NetSupport

NetSupport DNA

Handbuch

Version 4.80

Handbuch COPYRIGHT (C) 2020 NetSupport Ltd. Alle Rechte vorbehalten.

Die Informationen in diesem Dokument können ohne vorherige Benachrichtigung geändert werden. NetSupport Ltd. behält sich das Recht vor, dieses Dokument zu überarbeiten und von Zeit zu Zeit an seinem Inhalt Änderungen vorzunehmen, ohne dazu verpflichtet zu sein, eine oder mehrere Personen über solche Überarbeitungen und Änderungen in Kenntnis zu setzen.

Die in diesem Dokument beschriebene Software wird im Rahmen eines Lizenzvertrags geliefert und ist durch internationale Urheberrechtsgesetze geschützt. Sie dürfen es nur zur Sicherung kopieren und es ausschließlich gemäß der Beschreibung im Lizenzvertrag verwenden.

Alle stillschweigenden Garantien einschließlich von Garantien zur Marktgänglichkeit oder Eignung zu einem bestimmten Zweck sind auf die Bedingungen der ausdrücklichen, im Lizenzvertrag beschriebenen Garantien beschränkt.

Programm COPYRIGHT (C) 2020 NetSupport Ltd. Alle Rechte vorbehalten.

Warenzeichen

NetSupport und NetSupport DNA sind eingetragene Warenzeichen von NetSupport Ltd.

Windows, Windows 2008, XP, Vista, Windows 7, Windows 8/8.1 und Windows 10 sind Warenzeichen der Microsoft Corporation.

Andere Produkte, Warenzeichen oder eingetragene Warenzeichen sind das Eigentum ihrer jeweiligen Besitzer.

Software-Lizenzvertrag - NetSupport DNA Enterprise Edition

Lesen Sie diesen Vertrag bitte vor der Verwendung Ihrer Kopie der NetSupport Software durch. Es handelt sich hierbei um einen Rechtsvertrag zwischen Ihnen und PCI Software GmbH. Wenn Sie nicht an die Bedingungen dieses Lizenzvertrags gebunden sein möchten, dürfen Sie die Software weder laden, noch aktivieren oder verwenden.

LAUFZEIT: Vorbehaltlich der Kündigung unter nachfolgender Kündigungsklausel ist die Lizenzdauer unbeschränkt.

LIZENZ-ERTEILUNG: Vorbehaltlich Zahlung der geltenden Lizenzgebühren und Ihrer Erfüllung der Bedingungen dieses Vertrags erteilt PCI Software GmbH Ihnen hiermit das nicht-exklusive, nicht-übertragbare Recht, eine Kopie der angegebenen Version der von Ihnen gekauften Software zu benutzen.

BENUTZUNG: Die Software ist für die Volumennutzungsbedingungen lizenziert, die in der dafür geltenden Auftragsbestätigung, der Produktrechnung, dem Lizenzzertifikat oder der Produktverpackung angegeben sind. Sie können soviele Kopien der Software auf der Anzahl der Geräte anfertigen, installieren und benutzen, wie die Bedingungen vorgeben. Sie müssen einen angemessenen Mechanismus einsetzen, um sicherzustellen, dass die Anzahl der Geräte, auf denen die Software installiert worden ist, die Anzahl der von Ihnen beschafften Lizenzen nicht überschreitet.

SERVER-Benutzung. In dem Ausmaß, in dem dies in der dafür geltenden Auftragsbestätigung, Produktrechnung, Produktverpackung oder dem Lizenzzertifikat angegeben ist, können Sie die Software auf einem Gerät oder einem Server innerhalb einer Mehrbenutzer- oder Netzwerk-Umgebung benutzen ("Server-Benutzung"). Für jedes Gerät bzw. für jeden Arbeitsplatz, der irgendwann eine Verbindung mit der Software herstellen kann, ist eine separate Lizenz erforderlich, unabhängig davon, ob diese lizenzierten Geräte oder Plätze gleichzeitig eine Verbindung mit der Software haben oder die Software zu irgendeinem bestimmten Zeitpunkt tatsächlich benutzen. Ihre Nutzung der Software oder Hardware, die die Anzahl der Geräte oder Plätze reduziert, die direkt oder gleichzeitig mit der Software verbunden sind oder diese benutzen (z.B. "Multiplexing" oder "Pooling" Software oder Hardware) verringert nicht die Anzahl der erforderlichen Lizenzen. Genau gesagt muss die Anzahl Ihrer Lizenzen gleich der Anzahl der separaten Inputs an die Multiplexing- oder Pooling-Software bzw. das Hardware-"Front-End" sein). Wenn die Anzahl der Geräte oder Arbeitsplätze, die eine Verbindung mit der Software herstellen kann, die Anzahl der von Ihnen beschafften Lizenzen überschreitet, müssen Sie einen angemessenen Mechanismus einsetzen, der sicherstellt, dass Ihre Nutzung der Software die auf der von Ihnen beschafften Lizenz angegebenen Nutzungsgrenzen nicht überschreitet.

COPYRIGHT: Diese Software ist von internationalen Urheberrechtsgesetzen geschützt. Sie dürfen sie nur zur Sicherung kopieren. Die Software ist an Sie lizensiert, aber nicht verkauft.

EINSCHRÄNKUNGEN: Weder Sie noch ein beliebiger Weiterverkäufer darf diese Software vermieten, leasen, lizensierte Kopien davon [zur Ansicht] verkaufen, oder auf eine andere Weise die Rechte zur Verwendung dieser Software an eine Drittperson übertragen. Sie haben allerdings das Recht, Ihre Originalkopie zu verkaufen oder verschenken, vorausgesetzt dass Sie selbst keine Kopien davon behalten. Die Software darf weder geändert, zerlegt oder zurückentwickelt werden, ohne dazu vorher die schriftliche Genehmigung von PCI Software GmbH einzuholen.

BESCHRÄNKTE GARANTIE: PCI Software GmbH garantiert im Wesentlichen die Leistung der Software in Übereinstimmung mit den Begleitdokumenten für eine Dauer von neunzig (90) Tagen ab Verkaufsdatum. Die gesamte Haftbarkeit von PCI Software und Ihr ausschließliches Rechtsmittel ist entweder a) der Ersatz der fehlerhaften Software oder b) die Rückerstattung des gezahlten Preises. Das Rechtsmittel darf von PCI Software gewählt werden und unterliegt dem Beweis, dass das Produkt bei einer bevollmächtigten Stelle gekauft wurde.

Alle stillschweigenden Garantien, einschließlich von Qualitätsgarantien oder Garantien zur Eignung für einen bestimmten Zweck, sind auf die Bedingungen der ausdrücklichen Garantien beschränkt. PCI Software GmbH. ist auf keinen Fall haftbar für den Verlust von Gewinn, Daten oder Informationen beliebiger Art. Ferner übernimmt es auch keinerlei Haftung für spezielle, nebenher oder als Folge entstandene, indirekte oder andere ähnliche Schäden, die auf eine Verletzung des Garantievertrags oder die Verwendung der Software trotz Benachrichtigung über die Möglichkeit solcher Schäden zurückzuführen sind. In einigen Ländern ist die Einschränkung oder der Ausschluss von nebenher oder als Folge entstandenen Schäden nicht gestattet, d. h. dass sich obige Einschränkung oder Ausschluss u. U. nicht auf Sie bezieht. Die Garantie beeinträchtigt Ihre gesetzlich verankerten Rechte nicht, und Sie haben u. U. zusätzliche Rechte, die sich von Land zu Land unterscheiden. Auf jeden Fall geht die maximale Haftbarkeit von PCI Software nicht über den vom Endbenutzer/Lizenzinhaber bezahlten Preis hinaus.

KÜNDIGUNG: Sie können diese Lizenz und diesen Vertrag jederzeit kündigen, indem Sie das Programm und seine Dokumentation, zusammen mit allen Kopien in beliebiger Form, zerstören.

PCI Software GmbH. kann diese Lizenz sofort durch eine schriftliche Benachrichtigung an Sie kündigen, wenn Sie eine Bedingung dieser Lizenz ernsthaft verletzen und (im Falle einer Verletzung, die sich korrigieren lässt) innerhalb von 30 Tagen nach Erhalt einer diesbezüglichen schriftlichen Aufforderung durch PCI Software GmbH. die Verletzung nicht korrigiert haben (eine solche Aufforderung muss Sie über die Kündigungsabsicht von PCI Software in Kenntnis setzen). Nach der Kündigung müssen Sie das Original und sämtliche Kopien der Software zerstören oder an PCI Software GmbH zurückgeben und es PCI Software GmbH schriftlich bestätigen, dass dies getan wurde.

SUPPORT: Wenn bei der Installation der Software Probleme auftreten, müssen Sie sich zunächst einmal an Ihren Lieferanten wenden. Sie können separat Support und Wartung kaufen, was auch die Lieferung von Erweiterungen und Upgrades mit einschließt.

GELTENDES GESETZ: Dieser Vertrag unterliegt dem englischen Gesetz.

Inhalt

WILLKOMMEN BEI NETSUPPORT DNA 12
Informationen zu wichtigen Features 14
DNA Paket 30
INSTALLATION 31
Systemanforderungen 31
Planen einer Installation 32
Starten der Installation 35
NetSupport-Lizenzvertrag 35
Setuptyp auswählen 36
Benutzerdefiniertes Setup 37
SQL Server Installation 39
Einrichtung von Server 40
Datenbanksetup des Webservers 41
Unternehmenstyp wählen 44
Vorhandene Installation 46
Verwendung des DNA Datenbank-Assistenten 47
Installation und Setup der Datenbank zur Verwendung 48
Setup eines NetSupport DNA-Benutzers für den Zugriff auf die Datenbank 48
Setup von Administratorbenutzern für den Zugriff auf den DNA-Server 49
Registrieren einer Lizenz 50
Systemadmininistrator-Passwort zurücksetzen 52
Gateway-Einstellungen 53
SNMP Einstellungen 54
Mobilverbindungseinstellungen 55
Verschiedene Einstellungen 56
Installation über Active Directory 57
Option "Erweitert" - Befehlszeileninstallation 58
Installation von NetSupport DNA Agent auf Mac Systemen 60
NetSupport iOS Browser 61
NetSupport DNA Browser für Android 63

NetSupport DNA Chrome Agent 65
DNA Gateway 66
Server Gateway Konfigurator 67
Agent Gateway Konfigurator 69
SNMP-Server-Konfiguration 71
Gateway-Status 72
Aktualisierung von vorhandenen DNA-Versionen 73
NetSupport DNA Mobile Konsole 74
ERSTE SCHRITTE 75
Ausführen der Konsole 75
Das Konsolefenster 76
Zusätzliche Konsolebenutzer erstellen 81
Sicherer Modus 82
Erstellen oder Bearbeiten von Anmeldungen für Konsolebediener 84
Erstellen oder Bearbeiten von Konsolerollen 86
Suche und Verteilung-Tool 88
Suchen und Verteilen an PCs 89
Dialogfeld "Verteilungsoptionen" 91
Deployment unter Windows XP 93
Verteilung unter Windows Vista 94
Automatische Agent-Ermittlung 95
Verwaltung ermittelter Computer 96
Geräteermittlung 97
Anzeigeabschnitte 99
Integration mit Active Directory 101
Abteilung erstellen 103
Abteilungseigenschaften ändern 105
Hinzufügen von Agents zu Abteilungen 107
Dynamische Gruppen 109
Dynamische Gruppen-Editor 112
NetSupport DNA Konfiguration 115
Profile 115
Profile zuweisen 117

NetSupport DNA-Einstellungen 119
Agent 120
Anmeldungssteuerung 122
Internet-Metering- Einstellungen 123
Hardware Inventory 126
Benutzerdetails 127
Anwendungsmetering 129
Druckerüberwachungs-Einstellungen 130
USB-Gerätesteuerungs - Einstellungen 131
Titelblockierung Einstellungen 132
Softwareverteilung 135
Explorer 136
Softwareinventarisierung 137
Alerting 139
Anliegen melden Einstellungen 141
Begriffsüberwachung-Einstellungen 143
Acceptable Use Policy 145
Fernwartungseinstellungen 146
NetSupport DNA Risikoanalysen-Einstellungen 148
Energiemonitor 149
NetSupport DNA SNMP-Konfigurationseinstellungen 151
SNMP-Überwachungseinstellungen 152
SNMP-Alerteinstellungen 152
SNMP-Verlaufeinstellungen 153
Konsoleneinstellungen 154
Allgemein 156
Benutzeroberfläche 158
Active Directory-Einstellungen 160
E-Maileinstellungen 161
Automatische Ermittlung 162
Audit-Einstellungen 163
Dateispeicherort-Einstellungen 164
NetSupport DNA Cloud Konsole 165
Website-Anliegen verwalten 168

VERWENDUNG VON NETSUPPORT DNA 169
Konsolefenster - Zusammenfassungsbildschirm 169
Effizienzansicht 170
Explorer 172
Spotlight 177
Benutzerdetails 181
Benutzerdetails anfordern/bearbeiten 185
Dialogfeld „Benutzer binden“ 188
Angepasste Benutzerdetails 190
Angepasste Benutzerdetails - Steuerelemente 192
Aktivitätsüberwachung 197
Hardwareinventarisierung 201
Inventardaten für entfernte Benutzer oder nicht gescannte Geräte sammeln 204
Nicht-Standard-Hardware hinzufügen 205
Neuen PC erstellen 205
Alleinstehenden/entfernten Gerät importieren 207
Hardware-Zusatzgeräte hinzufügen 209
Hardware-Zusatzgeräte 211
Vertragsmanager 213
Softwareinventarisierung 215
Manager für installierte Programme 219
Installierte Programme zusammenführen 221
Installierte Programme bearbeiten 222
Lizenzmanagement für installierte Programme 224
Lizenzinfo 225
Anwendungsgruppen 226
Anwendungsgruppe bearbeiten 228
Anwendungsgruppen zusammenführen 230
USB-Geräte-Steuerung 231
Registrierung von USB-Geräten 234
USB-Gerät-Details 236
eSafety 237
eSafetyrollen 238

Verwalten der eSafety Administratoren und Benutzer 239
Hinzufügen oder bearbeiten von eSafety Administratoren und Benutzer 241
Begriffsüberwachung 243
Schlüsselwörter- und Begriffe-Datenbankliste 248
Schlüsselwörter und –begriffe erstellen oder bearbeiten 250
Begriffe importieren/exportieren 251
Überprüfung der ausgelösten Begriffe 253
Anwendung-ignorieren-Listen 258
URL-ignorieren-Listen 260
Begriff-Cloud 262
Anliegen 265
eSafety Ressourcen 269
Ein Anliegen melden 271
Ein Anliegen über eine Website melden 273
Notizen zu einem Anliegen hinzufügen 277
Anliegen archivieren 278
Risikoanalyse 279
Gefährdende-Anwendung-Listen 283
Gefährdende-URL-Listen 285
Alerting 287
PC-Alerts 291
Alert-Manager 292
DNA Alert-Assistent 293
Gruppendefinitionen 294
DNA Server\Konsolen-Alerts 296
Aktive Alerts 297
Aktive PC-Alerts überprüfen 298
Schließen von Alerts 302
History-Fenster 303
Energiemonitor 305
Energiekosten 308
Internet-Metering 309
Internet-Einschränkungen 313

Benutzung der Spotlight-Funktion, um URLs einer Genehmigt- bzw. Eingeschränkt-Liste hinzuzufügen 317
Anwendungsmetering 319
Anwendungseinschränkungen 323
Anwendungen nach Fenstertitel blockieren 325
Druckerüberwachung 327
Druckkosten konfigurieren 330
Softwareverteilung 332
Paketverwaltung 335
Neues Paket erstellen 336
Verteilen eines Pakets 338
Planen eines Pakets 342
Anbieten eines Pakets 344
Anfordern eines Pakets 345
Importieren eines Pakets 346
Softwareverteilungs-Warehouse 347
DNA Application Packager 349
DNA Application Packager - Script Builder 354
SNMP-Überwachung 357
SNMP-Alert 360
SNMP-Alert-Konfiguration 362
SNMP – Neues Alert erstellen 363
SNMP-Verlauf 364
Bericht- und Analysetools von DNA 367
Abfragetool 370
Erstellen einer neuen Abfrage 371
Vorhandene Abfrage bearbeiten 378
Abfrage ausführen 379
Geplante Abfragen 381
PCs, Benutzer und Geräte finden 383
Lesezeichen 386
Acceptable Use Policies 388
Audit-Protokoll 391
Tresor 392

Benutzerkonten verwalten 394
Chatten mit Agents 397
Benutzer suchen 398
Fernsteuerung 399
Nachricht senden 402
Agentstatus 403
Erstellung von QR-Code-Aufklebern 405
Datenbankwartung 407
NetSupport DNA Agent-Fenster 421
KONTAKTANGABEN 423

WILLKOMMEN BEI NETSUPPORT DNA

Bildungswesen
NetSupport DNA ist für leichtes Management der schul- oder campusweiten IT-Infrastruktur optimiert und bietet eine komplette Toolbox mit Funktionen zur Unterstützung des effektiven Managements von Schul-, Personal- und Schüler-Technologie. Diese Lösung bietet für jede einzelne Funktion leichte Installation und Benutzung.

Zeit sparen mit proaktiven Warnalerts für Probleme im gesamten Netzwerk – von Serverversagen, geringem Speicherplatz und nicht-autorisierten Software-Installationen zu Lizenzerfüllung und Hilfeanforderungen der Schüler. Berichte für das Führungsteam automatisch und regelmäßig erstellen und die unterstützenden Mobil-Apps benutzen, um sicherzustellen, das Schlüsseldaten für das IT-Personal zugänglich sind, egal es sich gerade befindet.

IT-Kosten reduzieren durch Identifizierung von Hardware, die entweder neu eingesetzt oder aktualisiert werden kann, statt ersetzt zu werden; Nachverfolgung der Softwarelizenz-ereitstellung und, was sehr wichtig ist, der Lizenznutzung – dadurch werden kostspielige Lizenzerneuerungen für Software vermieden, die nicht mehr gebraucht wird; Überwachung der Druckernutzung in der ganzen Schule; Energieüberwachung und Bereitstellung einer Energiemanagement-Richtlinie für die relevanten Bereiche der Schule.

Erzielen Sie eine sicherere Umgebung durch die Überwachung und Kontrolle der Internetnutzung mit Listen genehmigter und beschränkter URLs. Lassen Sie sich bei Schutzproblemen durch Schlüsselwortüberwachung warnen, und ermöglichen Sie es Schülern, etwaige Anliegen direkt einem Personalmitglied zu melden, dem sie vertrauen. Steuern Sie den Zugriff durch Endpoint-Sicherheit in der gesamten Schule; bieten Sie Benutzerakzeptierungsrichtlinien; überwachen Sie Schüler im Klassenzimmer und vieles mehr.

Unternehmens
Eine komplette ITAM Lösung für effektives Management des Unternehmens. NetSupport DNA bietet eine umfassende Suite von Funktionen zur Unterstützung des Managements und Verwaltung der IT Assets.

NetSupport DNA ist für leichte Installation konzipiert und leichte Benutzung ist bei allen Funktionen Priorität. NetSupport DNA bietet Flexiblität, so dass es Ihren Unternehmensanforderungen gemäß skaliert

werden kann – von einem einzigen SME zu großen Implementierungen mit mehreren Standorten – und zwar innerhalb Ihres IT-Budgets

Sparen Sie Zeit mit proaktiven Warnalerts für Probleme im gesamten Netzwerk – von Serverversagen, geringem Speicherplatz und nicht-autorisierten Software- Installationen zu Lizenzerfüllung und Hilfeanforderungen der Benutzer; mit Berichten, die automatisch und regelmäßig für das Führungsteam erstellt werden; und Benutzung der unterstützenden Mobil-Apps, um sicherzustellen, das Schlüsseldaten für das IT-Personal zugänglich sind, egal es sich gerade befindet.

IT-Kosten reduzieren durch Identifizierung von Hardware, die entweder neu eingesetzt oder aktualisiert werden kann, statt ersetzt zu werden; Nachverfolgung der Softwarelizenz-Bereitstellung und, was sehr wichtig ist, der Lizenznutzung – dadurch werden kostspielige Lizenzerneuerungen für Software vermieden, die nicht mehr gebraucht wird; Überwachung der Druckernutzung im ganzen Unternehmen; Energieüberwachung und Bereitstellung einer Energiemanagement-Richtlinie für die relevanten Bereiche des Unternehmens.

Fügen Sie Sicherheit hinzu durch Verhinderung des Zugriffs auf nicht-genehmigte Websites; Beschränkung der Benutzung wichtiger Anwendungen auf befugte Benutzer; tragen Sie dazu bei, die Unternehmensdaten durch profilierten Memorystick- Zugriff zu schützen; Lieferung von Benutzerakzeptanzrichtlinien; und Senden von Sicherheits-Alerts für unbefugte Aktivitäten wie Hardware- Entfernung, Deaktivierung der Antivirus- Services und mehr.

Informationen zu wichtigen Features

Leichte Installation
NetSupport DNA ist dafür konzipiert, eine komplette Suite von IT-Verwaltungsfunktionen zu bieten, und zwar ohne die kostspieligen Hardware-Käufe, Implementierungs- und anfänglichen Schulungskosten alternativer Lösungen.

Nach der Installation des Servermoduls (das benutzt wird, um die DNA Datenbank zu verwalten und Informationen hinzuzufügen), erkennt und installiert das Bereitstellungstool automatisch den DNA Agent auf den Ziel-Geräten. Die DNA Konsole (die vom IT-Techniker installiert wird) bietet volle DNA Systemsteuerung mit reichlichen Bildschirminformationen und Echtzeit-Berichterstattung.

Eine typische PC-Evaluierung für 50 Benutzer kann innerhalb von 30 Minuten betriebsbereit gemacht werden. Die Standardversion bietet eine zusätzliche Gateway-Komponente zur Verknüpfung mehrerer Remotestandorte, und SQL Server Express wird ebenfalls mitgeliefert, damit es für die Evaluierung benutzt werden kann. DNA verbindet sich mit Active Directory (einschließlich einmaligem Anmelden) und bietet die Fähigkeit, Abteilungszugriff und administrative Funktionen nach Konsolenbenutzer zu profilieren.

Automatische Geräteerkennung
Erhalten Sie Informationen über alle neuen Geräte, welche dem Netzwerk beigetreten sind und entscheiden Sie ob der Agent automatisch verteilt werden soll.

Sobald NetSupport DNA installiert und optimal auf Ihr Unternehmen eingestellt ist, wird es das Netzwerk ständig überwachen, neue Geräte erkennen, und dann bietet sich die Möglichkeit einer automatischen Verteilung des Agenten für zukünftige Verwaltung.

Hardware-Inventar
NetSupport DNA bietet eines der umfassendsten und detailliertesten Hardware-Inventar- Module im gegenwärtigen Markt. Von jedem Gerät werden vielfältige Informationen gesammelt, von den CPU- und BIOS-Typen zu Netzwerk-, Video- und Speicherinformationen.

Inventarberichte können entweder für einen einzelnen PC, eine gewählte Abteilung, für bedingungsbasierte „Dynamische Gruppen" oder für das gesamte Unternehmen angezeigt werden.

Außerdem gibt es ein Vertragsmodul zur Aufzeichnung der Miet- und Wartungsverträge für Geräte oder Peripheriegeräte einschließlich der Lieferantenangaben, Vertragsablaufdaten und Kosten.

Hardware-Inventar-Aktualisierungen können dafür konfiguriert werden, zu verschiedenen Zeitintervallen im Laufe des Tages oder beim Einschalten zu laufen und können bei Bedarf auch sofort ausgeführt werden. Es steht eine eigenständige Inventarkomponente zur Verfügung, die auf Nicht-Netzwerk- und Mobilgeräten eingesetzt werden kann, und außerdem können hochwertige Peripheriegeräte einem Gerät zugeordnet und erfasst werden.

Effizienzansicht
Das spezielle Dashboard zeigt auf einen Blick, wie die Schultechnologie verwendet wird sowie die Bereiche, in denen die Effizienz verbessert werden kann, um Kosten- und Zeiteinsparungen zu erzielen, indem z.B. angezeigt wird, welche PCs am wenigsten effizient genutzt werden (und somit anders eingesetzt werden können) oder welche Apps am wenigsten verwendet werden (und deshalb nicht weiter abonniert werden müssen).

SNMP Geräteermittlung
Die SNMP Ermittlungansicht ermöglicht es, NetSupport DNA dafür zu konfigurieren, eine Reihe von Netzwerkadressen zu scannen und alle geeigneten ermittelten Geräte zu melden, wie Drucker und Zugriffspunkte. Diese Posten können dann in DNA gespeichert werden, und die Echtzeitdaten (wie Tinte- oder Tonerstand) können von der Konsole aus überwacht werden.

Das SNMP Modul beinhaltet die Auffindung - und dann aktive Überwachung - aller ausgewählten SNMP-Geräte, Tracking -Statistiken und Verlauf für alle Daten auf einem bestimmten Gerät für einen festgelegten Zeitraum, wie z.B. Datenverkehr auf jeder Schnittstelle eines Netzwerk-Switch. Das Modul beinhaltet ebenfalls eine eigene Alertings-komponente, welche Dutzende von anpassbaren Warnungen unterstützt, welche erstellt und ausgelöst werden können, wenn die Daten spezifische Kriterien erfüllt sind. Alerts können automatisch an bestimmte Konsolen Benutzer oder vordefinierte E-Mail- Konten gesendet werden. Benutzerdefinierte Abfrage -basierte Reports und Ansichten können erstellt werden, um alle gesammelten Daten zu widerzuspiegeln.

Software-Inventar und Lizenzierung
Das Software-Modul ist dafür ausgelegt, Schulen beim Management der Lizenzeinhaltung zu helfen, Software-Überschreitungen durch Meldung

der installierten Software zu reduzieren und proaktiv PCs zu identifizieren, deren Software wenig oder gar nicht benutzt wird.

NetSupport DNA kann die Informationen für einen ausgewählten PC, eine Abteilung oder eine benutzerdefinierte Gruppe anzeigen und enthält ein umfassendes Modul zur Zuweisung und Nachverfolgung von Lizenznutzung. Das NetSupport DNA Softwarelizenz-Modul unterstützt das kontinuierliche Management aller Softwarelizenzen für alle Abteilungen und erfasst die Lieferanten, Einkaufs- und Rechnungsdetails, Abteilungs- und Kostenstellenzuweisung und Nachverfolgung der Wartungsverträge.

Eine Dateiüberprüfungsoption kann benutzt werden, um Dateien eines bestimmten Typs zu identifizieren, die lokal auf Geräten installiert sind. Diese kann benutzt werden, um sicherzustellen, dass Dokumente nicht lokal gespeichert sind und bei den Backup-Routinen des Unternehmens ausgelassen werden könnten.

Die hinzugefügte 'Suchfunktion' macht es leichter, die Programme oder Anwendungen zu finden, die Sie suchen, und das Installationsdatum der Hotfixes wird jetzt in einem Gerätesoftware-Inventar angezeigt – was dazu beiträgt, hervorzuheben, welche Geräte Updates erhalten haben.

Software Anwendungs-Metering ***(Version für das Bildungswesen)***
Das Anwendungs-Metering Modul berichtet über alle Anwendungen, die auf jedem PC oder Server benutzt werden, wobei die Zeiten, zu denen die Anwendungen geöffnet und geschlossen wurden, angegeben werden sowie die tatsächliche Zeiten, in denen sie aktiv waren.

Die Überwachung der Anwendungsnutzung gewährleistet, dass die Softwarelizenzen den richtigen Benutzern zugewiesen werden, und nur bei entsprechender Anwendungsaktivität für die Benutzer erneuert werden, was Kostenersparnisse ermöglicht.

Die Anwendungsnutzung kann auch für Benutzer oder Abteilungen entweder ganz oder nur nach Tageszeit eingeschränkt werden. Listen mit genehmigten und eingeschränkten Anwendungen zusammen mit den Zeiten, zu denen die Einschränkungen gelten, können zentral erstellt und durchgesetzt werden.

Zusätzlich zur Beschränkung von Anwendungen nach ihren spezifischen Namen können sie jetzt auch nach ihren Fenstertiteln blockiert oder beschränkt werden, was Technikern hilft, eine breitere Sicherheitsschicht hinzuzufügen und gleichzeitig die Produktivität zu erhalten.

Anwendungs-Metering ermöglicht es dem Unternehmen, die gegenwärtigen Lizenznutzungsraten für alle installierten Anwendungen zu überwachen und zu melden und sicherzustellen, dass die Anwendungsnutzung den Richtlinien des Unternehmens entspricht. Berichte können nach PC oder angemeldetem Benutzer erstellt werden.

Anonymisierten Anwendungs-Metering *(Version für das Unternehmen)*

Das Anonymisierten Anwendungs-Metering Modul berichtet über alle Anwendungen, einschließlich wobei die Zeiten, zu denen die Anwendungen geöffnet und geschlossen wurden, werden sowie die tatsächliche Zeiten, in denen sie aktiv waren.

Listen mit genehmigten und eingeschränkten Anwendungen zusammen mit den Zeiten, zu denen die Einschränkungen gelten, können zentral erstellt und durchgesetzt werden.

Zusätzlich zur Beschränkung von Anwendungen nach ihren spezifischen Namen können sie jetzt auch nach ihren Fenstertiteln blockiert oder beschränkt werden, was Technikern hilft, eine breitere Sicherheitsschicht hinzuzufügen und gleichzeitig die Produktivität zu erhalten.

Anwendungs-Metering ermöglicht es dem Unternehmen, die gegenwärtigen Lizenznutzungsraten für alle installierten Anwendungen zu überwachen und zu melden und sicherzustellen, dass die Anwendungsnutzung den Richtlinien des Unternehmens entspricht.

Internet-Metering

Von Online-Kollaboration und cloudbasierten Lösungen zu den sozialen Medien und mehr besteht ständiger Zugang zum Internet. Um die erfolgreiche Nutzung der Personalzeit und die effektive Nutzung der Unternehmensbandbreite zu gewährleisten und eine sichere Umgebung zu fördern, ist es unerlässlich, dass Unternehmen nicht nur Internet-Sicherheitsrichtlinien haben sondern auch mit die richtigen Tools, um diese durchzusetzen.

Das Internet-Metering-Modul bietet eine detaillierte Zusammenfassung aller Internetaktivitäten für jeden PC nach Benutzern, einschließlich Start- und Beendigungszeiten für jede besuchte URL und die aktive Zeit, die auf dieser Seite verbracht wurde. Die Ergebnisse können entweder nach Aktivität an einem bestimmten Gerät oder nach Benutzer angezeigt werden, egal wo dieser arbeitet. Der Schlüssel zur Unterstützung einer effektiven Richtlinie ist natürlich effektive Kontrolle. Mit NetSupport DNA lässt sich die Internet-Nutzung voll verwalten; es können Listen von genehmigten und eingeschränkten URLs und/oder Teil-URLs auf die

Profile angewendet werden. Wenn die Listen eingesetzt werden, kann NetSupport DNA uneingeschränkten Zugriff auf alle Websites erlauben, beschränkten Zugriff auf bestimmte Websites, die vom Unternehmen als genehmigt markiert worden sind, oder der Zugriff auf bestimmte Websites, die als ungeeignet markiert worden sind, kann blockiert werden.

Zusätzlich zur Beschränkung von Apps und Spielen nach ihren spezifischen Namen können sie jetzt auch nach ihren Fenstertiteln blockiert oder beschränkt werden, was Technikern hilft, eine breitere Sicherheitsschicht hinzuzufügen und gleichzeitig die Produktivität zu erhalten.

Der Zugriff kann auch nach Tageszeit gesteuert werden, beispielsweise um den Zugriff auf genehmigte Gaming oder Social Media Websites nur in der Mittagszeit oder außerhalb der Arbeitszeiten zuzulassen.

Hinweis: Die Funktion steht nur in der NetSupport DNA Version für das Bildungswesen zur Verfügung.

Unternehmen-Alerting
NetSupport DNA bietet ein extrem leistungsstarkes Alerting-Modul, mit dem das System die Operators automatisch benachrichtigen kann, wenn verschiedene Änderungen irgendwo im Unternehmen auftreten. Entsprechend der DNA Philosophy ist das System dafür konzipiert, leicht zu initiieren zu sein, und es kann eine beliebige Anzahl von benutzerdefinierten Alerts hinzugefügt werden.

Es gibt drei Arten von Alert: Server, Konsolen- und PC-Alert. Server-alerts melden Änderungen in den von NetSupport DNA im gesamten Unternehmen gesammelten Daten, einschließlich Alerts für Dinge wie neu hinzugefügte PCs, Änderungen in der Hardware, neu installierte/ entfernte Anwendungen etc. Konsolen-Alerts identifizieren Änderungen im Zusammenhang mit der NetSupport DNA Konsole, z.B. wenn eine DNA Lizenzgrenze überschritten wird, wenn ein Bediener hinzugefügt oder gelöscht wird und wenn ein DNA Update installiert wird. PC-Alerts melden Echtzeitänderungen oder -zustände, die auf einem spezifischen PC auftreten, wie zum Beispiel: CPU Nutzung über XX% für XX Minuten; freier Speicherplatz der auf unter XX% abfällt; Wegfall eines wichtigen Service (z.B. Antivirus Service oder IIS an einem Server), Druckerspooler-Alerts; Sicherheitsalerts (z.B. gescheiterte Anmeldungsversuche); und viele anderen. Als Teil einer SIEM (Sicherheitsinformationen und Vorfallsmanagement) Strategie, kann das

PC-Vorfallprotokoll auch überwacht werden, wobei Alerts für Fehler, Warnungen oder ausgewählte Auditergebnisse ausgelöst werden.

Alert-Benachrichtigungen können an vorgegebene Emailempfänger und/oder aktive Konsolenbenutzer geleitet werden (und zwar pro Alert, so dass die Art des Alerts entscheiden kann, welche Operators zu benachrichtigen sind). Außerdem werden ausstehende Alerts für die entsprechenden PCs in der Hauptunternehmenshierarchie-Strukturansicht identifiziert. Es können Aktionen zu einem PC-Alert hinzugefügt werden, so dass Sie wählen können, was geschieht, wenn ein Alert ausgelöst wird. Die verfügbaren Aktionen sind: Screenshot erfassen, Bildschirm aufzeichnen und Anwendung ausführen. Wenn Alerts identifiziert worden sind, können Bediener Notizen hinzufügen, und PC-Alerts können überprüft und freigegeben werden, oder es kann eine permanente Aufzeichnung von ihnen zur späteren Überprüfung gespeichert werden. Ein voller Verlauf aller PC-Alerts steht über die Verlauf-Funktion zur Verfügung.

Softwareverteilung
NetSupport DNA bietet eine Mehrfachzustellungsoption für Softwareverteilung.

Ein Softwareverteilungspaket wird erstellt, indem man entweder Parameter auf eine Sammlung von Dateien oder Ordnern anwendet oder den DNA App-Objekt-Manager benutzt, der die Eingabeaufforderungen, Tastaturanschläge und Mausklicks aufzeichnet, die während einer Testinstallation benutzt werden, und diese dann in einer Live-Bereitstellung automatisiert, so dass keine Operatoraktionen erforderlich sind.

Wenn das Anwendungspaket erstellt worden ist, kann es mit "Push" zur Bereitstellung automatisch an die Ziel-PCs gesendet oder alternativ „veröffentlicht" werden. Nachdem es veröffentlicht worden ist, können die Benutzer nachsehen, welche Anwendungen auf der Basis ihrer Abteilungszugehörigkeit für ihre PCs zu Verfügung stehen und sie nach Bedarf mit „Pull" herunterladen. NetSupport DNA enthält eine Zeitplanungsfunktkion, die es ermöglicht, Pakete an einem bestimmten Datum zu einer bestimmten Zeit bereitzustellen – normalerweise außerhalb der Hauptbürozeiten, wenn der Netzwerkverkehr am niedrigsten ist.

Bei Remote-Bereitstellungen wird die Erfordernis, Netzwerküberlastung zu minimieren, zur Priorität. In diesem Fall ermöglicht es NetSupport DNA einen Agent PC, am besten lokal zu den Zielgeräten, als Verteilungspunkt

zu nominieren. Nachdem die Software bereitgestellt worden ist, wird sie dann, statt direkt an jeden Remote-PC gesandt zu werden, nur an den designierten PC gesandt, der dann als Relais fungiert und die Software an seine lokalen PCs weiterverteilt.

Energieüberwachung und -verwaltung
Das Energieüberwachungsmodul bietet eine einfache und präzise Zusammenfassung der potentiellen Energieverschwendung in der gesamten Organisation durch Computersysteme, die außerhalb der Geschäftszeiten eingeschaltet bleiben.

NetSupport DNA kontrolliert auf den eingeschalteten Zustand aller Computer, und seine lokale Überwachungskomponente erstellt eine genaue Aufzeichnung aller Zeiten, zu denen ein Computer ein- oder ausgeschaltet oder im Ruhezustand war. Wenn sie alle Tageszeiten weiß, zu denen der Computer in Betrieb war, wird eine Berechnung des durchschnittlichen (und benutzerdefinierbaren) „Stromverbrauchs pro Gerät" ausgeführt, die die Berechnung des Energieverbrauch-Grundwerts für alle Computer erleichtert.

Mit Hilfe dieser Informationen können jetzt Energiemanagement-Richtlinien eingestellt werden. Ausgewählte PCs können dafür eingestellt werden, sich zu einer vorgegebenen Zeit am Ende des Tages automatisch auszuschalten und am nächsten Morgen wieder einzuschalten – und zwar alle zusammen oder gestaffelt. Außerdem können "Inaktivitätsrichtlinien angewendet werden, die es ermöglichen, Regeln dafür anzuwenden, dass Systeme, die eine Zeitlang inaktiv waren, in den Ruhezustand gehen, sich abmelden oder ausschalten.

Endgerätesicherheit
NetSupport DNA bietet eine einfache und effektive Lösung für das Management der USB Memorystickbenutzung, um zur Erhaltung der Sicherheit im Unternehmensnetzwerk beizutragen. Die Benutzung von Memorysticks kann für das ganzeUnternehmen oder für spezifische Abteilungen gesteuert werden, und die Benutzung kann auf vollen Zugriff, allen Zugriff sperren, schreibgeschützten Zugriff oder Ausführen von Anwendungen von unbekannten Memorysticks verhindern eingestellt werden. Alternativ können individuelle Memory-Sticks in NetSupport DNA "autorisiert" werden – für den aktuellen Tag, eine Woche oder unbegrenzt – und der Einsatz von Sticks im Unternehmen kann auf nur solche beschränkt werden, die autorisiert sind.

Ein Programmadministrator kann einen Memorystick an einen lokalen PC anschließen und seine Benutzung dann innerhalb der DNA-Konsole

entweder für eine bestimmte Abteilung oder einen bestimmten Benutzer autorisieren. Benutzer, die einen nicht-autorisierten Memorystick anschließen, können gegebenenfalls auch Remote-Autorisierung beantragen. NetSupport DNA kann nicht nur sowohl Wechsel- (Memorystick) und portable (Handy, Tablet, Kamera) Speichergeräte identifizieren, es bietet auch eine ähnliche Benutzungssteuerung für CD / DVD Geräte (einschließlich USB und virtuell). Außerdem kann es erkennen, ob Volumes auf Festplatten/USB-Laufwerken verschlüsselt sind (BitLocker).

Echtzeitüberwachung
Sie erhalten eine Echtzeitzusammenfassung all Ihrer PCs, wenn Sie Explorer Modus wählen. Ausgewählte PCs können in drei Formaten gezeigt werden – Symbol, Details oder Miniaturansicht – und diese können zu von Ihnen bestimmten Intervallen aktualisiert werden, z.B. alle fünf oder zehn Sekunden etc.

In Miniaturansicht sind die PC Bildschirme (einschließlich mehrfacher Monitore) sichtbar und bieten einen visuellen Überblick der gegenwärtigen Aktivitäten. Die Größe der Miniaturansichten kann je nach Anforderungen des Operators angepasst werden. Für ausgewählte Abteilungen (d.h. Finanzen oder Lehrer) können Datenschutzmodi eingestellt werden, so dass die Miniaturansicht weichgezeichnet ist.

Bei weiterem Drill-down zeigt die Details-Ansicht alle Details des gewählten PCs in einer Liste, in der alle aktiven Benachrichtigungen hervorgehoben sind, so dass es leicht ist, PCs zu identifizieren, die sofortige Aufmerksamkeit erfordern. Diese Ansicht bietet auch eine visuelle Zusammenfassung aller aktiven Richtlinien, die auf die einzelnen PCs angewendet werden.Diese Ansicht bietet eine visuelle Zusammenfassung aller aktiven Richtlinien, die auf jeden PC angewendet werden, sowie der PC-Leistungsdaten wie Realtime-Netzwerkverkehr, CPU und Speicher für jeden PC. Durch Rechtsklick auf einem PC kann ein Operator außerdem schnell PC-spezifische Funktionen starten, wie Strom ein/aus, Chat, Fernwartung, Nachrichten senden und andere. Der Benachrichtigungsfilter kann in allen drei Anzeigemodi benutzt werden, um PCs mit aktiven Benachrichtigungen innerhalb einer gewählten Zeitperiode hervorzuheben.

Für zusätzliche Flexibilität steht Explorer-Modus von der Benutzerstrukturansicht aus zur Verfügung, so dass Techniker die Daten auf Benutzerebene anzeigen können – beispielsweise welches Profil ihnen zugewiesen worden ist.

Techniker können jetzt auch die praktische Spotlight-Funktion benutzen, die ihnen hilft, mehr Details über einen ausgewählten PC auf einen Blick zu sehen (z.B. alle Anwendungen, Dienste, Websites und Prozesse, die in Gebrauch sind).

E-Sicherheit
NetSupport DNA, zusammen mit dem optionalen Klassenzimmer-management-Modul, bietet eine Reihe von Funktionen zur Unterstützung einer schulweiten E-Sicherheitsrichtlinie. In DNA beinhaltet diese sowohl Internet-Überwachung als auch Einschränkungen, die den Zugriff auf ungeeignete Websites verhindern; die Deaktivierung von Webcams auf Klassenzimmergeräten; Kontrolle des Zugriff auf den Inhalt von Memorysticks; Auslösung von Alerts, wenn Zuwiderhandlungen stattfinden – bis zur Durchsetzung von akzeptablen Nutzungsrichtlinien.

Schutz
Die NetSupport DNA Schlüsselwort- und Begriffsüberwachungsfunktion bietet Einsicht in und Alerts von allen Aktivitäten eines Schülers/IN, die darauf hinweisen könnten, dass dieser Aktivitäten nachgeht, durch die er gefährdet werden könnte. Details/Zusammenhang der ausgelösten Wörter können überprüft werden, wobei die Ergebnisse (verfügbar als Protokoll, Screenshot des Bildschirms, Webcam-Bild des Benutzers oder Bildschirmaufzeichnung, je nach Schweregrad und je nachdem, welche dieser Funktionen die Schule aktiviert – Funktionen stehen für zu Hause benutzte Geräte nicht zur Verfügung) bei Bedarf zur Nachverfolgung an einen Kollegen weitergeleitet werden können. Die erfassten Daten werden sicher im Schulnetzwerk (LAN) gespeichert, und es können nur designierte Mitglieder des eSafety-Personals auf die Informationen zugreifen.

Es wird eine ausführliche Erklärung und Definition jedes Schlüsselworts gegeben, um dem Personal zu helfen, die potentielle Gefahr für Schüler zu verstehen; außerdem erstellt der neue, auf Zusammenhangsinformationen basierende Risikoindex einen numerischen Risikoindexwert für jedes Ereignis auf der Basis einer hochentwickelten AI-Zusammenhangsrisikoanalyse. Dies ermöglicht es dem Personal, Ereignisse mit hohem Risiko und gefährdete Schüler leicht anzuzeigen. Das Personal kann auch den weiteren Zusammenhang einer Schüleraktivität aus einer detaillierten Zusammenfassung des Internet- und Anwendungsgebrauchs des Schülers ersehen (die auch gesteuert werden kann), die für jede gewählte Zeitperiode verfügbar ist. Altersgerechte Internetsteuerung kann auch mit Hilfe der Profile hinzugefügt werden. Außerdem können gefährdete Schüler zur

zusätzlichen Unterstützung hervorgehoben und nachverfolgt werden , und für jeden Schüler steht ein 'Verlauf der Anliegen' zur Verfügung.

Die von Azure gehostete eSafety-Cloud-Konsole speichert lokale Daten, um es dem eSafety-Personal zu ermöglichen, ausgelöste eSafety-Schlüsselwörter, neue, auf Zusammenhangsinformationen basierende Risiko-Alerts, von Schülern gemeldete Anliegen und die Wort-Cloud mit Trendthemen auch von unterwegs anzuzeigen. Das neue Cloud-Modul enthält auch eine für Smartphones optimierte Benutzeroberfläche, so dass eSafety-Personal schnell nach einem spezifischen Kind suchen und kürzlich gemeldete Alerts oder Anliegen überprüfen kann.

eSafety muss auch proaktiv sein, und NetSupport DNA ermöglicht Schülern deshalb den Zugriff auf Online-Unterstützungsressourcen - die Themen wie Frauenbeschneidung, Drogenabhängigkeit, Grooming und Mobbing behandeln – die alle vom NetSupport DNA eSafety Symbol auf dem PC des Schülers verfügbar sind. Mit der Anliegen melden Option können Schüler ihre Anliegen auch vertraulich einem Personalmitglied melden, dem sie vertrauen. (Verfügbar über den DNA Agent, der auf Schulgeräten installiert ist, oder außerhalb der Schulzeiten über eine Website.) Schüler teilen ihr Problem mit, indem sie einem Personalmitglied, dem sie vertrauen, eine Nachricht, Screenshots oder Dokumente senden; NetSupport DNA wird das Anliegen und etwaige Notizen nachverfolgen und sogar ein Alert an einen eSafety-Administrator senden, wenn das geplante Personalmitglied nicht innerhalb einer gewissen Zeit geantwortet hat. Anliegen können an ein anderes eSafety-Personalmitglied weiterverwiesen werden, beispielsweise, wenn das erste Personalmitglied Urlaub hat. In Situationen, in denen Lehrern ein Schüleranliegen verbal mitgeteilt wird, können sie dasselbe tun. Sie können das Anliegen über die ‘Anliegen hinzufügen’ Schaltfläche im eSafety-Menüband protokollieren.

Hinweis: Die Funktion steht nur in der NetSupport DNA Version für das Bildungswesen zur Verfügung.

Benutzerverwaltung

NetSupport DNA bietet eine Reihe von Funktionen zur Auffindung und Verwaltung von Benutzern innerhalb einer Netzwerkumgebung. Außer den Hauptbenutzerdaten (Name, Telefon etc) bietet DNA dem Kunden die Fähigkeit, die für jeden Gerätebenutzer zu sammelnden und zu sortierenden Daten anzupassen, einschließlich Nachverfolgung des Benutzerakzeptanzfomulars. DNA erfasst auch einen Änderungsverlauf für

die in Benutzerdaten eingegebenen Daten. Änderungen der Benutzerangaben werden aufgezeichnet, einschließlich der folgenden Felder: Personalnummer, Ort, Bestandskennzeichen und Besitzer.

Aktivitätenüberwachung
NetSupport DNA bietet jetzt eine einzige, zeitbasierte Zusammenfassung aller Aktivitäten eines spezifischen Benutzers, PCs oder einer Abteilung. Diese wird als chronologische Ansicht präsentiert und zeigt den Technikern, wann die Anmeldungssitzung begann und endete, welche Anwendungen benutzt wurden und wann, sowie die Internetnutzung* – über eine eingestellte Zeitspanne hinweg. Aktivitäten können als grafische Zeitskala oder textbasierte Rasteransicht angezeigt werden. Diese zeitsparende Funktion bedeutet, dass Techniker nicht jeden Bereich separat anzusehen brauchen und stattdessen das Gesamtbild der Aktivitäten auf einen Blick an einer Stelle sehen können. Sie kann beispielsweise den Benutzer und den Zeitpunkt zeigen, zu dem eine Anwendung auf einem bestimmten
PC gelöscht wurde.

* Die Funktion steht nur in der NetSupport DNA Version für das Bildungswesen zur Verfügung.

Profile
Um maximale Flexibilität zu bieten und Zeit zu sparen, ermöglicht NetSupport DNA es Ihnen, mehrfache Profile für verschiedene Gruppen von Geräten oder Benutzern zu erstellen (z.B. auf Abteilungsebene), und zwar jede mit ihren eigenen spezifischen Komponenteneinstellungen. Das bedeutet, dedizierte Einstellungen (wie Internet-Zugriff, Druck-Metering und viele andere) können auf spezifische Jahrgruppen angewendet werden, wie beispielsweise Marketing (für Facebook).

Anmeldungssteuerung
Es kann nicht nur verhindert werden, dass Personalmitglieder sich an mehreren Geräten anmelden, bei Bedarf kann ein Benutzer auch autorisiert werden, sich an mehreren PCs anzumelden (zwischen 1 und 5). Dies ist eine nützliche Funktion für Roaming-Personal oder -Techniker, die mehrere Geräte haben können.

Einen Benutzer finden
NetSupport DNA ermöglicht es jedem Benutzer, auf dessen Gerät DNA Agent installiert ist, einen anderen angemeldeten Benutzer zu suchen und ihm eine Nachricht zu senden (wenn diese Funktion aktiviert ist). Dies kann für Personalmitglieder nützlich sein, bei denen die NetSupport DNA

Konsole nicht installiert ist, die aber andere Benutzer im Unternehmen finden und kontaktieren müssen.

Lesezeichen
NetSupport DNA ermöglicht es Ihnen, Lesezeichen in den PC-, Benutzer- und Geräte-Strukturansichten zu erstellen und zu positionieren. Diese können bei größeren oder komplexen Strukturansichten nützlich sein, da sie es Ihnen ermöglichen, schnell an die Stelle zu navigieren, an der Sie arbeiten möchten.

Tresor
NetSupport DNA bietet eine Tresor-Komponente, die die sichere Speicherung von Seriennummern, Passwörtern und anderen vertraulichen IT-Daten ermöglicht. Der Zugriff auf den Tresor kann auf bestimmte Konsolenbenutzer beschränkt werden, und Aktivitäten können im zentralen DNA Audit-Trail aufgezeichnet werden.

System-Audit
NetSupport DNA enthält eine leistungsstarke Audit-Komponente, um alle gewählten Konsolenaktivitäten des Personals nachzuverfolgen. Die Audit-Funktion zeichnet Änderungen der Richtlinien und Einstellungen auf, wann Eingaben hinzugefügt / gelöscht worden sind, oder wo die Berechtigungen für einen Benutzer geändert worden sind.

Benutzerdefinierte Bilder
Um Elemente in der Hierarchiestrukturansicht stärker hervorzuheben, können Sie benutzerdefinierte Bilder auf Abteilungen, Dynamische Gruppen, PCs und Benutzer anwenden.

Zu den weiteren Tools zählen Echtzeit-Chat und Messaging innerhalb des Unternehmens, eine Echtzeit-Systemstatus-Anzeige für alle Geräte sowie eine Anzahl von Systemadministrationsfunktionen.

Durchsetzung der Acceptable Use Policies
Acceptable Use Policies (AUP) bilden einen festen Bestandteil der Schlüsselinformationen-Sicherheitsrichtlinien, die von den meisten Organisationen eingesetzt werden, und es ist ganz normal, dass neue Personalmitglieder eine AUP unterschreiben, bevor sie die Ressourcen der Gesellschaft zum ersten Mal benutzen, oder dass sie bestätigen, dass sie etwaige Änderungen solch einer Richtlinie gelesen haben, wenn diese aktualisiert wird.

NetSupport DNA bietet ein flexibles Modul zur Unterstützung der Zustellung und Nachverfolgung von AUPs im gesamten Unternehmen.

Richtlinien können auf spezifische Geräte oder Benutzer angewandt und jedes Mal angezeigt werden, wenn ein Benutzer sich anmeldet, oder sie können einmalig angezeigt und bestätigt werden. Es ist möglich, mehrere Richtlinien zu erstellen, was es erlaubt, dass eine Richtlinie ausgewählten Benutzern nur einmal angezeigt wird (zum Beispiel Lehrern), während eine andere Richtlinie anderen Benutzern jedes Mal angezeigt wird (zum Beispiel Schülern). Außerdem werden volle Nachverfolgung und Ausnahmenmeldung geboten.

Druckerüberwachung
NetSupport DNA enthält eine Druckerüberwachungsfunktion auf hoher Ebene. Individuelle Drucker im ganzen Unternehmen werden automatisch identifiziert und die Kosten für das Drucken (Schwarzweiß, Farbe usw.) können von der zentralen Konsolenansicht aus entweder global oder für jeden einzelnen Drucker zugewiesen werden. Falls erforderlich, können Drucker auch aus der Ansicht ausgelassen werden. NetSupport DNA bietet einen vollen Überblick der Druckeraktivitäten und angezeigten Kosten für das gesamte Unternehmen.

Organisationsberichte
NetSupport DNA bietet sowohl Bildschirm- als auf für den Ausdruck optimierte Berichte. Die Bildschirmberichte/ansichten enthalten unterstützende Balken- und Kreisdiagramme sowie "live" Drilldown-Funktionen für alle wichtigen Zusammenfassungsdaten. Außer den Berichten über einzelne Geräte, Benutzer und Abteilungen bietet NetSupport DNA auch dynamische Gruppen. Diese sind benutzerdefiniert und werden zur Hauptgesellschaftsstruktur hinzugefügt. Eine dynamische Gruppe könnte zum Bespiel identifizieren, welche PCs aufrüstbar sind, und solch eine Gruppe würde automatisch aus denen erstellt, die die geforderten Kriterien erfüllen – wie "alle PCs mit mehr als 'XX' Gb Ram, 'XX' Gb freiem Speicherplatz und XX Prozessor-Typ" und so weiter. Druckoptimierte Berichte sind für Managementberichterstattung gedacht und können zu einem geplanten Zeitpunkt erstellt und automatisch an spezifische Dateispeicherorte ausgegeben werden. Alle Berichte bieten Optionen für Drucken oder Export an PDF, DOC und XLS.

NetSupport unterstützt auch benutzerdefinierte Ansichten für alle Daten; das Abfrage-Tool bietet Benutzern eine einfache Schnittstelle zur Einstellung der benutzerdefinierten Ansichten. Das Abfrage-Tool benutzt eine einfache Drag & Drop Feldauswahl, die von Bedingungen und summenbasierten Funktionen unterstützt wird.

Mobilinventar
Diese Inventar App steht als unterstützendes Tool für NetSupport DNA zur Verfügung und kann kostenlos von Google Play und Apple App Stores heruntergeladen werden. Die DNA Mobil-App ermöglicht es Technikern, wenn sie nicht an ihrem Schreibtisch sind, ein detailliertes Hardware- und Software-Inventar für jeden PC im Unternehmensnetzwerk zu suchen und zu betrachten. Die Mobil-App bietet auch einen QR-Code-Scanner, um jeden PC augenblicklich identifizieren zu können, und zwar entweder mit dem von DNA auf dem Bildschirm angezeigten QR-Code oder mit dem am Gerät angebrachten Aufkleber. Außerdem hat NetSupport DNA eine QR-Code-Aufklebererstellungsfunktion einschließlich Anzeige der benutzerdefinierten Einzelheiten. Die App zeigt auch den Verlauf aller Hardware-Änderungen sowie der Software-Installationen und -Entfernungen.

Zusätzlich zu den Inventar- und Verlaufansichten zeigt die NetSupport DNA Mobil-App alle neuen PC Alerts, die im gesamten Netzwerk ausgelöst worden sind. Die App bietet auch eine Option zum Starten einer Remotesteuerungssitzung auf einem beliebigen gewählten PC direkt vom Smartphone oder Tablet aus – ideal sowohl für Remotesupport als auch für schnellen Zugriff auf den eigenen Desktop PC des Technikers.

Remotesteuerung
NetSupport DNA (Bildungswesen-Edition) bietet in der Standardversion leistungsstarke Fernwartungs- und Überwachungsfunktionen. Die Komponente enthält alles von Bildschirm anzeigen zu Dateiübertragung und mehr. Um die Remoteverwaltung von Geräten noch weiter zu unterstützen, können Schultechniker PowerShell- und Remotebefehl-Eingabeaufforderungssitzungen starten, die Registrierung eines Remote-PC bearbeiten und Remote-Geräte an-/abmelden.

Um zentrale IT-Unterstützung in Umgebungen mit mehreren Standorten zu erleichtern, ermöglicht Ihnen die integrierte DNA Gateway-Komponente nahtlose und sichere Fernwartung von Agent Geräten, egal an welchem Standort sich diese befinden.

Benutzer der Unternehmensversion haben die Option, eine Kopie von NetSupports preisgekrönter Fernwartungslösung NetSupport Manager zu integrieren, die Zugriff auf Arbeitsstationen und Server in Ihrem gesamten Unternehmen bietet, sowohl vor Ort als auch remote von unterwegs oder von einem Mobilgerät.

Klassenzimmermanagement (optional)
NetSupport wird in aller Welt als führend in Klassenzimmermanagement- und Orchestrierungssoftware anerkannt. NetSupport School ist eine preisgekrönte Klassenzimmerlösung, die eine komplette Auswahl von Überwachungs-, Prüfungs-, Kollaborations- und Orchestrierungstools für jede Klassenzimmerumgebung bietet.

NetSupport School hilft Lehrern und Ausbildern, die Effizienz des ICT-Unterrichts mit einer Suite abgestimmter Funktionen zu verbessern, die mit Lehrern für Lehrer entwickelt wurde. Lehrer und ihre Assistenten können Schüler zentral auf deren eigenen Geräten unterweisen; durch Überwachung und Steuerung der Nutzung von Apps, Websites, Drucken und mehr dazu beitragen, die Konzentration der Schüler aufrecht zu erhalten; das Lernen der Schüler durch den Einsatz digitaler Journale unterstützen; die einzigartige Schüler-Symbolleiste benutzen, um die Unterrichtsziele und erwarteten Ergebnisse anzuzeigen; und mit einem einzigartigen Frage-und-Antwort-Modul gezielte Teilnehmerbewertungen zu liefern, sowie Umfragen und vorbereitete Prüfungen auszuführen.

Außerdem bietet NetSupport School eine Überwachungs-App für Lehrerassistenten für den Einsatz im Klassenzimmer.

ServiceDesk (optional)
NetSupport ServiceDesk ist dafür konzipiert, mit NetSupport DNA integriert oder als eigenständige Lösung eingesetzt zu werden, und erfüllt alle Erwartungen als voll funktionierendes ITIL-kompatibles IT Service Management (ITSM) Tool, das die Hauptbereiche des ITIL's Best Practice Framework unterstützt – Vorfall, Problem, Änderung und Servicelevel-Management. Wenn es mit NetSupport DNA und unserer Remotezugriff-Lösung NetSupport Manager benutzt wird, haben die Support-Teams ein komplettes Netzwerkmanagement-Toolkit.

NetSupport ServiceDesk ist für jeden Benutzer vom Desktop oder Mobilgerät aus über einen Webbrowser zugänglich und ermöglicht die Anpassung vieler Hauptfunktionen innerhalb der Lösung. Von der Operatorfunktionalität zur Erstellung von spezifischen Dateneingabefeldern kann es so angepasst werden, dass es nahtlos in Ihre Organisation passt.

Leistungsstarke und anpassbare Workflowregeln tragen zur Gewährleistung eines effizienten und pünktlichen Service bei, gemäß den vereinbarten Servicelevels; automatisierte Emailverarbeitung ermöglicht weitere Zeitersparnis, und mit NetSupport ServiceDesks

kundenfreundlichem Self-Service-Portal können Benutzer nach Antworten suchen, bevor sie Support beantragen.

DNA Paket

Für völlige Flexibilität und ein gutes Preis-Leistungs-Verhältnis können Sie NetSupport DNA in modularen Paketen kaufen, entweder als unabhängige Lösung oder in Kombination mit einer unserer ergänzenden Unternehmens- oder Bildungswesenlösungen:

Paket A
NetSupport DNA (alle Komponenten im Standardpaket)

Paket B *(Bildungswesen)*
NetSupport DNA plus NetSupport School

Für weitere Informationen über NetSupport School besuchen Sie bitte www.netsupportschool.com.

Paket C *(Unternehmen)*
NetSupport DNA plus NetSupport Manager.

Für weitere Informationen über NetSupport Manager besuchen Sie bitte www.netsupportmanager.com.

INSTALLATION

Systemanforderungen

NetSupport DNA Server

Hardware-Mindestanforderungen: Single – Dual Core 2.00 GHz CPU 8 Gb RAM oder höher.*

Erforderlicher freier Speicherplatz: 20 Gb (je nach Größe des Unternehmens).

Windows Server 2008 R2 oder darüber (beste Praxis).
Windows 7, Windows 8.1 und Windows 10.

Unterstützte Datenbanken: SQL Server 2008 oder später. Wenn auf dem Zielsystem keine Version von SQL installiert ist, werden Sie, wenn der DNA Server installiert wird, aufgefordert SQL Express (SQL Express 2012 ist in der NetSupport DNA Setup-Datei enthalten) zu installieren oder einen Remote SQL Server anzugeben.

*Auf der installierten Agentbasis beruhende Empfehlungen finden Sie auf unserer Website unter www.netsupportsoftware.com/support.

Optionale Servermodule (SNMP Ermittlung, Remote-Gateways, Webserver)
Windows 7 oder höher.
Windows Server 2008 oder höher.

NetSupport DNA Cloud Server
Windows 10.
Windows Server 2008 R2 oder darüber.

NetSupport DNA Management-Konsole
Erforderlicher freier Speicherplatz: 392 MB
Windows 7 oder höher.
Windows Server 2008 R2 oder höher.

NetSupport DNA Mobilkonsolen-Apps
Android 4.03 oder höher.
iOS 9.3 oder höher.

NetSupport DNA Agent (Client)
Erforderlicher freier Speicherplatz: 105 MB
Windows Vista oder höher.

Windows Server 2008 oder höher.
Mac OS X 10.8 oder höher.
iOS 9.3 oder höher.
Chrome OS.
Android 5.01 oder höher.

Hinweis: Terminalserver-Umgebungen werden nur für die folgenden Komponenten unterstützt: Anwendungs-Metering, Acceptable Use Policies, Benutzerdetails, Druckerüberwachung, Internet-Metering und eSafety.

Zusätzliche "nur Inventar" Agents
Windows XP SP3.
Windows Mobile 8 oder höher.

Planen einer Installation

Bevor Sie mit der Installation beginnen, müssen Sie sich überlegen, welche Komponenten benötigt werden. NetSupport DNA besteht aus sechs Hauptkomponenten:

1. NetSupport DNA Server
2. NetSupport DNA SNMP-Server
3. NetSupport DNA Webserver
4. NetSupport DNA Konsole
5. NetSupport DNA Agent
6. NetSupport DNA Application Packager
7. NetSupport DNA Lokales Gateway
8. NetSupport DNA Remote-Gateway

NetSupport DNA Server
Der Computer, auf dem die Server-Software installiert ist und die Datenbank gespeichert wird, wird als NetSupport DNA Server bezeichnet.

Es muss ein zusätzlicher SQL Server installiert werden, damit der NetSupport DNA Server seine Datenbank betreiben kann. Der SQL Server arbeitet mit dem NetSupport DNA Server zusammen, indem er die Daten, die die DNA Datenbank sammelt, effektiv speichert und bei Bedarf abruft. NetSupport DNA kommt mit einem verfügbaren SQL Server, der automatisch installiert werden kann. Alternativ können Sie einen vorhandenen SQL Server benutzen, indem Sie die Anmeldungsdetails des Servers eingeben. Der SQL Server kann entweder auf demselben Computer ausgeführt werden wie der NetSupport DNA Server oder auf einem anderen Computer im Netzwerk.

Hinweis: Weitere Informationen finden Sie unter **SQL Server-Installation**.

NetSupport DNA SNMP-Server
Der SNMP-Server ist die Komponente, die es Ihnen ermöglicht, die SNMP-aktivierten Geräte zu überwachen und zu konfigurieren. Der SNMP-Server benötigt direkten Netzwerkzugriff auf die SNMP-Geräte. Sie müssen den DNS Namen oder die IP-Adresse Ihres NetSupport DNA Servers eingeben.

Hinweis: Sie können das Gateway benutzen, um mit den Geräten zu kommunizieren.

NetSupport DNA Webserver
Der Webserver wird auf einem Windows Gerät installiert. Dies ermöglicht es der NetSupport DNA Mobil-App, sich mit NetSupport DNA zu verbinden.

NetSupport DNA Konsole
Die Konsole ist die Hauptschnittstelle zur Ausführung von Befehlen und wird im Allgemeinen auf dem Computer eines Administrators installiert. Ein Administrator führt einen Befehl aus und die gesammelten Daten werden aus der DNA-Datenbank extrahiert, die sich im Server befindet. Konsolenbenutzer erhalten Administratorrechte. Bei der Installation wird zur Erstellung einer ersten Anmeldung durch einen Konsolenbenutzer aufgefordert, aber je nach Bedarf lassen sich auch zusätzliche Konsolenbenutzer hinzufügen.

Hinweise:
- Die Konsole kann auf mehreren Computern installiert warden.
- In der NetSupport DNA Version für das Bildungswesen steht eine Konsole auf Cloud-Basis zur Verfügung, die es Konsolenbedienern ermöglicht, Daten in einem Browser anzuzeigen, auch wenn sie nicht in der Nähe der DNA-Hauptkonsole arbeiten.

NetSupport DNA Agent (Client)
Der Agent ist der Endbenutzercomputer, auf dem Daten gesammelt werden.

NetSupoprt DNA Application Packager
NetSupport DNA bietet auch die Option, den Application Packager zu installieren. Der DNA Application Packager ergänzt die Softwareverteilungsfunktion und ist ein Programm, mit dem sich Produktinstaller von "niedriger Komplexität" aufzeichnen und

wieder abspielen lassen.

NetSupport DNA Lokales Gateway (Server)
Über das NetSupport DNA Gateway können Remote-Agents mit dem NetSupport DNA Server verbunden werden. Das Local Gateway kommuniziert mit dem zentralen NetSupport DNA Server. Das Local Gateway muss separat von den anderen NetSupport DNA Komponenten installiert werden.

Hinweis: Wenn das DNA Server Gateway auf demselben Gerät installiert ist wie ein NetSupport Konnektivitätsserver (NCS), steht die Fernwartungsfunktion über das DNA Gateway nicht zur Verfügung. (Gilt nur für Installationen für das Bildungswesen.)

NetSupport DNA Remote-Gateway (Agent)
Das Remote-Gateway fungiert als Proxyserver für die NetSupport DNA Remote-Agents und ermöglicht ihnen die Kommunikation mit dem NetSupport DNA Server. Das Remote-Gateway kann nur mit dem NetSupport DNA Agent installiert werden.

Hinweise:

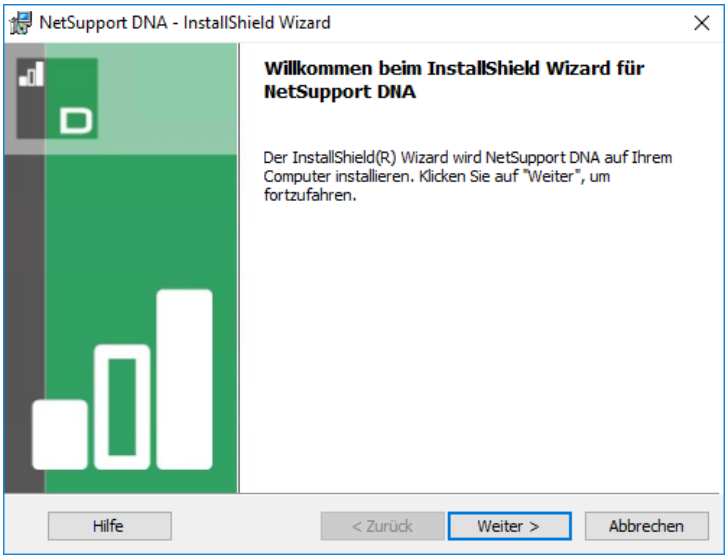
- Es können mehrere Remote-Gateways installiert werden (an jedem Remote-Standort eins), aber nur ein Local (zentrales) Gateway.
- Die NetSupport DNA Konsole muss in demselben Netzwerk sein wie der NetSupport DNA Server, um Gateway Agents erkennen zu können.
- Es wird empfohlen, DNA Server, Remote-Gateway- und Lokales Gateway-Komponenten auf Rechnern mit lösbaren DNS-Namen zu installieren und während der gesamten Konfiguration von Agents und Konsolen DNS-Namen zu verwenden. Wenn das nicht möglich ist, wird stark empfohlen, allen Rechnern, auf denen DNA Lokales-, Remote-Gateway- oder Gateway Server-Komponenten ausgeführt werden, feste IP-Adressen zuzuweisen.

Starten der Installation

Können Sie Ihre Kopie von NetSupport DNA von www.netsupportdna.com/downloads.asp herunterladen.

Klicken Sie im Menü auf die gewünschte Sprache und wählen Sie die Installationsoption für NetSupport DNA.

Die Installation von NetSupport DNA beginnt mit Einblenden eines Begrüßungsbildschirms.



Klicken Sie zur Fortsetzung auf **Weiter**.

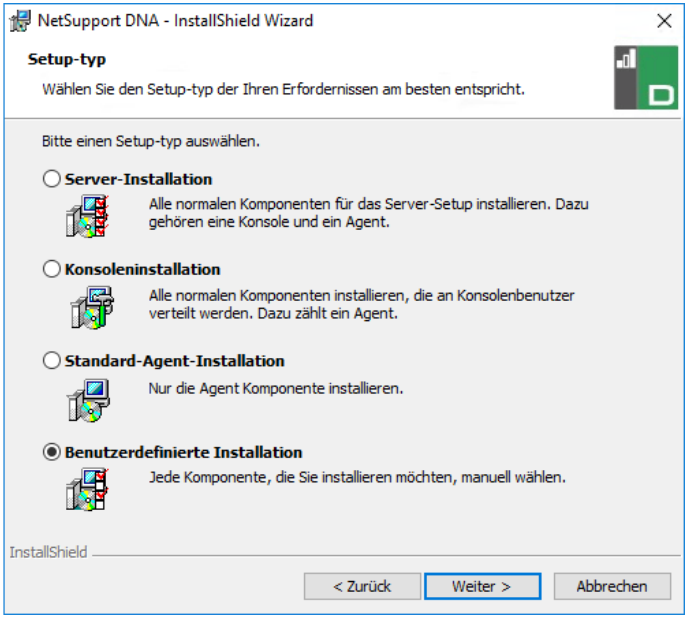
NetSupport-Lizenzvertrag

Der NetSupport-Lizenzvertrag wird eingeblendet. Lesen Sie den Lizenzvertrag sorgfältig durch, wählen Sie "Ich akzeptiere die Bedingungen des Lizenzvertrags" und klicken Sie zur Fortsetzung auf "Weiter".

Wenn Sie den Lizenzvertrag nicht akzeptieren (Ich akzeptiere die Bedingungen des Lizenzvertrags nicht) klicken Sie auf **Abbrechen**. NetSupport DNA wird nicht installiert und Sie erhalten Anweisungen, wie Sie das Installationsprogramm verlassen können.

Setuptyp auswählen

Wählen Sie den Setuptyp zur Installation auf der Arbeitsstation.



Serverinstallation
Installiert die NetSupport DNA Server-, Konsolen- und Agent-Komponenten.

Konsoleninstallation
Installiert die DNA Konsolen- und Agent-Komponenten.

Standard Agent (Client) Installation
Installiert nur die Agent-Komponente.

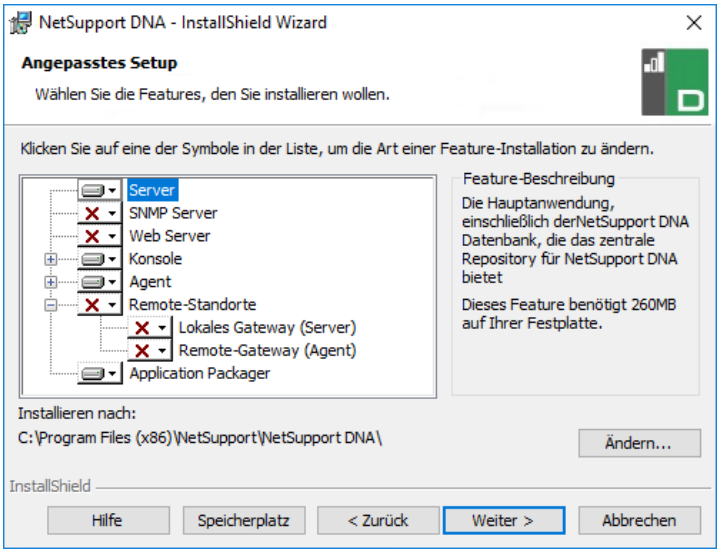
Benutzerdefinierte Installation
Ermöglicht es Ihnen zu wählen, welche Komponenten auf der Arbeitsstation installiert werden sollen.

Klicken Sie auf **Weiter**.

Benutzerdefiniertes Setup

Beschließen Sie, welche Features/Komponenten von DNA Sie installieren möchten.

Hinweis: Diese Bildschirmanzeige erscheint nur, wenn Sie im Setup-Typ Dialog **Benutzerdefinierte Installation** gewählt haben.



Server

Den Rechner, auf dem die Serversoftware installiert und die Datenbank gespeichert ist, nennt man den DNA Server.

Es ist ein verfügbarer SQL basierter Server zur Installation der DNA-Datenbank erforderlich. Der Server liefert die gesamte Funktionalität von NetSupport DNA. Er enthält die Repositories, in denen sämtliche gesammelten Daten gespeichert sind.

SNMP-Server

Der SNMP-Server ermöglicht es Ihnen, SNMP-aktivierte Geräte zu überwachen und zu konfigurieren.

Hinweis: Wenn Sie eine Nur-SNMP-Server-Installation ausführen, müssen Sie den Ort des NetSupport DNA Servers oder Remote-Gateway eingeben.

Webserver
Der Webserver wird auf einem Windows Gerät installiert. Dies ermöglicht es der NetSupport DNA Mobil-App, sich mit NetSupport DNA zu verbinden.

Es muss ein SQL-basierter Server zur Verfügung stehen, der die NetSupport DNA Datenbank enthält.

Agent (Client)
Die Agentkomponente muss auf Endbenutzerrechnern in Ihrem ganzen Netzwerk installiert werden. Der Server fragt Agentcomputer in regelmäßigen Abständen ab und sammelt und speichert Systeminformationen in der DNA-Datenbank.

Wenn Sie nur den Agent installieren, müssen Sie den Speicherort des Servers, der zur Verbindung mit Agents verwendet wird, eingeben.

Hinweis: NetSupport DNA beinhaltet ein Discovery- und Deploy-Tool. Dieses ist eine praktische Funktion zur entfernten Verteilung von DNA Agents an Windows PCs.

Interneteinschränkungen
Ermöglicht es Ihnen, die Internetblockierungsfunktion zu benutzen. Diese ist als Standard enthalten, wenn die Agent Komponente installiert wird.

Konsole
Die DNA Konsole ist das Hauptprogramm zur Ausführung von Befehlen. Sie fungiert als Benutzerschnittstelle. Ein Administrator führt einen Befehl aus und die gesammelten Daten werden aus der DNA-Datenbank, die sich im Server befindet, extrahiert.

Remote-Standorte
Lokales Gateway (Server)
Über das NetSupport DNA Gateway können Remote-Agents mit dem NetSupport DNA Server verbunden werden. Das Local Gateway kommuniziert mit dem zentralen NetSupport DNA Server. Das Local Gateway muss separat von den anderen NetSupport DNA Komponenten installiert werden.

Hinweis: Wenn das DNA Server Gateway auf demselben Gerät installiert ist wie ein NetSupport Konnektivitätsserver (NCS), steht die Fernwartungsfunktion über das DNA Gateway nicht zur Verfügung. (Gilt nur für Installationen für das Bildungswesen.)

Remote-Gateway (Agent)
Das Remote-Gateway fungiert als Proxyserver für die NetSupport DNA Remote-Agents und ermöglicht ihnen die Kommunikation mit dem NetSupport DNA Server. Das Remote-Gateway kann nur mit dem NetSupport DNA Agent installiert werden.

Hinweise:
- Es können mehrere Remote-Gateways installiert werden (an jedem Remote-Standort eins), aber nur ein Local (zentrales) Gateway.
- Die NetSupport DNA Konsole muss in demselben Netzwerk sein wie der NetSupport DNA Server, um Gateway Agents erkennen zu können.

Anwendungs-Packager
Der DNA Anwendungs-Packager ergänzt die Softwareverteilungsfunktion und ist ein Programm, mit dem sich Produktinstaller von "niedriger Komplexität" aufzeichnen und wieder abspielen lassen.

Die Installation von NetSupport DNA erfolgt standardmäßig in Ordner: C:\Programme\NetSupport \NetSupport DNA. Um in einem anderen Ordner zu installieren, klicken Sie auf **Ändern**. Um zu überprüfen, wie viel Speicherplatz für die Installation benötigt wird und den verfügbaren Speicherplatz zu betrachten, klicken Sie auf **Platz**.

Klicken Sie auf **Weiter**.

SQL Server Installation

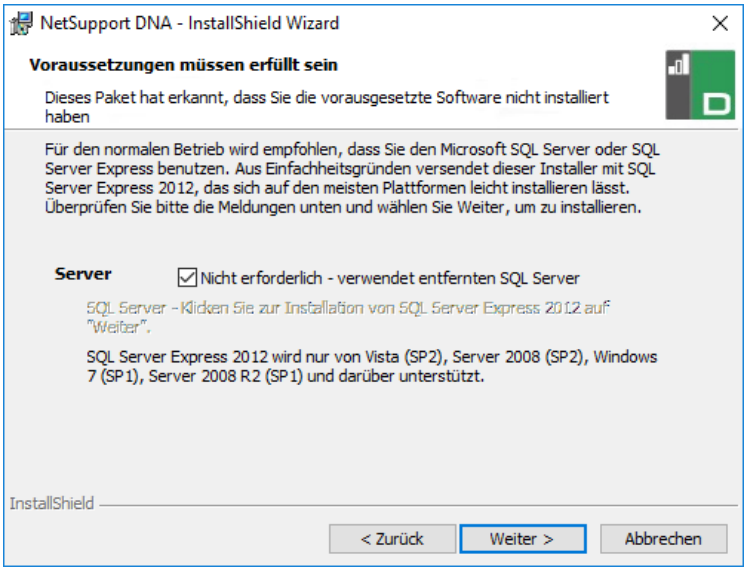
Der SQL Server, den Sie für die NetSupport DNA Datenbank benutzen wollen, kann entweder auf demselben Computer installiert werden wie der NetSupport DNA Server oder auf einem Remotecomputer.

Für unterstützte Betriebssysteme kann der NetSupport DNA Installer auf Wunsch Microsoft SQL Server Express 2012 im Zuge des Installationsprozesses installieren und konfigurieren.

Hinweis: Wenn Sie einen entfernten SQL Server benutzen, klicken Sie bitte hier für weitere Informationen darüber, wie Microsoft SQL Server Express für den Einsatz mit NetSupport DNA zu konfigurieren ist.

Wählen Sie **Weiter,** um einen Microsoft SQL Server zu installieren und zu konfigurieren.

Hinweis: Wenn Sie wählen, SQL Server Express 2012 innerhalb von NetSupport DNA zu installieren, werden Sie an die Konsolenbenutzer-Setup-Anzeige geleitet.

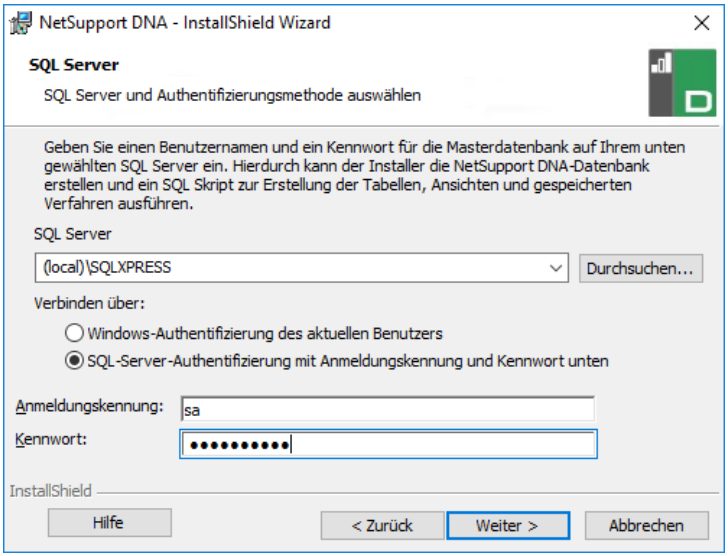


Einrichtung von Server

Wählen Sie den SQL Server für die Installation aus der Dropdownliste oder klicken Sie auf "Durchsuchen", um eine vollständige Liste aller SQL Server einzublenden.

Wählen Sie die angemessene Überprüfungsmethode, SQL oder Windows. Bei SQL müssen Sie den Benutzernamen und das Kennwort Ihrer Master-Datenbank eingeben.

Hinweis: Dieser Dialog erscheint nur, wenn die Server-Funktion installliert wird und Sie einen entfernten SQL Server benutzen.



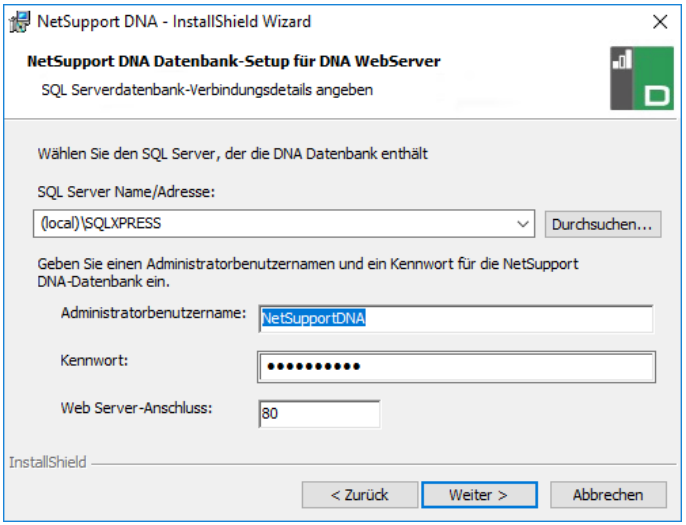
Klicken Sie auf **Weiter**.

Datenbanksetup des Webservers

Der DNA Webserver erfordert die Adresse des SQL-Servers, der die DNA-Datenbank von NetSupport enthält. Sie müssen ferner den Benutzernamen und das Kennwort, die vom NetSupport DNA-Server zur Verbindung mit der Datenbank verwendet werden, angeben.

Sie können auch den Anschluss, den der Webserver nach Verbindungen abfragt, konfigurieren. Standardmäßig ist diese Anschlusseinstellung Port 80. Wenn Sie die Anschlussnummer mit dem Webserver ersetzen, müssen Sie sicherstellen, dass dieser bei der Anmeldung in der mobilen Konsole zum Ende der Serveradresse hinzugefügt wird.

Hinweis: Diese Bildschirmanzeige erscheint nur, wenn Sie den Webserver installieren.

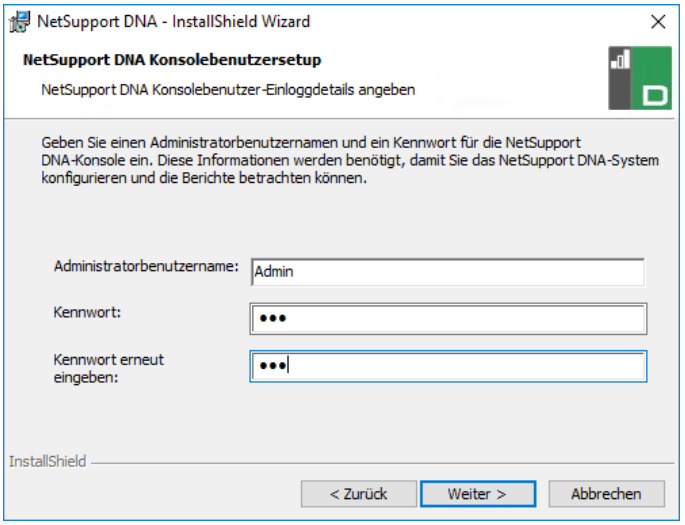


Hinweis: Wenn Sie den Benutzernamen oder das Kennwort nicht kennen, führen Sie auf dem Rechner, auf dem der NetSupport DNA-Server installiert ist, den DNADB-Assistenten aus. Sie können den Benutzernamen und das Kennwort ändern und die neuen Angaben im Installer-Dialogfeld eingeben. Zum Vornehmen dieser Änderung benötigen Sie den Benutzernamen und das Kennwort für den Administrator des SQL-Servers.

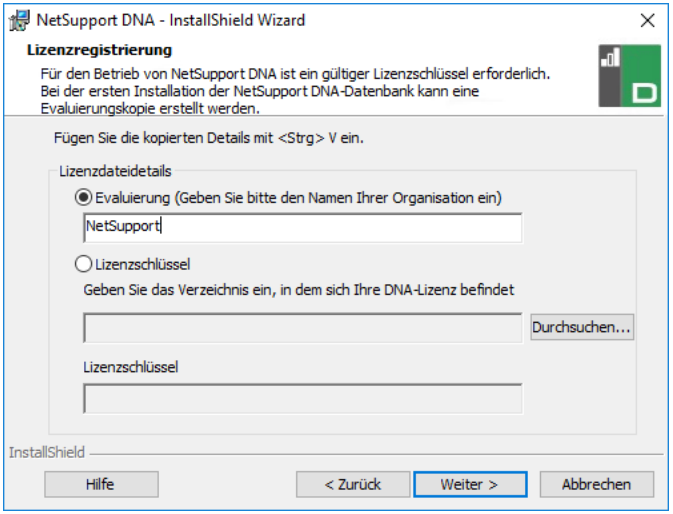
Geben Sie einen Benutzernamen und ein Kennwort für die DNA-Datenbank ein und klicken Sie auf **Weiter**.

Hinweis: Dieses Dialogfeld wird nur bei Installation eines Server Feature eingeblendet.

Geben Sie den Anmeldenamen und das Kennwort ein, die nach installation der DNA-Konsole für den Zugriff auf diese verwendet werden sollen. Zusätzliche Anmeldungen für Konsolebediener lassen sich nach der Installation erstellen.



Wählen Sie Testversion und geben Sie den Namen Ihrer Organisation ein oder die Lizenzangaben, die Sie erhalten haben. Sie müssen in das Verzeichnis gehen, in dem Sie die DNA-Lizenzdatei gespeichert haben, und die Lizenzschlüsselnummer eingeben. Bei der Lizenznummer wird die Groß-/Kleinschreibung berücksichtigt. Die standardmäßige Evaluierungslizenz für NetSupport DNA ist 30 Tage lang gültig und gestattet maximal 50 Benutzer.



Hinweis: Wenn Sie eine vorhandene Installation aktualisieren, erhalten Sie nur die Option zur Eingabe der Lizenzschlüsseldetails. Wenn Sie vorher eine Evaluierungslizenz verwendet haben und die Evaluierung fortsetzen möchten, müssen Sie die Software vor Installation der aktualisierten Version manuell deinstallieren. Bevor Sie mit dem Aktualisieren fortfahren, wird empfohlen, dass Sie eine Sicherheitskopie Ihrer Datenbank erstellen (vollständige Anweisungen hierzu finden Sie auf unserer Website unter www.netsupportsoftware.com/support).

Klicken Sie auf **Weiter**.

Wenn Sie die NetSupport DNA Konsole, Agent, SNMP Server oder das Lokale Gateway installieren, werden Sie aufgefordert, den DNS Namen oder die IP-Adresse für den NetSupport DNA Server einzugeben.

Hinweis: Wenn der DNS-Name oder die IP-Adresse nicht auffindbar sind, lässt sich die Installation nicht fortsetzen.

Wenn Sie die Remotegateway installieren, müssen Sie den DNS Namen oder die IP-Adresse für das Lokale Gateway eingeben. Bei Installation des DNA Servers haben Sie ebenfalls die Möglichkeit, diese Informationen einzugeben.

Klicken Sie auf **Weiter**.

Unternehmenstyp wählen

NetSupport DNA ist in zwei Versionen verfügbar: Unternehmen und Bildungswesen. Jede Version bietet eine Vielfalt von Komponenten, die auf den betreffenden Sektor zugeschnitten sind. Unternehmen und Bildungsinstitute profitieren gleichermaßen von der Flexibilität der Produktangebote – egal, ob Sie sich auf die Verwaltung mehrfacher Benutzer in der gesamten Organisation (Software-Verteilung, Alerting und Lizenzverwaltung) konzentrieren möchten oder darauf, auf dem gesamten Campus Kostenersparnisse zu erzielen (Drucküberwachung, Energieüberwachung und Energiemanagement).

Wählen Sie Ihren Unternehmenstyp und klicken Sie auf **Weiter**.

Es wurden genügend Informationen für den Beginn der Installation geliefert. Wenn Sie die Einstellungen überprüfen möchten, klicken Sie auf **Zurück**, oder sonst klicken Sie auf **Installieren**. Um die Installation zu beenden, klicken Sie auf **Abbrechen**.

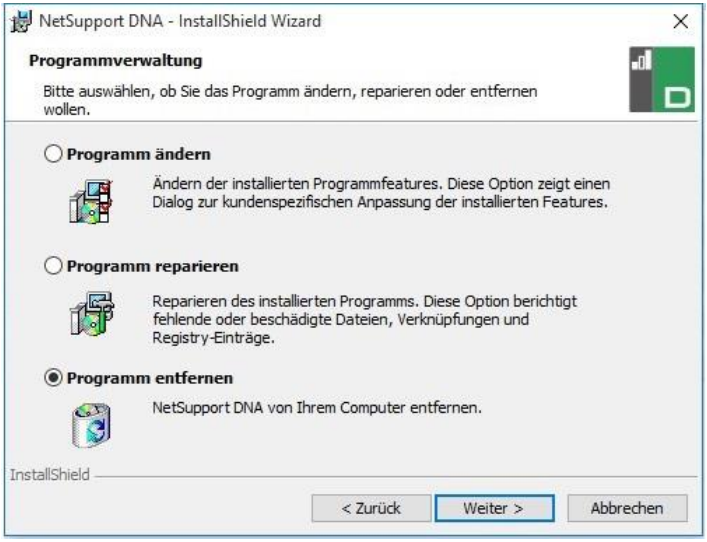
Auf dem letzten Bildschirm wird bestätigt, dass die Installation erfolgreich war. Wenn Sie die DNA Konsole installiert haben, erhalten Sie die Möglichkeit, diese zu starten.

Hinweise:

- Bei der Installation der Konsole und/oder des Servers ist es ratsam, den neusten SQL Native Client zu benutzen. Dieser kann von www.microsoft.com/en-us/download/details.aspx?id=50402 heruntergeladen werden.
- Nach der Installation lassen sich Ihre Datenbank, Konsole oder das Upgrade von einer Testversion auf eine vollständige Version mit einem praktischen Dienstprogramm aktualisieren. Siehe: Verwendung des DNA-Datenbankassistenten.

Vorhandene Installation

Dieser Bildschirm wird eingeblendet, wenn eine Kopie von NetSupport DNA bereits auf einer Arbeitsstation installiert ist.



Ändern

Hiermit können Sie die aktuell installierten DNA-Komponenten ändern.

Reparieren

Installiert alle vom vorherigen Setup installierten Programmfeatures neu und repariert alle Installationsfehler im Programm.

Entfernen

Diese Option löscht alle installierten Features.

Wählen Sie die gewünschte Option und klicken Sie auf **Weiter**.

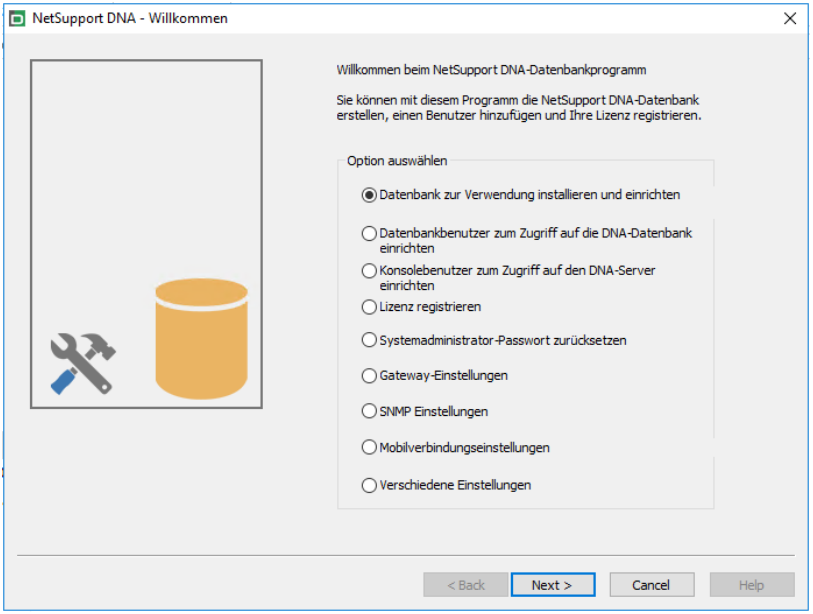
Verwendung des DNA Datenbank-Assistenten

Der DNA Datenbank-Assistent ist ein praktisches Dienstprogramm, das Sie nach der Installation ausführen können, wenn Sie Ihre DNA-Einstellungen ändern möchten.

Der Assistent kann benutzt werden, um die NetSupport DNA Datenbank zu erstellen; fügen Sie Datenbankbenutzer hinzu; fügen Sie Konsolenbenutzer hinzu; aktualisieren Sie die Lizenzdetails; setzen Sie das Administrator-Passwort zurück; fügen Sie NetSupport DNA Gateway-Einstellungen hinzu; stellen Sie die SNMP-Einstellungen ein; stellen Sie die Mobilverbindungseinstellungen ein; und stellen Sie sonstige Einstellungen ein, wie SQL Serveradresse, Zeitlimit für Abfragen und AD-Authentifizierung erzwingen.

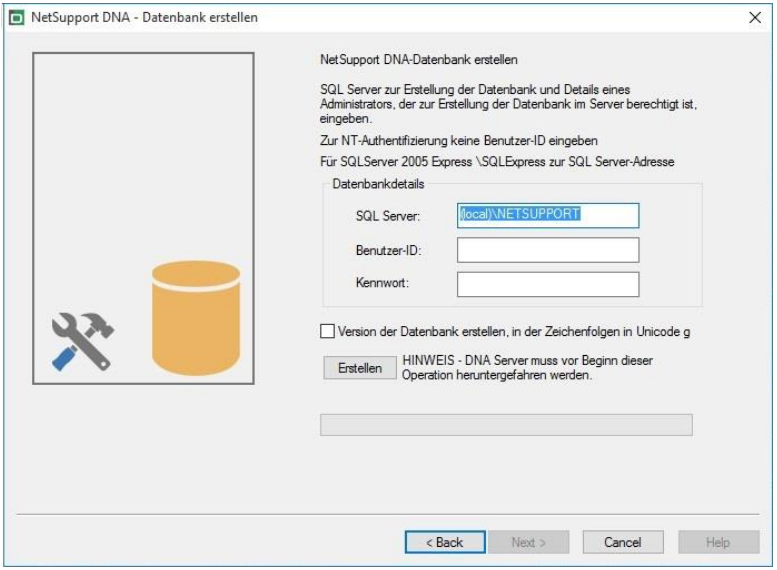
Während der Installation wird der DNA Datenbank-Assistent in den Serverordner des DNA-Programmverzeichnisses kopiert. Standard: c:\Programme\NetSupport\Netsupport DNA\Server\DNADBWizard.

Hinweis: Damit die Änderungen in Kraft treten, muss der Serverdienst neu gestartet werden.



Installation und Setup der Datenbank zur Verwendung

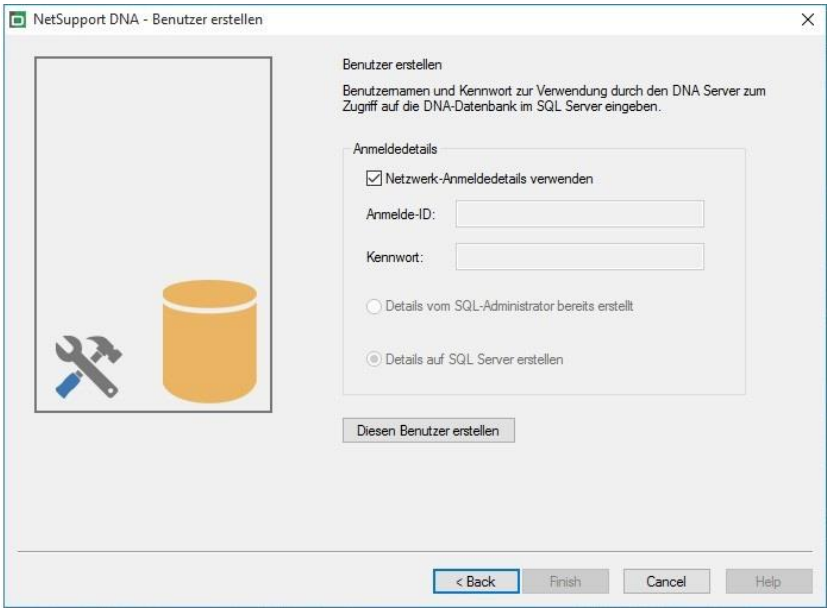
Geben Sie die Adresse/den Namen des SQL Servers ein, auf dem die DNA-Datenbank erstellt werden soll, sowie die Anmeldedetails des Administrators.



Setup eines NetSupport DNA-Benutzers für den Zugriff auf die Datenbank

Über dieses Dialogfeld können Sie den Benutzernamen und das Kennwort erstellen/ändern, die zum Zugriff auf die DNA-Datenbank im Server verwendet werden. Wenn Sie die vorhandenen Zugriffsdetails verwenden, überprüfen Sie, dass die Details vom SQL-Administrator bereits erstellt wurden.

Hinweis:	Es ist besser, keine bereits vorhandene Administratoranmeldung zu verwenden, da dies die Sicherheit anderer Datenbanken auf dem SQL Server gefährden könnte.

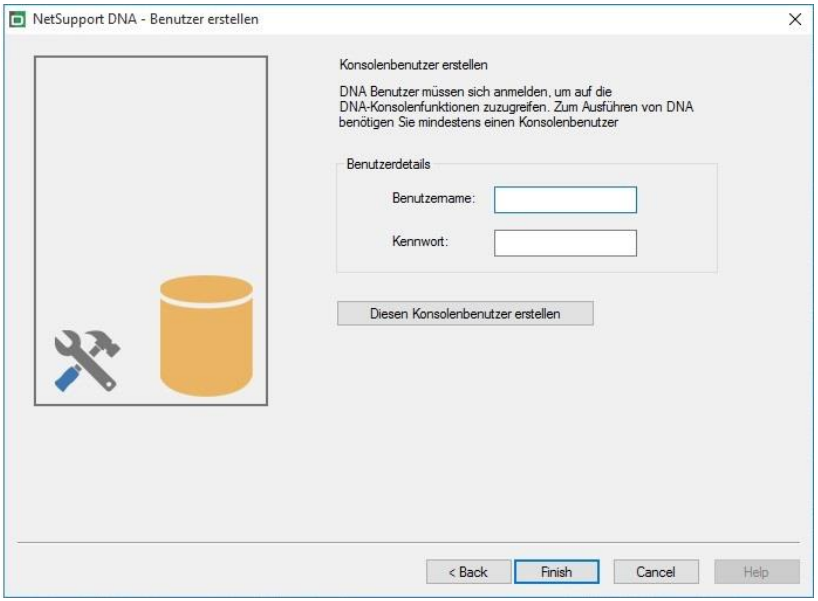


Setup von Administratorbenutzern für den Zugriff auf den DNA-Server

Wenn beim Erstellen des Konsolenbenutzers während der Installation ein Problem aufgetreten ist, können Sie mit dieser Option im Datenbankassistenten neue Konsolenbenutzer erstellen. Konsolenbenutzer erhalten Administratorrechte.

Hinweise:

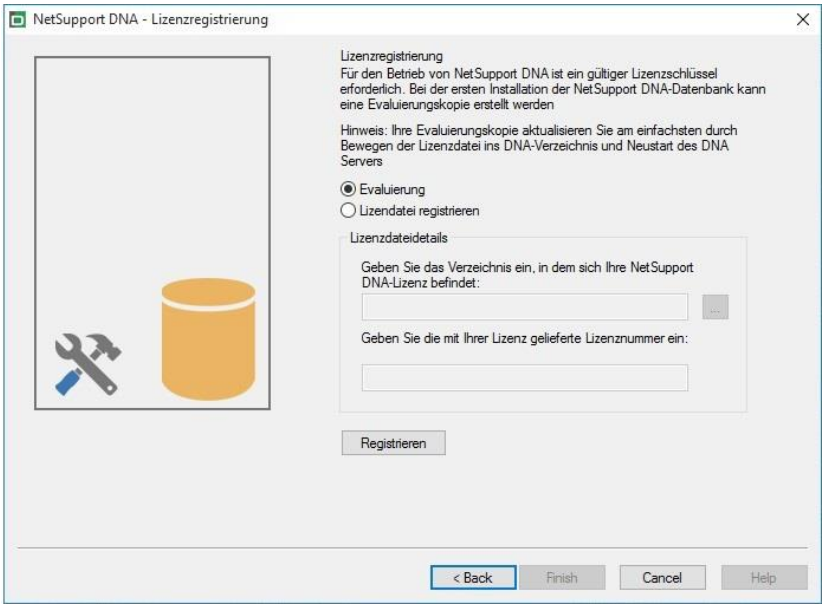
- Zusätzliche Konsolenbenutzer können auch über das Konsolenprogramm selbst erstellt werden.
- Für diesen Vorgang werden Administratorbenutzerrechte verlangt. Sie werden beim Klicken auf **Benutzer erstellen** zur Eingabe des richtigen Benutzernamens und Kennworts aufgefordert.



Registrieren einer Lizenz

Mit dem DB-Assistenten können Sie Ihre DNA-Lizenzdetails aktualisieren. Zum Beispiel beim Übergang von einer Evaluierungslizenz zu einer vollständigen Verkaufskopie.

Hinweis: Für diesen Vorgang werden Administratorbenutzerrechte verlangt. Sie werden beim Klicken auf **Registrieren** zur Eingabe des richtigen Benutzernamens und Kennworts aufgefordert.



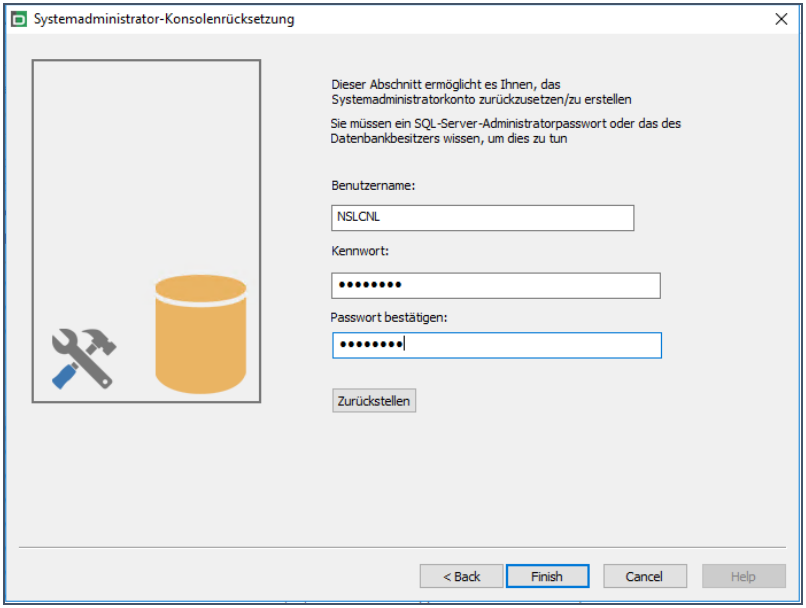
Um eine vollständige Lizenz zu registrieren, kopieren Sie die von NetSupport gelieferte Lizenzdatei in einen geeigneten Ordner und geben den Speicherort in das Dialogfeld “Registrierung” ein.

Geben Sie Ihre Lizenznummer ein, wobei die Groß-/Kleinschreibung berücksichtigt wird. Klicken Sie auf **Registrieren**, um die Lizenz zu aktualisieren.

Hinweis: Ein zentraler Aspekt des Alltagsbetriebs von DNA ist die Häufigkeit, mit der der Server Agentcomputer abfragt, um Daten für alle Hauptkomponenten zu sammeln (Evaluierungsstandard = 10 Minuten). Wenn Sie jedoch über eine große Agent-Basis verfügen, kann die Anzahl und Häufigkeit der Verbindungen die Leistung auf unerwünschte Weise beeinträchtigen. Um dem entgegenzuwirken, bestimmt DNA bei der Aktivierung einer "Verkaufs"-Version, ob aufgrund der registrierten Anzahl von Benutzerlizenzen ein passenderes Verbindungsintervall benötigt wird. Nach der Installation kann ein Konsolenbediener das Intervall für die einzelnen Komponenten ggf. manuell ändern.

Systemadmininistrator-Passwort zurücksetzen

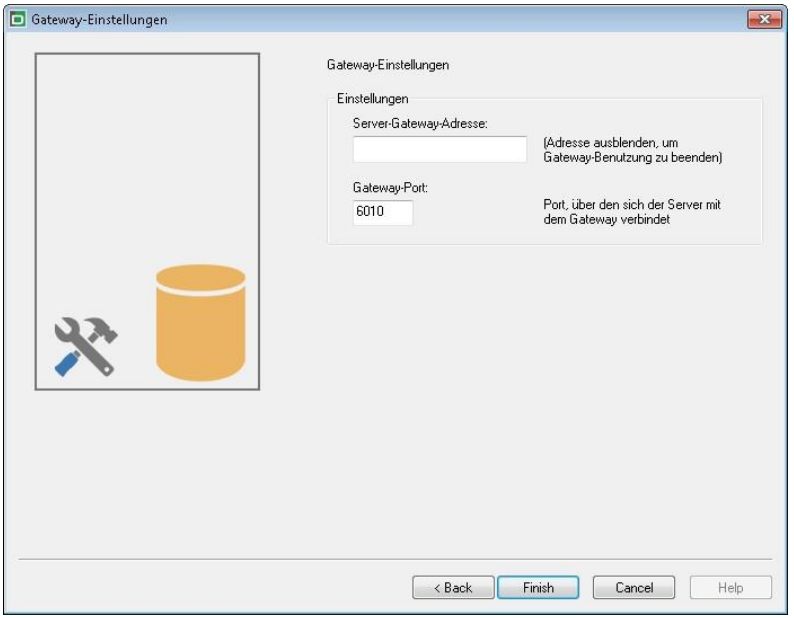
Diese Option ermöglicht es Ihnen, das Passwort für den Systemadministrator zurückzusetzen. Um es zurückzusetzen, müssen Sie das Adminstratorpasswort für den SQL-Server wissen.



