tools tab, click the **Audit Log** icon.
2. The Audit Log dialog will appear.



3. A list of Console users, along with details of the action the user has taken, in what component and the date and time this occurred will be displayed. The newest items will be listed at the top.
4. Filters can be applied to each column, select . A menu will appear, allowing you to select the items to be displayed.
5. To export the current list, click **Export**.
6. To print the current list, click **Print**.

Note: By default, audit entries are kept for thirty days. This can be changed in the Console Preferences - Audit settings.

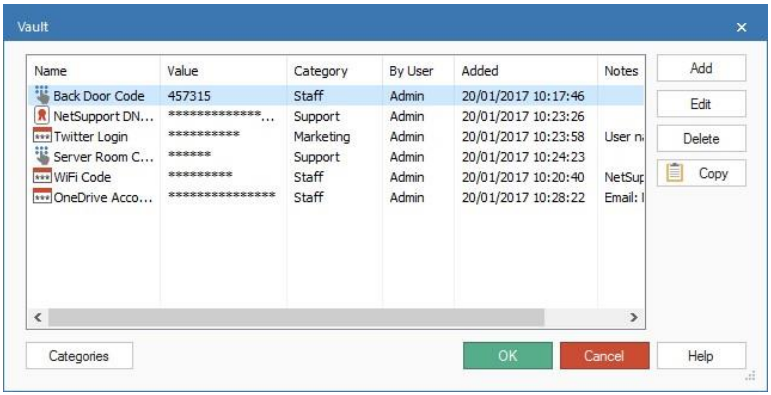
Vault

NetSupport DNA provides a Vault component, allowing you to store any sensitive or useful information such as passwords, licence details, door codes, etc. The Vault is a secure area within DNA that keeps all information centrally. Access to it can be restricted to certain Console Operators by setting the appropriate Role.

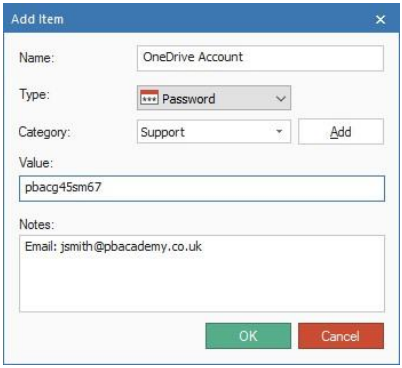
Note: Once data is stored in the Vault, Operators will need to enter their password to gain access to it.

Add a new entry to the Vault

1. In the Tools tab, click the **Vault** icon.
2. The Vault dialog will appear. Any existing entries will be displayed. From here, you can edit, delete and copy the selected entry.



3. Click **Add**.
4. The Add Item dialog will appear.



5. Enter a name for the item.
6. Select what type of item you are adding from the Type drop-down list.
7. Categories can be defined and assigned to the item, allowing you to group items together. To create a new category, click **Add**. It will then be available for selection from the Category drop-down list.
8. Enter the value for the item, add any information related to it and click **OK**.
9. The item will be listed in the main view and the value obscured. To see this, you will need to select it or mouse over it.
10. Click **OK**.

Manage User Accounts

NetSupport DNA allows Operators to manage users that are part of Active Directory. Operators can see user accounts that have been disabled or locked and they can reset the account or assign new passwords. NetSupport DNA also allows Agents to access this facility from the DNA Agent menu in the taskbar.

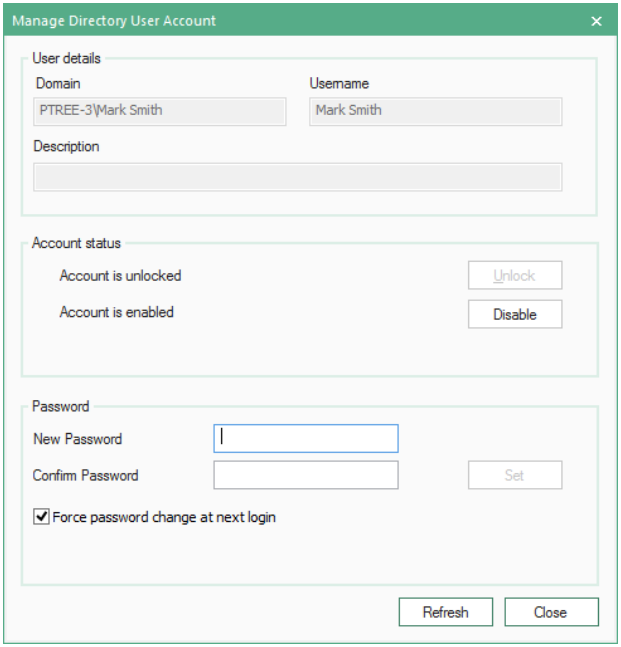
If non-domain administrators want to use this facility, you will need to apply the appropriate rights to them. For full instructions on how to do this, please visit our Knowledge Base and refer to technical document **Allow users to reset Active Directory passwords using NetSupport DNA**.

Manage user accounts from the NetSupport DNA Console

1. From the Users Tree view, right-click on the required Agent and select **Manage User Account**.

   Note: The first time you access this dialog, you will be asked to enter your user name and password.

2. The Manage Directory User Account dialog will appear.



From here, you can see the current user details, unlock the account, disable and enable the account and set a new password. When setting a new password, you can force the user to change this when they next log in.

Note: If complex passwords have been enabled, the reset facility will not enforce this. You should use the Force Password change at next login option to ensure this policy is adhered to.

Click **Refresh** to apply the changes.

Manage user accounts from the Agent
By default, this feature is disabled. This can be enabled in the DNA Configuration - Agent Settings.

1. Right click the DNA Agent icon in the system tray and select **Manage User Account**.
2. The Active Directory User Account dialog will appear. Enter the user name for the user account you want to manage and click **Modify**.
3. The Manage Directory User Account dialog will appear.
4. The Agent can unlock user accounts and set passwords as required.

Note: The Agent will not have access to enable/disable user accounts.

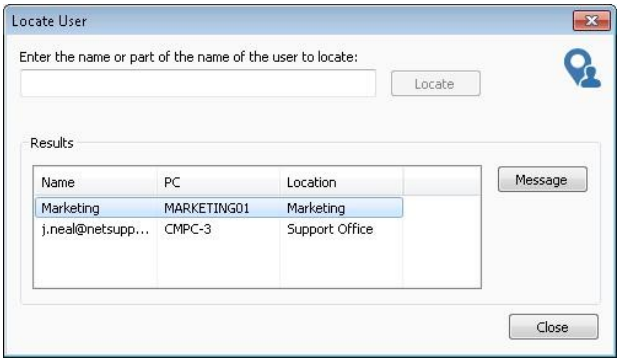
Locate a User

NetSupport DNA allows an Agent to locate logged on users and then send them a message. This may be useful for staff members that do not have the NetSupport DNA Console installed but need to contact other users in the organisation.

Notes:

- By default, this feature is disabled. This can be enabled in the DNA Configuration - Agent Settings.
- This feature will not locate users of shared computing resources, for example, Remote Desktop Services or Citrix users.

1. Right-click the DNA Agent icon in the system tray and select **Locate User**.
2. The Locate User dialog will appear.



3. Enter the name (or partial name) of the user you are searching for and click **Locate**.
4. A list of users matching the search will be displayed.
5. Select the user(s) to send a message to and click **Message**. Enter the required message and click **OK**.
6. The message will appear at the selected user(s).
7. Click **Close**.

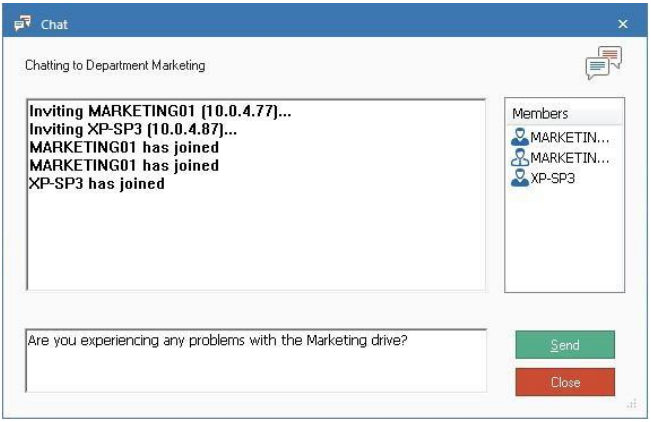
Chatting to Agents

NetSupport DNA allows you to chat to any number of connected Agents simultaneously, via a scrolling text window.

