TAKE CONTROL
IT'S YOUR SECURITY

TAMOSOFT

NetResident®

Help Documentation
Version 3.0

Contents

Introduction

Overview

NetResident is an advanced network content monitoring application that captures, stores, analyzes, and reconstructs network events such as e-mail messages, Web pages, downloaded files, instant messages, and voice conversations. NetResident uses cutting-edge monitoring technology to capture the required data from the network, saves it to a database, reconstructs it, and displays this content in an easy-to-understand format.

While NetResident is similar to network analyzers in many respects, it focuses on high-level protocols that are used to transfer content over the Internet or LAN. With NetResident, you do not need a profound understanding of networking technologies, have to use complex packet capturing and analysis software, or dig through network packets in order to reconstruct the actual data; NetResident does all the work for you and presents the high-level content as viewed by end users in your LAN. A convenient application console presents a clear picture of all captured network events that can be searched, grouped, or sorted by different criteria.

NetResident is used by businesses to detect sensitive information leaks; by government law enforcement, security agencies, and private surveillance providers for lawful interception needs; by forensic experts to inspect evidence and gain crucial information needed for criminal investigations; and even by parents to monitor their children's communication on the Internet.

NetResident offers many benefits to your organization. Unlike many data-loss detection solutions, NetResident can be quickly and easily deployed by the organization's network administrator and does not require substantial changes in the existing network infrastructure or software.

System Requirements

NetResident requires a portable computer with the following minimal system requirements:

- Microsoft Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2. Both 32- and 64-bit versions are supported.
- Intel Core 2 or similar CPU. A multi-core CPU, such as Intel i5 or i7, is recommended.
- 1 GB of RAM.

What Network Content NetResident Can Analyze

NetResident can analyze dozens of protocols. The table below summarizes its protocol analysis capabilities.

Short Name (used in the interface)	Protocol(s)	Description
Web	HTTP, HTTPS	Web contents, such as Web pages. Used mostly by Web browsers.
FTP	FTP	File transfer protocol. Used for downloading and uploading files from/to FTP servers.
Mail	POP3, SMTP, IMAP	Sending and receiving e-mail.
Telnet	TELNET	Telnet console communications.
News	NNTP	Reading and posting news to newsgroups.
ICQ/AIM	ICQ/AIM	Used in ICQ, Pidgin, Miranda, QIP, and a few other instant messaging applications.
Jabber	XMPP	Used in Psi, Gajim, Pidgin, Miranda, and many other instant messaging applications.
IRC	IRC	Used in KVIrc, mIRC, XChat, and many other applications.
Yahoo	Yahoo Messenger Protocol	Used in Yahoo Messenger
WebMail	Web-based E-mail Systems	Sending and receiving e-mail using Web-based services. Currently, NetResident supports Gmail, Live mail, AOL, Yahoo! Mail, Web.de, Gmx.de.
WebSocial	Social Networks	Posting messages in social networks. Currently, NetResident supports Twitter, Facebook, LinkedIn, MySpace, Xing, Google+, Tumblr, StudiVZ, MeinVZ, VKontakte, SchuelerVZ, Odnoklassniki, LiveInternet, and LiveJournal.
FileShare	File Sharing Systems	Downloading and uploading files from/to file sharing services.
OWA	Outlook Web Access	Sending e-mails in Outlook Web Access.
iCloud	iCloud	Files downloaded from iCloud.
MRA	Mail.ru Agent	Messaging and group chats in Mail.ru Agent.
VoIP	VoIP	Voice calls using SIP and H.323 protocols and RTP voice streams.

Encrypted Traffic Analysis

Unlike standard, non-encrypted network traffic analysis that can be performed passively, encrypted traffic analysis requires rather complex proactive interception techniques. To perform encrypted traffic decryption, NetResident acts as a “middleman” between the client and server.

Specifically, for each encrypted connection, NetResident generates a new temporary certificate that is signed using a self-signed root certificate. The root certificate is installed as a trusted certificate if/when you install NetResident agents.

While this method is very efficient for encrypted traffic analysis, some users might consider it excessively intrusive and insecure, as NetResident becomes capable of intercepting all the encrypted communications

on the computers on which agents are installed. If you do not trust NetResident and do not want this interception to occur, do not install NetResident agents.

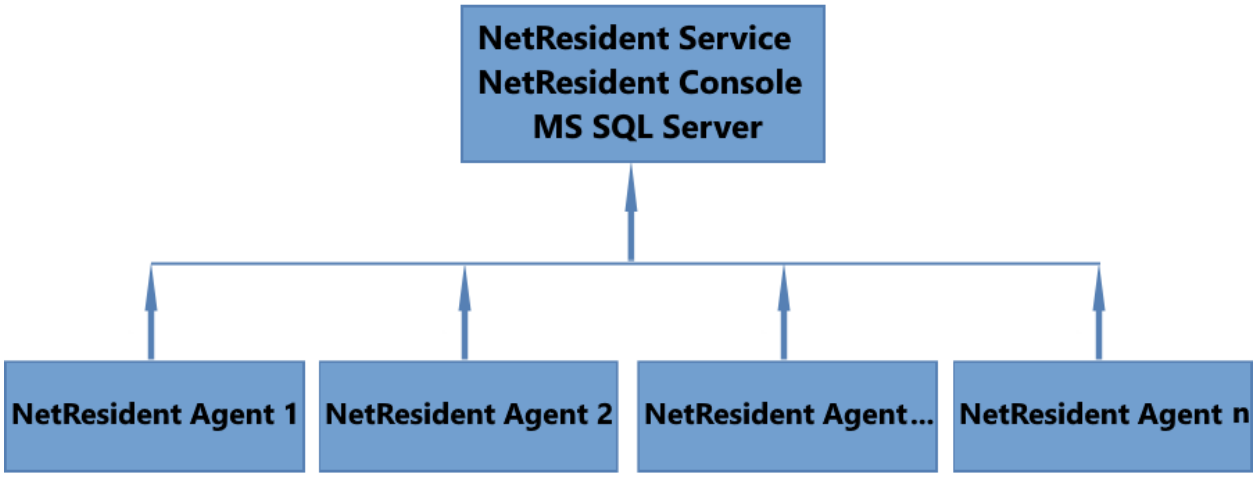
What's New in NetResident 3.0

NetResident 3.0 has been completely redesigned. It comes with a new engine and user interface. The following key changes have been implemented:

- New, improved user interface.
- Use of Microsoft SQL server for data storage.
- Distributed architecture using remote agents.
- Ability to decrypt encrypted communications.

NetResident Architecture

NetResident consists of the three main components: a service, a console, and agents. The picture below illustrates a typical NetResident installation that includes a computer running NetResident service, a console, an SQL server with the database (all of them usually installed on the same computer), and many agents installed on client computers on the LAN.



The core component of the application is the **NetResident Service**. The key function of the service is to link the components into a single system, capture network communications that go through the computer on which it is running, receive data from the agents, analyze the collected data, and store them in a database.

NetResident Agents are optional system components. They capture network communications that take place on the computers on which they are installed. Agents are instrumental for two reasons: They provide visibility into the traffic of LAN computers that otherwise cannot be seen from the "central" computer running NetResident service, and they are capable of decrypting encrypted traffic of the computer they are running on. Typically, agents are installed on multiple computers (one per computer), but deploying agents is not mandatory. If you want to analyze only the traffic that is visible to the computer running NetResident service, and if you do not need to analyze encrypted communications, then NetResident service is all that you need.

The **NetResident Console** is the only system component that has a user interface. The console allows you to interact with NetResident: explore the captured data, search and filter them, change system settings, and perform many other tasks. Normally, the console is installed on the same computer on which the NetResident service is installed, but this is not required. You can install it on any other computer, even in different LAN segments, as long as the console can connect to the computer running the NetResident service over the Internet.

The next chapter discusses deployment strategies in detail.

Deploying the Application

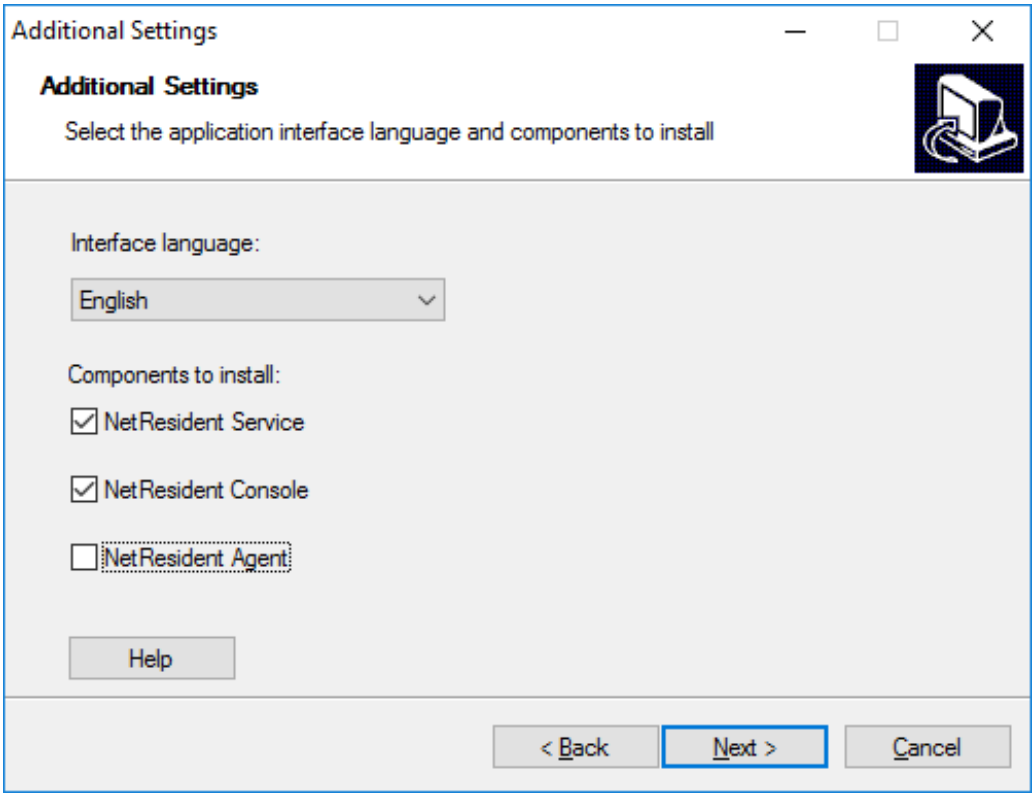
Before You Begin: Network Visibility

The key to successful network monitoring is the visibility of network traffic. If you need to monitor only one computer on the network, there is no network visibility question: You can simply install and run NetResident on that computer. However, if you need to monitor multiple computers on a LAN, it is important that you understand how to achieve network visibility (i.e., the ability to "see" network traffic of other stations from a single observation point).

In brief, to monitor other computers on your LAN, you need to install NetResident on a gateway computer or use a switch with the "port mirroring" feature. There are many possible network layouts, so if you are new to network monitoring, we recommend that you read the detailed, illustrated white paper by TamoSoft, Promiscuous Monitoring in Ethernet and Wi-Fi Networks (a PDF version is also available.)