Geben Sie den Benutzernamen des Systemadministrators und ein neues Passwort ein, und klicken Sie auf Zurücksetzen. Sie werden dann aufgefordert, die Details für den SQL-Server, die Benutzer-ID (falls erforderlich) und das SQL-Server-Administratorpasswort einzugeben; klicken Sie auf OK. Das Passwort für den Systemadministrator ist nun zurückgesetzt.

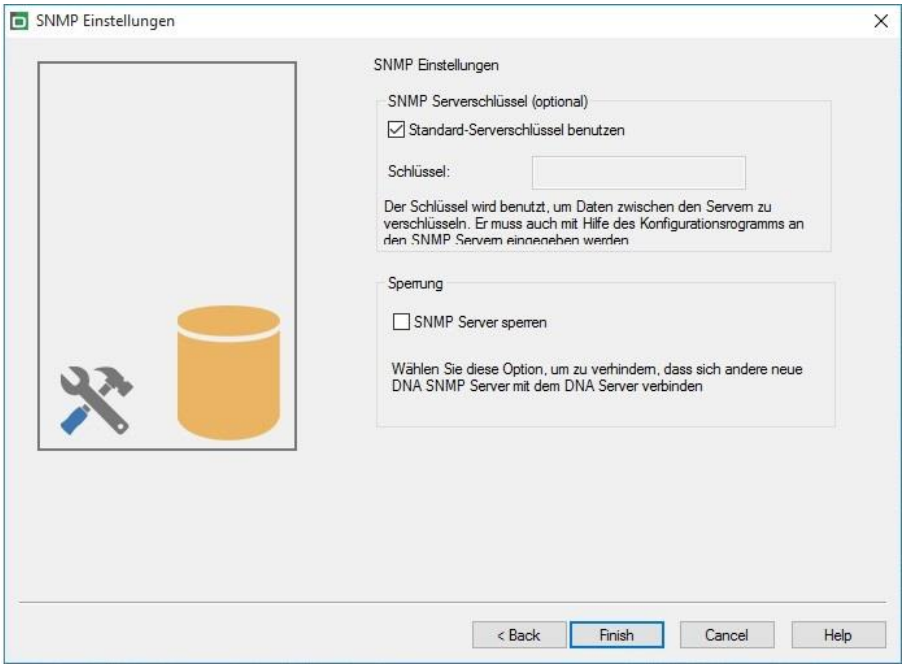
Gateway-Einstellungen

Die IP-Adresse und Anschlussnummer für den DNA Gateway können eingegeben werden, wenn Sie sie benutzen möchten und diese Informationen bei der Installation nicht eingegeben wurden. Oder wenn Sie mit der Nutzung des DNA Gateways aufhören möchten, entfernen Sie die Gateway-Adresse.



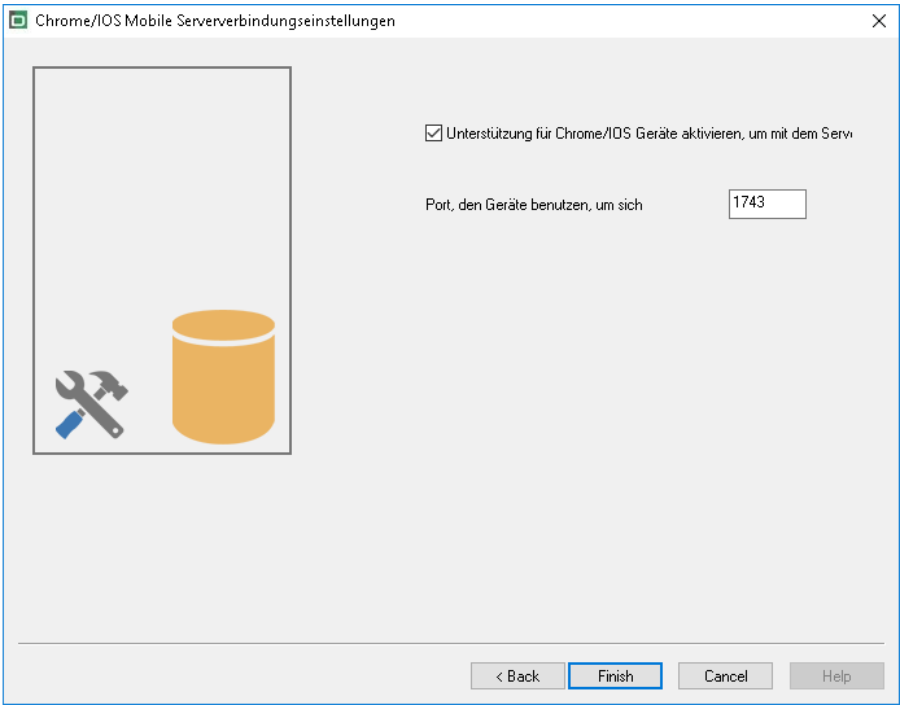
SNMP Einstellungen

Mit diesem Dialog können Sie einen SNMP Serverschlüssel einstellen. Dieser wird benutzt, um Daten zwischen Servern zu verschlüsseln und muss auch am SNMP Server eingestellt werden. Sie können die SNMP Server auch sperren und somit verhindern, dass sich andere SNMP Server mit dem DNA Server verbinden.



Mobilverbindungseinstellungen

In der Standardeinstellung lässt NetSupport DNA zu, dass sich Chrome und iOS Geräte mit dem Server verbinden, aber das kann von hier aus deaktiviert werden. Der Port, den die Geräte benutzen, um sich mit dem Server zu verbinden, ist Port 1743.



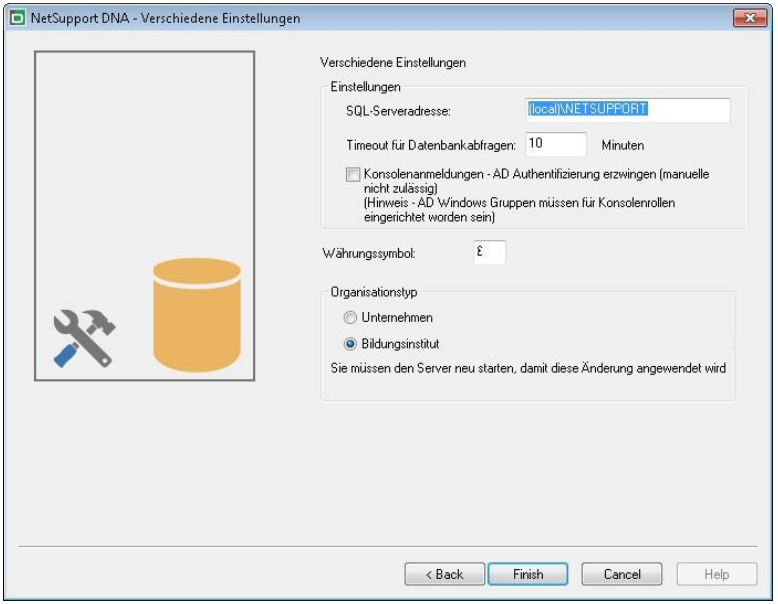
Verschiedene Einstellungen

Von diesem Dialog aus können Sie verschiedene NetSupport DNA Einstellungen ändern, wie die IP-Adresse des SQL Servers, Datenbankabfragen-Timeout, AD-Authentifizierung erzwingen, den Organisationstyp wählen und stellen Sie die Währung ein, die benutzt werden soll.
Standardmäßig ist das Fragetimeout der Datenbank auf 300 Sekunden eingestellt. Sie können dies durch Eingabe des gewünschten Wertes ändern.

Wenn Sie einer Konsolerolle eine Active Directory Windows-Gruppe zugewiesen haben, können Sie die AD-Authentifizierung erzwingen. Dann kann der Benutzer nur auf die DNA Konsole zugreifen, wenn er im Active Directory authentifiziert ist.

NetSupport DNA ist in zwei Versionen verfügbar: Unternehmen und Bildungswesen. Wählen Sie den gewünschten Organisationstyp.

NetSupport DNA stellt die Währung von dem lokalen System des Geräts ein, in dem sich der DNA Server befindet. Um die in der Datenbank benutzte Währung zu ändern, geben Sie hier das geforderte Währungssymbol ein.



Installation über Active Directory

NetSupport DNA ermöglicht es Ihnen, Agents über Active Directory Gruppenrichtlinien-Softwareverteilung zu installieren.

Um über Active Directory zu installieren, müssen Sie DNA.ini und die Agent.msi Datei suchen.

DNA.ini ist im folgenden Ordner auf dem NetSupport DNA Konsolengerät gespeichert:

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

Agent.msi ist vom Downloads-Bereich verfügbar:
www.netsupportdna.com/downloads.asp

Für eine umfassende Anleitung dazu, wie eine Active Directory-Bereitstellung konfiguriert wird, besuchen Sie bitte unsere Wissensbasis und lesen Sie den Produktartikel **Installing the NetSupport DNA Agent via Active Directory Group Policy software deployment** (Installieren des NetSupport DNA Agent über die Active Directory Gruppenrichtlinien-Software-Bereitstellung).

Option "Erweitert" - Befehlszeileninstallation

NetSupport DNA ermöglicht Administratoren die Installation von Konsole, Agent, Application Packager und der Agent- und Server-Gateways von der Befehlszeile mit den gelieferten MSI Installern. Ferner lassen sich Konsole, Agent und Application Packager über Active Directory installieren.

Installation von der Befehlszeile

1. Speichern Sie die MSI-Installationsdatei im gleichen Ordner wie die Konfigurationsdatei auf dem Zielcomputer oder einem zugreifbaren Share.
2. Bearbeiten Sie die INI-Datei, um die geeigneten Einstellungen für Ihre Installation vorzunehmen, z. B. ServerAddress=, InstallDir=
3. Führen Sie die Installation auf dem Zielcomputer gemäß folgendem Muster aus:

Installation des DNA Agents

msiexec.exe /qb /i „NetSupport DNA 300 client.msi"

Kontrollieren, für welche lokalen Benutzer die DNA-Konsole installiert ist

msiexec.exe /qb /i „NetSupport DNA 300 console.msi" ALLUSERS=2

ALLUSERS=""	Installiert das Paket ausschließlich für den aktuellen Benutzer.
ALLUSERS=1	Installiert das Paket für alle lokalen Benutzer.
ALLUSERS=2	Überprüft, ob der Benutzer Administratorrechte hat. Wenn ja, wird das Paket für alle Benutzer installiert, wenn nein, erfolgt die Installation nur für den aktuellen Benutzer. Für DNA MSI Installer nicht unterstützt.

Ein Beispiel für eine DNA.INI-Datei wurde im Installationsverzeichnis Ihrer Konsole erstellt. Dies ermöglicht die Benutzerdefinition verschiedener Parameter für die MSI-Installation.

Agent- und Konsoleoptionen

[All]

InstallDir=	Zur Nutzung des Standard-Installationsverzeichnisses leer lassen. Bezieht sich auch auf Installationen von Application Packager.
ServerAddress=	Geben Sie die IP-Adresse oder vorzugsweise den DNS-Namen des DNA Servers ein.

Optionen für nur den Agent

[Client]

EnableLSP=	1 = NetSupport LSP installieren, 0 = nicht installieren
RemoveUninstallOption=	1 = erscheint nicht unter „Software"

Installation über Active Directory (AD)

Bei der Installation von DNA über Active Directory sind keine besonderen Eigenheiten zu beachten.

1. Verschieben Sie die NetSupport DNA MSI- und INI-Datei in ein Share, auf das Ihre Computer/Benutzer zugreifen können, auf Ihrem AD Server.
2. Erstellen oder bearbeiten Sie ein Group Policy Object (GPO), das sich auf die Benutzer oder Computer, für die Sie DNA installieren möchten, bezieht.
3. Erstellen Sie je nach Bedarf entweder unter Computerkonfiguration oder Benutzerkonfiguration ein neues AD Software-Installationspaket.
4. Weisen Sie das Paket zu oder veröffentlichen Sie es.

Weitere Informationen über Softwareinstallationen unter Active Directory finden Sie in den Microsoft-Hilferessourcen unter http://support.microsoft.com/kb/816102

Installation von NetSupport DNA Agent auf Mac Systemen

Ein NetSupport DNA Agent kann auf Mac Systemen installiert werden, so dass Sie Ihre Mac Geräte effektiv verwalten können.

Hinweis: Der NetSupport DNA Mac Agent unterstützt Mac OS X 10.8 und darüber.

Installation NetSupport DNA

1. Der NetSupport DNA Agent wird als Standard Mac OS X .DMG Datei angeboten. Diese steht im Download-Bereich unserer Website zur Verfügung.
2. Um das Drive-Bild zu laden, kopieren Sie es auf die Festplatte und doppelklicken mit der Maus. Das geladene Drive-Bild ist nun auf dem Desktop verfügbar.
3. Der Installer wird automatisch ausgeführt. Befolgen Sie die Anweisungen auf dem Bildschirm.

Von Mac Agents unterstützte Funktionen:

- Volles Hardware- und Software-Inventar vom Agent-Gerät sammeln.
- Bediener automatisch über alle Hardware- und Software-Alerts benachrichtigen.
- Detaillierte Zusammenfassung aller Internet-Aktivitäten.*
- Eine Zusammenfassung aller benutzten Anwendungen.
- Realtime-Überwachung der Agent-Geräte in Symbol-, Detail- oder Miniaturansicht.
- Eine einzige Zusammenfassung auf Zeitbasis von allen Aktivitäten, die in einer chronologischen Ansicht dargestellt werden.
- Fernwartung von Agent-Geräten, die es Bedienern ermöglicht, Fehlersuchen und administrative Aufgaben remote auszuführen.
- Agents können ein Anliegen melden.*
- Schlüsselwörter und Begriffe überwachen.*

* Die Funktion steht nur in der NetSupport DNA Version für das Bildungswesen zur Verfügung.

NetSupport iOS Browser

NetSupport DNA bietet eine mobile Browser-App für iOS Tablets und Smartphones, die die wichtigsten NetSupport DNA Desktop-Managementfunktionen unterstützt. Wenn sie geöffnet wird, fragt sie das iOS Gerät ab, um die Systeminventar-Schlüsseldetails zu sammeln und Online-Aktivitäten zu überwachen. Die gesammelten Daten werden dynamisch an Ihren lokalen NetSupport DNA Server gesendet und stehen dann für die Berichterstattung innerhalb der NetSupport DNA Management Konsole zur Verfügung.

Die App unterstützt auch die wichtigsten NetSupport School Klassenzimmerunterricht-Tools, was die Realtime-Interaktion mit Schülern und deren Unterstützung während des Unterrichts ermöglicht.

Die NetSupport Browser-App kann für Geräte mit iOS 9.3 oder höher vom Apple App Store heruntergeladen werden.

Für Informationen darüber, wie Sie die NetSupport iOS Browser zentral konfigurieren und verteilen können, klicken Sie bitte hier.

Hinweis: In der Standardeinstellung benutzen Geräte Port 1743. Dies kann im NetSupport DNA Datenbank-Assistenten geändert werden.

Außerdem werden Standardbrowsernavigation-Funktionen geboten - einschließlich Lesezeichen, Registerkarten hinzufügen (mit der Option, eine Standard-Homepage einzustellen), Internetverlauf sowie die Option, die Standardsuchmaschine zu wechseln.

Unterstützte Funktionen:

- **Realtime-Überwachung** – Ein Administrator oder Lehrer/In kann über die Konsole eine Realtime-Zusammenfassung aller Geräte anzeigen. Ausgewählte Geräte können entweder in einer detaillierten Listenansicht oder als Realtime-Miniaturansichten aller Gerätebildschirme angezeigt werden.
- **Internet-Metering** (Bildungswesen-Version) – Es wird eine Zusammenfassung der Internetaktivitäten über die App aufgezeichnet, einschließlich der Start- und Endzeiten für jede besuchte URL und der aktiven Zeit, die auf einer Seite verbracht wurde.
- **Internetbeschränkungen** (Bildungswesen-Version) – Die Internetnutzung kann durch Durchsetzung der Listen von genehmigten und beschränkten Websites voll verwaltet werden.

- **eSafety Schlüsselwortüberwachung** (Bildungswesen-Version) – Dieses Tool hilft den Schulen, Schüler davor zu schützen, dass sie unangemessenen Online-Inhalten ausgesetzt werden. Es warnt das Personal, wenn Schüler Begriffe eingeben oder nach diesen suchen, die mit denen in der DNA Schlüsselwort-Datenbank übereinstimmen, was eSafety und Internetsicherheitsindikatoren für Selbstverletzung, Mobbing, Radikalisierung, sexuelle Ausbeutung von Kindern und vieles mehr bietet.
- **eSafety Anliegen melden** (Bildungswesen-Version) – Schüler können Anliegen jetzt direkt und diskret einem benannten Mitglied des Schulpersonals melden.
- **eSafety-Ressourcen** (Bildungswesen-Version) – Das eSafety-Ressourcen Symbol in der Symbolleiste der Browser App bietet Schülern sofortigen Zugriff auf eine Liste geeigneter Online-Unterstützungsressourcen.
- **Hardware-Inventar** – Wenn der DNA Browser auf einem Gerät geöffnet wird, wird ein Inventar dynamisch an den NetSupport DNA Server gesendet.
- **Unternehmens-Alerting** – Realtime-Alerts ermöglichen es den Konsolenbedienern, sofort jeden Benutzer zu identifizieren, der versucht hat, Zugriff auf eine beschränkte Website zu nehmen, oder der ein eSafety-Schlüsselwort ausgelöst hat.
- **Aktivität** – DNA Konsolenbediener können eine chronologische Ansicht der Geräteaktivität für eine gewählte Zeitspanne anzeigen.
- **Roaming-Daten sammeln** – Wenn Geräte außerhalb des Netzwerks benutzt werden, kann die App dafür konfiguriert werden, Aktivitäten im Hintergrund aufzuzeichnen, wobei die gespeicherten Daten dann vom DNA Server gesammelt werden, wenn die Verbindung zu ihm wiederhergestellt wird.

NetSupport DNA Browser für Android

NetSupport DNA bietet eine mobile Browser-App für Android Tablets und Smartphones, so dass Sie die wichtigsten Systeminventardetails sammeln und Online-Aktivitäten überwachen können. Die gesammelten Daten werden dynamisch an Ihren lokalen NetSupport DNA Server gesendet und stehen dann für die Berichterstattung innerhalb der NetSupport DNA Management Konsole zur Verfügung.

Die NetSupport DNA Browser für Android App kann mit Geräten mit Android 5.01 und darüber vom Google Play Store heruntergeladen werden.

Zu den Standardnavigationsfunktionen des Browsers zählen Lesezeichen, Registerkarten hinzufügen und Internetverlauf, und in der Symbolleiste der DNA Browser App wird außerdem die Option geboten, die Standardsuchmaschine zu ändern.

Unterstützte Funktionen:

- **Realtime-Überwachung** – Ein Administrator oder Lehrer/In kann über die Konsole eine Realtime-Zusammenfassung aller Geräte anzeigen. Ausgewählte Geräte können entweder in einer detaillierten Listenansicht oder als Realtime-Miniaturansichten aller Gerätebildschirme angezeigt werden.
- **Internet-Metering** (Bildungswesen-Version) – Es wird eine Zusammenfassung der Internetaktivitäten über die App aufgezeichnet, einschließlich der Start- und Endzeiten für jede besuchte URL und der aktiven Zeit, die auf einer Seite verbracht wurde.
- **Internetbeschränkungen** (Bildungswesen-Version) – Die Internetnutzung kann durch Durchsetzung der Listen von genehmigten und beschränkten Websites voll verwaltet werden.
- **eSafety Schlüsselwortüberwachung** (Bildungswesen-Version) – Dieses Tool hilft den Schulen, Schüler davor zu schützen, dass sie unangemessenen Online-Inhalten ausgesetzt werden. Es warnt das Personal, wenn Schüler Begriffe eingeben oder nach diesen suchen, die mit denen in der DNA Schlüsselwort-Datenbank übereinstimmen, was eSafety und Internetsicherheitsindikatoren für Selbstverletzung, Mobbing, Radikalisierung, sexuelle Ausbeutung von Kindern und vieles mehr bietet.
- **eSafety Anliegen melden** (Bildungswesen-Version) – Schüler können Anliegen jetzt direkt und diskret einem benannten Mitglied des Schulpersonals melden.

- **eSafety-Ressourcen** (Bildungswesen-Version) – Das eSafety-Ressourcen Symbol in der Symbolleiste der Browser App bietet Schülern sofortigen Zugriff auf eine Liste geeigneter Online-Unterstützungsressourcen.
- **Hardware-Inventar** – Wenn der DNA Browser auf einem Gerät geöffnet wird, wird ein Inventar dynamisch an den NetSupport DNA Server gesendet.
- **Software-Inventar** – Wenn der NetSupport DNA Browser an einem Gerät gestartet wird, wird ein volles Inventar der auf dem Gerät installierten Programme dynamisch an den NetSupport DNA Server gesendet, so dass es anschließend an der Konsole angezeigt werden kann.
- **Unternehmens-Alerting** – Realtime-Alerts ermöglichen es den Konsolenbedienern, sofort jeden Benutzer zu identifizieren, der versucht hat, Zugriff auf eine beschränkte Website zu nehmen, oder der ein eSafety-Schlüsselwort ausgelöst hat.
- **Aktivität** – Konsolenbediener können eine chronologische Ansicht der Geräteaktivität, der besuchten Websites und der ausgelösten eSafety-Begriffe für eine gewählte Zeitspanne anzeigen.
- **Chat** – Konsolenbediener können eine von zwei Personen geführte Chat-Sitzung mit einer beliebigen Anzahl von gewählten Benutzern starten.
- **Nachricht** – Konsolenbediener können eine einseitige Benachrichtigung an gewählte Benutzer aussenden.

NetSupport DNA Chrome Agent

Die NetSupport DNA Agent Erweiterung für Chrome OS unterstützt NetSupport DNAs Hauptfunktionen für Desktop-Management. Wenn sie geöffnet wird, fragt sie das iOS Gerät ab, um die Systeminventar-Schlüsseldetails zu sammeln und Online-Aktivitäten zu überwachen. Die gesammelten Daten werden dynamisch an Ihren lokalen NetSupport DNA Server gesendet und stehen dann für die Berichterstattung innerhalb der NetSupport DNA Management Konsole zur Verfügung.

Die NetSupport DNA Chrome Agent Erweiterung kann vom Google Play Store heruntergeladen werden.

Für Informationen darüber, wie Sie die NetSupport DNA Agent Erweiterung für Google Chrome zentral konfigurieren und verteilen können, klicken Sie bitte hier.

Hinweis: In der Standardeinstellung benutzen Geräte Port 1743. Dies kann im NetSupport DNA Datenbank-Assistenten geändert werden.

Unterstützte Funktionen:

- Vollständiges Hardware-Inventar von Agent-Geräten sammeln.
- Realtime-Überwachung der Agent-Geräte in Symbol-, Detail- oder Miniaturansicht.
- Agents können ein Anliegen melden.*
- Schlüsselwörter und Begriffe überwachen.*
- Detaillierte Zusammenfassung aller Internet-Aktivitäten.*
- DNA Konsolenbediener können eine chronologische Ansicht der Geräteaktivität für eine gewählte Zeitspanne anzeigen.
- Realtime-Alerts ermöglichen es den Konsolenbedienern, sofort jeden Benutzer zu identifizieren, der versucht hat, Zugriff auf eine beschränkte Website zu nehmen, oder der ein eSafety-Schlüsselwort ausgelöst hat.

* Die Funktion steht nur in der NetSupport DNA Version für das Bildungswesen zur Verfügung.

DNA Gateway

Über den DNA Gateway können entfernte Agents auf solide und sichere Methode über das Internet zur Suche nach und Verbindung mit Agents in entfernten Netzwerken. Durch Nutzung der eingeschlossenen Remote- und Lokale-Gateway-Komponenten können von mehreren entfernten Standorten Daten an einen zentralen Ort zurück übermittelt werden.

DNA Lokales Gateway (Server)
Über das NetSupport DNA Gateway können Remote-Agents mit dem NetSupport DNA Server verbunden werden. Das Local Gateway kommuniziert mit dem zentralen NetSupport DNA Server. Das Local Gateway muss separat von den anderen NetSupport DNA Komponenten installiert werden.

Hinweis: Wenn das DNA Server Gateway auf demselben Gerät installiert ist wie ein NetSupport Konnektivitätsserver (NCS), steht die Fernwartungsfunktion über das DNA Gateway nicht zur Verfügung. (Gilt nur für Installationen für das Bildungswesen.)

DNA Remote-Gateway (Agent)
Das Remote-Gateway fungiert als Proxyserver für die NetSupport DNA Remote-Agents und ermöglicht ihnen die Kommunikation mit dem NetSupport DNA Server. Das Remote-Gateway kann nur mit dem NetSupport DNA Agent installiert werden.

Hinweise:

- Es können mehrere Remote-Gateways installiert werden (an jedem Remote-Standort eins), aber nur ein Local (zentrales) Gateway.
- Die NetSupport DNA Konsole muss in demselben Netzwerk sein wie der NetSupport DNA Server, um Gateway Agents erkennen zu können.

Gateway-Installation
Die Gateway-Komponenten können nur auf Geräten mit Windows XP SP3 oder höher installiert werden.

Wählen Sie im Laufe der NetSupport DNA-Installation die zur Installation gewünschte Gateway-Komponente auf dem Bildschirm „Angepasstes Setup". Wenn Sie den Lokale-Gateway installieren, werden Sie zur Eingabe der IP-Adresse des DNA Servers aufgefordert. Die IP-Adresse des Lokales Gateways muss bei Installation des Remote-Gateways eingegeben werden.

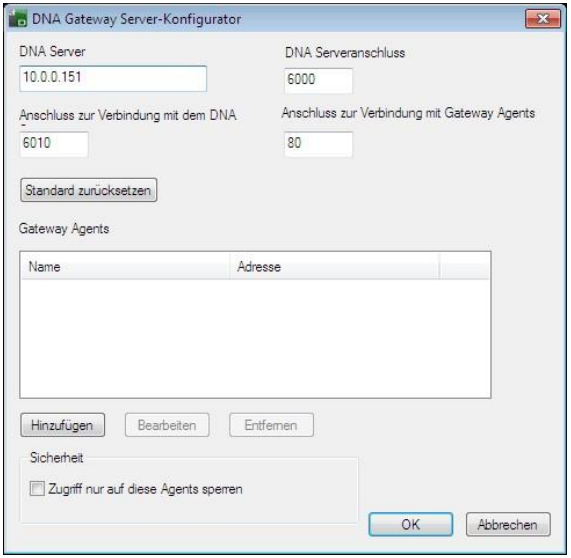
Hinweis: Zur Nutzung des DNA Gateways muss die IP-Adresse des Server Gateways im DNA Server eingegeben werden. Dies kann entweder während der Installation oder nach der Installation im DNA-Datenbankassistenten erfolgen.

Sie können die Parameter des Lokales und Remote Gateways im Server (Lokales) Gateway Konfigurator und dem Agent (Remote) Gateway Konfigurator konfigurieren.

Der aktuelle Status des Remote-Gateways und der verbundenen DNA Agents lässt sich im Dialogfeld „Gateway-Status" betrachten. Wählen Sie die Registerkarte „Tools" und klicken Sie auf das Symbol **Gateway-Status**.

Server Gateway Konfigurator

Mit dem Server Gateway Konfigurator können Sie die Parameter des Server Gateways konfigurieren. Während der Installation wird der Server Gateway Konfigurator in den Gateway-Ordner des DNA Programmverzeichnisses c:\Program files\NetSupport\NetSupport DNA\Gateway\DNAGatewayConfigS.exe kopiert.



DNA Server

Geben Sie die IP-Adresse des DNA Servers ein.

DNA Serveranschluss

Die Standardnummer des DNA Serveranschlusses ist 6000.

Anschluss zur Verbindung mit dem DNA Server

Der Standardanschluss von NetSupport, über den der DNA Server eine Verbindung zum Server Gateway herstellt, ist 6010.

Anschluss zur Verbindung mit Gateway Agents

Der Standardanschluss von NetSupport, über den der Server Gateway und der Agent Gateway kommunizieren, ist 80.

Standardanschlüsse zurücksetzen

Setzt alle Anschlusseinstellungen auf ihren Standardwert zurück.

Gateway Agents

Hier sind alle vom Server Gateway gefundenen Gateway Agents aufgelistet. Durch Anklicken der entsprechenden Schaltfläche können Sie Agents hinzufügen, bearbeiten und entfernen.

Sicherheit

Durch Auswahl von „Zugriff nur auf diese Agents sperren" lässt sich steuern, welche entfernten Rechner eine Verbindung zu Ihrem Server Gateway herstellen können.

Hinweis: Ferner haben Sie die Möglichkeit, die IP-Adresse des Server Gateways im DNA Datenbankassistenten zu konfigurieren.

Agent Gateway Konfigurator

Mit dem Agent Gateway Konfigurator können Sie die Parameter des Agent Gateways konfigurieren. Während der Installation wird der Agent Gateway Konfigurator in den Gateway-Ordner des DNA Programmverzeichnisses c:\Program files\NetSupport\NetSupport DNA\Gateway\DNAGatewayConfigC.exe kopiert.



DNA Gateway-Serveradresse

Geben Sie die IP-Adresse des Server Gateways ein.

Anschluss zur Verbindung mit dem Server Gateway

Der Standardanschluss von NetSupport, über den der Server Gateway und der Agent Gateway kommunizieren, ist 80.

Anschluss zur Verbindung durch DNA Agents

Der Standardanschluss von NetSupport, über den der Agent Gateway auf eine Verbindung mit DNA Agents wartet, ist 6000.

Anschluss zur Verbindung mit DNA Agents

Der Standardanschluss von NetSupport, über den DNA Agents auf eine Verbindung mit dem Agent Gateway warten, ist 6001.

Wiederholungszeitraum bei gescheiterten Verbindungen

Der Standardwiederholungszeitraum bei gescheiterten Verbindungen ist 300 Sekunden. Sie können diesen gegebenenfalls ändern.

Klicken Sie auf **Standardeinstellungen zurücksetzen**, damit alle Einstellungen auf ihren Standardwert zurückgesetzt werden.

Hinweis: Ferner haben Sie die Möglichkeit, die IP-Adresse des Server Gateways im DNA Datenbankassistenten zu konfigurieren.

SNMP-Server-Konfiguration

Der SNMP-Server-Konfigurator ermöglicht es Ihnen, die Parameter für den SNMP-Server zu konfigurieren. Während der Installation wird der SNMP-Server-Konfigurator an den SNMP-Server-Ordner des NetSupport DNA Programmverzeichnisses c:\Program Files\NetSupport\NetSupport DNA\SNMPServer\DNASNMPConfig.exe kopiert.

DNA Server
Die DNS Adresse des NetSupport DNA Servers.

Port, mit dem der DNA Server am SNMP-Server verbunden wird, um Daten zu sammeln
Der NetSupport Standardport, den der NetSupport DNA Server benutzt, um sich mit dem SNMP-Server zu verbinden, um Daten zu sammeln, ist 6005.

Port, an dem die Verbindung mit dem DNA Server hergestellt wird
Der NetSupport Standardport, den NetSupport DNA Geräte benutzen, um die Verbindung mit dem NetSupport DNA Server herzustellen ist 6000.

Port, an dem UDP Nachrichten vom DNA Server empfangen werden
Der NetSupport Standardport, der benutzt wird, um Nachrichten vom NetSupport DNA Server zu empfangen ist 6006.

Diagnostikinformationen
Bietet Informationen über den aktuellen Status des SNMP-Servers, die letzte Verbindungszeit und die SNMP-Geräte, die gegenwärtig überwacht werden.

Standardserverschlüssel benutzen
Ermöglicht es Ihnen, einen SNMP-Serverschlüssel einzustellen. Dieser wird benutzt, um Daten zwischen den Servern zu verschlüsseln und muss am SNMP-Server und am NetSupport DNA Server eingestellt werden.

Hinweis: Sie können einen Serverschlüssel im NetSupport DNA Datenbank-Assistenten einstellen.

Gateway-Status

Im Dialogfeld „Gateway-Status" können Sie den aktuellen Status Ihrer Remote-Gateway (Agent) überprüfen und sehen, welche DNA Agents mit den Remote-Gateway verbunden sind.

1. Wählen Sie die Registerkarte „Tools" und klicken Sie auf das Symbol **Gateway-Status**.
2. Das Dialogfeld „Gateway-Status" wird eingeblendet.
3. Die Remote-Gateway sind mit dem Namen, dem aktuellen Verbindungsstatus („OK" oder „Nicht verfügbar") und der letzten Verbindungszeit aufgelistet.
4. Um zu sehen, welche Agents mit einem Gateway verbunden sind, wählen Sie den gewünschten Gateway und klicken Sie auf **PCs**.
5. Von diesem Dialogfeld aus können Sie auch Remote-Gateway, die nicht mehr verbunden sind, löschen. Wählen Sie den gewünschten Gateway und klicken Sie auf **Löschen**.

Klicken Sie auf **Aktualisieren**, um die Informationen zu aktualisieren. Standardmäßig wird der Gateway-Status alle zehn Minuten aktualisiert.

Hinweis: Bei einem Neustart des Lokales-Gateways kann es fünf Minuten dauern, bis der Remote-Gateway die Verbindung wieder herstellt, außer wenn man den Remote-Gateway neu startet.

Aktualisierung von vorhandenen DNA-Versionen

Wenn Sie von einer früheren Version von NetSupport DNA (DNA 2.70 und besser) auf DNA aktualisieren, können Sie die neue Version vom DNA Installer aus installieren.

Hinweis: Wenn Sie von einer DNA-Version vor DNA 2.70 aktualisieren, konsultieren Sie bitte die Anleitungen auf unserer Website unter: www.netsupportsoftware.com/support.

1. Führen Sie die neue DNA SETUP.EXE auf dem PC aus, auf dem sich der DNA Server befindet.
2. Folgen Sie den Anleitungen auf dem Bildschirm. Die vorherige DNA-Version wird gelöscht und DNA wird installiert. Alle vorherigen DNA-Einstellungen bleiben bestehen.
3. Konsolen und Agents werden bei der nächsten Verbindung zum Server auf die neue Version aktualisiert.

NetSupport DNA Mobile Konsole

Die DNA Mobil-App ermöglicht es Technikern, wenn sie nicht an ihrem Schreibtisch sind, ein detailliertes Hardware- und Software-Inventar für jeden PC im Unternehmensnetzwerk zu suchen und zu betrachten. Die Mobil-App bietet auch einen QR-Code-Scanner, mit dem jedes Gerät augenblicklich identifiziert werden kann, und zwar entweder über einen QR-Code, der auf dem Bildschirm im DNA Agent Fenster angezeigt wird, oder über ein am Gerät angebrachtes Schild. Außerdem hat NetSupport DNA eine QR-Code-Aufklebererstellungsfunktion einschließlich Anzeige der benutzerdefinierten Einzelheiten. Die App zeigt auch den Verlauf aller Hardware-Änderungen sowie der Software-Installationen und -Entfernungen.

Zusätzlich zu den Inventar- und Verlaufansichten zeigt die NetSupport DNA Mobil-App alle neuen PC Alerts, die im gesamten Netzwerk ausgelöst worden sind.

Die NetSupport DNA Mobile Konsole App kann kostenlos von den Google Play und Apple App Stores heruntergeladen warden

Für weitere Informationen über die Installation und Konfiguration klicken Sie hier.

ERSTE SCHRITTE

Ausführen der Konsole

Nach der Installation können Administratoren (Konsolebenutzer) die DNA Konsole laden und mit dem Abfragen der Datenbank beginnen.

1. Wählen Sie {Start}{Programme}{NetSupport DNA}{DNA Konsole}.
2. Das Dialogfeld "Konsolenanmeldung" wird eingeblendet.



3. Bestätigen Sie die Richtigkeit der angegebenen Serveradresse/des Servernamens. Wenn sie nicht stimmen, können Sie die Angaben manuell ändern. Geben Sie den Benutzernamen und das Kennwort für die Konsole ein.
4. Klicken Sie auf **OK**.
5. Der Hauptkonsolebildschirm von NetSupport DNA wird eingeblendet.

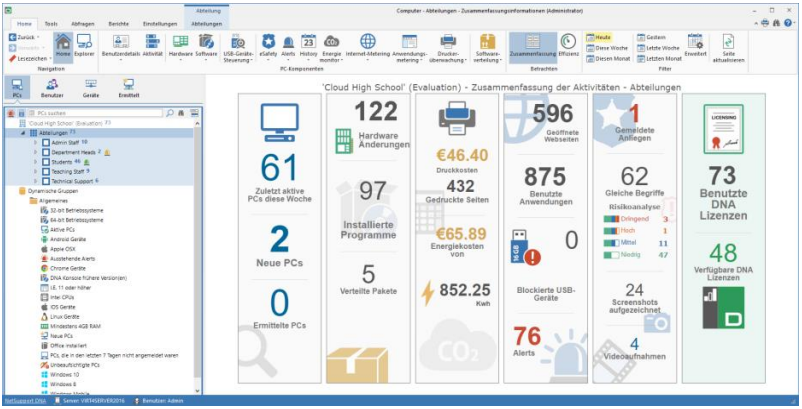
Hinweis: Wenn Sicherer Modus aktiviert ist, kann der Konsolenbenutzer drei Versuche machen, sich anzumelden, bevor sein Konto gesperrt wird. Das Konto muss dann von einem Administrator entsperrt werden, außer wenn der Konsolenbenutzer eine Emailadresse hat, und die Email-Einstellungen konfiguriert worden sind; in diesem Fall steht eine Rücksetzungsoption zur Verfügung, bei der ein vorübergehendes Passwort per Email gesendet wird. Der Konsolenbenutzer muss dieses Passwort dann beim nächsten Mal ändern, wenn er sich anmeldet.

Das Konsolefenster

Das Konsolefenster ist die wichtigste Schnittstelle für den Zugriff auf die zahlreichen Optionen von DNA. Eine praktische Strukturansicht ermöglicht es Ihnen, die Daten für jeden geforderten PC, jeden Benutzer, jedes Gerät oder ermittelten PC schnell anzuzeigen.

Wenn Sie sich zuerst bei der Konsole anmelden, erscheint eine Zusammenfassung, die einen Überblick über jede der Hauptkomponenten von NetSupport DNA bietet. Von dieser Ansicht kann zur Effizienzansicht gewechselt werden, die ein Dashboard bietet, das auf einen Blick zeigt, wie die Technologie verwendet wird, sowie die Bereiche, in denen die Effizienz verbessert werden kann, um Kosten- und Zeiteinsparungen zu erzielen

Hinweis: Nur ein Konsolebediener besitzt die Zugriffsrechte zum Ändern der DNA-Konfigurationseinstellungen. Weiteren Bedienern wird mitgeteilt, dass ihr Zugriff schreibgeschützt ist.



Ribbon/Die Symbolleiste

Der Ribbon bietet Zugriff auf alle Werkzeuge, Komponenten und Konfigurationsprogramme von DNA und ist in fünf Registerkarten unterteilt.

Home

Bietet Zugriff auf NetSupport DNA Komponenten. Einige Komponenten haben ein Dropdownmenü für den Zugriff auf die dazugehörigen Funktionen. Wenn eine Komponente aktiv ist, sind gleichzeitig Funktionssymbole im Zusammenhang mit der Komponente im Ribbon angezeigt.

Tools
Bietet Zugriff auf die NetSupport DNA Tools.

Abfragen
Mit dem Abfragetool von DNA können Sie Datenbankeinträge abrufen, die bestimmte Kriterien erfüllen. Abfragen zu der Komponente, die gerade betrachtet wird, sind aufgelistet, was ein schnelles Abrufen der rgebnisse ermöglicht.

Berichte
DNA liefert zahlreiche Bericht- und Analysetools. Es sind eine Reihe von vordefinierten Optionen verfügbar, mit denen Sie schnell Informationen über alle Hauptkomponenten von DNA betrachten können.

Einstellungen
Bietet Zugriff auf Profile, wo die Komponenteneinstellungen konfiguriert und Benutzern, Active Directory Gruppen, PCs und Abteilungen zugewiesen werden können. Sie können von hier aus auf die Konsolenanpassungen zugreifen, Bediener hinzufügen und diesen Rollen zuweisen. Und bei der DNA Version für das Bildungswesen können Sie die **Cloud-basierte eSafety-Konsolle** aktivieren, die dafür konzipiert ist, dem eSafety-Personal zu helfen, von unterwegs auf eSafety-Alerts zuzugreifen, und Sie können die Funktion Ein **Anliegen über eine Website** melden konfigurieren.

Hinweise:
- Wenn in der Strukturansicht eine Abteilung oder ein Benutzer gewählt wird, erscheint im Menüband eine zusätzliche Registerkarte. Diese Registerkarte bietet schnellen Zugriff auf die Funktionen, die für diese Abteilung bzw. diesen Benutzer zur Verfügung stehen.
- Welche Funktionen, die auf einer Registerkarte gezeigt werden, hängt davon ab, in welcher Strukturansicht Sie sich befinden.

Sie können das Menüband minimieren, indem Sie  oben rechts auf der Konsole anklicken.

Die hierarchische Strukturansicht

In der Strukturansicht sind alle dynamisch gefundenen DNA Agents aufgeführt. Die Struktur entspricht standardmäßig der Struktur Ihrer Arbeitsgruppe/Domäne, aber Sie können sie an individuelle Bedürfnisse anpassen, z. B. Agents nach geografischem Standort oder nach Abteilung gruppieren. Um Elemente in der Strukturansicht stärker hervorzuheben,

können Sie benutzerdefinierte Bilder an Abteilungen, Dynamische Gruppen, PCs und Benutzer zuweisen.
Um ein benutzerdefiniertes Bild auf einen PC oder Benutzer anzuwenden, wählen Sie diese in der Strukturansicht, klicken Sie sie mit der rechten Maustaste an und wählen Sie **Eigenschaften**. Nun erscheint der Eigenschaften Dialog. Klicken Sie auf  und durchsuchen Sie auf das geforderte Bild. Dieses erscheint nun in der Strukturansicht.



Hinweise:

- Dank der Integration von NetSupport mit Active Directory können Sie die Strukturansicht auch nach dem gleichen Muster wie Ihre Active Directory-Struktur einblenden. Informationen zum Betrachten von PCs in ihren Active Directory Containern finden Sie unter „Konsoleeinstellungen - Active Directory-Einstellungen". Sie können die AD Container gegebenenfalls in der Strukturansicht ausblenden.
- Es können Lesezeichen zu der Strukturansicht für PCs, Benutzer und Geräte hinzugefügt werden, so dass Sie schnell zum geforderten Speicherort navigieren können.
- In der Standardeinstellung werden nur die ersten 100 Elemente in einer Abteilung in der Strukturansicht angezeigt. Um alle Elemente anzuzeigen klicken Sie auf **Mehr**.

Die Strukturansicht kann zwischen den folgenden Optionen wechseln:

- **PCs**
- **Benutzer**
- **Geräte**
- **Ermittelt**

Oben in der Strukturansicht finden Sie ein Suchtool, mit dem Sie Agents in der Strukturansicht identifizieren und finden können.

Die Strukturansicht des **PCs** zeigt Daten für PCs und den PC-Eigentümer, der mit dem betreffenden PC verknüpft ist. Der PC-Eigentümer kann im Dialogfeld „Benutzer binden" geändert werden. Nicht standardmäßige Objekte lassen sich in der Struktur des PCs hinzufügen.

Hinweis: In der Standardeinstellung erscheinen mobile Agents in der Strukturansicht in einer Nicht-zugewiesen-Abteilung. Diese Agents können an eine entsprechende Abteilung verschoben werden. Siehe Agents zu Abteilungen hinzufügen.

Die **Benutzerstrukturansicht** zeigt Daten für die angemeldeten Benutzer und nicht auf den PC bezogene Daten. Nur die Registerkarten Explorer, Bentuzerdetails, Aktivität, USB-Geräte-Steuerung, eSafety*, Internet-Metering*, Applikationsmetering und Druckerüberwachung werden eingeblendet, wenn die Benutzerstrukturansicht ausgewählt ist.

Die **Geräte-Strukturansicht** zeigt Details der SNMP Agents.

Hinweis: Sie können anpassen, wie Agents in den Strukturansichten angezeigt werden. Klicken Sie auf  und wählen Sie einen Anzeigennamen auf der Liste.

Die **Ermittelte-Struktur-Ansicht** zeigt alle Computer, die beim Starten nicht gefunden wurden. Sie können NetSupport DNA dafür konfigurieren, das Netzwerk zu scannen und nach allen Geräten zu suchen, auf denen kein Agent installiert ist. Wenn diese ermittelt worden sind, können Sie ein einfaches Hardware-Inventar für das Gerät betrachten mit der Option, einen Agent dafür bereitzustellen.

Hinweis: Die ermittelte Strukturansicht kann bei Bedarf ausgeblendet werden. Wählen Sie die Einstellungen Registerkarte und klicken Sie auf dem **Allgemeines** Symbol. Nun erscheint der DNA Konfiguration Dialog: Klicken Sie die Option **Allgemeines** unter Konsolenanpassungen an und deaktivieren Sie **Ermittelte PC-Struktur zeigen**.

Ferner lassen sich dynamische Gruppen erstellen, welche die rasche Identifizierung von Agents, die bestimmte Kriterien erfüllen, ermöglichen. Eine typische Dynamische Gruppe wäre "alle PCs mit Windows 10". Es werden eine Anzahl von Effizienzgruppen und allgemeinen dynamischen Gruppen bereitgestellt.

Die Strukturansicht kann gefiltert werden, um nur PCs/Benutzer/Geräte zu zeigen, die mit einer Dynamische-Gruppen-Abfrage übereinstimmen. Wählen Sie die geforderte Dynamische Gruppe in der Strukturansicht, klicken Sie rechts und wählen Sie **Als Filter anwenden**. Nun erscheint eine Filterleiste oben in der Strukturansicht, die zeigt, welcher

Dynamische-Gruppe-Filter angewendet worden ist. Um den Filter zu entfernen, klicken Sie auf **Löschen**.

Informationsfenster

Im Informationsfenster sind die Daten angezeigt, die für jede der Hauptkomponenten von DNA gesammelt wurden. Zur leichteren Navigation werden Symbole für jede Komponente in allen Registerkarten außer der Tools- und Einstellungen-Registerkarte gezeigt.

Für jede Komponente stehen eine Vielfalt von Ansichten und Filtern zur Verfügung, die es Ihnen ermöglichen, Inhalt und Format der Daten anzupassen, die im Informationsfenster gezeigt werden.

Statusleiste

Die Statusleiste zeigt einen Link zur NetSupport DNA Website, den Server, mit dem die Konsole verbunden ist, den Benutzer, der gegenwärtig an der Konsole angemeldet ist, und, wenn Cloud* Zugriff aktiviert ist, ob die Daten zur Cloud synchronisiert werden. Beim Betrachten von Berichten können Sie zwischen Layouts hin- und herschalten und es ist ein Zoom-Slider verfügbar. Die Statusleiste lässt sich in der Registerkarte „Tools" aktivieren/deaktivieren.

* Die eSafety Komponente und Cloud stehen nur in der NetSupport DNA Version für das Bildungswesen zur Verfügung.

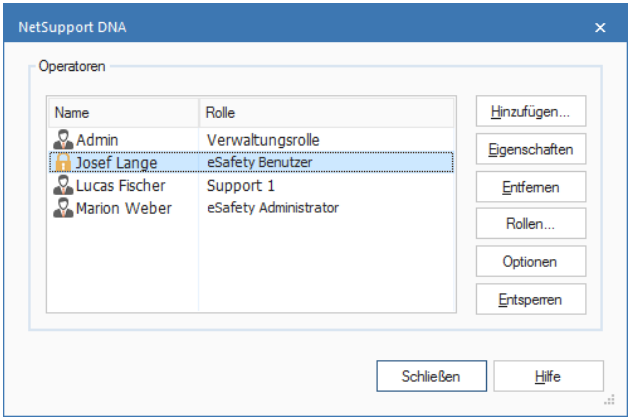
Zusätzliche Konsolebenutzer erstellen

Es können zusätzliche Anmeldungen für Konsolebenutzer erstellt werden. Jedem Benutzer werden Administrator- oder Bedienerrechte zugewiesen, was es Ihnen gestattet, die Funktionalität für gewisse Konsolebenutzer einzuschränken. Operatoren muss eine Rolle zugewiesen werden. Über eine Rolle können Sie die Zugriffsrechte für Benutzer definieren und so auf schnelle Weise mehreren Benutzern die gleichen Rechte zuweisen. Es lassen sich mehrere Rollen erstellen.

Um die Konsolensicherheit zu erhöhen, kann Sicherer Modus aktiviert werden. Dieser zwingt Konsolenbenutzer, komplexe Passwörter zu benutzen. Sie können vorgeben, woraus die sicheren Passwörter bestehen müssen und können die Option wählen, Bedienerkonten nach drei erfolglosen Anmeldeversuchen zu sperren.

Hinweis: In der NetSupport DNA Version für das Bildungswesen können Konsolenbenutzer beim Hinzufügen von Kontakten in der eSafety Funktion erstellt werden. Diesen Benutzern wird eine eSafety-Rolle zugewiesen worden sein, und sie können nur im eSafety-Benutzer konfigurieren Dialog bearbeitet oder gelöscht werden.

1. Wählen Sie in der Registerkarte Einstellungen das Symbol **Operatoren**. Das Dialogfeld "Konsolebediener" wird eingeblendet.



2. Um neue Operatoranmeldungen zu erstellen und diesen die entsprechende Rolle zuzuweisen, klicken Sie auf **Hinzufügen**. Wenn Sie einen vorhandenen Benutzer bearbeiten möchten, wählen Sie

seinen Namen und klicken auf **Eigenschaften**. Um Rollen zu erstellen oder zu bearbeiten, klicken Sie auf **Rollen**.

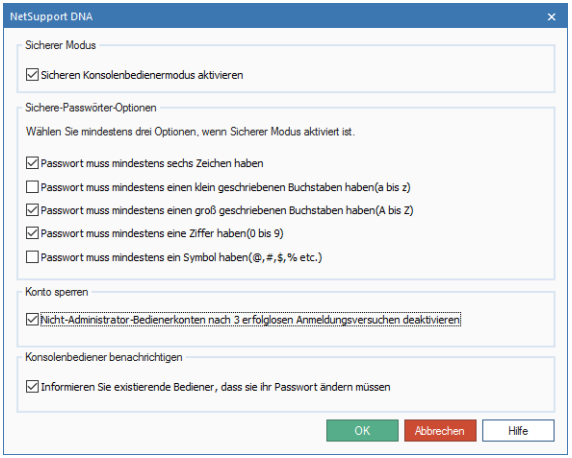
3. Um Sicheren Modus zu aktivieren und den geforderten Grad der komplexen Passwörter festzulegen, klicken Sie auf **Optionen.**
4. Um ein Objekt zu entfernen, wählen Sie seinen Namen und klicken auf **Entfernen**.
5. Von hier aus können deaktivierte Bedienerkonten wieder aktiviert werden. Wählen Sie den gesperrten Bediener, klicken Sie auf **Entsperren** und stellen Sie das Passwort zurück (der Bediener kann dieses bei der nächsten Anmeldung ändern).

Hinweis: Nur ein Konsolebediener besitzt die Zugriffsrechte zum Ändern der Konfigurationseinstellungen, wenn mehrere Bediener gleichzeitig angemeldet sind.

Sicherer Modus

Der Sichere Modus zwingt Konsolenbediener/Innen, komplexe Passwörter zu benutzen, um die Sicherheit der DNA Konsole zu erhöhen. Wenn diese Option aktiviert wird, muss der angemeldete Administrator sein Passwort sofort ändern, und andere Benutzer müssen ihre ändern, wenn sie sich beim nächsten Mal an der Konsole anmelden.

1. Wählen Sie in der Registerkarte Einstellungen das Symbol **Operatoren**.
2. Klicken Sie im Konsolenbediener-Dialog auf **Optionen**.
3. Nun erscheint der Dialog für den Sicheren Modus.



Sicherer Modus
Aktivieren Sie den Sicheren Modus für Konsolenbediener.

Optionen für Sicheres Passwort
Wählen Sie, welche Optionen Sie für die Erstellung komplexer Passwörter einsetzen möchten. Es müssen mindestens drei Optionen gewählt werden.

Konto deaktivieren
Diese Option deaktiviert die Konten von Nicht-Administratoren, wenn das Passwort dreimal erfolglos eingegeben worden ist.

Konsolenbediener benachrichtigen
Die Konsolenbediener werden per Email benachrichtigt, dass sie ihr Passwort beim nächsten Anmelden auf ein sicheres Passwort ändern müssen.

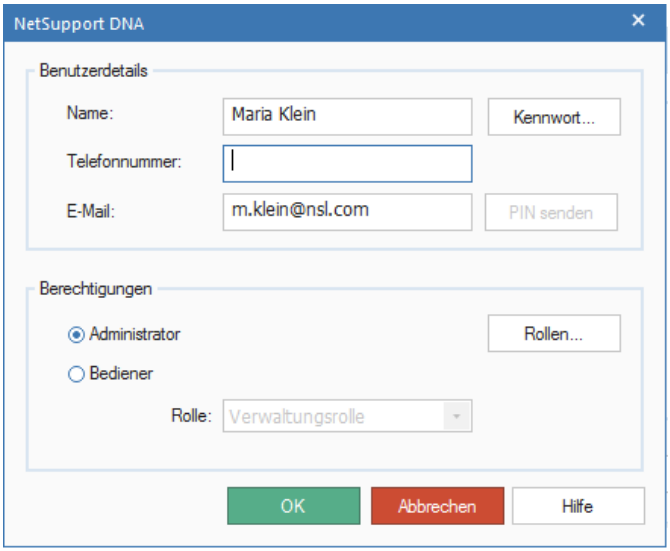
Hinweis: Email-Benachrichtigungen können erst gesandt werden, wenn die Email-Einstellungen konfiguriert worden sind.

Erstellen oder Bearbeiten von Anmeldungen für Konsolebediener

Mit diesem Dialogfeld lassen sich zusätzliche Anmeldungen für Konsolebediener erstellen oder bearbeiten.

1. Geben Sie den Benutzernamen ein, der gleichzeitig als Anmeldenamen dient, sowie die Kontaktnummer und E-Mail-Adresse des Benutzers.

Hinweis: Es muss eine einmalige Emailadresse für den Konsolenbediener eingegeben werden.



2. Klicken Sie auf **Kennwort**, um das Kennwort für vorhandene Bediener zu ändern (erscheint nur beim Bearbeiten vorhandener Bediener).

Hinweis: Bei der Einstellung eines Passworts wird Ihnen die Option geboten, darauf zu bestehen, dass der Benutzer/In dieses auf eins seiner eigenen Wahl ändert, wenn er sich zuerst anmeldet (Sie können den Benutzer per Email benachrichtigen, dass diese Änderung erforderlich ist). Durch Aktivierung des Sicherern Modus können Bediener gezwungen werden, komplexe Passwörter zu benutzen.

3. Wenn ein Bediener keine PIN erhalten hat (erforderlich, um sich zum ersten Mal bei der Cloud Konsole* anzumelden), können Sie sie von hier aus senden. Klicken Sie auf **PIN senden**/**PIN erneut senden** (diese Optionen erscheinen nur, wenn die Cloud Konsole aktiviert ist und die Bedienerrolle Zugriff auf die Cloud hat).
4. Sie können vollständige Administratorrechte zuweisen (die übrigen Felder sind nicht verfügbar) oder die Zugriffsebene festlegen, indem Sie Bedienerstatus wählen. Wählen Sie die Rolle, die dem Operator zugewiesen werden soll. Um eine neue Rolle zu erstellen, klicken Sie auf **Rollen**.
5. Klicken Sie auf **OK**, wenn Sie fertig sind. Sie werden zur Registrierung eines Kennworts für den neuen Benutzer aufgefordert.

* Die Funktion steht nur in der NetSupport DNA Version für das Bildungswesen zur Verfügung.

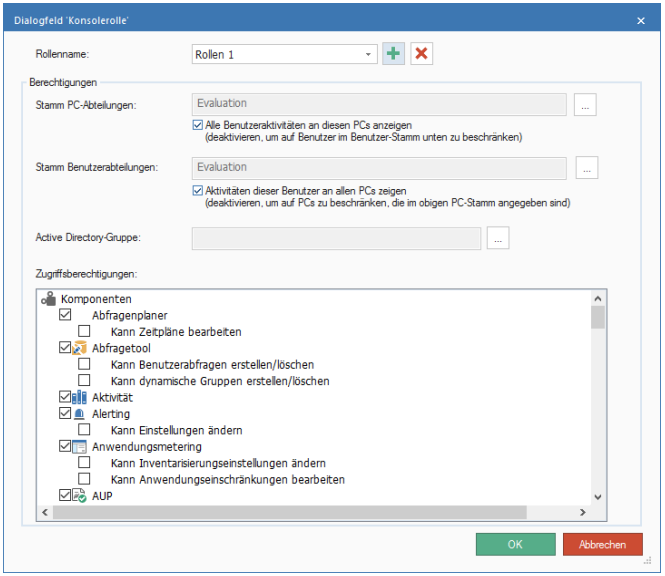
Erstellen oder Bearbeiten von Konsolerollen

Mit diesem Dialogfeld lassen sich Rollen erstellen oder vorhandene bearbeiten. Mit Rollen können Sie die Zugriffsrechte für Operatoren definieren. Nachdem eine Rolle erstellt ist, kann sie auf einfache Weise mehreren Operatoren zugewiesen werden.

Hinweis: Administratoren haben automatisch den vollen Zugriff und es kann ihnen die Administratorrolle zugewiesen werden.

1. Klicken Sie vom Operators-Dialog aus auf **Rollen**. Nun erscheint der Konsolenrollen-Dialog.
2. Klicken Sie auf , um eine neue Rolle zu erstellen, den Namen der Rolle einzugeben und zwischen einem Operator mit schreibgeschütztem Zugriff und einem Administrator-Operator zu unterscheiden. Sie können eine Kopie von einer existierenden Rolle anfertigen. Wählen Sie **Kopie einer Rolle**, und wählen Sie dann die zu kopierende Rolle in der Dropdown-Liste.

Hinweis: Standardmäßig sind beim Operator mit schreibgeschütztem Zugriff die Administrator-Zugriffsrechte deaktiviert und beim Administrator-Operator sind sie aktiviert.



3. Um bessere Kontrolle über die Bedienerrollen zu ermöglichen und darüber, auf welche Bereiche Bediener/Innen Zugriff haben, können Sie die Ebenen in der Strukturansicht wählen, die der Bediener sehen und in denen er arbeiten können soll, wenn er sich anmeldet (Abteilung oder Active Directory Container). Indem Sie auf  klicken, können Sie dies für die PC-Struktur und die Benutzerstruktur einstellen. In der Standardeinstellung können Sie alle Benutzeraktivitäten an den PCs sehen und alle Aktivitäten der Benutzer an jedem PC Ihrer Stammabteilungen. Wenn Sie beispielsweise in Ihrer PC-Stammabteilung die Support-Abteilung gewählt haben, und sich ein Benutzer, der nicht in dieser Abteilung ist, an einem Support-PC anmeldet, können Sie diese Aktivität sehen. Deaktivieren Sie das entsprechende Kontrollkästchen, um Zugriff auf PCs und Benutzer in der Stammabteilung zu beschränken.
4. Wenn die Konfigurationseinstellungen auf Active Directory Container eingestellt worden sind, stellt dies die Ebene ein, auf die der Bediener zugreifen kann.
5. Eine Active Directory Windows-Gruppe kann der Rolle durch Anklicken von  zugewiesen werden. Wenn der Benutzer ein Mitglied der Active Directory-Gruppe ist, wird er vorauthentifiziert, um ohne Einloggen auf die Konsole zugreifen zu können.

   Hinweis: Wenn der Benutzer aus der Active Directory-Gruppe entfernt wird, kann er immer noch auf die Konsole zugreifen, indem er sich mit seinem Benutzernamen und Kennwort einloggt. Sie können die Active Directory-Authentifizierung im DNA-Datenbankassistenten erzwingen, dann kann der Benutzer nur auf die Konsole zugreifen, wenn er im Active Directory authentifiziert ist.
6. Wählen Sie die Komponenten, die vom Operator verwaltet werden sollen.
7. Um eine Rolle zu entfernen, wählen Sie die gewünschte Rolle und klicken auf .
8. Klicken Sie auf **OK**, wenn Sie fertig sind. Die Rolle kann nun einem Operator zugewiesen werden.

Hinweis: In der NetSupport DNA Version für das Bildungswesen stehen zwei eSafetyrollen zur Verfügung, die sich auf die eSafety Funktion beziehen. Die eSafetyrollen können nur beim Hinzufügen von eSafety Kontakten zugewiesen werden. Siehe eSafetyrollen für weitere Informationen.

Suche und Verteilung-Tool

Das NetSupport DNA Suche und Verteilung-Tool ermöglicht es den Netzwerkadministratoren, NetSupport DNA Agent auf mehreren Arbeitsstationen zu installieren und zu konfigurieren, ohne diese Computer einzeln besuchen zu müssen.

Sie können das Netzwerk mit einem IP-Adressenbereich, dem vorhandenen Windows Netzwerk oder Active Directory durchsuchen.

Hinweis: NetSupport DNA bietet ein Tool für Automatische Agent-Ermittlung, mit dem Sie automatisch Geräte finden können, auf denen NetSupport DNA Agent noch nicht installiert ist.

Das NetSupport DNA Suche und Verteilung-Tool kann eingesetzt werden, um an Computer mit den folgenden Betriebssystemen bereitzustellen:

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

Hinweis: Wenn Sie Windows XP Home, Windows Vista Home Premium oder Windows 7 Starter/Home Edition benutzen, wird das NetSupport DNA Suche und Verteilung-Tool auf Grund der Betriebssystembeschränkungen nicht funktionieren.

Wie funktioniert NetSupport DNA Deploy?
Nachdem die Deploy-Optionen konfiguriert worden sind, funktioniert das NetSupport DNA Suche und Verteilung-Tool Hilfsprogramm, indem es die Verbindung mit dem Zielcomputer mit Datei- und Druckfreigabe herstellt.

Diese Methode erfordert Zugriff auf das Admin$ des Zielcomputers und eine Verbindung als Benutzer mit lokalem Administratorzugriff (evtl. werden die Benutzerdaten gefordert).

Nach der Authentifizierung werden die NetSupport DNA Agent Paket-Dateien über die Verbindung mit der Admin$ Freigabe an den folgenden Ordner auf dem Remote-PC kopiert:

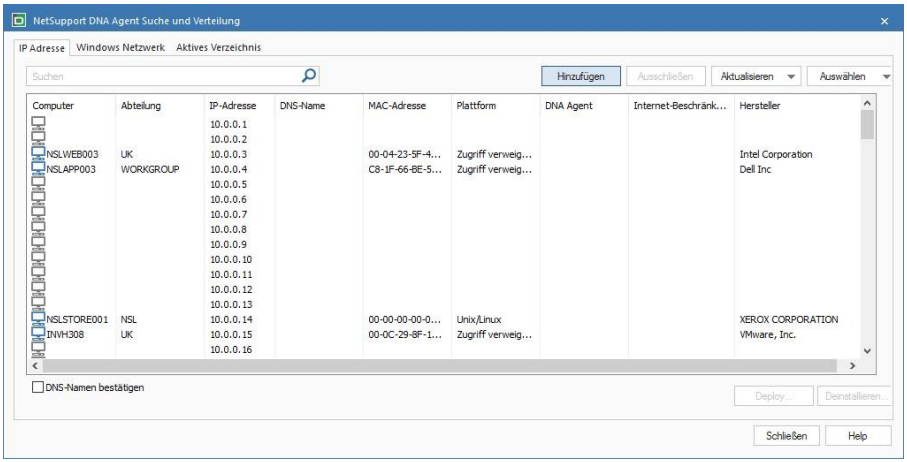
C:\Windows\pcirdist.tmp\

Nachdem die Dateien an den Ziel-PC gesandt worden sind, werden abschließend die Installationsdateien unter Benutzung des Remoteprozeduraufruf- (Remote Procedure Calls - RPC) Service ausgeführt.

Welche Anforderungen gelten?
Um NetSupport DNA Agent Komponenten erfolgreich für Ihren Ziel-PCs bereitzustellen, sind die Folgenden erforderlich:

- Datei- und Druckfreigabe müssen auf dem Ziel-PC aktiviert sein.
- Die Freigabe- und Sicherheitsrichtlinie für lokale Konten muss auf dem Ziel-PC auf {Klassisch} gestellt sein.
- Das Benutzerkonto, das für die Verbindung mit dem Ziel-PC benutzt wird, muss auf dem Ziel-PC Lokale Administratorrechte haben.
- Auf Ziel-PCs mit Windows Vista\7 muss Netzwerkermittlung aktiviert sein.
- UAC Remotebeschränkungen müssen für Ziel-PCs mit Windows Vista und Windows 7 in einer Arbeitsgruppenumgebung deaktiviert werden.

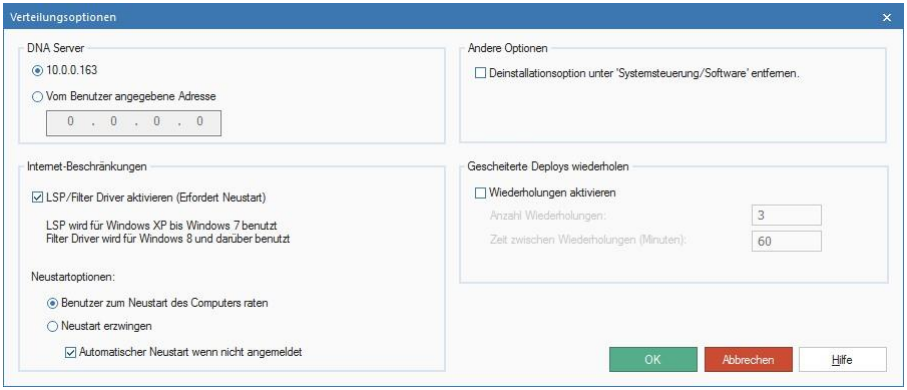
Suchen und Verteilen an PCs



1. Klicken Sie in der Registerkarte **Werkzeuge** auf das Symbol **Suche und Verteilung**. Wählen Sie die Methode zur Suche nach Computern, nach IP-Adresse über das Windows Netzwerk oder Active Directory.

2. Klicken Sie auf **Hinzufügen**.
3. Bei einer Suche nach IP-Adresse geben Sie den Adressbereich ein oder wählen aus einem früheren Eintrag eines IP-Adressbereichs (die letzten zehn Einträge sind gespeichert). Wählen Sie die Netzwerkgruppen, wenn Sie Windows Networking benutzen, oder die aufzunehmenden PCs, wenn Sie Active Directory benutzen.
4. Klicken Sie auf **OK**, um nach übereinstimmenden Computern zu suchen.
5. Um bei der Identifizierung der PCs zu helfen, die in die Verteilung ein- oder aus ihr ausgeschlossen werden sollen, lässt sich die Liste sortieren, indem Sie auf eine beliebige Spaltenüberschrift klicken. Sie können einen individuellen PC schnell finden, indem Sie ihn in das Suchfeld eingeben.
6. Sie können die Liste ggf. auch noch weiter verfeinern, indem Sie Computer entfernen, die Sie nicht in die Verteilung einschließen möchten. Zum Beispiel "ungültige" Agents oder solche, bei denen ein aktueller DNA Agent als bereits installiert identifiziert wurde. Klicken Sie auf Auswählen und wählen Sie in der Dropdownliste die gewünschte Aufgabe. Klicken Sie auf Ausschließen, um die markierten Elemente zu entfernen.
7. Wählen Sie aus den übrigen PCs diejenigen aus, an die verteilt werden soll. Um alle Computer einzuschließen, klicken Sie auf Auswählen – Alle Agents oder markieren mit Umschalt-Klick, Strg-Klick individuelle Objekte.
8. Klicken Sie auf **Deploy**, wenn Sie fertig sind.
9. Da es sein kann, dass die PCs zum Zeitpunkt der Verteilung in Betrieb sind, können Sie vor dem Beginn eine Warnung an die Benutzer senden. Klicken Sie auf **Optionen**. Das Dialogfeld "Verteilungsoptionen" wird eingeblendet.
10. Klicken Sie auf **Start**.
11. Zur entfernten Deinstallation eines DNA Agents klicken Sie auf **Deinstallieren**.

Dialogfeld "Verteilungsoptionen"



DNA Server

Bestätigen Sie die Adresse Ihres DNA Servers

Internet-Beschränkungen *(dieses Feature ist in der Unternehmen Version nicht verfügbar)*

Zur Nutzung der Internetblockierungsfunktionen von DNA wird die Aktivierung von LSP/Filter Driver empfohlen. Unter diesen Umständen muss der Agentcomputer zur Beendung der Installation neu gestartet werden. Ob die Computer in Betrieb sind, bevor Sie Ihre Auswahl treffen:

Neustartoptionen

Benutzer zum Neustart des Computers raten

Gibt dem Benutzer die Möglichkeit zum Neustart seines PCs, wenn er das möchte.

Neustart erzwingen

Es wird ein sofortiger Neustart ohne Warnung erzwungen.

Automatischer Neustart, wenn nicht angemeldet

Diese Option lässt sich mit allen der obigen Neustartoptionen einschließen.

Andere Optionen

Deaktiviert die Deinstallationsoption unter "Programme hinzufügen/entfernen", damit der Benutzer den DNA Agent nicht entfernen kann.

Gescheiterte Deploys wiederholen

Geben Sie an, ob das Deploy nach einem Fehler automatisch wiederholt werden soll. Bestimmen Sie die Anzahl der Wiederholungsversuche und die Pause zwischen ihnen.

Klicken Sie auf **OK**, um mit der Verteilung zu beginnen.

Hinweise:

- Bei der gleichzeitigen Verteilung an über 100 Computer erscheint eine Warnmeldung. Die Verteilung an eine große Anzahl von PCs ist mit potenziellen Overheads verbunden und es kann daher empfehlenswert sein, die Verteilung in mehreren Stadien durchzuführen.
- Es lassen sich gleichzeitig mehrere Deploy-Sitzungen ausführen, was ggf. das Verteilen an zusätzliche PC-Gruppen ermöglicht. Wiederholen Sie einfach den obigen Schritt 1, um ein neues Deploy-Fenster zu öffnen.

Deployment unter Windows XP

Für ein Deploy von NetSupport DNA Agent unter Windows XP Professional müssen Sie auf dem entfernten Rechner den Zugriff auf Admin$ Share haben, um das Paket für das Deploy zu übertragen. Standardmäßig ist der Zugriff auf Admin$ Share nicht erlaubt.

Aktivieren des Netzzugriffs:

1. Wählen Sie unter "Administrative Tools" die Option "Local Security Policy" (Lokale Sicherheitsrichtlinie).
2. Wählen Sie {Security Settings (Sicherheitseinstellungen)}{Local Policies (Lokale Richtlinien)}{Security Options (Sicherheitsoptionen)}
3. Wählen Sie {Network access : Sharing and security model for local accounts (Netzzugriff: Sharing und Sicherheitsmodell für lokale Accounts)}
4. Ändern Sie die Einstellung für diese Richtlinie auf {Classic – local users authenticate as themselves (Classic - lokale Benutzer authentifizieren als sie selbst)}

Admin$ Share ist jetzt verfügbar und Sie können das Deploy nach normalem Muster durchführen.

Bei Aktualisierungen von blockiert Windows Firewall standardmäßig alle Netzwerkaktivitäten durch NetSupport DNA. Damit NetSupport richtig funktioniert, haben wir ein Hilfsprogramm zur Konfiguration von Windows Firewall entwickelt.

Aktivieren von NetSupport DNA in der Windows Firewall-Konfiguration

1. Laden Sie die Datei ICFCONFIG.EXE herunter (Link bei www.netsupportsoftware.com/support)
2. Führen Sie das Hilfsprogramm auf einem Rechner, auf dem NetSupport DNA installiert ist, aus und verwenden Sie folgenden Befehl

   ICFCONFIG -e DNA
3. Hierdurch wird die Windows Firewall-Konfiguration so eingerichtet, dass NetSupport DNA richtig funktioniert.

Mit dem ICFCONFIG-Hilfsprogramm lassen sich auch NetSupport-Produkte aus der Windows Firewall-Konfiguration entfernen. Alle ICFCONFIG-Befehlszeilenoptionen finden Sie unter: www.netsupportsoftware.com/support.

Verteilung unter Windows Vista

Infolge erhöhter Sicherheitseinschränkungen unter Windows Vista kann die Verteilungsfunktion nicht zum Verteilen an Windows Vista-PCs, die nicht zu einer Domäne gehören, verwendet werden.

Bei der Verteilung an einen Windows Vista-PC innerhalb einer Domäne muss der Konsolebenutzer entweder in der Domäne angemeldet sein oder bei entsprechender Aufforderung Anmeldeinformationen eines Domänenkontos mit lokalen Administratorrechten für den Ziel-PC eingeben.

Hinweis: Die Benutzereingabeaufforderung zur Verteilung wird unter Windows Vista nicht unterstützt.

Automatische Agent-Ermittlung

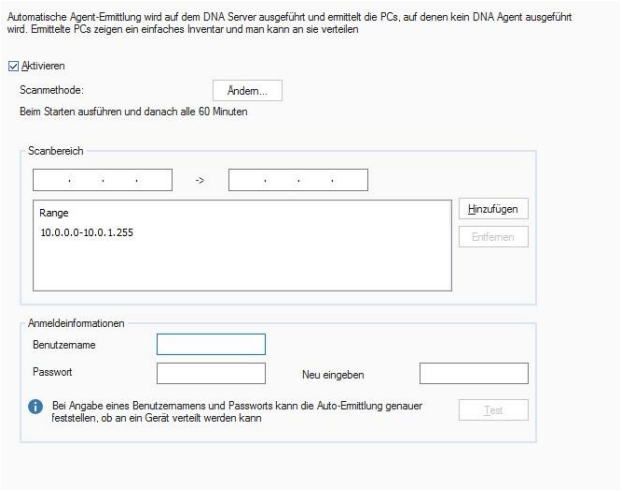
NetSupport DNA ermöglicht es Ihnen, automatisch Geräte im gesamten Netzwerk zu ermitteln, auf denen DNA Agent noch nicht installiert ist. Sie können Scanbereiche erstellen, mit denen Sie automatisch so viele IP-Adressbereiche scannen können wie erforderlich. Wenn der Agent gefunden worden ist, kann ein einfaches Hardware-Inventar angezeigt und ein DNA Agent bereitgestellt werden (an Windows Geräte).

Einstellung eines Scanbereichs

1. Klicken Sie in der Ermittelten Strukturansicht auf dem **Konfigurieren** Symbol.

   Hinweis: Wenn die automatische Ermittlung noch nicht aktiviert worden ist, erscheint im Informationsfenster eine Kopfzeile, die Ihnen dies meldet. Sie können hier auf die Konfigurationseinstellungen zugreifen.

2. Nun erscheinen die Einstellungen der Automatischen Ermittlung.



3. Wählen Sie **Aktivieren** und geben Sie die geforderten IP-Adressenbereiche ein, die gescannt werden sollen.
4. Die Eingabe der Domänen-Anmeldeinformationen ermöglicht es NetSupport DNA festzustellen, ob ein DNA Agent an ein Gerät verteilt werden kann.
5. Klicken Sie **OK**.
6. Ermittelte Computer werden in der Ermittelte-Strukturansicht aufgelistet.

Verwaltung ermittelter Computer

NetSupport DNA wird neue Computer im Netzwerk auch dann ermitteln, wenn der NetSupport DNA Agent gegenwärtig nicht auf ihnen installiert ist.

Neu ermittelte Computer werden unabhängig vom Typ in der Ermittelte-Strukturansicht aufgelistet. Wenn NetSupport DNA jedoch den Computertyp nicht feststellen kann, werden sie separat auf einer 'Unbekannt' Liste aufgeführt, und der Operator kann die Eigenschaften nach Bedarf manuell aktualisieren.

Wenn bei der Suche nach neuen Computern Domänen-Anmeldeinformationen angegeben worden sind, bietet NetSupport DNA ein einfaches Hardware-Inventar, bevor der entsprechende NetSupport DNA Agent installiert wird.

Wenn NetSupport DNA einen neuen Computer ermittelt, erscheint in der Standardeinstellung ein Popup, mit dem Sie darüber benachrichtigt werden. Dies kann in Konsolenanpassungen – Allgemeine Optionen deaktiviert werden.

In der Ermittelte-Liste können Sie wählen, ob der NetSupport DNA Agent an die geforderten Computer verteilt werden soll.

Hinweis: Der NetSupport DNA Agent kann nur an Windows Geräte verteilt werden.

Computer, an die kein Agent verteilt werden soll, können ignoriert werden und werden aus der Liste entfernt. Sie werden jedoch weiterhin im Ermittelte-Computer-Dialog angezeigt. Von hier aus können Sie sie, falls erforderlich, in der Ermittelten Strukturansicht verfügbar machen.

1. Klicken Sie in der Ermittelten Strukturansicht auf dem **Verwalten** Symbol.
2. Nun erscheint der Ermittelte Computer Dialog.
3. Hier sind alle ermittelten Computer aufgelistet.
4. Alle Computer, die ignoriert worden sind, können wieder in die Ermittelte-Strukturansicht aufgenommen werden.

Geräteermittlung

Die SNMP Ermittlungansicht ermöglicht es, NetSupport DNA dafür zu konfigurieren, eine Reihe von Netzwerkadressen zu scannen und alle geeigneten ermittelten Geräte zu melden, wie Drucker und Zugriffspunkte. Diese Posten können dann in DNA gespeichert werden, und die Echtzeitdaten (wie Tinte- oder Tonerstand) können von der Konsole aus überwacht werden.

Hinweis: Vergewissern Sie sich, dass an dem Gerät SNMP aktiviert ist, damit NetSupport DNA es ermitteln kann.

1. In the Geräte-Strukturansicht, klicken Sie auf **Geräteermittlung**.
2. Nun erscheint der SNMP-Überwachung-Dialog.



3. Wählen Sie den gewünschten NetSupport DNA SNMP-Server, der benutzt werden soll, in der Dropdown-Liste. Klicken Sie auf **Mehr**, um die Serverdetails zu zeigen und alle Geräte, die vom Server ermittelt worden sind.

4. Geben Sie den IP-Adressenbereich ein, in dem Sie Geräte scannen möchten und stellen Sie die zu benutzende Sicherheitsebene ein. In der Standardeinstellung benutzt die Standardsicherheitsebene einen 'öffentlichen' Community String und scannt nicht auf v3 Geräte. Um einen neuen Satz von Sicherheitseinstellungen zu erstellen, klicken Sie auf **Bearbeiten**.
5. Klicken Sie auf **Senden, um Geräte zu ermitteln**.

Hinweis: Je nach dem eingegebenen IP-Adressenbereich kann es einige Zeit dauern, bis die ermittelten Geräte zurückgegeben werden.

6. Der Status der Ermittlungsanforderung wird angezeigt. Sie können die vorangehenden Anforderungen scrollen, indem Sie die  Symbole benutzen.

Hinweis: Wenn Sie auf dem Status klicken, erscheint ein Dialog, der die Ermittlungsergebnisse zeigt.

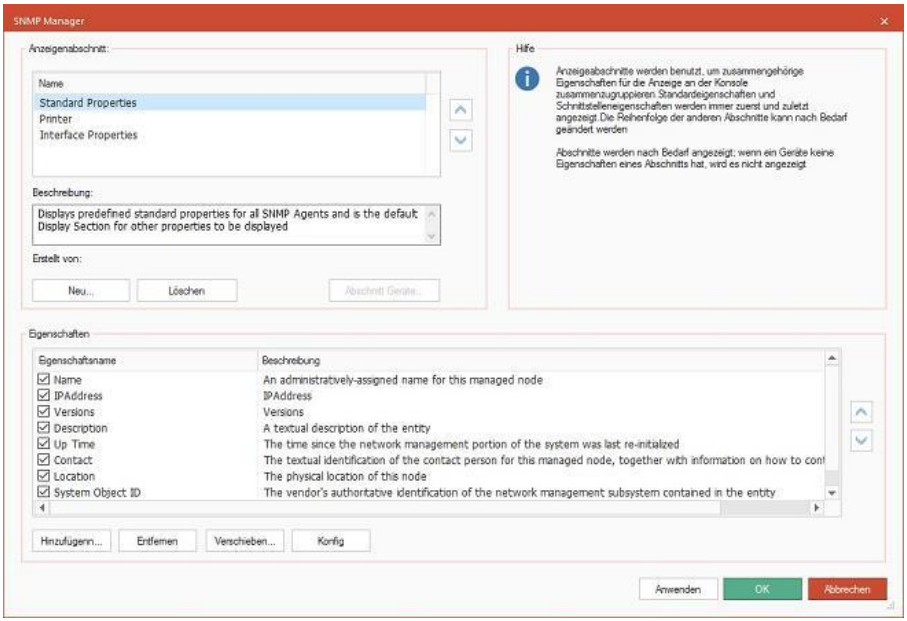
7. Die Scananforderung kann bei Bedarf erneut gesendet werden, indem Sie auf **Erneut senden** klicken.

Anzeigeabschnitte

In der NetSupport DNA Konsole werden verwandte SNMP-Eigenschaften in Anzeigeabschnitten zusammengruppiert. Dieser Dialog ermöglicht es Ihnen, Anzeigeabschnitte und die Eigenschaften darin zu verwalten und zu erstellen.

In der Standardeinstellung gibt es drei Abschnitte: Standardeigenschaften, Drucker-und Benutzeroberflächeneigenschaften.

Hinweis: Die Konsole zeigt einen Abschnitt nur dann, wenn das Gerät irgendwelche seiner Eigenschaften zurücksendet.



Um einen neuen Anzeigeabschnitt zu erstellen, wählen Sie **Neu** und geben Sie einen Namen und eine Beschreibung für den neuen Abschnitt ein.

Sie können sehen, welche Geräte Eigenschaften für einen Abschnitt zurücksenden. Wählen Sie den gewünschten Abschnitt und klicken Sie auf **Geräte im Abschnitt**.

Die Eigenschaften in jedem Abschnitt werden aufgelistet. Um die Reihenfolge zu ändern, in der sie gezeigt werden, klicken Sie auf Symbole

. Um die Eigenschaftenkonfiguration zu bearbeiten, klicken Sie auf **Konfig**. Die Eigenschaftenstatus-Übersicht wird nun angezeigt. Um eine Eigenschaft zu bearbeiten, wählen Sie die gewünschte Eigenschaft und klicken dann auf **Bearbeiten**.

Eigenschaften können von einem Abschnitt zum anderen verschoben werden. Wählen Sie die gewünschte Eigenschaft, klicken Sie auf **Verschieben** und wählen Sie dann den Abschnitt, zu dem die Eigenschaft verschoben werden soll.

Hinweis: Sie können voreingestellte Eigenschaften nicht aus den Standard- oder Benutzeroberflächeneigenschaften-Abschnitten verschieben.

Um neue Eigenschaften hinzuzufügen, klicken Sie auf **Hinzufügen**.

Hinweis: Für Informationen über OID Eigenschaften, besuchen Sie bitte unsere Wissensbasis und lesen Sie den Produktartikel **NetSupport DNA SNMP support** (NetSupport DNA SNMP-Unterstützung).

Integration mit Active Directory

NetSupport DNA wird in Active Directory integriert, sodass die PCs und Benutzer in der DNA Konsole ihre relative Position in der Active Directory Container-Struktur spiegeln können. Innerhalb der AD-Struktur vorgenommene Änderungen werden dann automatisch auch in DNA aufgenommen. Auch Benutzerinformationen lassen sich in Active Directory abrufen.

NetSupport liefert eine gebrauchsfertige Verwaltungsvorlage, NetSupportDNA.ADM. Sie enthält die konfigurierbaren Optionen. Während der Installation von NetSupport wird die Vorlage in den NetSupport DNA-Programmordner kopiert. Sie müssen sie in den Ordner, der alle vorhandenen ADM-Vorlagen enthält, kopieren.

Mit der NetSupportDNA.ADM-Vorlage können Sie die folgenden Policy-Einstellungen für NetSupport DNA konfigurieren: Anschlussverbindungsparameter, NetSupport DNA Server-Adresseigenschaften und Binding von NetSupport DNA-Benutzerdaten.

NetSupport DNA gibt Benutzern die Möglichkeit, sich automatisch ohne Anmeldung bei der DNA-Konsole einzuloggen, basierend auf der Mitgliedschaft in einer Windows-Gruppe. Beim Erstellen einer Konsolerolle können Sie der Rolle eine Active Directory-Windowsgruppe zuweisen. Über diese lässt sich der Benutzer aufgrund seiner Mitgliedschaft authentifizieren.

Hinweis: NetSupport DNA Agent kann mit Hilfe von Active Directory verteilt werden. Weitere Informationen finden Sie unter Installation über Active Directory.

Active Directory-Strukturansicht

Normalerweise zeigt NetSupport DNA die standardmäßige Abteilungsstrukturansicht an. Wenn Sie mit Active Directory arbeiten, kann es sich empfehlen, PCs und Benutzer in derselben Struktur einzublenden.

Hinweis: Der Active Directory Container-Ordner wird standardmäßig in der hierarchischen Strukturansicht angezeigt, aber er lässt sich gegebenenfalls auch ausblenden.

1. Klicken Sie auf dem **Allgemeines** Symbol in der Registerkarte Einstellungen.

2. Der DNA Konfigurationsdialog erscheint; wählen Sie die Option Active Directory Einstellungen.
3. Wählen Sie PCs falls zutreffend im Layout der AD Container und nicht der Abteilungen anzeigen.
4. Agents werden in den AD Container, der ihre Position in der Struktur widerspiegelt, verschoben.

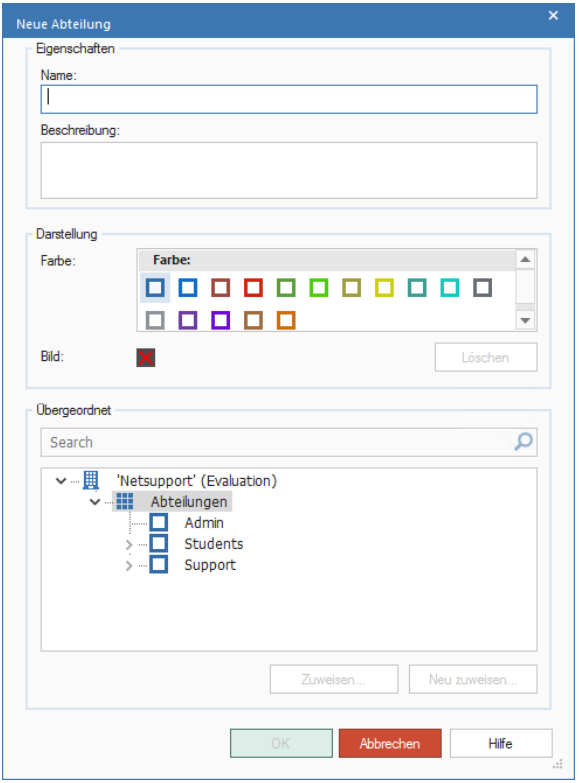
Hinweis: Nach dem Verschieben von Agents in Ihre Directory-Container kann es sein, dass sich vorherige Abteilungseinstellungen nicht auf die Active Directory-Container beziehen. Überprüfen Sie die Komponenten- und Agenteinstellungen um sicherzustellen, dass Sie die richtigen Einstellungen angewendet haben.

Weitere Angaben zur Konfiguration von Active Directory-Policys finden Sie unter www.netsupportsoftware.com/support.

Abteilung erstellen

Die Strukturansicht lässt sich stark konfigurieren, so dass Sie mit Ihrem DNA-Setup die Struktur Ihrer Organisation widerspiegeln können. Sie können Ihre eigenen benutzerdefinierten Bilder anwenden, um die Abteilung in der Strukturansicht stärker hervorzuheben. Abteilungen können manuell hinzugefügt und Agents wunschgemäß zwischen Abteilungen hin- und herverschoben werden.

1. Wählen Sie in der Strukturansicht die Abteilungen oder einen existierenden Abteilungsnamen.
2. Klicken Sie mit der rechten Maustaste und wählen Sie **Neue Abteilung**.
3. Das Dialogfeld "Neue Abteilung" wird eingeblendet.



4. Geben Sie den Abteilungsnamen und eine geeignete Beschreibung ein.

5. Die Darstellung der Abteilung in der Strukturansicht kann vom Benutzer definiert werden. Es kann eine Farbe auf die Abteilung angewendet werden und man kann ihr ein benutzerdefiniertes Bild zuordnen. Klicken Sie auf , um auf das geforderte Bild zu durchsuchen.
6. Beschließen Sie durch Wahl des übergeordneten Objekts, auf welcher Ebene der Strukturansicht die Abteilung eingefügt werden soll. Um auf eine übergeordnete Abteilung zu durchsuchen, geben Sie den Namen oder einen Teil des Namens der Abteilung ein und klicken Sie auf . Nun wird das erste übereinstimmende Element in der Strukturansicht zusammen mit der Anzahl der gefundenen Übereinstimmungen angezeigt. Sie können diese mit den Pfeilen durchblättern. Klicken Sie auf , um die Suche zu löschen.
7. Klicken Sie auf **OK**.

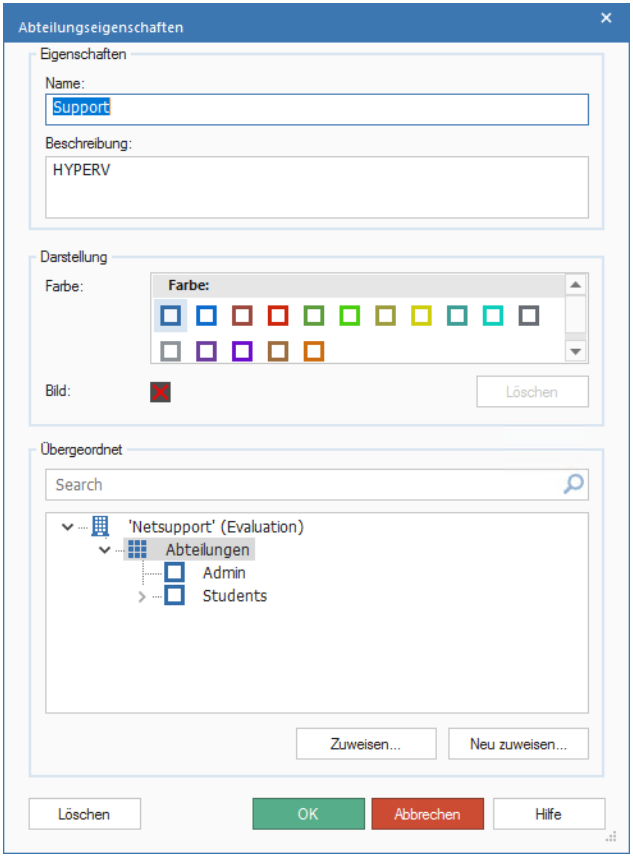
Hinweis: Die Optionen für Zuweisen/Neu zuweisen sind nur aktiv, wenn die Eigenschaften einer existierenden Abteilung bearbeitet werden.

Abteilungseigenschaften ändern

Dieses Dialogfeld lässt sich zu folgenden Zwecken verwenden:

- Allgemeine Eigenschaften der Abteilung ändern;
- Die Darstellung der Abteilung in der Strukturansicht ändern;
- Eine Abteilung mit einem neuen übergeordneten Objekt in der Struktur verknüpfen;
- Eine Abteilung löschen;
- Agent PCs zwischen Abteilungen verschieben.

1. Wählen Sie die gewünschte Abteilung in der Strukturansicht.
2. Klicken Sie mit der rechten Maustaste und wählen Sie **Eigenschaften**.



Eigenschaften

Bei Bedarf können der Abteilungsname und die Beschreibung geändert werden.

Darstellung

Die der Abteilung zugewiesene Farbe kann geändert werden, und wenn ein benutzerdefiniertes Bild hinzugefügt worden ist, kann dies bearbeitet werden (klicken Sie auf dem Bild und wählen Sie ein neues) oder gelöscht werden (klicken Sie auf **Löschen**). Wenn kein Bild zugeordnet ist, können Sie eins hinzufügen, indem Sie auf  klicken.

Übergeordnet

Die Abteilung lässt sich innerhalb der Strukturansicht verschieben. Klicken Sie hierzu auf ein neues übergeordnetes Objekt. Um auf eine übergeordnete Abteilung zu durchsuchen, geben Sie den Namen oder einen Teil des Namens der Abteilung ein und klicken Sie auf . Nun wird das erste übereinstimmende Element in der Strukturansicht zusammen mit der Anzahl der gefundenen Übereinstimmungen angezeigt. Sie können diese mit den Pfeilen durchblättern. Klicken Sie auf , um die Suche zu löschen.

Zuordnen

Ermöglicht es Ihnen, Agents zu der aktuellen Abteilung hinzuzufügen.

Erneut zuordnen

Ermöglicht es Ihnen, Agents aus der aktuellen Abteilung zu verschieben.

Hinweis: Nur Administratoren können Abteilungen erstellen oder PCs aus einer Abteilung in eine andere verschieben.

Löschen

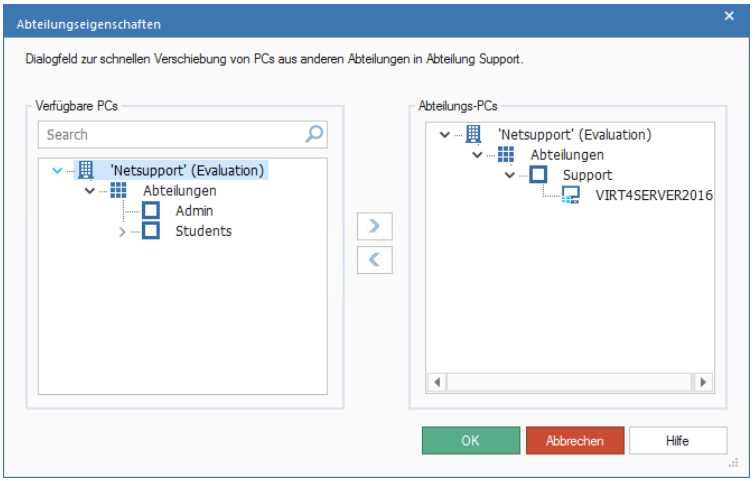
Die gewählte Abteilung kann aus der Struktur gelöscht werden, wenn zur Zeit keine Agents mit ihr verknüpft sind.

Hinzufügen von Agents zu Abteilungen

Beim Installieren eines DNA Agents wird dieser dynamisch zur passenden Domäne in der Konsolestrukturansicht hinzugefügt. Konsolebediener können jedoch die Strukturansicht anpassen, so dass sie zusätzliche Abteilungen enthält, und Agents zwischen diesen Bereichen verschieben.

Ein individueller Agent lässt sich verschieben, indem Sie einfach den gewünschten PC mit der Drag&&Drop-Funktion in der Strukturansicht an den gewünschten Ort bewegen. Oder die Benutzerdetails können bearbeitet werden. Klicken Sie den geforderten Agent in der Strukturansicht rechts an, wählen Sie **Details bearbeiten** und aktualisieren Sie das Abteilungsfeld. Mehrere Agents lassen sich leicht mit der Funktion Zuweisen/Neu zuweisen verschieben.

1. Klicken Sie in der Strukturansicht mit der rechten Maustaste auf die gewünschte Abteilung. Diejenige, in die oder aus der Sie Agents verschieben möchten.
2. Wählen Sie **Eigenschaften**. Die aktuellen Eigenschaften für die gewählte Abteilung werden angezeigt.
3. Klicken Sie auf **Zuweisen** oder **Neu zuweisen**, je nachdem, ob Sie Agent-PCs in die oder aus der Abteilung verschieben möchten.



4. Wählen Sie aus der Liste der verfügbaren PCs den PC, den Sie verschieben möchten,und klicken Sie auf click . Wiederholen Sie den Vorgang für alle weiteren PCs, die Sie verschieben möchten.

Hinweis: Um in der Strukturansicht nach einem Element zu suchen, geben Sie den Namen oder einen Teil des Namens des PCs in dem Suchen-Feld ein und klicken Sie auf . Nun wird das erste übereinstimmende Element in der Strukturansicht zusammen mit der Anzahl der gefundenen Übereinstimmungen angezeigt. Sie können diese mit den Pfeilen durchblättern. Klicken Sie auf , um die Suche zu löschen.

5. Wenn Sie den Agent-PC versehentlich verschoben haben, klicken Sie auf um ihn erneut der ursprünglichen Abteilung zuzuweisen.
6. Klicken Sie auf **OK**, wenn Sie fertig sind.

Dynamische Gruppen

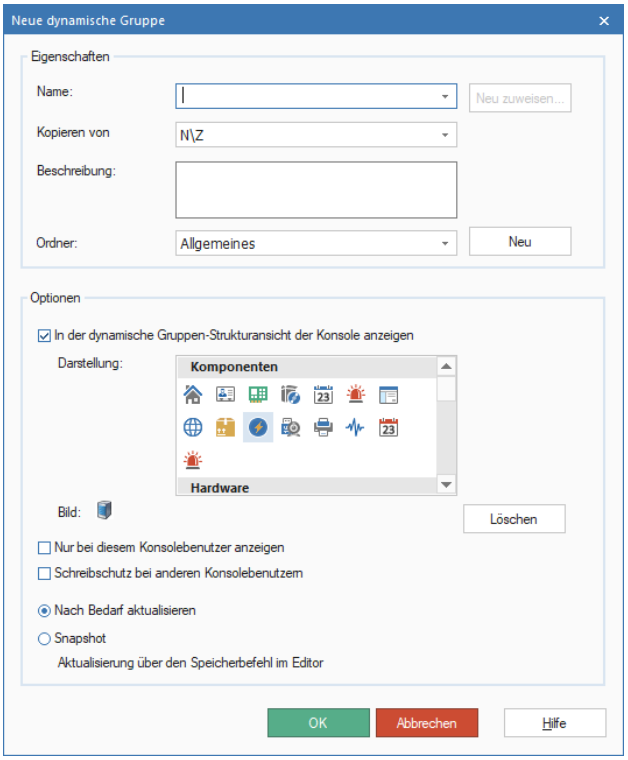
Diese Funktion bietet eine schnelle und einfache Methode zur Gruppierung von Agents aufgrund von spezifischen Bedingungen. Zu typischen Verwendungszwecken gehört die Identifizierung von Benutzern, die abgelaufene Hardware oder Software ausführen.

NetSupport DNA bietet eine Anzahl von vordefinierten Effizienzgruppen und allgemeinen dynamischen Gruppen. Dynamische Gruppen im Zusammenhang mit der Effizienzansicht werden in einem Effizienzordner gespeichert, und alle anderen werden in einem allgemeine Ordner in der Strukturansicht gespeichert. Sie können neue Ordner erstellen, indem Sie Dynamische Gruppen mit der rechten Maustaste anklicken und dann **Neuer Ordner** wählen - oder wenn Sie eine neue Dynamische Gruppe erstellen.

Hinweis: Die Strukturansicht kann gefiltert werden, um nur PCs/Benutzer/Geräte zu zeigen, die mit einer Dynamische-Gruppen-Abfrage übereinstimmen. Wählen Sie die geforderte Dynamische Gruppe in der Strukturansicht, klicken Sie rechts und wählen Sie **Als Filter anwenden**. Nun erscheint eine Filterleiste oben in der Strukturansicht, die zeigt, welcher Dynamische-Gruppe-Filter angewendet worden ist. Um den Filter zu entfernen, klicken Sie auf **Löschen**.

Erstellen einer neuen dynamischen Gruppe

1. Klicken Sie in der Strukturansicht mit der rechten Maustaste auf Dynamische Gruppen und wählen Sie **Neue dynamische Gruppe**.
2. Nun erscheint der Neue Dynamische Gruppe Dialog.



3. Geben Sie einen Namen und eine Beschreibung für die neue Gruppe ein.
4. Sie können eine existierende dynamische Gruppe kopieren (die Bedingungen der ursprünglichen Gruppe werden dann auf die neue dynamische Gruppe angewendet). Wählen Sie die geforderte dynamische Gruppe in der **Kopieren von** Dropdown-Liste.
5. Wählen Sie den Ordner, in dem die dynamische Gruppe gespeichert werden soll, in der **Ordner** Dropdown-Liste. Um einen neuen Ordner zu erstellen, klicken Sie auf **Neu**, geben Sie einen Namen für die Gruppe ein, und klicken Sie auf **OK**.
6. Wählen Sie alle zutreffenden Optionen:

   In der dynamische Gruppen-Strukturansicht der Konsole anzeigen

   Wenn es sich hierbei um eine einmalige Suche nach einer bestimmten Gruppe von PCs handelt, können Sie beschließen, die Gruppe nicht zur Strukturansicht hinzuzufügen.

Darstellung
Wenn eine neue Gruppe in Strukturansicht gezeigt wird, wählen Sie das geforderte Symbol, dass ihr zugeordnet wird. Es steht eine Auswahl von Bildern zur Verfügung. Alternativ können Sie ein benutzerdefiniertes Bild benutzen.

Bild
Um einer neuen Gruppe Ihr eigenes benutzerdefiniertes Bild zuzuweisen, klicken Sie auf  und durchsuchen Sie auf das gewünschte Bild.

Nur bei diesem Konsolebenutzer anzeigen
Wählen Sie diese Option, wenn Sie möchten, dass die neue Gruppe nur bei diesem Konsolebenutzer sichtbar ist.

Schreibschutz bei anderen Konsolebenutzern
Wenn Sie möchten, dass andere Konsolebenutzer die neue Gruppe betrachten, aber keine Änderungen an ihr vornehmen können, wählen Sie den Schreibschutz.

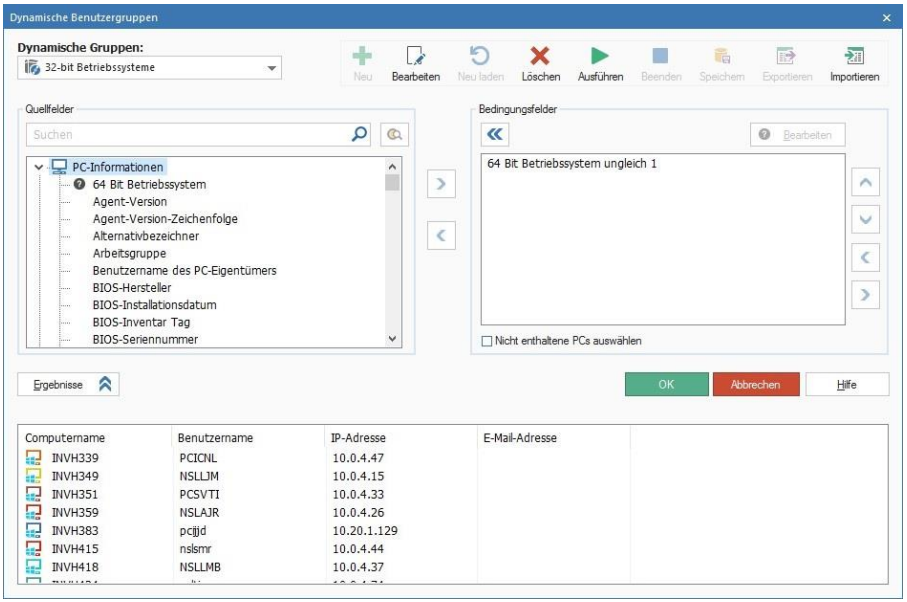
Nach Bedarf aktualisieren
Aktivieren Sie diese Option, wenn Sie möchten, dass neue Agent PCs, welche die Kriterien erfüllen, automatisch zu der Gruppe hinzugefügt werden.

Snapshot. Aktualisierung über den Speicherbefehl im Editor
Statt neue PCs automatisch zu der Gruppe hinzuzufügen, können Sie zu einem bestimmten Zeitpunkt einen Snapshot anfertigen und die Agentliste nach Bedarf aktualisieren. Verwenden Sie hierzu den Speicherbefehl im dynamische Benutzergruppen-Editor.

7. Um die Gruppe einem anderen Konsolebenutzer zuzuweisen, klicken Sie auf **Neu zuweisen**. Diese Funktion ist nur bei Bearbeitung der Eigenschaften einer vorhandenen Gruppe verfügbar.
8. Klicken Sie auf **OK**. Das Dialogfeld für den dynamische Benutzergruppen-Editor wird eingeblendet. Hier können Sie die Bedingung erstellen, die bestimmt, welche Agents für die Gruppe ausgewählt werden.

Dynamische Gruppen-Editor

Das Editor-Dialogfeld dient in erster Linie zum Erstellen der Bedingung, die bestimmt, welche Agents in eine dynamische Gruppe eingeschlossen werden. Sie können die Eigenschaften einer existierenden Gruppe bearbeiten, neue Gruppen erstellen, die Ausgabe von hier aus ausführen und dynamische Gruppen importieren und exportieren.



1. Das Dialogfeld lässt sich beim Erstellen einer neuen Gruppe oder dem Bearbeiten eines vorhandenen Objekts starten.

   Oder

   Klicken Sie mit der rechten Maustaste auf den Namen der dynamischen Gruppe in der Strukturansicht und wählen Sie **Eigenschaften**.

3. Im Dialogfeld können Sie sehen, welche Gruppe geladen ist. Wählen Sie ggf. in der Dropdownliste eine andere Gruppe aus.

   Es sind folgende Optionen verfügbar:

   Neu

   Dient zum Erstellen einer neuen dynamischen Gruppe.

Bearbeiten
Dient zum Ändern der Eigenschaften einer vorhandenen dynamischen Gruppe.

Neu laden
Hiermit können Sie die gespeicherte Version der Gruppeneigenschaften neu laden, wenn Sie alle vorgenommenen Änderungen ignorieren möchten. Diese Option ist nicht mehr verfügbar, nachdem die Ergebnisse ausgeführt wurden.

Löschen
Dient zum Löschen der aktuell geladenen dynamischen Gruppe.

Ausführen
Dient zum Ausführen der Ergebnisse der aktuell geladenen dynamischen Gruppe. Objekte, welche die angegebene Bedingung erfüllen, sind im Ergebnisfenster aufgeführt. Sie können die Ausgabe ein- oder ausblenden, indem Sie auf die Schaltfläche **Ergebnisse** klicken.

Beenden
Hiermit können Sie die Ausführung der Ergebnisse abbrechen.

Speichern
Wenn Sie sich bei der Eingabe der allgemeinen Eigenschaften für die Gruppe zum Erstellen eines Snapshots entschieden haben, d. h. dass alle neuen Agents, welche die Kriterien erfüllen, nicht automatisch zu der Gruppe hinzugefügt werden, können Sie die Agentliste durch Klicken auf **Speichern** aktualisieren.

Exportieren
Exportieren der dynamischen Gruppe an eine .XML Datei.

Hinweis: Sie können nur benutzerdefinierte dynamische Gruppen exportieren.

Importieren
Ermöglicht es Ihnen, eine dynamische Gruppe zu importieren.