1. Highlight an Agent or group of Agents in the Tree view.

   Note: The Chat feature is only available from the PCs Tree view.

2. Right-click and select **Chat**.
   Or
   In the Tools tab, click the **Chat** icon.
3. The Chat window will appear at the Console and Agent PCs, listing all Agents included in the chat session.



4. Enter the required text in the box provided and click **Send**.
5. The message will appear at all Agent PCs. The Agent also has the option to send messages or to leave the chat session by clicking **Close**.
6. The Console can end the chat session by clicking **Close**.

Remote Control

DNA's integrated remote control

Based on NetSupport's own remote control solution, NetSupport Manager, DNA's integrated remote control offers advanced functionality for the effective management of remote workstations. Watch, share or control the screen, mouse and keyboard of Agent PCs; transfer files to Agents; run command line instructions at the Agent using Remote Command Prompt or PowerShell; remotely view and edit the Registry; manage running applications, services and processes, and perform a remote login and logout at Agent machines.

Notes:

- This is only available in the Education Edition of NetSupport DNA.
- If any of the Agent machines you want to remote control are located on remote networks, you need to enter your external (public) gateway address into the Remote Control settings to enable the integrated remote control features at these devices.
- You can use the integrated remote control feature in NetSupport DNA to remote control a Mac machine that has the NetSupport Manager Client installed.*

NetSupport Manager

Alternatively, a full working copy of NetSupport Manager can be added to your NetSupport DNA purchase. For over 30 years, NetSupport Manager has consistently led the way with innovative features to aid in remote PC management.

Please visit our website, www.netsupportmanager.com, for more information.

NetSupport DNA can also be configured to use any third-party remote control application.

Configure remote control

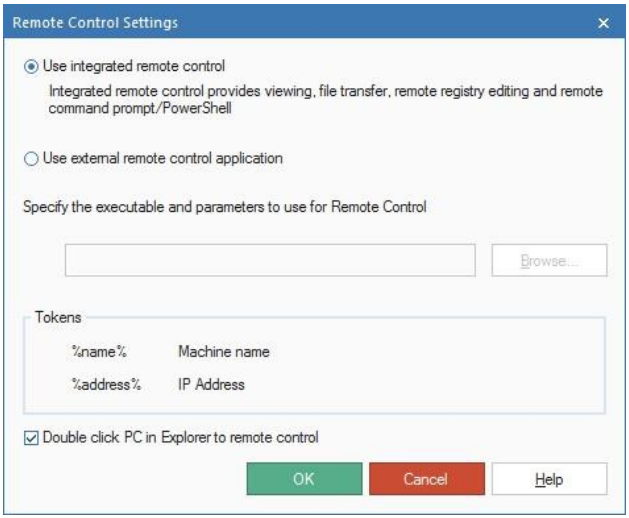
NetSupport DNA allows an Administrator to view any Agent machine individually, using the Remote Control tool.

Note: Integrated remote control can be used to remote control Agents running in RDP User Sessions.*

---

1. In the Tools tab, click the **Configure Remote Control** icon.

2. The Remote Control Settings dialog will appear. If you are using the integrated remote control, ensure the option is selected (the remaining fields will not be available). Alternatively, you can use an external remote control application. Click **Browse** to locate the appropriate executable and specify the relevant command parameters for initiating a remote control session with the required Agent PC.
3. A remote control session can be opened by double clicking on an Agent in Explorer mode: ensure **Double click PC in Explorer to remote control** is selected.



To launch a remote control session

1. Select an Agent in the Tree view. Right click and select **Remote – Remote Control**.
   Or
   In Explorer mode, double click on the Agent.

   Note: By right clicking and selecting **Remote**, you will also be able to perform a file transfer, open a remote command prompt and PowerShell session, edit the registry, manage the Agent's running applications, services and processes and perform a remote login and logout (a remote login and logout can also be performed at department and dynamic group level).
2. Assuming the target PC has the appropriate software installed, a View window to the selected Agent will appear at the Console.

Note: You can enable user acknowledgement, show an indicator at the Agent when a remote session is active and choose the default viewing mode in the Remote Control settings.

* For further information, please refer to www.netsupportsoftware.com/support.

Send a Message

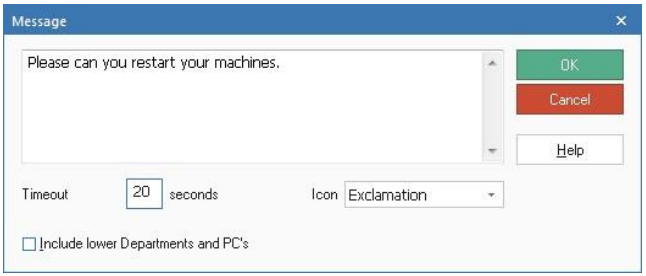
The message tool allows an administrator to send a message to an individual Agent, department or the company as a whole, by selecting the relevant choice in the Tree view.

To send a message

1. Select an Agent, department, AD container or the company in Tree view.

   Note: The Message feature is only available from the PCs Tree view.

2. Right-click and select **Message**.
   Or
   In the Tools tab, click the **Message** icon.
3. The Message dialog will appear.



4. Enter the message. Decide whether to show the message at Agent PCs for a specified time. To show how important the message is, you can select an icon to be displayed with it. If you have selected the company or a department, check **Include lower Departments and PCs** to indicate that sub-departments within that layer of the tree should also receive the message. Click **OK** to send.
5. The message will appear at the Agent PCs.

Agent Status

The Agent Status feature enables a Console user to check that Agent PCs are powered on. This can be useful when preparing to distribute software. Information can be retrieved on any machine known to the NetSupport DNA database.

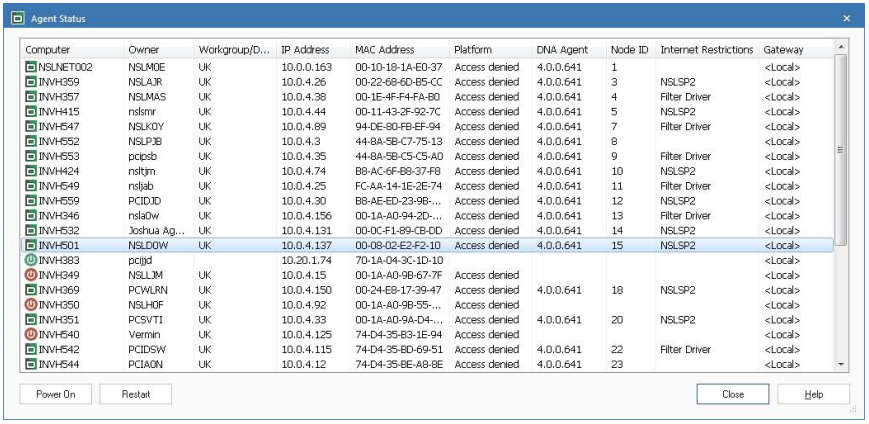
Note: The end-user PC must have a Wake-on-LAN card installed and be appropriately configured. The NetSupport DNA Console sends a Wake-on-LAN packet to the Agent instructing the workstation to power on.

To power on machines

1. Select the required company, department, AD container or Agent in the tree view.

   Note: The Agent Status feature is only available from the PCs Tree view.

2. Select the Tools tab and click the **Agent Status** icon.
   Or
   Right-click and choose **Agent Status**.
3. The Agent Status dialog will appear.