Step 1: Deploying the NetResident Service and Console

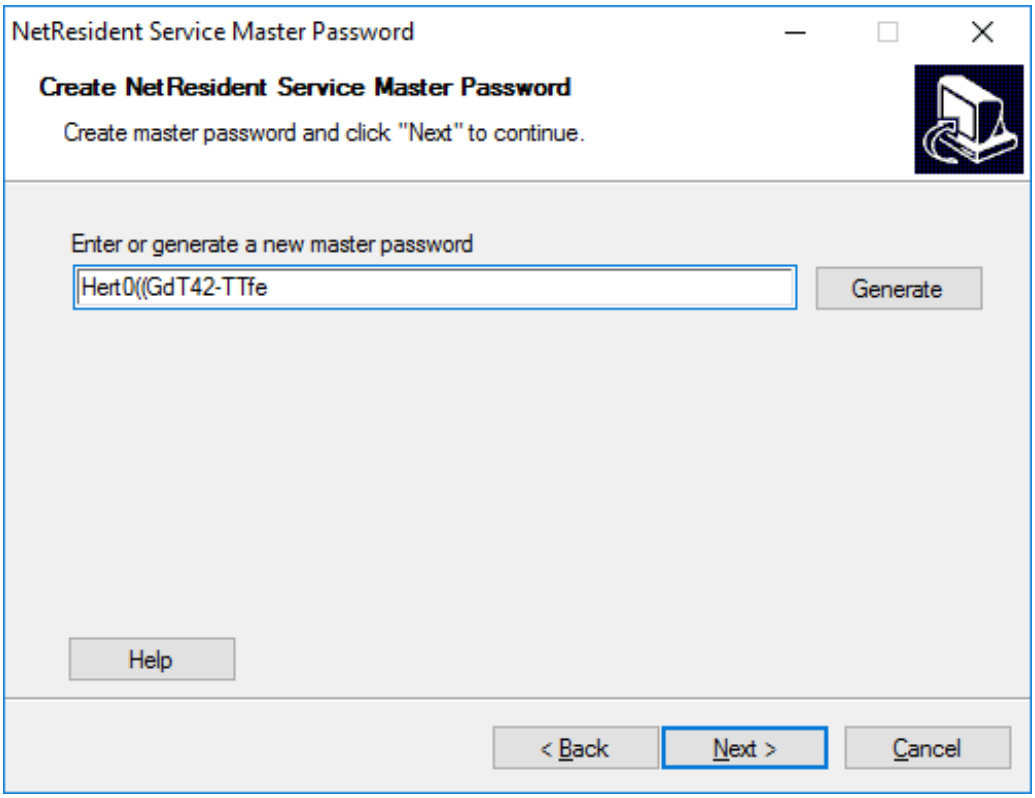
This is the first and, in many cases, only step in deploying NetResident. If you install NetResident on a computer that has network visibility sufficient for your purposes, such as a gateway computer through which LAN clients communicate with the Internet, or a computer that has an Ethernet adapter connected to the mirror port of a switch, or simply a standalone computer the communications of which you want to monitor, installing the NetResident service and console is sufficient. In this scenario, you may not need to install NetResident agents. The image below illustrates the setup screen on which you select only the service and console components:



The advantage of “agentless” data collection is simplicity: The application is installed on a single machine and does not require any additional steps. The drawbacks of this approach are as follows:

- It is often impossible to have access to all LAN traffic from a single observation point.
- The only way to intercept SSL-encrypted traffic, such as HTTPS, is to install agents. That is because passive monitoring using the NetResident service cannot decrypt encrypted data.

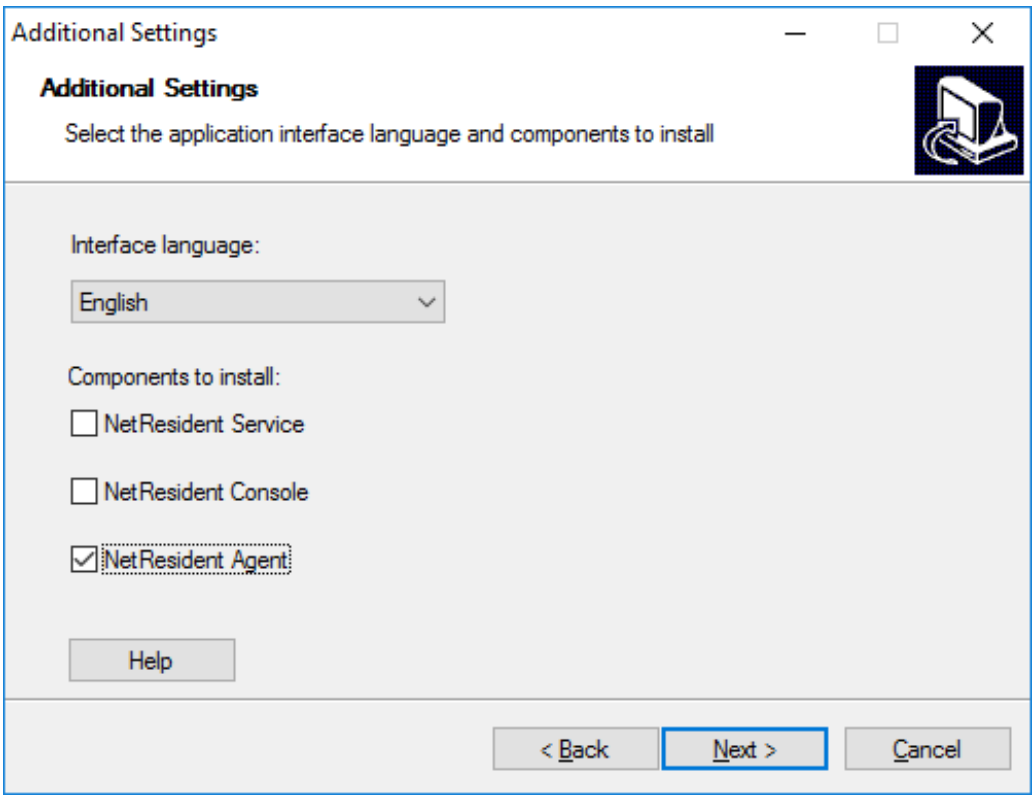
On the next screen, you will be prompted to create a master password that will be used by the NetResident service for authenticating all system components. The master password must be created when you install the NetResident service for the first time. You should enter a long, hard-to-guess password and remember it, because it will be required to by other system components. You can use the **Generate** button to have the installer generate a random 20-character password for you.



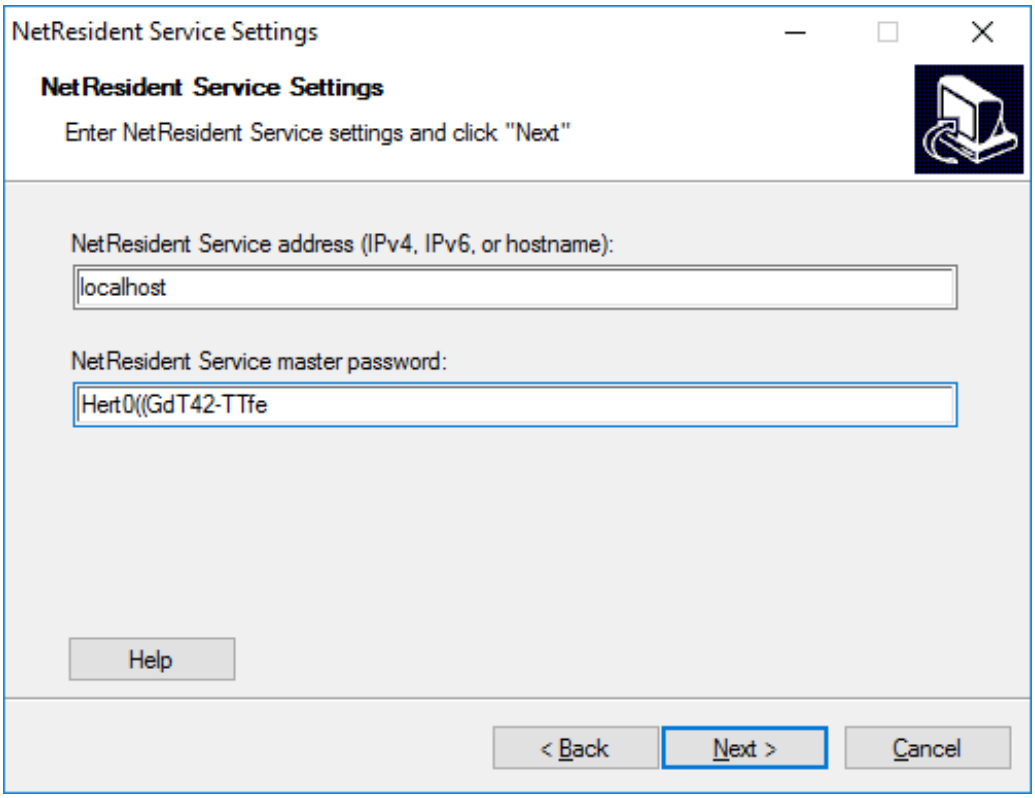
Step 2: Deploying NetResident Agents

This is an optional step that is required if you want to monitor encrypted communications and/or if it is impossible for the NetResident service to “see” all traffic on your LAN for some reason (e.g., multiple LAN segment, missing “port mirroring” feature in the LAN switches, etc.)

If you have decided to deploy agents, you must run the setup on each machine on which you want to monitor network traffic and select the specific component, namely **NetResident Agent**, during setup, as illustrated below:



On the next screen, you will be prompted to enter the data necessary to connect to the NetResident service.



The **address** field must be used to provide the agent with the IPv4 or IPv6 address or hostname of the computer on which the NetResident service has been previously installed, as the agents must “know” the address to which they would connect and send collected data. If you are not sure about the IP address or

the hostname of the computer running the NetResident service, execute the *ipconfig /all* command on that computer to find this information. In the **master password** field, you should provide the password that you previously chose when you installed the NetResident service.

Ensuring Connectivity Between the System Components

To be able to send monitoring data to the NetResident Service, the agents must have TCP/IP connectivity to the service. LAN administrators should note the following when configuring firewalls:

- The service is a server; the agents are clients.
- The service is listening for incoming connections on port 2111.

When you install the NetResident service, it creates a Windows firewall rule automatically. Third-party firewalls might require manual configuration.

Tips and Tricks

- Normally, the NetResident service and the NetResident console are installed on the same computer. However, you are free to install the console on any other computer, as long as it has network connectivity to the computer running the service.
- If you want to monitor encrypted communications on the computer on which the NetResident service is installed, install all three components (service, console, and agent) on the same computer. In the **service address** field, enter “localhost.”