Hinweis: Sie können keine dynamischen Gruppen importieren, die über Datenbankwartung exportiert worden sind.

Angeben der Bedingungsfelder

1. Wählen Sie in der Strukturansicht der Quellfelder das/die Feld(er), auf dem/denen die Bedingung beruhen soll. Klicken Sie auf  um die Objekte nacheinander in das Fenster "Bedingungsfelder" zu verschieben. Sie können durch Anklicken von  die aktuellen Werte für das Feld betrachten.
2. Der Bedingungseditor wird eingeblendet. Es lassen sich mehrere Bedingungen anwenden. Geben Sie sie nacheinander ein und klicken Sie auf **OK**.
3. Klicken Sie auf **Ausführen**, um die Ergebnisse abzurufen. Die dynamische Gruppe ist, zusammen mit den Agents, welche die Bedingung erfüllen, in der Konsolestrukturansicht aufgeführt.

Hinweis: Es kann manchmal sein, dass Sie schnell PCs betrachten möchten, welche die angegebene Bedingung nicht erfüllen. Im obigen Beispiel sind im Rahmen der Bedingung Agents markiert, auf denen Windows XP installiert ist, aber bei der Planung von wichtigen Einführungen kann es sein, dass Sie diese Bedingung umkehren und Agents einblenden möchten, auf denen es nicht installiert ist. Markieren Sie **Nicht in dieser Abfrage enthaltene PCs wählen**, um diese Option zu aktivieren, und klicken Sie zur Anzeige der Ergebnisse auf "Ausführen".

NetSupport DNA Konfiguration

Profile

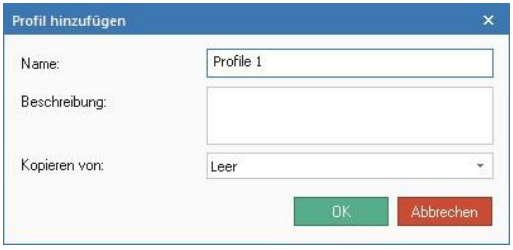
Um Ihnen maximale Flexibilität zu bieten, ermöglicht NetSupport DNA es Ihnen, mehrfache Profile für verschiedene Gruppen von Geräten oder Benutzern zu erstellen, jede mit eigenen spezifischen Komponenteneinstellungen. Dieses Profil kann auf Benutzer-, Active Directory Gruppen-, PC- und Abteilungsebene zugewiesen werden. Es steht ein Standardprofil zur Verfügung, das für alle Agents angewandt wird, denen noch kein Profil zugewiesen worden ist. Dieses Profil kann nicht entfernt werden, aber seine Einstellungen können geändert werden.

Hinweise:

- Profile, die auf Benutzerebene zugewiesen werden, setzen Profile, die auf anderen Ebenen zugewiesen worden sind, außer Kraft.
- Welches Profil den Agents zugewiesen ist, können Sie in Explorer-Modus und Detailansicht sehen, und wenn ein Agent gewählt ist, auch in der Strukturansicht in der PC- oder Benutzer-Registerkarte, die dann erscheint.
- Zugriff auf die Konsoleneinstellungen erhalten Sie über das Symbol Allgemeines auf der Registerkarte Einstellungen.
- Wenn Sie ein Upgrade von Version 4.40 ausführen, werden alle vorherigen Abteilungseinstellungen importiert, und es wird ein Profil erstellt, in dem diese enthalten sind.

Neues Profil erstellen

1. Klicken Sie auf der Registerkarte Einstellungen auf dem **Neues Profil erstellen** Symbol.
2. Nun erscheint der Profil hinzufügen Dialog.

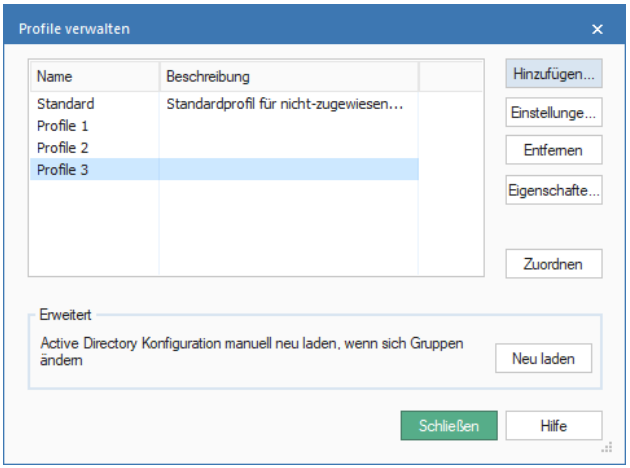


3. Geben Sie den Namen und die Beschreibung für das Profil ein. Sie können vorhandene Profile kopieren, indem Sie das relevante Profil in der Dropdownliste wählen.
4. Klicken Sie auf **OK**.

5. Nun erscheint der Einstellungen-Dialog. Konfigurieren Sie die geforderten Komponenten-Einstellungen und klicken Sie auf **Speichern**.
6. Der Profilzuweisung-Dialog erscheint. Das Profil kann Benutzern, einer Active Directory Gruppe, PCs und Abteilungen zugewiesen werden. Klicken Sie auf **Zuweisen** neben dem relevanten Bereich; daraufhin erscheint eine Struktur, die es Ihnen ermöglicht zu wählen, wem das Profil zugewiesen werden soll. Klicken Sie auf **OK**.
7. Das neue Profil wird dann im Profile verwalten Dialog aufgelistet.
8. Klicken Sie auf **Schließen**.

Existierende Profile verwalten

1. Klicken Sie in den Registerkarte-Einstellungen auf dem **Existierende Profile verwalten** Symbol.
2. Nun erscheint der Profile verwalten Dialog, der alle existierenden Profile auflistet. Wählen Sie das Profil, das Sie verwalten möchten.



3. Um die Eigenschaften eines Profils zu ändern, klicken Sie auf **Eigenschaften,** und nehmen Sie die gewünschten Änderungen am Namen und an der Beschreibung vor.
4. Um die Einstellungen für ein Profil zu ändern, klicken Sie auf **Einstellungen**.
5. Um zu ändern, wem das Profil zugewiesen ist, klicken Sie auf **Zuweisen**.
6. Um ein Profil zu entfernen, klicken Sie auf **Entfernen**.

Hinweis: Profile können nur gelöscht werden, wenn ihnen nichts zugewiesen ist. Um die Zuweisungen für ein Profil zu löschen, klicken Sie auf **Zuweisen** und dann auf **Löschen**.

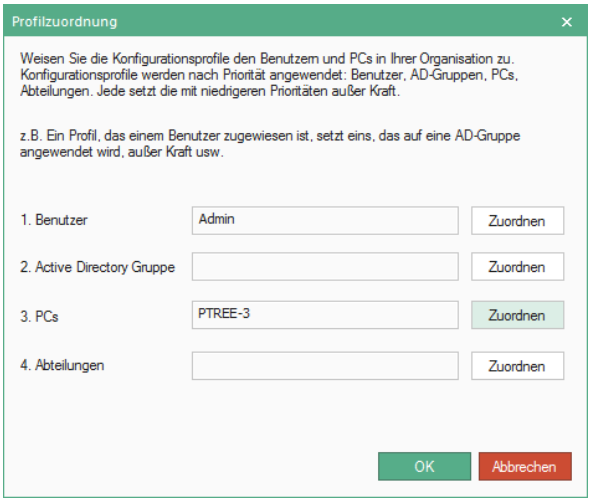
7. Klicken Sie auf **Neu laden,** um die Active Directory Konfiguration manuell neu zu laden, wenn Gruppen geändert worden sind.
8. Klicken Sie auf **Schließen**.

Profile zuweisen

Dieser Dialog ermöglicht es Ihnen, den geforderten Benutzern und PCs in Ihrer Organisation Profile zuzuweisen. Bei der Zuweisung von Profilen wird die folgende Hierarchie benutzt:

Benutzer	Das Profil wird einem mit Windows angemeldeten Benutzer zugewiesen.
Active Directory Gruppe	Das Profil wird Benutzern zugewiesen, die in Active Directory Gruppen enthalten sind.
	Hinweis: Wenn Sie einer Active Directory Gruppe ein Profil zuweisen, wird es nur auf Benutzer angewendet, die ein Mitglied der Active Directory Gruppe sind, und nicht auf: Kontakte, Dienstleistungskonten, Computer, Verteilergruppen oder andere Objekte. Die Profile werden nicht auf Mitglieder von Gruppen angewendet, die diese Gruppe als ihre Primäre Gruppe haben.
PCs	Das Profil wird einem PC zugewiesen.
Abteilungen	Das Profil wird einer Abteilung zugewiesen, und die PCs in dieser Abteilung erben dieses Profil.

Hinweis: Benutzer, denen auf Benutzer- oder Active Directory Ebene kein Profil zugewiesen worden ist, erben das Profil der Abteilung, zu der sie gehören (wenn der Abteilung ein Profil zugewiesen worden ist).



Klicken Sie auf **Zuweisen** neben dem relevanten Bereich; daraufhin erscheint eine Struktur, die es Ihnen ermöglicht zu wählen, wem das Profil zugewiesen werden soll. Klicken Sie auf **OK**.

Um alle Zuweisungen für das Profil zu löschen, klicken Sie auf **Löschen**.

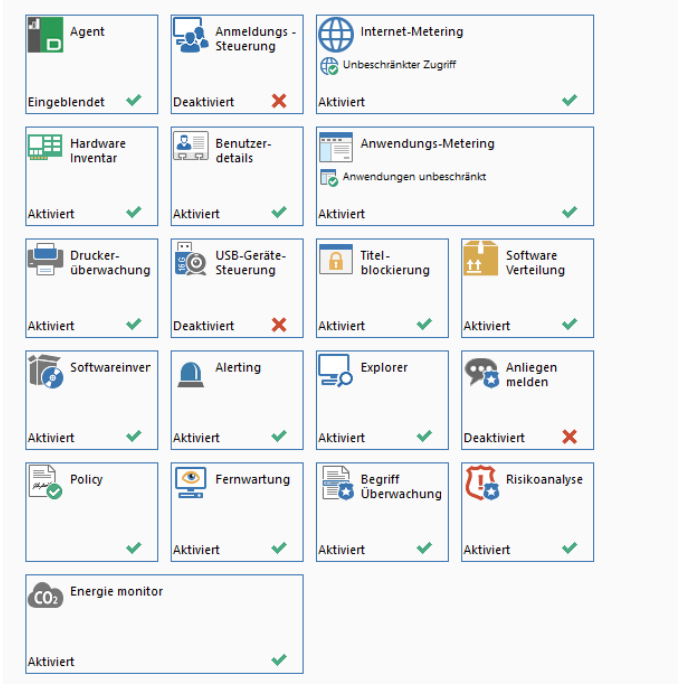
NetSupport DNA-Einstellungen

Der NetSupport DNA Konfigurator ermöglicht es Administratoren/Konsolenbedienern, auf jede der primären Funktionen von NetSupport DNA spezifische Einstellungen anzuwenden (die auf Benutzer-, Active Directory Gruppe-, PC oder Abteilungsebene zugewiesen werden können). Die Häufigkeit, mit der Inventardaten gesammelt werden, kann zum Beispiel auf individueller Abteilungsebene eingestellt werden, oder Sie können den Zugriff auf gewisse Websites durch bestimmte Benutzer blockieren.

Sie erhalten Zugriff auf die NetSupport DNA Konfigurationseinstellungen, wenn Sie Profile erstellen oder verwalten.

Hinweise:

- Zugriff auf die Konsoleneinstellungen erhalten Sie über das Symbol Allgemeines auf der Registerkarte Einstellungen.
- SNMP Komponenteneinstellungen stehen über die Geräte-Strukturansicht zur Verfügung; wählen Sie die Registerkarte Einstellungen und klicken Sie auf **Allgemeines**.

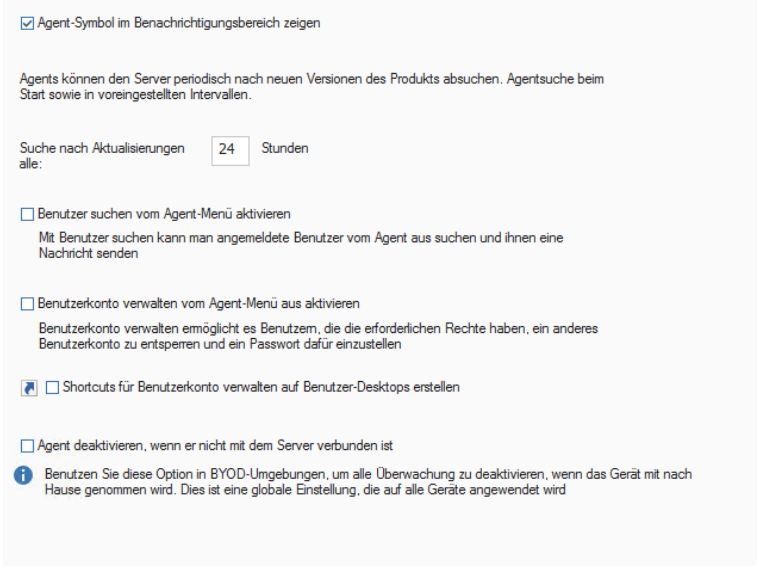


Es wird ein Überblick der Einstellungen für jede Komponente gezeigt, so dass Sie erkennen können, welche Komponenten gegenwärtig aktiviert sind. Dort wo Änderungen getätigt aber nicht gespeichert worden sind, erscheint ein gelber Stern. Wenn Änderungen an einer Komponente vorgenommen aber nicht gespeichert worden sind, erscheint ein gelber Indikator.

Wenn Sie ein Symbol anklicken, gelangen Sie zu den Einstellungen für den betreffenden Bereich.

Klicken Sie auf **Speichern**, um alle Änderungen zu speichern. Um zu den Standardeinstellungen zurückzugehen, klicken Sie auf **Zurücksetzen**.

Agent



Agentsymbol zeigen

Wenn diese Option aktiviert ist, wird das Agentsymbol in der Taskleiste auf dem Agent PC eingeblendet.

Alle *xx* Stunden nach Aktualisierungen suchen

Bei jedem Beginn eines DNA Agent-Services wird der Server automatisch nach aktualisierten Komponenten abgesucht. Während Agents aktiv sind, können Sie auch die Häufigkeit einstellen, mit der sie den Server abfragen. Wenn Sie zum Beispiel ein großes Netzwerk haben, kann es

empfehlenswert sein, dass Agents nur ein- bis zweimal täglich nach Aktualisierungen suchen. Oder wenn andererseits Aktualisierungen verfügbar sind, möchten Sie u. U., dass Agents häufiger nach diesen suchen.

Benutzer suchen vom Agent-Menü aktivieren

Ermöglicht es Agents, angemeldete Benutzer zu suchen und ihnen eine Nachricht zu senden.

Benutzerkonto verwalten im Agent-Menü aktivieren

Agents können vom Agent-Menü aus auf die Benutzer verwalten Funktion zugreifen; von hier aus können sie ein anderes Benutzerkonto entsperren und Passwörter dafür einstellen (wenn sie die erforderlichen Rechte haben).

> **Shortcuts für Benutzerkonto verwalten auf Benutzer-Desktops erstellen**
>
> Hiermit wird ein Shortcut für die Benutzerkonto verwalten Funktion auf den Benutzer-Desktops erstellt.

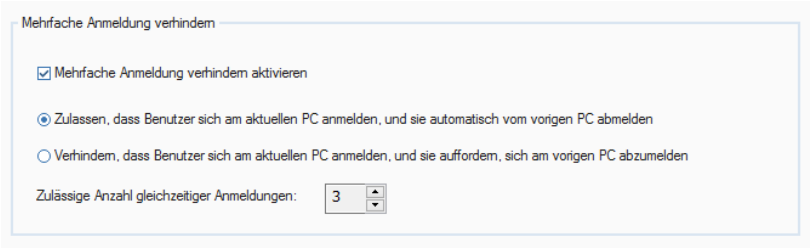
Agent deaktivieren, wenn er nicht mit dem Server verbunden ist

Wenn der Agent sich nicht mit dem DNA Server oder Agent Gateway verbinden kann, wird er deaktiviert, und es werden keine Überwachungsdaten gesammelt. Dies kann nützlich sein, wenn Sie keine Überwachungsdaten vom Agent sammeln möchten, wenn das Gerät mit nach Hause genommen wird.

Hinweise:

- Dies ist eine globale Einstellung, die für alle Geräte gilt.
- Diese Option wird auf Terminaldiensten nicht unterstützt.

Anmeldungssteuerung

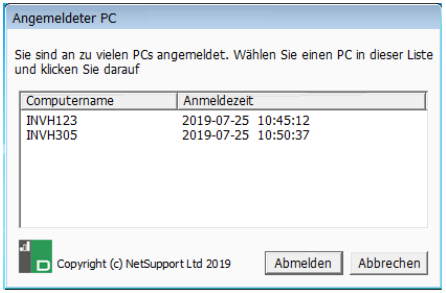


Mehrfache Anmeldung verhindern
Es kann Situationen geben, in denen ein Benutzer an mehr als einem PC gleichzeitig angemeldet sein muss. NetSupport DNA bietet Ihnen die Flexibilität, die Anzahl der für einen individuellen Benutzer zulässigen gleichzeitigen Anmeldungen einzustellen, und zwar für maximal 5 Geräte.

Hinweis: Diese Funktion wird nur für Domänen Windows Konten unterstützt, und steht nicht für Terminaldienst/RDP Sitzungen zur Verfügung.

Mehrfache Anmeldung verhindern aktivieren
Wenn dies aktiviert ist, können Sie wählen, wie mehrfache gleichzeitige Anmeldungen gehandhabt werden sollen:

Zulassen, dass Benutzer sich am aktuellen PC anmelden, und sie automatisch vom vorigen PC abmelden
Wenn der Benutzer versucht, die Anzahl der vorgegebenen gleichzeitigen PC-Anmeldungen zu überschreiten, wird er aufgefordert, einen der anderen PCs zu wählen, um sich aus diesem abzumelden. Wenn keine Anzahl von mehr als 1 vorgegeben wurde, wird die zweite Anmeldung zugelassen, aber der erste PC wird automatisch abgemeldet.



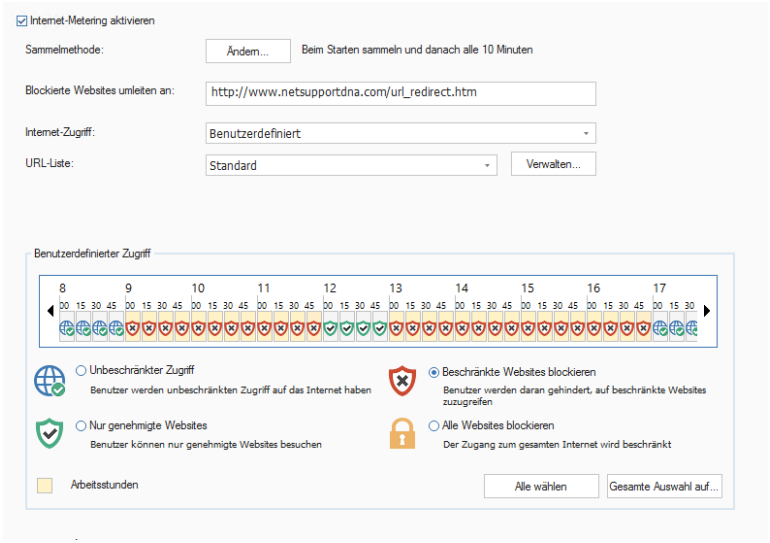
Hinweis: Der Benutzer wird auch dann am ersten PC abgemeldet, wenn das Gerät gesperrt ist, und Arbeit am ersten PC, die nicht gespeichert worden ist, geht verloren.

Verhindern, dass Benutzer sich am aktuellen PC anmelden, und sie auffordern, sich am vorigen PC abzumelden
Wenn der Benutzer in dieser Situation versucht, die vorgegebene Anzahl gleichzeitiger PC-Anmeldungen zu überschreiten, muss er sich manuell von einem der anderen PCs abmelden, um fortfahren zu können.

Zulässige Anzahl von gleichzeitigen Anmeldungen
Sie können dies für einen individuellen Benutzer auf maximal 5 gleichzeitige Netzwerkanmeldungen einstellen. Wenn eine Person versucht, sich mit denselben Anmeldeinformationen für ein Gerät mehr anzumelden als die vorgegebene Grenze, erscheint eine Warnung wie oben.

Internet-Metering- Einstellungen

Mit dem Internet-Metering können Bediener die Internetnutzung der Agents überwachen und einschränken. Sie haben die Möglichkeit, das Metering ein- oder auszuschalten und den Zugriff auf designierte Sites einzuschränken.



Internet-Metering aktivieren
Wenn Sie die Markierung dieses Feldes aufheben, wird das Internet-Metering ausgeschaltet.

Sammeln-Methode:
In der Standardeinstellung sammelt Internet-Metering Daten, wenn NetSupport DNA Agent startet und danach alle zehn Minuten. Klicken Sie auf **Ändern**, um die Einstellungen auf benutzerdefinierte Sammelzeiten ändern.

Hinweis: Wir empfehlen ein angemesseneres Intervall von 30 Minuten für die Datensammlung als Richtschnur, um die Genauigkeit der angezeigten Daten und den erhöhten Netzwerkverkehr von den DNA Agent-Maschinen gegeneinander auszubalancieren.

Blockierte Sites umleiten zu xxxxxxx
Geben Sie eine URL ein, zu der die Agents umgeleitet werden, wenn sie versuchen, eine blockierte Site zu besuchen.

Internetzugriff
Sie können nicht nur die Verwendung des Internets überwachen, sondern Agents auch daran hindern, bestimmte Sites zu besuchen. Wählen Sie die geforderte Zugriffsebene in der Dropdownmenü-Liste: Sie können wählen zwischen Unbeschränkter Zugriff, Zugriff jederzeit blockieren, Zugriff während der Bürozeiten oder außerhalb der Bürozeiten beschränken oder blockieren. Durch Auswahl von „Angepasst" lässt sich der Zugriff an Ihre eigenen Bedürfnisse anpassen.

URL-Liste
Einem Profil kann eine URL-Liste (eine Liste der genehmigten und/oder eingeschränkten Websites) zugewiesen werden. Wählen Sie die geforderte Liste im Dropdownmenü. Um Listen zu erstellen oder zu verwalten, klicken Sie auf **Verwalten**.

Hinweis: Damit die Liste aktiviert werden kann, muss die Internetzugriffsstufe auf eine der 'Eingeschränkter Internetzugriff' Optionen eingestellt sein. Oder, wenn benutzerdefinierter Zugriff benutzt wird, muss 'Genehmigte Websites' oder 'Eingeschränkte Websites blockieren' aktiviert sein.

Benutzerdefinierter Zugriff

Unbeschränkter Zugriff
Agents können zu jeder Tageszeit auf eine beliebige Site zugreifen.

Nur genehmigte Sites
Wenn diese Option aktiviert ist, können Agents nur Sites besuchen, die in der genehmigten Liste aufgeführt sind.

Alle Sites blockieren
Wenn diese Option aktiviert ist, können Agents keine Sites besuchen.

Beschränkte Sites blockieren
Wenn diese Option aktiviert ist, können Agents die Sites in der eingeschränkten Liste nicht besuchen.

Sie können den Internetzugriff von Agents zu bestimmten Tageszeiten einschränken. Wählen Sie die gewünschte Einschränkung und gehen Sie mit Hilfe der Pfeile zur gewünschten Zeit. Klicken Sie auf das gewünschte Segment zur Anwendung des betreffenden Symbols.

Hinweis: Standardmäßig ist der Zugriff nicht eingeschränkt.

Die gegenwärtigen Bürostunden werden gelb schattiert sein. Sie können in Konsolenanpassungen – Allgemein-Einstellungen für Ihre Organisation passend geändert werden.

Klicken Sie auf **Alle auswählen**, um die ausgewählte Einschränkung auf den ganzen Tag anzuwenden, oder auf „Alle Markierungen aufheben", um zum uneingeschränkten Zugriff zurückzukehren.

Hinweis: Diese Einstellungen stehen nur in der NetSupport DNA Version für das Bildungswesen zur Verfügung.

Hardware Inventory



Hardwareinventarisierung aktivieren

Heben Sie die Markierung auf, damit die Hardwareinventarisierung nicht ausgeführt wird.

Scan-Methode

In der Standardeinstellung läuft das Hardwareinventarisierung, wenn NetSupport DNA Agent startet und danach alle zehn Minuten. Klicken Sie auf Ändern, um die Einstellungen auf benutzerdefinierte Scan-Zeiten ändern.

Hinweis: Wir empfehlen ein angemesseneres Laufzeitintervall von 1440 Minuten als Richtschnur, um die Genauigkeit der angezeigten Daten und den erhöhten Netzwerkverkehr von den DNA Agent-Maschinen gegeneinander auszubalancieren.

Benutzerdetails

Agent- und Inventarinformationen lassen sich über das Dialogfeld "Benutzerdetails" aktualisieren.



Die Standardeinstellungen für das Dialogfeld können folgendermaßen geändert werden:

Benutzerdetails aktivieren

Wenn diese Option nicht markiert ist, ist die Funktion zum Zugriff auf das Dialogfeld "Benutzerdetails" an den Rechnern der Agents deaktiviert. Konsolebediener können das Dialogfeld auf Agentcomputern trotzdem noch öffnen.

Beim Start ausführen

Wenn diese Option aktiviert ist, werden unter „Benutzerdetails" Daten gesammelt, sobald der DNA Agent gestartet wird.

Sammeln-Methode:

In der Standardeinstellung sammelt Benutzerdetails Daten, wenn NetSupport DNA Agent startet und danach alle zehn Minuten. Klicken Sie auf **Ändern**, um die Einstellungen auf benutzerdefinierte Sammelzeiten ändern.

Begrüßungsseite zeigen

Das Dialogfeld "Benutzerdetails" umfasst standardmäßig zwei Seiten (Registerkarten), Willkommen und Allgemein. Anwender können zu diesen ggf. benutzerdefinierte Seiten hinzufügen. Heben Sie die Markierung dieses Feldes auf, um die Begrüßungsseite auszublenden.

Zusammenfassungsseite zeigen

Heben Sie die Markierung dieses Feldes auf, um die Zusammenfassungsseite auszublenden.

Begrüßungsnachricht

Wenn die Begrüßungsseite angezeigt ist, können Sie eine benutzerdefinierte Meldung/Eingabeaufforderung hinzufügen.

Begrüßungslogo

Das auf der Begrüßungsseite eingeblendete Standardbild lässt sich durch eine beliebige Bitmap ersetzen. Da die Datei bei der Anfrage nach Benutzerdetails nicht entfernt auf Agentcomputer heruntergeladen wird, muss sie im angegebenen Ordner auf dem Agentrechner oder dem NetSupport DNA-Komponentenordner des Agents gespeichert werden.

Klicken Sie auf **Ändern** und suchen nach der gewünschten Datei.

Anwendungsmetering

Mit dem Anwendungsmetering können Bediener die Anwendungsnutzung der Agents überwachen und einschränken. Sie haben die Möglichkeit, das Metering ein- oder auszuschalten und den Zugriff auf designierte Anwendungen einzuschränken.



Anwendungsmetering aktivieren

Wenn Sie die Markierung dieses Feldes aufheben, wird das Metering ausgeschaltet.

Sammeln-Methode:

In der Standardeinstellung sammelt Anwendungsmetering Daten, wenn NetSupport DNA Agent startet und danach alle zehn Minuten. Klicken Sie auf **Ändern**, um die Einstellungen auf benutzerdefinierte Sammelzeiten ändern.

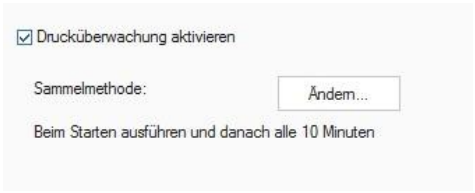
Hinweis: Wir empfehlen ein angemesseneres Intervall von 30 Minuten für die Datensammlung als Richtschnur, um die Genauigkeit der angezeigten Daten und den erhöhten Netzwerkverkehr von den DNA Agent-Maschinen gegeneinander auszubalancieren.

Anwendungseinschränkungen für das Unternehmen

Klicken Sie auf Einschränkungen, um eine Liste mit genehmigten/eingeschränkten Anwendungen zu erstellen, und wählen Sie, ob die Einschränkungen aktiviert oder deaktiviert werden sollen.

Hinweis: Diese Einstellung gilt für das gesamte Unternehmen.

Druckerüberwachungs-Einstellungen



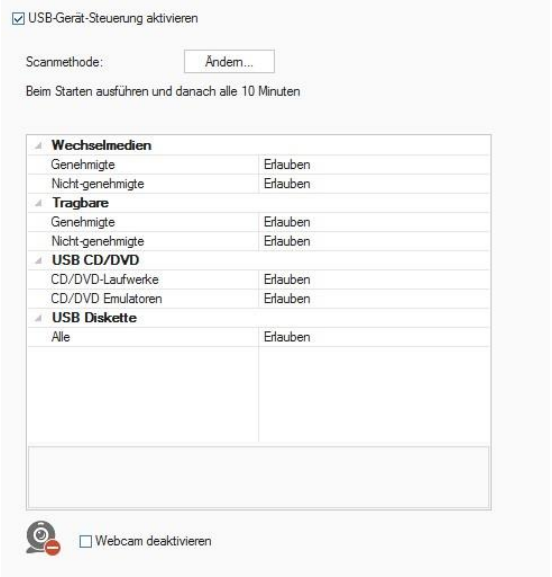
Druckerüberwachung aktivieren
Dieses Kontrollkästchen deaktivieren, um die Druckerüberwachung zu deaktivieren.

Sammeln-Methode:
In der Standardeinstellung sammelt Druckerüberwachung Daten, wenn NetSupport DNA Agent startet und danach alle zehn Minuten. Klicken Sie auf **Ändern**, um die Einstellungen auf benutzerdefinierte Sammelzeiten ändern.

Hinweis: Wir empfehlen ein angemesseneres Intervall von 30 Minuten für die Datensammlung als Richtschnur, um die Genauigkeit der angezeigten Daten und den erhöhten Netzwerkverkehr von den DNA Agent-Maschinen gegeneinander auszubalancieren.

USB-Gerätesteuerungs - Einstellungen

Die Benutzung von USB-Geräten kann gesteuert werden, und von hier aus können Sie den Status von genehmigten und nicht-genehmigten Geräten je nach Typ einstellen.



USB Gerätesteuerung aktivieren
Wählen Sie dieses Kontrollkästchen, um USB-Gerätesteuerung zu aktivieren.

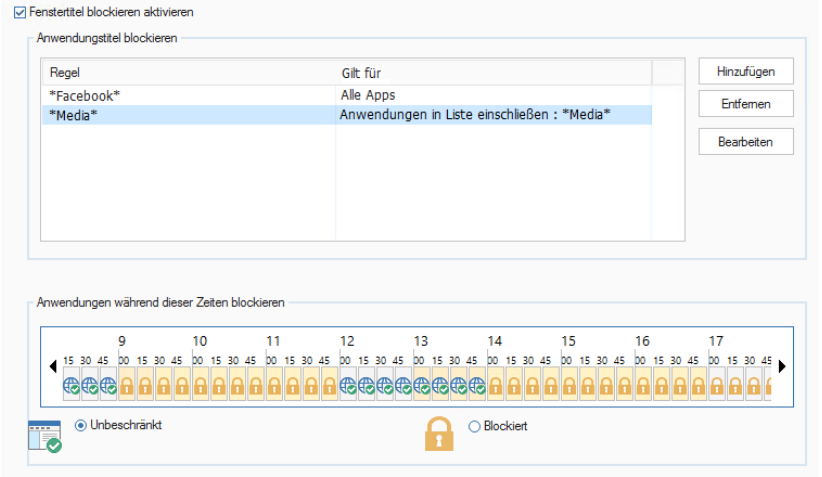
Scan-Methode
In der Standardeinstellung läuft das USB Gerätesteuerung, wenn NetSupport DNA Agent startet und danach alle zehn Minuten. Klicken Sie auf **Ändern**, um die Einstellungen auf benutzerdefinierte Scan-Zeiten ändern.

Sie können die Zugriffsebene je nach Gerätetyp für genehmigte und nicht-genehmigte Geräte einstellen. Die gegenwärtige Zugriffsebene wird angezeigt. Um diese zu ändern, wählen Sie den geforderten Gerätetyp und wählen dann die Zugriffsebene in der Dropdown-Liste. Der Zugriff kann auf vollen Zugriff, Zugriff ganz blockieren, nur schreibgeschützt zulassen oder Ausführung von Anwendungen verhindern eingestellt werden.

Webcam deaktivieren
Wählen Sie diese Option um zu verhindern, dass die Benutzer Webcams benutzen.

Titelblockierung Einstellungen

Zusätzlich zur Beschränkung von Websites und Anwendungen nach ihren spezifischen Namen ist jetzt auch die Blockierung von Apps, Websites und Spielen nach ihrem Fenstertitel möglich.



Es werden Regeln erstellt, die Platzhalter enthalten können, um zu bestimmen, für welche(n) Seitentitel die Blockierung gelten soll, und für zusätzliche Flexibilität steht Ihnen die Option zur Verfügung, benutzerdefinierte Listen zu erstellen, die bestimmte Anwendungen innerhalb einer spezifischen Gruppe einschließen oder ausschließen. Außerdem können Sie auch die Zeiten wählen, während denen diese Regeln gelten sollen.

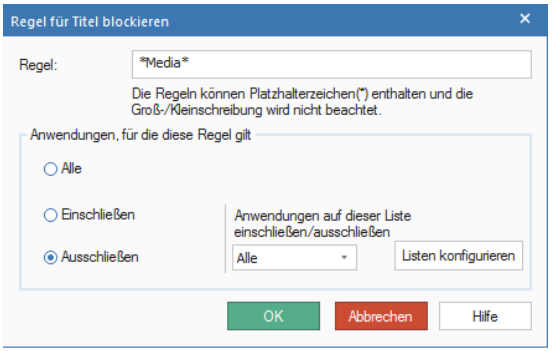
Fenstertitelblockierung aktivieren
Deaktivieren Sie dieses Kontrollkästchen, um die Fenstertitelblockierung auszuschalten.

Hinweis: Für diese Funktion muss Anwendungsmetering aktiviert sein.

Klicken Sie auf **Hinzufügen**, um eine neue Regel (einen neuen Titelnamen) zu erstellen.

Titelblockierung Regel

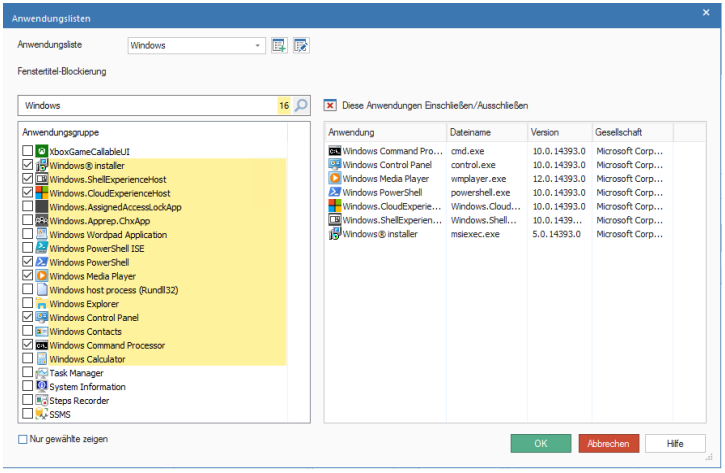
Geben Sie den Titel/die Regel für die Anwendung ein, die Sie blockieren möchten. Sie können Platzhalter benutzen, um sicherzustellen, dass Variationen des Fenstertitel eingeschlossen werden.



Diese Regel kann für alle übereinstimmenden Anwendungen gelten, oder Sie können benutzerdefinierte Listen erstellen, bei denen Sie die Regel wahlweise einschließen oder ausschließen können. Wählen Sie **Einschließen** oder **Ausschließen**, um die Listen zu aktivieren, wählen Sie die geforderte Liste im Dropdownmenü oder klicken Sie auf **Listen konfigurieren**, um eine neue Liste zu erstellen.

Anwendungslisten konfigurieren

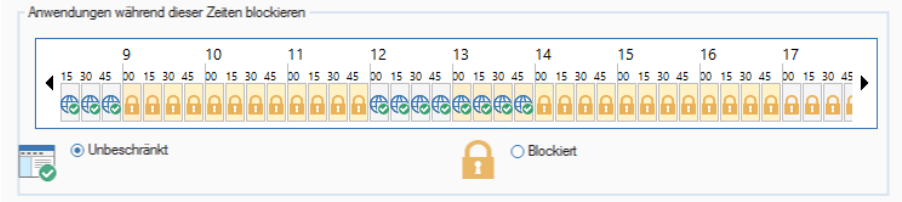
Um eine Titelblockierung-Anwendungsliste zu erstellen oder zu bearbeiten:



Anwendungsliste
Benutzen Sie das **Hinzufügen** oder **Bearbeiten** Symbol, um eine neue Liste zu erstellen oder die Eigenschaften einer existierenden Liste zu ändern. Geben Sie der Liste einen geeigneten Namen.

Fenstertitelblockierung
1. Fangen Sie an, den Namen der Anwendung oder Anwendungsgruppe einzutasten, die Sie in die Liste aufnehmen möchten. Alle übereinstimmenden Elemente werden hervorgehoben.
2. Wählen Sie die geforderten Apps, um zu bestätigen, dass Sie sie in die Liste aufnehmen möchten.
3. Wenn Sie damit fertig sind, klicken Sie auf OK. Sie kehren dann zum Titelblockierungsregel Dialog zurück.
4. Klicken Sie auf OK.

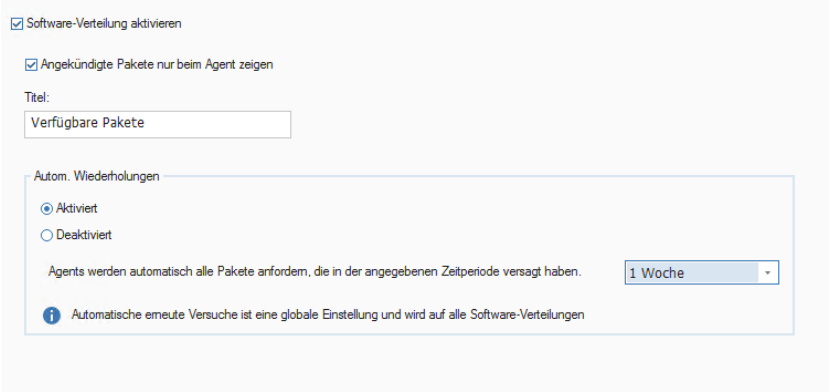
Sie können wählen, wann die Beschränkung/Blockierung gelten soll. Wählen Sie das geforderte Symbol (**Unbeschränkt** oder **Blockiert**), benutzen Sie die Pfeile, um zum gewünschten Zeitrahmen zu scrollen, und klicken Sie dann auf dem anzuwendenden Segment.



Die gegenwärtigen Bürostunden sind gelb schattiert. Diese können in **Konsolenanpassungen – Allgemeine Einstellungen** für Ihre Organisation angepasst werden.

Softwareverteilung

Die Einstellungen der Softwareverteilung bestimmen in erster Linie, ob die Paketanforderungsfunktion auf den Agentcomputern verfügbar ist.



Softwareverteilung aktivieren

Wenn diese Option nicht markiert ist, ist die Paketanforderungsfunktion auf den Agentcomputern deaktiviert.

Beim Agent nur angebotene Pakete zeigen

Mit der Paketanforderungsfunktion können Agents Pakete installieren, die vom Konsolebediener angeboten wurden. Diese werden in einem Dialogfeld, in dem der Agent auswählen kann, aufgelistet. Agents können zwar nur angebotene Pakete installieren, aber durch Deaktivieren dieses Feldes lässt sich eine vollständige Liste der Pakete zur Betrachtung durch die Agents einblenden.

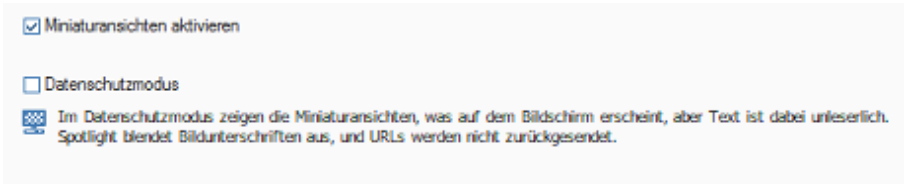
Titel

Sie können im Paketdialogfeld, das auf den Agent PCs eingeblendet wird, einen benutzerdefinierten Titel anzeigen.

Automatische Wiederholungen

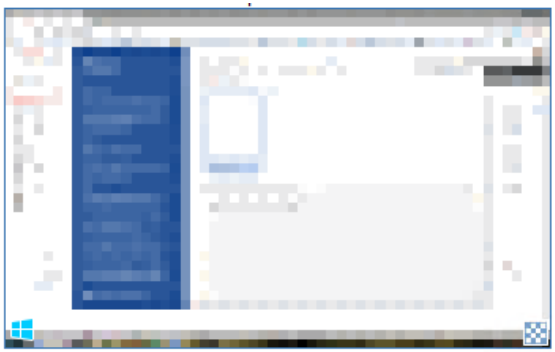
Sie können die automatische Wiederholungsoption ein-/ausschalten und gescheiterte Pakete so erneut verteilen. Die Zeitperiode, in der versagte Pakete noch auf automatische Anforderung für Agents zur Verfügung stehen sollen, kann festgelegt werden (von 1 Tag bis 6 Monate). Wählen Sie die geforderte Zeitperiode in der Dropdownliste.

Explorer



Miniaturansichten aktivieren
Dieses Kontrollkästchen deaktivieren, um die Miniaturansichten-Ansicht in Explorer zu deaktivieren.

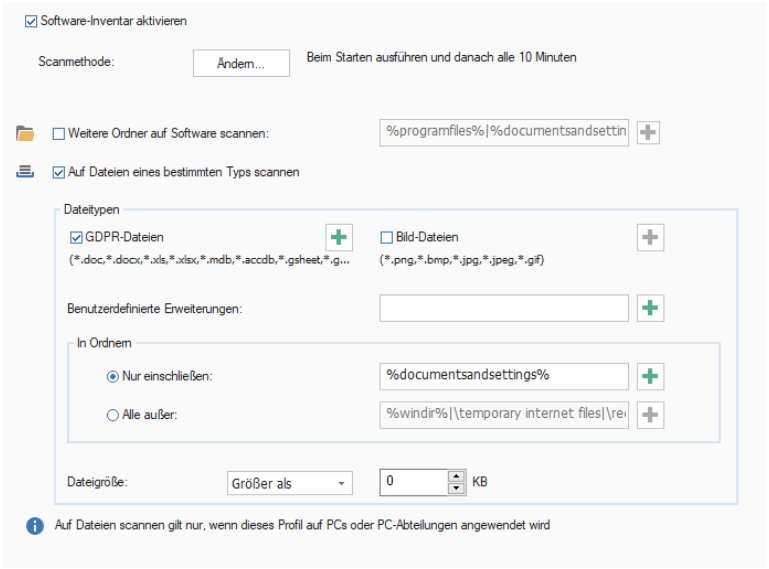
Datenschutz-Modus
Wenn dies aktiviert ist, können Sie immer noch die Agent-Miniaturansichten anzeigen, aber Text wird verpixelt, so dass er unleserlich ist.



Außerdem werden beim Anzeigen eines ausgewählten Agents in **Spotlight** Modus die Fenstertitel der gegenwärtig ausgeführten Anwendungen maskiert, und URLs werden nicht angezeigt.

Softwareinventarisierung

Das Inventarisierungstool scannt standardmäßig häufige Speicherorte, z. B. Programmdateien, auf der Suche nach den auf jedem Agent PC installierten exe-Dateien. Sie können jedoch die Suche auch auf zusätzliche Ordner und Dateitypen erweitern.



Softwareinventarisierung aktivieren

Wenn Sie diese Markierung aufheben, wird die Softwareinventarisierung deaktiviert.

Scan-Methode

In der Standardeinstellung läuft das Software-Inventar, wenn NetSupport DNA Agent startet und danach alle zehn Minuten. Klicken Sie auf **Ändern**, um die Einstellungen auf benutzerdefinierte Scan-Zeiten ändern.

Hinweis: Wir empfehlen ein angemesseneres Laufzeitintervall von 1440 Minuten als Richtschnur, um die Genauigkeit der angezeigten Daten und den erhöhten Netzwerkverkehr von den DNA Agent-Maschinen gegeneinander auszubalancieren.

Zusätzliche Ordner scannen

Hier können Sie Ordner angeben, die u. U. bei der Kompilierung des Inventars nicht standardmäßig eingeschlossen werden.

Auf Dateien eines bestimmten Typs scannen
Hiermit können Sie auf bestimmte Dateitypen scannen und benutzerdefinierte Erweiterungen angeben.

Dateitypen

GDPR-Dateien
Sie können wählen, ob GDPR-Dateien im Scan eingeschlossen werden sollen, so dass Sie schnell sehen können, wo sich potentielle GDPR-Dateien befinden. In der Standardeinstellung wird auf .doc, .docx, .xls und .xlsx Dateierweiterungen gescannt. Um andere Dateitypen einzuschließen, klicken Sie auf .

Bilddateien
Wählen Sie, ob Bilddateien für den Scan eingeschlossen werden sollen. In der Standardeinstellung wird auf .png, .bmp, .jpg, .jpeg und .gif Dateierweiterungen gescannt. Um andere Dateitypen einzuschließen, klicken Sie auf .

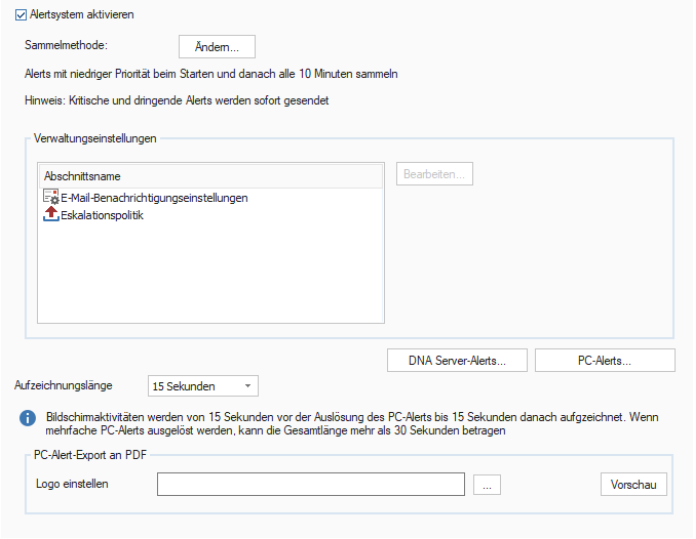
Benutzerdefinierte Erweiterungen
Geben Sie nötigenfalls die Erweiterung aller zusätzlichen Dateitypen an. Klicken Sie auf  und wählen Sie die Dateitypen in der Liste oder fügen Sie Ihre eigenen hinzu.

In Ordnern
Geben Sie an, welche Ordner ein- oder ausgeschlossen werden sollen.

Dateigröße
Geben Sie eine Mindest- oder Höchstgröße für Dateien an.

Alerting

Die E-Mail-Benachrichtigungseinstellungen müssen von hier aus konfiguriert werden, damit Sie eine Alert-Benachrichtigung per E-Mail senden können.



Alerting-System aktivieren

Wenn Sie die Markierung dieses Feldes aufheben, wird das Alerting ausgeschaltet.

Sammeln-Methode:

In der Standardeinstellung sammelt Alerting Alerts mit niedriger Priorität, wenn NetSupport DNA Agent startet und danach alle zehn Minuten.
Klicken Sie auf **Ändern**, um die Einstellungen auf benutzerdefinierte Sammelzeiten ändern.

Verwaltungseinstellungen

Sie können die Einstellungen für das DNA Alerting-System konfigurieren, indem Sie auf **Bearbeiten** klicken.

E-Mail-Benachrichtigungseinstellungen

Ermöglicht es Ihnen, die Email-Adresse eines Administrators anzugeben, der im Falle von nicht-beantworteten kritischen Alerts benachrichtigt werden soll, und zu wählen, ob eine Benachrichtigung erfolgen soll, wenn ein Alert geschlossen wird.

Administrator-Benachrichtigung
Geben Sie die E-Mail-Adresse des Administrators ein, der alle unbeantworteten Alerts erhält.

Beim Schließen E-Mail-Benachrichtigung senden
Option zum Senden von E-Mail-Benachrichtigungen an Alert-Nachrichtenempfänger beim Schließen eines Alerts.

Eskalationspolitik

Ermöglicht die Änderung der Zeit, die Bedienern zum Umgang mit Alerts zugewiesen wird, bevor diese auf die nächste Ebene gelangen. Sobald die angegebene Zeit für kritische Alerts überschritten ist, wird der Administrator per E-Mail benachrichtigt.

Hinweis: Nachdem Sie die obigen Werte in das Dialogfeld "Einstellungen" eingegeben haben, nehmen Sie die Werte durch Drücken der Eingabetaste an.

Durch Auswahl von DNA Server-Alerts oder PC-Alerts können Sie Alerts erstellen oder bearbeiten.

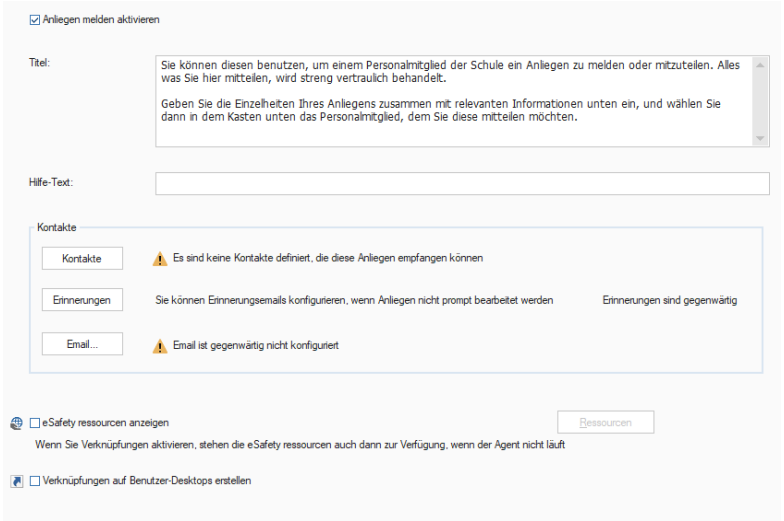
Aufzeichnungslänge
Wenn für ein PC-Alert die Aktion 'Bildschirm aufzeichnen' eingestellt ist, kann hier die Bildschirmaufzeichnungsdauer eingestellt werden. In der Standardeinstellung ist die Aufzeichnungsdauer auf fünfzehn Sekunden eingestellt (fünfzehn Sekunden bevor und nachdem das PC-Alert ausgelöst worden ist). Wählen Sie die gewünschte Zeit im Dropdown-Menü.

PC-Alert-Export an PDF
Wenn ein PC-Alert ausgelöst worden ist, können Sie die Details an eine PDF-Datei exportieren. Von hier aus können Sie das PDF mit dem Branding Ihrer Organisation anpassen, indem Sie ein Logo hinzufügen.

Hinweis: Sie können den Ordner, an den das PDF exportiert werden soll, in den Dateispeicherort-Einstellungen angeben.

Logo einstellen
Klicken Sie auf ..., um eine Bilddatei zu wählen. Es werden BMP, JPG und PNG Dateien unterstützt, und die maximale Dateigröße ist 5MB. Klicken Sie auf Vorschau, um zu sehen, wie das Logo in der PDF-Datei angezeigt wird.

Anliegen melden Einstellungen



Hinweis: Diese Einstellungen stehen nur in der NetSupport DNA Version für das Bildungswesen zur Verfügung.

Ein Anliegen melden aktivieren
Aktivieren Sie dieses Kontrollkästchen, um es Schülern zu ermöglichen, Anliegen zu melden.

Titel
Sie können den Text, der im Ein Anliegen melden Dialog gezeigt wird, durch Überschreiben des vorhandenen Texts anpassen.

Hilfe-Text
Ermöglicht es Ihnen, eine Zeile Hilfe-Text zum Ein Anliegen melden Dialog hinzuzufügen. Zum Beispiel könnten Sie vielleicht eine externe Telefonnummer oder Emailadresse angeben, die die Schüler kontaktieren können, wenn sie mit jemandem außerhalb der Schule sprechen möchten.

Kontakte
Damit Schüler ein Anliegen melden können, müssen zuerst Kontaktpersonen (Personalmitglieder, die Anliegen empfangen können) definiert werden. Klicken Sie auf **Kontakte,** um neue Kontakte zu erstellen, existierende zu bearbeiten, und zu wählen, welche Kontakte für dieses Profil zur Verfügung stehen sollen.

Wenn Anliegen nicht innerhalb von vier Stunden bearbeitet werden, wird ein Erinnerungsemail gesendet. Diese Option ist in der Standardeinstellung aktiviert. Um sie zu deaktivieren oder das Erinnerungsintervall zu ändern, klicken Sie auf **Erinnerungen**.

Hinweis: NetSupport DNA scannt nur während der definierten Arbeitsstunden auf Anliegen. Die Arbeitsstunden können Ihren Anforderungen entsprechend in Konsolenanpassungen – Allgemein-Einstellungen eingestellt werden.

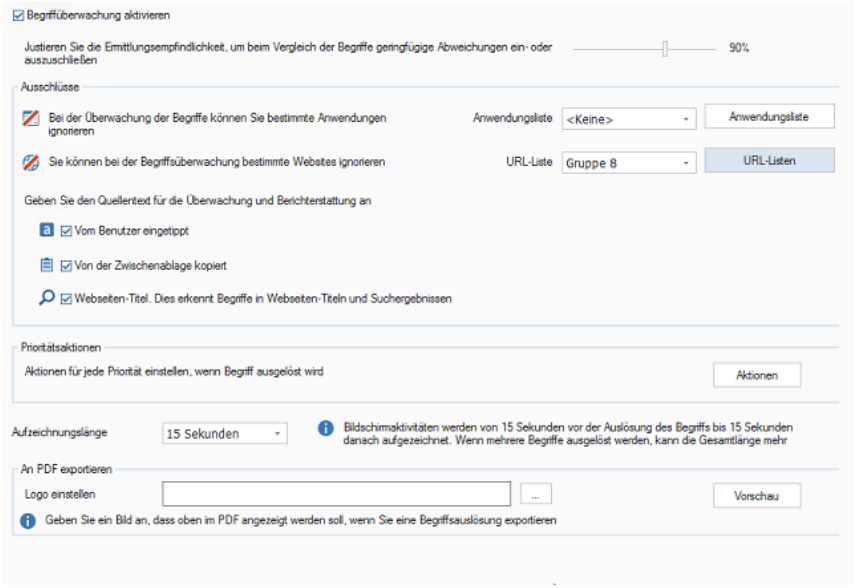
Für Kontakte, die eine Email-Benachrichtigung erhalten sollen, wenn Anliegen gemeldet werden, müssen Sie die Email-Einstellungen konfigurieren. Klicken Sie auf **Email**.

eSafety Ressourcen anzeigen
Wenn Sie diese Option wählen, wird ein Link zu einer Liste von eSafety Ressourcen (Websites und Helplines) aktiviert, die für Schüler vom NetSupport DNA Agent Menü aus zur Verfügung stehen, und wenn sie ein Anliegen gemeldet haben. Wenn Sie diese Option zum ersten Mal aktivieren, werden Sie aufgefordert, Ihre Region einzugeben, um sicherzustellen, dass eine Liste relevanter Ressourcen angezeigt wird. Um etwas zu der Liste hinzuzufügen oder sie zu bearbeiten, klicken Sie auf **Ressourcen**.

Verknüpfungen auf Benutzer-Desktops erstellen
Verknüpfungen zu Anliegen melden und eSafety Ressourcen (falls aktiviert) werden auf den Schüler-Desktops erstellt.

Hinweis: Das eSafety Ressourcen-Symbol wird auch dann zur Verfügung stehen, wenn NetSupport DNA Agent nicht ausgeführt wird.

Begriffsüberwachung-Einstellungen



Begriffüberwachung aktivieren
Deaktivieren Sie dieses Kontrollkästchen, um die Begriffsüberwachung-Funktion zu deaktivieren.

Für die Übereinstimmung von Schlüsselwörtern können Sie den Genauigkeitsgrad justieren, um festzulegen, wie genau Wörter vom Schüler getippt werden müssen, um gemeldet zu werden. In der Standardeinstellung ist der Grad auf 90% eingestellt, so dass geringfügige Rechtschreibfehler bei der Feststellung der Übereinstimmung berücksichtigt werden.

Wenn der Genauigkeitsgrad auf 100% eingestellt wird, wird nur dann eine Übereinstimmung festgestellt, wenn der Schüler das Schlüsselwort ganz genau eintippt. Je geringer der Prozentsatz, desto wahrscheinlicher ist es, dass der Begriff (oder ähnliche Wörter) als unangemessen gekennzeichnet wird.

Ausschlüsse
Bei der Überwachung auf Schlüsselwörter und Begriffe können bestimmte Anwendungen und Websites ignoriert werden.

Anwendungsliste
Um eine neue Anwendungsliste zu erstellen, klicken Sie auf **Anwendungslisten** und wählen dann, welche Anwendungen ignoriert werden sollen. Wenn die Liste erstellt worden ist, wählen Sie diese im Dropdownmenü. Alle Anwendungen in der Anwendungsliste werden dann für die Begriffsübereinstimmung ignoriert.

URL-Liste
Um eine URL-Liste zu erstellen, klicken Sie auf **URL-Listen** und wählen dann, welche Websites zu ignorieren sind. Wenn die Liste erstellt worden ist, wählen Sie diese im Dropdownmenü. Websites in der URL-Liste werden bei der Begriffsüberwachung ignoriert.

Quellentext
Entscheiden Sie, für welche Textarten Sie Überwachung und Berichterstattung wünschen: Vom Benutzer eingetippter Text, an die Zwischenablage kopierter Text und Text in Website-Titeln.

Prioritätsaktionen
Wenn ein Begriff ausgelöst worden ist, hängt die Aktion, die ausgeführt wird, von der eingestellten Prioritätsstufe ab. In der Standardeinstellung zeichnen alle Prioritätsstufen die Nutzung im eSafety Informationsfenster auf (außer wenn die Priorität auf Aus gestellt ist); mittleren und hohen Graden außerdem ein Alert generiert; bei hohem Grad wird zusätzlich ein Screenshot beim Schüler aufgenommen und ein Email gesandt, das die Benutzer informiert, dass ein Begriff ausgelöst worden ist. Bei dringendem Grad wird eine Bildschirmaufzeichnung bei dem Schüler/In erstellt, der den Begriff ausgelöst hat.

Hinweise:
- Email-Benachrichtigungen können erst gesandt werden, wenn die Email-Einstellungen konfiguriert worden sind. Die Benutzer, die bei Begriffsauslösungen Emailbenachrichtigungen erhalten sollen, können im eSafety Benutzer-Dialog eingestellt werden.
- Es kann ein Bild des Schülers aufgenommen werden, der den Begriff ausgelöst hat, wenn das Schülergerät eine aktive Webcam hat. In der Standardeinstellung ist diese Aktion deaktiviert, aber sie kann für beliebige Prioritätsstufen angewendet werden. Wenn die Webcam am Schülergerät gegenwärtig benutzt wird, oder wenn die Webcam in den USB-Gerätesteuerungseinstellungen deaktiviert worden ist, wird keine Webcam-Aufnahme gemacht.

Um die Aktionen, die für die einzelnen Prioritätsstufen ausgeführt werden, anzupassen, klicken Sie auf **Aktionen**.

Aufzeichnungsdauer
Hier kann die Bildschirmaufzeichnungsdauer für einen dringenden Prioritätsgrad eingestellt werden. In der Standardeinstellung ist die Aufzeichnungsdauer auf 15 Sekunden eingestellt (fünfzehn Sekunden bevor und nachdem der Begriff ausgelöst worden ist). Wählen Sie die gewünschte Zeit im Dropdown-Menü.

An PDF exportieren
Wenn ein Begriff ausgelöst worden ist, können Sie die Details an eine PDF-Datei exportieren. Von hier aus können Sie die PDF-Datei mit Ihrem Schullogo anpassen, indem Sie ein Logo hinzufügen.

Hinweis: Sie können den Ordner, an den das PDF exportiert werden soll, in den Dateispeicherort-Einstellungen angeben.

Logo einstellen
Klicken Sie auf ..., um eine Bilddatei zu wählen. Es werden BMP, JPG und PNG Dateien unterstützt, und die maximale Dateigröße ist 5MB. Klicken Sie auf **Vorschau,** um zu sehen, wie das Logo in der PDF-Datei angezeigt wird.

Hinweis: Diese Einstellungen stehen nur in der NetSupport DNA Version für das Bildungswesen zur Verfügung.

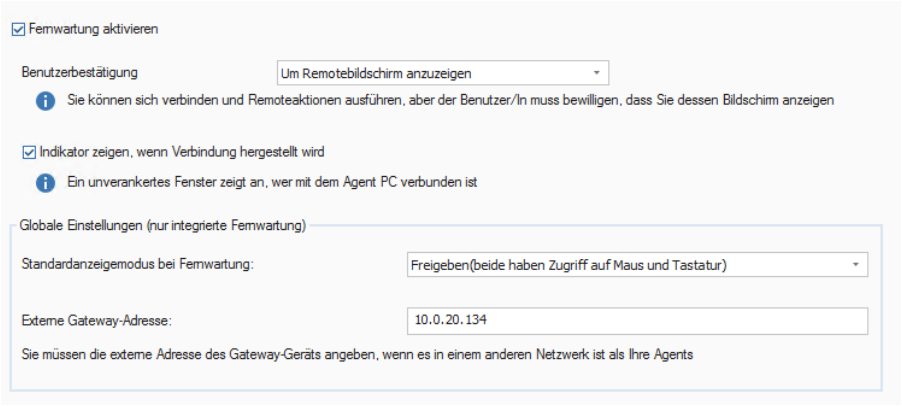
Acceptable Use Policy



Aktivieren
Deaktivieren Sie dieses Kontrollkästchen, um die Acceptable Use Policy Funktion zu deaktivieren.

Verwalten
Ermöglicht es Ihnen, die Acceptable Use Policies zu erstellen und zu verwalten. Klicken Sie auf **Verwalten**.

Fernwartungseinstellungen



Fernwartung aktivieren
Heben Sie die Markierung in diesem Kästchen auf, um die Fernwartungsfunktion zu deaktivieren.

Benutzerbestätigung
Wenn Benutzerbestätigung aktiviert ist, muss der Remotebenutzer (Agent) seine Einwilligung geben (durch Bestätigen einer Nachricht), damit Remoteaktionen und/oder die Anzeige seines Bildschirms erfolgen können. Wählen Sie die gewünschte Option in der Dropdownliste:

Keine
Sie können sich ohne Einwilligung des Benutzers verbinden und eine beliebige Aktion ausführen.

Um Remotebildschirm anzuzeigen
Sie können sich verbinden und Remoteaktionen ausführen, wie Dateien übertragen, Fernbefehlseingabeaufforderungen starten, aber der Benutzer/In muss einwilligen, damit Sie seinen Bildschirm anzeigen können.

Um Remoteaktionen auszuführen
Der Benutzer/In muss zuerst seine Einwilligung geben, damit Remoteaktionen ausgeführt werden können.

Indikator zeigen, wenn Verbindung besteht
Wenn eine Fernwartungssitzung aktiv ist, kann der Agent sehen, wer mit ihm verbunden ist.

Globale Einstellungen (nur integrierte Fernwartung)
Wählen Sie den Anzeigemodus bei der Fernwartung von Agents in der Dropdownliste. In der Standardeinstellung ist Freigabe-Modus eingestellt.

Teilen
Sowohl der Konsolenoperator als auch der Agent können Tastenanschläge und Mausbewegungen eingeben.

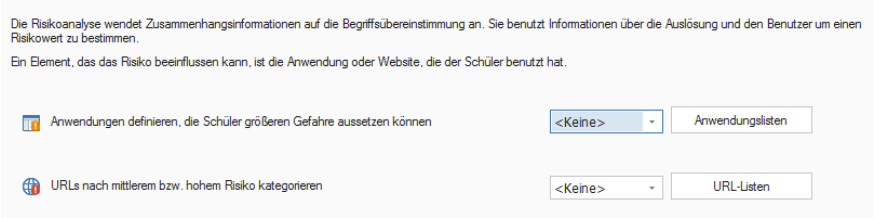
Beobachten
Nur der Agent kann Tastenanschläge und Mausbewegungen eingeben. Maus und Tastatur des Konsolenoperators sind deaktiviert.

Kontrollieren
Nur der Konsolenoperator kann Tastenanschläge und Mausbewegungen eingeben. Der Benutzer am Agent ist gesperrt.

Externe Gateway-Adresse
Wenn sich irgendwelche Agent-Geräte, die Sie fernwarten wollen, in einem Remote-Netzwerk befinden, müssen Sie Ihre externe (öffentliche) Gateway-Adresse eingeben, um die integrierten Fernwartungsfunktionen für diese Geräte zu aktivieren.

Hinweis: Diese Einstellungen stehen nur in der NetSupport DNA Version für das Bildungswesen zur Verfügung.

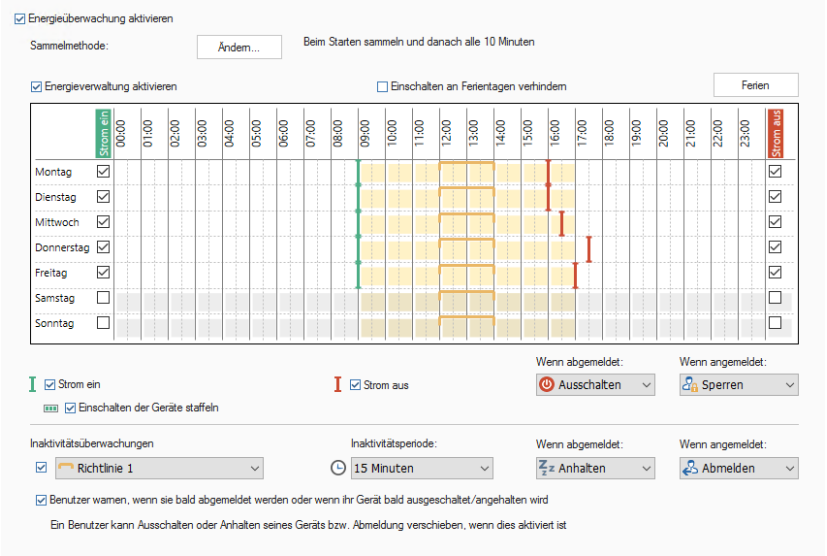
NetSupport DNA Risikoanalysen-Einstellungen



Anwendungen definieren, die Schüler größeren Gefahren aussetzen können
Sie können wählen, welche Anwendungen als größere Gefahr klassifiziert werden sollen. Diese Anwendungen können zu einer Anwendungsliste hinzugefügt werden, und es können mehrere Listen erstellt werden, so dass Sie verschiedenen Profilen verschiedene Listen zuweisen können. Klicken Sie auf **Anwendungslisten**.

URLs nach mittlerem bzw. hohem Risiko kategorisieren
Es können URL-Listen erstellt werden, die es Ihnen ermöglichen, Websites als mittleres oder hohes Risiko zu definieren. Es können mehrere Listen erstellt werden, so dass Sie verschiedenen Profilen verschiedene Listen zuweisen können. Klicken Sie auf **URL-Listen**.

Energiemonitor



Energiemonitor aktivieren

Wenn Sie diese Markierung aufheben, wird der Energiemonitor deaktiviert.

Sammeln-Methode:

In der Standardeinstellung sammelt Energiemonitor Daten, wenn NetSupport DNA Agent startet und danach alle zehn Minuten. Klicken Sie auf Ändern, um die Einstellungen auf benutzerdefinierte Sammelzeiten ändern.

Energieverwaltung aktivieren

Wählen Sie diese Option, um die Energiemanagement-Funktion zu aktivieren. Es wird ein Energiemanagementplan angezeigt.

Hinweis: Die gelb schattierten Bereiche zeigen die Arbeitsstunden der Organisation. Die Arbeitsstunden werden in Konsolenanpassungen – Allgemein-Einstellungen eingestellt.

Einschalten an Ferientagen verhindern

Diese Option schließt alle Ferientage aus, die im Einschalten-Zeitplan eingestellt worden sind. Um Ihre Ferienzeiten einzustellen, klicken Sie auf **Ferien**.

Strom ein
Wählen Sie diese Option, um die Einschalten-Funktion zu aktivieren. Wählen Sie die Tage, an denen die Geräte eingestellt werden sollen. Um die Zeit für das Einschalten der Geräte zu justieren, verschieben Sie den grünen Schieberegler auf die geforderte Zeitperiode.

Geräte gestaffelt einschalten
Mit dieser Option werden Geräte gestaffelt eingeschaltet statt alle gleichzeitig.

Strom aus
Wählen Sie diese Option, um die Ausschalten-Funktion zu aktivieren. Wählen Sie die Tage, an denen die Geräte ausgeschaltet werden sollen. Um die Zeit für die Ausschaltung der Geräte zu justieren, verschieben Sie den roten Schieberegler auf die geforderte Zeitperiode.

Sie können entscheiden, welche Aktionen erfolgen sollen, wenn sich ein Benutzer an- oder abmeldet, wenn Strom aus aktiviert ist: nichts tun, ausschalten, anhalten, sperren oder abmelden (wenn angemeldet).

Hinweis: Die Strom aus planen Funktion steht für Geräte mit einem Server-Betriebssystem und für Geräte, auf denen ein DNA Server oder ein SNMP Server oder ein Webserver oder ein DNA Remote (Agent) Gateway installiert ist, nicht zur Verfügung.

Inaktivitätsüberwachungen
Es können zwei Inaktivitätsrichtlinien eingestellt werden, so dass Sie Regeln dafür erstellen können, welche Aktion ausgeführt werden soll, wenn ein Gerät für eine vorgegebene Zeitspanne inaktiv ist. Wenn eine Richtlinie aktiviert ist, wird eine Markierung gezeigt. Sie können deren Größe verändern und sie auf die Zeitperiode ziehen, für die die Richtlinie gelten soll.

Benutzer warnen, wenn sie abgemeldet werden oder ihre Geräte bald ausgeschaltet/angehalten werden
Diese Option warnt Benutzer, wenn sie bald von ihren Geräten abgemeldet werden, oder wenn ihre Geräte bald ausgeschaltet oder angehalten werden. Der Benutzer hat dann die Möglichkeit, diese Aktion fünfzehn, dreißig oder sechzig Minuten aufzuschieben.

Hinweis: Der Benutzer kann sehen, ob ein Energiemanagement-Zeitplan eingestellt worden ist, und kann die Aktion im NetSupport DNA Agent Fenster verschieben.

NetSupport DNA SNMP-Konfigurationseinstellungen

Der NetSupport DNA SNMP-Konfigurator ermöglicht es den Administratoren/Konsolenoperators, spezifische Einstellungen auf Gesellschafts- oder Abteilungsebene für jede der SNMP-Primärfunktionen anzuwenden.

Um auf das NetSupport DNA Konfigurationsmenü zuzugreifen, markieren Sie die Abteilung oder Gesellschaft, auf die die Einstellungen angewandt werden sollen, in der Geräte-Strukturansicht, klicken dann rechts und wählen die Einstellungen oder klicken in der Einstellungen-Registerkarte auf dem **Allgemeines**-Symbol.

Hinweise:
- Diese Einstellungen erscheinen nur, wenn Sie in der Geräte-Strukturansicht sind.
- Dieser Dialog bietet auch Zugriff auf die Konsoleneinstellungen.

Es wird ein Überblick der Einstellungen für jede Komponente gezeigt, so dass Sie erkennen können, welche Komponenten gegenwärtig aktiviert sind. Dort wo Änderungen getätigt aber nicht gespeichert worden sind, erscheint ein gelber Stern.

Wenn Sie ein Symbol anklicken, gelangen Sie zu den Einstellungen für den betreffenden Bereich.



Klicken Sie auf **Speichern**, um alle Änderungen zu speichern. Sie werden gefragt, wie diese Einstellungen für die Abteilung angewandt werden sollen. Die Zurücksetzen Taste wird alle Abteilungseinstellungen löschen und auf die Standard- oder übergeordneten Einstellungen zurückgehen.

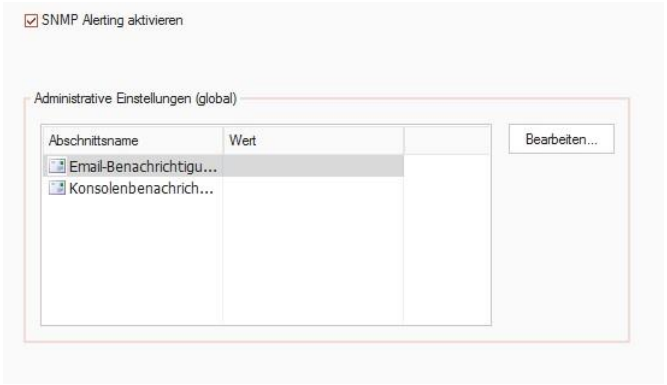
SNMP-Überwachungseinstellungen



SNMP-Überwachung aktivieren
Deaktivieren Sie dieses Kontrollkästchen, um die SNMP-Überwachung zu deaktivieren.

Scanmethode
In der Standardeinstellung wird die SNMP-Überwachung ausgeführt, wenn der SNMP-Server startet und danach alle sechzig Minuten. Klicken Sie auf **Ändern**, um die Einstellungen auf benutzerdefinierte Scan-Zeiten ändern.

SNMP-Alerteinstellungen



SNMP Alerting aktivieren
Wenn Sie die Markierung dieses Feldes aufheben, wird das Alerting ausgeschaltet.

Verwaltungseinstellungen
Sie können die Einstellungen für das DNA SNMP Alerting-System konfigurieren, indem Sie auf **Bearbeiten** klicken.

E-Mail-Benachrichtigungs
Ermöglicht es Ihnen, eine Emailadresse für einen Administrator/Operator anzugeben, der zu benachrichtigen ist, wenn ein SNMP-Alert aktiv wird.

Hinweis: Es können mehrere Emailadressen hinzugefügt werden. Sie müssen durch Semikolons getrennt werden.

Konsolenbenachrichtigungen
Wählen Sie, welche Konsolenbenutzer Konsolenbenachrichtigungen erhalten sollen.

SNMP-Verlaufeinstellungen



SNMP-Verlauf aktivieren
Deaktivieren Sie dieses Kontrollkästchen, um den SNMP-Verlauf zu deaktivieren.

Konsoleneinstellungen

Konsoleneinstellungen sind globale Einstellungen, die für die gesamte NetSupport DNA Konsole angewendet werden.

Hinweis: NetSupport DNAs Komponenteneinstellungen werden über die Profile konfiguriert.

Im Dialogfeld "Konsoleneinstellungen" können Bediener sieben Arten von Einstellungen konfigurieren.

Allgemein
Konfigurieren Sie die allgemeinen Einstellungen, die für die gesamte NetSupport DNA Konsole gelten, definieren Sie, wann NetSupport DNA auf verfügbare Updates kontrollieren soll, und die Arbeitsstunden und Ferienzeiten für Ihre Organisation einzustellen.

Benutzeroberfläche
Ermöglicht es Ihnen anzupassen, was in der Hierarchie-Strukturansicht gezeigt werden soll.

Active Directory-Einstellungen
Welche die Konfiguration der DNA-Komponenten aufgrund der Active Directory Container statt der Abteilungen ermöglichen.

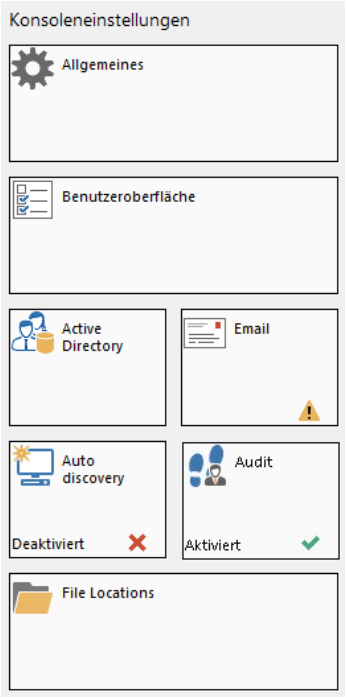
Email-Einstellungen
Ermöglicht es Ihnen, die Email-Einstellungen für die Sendung von Benachrichtigungen einzustellen.

Automatische Ermittlung
Die es Ihnen ermöglicht, die Automatische Agent-Ermittlung-Funktion freizugeben.

Audit
Ermöglicht es Ihnen, die Einstellungen für das NetSupport DNA Audit Protokoll zu konfigurieren.

Hinweis: Audit steht nicht zur Verfügung, wenn man von der Benutzer-, Geräte- oder Ermittelt-Struktur aus auf die Konsoleneinstellungen zugreift.

Dateispeicherorte
Ermöglicht es Ihnen anzugeben, wohin PDFs für PC-Alerts und durch eSafety* ausgelöste Begriffe exportiert werden sollen.



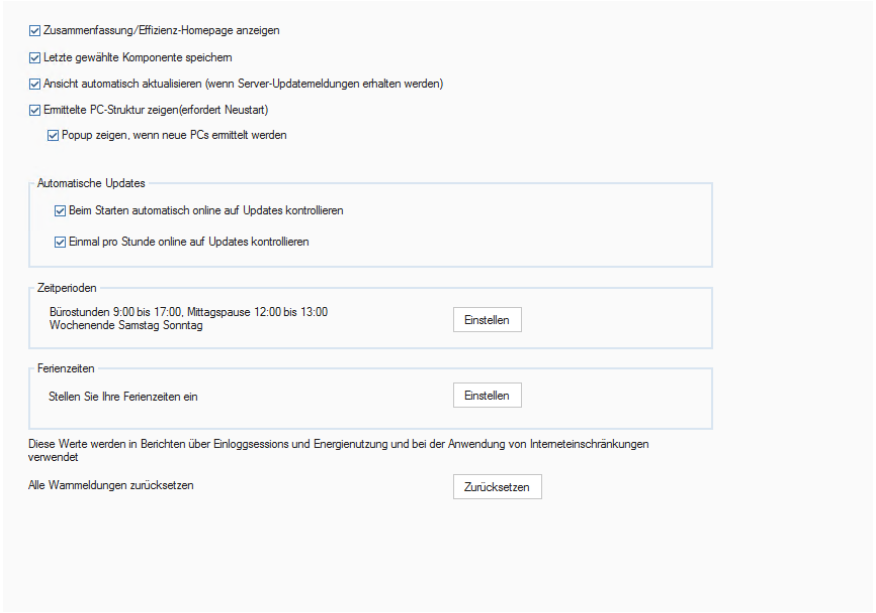
Um Zugriff auf die Konsoleneinstellungen zu erhalten, wählen Sie die Registerkarte Einstellungen und klicken Sie auf dem **Allgemeines** Symbol.

Wenn Sie ein Symbol anklicken, gelangen Sie zu den Einstellungen für den betreffenden Bereich.

Hinweis: Die gezeigten Komponenten hängen von dem Bereich ab, den Sie auf der Konsole betrachten.

Klicken Sie auf **Speichern**, um alle Änderungen zu speichern.

Allgemein



Zusammenfassung/Effizienz Homepage anzeigen
Wenn Sie die Markierung dieser Option aufheben, wird der Zusammenfassungs/Effizienzbildschirm ausgeblendet.

Letzte gewählte Komponente speichern

Wenn diese Option markiert ist, speichert die DNA Konsole die letzte Komponente, die ausgewählt war, wenn Sie die Konsole verlassen. Beim nächsten Aufruf der DNA Konsole gelangen Sie direkt zur betreffenden Komponente.

Ansicht automatisch aktualisieren

Wenn dies aktiviert ist, benachrichtigt NetSupport DNA Sie, wenn neue Updates zur Verfügung stehen (ein Indikator erscheint auf dem Seite aktualisieren Symbol im Menüband), so dass Sie die Ansicht aktualisieren können, sobald es Ihnen auskommt.

Ermittelte PC-Struktur zeigen (erfordert Neustart)
Diese Option ermöglicht es Ihnen, die ermittelte PC-Strukturansicht an der Konsole ein/auszublenden.

Popup zeigen, wenn neue PCs ermittelt werden
Wenn die Ermittelte Strukturansicht angezeigt wird, können Sie wählen, ob Sie benachrichtigt werden möchten, wenn neue PCs ermittelt werden.

Automatische Updates
In der Standardeinstellung kontrolliert NetSupport DNA automatisch, ob Updates zur Verfügung stehen. Wenn es welche findet, erscheint im Konsolenfenster eine Kopfzeilenleiste. Sie können die Updates von hier aus anzeigen und herunterladen.

Beim Starten automatisch online auf Updates kontrollieren
Jedes Mal wenn die Konsole startet, kontrolliert NetSupport DNA automatisch auf Updates.

Einmal pro Stunde online auf Updates kontrollieren
NetSupport DNA kontrolliert einmal pro Stunde auf Updates.

Zeitperioden

Die Arbeitstage und -stunden, die bei der Berichterstattung über Anmeldungssitzungen und Energieverbrauch sowie bei der Anwendung von Internetbeschränkungen benutzt werden, und auch um festzustellen, ob ein Begriff* innerhalb oder außerhalb der Unterrichtsstunden ausgelöst worden ist, können für Ihre Organisation angepasst werden. Klicken Sie auf **Einstellen**, um die Geschäftszeiten, Mittagspause und Wochenenden einzugeben.

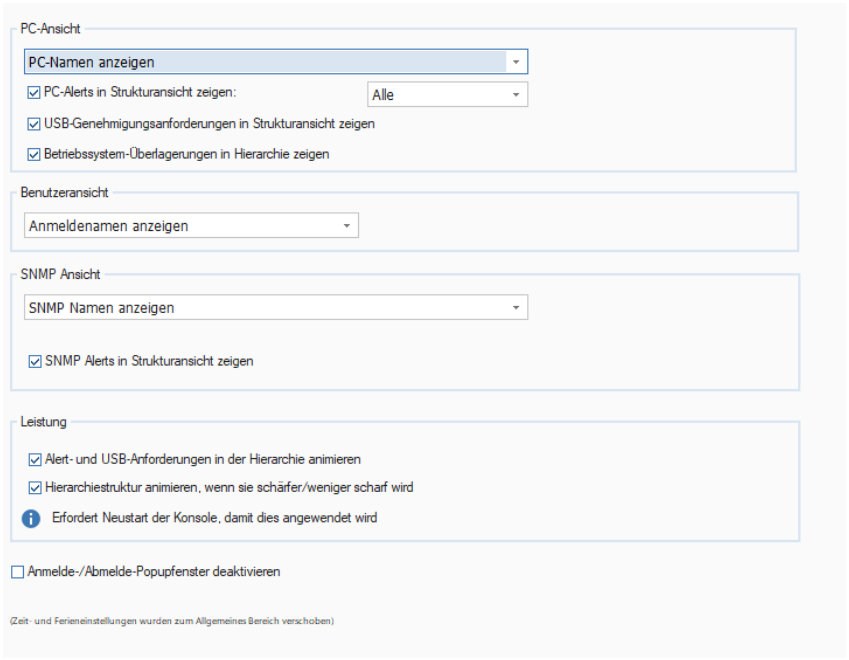
Ferienzeiten

NetSupport DNA ermöglicht es Ihnen, Ferienzeiten einzustellen. Diese Daten können dann vom Einschalten-Zeitplan in den Energieüberwachungseinstellungen ignoriert werden, so dass die Geräte nicht eingeschaltet werden. Klicken Sie auf **Einstellen**, um die Daten einzugeben.

Alle Warnmeldungen zurücksetzen
Wenn auf der Konsole eine Warnmeldung erscheint, können Sie wählen, diese nicht noch einmal zu zeigen. Wenn Sie diese Option wählen, werden alle Warnmeldungen zurückgesetzt, so dass sie jetzt gezeigt werden.

* Die Funktion steht nur in der NetSupport DNA Version für das Bildungswesen zur Verfügung.

Benutzeroberfläche



PC Ansicht

Wählen, wie die Agents in der PC-Strukturansicht gezeigt werden sollen.

PC-Alerts in Strukturansicht zeigen

Ermöglicht das Ein-/Ausschalten des Symbols, das beim Auslösen eines Alerts auf Agentebene in der Strukturansicht erscheint. Wählen Sie in der Dropdownliste, ob Sie alle Alert-Symbole oder nur PC- oder Server-Alerts ausschalten möchten.

USB-Genehmigungsanforderungen in Strukturansicht

Ermöglicht es Ihnen, USB- Genehmigungsanforderungen in der Strukturansicht zu zeigen/auszublenden.

Betriebssystem-Überlagerungen in Hierarchie zeigen

Blendet die Betriebssystem-Symbolüberlagerung an den Agents in PC-Strukturansicht ein/aus.

Benutzeransicht
Wählen, wie die Agents in der Benutzer-Strukturansicht gezeigt werden sollen.

SNMP Ansicht
Wählen, wie die Geräte in der Geräte-Strukturansicht gezeigt werden sollen.

SNMP Alerts in der Strukturansicht zeigen
Ermöglicht es Ihnen, das in der Geräte-Strukturansicht gezeigte Symbol ein/auszuschalten, wenn ein Alert ausgelöst worden ist.

Leistung
Alert- und USB-Anforderungen in der Hierarchie animieren
In der Standardeinstellung werden die Symbole für Alerts und USB-Anforderungen in der Hierarchiestrukturansicht animiert gezeigt. Um dies auszuschalten, deaktivieren Sie das Kontrollkästchen.

Hierarchiestruktur animieren, wenn sie schärfer/weniger scharf wird
In der Standardeinstellung wird ein hervorgehobenes Element in der Strukturansicht scharf gezeigt, und andere Elemente weniger scharf. Dies kann ausgeschaltet werden, so dass alle Elemente immer scharf bleiben.

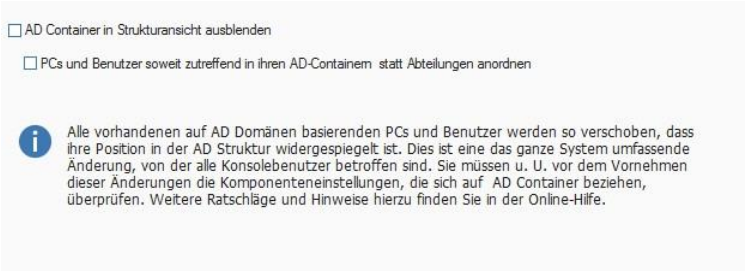
Hinweis: Damit diese Einstellungen angewendet werden, muss die NetSupport DNA Konsole neu gestartet werden.

Anmelde-/Abmelde-Popupfenster deaktivieren

Jedes Mal, wenn sich ein anderer Benutzer in der DNA Konsole an- oder abmeldet, wird bei Ihnen eine Popupmeldung eingeblendet. Durch Auswahl dieser Option lässt sich diese Popupmeldung deaktivieren.

Active Directory-Einstellungen

Normalerweise zeigt NetSupport DNA die standardmäßige Abteilungsstrukturansicht an. Wenn Sie mit Active Directory arbeiten, kann es sich empfehlen, PCs und Benutzer in derselben Struktur einzublenden.



AD Container in Strukturansicht ausblenden

Der AD Container-Ordner wird in der Strukturansicht standardmäßig angezeigt, auch wenn Sie die Container gerade nicht nutzen. Wenn Sie diese Option markieren, warden die AD Container in der Strukturansicht ausgeblendet.

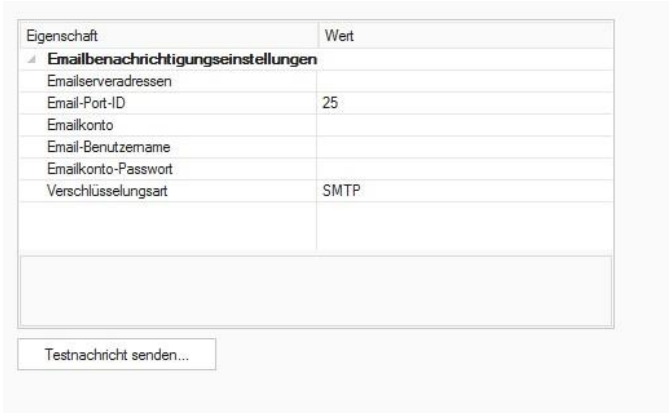
PCs falls zutreffend im Layout der AD Container und nicht der Abteilungen anzeigen

Wenn Sie diese Option markieren, werden Agents in den AD Container, der ihre Position in der Struktur widerspiegelt, verschoben.

Hinweis: Alle Änderungen an der Struktur müssen über Active Directory vorgenommen werden und sie werden dann von DNA automatisch erkannt.

Nach dem Verschieben von Agents in Ihre Directory-Container kann es sein, dass sich vorherige Abteilungseinstellungen nicht auf die Active Directory-Container beziehen. Überprüfen Sie die Komponenten- und Agenteinstellungen um sicherzustellen, dass Sie die richtigen Einstellungen angewendet haben.

E-Maileinstellungen



E-Mail-Benachrichtigungseinstellungen
Ermöglicht es Ihnen, die Email-Einstellungen für Benachrichtigungen zu konfigurieren, die an die Operators gesendet werden sollen.

E-Mail Server-Adresse
Geben Sie die E-Mail Server-Adresse, die Sie für das Alerting-System verwenden möchten, ein.

Server-Anschluss-ID
Geben Sie die TCP/IP-Anschlussnummer des E-Mail-Servers ein.

E-Mail-Konto
Geben Sie die E-Mail-Adresse ein, von der alle Benachrichtigungs-E-Mails gesendet werden.

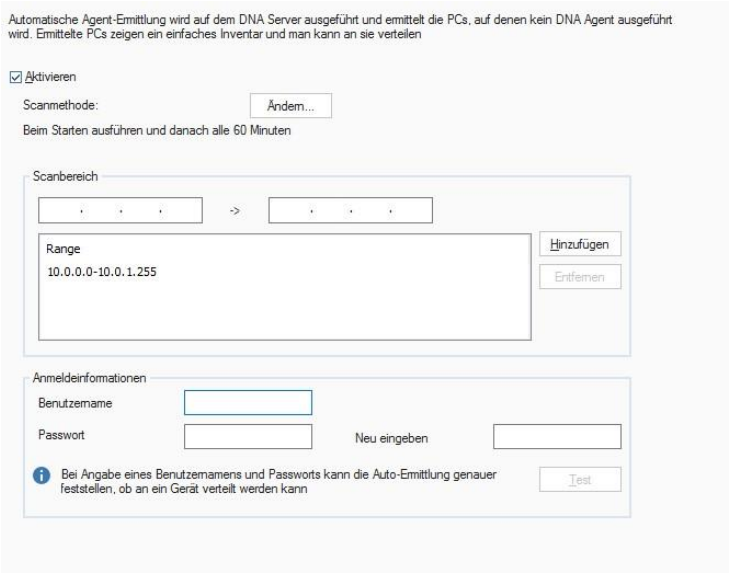
E-Mail-Benutzerkonto
Geben Sie den Anmeldenamen des obigen E-Mail-Kontos ein.

E-Mail Konto-Authentifizierung
Geben Sie das Kennwort für das E-Mail-Konto ein.

Verschlüsselungsart
Wählen Sie die Verschlüsselungsart in der Dropdown-Liste, SSL, TSL oder SMTP.

Testnachricht senden
Ermöglicht es Ihnen, eine Testnachricht zu senden. Geben Sie die Email-Adresse ein, an die die Testnachricht gesendet werden soll.

Automatische Ermittlung



Aktivieren
Diese Option aktiviert die automatische Ermittlung.

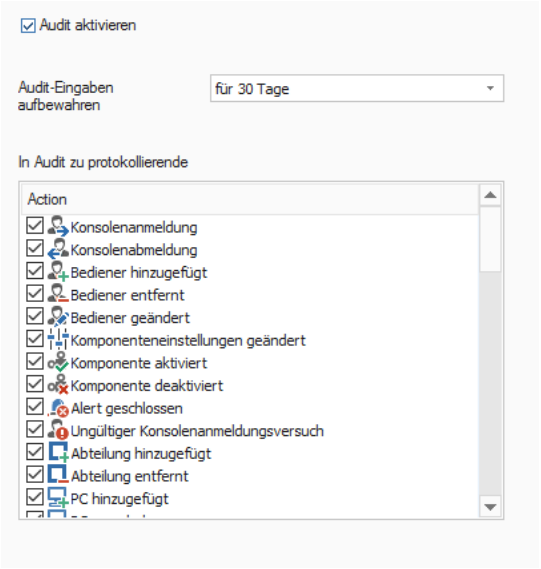
Scannen alle ...
In der Standardeinstellung wird die automatische Ermittlung beim Starten ausgeführt und danach alle sechzig Minuten. Klicken Sie auf Ändern, um die Einstellungen auf benutzerdefinierte Scan-Zeiten ändern.

Scanbereich
Geben Sie den geforderten zu scannenden IP-Adressenbereich ein und klicken Sie auf Hinzufügen, um ihn in die Liste aufzunehmen.

Anmeldeinformationen
Sie können einen Benutzernamen und ein Passwort eingeben, um festzustellen, ob ein DNA Agent für das Gerät bereitgestellt werden kann.

Test
Ermöglicht es Ihnen, die von Ihnen eingegebenen Anmeldeinformationen zu testen.

Audit-Einstellungen

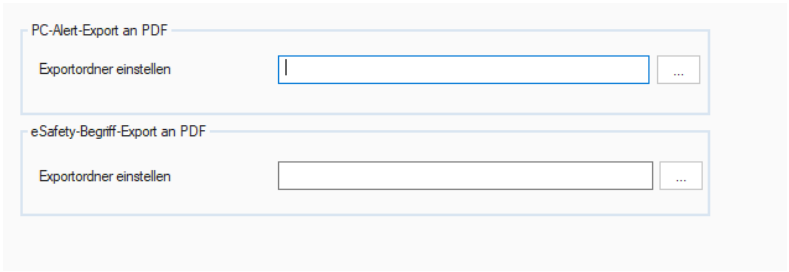


Audit aktivieren
Auswahl in diesem Kästchen aufheben, um das Audit-Protokoll zu deaktivieren.

Audit-Eingaben aufbewahren
Wählen Sie, wie lange Audit-Eingaben aufbewahrt werden sollen: dreißig Tage, sechzig Tage, neunzig Tage oder unbegrenzt.

In Audit zu protokollierende Aktionen
Die Aktionen, die protokolliert werden können, sind aufgelistet. Heben Sie die Auswahl aller Aktionen auf, die nicht protokolliert werden sollen.

Dateispeicherort-Einstellungen



PC-Alert-Export an PDF
Wenn ein PC-Alert ausgelöst worden ist, können Sie die Details an eine PDF-Datei exportieren. Von hier aus können Sie den Standardordner vorgeben, an den das PDF exportiert werden soll.

Exportordner einstellen
Klicken Sie auf ..., um den Ordner anzugeben, an den die PDF-Datei exportiert wird.

eSafety-Begriff-Export an PDF
Wenn ein Begriff ausgelöst worden ist, können Sie die Details an eine PDF-Datei exportieren. Von hier aus können Sie die PDF-Datei mit Ihrem Schullogo anpassen, indem Sie ein Logo hinzufügen und den Ordner angeben, an den die PDF-Datei exportiert wird.

Exportordner einstellen
Klicken Sie auf ..., um den Ordner anzugeben, an den die PDF-Datei exportiert wird.

Hinweis: Diese Option erscheint nur in der Bildungswesen-Edition von NetSupport DNA.

NetSupport DNA Cloud Konsole

Zusätzlich zur Windows Hauptkonsole bietet NetSupport DNA eine eSafety-Konsole auf Cloud-Basis, die außerhalb des lokalen Netzwerks benutzt werden kann und Konsolenbedienern von jedem beliebigen Gerät Zugriff auf die Daten ermöglicht. Eine für Smartphones optimierte Benutzeroberfläche ermöglicht es dem eSafety-Personal, schnell nach einem spezifischen Schüler zu suchen und kürzlich gemeldete Alerts oder Anliegen zu überprüfen.

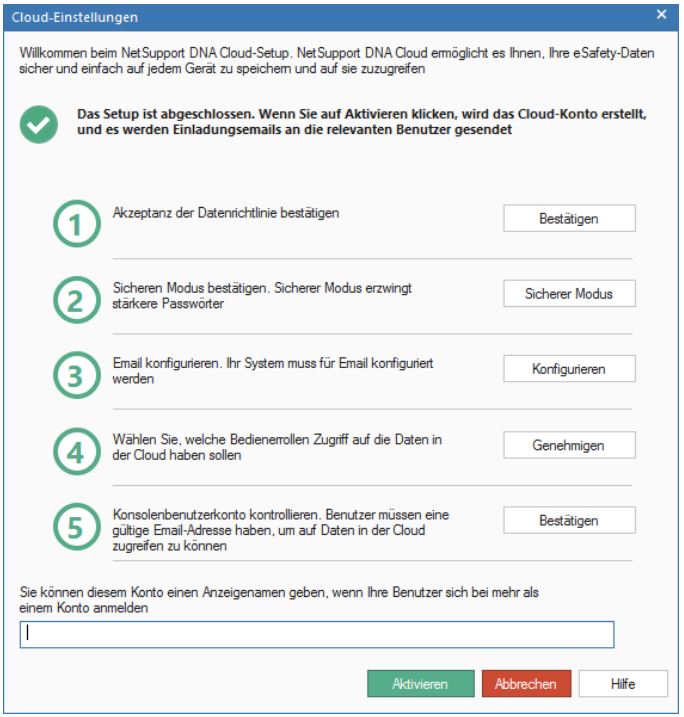
Hinweise:

- Diese Funktion steht nur in der NetSupport DNA Version für das Bildungswesen zur Verfügung.
- In dieser Version der DNA Cloud-Konsole sind nur die eSafety-Komponenten, Begriffsüberwachung, Anliegen Melden und die Risikoanalyse aktiviert.
- Wenn Sie die Funktion Ein **Anliegen über eine Website** melden benutzen möchten, muss auch die Cloud-Konsole aktiviert werden.

Zugriff auf die Cloud Konsole aktivieren

1. Klicken Sie in der Einstellungen Registerkarte auf dem **Cloud-Einstellungen** Symbol im Menüband.
   Oder
   Klicken Sie in der grünen Kopfzeile an der Konsole, wenn diese gezeigt wird, auf **Setup**.
2. Nun erscheint der Cloud-Einstellungen Dialog. Dieser leitet Sie durch die erforderlichen Schritte für die Einrichtung des Cloud-Zugriffs.

   Hinweis: Wenn ein Schritt abgeschlossen ist, erscheint er in grün.



Schritt 1
Klicken Sie auf **Bestätigen,** um die Cloud Benutzerrichtlinie zu akzeptieren. Lesen Sie die Richtlinie und wählen Sie **Ich habe diese Richtlinie gelesen und stimme ihr zu** und klicken Sie dann auf **OK**.

Schritt 2
Wir empfehlen, Sicheren Modus zu aktivieren, da dieser die Konsolenbediener zwingt, komplexe Passwörter zu benutzen, die die Sicherheit bei der Benutzung der Cloud erhöhen. Klicken Sie auf **Sicherer Modus**.

Schritt 3
Bevor Sie fortfahren können, müssen die Emaileinstellungen für NetSupport DNA konfiguriert werden. Klicken Sie auf **Konfigurieren**.

Schritt 4
Sie müssen wählen, welche Bedienerrollen Zugriff auf die Cloud haben sollen; klicken Sie auf **Genehmigen**. Nun erscheint eine Liste der verfügbaren Rollen. Wählen Sie die geforderten Rollen für den Cloud-Zugriff. Um eine neue Rolle zu erstellen, klicken Sie auf **Rollen**.

Hinweis: In der Standardeinstellung hat der Systemadministrator immer Zugriff auf die Cloud.

Schritt 5
Wenn Sie noch keine Emailadressen für Ihre Benutzer eingestellt haben, müssen Sie dies tun, damit Cloud-Zugriff aktiviert werden kann. Klicken Sie auf **Bestätigen**. Nun erscheint eine Liste verfügbarer Benutzer, denen Rollen mit aktiviertem Cloud-Zugriff zugewiesen worden sind. Geben Sie eine gültige Emailadresse ein und klicken Sie auf **OK**.

Hinweis: Dies ist die Emailadresse, mit der sich die Benutzer bei der Cloud-Konsole anmelden werden.

3. Falls erforderlich, können Sie einen Namen für das Cloud-Konto eingeben. Dies kann nützlich sein, wenn Benutzer Zugriff auf mehr als ein Konto haben.
4. Wenn alle Schritte grün sind, klicken Sie auf **Aktivieren**.
5. Es wird ein Konto in Microsoft Azure erstellt, und Ihre Daten werden ´mit der Cloud synchronisiert. Benutzer erhalten per Email eine Einladung, die es ihnen ermöglicht, sich bei der Cloud-Konsole anzumelden. Der Status der Cloud wird auf der Statusleiste angezeigt, und Sie können dort klicken, um auf die Cloud Konsole zuzugreifen.

Hinweis: Aus Sicherheitsgründen müssen Sie, wenn Sie sich zum ersten Mal anmelden (oder wenn ein existierender Bediener seine Emailadresse ändert), eine PIN eingeben (die Sie in der Emaileinladung erhalten), um zu bestätigen, wer Sie sind. Sie können bei der Bearbeitung der Konsolenbediener manuell per Email eine PIN senden oder erneut senden.

Um Zugriff auf die Cloud-Konsole zu deaktivieren, klicken Sie im Cloud-Einstellungen Dialog auf **Deaktivieren**. Dann werden alle in der Cloud gespeicherten Daten gelöscht.

Website-Anliegen verwalten

Zusätzlich zu der Option, ein Anliegen über ein DNA Agent aktiviertes Gerät zu melden, können Sie gefährdeten Schülern auch einen benutzerdefinierten Ein Anliegen melden Link auf einer Website bieten, beispielsweise auf der Website Ihrer Schule, den die Schüler außerhalb der Unterrichtszeiten benutzen können oder wenn sie gerade keinen Zugriff auf ein Agent-Gerät haben.

Hinweise:

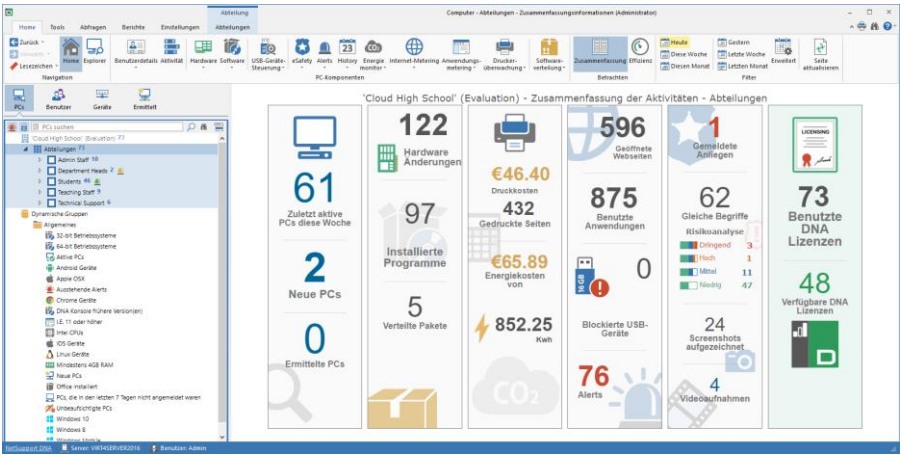
- Steht nur in der Bildungswesen Edition von NetSupport DNA zur Verfügung.
- Die NetSupport DNA Cloud-Konsole muss aktiviert sein, damit Sie diese Funktion benutzen können.

Anweisungen dafür, wie Sie diese Funktion konfigurieren und implentieren können, finden Sie unter dem Thema '**Ein Anliegen über eine Website melden**' im eSafety Abschnitt in diesem Handbuch.

VERWENDUNG VON NETSUPPORT DNA

Konsolefenster - Zusammenfassungsbildschirm

Die Zusammenfassungsanzeige bietet einen Überblick über die wichtigsten NetSupport DNA Funktionen. Von hier aus können Sie schnell zum eigentlichen Informationsfenster für diese Komponente gehen, indem Sie auf dem entsprechenden Symbol klicken. Außerdem erhalten Sie eine Zusammenfassung Ihrer NetSupport DNA Lizenzen, und wenn Sie dadraf klicken, erscheinen Ihre ausführlichen Lizenzinformationen.



Wie bei allen DNA-Komponenten lassen sich die Daten auf den Ebenen Unternehmen, Abteilung, AD Container, dynamische Gruppe oder Agent betrachten. Wählen Sie hierzu einfach in der Strukturansicht die gewünschte Option.

Die Daten können für eine vorgegebene Zeitspanne angezeigt werden. Um zwischen den verschiedenen Zeitperioden zu wechseln, klicken Sie das entsprechende Symbol im Ansicht-Bereich des Menübands an. Wenn Sie auf Erweitert klicken, können Sie einen benutzerdefinierten Datum-/Zeitfilter anwenden.

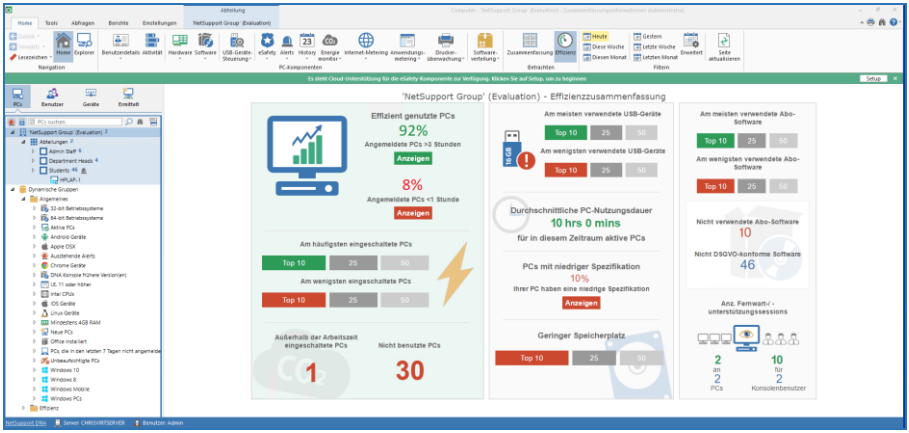
Sie können die Zusammenfassungsanzeige betrachten, indem Sie auf dem Home Symbol im Menüband klicken.

Hinweis: Standardmäßig wird die Zusammenfassung angezeigt. Wenn die Effizienzansicht angezeigt wird, auf das Symbol **Zusammenfassung** im Menüband klicken.