4. If any of the PCs are not currently powered on, only the IP and MAC addresses will be displayed.
5. Highlight the required PCs (multiple machines can be selected) and click **Power On**.
6. The NetSupport DNA Agent can also be restarted from this dialog. Highlight the required PCs and click **Restart**.

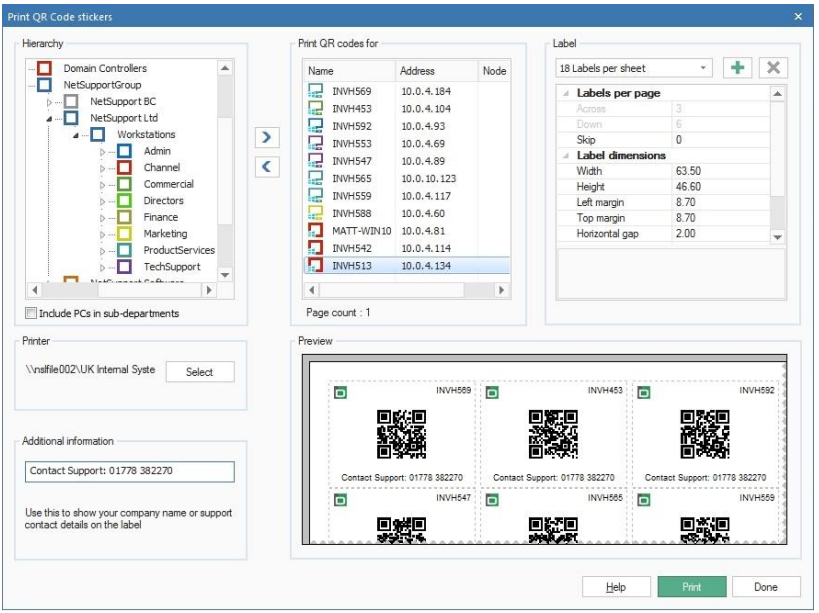
Note: A power schedule can be set, allowing you to automatically power on and off machines at certain times on set days. See NetSupport DNA Configuration - Energy Monitor Settings.

Creating QR Code labels

NetSupport DNA provides a QR code label creation facility, including support for custom details. The NetSupport DNA Mobile Console app includes a QR code scanner to help instantly identify any machine, either from an on-screen QR code displayed in the DNA Agent window or from a label fixed to the device.

To print QR code labels

1. In the Tools tab, click the **Print QR Codes** icon in the ribbon.
2. The Print QR Code stickers dialog will appear.



3. From the Hierarchy, select the company, AD container, department or users to create a QR code for by selecting ›. You can include all Agents within a company, AD container or department by selecting **Include PCs in sub-departments**.
4. Decide how many labels you want to print per sheet and the label size. Click + to create a custom sheet.
5. Select which printer to use and, if required, add any additional information to the label. A preview of what the sheet will look like will be displayed.
6. Click **Print**.

Database Maintenance

The Database Maintenance utility enables you to purge the NetSupport DNA database of redundant data, applications and programs, remove Agent PCs that are no longer in use, remove users, create backups of key data using an export/import facility and set a data retention policy, allowing you to schedule automatic deletion of old data.

Note: You can limit the number of Console Users who have access to this facility by assigning Operator (rather than Administrator) rights when creating Console Users.

1. In the Tools tab, click the **Database Maintenance** icon. The Database Maintenance dialog will appear. Select the appropriate tab.

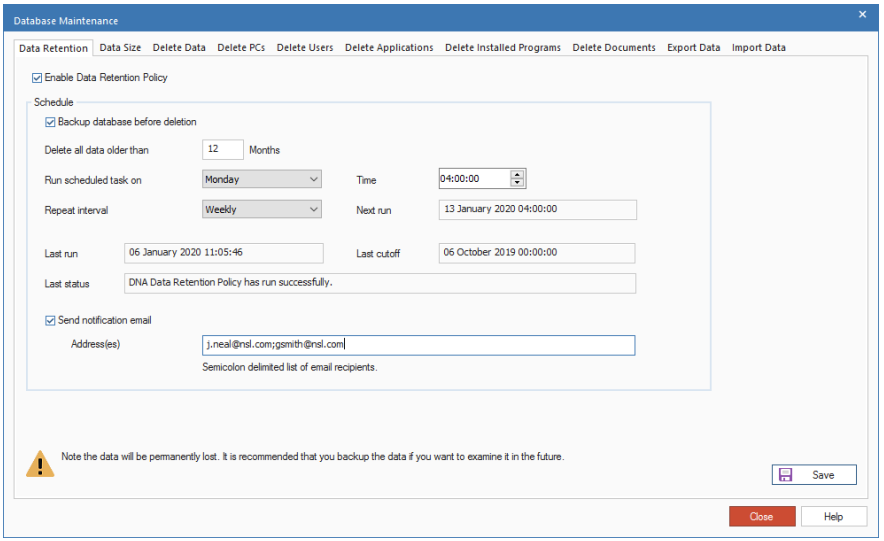
Data Retention

To keep the NetSupport DNA database at a manageable size, you can delete old data automatically by creating a data retention policy. You can choose how old the data must be before it is deleted (the data can be backed up before it is removed), schedule the policy to run on a specific day/time and choose how often the policy runs. A notification email can be sent each time the scheduled policy runs, notifying selected Console Users of whether this was successful, how many records were deleted and how much database space was recovered.

Note: If the policy fails, a Console alert will be raised advising you of this.

The following data will be deleted from the DNA database:

- Internet Metering
- History
- Application Metering
- Login sessions
- Power sessions
- USB device use
- Print cost data
- Software Distribution
- eSafety - triggered phrases, screen shots and recordings.



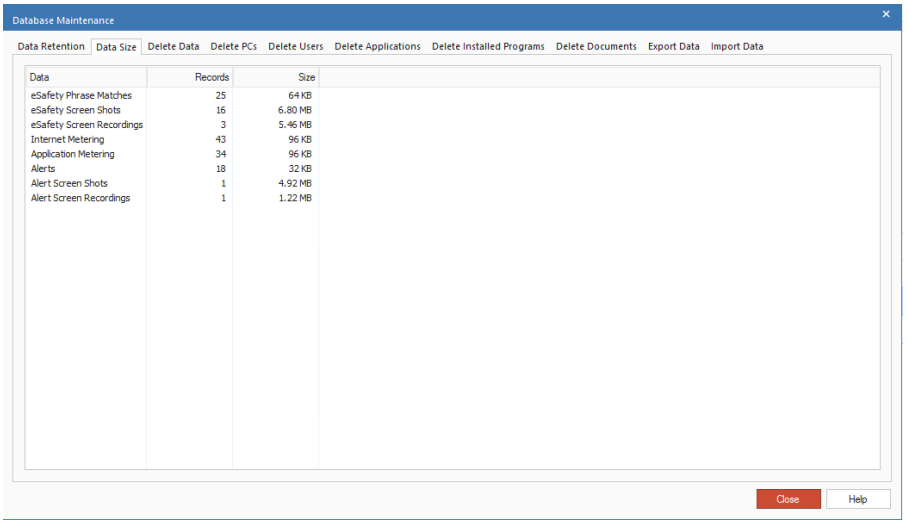
1. Select **Enable Data Retention Policy**.
2. By default, the database will be backed up before it is deleted. Clearing the **Backup database before deletion** option will result in unrecoverable the data loss. We do not recommend this option is disabled unless you perform your own regular backups.
3. Enter the age of the data to be deleted (all data older than this will be removed) in the **Delete all data older than** field. The default is 12 months, the minimum is 3 months and the maximum is 120 months.
4. Select the day of the week the policy is to run on from the **Run scheduled task on** drop-down menu and specify a time.
5. Choose how often the policy runs from the **Repeat interval** drop-down menu.
6. The **Next run** field will now be populated with the date and time the policy is due to run. If a policy has already run, the date and status of this will be displayed.
7. A notification email can be sent, enter the required email address in the **Send notification email** field. Multiple addresses can be entered. Separate each address with a semicolon.

   Note: The email settings must be configured before email notifications can be sent.