Setting Up the Database

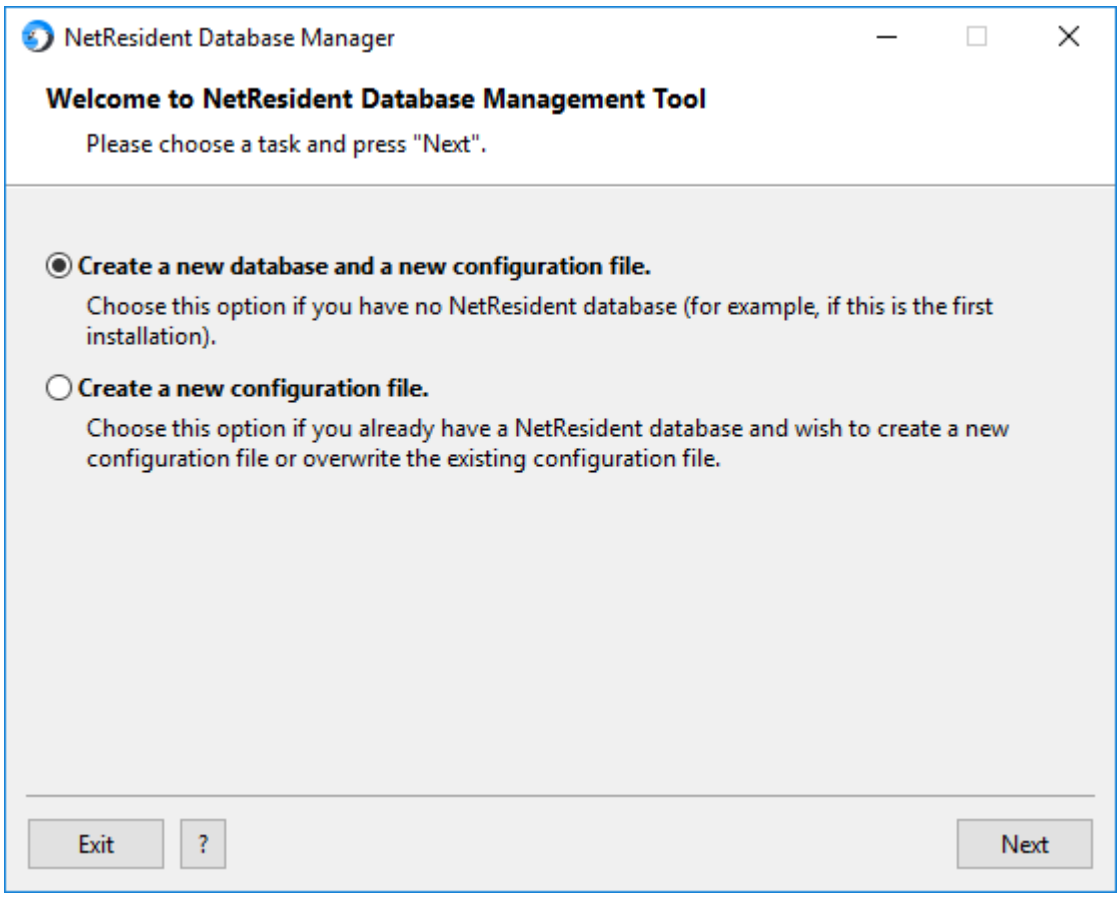
NetResident saves all of the network content that has been captured and analyzed in a Microsoft SQL Server database, which ensures high performance and flexibility in content searching. Therefore, to be able to use NetResident, you can either use an existing installation of Microsoft SQL Server (version 2008 R2 or higher is required) deployed on one of the computers on your LAN, or make a new installation with the help of the **NetResident Database Manager**, which will help you automatically download and install Microsoft SQL Server 2014 SP2 Express or Microsoft SQL Server 2016 SP1 Express, depending on your Windows version and its bitness.

The SQL server may be installed either on the computer on which the NetResident Service is installed or on a different computer on your LAN. If the SQL server is installed on a different computer, please make sure that SQL Server Browser is also installed and running on that computer.

> The Express edition of Microsoft SQL server has a limit of 10 GB per database. In order to bypass this restriction, the **NetResident Database Manager** allows you to create multiple databases with different names.

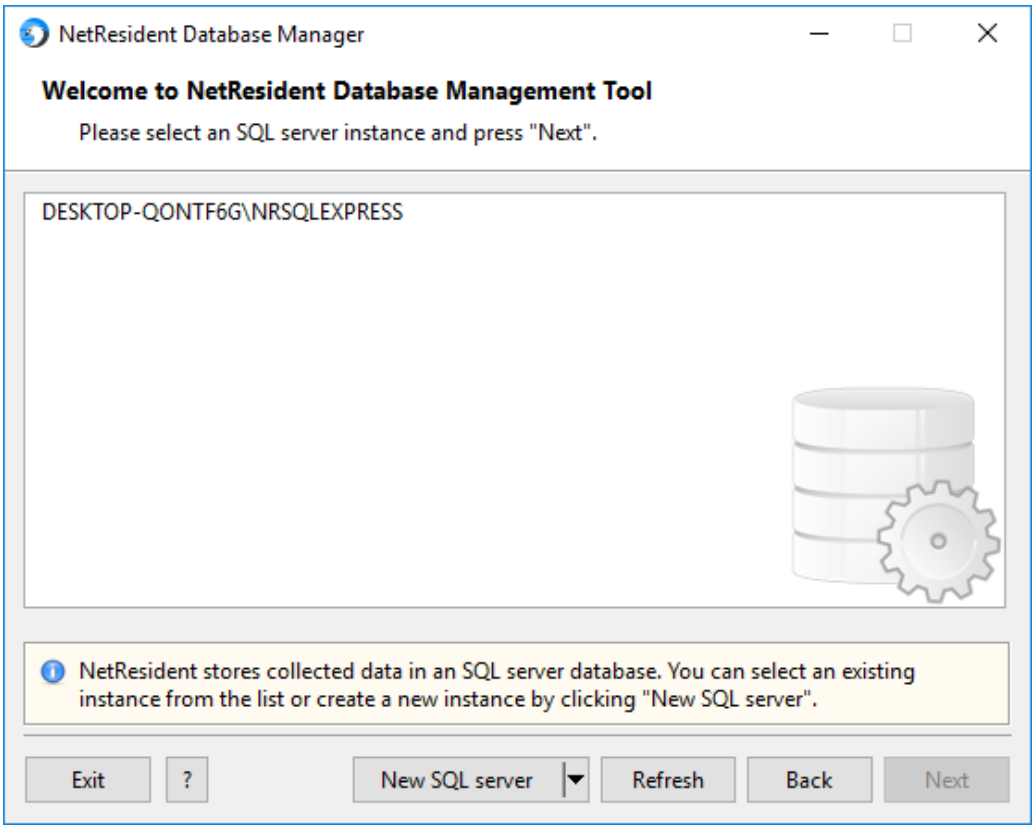
Step 1: Creating a New Database and Configuration File

The **NetResident Database Manager** is automatically launched after you have installed the NetResident Service. The first step of the wizard creates a new database to be used with NetResident and a new configuration file for the NetResident service. The function of the configuration file is to "tell" the NetResident service the database location and name. If this is the first installation, you should select **Create a new database and a new configuration file**, but if you have already created a database in the past (e.g., if you are reinstalling NetResident), you should select **Create a new configuration file**.



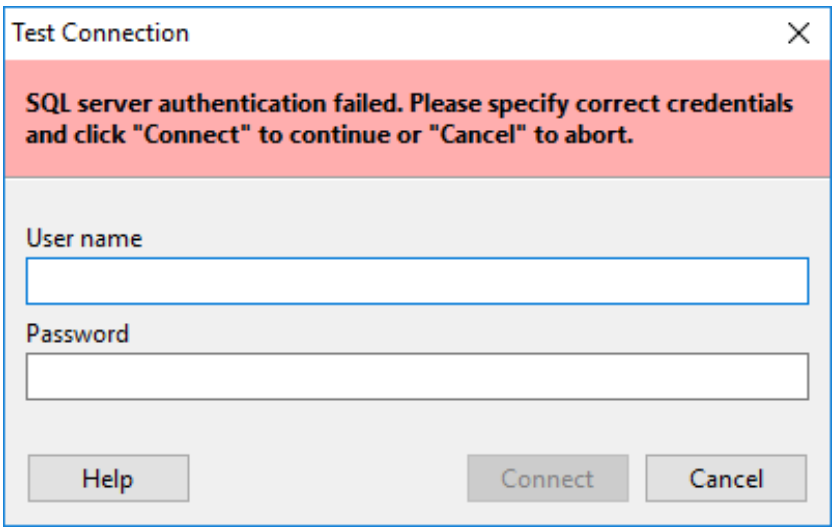
Step 2: Selecting an SQL Server

In this step, the wizard allows you to either select an existing SQL server instance for use with NetResident or create a **New SQL server**:



If you create a new SQL server, you should specify a new server name, which must be unique for the given computer. After that, the wizard will automatically download Microsoft SQL Server 2014 SP2 Express or Microsoft SQL Server 2016 SP1 Express from Microsoft's official Web site (an Internet connection is required) and then install it. Once the installation has been completed, a new SQL server instance will appear on the list of available servers.

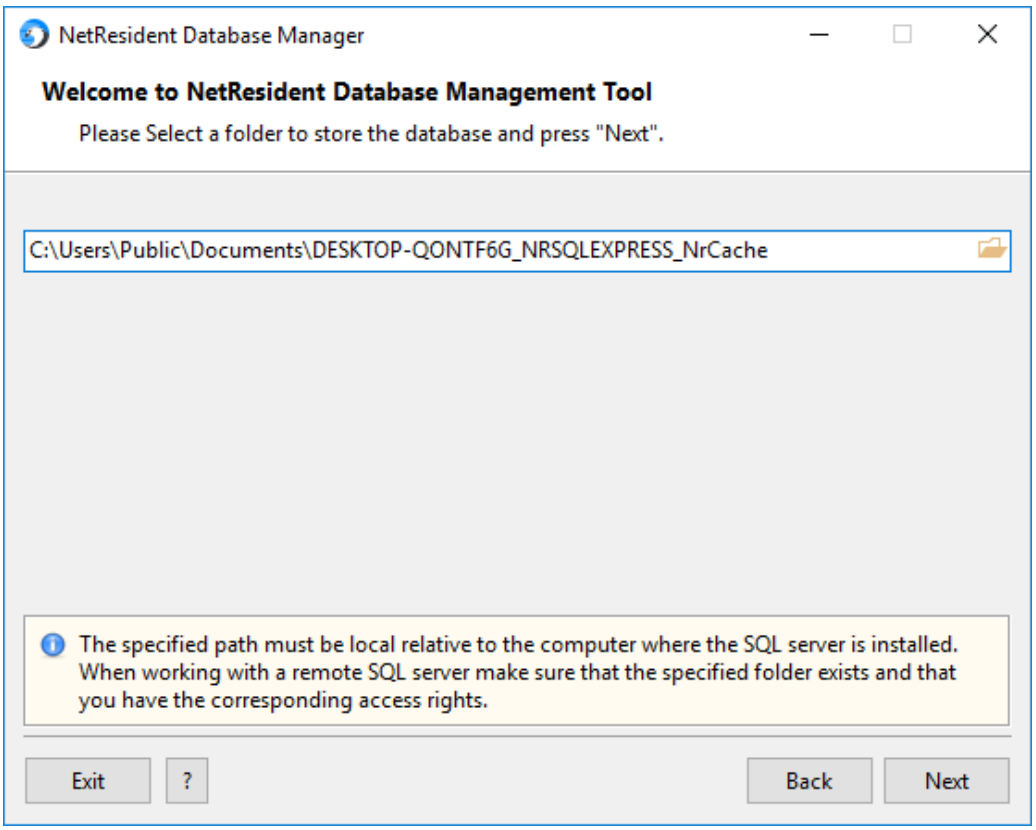
If you decide to use an existing SQL server, select one of the server instances listed in the wizard window. You may want to click **Refresh** to update the list of servers to display all running server instances on your LAN and the local host. Once you have selected an existing SQL server, click **Next** to have the **NetResident Database Manager** connect to the selected SQL server. If the connection attempt fails, you will see the following dialog:



Typically, this might happen when trying to connect to an SQL server that was not installed by the **NetResident Database Manager**, in which case you should enter the correct SQL server login and password. You should contact the server administrator to get the credentials or try to use the default "sa" account; see this document if you encounter a problem.