Sie können die Zusammenfassungsanzeige auch ausblenden – wählen Sie die Einstellungen-Registerkarte und klicken Sie das **Allgemeines** Symbol an. Nun erscheint der DNA Konfigurationsdialog. Klicken Sie auf der **Allgemeines** Option unter Konsolenanpassungen und deaktivieren Sie **Zusammenfassung/Effizienz Homepage anzeigen**. Dies kann nützlich sein, wenn Sie eine große Anzahl Systeme (1000+) haben, da in solchen Fällen die Anzeige der Zusammenfassungsseite zeitraubend sein kann.

Effizienzansicht

NetSupport DNA lässt Sie auf einen Blick sehen, wie effizient Hardware und Software in Ihrer Organisation verwendet werden. Die Effizienzansicht bietet ein Dashboard, das die Hauptbereiche der Effizienzdaten hervorhebt, beispielsweise wie viele PC außerhalb der Arbeitszeit eingeschaltet gelassen wurden, die Anzahl der ungenutzten PCs, die PCs mit der niedrigsten Spezifikation und dem geringsten Speicherplatz, die am häufigsten und am wenigsten genutzten USB-Geräte und Anwendungen und mehr. Durch Anklicken des entsprechenden Symbols im Dashboard können Sie die entsprechenden PCs identifizieren und Probleme managen, z.B. ungenutzte PCs außer Betrieb nehmen, sicherstellen, dass PCs über Nacht abgeschaltet werden und PCs mit niedriger Spezifikation aktualisieren.



1. Auf das Symbol **Homepage** im Menüband und dann auf **Effizienz** klicken.
2. Das Dashboard der Effizienzansicht wird angezeigt.

Die Daten können für einen gewählten Zeitraum angezeigt werden. Um zwischen verschiedenen Zeiträumen hin und her zu schalten, auf das entsprechende Symbol in der Menübandgruppe „Ansicht" klicken. Auf **Erweitert** klicken, um einen benutzerdefinierten Datumfilter anzuwenden.

Wenn Sie auf ein Symbol im Dashboard klicken, bringt Sie dies zu der entsprechenden dynamischen Gruppe im Effizienzordner in der Strukturansicht, so dass Sie die PCs in der relevanten Komponente sehen können (oder es wird ein Dialogfeld eingeblendet, das die gewünschten Daten anzeigt).

Damit NetSupport DNA weiß, welche Anwendungen als Abo-Software klassifiziert sind, müssen Sie sie der Kategorie Abo-Software im Anwendungsmanager zuordnen.

1. Das Symbol **Softwareinventar** im Menüband wählen.
2. Auf den Dropdown-Pfeil im Symbol **Softwareinventar** klicken und {Anwendungsmanager} aus dem Menü wählen
   oder
   auf das Symbol **Anwendungsmanager** in der Softwareinventargruppe klicken.
3. Der Softwaremanagerdialog wird eingeblendet. Das Register „Anwendungen" wählen.
4. Es wird eine Liste der Anwendungen angezeigt; die gewünschte Anwendung wählen und auf **Bearbeiten** klicken.
5. Im Abschnitt „Anwendungskategorien" auf **Zuordnen** klicken.
6. **Abo-Software** wählen und Sie auf **OK** klicken.
7. Auf **OK** klicken.
8. Diese Schritte für alle anderen Anwendungen wiederholen und auf **OK** klicken, wenn Sie fertig sind.
9. Die Anwendungen sind jetzt als Abo-Software klassifiziert.

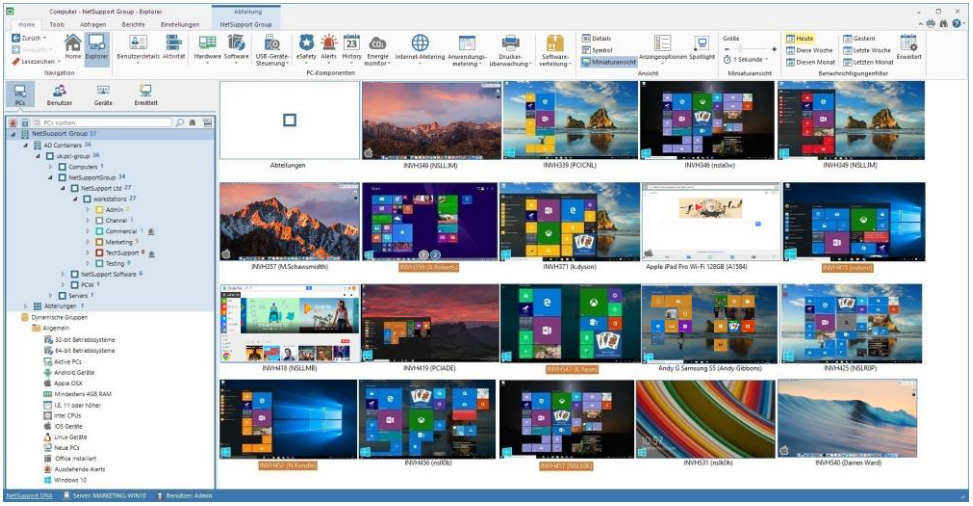
Explorer

Explorer-Modus bietet eine Real-Time-Übersicht aller PCs und Benutzer im Netzwerk, wobei die mit aktuellen Benachrichtigungen hervorgehoben werden, so dass Bediener sie schnell identifizieren und die Probleme lösen können. Es werden alle aktiven Richtlinien zusammen mit dem zugewiesenen Profil, den Leistungsdaten und vielen weiteren Informationen angezeigt. Die Datenansicht kann mit Symbolen, Details oder Miniaturansichten (in denen die PC-Bildschirme sichtbar sind) gezeigt werden. Datenschutz-Modus kann eingestellt werden, um Miniaturansichten weichzuzeichnen, was Datenschutz und Vertraulichkeit bietet.

Die **Spotlight**-Funktion dient ähnlichen Zwecken wie Task-Manager und bietet eine schnelle und leichte Methode, gegenwärtig an einem gewählten Agent-PC ausgeführte Prozesse und Dienste anzuzeigen und zu verwalten, hat aber den zusätzlichen Vorteil, dass sie Ihnen auch Interaktion mit offenen Anwendungen und Websites ermöglicht.

1. Klicken Sie auf dem **Explorer** Symbol im Menüband. Nun erscheint das Explorer-Fenster.

Hinweis: Wenn die Komponentensymbole ausgeblendet sind, klicken Sie auf die Registerkarte **Home**.



Die hierarchische Strukturansicht lässt sich zwischen PCs und Benutzern umschalten. Die PC-Strukturansicht zeigt PCs und den PC-Besitzer, der dem PC zugeordnet ist, und die Benutzer-Strukturansicht zeigt angemeldete Benutzer.

Wählen Sie in der hierarchischen Strukturansicht die Ebene, auf der Sie die Informationen betrachten möchten: Unternehmen, Abteilung, AD Container, dynamische Gruppe oder individueller Agent.

Das Informationsfenster zeigt nun die gewählten Agents. Wenn Sie einen Agent rechts anklicken, können Sie aus einer Reihe verfügbarer Funktionen wählen. Sie können zum Beispiel eine Nachricht senden, eine Chatsitzung starten, Geräte einschalten etc.

Hinweise:

- Sie können eine Fernwartungssitzung öffnen, indem Sie einen Agent doppelt anklicken. Vergewissern Sie sich, dass die Option **Für Fernwartung PC in Explorer doppelt anklicken** aktiviert ist. Wählen Sie die **Tools** Registerkarte und dann **Fernwartung konfigurieren**. Diese Funktion steht nur in der Bildungswesen-Edition von NetSupport DNA zur Verfügung oder in der Unternehmen-Edition, wenn Sie NetSupport Manager oder die Fernwartungsanwendung einer Drittpartei installiert haben.
- Wenn sich irgendwelche Agent-Geräte, die Sie fernwarten wollen, in einem Remote-Netzwerk befinden, müssen Sie Ihre externe (öffentliche) Gateway-Adresse in den Fernwartungseinstellungen eingeben, um die integrierten Fernwartungsfunktionen für diese Geräte zu aktivieren.

Benachrichtigungen werden angezeigt, wenn ein Agent einen Begriff* ausgelöst hat, ein Alert ausgelöst hat oder Genehmigung für ein USB-Gerät angefordert hat. In der Standardeinstellung werden Agents hervorgehoben, wenn sie eine Benachrichtigung haben. Um dies auszustellen, wählen Sie im Menüband **Optionen anzeigen** und deaktivieren Sie die Option **PCs mit Benachrichtigungen hervorheben**.

* Diese Funktionen stehen nur in der NetSupport DNA Version für das Bildungswesen zur Verfügung.

Benachrichtigungen können für eine vorgegebene Zeitperiode angezeigt werden. Um zwischen verschiedenen Zeitperioden zu wechseln, klicken Sie auf dem entsprechenden Symbol im Benachrichtigungsfilter-Abschnitt

im Menüband. Wenn Sie auf **Erweitert** klicken, können Sie einen benutzerdefinierten Datum-/Zeitfilter anwenden.

Die gezeigten Arbeitsstunden können im DNA Konfigurationskatalog für Ihre Organisation angepasst werden. Siehe Konsolenanpassungen – Allgemein für weitere Informationen.

Wenn der Agent auf einem Laptop oder einem Mobilgerät ausgeführt wird, werden in der Details- oder Miniaturansicht, der Drahtlos-Status und Akkustand angezeigt.

Hinweis: Um die Abteilung-Symbole im Informationsfenster auszublenden, wählen Sie im Menüband **Optionen anzeigen** und deaktivieren Sie die Option **Abteilungen zeigen**.

In der Benutzer-Strukturansicht können Sie wählen, nur die Benutzer anzuzeigen, die aktuell angemeldet sind. Klicken Sie dafür auf dem **Angemeldet-**Symbol im Menüband.

Agents können in drei Modi angezeigt werden:

Details
Im Informationsfenster wird eine detaillierte Ansicht der Agents aufgelistet. Der Agent-Computer/Benutzername, die Abteilung, IP-Adresse*, letzte Verbindungszeit*, der gegenwärtig angemeldete Benutzer*, zugeordnetes Profil und das Betriebssystem* werden zusammen mit Benachrichtigungen, aktiven Richtlinien (Einschalt- und Ausschaltzeitplan, Inaktivitätsrichtlinie, Web- und Anwendungseinschränkungen, USB, CD, Webcam, Miniaturansichten- und Datenschutzmodus-Richtlinien), leistungsdaten (CPU-Auslastung, Speicherauslastung, Netzwerkauslastung – empfangene/gesendete Bytes und freier Speicherplatz) und Akku- und Drahtlos-Anzeigen angezeigt.

* Diese Spalten werden in der Benutzerstruktur nicht angezeigt.

Hinweise:
- Um die angezeigten Spalten anzupassen, wählen Sie im Menüband **Optionen anzeigen** und wählen Sie dann, welche Spalten im PC/Benutzer-Spalten-Abschnitt angezeigt werden sollen.
- Leistungsdaten können hervorgehoben werden, wenn sie einen bestimmten vorgegebenen Grenzwert erreichen, so dass Sie Agents mit hoher CPU-, Speicher- oder Netzwerknutzung schnell erkennen können. Wählen Sie im Menüband **Anzeigeoptionen** und schieben Sie den Markieren-Schieberegler unter Leistungsdaten auf den gewünschten Stand.

Symbol
Zeigt ein Symbol für jeden Agent. Das Betriebssystem des Agents läuft, und es werden auch aktive Benachrichtungen angezeigt.

Miniaturansicht
Es wird eine Miniaturansicht der Agent-Bildschirme gezeigt. Wenn ein Agent mehrere Monitore benutzt, können Sie die Ansicht zwischen den beiden Monitoren hin- und herschalten. Wenn Sie einen Agent in der Strukturansicht gewählt haben, werden beide Monitore als Miniaturansicht gezeigt. Wenn ein Benutzer an mehr als einem Gerät angemeldet ist, wird in der Benutzer-Strukturansicht eine Miniaturansicht von jedem Gerät gezeigt. Neben dem Agent werden Symbole angezeigt, die zeigen, bei welchen Agents Miniaturansichten deaktiviert sind, wenn sie sich im Datenschutzmodus befinden.

Hinweise:
- Die Miniaturansichten-Ansicht kann in DNA Konfiguration – Explorer Einstellungen deaktiviert werden.
- Sie können wählen, nur Agents anzuzeigen, deren Miniaturansichten abgerufen werden können. Wählen Sie im Menüband **Optionen anzeigen** und dann die Option **Nur Geräte anzeigen, die Miniaturansichten unterstützen**.

Größe der Miniaturansicht anpassen
Die Größe der Agent-Miniaturansichten kann den individuellen Anforderungen entsprechend geändert werden.

1. Wählen Sie die geforderte Größe mit dem Größenschieberegler im Menüband.
   Oder
   Klicken Sie auf dem + oder – Symbol im Menüband.

Ändern der Aktualisierungsrate für Miniaturansichten
Je nachdem, wie genau Sie die Agent-Aktivitäten überwachen möchten, können Sie das Aktualisierungsintervall für die Miniaturansichten entsprechend einstellen.

1. Wählen Sie das  Dropdown-Menü im Menüband.
2. Wählen Sie das gewünschte Zeitintervall in den verfügbaren Optionen.

Datenschutz-Modus
Bei der Anzeige der Agent-Miniaturansichten kann der angezeigte Text weichgezeichnet werden, um ihn unleserlich zu machen.

1. Wählen Sie the Registerkarte Einstellungen.
2. Klicken Sie auf **Neues Profil erstellen,** um ein neues Profil zu erstellen, bei dem diese Einstellung aktiviert ist, oder klicken Sie auf **Existierendes Profil verwalten,** um Datenschutz-Modus in einem existierenden Profil zu aktivieren.
3. Im NetSupport DNA Konfiguration Dialog wählen Sie die **Explorer** Option.
4. Wählen Sie **Datenschutz-Modus**.

Abfragen
Wählen Sie zur Anzeige des Abfragefensters die Registerkarte „Abfragen".

Mit dem Abfragetool von DNA können Sie Datenbankeinträge abrufen, die bestimmte Kriterien erfüllen. Abfragen zu der Komponente, die gerade betrachtet wird, sind aufgelistet, was ein schnelles Abrufen der Ergebnisse ermöglicht.

Klicken Sie in der Menüleiste auf dem **Abfrage hinzufügen** Symbol, um eine neue Abfrage zu erstellen, oder klicken Sie auf dem **Abfrage bearbeiten** Symbol in der Menüleiste, um ein in der Liste vorhandenes Objekt zu bearbeiten.

Berichte
Wählen Sie zur Anzeige des Berichtfensters die Registerkarte „Berichte".

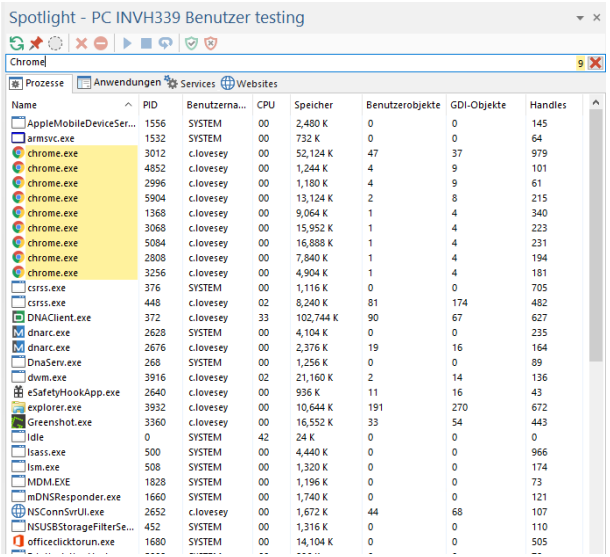
Jeder Komponente ist eine Reihe von vordefinierten Managementberichten, die vom Crystal Reports-Modul gespeist werden, beigefügt. Wählen Sie den geforderten Bericht in der Dropdown-Liste. Die Ergebnisse erscheinen im Informationsfenster. Sie lassen sich ggf. exportieren.

Die Häufigkeit, mit der der Server Daten sammelt, lässt sich mit der Option "DNA-Einstellungen" ändern.

Spotlight

Die **Spotlight**-Funktion in **Explorer**-Modus dient ähnlichen Zwecken wie Task-Manager. Sie bietet eine schnelle und leichte Methode, gegenwärtig an einem gewählten Agent-PC ausgeführte Prozesse und Dienste anzuzeigen und zu verwalten, hat aber den zusätzlichen Vorteil, dass sie Ihnen auch die Interaktion mit offenen Anwendungen und Websites ermöglicht.

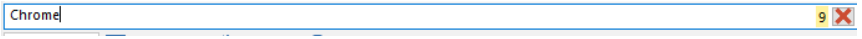
1. Klicken Sie auf dem **Explorer** Symbol im Menüband.
2. Klicken Sie im **Ansicht** Abschnitt des Menübands auf **Spotlight**. Nun erscheint der Spotlight Bereich im Informationsfenster. Der Spotlight-Bereich kann 'angedockt' oder 'unverankert' sein. Klicken Sie auf der Nach-unten-Taste oben rechts in dem Bereich oder klicken Sie eine freie Fläche rechts an, und wählen Sie dann die gewünschte Option. Wenn Sie vom Explorer-Modus weg gehen, bleibt der Spotlight-Bereich sichtbar.
3. Wenn in der Hierarchiestruktur oder im Informationsfenster noch kein Agent-Gerät gewählt worden ist, werden Sie nun aufgefordert, eins zu wählen.
4. Wenn Sie eins gewählt haben, werden die gegenwärtig ausgeführten Prozesse, Anwendungen, Dienste und aktiven Websites aktualisiert. Klicken Sie auf jeder Registerkarte, um den gegenwärtigen Status von jeder der vier Optionen zu sehen.



Hinweis: Die Titelleiste des Spotlight Bereichs zeigt an, ob **Datenschutzmodus** gegenwärtig aktiv ist. Dies wird bestimmte Spotlight-Funktionen deaktivieren, wie unten beschrieben.

Suchleiste

Die Suchleiste ermöglicht es Ihnen, spezifische Elemente schnell in jeder Liste zu identifizieren. Geben Sie einfach die geforderten Kriterien ein, und die übereinstimmenden Elemente werden hervorgehoben. Die Leiste zeigt an, wie viele übereinstimmende Elemente es gibt.



Symbolleiste

Die Symbole auf der Symbolleiste haben folgende Funktionen:

	Liste(n) aktualisieren	Fordert den gewählten Agent PC auf, die Daten für jede Registerkarte neu zu senden.
	Heftet den gewählten PC an	Hält die gegenwärtig angezeigten Informationen auf dem Bildschirm, während Sie zu anderen PCs navigieren, um verschiedene Aufgaben auszuführen. Sie müssen den aktuellen PC lösen, um die Daten von einem anderen Gerät anzeigen zu können.
	Aktuellen PC löschen	Dies löscht alles im Spotlight-Bereich, egal ob ein PC angeheftet ist oder nicht. Der Bereich wird nicht geschlossen. Dies ist nützlich, um einen angehefteten PC zu löschen, und auch um alles im Bereich zu löschen, wenn Sie den Explorer-Modus verlassen.
	Prozess oder Anwendung schließen	Bezieht sich auf die Prozess- und Anwendungen-Registerkarten; schließt den gewählten Prozess bzw. die gewählte Anwendung.

	Anwendung blockieren	Bezieht sich auf die Anwendungen-Registerkarte; ermöglicht es Ihnen, den Fenstertitel der gewählten Anwendung schnell zu einer Blockiert-Liste hinzuzufügen. Der Anwendungsblockierung hinzufügen Dialog erscheint, der es Ihnen ermöglicht, den angezeigten Titel falls erforderlich zu bearbeiten und ein Profil zu wählen, zu dem das Element hinzugefügt werden soll. **Hinweis:** Wenn **Datenschutzmodus** aktiv ist, werden die Anwendungstitel maskiert, und die Blockieren-Option wird deaktiviert.
	Dienst starten	Gilt für die Dienste-Registerkarte; startet den gewählten Dienst.
	Dienst beenden	Gilt für die Dienste-Registerkarte; beendet den gewählten Dienst.
	Dienst neu starten	Gilt für die Dienste-Registerkarte; startet den gewählten Dienst erneut.
	URL genehmigen	Gilt für die Websites Registerkarte; fügt die gewählte URL zu einer Liste genehmigter Websites hinzu. Nun erscheint der Website hinzufügen Dialog, der es Ihnen ermöglicht, die URL-Details falls erforderlich zu bearbeiten und eine URL-Liste zu wählen, zu der das Element hinzugefügt werden soll. **Hinweis:** Wenn Datenschutzmodus aktiv ist, ist diese Option deaktiviert, und URLs werden nicht angezeigt.
	URL einschränken	Gilt für die Websites Registerkarte; fügt die gewählte URL zu einer Liste eingeschränkter Websites hinzu. Nun erscheint der Website hinzufügen Dialog, der es Ihnen ermöglicht, die URL-Details falls erforderlich zu bearbeiten und eine URL-Liste zu wählen, zu der das Element hinzugefügt werden soll. **Hinweis:** Wenn Datenschutzmodus aktiv ist, ist diese Option deaktiviert, und URLs werden nicht angezeigt.

Hinweis: Sie können die Aktionen nicht nur über die Symbolleistensymbole ausführen sondern auch, indem Sie ein Element in jeder der Listen rechts anklicken.

Benutzerdetails

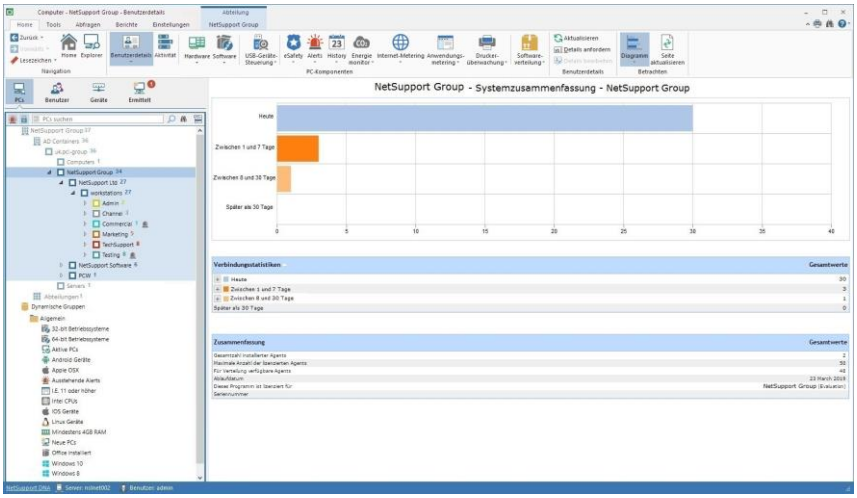
NetSupport DNA bietet eine Reihe von Funktionen zur Auffindung und Verwaltung von Benutzern innerhalb einer Netzwerkumgebung. Außer den Hauptbenutzerdaten (Name, Telefon etc) bietet DNA dem Kunden die Fähigkeit, die für jeden Gerätebenutzer zu sammelnden und zu sortierenden Daten anzupassen, einschließlich Nachverfolgung des Benutzerakzeptanzfomulars. DNA erfasst auch einen Änderungsverlauf für die in Benutzerdaten eingegebenen Daten. Änderungen der Benutzerangaben werden aufgezeichnet, einschließlich der folgenden Felder: Personalnummer, Ort, Bestandskennzeichen und Besitzer.

Hinweis: Es gibt eine Active Directory Policy, mit der sich Benutzerdetails aus Active Directory abrufen lassen. Wenn die betreffenden Informationen verfügbar sind, werden Name, Firma, E-Mail-Adresse, Handy, Pager, Telefonnummer und Ort abgerufen und im Dialogfeld „Benutzerdetails" angezeigt. Diese Details sind nicht zur Bearbeitung in DNA verfügbar und alle Änderungen müssen über Active Directory vorgenommen werden. Solche Änderungen werden dann von DNA automatisch übernommen.

NetSupport DNA ermöglicht es Ihnen auch, Active Directory Konten zu verwalten und die Benutzerkonten anzuzeigen, die deaktivert oder gesperrt worden sind, so dass Sie diese, falls erforderlich, schnell entsperren oder zurückstellen können.

1. Klicken Sie auf das Symbol **Benutzerdetails** im Ribbon. Das Dialogfeld „Benutzerdetails" wird eingeblendet.

   Hinweis: Wenn die Komponentensymbole ausgeblendet sind, klicken Sie auf die Registerkarte **Home**.



Die hierarchische Strukturansicht lässt sich zwischen PCs und Benutzern umschalten. Die Strukturansicht des PCs zeigt Daten für PCs und den PC-Eigentümer, der mit dem betreffenden PC verknüpft ist. Die Benutzerstrukturansicht zeigt Daten für die angemeldeten Benutzer und nicht auf PCs bezogene Daten.

Wenn DNA eine Verbindung zu einem PC herstellt, wird der angemeldete Benutzer automatisch zum PC-Eigentümer, vorausgesetzt dass er nicht schon Eigentümer eines anderen PCs ist. Wenn dies nicht erwünscht ist, können Sie im Dialogfeld „Benutzer binden" eine neue Benutzerzuweisung vornehmen.

Hinweis: Ein PC kann nur einen PC-Eigentümer haben, während ein Benutzer Eigentümer von mehr als einem PC sein kann. Sie können Benutzern im Dialogfeld „Benutzerdetails bearbeiten" PCs zuweisen.

Wählen Sie in der hierarchischen Strukturansicht die Ebene, auf der Sie die Informationen betrachten möchten: Unternehmen, Abteilung, AD Container ,dynamische Gruppe oder individueller Agent.

Im Fenster "Benutzerdetails" sehen Sie die Gesamtzahl der DNA Agent-Serververbindungen für verschiedene Zeitspannen in Grafik- und Listenformat. Um den Graph in einem anderen Format anzuzeigen, klicken Sie auf dem **Diagramm**-Symbol-Dropdownpfeil in der Menüleiste und wählen das entsprechende Format. Um die aktive Ansicht auszudrucken, klicken Sie auf dem Symbol oben auf der Konsole.

Hinweis: Durch Anklicken des Chart-Symbols im Ribbon wird die Grafik ein-/ausgeblendet.

Verbindungsstatistiken mit Angabe von PC-Anwender, PC-Eigentümer, Abteilung und letzter Verbindung sind für jeden DNA Agent aufgeführt und lassen sich für das ganze Unternehmen, eine Abteilung oder eine dynamische Gruppe betrachten. Beim Betrachten auf Unternehmens- oder Abteilungsebene wird gleichzeitig eine Zusammenfassung Ihrer NetSupport DNA-Lizenzdetails eingeblendet.

Beim Betrachten von Daten auf Agentebene können Sie zwischen „Allgemein" (PC Eigentümer-, Asset- und Wartungsinformationen) und Anmeldesessions (PC/Benutzer-Anmeldeinformationen). Klicken Sie im Benutzerangaben-Menüband auf dm entsprechenden Symbol oder klicken Sie auf dem Benutzerangaben-Dropdown-Symbol und wählen Sie {Anzeigen- Allgemeines/Anmeldungssitzungen}.

In der Benutzerstrukturansicht werden alle Agent-Anmeldesessions für die gewählte Zeitspanne angezeigt. Sie können die Daten für eine spezifische Zeitperiode betrachten. Um zwischen verschiedenen Zeitperioden hin- und herzuschalten, klicken Sie das entsprechende Symbol im Filterbereich des Menübands an. Wenn Sie auf Erweitert klicken, können Sie einen benutzerdefinierten Datum-/Zeitfilter anwenden. Aufgelistete Beschreibungen lassen sich erweitern, so dass Sie ein individuelles Agentbreakdown für jedes Objekt erhalten. Die gezeigten Arbeitsstunden können im DNA Konfigurationskatalog für Ihre Organisation angepasst werden. Siehe Konsolenanpassungen – Allgemein für weitere Informationen.

Active Directory Benutzerkonten können verwaltet werden, so dass Sie Konten entsperren, Konten aktivieren oder deaktivieren und Passwörter einstellen können. Klicken Sie einen Agent in der Benutzerstruktur mit der rechten Maustaste an und wählen Sie **Benutzerkonto verwalten**.

In der Bildungswesen-Version von NetSupport DNA können Sie Agents (Schüler) als gefährdet markieren. Auf diese Weise können gefährdete Schüler von eSafety Benutzern leicht identifiziert und unterstützt werden. Schüler können im Benutzer bearbeiten Dialog als gefährdet markiert werden oder indem man den Schüler in der Benutzer-Strukturansicht rechts anklickt und **Gefährdeter Schüler** wählt. Der Schüler wird dann in der entsprechenden dynamischen Gruppe in der Benutzer-Strukturansicht gezeigt.

Hinweis: Das in der Konsole angezeigte Datum-/Zeitformat stimmt mit dem Format in dem Rechner, in dem der DNA Server installiert ist, überein. Um das Format in der Konsole zu ändern, müssen Sie zunächst das Format in diesem Rechner ändern. Für weitere Informationen wenden Sie sich bitte an unser Support-Team www.netsupportsoftware.com/support.

Mit einer Schnellaktualisierungsfunktion können Sie Daten außerhalb der angegebenen Häufigkeit aktualisieren. Dies kann nützlich sein, wenn Sie bestimmte Agents oder Abteilungen anpeilen möchten. Klicken Sie mit der rechten Maustaste auf das gewünschte Objekt in der Strukturansicht und wählen Sie „Aktualisieren" oder klicken Sie im Menü oder Ribbon „Benutzerdetails" auf „Aktualisieren".

Abfragen

Wählen Sie zur Anzeige des Abfragefensters die Registerkarte „Abfragen".

Mit dem Abfragetool von DNA können Sie Datenbankeinträge abrufen, die bestimmte Kriterien erfüllen. Abfragen zu der Komponente, die gerade betrachtet wird, sind aufgelistet, was ein schnelles Abrufen der Ergebnisse ermöglicht.

Klicken Sie in der Menüleiste auf dem Abfrage hinzufügen Symbol, um eine neue Abfrage zu erstellen, oder klicken Sie auf dem Abfrage bearbeiten Symbol in der Menüleiste, um ein in der Liste vorhandenes Objekt zu bearbeiten.

Berichte

Wählen Sie zur Anzeige des Berichtfensters die Registerkarte „Berichte".

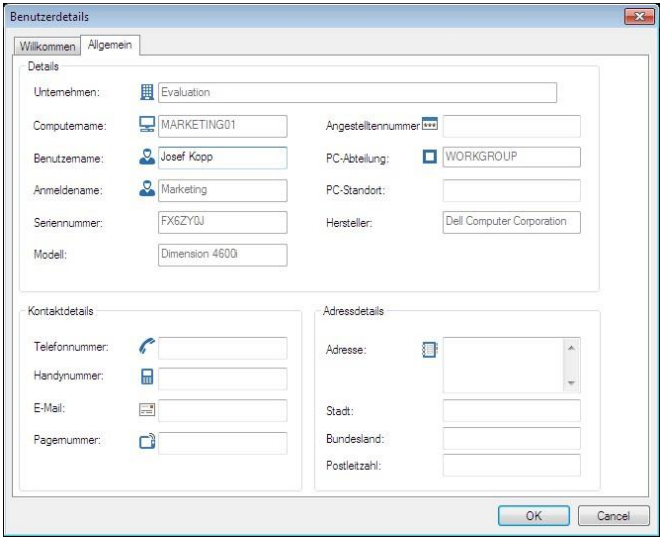
Jeder Komponente ist eine Reihe von vordefinierten Managementberichten, die vom Crystal Reports-Modul gespeist werden, beigefügt. Wählen Sie den geforderten Bericht in der Dropdown-Liste. Sie lassen sich ggf. Exportieren.

Benutzerdetails anfordern/bearbeiten

Benutzer und damit verknüpfte Inventardetails lassen sich durch die Agents selbst oder durch Konsolebediener mit den entsprechenden Befugnissen aktualisieren.

Über die Option Aktuelle Benutzerdaten anfordern können Konsolebediener entfernt auf den Agent PCs das Dialogfeld "Benutzerdetails" starten.

1. Während die Registerkarte "Benutzerdetails" ausgewählt ist, markieren Sie einen Agent, eine Abteilung, eine AD Container oder das Unternehmen in der PCs Strukturansicht.
2. Klicken Sie mit der rechten Maustaste und wählen Sie **Details anfordern**.
   Oder
   Klicken Sie auf den Dropdownpfeil für das Symbol der Benutzerdetails und wählen Sie im Menü die Option {Details anfordern}.
   Oder
   Klicken Sie auf das Symbol **Details anfordern** in der Gruppe **Benutzerdetails**.
3. Auf den gewählten Rechnern wird das Dialogfeld "Benutzerdetails" eingeblendet. Hier können Agents Ihre Informationen ergänzen oder aktualisieren.



Beim Start auf den Agent PCs wird standardmäßig eine Begrüßungsseite eingeblendet. Diese kann benutzerdefinierbare Meldungen/Eingabeaufforderungen enthalten oder Sie kann mit der Einstellungsoption für Benutzerdetails deaktiviert werden. Weitere Angaben hierzu finden Sie unter "DNA-Einstellungen" .

Beim Agent

Agents können ihre eigenen Benutzer- und Inventardetails aktualisieren.

1. Klicken Sie mit der rechten Maustaste auf das Agentsymbol in der Taskleiste und wählen Sie **Benutzerdetails bearbeiten**.
2. Das Dialogfeld "Benutzerdetails" wird eingeblendet.

Bearbeiten der Benutzerangaben

Konsoleoperatoren mit der nötigen Berechtigung können die Informationen für einen bestimmten Agent bearbeiten. Operatoren können sowohl in der Strukturansicht des PCs als auch in der Benutzerstrukturansicht Benutzerdetails für Agents bearbeiten.

Hinweis: Beim Bearbeiten von Benutzerdetails in der Benutzerstrukturansicht werden nur Benutzerinformationen und keine Asset-Details angezeigt.

Bearbeiten der Benutzerangaben von der PC-Strukturansicht aus

1. Wählen Sie in der Strukturansicht des PCs einen Agent aus.
2. Klicken Sie mit der rechten Maustaste und wählen Sie **Details bearbeiten**.
   Oder
   Klicken Sie auf den Dropdownpfeil für das Symbol der Benutzerdetails und wählen Sie im Menü die Option {Details bearbeiten}.
   Oder
   Klicken Sie auf das Symbol **Details bearbeiten** in der Gruppe **Benutzerdetails**.
3. Das Dialogfeld "Benutzerdetails" wird eingeblendet.
4. Hier können Sie allgemeine Agent- und Asset-Details bearbeiten und Leasing- oder Wartungsinformationen betrachten.

Hinweis: Mit jedem PC ist ein PC-Eigentümer verknüpft. Wenn dies nicht erwünscht ist, können Sie den PC-Eigentümer im Dialogfeld „Benutzer binden" ändern. Ein PC kann nur einen PC-Eigentümer haben.

Bearbeiten der Benutzerangaben von der Benutzer-Strukturansicht aus

1. Wählen Sie in der Benutzerstrukturansicht einen Agent aus.
2. Klicken Sie mit der rechten Maustaste und wählen Sie **Bearbeiten**.
   Oder
   Klicken Sie auf den Dropdownpfeil für das Symbol der Benutzerdetails und wählen Sie im Menü die Option {Details bearbeiten}.
   Oder
   Klicken Sie auf das Symbol **Details bearbeiten** in der Gruppe **Benutzerdetails**.
3. Das Dialogfeld "Benutzerdetails" wird eingeblendet.
4. Hier können Sie die allgemeinen Details des Agents bearbeiten. Alle PCs, deren Eigentümer der betreffende Benutzer ist, werden eingeblendet. Klicken Sie auf , um PCs hinzuzufügen oder zu entfernen. Benutzer können Eigentümer von mehr als einem PC sein.

Hinweis: In der Bildungswesen-Version von NetSupport DNA können Sie wählen, gefährdete Schüler zu identifizieren. Wählen Sie die Option **Diesen Schüler als gefährdet markieren.** (Diese Option erscheint nur, wenn wenn die Benutzerdetails von der Benutzerstruktur aus bearbeitet werden.) Gefährdete Schüler werden dann in der dynamischen Gruppe Gefährdete Schüler angezeigt. Die Dynamische Gruppen Liste in der Struktur muss aktualisiert werden, um diese anzuzeigen.

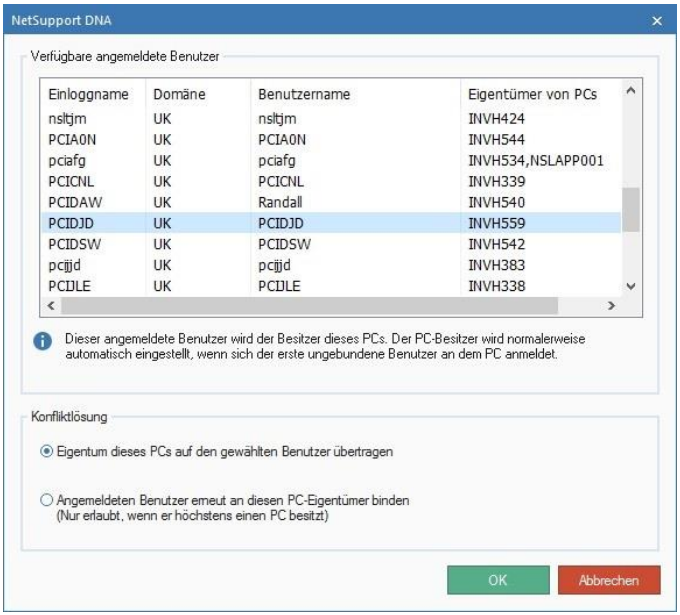
Dialogfeld „Benutzer binden"

Wenn DNA eine Verbindung zu einem Agent PC herstellt, bindet es den angemeldeten Benutzer automatisch als Eigentümer an den betreffenden PC, vorausgesetzt dass dieser Benutzer nicht bereits Eigentümer von anderen PCs ist. Es kann vorkommen, dass der falsche Benutzer an einen PC gebunden ist. In solchen Fällen können Sie den Eigentümer des PCs mithilfe des Dialogfelds „Benutzer binden" ändern.

Es gibt zwei Methoden zur Neuzuweisung des PC-Eigentümers. „Eigentum übertragen": Hiermit wird der ausgewählte angemeldete Benutzer zum Eigentümer des PCs. Der neue Benutzer übernimmt dabei sämtliche Benutzerdetails und alle vorherigen Benutzerdaten für diesen PC werden gelöscht. „Angemeldeten Benutzer neu binden": Hiermit wird der angemeldete Benutzer als Eigentümer an diesen PC gebunden, aber die bereits mit dem PC verknüpften Benutzerdetails bleiben erhalten, es werden nur die Anmeldedetails des Benutzers geändert. Diese Methode ist nur dann zugelassen, wenn der angemeldete Benutzer nicht Eigentümer von mehr als einem PC ist.

Hinweis: Sie können auch über das Dialogfeld „Benutzerdetails bearbeiten" in der Benutzerstrukturansicht einen PC an einen Benutzer binden.

1. Wählen Sie den gewünschten PC in der Strukturansicht des PCs.
2. Klicken Sie mit der rechten Maustaste und wählen Sie **PC-Eigentümer ändern**.
   Oder
   Klicken Sie auf den Dropdownpfeil für das Symbol der Benutzerdetails und wählen Sie im Menü die Option {PC-Eigentümer ändern}.
3. Das Dialogfeld „Benutzer binden" wird eingeblendet.



4. Die verfügbaren Anmeldenamen werden zusammen mit allen PCs, die bereits Eigentümer haben, eingeblendet (Sie müssen nach rechts scrollen, um diese zu sehen).
5. Wählen Sie den Anmeldenamen, an den Sie das Eigentum übertragen wollen, und wählen Sie die gewünschte Auflösung.
6. Klicken Sie auf **OK**.

Angepasste Benutzerdetails

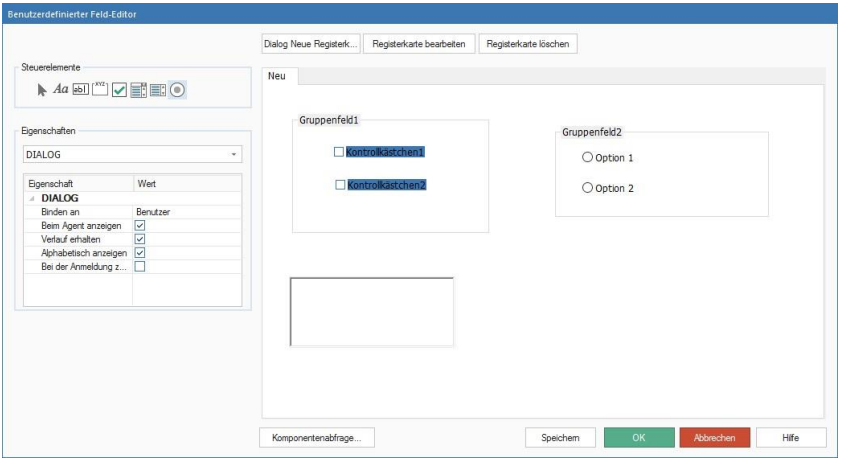
Standardmäßig wird eine Reihe von Benutzer- und Inventarinformationen dynamisch aufgezeichnet. Die Daten lassen sich mit den Optionen "Benutzerdetails anfordern" und "Benutzerdetails bearbeiten" aktualisieren.

Wenn die Standardseiten, "Allgemein" und "Inventar", Ihren Anforderungen nicht vollständig gerecht werden, können Sie zusätzliche angepasste Registerkarten erstellen.

1. Klicken Sie in der Registerkarte „Werkzeuge" auf das Symbol **Angepasste Benutzerdetails**.

   Oder

   Klicken Sie auf den Dropdownpfeil für das Symbol der Benutzerdetails und wählen Sie im Menü die Option {Angepasste Benutzerdetails}.
2. Das Dialogfeld **Editor für benutzerdefinierte Felder** wird eingeblendet. Hier können Sie eine beliebige Anzahl von angepassten Registerkarten erstellen.



3. Klicken Sie auf **Neue Registerkarte**, um eine neue Seite zu erstellen und einen passenden Namen einzugeben. Um Zeit zu sparen, können Sie den Inhalt einer vorhandenen Registerkarte kopieren, falls Sie ähnliche Felder benötigen. (Mit **Registerkarte bearbeiten** lässt sich der Name einer vorhandenen Seite ändern.) Klicken Sie auf **OK**.
4. Geben Sie die Eigenschaften für die Registerkarte ein.

5. Entscheiden Sie, ob Informationen auf der neuen Registerkarte beim Betrachten des Fensters "Benutzerdetails" mit dem angemeldeten Benutzer oder dem physikalischen PC verknüpft sein sollen.
6. Sie können die Registerkarte für Benutzer ausblenden, wenn Sie möchten, dass ausschließlich Konsolebenutzer die Informationen aktualisieren können. Heben Sie die Markierung des Feldes Beim Agent anzeigen auf, um diese Registerkarte beim Start des Dialogfelds "Benutzerdetails" auf den Agent PCs auszuschließen.
7. **Änderungshistory pflegen.** Wenn diese Option markiert ist, werden alle Änderungen an den Benutzer-/Inventardaten auf dieser Seite festgehalten. Um den Änderungen betrachten, klicken Sie auf das Symbol **Verlauf** im Ribbon.
8. Die Reihenfolge der Felder wird alphabetisch in der Konsolenansicht angezeigt. Heben Sie die Markierung von **Alphabetisch in 'Konsolenansicht' anzeigen** auf, um die Reihenfolge der Felder zu steuern.
9. Beim Aufbau der Seite müssen Sie die passenden Steuerelemente hinzufügen. Wählen Sie einen Control und ziehen ihn mit der Drag&&Drop-Funktion an den gewünschten Ort auf der Seite.
10. Geben Sie die Eigenschaften und assoziierten Werte für jeden Control ein.
11. Durch Klicken auf **Speichern** können Sie die neue Seite jederzeit absichern.
12. Klicken Sie auf **OK**, wenn die Seite vollständig ist.

Komponentenabfrage

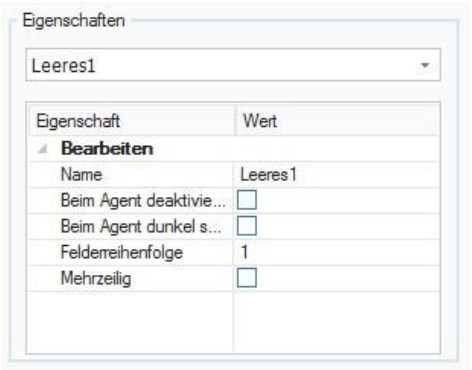
Klicken Sie auf diese Option zur Erstellung eines vorgefertigten Berichts, der die Felder auf der Seite enthält. Zum Laden, Bearbeiten und Ausführen der Ausgabe verwenden Sie das Abfragetool.

Angepasste Benutzerdetails - Steuerelemente

Eine benutzerdefinierte Benutzer/Inventar-Registerkarte kann verschiedene Steuerelemente/Eingabefelder beinhalten.



Wählen Sie den gewünschten Control, ziehen ihn mit der Drag&&Drop-Funktion an den gewünschten Ort auf der Seite und geben die assoziierten Eigenschaften ein.



	Zweck	Eigenschaften
	Dient dazu, Objekte auf der Seite zu verschieben und ihre Größe zu verändern.	
Aa	Ermöglicht das Hinzufügen der Textbeschreibungen für die einzelnen Eingabefelder. Die Beschreibungen sind auf der Registerkarte als Leitfaden für Benutzer beim Aktualisieren ihrer Details angezeigt, aber im Informationsfenster "Benutzer-details" auf der Konsole erscheinen sie nicht.	Mit der Drag&Drop-Funktion an den gewünschten Ort ziehen. Jedes Mal, wenn dieses Steuerelement hinzugefügt wird, erhält es zunächst einmal einen sequenzielen Namen, Text 1, Text 2, usw. Ändern Sie zur Eingabe der gewünschten Feldbeschreibung die Steuereigenschaften. Im Fenster "Eigenschaften" sind zwei Objekte aufgeführt. Der Name des Steuerelements und der aktuell zugewiesene Textwert. Ersetzen Sie den Textwert mit Ihrer eigenen Bezeichnung.

	Erstellt ein Textfeld, in das Benutzer freien Text eingeben können. Zu Eingabezwecken würden Sie generell neben dem Feld ein Textbeschreibungs-element hinzufügen. Im Informationsfenster "Benutzer-details" an der Konsole kann Beschreibungstext eingegeben werden.	Im Fenster "Eigenschaften" ist diesem Steuerelement der Name Edit 1, Edit 2, usw. zugewiesen. Diese Beschreibung erscheint im Informationsfenster "Benutzerdetails", wenn Sie die Eigenschaften nicht ändern. Ändern Sie den Wert für die Eigenschaft Name auf die gewünschte Bezeichnung. Mit den beiden anderen Eigenschaften, Beim Agent deaktivieren und Beim Agent dunkel schalten, kann das Feld bei Benutzern ebenfalls ausgeblendet werden, d. h. dass nur Bediener die Details aktualisieren können. Damit Text auf mehr als einer Zeile eingegeben werden kann, aktivieren Sie die Option Mehrzeilig. Um die Reihenfolge der Anzeigefelder in der Konsole festzulegen, klicken Sie auf Feldreihenfolge. Klicken Sie auf das erscheinende Symbol und das Dialogfeld „Feldreihenfolge“ wird eingeblendet.
	Gruppenfeld. Nützlich zur Einteilung des Eingabe-formulars in offensichtliche Kategorien. Ermöglicht das Zeichnen eines Feldes um eine Feldergruppe und die Anwendung einer Kategorie-überschrift.	Ziehen Sie das Steuerelement an den gewünschten Ort und erweitern Sie das Feld mit den Ziehpunkten auf die gewünschte Größe. Um eine passende Beschreibung hinzuzufügen, ändern Sie den Wert der Texteigenschaft.
	Kontrollkästchen Es werden im Allgemeinen mehrere solche Steuerelemente verwendet, so dass der Benutzer eine Auswahl an Antworten hat. Zum Beispiel 18-35, 36-50, usw. Benutzer markieren das zutreffende Feld.	Ziehen Sie das Steuerelement mit der Drag&&Drop-Funktion an den gewünschten Ort. Es heißt zunächst einmal Check Box 1, Check Box 2, usw. Um den Namen auf dem Eingabeformular zu ändern, modifizieren Sie die Textwerteigenschaft, um die Beschreibung im Fenster "Benutzerdetails" zu ändern, modifizieren Sie die Namenswerteigen-schaft. Dieses Feld lässt sich ggf. beim Agent deaktivieren. Um die Reihenfolge der Anzeigefelder in der Konsole festzulegen, klicken Sie auf Feldreihenfolge. Klicken Sie auf das erscheinende Symbol und das Dialogfeld „Feldreihenfolge“ wird eingeblendet.

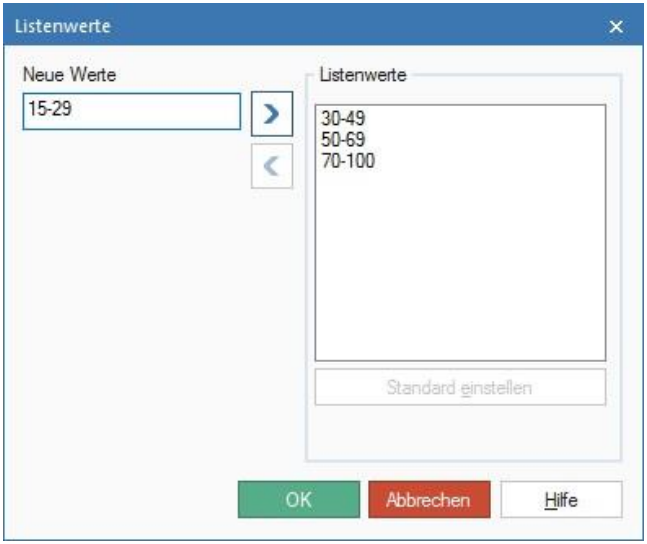
 Bietet eine Antwortauswahl in Form einer Dropdownliste. Sie würden generell neben dem Feld ein Textbeschreibungs-element hinzufügen.	Ziehen Sie das Steuerelement mit der Drop-Funktion an den gewünschten Ort. Um im Fenster "Benutzerdetails" eine Beschreibung hinzuzufügen, ändern Sie die Namenswerteigenschaft. Dieses Feld lässt sich ggf. beim Agent deaktivieren oder dunkel schalten. Um die Werte für die Dropdownliste einzugeben, klicken Sie auf die Eigenschaft "Listenwerte". Klicken Sie auf das erscheinende Symbol und das Dialogfeld "Listenwerte" wird eingeblendet. Um die Reihenfolge der Anzeigefelder in der Konsole festzulegen, klicken Sie auf Feldreihenfolge. Klicken Sie auf das erscheinende Symbol und das Dialogfeld „Feldreihenfolge" wird eingeblendet.
 Listenfeld Es wird eine Werteliste eingeblendet, in welcher der Benutzer die gewünschte Antwort auswählen kann. Sie würden generell neben dem Feld ein Textbeschreibungselement hinzufügen.	Ziehen Sie das Steuerelement mit der Drop-Funktion an den gewünschten Ort. Um im Fenster "Benutzerdetails" eine Beschreibung hinzuzufügen, ändern Sie die Namenswerteigenschaft. Dieses Feld lässt sich ggf. beim Agent deaktivieren oder dunkel schalten. Um die Werte einzugeben, klicken Sie auf die Eigenschaft "Listenwerte". Klicken Sie auf das erscheinende Symbol und das Dialogfeld "Listenwerte" wird eingeblendet. Um die Reihenfolge der Anzeigefelder in der Konsole festzulegen, klicken Sie auf Feldreihenfolge. Klicken Sie auf das erscheinende Symbol und das Dialogfeld „Feldreihenfolge" wird eingeblendet.

	Optionsfeld. Ähnlich wie bei Kontrollkästchen erhalten Benutzer hier eine Auswahl an Antworten, aber es lässt sich nur eine Schaltfläche auswählen. Nur die markierte Option wird im Fenster "Benutzerdetails" festgehalten.	Ziehen Sie den Control mit der Drag&&Drop-Funktion an den gewünschten Ort. Da es mehr als eine Auswahlmöglichkeit geben muss, werden standardmäßig zwei Optionen hinzugefügt. Wenn Sie die Textbeschreibungen abwandeln möchten, ändern Sie durch Klicken auf das Feld "Listenwerte" die Optionsfeldeigenschaft. Klicken Sie auf das erscheinende Symbol und das Dialogfeld Listenwerte für Optionsfelder wird eingeblendet. In diesem Dialogfeld können Sie die gewünschte Anzahl Optionen und damit verknüpfte Beschreibungen eingeben. Dieses Feld lässt sich ggf. deaktivieren und beim Agent dunkel schalten. Um die Reihenfolge der Anzeigefelder in der Konsole festzulegen, klicken Sie auf Feldreihenfolge. Klicken Sie auf das erscheinende Symbol und das Dialogfeld „Feldreihenfolge" wird eingeblendet.

Hinweis: Stellen Sie beim Ändern der Feldreihenfolge von Controls sicher, dass die alphabetische Ansicht unter „Konsoleansicht" deaktiviert ist.

Dialogfeld "Listenwerte"

Beim Erstellen von benutzerdefinierten Registerkarten mit Benutzerdetails können Sie in diesem Dialogfeld gewählte Optionen für ein Dropdownlistenfeld und die Optionsfelder aufführen.



1. Geben Sie den neuen Wert ein und klicken Sie auf  um ihn zum Fenster "Listenwerte" hinzuzufügen. Wiederholen Sie den Vorgang für jede der gewählten Optionen.
2. Einer der Werte lässt sich als Standardeingabe für das Feld auswählen. Wählen Sie das Objekt und klicken Sie auf **Standard einstellen**. If Wenn kein Standardwert zugewiesen ist, wird beim Betrachten durch den Benutzer ein leeres Feld eingeblendet.

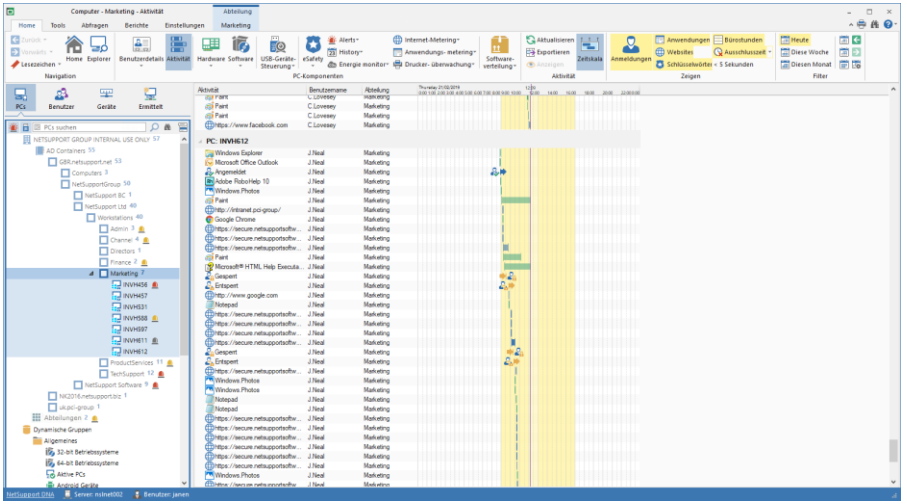
   Hinweis: Beim Eingeben der Werte für das Optionsfeld müssen Sie einen Standardwert einstellen.
3. Klicken Sie auf **OK**, wenn Sie fertig sind.

Aktivitätsüberwachung

Die Aktivitäten-Komponente bietet in einer einzigen chronologischen Ansicht die Agent-Anmeldungssitzungen, Anwendungsnutzung, Internet-Nutzung* und alle ausgelösten eSafety* Begriffe für einen spezifischen Benutzer, einen PC oder eine Abteilung für eine vorgegebene Zeitspanne. Sie können wählen, welche Informationen Sie anzeigen möchten und auch nicht-relevante Anwendungen ausschließen, um die angezeigten Daten anzupassen. Aktivitäten können als grafische Zeitskala oder textbasierte Rasteransicht angezeigt werden.

1. Klicken Sie auf dem **Aktivitäten** Symbol im Menüband. Nun erscheint das Aktivitäten-Fenster.

Hinweis: Wenn die Komponentensymbole ausgeblendet sind, klicken Sie auf die Registerkarte Home.



Die hierarchische Strukturansicht lässt sich zwischen PCs und Benutzern umschalten. Die Strukturansicht des PCs zeigt Daten für den PC-Eigentümer, der mit dem betreffenden PC verknüpft ist, und die Benutzerstrukturansicht zeigt Daten für angemeldete Benutzer.

Wählen Sie in der hierarchischen Strukturansicht die Ebene, auf der Sie die Informationen betrachten möchten: Unternehmen, Abteilung, AD Container, dynamische Gruppe oder individueller Agent.

Sie können die Daten für eine spezifische Zeitperiode betrachten. Um zwischen verschiedenen Zeitperioden hin- und herzuschalten, klicken Sie das entsprechende Symbol im Filterbereich des Menübands an. Wenn Sie auf **Erweitert** klicken, können Sie einen benutzerdefinierten Datum-/Zeitfilter anwenden.

Die gezeigten Arbeitsstunden können im DNA Konfigurationskatalog für Ihre Organisation angepasst werden. Siehe Konsolenanpassungen – Allgemein für weitere Informationen.

Hinweis: Sie können Aktivitäten nur für maximal 31 Tage anzeigen.

In der Standardeinstellung werden die Aktivitäten in einer Zeitskala angezeigt. Um zwischen Zeitskala und textbasierter Rasteransicht umzuschalten, klicken Sie auf dem **Zeitskala** Symbol im Menüband.

Um die im Informationsfenster angezeigten Daten anzupassen, klicken Sie auf dem entsprechenden Symbol im Zeigen-Abschnitt des Menübands. (Wenn das Symbol gelb schattiert ist, wird die Aktivität angezeigt).

Es wird vielleicht bestimmte Anwendungen oder Websites geben, die Sie nicht anzuzeigen brauchen – diese können von der Aktivitätenliste ausgeschlossen werden. Wählen Sie die geforderte Anwendung/Website in der Liste, klicken Sie sie mit der rechten Maustaste an und wählen **Sie Aus Aktivität und Anwendungs-/Internetmetering ausblenden**. Die Anwendung bzw. Website wird dann aus der Aktivitätenliste entfernt und auch aus dem Anwendungs-/Internetmetering.

Hinweise:

- Um eine ausgeblendete Anwendung wieder zur Liste hinzuzufügen, klicken Sie auf dem Dropdown-Pfeil **des Software-Inventar/Anwendungs-Metering** Symbols und wählen Sie im Menü {Anwendungsmanager}, wählen Sie dann die Anwendungen-Registerkarte, suchen Sie die geforderte Anwendung in der List, klicken Sie auf **Bearbeiten** und wählen Sie dann In **Anwendungs-Metering-Ansichten zeigen**.
- Anwendungs- und Website-Besuche die kürzer sind als die angegebene Zeitdauer können ignoriert werden. Wählen Sie das Zeit-ausschließen-Dropdownsymbol im Menüband und wählen Sie die geforderte Zeitdauer, die ausgeschlossen werden soll. Besuche, die kürzer sind als diese Zeit, werden dann nicht mehr angezeigt.

Wenn Aktivität in der Zeitskala angezeigt wird, werden die Start- und Endzeiten für Elemente als horizontaler Balken angezeigt (Websites = blau, Anwendungen = grün), Benutzeranmeldungen/-abmeldungen werden als einzelnes Ereignis gezeigt, und wenn ein eSafety* Begriff ausgelöst wird, wird ein Schild mit dem Risikoindexwert angezeigt. Die Bürostunden sind gelb schattiert, und die aktuelle Zeit wird durch eine lila Linie hervorgehoben. Websites und ausgelöste eSafety* Begriffe können von hier aus angezeigt werden; wählen Sie das Auftreten auf der Zeitskala und klicken Sie auf dem Anzeigen Symbol im Menüband. Sie können die Zeitskala vergrößern oder verkleinern, indem Sie Strg drücken und das Mausrad drehen.

Die aktuellen Aktivitätendaten können an eine .CSV Datei exportiert werden; klicken Sie im Menüband auf dem **Exportieren** Symbol.

Eine Schnellaktualisierung-Funktion ermöglicht es Ihnen, die Daten außerhalb der Standardfrequenz zu aktualisieren. Dies kann nützlich sein, wenn Sie bestimmte Agents oder Abteilungen anpeilen möchten. Klicken Sie im Menüband auf **Aktualisieren**.

Hinweis: Das in der Konsole angezeigte Datum-/Zeitformat stimmt mit dem Format in dem Rechner, in dem der DNA Server installiert ist, überein. Um das Format in der Konsole zu ändern, müssen Sie zunächst das Format in diesem Rechner ändern. Für weitere Informationen wenden Sie sich bitte an unser Support-Team www.netsupportsoftware.com/support.

Abfragen
Wählen Sie zur Anzeige des Abfragefensters die Registerkarte „Abfragen".

Mit dem Abfragetool von DNA können Sie Datenbankeinträge abrufen, die bestimmte Kriterien erfüllen. Abfragen zu der Komponente, die gerade betrachtet wird, sind aufgelistet, was ein schnelles Abrufen der Ergebnisse ermöglicht.

Klicken Sie in der Menüleiste auf dem **Abfrage hinzufügen** Symbol, um eine neue Abfrage zu erstellen, oder klicken Sie auf dem **Abfrage bearbeiten** Symbol in der Menüleiste, um ein in der Liste vorhandenes Objekt zu bearbeiten.

Berichte
Wählen Sie zur Anzeige des Berichtfensters die Registerkarte „Berichte".

Jeder Komponente ist eine Reihe von vordefinierten Managementberichten, die vom Crystal Reports-Modul gespeist werden, beigefügt. Wählen Sie den geforderten Bericht in der Dropdown-Liste. Die Ergebnisse erscheinen im Informationsfenster. Sie lassen sich ggf. exportieren.

* Die Funktion steht nur in der NetSupport DNA Version für das Bildungswesen zur Verfügung.

Hardwareinventarisierung

NetSupport DNA bietet eines der umfassendsten und detailliertesten Hardware-Inventar- Module im gegenwärtigen Markt. Von jedem Gerät werden vielfältige Informationen gesammelt, von den CPU- und BIOS-Typen zu Netzwerk-, Video- und Speicherinformationen.

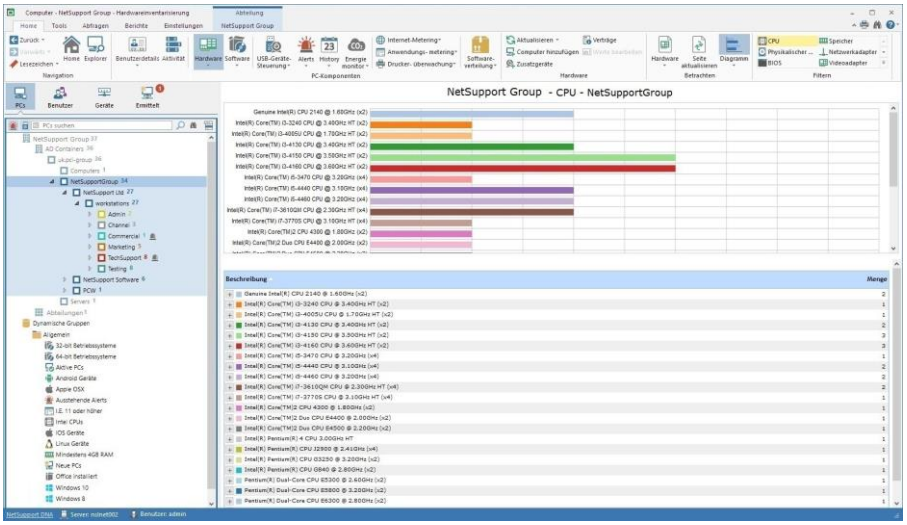
Inventarberichte können entweder für einen einzelnen PC, eine gewählte Abteilung, für bedingungsbasierte „Dynamische Gruppen" oder für das gesamte Unternehmen angezeigt werden.

Außerdem gibt es ein Vertragsmodul zur Aufzeichnung der Miet- und Wartungsverträge für Geräte oder Peripheriegeräte einschließlich der Lieferantenangaben, Vertragsablaufdaten und Kosten.

Hardware-Inventar-Aktualisierungen können dafür konfiguriert werden, zu verschiedenen Zeitintervallen im Laufe des Tages oder beim Einschalten zu laufen und können bei Bedarf auch sofort ausgeführt werden. Es steht eine eigenständige Inventarkomponente zur Verfügung, die auf Nicht-Netzwerk- und Mobilgeräten eingesetzt werden kann, und außerdem können hochwertige Peripheriegeräte einem Gerät zugeordnet und erfasst werden.

1. Klicken Sie im Ribbon auf das Hardwaresymbol. Das Fenster **Hardwareinventarisierung** wird eingeblendet.

Hinweis: Wenn die Komponentensymbole ausgeblendet sind, klicken Sie auf die Registerkarte **Home**.



Wählen Sie in der hierarchischen Strukturansicht die Ebene, auf der Sie die Hardwareinformationen betrachten möchten: Unternehmen, Abteilung, AD Container, dynamische Gruppe oder individueller Agent.

Hinweis: Ein fokussiertes Inventar für PCs wird in der Ermittelte-Strukturansicht gezeigt.

Im Informationsfenster ist ein Breakdown für jedes gewählte Objekt in Grafik- und Listenformat angezeigt. Um den Graph in einem anderen Format anzuzeigen, klicken Sie auf dem **Diagramm**-Symbol-Dropdownpfeil in der Menüleiste und wählen das entsprechende Format.

Um die aktive Ansicht auszudrucken, klicken Sie auf dem  Symbol oben auf der Konsole.

Hinweis: Durch Anklicken des Chart-Symbols im Ribbon wird die Grafik ein-/ausgeblendet.

Sie können zwischen den angezeigten Hardware-Komponenten hin- und herschalten, indem Sie auf dem entsprechenden Symbol im Filterbereich des Menübands klicken.

Die aufgelisteten Beschreibungen können erweitert werden, um eine individuelle Agent-Aufgliederung für jedes Objekt zu erhalten; diese können bei Bedarf exportiert oder ausgedruckt werden. Bei der

Betrachtung auf Agent-Ebene in der Strukturansicht wird ein komplettes Hardware-Inventar für den PC gezeigt. Nicht angezeigte oder falsche Werte können bearbeitet werden. Klicken Sie auf dem **Hardware-Inventar** Dropdownpfeil und wählen Sie im Menü {Werte bearbeiten} oder wählen Sie das **Werte bearbeiten** Symbol im Menüband.

Um die mit den Geräten verbundenen Leasing- oder Wartungsverträge anzuzeigen, klicken Sie auf der **Hardware-Inventar** Dropdownliste und wählen das {Anzeigen- Verträge} Symbol oder klicken Sie auf dem **Verträge** Symbol im Hardware-Inventar-Bereich des Menübands.

Abfragen

Wählen Sie zur Anzeige des Abfragefensters die Registerkarte „Abfragen".

Mit dem Abfragetool von DNA können Sie Datenbankeinträge abrufen, die bestimmte Kriterien erfüllen. Abfragen zu der Komponente, die gerade betrachtet wird, sind aufgelistet, was ein schnelles Abrufen der Ergebnisse ermöglicht.

Klicken Sie in der Menüleiste auf dem Abfrage hinzufügen Symbol, um eine neue Abfrage zu erstellen, oder klicken Sie auf dem Abfrage bearbeiten Symbol in der Menüleiste, um ein in der Liste vorhandenes Objekt zu bearbeiten.

Berichte

Wählen Sie zur Anzeige des Berichtfensters die Registerkarte „Berichte".

Jeder Komponente ist eine Reihe von vordefinierten Managementberichten, die vom Crystal Reports-Modul gespeist werden, beigefügt. Wählen Sie den geforderten Bericht in der Dropdown-Liste. Die Ergebnisse erscheinen im Informationsfenster. Sie lassen sich ggf. exportieren.

Hinweise:

- Die Häufigkeit, mit der der Server Daten sammelt, lässt sich mit der Option "DNA-Einstellungen" ändern.
- Wenn Sie wissen, dass das Inventar für einen bestimmten Agent oder eine Abteilung bnicht mehr aktuell ist, können Sie die Schnellaktualisierungsfunktion verwenden. Klicken Sie mit der rechten Maustaste auf das gewünschte Objekt in der Strukturansicht und wählen Sie **Aktualisieren** oder klicken Sie im Menü oder Ribbon **Hardware** auf **Aktualisieren**.

- Wenn eine Fehlermeldung bezüglich des 16-Bit MS-DOS Subsystems eingeblendet wird, konsultieren Sie bitte die technische Supportwebsite von NetSupport unter www.netsupportsoftware.com/support.

Inventardaten für entfernte Benutzer oder nicht gescannte Geräte sammeln

Damit genaue Informationen über das Inventar verfügbar sind, müssen unbedingt alle Daten zu Benutzer, Hardware und Software aufgezeichnet werden. Der DNA Server ruft zwar automatisch Informationen von den Rechnern ab, auf denen ein Agent installiert ist, aber es treten wahrscheinlich trotzdem Instanzen auf, in denen gewisse Objekte nicht auffindbar sind. Sie haben vielleicht Benutzer in entfernten Büros, die nicht an das Netzwerk angeschlossen sind, und Sie werden wahrscheinlich Zusatzgeräte wie Router, Webcams, usw. kaufen.

Um sicherzustellen, dass auch diese Informationen bekannt sind, liefert DNA die Tools zum Sammeln von Daten für entfernte/alleinstehende PCs und dem Protokollieren von Details für Zusatzgeräte.

Um die Identifizierung zu erleichtern, können Sie in der Konsolestrukturansicht spezifische Abteilungen für die Speicherung dieser "nicht gescannten" Objekte erstellen, oder Sie können ein Zusatzgerät mit einem bestimmten Agent verknüpfen.

Nicht-Standard-Hardware hinzufügen

DNA liefert die Tools zur Protokollierung der Details für Objekte, die sich dynamisch nicht finden lassen. Es kann sich dabei um einen entfernten oder alleinstehenden PC handeln, oder Sie haben u. U. zusätzliche Hardwaregeräte, die aufgezeichnet werden müssen, damit das Inventarregister stimmt.

1. Klicken Sie auf den Dropdownpfeil des Hardwaresymbols und wählen Sie im Menü die Option {Computer hinzufügen}.
   Oder
   Klicken Sie auf das Symbol **Computer hinzufügen** der Hardware-Inventarisierungsgruppe.
2. Wählen Sie eine der beiden verfügbaren Optionen und klicken Sie auf **Weiter**

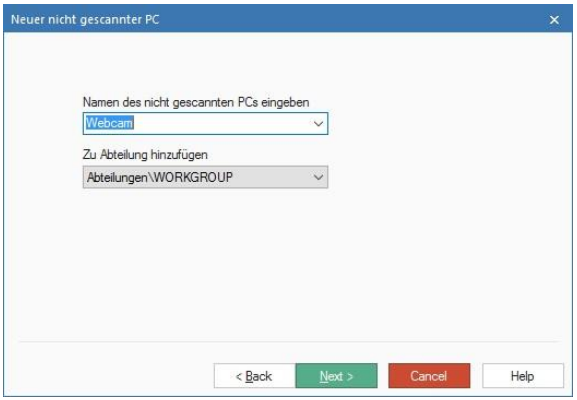


Neuen PC erstellen

Wählen Sie diese Option, um ein nicht gescanntes Hardwareobjekt/Zusatzgerät mit einer Abteilung zu verknüpfen.

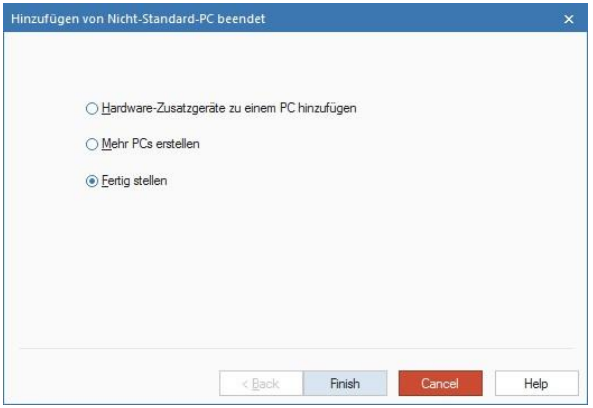
Nicht gescannte Geräte hinzufügen

Geben Sie den Namen des PCs/Geräts, der/das hinzugefügt werden soll, ein und wählen Sie die Abteilung, mit der das Objekt verknüpft werden soll. Klicken Sie auf **Weiter**.



Klicken Sie auf **Weiter**.

Bevor das neue Objekt zur Strukturansicht hinzugefügt wird, wählen Sie eine der folgenden Optionen:



Hardware-Zusatzgeräte zu einem PC hinzufügen

Sie können die neue Hardware einfach als alleinstehendes Objekt zur Struktur hinzufügen oder Zusatzgeräte mit ihr verknüpfen und so eine "Mini"-Hardware-Inventarseite für das Gerät erstellen.

Mehr PCs erstellen

Ermöglicht die Wiederholung des Prozesses für nicht gescannte Objekte.

Fertig stellen
Fügt das neue Objekt zur Strukturansicht hinzu und bringt Sie ins Hardware-Inventarfenster zurück.

Nicht gescannte Objekte lassen sich in der Strukturansicht leicht identifizieren, da vor jedem von ihnen steht. //.



Alleinstehenden/entfernten Gerät importieren

Wählen Sie diese Option, um Inventardaten für ein eigenständiges oder Remote-Gerät hinzuzufügen.

Entfernten PC hinzufügen
Mit diesem Programm lässt sich das Hardware/Software-Inventar für "alleinstehende" PCs, die nicht dynamisch von DNA gefunden werden können, importieren.

Inventardaten von Windows Geräten abrufen
Die im DNA-Programmordner installierte Datei DNAInv.exe wird auf dem entfernten PC ausgeführt. Dieser erstellt seinerseits eine BIN-Datei, welche die Inventardaten enthält. Der Bediener importiert die BIN-Datei in DNA und der Benutzer wird zusammen mit den verknüpften Hardware- und Software-Inventardaten zur Konsole hinzugefügt.

Erhalten der Inventardaten

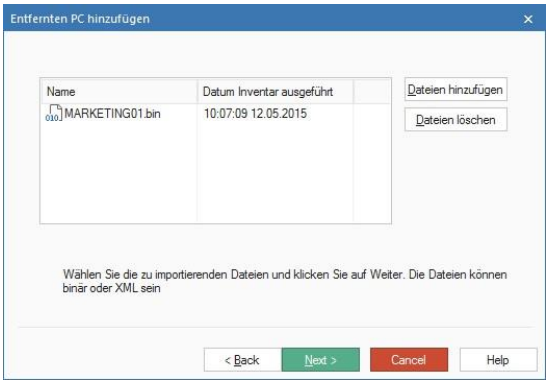
1. Kopieren Sie die Datei DNAInv.exe aus c:\Programme\netsupport\netsupport_dna\console\ und senden/emailen/transportieren Sie sie an den/die gewünschte(n) Benutzer.
2. Führen Sie die Datei auf den gewünschten Rechnern aus. Die Inventardaten werden in einer neuen Datei aufgezeichnet: 'machine_name.BIN'. Diese ist an den Bediener/Administrator zurückzusenden.
3. Nach Empfang der BIN-Datei muss sie der Bediener an einen passenden Speicherort kopieren, so dass sie zum Import der aufgezeichneten Inventardaten bereit ist.

Importieren der Daten

1. Klicken Sie auf den Dropdownpfeil des Hardwaresymbols und wählen Sie im Menü die Option {Computer hinzufügen}.

   Oder

   Klicken Sie auf das Symbol **Computer hinzufügen** der Hardware-Inventarisierungsgruppe.
2. Das Dialogfeld "PC-Typ auswählen" wird eingeblendet. Wählen Sie **Alleinstehenden/entfernten PC importieren** und klicken auf **Weiter**.
3. Das Dialogfeld "Entfernten PC hinzufügen" wird eingeblendet.



4. Klicken Sie auf **Dateien hinzufügen** und suchen nach den BIN oder XML-Dateien. Jede Datei, die Sie auswählen, wird zum Dialogfeld hinzugefügt.
5. Klicken Sie auf **Weiter**. Das Inventar für jeden angezeigten Rechner wird importiert und die Benutzerdetails werden zur Strukturansicht hinzugefügt.



6. Klicken Sie auf **Fertig stellen**, um den Prozess zu beenden oder klicken Sie auf **Anderen PC erstellen**, um ein anderes Inventar zu importieren. Sie können ggf. auch zusätzliche Hardwareobjekte zu dem neuen Datensatz hinzufügen.

Hardware-Zusatzgeräte hinzufügen

Sämtliche zusätzliche/nicht gescannte Hardware muss aufgezeichnet werden, um ein korrektes Inventarprotokoll zu führen. DNA ermöglicht die manuelle Verknüpfung der Details dieser Komponenten mit ihren jeweiligen "Eigentümern"'. Geräte lassen sich mit individuellen PCs oder Gruppen verknüpfen.

1. Sie können beim Erstellen des "nicht gescannten" Hardware-Datensatzes ein Zusatzgerät hinzufügen.

   Oder

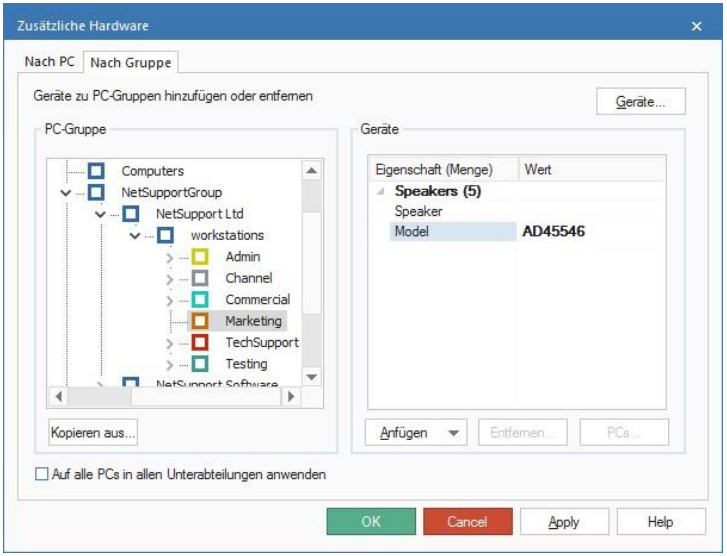
   Um das Gerät mit einem vorhandenen Objekt in der Strukturansicht zu verknüpfen, klicken Sie mit der rechten Maustaste auf einen Agent oder ein "nicht gescanntes" Objekt in der Struktur und wählen Zusatzgerät.

   Oder

   Klicken Sie auf den Dropdownpfeil des Hardwaresymbols und wählen Sie im Menü die Option {Zusatzgerät - Hinzufügen}.

   Oder

   Klicken Sie auf das **Zusatzgerät-Symbol** in der Hardware-Inventarisierungsgruppe.



Zusatzgeräte nach PC hinzufügen

1. Wählen Sie die Registerkarte „Nach PC" und wählen Sie in der Strukturansicht den PC, mit dem die Hardware verknüpft werden soll.
2. Klicken Sie zum Erstellen eines neuen Geräts auf **Geräte**. Erstellte Geräte warden in der Dropdownliste **Anfügen** aufgeführt. Wählen Sie das gewünschte Gerät in der Liste der Objekte, die mit dem PC verknüpft werden sollen.
3. Geben Sie die Gerätewerte, zum Beispiel die spezifische Marke/das Modell des Geräts, die im Hardwareinventar aufgeführt werden sollen, ein.
4. Klicken Sie auf **Anwenden**.
5. Geräte lassen sich von einem PC auf einen anderen kopieren. Klicken Sie auf **Kopieren von** und wählen Sie den PC, von dem Sie die Daten kopieren möchten. Alle mit diesem PC verknüpften Daten werden kopiert.
6. Sie können durch Wiederholen dieses Prozesses weitere Geräte hinzufügen oder wenn Sie fertig sind auf OK klicken. Um ein Objekt zu entfernen, wählen Sie das gewünschte Gerät und klicken auf **Entfernen**.

Zusatzgeräte nach Gruppe hinzufügen

1. Wählen Sie die Registerkarte „Nach Gruppe" und wählen Sie in der Strukturansicht die Abteilung oder dynamische Gruppe, mit denen die Hardware verknüpft werden soll.

   Hinweis: Sie können alle Agents in der gewählten Abteilung einschließen, indem Sie die Option **Auf die PCs in allen Unterabteilungen anwenden** markieren.

2. Klicken Sie zum Erstellen eines neuen Geräts auf **Geräte**. Erstellte Geräte warden in der Dropdownliste **Anfügen** aufgeführt. Wählen Sie das gewünschte Gerät in der Liste der Objekte, die mit dem PC verknüpft werden sollen.
3. Geben Sie die Gerätewerte, zum Beispiel die spezifische Marke/das Modell des Geräts, die im Hardwareinventar aufgeführt werden sollen, ein.
4. Klicken Sie auf **Anwenden**.
5. Geräte lassen sich von einer Gruppe in eine andere kopieren. Klicken Sie auf **Kopieren von** und wählen Sie die Gruppe, aus der Sie die Daten kopieren möchten. Alle mit dieser Gruppe verknüpften Daten werden kopiert.
6. Sie können durch Wiederholen dieses Prozesses weitere Geräte hinzufügen oder wenn Sie fertig sind auf **OK** klicken.

Hinweis: Wenn Sie sehen wollen, welche PCs mit einem Gerät verknüpft sind, wählen Sie das gewünschte Gerät und klicken Sie auf **PCs**.

7. Zum Entfernen des Geräts klicken Sie auf „Entfernen", wählen die Gruppe, aus der das Gerät entfernt werden soll und dann das gewünschte Gerät. Klicken Sie auf **OK**. Das Gerät wird aus allen PCs in der gewählten Gruppe entfernt.

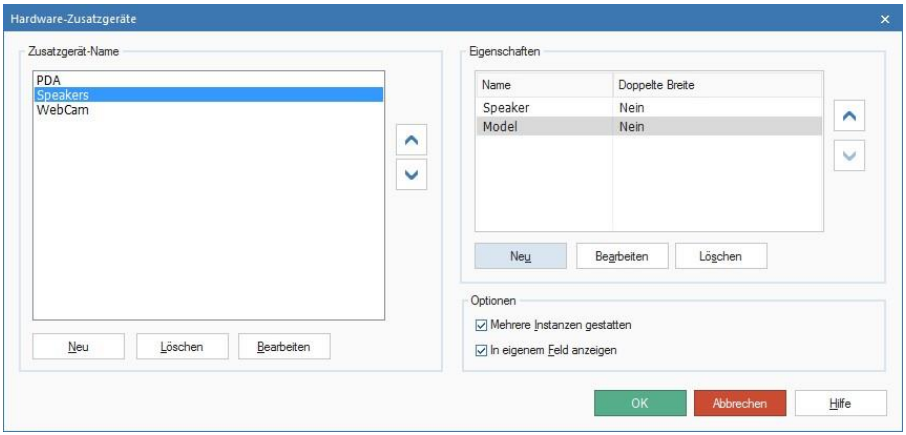
Hardware-Zusatzgeräte

Mit diesem Dialogfeld können Sie ein Register nicht gescannter Hardwaregeräte, zusammen mit ihren verknüpften Eigenschaften, kompilieren. Aufgelistete Objekte lassen sich dann mit Agents oder nicht gescannten Zusatzgeräten verknüpfen.

1. Sie können beim Hinzufügen von Zusatzgeräten zu einem vorhandenen Datensatz in der strukturansicht ein neues Gerät erstellen.

   Oder

   Sie können eine Geräteliste vorbereiten. Klicken Sie auf den Dropdownpfeil des **Hardwaresymbols** und wählen Sie im Menü die Option {Zusatzgerät-Management}. Diese lassen sich dann zu einem späteren Zeitpunkt anfügen.



Zusatzgerät-Name

Neu

Klicken Sie auf **Neu**, um ein Gerät zur Liste hinzuzufügen. Durch Klicken auf die Pfeile können Sie die Liste sortieren.

Bearbeiten
Dient zum Ändern des Namens eines Listenobjekts.

Löschen
Entfernt das Gerät aus der Liste und aus allen Hardwareinventaren, in denen es erscheint.

Optionen

Mehrere Instanzen gestatten
Wenn diese Option markiert ist, können Sie mehrere Instanzen des Geräts mit dem Inventar eines Benutzers verknüpfen. Zum Beispiel zwei digitale Kameras mit verschiedenen Marken-/Modellnummern.

In eigenem Feld anzeigen
Wenn diese Option markiert ist, wird jede Instanz des Geräts in einem neuen Feld auf der Hardwareinventarisierungsseite aufgelistet. Wenn es jedoch mehrere Instanzen desselben Gerätes gibt, empfiehlt es sich u. U., sie im gleichen Feld zusammen zu gruppieren.

Eigenschaften
Sie können die Eigenschaften des neuen Objekts bearbeiten und zusätzliche Objekte mit dem Gerät verknüpfen, je nachdem, wie viele verwandte Informationen Sie aufzeichnen möchten.

Neu
Verknüpft zusätzliche Objekte mit dem Primärgerät. Klicken Sie auf **Neu** und geben Sie den Gerätenamen ein. Je nach der Informationsmenge, die eingegeben werden soll, können Sie ein Feld mit doppelter Breite bereitstellen. Klicken Sie auf **OK**.

Mit den Pfeiltasten lassen sich die Geräte in der Reihenfolge anordnen, in der Sie sie auf der Inventarseite anzeigen möchten.

Bearbeiten
Ermöglicht das Bearbeiten der Eigenschaften eines Geräts**.**

Löschen
Entfernt ein Gerät aus der Liste und aus allen Inventaren, an die es angefügt ist.

Wenn alle Details eingegeben sind, klicken Sie auf **OK**.

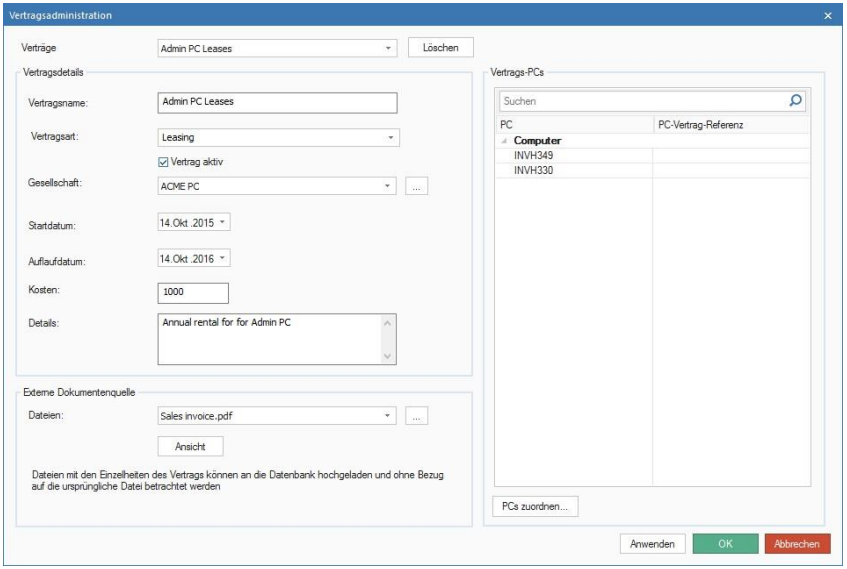
Vertragsmanager

NetSupport DNA ermöglicht es Ihnen, Leasing-/Wartungsverträge in Verbindung mit den Geräten und Peripheriegeräten aufzuzeichnen. Nachdem ein Vertrag erstellt worden ist, kann er einer beliebigen Anzahl von Geräten zugeordnet werden. Dokumente, die sich auf den Leasing-/Wartungsvertrag beziehen, können angehängt werden, so dass Sie alle Informationen, die sich auf den Vertrag beziehen, zusammen speichern können. Die Vertragsinformationen werden dann im Benutzerdetails-Dialog und im Hardwareinventar-Informationsfenster für das Gerät angezeigt.

Hinweis: Wenn Sie einen Upgrade einer früheren Version von NetSupport DNA ausführen und die Leasing-/Verwaltungsdetails den PCs zugeordnet haben, können diese Details übertragen und im Verträge-Feld angezeigt werden. Sie müssen diese den entsprechenden PCs zuordnen.

Neuen Vertrag hinzufügen

1. Klicken Sie auf dem **Hardware- Inventar**-Dropdownpfeil und wählen Sie im Menü {Verträge}.
2. Nun erscheint der Vertragsmanager-Dialog. Die existierenden Verträge können betrachtet werden, indem man sie in der **Verträge-**Dropdownliste wählt.



3. Geben Sie den Namen für den Vertrag ein.
4. Wählen Sie die Vertragsart in der Dropdownliste - **Leasing** oder **Verwaltung** – und wählen Sie, ob der Vertrag aktiv ist.
5. Lieferantendetails können dem Vertrag zugeordnet werden, um einen neuen Unternehmensdatensatz zu erstellen; klicken Sie auf  im **Vertragsdetails** Abschnitt. Nun erscheint der Unternehmen-Dialog, der es Ihnen ermöglicht, Details für das Unternehmen einzugeben. Existierende Unternehmen können in der **Unternehmen** Dropdownliste gewählt werden.
6. Geben Sie die Start- und Ablaufdaten, Kosten und andere Informationen zum Vertrag ein.
7. Um dem Vertrag Dateien (PDFs, Emails, Word Dokumente etc.) anzuhängen, klicken Sie auf  im **Externe Dokumentquellen** Abschnitt. Daraufhin erscheint der Externe Dokumente Dialog, der es Ihnen ermöglicht, die Dateien zu durchsuchen und Dateien hinzuzufügen. Sie können die Dateien, die dem Datensatz bereits angehängt worden sind, anzeigen, indem Sie den Pfeil anklicken, um die Dropdownmenü-Liste zu sehen.
8. Um diesem Vertrag PCs zuzuordnen, klicken Sie auf **PCs zuordnen**.

Hinweis: Sie können schnell nach Geräten suchen, indem Sie sie im Suchfeld eintippen und dann auf  klicken .

9. Klicken Sie auf **Anwenden,** um diese Aufzeichnungen zu speichern.

Hinweis: Um einen Vertragsdatensatz zu löschen, wählen Sie den geforderten Vertrag in der **Verträge** Dropdownliste und klicken dann auf **Löschen**.

Softwareinventarisierung

Das Software-Modul ist dafür ausgelegt, Schulen beim Management der Lizenzeinhaltung zu helfen, Software-Überschreitungen durch Meldung der installierten Software zu reduzieren und proaktiv PCs zu identifizieren, deren Software wenig oder gar nicht benutzt wird.

Es wird eine detaillierte Zusammenfassung aller Programme und Anwendungen erstellt, die auf den einzelnen PCs installiert sind, einschließlich Windows 8 & 10 Store Apps. NetSupport DNA kann die Informationen für einen ausgewählten PC, eine Abteilung oder eine benutzerdefinierte Gruppe anzeigen und enthält ein umfassendes Modul zur Zuweisung und Nachverfolgung der Lizenznutzung. Das NetSupport DNA Softwarelizenz-Modul unterstützt das kontinuierliche Management aller Softwarelizenzen für alle Abteilungen und erfasst die Lieferanten, Einkaufs- und Rechnungsdetails, Abteilungs- und Kostenstellenzuweisung und Nachverfolgung der Wartungsverträge.

Die Daten lassen sich im Informationsfenster in verschiedenen Formaten betrachten:

Programmen
Blendet eine Liste aller im Dialogfeld „Software" angezeigten Programmen ein und es lassen sich hier auch die Lizenzebenen verwalten.

Anwendungen
Bietet eine viel detailliertere Ansicht der auf einem PC installierten Applikationen, denn es werden hier alle ausführbaren Dateien, die auf dem Ziel-PC gefunden wurden, eingeblendet.

Dateien
Ermöglicht es ihnen, die Suche bei Bedarf durch zusätzliche Dateiarten (wie GDPR-Dateien) zu erweitern.

Hotfixes
Bietet Ihnen eine Liste der Hotfixes, die auf den einzelnen PCs installiert sind.

1. Klicken Sie im Ribbon auf das Softwaresymbol. Das Fenster **Softwareinventarisierung** wird eingeblendet.

Hinweis: Wenn die Komponentensymbole ausgeblendet sind, klicken Sie auf die Registerkarte **Home**.



Wählen Sie in der hierarchischen Strukturansicht die Ebene, auf der Sie die angezeigten Daten betrachten möchten: Unternehmen, Abteilung, AD Container, dynamische Grupe oder individueller Agent.

Sie können zwischen Programme, Anwendungen, Dateien und Hotfixes hin- und herschalten, indem Sie auf dem Software-Inventar-Dropdownpfeil klicken und {Anzeigen- Programme/Anwendungen/ Dateien/Hotfixes} wählen oder auf dem entsprechenden Symbol im Menüband klicken.

Um den Graph in einem anderen Format anzuzeigen, klicken Sie auf dem Diagramm-Symbol-Dropdownpfeil in der Menüleiste und wählen das entsprechende Format. Um die aktive Ansicht auszudrucken, klicken Sie auf dem  Symbol oben auf der Konsole.

Hinweis: Durch Anklicken des Chart-Symbols im Ribbon wird die Grafik ein-/ausgeblendet.

Mit Software-Inventar können Sie leicht die Lizenznutzung überwachen und eventuelle Lizenzierungsprobleme aufzeigen. Die Anzahl der für jedes Programm gekauften Lizenzen lässt sich im Dialog „Programm-Manager" festhalten . Beim Betrachten von Programmen werden dann detaillierte Lizenzinformationen angezeigt. Sie können die einzelnen Beschreibungen erweitern und so Details über die Agent PCs, auf denen die Applikation installiert ist, erfahren.

Hinweis: Die Lizenzinformationen werden nur dann eingeblendet, wenn die Applikation im Dialogfeld „Applikationsgruppe bearbeiten" dem installierten Programm zugewiesen wurde und die Lizenzinformationen im Manager für installierte Programme konfiguriert sind.

Beim Anzeigen von Anwendungen kann die Anwendungsliste eingeschränkt werden, wenn Sie feststellen, dass für dieselbe Software mehrere Eingaben erfasst worden sind. Beispielsweise verschiedene Versionen desselben Produkts. Mit der Option "Anwendungsgruppen" lassen sich Objekte in einem einzigen Datensatz zusammenführen und Sie können die Gesamtzahl der Lizenzen aufzeichnen. In einem solchen Fall spiegelt die Anzahl unter "Menge" u. U. nicht wahrheitsgetreu wider, auf wie vielen PCs bestimmte Anwendungen ausgeführt werden, da Agents mit mehr als einem Objekt in der zusammengeführten Gruppe als Mehrfacheinträge gezählt werden. Um eine einmalige Zahl zu erzielen, klicken Sie auf dem **Einmalige zeigen** Symbol im Menüband.

Hinweis: Installierte Programme lassen sich auch mit dem Programm-Manager zusammenführen. Zusammengeführte Programme werden auf Unternehmens- und Abteilungsebene in der Hierarchie als „Zusammengeführte Gruppe" angezeigt, aber auf PC-Ebene erscheinen sie als das Ursprungsprogramm.

Eine nützliche Art, spezifische Programme und Anwendungen anzuzeigen und die angezeigten Datenmengen zu beschränken, besteht darin, 'ähnliche' Objekte zu Kategorien zusammenzugruppieren. Siehe Anwendungsgruppen oder Installierte-Programme-Manager für weitere Informationen. Um eine Kategorie zu zeigen, klicken Sie auf dem Diagramm-Symbol-Dropdownpfeil im Menüband und wählen Kategorien. Wählen Sie die Gruppe, die Sie anzeigen möchten, und klicken Sie auf **OK**. Das Informationsfenster zeigt jetzt nur die Daten für diese Kategorie. Eine gelbe Kopfzeile zeigt an, welche Kategorie Sie gerade betrachten. Sie können zwischen Kategorien wechseln und Kategorien von hier aus löschen.

Standardmäßig sucht DNA die Agent PCs nach ausführbaren Dateien ab, aber Sie können ggf. auch zusätzliche Dateitypen (wie GDPR-Dateien, Bild-Dateien und benutzerdefinierte Dateierweiterungen) hinzufügen. Mit der Option **DNA Softwareinventarisierung - Einstellungen** lässt sich angeben, welche anderen Dateien in die Suche aufzunehmen sind. Die Ergebnisse lassen sich betrachten, indem Sie auf das Dateiensymbol im Software-Inventarisierungsribbon klicken.

Wenn Sie Dateien anzeigen, können Sie filtern, welche Dateitypen im Informationsfenster gezeigt werden sollen. Wählen Sie das Typen-Symbol im Menüband und wählen Sie dann in der Liste die Dateitypen, die gezeigt werden sollen. Sie können GDPR- und Bilddateien schnell einschließen/ausschließen, indem Sie die entsprechende Option wählen. Klicken Sie auf **OK**. Daraufhin erscheint eine gelbe Kopfzeile, die angibt, welche Dateitypen angezeigt werden. Klicken Sie auf **Löschen,** um zur Anzeige aller Dateitypen zurückzukehren.

Hinweis: Dateitypen erscheinen nur dann in der Dateitypen-Liste, wenn sie in den Software-Inventareinstellungen konfiguriert worden sind.

Abfragen

Wählen Sie zur Anzeige des Abfragefensters die Registerkarte „Abfragen".

Mit dem Abfragetool von DNA können Sie Datenbankeinträge abrufen, die bestimmte Kriterien erfüllen. Abfragen zu der Komponente, die gerade betrachtet wird, sind aufgelistet, was ein schnelles Abrufen der Ergebnisse ermöglicht

Klicken Sie in der Menüleiste auf dem Abfrage hinzufügen Symbol, um eine neue Abfrage zu erstellen, oder klicken Sie auf dem Abfrage bearbeiten Symbol in der Menüleiste, um ein in der Liste vorhandenes Objekt zu bearbeiten.

Berichte

Wählen Sie zur Anzeige des Berichtfensters die Registerkarte „Berichte".

Jeder Komponente ist eine Reihe von vordefinierten Managementberichten, die vom Crystal Reports-Modul gespeist werden, beigefügt. Wählen Sie den geforderten Bericht in der Dropdown-Liste. Die Ergebnisse erscheinen im Informationsfenster. Sie lassen sich ggf. exportieren.

Hinweise:

- Die Häufigkeit, mit der der Server Daten sammelt, lässt sich mit der Option "DNA-Einstellungen"ändern.
- Wenn Sie wissen, dass das Inventar für einen bestimmten Agent oder eine Abteilung nicht mehr aktuell ist, können Sie die Schnellaktualisierungsfunktion verwenden. Klicken Sie mit der rechten Maustaste auf das gewünschte Objekt in der Strukturansicht

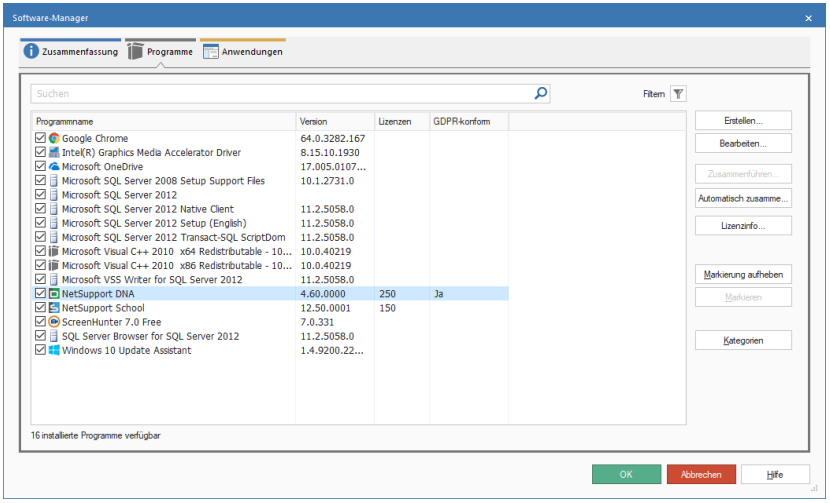
und wählen Sie „Aktualisieren" oder klicken Sie im Menü oder dem Ribbon „Softwareinventarisierung" auf „Aktualisieren".

Manager für installierte Programme

In diesem Dialogfeld werden die installierten Programme gemäß dem Dialogfeld „Software" auf dem Agent-PC angezeigt. Sie können den Inhalt anpassen, um den Umgang mit der Liste zu vereinfachen. Hier lassen sich die Optionen für die Inventarisierung auswählen, verschiedene Versionen derselben Software in einen einzigen Datensatz zusammenführen sowie Lizenzebenen verwalten.

1. Klicken Sie auf den Dropdownpfeil für das Symbol der Software und wählen Sie im Menü die Option {Programm-Manager}.
   Oder
   Klicken Sie auf das Symbol **Programm-Manager** der Softwareinventarisierungsgruppe.
2. Nun erscheint der Softwaremanager-Dialog. Wählen Sie die Registerkarte Programme.
3. Es werden die installierten Programme angezeigt, und, falls diese erfasst worden sind, die Anzahl der innegehaltenen Lizenzen und ob das Programm GDPR-konform ist. Das Kontrollkästchen neben jedem Programm zeigt an, ob es zum Inventar gehört oder nicht.

Hinweis: Sie können ein Programm im Programmdetail-Dialog als GDPR-konform markieren.



Sie können ein bestimmtes Programm schnell finden, indem Sie es im Suchfeld eintippen.

Um die Liste übersichtlicher zu machen, können Sie die angezeigten

Programme filtern. Wenn Sie auf  klicken, erscheint der Installierte Programme Filter Dialog. Von hier aus können Sie wählen, welche Programmgruppen angezeigt werden sollen.

Es können Programm-Kategorien erstellt werden, mit denen Sie ähnliche Programme gruppieren können. Das Software-Inventar-Fenster ermöglicht es Ihnen, die Programme nach Gruppe anzuzeigen, statt 'Alle' Objekte aufzulisten, was die Nachverfolgung spezifischer Aufzeichnungen erleichtert.

Wenn ein installiertes Programm nicht aufgeführt ist, können Sie durch Anklicken von **Erstellen** ein neues Programm erstellen und es mit der entsprechenden Anwendungsgruppe verbinden.

Hinweis: Wenn das gewünschte installierte Programm nicht erscheint, stellen Sie sicher, dass der PC, auf dem das Softwareprogramm installiert ist, eine Verbindung zum Server hergestellt hat

Mehrere Versionen desselben Produkts können in eine neue installierte Programmgruppe zusammengeführt werden. Wählen Sie die gewünschten Objekte (durch Umschalt-Klick oder Strg-Klick) und klicken Sie auf **Zusammenführen**. Um die Zusammenführung von Programmen aufzuheben, wählen Sie die gewünschte Gruppe und klicken auf **Bearbeiten**.

Hinweis: Sie können Programme mit ähnlichen Namen automatisch zusammenführen. Klicken Sie auf **Automatisch zusammenführen;** dann erscheint ein Dialog. Um vorhandene installierte Programme zusammenzuführen, klicken Sie auf **Jetzt automatisch zusammenführen**. In der Standardeinstellung werden neue Programme automatisch zusammengeführt. Um dies auszuschalten, deaktivieren Sie **Automatische Zusammenführung aktivieren**.

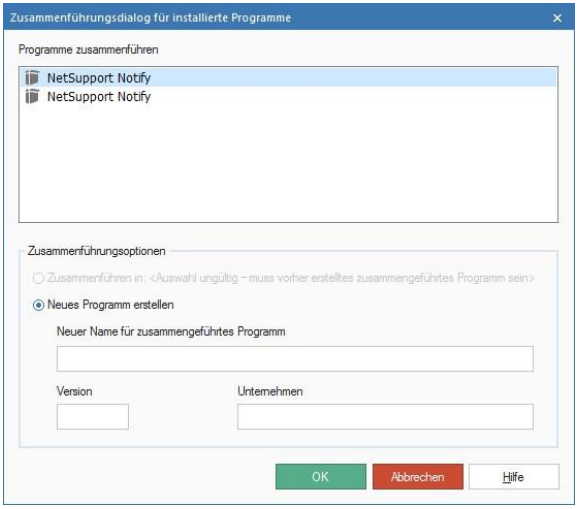
Zur Verwaltung der Lizenzinformationen für ein Programm wählen Sie das gewünschte Programm und klicken auf **Lizenzinformationen**.

Wenn Sie bei Aktualisierungen von einer früheren Version von DNA Applikationsgruppen Lizenzen zugewiesen haben, wird der Lizenzkonvertierungsassistent eingeblendet, damit Sie Ihre Lizenzen dem neuen Dialogfeld „Installierte Programme" zuweisen können.

Installierte Programme zusammenführen

In diesem Dialogfeld können Sie mehrere installierte Programme in eine einzige Gruppe zusammenführen. Es eignet sich ideal zur Suche verschiedener Versionen derselben Software. Die Programme, die Sie zusammenführen, werden angezeigt.

Hinweis: Programme dürfen nur zusammengeführt werden, wenn es sich effektiv um dasselbe Produkt handelt, z. B. NetSupport Manager 10.01 und NetSupport Manager 10.02. Die zusammengeführten installierten Programme werden zu Lizenzzwecken als dasselbe Produkt behandelt. Die Gruppierung verschiedenartiger Produkte kann zu unvorhersehbaren Ergebnissen führen und sich negativ auf die Lizenzierung auswirken.



Zusammenführungsoptionen

Zusammenführen in 'xxxxxxxxxxx'

Das neue Programm wird in eine vorher erstellte zusammengeführte Gruppe zusammengeführt. Klicken Sie auf den gewünschten Namen, um ihn auszuwählen.

Neues Programm erstellen
Oder geben Sie einen neuen Namen für die Gruppe ein.

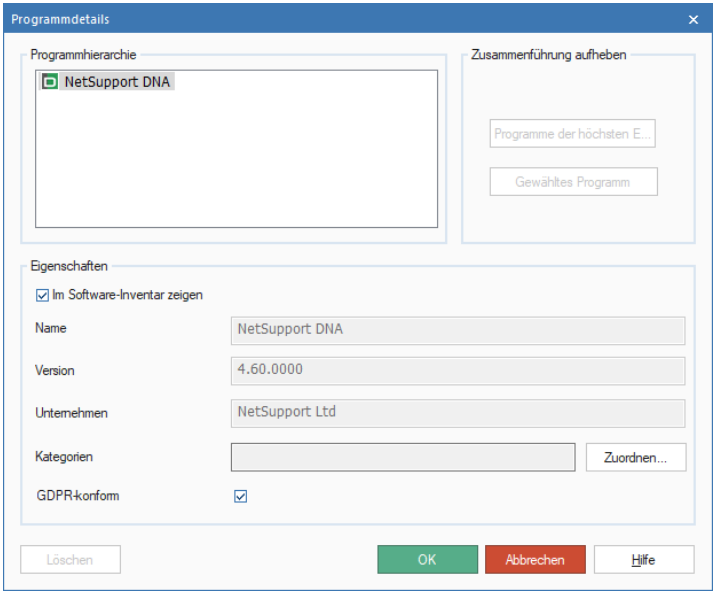
Version
Geben Sie gegebenenfalls die Version des Programms ein.

Unternehmen
Geben Sie gegebenenfalls den Unternehmensnamen ein.

