Quest

Quest ExpertAssist 8.7.1

User Guide

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

(missing or bad snippet)

ExpertAssist User Guide
Updated - January 2019
Version - 8.7.1

Contents

Overview

Quest™ExpertAssist is the perfect choice for anyone who has ever needed to access and control a PC or server from elsewhere, be it from down the hall or from halfway around the world. All that is required to control a PC or server is a web browser or WAP-enabled wireless device.

ExpertAssist is a remote administration tool that lets you control and administer Microsoft® Windows®-based computers over a local area network or the Internet. Originally designed for network administrators, ExpertAssist has evolved to offer a wide variety of remote computing solutions for an equally wide variety of users. Today, ExpertAssist provides many useful capabilities such as Java-based desktop remote control, file transfer protocol (FTP) for downloading and uploading of files, configuration of the host computer, remote-to-local printing, advanced scripting, and dozens of other features.

ExpertAssist acts as the host software on the machine that is to be controlled or accessed. The client (the remote computer that is used to access the host) requires no special software. The client software is any Java-enabled web browser (see System Requirements). Many Remote Control features can also be accessed and controlled using such client software as that found in handheld PDAs and WAP-enabled mobile telephones.

System Requirements

Operating Systems Support

Quest ExpertAssist can be deployed to the following operating systems.

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows 8.1 (32-bit or 64-bit)
- Microsoft Windows 10 (32-bit or 64-bit)
- Windows Server 2008 R2 any Service Packs
- Windows 7 (32-bit or 64-bit) Service Pack 1 or later
- Windows Server 2008 (32-bit or 64-bit) any Service Packs
- Windows Server 2016

Where possible, be sure to have the latest Service Pack installed on a remote computer when you are deploying Quest ExpertAssist.

Browser Requirements

The following web browsers can be used to manage ExpertAssist hosts:

1. Web Browsers:
   • Windows Internet Explorer 11
   • Mozilla Firefox (latest version recommended)
   • Google Chrome (latest version recommended)
   Microsoft Edge (latest version recommended)
2. Latest Java Runtime Environment (Oracle and OpenJDK supported)

Additional Software Requirements

- PowerShell 1.x command line shell installed on the remote computer for the Scripting functionality

Licensing ExpertAssist

The ExpertAssist component is licensed as a part of the overall Desktop Authority licensing framework. Therefore, a valid Desktop Authority license (Standard or Professional) is required in order to use ExpertAssist.

Remotely Accessing a Workstation

When the ExpertAssist software installation is complete, each workstation may be accessed from any machine using a Java-enabled web browser.

To access the host machine:

1. Open an Internet browser.
2. In the Location/Address bar, enter the FQDN, DNS name or the IP address of the host machine as shown in the examples below.

Example:

- http://pc345-XP:2000
- http://192.168.3.26:2000
- http://192.168.3.26:5050

where:

- "`192.168.3.26`" represents the IP address of the host machine.
- "`2000`" represents the default port entered on the ExpertAssist configuration tab.
- "`pc345-XP`" represents the DNS machine name of the host machine.
- "`5050`" represents the port custom defined via the ExpertAssist configuration tab

Logging In

After entering the URL into your browser and pressing enter, the ExpertAssist login screen will be displayed.

Windows Authentication

Depending upon who is logging in to the system, the SAM database, Active Directory, and ExpertAssist's own user database are accessed for authentication.

For the first-time logon:

1. Log on as someone who is a member of the local Administrators group.

   This default behavior can be changed later by granting Windows users or groups access to ExpertAssist through the **Access Control** section of the **Security** node.

2. Type in the credentials that can be used to authenticate on the remote computer and click **Login**.

NTLM

ExpertAssist will use the current credentials (those entered by you at the Windows logon screen on the computer running the browser) to identify the computer to the remote computer. This is only available on local networks.

To login using your current Windows login credentials:

Click the **Login** button within the **NTLM** section.

If available, NTLM requires that the remote computer IP address be added to the Local intranet security zone in your browser.