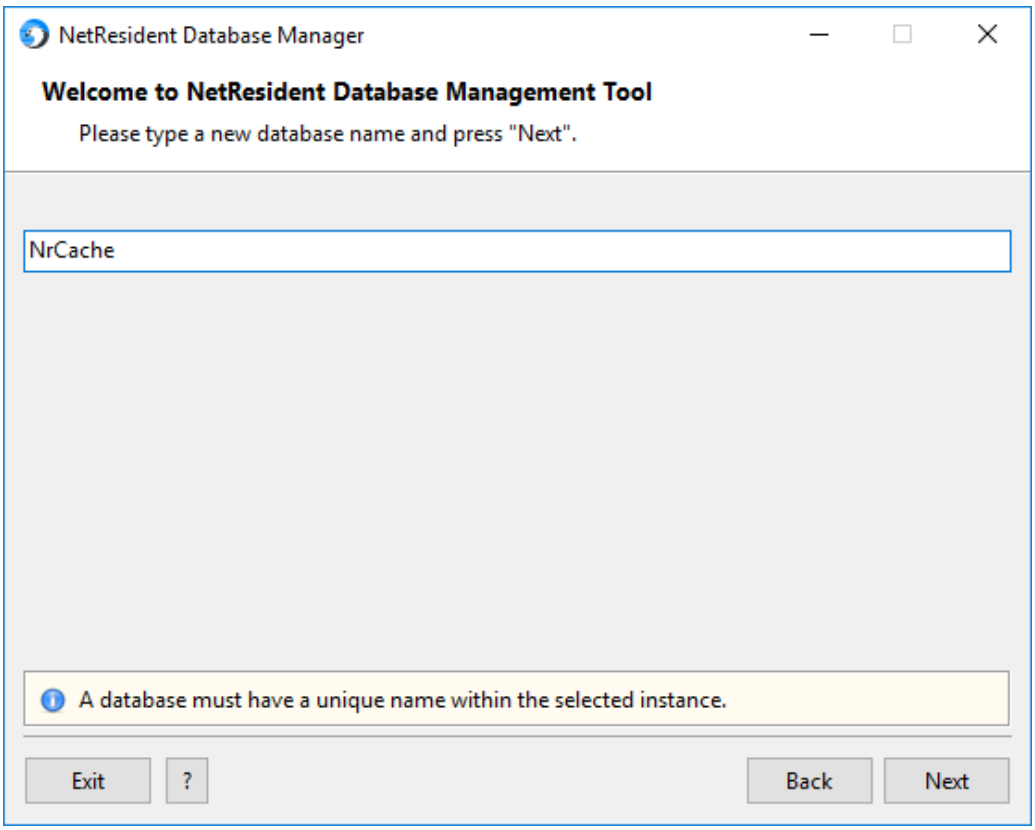
Step 3: Selecting a Database Location and Name

If you are creating a new database, you will also be prompted to select the folder in which the database is stored, as shown below:



Important: The path to the folder in which you plan to have the database file must be a local path relative to the computer on which the database is installed. You should NOT use the UNC format. Additionally, the computer's NETWORK SERVICE account must have read/write access to the specified folder.

On the next screen, you will be prompted to select a name for your new database, as illustrated below. The name must be unique for the given database instance. When selecting a name, please follow the guidelines.



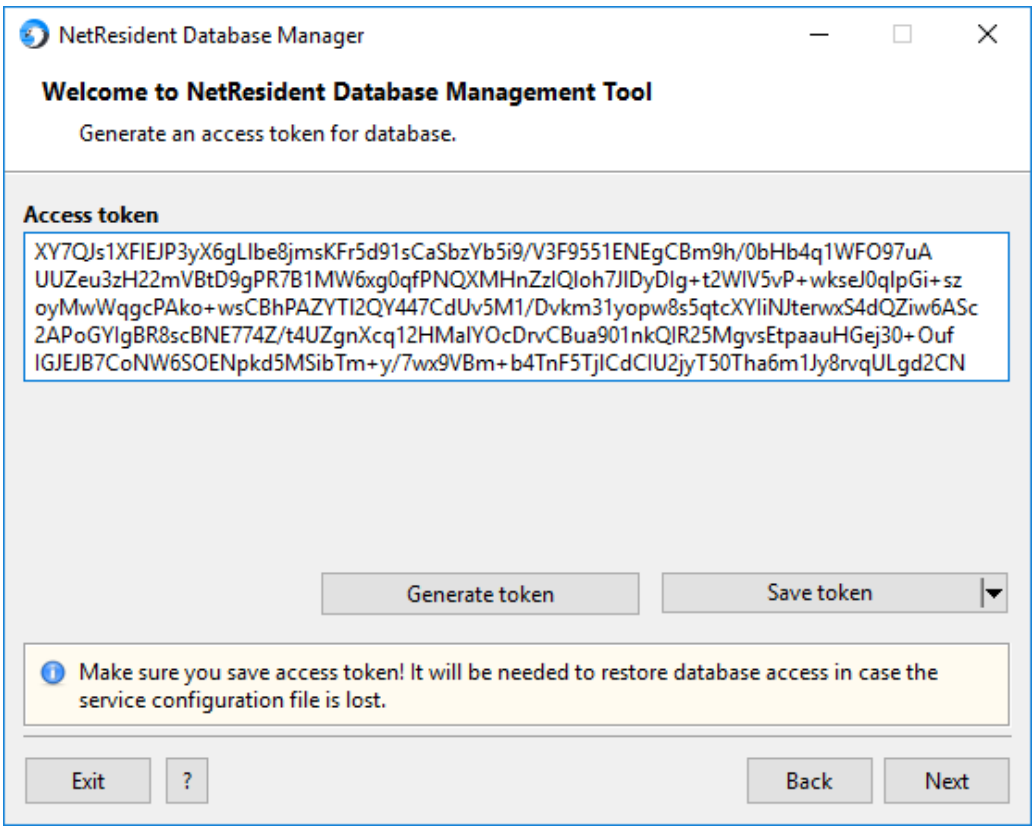
Step 4: Setting Database Access Token

In order to access the database, the application needs an access token, which is basically an encrypted piece of information that contains all the necessary credentials. In this step, the wizard prompts you to do one of the following:

(a) If this a new, clean installation, use the **Generate Token** button to generate a new access token.

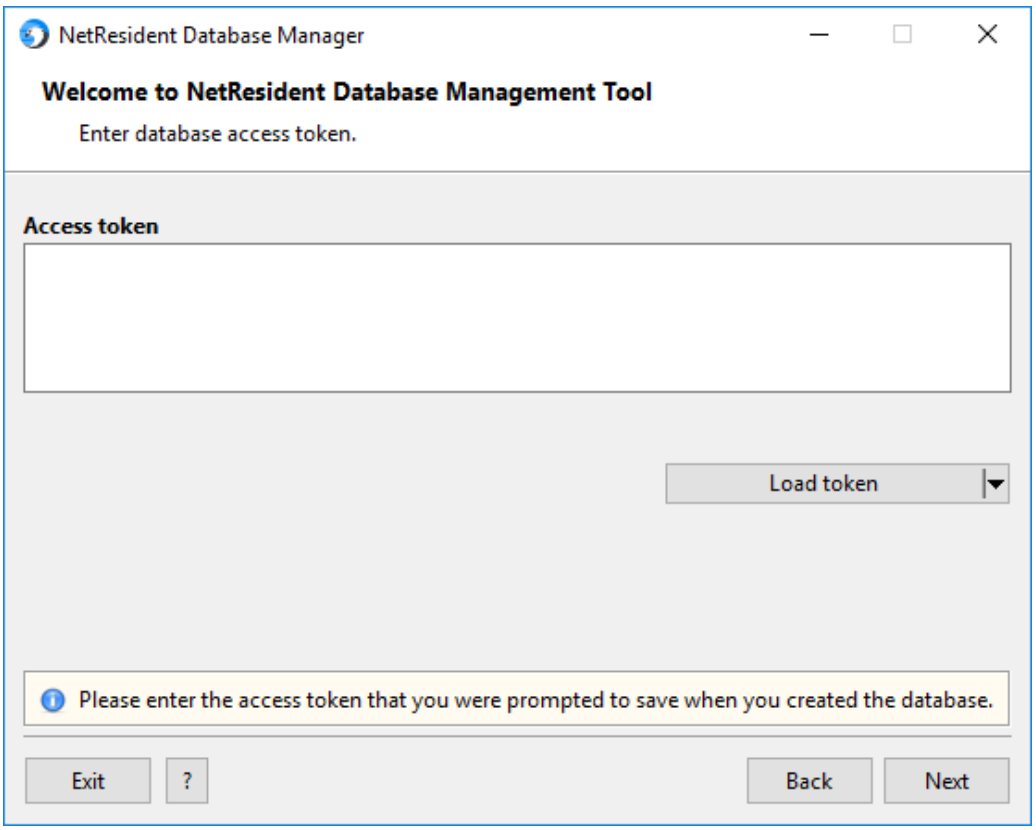
(b) If you have created a new database for an existing installation, you can use a previously saved token. Normally, it is automatically loaded for you from the database configuration file.

Note that the SQL credentials contained in the token override the existing SQL credentials, so an attempt to change existing SQL credentials will generate a warning. The access token entry dialog is illustrated below.



Important: Be sure to save the access token, as you might need it to access the database if the configuration file is lost. Normally, the access token is stored in the encrypted configuration file, and you do not need to reenter it.

(c) If you are creating a new configuration file for an existing database, enter the access token that you generated in the past, when you were creating the database. Note that you will be prompted to enter the access token only if no configuration file exists. Otherwise, the access token will be automatically read from the configuration file. Automatic loading of the access token from the configuration file is always a better option. The access token entry dialog is illustrated below.