Klicken Sie auf **OK**, um die neue Gruppe zu erstellen. Die Zusammenführung der Programme kann später gegebenenfalls wieder aufgehoben werden.

Installierte Programme bearbeiten

In diesem Dialogfeld sehen Sie die Eigenschaften eines installierten Programms. Wenn es sich bei dem Objekt um eine zusammengeführte Gruppe handelt, werden alle Programme in der Gruppe aufgeführt. Zusammengeführte installierte Programme lassen sich gegebenenfalls hier wieder trennen.



Zusammenführung aufheben

Programme der höchsten Ebene

Die Zusammenführungen aller Programme in der Gruppe werden aufgehoben.

Ausgewählte Programme

Das ausgewählte Programm wird von der Gruppe getrennt.

Hinweis: Wenn die Zusammenführung der Gruppe aufgehoben wird, kehren Lizenzen zum Ursprungsprogramm zurück. Alle Lizenzen, die der Gruppe nach der Zusammenführung zugewiesen wurden, müssen manuell dem richtigen installierten Programm zugewiesen werden.

Eigenschaften

Zeigt die Eigenschaften des Programms. Für eine zusammengeführte Gruppe lassen sich diese Details ändern. Name, Version und Gesellschaftsdetails können nur für eine zusammengeführte Gruppe bearbeitet werden.

In Display zeigen

Ermöglicht die Beschränkung der Anzahl Objekte, die in der Softwareinventarisierung aufgeführt sind. Wenn diese Option nicht markiert ist, wird das Programm aus der Liste der angezeigten Objekte entfernt.

Kategorien

Ermöglicht es Ihnen, das Programm einer Kategorie zuzuordnen. Klicken Sie auf Zuordnen, und der Programmkategorien-Dialog erscheint.

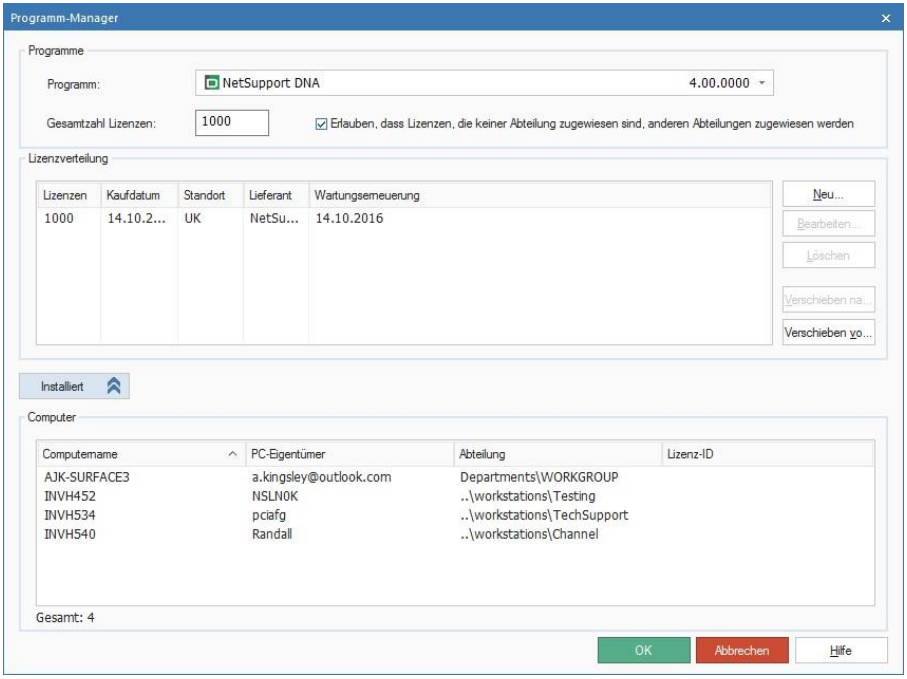
GDPR-konform

Ermöglicht es Ihnen zu bestätigen, dass ein Programm GDPR-konform ist.

Lizenzmanagement für installierte Programme

In DNA können Sie für jedes installierte Programm Lizenzinformationen festhalten. Vollständige Lizenzinformationen wie Einkaufsdetails, Angaben zu Drittpersonen und Wartungsdetails lassen sich im Dialogfeld „Lizenzinformationen" speichern. Lizenzen können auch Abteilungen zugewiesen werden. Alle nicht zugewiesenen Lizenzen sind für alle Abteilungen, denen noch keine Lizenzen zugewiesen wurden, verfügbar.

Hinweis: Um zu verhindern, dass nicht zugewiesene Lizenzen anderen Abteilungen zugewiesen werden, deaktivieren Sie die Option **Zuweisung noch keiner Abteilung zugewiesener Lizenzen zu anderen Abteilungen erlauben**.



Wählen Sie die Anwendung aus der Programmdropdownliste, in der Sie die Lizenzinformationen festhalten wollen. Klicken Sie auf **Neu** und geben Sie die gewünschten Angaben ein. Um Lizenzinformationen zu ändern, wählen Sie den aktuellen Record und klicken auf **Bearbeiten**.

Wenn Sie die Lizenzinformationen bei der falschen Anwendung festgehalten haben, können Sie sie zur richtigen Anwendung verschieben.

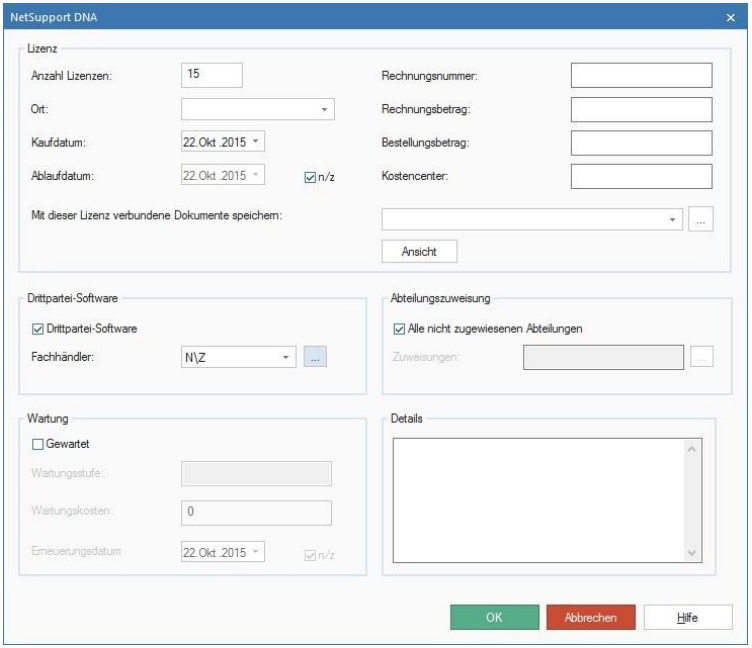
Klicken Sie auf Verschieben an und wählen Sie die entsprechende Anwendung auf der Liste, um Lizenzinformationen an ein anderes Programm zu übertragen. Klicken Sie auf **Verschieben von**, um Lizenzinformationen von einer anderen Anwendung zu übertragen.

Klicken Sie auf **Installiert**, um Angaben über den Installationsort der Lizenzen einzublenden.

Lizenzinfo

Geben Sie die gewünschten Lizenzinformationen ein.

Wenn der Softwarelieferant zur Zeit nicht aufgeführt ist, klicken Sie auf ..., um einen neuen Händlerrecord zu erstellen.



Lizenzen lassen sich gegebenenfalls Abteilungen zuweisen. Deaktivieren Sie alle nicht zugewiesenen Abteilungen und klicken Sie auf ..., um die Abteilung und Anzahl der zuzuweisenden Lizenzen anzugeben.

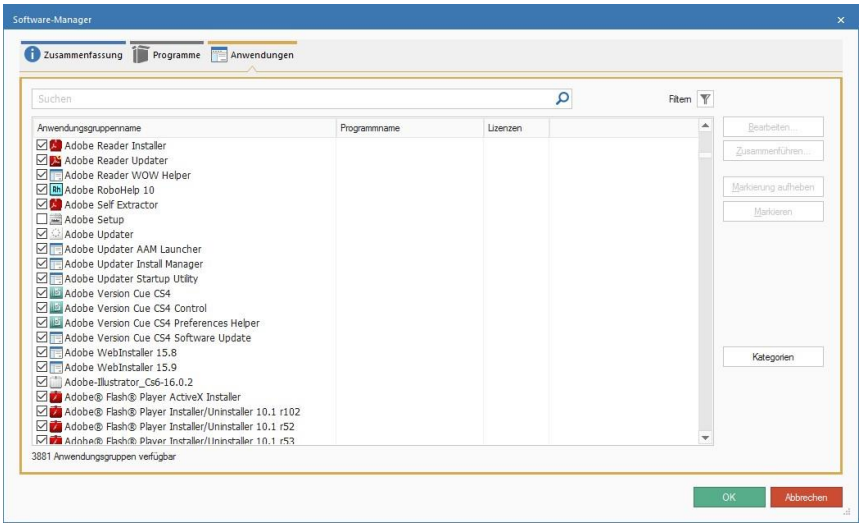
Anwendungsgruppen

Bei der Software-Applikationen werden alle gescannten Anwendungen zwar standardmäßig eingeschlossen, aber Sie können den Inhalt anpassen, um den Umgang mit der Liste zu vereinfachen. Mit der Option "Anwendungsgruppen" können Sie bestimmen, welche Objekte in das Inventar aufgenommen werden und es lassen sich mehrere Versionen derselben Software in den gleichen Record zusammenführen. Lizenzstufen lassen sich ebenfalls verwalten.

The erner können Sie über die Option **Anwendungsmetering** auf die Gruppen zugreifen.

1. Klicken Sie auf den Dropdownpfeil des Softwaresymbols und wählen Sie im Menü die Option {Anwendungsmanager}.
   Oder
   Klicken Sie auf das Symbol **Anwendungsmanager** der Softwareinventarisierungsgruppe.
2. Der Softwaremanager-Dialog erscheint. Wählen Sie die Anwendungen-Registerkarte.
3. Hier sind die auf allen Agent PCs gefundenen Anwendungen aufgeführt, sowie die Anzahl der Lizenzen, wenn diese aufgezeichnet wurde. Das Kontrollkästchen neben jeder Anwendung zeigt an, ob sie zum Inventar gehört oder nicht.

Hinweis: Die Lizenzinformationen werden nur dann eingeblendet, wenn die Applikation im Dialogfeld „Applikationsgruppe bearbeiten" dem installierten Programm zugewiesen wurde und die Lizenzinformationen im Manager für installierte Programme konfiguriert sind.



Sie können eine bestimmte Anwendung schnell finden, indem Sie sie im Suchfeld eintippen.

Um die Liste übersichtlicher zu machen, können Sie die angezeigten Anwendungen filtern. Wenn Sie auf  klicken, erscheint der Anwendungsgruppenfilter-Dialog. Von hier aus können Sie wählen, welche Gruppen angezeigt werden sollen.

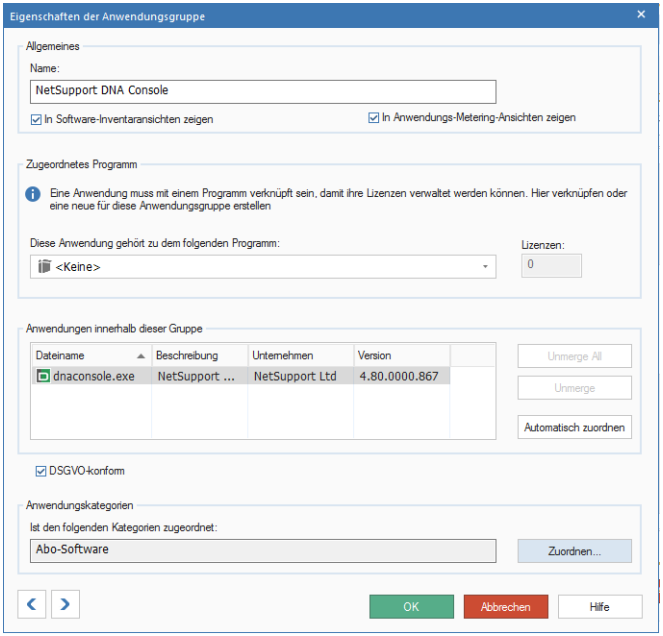
Es können Anwendungsgruppen-Kategorien erstellt werden, mit denen Sie ähnliche Anwendungen gruppieren können. In den Fenstern "Softwareinventarisierung" und "Anwendungsmetering" lassen sich Objekte nach Gruppe anzeigen statt "alle" Objekte aufzuführen. Die Suche nach spezifischen Records wird dadurch erleichtert. Klicken Sie auf Kategorien.

Um die Eigenschaften einer Applikation zu ändern, wählen Sie das entsprechende Objekt in der Liste und klicken auf **Bearbeiten**.

Mehrere Anwendungen lassen sich zu einer neuen Anwendungsgruppe zusammenführen. Wählen Sie die gewünschten Objekte (durch Umschalt-Klick oder Strg-Klick) und klicken Sie auf **Zusammenführen**.

Anwendungsgruppe bearbeiten

In diesem Dialogfeld können Sie die Eigenschaften einer Applikationsgruppe bearbeiten.



Allgemein

Name

Zeigt den Namen der gewählten Anwendung an. Sie können die aufgeführte Beschreibung für beliebige Objekte ggf. ändern.

In Softwareliste zeigen

Ermöglicht die Beschränkung der Anzahl Objekte, die in der Softwareinventarisierung aufgeführt sind. Wenn diese Option nicht markiert ist, wird die Anwendung aus der Liste der angezeigten Objekte entfernt.

In Anwendungsmetering zeigen

Wenn die Markierung aufgehoben wird, wird die Anwendung aus dem Anwendungs-Metering- und Aktivitäten-Informationsfenster entfernt.

Anwendungen in dieser Gruppe
Ermöglicht das Verknüpfen der Applikation mit dem installierten Programmeintrag, sodass alle Lizenzinformationen für das installierte Programm angezeigt werden. Lizenzen können im Manager für installierte Programme verwaltet werden.

Hinweis: Damit die Lizenzen angezeigt werden, muss die Applikation mit dem installierten Programm verknüpft sein.

Anwendungen in dieser Gruppe
Zeigt alle anderen Anwendungen, die in dieser Gruppe enthalten sind.

Zusammenführen rückgängig/Alle Zusammenführungen aufheben
Zusammengeführte Anwendungen lassen sich ggf. wieder trennen.

Automatisch zuordnen
Ermöglicht es Ihnen, Beschreibungen/Schlüsselwörter zu erstellen, die eine Anwendung bei Übereinstimmung automatisch dieser Gruppe hinzufügen werden.

DSGVO-konform
Hier können Sie bestätigen, dass die Anwendung DSGVO-konform ist.

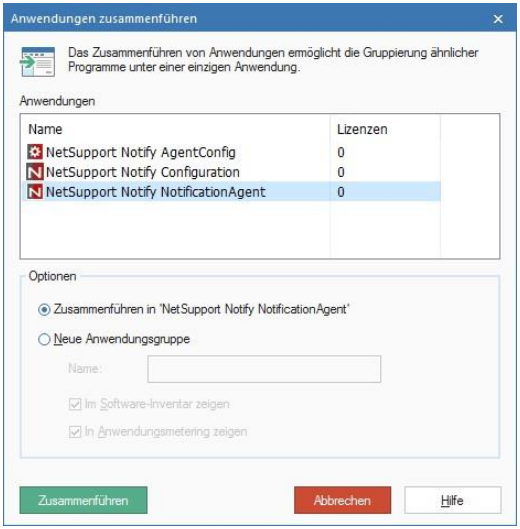
Anwendungskategorien
Ermöglicht es Ihnen, die Anwendung einer Kategorie zuzuordnen. Klicken Sie auf Zuordnen; nun erscheint der Anwendungsgruppenkategorien-Dialog.

Hinweis: Damit eine Anwendung in der Effizienzansicht als Abo-Software angezeigt wird, müssen Sie sie der Kategorie Abo-Software zuweisen.

Scrollen Sie mit  rückwärts oder vorwärts durch die einzelnen Objekte, um die Anwendungseigenschaften einzublenden. Geben Sie ggf. eine neue Beschreibung ein.

Anwendungsgruppen zusammenführen

In diesem Dialogfeld können Sie mehrere Anwendungen in eine einzige Gruppe zusammenführen. Ideal für die Suche verschiedener Versionen derselben Software.



Zusammenführen in 'xxxxxxxxxxx'

Der neuen Anwendungsgruppe kann der Name eines der aufgeführten Objekte zugewiesen werden. Klicken Sie auf den gewünschten Namen, um ihn auszuwählen.

Neue Anwendungsgruppe

Oder geben Sie einen neuen Namen für die neue Gruppe ein.

In Softwareliste zeigen

Wenn diese Option nicht markiert ist, erscheint die neue Anwendungsgruppe nicht in der Softwareinventarisierung.

In Anwendungsmetering zeigen

Wenn diese Option nicht markiert ist, wird die Anwendungsgruppe aus dem Informationsfenster für das Anwendungsmetering entfernt.

Klicken Sie auf **Zusammenführen**, um die neue Gruppe zu erstellen. Das Zusammenführen der Anwendungen kann später ggf. wieder rückgängig gemacht werden.

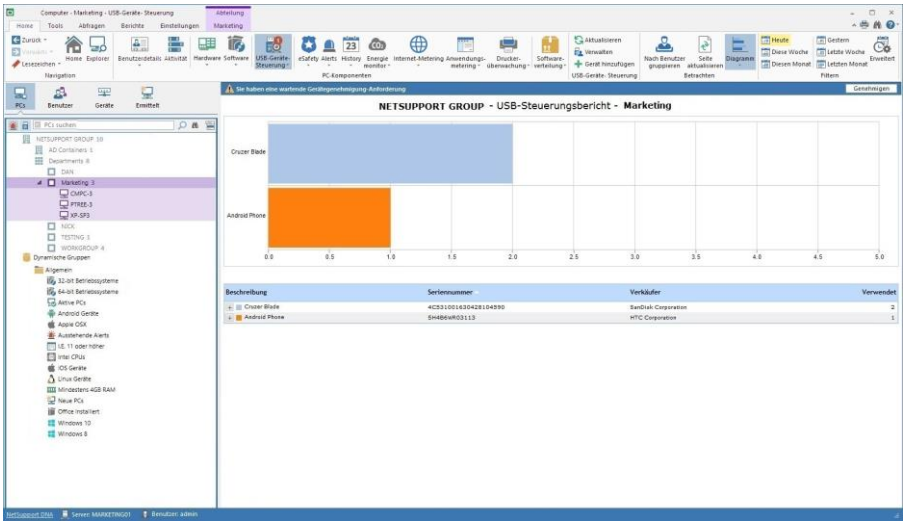
USB-Geräte-Steuerung

NetSupport DNA bietet eine einfache und effektive Lösung für das Management der USB Memorystickbenutzung, um zur Erhaltung der Sicherheit im Unternehmensnetzwerk beizutragen. Die Benutzung von Memorysticks kann für das ganzeUnternehmen oder für spezifische Abteilungen gesteuert werden, und die Benutzung kann auf vollen Zugriff, allen Zugriff sperren, schreibgeschützten Zugriff oder Ausführen von Anwendungen von unbekannten Memorysticks verhindern eingestellt werden. Alternativ können individuelle Memorysticks in NetSupport DNA "autorisiert" werden, und die Benutzung von Memorysticks im Unternehmen kann auf diese autorisierten beschränkt werden.

Ein Programmadministrator kann einen Memorystick an einen lokalen PC anschließen und seine Benutzung dann innerhalb der DNA-Konsole entweder für eine bestimmte Abteilung oder einen bestimmten Benutzer autorisieren. Wenn Autorisierung für einen Benutzer erteilt wird, kann die Genehmigung auf eine begrenzte Zeitspanne beschränkt werden. Benutzer, die einen nicht-autorisierten Memorystick anschließen, können gegebenenfalls auch Remote-Autorisierung beantragen. NetSupport DNA kann nicht nur sowohl Wechsel- (Memorystick) und portable (Handy, Tablet, Kamera) Speichergeräte identifizieren, es bietet auch eine ähnliche Benutzungssteuerung für CD / DVD Geräte (einschließlich USB und virtuell).

1. Klicken Sie auf dem **USB-Geräte-Steuerung** Symbol im Menüband. Nun erscheint das USB-Geräte-Steuerung-Fenster.

   Hinweis: Wenn die Komponentensymbole ausgeblendet sind, klicken Sie auf die Registerkarte **Home**.



Wählen Sie in der hierarchischen Strukturansicht die Ebene, auf der Sie die Meteringdaten betrachten möchten: Unternehmen, Abteilung, AD Container, dynamische Gruppe oder individueller Agent.

Im Informationsfenster ist ein Breakdown für jedes gewählte Objekt in Grafik- und Listenformat angezeigt. Um den Graph in einem anderen Format anzuzeigen, klicken Sie auf dem Diagramm-Symbol-Dropdownpfeil in der Menüleiste und wählen das entsprechende Format.

Um die aktive Ansicht auszudrucken, klicken Sie auf dem  Symbol oben auf der Konsole.

Hinweis: Durch Anklicken des Chart-Symbols im Ribbon wird die Grafik ein-/ausgeblendet.

Sie können die Daten für eine spezifische Zeitperiode betrachten. Um zwischen verschiedenen Zeitperioden hin- und herzuschalten, klicken Sie das entsprechende Symbol im Filterbereich des Menübands an. Wenn Sie auf Erweitert klicken, können Sie einen benutzerdefinierten Datum-/Zeitfilter anwenden. Aufgelistete Beschreibungen lassen sich erweitern, so dass Sie ein individuelles Agentbreakdown für jedes Objekt erhalten.

Die gezeigten Arbeitsstunden können im DNA Konfigurationskatalog für Ihre Organisation angepasst werden. Siehe Konsolenanpassungen – Allgemein für weitere Informationen.

Wenn Sie **Nach Benutzer gruppieren** auswählen, können Sie die USB-Gerätesnutzung nach der Benutzer-ID von Agents statt dem PC betrachten. Diese Option ist in der Benutzerstrukturansicht nicht verfügbar.

Wenn Sie **Nach PC gruppieren** auswählen, können Sie die USB-Gerätesnutzung nach PC-Details und nicht Benutzerdetails des Agents betrachten, während Sie sich in der Benutzerstrukturansicht befinden. Diese Option ist in der Strukturansicht des PCs nicht verfügbar.

Hinweis: In der Standardeinstellung ist die USB-Geräte-Steuerung deaktiviert. Sie können sie in der DNA Konfiguration – USB-Geräte-Steuerungseinstellungen aktivieren und auch die Zugriffsebene für die verschiedenen Gerätetypen voreinstellen.

Wenn Agents ein Gerät in ihren Computer einstecken, werden sie gefragt, ob sie das Gerät registrieren möchten. Dann wird der Konsolenoperator benachrichtigt, dass eine Genehmigungsanforderung vorliegt; oben im USB-Geräte-Steuerung Symbol und im Informationsfenster erscheint ein Benachrichtigungssymbol. Sie können dann die Genehmigungsanforderungen verwalten.

Hinweis: USB-Gerät-Anforderungen werden auch in der Strukturansicht gezeigt, und Sie können diese ein-/ausschalten, indem Sie auf  klicken.

Geräte können für Abteilungen oder Benutzer registriert und genehmigt werden, bevor sie an die Benutzer ausgegeben werden. Klicken Sie auf dem Dropdownpfeil des USB-Geräte-Steuerung Symbols und wählen Sie {Gerät hinzufügen} oder klicken Sie auf dem Gerät hinzufügen Symbol im Menüband. Stecken Sie das zu registrierende Gerät ein. Nun erscheint der USB-Gerätdetails Dialog, mit dem Sie das Gerät registrieren können.

Das Interval, mit dem der Server auf Geräte scannt, kann in der NetSupport DNA Einstellungen-Option angepasst werden.

Abfragen
Wählen Sie zur Anzeige des Abfragefensters die Registerkarte „Abfragen".

Mit dem Abfragetool von DNA können Sie Datenbankeinträge abrufen, die bestimmte Kriterien erfüllen. Abfragen zu der Komponente, die gerade

betrachtet wird, sind aufgelistet, was ein schnelles Abrufen der Ergebnisse ermöglicht.

Klicken Sie in der Menüleiste auf dem Abfrage hinzufügen Symbol, um eine neue Abfrage zu erstellen, oder klicken Sie auf dem Abfrage bearbeiten Symbol in der Menüleiste, um ein in der Liste vorhandenes Objekt zu bearbeiten.

Berichte
Wählen Sie zur Anzeige des Berichtfensters die Registerkarte „Berichte".

Jeder Komponente ist eine Reihe von vordefinierten Managementberichten, die vom Crystal Reports-Modul gespeist werden, beigefügt. Wählen Sie den geforderten Bericht in der Dropdown-Liste. Die Ergebnisse erscheinen im Informationsfenster. Sie lassen sich ggf. exportieren.

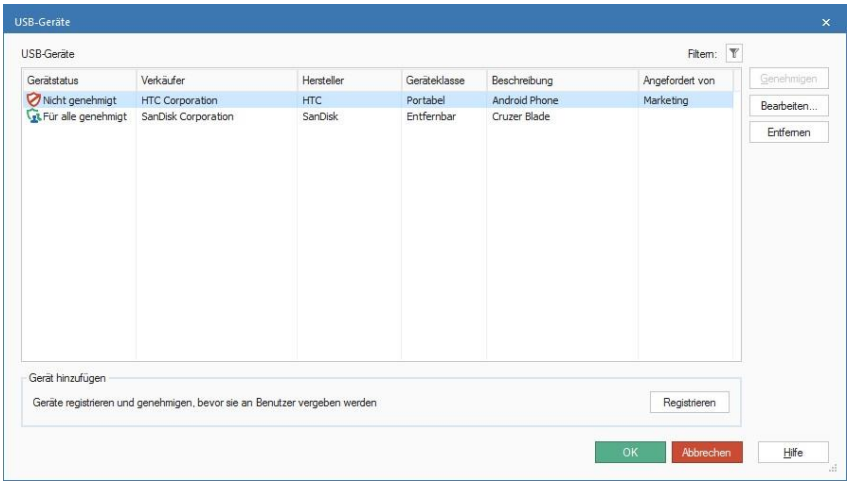
Registrierung von USB-Geräten

Wenn USB-Geräte-Steuerung aktiviert ist, und ein Agent ein USB-Gerät in seinen Computer einsteckt, das noch nicht genehmigt worden ist, wird dem Agent gemeldet, dass das Gerät blockiert ist, und er wird gefragt, ob er Zugriff für das Gerät anfordern möchte. Die Konsolenoperators werden an der Konsole über alle Genehmigungsanforderungen benachrichtigt.

Verwaltung von Genehmigungsanforderungen

1. Klicken Sie auf dem Dropdownpfeil des **USB-Geräte-Steuerung** Symbols und wählen Sie {Verwalten}.
   Oder
   Klicken Sie auf dem **Verwalten** Symbol im Menüband.
   Oder
   Klicken Sie in der Genehmigungsbenachrichtung im Informationsfenster auf **Genehmigen**.
2. Der USB-Geräte Dialog erscheint. Es wird eine Liste aller USB-Geräte angezeigt, die den Gerätstatus und Details zeigt.

Hinweis: Sie können die USB-Geräte, die angezeigt werden, filtern, indem Sie auf dem **Filter** Symbol klicken und wählen, welcher Gerätstatus angezeigt werden soll.



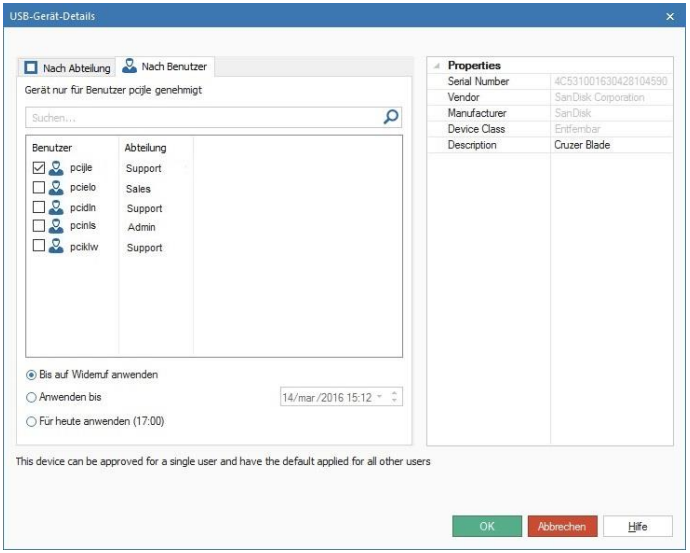
3. Wählen Sie das Gerät, das auf Authorisierung wartet und klicken Sie auf **Genehmigen,** um die Anforderung zu authorisieren.
4. Um vorhandene Geräte zu bearbeiten, klicken Sie auf **Bearbeiten**.
5. Um ein Gerät zu entfernen, klicken Sie auf **Entfernen**.

USB-Gerät hinzufügen
USB-Geräte können im Voraus genehmigt werden, bevor sie an die Benutzer ausgehändigt werden.

1. Klicken Sie auf dem Dropdownpfeil des USB-Geräte-Steuerung Symbols und wählen Sie {Gerät hinzufügen}.
   Oder
   Klicken Sie auf dem **Gerät hinzufügen** Symbol im Menüband.
   Oder
   Klicken Sie im Gerät verwalten Dialog auf **Registrieren**.
2. Stecken Sie das USB-Gerät in einen Port, um es zu registrieren.
3. Nun erscheint der USB-Gerät-Details Dialog, der es Ihnen ermöglicht, das Gerät für Abteilungen oder individuelle Benutzer zu authorisieren.

USB-Gerät-Details

Dieser Dialog ermöglicht es Ihnen, USB-Geräte für Abteilungen oder individuelle Benutzer zu genehmigen.



Es werden die Eigenschaften für das Gerät angezeigt, das Sie gerade genehmigen. Die Beschreibung kann durch Überschreiben im Beschreibung-Feld geändert werden.

Wählen Sie die Registerkarte Nach Abteilung und haken Sie die Abteilungen an, für die das Gerät genehmigt werden soll, oder klicken Sie auf die Registerkarte Nach Benutzer, um es für individuelle Benutzer zu authorisieren, und haken Sie die Benutzer an, für die das Gerät genehmigt werden soll. Heben Sie die Markierungen von Abteilungen oder Benutzern auf, für die Sie das Gerät nicht genehmigen wollen.

Sie können schnell nach Benutzern suchen, indem Sie sie im Suchfeld eingeben und dann auf klicken. Wenn Sie nach Benutzer genehmigen, haben Sie die Option, die Genehmigung bis auf Widerruf anzuwenden oder sie zeitlich zu begrenzen.

Es wird der Standardstatus für die aktuelle Abteilung angezeigt. Sie können diesen auf das Gerät anwenden, indem Sie auf **Anwenden** klicken.

eSafety

NetSupport DNA hilft Ihnen, die Schutzstrategie Ihrer Schule zu verbessern mit Hilfe der Schlüsselwort- und Begriff-Überwachungsfunktion, die einen Einblick in die und Alerts bei Aktivitäten eines Schülers zu bietet, die darauf hinweisen könnten, das das Kind Aktivitäten nachgeht, die es in Gefahr bringen könnten. Jedes Mal wenn ein Begriff ausgelöst wird, wird eine Risikoanalyse ausgeführt und ein Risikoindexwert zugeordnet, der es dem eSafety-Personal ermöglicht festzustellen, welche ausgelösten Begriffe das größte Risiko darstellen. Zusätzlich ermöglicht es die "Anliegen melden" Funktion den Schülern, ihre Anliegen direkt und diskret einem benannten Personalmitglied zu melden. Dieses erhält dann umgehend ein Alert und kann das Anliegen nachverfolgen und alle folgenden Aktionen direkt in NetSupport DNA aufzeichnen.

Hinweis: Die eSafety Funktion steht nur in der NetSupport DNA Version für das Bildungswesen zur Verfügung.

1. Klicken Sie auf dem **eSafety** Symbol im Menüband.

   Hinweis: Wenn die Komponentensymbole ausgeblendet sind, klicken Sie auf die Registerkarte **Home**.

In eSafety stehen drei Modi zur Verfügung:

Begriffsüberwachung
Anliegen melden
Risikoanalyse

Um zwischen Begriffsüberwachung, Anliegen melden und Risikoanalysen-Modus hin- und herzuschalten, klicken Sie auf dem **Begriffe-**, **Anliegen-** bzw. **Risikoanalyse-**Symbol im Menüband.

Hinweis: eSafety-Daten können auch an der Cloud Konsole angezeigt werden, was es dem eSafety-Personal ermöglicht, auch von außerhalb des lokalen Netzwerks mit einem beliebigen Gerät auf die Daten zuzugreifen.

eSafetyrollen

NetSupport DNA bietet zwei vordefinierte eSafetyrollen: eSafety Administrator, die dem Benutzer vollen Zugriff auf die eSafety Funktionen bietet, und eSafety Benutzer, die es dem Benutzer nur ermöglicht, die ihm zugewiesenen Anliegen zu sehen, eSafety Benutzer, die es dem Benutzer nur ermöglicht, die ihm zugewiesenen Anliegen zu sehen, und die auf ausgelöste Begriffe reagieren können. Der Zugriff auf Anliegen ist auf eSafetyrollen beschränkt, so dass verhindert wird, dass andere Konsolenbenutzer die Anliegen sehen.

Hinweise:

- Die eSafety-Rollen bieten nur Zugriff auf Benutzerdetails, Aktivität, Internet-Metering und eSafety-Komponenten.
- Diese Rollen können nur im eSafety Benutzer Dialog zugewiesen werden, nicht bei der Erstellung eines Konsolenoperators.
- Ein eSafety Administrator hat keinen Zugriff auf die eSafety Einstellungen.

Zuweisung der eSafetyrollen

1. Klicken Sie auf dem **eSafety** Symbol im Menüband.
2. Wählen Sie die **eSafety** Symbol-Dropdownliste und dann {eSafety Benutzer}.
   Oder
   Klicken Sie auf dem **eSafety Benutzer** Symbol im Menüband.
3. Klicken Sie auf **Hinzufügen,** um einen neuen Kontakt zu erstellen.
4. Nun erscheint der eSafety Benutzer-Dialog.
5. Wählen Sie **Neuen Konsolenbenutzer erstellen**, wählen Sie die geforderte Rolle in der Dropdownliste und klicken Sie auf **Erstellen**.

Hinweis: Sie können den Kontakt einem existierenden Konsolenbenutzer zuweisen. Wählen Sie **Dazugehöriger Konsolenbenutzer** und wählen Sie dann einen Konsolenbenutzer in der Dropdownliste. Außerdem müssen die eSafety Zugriffsrechte für den Konsolenbenutzer in seiner Konsolenrolle aktiviert werden, damit er Zugriff auf die eSafety Funktionen hat.

Zugriff beschränken

Nachdem Sie einen eSafety Administrator erstellt haben, kann der Zugriff beschränkt werden, so dass andere Konsolenbenutzer die Kontakte nicht verwalten können.

1. Klicken Sie auf dem **eSafety** Symbol im Menüband.
2. Wählen Sie die **eSafety** Symbol-Dropdownliste und dann {eSafety Benutzer}.
   Oder
   Klicken Sie auf dem **eSafety Benutzer** Symbol im Menüband.
3. Nun erscheint der eSafety Benutzer konfigurieren Dialog.
4. Wählen Sie die Option **Zugriff auf eSafety Administrator-Benutzer beschränken**.

Hinweis: Diese Beschränkung kann nur von einem eSafety Administrator aktiviert werden.

Verwalten der eSafety Administratoren und Benutzer

Dieser Dialog zeigt die Benutzer, die erstellt worden sind, damit die Schüler ihnen Anliegen melden können, und die auf ausgelöste Begriffe reagieren können. Von hier aus können Sie neue Benutzer hinzufügen, existierende Benutzer bearbeiten und bei der Definition von Profilen wählen, welche Benutzer zur Verfügung stehen.

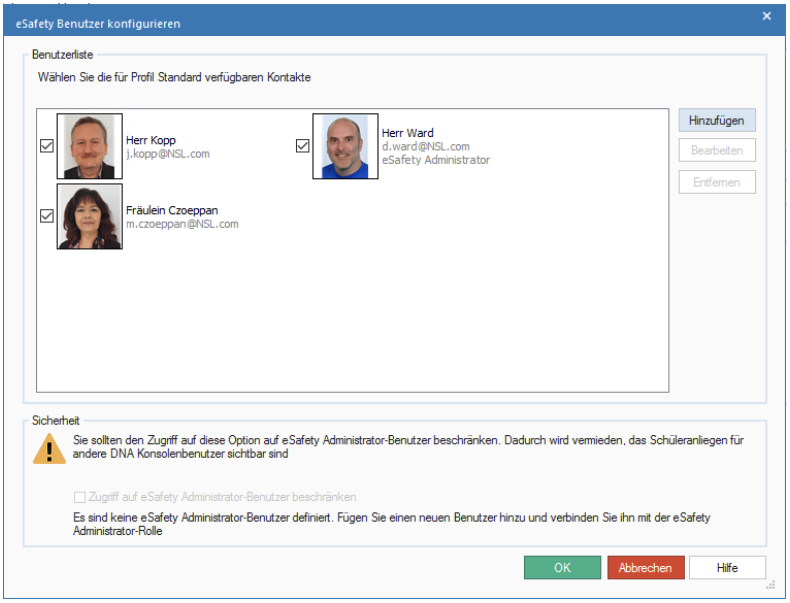
Hinweise:

- Dieser Dialog steht nur zur Verfügung, wenn Anliegen melden in den DNA Konfiguration – Anliegen melden Einstellungen aktiviert worden ist.
- Wenn Sie von den Anliegen melden Einstellungen aus auf diesen Dialog zugreifen, werden Sie die Benutzer wählen, die für das betreffende Profil zur Verfügung stehen. Dies ermöglicht es Ihnen, jedem Profil eine andere Liste von Benutzern zuzuweisen.
- Wenn Sie außerdem möchten, dass das ernannte eSafety-Personal Schüleranliegen empfangen kann, die über eine Website gemeldet werden, müssen Sie sich vergewissern, dass diese Option aktiviert ist, wenn Sie den Benutzer erstellen.

1. Klicken Sie auf dem **eSafety** Symbol im Menüband.
2. Wählen Sie die **eSafety** Symbol-Dropdownliste und dann {eSafety Benutzer}.

   Oder

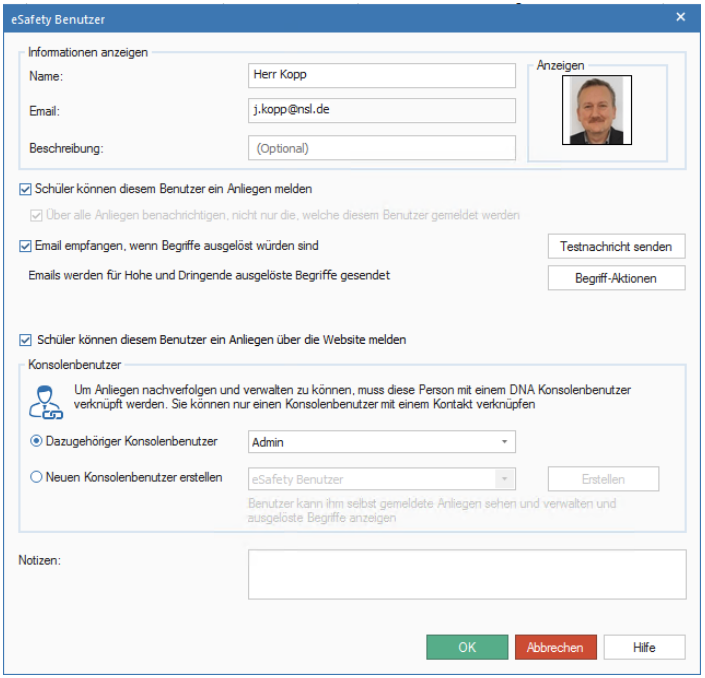
   Klicken Sie auf dem **eSafety Benutzer** Symbol im Menüband.
3. Nun erscheint der eSafety Benutzer konfigurieren Dialog.



4. Alle existierenden Benutzer sind dort aufgelistet.
5. Um einen neuen Benutzer hinzuzufügen, klicken Sie auf **Hinzufügen**.
6. Um einen existierenden Benutzer zu bearbeiten, klicken Sie auf **Bearbeiten**.
7. Um einen Benutzer zu löschen, klicken Sie auf **Entfernen**.
8. Sie können definieren, welche Benutzer zur Verfügung stehen, wenn Sie die Kontakte für die Profile wählen. Benutzer, die angehakt sind, stehen für alle Profile zur Auswahl zur Verfügung. Wenn ein Benutzer nicht zur Verfügung stehen soll, entfernen Sie das Häkchen, und der Benutzer wird dann nicht mehr erscheinen, wenn man von den Anliegen melden Einstellungen aus auf diesen Dialog zugreift.
9. Der Zugriff auf diesen Bereich kann auf eSafety Administratoren beschränkt werden, um zu verhindern, dass andere Konsolenbenutzer Benutzer verwalten. Wählen Sie **Zugriff auf eSafety Administrations-Benutzer beschränken**. Diese Option kann nur aktiviert werden, wenn der gegenwärtig angemeldete Benutzer ein eSafety Administrator ist.

Hinzufügen oder bearbeiten von eSafety Administratoren und Benutzer

Dieser Dialog ermöglicht es Ihnen, existierende Benutzer zu bearbeiten und neue Benutzer zu erstellen, denen die Schüler Anliegen melden können, und die auf ausgelöste Begriffe reagieren können.



1. Geben Sie den Namen, die Emailadresse und eine Beschreibung für den Benutzer ein.
2. Wenn Sie auf dem Anzeigenbild klicken, können Sie ein Foto oder Bild hinzufügen, das dem Benutzer zugeordnet wird.
3. Deaktivieren Sie das Kontrollkästchen **Schüler können diesem Benutzer Anliegen melden**, wenn Sie nicht möchten, dass Schüler diesem Benutzer ein Anliegen melden können.
4. Sie können für einen eSafety Benutzer/In einstellen, dass er über alle gemeldeten Anliegen benachrichtigt wird – wählen Sie **Über alle Anliegen benachrichtigen, nicht nur die, die diesem Benutzer gemeldet werden**. Diese Option steht für eSafety Administratoren nicht zur Verfügung, da diese in der Standardeinstellung alle Anliegen sehen können.

5. Dem Benutzer kann ein Email gesandt werden, wenn ein überwachter Begriff ausgelöst worden ist: wählen Sie **Email empfangen, wenn Begriffe ausgelöst worden sind**. In der Standardeinstellung werden Emails für Begriffe mit hoher und dringender Priorität gesandt – klicken Sie auf **Begriff-Aktionen,** um dies zu ändern. Um ein Test-Email an den Benutzer zu senden, klicken Sie auf **Testnachricht senden**. Um ein Test-Email senden zu können, müssen die Email-Einstellungen konfiguriert worden sein.
6. Wenn Sie außerdem möchten, dass dieser Benutzer Schüleranliegen empfangen kann, die über eine Website gemeldet werden, wählen Sie **Schüler können diesem Benutzer ein Anliegen über die Website melden**.

Hinweis: Um diese Methode zur Meldung von Anliegen zu benutzen, muss die **DNA Cloud Konsole** aktiviert sein.

7. Der neue Benutzer muss einem Konsolenbenutzer zugeordnet werden. Wählen Sie einen existierenden in der Dropdownliste oder wählen Sie **Neuen Konsolenbenutzer erstellen,** um einen neuen Konsolenbenutzer zu erstellen. Es gibt zwei Rollen, aus denen Konsolenbenutzer kreiert werden können: eSafety Administrator, die dem Benutzer vollen Zugriff auf die eSafety Funktionen bietet, und eSafety Benutzer, was dem Benutzer ermöglicht, die ihm selbst zugewiesenen Anliegen zu sehen und zu verwalten und alle Begriffe anzuzeigen, die ausgelöst worden sind.

Hinweis: Bei Zuordnung zu einem existierenden Konsolenbenutzer müssen Sie sich vergewissern, dass dessen Konsolenrolle ausreichende eSafety-Rechte mit sich bringt, um Anliegen anzuzeigen. Andernfalls müssen Sie einen neuen Konsolenbenutzer erstellen.

8. Wenn Sie einen neuen Konsolenbenutzer/In erstellen, klicken Sie auf **Erstellen** und geben Sie ein Passwort für den Benutzer ein. Bei der Standardeinstellung wird der Konsolenbenutzer aufgefordert, dieses Passwort beim ersten Anmelden zu ändern, und per Email über die Passwort-Aktualisierung benachrichtigt. Deaktivieren Sie diese Optionen, wenn Sie sie nicht wünschen, und klicken Sie dann auf **OK**.
9. Einschließlich relevanter Notizen.
10. Klicken Sie auf **OK**.

Begriffsüberwachung

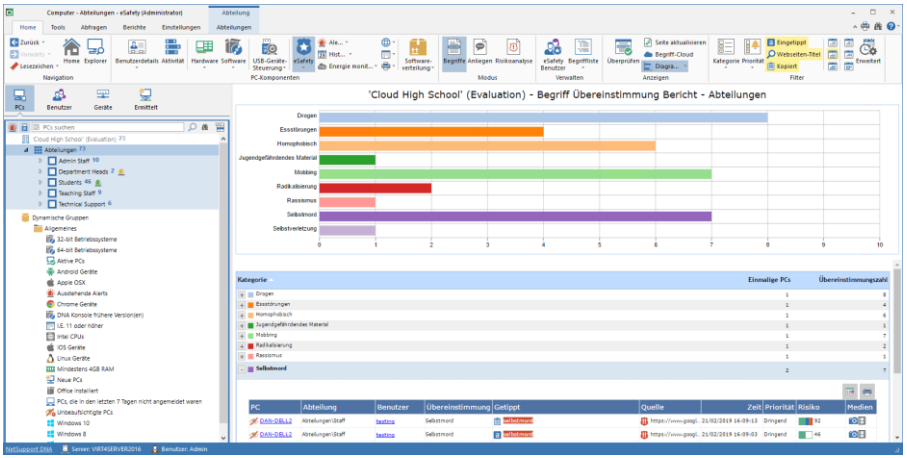
Die NetSupport DNA Schlüsselwort- und Begriffsüberwachungsfunktion bietet Einsicht in und Alerts von allen Aktivitäten der Schüler, die darauf hinweisen könnten, dass diese Aktivitäten nachgehen, durch die sie gefährdet werden könnten. Mit Hilfe einer Datenbank von mitgelieferten eSafety-Schlüsselwörtern und Begriffen, die eine Reihe von Themen umfassen, von Selbstverletzung, Mobbing und Rassismus zu Radikalisierungsgefahren, fungiert NetSupport DNA als Ihre Augen und Ohren bei der Überwachung des Schulnetzwerks. Details/Zusammenhang der ausgelösten Wörter können überprüft werden, wobei die Ergebnisse (verfügbar als Protokoll, Screenshot des Bildschirms, Webcam-Bild des Benutzers oder Bildschirmaufzeichnung, je nach Schweregrad und je nachdem, welche dieser Funktionen die Schule aktiviert – Funktionen stehen für zu Hause benutzte Geräte nicht zur Verfügung) bei Bedarf zur Nachverfolgung an einen Kollegen weitergeleitet werden können. Jedes Mal wenn ein Begriff ausgelöst wird, wird eine Risikoanalyse ausgeführt und ein Risikoindexwert zugewiesen, der es dem eSafety-Personal ermöglicht zu sehen, welche ausgelösten Begriffe das größte Risiko darstellen. Eine innovative Wort-Cloud hebt die Themen mit steigendem Trend für die gesamte Schule hervor und hilft Ihnen, die Ereignisse in einem weiteren Zusammenhang zu sehen.

Hinweis: Schüler können als gefährdet markiert werden, so dass sie von eSafety Benutzern leicht identifiziert und unterstützt werden können. Sie können Schüler als gefährdet markieren, wenn Sie die Benutzerdetails bearbeiten oder indem Sie den Agent in der Benutzerstrukturansicht rechts anklicken. Sie werden dann in der Benutzer-Strukturansicht in der entsprechenden dynamischen Gruppe angezeigt.

1. Klicken Sie auf dem **eSafety** Symbol im Menüband.

   Hinweis: Wenn die Komponentensymbole ausgeblendet sind, klicken Sie auf die Registerkarte „Home".

2. Wählen Sie das **Begriffe** Symbol im Menüband.



Wählen Sie in der hierarchischen Strukturansicht die Ebene, auf der Sie die Meteringdaten betrachten möchten: Unternehmen, Abteilung, AD Container, dynamische Gruppe oder individueller Agent.

Im Informationsfenster ist ein Breakdown für jedes gewählte Objekt in Grafik- und Listenformat angezeigt. Um den Graph in einem anderen Format anzuzeigen, klicken Sie auf dem Diagramm-Symbol-Dropdownpfeil in der Menüleiste und wählen das entsprechende Format.

Um die aktive Ansicht auszudrucken, klicken Sie auf dem  Symbol oben auf der Konsole.

Hinweis: Durch Anklicken des Chart-Symbols im Ribbon wird die Grafik ein-/ausgeblendet.

Wenn ein Schüler ein Schlüsselwort oder einen Schlüsselbegriff eingibt, der mit einem Begriff in der Datenbank übereinstimmt, werden Sie über ein Informationsfenster benachrichtigt und, je nach Prioritätsgrad, wird ein Alert ausgelöst, ein Email gesandt, das Benutzern meldet, dass ein Begriff ausgelöst worden ist, und ein Screenshot oder eine Bildschirmaufnahme erstellt. Sie können die Aktionen für jede Prioritätsstufe in den Begriffüberwachungseinstellungen (können unterschiedliche Aktionen für jedes Profil eingestellt werden) einstellen oder beim Hinzufügen oder Ändern eines Begriffs.

Hinweise:

- Es kann ein Bild des Schülers aufgenommen werden, der den Begriff ausgelöst hat, wenn das Schülergerät eine aktive Webcam hat. In der Standardeinstellung ist diese Aktion deaktiviert, aber sie kann für beliebige Prioritätsstufen angewendet werden. Dies kann nützlich sein, wenn ein Begriff mit hohem Risiko (wie beispielsweise einem Selbstmordbegriff) auf einem gemeinschaftlichen Schul-PC ausgelöst worden ist und auf keine andere Weise festgestellt werden kann, wer am PC gesessen hat. Wenn die Webcam am Schülergerät gegenwärtig benutzt wird, oder wenn die Webcam in den USB-Gerätesteuerungseinstellungen deaktiviert worden ist, wird keine Webcam-Aufnahme gemacht.
- Email-Benachrichtigungen können erst gesandt werden, wenn die Email-Einstellungen konfiguriert worden sind. Sie können die Benutzer einstellen, die Emailbenachrichtigungen über ausgelöste Begriffe erhalten sollen. Dafür muss die Option **Emails empfangen, wenn Begriffe ausgelöst worden sind** im eSafety Benutzer-Dialog gewählt werden.
- Damit ein Alert ausgelöst werden kann, muss das 'eSafety Schlüsselbegriff ausgelöst' Alert in Alerting aktiviert sein.

Es kann ein Genauigkeitsgrad eingestellt werden, der bestimmt, wie genau Wörter von den Schülern eingetippt werden müssen, um als potentiell besorgniserregend markiert zu werden. Sie können diesen Grad in den DNA Konfiguration - Begriffsüberwachung-Einstellungen dafür anpassen, wie genau die Wörter übereinstimmen sollen.

Sie können die Daten für eine spezifische Zeitspanne betrachten. Um zwischen verschiedenen Zeitperioden umzuschalten, klicken Sie auf dem entsprechenden Symbol im Filter-Abschnitt des Menübands. Wenn Sie auf **Erweitert** klicken, können Sie einen benutzerdefinierten Datums-/Zeitfilter anwenden. Die aufgelisteten Beschreibungen können erweitert werden, um für jedes Objekt einen individuellen Agent-Strukturplan zu bieten.

Die gezeigten Arbeitsstunden können im DNA Konfigurationskatalog für Ihre Organisation angepasst werden. Siehe Konsolenanpassungen – Allgemein für weitere Informationen.

Hinweis: Um einen dazugehörigen Screenshot, eine Bildschirmaufzeichnung oder ein Webcam-Bild anzuzeigen , klicken Sie auf dem entsprechenden Mediensymbol neben dem Eintrag des individuellen Agents in der detaillierten Listenansicht.

Eine nützliche Methode, auf spezifische Schlüsselwörter und Begriffe abzuzielen (und die angezeigten Datenmengen zu begrenzen), besteht darin, bestimmte Kategorien, Prioritätsstufen und Quellentextarten anzuzeigen. Um zu wählen, welche Kategorien angezeigt werden sollen, klicken Sie auf dem **Kategorien** Symbol, wählen die gewünschte Gruppe, die angezeigt werden soll, und klicken dann auf **OK**. Um die Daten für einen Prioritätsgrad auszublenden, klicken Sie auf dem **Priorität** Symbol, wird die Auswahl des relevanten Kontrollkästchens aufgehoben und klicken dann auf **OK**. Um Daten für eine Quellentextart auszublenden, klicken Sie auf der entsprechenden Quellenart, um die gelbe Schattierung zu löschen. Das Informationsfenster wird jetzt nur die Daten für die gewählten Kategorien, Prioritätsstufen und Quellentextarten anzuzeigen.

Hinweis: Sie können wählen, bestimmte Quellentextarten nicht zu überwachen, und zwar in DNA Konfiguration – Begriffsüberwachung-Einstellungen.

Es mag Anwendungen und Websites geben, von denen Sie nicht möchten, dass sie eine Schlüsselwortübereinstimmung auslösen; in diesem Fall können Sie wählen, bestimmte Anwendungen und Websites zu ignorieren. Es können Anwendungs- und URL-Listen erstellt werden, die die bei der Begriffsüberwachung zu ignorierenden Anwendungen/Websites enthalten, und diese können in den Begriffsüberwachung-Einstellungen auf Profile angewendet werden.

Sie können die ausgelösten Begriffe überprüfen, indem Sie im Menüband auf **Überprüfen** klicken. Es wird ein Überblick über den Begriff angezeigt, wer ihn ausgelöst hat, was eingetastet worden ist, um ihn auszulösen, sowie Details des Risikoindexwerts, zusammen mit Screenshots, Bildschirmaufzeichnungen und Webcam-Bildern. Von hier aus können Sie drucken, speichern, Emails senden, an PDF exportieren und, wenn ein Screenshot, eine Bildschirmaufzeichnung oder ein Webcam-Bild angehängt ist, einen Verlauf sehen, der angibt, wer diese angesehen hat. Wenn der ausgelöste Begriff als falsche Übereinstimmung bewertet wird, kann er als falscher Alarm markiert werden und erscheint nicht mehr im Hauptinformationsfenster.

Hinweis: Ausgelöste Begriffe, die als falscher Alarm markiert worden sind, können noch angezeigt werden, indem Sie auf dem **Kategorie** Symbol im Menüband klicken und **Falsche Alarme zeigen** wählen. Wenn Sie im Ausgelöste Begriffe Dialog falsche Alarme überprüfen, können Sie alle hinzugefügten Notizen

sehen und den ausgelösten Begriff auch aus der Falscher Alarm Kategorie entfernen.

NetSupport DNA bietet eine Schlüsselwort-Datenbank von übereinstimmenden Wörtern und Begriffe, die auf gefährliche oder unangebrachte Aktivitäten hinweisen können. Zu diesen können weitere hinzugefügt werden, um mit aktuellen Trends auf dem Laufenden zu bleiben. Um Schlüsselwörter und –begriffe zu verwalten und neue hinzuzufügen, klicken Sie auf dem **Begriffliste** Symbol im Verwalten-Abschnitt des Menübands.

NetSupport DNA bietet eine Auswahl von Begriffen in verschiedenen Sprachen. Sie können diese in die Begriffsüberwachung aufnehmen, indem Sie die aufzunehmende Sprache in der Sprachdatei- Dropdown-Liste in der Schlüsselwörter- und Begriffe-Datenbankliste wählen.

Eine Begriff-Cloud bietet eine visuelle Darstellung der häufigsten Begriff- oder Schlüsselwortübereinstimmungen für eine gegebene Zeitperiode.

Ausgelöste Begriffe können mit dem Datenbankwartung-Hilfsprogramm aus der Datenbank entfernt werden. Es wird Ihnen auch die Option geboten, dazugehörige Screenshots und Aufzeichnungen zu entfernen und die ausgelösten Begriffe in der Datenbank zu lassen.

Hinweis: Sie können alle ausgelösten Begriffe nach Risiko anzeigen statt nach Begriffkategorie, indem Sie im Menüband auf **Risikoanalyse** klicken.

Abfragen
Wählen Sie zur Anzeige des Abfragefensters die Registerkarte „Abfragen".

Mit dem Abfragetool von DNA können Sie Datenbankeinträge abrufen, die bestimmte Kriterien erfüllen. Abfragen zu der Komponente, die gerade betrachtet wird, sind aufgelistet, was ein schnelles Abrufen der Ergebnisse ermöglicht.

Klicken Sie in der Menüleiste auf dem Abfrage hinzufügen Symbol, um eine neue Abfrage zu erstellen, oder klicken Sie auf dem Abfrage bearbeiten Symbol in der Menüleiste, um ein in der Liste vorhandenes Objekt zu bearbeiten.

Berichte
Wählen Sie zur Anzeige des Berichtfensters die Registerkarte „Berichte".

Jeder Komponente ist eine Reihe von vordefinierten Management-berichten, die vom Crystal Reports-Modul gespeist werden, beigefügt. Wählen Sie den geforderten Bericht in der Dropdown-Liste. Die Ergebnisse erscheinen im Informationsfenster. Sie lassen sich ggf. exportieren.

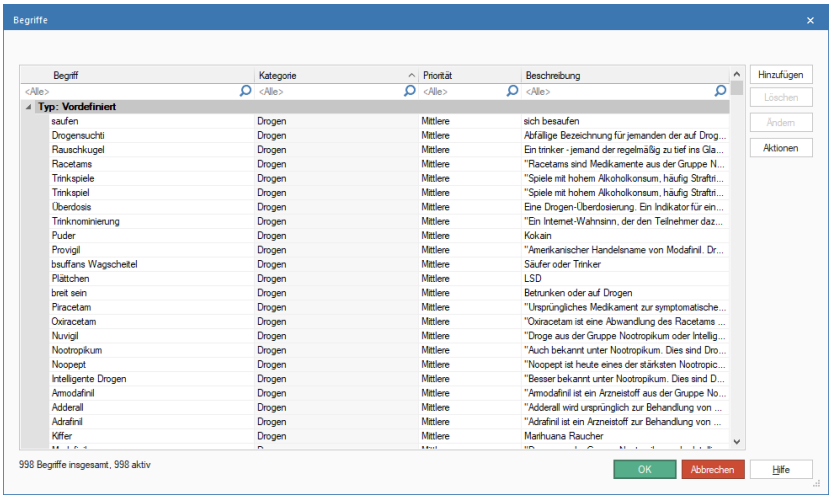
Schlüsselwörter- und Begriffe-Datenbankliste

NetSupport DNA bietet eine Datenbank mit vordefinierten Schlüsselwörtern und -begriffen. Um mit aktuellen Trends mitzuhalten, können Sie Ihre eigenen Begriffe hinzufügen. Schlüsselwörter können Kategorien zugeordnet werden, und Sie können den Prioritätsgrad danach einstellen, wie genau Sie den Begriff überwachen möchten. Bei allen Prioritätsgraden wird die Benutzung im eSafety Informationsfenster aufgezeichnet (außer wenn die Priorität auf Aus gestellt ist). In der Standardeinstellung wird bei mittleren und höheren Graden außerdem ein Alert generiert; bei hohem Grad wird zusätzlich ein Screenshot beim Schüler aufgenommen und ein Email gesandt, das die Benutzer informiert, dass ein Begriff ausgelöst worden ist. Bei dringendem Grad wird eine Bildschirmaufzeichnung bei dem Schüler/In erstellt, der den Begriff ausgelöst hat.

Hinweise:

- Benutzerdefinierte Schlüsselwörter können als .CSV Datei importiert oder exportiert werden.
- Email-Benachrichtigungen können erst gesandt werden, wenn die Email-Einstellungen konfiguriert worden sind. Die Benutzer, die bei Begriffsauslösungen Emailbenachrichtigungen erhalten sollen, können im eSafety Benutzer-Dialog eingestellt werden.
- Die Dauer der Bildschirmaufzeichnung für einen dringenden Prioritätsgrad kann in den Begriffsüberwachungseinstellungen eingestellt werden.

1. Klicken Sie das **eSafety** Symbol im Menüband an und wählen Sie das **Begriffe** Symbol.
2. Wählen Sie die **eSafety** Symbol-Dropdownliste und dann {Schlüsselwörter und –begriffe verwalten}.
   Oder
   Klicken Sie auf dem **Begriffeliste** Symbol im Verwalten-Abschnitt des Menübands.
3. Nun erscheint der Begriffe Dialog.



4. Es wird eine Liste von vordefinierten und benutzerdefinierten Schlüsselwörtern und –begriffen aufgeführt. Die Kategorie, zu der der Begriff gehört, wird zusammen mit der aktuellen Prioritätsstufe und einer Beschreibung des Begriffs angezeigt. Die Gesamtanzahl der Begriffe in der Datenbank und die Anzahl der aktiven Begriffe wird unten im Fenster angezeigt.
5. Sie können die angezeigten Daten filtern oder auf bestimmte Schlüsselwörter durchsuchen, indem Sie in den Suchfeldern oben in jeder Spalte tippen.
6. Sie können die Kategorie, Priorität oder Beschreibung der einzelnen Begriffe in der Liste selbst ändern. Um mehrere Objekte zu ändern, wählen Sie die geforderten Begriffe und klicken dann auf **Ändern**.

Hinweis: Sie können die Priorität nur bei vordefinierten Begriffen ändern.

7. Um einen neuen Begriff hinzuzufügen, klicken Sie auf **Hinzufügen** und geben dann die geforderten Informationen für den Begriff ein.
8. Um einen Begriff zu löschen, wählen Sie ihn und klicken dann auf **Löschen**.

Hinweis: Sie können nur benutzerdefinierte Begriffe löschen.

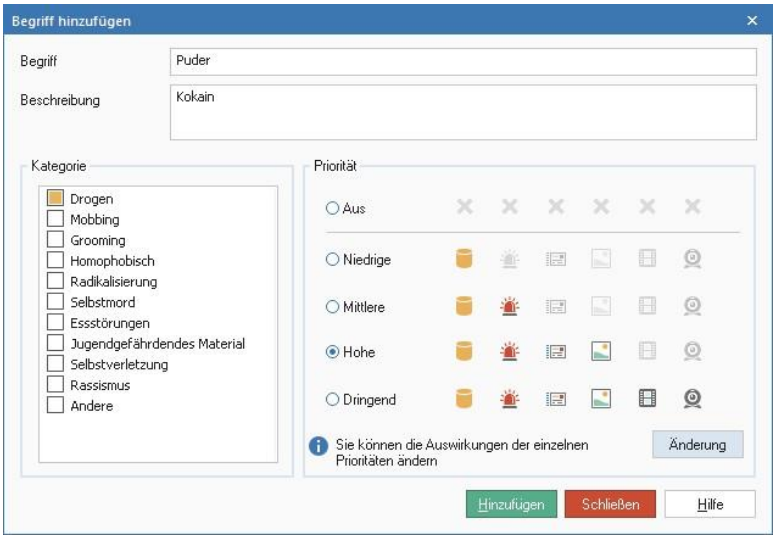
9. Die für jede Priorität ausgeführte Aktion kann angepasst werden, indem Sie auf **Aktionen** klicken.

Hinweis: In den Begriffsüberwachung-Einstellungen können unterschiedliche Aktionen für jedes Profil eingestellt werden.

Wir freuen uns stets über alle Kommentare zu den Begriffen in der Begriffsliste. Senden Sie dem eSafety-Team bitte ein Email unter safeguarding@netsupportsoftware.com.

Schlüsselwörter und –begriffe erstellen oder bearbeiten

Dieser Dialog wird benutzt, um neue Schlüsselwörter und –begriffe zu erstellen oder vorhandene zu bearbeiten.



1. Geben Sie das Schlüsselwort oder den Begriff ein, den Sie überwachen möchten, und eine Beschreibung davon.
2. Wählen Sie, auf welche Kategorie der Begriff sich bezieht und stellen Sie den Prioritätsgrad ein.

Hinweis: Die Aktionen, die bei den einzelnen Prioritäten ausgeführt werden, werden angezeigt. Klicken Sie auf **Ändern,** um sie anzupassen. In den Begriffsüberwachung-Einstellungen können unterschiedliche Aktionen für jedes Profil eingestellt werden.

3. Klicken Sie auf **Hinzufügen,** um den Begriff zur benutzerdefinierten Liste hinzuzufügen.

Hinweis: Beim Bearbeiten vordefinierter Begriffe können Sie nur die Prioritätsstufe und die ausgeführten Aktionen ändern.

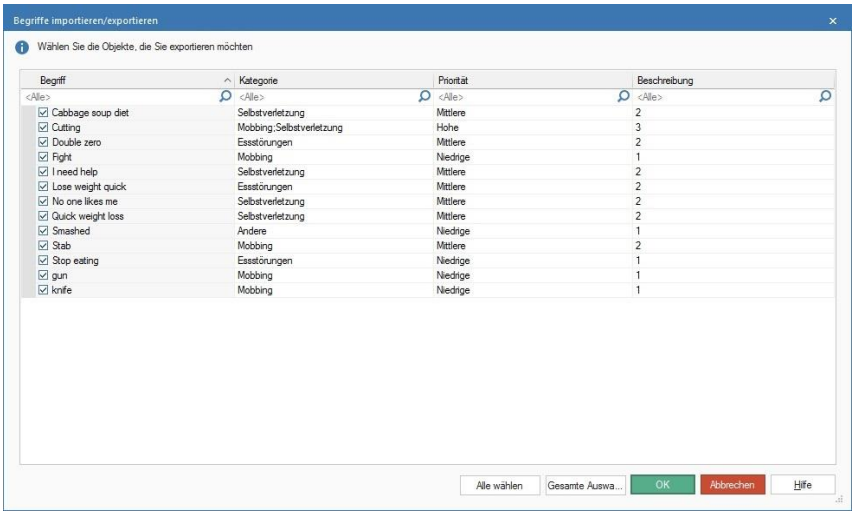
Begriffe importieren/exportieren

NetSupport DNA emöglicht es Ihnen, Schlüsselwörter und Begriffe in eine .CSV Datei zu importieren bzw. aus einer .CSV Datei zu exportieren.

Hinweis: Es können nur benutzerdefinierte Schlüsselwörter importiert oder exportiert werden.

Begriffe exportieren

1. Klicken Sie das **eSafety** Symbol im Menüband an und wählen Sie das **Begriffe** Symbol.
2. Wählen Sie die **eSafety** Symbol-Dropdownliste und dann {Exportieren}.
   Oder
   Wählen Sie die Begriffliste Symbol-Dropdownliste und dann {Exportieren}.
3. Nun erscheint der Begriffe importieren/exportieren Dialog.



4. Es wird eine Liste der benutzerdefinierten Begriffe angezeigt, die zum Exportieren zur Verfügung stehen.
5. Vergewissern Sie sich, dass die Begriffe, die Sie exportieren möchten, angehakt sind, und klicken Sie auf **OK**.

Hinweis: Um alle aufgelisteten Begriffe zu wählen, klicken Sie auf Alle auswählen.

6. Geben Sie einen Namen und Speicherort für die .CSV Datei ein.
7. Klicken Sie auf **Speichern**.

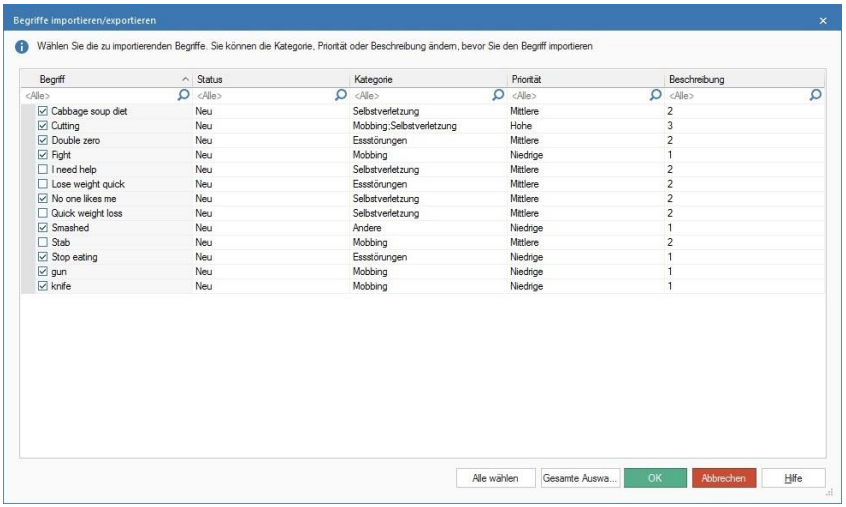
Begriffe importieren
Es können nur .CSV-Dateien importiert werden. Die Datei muss in der Reihenfolge Begriffsname, Kategorie, Prioritätsstufe und Beschreibung formatiert sein.

Die Begriffskategorie und die Prioritätsstufe muss jeweils einen numerischen Wert haben. Eine Liste der Werte ist:

Kategorie	**Wert**	**Priorität**	**Wert**
Drogen	1	Aus	0
Mobbing	4	Niedrige	1
Grooming	8	Mittlere	2
Homophobisch	32	Hohe	3
Radikalisierung	64	Dringend	4
Selbstmord	128		
Essstörungen	256		
Jugendgefährdendes Material	512		
Selbstverletzung	1024		
Rassismus	2048		
Andere	4096		

Hinweis: Die .CSV-Datei muss geschlossen werden, ehe sie importiert werden kann. Wenn die Datei geöffnet ist, kann sie nicht importiert werden.

Begriffe importieren
1. Klicken Sie das **eSafety** Symbol im Menüband an und wählen Sie das **Begriffe** Symbol.
2. Wählen Sie die **eSafety** Symbol-Dropdownliste und dann {Importieren}.
   oder
   Wählen Sie die Begriffliste Symbol-Dropdownliste und dann {Importieren}.
3. Wählen Sie die zu importierenden .CSV Dateien und klicken Sie auf **Öffnen**.
4. Die Begriffe werden im Begriffe importieren/exportieren Dialog angezeigt.



5. Von hier aus können Sie die Kategorie, Priorität und Beschreibung ändern, indem Sie auf dem entsprechenden Feld klicken.
6. Vergewissern Sie sich, dass die Begriffe, die Sie importieren möchten, angehakt sind. Um alle aufgelisteten Begriffe zu wählen, klicken Sie auf Alle auswählen.

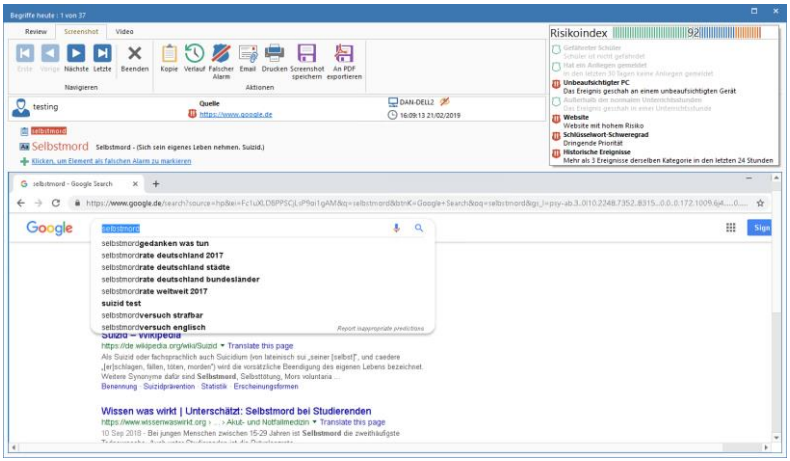
Hinweis: Wenn der Begriff bereits in der Datenbank existiert, wird der Status als vorhanden angezeigt. Diese Begriffe können dennoch importiert werden.

7. Klicken Sie auf **OK**.

Überprüfung der ausgelösten Begriffe

Von hier aus können ausgelöste Begriffe überprüft und freigegeben werden.

1. Wählen Sie die Zeitperiode, für die Sie ausgelöste Begriffe anzeigen möchten, indem Sie auf dem entsprechenden Symbol im Filterabschnitt des Menübands klicken.
2. Klicken Sie das **Überprüfen** Symbol im Menüband an.
3. Nun erscheint der Ausgelöste Begriffe Dialog.



4. Durchscrollen Sie die ausgelösten Begriffe mit den Vor- und Zurück-Pfeilen.
5. Für alle Begriffe wird eine Überprüfen-Registerkarte angezeigt, die einen Überblick über den Begriff bietet, wer ihn ausgelöst hat, was eingetastet worden ist, um ihn auszulösen, und den Indexwert (zusammen mit den Faktoren, die benutzt wurden, um den Wert zu errechnen, so dass Sie sehen können, ob weitere Maßnahmen erforderlich sind). Diese Details können an die Zwischenablage kopiert werden, indem Sie das **Kopieren** Symbol anklicken.

Begriffe, die als "hohe" Priorität gekennzeichnet sind, haben eine Screenshot-Registerkarte, die es Ihnen ermöglicht, den Screenshot anzuzeigen, der erfasst wurde, als der Begriff ausgelöst wurde, und die, die als "dringende" Priorität gekennzeichnet sind, haben auch eine Video-Registerkarte, die es Ihnen ermöglicht, eine Bildschirmaufzeichnung des Ereignisses anzuzeigen.

Hinweis: Eine Webcam-Registerkarte erscheint, wenn Sie die Webcam-Aktion für eine Prioritätsstufe gewählt haben (diese ist in der Standardeinstellung ausgeschaltet und kann bei der Anpassung der ausgeführten Aktionen aktiviert werden). Die Webcam-Registerkarte zeigt ein einziges Bild, das von einer aktiven Webcam am Schülergerät aufgenommen wird und es Ihnen ermöglicht, die Person, die das Schlüsselwort eingetastet hat, leicht zu identifizieren. Dies kann nützlich sein, wenn ein Begriff mit hohem Risiko (wie beispielsweise einem Selbstmordbegriff) auf einem gemeinschaftlichen Schul-PC ausgelöst worden ist und auf keine andere Weise festgestellt werden kann, wer am PC gesessen hat.

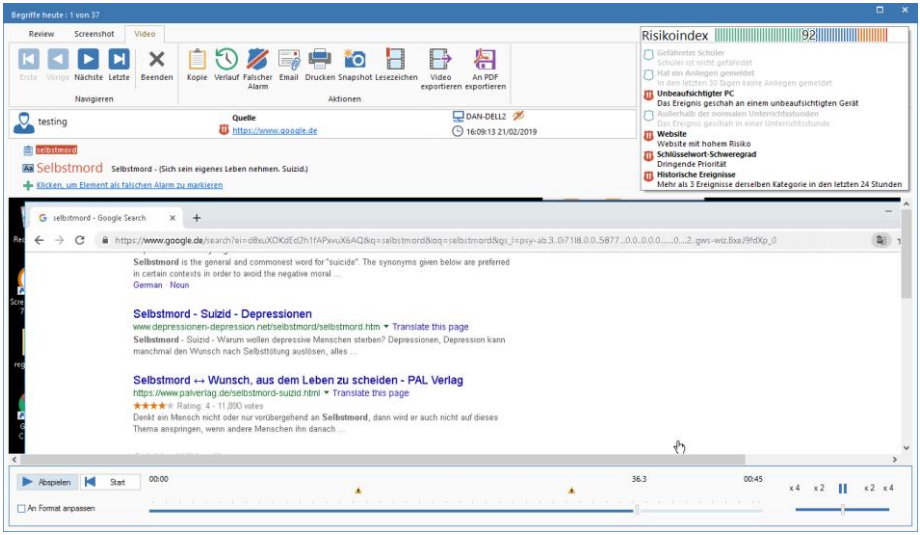
6. Sie können eine Kopie des ausgelösten Begriffs drucken oder emailen, indem Sie auf dem entsprechenden Symbol klicken. Um einen Verlauf anzuzeigen, der zeigt, wer den Screenshot, die Videoaufzeichnung oder das Webcam-Bild angezeigt hat, klicken Sie auf **Verlauf**. Die Details des ausgelösten Begriffs können an ein PDF exportiert werden, indem Sie auf **An PDF exportieren** klicken.

   Hinweis: Sie können den Standardordner, an den das PDF exportiert werden soll, in den Dateispeicherort-Einstellungen angeben und das PDF in den Begriffsüberwachung-Einstellungen mit dem Branding Ihrer Schule anpassen.

7. Wenn der ausgelöste Begriff als falsche Übereinstimmung bewertet wird, kann er als falscher Alarm markiert werden und erscheint nicht mehr im Hauptinformationsfenster. Um einen individuellen Begriff als falschen Alarm zu markieren, wählen Sie **Klicken, um Element als falschen Alarm zu markieren**, geben Sie eine Notiz ein (es erscheint eine Dropdownliste mit früheren Eingaben, oder Sie können Ihre eigene eintippen) und drücken Sie die **Eingabetaste**. Um mehrere Elemente als falsch zu markieren, klicken Sie auf **Falscher Alarm** für die geforderten ausgelösten Begriffe und klicken Sie dann auf **Beenden**. Nun erscheint ein Dialog, in dem Sie aufgefordert werden zu bestätigen, dass diese Begriffe falsche Übereinstimmungen sind, und Sie können eine Notiz für diese Elemente hinzufügen.

Hinweis: Ausgelöste Begriffe, die als falscher Alarm markiert worden sind, können noch angezeigt werden, indem Sie auf dem **Kategorie** Symbol im Menüband klicken und **Falsche Alarme zeigen** wählen. Wenn Sie falsche Alarme in dem Ausgelöste Begriffe überprüfen Dialog überprüfen, können Sie alle Notizen sehen, die hinzugefügt worden sind, den Konsolenbenutzer, der sie als falschen Alarm markiert hat sowie das Datum und die Zeit. Um einen ausgelösten Begriff aus der Falscher Alarm Kategorie zu entfernen, klicken Sie auf **Falscher Alarm** und klicken Sie dann auf **Beenden**.

Anzeigen einer Bildschirmaufzeichnung



Beim Anzeigen einer Bildschirmaufzeichnung erscheinen Steuerelemente für die Wiedergabe, die es Ihnen ermöglichen, zu beobachten, was beim Agent geschah, als der Begriff ausgelöst wurde.

Eine Zeitskala zeigt, wo der Begriff in der Aufzeichnung ausgelöst worden ist und ob Lesezeichen hinzugefügt worden sind. Sie können den Schieberegler benutzen, um zur gewünschten Position zu gehen. Klicken Sie auf **Play**, um die Aufzeichnung zu beginnen – in der Standardeinstellung beginnt sie da, wo der Begriff ausgelöst worden ist (wenn Sie auf **Start** klicken, gelangen Sie zum Anfang der Aufzeichnung).

Sie können in der Aufzeichnung vor- und zurücklaufen, indem Sie auf dem Schieberegler ganz rechts im Dialog klicken. Wenn Sie den Schieberegler freigeben, wird die Aufzeichnung an dieser Stelle angehalten. Wählen Sie **Auf Größe anpassen,** um den gesamten Schülerbildschirm im Anzeigebereich zu zeigen.

Es können Lesezeichen hinzugefügt werden, um wichtige Bereiche der Aufzeichnung zu markieren. Vergewissern Sie sich, dass Sie an der richtigen Stelle auf der Zeitskala sind und klicken Sie auf **Lesezeichen**. Geben Sie eine Beschreibung für das Lesezeichen ein; Sie können eine Liste der Lesezeichen anzeigen, indem Sie auf klicken, und Sie können Lesezeichen von hier aus entfernen. Klicken Sie auf **OK**.

Hinweis: Es kann eine Momentaufnahme der Aufzeichnung gespeichert werden. Klicken Sie auf **Snapshot**, geben Sie einen Namen für den Screenshot ein, wählen Sie den Dateityp, in dem er gespeichert werden soll, und klicken Sie dann auf **Speichern**.

Eine Bildschirmaufzeichnung kann in eine Videodatei konvertiert werden, so dass sie außerhalb der DNA Konsole auf verschiedenen Media Players wiedergegeben werden kann. Sie kann in WMV und AVI Formate konvertiert werden. Klicken Sie auf **Video exportieren**; der Dateiwiedergabe-Konvertierungsassistent führt Sie nun durch den Konvertierungsprozess.

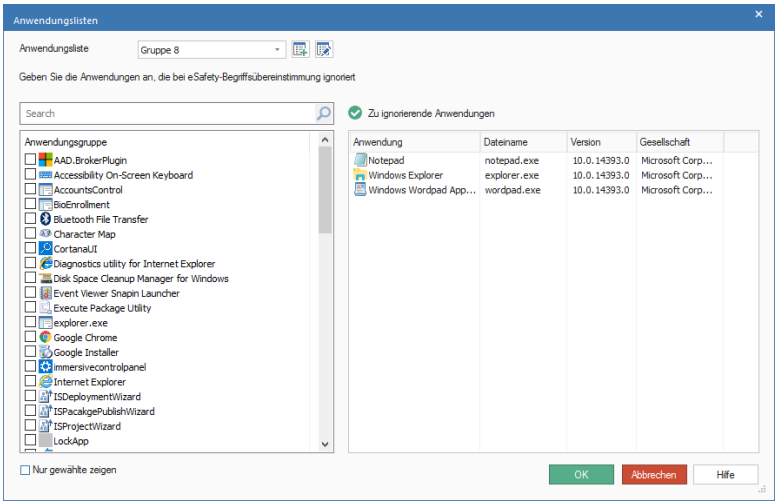
Hinweis: In der Standardeinstellung beträgt die Länge der Bildschirmaufzeichnung 15 Sekunden (fünfzehn Sekunden bevor und nachdem der Begriff ausgelöst wird). Dies kann in den Begriffsüberwachungseinstellungen angepasst werden.

Anwendung-ignorieren-Listen

Bei der Überwachung von Schlüsselwörtern und Begriffen kann es Anwendungen geben, von denen aus keine Schlüsselwortübereinstimmungen ausgelöst werden sollen; in diesem Fall können Sie wählen, dass bestimmte Anwendungen ignoriert werden. Es können Anwendungslisten erstellt werden, die es Ihnen ermöglichen, eine Liste von Anwendungen zu haben, die bei der Begriffsüberwachung ignoriert werden. Es können mehrere Listen erstellt werden, so dass Sie verschiedenen Profilen verschiedene Listen zuordnen können.

Erstellung und Anwendung einer Anwendungsliste

1. Wählen Sie in der Einstellungen-Registerkarte **Existierende Profile verwalten**.
2. Wählen Sie das geforderte Profil in der Liste und klicken Sie auf **Einstellungen**.
3. Wählen Sie **Begriffsüberwachung**.
4. Nun erscheinen die Begriffsüberwachung-Einstellungen.
5. Klicken Sie auf **Anwendungslisten**.
6. Der Anwendungslisten-Dialog erscheint.



7. Um eine neue Anwendungsliste zu erstellen, klicken Sie auf . Geben Sie einen Namen und, falls gefordert, eine Beschreibung für die Liste ein. Sie können eine vorhandene Liste kopieren, indem Sie sie in der 'Kopieren von' Dropdownliste wählen. Klicken Sie auf **OK**. Um eine vorhandene Liste zu bearbeiten, klicken Sie auf .

8. Nun erscheint eine Liste von Anwendungen. Wählen Sie die Anwendungen, die in die Anwendungsliste aufgenommen werden sollen.
9. Klicken Sie auf **OK**.
10. Wählen Sie die geforderte Anwendungsliste im Anwendungslisten-Dropdownmenü.
11. Klicken Sie auf **Speichern**, um die Änderungen anzuwenden.

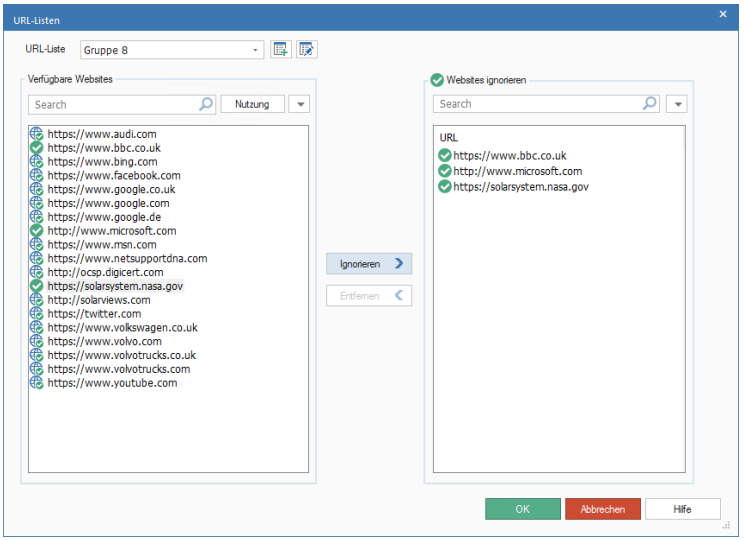
URL-ignorieren-Listen

Bei der Überwachung von Schlüsselwörtern und Begriffen kann es Websites geben, die Sie ignorieren möchten. Es kann eine URL-Liste erstellt werden, die es Ihnen ermöglicht, alle Begriffsübereinstimmungen von Websites zu ignorieren, die in der Liste enthalten sind. Es können mehrere Listen erstellt werden, so dass Sie verschiedenen Profilen verschiedene URL-Listen zuordnen können.

Hinweis: Es können auch URL-Listen für Internetbeschränkungen mit genehmigten oder beschränkten Websites erstellt werden, die Ihnen die Kontrolle darüber ermöglichen, welche Websites von den Agents besucht werden.

Erstellung und Anwendung einer URL-Liste

1. Wählen Sie in der Einstellungen-Registerkarte **Existierende Profile verwalten**.
2. Wählen Sie das geforderte Profil in der Liste und klicken Sie auf **Einstellungen**.
3. Wählen Sie **Begriffsüberwachung**.
4. Nun erscheinen die Begriffsüberwachung-Einstellungen.
5. Klicken Sie auf **URL-Listen**.
6. Der URL-Listen Dialog erscheint. Websites, die bereits von Agents besucht worden sind, werden automatisch in der Verfügbare Websites Liste aufgeführt, und die Standard-URL-Liste wird angezeigt.



7. Um eine neue Website-Liste zu erstellen, klicken Sie auf . Nun erscheint der URL-Liste Dialog. Geben Sie einen Namen und, falls gefordert, eine Beschreibung für die Liste ein. Sie können eine vorhandene Liste kopieren, indem Sie sie in der 'Kopieren von' Dropdownliste wählen. Klicken Sie auf **OK**.

   Hinweis: Es kann eine Internetbeschränkungsliste kopiert werden; URLs in der Genehmigte Websites Liste werden dann zur Websites ignorieren Liste hinzugefügt.

   Um eine vorhandene Liste zu bearbeiten, klicken Sie auf .
8. Um eine vorhandene URL zur Websites ignorieren Liste hinzuzufügen, wählen Sie die URL in der Verfügbare Websites Liste und klicken Sie auf **Ignorieren**, oder schieben Sie die URL mit Drag & Drop auf die Liste.
9. Um eine neue Website zur Liste hinzuzufügen, klicken Sie auf in der Websites ignorieren Liste, wählen Sie **URL hinzufügen** und geben Sie die geforderten Details ein. Die neue Website erscheint nun in der Websites ignorieren Liste und wird auch automatisch zur Verfügbare Websites Liste hinzugefügt. Zum Löschen von URLs klicken Sie auf wählen URL löschen.
10. Wenn die geforderten URLs zur Websites ignorieren Liste hinzugefügt worden sind, klicken Sie auf **OK**.
11. Wählen Sie die geforderte URL Liste im URL Listen Dropdownmenü.
12. Klicken Sie auf **Speichern**, um die Änderungen anzuwenden.

Wählen Sie zum Betrachten vollständiger Daten zur Websitenutzung die gewünschte Website in der Liste „Verfügbare Sites" und klicken Sie auf die **Nutzungsschaltfläche**. Das Dialogfeld „Websitenutzung" wird eingeblendet. Hier sehen Sie, welche Benutzer auf die Website zugegriffen und wie oft sie diese besucht haben. Wenn Sie auf einen Benutzer klicken, erscheint eine vollständige Aufstellung der Zeiten und Dauer des Zugriffs auf die Website durch den betreffenden Benutzer.

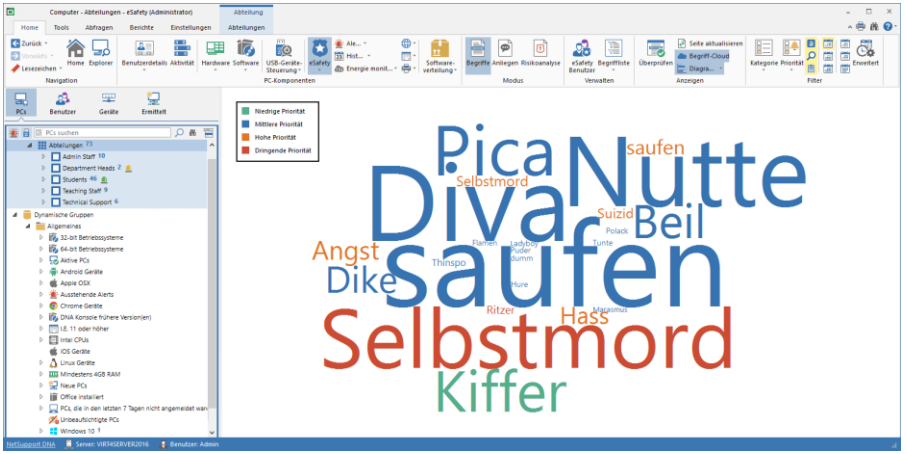
Begriff-Cloud

Die Begriffswolke bietet eine visuelle Darstellung aller ausgelösten Begriffe und hebt Trends in den Themen für die gesamte Schule hervor. Wenn Sie irgendein Wort in der Cloud anklicken, können Sie im Detail sehen, was die Schüler eingetastet haben und welche Anwendung benutzt wurde.

1. Klicken Sie das **eSafety** Symbol im Menüband an und wählen Sie das **Begriffe** Symbol.

   Hinweis: Sie können die Begriffe-Cloud nach Risiko anzeigen; klicken Sie auf dem **Risikoanalyse** Symbol.

2. Klicken Sie auf dem **Begriff-Cloud** Symbol im Menüband.

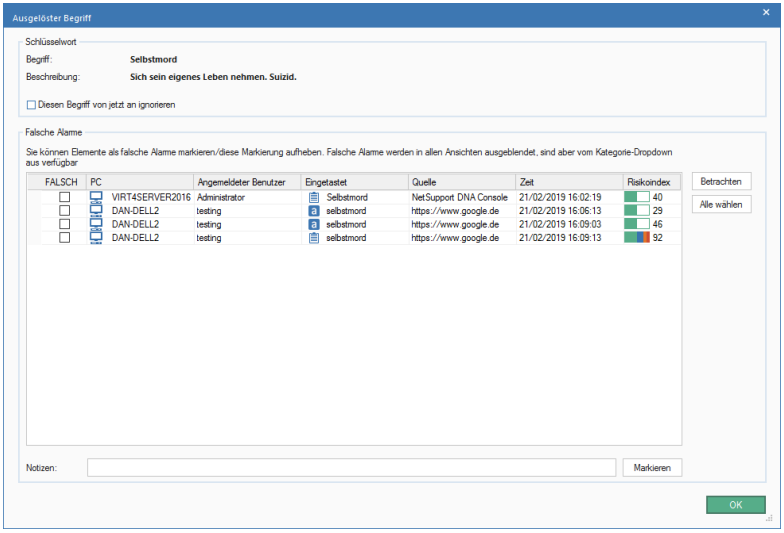


Sie können die angezeigten Datenmengen beschränken, indem Sie bestimmte Kategorien, Prioritätsstufen und Quellentextarten anzeigen. Um zu wählen, welche Kategorien angezeigt werden sollen, klicken Sie auf dem **Kategorie** Symbol, vergewissern Sie sich, dass die geforderten Gruppen gewählt sind, und klicken Sie auf **OK**. Um die Daten für eine Prioritätsstufe auszublenden, klicken Sie auf dem **Priorität** Symbol, heben Sie die Auswahl in den entsprechenden Kontrollkästchen auf und klicken Sie auf **OK**. Um Daten für eine Quellentextart auszublenden, klicken Sie auf der entsprechenden Quellenart, um die gelbe Schattierung zu löschen. Die Begriff-Wolke zeigt jetzt nur Daten für die gewählten Kategorieren, Prioritätsstufen und Quellentextarten.

Die Begriffe-Cloud kann entweder einfarbig angezeigt werden, oder die Begriffe können je nach Prioritätsebene in verschiedenen Farben gezeigt werden, so dass Sie Begriffe, die ein größeres Risiko darstellen, auf einen Blick erkennen können. Klicken Sie die Begriffe-Cloud mit der rechten Maustaste an, wählen Sie **Farbe** und dann die gewünschte Option.

Nutzung anzeigen

1. Klicken Sie ein Wort in der Begriff-Cloud an.
   Oder
   Klicken Sie ein Wort rechts an und wählen Sie **Nutzung anzeigen**.
2. Nun erscheint der Begriff ausgelöst Dialog.



3. Es wird eine Liste von Benutzern angezeigt, die den Begriff ausgelöst haben, was eingetippt wurde und wo, sowie der Risikoindexwert. Von hier aus können Sie wählen, den Begriff von jetzt an zu ignorieren, so dass er nicht mehr in der Begriff-Cloud oder dem Informationsfenster erscheint. Um die vollen Details eines ausgelösten Begriffs anzuzeigen, heben Sie das geforderte Vorkommen hervor und klicken Sie auf **Anzeigen**.
4. Ein ausgelöstes Objekt kann als falscher Alarm markiert werden. Diese Vorfälle werden dann nicht im Informationsfenster gemeldet, werden aber weiterhin gespeichert. Wählen Sie das geforderte Element; Sie können alle Vorkommen wählen, indem Sie auf **Alle wählen** klicken.

Es kann eine Notiz hinzugefügt werden, so dass Sie den Grund angeben können, aus dem der ausgelöste Begriff als falscher Alarm markiert worden ist. Klicken Sie auf **Markieren**. Falsche Alarme können angezeigt werden, indem man auf dem **Kategorie** Symbol im Menüband klickt und **Falsche Alarme zeigen** wählt.

Hinweis: Es kann ein Bild der Begriff-Cloud gespeichert werden. Klicken Sie in der Begriff-Cloud rechts und wählen Sie **Speichern als**.

Anliegen

Ein Schüler/In, der sich gefährdet fühlt, kann einer Person in der Schule, der er vertraut, ein Anliegen melden, und zwar über die DNA Agent Komponente, die auf den Schulgeräten installiert ist, oder über einen Weblink. Nachdem ein Anliegen gemeldet und das entsprechende Personalmitglied benachrichtigt worden ist, kann das Anliegen nachverfolgt und ein laufendes Auditprotokoll aller daraus resultierenden nachfolgenden Aktivitäten geführt werden.

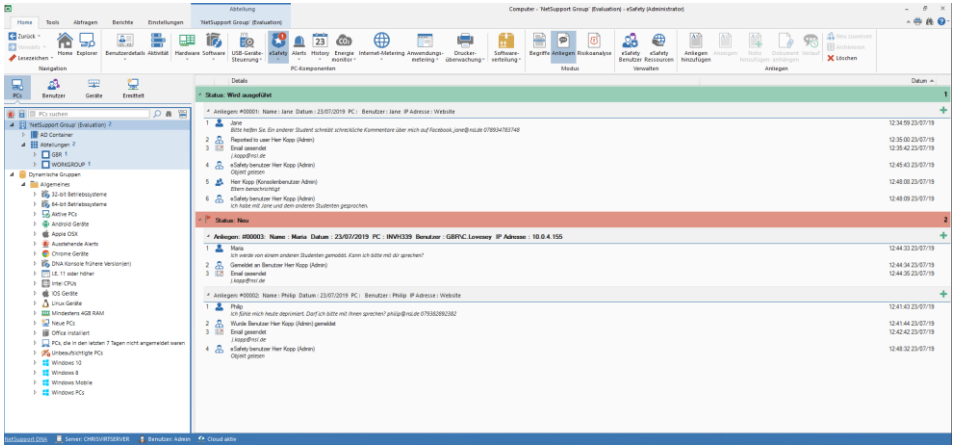
Hinweise:

- In der Standardeinstellung ist Ein Anliegen melden deaktiviert. Sie können die Funktion in DNA Konfiguration - Anliegen melden Einstellungen aktivieren.
- Schüler können als gefährdet markiert werden, so dass sie von eSafety Benutzern leicht identifiziert und unterstützt werden können. Sie können Schüler bei der Bearbeitung der Benutzerdetails als gefährdet markieren. Sie werden dann in der Benutzer-Strukturansicht in der entsprechenden dynamischen Gruppe angezeigt.

1. Klicken Sie auf dem **eSafety** Symbol im Menüband.

   Hinweis: Wenn die Komponentensymbole ausgeblendet sind, klicken Sie auf die Registerkarte „Home".

2. Wählen Sie das **Anliegen** Symbol im Menüband.



Bevor Schüler ein Anliegen melden können, müssen Kontakte definiert werden, aus denen die Schüler wählen können, an wen das Anliegen gesandt werden soll. Klicken Sie auf **eSafety Benutzer** im Verwalten-Abschnitt des Menübands.

Es kann vorkommen, dass Schüler einem Lehrer ein Anliegen direkt und verbal melden. In diesen Fällen kann der Lehrer ein Anliegen von der DNA Konsole aus hinzufügen, so dass es zusammen mit den anderen Anliegen nachverfolgt werden kann. Klicken Sie auf **Anliegen hinzufügen** im Menüband, geben Sie die vom Schüler erhaltenen Informationen ein und weisen Sie das Anliegen dem entsprechenden eSafety Kontakt zu.

Wenn ein Schüler ein Anliegen meldet, haben Sie die Möglichkeit, Links zu eSafety Ressourcen (Websites und Helplines) anzugeben, die den Schülern alternative Unterstützungsmechanismen bieten. Um diese anzuzeigen, müssen Sie die **eSafety Ressourcen anzeigen** Option in DNA Konfiguration – Anliegen melden Einstellungen aktivieren. Um Ihre Region zu ändern, etwas hinzuzufügen oder die Liste der Unterstützungs-Websites zu bearbeiten, klicken Sie auf **eSafety Ressourcen** im Verwalten Abschnitt des Menübands.

Sobald ein Schüler ein Anliegen gemeldet hat, erscheint ein Benachrichtigung Symbol oben im **eSafety** Symbol, und das neue Anliegen wird im Informationsfenster angezeigt. Das Personalmitglied, dem das Anliegen gemeldet wurde, erhält ein Email, in dem es benachrichtigt wird, dass ein Anliegen gemeldet worden ist, und in dem es aufgefordert wird, sich an der NetSupport DNA Konsole anzumelden, um es zu anzuzeigen.

Hinweise:

- Um Benachrichtigungen per Email zu senden, müssen Sie die Emaileinstellungen in den NetSupport Emaileinstellungen konfiguriert und eine Emailadresse für das Personalmitglied im eSafety Benutzerdialog definiert haben.
- Im Begriffsüberwachung-Informationsfenster erscheint eine Kopfzeile, die anzeigt, wenn neue Anliegen gemeldet worden sind; klicken Sie auf **Anzeigen**, um in den Anliegen Modus zu gehen.

Der Zugriff auf die Anzeige aktueller Anliegen ist ausschließlich auf eSafetyrollen beschränkt. Ein Konsolenbenutzer kann die Anliegen nur dann anzeigen, wenn Sie ihn/sie mit einem eSafety Kontakt verknüpft haben.

Anliegen werden nach Status angezeigt (neu, wird bearbeitet, geschlossen oder archiviert).

Die Kopfzeile jedes Anliegens wird den Benutzer/Schüler und die PC-Details enthalten, soweit diese bekannt sind. Wenn ein Anliegen über einen DNA Agent gemeldet wurde, wird die **IP-Adresse** des benutzten Geräts angegeben. Andernfalls wird die **Website** gezeigt, wenn der Schüler das Anliegen über Ihren benutzerdefinierten Weblink gemeldet hat.

Wenn einem Anliegen ein Screenshot angehängt ist, erscheint das Bild einer Kamera daneben. Wenn Sie darauf klicken, wird das Bild gezeigt. Von hier aus können Sie einen Verlauf davon, wer die Screenshots angesehen hat, ausdrucken, speichern, emailen und anzeigen. Um ein individuelles Anliegen anzuzeigen, wählen Sie das betreffende Anliegen und klicken auf **Anzeigen**.

Es können Notizen zu einem Anliegen hinzugefügt werden, um anzugeben, welche Fortschritte gemacht worden sind. Diese werden in chronologischer Reihenfolge gezeigt. Jede Notiz hat ein Bild, um ihren Typ anzuzeigen. Um eine Notiz hinzuzufügen, wählen Sie das geforderte Anliegen und klicken Sie dann auf **Notiz hinzufügen** oder auf .

Dokumente mit Informationen, die für das Anliegen relevant sind, können hinzugefügt werden. Wählen Sie das geforderte Anliegen und klicken Sie dann auf **Dokument anhängen**. Wählen Sie eine Datei und klicken Sie dann auf **Öffnen**. Die Datei wird nun zum Anliegen hinzugefügt. Um ein Dokument anzuzeigen, das einem Anliegen angehängt worden ist, klicken Sie auf .

Hinweis: Schüler können ein Dokument anhängen, wenn sie ein Anliegen melden.

Wenn Anliegen nicht innerhalb einer vordefinierten Zeit bearbeitet werden, wird ein Erinnerungsemail gesendet. Erinnerungen können in der DNA Konfiguration – Anliegen melden Einstellungen konfiguriert werden.

Der Verlauf aller von einem Schüler gemeldeten Anliegen kann angezeigt werden. Wählen Sie ein Anliegen des Schülers, der gezeigt werden soll, und klicken Sie auf **Verlauf**. Daraufhin erscheint der Anliegenverlauf-Dialog, der es Ihnen ermöglicht, alle von dem Schüler gemeldeten Anliegen im Kalenderformat nach Tag, Woche oder Monat anzuzeigen. eSafety Benutzer können nur die Anliegen anzeigen, die ihnen

zugewiesen worden sind, außer wenn sie befugt sind, alle Anliegen zu sehen.

Manchmal kann es erforderlich sein, ein Anliegen einem anderen eSafety Benutzer neu zuzuweisen. Wählen Sie das Anliegen, das neu zugewiesen werden soll, und klicken Sie auf **Neu zuweisen**. Nun erscheint der Anliegen neu zuweisen Dialog, der eine Liste der zur Verfügung stehenden eSafety Benutzer zeigt. Wählen Sie den gewünschten Benutzer und klicken Sie auf **Neu zuweisen**. Sowohl der gegenwärtige als auch der neue Benutzer werden per Email über diese Änderung benachrichtigt.

Hinweis: Anliegen können nur von eSafety Administratoren neu zugewiesen werden.

Nachdem die Anliegen bearbeitet worden sind, können sie archiviert werden. Archivierte Anliegen sind weiterhin für Prüfungszwecke sichtbar, aber es kann nichts mehr zu ihnen hinzugefügt werden.

Es können Situationen auftreten, in denen Anliegen gelöscht werden müssen, beispielsweise wenn sie versehentlich gemeldet worden sind, oder wenn sie mehr als ein gewisses Alter haben. Wählen Sie das geforderte Anliegen und klicken Sie auf **Löschen**. Sie können dieses Anliegen, alle Anliegen für einen gewählten Benutzer, alle vor einem bestimmten Datum gemeldeten Anliegen oder alle archivierten Anliegen löschen.

Hinweis: Anliegen können erst gelöscht werden, wenn dies von einem zweiten eSafety Administrator autorisiert worden ist. Sie werden aufgefordert, einen eSafety Administrator in einer Liste zu wählen, der dann sein Passwort eingeben muss. Wenn es bei Ihnen nur einen eSafety Administrator gibt, müssen Sie einen weiteren erstellen, um Anliegen löschen zu können.

eSafety Ressourcen

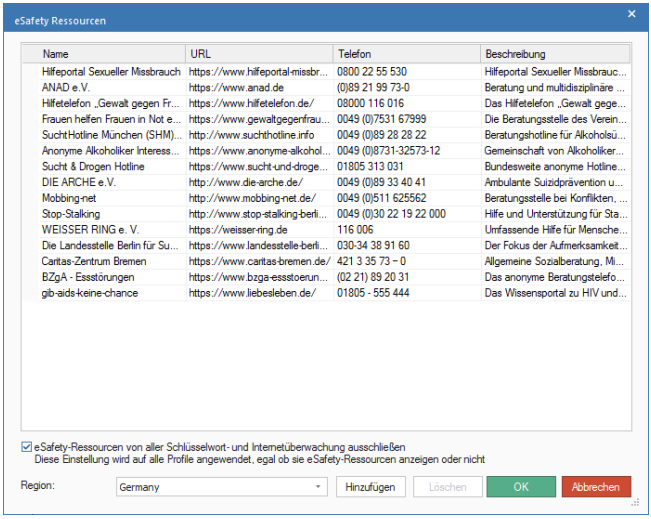
Wenn Schüler ein Anliegen melden, können ihnen Links zu eSafety Ressourcen zur Verfügung gestellt werden, und zwar sowohl vom NetSupport DNA Agent Menü aus als auch von einem Desktop-Symbol aus. Dieser Link bietet den Schülern Details von Unterstützungs-Websites und Helplines, die sie benutzen können, wenn sie lieber mit jemandem außerhalb der Schule sprechen möchten.

Hinweise:

- Diese Funktion kann in den Anliegen melden Einstellungen aktiviert werden; wählen Sie **eSafety-Ressourcen zeigen**.
- Auf den Schüler Desktops kann ein eSafety Ressourcen-Symbol angezeigt werden. Wählen Sie **Verknüpfungen auf Benutzer-Desktops erstellen** in den Anliegen-melden-Einstellungen. Dieses Symbol wird auch dann zur Verfügung stehen, wenn NetSupport DNA Agent nicht ausgeführt wird.

Um Ressourcen hinzuzufügen oder zu bearbeiten

1. Klicken Sie auf dem **eSafety** Symbol im Menüband und wählen Sie das **Anliegen** Symbol.
2. Wählen Sie das **eSafety** Symbol-Dropdownmenü und dann {eSafety Ressourcen}.
   Oder
   Klicken Sie auf dem **eSafety Ressourcen** Symbol im Menüband.
3. Nun erscheint der eSafety Ressourcen-Dialog.