Typically, the browser will automatically figure out for you if the remote computer is on the local network or not by analyzing the remote computer's IP address class. If not, make sure to manually add the remote computer's address to the Local intranet security zone in your browser, otherwise you will be prompted to enter your credentials despite using NTLM. The behavior is by browser design and depends on the Logon radio button setting in the security zone setting. This setting is typically set to Automatic logon only in Intranet zone in zones' settings.

Smart Card

This logon type will verify your identity based on the credentials stored on a Smart Card. Smart Card support is available on computers running Microsoft Windows 7 or later.

To login using credentials stored on a Smart Card:

Click the **Login** button within the **Smart Card** section.

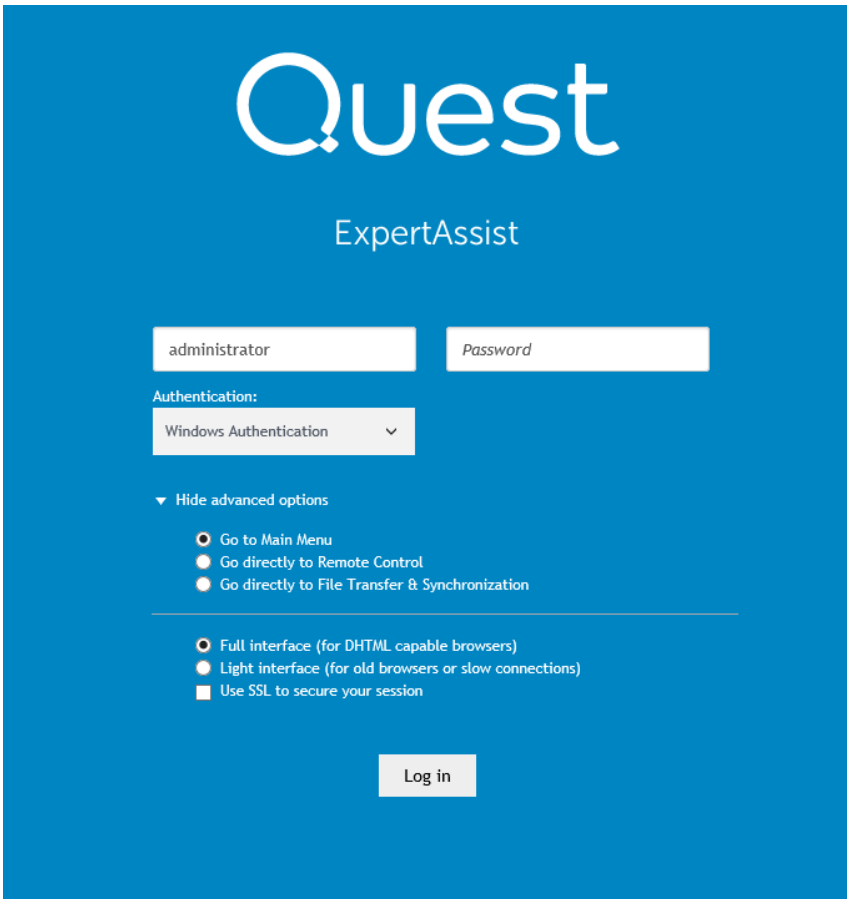
Advanced Options

Additional login and access options are detailed below.

To get access to additional login options:

Click on the **Show advanced options** button in the login window

Figure 1: Login screen with additional options.



Go directly to

Using any of the first three buttons selects whether to go directly to Remote Control, to File Transfer & Synchronization or to the Main Menu page (default) directly upon login.

Full/Light Interface

Choose between the full and light interfaces. The full interface is for DHTML capable browsers. The light interface is more suitable for old browsers or users with slow connections.