8. Click **Save** to activate the data retention policy.

Data Size

This option provides a useful indicator of how many records, and more pertinently, the associated data size, are currently stored in the DNA database for the eSafety* (number of phrase matches as well as screen shots and recordings associated with the keyword triggers), Internet and Application metering and Alerts (number of alerts along with screen shots and recordings attached to the alert) components - providing you with the information needed to perform the required housekeeping to keep the NetSupport DNA database at a manageable size.



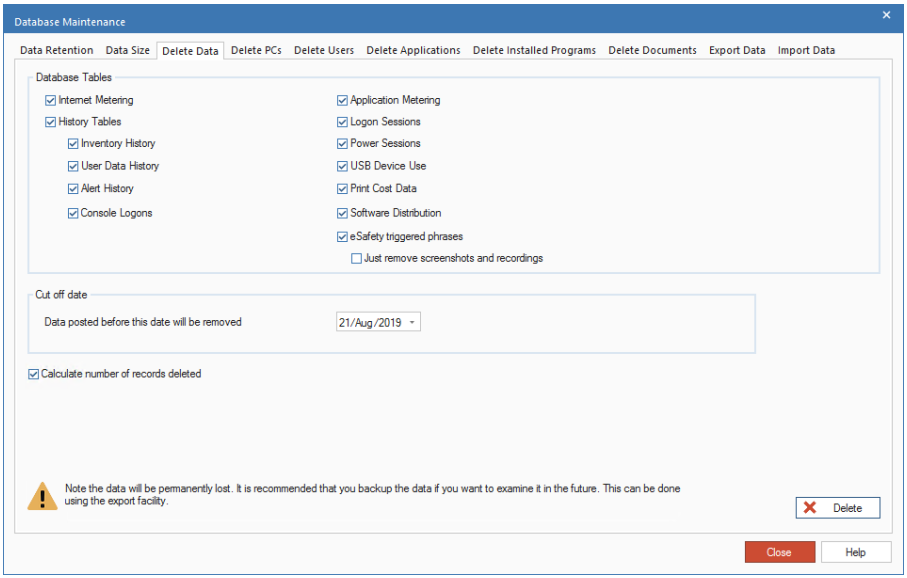
* The eSafety component is only available in the Education Edition of NetSupport DNA.

Delete Data

This option enables you to delete records from the NetSupport DNA Database tables based on a specific cut-off date.

Notes:

- If you are in the Devices Tree view, you will see data relating to SNMP devices.
- In the Education Edition of NetSupport DNA, an option for eSafety-triggered phrases will be displayed, allowing you to remove data relating to keyword and phrase monitoring.

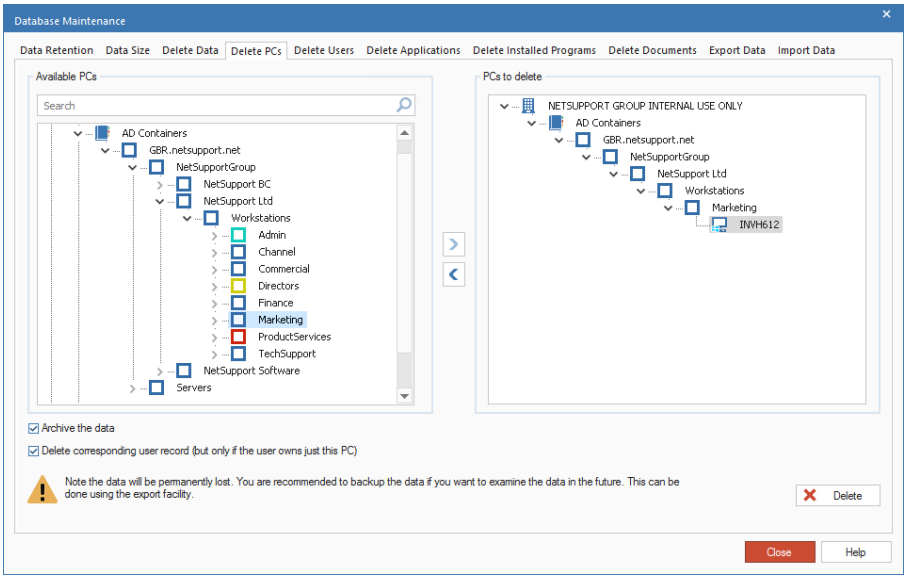


1. Select the database tables to include in the purge.
2. Choose the required 'cut-off' date. All records logged prior to the specified date will be deleted.
3. Click **Delete** and confirm that you wish to proceed.
4. A confirmation dialog will appear indicating how many records have been deleted.

Note: If you don't wish to know the number of records deleted in the final confirmation dialog, un-check **Calculate number of records deleted**.

Delete PCs

As your installation base changes, you may find that managing licence levels becomes difficult because the database is holding details of Agent PCs that are no longer in use. This option enables you to 'retire' PCs and remove any related data.



1. From the **Available PCs** list, select the PCs to remove. This can be done by individual PC, department level (if multiple PCs are to be removed) or by Dynamic Group.

   Note: To search for an item in the Tree view, enter the name or partial name of the PC or department in the search box and click . The first matching item in the Tree view will be displayed along with the number of matches found. You can scroll through these using the arrows. Click to clear the search.

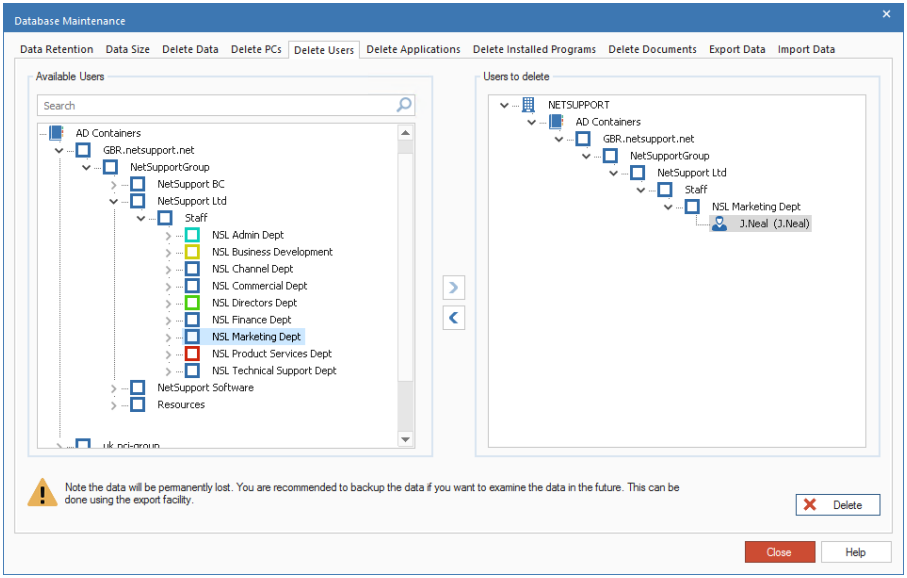
2. Click to add the selected items to the **PCs to delete** list.

   Individual PCs can be removed from the list by clicking . This is useful if not all machines within a department are to be deleted.
3. If you do not want to permanently lose the data, you can store the records in an archive file. Ensure the **Archive the data** option is checked.

4. If required, you can also delete the corresponding user data with the PC, if the user is the owner of *only* this PC. Ensure the **Delete corresponding user record** option is checked.
5. Click **Delete**. If archiving, you will be prompted for a file name and location. The data is copied to the archive but remains in the database. Once archiving is complete, you will be prompted to continue with the deletion.

Delete Users

You may find the database is holding details of users that are no longer required. This option enables you to delete users and remove any related data.



1. From the **Available Users** list, select the users to remove. This can be done by individual PC, department level (if multiple PCs are to be removed) or by Dynamic Group.