4. Es wird eine Liste von Standardressourcen bereitgestellt. Wählen Sie die Region in der Dropdownliste, um diese für Ihr Land anzuzeigen.
5. Sie können diese URLs von der Berichterstattung in Internet-Metering ausschließen oder alles, was in sie eingetastet wird, von den Übereinstimmungen in der Begriffsüberwachung ausschließen. Klicken Sie auf **eSafety-Ressourcen von aller Schlüsselwort- und Internetüberwachung ausschließen**.

Hinweis: Dies ist eine globale Einstellung, die auf alle Profile angewendet werden wird, auch wenn eSafety-Ressourcen deaktiviert sind.

6. Um ein neues Objekt hinzuzufügen, klicken Sie auf **Hinzufügen** und geben die erforderlichen Details ein.
7. Um ein vorhandenes Objekt zu bearbeiten, klicken Sie auf dem geforderten Feld und überschreiben die Informationen.
8. Um ein Objekt zu löschen, wählen Sie das geforderte Objekt und klicken dann auf **Löschen**.
9. Klicken Sie auf **OK**.

Ein Anliegen melden

Schüleranliegen können entweder über den auf Schulgeräten installierten DNA Agent oder über einen Weblink direkt einem ausgewählten Personalmitglied gemeldet werden.

Hinweise:

- In der Standardeinstellung ist Ein Anliegen melden deaktiviert. Sie können die Funktion in DNA Konfiguration - Anliegen melden Einstellungen aktivieren und auch den Text anpassen, der im Ein Anliegen melden Dialog erscheint.
- Anliegen können auch von der NetSupport DNA Konsole aus gemeldet werden. Dies kann nützlich sein, wenn ein Schüler/In einem Lehrer/In verbal ein Anliegen meldet; der Lehrer kann das Anliegen dann manuell protokollieren und dem entsprechenden Personalmitglied zuweisen, so dass es nachverfolgt werden kann.

Ein Anliegen über den DNA Agent melden

1. Klicken Sie das NetSupport DNA Symbol in der Symbolleiste rechts an und wählen Sie {Ein Anliegen melden}.

   Oder

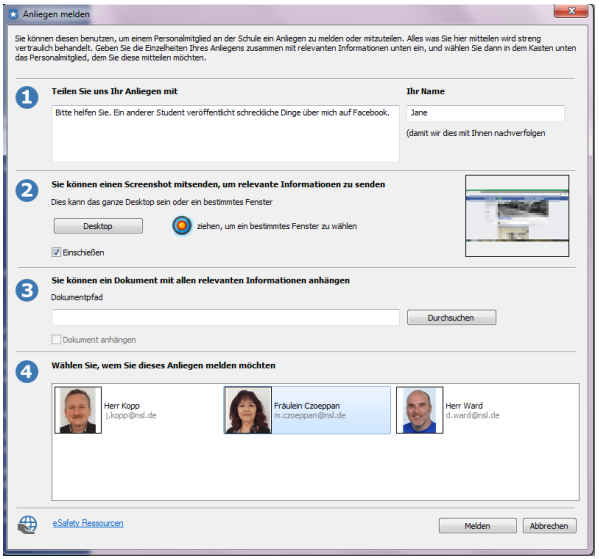
   Klicken Sie auf dem  Symbol in der Symbolleiste.

   Oder

   Klicken Sie auf dem Desktop-Symbol **Ein Anliegen melden**.

   Hinweis: Um das Desktop-Symbol anzuzeigen, müssen Sie die Option **Verknüpfung auf Benutzer-Desktop erstellen** in DNA Konfiguration - Anliegen-melden-Einstellungen aktivieren.

2. Nun erscheint der Ein Anliegen melden Dialog.



3. Von hier aus kann der Schüler alle Informationen über das Anliegen zusammen mit seinem Namen eingeben.

Hinweise:

- Die Texteingabe der Schüler ist auf 512 Zeichen begrenzt.
- Der gegenwärtig angemeldete Benutzername wird gemeldet, wenn ein Anliegen gemeldet wird.

4. Klicken Sie auf **Desktop,** um einen Screenshot des ganzen Desktop aufzunehmen, oder, um einen Screenshot eines einzelnen Fensters aufzunehmen, ziehen Sie das Symbol auf das geforderte Fenster.
5. Dem Anliegen kann ein Dokument angehängt werden, so dass zusätzliche Informationen aufgenommen werden können. Klicken Sie auf **Durchsuchen,** um die gewünschte Datei auszuwählen, und dann auf **Öffnen**.
6. Es erscheint eine Liste der Personalmitglieder, denen das Anliegen gemeldet werden kann, und der Schüler/In kann wählen, an wen es gesendet werden soll.
7. Den Schülern kann ein Link zu eSafety Ressourcen zur Verfügung gestellt werden, die ihnen alternative Unterstützungsmechanismen bieten. Diese Option muss in den DNA Konfiguration – Anliegen melden Einstellungen aktiviert werden.
8. Klicken Sie auf **Melden**.
9. Das Anliegen wird nun dem entsprechenden Personalmitglied gemeldet.

Ein Anliegen über eine Website melden

Während des Schultags steht den Schülern die Anliegen melden Option über die DNA Agent Komponente zur Verfügung. Für zusätzliche Flexibilität können Sie den Schülern die selbe Funktion auch außerhalb der Schulzeiten über eine benutzerdefinierte Anliegen melden Schaltfläche und ein Formular bieten, das Sie erstellen und in einer Website Ihrer Wahl, beispielsweise Ihrer Schulwebsite, einbetten können.

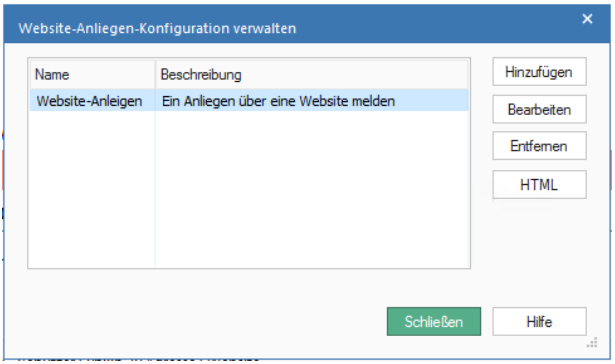
Ein praktischer Assistent in der DNA Konsole hilft Ihnen, einen **HTML-Ausschnitt** zu erstellen, der den erforderlichen Code enthält.

Hinweise:

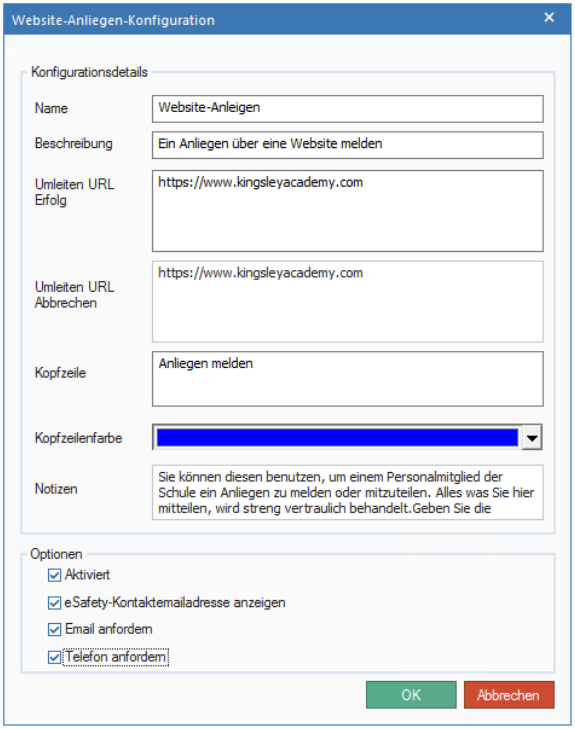
- Um diese Methode zur Meldung von Anliegen zu benutzen, muss die **DNA Cloud Konsole** aktiviert sein.
- Vergewissern Sie sich, dass die entsprechenden eSafety-Benutzerkonten dafür konfiguriert sind, Über Website gemeldete Anliegen zu empfangen.

Verwaltung von Website-Anliegen

1. Wählen Sie die **Einstellungen**-Registerkarte in der DNA Konsole (der Windows Hauptkonsole).
2. Klicken Sie auf dem **Website-Anliegen verwalten** Symbol. Nun erscheint der **Website-Anliegen-Konfiguration** Dialog.



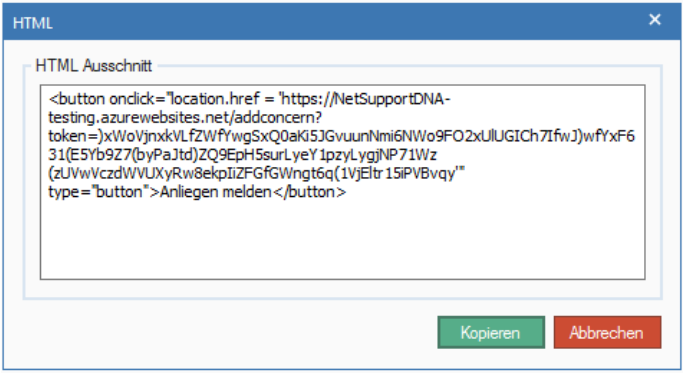
3. Es steht ein nützlicher Assistent zur Verfügung, der Ihnen hilft, die erforderlichen Elemente für eine Anliegen melden Schaltfläche und ein Formular zu bauen, um widerum den HTML-Ausschnitt zu kompilieren, der an die von Ihnen gewählte Website kopiert werden muss. Klicken Sie auf **Hinzufügen**. Nun erscheint der **Website-Anliegen-Konfigurationsassistent**.



- Geben Sie einen geeigneten **Namen und eine Beschreibung** ein, um jede Konfiguration (HTML-Ausschnitt), die Sie erstellen, zu identifizieren. Dies sind die Details, die im **Website-Anliegen-Konfiguration** verwalten Dialog erscheinen.
- Geben Sie eine **Umleiten-URL** an, die benutzt werden soll, wenn ein Schüler erfolgreich ein Anliegen gemeldet hat. Vergewissern Sie sich, dass es die vollständige URL ist, einschließlich http(s)//.
- Geben Sie eine **Umleiten-URL** an, die benutzt werden soll, wenn der Schüler die Anforderung abbricht. Vergewissern Sie sich, dass es die vollständige URL ist, einschließlich http(s)//.
- Geben Sie einen **Kopfzeilennachricht** ein, die oben auf der Webseite erscheinen soll.
- Wählen Sie eine **Kopfzeilenfarbe**.
- Es ist eine **Standardnotiz** enthalten, die auf der Webseite erscheinen wird, aber Sie können auf Wunsch auch Ihre eigene benutzerdefinierte Nachricht/Anweisung eingeben.

- **Optionen:**
  - In der Standardeinstellung ist das Anliegen melden Formular stets aktiviert. Wenn es deaktiviert wird, erscheint eine Nachricht, wenn Schüler versuchen, auf das Formular zuzugreifen.
  - Das Formular zeigt die Mitglieder des eSafety-Personals **(eSafety-Kontakte)**, an die Schüler ihre Anliegen senden können. Sie können wählen, ob die Emailadresse der Person auf dem Formular erscheinen soll.
  - Sie können auf dem Formular ein Feld hinzufügen, in dem der Schüler/In aufgefordert wird, seine Emailadresse einzugeben.
  - Sie können auch um die Telefonnummer des Schülers bitten.

4. Klicken Sie auf **OK**, wenn Sie mit dem Assistenten fertig sind. Sie werden dann zum **Website-Anliegen verwalten Konfiguration** Dialog zurückgeleitet.
5. Klicken Sie auf **HTML**, um den erstellten Code zu sehen. Sie können die Textbeschreibung, die auf der **Anliegen melden** Schaltfläche erscheinen wird, bei Bedarf bearbeiten.

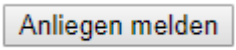


6. Klicken Sie auf **Kopieren**, um den HTML-Ausschnitt zu wählen, entscheiden Sie, auf welcher Seite Ihrer Website die Anliegen melden Schaltfläche erscheinen soll, und betten Sie die HTML im Quellcode für die geforderte Webseite ein. Bei Bedarf können Sie den Code an diesem Punkt noch weiter an Ihre individuellen Erfordernisse anpassen, beispielsweise indem Sie den Text bearbeiten, der auf der Anliegen melden Schaltfläche erscheinen soll.

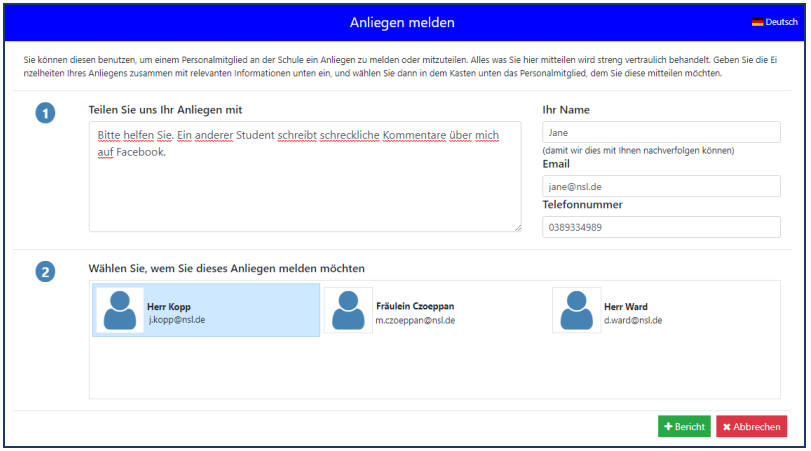
Überprüfung des Formulars

Wenn Sie das Formular überprüfen möchten, bevor Sie es zu Ihrer Website hinzufügen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie **Notepad** oder ein ähnliches Programm und fügen Sie die kopierte HTML ein. Speichern Sie die Datei unter einem geeigneten Namen und vergessen Sie nicht .HTML als Erweiterung hinzuzufügen.
2. Führen Sie die HTML Datei aus, und Sie werden nun als Erstes die **Anliegen melden** Schaltfläche sehen.



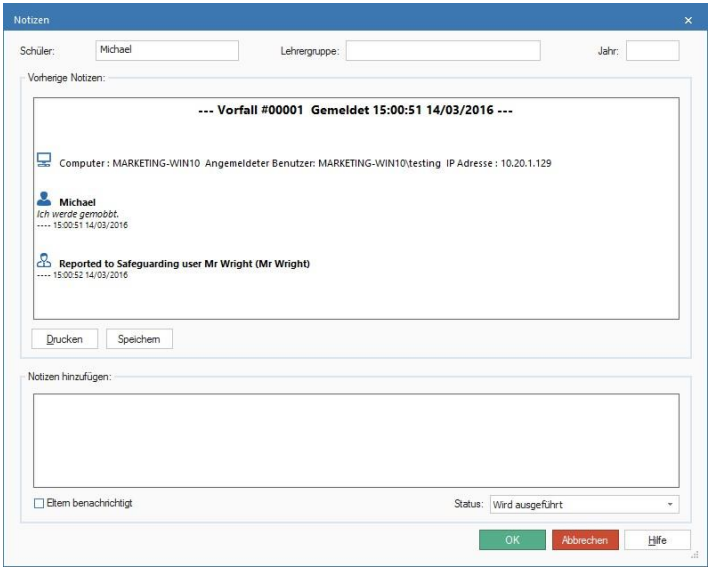
3. Klicken Sie auf der Schaltfläche. Nun wird sich das Hauptformular öffnen. Füllen Sie das Formular aus, wählen Sie einen eSafety-Benutzer und and klicken Sie auf **Melden**. Melden Sie sich an Ihrer NetSupport DNA Konsole an; Sie müssten nun das gemeldete Anliegen in der eSafety Komponente anzeigen können. Vergewissern Sie sich, dass die Umleiten-URL ordnungsgemäß funktioniert, und dass der benannte eSafety-Benutzer eine **Neues Anliegen zugewiesen** Email erhalten hat.



Hinweis: Fotos, die Ihren eSafety-Benutzern zugewiesen sind, können gegenwärtig nicht gezeigt werden.

Notizen zu einem Anliegen hinzufügen

Dieser Dialog wird benutzt, um Notizen zu einem Anliegen hinzuzufügen.

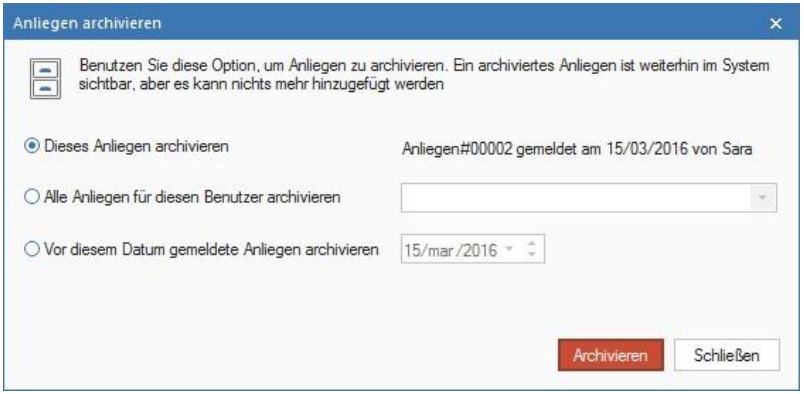


1. Es wird ein voller Verlauf der Notizen angezeigt, die sich auf das Anliegen beziehen. Dieser kann ausgedruckt oder als .RTF gespeichert werden.
2. Der Name des Schülers, die Lehrergruppe und das Jahr des Schülers, auf den sich das Anliegen bezieht, können bei Bedarf hinzugefügt werden.
3. Geben Sie Ihre Notiz im **Notizen hinzufügen** Kasten ein.
4. Der Status des Anliegens kann geändert werden, indem man die entsprechende Option in der Dropdownliste wählt.
5. Wenn die Eltern des Schülers über die Angelegenheit unterrichtet worden sind, können Sie die Option **Eltern benachrichtigt** wählen, um dies zu melden.
6. Klicken Sie auf **OK**.
7. Ihre Notiz wird nun zum Anliegen hinzugefügt.

Anliegen archivieren

Nachdem die Anliegen bearbeitet worden sind, können sie archiviert werden. Archivierte Anliegen sind weiterhin für Prüfungszwecke sichtbar, aber es kann nichts mehr zu ihnen hinzugefügt werden.

1. Wählen Sie das zu archivierende Anliegen und klicken Sie auf **Archivieren**.
2. Nun erscheint der Anliegen archivieren Dialog.



3. Sie können nur dieses Anliegen, alle Anliegen für einen Benutzer (wählen Sie den Benutzer im der Dropdownliste) oder alle Anliegen vor einem bestimmten Datum archivieren.
4. Klicken Sie auf **Archivieren**.

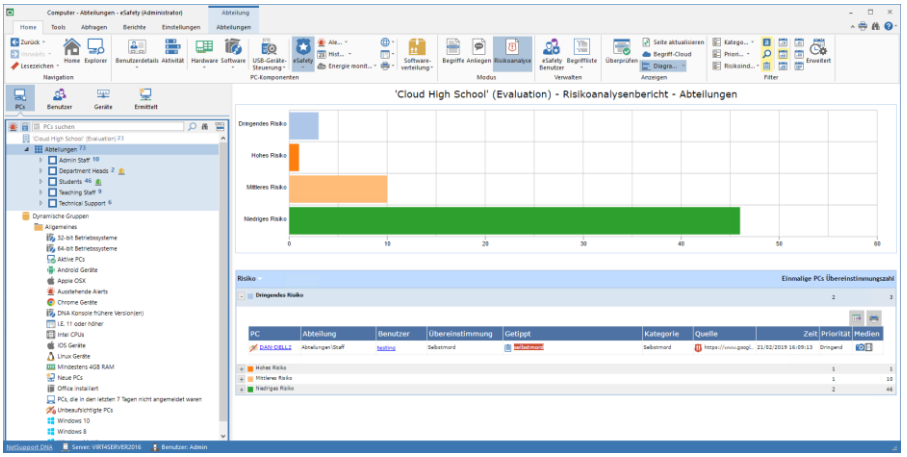
Risikoanalyse

NetSupport DNA führt einen auf Zusammenhangsinformationen basierenden Risikoindex aus, der automatisch Ereignisse mit hohem Risiko und gefährdete Schüler hervorhebt. Es bewertet den Zusammenhang und den Verlauf der Aktivitäten eines Schülers – von den benutzten Geräten, der Tageszeit und den besuchten Websites (einschließlich von eventuell zuvor ausgelösten Alerts) – und erstellt aus diesen Informationen einen numerischen Risikoindexwert. Ein hoher Risikoindex würde sich ergeben, wenn ein Schüler wiederholt ein eSafety-Thema (z.B. Selbstmord) in der Freizeit recherchiert hat und in einer nicht-überwachten Situation, wie beispielsweise der Bibliothek. Ein niedrigerer Indexwert könnte sich ergeben, wenn ein Schüler während der Unterrichtszeiten ein Schlüsselwort mit niedrigem Risiko in einer lokalen Anwendung sucht, die eventuell für Unterrichtsthemen benutzt worden ist.

1. Klicken Sie auf dem **eSafety** Symbol im Menüband.

   Hinweis: Wenn die Komponentensymbole ausgeblendet sind, klicken Sie auf die Registerkarte „Home".

2. Wählen Sie das **Risikoanalyse** Symbol im Menüband.



Wählen Sie in der hierarchischen Strukturansicht die Ebene, auf der Sie die Meteringdaten betrachten möchten: Unternehmen, Abteilung, AD Container, dynamische Gruppe oder individueller Agent.

Im Informationsfenster ist ein Breakdown für jedes gewählte Objekt in Grafik- und Listenformat angezeigt. Um den Graph in einem anderen Format anzuzeigen, klicken Sie auf dem **Diagramm**-Symbol-Dropdownpfeil in der Menüleiste und wählen das entsprechende Format.

Um die aktive Ansicht auszudrucken, klicken Sie auf dem  Symbol oben auf der Konsole.

Hinweis: Durch Anklicken des **Chart**-Symbols im Ribbon wird die Grafik ein-/ausgeblendet.

Sie können die Daten für eine spezifische Zeitspanne betrachten. Um zwischen verschiedenen Zeitperioden umzuschalten, klicken Sie auf dem entsprechenden Symbol im Filter-Abschnitt des Menübands. Wenn Sie auf **Erweitert** klicken, können Sie einen benutzerdefinierten Datums-/Zeitfilter anwenden.

Die Daten werden nach der Gefahr angezeigt, die der ausgelöste Begriff darstellt (mittlere, hohe, und dringende). Aufgelistete Beschreibungen können erweitert werden, um für jedes Element einen Strukturplan des individuellen Agents anzuzeigen.

Eine nützliche Methode, auf spezifische Schlüsselwörter- und begriffe abzuzielen (und die angezeigte Datenmenge zu beschränken) besteht darin, bestimmte Kategorien, Prioritätsstufen, Risiken und Quelltexttypen anzuzeigen. Um zu wählen, welche Kategorien angezeigt werden sollen, klicken Sie auf dem **Kategorien** Symbol, wählen die gewünschte Gruppe, die angezeigt werden soll, und klicken dann auf **OK**. Um die Daten für einen Prioritätsgrad auszublenden, klicken Sie auf dem **Priorität** Symbol, wird die Auswahl des relevanten Kontrollkästchens aufgehoben und klicken dann auf **OK**. Um Daten eines Risikoindextyps auszublenden, klicken Sie auf dem **Risikoindex** Symbol, eben Sie die Wahl des entsprechenden Kästchens auf und klicken Sie auf **OK**. Um Daten für eine Quellentextart auszublenden, klicken Sie auf der entsprechenden Quellenart, um die gelbe Schattierung zu löschen. Das Informationsfenster zeigt dann nur die Daten für die gewählten Kategorien, Prioritätsstufen, Risiken und Quellentexttypen.

Um einen dazugehörigen Screenshot, eine Bildschirmaufzeichnung oder ein Webcam-Bild anzuzeigen , klicken Sie auf dem entsprechenden Mediensymbol neben dem Eintrag des individuellen Agents in der detaillierten Listenansicht.

Für jeden ausgelösten Begriff können die vollen Details angezeigt werden, klicken Sie auf **Überprüfen**. Von hier aus können Sie sehen, wer den Begriff ausgelöst hat, zusammen mit den Faktoren, aus denen sich der Risikoindexwert ergibt, so dass Sie sehen können, ob weitere Maßnahmen erforderlich sind. Sie können drucken, speichern, emailen, an PDF exportieren, und, wenn ein Screenshot, eine Aufzeichnung oder ein Webcam-Bild angehängt ist, einen Verlauf dafür sehen, wer diese angezeigt hat.

Es können Listen Gefährdender Anwendungen und URLs erstellt werden, die Anwendungen und Websites enthalten, die als größere Gefahr für Schüler betrachtet werden. Es können mehrere Listen erstellt werden, so dass Sie verschiedenen Profilen verschiedene Listen zuordnen können.

Hinweis: Alle Begriffe, die außerhalb der Unterrichtsstunden ausgelöst werden, werden als höheres Risiko klassifiziert. Sie können die Unterrichtsstunden im DNA Konfigurationsdialog für Ihre Schule passend ändern. Siehe Konsolenanpassungen – Allgemein für weitere Informationen.

Unbeaufsichtigte PCs definieren
PCs in unbeaufsichtigten Umgebungen, wie beispielsweise der Bibliothek, können als höheres Risiko eingestuft werden als solche in Klassenzimmern. Sie können vorgeben, welche PCs in Ihrem Netzwerk unbeaufsichtigt sind, und alle auf diesen ausgelösten Begriffe werden einen höheren Risikoindex erhalten.

1. Wählen Sie einen Agent, eine Abteilung oder eine dynamische Gruppe in der PC-Strukturansicht.
2. Klicken Sie mit der rechten Maustaste und wählen Sie **PC-Beaufsichtigung**.
3. Klicken Sie auf **Unbeaufsichtigt** und dann auf **OK**.
4. Die PCs werden in der Strukturansicht in der dynamischen Gruppe Unbeaufsichtigte PCs angezeigt.

Abfragen
Wählen Sie zur Anzeige des Abfragefensters die Registerkarte „Abfragen".

Mit dem Abfragetool von DNA können Sie Datenbankeinträge abrufen, die bestimmte Kriterien erfüllen. Abfragen zu der Komponente, die gerade betrachtet wird, sind aufgelistet, was ein schnelles Abrufen der Ergebnisse ermöglicht.

Klicken Sie in der Menüleiste auf dem **Abfrage hinzufügen** Symbol, um eine neue Abfrage zu erstellen, oder klicken Sie auf dem **Abfrage bearbeiten** Symbol in der Menüleiste, um ein in der Liste vorhandenes Objekt zu bearbeiten.

Berichte
Wählen Sie zur Anzeige des Berichtfensters die Registerkarte „Berichte".

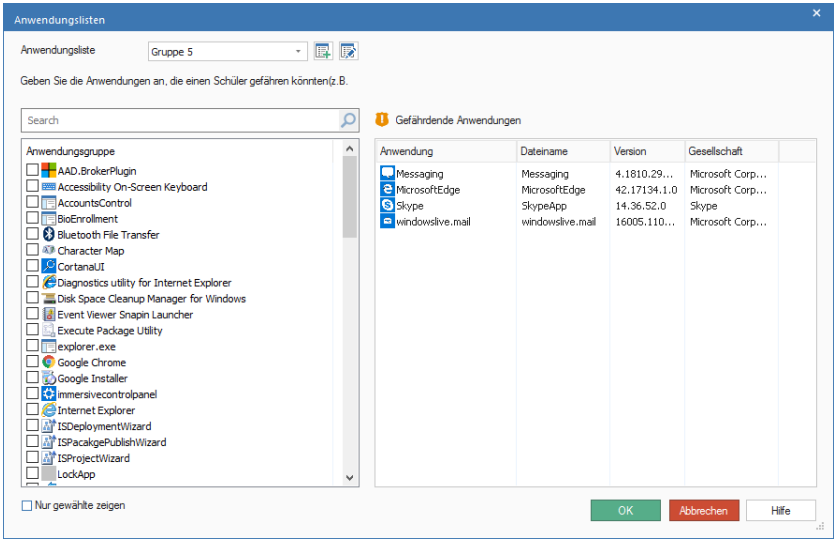
Jeder Komponente ist eine Reihe von vordefinierten Managementberichten, die vom Crystal Reports-Modul gespeist werden, beigefügt. Wählen Sie den geforderten Bericht in der Dropdown-Liste. Die Ergebnisse erscheinen im Informationsfenster. Sie lassen sich ggf. exportieren.

Gefährdende-Anwendung-Listen

Es können Anwendungslisten erstellt werden, die es Ihnen ermöglichen, Anwendungen zu definieren, die Schüler höheren Gefahren aussetzen können. Beispielsweise können Übereinstimmungen in Skype als eine größere Gefahr betrachtet werden als solche, die in Microsoft Word ausgelöst werden. Es können mehrere Listen erstellt werden, so dass Sie verschiedenen Profilen verschiedene
Listen zuordnen können.

Erstellung und Anwendung einer Anwendungsliste

1. Wählen Sie in der Einstellungen-Registerkarte **Existierende Profile verwalten**.
2. Wählen Sie das geforderte Profil in der Liste und klicken Sie auf **Einstellungen**.
3. Wählen Sie **Risikoanalyse**.
4. Nun werden die Risikoanalyseneinstellungen gezeigt.
5. Klicken Sie auf **Anwendungslisten**.
6. Der Anwendungslisten-Dialog erscheint.



7. Um eine neue Anwendungsliste zu erstellen, klicken Sie auf . Geben Sie einen Namen und, falls gefordert, eine Beschreibung für die Liste ein. Sie können eine vorhandene Liste kopieren, indem Sie sie in der 'Kopieren von' Dropdownliste wählen. Klicken Sie auf **OK**. Um eine vorhandene Liste zu bearbeiten, klicken Sie auf .

8. Nun erscheint eine Liste von Anwendungen. Wählen Sie die Anwendungen, die in die Anwendungsliste aufgenommen werden sollen.
9. Klicken Sie auf **OK**.
10. Wählen Sie die geforderte Anwendungsliste im Anwendungslisten-Dropdownmenü.
11. Klicken Sie auf **Speichern**, um die Änderungen anzuwenden.

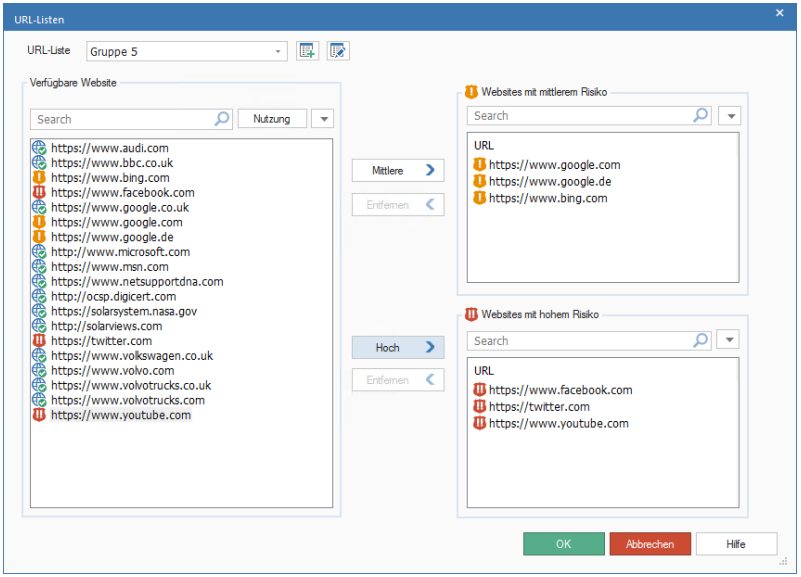
Gefährdende-URL-Listen

Es können Listen gefährdender URL erstellt werden, die es Ihnen ermöglichen, Websites zu definieren, die ein mittleres oder hohes Risiko für Schüler darstellen. Es können mehrere Listen erstellt werden, so dass Sie verschiedenen Profilen verschiedene Listen zuordnen können.

Hinweis: Es können auch URL-Listen für Internetbeschränkungen mit genehmigten oder beschränkten Websites erstellt werden, die Ihnen die Kontrolle darüber ermöglichen, welche Websites von den Agents besucht werden.

Erstellung und Anwendung einer URL-Liste

1. Wählen Sie in der Einstellungen-Registerkarte **Existierende Profile verwalten**.
2. Wählen Sie das geforderte Profil in der Liste und klicken Sie auf **Einstellungen**.
3. Wählen Sie **Risikoanalyse**.
4. Nun werden die Risikoanalyseneinstellungen gezeigt.
5. Klicken Sie auf **URL-Listen**.
6. Der URL-Listen Dialog erscheint. Websites, die bereits von Agents besucht worden sind, werden automatisch in der Verfügbare Websites Liste aufgeführt, und die Standard-URL-Liste wird angezeigt.



7. Um eine neue Website-Liste zu erstellen, klicken Sie auf . Nun erscheint der URL-Liste Dialog. Geben Sie einen Namen und, falls gefordert, eine Beschreibung für die Liste ein. Sie können eine vorhandene Liste kopieren, indem Sie sie in der 'Kopieren von' Dropdownliste wählen.

   Hinweis: Es kann eine Liste von Internetbeschränkungen kopiert werden. URLs in der Liste genehmigter Websites werden zu der Liste von Websites mit mittlerem Risiko hinzugefügt, und URLs in der Liste mit beschränkten Websites werden zu der Liste von Websites mit hohem Risiko hinzugefügt.

   Klicken Sie auf **OK**. Um eine vorhandene Liste zu bearbeiten, klicken Sie auf .
8. Um eine vorhandene URL zu der Liste der Websites mit mittlerem oder hohem Risiko hinzuzufügen, wählen Sie die URL in der Liste verfügbarer Websites und klicken dann auf **Mittleres** oder **Hohes**, oder Sie können die URL mit Drag & Drop auf die gewünschte Liste ziehen.
9. Um eine neue Website zur Liste hinzuzufügen, klicken Sie auf in der Liste von Websites mit mittlerem bzw. hohem Risiko, wählen Sie **URL hinzufügen**, und geben Sie die geforderten Details ein. Die neue Website erscheint nun auf der entsprechenden Website-Liste und wird außerdem automatisch zur Liste verfügbarer Websites hinzugefügt. Zum Löschen von URLs klicken Sie auf wählen **URL löschen**.
10. Wenn die geforderten URLs hinzugefügt worden sind, klicken Sie auf **OK**.
11. Wählen Sie die geforderte URL Liste im URL Listen Dropdownmenü.
12. Klicken Sie auf **Speichern**, um die Änderungen anzuwenden.

Wählen Sie zum Betrachten vollständiger Daten zur Websitenutzung die gewünschte Website in der Liste „Verfügbare Sites" und klicken Sie auf die **Nutzungsschaltfläche**. Das Dialogfeld „Websitenutzung" wird eingeblendet. Hier sehen Sie, welche Benutzer auf die Website zugegriffen und wie oft sie diese besucht haben. Wenn Sie auf einen Benutzer klicken, erscheint eine vollständige Aufstellung der Zeiten und Dauer des Zugriffs auf die Website durch den betreffenden Benutzer.

Alerting

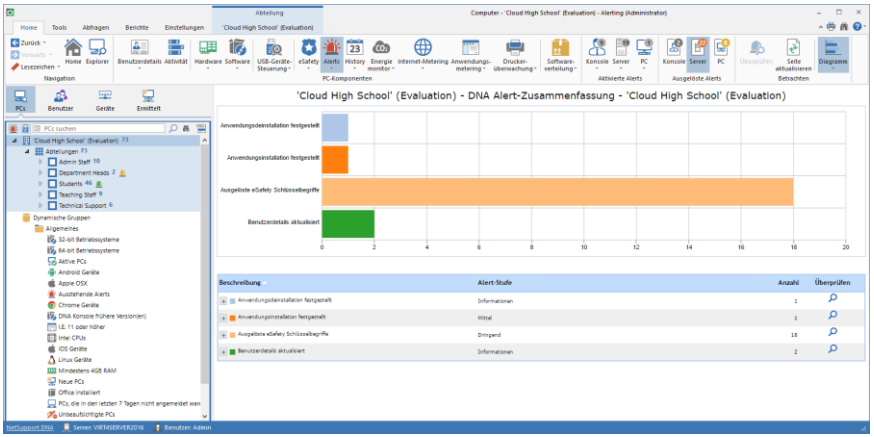
NetSupport DNA bietet ein extrem leistungsstarkes Alerting-Modul, mit dem das System die Operators automatisch benachrichtigen kann, wenn verschiedene Änderungen irgendwo im Unternehmen auftreten. Es gibt drei Arten von Alert: Server, Konsolen- und PC-Alerts. Serveralerts melden Änderungen in den von NetSupport DNA im gesamten Unternehmen gesammelten Daten, einschließlich Alerts für Dinge wie neu hinzugefügte PCs, Änderungen in der Hardware, neu installierte / entfernte Anwendungen etc. Konsolen-Alerts identifizieren Änderungen im Zusammenhang mit der NetSupport DNA Konsole, z.B. wenn eine DNA Lizenzgrenze überschritten wird, wenn ein Bediener hinzugefügt oder gelöscht wird und wenn ein DNA Update installiert wird. PC Alerts melden Echtzeitänderungen oder -zustände, die auf einem spezifischen PC auftreten, wie zum Beispiel: CPU Nutzung über XX% für XX Minuten; freier Speicherplatz der auf unter XX% abfällt; Wegfall eines wichtigen Service (z.B. Antivirus Service oder IIS an einem Server), Druckerspooler-Alerts; Sicherheitsalerts (z.B. gescheiterte Anmeldungsversuche); und viele anderen. Als Teil einer SIEM (Sicherheitsinformationen und Vorfallsmanagement) Strategie, kann das PC-Vorfallprotokoll auch überwacht werden, wobei Alerts für Fehler, Warnungen oder ausgewählte Auditergebnisse ausgelöst werden.

Alert-Benachrichtigungen können an vorgegebene Emailempfänger und/oder aktive Konsolenbenutzer geleitet werden (und zwar pro Alert, so dass die Art des Alerts entscheiden kann, welche Operators zu benachrichtigen sind).

Hinweis: NetSupport DNA bietet auch SNMP Alerts, die Änderungen der SNMP Geräteeigenschaften identifizieren.

1. Klicken Sie auf das Symbol **Alerts** im Ribbon. Das Alert-Fenster wird eingeblendet.

   Hinweis: Wenn die Komponentensymbole ausgeblendet sind, klicken Sie auf die Registerkarte **Home**.



Wählen Sie in der hierarchischen Strukturansicht die Ebene, auf der Sie die angezeigten Daten betrachten möchten: Unternehmen, Abteilung, AD Container, dynamische Grupe oder individueller Agent.

Sie können zwischen PC-, Server- und Konsolen-Alerts umschalten, indem Sie die **Alerts** Symbol-Dropdownliste anklicken und {Anzeigen–Server-Alerts\Konsolen-Alerts\PC-Alerts} wählen, oder indem Sie das entsprechende Symbol im Menübandabschnitt Aktive Alerts anklicken.

Im Informationsfenster ist ein Breakdown für jedes gewählte Objekt in Grafik- und Listenformat angezeigt. Um den Graph in einem anderen Format anzuzeigen, klicken Sie auf dem **Diagramm**-Symbol-Dropdownpfeil in der Menüleiste und wählen das entsprechende Format.

Um die aktive Ansicht auszudrucken, klicken Sie auf dem  Symbol oben auf der Konsole.

Hinweis: Durch Anklicken des Chart-Symbols im Ribbon wird die Grafik ein-/ausgeblendet.

Um Alerts zu konfigurieren und zu erstellen, klicken Sie auf dem **Konsole**/**Server**/**PC** Symbol im Aktivierte Alerts Bereich im Menüband. Sie können sehen, welche Alerts gegenwärtig laufen, indem Sie die Dropdownliste unter dem geforderten Symbol wählen.

Werden ausstehende Alerts für die entsprechenden PCs in der Hauptunternehmenshierarchie-Strukturansicht identifiziert. Wenn Alerts identifiziert worden sind, können Sie die Details im Informationsfenster

anzeigen, indem Sie auf klicken. Wenn Sie wünschen, können Sie das Alert dann schließen, und Sie können Notizen zu PC-Alerts hinzufügen. Wenn ein PC-Alert geschlossen worden ist, haben Sie von der Verlauf-Funktion aus weiterhin Zugriff auf die Details.

Hinweis: Sie können Alerts in der Strukturansicht zeigen / ausblenden, indem Sie auf  klicken.

Es kann eine Aktion zu einem PC-Alert hinzugefügt werden, so dass Sie wählen können, was geschieht, wenn ein Alert ausgelöst wird. Die verfügbaren Optionen sind: Screenshot erfassen (dieser kann dem Email angehängt werden, das gesendet wird, wenn das Alert aktiviert wird), Bildschirm aufnehmen und Anwendung ausführen. Diese werden im DNA Alert Assistenten hinzugefügt. Wenn ein Alert ausgelöst worden ist, können Sie es überprüfen, indem Sie das **PC** Symbol im Ausgelöste Alerts Bereich des Menübands wählen und auf **Überprüfen** klicken. Nun wird ein Überblick des Alerts gezeigt und wer es ausgelöst hat, zusammen mit eventuellen Screenshots und Bildschirmaufzeichnungen. Von hier aus können Sie drucken, speichern, an PDF exportieren und, wenn ein Screenshot oder eine Aufzeichnung angehängt ist, einen Verlauf der Personen sehen, die es angesehen haben.

Abfragen
Wählen Sie zur Anzeige des Abfragefensters die Registerkarte „Abfragen". Mit dem Abfragetool von DNA können Sie Datenbankeinträge abrufen, die bestimmte Kriterien erfüllen. Abfragen zu der Komponente, die gerade betrachtet wird, sind aufgelistet, was ein schnelles Abrufen der Ergebnisse ermöglicht.

Klicken Sie in der Menüleiste auf dem Abfrage hinzufügen Symbol, um eine neue Abfrage zu erstellen, oder klicken Sie auf dem Abfrage bearbeiten Symbol in der Menüleiste, um ein in der Liste vorhandenes Objekt zu bearbeiten.

Berichte
Wählen Sie zur Anzeige des Berichtfensters die Registerkarte „Berichte". Jeder Komponente ist eine Reihe von vordefinierten Managementberichten, die vom Crystal Reports-Modul gespeist werden, beigefügt. Wählen Sie den geforderten Bericht in der Dropdown-Liste. Die Ergebnisse erscheinen im Informationsfenster. Sie lassen sich ggf. exportieren.

Hinweise:

- Das in der Konsole angezeigte Datum-/Zeitformat stimmt mit dem Format in dem Rechner, in dem der DNA Server installiert ist, überein. Um das Format in der Konsole zu ändern, müssen Sie zunächst das Format in diesem Rechner ändern. Für weitere Informationen wenden Sie sich bitte an unser Support-Team www.netsupportsoftware.com/support.
- Die Häufigkeit, mit welcher der Server Daten sammelt, lässt sich mit der Option "DNA-Einstellungen" ändern. Dies gilt nicht für kritische, dringende oder hohe Alerts, deren Daten sofort an den Server gesendet werden.

PC-Alerts

Mit PC-Alerts können Bediener Veränderungen identifizieren, die auf einem bestimmten PC stattfinden. Es gibt eine Reihe von vordefinierten Alerts, die der Bediener einrichten kann, z. B. Platz-Alerts, Sicherheits-Alerts, usw. Der Bediener gibt dann die Bedingungen für das Alert ein, wer benachrichtigt werden soll und welche Aktionen ausgeführt werden sollen, wenn das Alert ausgelöst wird. Sobald das Alert an der Konsole aktiv ist, können Sie die vollen Details ansehen und eine permanente Aufzeichnung zur späteren Überprüfung speichern.

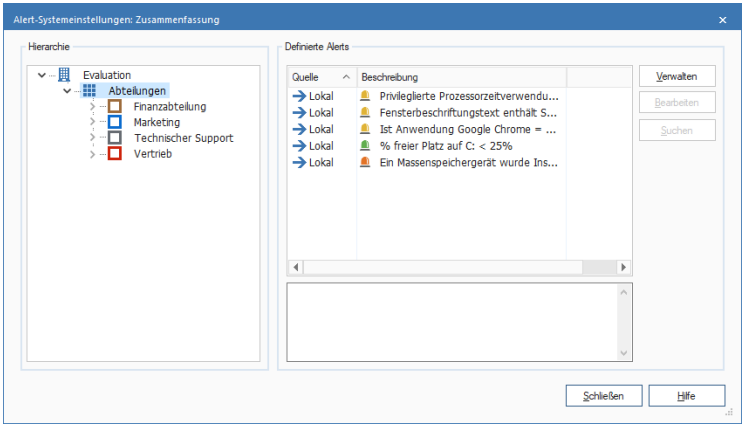
1. Markieren Sie ein Unternehmen, eine Abteilung oder eine AD Container während die Registerkarte "Alerts" ausgewählt ist.
2. Klicken Sie mit der rechten Maustaste und wählen Sie **PC-Alerts**.

   Oder

   Klicken Sie auf den Dropdownpfeil für das Alertsymbol und wählen Sie im Menü die Option {PC-Alerts}.

   Oder

   Klicken Sie auf das Symbol **PC-Alerts** im Aktivierte Alerts Bereich im Menüband.
3. Das DNA Alert-Managementsystem wird eingeblendet.



4. Wählen Sie die gewünschte Ebene in der Hierarchie und eine Beschreibung aller vorhandenen Alerts wird eingeblendet. Auf der Ursprungsebene als lokale Alerts identifizierte Alerts wurden ursprünglich auf dieser Ebene erstellt, vererbte Alerts wurden vom übergeordneten Unternehmen oder der übergeordneten Abteilung übernommen.

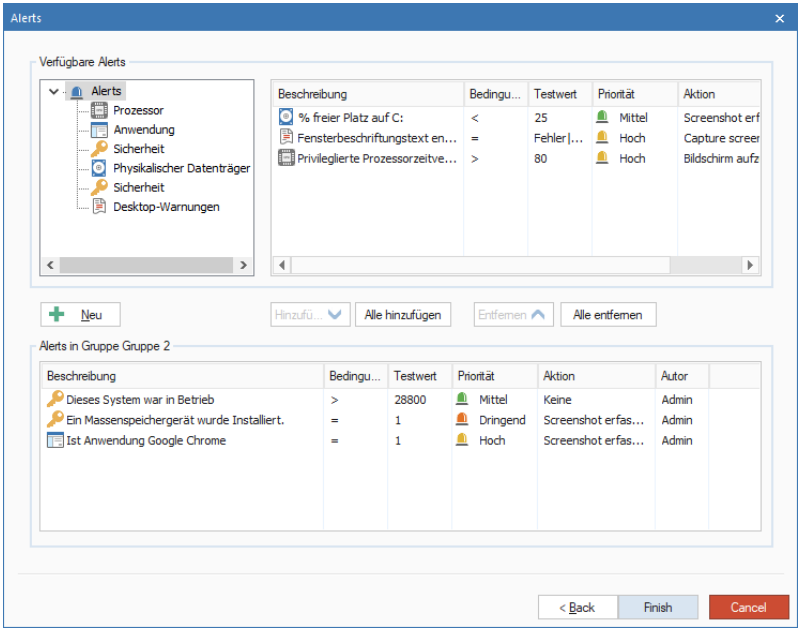
5. Wählen Sie **Verwalten**. Das Dialogfeld "Alert-Manager" wird eingeblendet. Hier können Sie neue Alerts erstellen oder vorhandene Alerts bearbeiten und löschen.
6. Um die Eigenschaften eines vorhandenen Alerts zu ändern, klicken Sie auf **Bearbeiten**. Sie können einen geerbten Alert nicht direkt bearbeiten, sondern nur einen lokalen Alert. Um einen geerbten Alert zu ändern, wählen Sie den geforderten Alert und klicken dann auf **Suchen**.

Alert-Manager

In diesem Dialogfeld können Sie neue Alerts erstellen, die Eigenschaften für vorhandene Alerts bearbeiten und Alerts auf Unternehmens- oder Abteilungsebene zuweisen.

1. Wählen Sie in der Strukturansicht, ob Sie ein Alert erstellen oder Gruppendefinitionen einrichten möchten.

Hinweis: Gruppendefinitionen sind eine Sammlung von Alerts, die sich auf ein Unternehmen oder eine Abteilung anwenden lassen.

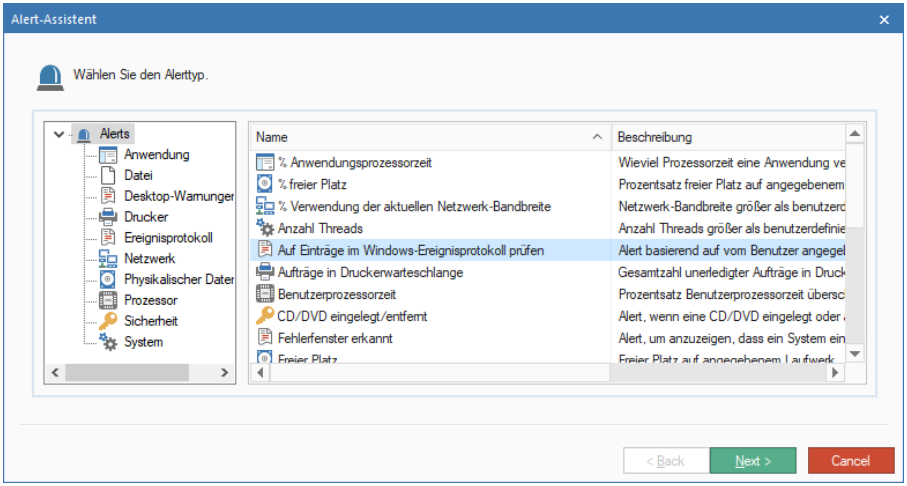


2. Klicken Sie auf **Neu**, um ein neues Alert oder Gruppendefinitionen zu erstellen.
   Oder
   um die Eigenschaften eines vorhandenen Alerts zu ändern, klicken Sie auf **Bearbeiten**.
   Oder
   klicken Sie auf **Löschen**, um ein Alert, das nicht mehr benötigt wird, zu entfernen.
3. Wenn ein Alert erstellt wurde, erscheint eine Beschreibung davon. Um ein Alert zu aktivieren, müssen Sie es in die aktuelle Abteilung aufnehmen. Verwenden Sie die entsprechenden Schaltflächen zum Hinzufügen/Entfernen von Alerts.
4. Wenn Sie mit den Änderungen zufrieden sind, klicken Sie auf **Speichern**, gefolgt von **Schließen**.

Hinweis: Wenn Sie ein zurzeit aktives Alert bearbeiten, lassen sich nicht alle Felder ändern. Um die Haupteigenschaften eines Alerts zu ändern, müssen Sie es vorher deaktivieren.

DNA Alert-Assistent

Der DNA Alert-Assistent führt Sie durch den Einrichtungsprozess für PC-Alerts. Sie können die Eigenschaften durch Eingabe der gewünschten Bedingungsparameter anpassen.



1. Wählen Sie eines der vordefinierten Alerts und markieren es. Klicken Sie auf **Weiter**.

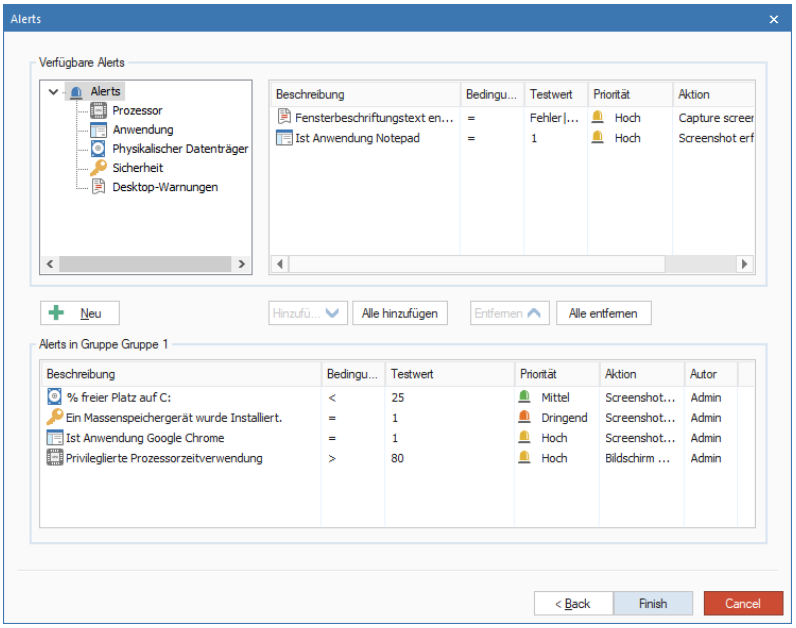
2. Geben Sie die geforderten Eigenschaften ein, bestimmen Sie einen Prioritätsgrad für das Alert und wählen Sie die Aktion, die erfolgen soll, wenn das Alert ausgelöst wird. Wählen Sie **Erweitert** für zusätzliche Konfigurationsoptionen.
3. Klicken Sie auf **Weiter**. Es wird eine Liste der Konsolebediener eingeblendet. Wählen Sie den Bediener, der beim Auslösen des Alerts kontaktiert werden soll. Mit den entsprechenden Schaltflächen lassen sich Bediener, die benachrichtigt werden sollen, hinzufügen oder entfernen.
4. Wählen Sie, auf welche Weise der Bediener beim Auslösen des Alerts kontaktiert werden soll. Wählen Sie entweder **Konsolenachricht** oder **E-Mail-Benachrichtigung**.
5. Klicken Sie auf **Fertig stellen**. Eine Beschreibung des Alerts wird nun im Alert-Manager angezeigt.

Hinweis: Um eine Benachrichtigung per E-Mail zu senden, müssen Sie sicherstellen, dass Sie die E-Mail-Einstellungen in den DNA Alerting-Systemeinstellungen konfiguriert und im Dialogfeld "Konsolebediener" eine E-Mail-Adresse für den Bediener definiert haben.

Gruppendefinitionen

Gruppendefinitionen sind eine Sammlung von Alerts, die sich auf ein Unternehmen oder eine Abteilung anwenden lassen.

1. Wählen Sie in der Strukturansicht des Dialogfelds "Alert-Manager " die Option **Gruppendefinitionen** und klicken Sie auf **Neu**.
2. Das Dialogfeld "Gruppendefinitionen" wird eingeblendet. Geben Sie einen Namen und eine Beschreibung für das Gruppen ein und klicken Sie auf **Weiter**.
3. Alle vorher erstellten Alerts sind aufgeführt. Markieren Sie in der Strukturansicht ein Alert, das Sie in das Gruppen aufnehmen möchten.

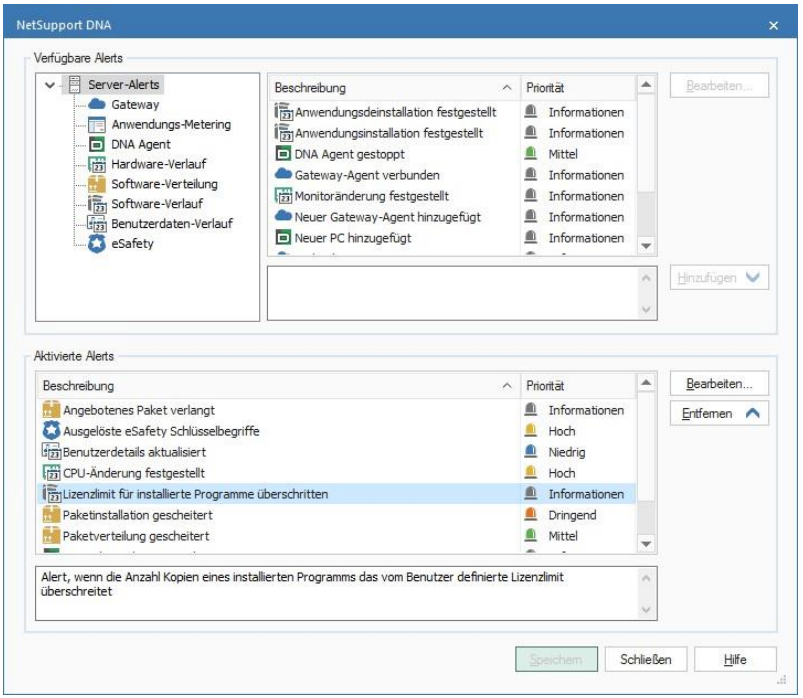


4. Um einen neuen Alert zu erstellen, klicken Sie auf **Neu**. Der Alert-Assistent wird eingeblendet. Wenn das Alert erstellt ist, wird es in dieses Dialogfeld aufgenommen.
5. Mit den entsprechenden Schaltflächen lassen sich Alerts zum aktuellen Gruppen hinzufügen oder aus diesem entfernen.
6. Klicken Sie auf **Fertig stellen**. Das Gruppen erscheint nun im Dialogfeld "Alert-Manager". Es lässt sich aktivieren, indem Sie es zur aktuellen Abteilung hinzufügen.

DNA Server\Konsolen-Alerts

Mit Server-Alerts können Bediener Änderungen an den von NetSupport DNA im ganzen Unternehmen gesammelten Daten identifizieren. DNA Server-Alerts sind Alerts für individuelle PCs, z.B. wenn ein Benutzer versucht, Zugriff auf eine eingeschränkte Website zu nehmen. Konsolen-Alerts identifizieren Änderungen im Bezug auf die NetSupport DNA Konsole. Alerts, die nicht individuelle PCs betreffen, fallen unter Konsolen-Alerts, beispielsweise wenn ein neuer Bediener hinzugefügt wird.

1. Klicken Sie auf den Dropdownpfeil für das Alertsymbol und wählen Sie im Menü die Option {DNA Server\ Konsolen-Alerts}.
   Oder
   Klicken Sie auf das Symbol **DNA Server\ Konsolen-Alerts** im Aktivierte Alerts Bereich im Menüband.
2. Das Server\Konsolen-Alerts wird eingeblendet.



3. Eine Auswahl vordefinierter Alerts erscheint in der Liste "Verfügbare Server-Alerts". Alle aktiven Alerts werden in der Liste der aktivierten

Alerts aufgeführt. Mit den entsprechenden Schaltflächen können Sie Alerts zur Liste der aktivierten Alerts hinzufügen oder sie aus dieser entfernen.

4. Die Prioritätsstufe und Benachrichtigungsdetails (nur für Server-Alerts) für ein Alert lassen sich durch Auswahl von **Bearbeiten** ändern.
5. Wenn alle Änderungen beendet sind, drücken Sie auf die Schaltfläche **Speichern** und **schließen**.

Aktive Alerts

Wenn ein Alert aktiv geworden ist, wird der Bediener entweder über eine Konsolenachricht oder eine E-Mail-Benachrichtigung davon in Kenntnis gesetzt, je nach der beim Erstellen des Alerts gewählten Methode.

Hinweis: Das Alert-Symbol im Menüband wechselt auf rot, wenn es ausstehende Alerts gibt.

Benachrichtigung per Konsolenachricht

Beim Auslösen eines Alerts wird der Bediener mit einem passenden Identifikator benachrichtigt. Dieser erscheint neben der Unternehmens-, Abteilungs- oder Agentebene in der Hierarchie-Strukturansicht (je nachdem, welche Ebene geöffnet ist). Der Bediener kann vollständige Details zu dem Alert im Informationsfenster betrachten.



Hinweis: Sie können Alerts in der Strukturansicht zeigen / ausblenden, indem Sie auf  klicken.

Bei kritischen, dringenden und hohen Server und PC-Alerts wird rechts an der Taskleiste des PCs ein Benachrichtigungsfenster eingeblendet. Dies gewährleistet, dass die Bediener sofort benachrichtigt werden, unabhängig vom Abschnitt der DNA Konsole, den sie gerade betrachten.

Im Benachrichtigungsfenster wird angezeigt, welches Alert aktiviert wurde. Der Bediener kann auf das Fenster klicken und gelangt so in die Registerkarte für das Alert, wo vollständige Informationen sichtbar sind.

E-Mail-Benachrichtigung

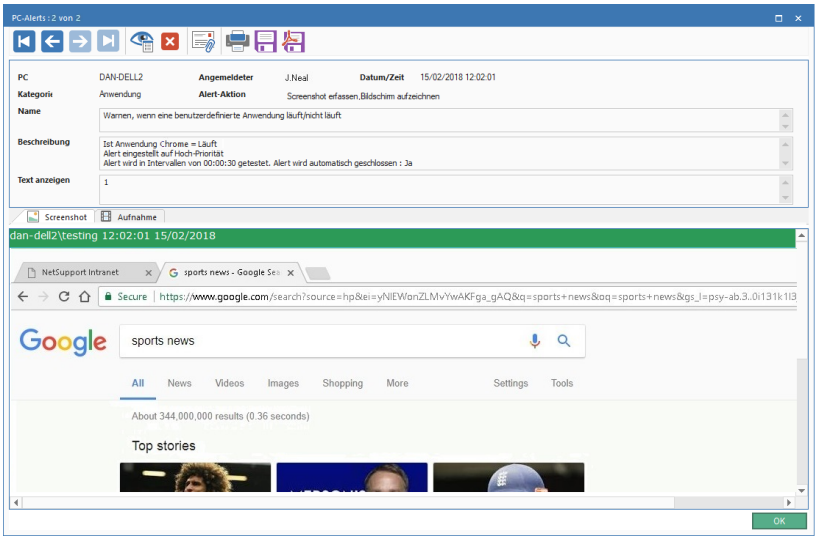
Sobald ein Alert aktiv wird, erhält der betreffende Bediener eine E-Mail mit der Mitteilung, dass das Alert ausgelöst wurde. Die Email enthält die Prioritätsstufe des Alerts, das Datum und die Zeit, zu der das Alert ausgelöst wurde, Details des Systems und Benutzers und wie lange es aktiv war.

Von hier aus können Sie die vollen Details anzeigen und das Alert schließen, indem Sie auf klicken. PC-Alerts können überprüft werden, und Sie können eine permanente Aufzeichnung davon als Datei speichern.

Aktive PC-Alerts überprüfen

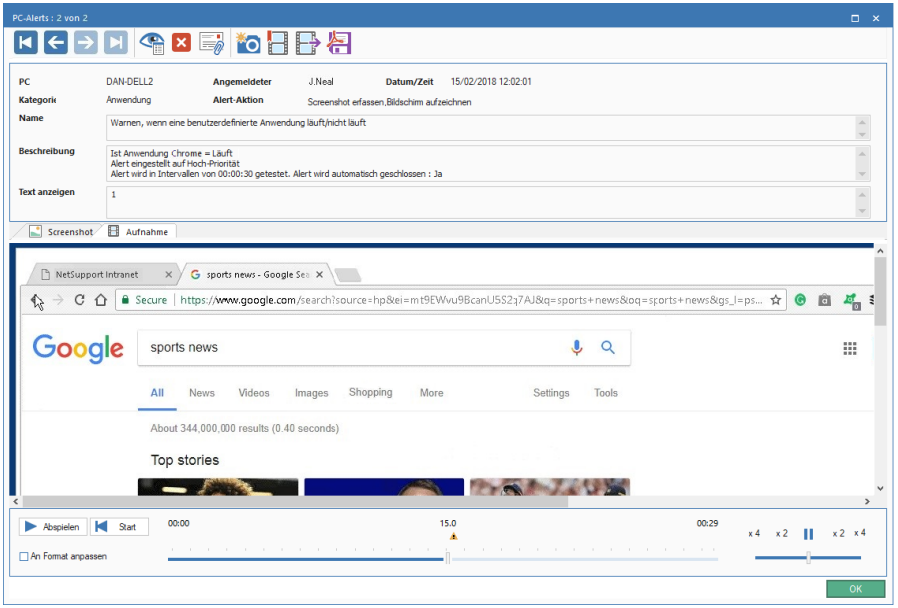
PC-Alerts, die ausgelöst worden sind, können von hier aus überprüft und freigegeben werden.

1. Klicken Sie auf das Symbol **PC** im Ausgelöste Alerts Bereich im Menüband.
2. Klicken Sie das **Überprüfen** Symbol im Menüband an.
3. Der PC-Alerts Dialog wird gezeigt.



4. Um die aktiven Alerts zu durchscrollen, benutzen Sie die Vor- und Zurück-Pfeile.
5. Es wird ein Überblick des Alerts gezeigt und wer ihn aktiviert hat. Alerts für derenAktionen Screenshot-Erfassung eingestellt ist, werden einen Screenshot enthalten, und die, die für Bildschirm aufzeichnen eingestellt sind, werden eine Bildschirmaufzeichnung enthalten.
6. Sie können ausdrucken, speichern und emailen, und wenn ein Screenshot, Bildschirmaufzeichnung oder und Webcam-Bild angehängt ist, können Sie im Verlauf sehen, wer diesen angesehen hat.
7. Die Alert-Details können an ein PDF exportiert werden, indem Sie auf  klicken. Sie können den Standardordner, an den das PDF exportiert werden soll, in den Dateispeicherort-Einstellungen angeben, und das PDF in den Alerting-Einstellungen mit dem Branding Ihrer Organisation anpassen.
8. Um ein Alert zu schließen, klicken Sie auf  und dann auf **OK**. Nun erscheint ein Alerts schließen Dialog. Eine Beschreibung dafür, warum Sie das Alert schließen, kann hinzugefügt werden. Klicken Sie auf **Ja**. Die Verlaufkomponente bietet einen Verlauf aller geschlossenen PC-Alerts.

Anzeigen einer Bildschirmaufzeichnung



Wenn eine Bildschirmaufzeichnung angezeigt wird, erscheinen Playback-Steuerelemente, die es Ihnen ermöglichen zu sehen, was beim Agent geschah, als das Alert ausgelöst wurde.

Eine Zeitskala zeigt, wo das Alert in der Aufzeichnung ausgelöst wurde, und ob Lesezeichen hinzugefügt worden sind. Sie können den Schieberegler benutzen, um zur gewünschen Position zu gehen. Klicken Sie auf **Play**, um die Aufzeichnung zu starten - in der Standardeinstellung beginnt sie dort, wo das Alert ausgelöst wurde (wenn Sie auf **Start** klicken, gelangen Sie zum Anfang der Aufzeichnung). Sie können in der Aufzeichnung vor- und zurücklaufen, indem Sie auf dem Schieberegler ganz rechts im Dialog klicken. Wenn Sie den Schieberegler freigeben, wird die Aufzeichnung an dieser Stelle angehalten. Wählen Sie **Auf Größe anpassen**, um den gesamten Schülerbildschirm im Anzeigebereich zu zeigen.

Es können Lesezeichen hinzugefügt werden, um wichtige Bereiche der Aufzeichnung zu markieren. Vergewissern Sie sich, dass Sie an der gewünschten Stelle der Zeitskala sind, und klicken Sie dann auf  .

Geben Sie eine Beschreibung für das Lesezeichen ein, und klicken Sie dann auf **OK**.

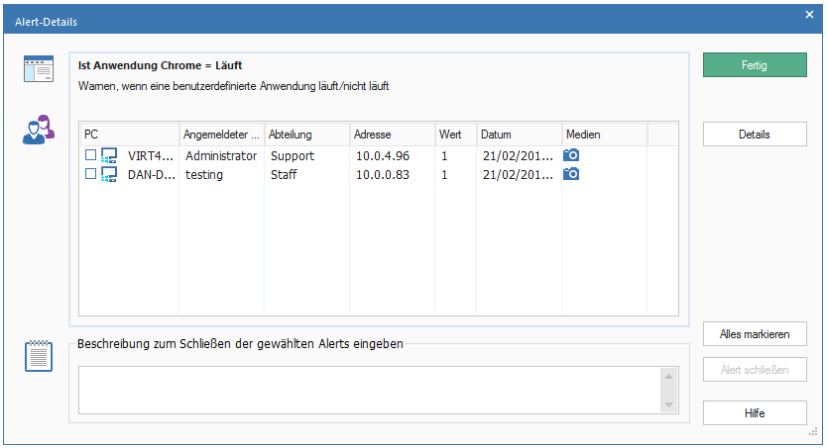
Hinweis: Es kann eine Momentaufnahme der Aufzeichnung gespeichert werden. Klicken Sie auf , geben Sie einen Namen für den Screenshot ein, wählen Sie den Dateityp, in dem er gespeichert werden soll, und klicken Sie dann auf **Speichern**.

Eine Bildschirmaufzeichnung kann in eine Videodatei konvertiert werden, so dass sie außerhalb der DNA Konsole auf verschiedenen Media Players wiedergegeben werden kann. Sie kann in WMV und AVI Formate konvertiert werden. Klicken Sie auf ; der Dateiwiedergabe-Konvertierungsassistent führt Sie nun durch den Konvertierungsprozess.

Hinweis: In der Standardeinstellung beträgt die Länge der Bildschirmaufzeichnung 15 Sekunden (fünfzehn Sekunden bevor und nachdem der Begriff ausgelöst wird). Dies kann in den Alerting-Einstellungen angepasst werden.

Schließen von Alerts

Nach Identifizierung des Alerts kann es der Bediener schließen, indem er auf die im Informationsfenster klickt. Folgendes Dialogfeld wird eingeblendet.



Details des Alerts werden zusammen mit einer Liste der PCs, für die das Alert unerledigt ist, eingeblendet. Sie können die vollständigen Details der PC-Alerts und der damit verbundenen Medien anzeigen und freigeben, indem Sie auf **Details** klicken (PC-Alerts können auch geschlossen werden, während man die vollständigen Details anzeigt).

Wenn das Alert von mehr als einem PC ausgelöst worden ist, wählen Sie die PCs, für die das Alert geschlossen werden soll; geben Sie, falls erforderlich, eine Beschreibung ein und klicken Sie dann auf **Alert schließen,** um das Alert zu schließen. Zum Schließen von DNA Server-Alerts oder Konsole-Alerts brauchen Sie keine Beschreibung einzugeben. Das Alert verschwindet aus dem Informationsfenster. Eine vollständige History aller PC-Alerts finden Sie in der History-Komponente.

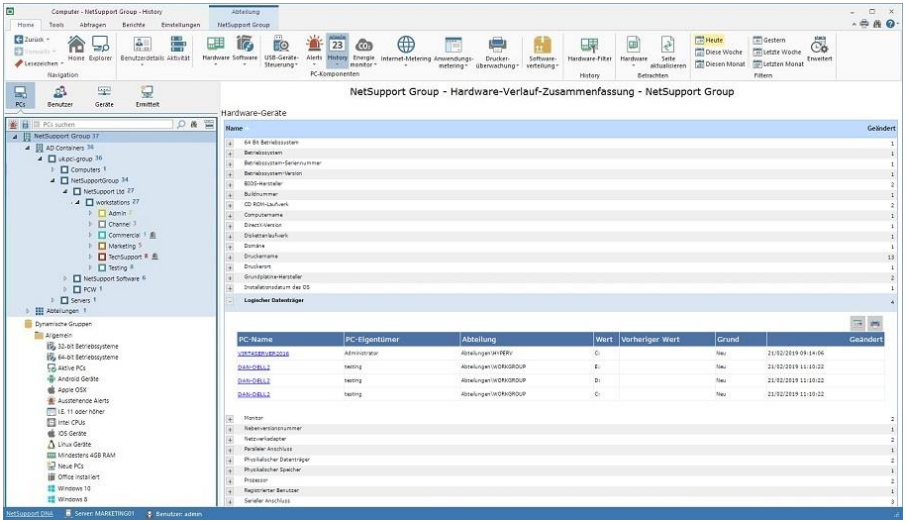
History-Fenster

Die Verlauf-Option ermöglicht es Ihnen, Änderungen nachzuverfolgen, die im Agent-Hardware-Inventar, Software-Inventar und an den Benutzerangaben vorgenommen worden sind, und auch den Alerting- und Konsolenanmeldungsverlauf anzuzeigen.

Jedes Mal wenn NetSupport DNA Daten sammelt, vergleicht es die aktuellen Angaben mit den bereits auf dem Server gespeicherten Informationen, und wenn es Unterschiede findet, werden diese im Verlauf erfasst.

1. Klicken Sie im Ribbon auf das **Verlaufssymbol**. Das Fenster "History-Zusammenfassung" wird eingeblendet.

Hinweis: Wenn die Komponentensymbole ausgeblendet sind, klicken Sie auf die Registerkarte **Home**.



Sie können die History auf folgenden Ebenen betrachten: Unternehmen, Abteilung, AD Container, dynamische Gruppe oder Agent. Wählen Sie die gewünschte Ebene in der hierarchischen Strukturansicht.

Um zwischen den Ansichten hin- und herzuschalten, klicken Sie auf der Verlauf-Symbol-Dropdownliste und wählen {Anzeigen- Hardware\ Software\Benutzerdaten\Alerting\Konsolenanmeldungsverlauf} oder auf dem entsprechenden Symbol im Menüband.

Sie können die Daten für eine spezifische Zeitperiode betrachten. Um zwischen verschiedenen Zeitperioden hin- und herzuschalten, klicken Sie das entsprechende Symbol im Filterbereich des Menübands an. Wenn Sie auf Erweitert klicken, können Sie einen benutzerdefinierten Datum-/Zeitfilter anwenden. Aufgelistete Beschreibungen lassen sich erweitern, so dass Sie ein individuelles Agentbreakdown für jedes Objekt erhalten. Die gezeigten Arbeitsstunden können im DNA Konfigurationskatalog für Ihre Organisation angepasst werden. Siehe Konsolenanpassungen – Allgemein für weitere Informationen.

Das in der Konsole angezeigte Datum-/Zeitformat stimmt mit dem Format in dem Rechner, in dem der DNA Server installiert ist, überein. Um das Format in der Konsole zu ändern, müssen Sie zunächst das Format in diesem Rechner ändern. Für weitere Informationen wenden Sie sich bitte an unser Support-Team www.netsupportsoftware.com/support.

Hinweis: Es kann sein, dass Sie für gewisse in der History festgehaltene Hardwareänderungen kein Tracking durchführen möchten. Durch Klicken Sie auf den Dropdownpfeil für das History-Symbol und wählen Sie im Menü die Option {Filter für Hardwareänderungen} oder klicken Sie auf das Symbol „Filter für Hardwareänderungen" im Ribbon „History" können Sie die Anzeige von Objekten in der Konsole deaktivieren und vorhandene Daten für deaktivierte Objekte löschen.

Abfragen
Wählen Sie zur Anzeige des Abfragefensters die Registerkarte „Abfragen". Mit dem Abfragetool von DNA können Sie Datenbankeinträge abrufen, die bestimmte Kriterien erfüllen. Abfragen zu der Komponente, die gerade betrachtet wird, sind aufgelistet, was ein schnelles Abrufen der Ergebnisse ermöglicht. Klicken Sie in der Menüleiste auf dem Abfrage hinzufügen Symbol, um eine neue Abfrage zu erstellen, oder klicken Sie auf dem Abfrage bearbeiten Symbol in der Menüleiste, um ein in der Liste vorhandenes Objekt zu bearbeiten.

Berichte
Wählen Sie zur Anzeige des Berichtfensters die Registerkarte „Berichte". Jeder Komponente ist eine Reihe von vordefinierten Managementberichten, die vom Crystal Reports-Modul gespeist werden, beigefügt. Wählen Sie den gewünschten Bericht. Wählen Sie den geforderten Bericht in der Dropdown-Liste. Sie lassen sich ggf. exportieren.

Energiemonitor

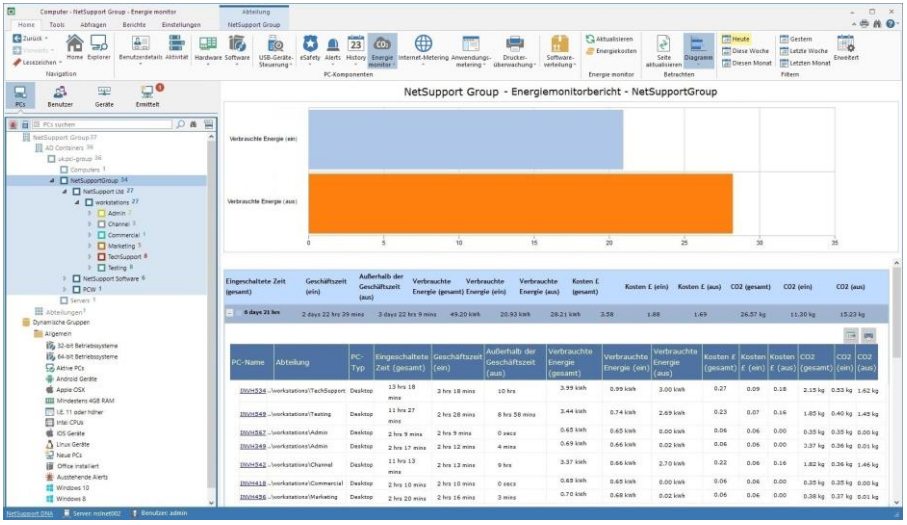
Das Energieüberwachungsmodul bietet eine einfache und präzise Zusammenfassung der potentiellen Energieverschwendung in der gesamten Organisation durch Computersysteme, die außerhalb der Geschäftszeiten eingeschaltet bleiben.

NetSupport DNA kontrolliert auf den eingeschalteten Zustand aller Computer, und seine lokale Überwachungskomponente erstellt eine genaue Aufzeichnung aller Zeiten, zu denen ein Computer ein- oder ausgeschaltet oder im Ruhezustand war. Wenn sie alle Tageszeiten weiß, zu denen der Computer in Betrieb war, wird eine Berechnung des durchschnittlichen (und benutzerdefinierbaren) „Stromverbrauchs pro Gerät" ausgeführt, die die Berechnung des Energieverbrauch-Grundwerts für alle Computer erleichtert.

Auf der Basis dieser Informationen können Computer in ausgewählten Abteilungen dafür eingestellt werden, am Ende jedes Tages automatisch auszuschalten und am nächsten Morgen wieder einzuschalten.

1. Klicken Sie auf das **Energiemonitorsymbol**. Das Fenster „Energiemonitor" wird eingeblendet.

   Hinweis: Wenn die Komponentensymbole ausgeblendet sind, klicken Sie auf die Registerkarte **Home**.



Wählen Sie in der hierarchischen Strukturansicht die Ebene, auf der Sie die angezeigten Daten betrachten möchten: Unternehmen, Abteilung, AD Container, dynamische Gruppe oder individueller Agent.

Gesamte eingeschaltete Zeit, Energieverbrauch, Kosten und CO2 Emissionen sowohl während als auch außerhalb der Arbeitsstunden werden in einem Graph und in Listenformat angezeigt. Um den Graph in einem anderen Format anzuzeigen, klicken Sie auf dem **Diagramm**-Symbol-Dropdownpfeil in der Menüleiste und wählen das entsprechende Format. Um die aktive Ansicht auszudrucken, klicken Sie auf dem  Symbol oben auf der Konsole.

Hinweis: Durch Anklicken des Chart-Symbols im Ribbon wird die Grafik ein-/ausgeblendet.

Sie können die Daten für eine spezifische Zeitperiode betrachten. Um zwischen verschiedenen Zeitperioden hin- und herzuschalten, klicken Sie das entsprechende Symbol im Filterbereich des Menübands an. Wenn Sie auf Erweitert klicken, können Sie einen benutzerdefinierten Datum-/Zeitfilter anwenden. Aufgelistete Beschreibungen lassen sich erweitern, so dass Sie ein individuelles Agentbreakdown für jedes Objekt erhalten. Die gezeigten Arbeitsstunden können im DNA Konfigurationskatalog für Ihre Organisation angepasst werden. Siehe Konsolenanpassungen – Allgemein für weitere Informationen.

Die für Stromverbrauch, Energiekosten und CO2 Emissionen benutzten Werte können angepasst werden. Klicken Sie auf der Dropdownliste des **Energieüberwachung-** Symbols und wählen Sie {Energiekosten} oder klicken Sie im Menüband auf dem **Energiekosten-**Symbol.

Es kann ein Energiemanagementplan eingestellt werden, um Geräte an ausgewählten Tagen und zu bestimmten Zeiten automatisch ein- und auszuschalten. Sie können auch einstellen, welche Aktionen ausgeführt werden sollen, wenn ein Benutzer noch an einem Gerät angemeldet ist, wenn es Zeit ist auszuschalten. Es können Inaktivitätsrichtlinien erstellt werden, bei denen Sie wählen können, was geschehen soll, wenn ein Gerät für eine vorgegebene Zeitspanne inaktiv gewesen ist: Sie können ein Gerät beispielsweise dafür einstellen, sich auszuschalten, wenn zwischen 17:00 und 19:00 Uhr dreißig Minuten lang keine Aktivität stattgefunden hat. Ein Energiemanagementplan kann in NetSupport DNA – Energieüberwachungseinstellungen eingestellt werden.

Es können Ferienzeiten definiert werden, so dass Geräte aus dem Einschalten-Zeitplan für diese Daten ausgeschlossen werden können. Sie können die Ferienzeiten in Konsolenanpassungen – Benutzerschaltfläche eingeben. Dann muss die Option **Einschalten während der Ferien verhindern** in NetSupport DNA – Energieüberwachungseinstellungen aktiviert werden.

Hinweis: Agent-Geräte können ein- oder ausgeschaltet werden, indem Sie die gewünschte Ebene in der Struktur rechts anklicken und {Energiemanagement – Strom ein /Strom aus } wählen.

Wenn Sie wissen, dass das Inventar für einen bestimmten Agent oder eine Abteilung nicht mehr aktuell ist, können Sie die Schnellaktualisierungsfunktion verwenden. Klicken Sie mit der rechten Maustaste auf das gewünschte Objekt in der Strukturansicht und wählen Sie „Aktualisieren" oder klicken Sie im Menü oder der Gruppe „Energiemonitor" auf „Aktualisieren".

Abfragen

Wählen Sie zur Anzeige des Abfragefensters die Registerkarte „Abfragen".

Mit dem Abfragetool von DNA können Sie Datenbankeinträge abrufen, die bestimmte Kriterien erfüllen. Abfragen zu der Komponente, die gerade betrachtet wird, sind aufgelistet, was ein schnelles Abrufen der Ergebnisse ermöglicht.

Klicken Sie in der Menüleiste auf dem Abfrage hinzufügen Symbol, um eine neue Abfrage zu erstellen, oder klicken Sie auf dem Abfrage bearbeiten Symbol in der Menüleiste, um ein in der Liste vorhandenes Objekt zu bearbeiten.

Berichte

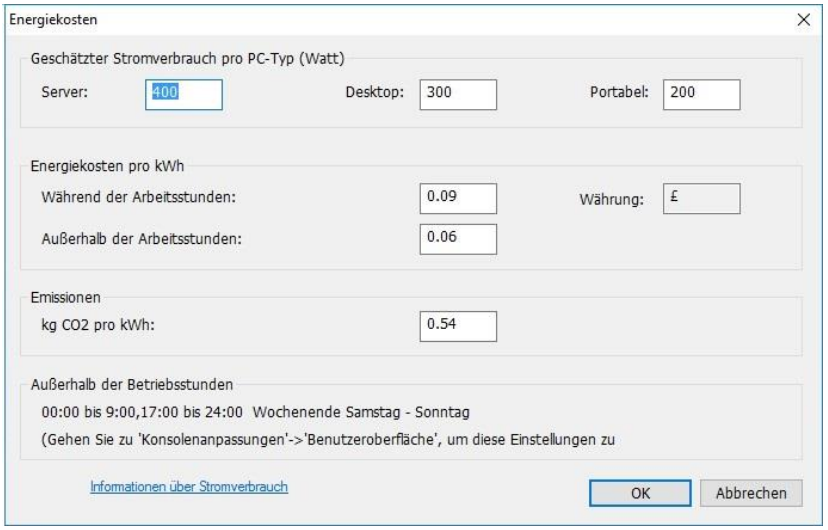
Wählen Sie zur Anzeige des Berichtfensters die Registerkarte „Berichte".

Jeder Komponente ist eine Reihe von vordefinierten Managementberichten, die vom Crystal Reports-Modul gespeist werden, beigefügt. Wählen Sie den geforderten Bericht in der Dropdown-Liste. Sie lassen sich ggf. exportieren.

Die Häufigkeit, mit der der Server Daten sammelt, lässt sich mit der Option "DNA-Einstellungen" ändern.

Energiekosten

Die zur Berechnung von Stromverbrauch, Kosten und CO2-Emissionen in der Energiemonitorkomponente nötigen Werte lassen sich hier einstellen. Außerdem können Sie auch die Einstellungen für den Energieplan konfigurieren.



Geschätzter Stromverbrauch pro PC-Typ (Watt)
Der geschätzte Stromverbrauch für die einzelnen PC-Typen lässt sich hier angeben.

Energiekosten pro kWh
Geben Sie den Energiepreis pro kWh ein. Sie können die Werte für inner- und außerhalb der Geschäftszeiten eingeben. Das Währungssymbol zeigt die benutzte Währung. Diese kann im DNA Datenbank-Assistent – Sonstige Einstellungen geändert werden.

Emissionen
Standardmäßig ist der Emissionswert auf 0,54kg CO2 pro kWh eingestellt.

Außerhalb der Geschäftszeiten
Die Bürostunden und –tage werden angezeigt. Sie können in Konsolenanpassungen – Allgemein-Einstellungen für Ihre Organisation passend geändert werden.

Internet-Metering

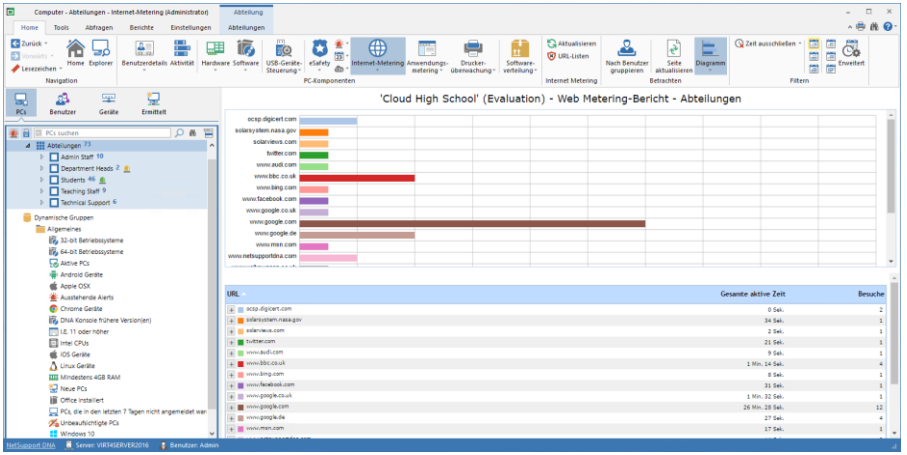
Das Internet-Metering-Modul bietet eine detaillierte Zusammenfassung aller Internetaktivitäten für jeden PC nach Schülern, einschließlich Start- und Beendigungszeiten für jede besuchte URL und die aktive Zeit, die auf dieser Seite verbracht wurde. Die Ergebnisse können nach Gerät oder Benutzer angezeigt werden. Der Schlüssel zur Unterstützung einer effektiven E-Sicherheitsrichtlinie ist natürlich effektive Kontrolle. NetSupport DNA ermöglicht volles Management der Internetnutzung; Listen mit genehmigten und eingeschränkten URLs und/oder Sub-URLs können zentral implementiert werden. Wenn die Listen eingesetzt werden, kann NetSupport DNA uneingeschränkten Zugriff auf alle Websites erlauben, beschränkten Zugriff auf bestimmte Websites, die von der Schule als genehmigt markiert worden sind, oder den Zugriff auf bestimmte Websites, die als ungeeignet markiert worden sind, blockieren.

Der Zugriff kann auch nach Tageszeit gesteuert werden, beispielsweise um den Zugriff auf genehmigte Gaming-Websites für Schulclubs außerhalb der Unterrichtszeiten zuzulassen.

Hinweis: Die Internet-Metering Funktion steht nur in der NetSupport DNA Version für das Bildungswesen zur Verfügung.

1. Klicken Sie im Ribbon auf das **Internet Metering-Symbol**. Das Fenster "Internet Metering" wird eingeblendet.

   Hinweis: Wenn die Komponentensymbole ausgeblendet sind, klicken Sie auf die Registerkarte **Home**.



Die hierarchische Strukturansicht lässt sich zwischen PCs und Benutzern umschalten. Die Strukturansicht des PCs zeigt Daten für den PC-Eigentümer, der mit dem betreffenden PC verknüpft ist, und die Benutzerstrukturansicht zeigt Daten für angemeldete Benutzer.

Wählen Sie in der hierarchischen Strukturansicht die Ebene, auf der Sie die angezeigten Daten betrachten möchten: Unternehmen, Abteilung, AD Container, dynamische Grupe oder individueller Agent.

Im Informationsfenster ist ein Breakdown für jedes gewählte Objekt in Grafik- und Listenformat angezeigt. Um den Graph in einem anderen Format anzuzeigen, klicken Sie auf dem Diagramm-Symbol-Dropdownpfeil in der Menüleiste und wählen das entsprechende Format.

Um die aktive Ansicht auszudrucken, klicken Sie auf dem  Symbol oben aufder Konsole.

Hinweis: Durch Anklicken des Chart-Symbols im Ribbon wird die Grafik ein-/ausgeblendet.

Sie können die Daten für eine spezifische Zeitperiode betrachten. Um zwischen verschiedenen Zeitperioden hin- und herzuschalten, klicken Sie das entsprechende Symbol im Filterbereich des Menübands an. Wenn Sie auf Erweitert klicken, können Sie einen benutzerdefinierten Datum-/Zeitfilter anwenden. Aufgelistete Beschreibungen lassen sich erweitern, so dass Sie ein individuelles Agentbreakdown für jedes Objekt erhalten. Sites, die kürzer als eine angegebene Zeitspanne aktiv waren, lassen sich ggf. ignorieren.

Hinweis: Die gezeigten Arbeitsstunden können im DNA Konfigurationskatalog für Ihre Organisation angepasst werden. Siehe Konsolenanpassungen – Allgemein für weitere Informationen.

Standardmäßig wird die Internet-Nutzung durch die Websites, auf die zugegriffen wurde, angezeigt. Wenn Sie Nach Benutzer gruppieren auswählen, können Sie die Internet-Nutzung nach der Benutzer-ID von Agents statt dem PC betrachten. Diese Option ist in der Benutzerstrukturansicht nicht verfügbar.

Wenn Sie Nach PC gruppieren auswählen, können Sie die Internet-Nutzung nach PC-Details und nicht Benutzerdetails des Agents betrachten, während Sie sich in der Benutzerstrukturansicht befinden. Diese Option ist in der Strukturansicht des PCs nicht verfügbar.

Hinweis: Wenn Sie in der Strukturansicht die verschiedenen Ebenen wählen, können Sie die Internet-Nutzung der Agents auf PCs auf verschiedenen Ebenen der Organisation anzeigen.

Mit einer Schnellaktualisierungsfunktion können Sie Daten außerhalb der angegebenen Häufigkeit aktualisieren. Dies kann nützlich sein, wenn Sie bestimmte Agents oder Abteilungen anpeilen möchten. Klicken Sie mit der rechten Maustaste auf das gewünschte Objekt in der Strukturansicht und wählen Sie **Aktualisieren** oder klicken Sie im Menü oder Ribbon **Internet** auf **Aktualisieren**.

Die Anzahl der angezeigten URL lässt sich einschränken, indem Sie spezifische Sites aus der Liste ausschließen. Wenn Sie zum Beispiel eine genehmigte Liste mit Sites, die Benutzer besuchen dürfen, haben, nehmen Sie diese u. U. nicht in die Metering-Statistik auf. Weitere Angaben hierzu finden Sie unter Anwendung von Internet-Einschränkungen.

Es können URL-Listen erstellt werden, die Ihnen Kontrolle über die von den Agents besuchten Websites ermöglichen. Klicken Sie auf dem **URL-Listen** Symbol im Menüband. Wenn die URL-Listen definiert worden sind, können sie bestimmten Profilen zugeordnet werden. Siehe Internet-Metering-Einstellungen.

Abfragen
Wählen Sie zur Anzeige des Abfragefensters die Registerkarte „Abfragen".

Mit dem Abfragetool von DNA können Sie Datenbankeinträge abrufen, die bestimmte Kriterien erfüllen. Abfragen zu der Komponente, die gerade betrachtet wird, sind aufgelistet, was ein schnelles Abrufen der Ergebnisse ermöglicht.

Klicken Sie in der Menüleiste auf dem Abfrage hinzufügen Symbol, um eine neue Abfrage zu erstellen, oder klicken Sie auf dem Abfrage bearbeiten Symbol in der Menüleiste, um ein in der Liste vorhandenes Objekt zu bearbeiten.

Berichte
Wählen Sie zur Anzeige des Berichtfensters die Registerkarte „Berichte".

Jeder Komponente ist eine Reihe von vordefinierten Managementberichten, die vom Crystal Reports-Modul gespeist werden, beigefügt. Wählen Sie den geforderten Bericht in der Dropdown-Liste. Die Ergebnisse erscheinen im Informationsfenster. Sie lassen sich ggf. exportieren.

Hinweise:
- Das in der Konsole angezeigte Datum-/Zeitformat stimmt mit dem Format in dem Rechner, in dem der DNA Server installiert ist, überein. Um das Format in der Konsole zu ändern, müssen Sie zunächst das Format in diesem Rechner ändern. Für weitere Informationen wenden Sie sich bitte an unser Support-Team www.netsupportsoftware.com/support.
- Die Häufigkeit, mit der der Server Daten sammelt, lässt sich mit der Option "DNA-Einstellungen" ändern. Dies ermöglicht Ihnen gleichzeitig die Aktivierung von etwaigen Einschränkungen der Internet-Nutzung.

Internet-Einschränkungen

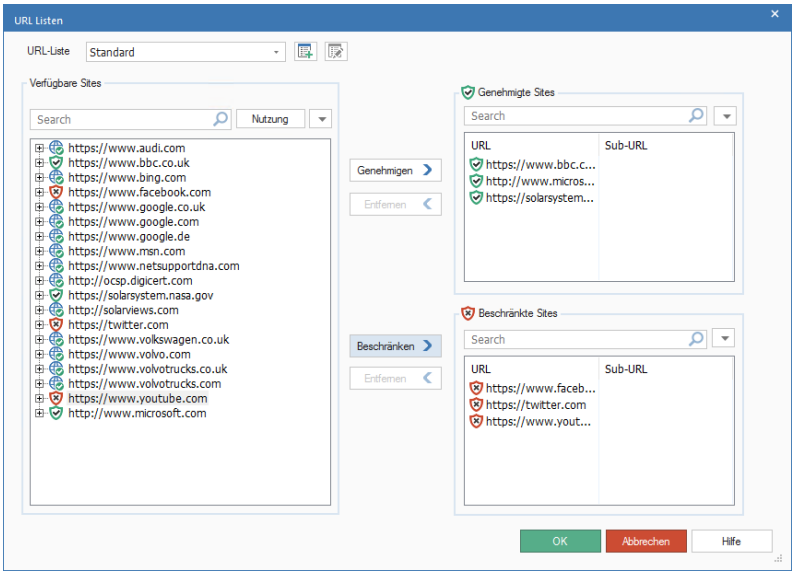
Sie können die von Agents besuchten Sites kontrollieren, indem Sie genehmigte und eingeschränkte Listen erstellen. Sie bestimmen, welche URL Benutzer besuchen dürfen oder nicht, und dann aktivieren Sie die gewünschte Liste über die Internet-Metering-Einstellungen. Es können mehrfache Listen erstellt werden, mit denen Sie verschiedenen Profilen unterschiedliche genehmigte/eingeschränkte Websites zuweisen können.

Sub-URL lassen sich unter einer Haupt-URL hinzufügen. Hierdurch können Sie den Zugriff auf bestimmte Bereiche einer Website einschränken/genehmigen. Sie können also zum Beispiel den Zugriff auf www.bbc.co.uk erlauben und gleichzeitig den Zugriff auf www.bbc.co.uk/sport beschränken.

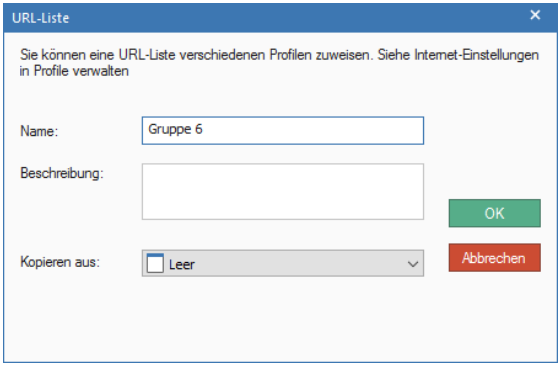
Hinweis: Um die Internet-Blockierfunktion zu benutzen, müssen Sie sich zunächst vergewissern, dass an den Agent-Geräten die NetSupport DNA Internet-Einschränkungen aktiviert sind. Bei der Installation eines Agents sind die Internet-Beschränkungen in der Standardeinstellung aktiviert. Sie können auch einen NetSupport DNA Agent mit aktivierten Internet-Beschränkungen an die geforderten PCs verteilen.

Erstellen einer Liste genehmigter/eingeschränkter URL

1. Klicken Sie auf den Dropdownpfeil des Symbols **Internet Metering** und wählen Sie im Menü die Option {URL-Listen}.
   Oder
   Klicken Sie auf das Symbol **URL-Listen** der Internet Metering-Gruppe.
2. Der URL-Listen Dialog erscheint. Websites, die bereits von Agents besucht worden sind, werden automatisch in der Verfügbare Websites Liste aufgeführt, und die Standard-URL-Liste wird angezeigt.



3. Um eine neue Website-Liste zu erstellen, klicken Sie auf  . Nun erscheint der URL-Liste Dialog.



Geben Sie einen Namen und, falls gefordert, eine Beschreibung für die Liste ein. Sie können eine vorhandene Liste kopieren, indem Sie sie in der 'Kopieren von' Dropdownliste wählen.

Hinweis: Es kann eine eSafety Schlüsselwortüberwachung- oder Risikoanalysen-URL-Liste kopiert werden. URLs aus dieser Liste werden zur entsprechenden Websites-Liste hinzugefügt.

Klicken Sie auf **OK**. Um eine vorhandene Liste zu bearbeiten, klicken Sie auf .

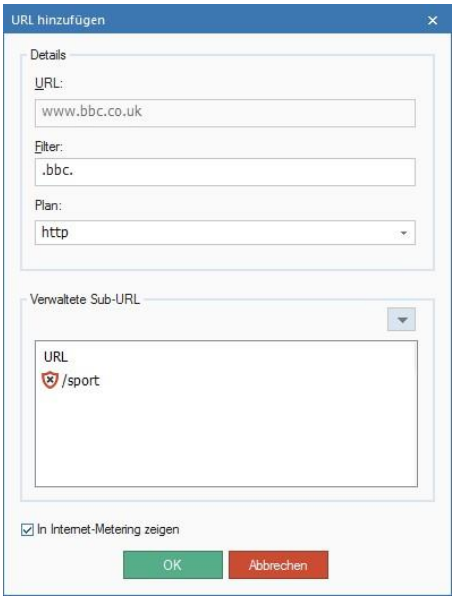
4. Achten Sie darauf, dass Sie im Dropdownmenü die richtige Liste wählen, um genehmigte/eingeschränkte Websites hinzuzufügen.
5. Um eine vorhandene URL zur Genehmigte oder Eingeschränkte Websites Liste hinzuzufügen, wählen Sie die URL in der Verfügbare Websites Liste. Sie können den Filter zum Inkraftsetzen der URL-Einschränkungen zur Feineinstellung, bei welchem Auftreten die URL betroffen sind, ändern.
   Zum Beispiel: Wenn Sie www.amazon.com als URL eingeben, wird automatisch der Filter .amazon erstellt. Mit diesem Filter werden www.amazon.com und www.amazon.co.uk blockiert. Wenn Sie den Filter hingegen zu .amazon.com ändern, wirkt sich die Interneteinschränkung nicht auf amazon.co.uk aus.

   Für weitere Informationen wenden Sie sich bitte an unser Support-Team www.netsupportsoftware.com/support.
6. Klicken Sie auf und wählen Sie **URL bearbeiten,** um den Filter eines aufgelisteten Elements zu bearbeiten und anzugeben, ob die Website von der Anzeige im Internet-Metering ausgeschlossen werden soll. Klicken Sie auf **OK**.

Hinweis: Sie können entweder den Plan HTTP oder HTTPS angeben. Interneteinschränkungen werden hierdurch nicht beeinträchtigt, aber im Internet Metering-Bericht auf PC-Ebene angezeigte Hyperlinks stellen mit Sicherheit einen Link zur richtigen Website her.

7. Übertragen Sie die gewählte URL in die Liste mit genehmigten oder eingeschränkten Sites, indem Sie auf Genehmigen oder Beschränken klicken oder die URL mit der Drag&&Drop-Funktion in die gewünschte Kategorie ziehen. Neben der URL in der Liste mit verfügbaren Sites wird ein passendes Symbol eingeblendet. Dieses zeigt an, ob das betreffende Objekt genehmigt oder eingeschränkt ist.
8. Um eine neue Site zur Liste mit genehmigten oder eingeschränkten Sites hinzuzufügen, klicken Sie auf in der Genehmigte oder Eingeschränkte Websites Liste, Wählen Sie **URL hinzufügen** und geben Sie die gewünschten Details ein. Die neue Website erscheint nun in der entsprechenden Website-Liste und wird außerdem automatisch zur Liste der Verfügbaren Websites hinzugefügt. Zum Löschen von URLs klicken Sie auf wählen **URL löschen**.
9. Jeder URL kann eine Sub-URL, die sich genehmigen oder einschränken lässt, zugewiesen werden.

Wählen Sie in der genehmigten oder eingeschränkten Liste die gewünschte URL und klicken Sie auf und wählen Sie **URL bearbeiten**. Das Dialogfeld „URL bearbeiten" wird eingeblendet.



10. Klicken Sie auf in der Liste „Verwaltete Sub-URLs" und wählen Sie **URL hinzufügen**. Geben Sie die Sub-URL ein und wählen Sie, ob Sie die URL genehmigen oder einschränken möchten. Klicken Sie auf **OK**. Die Sub-URL wird in der Liste mit genehmigten Sites angezeigt.
11. Klicken Sie auf **OK**.

Wählen Sie zum Betrachten vollständiger Daten zur Websitenutzung die gewünschte Website in der Liste „Verfügbare Sites" und klicken Sie auf die **Nutzungsschaltfläche**. Das Dialogfeld „Websitenutzung" wird eingeblendet. Hier sehen Sie, welche Benutzer auf die Website zugegriffen und wie oft sie diese besucht haben. Wenn Sie auf einen Benutzer klicken, erscheint eine vollständige Aufstellung der Zeiten und Dauer des Zugriffs auf die Website durch den betreffenden Benutzer.

Hinweis: Um URLs von der Anzeige in der Metering-Liste auszuschließen, klicken Sie die geforderte URL an, wählen **URL bearbeiten** und deaktivieren dann **Internet-Metering anzeigen**. Dies ist beispielsweise dann nützlich, wenn Sie URLs, deren Benutzung für Benutzer genehmigt ist, nicht anzeigen wollen.

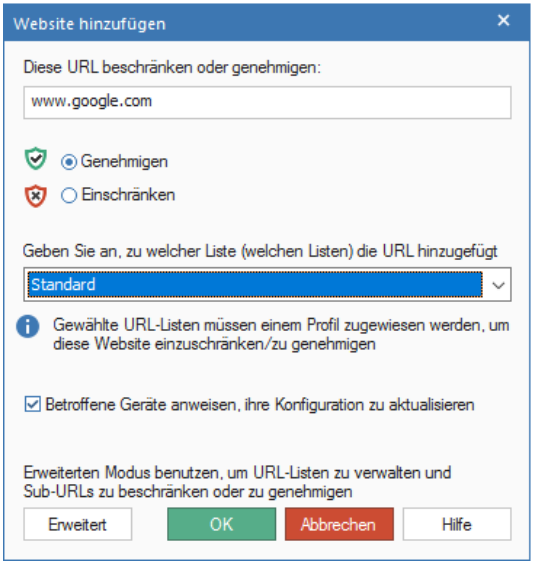
Einem Profil eine URL-Liste zuweisen
URL-Listen können jederzeit Profilen zugewiesen und aktiviert werden, wenn dies in den Internet-Metering-Einstellungen erforderlich ist.

1. Wählen Sie in der Einstellungen-Registerkarte **Existierende Profile verwalten**.
2. Wählen Sie das geforderte Profil in der Liste und klicken Sie auf **Einstellungen**.
3. Wählen Sie **Internet-Metering**.
4. Nun werden die Internet-Metering-Einstellungen angezeigt.
5. Wählen Sie die geforderte URL-Liste im URL-Listen-Dropdownmenü.
6. Damit die Liste aktiviert werden kann, muss die Internetzugriffsstufe auf eine der 'Eingeschränkter Internetzugriff' Optionen eingestellt sein. Oder, wenn benutzerdefinierter Zugriff benutzt wird, muss 'Genehmigte Websites' oder 'Eingeschränkte Websites blockieren' aktiviert sein.
7. Klicken Sie auf **Speichern,** um die Änderungen anzuwenden.

Benutzung der Spotlight-Funktion, um URLs einer Genehmigt- bzw. Eingeschränkt-Liste hinzuzufügen

Die Spotlight-Funktion, die in Explorer-Modus zur Verfügung steht, bietet eine schnelle und leichte Methode, URLs einer Genehmigt- bzw. Eingeschränkt-Liste zuzuweisen.

1. Wählen Sie im Menüband **Explorer-Modus**.
2. Wählen Sie ein Agent-Gerät im Informationsfenster oder in der Hierarchiestruktur.
3. Im Ansicht-Abschnitt des Menübands wählen Sie **Spotlight**. Daraufhin öffnet sich das Spotlight-Fensster, und es werden die Prozesse, Dienste, Anwendungen und Websites angezeigt, die gegenwärtig an dem gewählten Gerät ausgeführt werden.
4. Klicken Sie auf der **Websites** Registerkarte. Nun erscheint eine Liste der gegenwärtig geöffneten Websites.
5. Klicken Sie die geforderte Website mit der rechten Maustaste an und wählen Sie Website **einschränken** oder Website **genehmigen**.
6. Nun erscheint der **Website hinzufügen** Dialog.



- Kontrollieren Sie, dass die angezeigte URL korrekt ist und bestätigen Sie, ob die URL zu der zuvor gewählten Liste der Genehmigten URLs oder der Eingeschränkten URLs hinzugefügt werden soll.
- Wenn Sie mehrere URL-Listen für verschiedene Profile erstellt haben, wählen Sie die, zu der diese URL hinzugefügt werden soll.
- In der Standardeinstellung können Sie die betreffenen Geräte sofort mit der neuen URL-Liste aktualisieren. Wenn dies deaktiviert ist, werden die Änderungen angewendet, wenn die Agent-Geräte neu gestartet werden.
- Klicken Sie auf **OK**.

Die angegebene URL wird zu der entsprechenden Liste **Genehmigter** / **Eingeschränkter** URLs hinzugefügt.

Hinweis: Sie können schnell auf den URL-Listen Dialog zugreifen, indem Sie auf **Erweitert** klicken.

Anwendungsmetering

Das Anwendungs-Metering Modul berichtet über alle Anwendungen, die auf jedem PC oder Server benutzt werden, wobei die Zeiten, zu denen die Anwendungen geöffnet und geschlossen wurden, angegeben werden sowie die tatsächliche Zeiten, in denen sie aktiv waren.