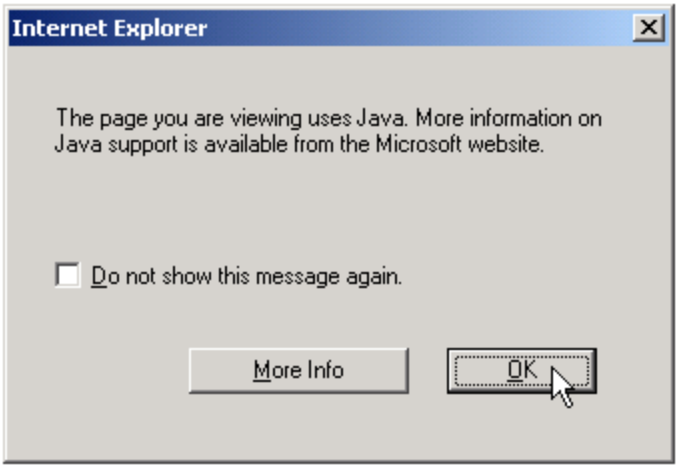
This only works for ExpertAssist users defined within the Access Control page. ExpertAssist administrators always have full interface enabled for them unless specified explicitly. See details in the Access Control section.

Automatic Java Download

Several Quest ExpertAssist functionalities, such as Remote Control, File Transfer, and Performance Viewer, require that you have Java Runtime Environment (JRE) installed on the client computer where you are managing the remote computer from. If you have logged into Quest ExpertAssist using one of the three available authentication options, and you do not have JRE installed on your local computer, you will be prompted by your browser right before you will see the Quest ExpertAssist user interface.

Quest ExpertAssist requires that you have at least JRE version 1.5.0_5 installed on the local computer to work with applets.

Figure 2: The browser prompts for Java update before launching EA.



Click **OK** to close the message box and let the browser to show you the Quest ExpertAssist user interface.

In the topmost frame on the user interface you will see that the Performance Viewer applet is not working and Quest ExpertAssist shows the “Java is not installed” message.

Click on the download link within the frame and Quest ExpertAssist will automatically open the new browser window or tab and redirect you to the JRE download page.

If you are running your browser on a server with Windows Server 2003 or above with Internet Explorer Enhanced Security Configuration (IEESC) mode enabled, please make sure to add the web sites to the Trusted Sites zone when prompted by browser. This behavior is by browser’s design.

You can eliminate these browser web site blocking prompts and difficulties with downloading the JRE by disabling the IEESC on your local operating system.

Download and install the JRE on your local computer. Once installed, Java runtime will enable Quest ExpertAssist to allow you use its applets.

If the automatic installation provided by site does not work for you, either use relaxed browser security settings for the JRE download site, or choose the manual download option.

If prompted by a Java security warning, accept the warning by clicking Yes.

Figure 3: Java security warning.

This warning is normal since Quest ExpertAssist is using a self-signed security certificate, which typically gets automatically issued to the DNS name of the remote computer. Thus, if you are connecting to the remote computer by using the IP address or the NetBIOS name in the URL, JRE will locate the mismatch between the "issued to" string in the client certificate and the computer name in the URL and a warn you about this. In the figure above you may see that the JRE warns the user accessing Quest ExpertAssist by using the https://gluon:port/ntlm URL in the browser since the certificate has been issued to gluon.internal.corp. In the example above, you could avoid having the JRE warning message by accessing Quest ExpertAssist using the DNS name of the remote computer in the URL https://gluon.internal.corp:port/ntlm.

Bypassing the Login Screen

You can bypass the login screen entirely when logging into EA by using one of the following methods.

To force an NTLM login:

Append `/ntlm/` to the URL with which you access the ExpertAssist.

Example,
The URL `http://MAILSERVER:2000` would become `http://MAILSERVER:2000/ntlm/`.

NOTE: Be careful not to forget the trailing slash!

To bypass the menu system and access certain parts of ExpertAssist with NTLM login:

Use the following URL examples for guidance:

- **Remote Control:**
  http://machine.name.here:2000/ntlm/remctrl.html
- **Command Prompt:**
  http://machine.name.here:2000/ntlm/telnet.html
- **Chat:**
  http://machine.name.here:2000/ntlm/chat.html

To force a normal login (with user name and password credentials):

Specify a username and password with which you access the Remote Control host right in the URL.

Example,
The URL `http://MAILSERVER:2000` would become
`http://MAILSERVER:2000/login:username:password:domain/`.

NOTE: Be careful not to forget the trailing slash!

The domain is optional. If omitted, an attempt will be made to authenticate on the computer on which it's running and the domain to which it belongs.