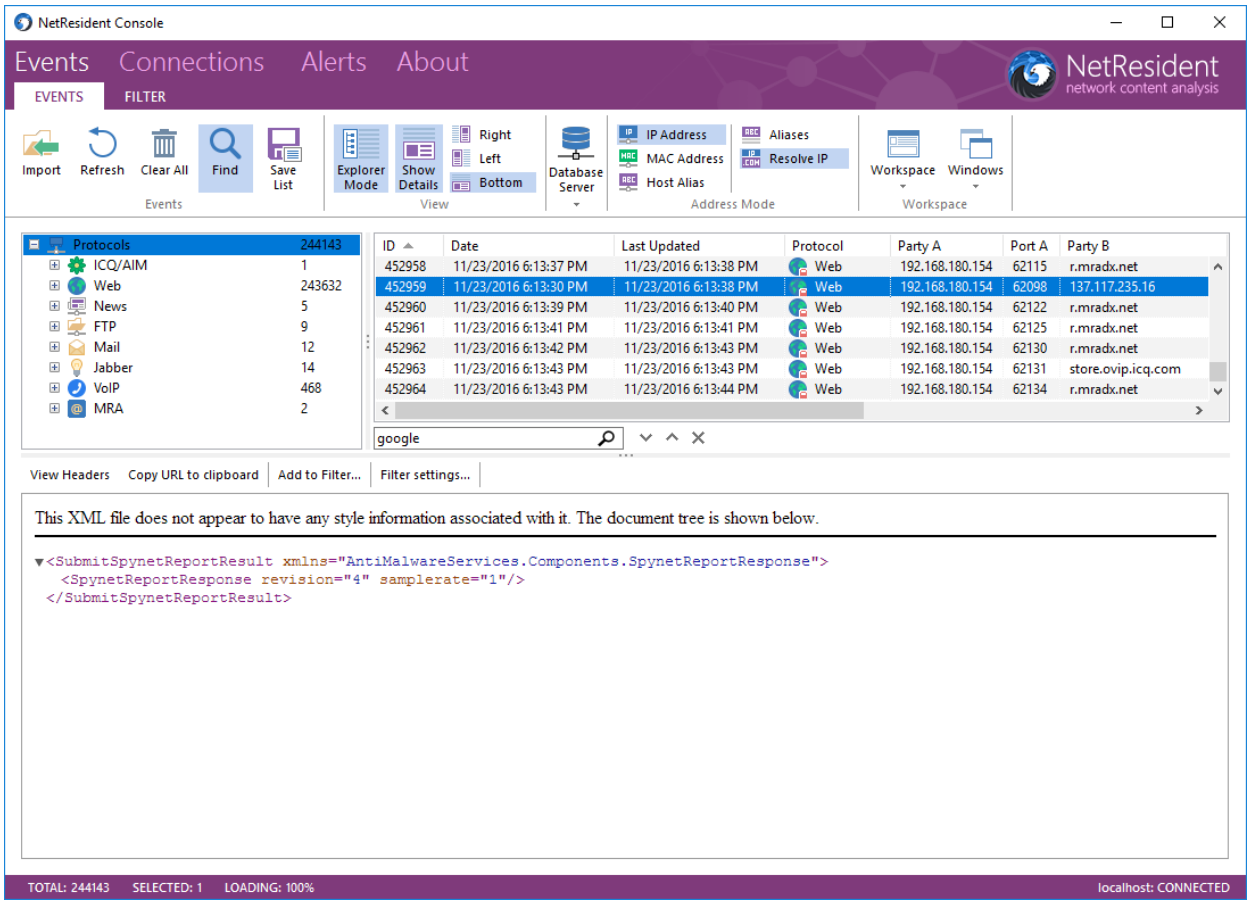


Step 5: Summary

In the final step, you will be shown the summary of your database configuration task. If all the data are correct, click **Execute** to start the task execution. If some of the data are incorrect, use the **Back** button to go back to the previous steps and correct the data.

Working with NetResident

Users interact with NetResident utilizing the NetResident Console, illustrated below:



The **NetResident Console** icon is placed on the desktop during the application installation; double-click on the icon to launch the console. The console allows you to perform the following tasks:

- Display, search, and filter the events that have been captured and analyzed by NetResident.
- Control the NetResident service.
- Control the NetResident agents.
- Configure alerts.

The console interface consists of three pages: **Events**, **Connections**, and **Alerts**. Each page includes a menu bar with one or several tabs.

Events

The **Events** page is the main interface element that displays the list of network events and allows you to view the detailed information on every event, as well as its contents. Working with this page is simple: You can select any event on the list (e.g., a Web page) and its content will be immediately displayed on the details panel. Data layout may be customized using the **Events** tab.

The **Events** list receives information from all of the data-collection points that have been installed by the user, which includes the NetResident service and may include NetResident agents. The captured data are

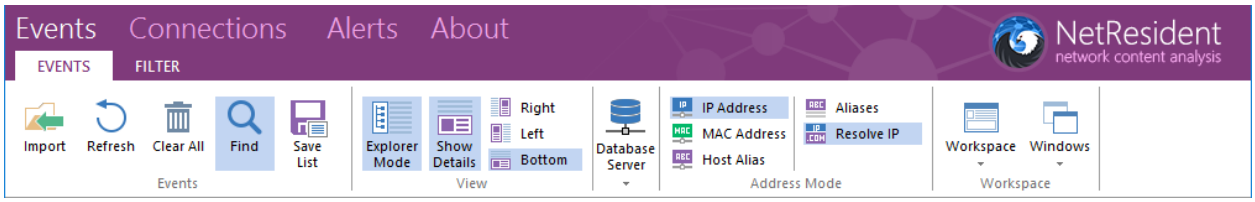
automatically fed to the console, and the console refreshes the event list every 30 seconds. You can also manually refresh the list by clicking the **Refresh** button.

Because the number of captured events in a busy network might be extremely high, the unfiltered event list might be populated with thousands or millions of events. Exploring such a list would be problematic unless you use the **Filter** tab that allows you focus on specific protocols, dates, or workstations.

Another tool that may dramatically simplify event browsing is the **Explorer**. Located on the left side on the **Events** tab, the Explorer groups events by protocol and date. When you select a specific node, the event list displays only those events that match the selected protocol and date. Also, a few protocol-specific columns are automatically added to the event list. The Explorer builds the node list "on-the-fly," without contacting the database server, so the node list consist of only those events that passed the main filter and display filter.

The **Events** page menu has two tabs, **Events** and **Filter**.

Events Tab



With the **Events** tab menu commands, you can change the way data are presented by the application. The commands are described below.

Events

- **Import** – imports data from capture files generated by TamoSoft and a number of third-party products. See Analyzing Imported Capture Files for more information.
- **Refresh** – reloads the event list from the NetResident service using the last applied filter.
- **Clear All** – deletes all events from the database; this operation is irreversible.
- **Find** – shows or hides the search panel that allows you to search for matches in the event list, e.g. date, source, address, etc.
- **Save List** – exports the event list in a number of formats: HTML, CSV, TXT and RTF.

View

- **Explorer mode** – shows or hides the event explorer panel.
- **Show Details** – shows or hides the panel that displays event contents.
- **Right, Left, Bottom** – controls the position of the panel that displays event contents.

Database server

- **Select database** – allows you to select a database from which the events are displayed.

Address Mode

- **IP Address** – makes the "Party A" and "Party B" columns display the IP addresses of the parties.
- **MAC Address** – makes the "Party A" and "Party B" columns display the MAC addresses of the parties.

- **Host Alias** – makes the “Party A” and “Party B” columns display the user-assigned aliases of the parties rather than their IP or MAC addresses.
- **Aliases** – displays the windows that allow creating or editing aliases.
- **Resolve IP** – when this option is on, the application will try to resolve all IP addresses to corresponding host names.

Workspace

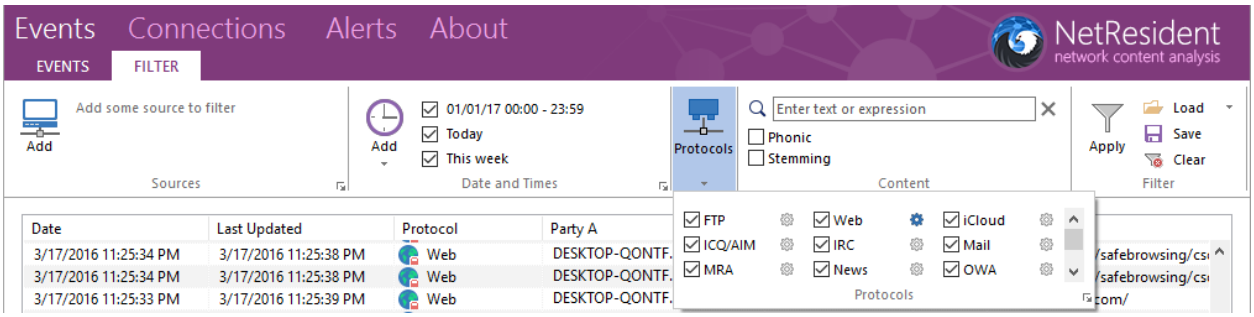
Workspace

- **Load** – loads a workspace from a file.
- **Save** – saves the current workspace to a file.
- Additionally, the menu may contain the list of the most recently used workspaces.

Windows

- **New Window** – opens another console instance. You can use several windows at the same time. For example, you may want to view today’s events in the first window and yesterday’s events in another window.
- **Arrange All**, **Side by Side** – controls the positions of the opened console windows.

Filter Tab



With the **Filter** tab menu commands, you can focus on the events that are of interest to you and filter out the events that are not important. Once you have configured the filter(s), be sure to click **Apply** to apply your new filter set.

Sources

- **Add** – allows you to specify sources of network events. These may include the NetResident service, agents, manually imported capture files, or automatically imported capture files. Initially, when no sources have been added, NetResident displays events from all source. If/when you add a source or multiple sources and click **Apply** (located in the **Filter** frame to the right), only the events from these sources will be displayed.

Date and Times

- **Add** – allows you to specify date and time ranges of network events. Initially, when no ranges have been added, NetResident displays events that occurred at any time. If/when you add a date and time range and click **Apply** (located in the **Filter** frame to the right), only the events within

these ranges will be displayed. You can also click on the arrow to use one of the presets: **Today**, **Yesterday**, or **This Week**.

Protocols

- **Web, FTP, etc.** – check or uncheck the boxes next to the protocol names to include or exclude the events based on the respective protocols. Click on the gear-wheel icon available for some of the protocols for additional filter settings. For example, you can exclude or include events depending on the web site address. Click **Apply** to apply the filter. Please note that this filter is a display filter; see Understanding the Difference Between the Display and Capture Filters for more information.

Content

- **Contains text** – allows you to perform free text search. A search request consists of an unstructured natural language or "plain English" query. In a natural language search request, words such as AND and OR are disregarded. Use quotation marks to indicate a phrase, + (plus) to indicate a word that must be present, and - (minus) to indicate a word that must not be present. Enter a text string and click **Apply** to have NetResident display only those events that contain the entered text. Note that database indexing takes time, so matching event may not appear immediately.
- **Stemming** – if you check this box, your search will include other grammatical forms of the words in your search request. For example, with stemming enabled, a search for "apply" would also find "applies." This option has no effect for non-English searches.
- **Phonic** – if you check this box, your search will find words that sound similar to the words in your request, like "Smith" and "Smythe." This option has no effect for non-English searches.

Filter

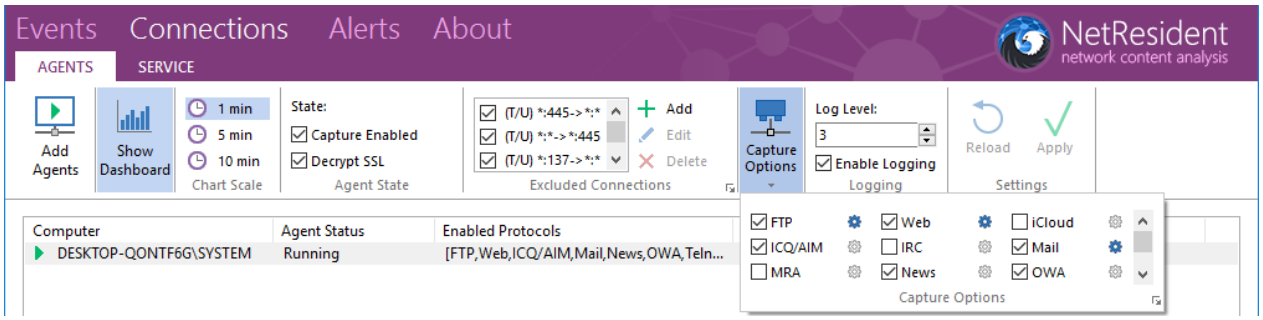
- **Apply** – applies the current filter set and reloads the events.
- **Load** – allows you to load a filter set that you saved in the past. Clicking on the arrow lists the most recently saved filter sets.
- **Save** – saves the current filter set to a file.
- **Clear** – removes all filters, including additional filter settings, and reloads the events.

The filter settings are automatically saved when you close the application and restored when you run it again.