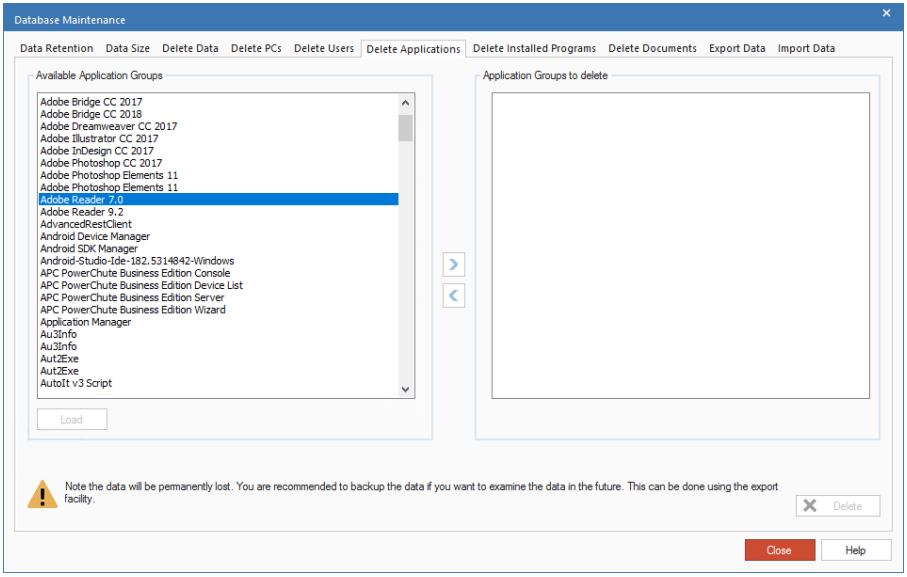
Note: To search for an item in the Tree view, enter the name or partial name of the user or department in the search box and click . The first matching item in the Tree view will be displayed along with the number of matches found. You can scroll through these using the arrows. Click to clear the search.

2. Click  to add the selected items to the **Users to delete** list.

   Individual users can be removed from the list by clicking . This is useful if not all users within a department are to be deleted.
3. Click **Delete**.

Delete Applications

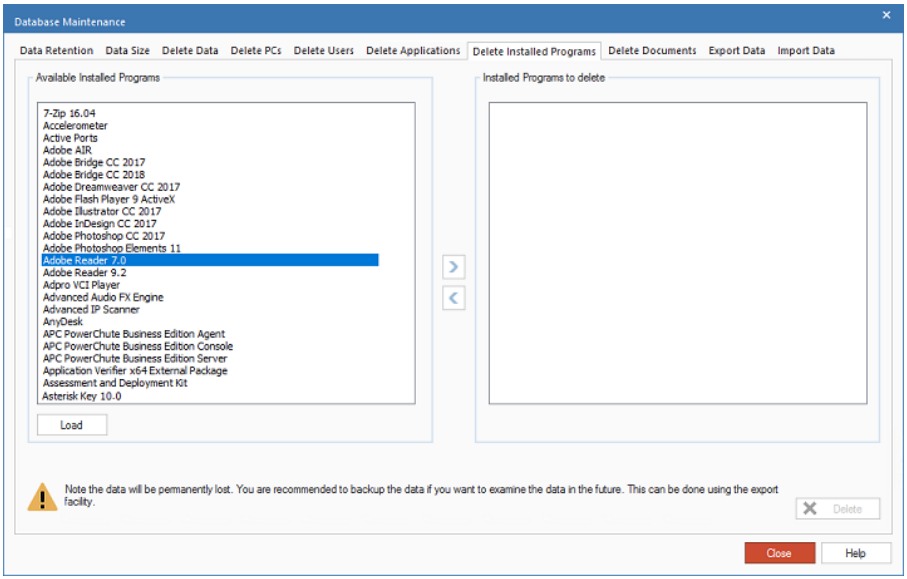
This tab enables you to remove applications from the NetSupport DNA database that are no longer referenced by any Agent PCs. Any application that is not referenced in the Application Metering or Software Inventory components will be listed for possible deletion.



1. Click **Load** to display the applications in the **Available Application Groups** list. Select the applications to be deleted. Multiple items can be selected.
2. Click  to transfer the selected items to the **Application Groups to Delete** list.
3. Click **Delete**.

Delete Installed Programs

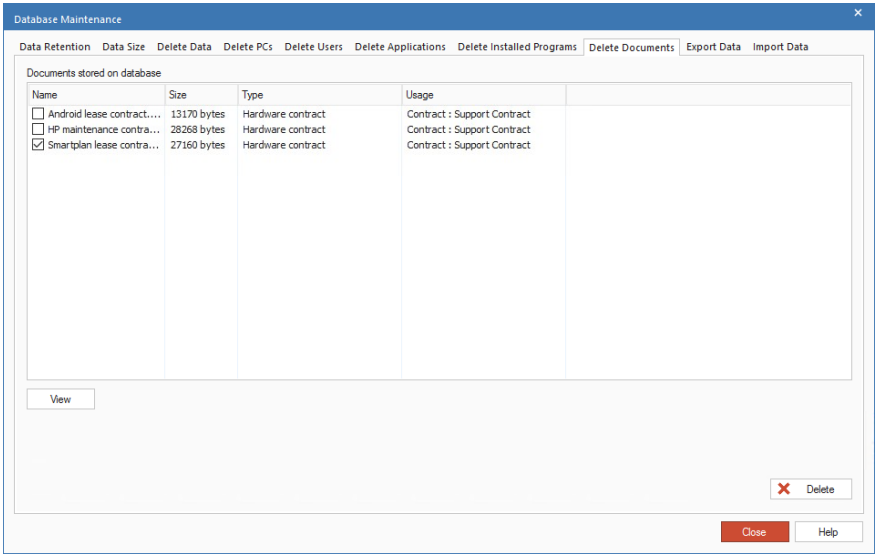
This tab enables you to remove installed programs from the NetSupport DNA database that are no longer referenced by any Agent PCs. Any installed program that is not referenced in the Application Metering or Software Inventory components will be listed for possible deletion.



1. Click **Load** to display the installed programs in the **Available Installed Programs** list. Select the installed program to be deleted. Multiple items can be selected.
2. Click  to transfer the selected items to the **Installed Programs to delete** window.
3. Click **Delete**.

Delete Documents

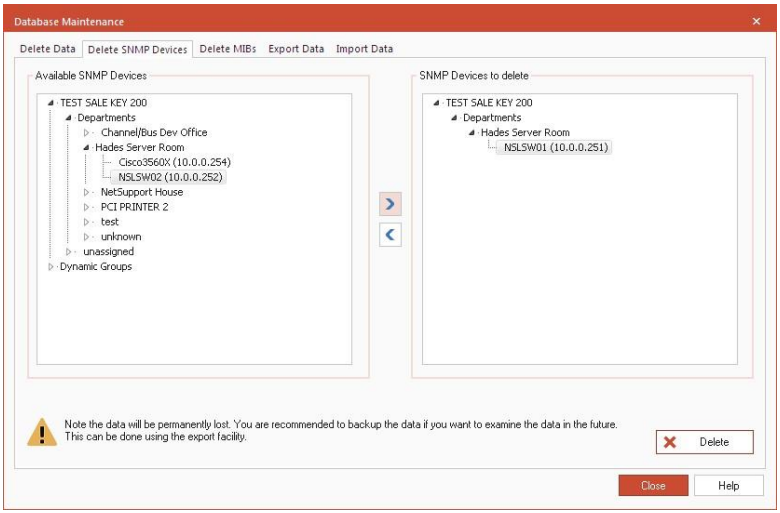
This option enables you to delete documents from the NetSupport DNA database.



1. Select the documents you wish to remove.
2. To view documents before you remove them, click **View**.
3. Click **Delete** and confirm that you wish to proceed.