Here are some URLs as an example:

- **Remote Control:**
  http://your.machine.here:2000/login:yourloginname:yourpassword/remctrl.html
- **Command Prompt:**
  http://your.machine.here:2000/login:yourloginname:yourpassword/telnet.html
- **Chat:**
  http://your.machine.here:2000/login:yourloginname:yourpassword/chat.html

Accessing ExpertAssist through a Firewall

Most corporations today employ certain security measures to protect their computer networks from hostile intrusion. One of the common measures includes creating a firewall. A firewall is a system designed to prevent unauthorized access to a private (internal) network. Firewalls can be implemented either as hardware or software, or a combination of the two.

The most common use of a firewall is to prevent unauthorized intrusion from Internet users attempting to access a private network or Intranet. A firewall examines all traffic entering or leaving the internal network/Intranet, ensuring that traffic meets security criteria established by the Network Administrator.

ExpertAssist can be configured to work with a computer protected by a firewall. This requires mapping an external, incoming port on the firewall to the internal IP and port on the computer running the ExpertAssist host.

From outside the LAN, gain access to the computer running the ExpertAssist host by entering the router's IP address and the port to which the desired machine is mapped.

Example:

Router:
External IP address: 111.111.111.111

ExpertAssist host:
IP address: 192.168.0.10, Port: 2000
(port 2000 is the default but this can also be changed)

Map a firewall port to the Computer. In this case, pick a port on the router (say, 5200) and map it to 192.168.0.10:2000.

The procedure for mapping ports from routers to computers is router-specific. Usually the router will have a web-based interface that allows configuration and maintenance. Sometimes router companies refer to this action as Port Forwarding or Port Mapping.

Access the ExpertAssist Host through the firewall

Having done the above, fully access the ExpertAssist host with the URL http://111.111.111.111:5200 - that is the firewall's external IP, followed by the port mapped to the ExpertAssist host.

User Interface

The user interface is designed to make using the ExpertAssist quick and easy to use. For details on each section follow the links below.

Menu

Every page of the ExpertAssist host can be reached from the left hand menu tree of the Manager. The menu tree is expandable and collapsible like Windows Explorer so you can find the pages you need quickly.

The sub-sections of each item in the menu tree are labeled as follows:

- Home
- Remote Control
- File Transfer
- Help Desk Chat
- Computer Management
- Computer Settings
- Server Functions
- Scheduling & Alerts
- Performance Monitoring
- Security
- Preferences
- Custom Pages

Performance Data Viewer

On each page of the ExpertAssist you can see a real-time Performance Data Viewer. This java applet is to the right of the logo in the top frame. It shows CPU load (green) and Memory load (red) and is updated every few seconds so you can get instant feedback on the effects of performance intensive processes.

Figure 4: Performance Data Viewer.

To disable the Performance Data Viewer:

Use the Appearance.section of the Preferences node.

QuickLinks

QuickLinks are accessible from every page of the ExpertAssist.

The QuickLinks menu is situated in the top frame of the page so that your favorite pages are always only a click away.

To add your favorite pages to the QuickLinks drop down menu:

Click the star icon in the tool bar of the page you are viewing.

To edit your QuickLinks:

Click on -- Edit your QuickLinks -- in the QuickLinks drop-down menu.

To access the QuickLinks:

Open the System Overview tab of Home page.

End Remote Session

If you are inactive for 10 minutes you will be logged out automatically.

To close the remote session:

Click the red **End Remote Session** button in the top right corner of the screen, to the right of your computer's name.

To modify the session idle timeout time:

Use the Network page under **Preferences** section.

Time

The time on the remote machine is displayed above the log out button.

Main Content Window

The main content window is where you will do most of your interaction with the host machine via the ExpertAssist. For the most part this should be self explanatory.

On most pages you will see a tool bar at the top. Below is a quick key to the buttons you'll encounter on these toolbars.

Table 1: Main content toolbar buttons.




Refresh	Paste	Permissions	Download files
 Delete	 Rename	 Execute	 Find files
 Cut	 Edit	 Create new folder	 Set sharing properties
 Copy	 Change attributes	 Upload files	 Create rule
 Export to CSV	 View	 Browse	 Parent

System Tray Icon

The ExpertAssist deploys a system tray (notification area) icon on each client that the ExpertAssist service is deployed on. The icon serves many purposes.