Connections

The **Connections** page is an interface element that has two key functions: It allows you to control the deployed agents and the NetResident service. On the **Agents** tab, you can view the list of connected agents and their statuses, as well as per-agent statistics. You can also control individual agents. On the **Service** tab, you can view information on the NetResident service you are currently connected to and change its settings.

Agents Tab



Add Agents

Displays the dialog that allows you to deploy NetResident agents on your LAN. This is possible only for networks with domain controllers.

Show Dashboard

Shows or hides the dashboard that displays statistics for the selected agent.

Chart Scale

Sets the chart update speed. Each chart point can correspond to data collected over a period of 1, 5, or 10 minutes.

Agent State

- **Capture Enabled** – enables or disables the selected agent(s). When an agent is disabled, it no longer collects and sends data.
- **Decrypt SSL** – enables or disables encrypted traffic interception.

Excluded Connections

Allows managing the list of connections that are ignored by NetResident agents. See Adding Exceptions to NetResident Agents for more information.

Capture Options

- **Web, FTP, etc.** – check or uncheck the boxes next to the protocol names to include or exclude the events based on the respective protocols for the selected agent. Click on the gear-wheel icon available for some of the protocols for additional filter settings. For example, you can exclude or include events depending on the web site address. Please note that this filter is a capture filter; see Understanding the Difference Between the Display and Capture Filters for more information.

Logging

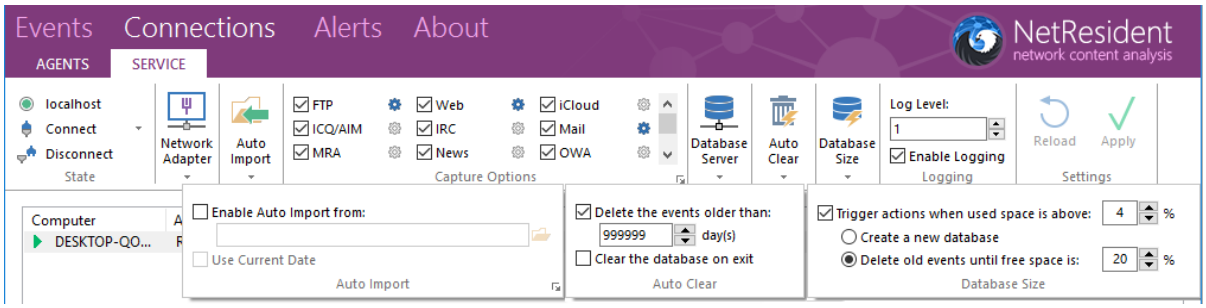
- **Log Level** – by default, every NetResident component, including agents, logs important debugging information to a log file. You can change the amount for details included in the log. Normally, you should not change the default value (1) unless you are advised to do so by the TamoSoft support staff.
- **Enable Logging** – check or uncheck to enable or disable logging for the selected agent.

Settings

- **Reload** – refreshes the agent's parameters and displays the updated settings.
- **Apply** – applies the changes you have made to any of the agent's parameters and saves the current settings for the selected agent.

> When an agent connects to the NetResident service for the first time, it receives the default set of parameters from the service. After that, the agent's settings can be customized on the per-agent basis using the **Agents** tab described above.

Service Tab



State

- **Hostname** – displays the hostname or IP address of the NetResident service instances to which the NetResident console is currently connected.
- **Connect** – displays the dialog that allows you to connect to the NetResident service. Note that when you start the NetResident console, it automatically connects the NetResident service address it was connected to the last time you ran the application.
- **Disconnect** – disconnects the console from the service.

Network Adapter

- **Adapter** – allows you to select a network adapter to be used for capturing network traffic. Additionally, you can select **Offline mode**, in which case the NetResident service does not capture live network data.
- **Use non-promiscuous mode** – check this box only if your adapter cannot operate in promiscuous mode. This option must always be selected for wireless (802.11) adapters.
- **MAC, IP, MASK** – displays the network address settings of the selected adapter.

Auto Import

- **Folder** – allows you to configure the NetResident service to import network events from capture files generated by another packet-capture application. For example, you may want to use a Wi-Fi packet analyzer to sniff packets and automatically save them in a certain folder. If you enter the path to that folder in the provided field, the NetResident service will monitor that folder and automatically analyze new capture files as soon they are saved to that folder by the third-party application.

- **Enabled** – check this box to enable automatic log import.
- **Use current date** – if this box is checked, when you import log files, the original date stamps in the log file are replaced by the current date.

Capture Options

- **Web, FTP, etc.** – check or uncheck the boxes next to the protocol names to include or exclude the events based on the respective protocols. Click on the gear-wheel icon available for some of the protocols for additional filter settings. For example, you can exclude or include events depending on the web site address. Please note that this filter is a capture filter; see Understanding the Difference Between the Display and Capture Filters for more information.

Database Server

- **Select database** – allows you to select the database that is used by the NetResident service and agents for recording captured network events.

Auto Clear

- **Delete the events older than** – if you check this box, the events that are older than *n* days are automatically deleted from the database.
- **Clear the database on exit** – if you check this box, all events are automatically deleted when the NetResident service is stopped.

Database Size

- **Trigger actions when used space is above %** – the percentage of used database space after reaching which one the user-configured actions is triggered. If this option is not turned on, the application **stops recording any events** (collected by agents, extracted from the log files, or captured locally) when the database is full.
- **Create a new database** – a new database will be created on the same SQL server and in the same directory as the currently used database.
- **Delete old events until free space is %** – when the used database space limit is reached, the old events will be deleted from the database until the percentage of free space reaches the specified value.

Logging

- **Log Level** – by default, every NetResident component, including the service, logs important debugging information to a log file. You can change the amount for details included in the log. Normally, you should not change the default value (1) unless you are advised to do so by the TamoSoft support staff.
- **Enable Logging** – check or uncheck to enable or disable logging for the NetResident service.

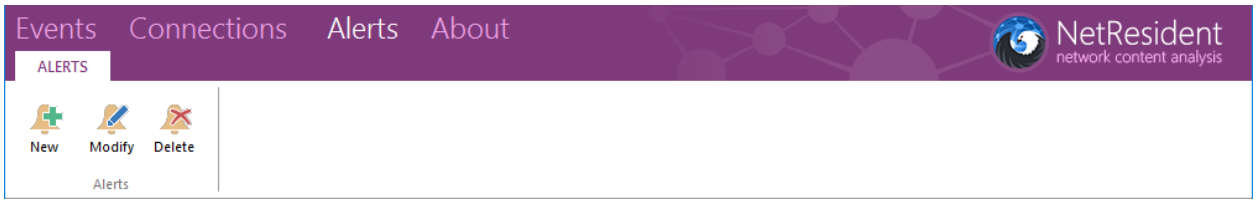
Settings

- **Reload** – refreshes the NetResident service parameters and displays the updated settings.
- **Apply** – applies the changes you have made to the service parameters and saves the current settings.

Alerts

Alerts allows you to create and modify alerts (i.e., notifications that are displayed by the application when a network event meets the conditions specified in the alert). For example, you can make NetResident notify you when a certain text is found in an event.

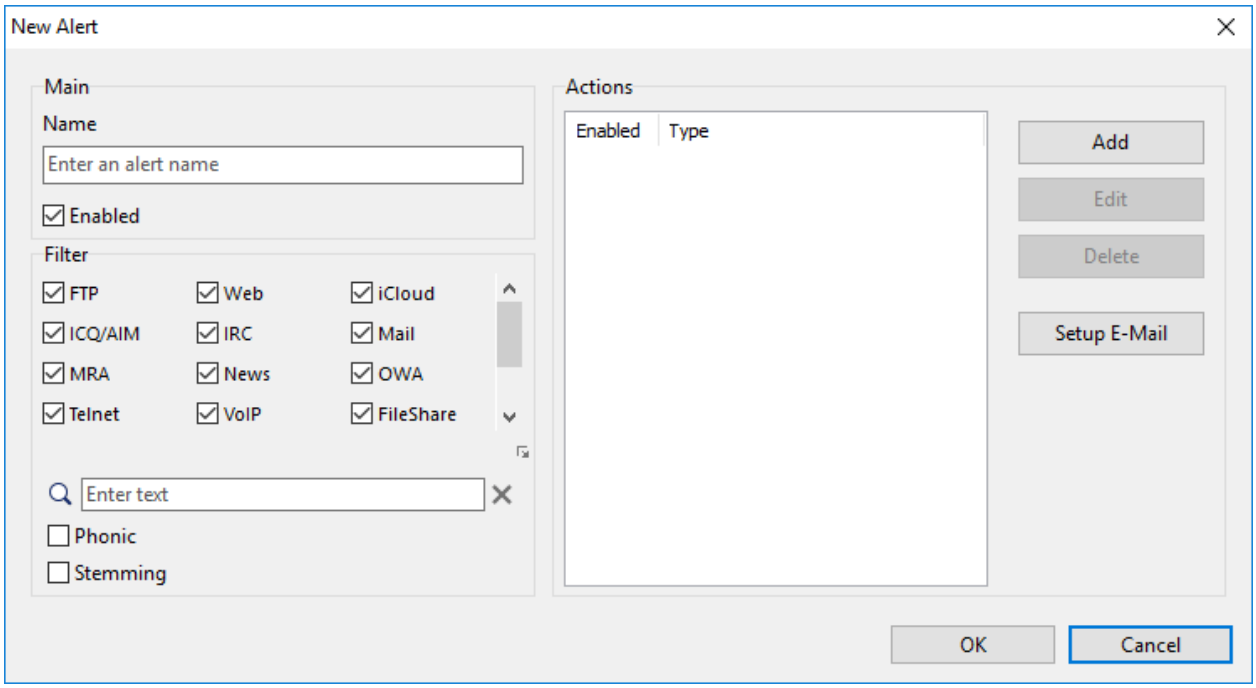
Alerts Tab



Alerts

- **New** – creates a new alert.
- **Modify** – modifies an existing alert.
- **Delete** – deletes an existing alert.

Existing alerts can be turned on and off using the checkbox next to the alert name. When you create a new alert or modify an existing one, the follow dialog is displayed:



Enter a unique **Name** for the alert and check the **Enabled** box to make the alert active. The **Filter** frame allows you to select the protocols that the alert applies to and to specify the text to search for. For example, if you want to be alerted when the word “specifications” is found in an FTP file transfer, check the **FTP** box and enter “specifications” in the text field. The text you search for should consists of an unstructured natural language or “plain English” query. In a natural language search request, words such as AND and OR are disregarded. Use quotation marks to indicate a phrase, + (plus) to indicate a word that must be present, and - (minus) to indicate a word that must not be present. If you check the **Stemming** box, your search will include other grammatical forms of the words in your search request. For example,

with stemming enabled, a search for “apply” would also find “applies.” This option has no effect for non-English searches. If you check the **Phonic** box, your search will find words that sound similar to the words in your request, like “Smith” and “Smythe.” This option has no effect for non-English searches.