Die Überwachung der Anwendungsnutzung gewährleistet, dass die Softwarelizenzen den richtigen Benutzern zugewiesen werden, und nur bei entsprechender Anwendungsaktivität für die Benutzer erneuert werden, was Kostenersparnisse ermöglicht.

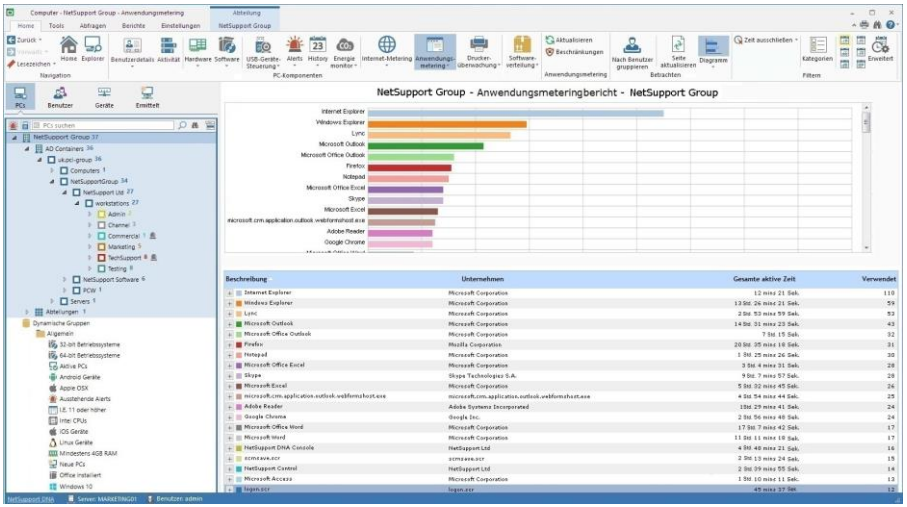
Die Anwendungsnutzung kann auch für Benutzer oder Abteilungen entweder ganz oder nur nach Tageszeit eingeschränkt werden. Listen mit genehmigten und eingeschränkten Anwendungen zusammen mit den Zeiten, zu denen die Einschränkungen gelten, können zentral erstellt und durchgesetzt werden.

Anwendungs-Metering ermöglicht es dem Unternehmen, die gegenwärtigen Lizenznutzungsraten für alle installierten Anwendungen zu überwachen und zu melden und sicherzustellen, dass die Anwendungsnutzung den Richtlinien des Unternehmens entspricht. Berichte können nach PC oder angemeldetem Benutzer erstellt werden.

Hinweis: Die Unternehmen Edition von NetSupport DNA bietet Anonymisiertes Anwendungs-Metering, das über alle Anwendungen berichtet, aber nicht auf Benutzerebene.

1. Klicken Sie im Ribbon auf das Symbol **Anwendungsmetering**. Das Fenster "Anwendungsmetering" wird eingeblendet.

   Hinweis: Wenn die Komponentensymbole ausgeblendet sind, klicken Sie auf die Registerkarte **Home**.



Die hierarchische Strukturansicht lässt sich zwischen PCs und Benutzern umschalten. Die Strukturansicht des PCs zeigt Daten für den PC-Eigentümer, der mit dem betreffenden PC verknüpft ist, und die Benutzerstrukturansicht zeigt Daten für angemeldete Benutzer.

Wählen Sie in der hierarchischen Strukturansicht die Ebene, auf der Sie die Meteringdaten betrachten möchten: Unternehmen, Abteilung, AD Container, dynamische Gruppe oder individueller Agent.

Im Informationsfenster ist ein Breakdown für jedes gewählte Objekt in Grafik- und Listenformat angezeigt. Um den Graph in einem anderen Format anzuzeigen, klicken Sie auf dem **Diagramm**-Symbol-Dropdownpfeil in der Menüleiste und wählen das entsprechende Format.

Um die aktive Ansicht auszudrucken, klicken Sie auf dem  Symbol oben auf der Konsole.

Hinweis: Durch Anklicken des Chart-Symbols im Ribbon wird die Grafik ein-/ausgeblendet.

Sie können die Daten für eine spezifische Zeitperiode betrachten. Um zwischen verschiedenen Zeitperioden hin- und herzuschalten, klicken Sie das entsprechende Symbol im Filterbereich des Menübands an. Wenn Sie auf Erweitert klicken, können Sie einen benutzerdefinierten Datum-/Zeitfilter anwenden. Aufgelistete Beschreibungen lassen sich erweitern, so dass Sie ein individuelles Agentbreakdown für jedes Objekt erhalten.

Anwendungen, die kürzer als eine angegebene Zeitspanne geöffnet waren, lassen sich ggf. ignorieren.

Wenn Sie **Nach Benutzer gruppieren** auswählen, können Sie die Anwendungsnutzung nach der Benutzer-ID von Agents statt dem PC betrachten. Diese Option ist in der Benutzerstrukturansicht nicht verfügbar.

Wenn Sie **Nach PC gruppieren** auswählen, können Sie die Applikationsnutzung nach PC-Details und nicht Benutzerdetails des Agents betrachten, während Sie sich in der Benutzerstrukturansicht befinden. Diese Option ist in der Strukturansicht des PCs nicht verfügbar.

Hinweis: Durch Auswahl verschiedener Ebenen in der Hierarchie-Struktur können Sie die Anwendungsnutzung von Agents auf PCs verschiedener Organisationsebenen betrachten.

Eine nützliche Art, eine spezifische Anwendungsnutzung anzuvisieren und die Menge der angezeigten Daten zu beschränken, ist die Gruppierung 'ähnlicher' Anwendungen in Kategorien. Wenn Sie z. B. herausfinden möchten, wie viel Zeit mit dem Spielen von Solitaire verbracht wird, können Sie eine Gruppe erstellen, die Spiele enthält. Weitere Angaben hierzu finden Sie unter "Anwendungsgruppen". Um eine Kategorie zu zeigen, klicken Sie auf dem Diagramm-Symbol-Dropdownpfeil im Menüband und wählen Kategorien. Wählen Sie die Gruppe, die Sie anzeigen möchten, und klicken Sie auf **OK**. Das Informationsfenster zeigt jetzt nur die Daten für diese Kategorie. Eine gelbe Kopfzeile zeigt an, welche Kategorie Sie gerade betrachten. Sie können zwischen Kategorien wechseln und Kategorien von hier aus löschen.

Mit einer Schnellaktualisierungsfunktion können Sie Daten außerhalb der angegebenen Häufigkeit aktualisieren. Dies kann nützlich sein, wenn Sie bestimmte Agents oder Abteilungen anpeilen möchten. Klicken Sie mit der rechten Maustaste auf das gewünschte Objekt in der Strukturansicht und wählen Sie „Aktualisieren" oder klicken Sie im Menü oder dem Ribbon „Anwendungen" auf „Aktualisieren".

Abfragen

Wählen Sie zur Anzeige des Abfragefensters die Registerkarte „Abfragen".

Mit dem Abfragetool von DNA können Sie Datenbankeinträge abrufen, die bestimmte Kriterien erfüllen. Abfragen zu der Komponente, die gerade betrachtet wird, sind aufgelistet, was ein schnelles Abrufen der Ergebnisse ermöglicht.

Klicken Sie in der Menüleiste auf dem Abfrage hinzufügen Symbol, um eine neue Abfrage zu erstellen, oder klicken Sie auf dem Abfrage bearbeiten Symbol in der Menüleiste, um ein in der Liste vorhandenes Objekt zu bearbeiten.

Berichte

Wählen Sie zur Anzeige des Berichtfensters die Registerkarte „Berichte".

Jeder Komponente ist eine Reihe von vordefinierten Managementberichten, die vom Crystal Reports-Modul gespeist werden, beigefügt. Wählen Sie den geforderten Bericht in der Dropdown-Liste. Die Ergebnisse erscheinen im Informationsfenster. Sie lassen sich ggf. exportieren.

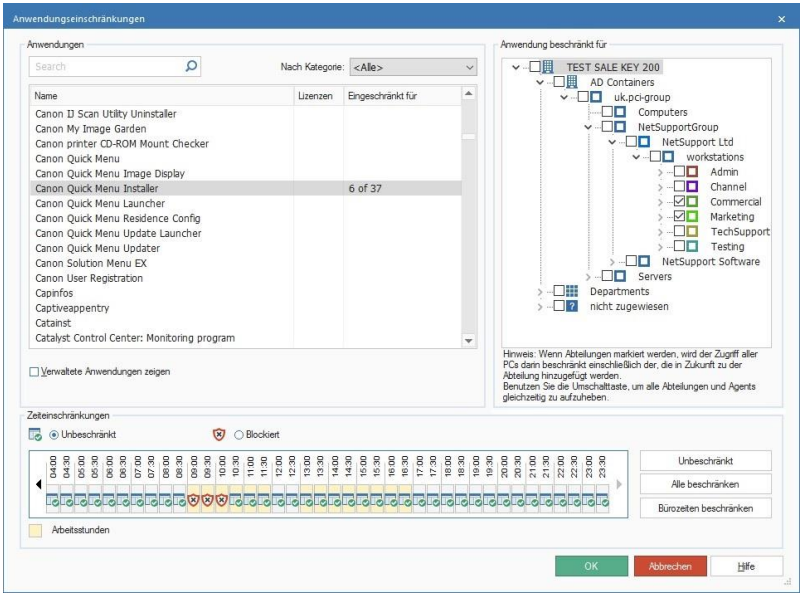
Hinweise:

- Die Häufigkeit, mit der der Server Daten sammelt, lässt sich mit der Option "DNA-Einstellungen" ändern.
- Das in der Konsole angezeigte Datum-/Zeitformat stimmt mit dem Format in dem Rechner, in dem der DNA Server installiert ist, überein. Um das Format in der Konsole zu ändern, müssen Sie zunächst das Format in diesem Rechner ändern. Für weitere Informationen wenden Sie sich bitte an unser Support-Team www.netsupportsoftware.com/support.

Anwendungseinschränkungen

Um sicherzustellen, dass die Anwendungsnutzung Ihrer Firmenpolitik entspricht, können Sie Listen mit genehmigten oder beschränkten Anwendungen erstellen und Zeitrahmen für die Gültigkeit dieser Einschränkungen festlegen.

1. Klicken Sie auf den Dropdownpfeil des Symbols **Anwendungsmetering** und wählen Sie im Menü die Option {Einschränkungen}.
   Oder
   Klicken Sie auf das Symbol **Einschränkungen** der Anwendungsmeteringgruppe.
2. Das Dialogfeld "Anwendungseinschränkungen" wird eingeblendet.



Es wird eine Liste aller Anwendungen mit Lizenzdetails und der Anzahl Agents, für die die Anwendung genehmigt oder eingeschränkt ist, eingeblendet.

Hinweis: Die Lizenzinformationen werden nur dann eingeblendet, wenn die Anwendungsgruppe im Dialogfeld „Anwendungsgruppe bearbeiten" dem relevanten installierten Programm zugewiesen wurde.

Suche
Sie können schnell nach Anwendungen suchen, indem Sie sie in das Suchfeld eingeben und auf klicken.

Nach Kategorie
Zum Betrachten von zusammen gruppierten Anwendungen wählen Sie die gewünschte Kategorie in der Dropdownliste.

Hinweis: Im Anwendungsgruppen-Dialog können Kategorien erstellt werden.

Verwaltete Anwendungen zeigen
Wenn diese Option markiert ist, können Sie auf einen Blick sehen, welche Anwendungen bereits eingeschränkt sind und auf welche Benutzer sich dies bezieht. Alle Anwendungen mit verfügbaren Lizenzdetails werden ebenfalls angezeigt.

Wenn diese Option nicht markiert ist, wird eine vollständige Liste mit gescannten Anwendungen eingeblendet, in der Sie auswählen können, welche Anwendungen Sie einschränken möchten.

Um Beschränkungen einzustellen
1. Markieren Sie die gewünschte Anwendung in der Liste. Das Anwendung beschränkt für Fenster listet die Strukturansicht auf.
2. Um die Benutzung einer Anwendung für bestimmte Agents zu beschränken, versehen Sie den geforderten PC in der Strukturansicht mit einem Häkchen. Wenn Sie eine Abteilung anhaken, wird die Anwendung für alle PCs in dieser Abteilung beschränkt (einschließlich neuer PCs, die in Zukunft hinzugefügt oder versetzt werden).
3. Sie können wählen, den Zugriff während bestimmter Tageszeiten zu beschränken. Wählen Sie Blockiert, scrollen Sie dann mit den Pfeiltasten zum gewünschten Zeitrahmen und klicken Sie auf dem Segment, um die Beschränkung anzuwenden. Für unbeschränkten Zugriff wählen Sie Unbeschränkt.
4. Wenn Sie auf **Unbeschränkt** klicken, lassen Sie damit unbeschränkten Zugriff für den ganzen Tag zu. Wenn Sie auf **Bürostunden einschränken** klicken, wird der Zugriff nur während der **Bürostunden eingeschränkt**.

Hinweis: Die gegenwärtigen Bürostunden werden gelb schattiert sein. Sie können in Konsolenanpassungen – Allgemein-Einstellungen für Ihre Organisation passend geändert werden.

5. Im Fenster "Anwendungsliste" sehen Sie, für wie viele Agents die Einschränkung gilt. Klicken Sie auf **OK**, um die Details zu speichern.

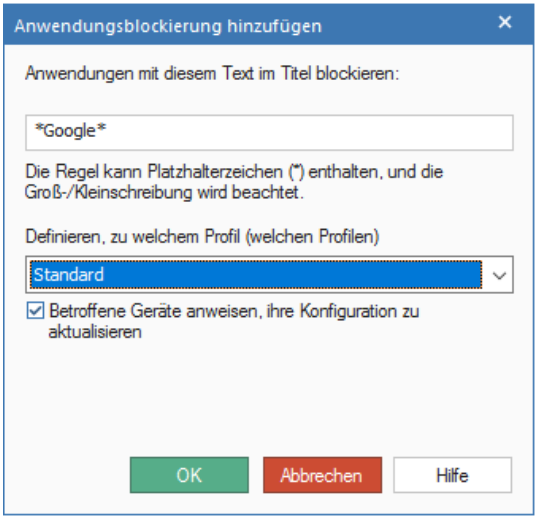
Um Beschränkungen anzuwenden

1. In der Einstellungen-Registerkarte wählen Sie **Vorhandene Profile verwalten**.
2. Wählen Sie das geforderte Profil in der Liste und klicken Sie auf **Einstellungen**.
3. Wählen Sie **Anwendungsmetering**.
4. Die Anwendungsmetering-Einstellungen werden nun angezeigt.
5. Klicken Sie unter **Unternehmensanwendungsbeschränkungen** auf Aktivieren.
6. Klicken Sie auf **Speichern**.
7. Die Anwendungsbeschränkungen, die Sie erstellt haben, werden auf die gesamte Organisation angewendet.

Anwendungen nach Fenstertitel blockieren

Sie können Anwendungen jetzt nicht nur nach ihren Namen sondern auch nach Fenstertitel blockieren. Die Spotlight-Funktion, die in Explorer-Modus zur Verfügung steht, bietet eine schnelle und leichte Methode, gegenwärtig ausgeführte Anwendungen zu den Titelblockierung-Einstellungen hinzuzufügen:

1. Wählen Sie im Menüband **Explorer-Modus**.
2. Wählen Sie ein Agent-Gerät im Informationsfenster.
3. Im Ansicht-Abschnitt des Menübands wählen Sie **Spotlight**. Nun öffnet sich das Spotlight-Fenster, und es werden die Prozesse, Dienste, Anwendungen und Websites angezeigt, die gegenwärtig an dem gewählten Gerät ausgeführt werden.
4. Klicken Sie auf der **Anwendungen** Registerkarte.
5. Klicken Sie geforderte Anwendung mit der rechten Maustaste an und wählen Sie **Blockieren**. (Sie können die Anwendung auch Schließen, wenn Sie das vorziehen.)
6. Nun erscheint der **Anwendungsblockierung hinzufügen** Dialog.



7. Daraufhin erscheint der Fenstertitel der gegenwärtig ausgeführten Anwendung. Um sicherzustellen, dass alle Anwendungen mit ähnlichen Titeln blockiert werden, können Sie den Titel bearbeiten und Platzhalterzeichen verwenden.
8. Wählen Sie in der Dropdownliste das Profil, auf das diese Beschränkung angewendet werden soll.
9. In der Standardeinstellung können Sie die betreffenen Geräte sofort mit der aktualisierten Blockiert-Liste aktualisieren. Wenn dies deaktiviert ist, werden die Änderungen angewendet, wenn die Agent-Geräte neu gestartet werden.
10. Klicken Sie auf OK.
11. Die Anwendung wird nun zu den **Titelblockierung-Einstellungen** hinzugefügt.

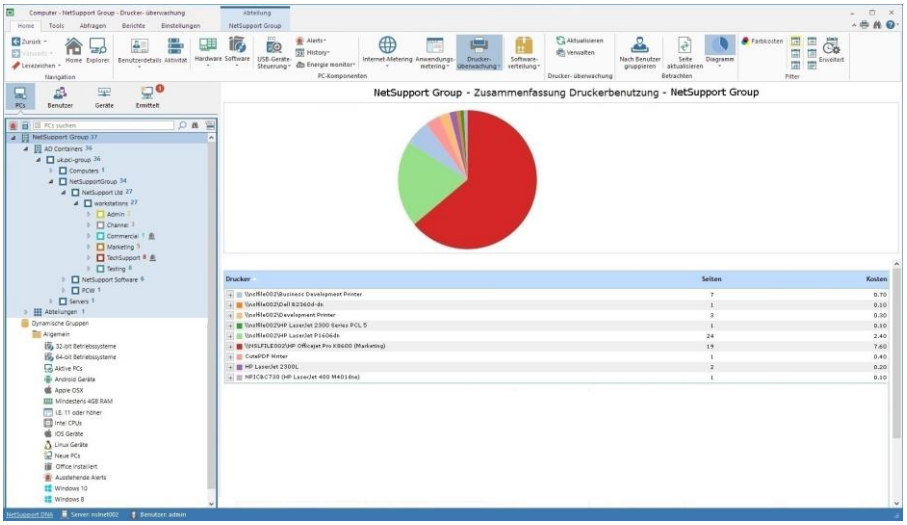
Druckerüberwachung

NetSupport DNA enthält eine Druckerüberwachungsfunktion auf hoher Ebene. Individuelle Drucker im ganzen Unternehmen werden automatisch identifiziert und die Kosten für das Drucken (Schwarzweiß, Farbe usw.) können von der zentralen Konsolenansicht aus entweder global oder für jeden einzelnen Drucker zugewiesen werden. Falls erforderlich, können Drucker auch aus der Ansicht ausgelassen werden. NetSupport DNA bietet einen vollen Überblick der Druckeraktivitäten und angezeigten Kosten für das gesamte Unternehmen.

Hinweis: Die Druckerüberwachung basiert auf Druckerbenachrichtigungen, die zum DNA Agent zurückgesandt werden und diesem melden, was gedruckt worden ist. Eine Druckerumgebung, in der dies verhindert wird, oder in der die Identifizierung von Druckeraufträgen in Benachrichtigungen modifiziert worden ist, kann zu unerwarteten Ergebnissen führen. Dies kann beispielsweise der Fall sein, wenn die Authentifizierung an einen Druckerserver andere Anmeldeinformationen benutzt als den Benutzernamen, mit dem der Benutzer sich angemeldet hat, wenn das Drucken an Servern in einer anderen Domäne ausgeführt wird, oder wenn die Druckerbenachrichtigungen von Firewalls oder Proxyservern blockiert werden.

1. Klicken Sie das **Druckerüberwachung** Symbol im Menüband an. Nun erscheint das Druckerüberwachung-Fenster.

   Hinweis: Wenn die Komponentensymbole ausgeblendet sind, klicken Sie auf die Registerkarte **Home**.



Wählen Sie in der hierarchischen Strukturansicht die Ebene, auf der Sie die Meteringdaten betrachten möchten: Unternehmen, Abteilung, AD Container, dynamische Gruppe oder individueller Agent.

Im Informationsfenster ist ein Breakdown für jedes gewählte Objekt in Grafik- und Listenformat angezeigt. Um den Graph in einem anderen Format anzuzeigen, klicken Sie auf dem Diagramm-Symbol-Dropdownpfeil in der Menüleiste und wählen das entsprechende Format.

Um die aktive Ansicht auszudrucken, klicken Sie auf dem  Symbol oben auf der Konsole.

Hinweis: Durch Anklicken des Chart-Symbols im Ribbon wird die Grafik ein-/ausgeblendet.

Sie können die Daten für eine spezifische Zeitperiode betrachten. Um zwischen verschiedenen Zeitperioden hin- und herzuschalten, klicken Sie das entsprechende Symbol im Filterbereich des Menübands an. Wenn Sie auf Erweitert klicken, können Sie einen benutzerdefinierten Datum-/Zeitfilter anwenden. Aufgelistete Beschreibungen lassen sich erweitern, so dass Sie ein individuelles Agentbreakdown für jedes Objekt erhalten.

Die gezeigten Arbeitsstunden können im DNA Konfigurationskatalog für Ihre Organisation angepasst werden. Siehe Konsolenanpassungen – Allgemein für weitere Informationen.

Wenn Sie Nach Benutzer gruppieren auswählen, können Sie die Druckersnutzung nach der Benutzer-ID von Agents statt dem PC betrachten. Diese Option ist in der Benutzerstrukturansicht nicht verfügbar.

Wenn Sie Nach PC gruppieren auswählen, können Sie die Druckersnutzung nach PC-Details und nicht Benutzerdetails des Agents betrachten, während Sie sich in der Benutzerstrukturansicht befinden. Diese Option ist in der Strukturansicht des PCs nicht verfügbar.

In der Standardeinstellung werden alle Druckarten aufgelistet. Sie können nur die Farbdruckkosten anzeigen, indem Sie Farbkosten im Menüband anklicken.

Um die Kosteneinstellungen für das Drucken zu konfigurieren, wählen Sie die Druckerüberwachung Symbol-Dropdownliste und wählen dann {Verwalten} oder klicken Sie auf dem Verwalten Symbol im Menüband.

Dies kann nützlich sein, um auf bestimmte Agents oder Abteilungen zu fokussieren. Klicken Sie das geforderte Objekt in der Strukturansicht rechts an und wählen Sie Update, oder klicken Sie im Druckerüberwachung Symbol-Dropdownmenü oder im Menüband auf Update.

Abfragen
Wählen Sie zur Anzeige des Abfragefensters die Registerkarte „Abfragen".

Mit dem Abfragetool von DNA können Sie Datenbankeinträge abrufen, die bestimmte Kriterien erfüllen. Abfragen zu der Komponente, die gerade betrachtet wird, sind aufgelistet, was ein schnelles Abrufen der Ergebnisse ermöglicht.

Klicken Sie in der Menüleiste auf dem Abfrage hinzufügen Symbol, um eine neue Abfrage zu erstellen, oder klicken Sie auf dem Abfrage bearbeiten Symbol in der Menüleiste, um ein in der Liste vorhandenes Objekt zu bearbeiten.

Berichte
Wählen Sie zur Anzeige des Berichtfensters die Registerkarte „Berichte".

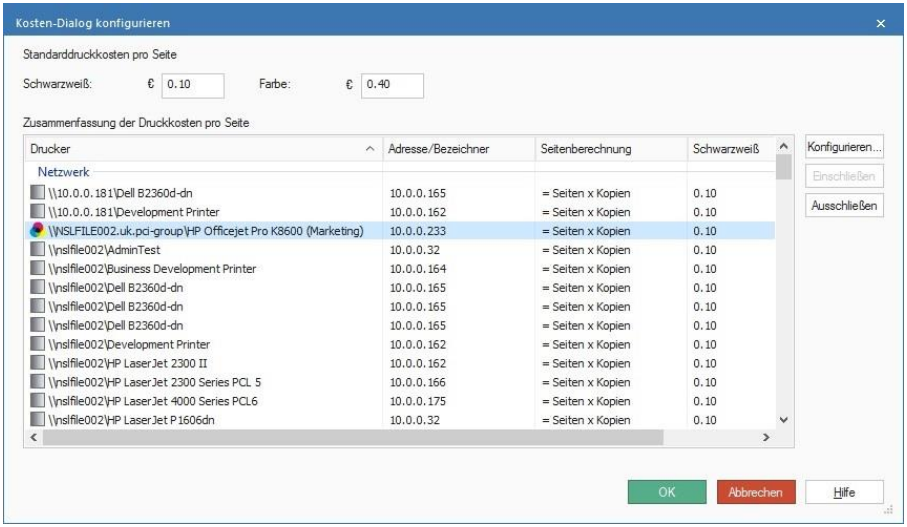
Jeder Komponente ist eine Reihe von vordefinierten Managementberichten, die vom Crystal Reports-Modul gespeist werden, beigefügt. Wählen Sie den geforderten Bericht in der Dropdown-Liste.

Die Ergebnisse erscheinen im Informationsfenster. Sie lassen sich ggf. exportieren.

Druckkosten konfigurieren

Dieser Dialog zeigt alle Drucker im gesamten Unternehmen. Von hier aus können Sie Drucker ausschließen, die nicht überwacht werden sollen, sowie auch die mit dem Drucken verbundenen Kosten einstellen und konfigurieren.

1. Wählen Sie die Druckerüberwachung Symbol-Dropdownliste und wählen dann {Verwalten}.
   Oder
   Klicken Sie auf dem **Verwalten** Symbol im Menüband.



Es wird eine Zusammenfassung aller Drucker in der Gesellschaft aufgelistet mit einem Bezeichner, der angibt, ob es sich um einen Schwarzweiß- oder einen Farbdrucker handelt. In der Standardeinstellung werden alle Drucker für die Überwachung im Informationsfenster in die Liste aufgenommen. Sie können Drucker, die Sie nicht überwachen möchten, ausschließen, indem Sie auf **Ausschließen** klicken. Um alle Drucker mit demselben Namen auszuschließen (dies kann nützlich sein, wenn Sie alle Instanzen von Adobe PDF ausschließen möchten), klicken Sie den geforderten Druckernamen rechts an und wählen Sie Alle 'xxx' aus der Liste ausschließen.

Hinweis: Drucker, die ausgeschlossen werden, werden in einen Ausgeschlossen-Bereich unten auf der Druckerliste verschoben und können von dort aus wieder aufgenommen werden.

In der Normaleinstellung sind die Druckkosten pro Seite auf €0.10 für Schwarzweiß und €0.40 für Farbdruck eingestellt. Überschreiben Sie dies, um die Kosten zu ändern.

Wenn Sie die Kosten hier ändern, werden sie für alle Drucker geändert. Sie können die Kosten für individuelle Drucker ändern, indem Sie den Drucker wählen und dann auf **Konfigurieren** klicken.

Hinweis: Wenn Schwarzweiß-Dokumente auf einem Farbdrucker gedruckt werden, werden sie zu Farbdruckkosten berechnet, außer wenn der Benutzer die Grauskala gewählt hat.

Softwareverteilung

DNA bietet eine mehrfache Lieferungsoption für die Softwareverteilung, was zeitgerechte und kostengünstige Anwendungsdeployments im ganzen Unternehmen ermöglicht. Ein Bediener definiert ein Softwarepaket, das eine Sammlung der Dateien oder Ordner, die verteilt werden sollen, enthält. Nachdem das Paket erstellt ist, kann es automatisch an Ziel-PCs verteilt oder zentral "veröffentlicht/angeboten" werden, damit Benutzer auf Verlangen darauf zugreifen und es installieren können. Definierte Pakete lassen sich auch für die Verteilung zu bestimmten Zeitpunkten "planen".

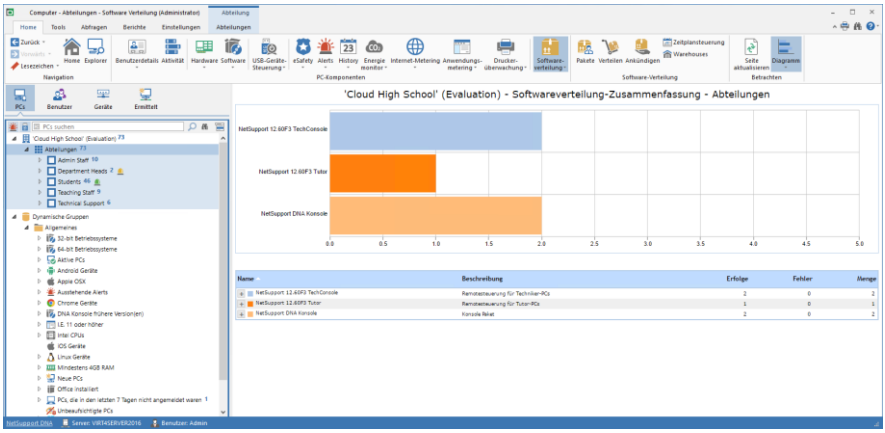
Es lassen sich auch Aktionsparameter in das Paket aufnehmen, was es Ihnen zum Beispiel ermöglicht, alle während der Anwendungsinstallation erforderlichen Eingabeaufforderungen an den Benutzer einzubauen, so dass sich das Paket dann ohne Eingriffe an das System eines Benutzers verteilen lässt.

Beim Planen einer Deploy-Funktion können Sie die Hardware- und Softwareinventarisierungsfeatures von DNA verwenden, um den aktuellen Inventarstatus in Ihrer Organisation zu beurteilen und so die Kompatibilität zu gewährleisten. Ähnlich konfigurierte Systeme lassen sich zusammen gruppieren, um eine möglichst effiziente Einführung zu gewährleisten.

DNA berücksichtigt auch die Auswirkungen, die ein Deploy großer Pakete im ganzen Netzwerk haben kann. Netzwerkoverheads wachsen natürlich, während Pakete vom DNA Server an mehrere Agentcomputer verteilt werden. Damit die Überlastung weniger akut wird, können Sie in der Nähe der Agentcomputer ein "Verteilungswarehouse" erstellen. Das Paket wird an das Warehouse gesendet und genannte Agents werden dann von diesem lokalen "Server" aus bedient.

1. Klicken Sie im Ribbon auf das **Software-Verteilungssymbol**. Das Fenster „Softwareverteilung“ wird eingeblendet.

   Hinweis: Wenn die Komponentensymbole ausgeblendet sind, klicken Sie auf die Registerkarte **Home**.



Wählen Sie in der hierarchischen Strukturansicht die Ebene, auf der Sie die Verteilungsdaten betrachten möchten: Unternehmen, Abteilung, AD Container, dynamische Gruppe oder individueller Agent.

Im Hauptinformationsfenster ist ein Breakdown der verteilten Pakete für jedes gewählte Objekt in Grafik- und Listenformat angezeigt. Um den Graph in einem anderen Format anzuzeigen, klicken Sie auf dem **Diagramm**-Symbol-Dropdownpfeil in der Menüleiste und wählen das entsprechende Format. Um die aktive Ansicht auszudrucken, klicken Sie auf dem  Symbol oben auf der Konsole.

Hinweis: Durch Anklicken des Chart-Symbols im Ribbon wird die Grafik ein-/ausgeblendet.

Für jedes aufgeführte Paket wird eine Reihe von erfolgreichen oder gescheiterten Verteilungen bereitgestellt. Die Drilldownlisten lassen sich erweitern, so dass Sie ein individuelles Agentbreakdown für jedes Objekt erhalten.

Hinweis: Das in der Konsole angezeigte Datum-/Zeitformat stimmt mit dem Format in dem Rechner, in dem der DNA Server installiert ist, überein. Um das Format in der Konsole zu ändern, müssen Sie zunächst das Format in diesem Rechner ändern. Für weitere Informationen wenden Sie sich bitte an unser Support-Team www.netsupportsoftware.com/support.

Abfragen

Wählen Sie zur Anzeige des Abfragefensters die Registerkarte „Abfragen".

Mit dem Abfragetool von DNA können Sie Datenbankeinträge abrufen, die bestimmte Kriterien erfüllen. Abfragen zu der Komponente, die gerade betrachtet wird, sind aufgelistet, was ein schnelles Abrufen der Ergebnisse ermöglicht.

Klicken Sie in der Menüleiste auf dem **Abfrage hinzufügen** Symbol, um eine neue Abfrage zu erstellen, oder klicken Sie auf dem **Abfrage bearbeiten** Symbol in der Menüleiste, um ein in der Liste vorhandenes Objekt zu bearbeiten.

Berichte

Wählen Sie zur Anzeige des Berichtfensters die Registerkarte „Berichte".

Jeder Komponente ist eine Reihe von vordefinierten Managementberichten, die vom Crystal Reports-Modul gespeist werden, beigefügt. Wählen Sie den geforderten Bericht in der Dropdown-Liste. Die Ergebnisse erscheinen im Informationsfenster. Sie lassen sich ggf. exportieren.

Paketverwaltung

1. Klicken Sie auf den Dropdownpfeil des Software-Verteilungssymbols und wählen Sie im Menü die Option {Paketverwaltung}.

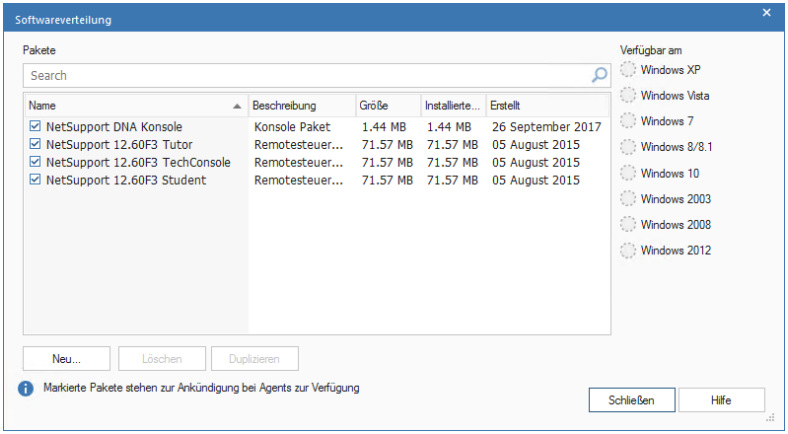
   Oder

   Klicken Sie auf das Symbol **Pakete** der Software-Verteilungsgruppe.

   Oder

   Klicken Sie in der Registerkarte **Werkzeuge** auf das Symbol **Paketverwaltung**.

2. Das Dialogfeld "Paketverwaltung" wird eingeblendet. Hier sind Angaben zu vorhandenen Paketen aufgeführt. Alle, die markiert sind, werden auf Agent PCs angeboten.



3. Klicken Sie auf **Neu**, um zusätzliche Pakete zur Verteilung zu erstellen.

   Oder

   Klicken Sie auf **Löschen**, wenn ein Paket in der Liste nicht mehr benötigt wird.

   Oder

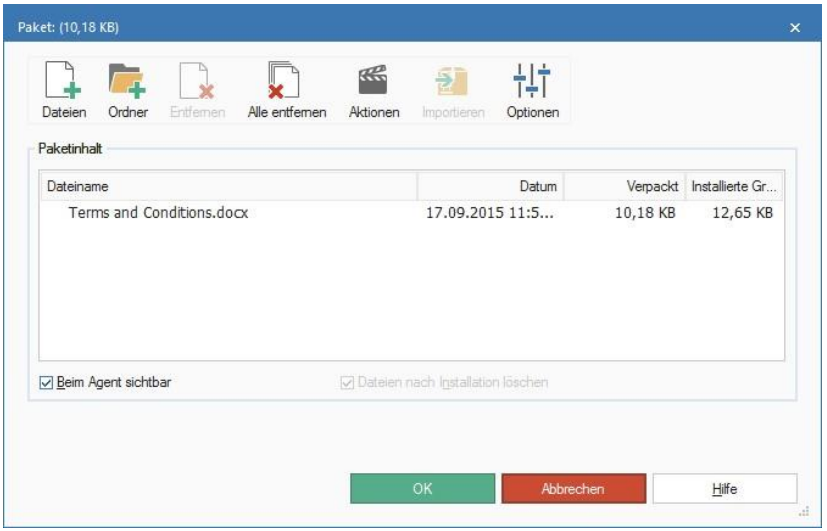
   Klicken Sie auf **Duplizieren**, um eine Kopie eines vorhandenen Pakets anzufertigen. Dies kann nützlich sein, wenn Sie dasselbe Paket mit zusätzlichen Parametern verteilen möchten. Die geänderte Version wird zur Liste hinzugefügt.

Verfügbar am

Zeigt die unterstützten Betriebssysteme für die einzelnen Pakete an. Dies lässt sich beim Erstellen eines neuen Pakets angeben.

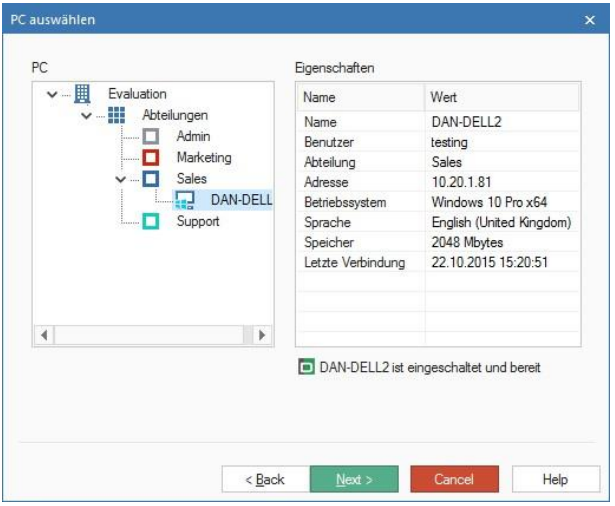
Neues Paket erstellen

In diesem Dialogfeld können Sie angeben, welche Dateien/Ordner und zusätzlichen Aktionsparameter in das Paket eingeschlossen werden sollen.



1. Wählen Sie Dateien oder Ordner und suchen Sie die Datei(en), die in ein Paket zur Verteilung integriert werden sollen. Die Datei wird in der Liste "Paketinhalt" eingeblendet.
2. Markieren Sie das Paket und klicken Sie auf **Aktionen**, um die gewünschten Parameter/Befehlszeilenanleitungen hinzuzufügen. Diese werden ausgeführt, wenn das verteilte Pakte auf Agent PCs eintrifft. Es sind auch verschiedene vordefinierte Parameter verfügbar, einschließlich des **Kopierbefehls**, der zum Kopieren von Dateien, wie z. B. Bildern, aus ihrem ursprünglichen Speicherort in den angegebenen Zielordner dient. Klicken Sie auf **OK**.
3. Klicken Sie auf **Optionen** und entscheiden Sie, ob das Paket mit dem Standardadministrationskonto von NetSupport DNA verteilt werden soll oder mit einem in Ihrer Domäne existierenden Admin-Benutzernamen und Passwort.

4. Wählen Sie **Beim Agent sichtbar**, wenn Sie dieses Paket zum Anbieten an Agents verfügbar machen möchten (gilt nur für Abteilungen und Unternehmen).
5. Nach der Installation lassen sich die Paketsetupdateien von dem/den Agentcomputer(n) entfernen. Wählen Sie **Dateien nach der Installation löschen**.
6. Klicken Sie auf **OK**.
7. Das Dialogfeld "Paket testen" wird eingeblendet. Bevor Sie das Paket speichern, können Sie seine Zuverlässigkeit testen oder, wenn Sie zufrieden sind, klicken Sie auf **Paket speichern**.



8. Geben Sie einen Namen und eine Beschreibung für das Paket ein. Sie können auch angeben, welche Betriebssysteme von dem Paket unterstützt werden. Standardmäßig sind alle ausgewählt. Agents, die nicht mit den angegebenen Betriebssystemen übereinstimmen, werden aus der Verteilung ausgeschlossen. Klicken Sie zur Bestätigung auf **Fertig stellen**. Das Paket wird verteilungsbereit an den Server gesendet.

Mit der Importfunktion können Sie Pakete zur Bearbeitung vom Server abrufen.

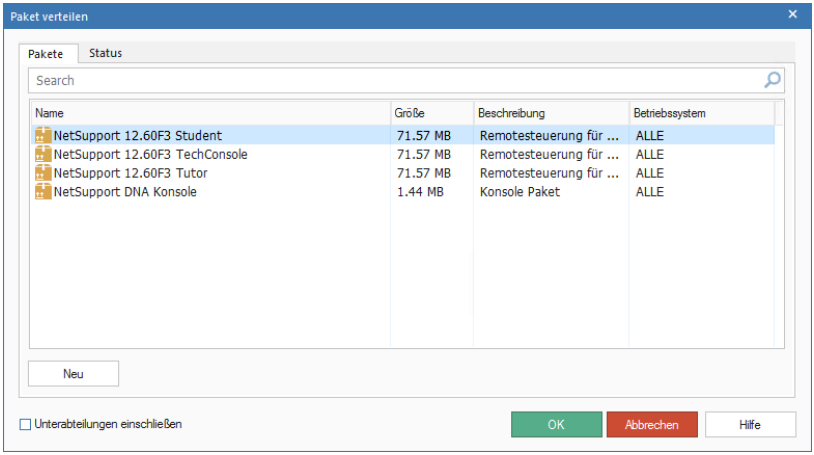
Verteilen eines Pakets

Nachdem Sie das gewünschte Paket erstellt haben, kann dieses an gewählte Agents verteilt werden.

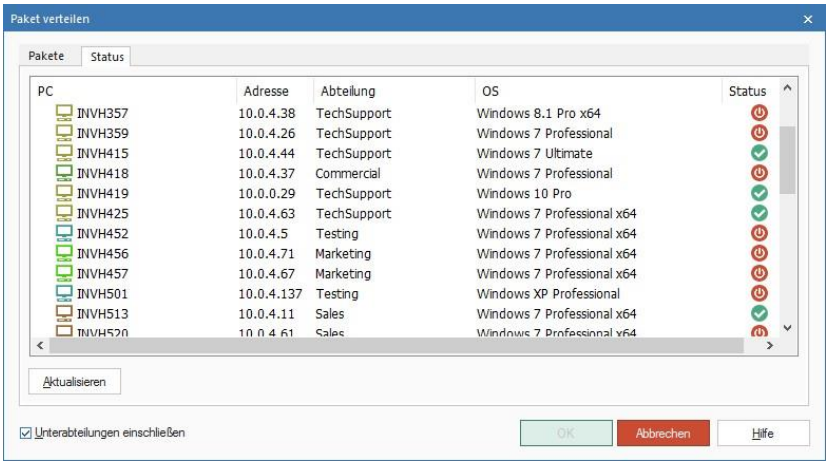
1. Markieren Sie in der Strukturansicht den Agent, die Abteilung, die AD Container, die dynamische Gruppe oder das Unternehmen, an die Sie das Paket verteilen möchten.
2. Klicken Sie mit der rechten Maustaste and wählen Sie **Verteilen**.

   Oder

   Klicken Sie auf den Dropdownpfeil des Software-Verteilungssymbols und wählen Sie im Menü die Option {Verteilen}.
   Oder
   Klicken Sie auf das Symbol **Verteilen** in der Software-Verteilungsgruppe.



3. Alle vorher erstellten Pakete sind aufgeführt. Markieren Sie die gewünschte Datei. Wenn das gewünschte Paket nicht verfügbar ist, können Sie es von hier aus erstellen. Klicken Sie auf **Neu**.
4. Wenn Sie an ein Unternehmen, eine Abteilung oder eine AD Container verteilen, stellen Sie sicher, dass das Feld Unterabteilungen einschließen markiert ist, wenn Sie alle Abteilungen/Agents im betreffenden Bereich einschließen möchten.
5. Bevor Sie fortfahren, können Sie den Status der PCs, an die Sie verteilen werden, überprüfen. Dies zeigt an, ob die PCs verfügbar (grün), nicht verfügbar (rot) oder abgemeldet (gelb) sind.

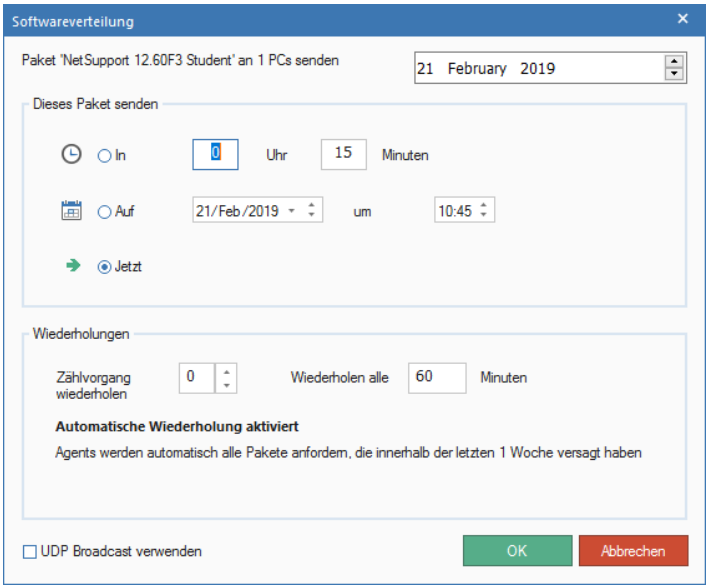


6. Klicken Sie auf **OK**. Das Dialogfeld "Verteilung planen" wird eingeblendet. Geben Sie an, ob das Paket sofort oder zu einem bestimmten Datum/Zeitpunkt verteilt werden soll. Spätere Verteilungen lassen sich im Dialogfeld "Pakete planen" betrachten. Sie können mehrere Wiederholungsversuche einstellen, falls die Verteilung fehlschlägt, und das Intervall zwischen den Wiederholungsversuchen lässt sich ebenfalls festlegen.

   Ferner ermöglicht die automatische Wiederholungsfunktion den Umgang mit gescheiterten Verteilungen für PCs, die zum Sendezeitpunkt der Verteilung abgeschaltet oder nicht verfügbar sind. Mit der NetSupport DNA Einstellungen-Option können Sie automatische erneute Versuche aktivieren/deaktivieren und die Zeitperiode festlegen, für die versagte Pakete noch auf automatische Anforderung für Agents zur Verfügung stehen sollen.

   Für eine Verteilung mit der Broadcast-Methode wählen Sie ggf. die Option **UDP Broadcast verwenden**.

Hinweis:	Bei Verwendung der Broadcast-Verteilungsmethode müssen sich die PCs im gleichen Teilnetz wie der DNA Server befinden, da sonst die Verteilung fehlschlägt.



7. Klicken Sie auf **OK**, um das Paket zu verteilen. Die Ergebnisse werden im Verteilungsfenster eingeblendet.

Hinweis: Bei der Erstellung eines Pakets können Sie bestimmen, welche Anmeldeinformationen (Benutzername und Passwort) benutzt werden, wenn das Paket an einen Agent gesendet wird. Wenn keine Anmeldeinformationen angegeben werden, benutzt NetSupport DNA die Standard-'SYSTEM'-Anmeldeinformationen (empfohlen), die vollen Zugriff für die Installation der MSI Installer bieten und die lokalen Dateien des Agents ändern. Wenn das Paket spezifische Anmeldeinformationen erfordert, beispielsweise für den Zugriff auf eine Netzwerkressource, können Sie diese eingeben.

Wenn ein Paket gesendet wird und ein Benutzer beim Agent angemeldet ist:

- Werden die bereitgestellten Anmeldeinformationen benutzt, um alle Teile des Pakets auszuführen.
- Wenn die Anmeldeinformationen unrichtig sind, wird das Paket nicht ausgeführt, und NetSupport DNA meldet den Fehler.

Wenn ein Paket gesendet wird und der Agent abgemeldet ist:

- Werden die bereitgestellten Anmeldeinformationen nur benutzt, wenn Zugriff auf Netzwerkressourcen erforderlich ist. Für alle anderen Elemente des Pakets werden die Standardanmeldeinformationen benutzen.
- Wenn die Anmeldeinformationen unrichtig sind, wird das Paket nicht ausgeführt, und NetSupport DNA wird den Fehler nicht melden.

Planen eines Pakets

Beim Erstellen eines Pakets, das Sie verteilen möchten, lässt sich die Verteilung für ein bestimmtes Datum oder einen Zeitpunkt planen. Das ist besonders nützlich, wenn Sie Dateien außerhalb der Bürozeiten verteilen wollen. Dieses Dialogfeld dient zum Bearbeiten der Eigenschaften geplanter Verteilungen oder dem Erstellen neuer Zeitpläne.

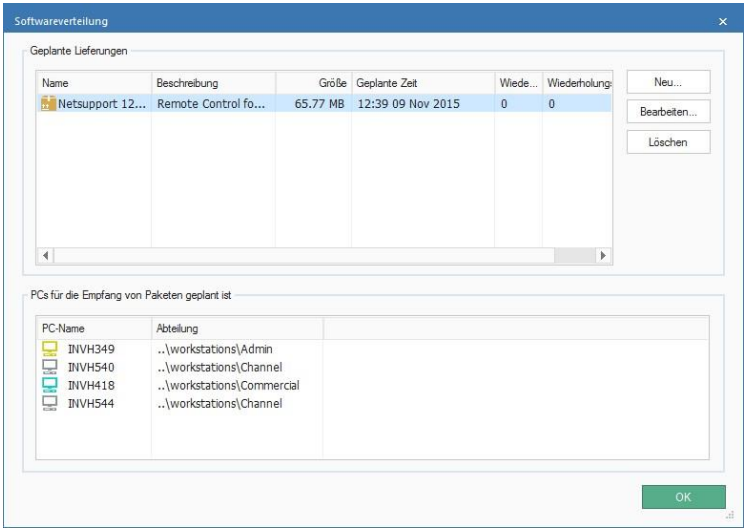
1. Während die Registerkarte "Softwareverteilung" ausgewählt ist, markieren Sie einen Agent, eine Abteilung, eine AD Container, eine dynamische Gruppe oder ein Unternehmen in der Strukturansicht.
2. Klicken Sie mit der rechten Maustaste und wählen **Zeitplansteuerung**.

   Oder

   Klicken Sie auf den Dropdownpfeil des Software-Verteilungssymbols und wählen Sie im Menü die Option {Zeitplansteuerung}.

   Oder

   Klicken Sie auf das Symbol **Zeitplansteuerung** in der Software-Verteilungsgruppe.
3. Das Dialogfeld "Geplante Pakete" wird eingeblendet, sowie Details für alle Pakete, deren Verteilung Sie geplant haben und die Namen aller Agents, die den Paketen zugeordnet sind.

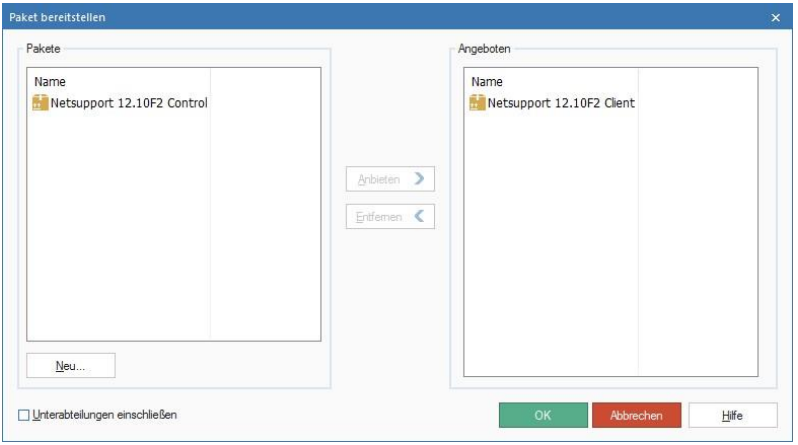


4. Klicken Sie auf **Neu**, um einen Verteilungsplan zu erstellen.
   Oder
   klicken Sie auf **Bearbeiten**, um die Verteilungsdetails eines vorhandenen geplanten Pakets zu ändern.
   Oder
   klicken Sie auf **Löschen**, wenn ein Paket in der Liste nicht mehr verteilt werden soll.
5. Klicken Sie auf **OK**, wenn Sie fertig sind.

Anbieten eines Pakets

Das Anbieten oder Veröffentlichen eines Pakets gibt Agents die Möglichkeit, ein Paket zu installieren, wann es ihnen passt. Pakete werden auf die übliche Weise erstellt, aber statt sofort verteilt zu werden, bleiben die Setupdateien beim Server und lassen sich nach Bedarf von genannten Agents abrufen.

1. Markieren Sie in der Strukturansicht die Abteilung, AD Container oder das Unternehmen, denen Sie das Paket anbieten möchten.
2. Klicken Sie mit der rechten Maustaste and wählen Sie **Anbieten**.
   Oder
   Klicken Sie auf den Dropdownpfeil des Software-Verteilungssymbols und wählen Sie im Menü die Option {Anbieten}.
   Oder
   Klicken Sie auf das Symbol **Anbieten** der Softwareverteilungsgruppe.
3. Das Dialogfeld "Paket anbieten" wird eingeblendet. Alle mit aktivierter Option **Beim Agent sichtbar** erstellten Pakete sind aufgeführt. Zum Erstellen eines neuen Pakets klicken Sie auf **Neu**.

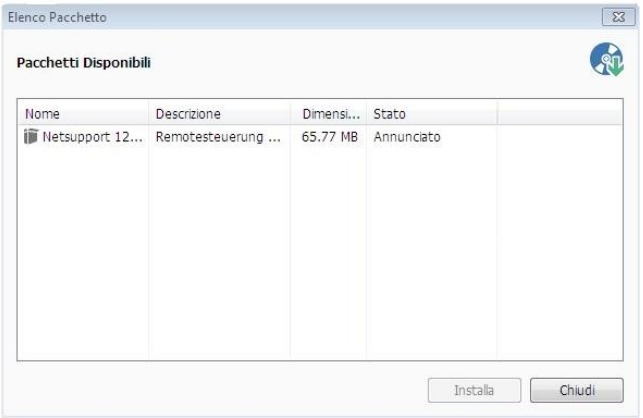


4. Wählen Sie das gewünschte Paket und klicken Sie auf **Anbieten**, um es in das Feld "Angeboten" zu übertragen.
5. Wählen Sie **Unterabteilungen einschließen**, wenn Sie möchten, dass alle nachfolgenden Abteilungen/Agents in die Verteilung eingeschlossen werden.
6. Klicken Sie auf **OK**.

Anfordern eines Pakets

Angebotene Pakete lassen sich mit dem Paketanforderungstool durch Agents vom Server abrufen.

1. Klicken Sie auf dem Agentcomputer mit der rechten Maustaste auf das DNA-Symbol in der Taskleiste und wählen Sie **Paket anfordern**.
2. Das Dialogfeld Paketliste wird eingeblendet, in dem alle für diesen Agent verfügbaren Pakete aufgeführt sind.



3. Markieren Sie das gewünschte Paket und klicken Sie auf **Abrufen**. Die Anwendungs-Setupdateien werden beim Agent ausgeführt. Der Status des Pakets ändert sich zur Anzeige, dass es an den Agent geliefert wurde

Hinweis: Konsolebediener können den Zugriff eines Agents auf die Paketanforerungsfunktion sperren, indem sie die Software-Verteilungseinstellungen bearbeiten. Sie können auch gemäß obigem Muster "nicht" angebotene Pakete in die Paketliste aufnehmen, während Agents nur zur Installation von angebotenen Objekten befähigt sind.

Importieren eines Pakets

Mit der Importoption lässt sich ein gespeichertes Verteilungspaket vom Server abrufen, um den Paketinhalt zu bearbeiten.

1. Klicken Sie auf den Dropdownpfeil des Software-Verteilungssymbols und wählen Sie im Menü die Option {Paketverwaltung}.
   Oder
   Klicken Sie auf das Symbol **Pakete** der Software-Verteilungsgruppe.
   Oder
   Klicken Sie in der Registerkarte „Werkzeuge" auf das Symbol **Paketverwaltung**.
2. Das Dialogfeld Paketverwaltung wird eingeblendet.
3. Wählen Sie **Neu**. Nun erscheint der Paketverteilungsdialog.
4. Wählen Sie Importieren. Bewegen Sie sich zum Paketordner, C:\programme\netsupport\netsupport dna\server\pakete, und wählen Sie das gewünschte Paket. Klicken Sie auf Öffnen.
5. Klicken Sie ggf. auf Aktionen, um zusätzliche Parameter einzuschließen.
6. Klicken Sie auf **OK**.
7. Das Dialogfeld "Paket testen" wird eingeblendet. Bevor Sie das Paket speichern, können Sie seine Zuverlässigkeit testen oder, wenn Sie zufrieden sind, klicken Sie auf **Paket speichern**.
8. Geben Sie einen Namen und eine Beschreibung für das Paket ein und klicken Sie auf **OK**. Das Paket wird verteilungsbereit erneut an den Server gesendet.

Softwareverteilungs-Warehouse

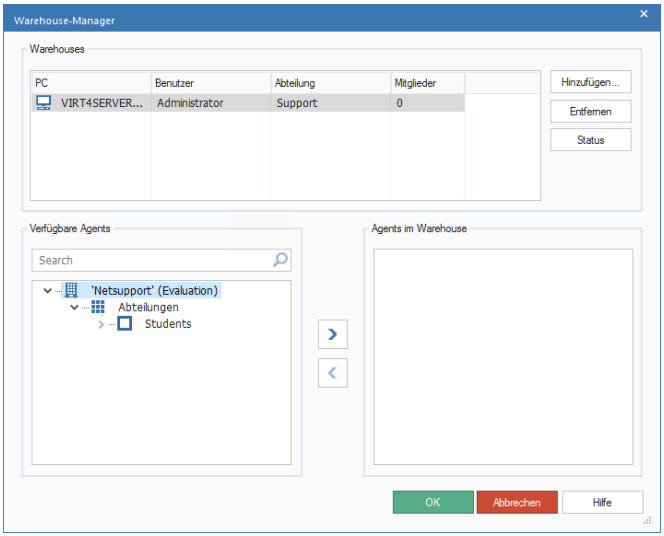
Berücksichtigen Sie bei der Planung eines umfangreichen Deploys, welche Folgen dies für das Netzwerk haben wird. An mehrere Agents über entfernte Netzwerke verteilte Pakete wirken sich natürlich auf die Ressourcen aus.

Um die Überlastung einzudämmen, können Sie bei DNA einen Agent, der sich im Idealfall am gleichen Ort wie die Zielcomputer befindet, zum "Verteilungs-Warehouse" ernennen. Beim Deploy des Pakets muss der Server so nicht an einen Agent nach dem anderen verteilen, sondern alles wird beim Warehouse Agent installiert, der dann an die übrigen Zielcomputer verteilt.

1. Klicken Sie auf den Dropdownpfeil des Software-Verteilungssymbols und wählen Sie im Menü die Option {Warehouses}.

   Oder

   Klicken Sie auf das Symbol **Warehouses** in der Software-Verteilungsgruppe.
2. Das Dialogfeld "Warehouse-manager" wird eingeblendet.
3. Vorhandene Warehouse PCs sind aufgeführt. Markieren Sie ein Objekt, um aktuell von diesem Warehouse bediente Agents und Details der Agents, die zum Hinzufügen verfügbar sind, zu betrachten. Klicken Sie auf **Status**, um Details für die aktuell im Warehouse befindlichen Pakete anzuzeigen.



4. Zum Erstellen eines neuen Warehouses klicken Sie auf Hinzufügen. Das Dialogfeld Warehouse auswählen wird eingeblendet. Hier können Sie einen Agentcomputer zum Host für das Warehouse ernennen.
5. Wählen Sie die Agents, die vom Warehouse bedient werden sollen. Markieren Sie in der Struktur **Verfügbare Agents** den gewünschten Agent und klicken Sie auf . Um einen Agent aus dem Warehouse zu entfernen, klicken Sie auf .

   Hinweis: Um in der Strukturansicht nach einem Element zu suchen, geben Sie den Namen oder einen Teil des Namens des PCs in dem Suchen-Feld ein und klicken Sie auf . Nun wird das erste übereinstimmende Element in der Strukturansicht zusammen mit der Anzahl der gefundenen Übereinstimmungen angezeigt. Sie können diese mit den Pfeilen durchblättern. Klicken Sie auf , um die Suche zu löschen.

6. Klicken Sie auf **OK**.

DNA Application Packager

DNA Application Packager ergänzt die Softwareverteilungsfunktion und eignet sich ideal für Situationen, in denen die Anwendung, die eingeführt werden soll, keine eigene, "unbeaufsichtigte" Installationsroutine besitzt. (Wenn die Software, die installiert werden soll, unbeaufsichtigte/automatische Routinen unterstützt, wird empfohlen, diese zu verwenden.) Mit dem Packager können Bediener Installationsprogramme von Drittparteien aufzeichnen und wieder abspielen. Alle nötigen Tastenanschläge und Mausbewegungen werden in einem Skript gespeichert, das dann auf den Agent-PCs ohne Eingriffe durch den Benutzer wieder abgespielt wird. Die Softwareverteilungsoption von DNA wird verwendet, um das gespeicherte Skript an die gewünschten Agent PCs zu senden.

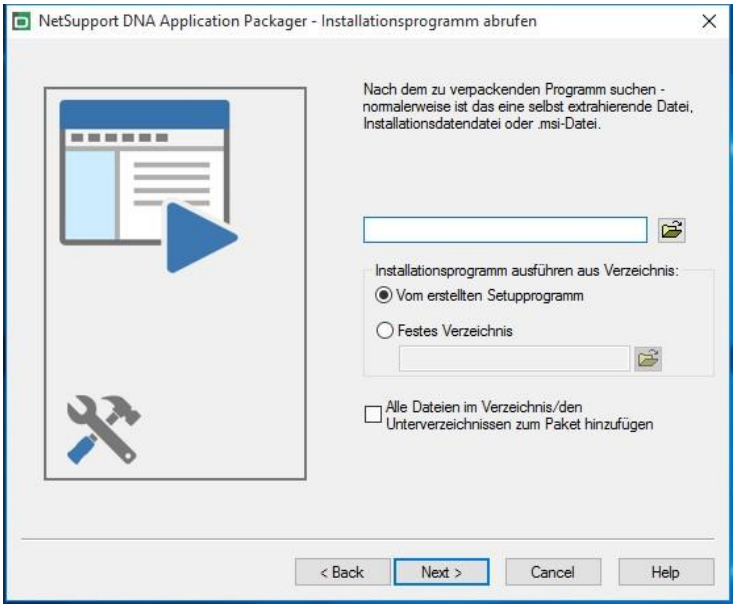
Hinweis: Mit dem Application Packager lassen sich Produktinstaller von "niedriger Komplexität" aufzeichnen und wieder abspielen. Der Packager beruht auf der Anzeige derselben Abfolge von Installerbildschirmen bei Ausführung der Installation auf den Zielcomputern. Wenn im Laufe des Playbacks unerwartete Dialogfelder erscheinen, wird das Installationsverfahren unterbrochen.

Es ist ein Skriptbearbeitungstool verfügbar, mit dem Sie ggf. gewisse Unterschiede beseitigen können.

1. Wählen Sie zum Laden des Packagers die Optionen {Start}{Programme}{NetSupport DNA}{DNA Application Packager}.
2. Das Dialogfeld "Willkommen" des Application Packagers wird eingeblendet. Sie werden vom Packager-Assistenten durch den Aufnameprozess geführt.
3. Klicken Sie auf **Weiter**.

Installationsprogramm abrufen

Geben Sie in diesem Dialogfeld an, welches Programm verpackt und in welches Verzeichnis die installierten Setupdateien auf dem Agent PC extrahiert werden sollen.

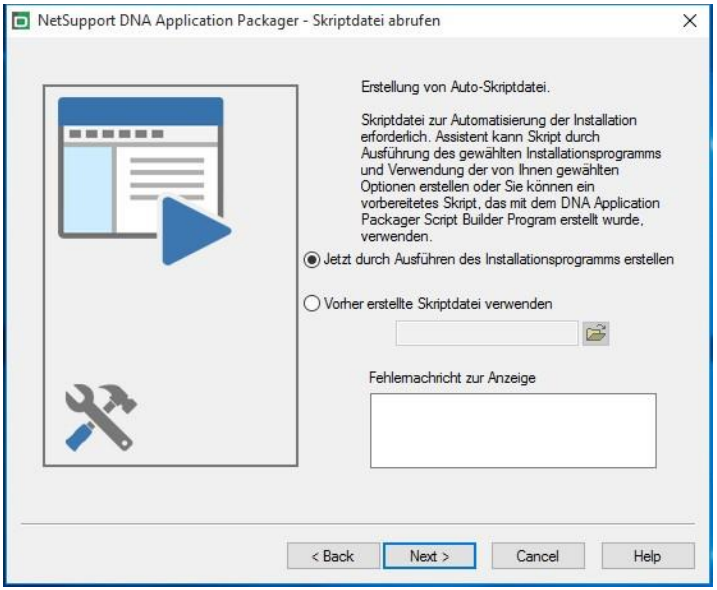


1. Finden Sie mit der Suchfunktion die gewünschte Programmsetup-Datei.
2. Geben Sie an, von wo aus das installierte Programm auf den Agentcomputern ausgeführt werden soll. Bei ihrer Verteilung an die Agent PCs wird die vom Packager erstellte exe-Datei in c:\programme\netsupport\netsupport dna\client\pakete gespeichert. Wenn Sie kein anderes festes Verzeichnis, von dem aus Setup in der Zukunft ausgeführt werden soll, angeben, wird immer vom obigen Setupprogramm-Verzeichnis aus auf es zugegriffen.
3. Wählen Sie **Alle Dateien im Verzeichnis/Unterverzeichnis zum Paket hinzufügen**, wenn Sie möchten, dass diese zusätzlichen Dateien während der Installation verfügbar sind. Nach erfolgreicher Installation werden sie gelöscht.
4. Klicken Sie auf **Weiter**.

Skriptdatei abrufen

Wenn die verpackte Anwendung an Agent PCs verteilt wird, sind die für die Installation notwendigen Aktionen in einem vordefinierten Skript festgehalten. Das Skript lässt sich in diesem Stadium durch Ausführen der Installation und Aufzeichnen der Tastatur-/Mausbewegungen erstellen, oder vielleicht haben Sie ein vorhandenes Skript, welches das Verfahren enthält.

Application Packager von DNA enthält ein Skripterstellungsprogramm, mit dem Sie manuell Skriptdateien erstellen und bearbeiten können.



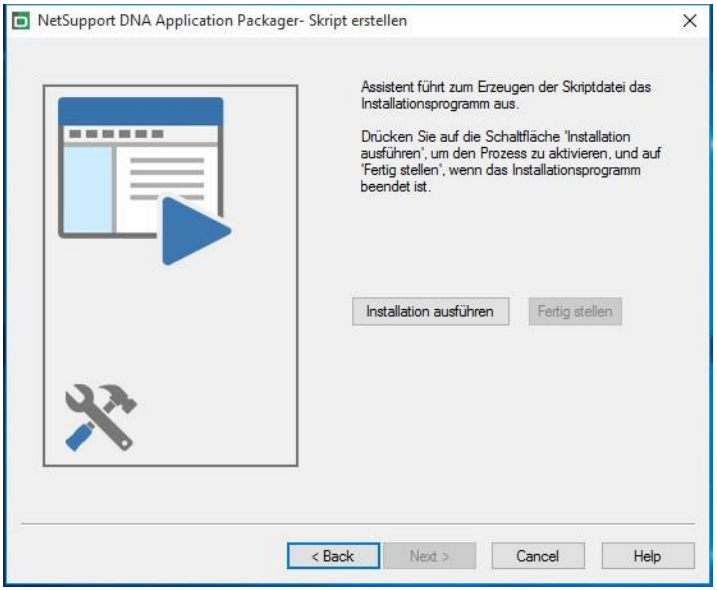
Wenn Sie eine vorher erstellte Skriptdatei verwenden möchten, suchen Sie nach der passenden *.rscrpt-Datei.

Wenn bei der Installation Probleme auftreten, können Sie eine benutzerdefinierte Meldung einblenden. Geben Sie eine passende Fehlermeldung in das dafür vorgesehene Feld ein.

Klicken Sie auf **Weiter**.

Skript erstellen

Dieses Dialogfeld erscheint, wenn Sie sich für die Erstellung des Skripts durch jetziges Ausführen des Installationsprogramms statt der Verwendung einer vordefinierten *.rscrpt-Datei entschieden haben.



Klicken Sie auf Installation ausführen, um den Installer des gewählten Programms zu starten. Die Installation wird auf dem Rechner des Bedieners in Echtzeit ausgeführt. Während Sie den Prozess durchlaufen, wird jeder Tastendruck und jede Mausbewegung aufgezeichnet und zur Skriptdatei hinzugefügt. Denken Sie daran, dass die Installation nach ihrer Verteilung genau so auf den Agent PCs ausgeführt wird. Wenn Sie versehentlich eine falsche Taste drücken oder eine ungewollte Option auswählen, können Sie das Skript vor seiner Verteilung an die Agents bearbeiten.

Wenn die Installation beendet ist, klicken Sie auf **Fertig stellen**.

Klicken Sie zur Fortsetzung auf **Weiter**.

Zusätzliche Dateien

In manchen Fällen kann das angegebene Setup zur Beendung der Installation zusätzliche Dateien benötigen, oder es gibt u. U. eine Reihe

verknüpfter Anwendungsdateien, die Sie mit dem Setup bündeln und für Benutzer nach der Installation verfügbar machen möchten.

Quellverzeichnis

Geben Sie den Speicherort der "zusätzlichen" Installations- und/oder Anwendungsdateien an und bestimmen Sie, ob der Inhalt von Unterverzeichnissen eingeschlossen werden soll.

Zielverzeichnis

Identifizieren Sie auf den Agentcomputern ein Zielverzeichnis, in das die Dateien extrahiert werden sollen.

Klicken Sie auf **Weiter**.

Erstellungsoptionen

Name für erstelltes Programm

Entscheiden Sie, ob die ausführbare Datei verteilungsbereit gespeichert werden soll.

Optionen

Maus/Tastatur sperren

Während des Installationsverfahrens können Sie die Maus und Tastatur der Agents sperren, um sicherzustellen, dass der automatische Prozess nicht von Benutzern unterbrochen wird.

Abbrechen des Skripts erlauben

Ermöglicht Agents den Unterbruch der Installation durch Drücken von STRG-UNTBR.

Kennwortdetails

Mit diesen Optionen können Sie die verteilte Datei durch ein Kennwort schützen und das Dialogfeld, das auf Agentcomputern erscheint, anpassen.

Mit diesen Optionen können Sie die verteilte Datei durch ein Kennwort schützen und das Dialogfeld, das auf Agentcomputern erscheint, anpassen.

DNA Application Packager - Script Builder

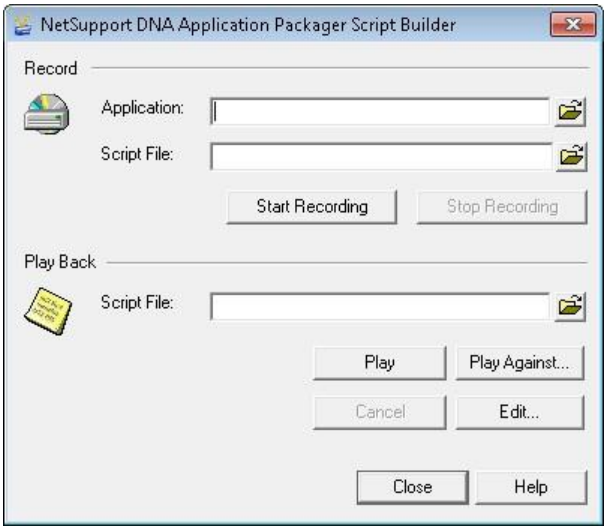
Im Application Packager von DNA haben Bediener die Möglichkeit, Installationsprogramme von Drittparteien aufzuzeichnen und wieder abzuspielen. Dies eignet sich ideal für Anwendungen, die keine "unbeaufsichtigte" Installationsfunktion bieten. Der Packager führt Bediener durch das Installationsverfahren und zeichnet dabei die erscheinenden Dialogfelder und getätigten Antworten auf. Diese Informationen werden in einem Skript gespeichert.

Wenn Sie mit dem aufgezeichneten Verfahren zufrieden sind, können Sie es an Agent PCs verteilen. Es kann jedoch vorkommen, dass Ihrer Ansicht nach eine auf dem Bedienercomputer aufgezeichnete Aktion bei der Ausführung der Installation auf den Agent PCs nicht benötigt wird oder dass Sie versehentlich einen falschen Mausklick oder Tastendruck vorgenommen haben.

Mit dem Script Builder können Sie im Application Packager erstellte Skripts bearbeiten oder neue Skripts aufzeichnen.

1. Zum Laden von Script Builder gehen Sie zu c:\programme\netsupport \netsupport dna\konsole\ 

2. Das Dialogfeld "Script Builder" wird eingeblendet.



Neues Skript aufzeichnen

Das Application Packager-Programm liefert zwar einen praktischen Assistenten, der Sie durch das Erstellungsverfahren für das Installerskript führt, aber Sie können die gewünschten Aktionen auch mit dem Script Builder aufzeichnen.

Anwendung

Geben Sie den Speicherort und Namen der gewünschten Anwendungs-Setupdatei ein.

Skriptdatei

Geben Sie einen Speicherort und Namen für die neue Skriptdatei ein.

Klicken Sie auf **Aufnahme beginnen**, um die angegebene Setupdatei zu starten. Der gewählte Anwendungsinstaller wird gestartet und der Script Builder zeichnet die erscheinenden Dialogfelder sowie die Maus-/Tastaturbewegungen, die der Bediener ausführt, auf. Die Installation findet auf dem Computer des Bedieners in Echtzeit statt, aber denken Sie auch daran, dass dies der Prozess ist, der bei der Verteilung des Skripts auf den Agent PCs ausgeführt wird.

Wenn die Installation beendet ist, klicken Sie auf **Aufnahme beenden**.

Wenn Sie das fertige Skript überprüfen oder infolge einer falschen Aktion Änderungen vornehmen möchten, klicken Sie auf **Bearbeiten**.

Skript bearbeiten

Mit dem Script Builder lassen sich gespeicherte Installerskripts wieder abspielen oder bearbeiten.

Playback

Öffnen Sie das gespeicherte Skript (*.rscrpt file).

Klicken Sie auf **Abspielen**, um die aufgezeichneten Aktionen wieder abzuspielen.

Sie können auch testen, ob sich ein vorhandenes Skript erfolgreich mit einer anderen Setupdatei ausführen lässt, zum Beispiel einer aktualisierten Version der bereits genutzten Anwendung. Klicken Sie auf **Abspielen** gegen und suchen Sie nach der nächsten Setupdatei.

Beim Playback des Skripts werden u. U. Fehler oder fehlende Aktionen aufgedeckt. Klicken Sie auf Bearbeiten, um Änderungen am Skript vorzunehmen. Der Skripteditor wird eingeblendet.

Im linken Fensterbereich sind Angaben zu den aufgezeichneten Dialogfeldern (Formularen) und durchgeführte Aktionen, wie z. B. Mausklicks, usw., aufgeführt. Wenn Sie eine Zeile des Skripts markieren, erscheinen im rechten Fensterbereich damit verknüpfte Informationen.

Neue Objekte lassen sich ggf. zum Skript hinzufügen:

Hinzufügen
Ermöglicht das Hinzufügen von zusätzlichen Aktionen zu einem Formular.

Formular hinzufügen von
Ermöglicht das Einfügen eines Formulars aus einem anderen Skript. Geben Sie den Namen der Skriptdatei ein und klicken Sie auf "Laden". Das ganze Skript wird eingeblendet.

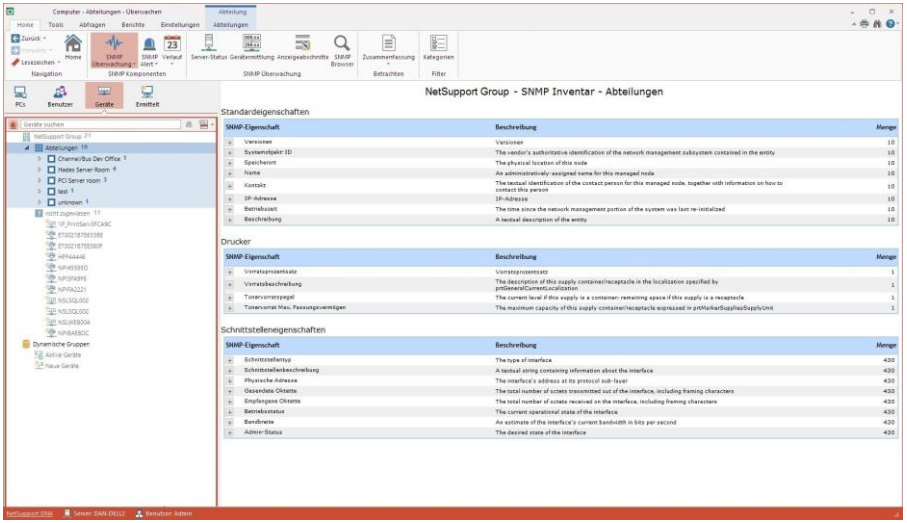
Wählen Sie das individuelle Formular, das Sie hinzufügen möchten.

SNMP-Überwachung

Wenn Geräte wie Drucker und Zugriffspunkte ermittelt worden sind, werden sie in NetSupport DNA gespeichert. Die Echtzeitdaten (wie Druckfarben- und Tonerstand) können dann von der Konsole aus überwacht werden.

1. Klicken Sie in der Geräte-Strukturansicht auf dem **SNMP-Überwachung**-Symbol im Menüband. Nun erscheint das SNMP-Überwachung-Fenster.

Hinweis: Wenn die Komponentensymbole ausgeblendet sind, klicken Sie auf die Registerkarte **Home**.



Wenn die SNMP-Geräte ermittelt worden sind, werden sie in der Strukturansicht gezeigt.

Hinweis: Die Geräte werden in der Strukturansicht automatisch nach den in ihren Speicherorteigenschaften gespeicherten Werten gruppiert.

Wählen Sie in der hierarchischen Strukturansicht die Ebene, auf der Sie die angezeigten Daten betrachten möchten: Unternehmen, Abteilung, dynamische Gruppe oder individueller Geräte.

Im Informationsfenster ist ein Breakdown für jedes gewählte Objekt in Grafik- und Listenformat angezeigt. Die SNMP-Eigenschaften werden zu Anzeigeabschnitten zusammengruppiert. Um die aktive Ansicht auszudrucken, klicken Sie auf dem  Symbol oben auf der Konsole.

Hinweis: Sie können Anzeigeabschnitte und Eigenschaften erstellen und verwalten; klicken Sie auf dem **Anzeigeabschnitte** Symbol im Menüband.

Um die Anzahl der im Informationsfenster gezeigten Daten zu beschränken, können Sie wählen, nur bestimmte SNMP-Kategorien anzuzeigen. Um eine Kategorie anzuzeigen, klicken Sie auf dem **Kategorien** Symbol im Menüband. Wählen Sie die geforderten anzuzeigenden Kategorien und klicken Sie auf **OK**. Das Informationsfenster zeigt jetzt nur die Daten für diese Kategorie. Eine gelbe Kopfzeile zeigt an, welche Kategorie Sie gerade betrachten. Sie können zwischen Kategorien wechseln und Kategorien von hier aus löschen.

Um Leasing- oder Wartungsverträge anzuzeigen, die den Geräten zugeordnet worden sind, klicken Sie auf der **SNMP-Überwachung** Dropdown-Liste und wählen Sie {Anzeigen- Verträge} oder klicken Sie auf dem **Verträge** Symbol im Menüband.

Um den Status Ihrer SNMP-Server anzuzeigen, klicken Sie auf dem **DNA SNMP-Serverstatus** Symbol im Menüband.

Die Häufigkeit, mit der der Server Daten sammelt, lässt sich mit der Option "DNA-Einstellungen" ändern.

Mit einer Schnellaktualisierungsfunktion können Sie Daten außerhalb der angegebenen Häufigkeit aktualisieren. Dies kann nützlich sein, wenn Sie bestimmte Geräte oder Abteilungen anpeilen möchten. Klicken Sie mit der rechten Maustaste auf das gewünschte Objekt in der Strukturansicht und wählen Sie „Aktualisieren" oder klicken Sie im Menü oder dem Ribbon „SNMP-Überwachung" auf „Aktualisieren".

Abfragen
Wählen Sie zur Anzeige des Abfragefensters die Registerkarte „Abfragen".

Mit dem Abfragetool von DNA können Sie Datenbankeinträge abrufen, die bestimmte Kriterien erfüllen. Abfragen zu der Komponente, die gerade betrachtet wird, sind aufgelistet, was ein schnelles Abrufen der Ergebnisse ermöglicht.

Klicken Sie in der Menüleiste auf dem Abfrage hinzufügen Symbol, um eine neue Abfrage zu erstellen, oder klicken Sie auf dem Abfrage bearbeiten Symbol in der Menüleiste, um ein in der Liste vorhandenes Objekt zu bearbeiten.

Berichte
Wählen Sie zur Anzeige des Berichtfensters die Registerkarte „Berichte".

Jeder Komponente ist eine Reihe von vordefinierten Managementberichten, die vom Crystal Reports-Modul gespeist werden, beigefügt. Wählen Sie den geforderten Bericht in der Dropdown-Liste. Die Ergebnisse erscheinen im Informationsfenster. Sie lassen sich ggf. exportieren.

SNMP-Alert

NetSupport DNA bietet eine Alerting-Funktion, die es Ihnen ermöglicht, Änderungen in den gesammelten SNMP-Daten zu identifizieren, beispielsweise, wenn der Druckertoner auf unter XX% abfällt.

Alert-Benachrichtigungen können an vorgegebene Emailempfänger und/oder aktive Konsolenbenutzer geleitet werden

1. Klicken Sie in der Geräte-Strukturansicht auf dem **SNMP-Alert** Symbol im Menüband. Nun erscheint das SNMP-Alertfenster.

Hinweis: Wenn die Komponentensymbole ausgeblendet sind, klicken Sie auf die Registerkarte **Home**.

Wählen Sie in der hierarchischen Strukturansicht die Ebene, auf der Sie die angezeigten Daten betrachten möchten: Unternehmen, Abteilung, dynamische Grupe oder individueller Geräte.

Im Informationsfenster ist ein Breakdown für jedes gewählte Objekt in Grafik- und Listenformat angezeigt. Die aufgelisteten Beschreibungen können erweitert werden, um einen individuellen Gerätestrukturplan für jedes Objekt zu zeigen. Um den Graph in einem anderen Format anzuzeigen, klicken Sie auf dem Diagramm-Symbol-Dropdownpfeil in der Menüleiste und wählen das entsp rechende Format. Um die aktive Ansicht auszudrucken, klicken Sie auf dem  Symbol oben auf der Konsole.

Hinweis: Durch Anklicken des Chart-Symbols im Ribbon wird die Grafik ein-/ausgeblendet.

Werden ausstehende Alerts für die entsprechenden Geräte in der Hauptunternehmenshierarchie-Strukturansicht identifiziert. Wenn Alerts identifiziert worden sind, kann ein Operator Notizen hinzufügen. Ein voller Verlauf aller Alerts steht über die Verlauf-Funktion zur Verfügung.

Hinweis: Sie können Alerts in der Strukturansicht zeigen / ausblenden, indem Sie auf  klicken.

Um die Eigenschaften für ein Alert zu konfigurieren, wählen Sie die SNMP-Alert Symbol Dropdown-Liste und klicken Sie auf **Alert Konfig**.

Abfragen
Wählen Sie zur Anzeige des Abfragefensters die Registerkarte „Abfragen".

Mit dem Abfragetool von DNA können Sie Datenbankeinträge abrufen, die bestimmte Kriterien erfüllen. Abfragen zu der Komponente, die gerade betrachtet wird, sind aufgelistet, was ein schnelles Abrufen der Ergebnisse ermöglicht.

Klicken Sie in der Menüleiste auf dem Abfrage hinzufügen Symbol, um eine neue Abfrage zu erstellen, oder klicken Sie auf dem Abfrage bearbeiten Symbol in der Menüleiste, um ein in der Liste vorhandenes Objekt zu bearbeiten.

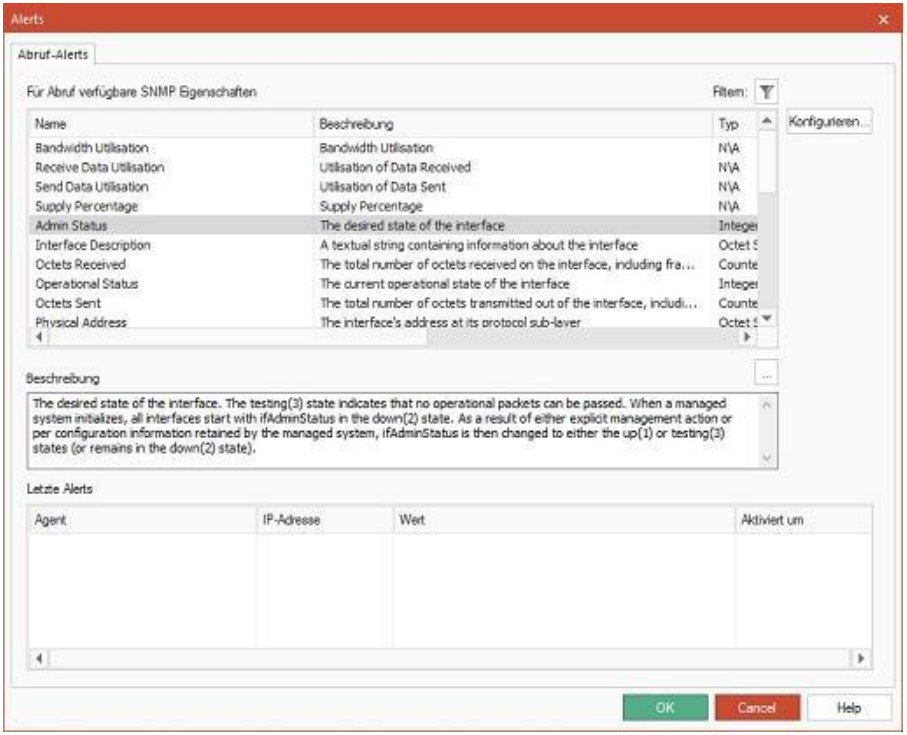
Berichte
Wählen Sie zur Anzeige des Berichtfensters die Registerkarte „Berichte".

Jeder Komponente ist eine Reihe von vordefinierten Managementberichten, die vom Crystal Reports-Modul gespeist werden, beigefügt. Wählen Sie den geforderten Bericht in der Dropdown-Liste. Die Ergebnisse erscheinen im Informationsfenster. Sie lassen sich ggf. exportieren.

Hinweis: Das in der Konsole angezeigte Datum-/Zeitformat stimmt mit dem Format in dem Rechner, in dem der DNA Server installiert ist, überein. Um das Format in der Konsole zu ändern, müssen Sie zunächst das Format in diesem Rechner ändern. Weitere Angaben hierzu finden Sie unter www.netsupportsoftware.com/support.

SNMP-Alert-Konfiguration

Dieser Dialog ermöglicht es Ihnen, die SNMP-Eigenschaften zu sehen, die für Alerts zur Verfügung stehen.



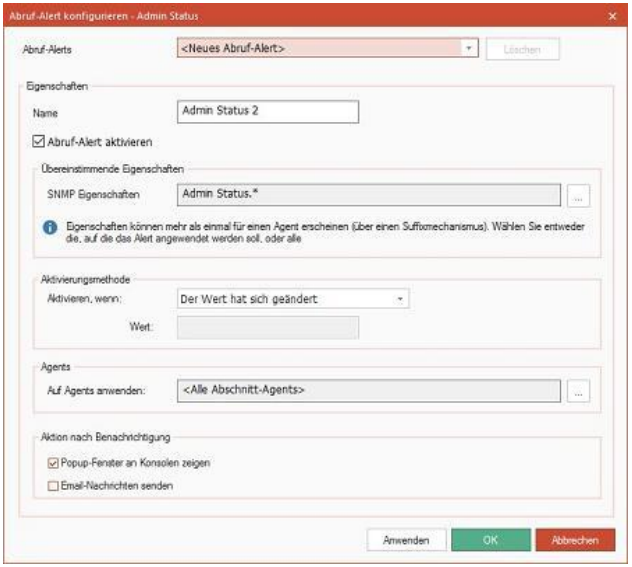
Um die Liste übersichtlicher zu machen, können Sie die angezeigten Eigenschaften filtern. Klicken Sie auf  und der Abruffilter-Dialog erscheint.

Um ein neues Alert zu erstellen oder ein vorhandenes zu konfigurieren, wählen Sie die geforderte SNMP-Eigenschaft und klicken dann auf Konfigurieren.

Details der aktiven Alerts werden im Abschnitt Letzte Alerts gezeigt.

SNMP – Neues Alert erstellen

Dieser Dialog ermöglicht es Ihnen, neue SNMP-Alerts zu erstellen und die Eigenschaften für existierende SNMP-Alerts zu konfigurieren.



Um ein neues Alert zu erstellen

1. Wählen Sie **Neues Abrufalert** in der Abrufalerts-Dropdown-Liste.

   Hinweis: In dieser Dropdown-Liste erscheint eine Liste aller existierenden Alerts für die gewählte Eigenschaft.

2. Es wird ein Standardname gezeigt, den Sie auf Wunsch ändern können.
3. Vergewissern Sie sich, dass **Abrufalert aktivieren** gewählt ist.
4. Wählen Sie die SNMP-Eigenschaften, die für das Alert gelten sollen. Klicken Sie auf ... .
5. Wählen Sie, in welchen Fällen das Alert aktiviert werden soll, in der Dropdown-Liste, und geben Sie, falls erforderlich, den Wert ein.
6. Wählen Sie die Geräte, auf die das Alert angewendet werden soll. Klicken Sie auf ... .
7. Wählen Sie die Benachrichtigungsmethode, wenn das Alert aktiv ist: Popup-Fenster an der Konsole und/oder Emailnachricht.

   Hinweis: Sie können die Empfänger für Alerts in den SNMP-Alert-Einstellungen einstellen.

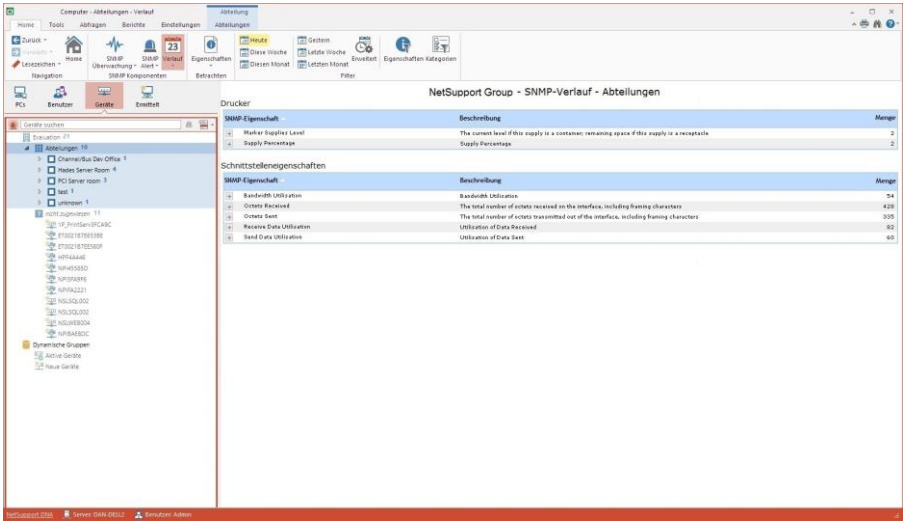
SNMP-Verlauf

Die Verlaufoption ermöglicht es Ihnen, Änderungen nachzuverfolgen, die an einer Geräte-SNMP-Eigenschaft ausgeführt worden sind, und den Alerting-Verlauf anzuzeigen.

Jedes Mal wenn NetSupport DNA Daten sammelt, vergleicht es die aktuellen Angaben mit den bereits auf dem Server gespeicherten Informationen, und wenn es Unterschiede findet, werden diese im Verlauf erfasst.

1. In der Geräte-Strukturansicht, klicken Sie auf dem **Verlauf** Symbol im Menüband. Nun erscheint das Verlaufübersicht-Fenster.

Hinweis: Wenn die Komponentensymbole ausgeblendet sind, klicken Sie auf die Registerkarte **Home**.



Sie können die History auf folgenden Ebenen betrachten: Unternehmen, Abteilung, dynamische Gruppe oder Geräte. Wählen Sie die gewünschte Ebene in der hierarchischen Strukturansicht.

Um zwischen den Ansichten hin- und herzuschalten, klicken Sie auf der **Verlauf**-Symbol-Dropdownliste und wählen {Anzeigen-Eigenschaften\Abruf-Alerts} oder auf dem entsprechenden Symbol im Menüband.

Sie können die Daten für eine spezifische Zeitperiode betrachten. Um zwischen verschiedenen Zeitperioden hin- und herzuschalten, klicken Sie das entsprechende Symbol im Filterbereich des Menübands an. Wenn Sie auf **Erweitert** klicken, können Sie einen benutzerdefinierten Datum-/Zeitfilter anwenden. Aufgelistete Beschreibungen lassen sich erweitern, so dass Sie ein individuelles Gerätebreakdown für jedes Objekt erhalten. Die gezeigten Arbeitsstunden können im DNA Konfigurationskatalog für Ihre Organisation angepasst werden. Siehe Konsolenanpassungen – Allgemein für weitere Informationen.

Das in der Konsole angezeigte Datum-/Zeitformat stimmt mit dem Format in dem Rechner, in dem der DNA Server installiert ist, überein. Um das Format in der Konsole zu ändern, müssen Sie zunächst das Format in diesem Rechner ändern. Für weitere Informationen wenden Sie sich bitte an unser Support-Team www.netsupportsoftware.com/support.

Hinweis: Es kann sein, dass Sie für gewisse in der History festgehaltene Hardwareänderungen kein Tracking durchführen möchten. Können Sie die Anzeige von Objekten in der Konsole deaktivieren und vorhandene Daten für deaktivierte Objekte löschen. Klicken Sie auf dem **Eigenschaften** Symbol im Menüband.

Um die Anzahl der im Informationsfenster gezeigten Daten zu beschränken, können Sie wählen, nur bestimmte SNMP-Kategorien anzuzeigen. Um eine Kategorie anzuzeigen, klicken Sie auf dem **Kategorien** Symbol im Menüband. Wählen Sie die geforderten anzuzeigenden Kategorien und klicken Sie auf **OK**. Das Informationsfenster zeigt jetzt nur die Daten für diese Kategorie. Eine gelbe Kopfzeile zeigt an, welche Kategorie Sie gerade betrachten. Sie können zwischen Kategorien wechseln und Kategorien von hier aus löschen.

Abfragen
Wählen Sie zur Anzeige des Abfragefensters die Registerkarte „Abfragen".

Mit dem Abfragetool von DNA können Sie Datenbankeinträge abrufen, die bestimmte Kriterien erfüllen. Abfragen zu der Komponente, die gerade betrachtet wird, sind aufgelistet, was ein schnelles Abrufen der Ergebnisse ermöglicht.

Klicken Sie in der Menüleiste auf dem Abfrage hinzufügen Symbol, um eine neue Abfrage zu erstellen, oder klicken Sie auf dem Abfrage bearbeiten Symbol in der Menüleiste, um ein in der Liste vorhandenes Objekt zu bearbeiten.

Berichte
Wählen Sie zur Anzeige des Berichtfensters die Registerkarte „Berichte".

Jeder Komponente ist eine Reihe von vordefinierten Managementberichten, die vom Crystal Reports-Modul gespeist werden, beigefügt. Wählen Sie den geforderten Bericht in der Dropdown-Liste. Die Ergebnisse erscheinen im Informationsfenster. Sie lassen sich ggf. exportieren.

Bericht- und Analysetools von DNA

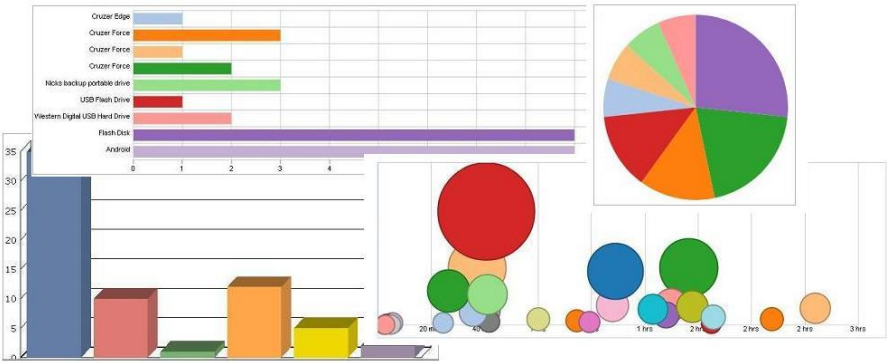
NetSupport DNA bietet sowohl Bildschirm- als auf für den Ausdruck optimierte Berichte. Die Bildschirmberichte/ansichten enthalten unterstützende Balken- und Kreisdiagramme sowie "live" Drilldown-Funktionen für alle wichtigen Zusammenfassungsdaten. Außer den Berichten über einzelne Geräte, Benutzer und Abteilungen bietet NetSupport DNA auch dynamische Gruppen. Diese sind benutzerdefiniert und werden zur Hauptgesellschaftsstruktur hinzugefügt. Eine dynamische Gruppe könnte zum Bespiel identifizieren, welche PCs aufrüstbar sind, und solch eine Gruppe würde automatisch aus denen erstellt, die die geforderten Kriterien erfüllen – wie "alle PCs mit mehr als 'XX' Gb Ram, 'XX' Gb freiem Speicherplatz und XX Prozessor-Typ" und so weiter.

Druckoptimierte Berichte sind für Managementberichterstattung gedacht und können zu einem geplanten Zeitpunkt erstellt und automatisch an spezifische Dateispeicherorte ausgegeben werden. Alle Berichte bieten Optionen für Drucken oder Export an PDF, DOC und XLS .

NetSupport unterstützt auch benutzerdefinierte Ansichten für alle Daten; das Abfrage-Tool bietet Benutzern eine einfache Schnittstelle zur Einstellung der benutzerdefinierten Ansichten. Das Abfrage-Tool benutzt eine einfache Drag & Drop Feldauswahl, die von Bedingungen und summenbasierten Funktionen unterstützt wird.

Analyse auf dem Bildschirm

Beim Betrachten einer der Komponentenregisterkarten erscheinen die nformationen für ein gewähltes Unternehmen, eine Abteilung oder einen Agent in Grafik- und Listenformat.



Die Daten lassen sich durch Wahl der passenden Option im Dropdownmenü des Chart-Symbols in einer Reihe von grafischen Formaten darstellen.

Hinweis: Durch Anklicken des Chart-Symbols im Ribbon wird die Grafik ein-/ausgeblendet.

Unter der Grafik sehen Sie dieselben Records in einem Listenformat. Sie können diese Informationen durch Anklicken von auf eine detailliertere Übersicht erweitern. Hierdurch werden alle individuellen Agentrecords eingeblendet.

Um die aktive Ansicht auszudrucken, klicken Sie auf dem  Symbol oben auf der Konsole.

Abfragen

Wählen Sie zur Anzeige des Abfragefensters die Registerkarte „Abfragen".

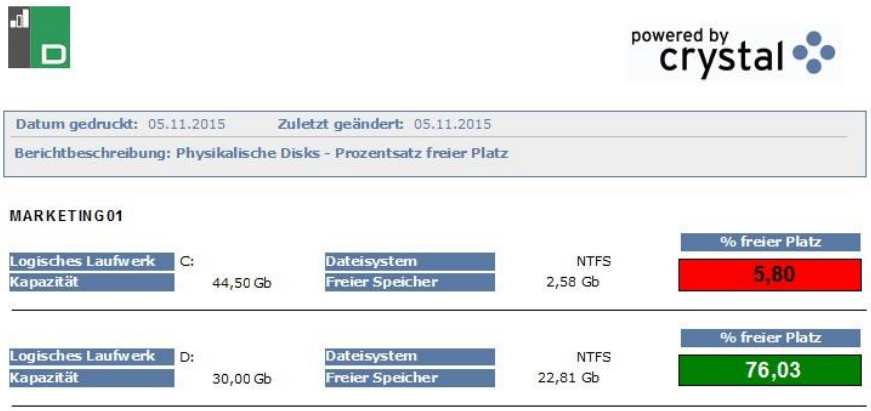
Mit dem Abfragetool von DNA lassen sich Ausgaben an Ihre speziellen Bedürfnisse anpassen. Abfragen können mit der Komponente, auf die sie sich beziehen, verknüpft werden, um ein schnelles Abrufen der Ergebnisse zu ermöglichen.

Klicken Sie in der Menüleiste auf dem **Abfrage hinzufügen** Symbol, um eine neue Abfrage zu erstellen, oder klicken Sie auf dem Abfrage **bearbeiten** Symbol in der Menüleiste, um ein in der Liste vorhandenes Objekt zu bearbeiten.

Berichte

Wählen Sie zur Anzeige des Berichtfensters die Registerkarte „Berichte".

DNA liefert eine Reihe von vordefinierten Crystal Reports für jede Komponente. Wählen Sie den geforderten Bericht in der Dropdown-Liste und die Ergebnisse werden im Informationsfenster angezeigt.



Man kann alle verfügbaren Berichte als PDF, DOC, XLS, XML, HTML, CSV und RTF exportieren. Wählen Sie dazu im Ribbon „Berichte" das **Exportsymbol**.

Zum Scrollen durch die Berichtseiten lassen sich die Steuerelemente im Ribbon „Berichte" verwenden.

Hinweis: Sie können mithilfe der Steuerelemente in der Statusleiste zwischen Seitenlayouts umschalten und Berichte vergrößern und verkleinern.

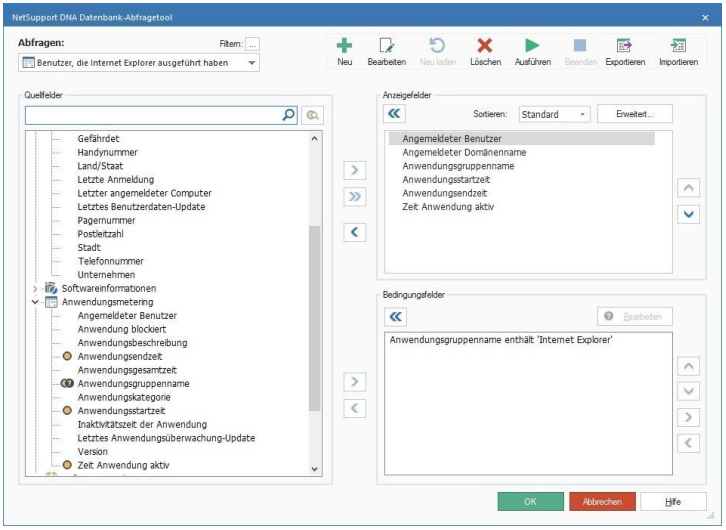
Abfragetool

Das Abfragetool stellt noch eine zusätzliche Erweiterung der in DNA verfügbaren Berichtoptionen dar. Während auf dem Bildschirm angezeigte und vordefinierte Crystal-Berichte zahlreiche vorgefertigte Informationen liefern, ermöglicht das Abfragetool das Anpassen der Ausgabe an Ihre speziellen Bedürfnisse.

Die Ergebnisse lassen sich auf dem Bildschirm betrachten, ausdrucken oder exportieren. Jede gespeicherte Abfrage kann an die DNA-Komponente, auf die sie sich bezieht, angefügt und so jederzeit leicht wieder abgerufen werden.

1. Klicken Sie auf der Tools-Registerkarte auf dem **Abfrage**-Symbol. Das Dialogfeld „Abfragetool" wird eingeblendet Von hier aus können Sie Abfragen erstellen, bearbeiten, löschen, ausführen, importieren und exportieren.

Hinweis: Sie können die Anzahl der gezeigten Abfragen auf nur die in bestimmten Gruppen filtern. Klicken Sie auf , um anzugeben, welche Abfragegruppen angezeigt werden sollen. Beim Erstellen und Bearbeiten einer Abfrage können Sie im Abfrageeigenschaften-Dialog Abfragegruppen erstellen und Abfragen zu einer Gruppe hinzufügen.



Erstellen einer neuen Abfrage

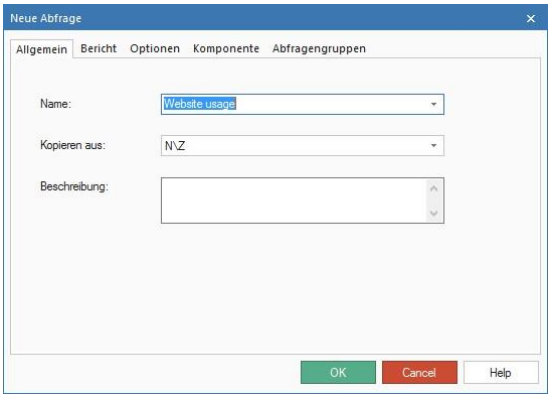
1. Klicken Sie im Abfragetool-Dialog auf **Neu**.

   Oder

   Im Konsolenfenster wählen Sie die Abfragen-Registerkarte und dann die entsprechende Komponente, der die Abfrage angefügt werden soll. Klicken Sie im Menüband auf dem **Abfrage hinzufügen** Symbol.

   Hinweis: Mit dieser Methode können Sie die Komponente, der die Abfrage hinzugefügt ist, nicht ändern.

2. Das Dialogfeld „Neue Abfrage" wird eingeblendet. Geben Sie die Eigenschaften einer neuen Abfrage ein.



Allgemein

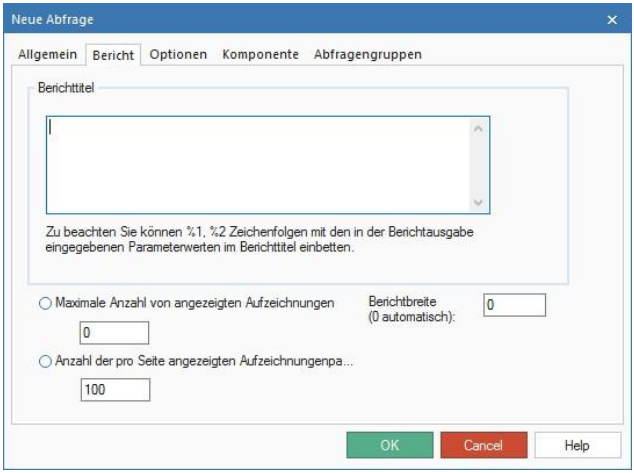
Name und Beschreibung

Geben Sie einen sinnvollen Namen und eine Beschreibung für die Abfrage ein. Der Name wird zur Dropdownliste mit Abfragen, aus der Sie bei jedem Laden eines Berichts auswähle können, hinzugefügt.

Kopieren aus

Um Zeit zu sparen, können Sie den Inhalt einer vorhandenen Abfrage kopieren und ihn als Grundlage für den neuen Bericht verwenden. Die Felder und alle damit verknüpften Kriterien lassen sich dann wunschgemäß bearbeiten.

Bericht



Geben Sie einen Titel für den Bericht ein. Dieser wird in die Endausgabe aufgenommen. Zu Flexibilitätszwecken können Sie angeben, dass beim Ablaufen eine veränderliche Bedingung mit dem Format %1, %2, usw. eingegeben werden soll. Die Nutzungsbeschränkungen fürdiese Funktion finden Sie im nachfolgenden Hinweis.