Delete SNMP Devices

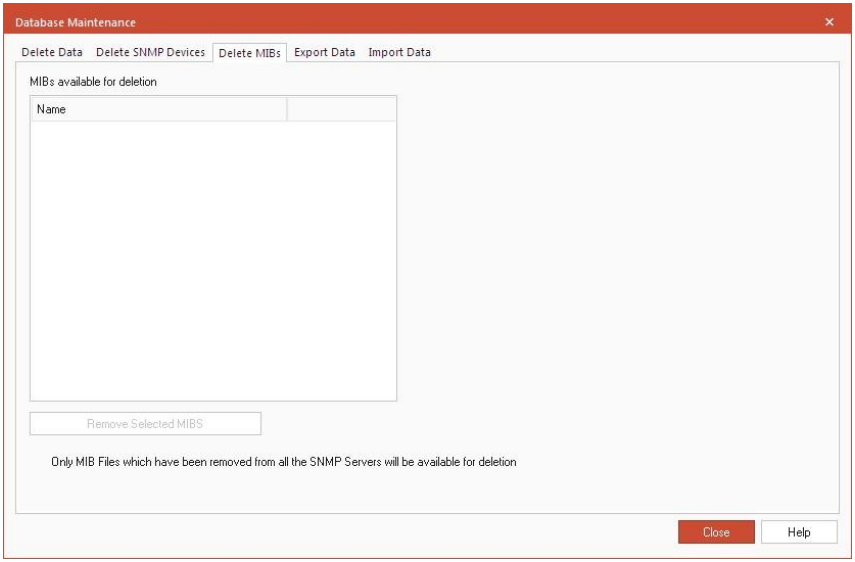
You may find the database is holding details of Devices that are no longer required. This option enables you to delete Devices and remove any related data.



1. From the Available SNMP Devices list, select the Devices to remove. This can be done by individual Device, department level (if multiple Devices are to be removed) or by Dynamic Group.
2. Click  to add the selected items to the SNMP Devices to delete list. Individual
3. Devices can be removed from the list by clicking . This is useful if not all users within a department are to be deleted.

Delete MIBs

This option allows you to delete MIB files that are no longer required.



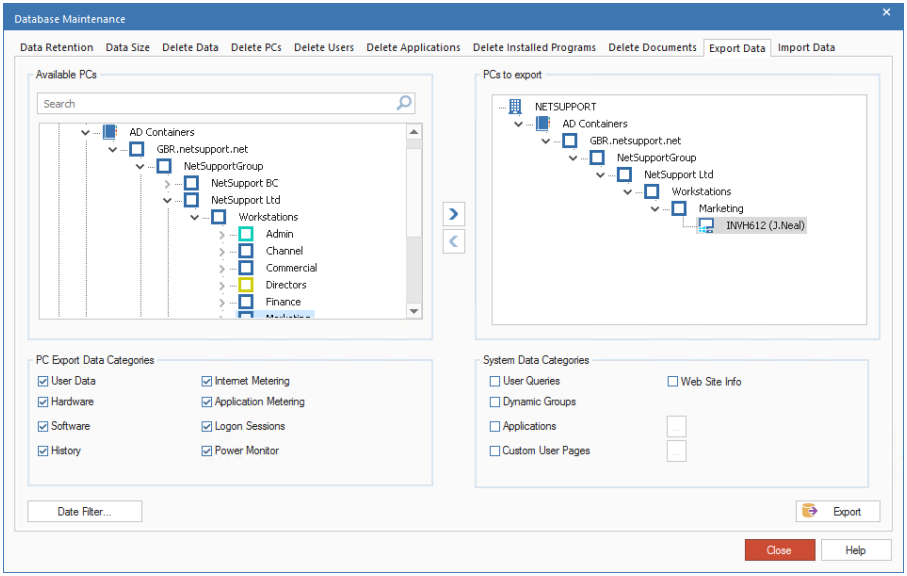
Note: For a MIB to be available for deletion it must be deleted from the device and the data must be removed from the NetSupport DNA database.

1. Select the required MIB from the list and select **Remove Selected MIBs**.

Export Data

This option enables data in the NetSupport DNA database to be exported. This can act as a secure backup in the event of a database corruption or it can be imported to another database.

Note: If you are in the Devices Tree view, you will see data relating to SNMP devices.



1. In the Available PCs Tree, select the Agent(s) to export data from.

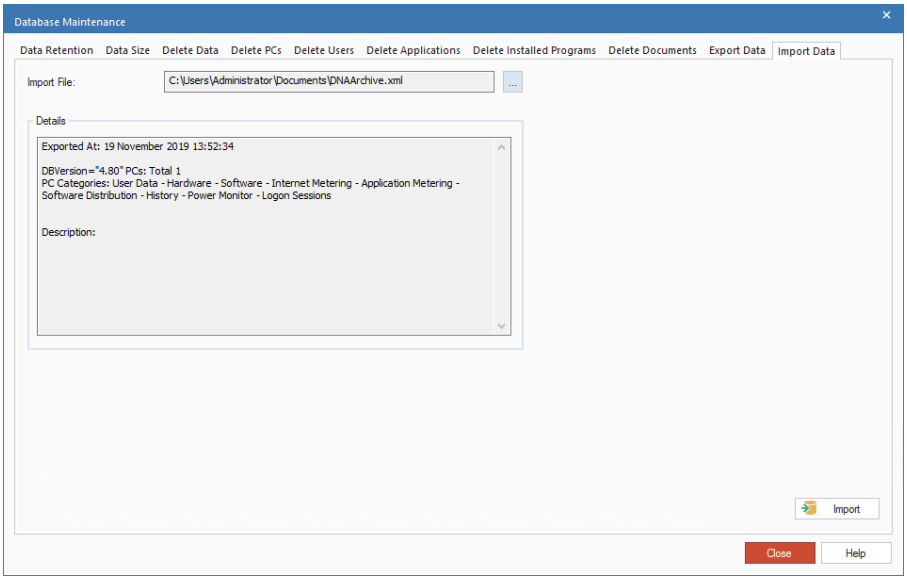
   Note: To search for an item in the Tree view, enter the name or partial name of the PC or department in the search box and click . The first matching item in the Tree view will be displayed along with the number of matches found. You can scroll through these using the arrows. Click to clear the search.

2. Click to transfer to the PCs to export window.
3. Deselect any data categories that you do not wish to include.
4. You can further limit the amount of exported data by applying a **Date filter**.
5. Indicate if any additional system data is to be included. In the case of Applications and Custom User pages, click and select the items to include.

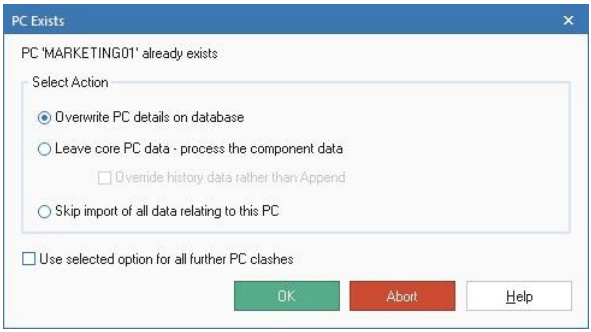
6. Click **Export** when ready. Enter a name for the .XML file that will be created. You will be prompted to enter a suitable description. This will help identify the data, if re-importing.
7. Click **OK**. A confirmation message will appear when the export is complete.

Import Data

This option allows you to import data that has previously been exported.



1. Click and browse for the required export file.
2. The Details window will provide a summary of the file content.
3. Click **Import**. If there are potential clashes between the data being imported and information already present, you will be prompted to take appropriate action.



Overwrite PC details on database
Continue importing the data, replacing information currently held in the database.

Leave core PC data - process the component data
Only import component related data, Internet Metering, Application Metering etc. Existing user/PC details will not be overwritten.

Override history data rather than Append
The history data will be overridden instead of appended.