When the text specified in the alert is found in an event, the corresponding record is added to the log window (located below the alert list). Additionally, the user can be notified by a number of configurable **Actions:**

- **Beep** – the computer beeps.
- **Play file** – the specified WAV file is played back.
- **Send e-mail** – sends an e-mail to the specified e-mail address. You MUST configure NetResident to use your SMTP server prior to sending e-mail. Use the **E-mail Setup** button to enter your SMTP server settings.
- **Show message** – displays the specified message as a system tray notification balloon.
- **Set a priority** – changes the event’s priority to the specified value.
- **Add a comment** – adds the specified comment to the event.
- **Pronounce message** – makes Windows speak the specified text using the text-to-speech engine. By default, Windows only comes with English computer voices, so Windows may not be able to pronounce messages correctly if the text is entered in a language other than English.
- **Write to syslog** – sends the message to the specified IP address using the syslog protocol.
- **Send SNMP trap** – sends the message to the specified IP address using the SNMP protocol. The MIB file containing OID descriptions is available upon request.
- **Launch application** – launches the specified application (additional command line parameters are supported).

Multiple actions can be configured for a single alert.

Note that alerts are updated **once a minute**, so once a matching event has occurred, it may take up to a minute before the corresponding action(s) are performed. Also, note that when you add a new alert, the entire database is searched, so the alert may be triggered even if the related events took place in the past.

About

About Tab

Help

- **Web Site** – opens the TamoSoft web site.
- **Help** – displays help documentation.
- **Help (PDF)** - displays help documentation in PDF format.

Update

- **Check Now** – finds out if software updates are available.
- **Enable automatic updates** – check this box to have the application automatically check for updates. You can also specify how frequently to perform such checks.

Language

- **English** (or another language) – allows you to change the user interface language.

Understanding the Difference Between the Display and Capture Filters

Network content captured and analyzed by NetResident may be filtered on two levels:

- **Display filter:** You may apply this filter to the data that have already been captured. For example, if NetResident has been running for a week and you want to focus only on the events that occurred last Sunday, you can use the **Filter** tab on the **Events** page to set the specific date. This will allow you to temporarily discard the events that took place on other days. Now, if you want to focus on the events that occurred last Monday, you can simply change the filter to see the events for another day.

- **Capture filter**: You may use this filter to limit the type of events that are captured by NetResident. By default, NetResident captures and stores all the events that it can analyze, such as e-mails, Web pages, and IM chat sessions. However, some users may not want to capture and store all of this network content in order to decrease the database size and improve overall application performance. For example, you may want to completely exclude FTP file transfers. This can be done on the **Agents** and **Service** tabs of the **Connections** page, where you can find the **Capture Options** button. Use it to select the types of protocols you want the application to capture.

The difference between these two filter types is that in the case of using the **display filter**, all of the events are still stored in the database, and you can use the display filter to select only those events that are currently of interest to you. In the case of using the **capture filter**, the excluded events are lost forever; for example, if you disabled capturing FTP file transfers some time ago, you cannot restore the missed events by enabling the capturing of FTP file transfers again.

Remote Connections

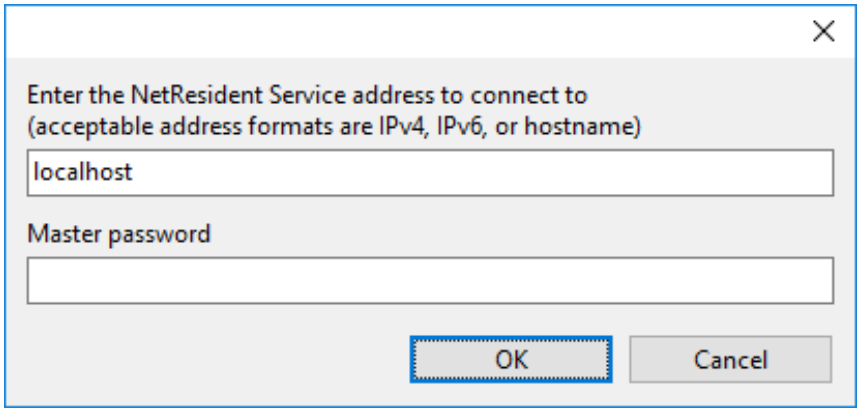
As mentioned before, the NetResident console is a system component that connects to the NetResident service, processes data, and presents it to the user via a graphical user interface. The connection between the service and console is made over TCP/IP, which means that you can connect to the NetResident service running on any computer, as long as you can connect to it over TCP/IP and know the password.

When you start NetResident, it initiates a connection to the NetResident service you connected to last time. By default, this is the local PC, but you can remotely connect to any computer on which NetResident is installed. In order to connect to another NetResident service, do the following:

- Click **Connections => Service => State => Disconnect** to disconnect from the NetResident service you are currently connected to.

- Click **Connections => Service => State => Connect**.

The following dialog window will be displayed:



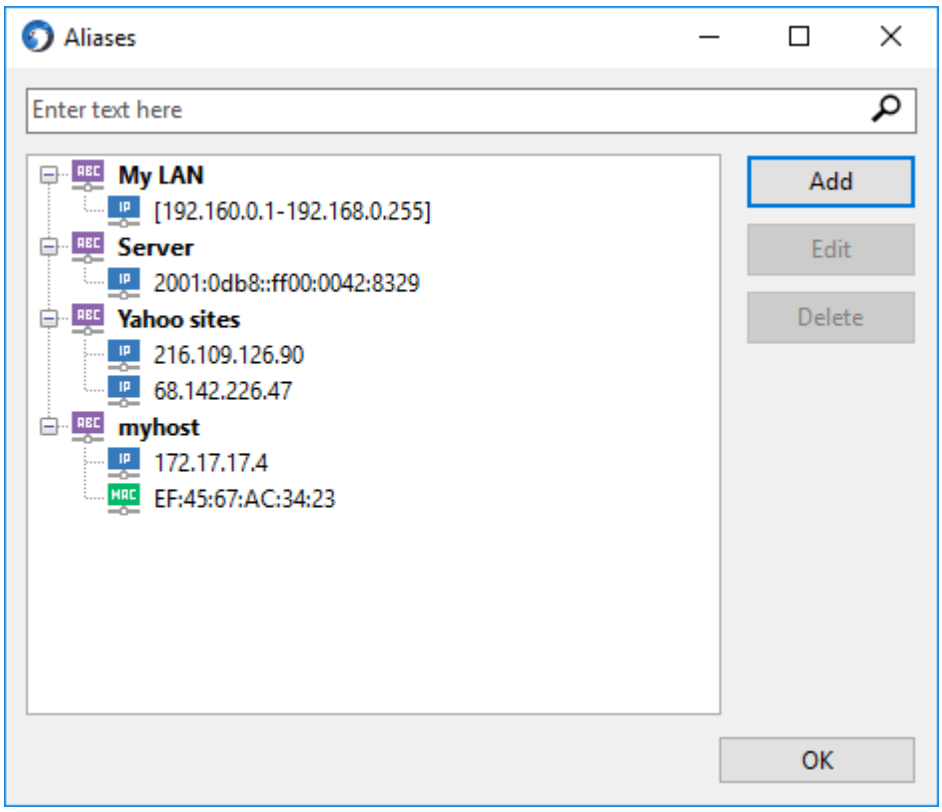
You should enter the IP address or host name of the computer running the NetResident service, as well as the master password that you selected when you installed the NetResident service. Click **OK** to connect.

Aliases

Aliases are easy-to-remember, human-readable names that can be substituted for MAC or IP addresses displayed in the **event list**. This can make it easier to recognize and analyze network events.

Once an alias is assigned to an IP or MAC address, it will replace the corresponding address in the **events list**. You can choose how the hosts participating in the communications are displayed: by **IP Address**, by **MAC Address**, or by **Host Alias**. An alias may also be assigned to a range of IP addresses. This is very convenient, as it allows you to have just one name for a group of network devices (e.g., all computers on a LAN). Each alias is unique. However, you can assign the same alias to several MAC or IP addresses, thus forming a group. This is useful if a computer has several network addresses and you would like to identify them all by one name. Additionally, the application can resolve IP addresses to hostnames.

These configuration settings can be found in the **Events** => **View => Address Mode** ribbon group. You can add, edit, or delete aliases by clicking **Aliases** in that group.



Click the **Add** button to add a station. Enter an alias name and click the **Add** button. A dialog window will open, prompting you to enter the address for the alias and select its type: **IP Address**, **IP Address Range**, or **MAC Address**. If you would like to add a range of IP addresses, select the **IP Address Range** radio button and enter the starting and ending IP addresses for the range in the corresponding fields.

Click **OK** to update the list of aliases or **Cancel** to discard the changes. You can edit an alias by selecting it and clicking on the **Edit** or **Delete** buttons.

You may also assign aliases to hosts by right-clicking on a network event in the **events list** and choosing the corresponding item from the pop-up menu.

Workspaces

Workspaces are sets of interface configuration settings. They allow configuring of the interface for a specific task or for a specific user and then saving and restoring such configurations. NetResident maintains a history of previously saved workspaces and makes it possible to switch between them quickly.

A workspace stores the following parameters:

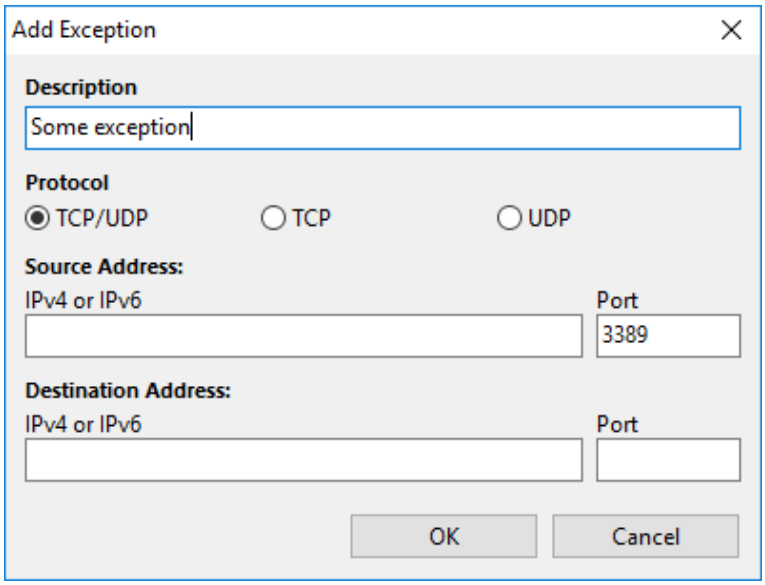
- The size and state of the application's main window.
- Currently selected database.
- Appearance of the event list.
- Display filters.
- Individual local plug-in configurations.
- Alias lists for IP and MAC addresses.

Adding Exceptions to NetResident Agents

It is possible to configure NetResident agents to ignore network traffic based on the source and/or destination IP addresses and/or ports. In essence, you are adding an exception, just like you add exceptions to a firewall. This feature may be useful in the following cases:

- Increasing system performance. Some protocols may generate much traffic that you do not want to analyze; excluding this traffic from analysis allows the application to "focus" on the traffic that is more important.
- Privacy reasons. You may want to prevent NetResident from analyzing certain network events.
- Dealing with software compatibility issues. Some third party software may not work correctly when running on the same computer where NetResident agent is installed.

To add an exception, navigate to the **Excluded Connections** frame on the **Agents** tab and click **Add**. The follow dialog is displayed:



The **Description** field contains an optional description of the exception being added. The **Protocol** field contains the protocol name to which the exception is applicable. Under **Source Address**, enter the source IP address and source port of the packets that you want to have ignored. Under **Destination Address**, enter the destination IP address and destination port of the packets that you want to have ignored. To add an exception successfully, you must specify at least one of the four parameters. To specify any IP address, leave the field blank or use "0.0.0.0" or "::". To specify any port, leave the field blank or use "0". For example, the image above illustrates a rule that would ignore any traffic originating from port 3389 regardless of the source and destination IP addresses and regardless of the destination port.