Zum Beispiel:
Computer und Benutzer, die %1 länger als 20 Minuten besucht haben.
Dies ermöglicht es Ihnen, eine variable Bedingung einzugeben (zum Beispiel www.netsupportdna.com), wenn die Abfrage ausgeführt wird.

Maximale Anzahl von angezeigten Aufzeichnungen

Geben Sie die Gesamtanzahl der anzuzeigenden Datensätze an. Dies kann nützlich sein, wenn Sie die „höchsten zehn" oder „höchsten zwanzig" Datensätze anzeigen möchten.

Anzahl der pro Seite angezeigten Aufzeichnungenpage

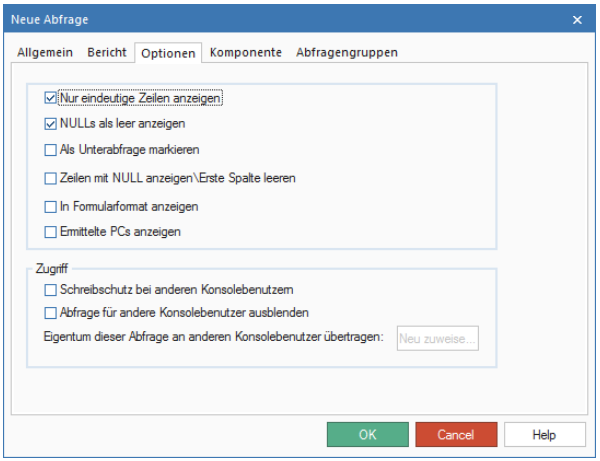
Geben Sie ein, wie viele Records pro Seite gedruckt werden sollen.

Hinweis: Diese Option steht nicht zur Verfügung, wenn Maximal anzuzeigende Anzahl von Datensätzen gewählt worden ist.

Berichtbreite

Im Allgemeinen wird die Ausgabe an die Seite angepasst, aber Sie können eine Zeichenbreite angeben, wenn Ihnen eine andere Anzeigebreite besser gefällt Nur eindeutige Zeilen anzeigen Durch Markieren dieser Option können Sie verhindern, dass mehrere Instanzen desselben Records eingeschlossen werden.

Optionen



Nur eindeutige Zeilen anzeigen

Durch Markieren dieser Option können Sie verhindern, dass mehrere Instanzen desselben Records eingeschlossen werden.
Denken Sie daran, welche Ausgabe die Abfrage wahrscheinlich erzeugen wird und beschließen Sie, ob Sie duplizierte Records ausschließen möchten. Alle angezeigten Felder müssen übereinstimmen, damit der Record ignoriert wird.

NULLs als leer anzeigen

Leere Felder leer lassen statt sie als NULL anzuzeigen.

Als Unterabfrage markieren

Unterabfragen bieten die Möglichkeit, den in einer vorhandenen Abfrage angegebenen Kriterien entgegengesetzte Kriterien laufen zu lassen. Sie haben zum Beispiel u. U. eine Abfrage zur Suche nach PCs, auf denen ein bestimmtes Hotfix installiert ist. Aber es ist gleichzeitig möglich, dass Sie auch diejenigen PCs finden möchten, auf denen kein Hotfix installiert ist.

Erstellen Sie im ersten Fall eine Unterabfrage und geben die gewünschte Bedingung ein. Zum Beispiel PCs, auf denen Hotfix 12345678 installiert ist.

Erstellen Sie zweitens eine neue Abfrage mit der Suchbedingung nach PCs, die im obigen Beispiel nicht gefunden wurden.

Zeilen mit NULL anzeigen\Erste Spalte leeren

Wenn die erste Informationsspalte für einen Record leer ist, können Sie diesen Record ignorieren.

In Formularformat anzeigen

Eignet sich perfekt für Abfragen, die minimale Ergebnisse erzeugen. Sie können hiermit die einzelnen Datensätze im Formularstil statt in individuellen Reihen anzeigen.

Ermittelte PCs anzeigen

Normalerweise werden nur Benutzer mit einem NetSupport DNA Agent in den Abfrageergebnissen angezeigt. Wenn Sie diese Option wählen, werden auch andere ermittelte PCs aufgelistet.

Zugriff

Schreibschutz bei anderen Konsolebenutzern

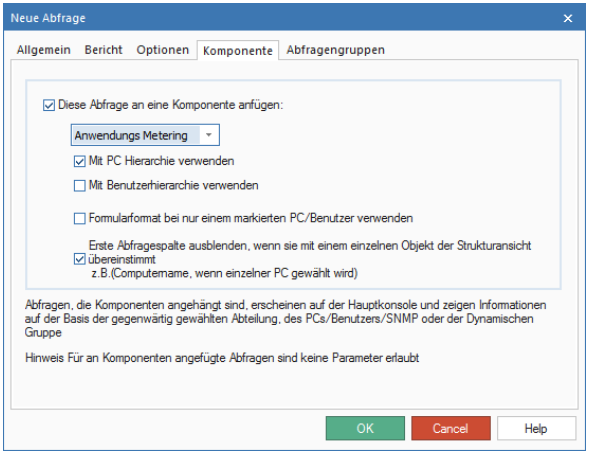
Wenn Sie diese Option auswählen, können andere Konsolebenutzer die Abfrage zwar betrachten, aber keine Änderungen an ihr vornehmen.

Abfrage für andere Konsolebenutzer ausblenden

Blendet die Abfrage bei anderen Konsolebenutzern aus.

Hinweis: Keine anderen Benutzer (einschließlich Administratoren) können die von einem Konsolebenutzer eingestellten obigen beiden Eigenschaften ändern. Die Abfrage lässt sich neu einem anderen Benutzer zuweisen, und dieser wird dann zum Eigentümer der Abfrage. Klicken Sie auf **Neu zuweisen**.

Komponente



Diese Abfrage an eine Komponente anfügen

Sie können die Abfrage an die Komponente anfügen, auf die sie sich bezieht: Anwendungsmetering, usw. Dies bedeutet, dass sich das Ergebnis durch Auswahl der Registerkarte **Abfragen** im entsprechenden Informationsfenster betrachten lässt.

Hinweis: Da es keinen Mechanismus zur Eingabe von Parametern über die Registerkarte "Abfragen" gibt, fügen Sie einer Komponente keine Abfragen hinzu, wenn der Titel eine Variable erfordert. Berichte dieser Art lassen sich nur von der Option **Abfragetool** ausführen.

Verwendung mit der PC-Hierarchie

In der Standardeinstellung wird die Abfrage mit der PC-Hierarchie benutzt. Haben Sie die Wahl dieser Option auf, wenn Sie die Abfrage nicht mit der Hierarchie des PCs benutzen möchten.

Mit Benutzerhierarchie verwenden

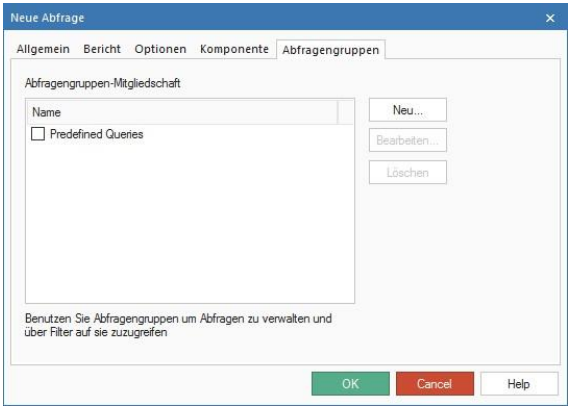
Die Auswahl dieser Option ermöglicht es, die Abfrage mit der Benutzer-Hierarchie zu verwenden.

Hinweis: Diese Option erscheint nur für Komponenten, die in der Benutzer-Hierarchie zur Verfügung stehen.

Formularformat bei nur einem markierten PC verwenden
Beim Ausführen der Abfrage im Konsolefenster können Sie in der Struktur einen individuellen Agentnamen markieren, um ausschließlich die Datensätze für den betreffenden Benutzer aufzurufen. Es lässt sich dabei gleichzeitig das Formularformat aktivieren.

Erste Abfragespalte ausblenden, wenn sie mit einem einzelnen Objekt der Strukturansicht übereinstimmt, z.B.(Computername, wenn einzelner PC gewählt wird)
Wenn die erste Spalte der Abfrage mit einem Objekt in der Strukturansicht übereinstimmt, wird diese Spalte ausgeblendet. Wenn die erste Spalte in der Abfrage beispielsweise Computername ist, und Sie einen einzelnen PC in der Strukturansicht auswählen, wird die Computername-Spalte nicht in der Abfrage erscheinen.

Abfragegruppen



Es können Abfragegruppen erstellt werden, mit denen Sie die Anzahl der Abfragen im Abfrage-Tool filtern können. Eine Standardgruppe, Vordefinierte Abfragen, führt alle existierenden Abfragen auf. Um eine neue Gruppe zu erstellen, klicken Sie auf Neu und geben einen Namen und eine Beschreibung für die neue Gruppe ein.

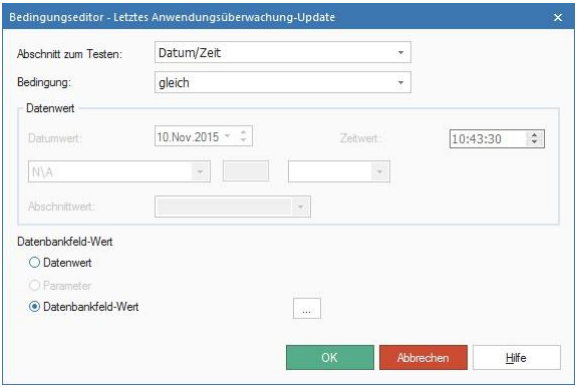
Klicken Sie auf **OK**, um zum Hauptdialogfeld "Abfragetool" zurückzukehren.

3. Wählen Sie in der Quellenfeldliste die Objekte, die in die Ausgabe aufgenommen werden sollen. Sie können eine spezifische Quelle schnell finden, indem Sie sie im Suchfeld eintippen. Klicken Sie auf ›

, um die Objekte an das Anzeigenfelder-Fenster zu übertragen. Sie können alle Felder in einer bestimmten Kategorie übertragen, indem Sie auf . Sie können durch Anklicken von  die aktuellen Werte für das Feld betrachten.

Hinweis: Wenn Sie ein Quellenfeld doppelt anklicken, wird dies ebenfalls zum Anzeigefelder-Fenster hinzugefügt.

4. Ordnen Sie die Anzeigefelder in die Reihenfolge, in der sie erscheinen sollen, indem Sie auf  und . klicken. Wenn Sie möchten, dass die Ausgabe nach einem bestimmten Feld sortiert wird, wählen Sie das betreffende Objekt und wählen in der Dropdownliste die gewünschten Sortierkriterien.
5. Um die angezeigten Felder anzupassen, klicken Sie auf **Erweitert**.
6. Sie können die Datenbank nach spezifischen Records abfragen, indem Sie Bedingungen hinzufügen. Wählen Sie das/die Quellfeld(er) und klicken Sie auf  um es/sie in das Fenster "Bedingungsfelder" zu übertragen. Der Bedingungseditor-Dialog erscheint und ermöglicht es Ihnen, die Bedingungen einzustellen.
7. Die Abfrage wird gespeichert, wenn Sie sie ausführen oder auf **OK** klicken.



Wählen Sie in der Dropdownliste die Bedingung, die beim Abfragen der Datenbank auf der Suche nach Agents, welche die angegebenen Kriterien erfüllen, angewendet werden soll. Die Bedingung lässt sich mit einem genauen Datenwert oder einem Feldnamen vergleichen, oder Sie können einen benutzerdefinierten Wert eingeben.

Hinweise:
- Wenn Sie bei der Erstellung der Abfrage eine variable Bedingung vorgegeben haben, vergewissern Sie sich, dass das **Parameterwert** Feld aktiviert ist.
- Wenn Sie PCs identifizieren möchten, die in der Unterabfrage nicht gefunden wurden, stellen Sie sicher, dass die Bedingung "nicht in Unterabfrage" ausgewählt ist, und wählen in der Liste die gewünschte verfügbare Unterabfrage.
- Wenn Sie eine Datenfeldbedingung hinzufügen, können Sie die Abfrageergebnisse nach Datum filtern, u.a. mit einem globalen Datenfilter aus der **Datenwert** Dropdown-Liste.

Eine Abfrage exportieren
1. Wählen Sie vom Abfrage-Tool aus die geforderte Abfrage, die exportiert werden soll, in der Dropdown-Liste.
2. Klicken Sie auf **Exportieren** und dann auf **Speichern**.
3. Die gewählte Abfrage wird dann an eine .XML Datei exportiert.

Abfrage importieren
1. Klicken Sie im Abfrage-Tool auf **Importieren**.
2. Wählen Sie die zu importierende Datei und klicken Sie auf **Öffnen**.
3. Die gewählte Abfrage wird nun im Abfrage-Tool angezeigt.

Hinweis: Sie können keine Abfragen importieren, die mit dem Datenbankwartungstool exportiert worden sind.

Vorhandene Abfrage bearbeiten

1. Wählen Sie im Abfrage-Tool die zu bearbeitende Abfrage in der Dropdown-Liste.

   Oder

   Wählen Sie die Abfragen-Registerkarte und dann die relevante Komponente. Wählen Sie die zu bearbeitende Abfrage in der Dropdown-Liste und klicken Sie auf **Abfrage bearbeiten**.
2. Die verknüpften Informationen werden in den Anzeige- und Bedingungsfeldern eingeblendet.
3. Sie können die Anzeige/Bedingungen-Felder mit den entsprechenden Tasten hinzufügen oder entfernen.
4. Um die Abfrageeigenschaften zu bearbeiten, klicken Sie auf **Bearbeiten**.
5. Alle Änderungen werden gespeichert, wenn Sie eine Abfrage ausführen oder auf **OK** klicken.

Abfrage ausführen

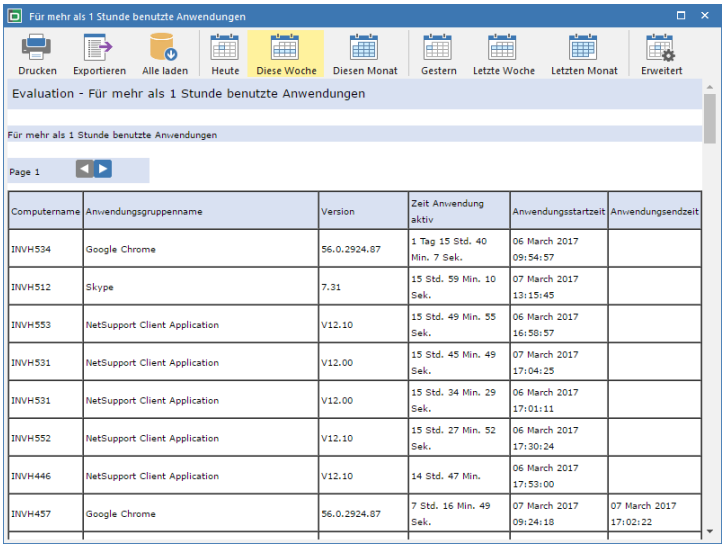
Abfragen lassen sich aus dem Hauptdialogfeld für das Abfragetool oder, wenn sie an eine Komponente angefügt sind, aus der betreffenden Komponentenregisterkarte im Konsolefenster ausführen.

Abfragen vom Abfrage-Tool-Dialog aus ausführen

1. Wählen Sie die Tools-Registerkarte und klicken Sie auf dem **Abfrage** Symbol.
2. Daraufhin erscheint das Abfrage-Tool. Wählen Sie in der Dropdownliste mit Abfragen das Objekt, das Sie ausführen möchten. Sie können die Eigenschaften und Felder ggf. vor Ausführen der Abfrage bearbeiten.
3. Klicken Sie auf **Ausführen**.

Hinweis: Wenn Sie für die Abfrage eine variable Bedingung vorgegeben haben, werden Sie aufgefordert, den Wert einzugeben.

4. Die Ergebnisse werden im Fenster "Abfrageergebnisse" eingeblendet. Wie viele Datensätze pro Seite erscheinen lässt sich im Feld **Anzahl der gleichzeitig angezeigten Reihen** im Dialogfeld "Abfrageeigenschaften" festlegen. Wenn Sie die Datensätze lieber in einer fortlaufenden Liste anzeigen möchten, klicken Sie auf **Alle laden**.



Computername	Anwendungsgruppenname	Version	Zeit Anwendung aktiv	Anwendungsstartzeit	Anwendungsendzeit
INVH534	Google Chrome	56.0.2924.87	1 Tag 15 Std. 40 Min. 7 Sek.	06 March 2017 09:54:57	
INVH512	Skype	7.31	15 Std. 59 Min. 10 Sek.	07 March 2017 13:15:45	
INVH553	NetSupport Client Application	V12.10	15 Std. 49 Min. 55 Sek.	06 March 2017 16:58:57	
INVH531	NetSupport Client Application	V12.00	15 Std. 45 Min. 49 Sek.	07 March 2017 17:04:25	
INVH531	NetSupport Client Application	V12.00	15 Std. 34 Min. 29 Sek.	06 March 2017 17:01:11	
INVH552	NetSupport Client Application	V12.10	15 Std. 27 Min. 52 Sek.	06 March 2017 17:30:24	
INVH446	NetSupport Client Application	V12.10	14 Std. 47 Min.	06 March 2017 17:53:00	
INVH457	Google Chrome	56.0.2924.87	7 Std. 16 Min. 49 Sek.	07 March 2017 09:24:18	07 March 2017 17:02:22

5. Die Ergebnisse lassen sich ggf. ausdrucken oder exportieren.

   Drucken

   Standardmäßig wird nur die aktuell angezeigte Seite ausgedruckt. Um alle Ergebnisse auszudrucken, klicken Sie auf **Alle laden**. Die Datensätze werden dann in einer fortlaufenden Liste angezeigt.

   Exportieren

   Die Ergebnisse lassen sich in den Formaten XML, HTML oder CSV (Werte mit Kommas getrennt) exportieren. Klicken Sie auf **Exportieren**, um das Dialogfeld "Exportoptionen" einzublenden und das gewünschte Format auszuwählen. Bei Verwendung von HTML können Sie Bilder oder das NetSupport DNA-Logo aus den Ergebnissen entfernen. Ähnlich wie bei der Druckoption wird auch hier standardmäßig nur die aktuell angezeigte Seite exportiert.

   Um alle Datensätze einzuschließen, markieren Sie das Feld **Alle Seiten**. Klicken Sie auf "OK" und speichern Sie die Exportdatei an einem geeigneten Ort.

Ausführen von Abfragen aus dem Konsolefenster

Wenn eine Abfrage an eine Komponente angefügt wurde, lässt sie sich direkt von der Komponente im Konsolefenster ausführen.

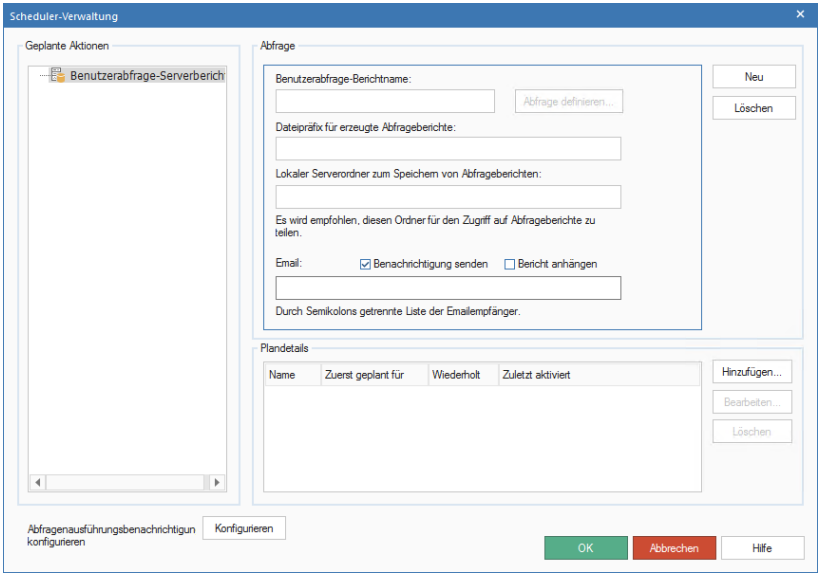
1. Wählen Sie die Abfragen-Registerkarte und dann die gewünschte Komponente.
2. Eine Liste der angefügten Komponentenabfragen wird eingeblendet.
3. Klicken Sie auf die gewünschte **Abfrage**. Die Ergebnisse werden im Informationsfenster angezeigt. Die Ergebnisse lassen sich durch Anklicken einer Abteilung oder eines Agents in der Struktur neu definieren. Ein einzelner Agent lässt sich im Formularformat anzeigen, wenn die entsprechende Option in den Abfrageeigenschaften aktiviert ist.

Geplante Abfragen

Mit dem Tool "Geplante Abfragen" können Sie Abfragen erstellen und planen, dass diese zu einem bestimmten Datum/einer bestimmten Zeit oder in regelmäßigen Intervallen ausgeführt werden. Die Abfragen erzeugen Berichte, welche auf dem Server PC in den Formaten HTML und XML gespeichert werden.

Hinweis: Vorhandene Abfragen lassen sich nicht planen.

1. Auf der Tools-Registerkarte, klicken Sie auf dem **Abfragen planen** Symbol.
2. Das Dialogfeld "Scheduler-Verwaltung" wird eingeblendet.



3. Klicken Sie auf **Neu**, geben Sie einen Benutzerabfrage-Berichtnamen ein, und wählen Sie **Abfrage definieren**.
4. Nun erscheint der Neue Abfrage Dialog. Geben Sie die geforderten Eigenschaften für die Abfrage ein und klicken Sie auf **OK**.

Hinweis: 'Als Unterabfrage markieren', 'schreibgeschützt für andere Konsolenbenutzer' und 'Abfrage für andere Konsolenbenutzer ausblenden' werden nicht zur Verfügung stehen. Wenn Sie Abfragen planen, können Sie die Abfrage auch nicht einer Komponente anhängen.

5. Wählen Sie im Abfrage-Tool die Quellenfelder, die in die Abfrage aufgenommen werden sollen, und fügen Sie eventuelle Bedingungen hinzu.
6. Geben Sie einen Dateinamen für den erzeugten Abfragebericht ein (das Datum/die Zeit werden automatisch an den Dateinamen angehängt).
7. Es kann eine Email-Benachrichtigung gesendet werden, wenn ein Bericht ausgeführt worden ist; klicken Sie auf **Benachrichtigung senden** und geben Sie die geforderten Emailadressen ein. Um eine Kopie des Abfrageberichts darin aufzunehmen, klicken Sie auf **Bericht anhängen**.
8. Geben Sie auf dem Server PC, auf dem die Berichte erzeugt werden sollen, ein gültiges Verzeichnis ein. Dieses Verzeichnis muss bereits vorhanden und für den DNA Service zugänglich sein.
9. Um den Bericht zu planen, klicken Sie auf **Hinzufügen**. Das Dialogfeld "Aktionszeiten planen" wird eingeblendet. Hier können Sie das gewünschte Datum und die Zeit für die Ausführung des Berichts auswählen und festlegen, ob die Ausführung wiederholt werden soll. Klicken Sie auf **OK**, um die Einstellung zu speichern.
10. Details der geplanten Zeiten werden nun im Dialogfeld angezeigt und lassen sich wunschgemäß bearbeiten oder löschen.
11. In der Standardeinstellung wird nur dann eine Konsolenbenachrichtigung gesendet, wenn ein Fehler bei der Ausführung einer geplanten Abfrage auftritt. Klicken Sie auf **Konfigurieren**, um zu wählen, ob Sie jedesmal benachrichtigt werden möchten, wenn eine geplante Abfrage ausgeführt wird, und ob eine Emailbenachrichtigung gesendet werden soll.
12. Klicken Sie auf **OK**, wenn Sie fertig sind.
13. Die erzeugten Berichte sind im auf dem Server PC angegebenen Verzeichnis in den Formaten HTML und XML verfügbar.

PCs, Benutzer und Geräte finden

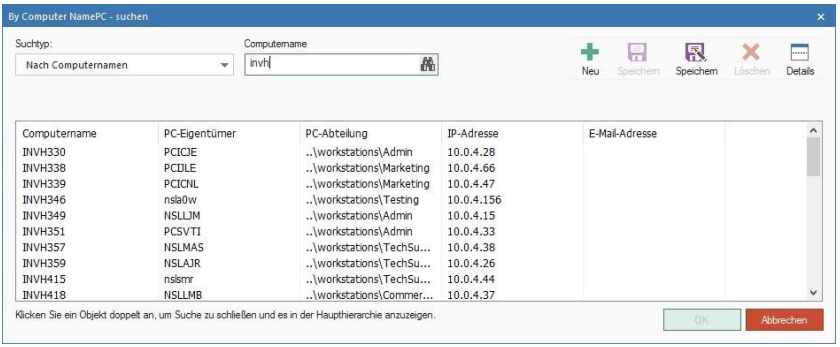
NetSupport DNA bietet ein PC/Benutzer/SNMP Agent finden Tool, das eingesetzt wird, um Agents in den PCs-, Benutzer- oder Geräte-Strukturansichten zu suchen und zu identifizieren. Es wird eine vordefinierte Liste an Suchparametern bereitgestellt oder Sie können Ihre eigenen erstellen. Es wird auch eine Schnellsuche-Funktion geboten, die es Ihnen ermöglicht, eine Suche innerhalb der PC- und Benutzer-Strukturansicht auszuführen.

Schnellsuche
Sie können von der Suchleiste oben in der Strukturansicht aus eine Suche innerhalb der PC- und Benutzer-Strukturansicht ausführen.

1. Geben Sie den Namen oder einen Teil des Namens im Suchfeld ein und klicken Sie auf . Die Suche kann auf dem PC-Namen, dem Bestandskennzeichen, der BIOS Seriennummer in der PC-Struktur oder dem Anmeldenamen in der Benutzerstruktur basieren. Um zwischen den Modi umzuschalten, klicken Sie auf .
2. Nun wird das erste übereinstimmende Element in der Strukturansicht zusammen mit der Anzahl der gefundenen Übereinstimmungen angezeigt. Sie können diese mit den Pfeilen durchblättern.
3. Die Suchergebnisse können in der Strukturansicht als Filter benutzt werden; klicken Sie auf . Nun erscheint eine Filterleiste oben in der Strukturansicht, die zeigt, welche Suchfilter angewendet werden. Wenn ein Filter angewendet wird, können Sie die Suche innerhalb des Filters ausführen. Zur Entfernung des Filters klicken Sie auf **Löschen**.
4. Klicken Sie auf , um die Suche zu löschen.

PC/Benutzer/SNMP Agent suchen Tool

1. Geben Sie in der Suchleiste oben in der PC-, Benutzer- oder Geräte-Strukturansicht Ihre Suchbegriffe ein und klicken Sie auf . Nun erscheint der PC/Benutzer/SNMP Agent suchen Dialog, der die Ergebnisse Ihrer Suche zeigt.
   Oder
   Klicken Sie auf  oben rechts auf der Konsole, um das PC/Benutzer/SNMP Agent suchen Tool zu öffnen.



2. Wählen Sie in der Dropdownliste einen vordefinierten Suchtyp und geben einen assoziierten Wert ein, um die Suche einzuschränken**.** Es lassen sich auch teilweise Informationen eingeben, wenn Sie die genauen Details nicht kennen. Wenn Sie zum Beispiel nach Computernamen suchen, alle Computer die mit Test beginnen.
3. Sie können zusätzliche Suchparameter einschließen, indem Sie auf Details klicken.
4. Klicken Sie auf .
5. Eine Liste der übereinstimmenden Agents wird eingeblendet.
6. Wählen Sie den gewünschten Agent in der Liste und klicken Sie auf **OK**.
7. Der gewählte Agent wird nun gesucht und in der Strukturansicht hervorgehoben.

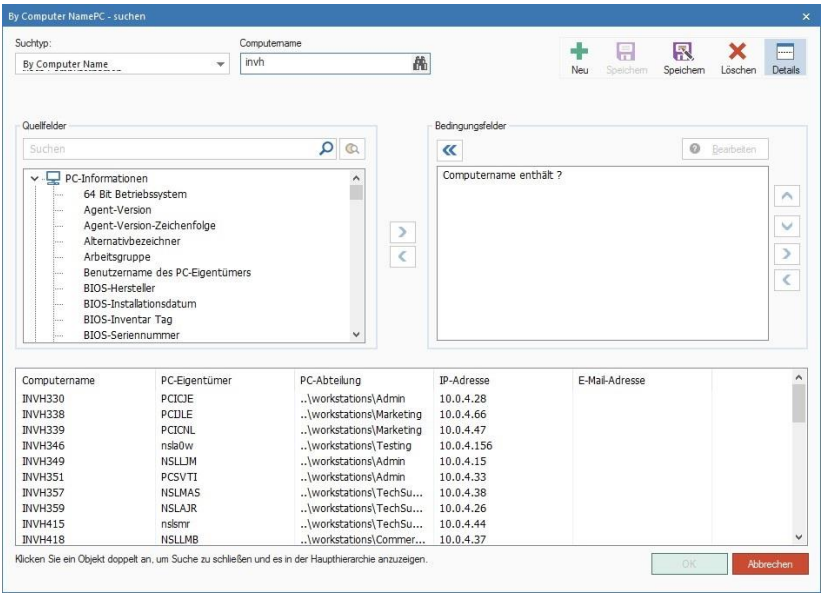
Erstellen von Suchparametern

Wenn Sie die vordefinierten Suchparameter zu stark einschränken, können Sie neue Abfragen erstellen, die zur zukünftigen Verwendung zu der Liste hinzugefügt werden. Zum Beispiel die Suche nach Benutzern, die eine bestimmte Website besucht haben.

1. Klicken Sie im Dialogfeld "Suchen" auf **Neu**.
2. Wählen Sie in der Quellenfeldliste die Objekte, die in die Ausgabe aufgenommen warden sollen. Sie können eine spezifische Quelle schnell finden, indem Sie sie im Suchfeld eintippen. Klicken Sie auf , um die Objekte an das Anzeigenfelder-Fenster zu übertragen.

   Sie können durch Anklicken von  die aktuellen Werte für das Feld betrachten.

3. Das Dialogfeld "Bedingungseditor" wird eingeblendet. Geben Sie die gewünschte Bedingung ein. Klicken Sie auf **Bearbeiten**, um bearbeiten vorhandene Bedingungs.



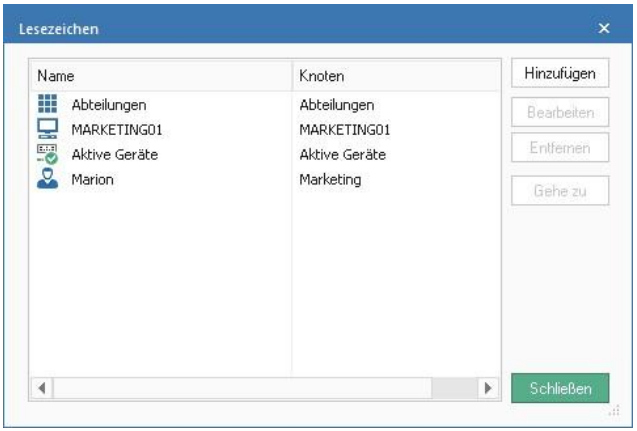
4. Klicken Sie auf Speichern als, um die Anfrage zu speichern. Geben Sie einen Namen ein und klicken Sie auf **OK**. Die neue Abfrage wird zur Dropdownliste „Suchtyp" hinzugefügt.
5. Stellen Sie zum Durchführen der Suche sicher, dass die gewünschte Abfrage in der Dropdownliste ausgewählt ist, geben Sie den assoziierten Parameter ein und klicken Sie auf . Übereinstimmende Agents werden aufgeführt.
6. Wählen Sie den gewünschten Agent in der Liste und klicken Sie auf **OK**.
7. Der gewählte Agent wird gesucht und in der Strukturansicht hervorgehoben.

Lesezeichen

NetSupport DNA ermöglicht es Ihnen, innerhalb der PC-, Benutzer- und Geräte-Strukturansichten Lesezeichen zu erstellen und zu positionieren. Dies kann nützlich sein, wenn Sie eine große und komplexe Struktur haben, da Sie dann schnell zu der Stelle navigieren können, an der Sie arbeiten möchten.

Lesezeichen hinzufügen

1. Navigieren Sie zu der Stelle in der Strukturansicht, an der Sie das Lesezeichen setzen möchten.
2. Klicken Sie auf dem **Lesezeichen** Symbol im Menüband.
3. Nun erscheint der Lesezeichen Dialog. Es werden alle vorhandenen Lesezeichen angezeigt, und Sie können diese dann bearbeiten, entfernen oder von hier aus auf ein Lesezeichen gehen.



4. Klicken Sie auf **Hinzufügen**, um einen Namen für das Lesezeichen einzugeben und klicken Sie dann auf **OK**.
5. Das neue Lesezeichen wird nun hinzugefügt.

Hinweis: Sie können auch ein neues Lesezeichen hinzufügen, indem Sie auf dem Dropdown-Pfeil im **Lesezeichen** Symbol im Menüband klicken und **Lesezeichen hinzufügen** wählen. Geben Sie den Namen für das Lesezeichen ein und klicken Sie auf **OK**.

Lesezeichen suchen

1. Klicken Sie auf dem **Lesezeichen** Symbol im Menüband.
2. Nun erscheint der Lesezeichen Dialog. Es wird eine Liste von Lesezeichen angezeigt.
3. Wählen Sie das geforderte Lesezeichen und klicken Sie dann auf **Gehezu**.
4. Die Strukturansicht wird nun an der geforderten Stelle geöffnet.

Oder

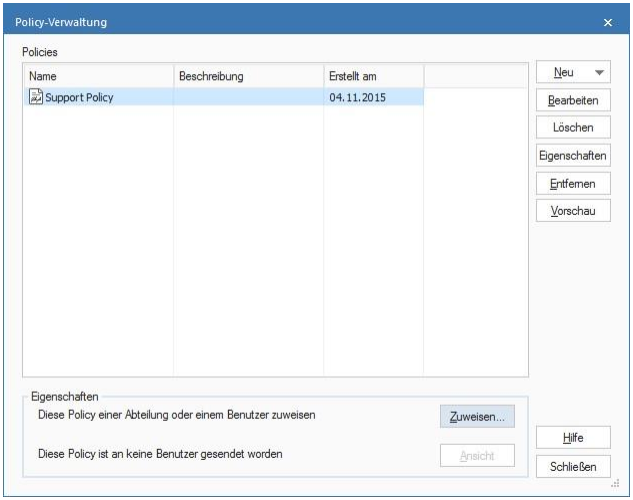
1. Klicken Sie auf dem Dropdown-Pfeil auf dem **Lesezeichen** Symbol im Menüband.
2. Es wird eine Liste von Lesezeichen angezeigt.
3. Klicken Sie auf dem geforderten Lesezeichen.
4. Die Strukturansicht wird nun an der geforderten Stelle geöffnet.

Acceptable Use Policies

Acceptable Use Policies (AUP) bilden einen festen Bestandteil der Schlüsselinformationen-Sicherheitsrichtlinien, die von den meisten Organisationen eingesetzt werden, und es ist ganz normal, dass neue Personalmitglieder eine AUP unterschreiben, bevor sie die Ressourcen der Gesellschaft zum ersten Mal benutzen, oder dass sie bestätigen, dass sie etwaige Änderungen solch einer Richtlinie gelesen haben, wenn diese aktualisiert wird.

NetSupport DNA bietet ein flexibles Modul zur Unterstützung der Zustellung und Nachverfolgung von AUPs im gesamten Unternehmen. Richtlinien können auf spezifische Geräte oder Benutzer angewandt und jedes Mal angezeigt werden, wenn ein Benutzer sich anmeldet, oder sie können einmalig angezeigt und bestätigt werden. Es ist möglich, mehrere Richtlinien zu erstellen, was es erlaubt, dass eine Richtlinie ausgewählten Benutzern nur einmal angezeigt wird (zum Beispiel Lehrern), während eine andere Richtlinie anderen Benutzern jedes Mal angezeigt wird (zum Beispiel Schülern). Außerdem werden volle Nachverfolgung und Ausnahmenmeldung geboten.

1. Klicken Sie die Tools-Registerkarte auf dem **AUP verwalten** Symbol an.
   Oder
   Klicken Sie auf den Dropdownpfeil für das Symbol der Benutzerdetails und wählen Sie im Menü die Option {Acceptable Use Policies}.
2. Nun erscheint der Policy verwalten Dialog.



Um eine neue Acceptable Use Policy zu erstellen

1. Klicken Sie auf **Neu** und wählen Sie **Leer**.

   Hinweis: Es wird ein Vorlagebeispiel geboten. Sie können dies benutzen oder bearbeiten, indem Sie **Neu** wählen und dann **Von Vorlage**.

2. Geben Sie den gewünschten Text für die Policy ein, und klicken Sie dann auf **OK**.
3. Nun erscheint der Policy-Eigenschaften Dialog.

Name
Geben Sie einen einmaligen Namen für die Policy ein.

Benutzer können diese Policy ablehnen
Diese Option ermöglicht es dem Benutzer, die Policy abzulehnen.

Hinweis: Der Benutzer wird von seinem Computer abgemeldet, wenn er der Policy nicht zustimmt.

Beschreibung
Geben Sie eine Beschreibung für die Policy ein.

PC-Abteilung-Zuordnung
Jedes Mal zeigen, wenn sich jemand anmeldet
Die Policy wird jedes Mal gezeigt, wenn sich ein Benutzer an seinem Gerät anmeldet.

Einmal pro Benutzer zeigen
Die Policy wird nur einmal pro Benutzer gezeigt.

Benutzerzuordnung
Jedes Mal anzeigen, wenn sich ein Benutzer anmeldet
Die Richtlinie wird jedes Mal angezeigt, wenn sich ein Benutzer anmeldet.

Einmal pro Benutzer anzeigen
Die Richtlinie wird jedem Benutzer nur einmal angezeigt.

Einmal pro Benutzer anzeigen (hat Vorrang vor Zuordnungen dieser Richtlinie durch die PC-Abteilung)
Wenn für einen Benutzer eingestellt wurde, dass eine Richtlinie nur einmal angezeigt werden soll, und wenn dieser sich an einem PC anmeldet, für den eingestellt wurde, dass die Richtlinie jedes Mal angezeigt wird, hat die Einstellung der PC-Abteilung Vorrang. Wenn

diese Option gewählt wird, wird die Einstellung der PC-Abteilung außer Kraft gesetzt, und die Richtlinie wird nur einmal pro Benutzer angezeigt.

Bestätigung

Keine
Es ist keine Bestätigung vom Benutzer erforderlich.

Benutzer muss Kästchen anhaken
Der Benutzer muss ein Kästchen anhaken, um die Policy zu bestätigen.

Benutzer muss seinen Namen eingeben
Der Benutzer muss seinen Namen eingeben, um die Policy zu bestätigen.

Benutzer abmelden, wenn die Policy nicht innerhalb von 5 Minuten bestätigt wird
Wenn der Benutzer die Policy nicht innerhalb von 5 Minuten bestätigt, wird er von seinem Gerät abgemeldet.

4. Klicken Sie auf **OK**.
5. Die Policy wird nun im Policy-Verwaltung Dialog aufgelistet.
6. Um eine Vorschau der Policies zu sehen, bevor Sie sie zuordnen, klicken Sie auf **Vorschau**.
7. Um eine Policy irgendwelchen Abteilungen oder Benutzern zuzuordnen, wählen Sie die gewünschte Policy und klicken dann auf **Zuordnen**.

Benutzerbestätigungen nachverfolgen

1. Wählen Sie die geforderte Policy in der Liste.
2. Klicken Sie auf **Ansicht**.

Hinweis: Wenn die Policy von keinem Benutzer gesendet oder bestätigt worden ist, steht diese Option nicht zur Verfügung.

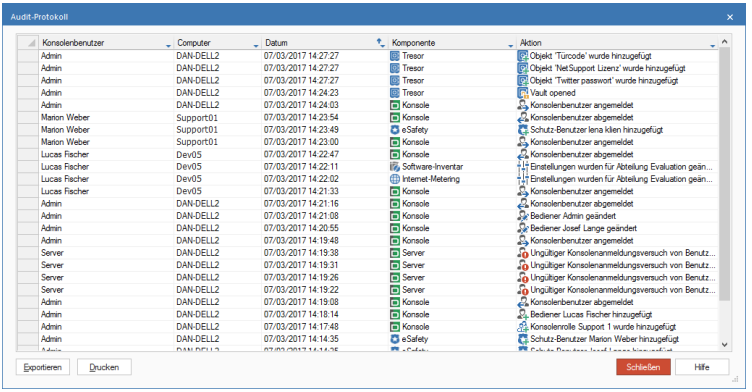
3. Nun erscheint der Policy-Bestätigungen Dialog. Hier können Sie die Benutzer sehen, die die Policy bestätigt haben sowie das Datum und die Zeit der Bestätigung und auf welchem PC sie bestätigt wurde.

Audit-Protokoll

NetSupport DNA bietet ein Audit-Protokoll, das es Ihnen ermöglicht, die Aktionen nachzuverfolgen, die Konsolenbenutzer innerhalb der NetSupport DNA Konsole ausgeführt haben. Es werden Konsolenaktivitäten aufgezeichnet, wie wann Benutzer sich an der Konsole an- und abgemeldet haben, wann Komponenten aktiviert oder deaktiviert worden sind, sowie alle Änderungen der Komponenteneinstellungen.

Hinweis: In Konsolenanpassungen – Audit-Einstellungen können Sie wählen, welche Aktionen protokolliert werden sollen.

1. Klicken Sie auf der Tools-Registerkarte auf dem **Audit-Protokoll** Symbol.
2. Nun erscheint der Audit-Protokoll Dialog.



3. Es wird eine Liste der Konsolenbenutzer angezeigt, zusammen mit Einzelheiten der Aktionen, die der Benutzer/In ausgeführt hat, in welcher Komponente sowie das Datum und die Zeit, zu der dies geschehen ist. Die neusten Objekte werden ganz oben aufgelistet.
4. Es können für jede Spalte Filter angewendet werden; wählen Sie . Daraufhin erscheint ein Menü, mit dem Sie die Objekte wählen können, die angezeigt werden sollen.
5. Um die aktuelle Liste zu exportieren, klicken Sie auf **Exportieren**.
6. Um die aktuelle Liste zu drucken, klicken Sie auf **Drucken**.

Hinweis: In der Standardeinstellung werden Audit-Eingaben 30 Tage lang gespeichert. Dies kann in den Konsolenanpassungen – Audit-Einstellungen geändert werden.

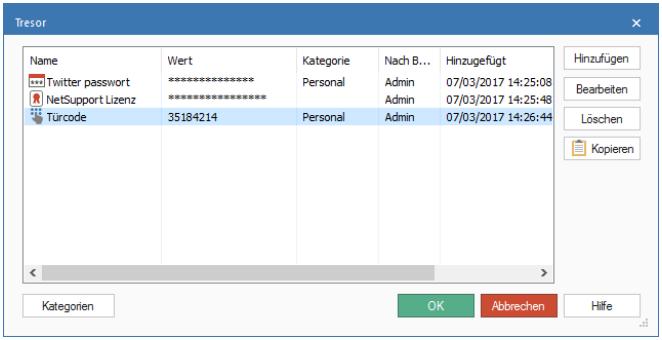
Tresor

NetSupport DNA bietet eine Tresor Komponente, die es Ihnen ermöglicht, vertrauliche oder nützliche Informationen wie Passwörter, Lizenzdetails, Türcode etc. zu speichern. Der Tresor ist ein sicherer Bereich innerhalb von DNA, der alle Informationen zentral aufbewahrt, und der Zugriff auf ihn kann auf bestimmte Konsolenbenutzer beschränkt werden, indem man die entsprechende Rolle einstellt.

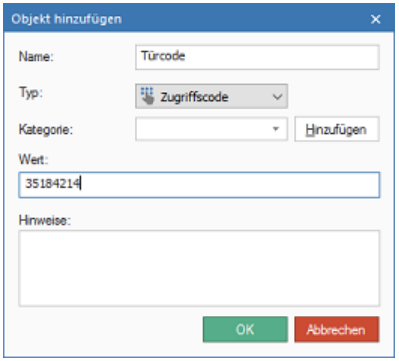
Hinweis: Nachdem Daten im Tresor gespeichert worden sind, müssen Bediener ihr Passwort eingeben, um auf sie zuzugreifen.

Neuen Eintrag zum Tresor hinzufügen

1. Auf der Tools Registerkarte auf dem **Tresor** Symbol klicken.
2. Nun erscheint der Tresor Dialog. Es werden alle vorhandenen Einträge angezeigt. Von hier aus können Sie den gewählten Eintrag bearbeiten, löschen und kopieren.



3. Klicken Sie auf **Hinzufügen**.
4. Nun erscheint der Objekt hinzufügen Dialog.



5. Geben Sie einen Namen für das Objekt ein.
6. Wählen Sie in der Dropdown-Liste, welche Art von Objekt Sie hinzufügen.
7. Sie können Kategorien definieren und dem Objekt zuordnen, so dass Sie Objekte zusammen gruppieren können. Um eine neue Kategorie zu erstellen, klicken Sie auf **Hinzufügen**. Sie wird dann in der Kategorien-Dropdownliste zur Auswahl zur Verfügung stehen.
8. Geben Sie den Wert für das Objekt ein, fügen Sie eventuelle Informationen hinzu, die sich auf das Objekt beziehen, und klicken Sie dann auf **OK**.
9. Das Objekt wird nun in der Hauptansicht aufgelistet, wobei der Wert aber verdeckt sein wird. Um ihn zu sehen, müssen Sie ihn wählen oder mit der Maus darüber fahren.
10. Klicken Sie auf **OK**.

Benutzerkonten verwalten

NetSupport DNA ermöglicht es Operators, Benutzer zu verwalten, die Bestandteil des Active Directory sind. Operators können die Benutzerkonten sehen, die deaktiviert oder gesperrt worden sind, und Konten zurücksetzen oder neue Passwörter zuweisen. NetSupport DNA ermöglicht Agents auch den Zugriff auf diese Funktion vom DNA Agent-Menü auf der Taskleiste aus.

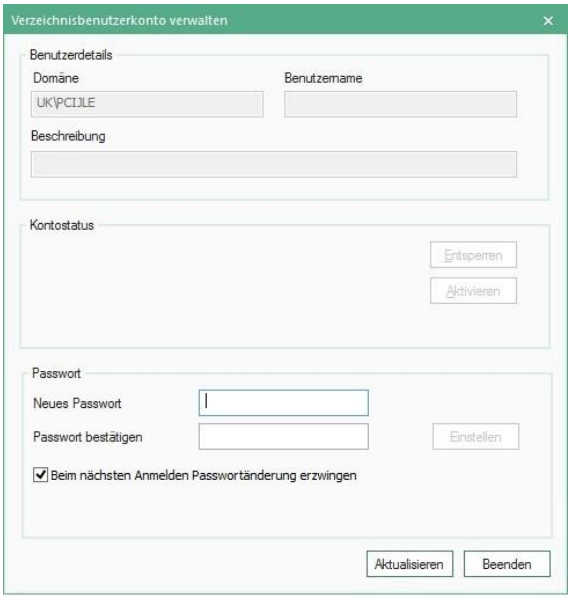
Wenn Nicht-Domänen-Administratoren diese Funktion benutzen möchten, müssen ihnen die entsprechenden Rechte zugewiesen werden. Für eine umfassende Anleitung dazu, wie dies getan wird, besuchen Sie bitte unsere Wissensbasis und lesen Sie den Produktartikel **Allow users to reset Active Directory passwords using NetSupport DNA** (Benutzern erlauben, mit NetSupport DNA Passwörter im Active Directory rückzusetzen).

Benutzerkonten verwalten von der NetSupport DNA Konsole aus

1. Klicken Sie in der Benutzer-Strukturansicht den geforderten Agent rechts an und wählen Sie **Benutzerkonto verwalten**.

   Hinweis: Wenn Sie zum ersten Mal auf diesen Dialog zugreifen, werden Sie aufgefordert, Ihren Benutzernamen und Ihr Passwort einzugeben.

2. Nun erscheint der Verzeichnisbenutzerkonto verwalten Dialog.



Von hier aus können Sie die gegenwärtigen Benutzerdetails sehen, das Konto entsperren, das Konto deaktivieren und aktivieren und ein neues Passwort einstellen. Wenn Sie ein neues Passwort einstellen, können Sie den Benutzer zwingen, dieses beim nächsten Anmelden zu ändern.

Hinweis: Wenn Komplexe Passwörter aktiviert ist, wird die Zurückstellen-Funktion dies nicht erzwingen. Sie müssen die Option **Beim nächsten Anmelden Passwortänderung erzwingen** benutzen, um sicherzustellen, dass diese Richtlinie eingehalten wird.

Klicken Sie auf **Aktualisieren**, um die Änderungen anzuwenden.

Benutzerkonten vom Agent aus verwalten
In der Standardeinstellung ist diese Funktion deaktiviert. Sie kann in DNA Konfiguration – Agent-Einstellungen aktiviert werden.

1. Klicken Sie das DNA Agent Symbol in der Taskleiste mit der rechten Maustaste an und wählen Sie **Benutzerkonto verwalten**.
2. Nun erscheint der Active Directory Benutzerkonto Dialog. Geben Sie den Benutzernamen für das Benutzerkonto ein, das Sie verwalten möchten und klicken Sie auf **Ändern**.

3. Nun erscheint der Verzeichnisbenutzerkonto verwalten Dialog.
4. Der Agent kann bei Bedarf Benutzerkonten entsperren und Passwörter einstellen.

Hinweis: Der Agent hat keinen Zugriff, um Benutzerkonten zu aktivieren/deaktivieren.

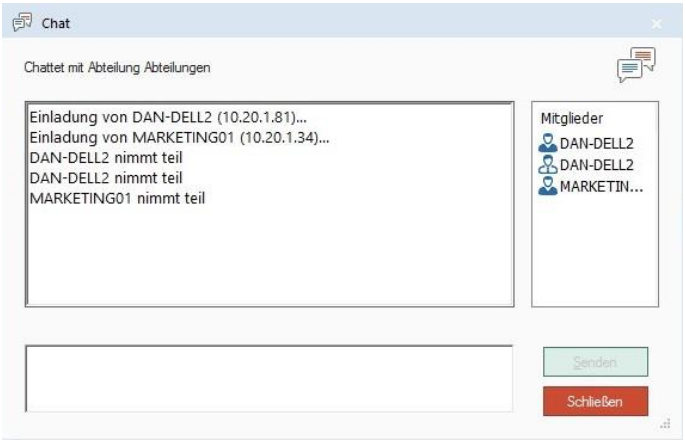
Chatten mit Agents

NetSupport DNA ermöglicht das gleichzeitige Chatten mit einer beliebigen Anzahl Agents über ein scrollbares Textfenster.

1. Markieren Sie in der Strukturansicht einen Agent oder eine Agentgruppe.

Hinweis: Die Chatfunktion ist nur von der Strukturansicht des PCs aus verfügbar.

2. Klicken Sie mit der rechten Maustaste und wählen Sie **Chat**.
   Oder
   Klicken Sie in der Registerkarte „Werkzeuge" auf das **Chatsymbol**.
3. Auf den Konsole- und Agent-PCs wird ein Chatfenster eingeblendet, in dem alle in der Chatsitzung eingeschlossenen Agents aufgeführt sind.



4. Geben Sie den gewünschten Text in das dafür vorgesehene Feld ein und klicken Sie auf **Senden**.
5. Die Nachricht wird auf allen Agent PCs eingeblendet. Der Agent hat auch die Möglichkeit, Nachrichten zu senden oder die Chatsitzung durch Klicken auf **Schließen** zu verlassen.
6. Die Konsole kann die Chatsitzung durch Klicken auf **Schließen** beenden.

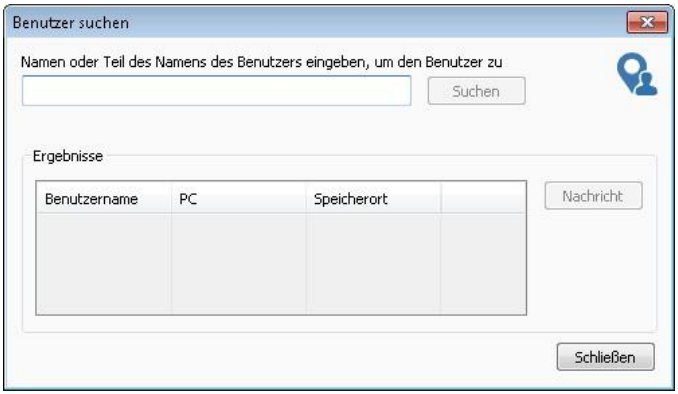
Benutzer suchen

NetSupport DNA ermöglicht es einem Agent, angemeldete Benutzer zu finden und ihnen eine Nachricht zu senden. Dies kann für Personalmitglieder nützlich sein, die mit anderen Benutzern Kontakt aufnehmen möchten, wenn die NetSupport DNA Konsole nicht bei ihnen installiert ist.

Hinweise:

- In der Standardeinstellung ist diese Funktion deaktiviert. Sie kann in DNA Konfiguration – Agent-Einstellungen aktiviert werden.
- Diese Funktion wird Benutzer in virtuellen Sitzungen, wie beispielsweise Desktop-Fernwartung oder Citrix-Benutzer, nicht auffinden.

1. Klicken Sie das DNA Agent Symbol in der Taskleiste mit der rechten Maustaste an und wählen Sie **Benutzer suchen**.
2. Nun erscheint der Benutzer suchen Dialog.



3. Geben Sie den Namen oder einen Teil des Namens des Benutzers ein, den Sie suchen und klicken Sie auf **Suchen**.
4. Daraufhin erscheint eine Liste der Benutzer, die mit der Suche übereinstimmen.
5. Wählen Sie den bzw. die Benutzer, an die eine Nachricht gesandt werden soll, und klicken Sie auf **Nachricht**. Geben Sie die gewünschte Nachricht ein und klicken Sie dann auf **OK**.
6. Die Nachricht wird nun bei dem gewählten Benutzer bzw. den gewählten Benutzern erscheinen.
7. Klicken Sie auf **Schließen**.

Fernsteuerung

DNAs integrierte Fernwartung
NetSupport Manager, DNAs integrierte Fernwartung, basiert auf NetSupports eigener Fernwartungslösung und bietet hochentwickelte Funktionalität für das effektive Management von entfernten Arbeitsstationen. Sie können den Bildschirm, die Maus und die Tastatur der Agent-PCs beobachten, freigeben oder steuern; Dateien an Agents übertragen; Befehlszeilenanweisungen über Remotebefehl-Eingabeaufforderung oder PowerShell am Agent ausführen; die Registrierung remote anzeigen und bearbeiten; laufende Anwendungen, Dienste und Prozesse verwalten, und eine Remote-Anmeldung oder –Abmeldung an Agent-Geräten ausführen.

Hinweise:

- Diese Funktionen stehen nur in der NetSupport DNA Version für das Bildungswesen zur Verfügung.
- Wenn sich irgendwelche Agent-Geräte, die Sie fernwarten wollen, in einem Remote-Netzwerk befinden, müssen Sie Ihre externe (öffentliche) Gateway-Adresse in den Fernwartungseinstellungen eingeben, um die integrierten Fernwartungsfunktionen für diese Geräte zu aktivieren.
- Sie können die integrierte Fernwartungsfunktion in NetSupport DNA benutzen, um ein Mac Gerät, auf dem NetSupport Manager Client installiert ist, fernzuwarten.*

NetSupport Manager
Oder Sie haben die Möglichkeit, eine vollständige Arbeitskopie von NetSupport Manager zu Ihrem DNA-Kauf hinzuzufügen. Seit mehr als 30 Jahren verfolgt NetSupport Manager konsequent Wege durch innovative Funktionen das Fernwartungs-PC-Management zu unterstützen.

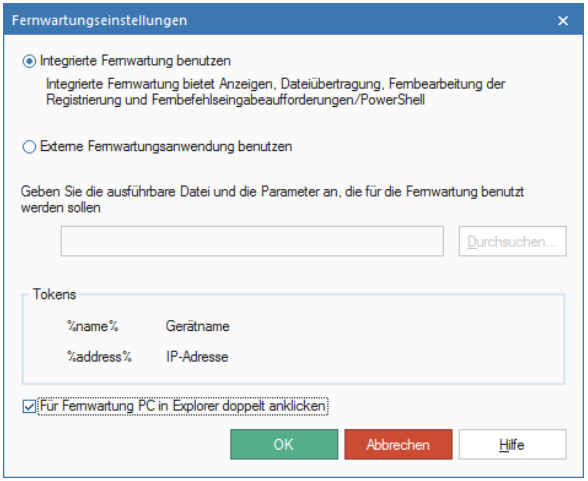
Für weitere Informationen besuchen Sie unsere Website, www.netsupportmanager.com, oder lesen Sie die NetSupport Manager-Dokumentation.

DNA lässt sich auch zur Verwendung einer beliebigen, von einer Drittpartei hergestellten Fernsteuerungsanwendung konfigurieren.

Fernsteuerung konfigurieren
DNA ermöglicht es Administratoren, über das Fernsteuerungstool beliebige Agentcomputer individuell zu betrachten.

Hinweis: Die integrierte Fernwartung kann benutzt werden, um Agents fernzuwarten, die RDP Benutzersitzungen ausführen.*

1. Klicken Sie in der Registerkarte „Werkzeuge" auf das Symbol **Fernwartungssymbol konfigurieren**.
2. Das Dialogfeld "Fernsteuerungseinstellungen" wird eingeblendet. Wenn Sie die integrierte Fernwartung benutzen, vergewissern Sie sich, dass die Option gewählt ist (die übrigen Felder werden nicht zur Verfügung stehen). Alternativ können Sie auch eine externe Fernwartungsanwendung benutzen. Klicken Sie auf **Durchsuchen**, um die entsprechende ausführbare Datei zu suchen, und geben Sie die relevanten Befehlsparameter für die Initiierung einer Fernwartungssitzung mit dem geforderten Agent PC an.
3. Eine Fernwartungssitzung kann dadurch geöffnet werden, dass man einen Agent in Explorer Modus doppelt anklickt; dafür sollte man sich vergewissern, dass **Für Fernwartung PC in Explorer doppelt anklicken** gewählt ist.



Starten einer Fernsteuerungssitzung

1. Wählen Sie in der Strukturansicht einen Agent aus. Klicken Sie mit der rechten Maustaste und wählen Sie **Fernwartung** - **Fernsteuerung**.

   Oder

   Den Agent in Explorer Modus doppelt anklicken.

Hinweis: Indem Sie rechts klicken und **Remote** wählen, können Sie auch Dateiübertragungen ausführen, eine Remotebefehl-Eingabeaufforderung und PowerShell Sitzung öffnen, die Registrierung bearbeiten, die laufenden Anwendungen, Dienste und Prozesse des Agents verwalten und eine Remote-Anmeldung oder -Abmeldung ausführen (eine Remote-Anmeldung oder -Abmeldung kann auch auf Abteilungs- oder Dynamische-Gruppe-Ebene ausgeführt werden).

2. Wenn auf dem Ziel-PC die richtige Software installiert ist, erscheint bei der Konsole ein Betrachtungsfenster für den gewählten Agent.

Hinweis: Sie können Benutzerbestätigung aktivieren, einen Indikator am Agent anzeigen, wenn eine Fernwartungssitzung aktiv ist, und den Standardanzeigemodus in den Fernwartungseinstellungen wählen.

Siehe Softwareverteilung, um herauszufinden, wie man ein Paket zur Verteilung an Agents erstellt.

* Für weitere Informationen besuchen Sie unsere Website, www.netsupportsoftware.com/support.

Nachricht senden

Mit dem Nachrichttool können Administratoren eine Nachricht an einen individuellen Agent, eine Abteilung oder das gesamte Unternehmen senden. Sie müssen dazu in der Strukturansicht die entsprechende Auswahl treffen.

1. Wählen Sie in der Strukturansicht einen Agent, eine Abteilung, eine AD Container oder ein Unternehmen aus.

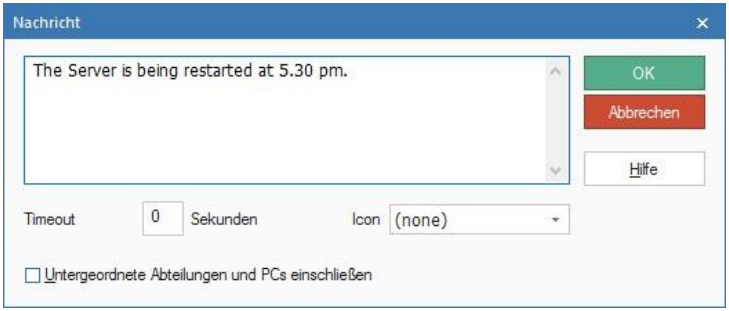
   Hinweis: Die Nachrichtfunktion ist nur von der Strukturansicht des PCs aus verfügbar.

2. Klicken Sie mit der rechten Maustaste und wählen Sie **Nachrich**.

   Oder

   Klicken Sie in der Registerkarte „Werkzeuge" auf das **Nachrichtensymbol**.

3. Das Dialogfeld "Nachricht" wird eingeblendet.



4. Geben Sie die Nachricht ein. Bestimmen Sie, ob die Nachricht an den Agent PCs für eine vorgegebene Zeitdauer gezeigt werden soll. Um anzuzeigen, wie wichtig die Nachricht ist, können Sie ein Symbol wählen, das zusammen mit ihr angezeigt wird. Wenn Sie das Unternehmen oder eine Abteilung gewählt haben, markieren Sie Unterabteilungen und PCs einschließen, damit die Nachricht auch an Unterabteilungen auf dieser Strukturebene gesendet wird. Klicken Sie auf **OK**, um die Nachricht abzusenden.
5. Die Nachricht erscheint dann auf den Agent PCs.

Agentstatus

Mit dem Feature Agentstatus kann ein Konsolebenutzer überprüfen, dass Agent PCs eingeschaltet sind. Dies kann bei der Vorbereitung auf eine Softwareverteilung nützlich sein. Informationen lassen sich auf allen Computern, die der DNA-Datenbank bekannt sind, abrufen.

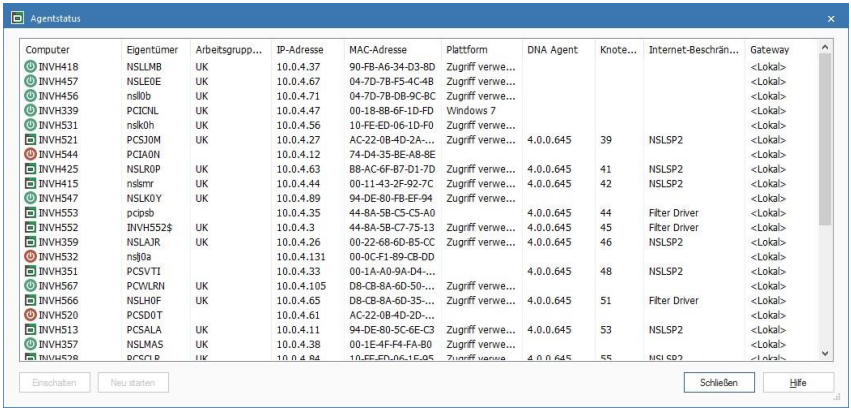
Hinweis: Auf dem PC des Endbenutzers muss eine Wake-on-Lan-Karte installiert und er muss richtig konfiguriert sein. Die DNA Konsole sendet ein Wake-on-Lan-Paket an den Agent. Dieses weist die Arbeitsstation zum Einschalten an.

Einschalten von Rechnern

1. Wählen Sie das gewünschte Unternehmen oder die gewünschte Abteilung in der Strukturansicht.

   Hinweis: Die Funktion „Agentstatus" ist nur von der Strukturansicht des PCs aus verfügbar.

2. Wählen Sie die Registerkarte „Werkzeuge" und klicken Sie auf das Symbol **Agent-Status**.
   Oder
   Klicken Sie mit der rechten Maustaste und wählen Sie **Agentstatus**.
3. Jetzt erscheint der Agent-Status-Dialog.



4. Wenn PCs aktuell nicht eingeschaltet sind, werden nur die IP- und MAC-Adressen angezeigt.
5. Markieren Sie die gewünschten PCs - es lassen sich mehrere Rechner auswählen – und klicken Sie auf Einschalten.

6. Von diesem Dialog aus lässt sich auch der DNA Agent neu starten. Markieren Sie die gewünschten PCs und klicken Sie auf **Neu starten**.

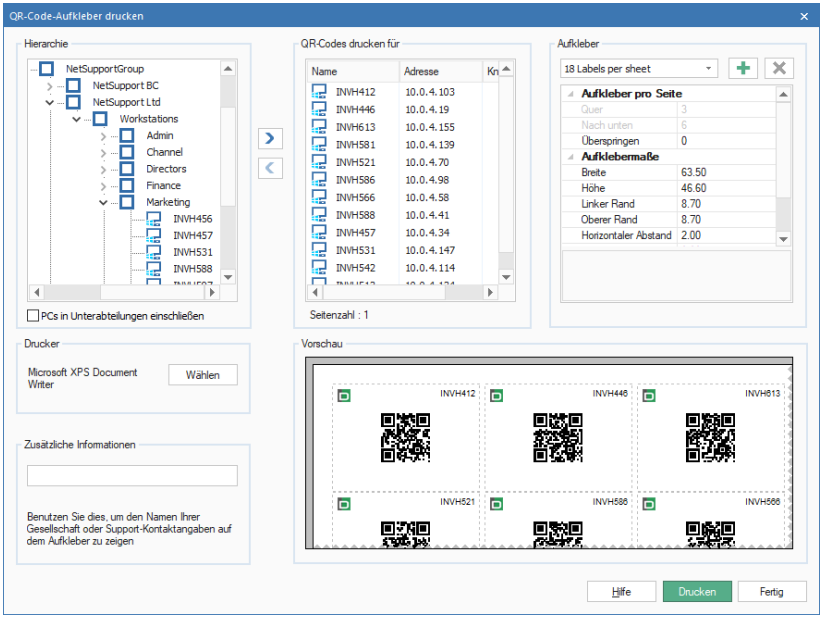
Hinweis: Es kann ein Energiezeitplan eingestellt werden, der es Ihnen ermöglicht, Geräte an den eingestellten Tagen zu bestimmten Zeiten automatisch ein- und auszuschalten. Siehe NetSupport DNA Konfiguration – Energieüberwachungseinstellungen.

Erstellung von QR-Code-Aufklebern

Außerdem hat NetSupport DNA eine QR-Code-Aufklebererstellungs-funktion einschließlich Anzeige der benutzerdefinierten Einzelheiten. Die NetSupport DNA Mobile Konsolen-App enthält einen QR-Code-Scanner, mit dem jedes Gerät augenblicklich identifiziert werden kann, und zwar entweder über einen QR-Code, der auf dem Bildschirm im DNA Agent Fenster angezeigt wird, oder über ein am Gerät angebrachtes Schild.

QR-Code-Aufkleber drucken

1. Klicken Sie in der Registerkarte Tools auf dem **QR-Code drucken** Symbol im Menüband.
2. Nun erscheint der Barcode-Aufkleber drucken Dialog.



3. Wählen Sie in der Hierarchie die Gesellschaft, den AD-Container, die Abteilung oder den Benutzer, für die ein QR-Code erstellt werden soll, indem Sie  wählen. Sie können alle Agents innerhalb einer Gesellschaft, eines AD-Containers oder einer Abteilung wählen, indem Sie **Alle PCs in Unterabteilungen einschließen** wählen.

4. Bestimmen Sie die Aufklebergröße und wie viele Aufkleber pro Bogen gedruckt werden sollen. Klicken Sie auf , um einen benutzerdefinierten Bogen zu erstellen.
5. Wählen Sie, welcher Drucker benutzt werden soll, und fügen Sie, falls erforderlich, etwaige zusätzliche Informationen zum Aufkleber hinzu. Daraufhin erscheint eine Vorschau des Bogens.
6. Klicken Sie auf **Drucken**.

Datenbankwartung

Damit die DNA-Datenbank übersichtlich bleibt, wird empfohlen, dass Sie historische oder unerwünschte Records regelmäßig löschen/archivieren. Das Datenbankwartungsprogramm ermöglicht es, aus der Datenbank von NetSupport DNA überflüssige Daten, Anwendungen und Programme zu löschen, nicht mehr verwendete Agent PCs zu löschen, Benutzer zu löschen, mit einer Export-/Import-Funktion Sicherungskopien wichtiger Daten anzufertigen und Datenspeicherungsregeln zu erstellen, durch die alte Daten automatisch gelöscht werden können.

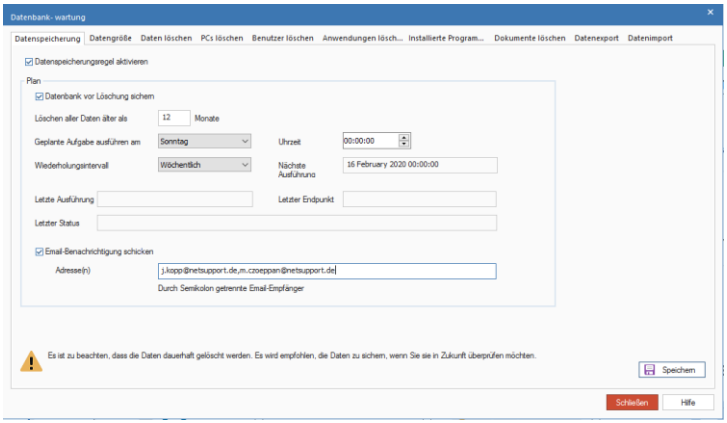
Hinweis: Sie können die Anzahl der Konsolebenutzer, die auf diese Funktion Zugriff haben, beschränken, indem Sie beim Erstellen von Konsolebenutzern Bediener- statt Administratorrechte zuweisen.

1. Klicken Sie in der Registerkarte „Werkzeuge" auf das Symbol **Datenbankwartung**. Wählen Sie die gewünschte Registerkarte.

Datenspeicherung

Damit die Datenbank von NetSupport DNA übersichtlich bleibt, können Sie eine Datenspeicherungsregel erstellen, um alte Daten automatisch zu löschen. Sie können wählen, wie alt die Daten sein müssen, ehe sie gelöscht werden (die Daten können vor dem Löschen gesichert werden), Sie können die Regel so einrichten, dass sie an einem bestimmten Tag/zu einer bestimmten Uhrzeit ausgeführt wird, und Sie können wählen, wie oft die Regel ausgeführt wird. Eine Email-Benachrichtigung kann jedes Mal geschickt werden, wenn die Regel ausgeführt werden soll, wobei ausgewählte Konsolenbenutzer darüber benachrichtigt werden, ob dies erfolgreich war, wie viele Datensätze gelöscht wurden und wie viel Speicherplatz in der Datenbank zurückgewonnen wurde.

Hinweis: Wenn die Regel versagt, wird ein Konsolenalert ausgelöst, der Sie entsprechend informiert.



Die folgenden Daten werden aus der DNA-Datenbank gelöscht:

- Internet-Metering
- History
- Anwendungs-Metering
- Anmeldesitzungen
- Ein-/Ausschaltsitzungen
- USB-Gerätenutzung
- Druckkostendaten
- Softwareverteilung
- eSicherheit - ausgelöste Begriffe, Screenshots und Aufzeichnungen.

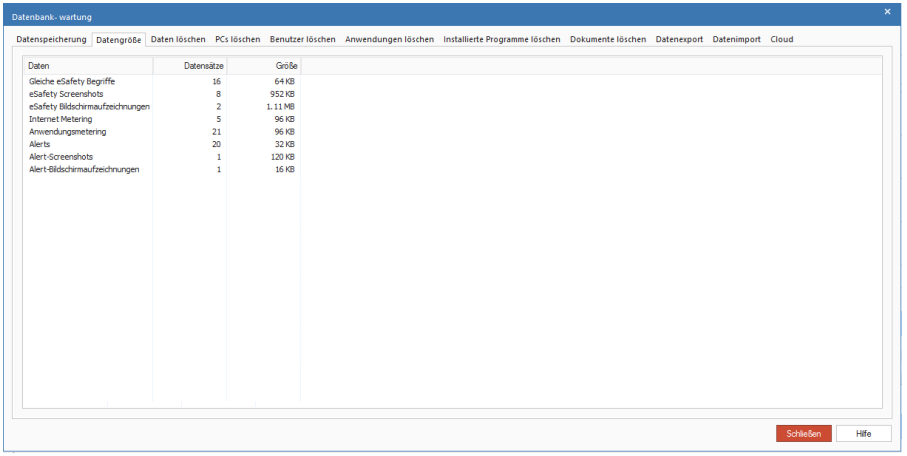
1. **Datenspeicherungsregel aktivieren** wählen.
2. Standardmäßig wird die Datenbank gesichert, ehe sie gelöscht wird. Wenn die Option **Datenbank vor Löschung sichern** deaktiviert wird, führt dies zu einem nicht wiederherstellbaren Datenverlust. Wir empfehlen nur dann, diese Option zu deaktivieren, wenn Sie regelmäßig Ihre eigene Sicherung durchführen.
3. Im Feld **Löschen aller Daten älter als** das Alter der zu löschenden Daten eingeben (alle Daten, die älter sind, werden gelöscht). Die Standardeinstellung ist 12 Monate, das Mindestalter ist 3 Monate und das Höchstalter ist 120 Monate.
4. Im Dropdownmenü **Geplante Aufgabe ausführen am** den Wochentag wählen, an dem die Regel ausgeführt werden soll, und die Uhrzeit eingeben.
5. Wählen Sie im Dropdownmenü **Wiederholungsintervall**, wie oft die Regel ausgeführt werden soll.

6. Das Feld **Nächste Ausführung** wird jetzt mit dem Datum und der Uhrzeit ausgefüllt, an dem die Regel ausgeführt wird. Wenn eine Regel schon ausgeführt worden ist, wird das Datum und ihr Status angezeigt.
7. Eine Email-Benachrichtigung kann geschickt werden; dazu die gewünschte Email-Adresse im Feld **Email-Benachrichtigung schicken** eingeben. Es können mehrere Adressen eingegeben werden. Die Adressen durch ein Semikolon trennen.

   Hinweis: Die Email-Einstellungen müssen konfiguriert werden, ehe Email-Benachrichtigungen geschickt werden können.
8. Auf **Speichern** klicken, um die Datenspeicherungsregel zu aktivieren.

Datengröße

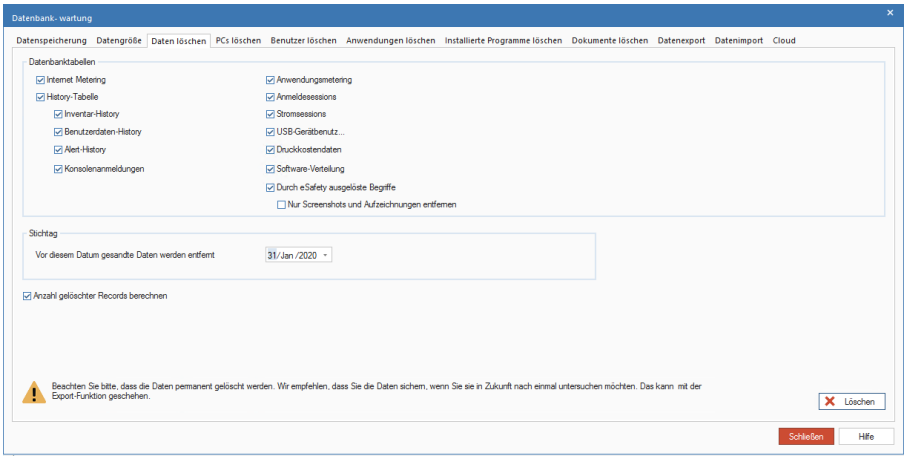
Diese Option bietet einen nützlichen Indikator dafür, wie viele Datensätze - und was noch wichtiger ist, welche damit verbundenen Datenvolumen – aktuell in der DNA Datenbank für die Komponenten eSafety* (Anzahl der Begriffsübereinstimmungen sowie Screenshots und Aufzeichnungen, die mit Schlüsselwortauslösungen verbunden sind), Internet- und Anwendungsmetering und Alerts (Anzahl der Alerts zusammen mit den Screenshots und Aufzeichnungen, die den Alerts angehängt sind) gespeichert sind – was Ihnen die Informationen bietet, die für die erforderliche Haushaltsführung benötigt werden, um die Größe der NetSupport DNA Datenbank auf einen handhabbaren Umfang beschränkt zu halten.



* Diese Funktionen steht nur in der NetSupport DNA Version für das Bildungswesen zur Verfügung.

Daten löschen

Mit dieser Option können Sie aufgrund von einem spezifischen Stichdatum Records aus den DNA-Datenbanktabellen löschen.



Hinweise:

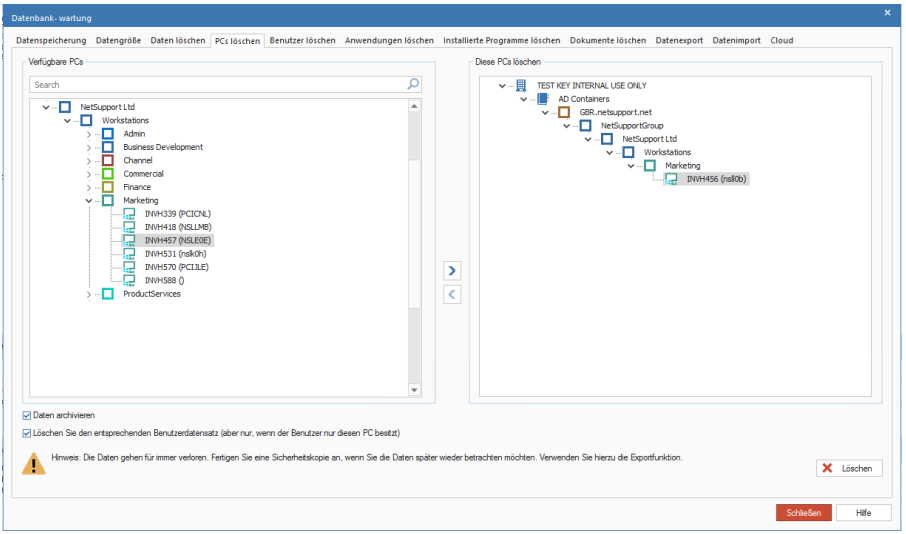
- Wenn Sie in der Geräte-Strukturansicht sind, sehen Sie Daten, die sich auf SNMP-Geräte beziehen.
- In der Bildungswesen-Version von NetSupport DNA erscheint eine Option für von eSafety ausgelöste Begriffe, so dass Sie Daten, die sich auf die Schlüsselwort- und Begriffüberwachung beziehen, entfernen können.

1. Wählen Sie die Datenbanktabellen, die Sie in den Löschvorgang einschließen möchten. *(Internet Metering - dieses Feature ist in der Unternehmen Version nicht verfügbar)*
2. Wählen Sie das gewünschte Stichdatum. Alle vor dem angegebenen Datum aufgezeichneten Records werden gelöscht.
3. Klicken Sie auf **Löschen** und bestätigen Sie, dass Sie fortfahren möchten.
4. Es wird ein Bestätigungsdialogfeld eingeblendet, in dem Sie sehen können, wie viele Records gelöscht wurde.

Hinweis: Wenn Sie nicht wollen, dass im letzten Bestätigungsdialogfeld die Anzahl der gelöschten Records angezeigt wird, deaktivieren Sie die Option **Anzahl gelöschter Records berechnen**.

PCs löschen

Während sich Ihre Installationsbasis verändert, werden Sie u. U. feststellen, dass die Verwaltung von Lizenzstufen schwierig wird, weil die Datenbank Details über Agent PCs, die nicht mehr verwendet werden, enthält. Mit dieser Option können Sie PCs löschen und alle damit verknüpften Daten entfernen.



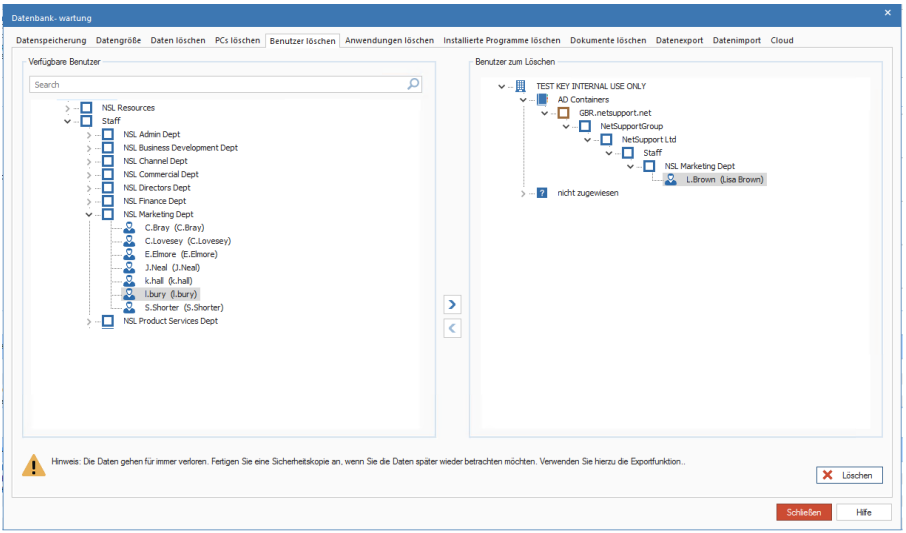
1. Wählen Sie aus der Liste der verfügbaren PCs die PCs, die Sie löschen möchten. Dies kann nach individuellem PC, auf Abteilungsebene, wenn mehrere PC entfernt werden sollen, oder nach Dynamischer Gruppe geschehen.

Hinweis: Um in der Strukturansicht nach einem Element zu suchen, geben Sie den Namen oder einen Teil des Namens des PCs, oder der Abteilung in dem Suchen-Feld ein und klicken Sie auf . Nun wird das erste übereinstimmende Element in der Strukturansicht zusammen mit der Anzahl der gefundenen Übereinstimmungen angezeigt. Sie können diese mit den Pfeilen durchblättern. Klicken Sie auf , um die Suche zu löschen.

2. Klicken Sie auf ›› um die gewählten Objekte zur Liste Diese PCs löschen hinzuzufügen. Individuelle PCs lassen sich aus der Liste entfernen, indem Sie auf ‹‹. klicken. Das ist nützlich, wenn Sie nicht alle PCs in einer Abteilung löschen möchten.
3. Wenn Sie die Daten nicht permanent verlieren wollen, können Sie die Records in einerv Archivdatei speichern. Stellen Sie sicher, dass die Option Daten archivieren markiert ist.
4. Wenn Sie möchten, können Sie die entsprechenden Benutzerdaten auch mit dem PC löschen, wenn der Benutzer nur der Besitzer dieses PCs ist. Stellen Sie sicher, dass die Option **Entsprechenden Benutzerrecord löschen** markiert ist.
5. Klicken Sie auf Löschen. Beim Archivieren werden Sie zur Eingabe eines Dateinamens und Speicherorts aufgefordert. Die Daten werden ins Archiv kopiert, aber bleiben gleichzeitig in der Datenbank. Wenn die Archivierung beendet ist, werden Sie gefragt, ob Sie den Löschvorgang fortsetzen möchten.

Benutzer löschen

Es kann vorkommen, dass die Datenbank nicht mehr benötigte Benutzerdetails enthält. Mit dieser Option können Sie Benutzer löschen und alle damit verknüpften Daten entfernen.



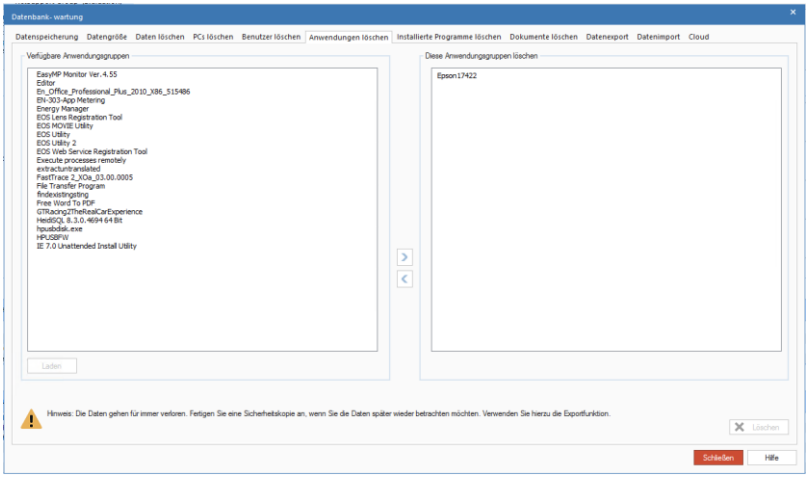
1. Wählen Sie aus der Liste der verfügbaren Benutzer diejenigen aus, die Sie löschen möchten. Dies kann nach individuellem Benutzer, auf Abteilungsebene, wenn mehrere Benutzer entfernt werden sollen, oder nach Dynamischer Gruppe geschehen.

   Hinweis: Um in der Strukturansicht nach einem Element zu suchen, geben Sie den Namen oder einen Teil des Namens der Benutzer oder der Abteilung in dem Suchen-Feld ein und klicken Sie auf . Nun wird das erste übereinstimmende Element in der Strukturansicht zusammen mit der Anzahl der gefundenen Übereinstimmungen angezeigt. Sie können diese mit den Pfeilen durchblättern. Klicken Sie auf , um die Suche zu löschen.

2. Klicken Sie auf , um die gewählten Objekte zur Liste „Diese Benutzer löschen" hinzuzufügen. Individuelle Benutzer lassen sich aus der Liste entfernen, indem Sie auf klicken. Das ist nützlich, wenn Sie nicht alle Benutzer in einer Abteilung löschen möchten.
3. Klicken Sie auf **Löschen**.

Anwendungen löschen

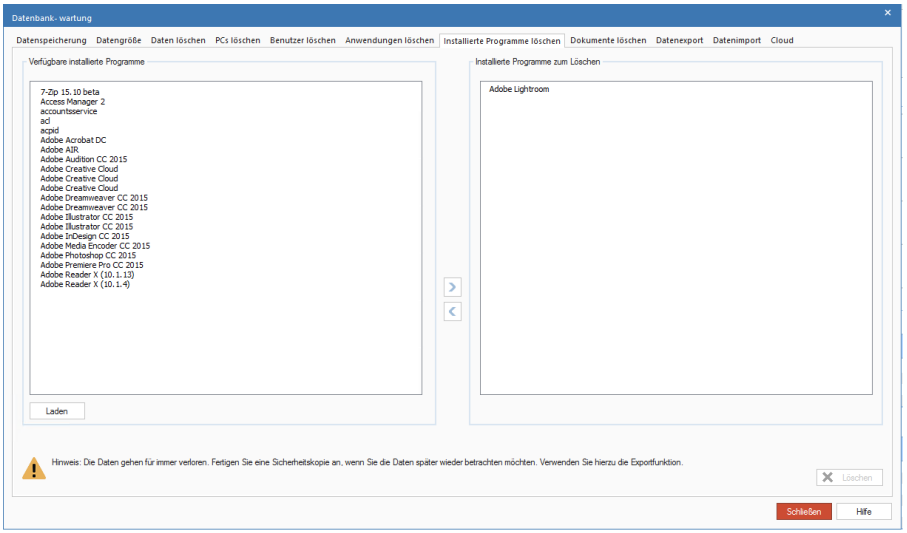
Ermöglicht das Löschen aus der DNA-Datenbank von Anwendungen, auf die durch keine Agent PCs mehr verwiesen wird. Alle Anwendungen, auf die weder in den Anwendungsmetering-, noch den Softwareinventarkomponenten verwiesen wird, sind zum Löschen aufgeführt.



1. Klicken Sie auf „Laden", um die Applikationen unter „Verfügbare Applikationen" anzuzeigen. Wählen Sie die Applikationen, die Sie löschen möchten. Es lassen sich mehrere Objekte auswählen.
2. Klicken Sie auf , um die gewählten Objekte in das Fenster **Diese Anwendungensgruppen löschen** zu verschieben.
3. Klicken Sie auf **Löschen**.

Installierte Programme löschen

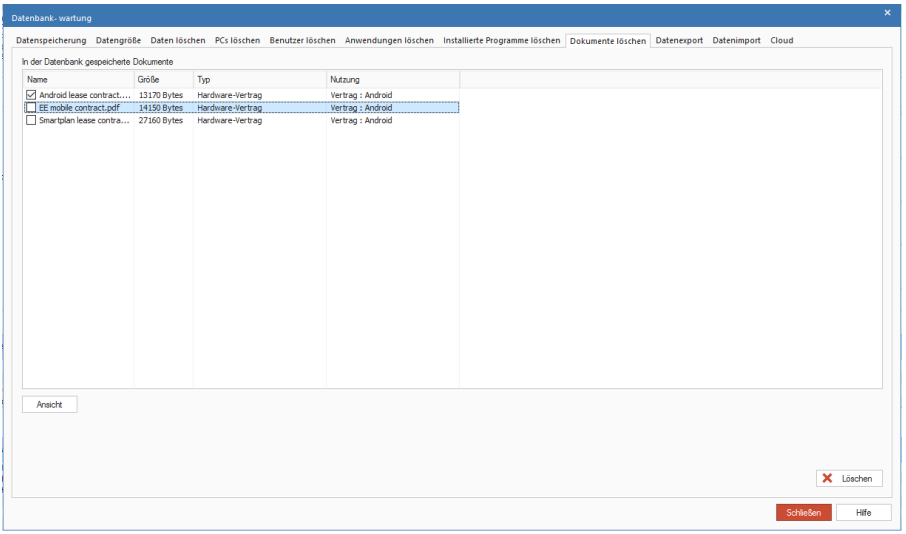
Ermöglicht das Löschen aus der DNA-Datenbank von installierten Programmen, auf die durch keine Agent PCs mehr verwiesen wird. Alle installierten Programme, auf die nicht durch die Applikationsmetering oder Softwareinventarisierungskomponenten verwiesen wird, werden zum Löschen aufgelistet.



1. Klicken Sie auf „Laden", um die installierten Programme in der Liste „Verfügbare installierte Programme" anzuzeigen. Wählen Sie das installierte Programm, das Sie löschen möchten. Es lassen sich mehrere Objekte auswählen.
2. Klicken Sie auf , um die gewählten Objekte in das Fenster „Diese installierten Programme löschen" zu verschieben.
3. Klicken Sie auf **Löschen**.

Registerkarte Dokumente löschen

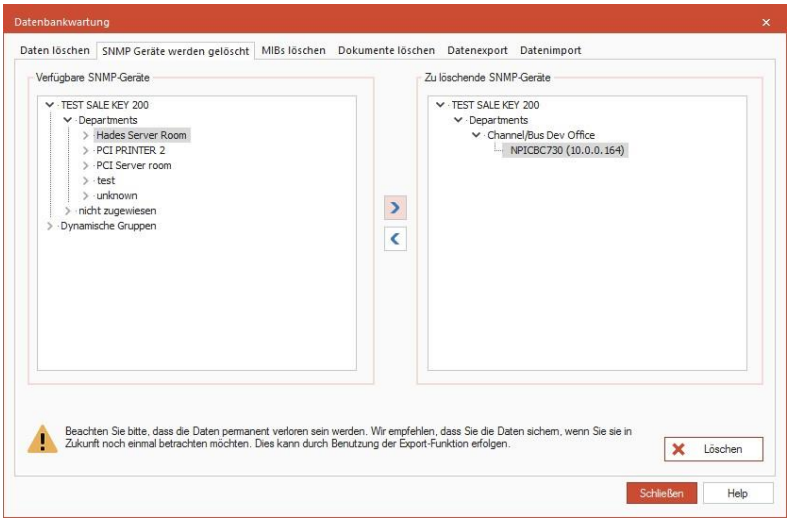
Diese Option ermöglicht es Ihnen, Dokumente aus der NetSupport DNA Datenbank zu löschen.



1. Wählen Sie das Dokument, das Sie entfernen möchten.
2. Um Dokumente anzuzeigen, bevor Sie sie entfernen, klicken Sie auf **Ansicht**.
3. Klicken Sie auf **Löschen** und bestätigen Sie, dass Sie fortfahren möchten.

SNMP-Geräte löschen

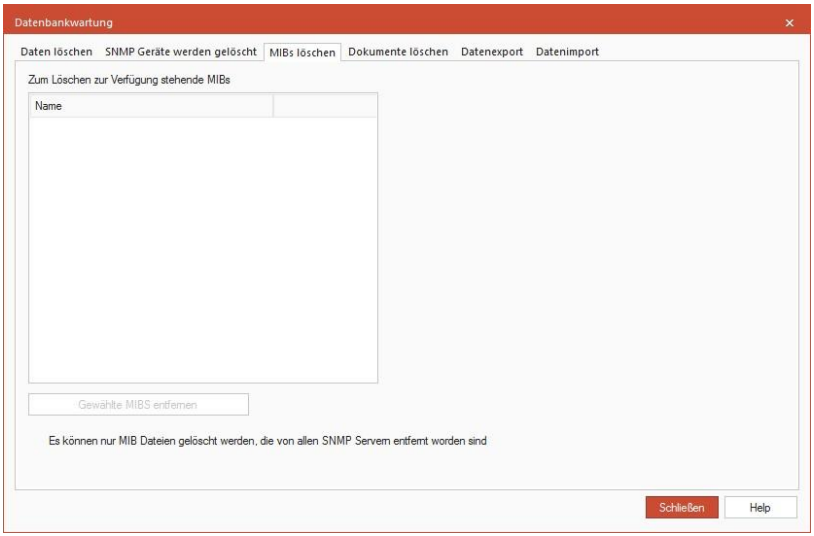
Sie könnten feststellen, dass die Datenbank Details von Geräten enthält, die nicht mehr gebraucht werden. Diese Option ermöglicht es Ihnen, Geräte zu löschen und die damit verbundenen Daten zu entfernen.



1. Wählen Sie in der Liste Zur Verfügung stehende SNMP-Geräte die zu entfernenden Geräte. Dies kann über das individuelle Gerät, auf Abteilungsebene (wenn mehrere Geräte entfernt werden sollen) oder nach Dynamischer Gruppe geschehen.
2. Klicken Sie auf  , um die gewählten Objekte zu der Liste der zu löschenden SNMP-Geräte hinzuzufügen. Individuelle Geräte können aus der Liste entfernt werden, indem Sie auf  klicken. Dies ist nützlich, wenn nicht alle Benutzer in einer Abteilung entfernt werden sollen.
3. Klicken Sie auf **Löschen**.

MIB löschen Registerkarte

Diese Option ermöglicht es Ihnen, MIB Dateien zu löschen, die nicht mehr gebraucht werden.



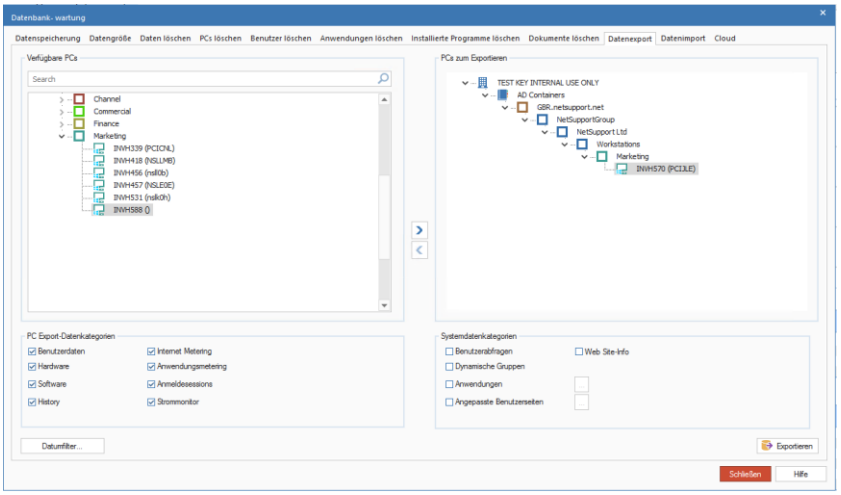
Hinweis: Eine MIB kann nur dann gelöscht werden, wenn sie auf dem Gerät gelöscht worden ist, und die Daten müssen aus der NetSupport DNA Datenbank entfernt werden.

1. Wählen Sie die geforderte MIB in der Liste und wählen Sie dann Gewählte MIBs entfernen.

Daten exportieren

Mit dieser Option lassen sich die Daten in der DNA-Datenbank exportieren. Dies kann für den Fall, dass die Datenbank beschädigt wird, als Sicherungskopie dienen oder die Daten lassen sich in eine andere Datenbank importieren.

Hinweis: Wenn Sie in der Geräte-Strukturansicht sind, sehen Sie Daten, die sich auf SNMP-Geräte beziehen.



1. Wählen Sie in der Struktur Verfügbare PCs den/die Agent(s), von dem/denen Sie Daten exportieren möchten. Klicken Sie auf  um die Daten in das Fenster PCs zum Exportieren zu übertragen. (*Internet Metering - dieses Feature ist in der Unternehmen Version nicht verfügbar)*

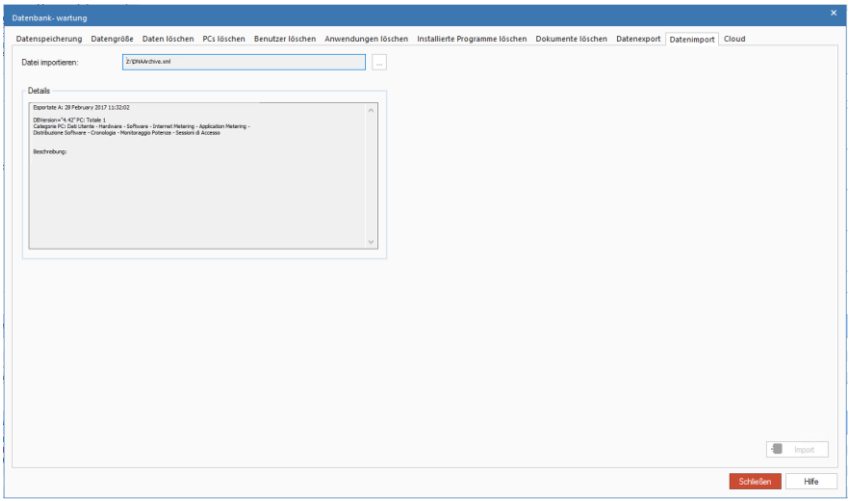
   Hinweis: Um in der Strukturansicht nach einem Element zu suchen, geben Sie den Namen oder einen Teil des Namens des PCs, oder der Abteilung in dem Suchen-Feld ein und klicken Sie auf . Nun wird das erste übereinstimmende Element in der Strukturansicht zusammen mit der Anzahl der gefundenen Übereinstimmungen angezeigt. Sie können diese mit den Pfeilen durchblättern. Klicken Sie auf , um die Suche zu löschen.

2. Heben Sie die Markierung aller Datenkategorien, die Sie nicht einschließen möchten, auf.
3. Die Menge der exportierten Daten lässt sich durch Anwendung eines Datenfilters noch weiter beschränken.
4. Geben Sie an, ob zusätzliche Systemdaten eingeschlossen werden sollen. Für Anwendungen und benutzerdefinierte Seiten klicken Sie auf  und wählen die Objekte, die Sie einschließen möchten.
5. Klicken Sie auf **Export**, wenn Sie fertig sind. Geben Sie einen Namen für die XML-Datei, die erstellt werden wird, ein. Sie werden zur Eingabe einer passenden Beschreibung aufgefordert. Dies wird dabei helfen, die Daten beim erneuten Import zu identifizieren.

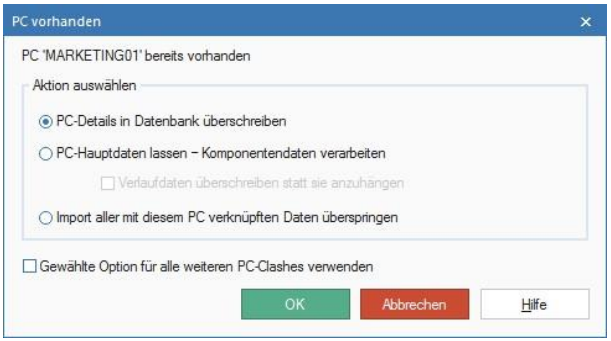
6. Klicken Sie auf **OK**. Wenn der Export beendet ist, erscheint eine Bestätigungsmeldung.

Daten importieren

Zum erneuten Import von vorher exportierten Daten.



1. Klicken Sie auf … und suchen Sie nach der gewünschten Exportdatei.
2. Das Fenster "Details" liefert eine Zusammenfassung des Dateiinhalts.
3. Klicken Sie auf **Import**. Wenn Konflikte zwischen den importierten Daten und bereits vorhandenen Informationen möglich sind, werden Sie zur Durchführung der zu ihrer Behebung nötigen Aktionen aufgefordert.



PC Details in der Datenbank überschreiben

Der Datenimport wird fortgesetzt. Es werden dabei aktuelle Informationen in der Datenbank überschrieben.

PC-Hauptdaten stehen lassen – Komponentendaten verarbeiten

Nur auf Komponenten bezogene Daten importieren, Anwendungsmetering, usw. Vorhandene Benutzer-/PC-Angaben werden nicht überschrieben.

Verlaufdaten überschreiben, statt sie anzuhängen

Die Verlaufdaten werden überschrieben statt angehängt.

Import aller Daten zu diesem PC überspringen

Import abbrechen.

Gewählte Option für alle weiteren PC-Konflikte verwenden

Gewählte Option als Standard für alle zukünftigen Vorgänge einstellen.

4. Wenn der Import beendet ist, erscheint eine Bestätigungsmeldung.

Cloud

In bestimmten Fällen kann unser technisches Supportteam Ihnen SQL-Skripte zur Verfügung stellen, um PC-Duplikate zu löschen. Wenn Sie die Cloud-Konsole von NetSupport DNA verwenden, müssen Sie PC-Duplikate von hier aus löschen, damit Windows und die Cloud-Konsole synchronisiert sind. Diese Option ermöglicht es, PC-Duplikate und die zugehörigen Daten aus der Cloud-Konsole zu löschen.

Hinweis: Diese Registerkarte wird nur in der Version von NetSupport DNA für das Bildungswesen angezeigt und nur dann, wenn die Cloud-Konsole aktiviert ist.

1. Auf **PC-Duplikate aus der Cloud-Datenbank löschen** klicken.
2. Eine Bestätigung wird eingeblendet, die fragt, ob Sie die PC-Duplikate aus der Cloud-Konsole löschen möchten. Klicken Sie auf **Ja**.

NetSupport DNA Agent-Fenster

Das Agent-Fenster bietet den Agents den Status der Schlüsselkomponenten, die Auswirkungen auf sie haben können, sowie eine Übersicht über NetSupport DNA.

Hinweis: Das Agent Fenster steht nur für NetSupport DNA Windows Desktop und Mac Agents zur Verfügung.

Wenn ein Agent das NetSupport DNA Agent Symbol in der Taskleiste rechts anklickt, erscheint eine Liste von Optionen.

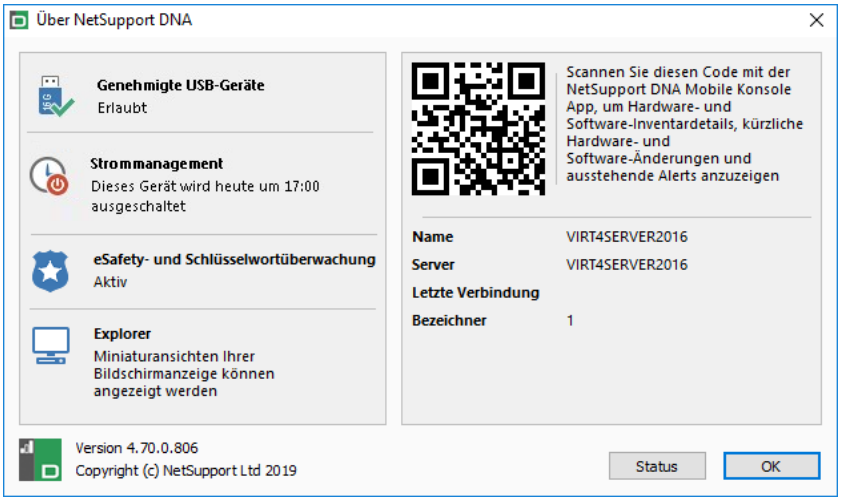
Von hier aus kann der Windows Agent:

- das Agent-Hauptfenster öffnen
- einen anderen angemeldeten Benutzer/In suchen und ihm eine Nachricht senden (wenn dies an der Konsole aktiviert ist)
- benutzerkonto verwalten (wenn dies an der Konsole aktiviert ist)
- ein Anliegen melden*
- auf eSafety Ressourcen zugreifen*
- feststellen, ob ein Energieplan angewendet wird
- ein Paket anfordern
- etwaige USB-Gerät-Genehmigungsanforderungen sehen
- Benutzerangaben bearbeiten (diese Option kann in der Konsole deaktiviert werden).

Der Mac Agent kann:

- ein Anliegen melden*
- auf eSafety Ressourcen zugreifen*
- die NetSupport DNA Website öffnen
- das Agent-Hauptfenster öffnen.

Um das Agent-Hauptfenster zu öffnen, wählen Sie auf der Liste **Über DNA**.



Die Agents Der Agent erhält Details über NetSupport DNA und den Server, mit dem er verbunden ist. Es wird ein QR-Code angezeigt, der von der NetSupport DNA Mobilkonsole gescannt werden kann. Dies ermöglicht es den Technikern, den PC zu identifizieren und die Hardware- und Software-Inventardetails, kürzliche Hardware- und Softwareänderungen und ausstehende Alerts zu sehen.

Windows Agents wird auch den Status von genehmigten und nicht-genehmigten USB-Geräten sehen, ob ein Stromzeitplan oder eine Inaktivitäts-Richtlinie eingestellt ist, ob eSafety* (Anliegen melden und Begriffe überwachen) aktiv ist, und kann außerdem den Status für Explorer-Modus sehen.

Der Agent kann den gegenwärtigen Status der einzelnen Komponenten sehen, indem er auf **Status** klickt.

* Diese Funktionen stehen nur in der NetSupport DNA Version für das Bildungswesen zur Verfügung.

KONTAKTANGABEN

Deutschland, Österreich und Schweiz
www.pci-software.de
Technischer Support: support@netsupportsoftware.com
Verkauf: *sales@pci-software.de*

Großbritannien und international
www.netsupportsoftware.com
Technischer Support: support@netsupportsoftware.com
Verkauf: sales@netsupportsoftware.com

Nordamerika
www.netsupport-inc.com
Technischer Support: support@netsupportsoftware.com
Verkauf: *sales@netsupport-inc.com*

Kanada
www.netsupport-canada.com
Technischer Support: *support@netsupportsoftware.com*
Verkauf: *sales@netsupport-canada.com*

Japan
www.netsupportjapan.com
Technischer Support: *support@netsupportsoftware.com*
Verkauf: *sales@netsupportjapan.com*