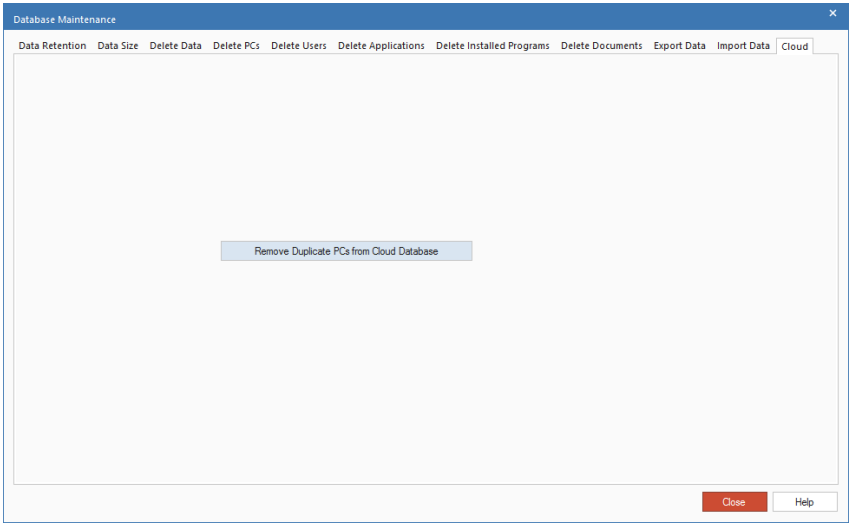
Skip import of all data relating to this PC
Cancel the import.

Use selected option for all further PC clashes
Set the chosen option as the default for future procedures.

4. A confirmation message will appear when the import is complete.

Cloud

In certain circumstances, our technical support team may provide you with SQL scripts to remove duplicate PCs. If you are using the NetSupport DNA Cloud Console, you will need to remove the duplicate PCs from here to ensure both the Windows and Cloud Console are synchronised. This option allows you to remove duplicate PCs and the associated data from the Cloud Console.



Note: This tab will only appear in the Education Edition of NetSupport DNA and if you have the Cloud Console enabled.

1. Click **Remove Duplicate PCs from Cloud Database**.
2. A confirmation will appear asking if you want to remove duplicate PCs from the Cloud Console. Click **Yes**.

NetSupport DNA Agent Window

The Agent window provides Agents with a status of key components that can affect them, along with an overview of NetSupport DNA.

Note: The Agent window is only available for NetSupport DNA Windows Desktop and Mac Agents.

When an Agent right-clicks the NetSupport DNA Agent icon in their system tray, a list of options will be displayed.

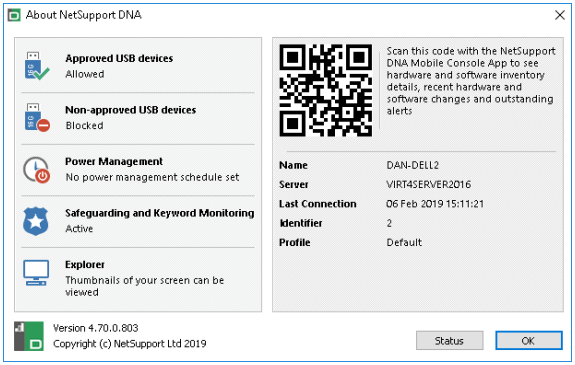
From here, the Windows Agent can:

- open the main Agent window
- locate and send a message to another logged on user (if enabled in the Console)
- manage user accounts (if enabled in the Console)
- report a concern*
- access safeguarding resources*
- see if a power schedule is in force
- request a package
- see any USB Device approval requests
- edit user details (this option can be disabled in the Console).

The Mac Agent can:

- report a concern*
- access safeguarding resources*
- open the NetSupport DNA website
- open the main Agent window.

To open the main Agent window, select **About DNA** from the list.



The Agent is provided with details of NetSupport DNA and the Server they are connected to. A QR code is displayed, which can be scanned by the NetSupport DNA Mobile Console. This enables technicians to identify the machine and see the hardware and software inventory details, recent hardware and software changes and any outstanding alerts.

Windows Agents will also see the status for approved and non-approved USB devices; if a power schedule has been set; if safeguarding* (reporting a concern and phrase monitoring) is active; and Explorer mode.

The Agent can see the current status for each of the components by clicking **Status**.

* These features are only available in the Education Edition of NetSupport DNA.

CONTACT US

UK & International
www.netsupportsoftware.com
Technical Support: *support@netsupportsoftware.com*
Sales: *sales@netsupportsoftware.com*

North America
www.netsupport-inc.com
Technical Support: *support@netsupportsoftware.com*
Sales: *sales@netsupport-inc.com*

Canada
www.netsupport-canada.com
Technical Support: *support@netsupportsoftware.com*
Sales: *sales@netsupport-canada.com*

Germany, Austria and Switzerland
www.pci-software.de
Technical Support: *support@netsupportsoftware.com*
Sales: *sales@pci-software.de*

Japan
www.netsupportjapan.com
Technical Support: *support@netsupportsoftware.com*
Sales: *sales@netsupportjapan.com*

INDEX

about NetSupport DNA, 12
acceptable use policies, 353
  settings, 139
active directory, 53, 97
activity monitoring, 184
add non standard hardware, 190
add remote user, 190
adding bookmarks, 351
agent
  add to department, 103
  Android, 59
  chat, 363
  Chrome, 61
  iOS, 57
  locate a user, 362
  power on, 368
  request package, 312
  settings, 116
  window, 386
agent gateway configurator, 64
agent settings, 116
agent status tool, 368
agent window, 386
alerting, 262
  active alerts, 270
  alert manager, 266
  closing alerts, 274
  console alerts, 269
  dna server alerts, 269
  group definitions, 268
  history, 275
  pc alerts, 264
  review pc alerts, 272
  setting up alerts, 267
  settings, 133
alerts, 262
allow concurrent logins, 117
Android, 59
application groups, 210
application metering, 290
  apply restrictions, 293
  block apps by window title using Spotlight, 295
  configure settings, 123
  window title blocking, 126
application packager, 316
  script builder, 320
apply internet restrictions using spotlight, 169
approved application lists, 293
approved web site lists, 284, 288
archive data, 371
assigning profiles, 113
audit
  settings, 156
audit log, 357
automatic agent discovery, 91
barcodes, 370
bind users, 177
block application by window title, 295
block apps by window title, 126
block internet sites, 119
bookmarks, 351
browser for Android, 59
change pc owner, 177
chatting to agents, 363
check database size, 371
Chrome, 61
client
  configure settings, 116
closing alerts, 274
cloud console, 158
complex passwords, 80
component settings, 115
concerns, 244
  adding notes, 254
  archiving, 255
  reporting via a website, 250
  reporting via the DNA Agent, 249
  safeguarding resources, 247
concurrent logins, 117
configure DNA settings, 111
configure remote control, 364
console
  chatting to agents, 363
  cloud, 158
  configure DNA settings, 111
  create additional operator logins, 77
  create departments, 99
  create dynamic groups, 105

create roles, 82
discovery & deploy tool, 84
installation, 37
login, 71
monitor application usage, 290
monitor internet usage, 281
move agents between departments, 103
remote control an agent, 364
run query, 344
screen layout, 72
starting, 71
user details, 172
console alerts, 269
console preferences, 148
active directory settings, 153
audit, 156
auto discovery, 155
email settings, 154
file locations, 157
general, 150
user interface, 152
console roles, 82
contact NetSupport, 388
contracts, 198
create
approved & restricted application lists, 293
approved & restricted web site lists, 284
console logins, 77
departments, 99
dynamic groups, 105
non windows based PC, 190
query, 335
reports, 332
roles, 82
safeguarding user accounts, 221
warehouse, 314
create or edit roles, 82
creating qr code labels, 370
crystal reports, 332
custom user details, 178
data retention, 371
database
installation, 37
maintenance, 371
database maintenance
cloud, 385
data retention policy, 371
data size, 373
delete applications, 377
delete data, 374
delete documents, 379
delete installed programs, 378
delete MIBs, 381
delete PCs, 375
delete SNMP devices, 380
delete users, 376
export data, 382
import data, 383
database wizard, 43
delete
PCs from database, 371
records from database, 371
delete users, 371, 376
departments
add agents, 103
change properties, 101
create, 99
deploy
deploy tool, 85
options dialog, 87
Windows Vista, 90
Windows XP, 89
deploy agent, 84
device discovery, 94
discovery
automatic agent discovery, 91
devices, 94
discovery & deploy tool, 84
display sections, 95
distribution. *See* software distribution
dna agent window, 386
DNA database wizard, 43
gateway settings, 49
install and set up database, 44
licence registration, 47
miscellaneous settings, 52
mobile connection settings, 51
reset administrator password, 48
set up console user, 46