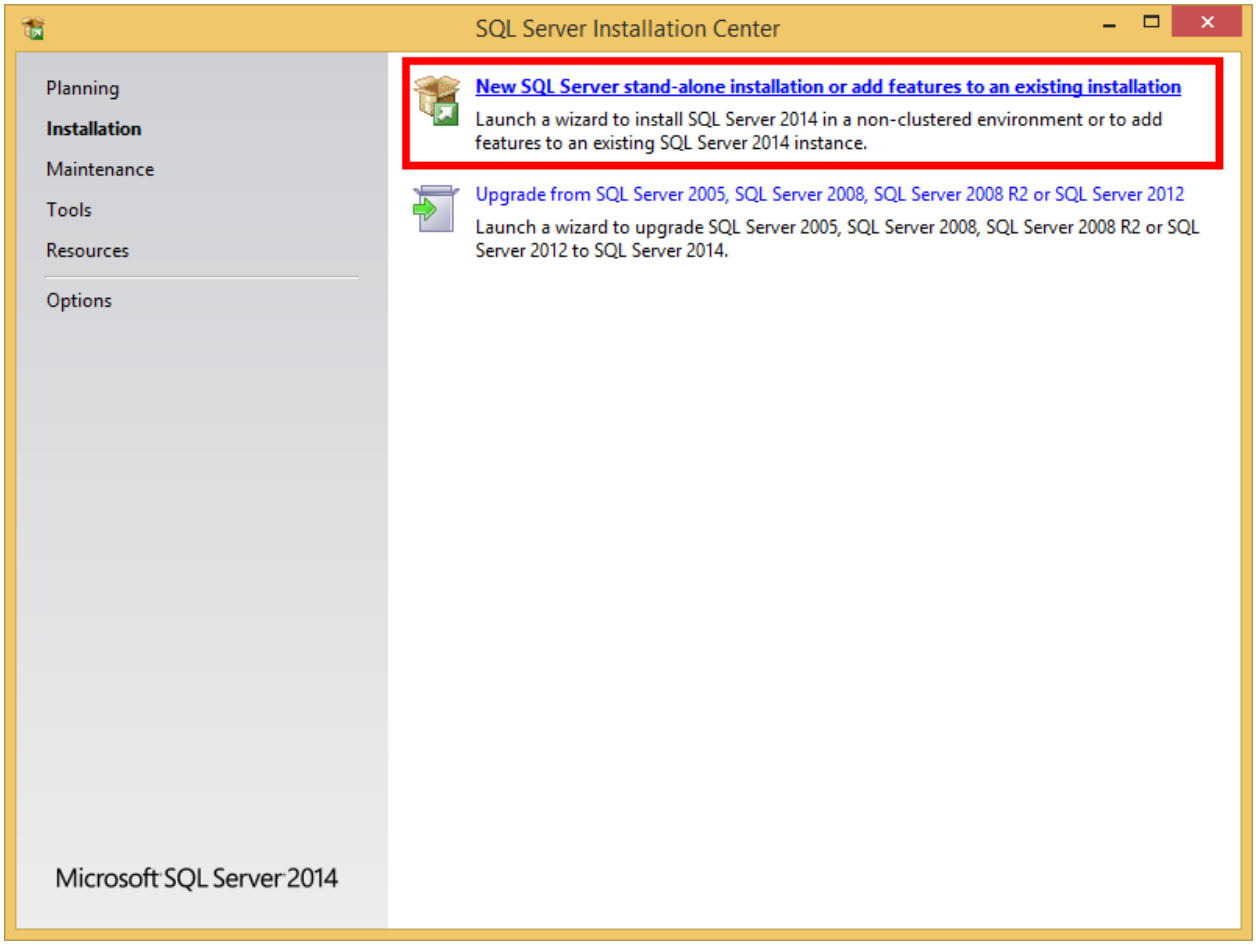
By default, each NetResident agent is installed with the following set of exceptions:

	Source IP address	Source Port	Destination IP address	Destination Port
1	any	445	any	any
2	any	any	any	445
3	any	137	any	any
4	any	any	any	137
5	any	139	any	any
6	any	any	any	139

7	any	2221	any	any
8	any	any	any	2221
9	any	3389	any	any
10	any	any	any	3389

Manual SQL Server Installation

NetResident uses an SQL server instance for storing and retrieving captured network events. Normally, an SQL server is automatically installed by NetResident, as described in this help file. Automatic installation is highly recommended, as it helps you avoid mistakes when configuring the server. However, you can also install an SQL server yourself. This process is overviewed below. This overview is based on Microsoft® SQL Server® 2014 Service Pack 1; for other versions, the process might have minor distinctions.



Only the key installation steps are covered in this overview; less important steps, such as EULA acceptance, are skipped.

1. Once the installation package has been unpacked, the **SQL Server Installation Center** window shows up. Select **New SQL Server**.
2. On the **Installation Type** step, select **Perform a New Installation**.
3. On the **Feature Selection** step, check all the available components.
4. On the **Instance Configuration** step, select **Named instance** and enter any name for your SQL server. Copy and paste the same server name into the **Instance ID** field. The server name must be unique within the given computer. Be sure to remember the SQL server name that you have chosen. You will need it later, when you run the **NetResident Database Manager.**
5. On the **Server Configuration** step, select the **Collation** tab and then select **Latin1_General_100_CI_AS** from the drop-down list. The **Service Accounts** tab should not be modified.
6. On the **Database Engine Configuration** step, select **Mixed Mode**. This is very important; without this selection, NetResident will not be able to use the SQL server. Also, specify a strong password

for the administrator (“sa”) account. Be sure to remember the administrative password. You will need it later, when you run the **NetResident Database Manager.**

7. Complete the installation. You can now refer to the Setting Up the Database chapter to configure NetResident to use your database.

Analyzing Imported Capture Files

In addition to capturing live network data, NetResident allows you to import network data from capture files generated by a number of network analyzers and monitors. The current version can import files in the CommView®, CommView® for WiFi, Network Instruments Observer®, Network General Sniffer® for DOS/Windows, Microsoft® NetMon, WildPackets EtherPeek™ and AiroPeek™, Wireshark/Tcpdump, and Wireshark/pcapng formats. Two import modes are available.

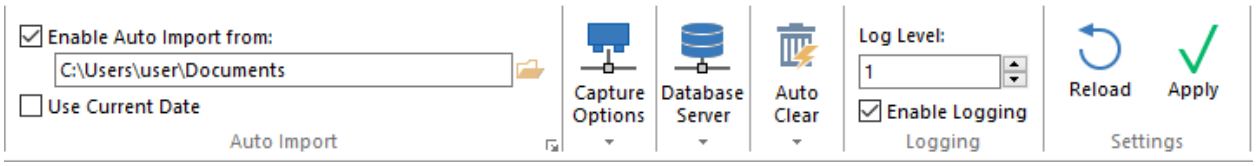
Manual Import

Click **Import** in **Events => View => Events** and select a capture file to import. The NetResident service will process the file contents, applying your capture filter(s). Once the file has been processed, new events will show up in the event list of the NetResident console.

Automatic Import

Automatic import allows you to specify a folder that will be "watched" by NetResident for any changes. As soon a new file is added to that folder, it will be immediately imported and new events will show up in the event list of the NetResident console.

To configure this functionality, locate the **Connections => Service => Auto Import** group on the tool bar and select the **Folder** as shown below. Check the **Enabled** box and then click **Save** to apply the settings. Check the **Use Current Date** box, if you want to replace the data stamps in the file being imported by the current system date.



Frequently Asked Questions

Q. My HTTP plugin does not always display HTML pages correctly. For instance, some images are not displayed. Why is this so?

A. A typical HTML page represents a collection of a dozen of independent objects: HTML code, images, CSS styles, and others. A browser requests each of these objects; however, most of these objects are cached (saved to the computer's hard drive for future access) and hence not requested from the network every time a Web page is viewed. NetResident does not have access to your browser's cache; therefore, it cannot "see" these objects. This is not a problem with NetResident; you can always reload the Web page in your browser (you need to perform a complete reload; in Internet Explorer, this is achieved by clicking on the **Refresh** button while holding down the Shift key). This will allow NetResident to log and store all Web page elements.

Q. When I try to import CommView or CommView for WiFi log files, I am unable to display the contents of some of the files. I believe I have all parameters set correctly regarding the event viewer and filtering.

A. It is important to understand that the import procedure has its own filter, and the content displaying mechanism has its own filter. When you were importing the file, the content was possibly filtered out during the import phase if you applied filters. Once the import phase is over, the application uses the display filter to show the contents. There is a chance that the application is configured to show only the data collected during the last two days, while the logs contained sessions that were outside this time frame. You may want to disable the display filter to have the application show the data.

Q. Why does the NetResident service insist on starting if I just want to review LOG files and not capture current data?

A. The database is maintained by the service. The GUI is simply a console that "talks" to the service. All data processing and filtering is performed by the service as well, so it has to be running.

Q. Can you give some performance metrics when NetResident is being used to monitor a heavily loaded network?

A. The program's performance depends on the CPU speed and RAM size. If you use the default monitoring settings (i.e., when all the plug-ins are enabled and all the ports are being monitored, an average Pentium4 3 GHz PC with 512 Mbytes of RAM can monitor a fully used 100 Mbit link. To monitor faster network links, you should set up filtering by station, limit the ports being monitored, and disable unnecessary plugins. The performance also depends on the type of traffic being monitored, so additional filters should be applied only if you experience performance problems.

Q. For some ICQ and AIM chat sessions, one of the parties' ID number is shown as "Not detected." Why is it not detected?

A. This happens when an ICQ or AIM chat session (including the authentication phase) begins before NetResident starts capturing network packets. If capturing is started in the middle of a chat session, the ID can sometimes be found (as it is contained in some service packets, which are sent intermittently), although this cannot be guaranteed.

Q. Can your VoIP module be used for logging Skype conversations?

A. No, sorry. Skype uses robust encryption; it is impossible to decrypt Skype conversations.

Q. Why does NetResident not show the amount of transferred data in terms of bytes?

A. NetResident does not always store transferred data in their original form. Rather, it processes data for more convenient presentation. It is not uncommon for a single network session to be divided into several separate events, or several network sessions to be combined into one event. Besides, some transferred data simply are not supposed to be processed by current NetResident plugins. That said, NetResident cannot and is not supposed to display reliable network data statistics.

Q. I use NetResident 2.x. Can I import my existing database into NetResident 3.0?

A. Unfortunately, no. NetResident 3.0 is a completely new product that uses a new database structure, so importing is not possible.

Q. I use NetResident 2.x. Can I install NetResident 3.0 on the same computer?

A. Yes, these applications can work side by side.

Sales and Support

At TamoSoft, we want you to be happy with your purchase. That is why we encourage you to try our products and technical support free of charge for 30 days before you make a decision regarding your purchase. By making the most of these free evaluations, you can fully test the software and make sure that it does everything you need. When you are ready to buy, we welcome you to http://www.tamos.com/order/ to order directly from us or through our partners and resellers.

As a registered user, you will receive:

- A fully functional, unrestricted copy of the software
- Free updates that will be released within one year from the date of purchase
- Information on updates and new products
- Free technical support

Prices, terms, and conditions are subject to change without notice. Please check our Web site for the latest product offerings and prices.

For technical support, please visit http://www.tamos.com/support/.