set up database user, 45
snmp settings, 50
DNA gateway, 62
agent gateway configurator, 64
server gateway configurator, 63
status, 62
DNA server alerts, 269
DNA settings, 115
dynamic groups, 105
editor, 108
edit
application groups, 210
department properties, 101
DNA settings, 111
query, 343
user details, 175
edit installed programs, 207
efficiency view, 162
enable thumbnails, 130
energy monitor, 277
energy monitor settings, 143
esafety, 220
concerns, 244
keywords and phrases, 229
phrase monitoring, 225
phrase monitoring settings, 137
report concern settings, 135
reporting a concern, 249
risk analysis, 256
safeguarding roles, 221
vulnerable students, 174
existing installation, 42
explorer, 164
settings, 130
spotlight, 164, 169
thumbnail view, 164
export
database maintenance, 382
features, 14
install server & console, 37
installing, 34
file extensions
software inventory scan, 131
file location settings, 157
gateway, 62
agent gateway configurator, 64
server gateway configurator, 63
status, 68
GDPR, 200, 207
getting started
console screen layout, 72
create departments, 99
start console, 71
group definitions, 268
hardware
contract manager, 198
peripherals, 194
hardware inventory, 187
add non standard hardware, 190
configure settings, 121
history, 275
include peripheral devices, 190
hide/show agent icon, 116
history window, 275
housekeeping, 371
import
database maintenance, 383
software distribution package, 313
stand alone or remote PC, 190
installation, 28
active directory, 53
Android, 59
Chrome agent, 61
command line installation, 54
custom, 34
existing, 42
install server & console, 37
iOS, 57
Mac agent, 56
planning, 28, 29
reconfigure install options, 43
register license using DNA database wizard, 47
reset system admin password using DNA database wizard, 48
select enterprise type, 41
select setup type, 33
SQL server, 36
starting, 32
upgrading, 69
using the DNA database wizard, 43
web server, 39

installed programs manager, 204
integrated remote control, 364
integration with active directory, 97
internet metering, 281
  apply restrictions, 284
  apply restrictions using spotlight, 169, 288
  block sites, 119
  configure settings, 119
introduction, 12
  DNA packs, 27
  features, 14
inventory
  hardware, 187
  software, 200
iOS browser, 57
keyword and phrase monitoring, 225
  creating, 231
licence levels, 204
licence management, 208
license registration
  DNA database wizard, 47
load console, 71
locate a user, 362
logging in, 71
logon control settings, 117
Mac, 56
manage user accounts, 360
manage web concern, 160, 250
merge
  application groups, 210
merge installed programs, 205
message
  send to agents, 367
metering
  monitor application usage, 290
  monitor internet usage, 281
mobile console, 70
monitor application usage, 290
monitor internet usage, 281
monitor printing, 297
move agents between departments, 103
multiple logins, 117
NetSupport
  contact us, 388
NetSupport DNA
  application packager, 316
  DNA purchase packs, 27
  features, 14
  installation, 28
  remote control, 364
  reporting, 332
  settings, 111
  system requirements, 28
non scanned hardware, 190
package. *See* software distribution
password
  reset system admin password, 48
  using the DNA database wizard, 43
pc alerts, 264
peripheral hardware, 190
phrase cloud, 242
phrase monitoring, 225
  adding new, 231
  application ignore lists, 239
  export, 232
  import, 232
  keywords and phrases, 229
  phrase cloud, 242
  review, 235
  settings, 137
  url ignore lists, 240
pixelate thumbnails, 130
planning an installation, 28
planning and installation, 29
power on agent PC, 368
pre-requisites, 28
prevent multiple logins, 117
print monitor, 297
  configure print costs, 299
  settings, 124
privacy mode, 130
profiles, 111
  assigning, 113
properties
  departments, 101
purchase packs, 27
QR codes, 370
queries
  scheduled queries, 346
query tool, 335
  edit query, 343

run query, 344
reassign agents to departments, 103
reconfigure install options, 43
redirect blocked sites, 119
remote control, 364
settings, 140
user acknowledgement, 140
report concern
settings, 135
via a website, 250
via the DNA Agent, 249
reports, 332
request user acknowledgement, 140
request user details, 175
reset system admin password using DNA database wizard, 48
resource scan, 131
restrict application usage, 293
restrict internet usage, 284, 288
restricted application lists, 293
restricted web site lists, 284, 288
review pc alerts, 272
risk analysis, 256
at risk application lists, 259
at risk url lists, 260
settings, 142
roles, 82
run console, 71
run query, 344
safeguarding, 220
roles, 221
safeguarding console, 158
safeguarding roles, 221
scan
for specific file types, 131
scheduled queries, 346
screen layout
console, 72
screen recording, 237
script builder, 320
secure area, 358
secure mode, 80
select features to install, 34
send message, 367
server gateway configurator, 63
server installation, 37
set concurrent logins, 117
settings, 111
acceptable use policies, 139
agent, 116
alerting, 133
application metering, 123
client, 116
console preferences, 148
DNA Cloud Console, 158
energy monitor, 143
explorer, 130
hardware inventory, 121
internet metering, 119
logon control, 117
manage web concern, 160
phrase monitoring, 137
print monitor, 124
remote control, 140
report concern, 135
risk analysis, 142
show/hide agent icon, 116
software distribution, 129
software inventory, 131
USB device control, 125
user details, 122
window title blocking, 126
show/hide agent icon, 116
SNMP
alert, 326
alert configuration, 328
alerting settings, 146
configuration settings, 145
creating alerts, 329
discovery, 94
display sections, 95
history, 330
history settings, 147
monitor, 324
monitor settings, 146
server configuration, 66
SNMP alerts, 326
configuration, 328
new alerts, 329
SNMP history, 330
software distribution, 301
advertise package, 311

agent request package, 312
application packager, 316
configure settings, 129
create package, 305
distribute package, 307
import package, 313
package admin, 304
scheduling a package, 310
script builder, 320
warehouse, 314
software inventory, 200
application groups, 210
configure settings, 131
edit installed programs, 207
for non scanned users, 190
history, 275
installed programs manager, 204
licence levels, 204
licence management, 208
merge installed programs, 205
resource scan, 131
spotlight, 169
approved & restricted web site lists, 288
block apps by window title, 169, 295
currently running processes, 169
currently running services, 169
internet restrictions, 169
start console, 71
starting a DNA installation, 32
summary screen, 161
system requirements, 28
thumbnails
enable, 130
enable privacy mode, 130
explorer mode, 164
tools
agent discovery & deploy, 84
agent status, 368
chatting to agents, 363
database maintenance, 371
query tool, 335
remote control, 364
send a message, 367
track inventory changes, 275
tree view
add new department, 99
add non scanned items, 190
change pc owner, 177
create dynamic groups, 105
update install details, 43
upgrading from existing dna versions, 69
USB device control, 214
registering USB devices, 217
settings, 125
USB device details, 218
user acknowledgement, 140
user defined fields editor, 178
user details, 172
bind users dialog, 177
change pc owner, 177
customise, 178
edit, 175
settings, 122
show welcome page, 122
user logins
concurrent logins, 117
vault, 358
view agent remotely, 364
vulnerable students, 174
warehouse, 314
web concerns, 160, 250
web metering, 281
apply restrictions, 284
apply restrictions using spotlight, 288
settings, 119
welcome to NetSupport DNA, 12
window
efficiency view, 162
window
block apps by window title, 126
console screen layout, 72
summary, 161
window
user details, 172
window
hardware inventory, 187
window
software inventory, 200
window
alerting, 262
window

history, 275
window
energy monitor, 277
window
internet metering, 281
window
application metering, 290
window
software distribution, 301
wizard
application packager, 316
DNA database wizard, 43