The icon will change on the remote computer when the computer is remotely controlled via the Remote Control applet.

To enable/disable the system tray icon on the host computer:

Use the **Appearance** section of the **Preferences** node to modify the Systray Settings.

To open a dialog with the ExpertAssist status and configuration settings, as well as access support information:

Double-click the notification area icon and make the necessary changes or view the information.

To open the ExpertAssist system tray context menu:

Right-click the ExpertAssist system tray. Use the menu options described below:

Open ExpertAssist

This is the default action. Choosing this is equivalent to double-clicking the icon. Select this menu item to load the ExpertAssist management dialog. From this dialog you can open the ExpertAssist using the default web browser, see the ExpertAssist status (enabled or disabled), if the ExpertAssist is currently being accessed or not, and a link to download the documentation.

Open ExpertAssist Web Interface

Select this menu item to load the ExpertAssist on the local machine using the default web browser. NTLM Login will be used.

Open Status Window

Selecting this item displays the ExpertAssist status window. The status window will display a log of all events that have occurred during the past remote management sessions.

Enable/Disable ExpertAssist

Here you can turn the ExpertAssist services on and off at will.

Enable/Disable Status Indicators

Here you can enable or disable the memory and CPU usage indicators.

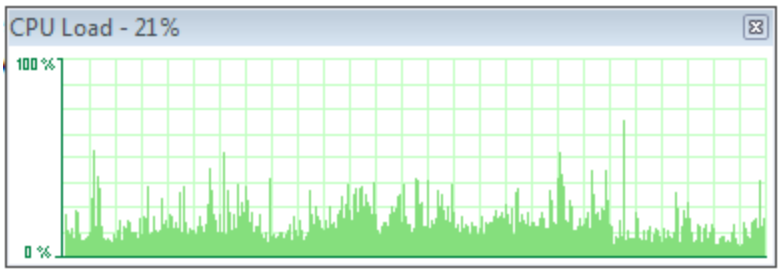
Show Performance Windows

This menu provides a selection of performance indicators to display on your desktop.

The menu selections displayed are based on the performance data ExpertAssist is able to collect from the client. The software automatically collects performance data on CPU usage (total and broken down by individual CPU on SMP systems), and various memory counters. You also can monitor network performance and drive usage in the real time.

When you select an item from this menu, a window will pop up, similar to this:

The performance window.



Double-clicking the performance window will shrink it to a smaller format.

You can have as many of these windows up on your screen as you want. They are persistent – that is, they will automatically appear in their previous position following a reboot.

About

Opens the ExpertAssist About window, providing the software manufacturer and license information.

Home

Home is the page that you will see when you start up the ExpertAssist. Here you will find a useful at-a-glance System Overview information. Your current Quest ExpertAssist licensing status, legal notices, and technical support contacts are available on the separate tabs.

Each tab is described below.

System Overview

System Overview.

About

The About tab provides info on the version of Quest ExpertAssist you are currently using.

Licenses

This tab contains a link to the page with legal terms and conditions of your license for your reference.

Legal Notices

This tab provides info on general copyright data.

Contacts

Contacts is a link to the product owner site to find out more about this and other products.

Here you'll also find the support pages, along with the popular forums and Knowledgebase articles. If the answer isn't in the manual you may well find it there.

System Overview

When you start up ExpertAssist, you will see the **System Overview** tab. It contains a multitude of useful information about the host computer.

Welcome

At the top of the page you'll see the following info:

- A welcome message which displays who you're logged in as.
- The date and time of the host machine.

  Click on the date and time (highlighted in blue) to open a page where you can set the time on that machine.

  The date and time of the host machine page is also accessible on the Time page of the Computer Settings.
- Information about when the machine was last rebooted;
- Information on how long the machine has been running;
- Information on how much data has been sent to how many clients.

Security

In the top right corner of the System Overview section of the ExpertAssist Home page, you can see a summary of your security data. This includes the following:

- The authentication method used to log in;
- Information on the Secure Sockets Layer (SSL) connection.

QuickLinks

QuickLinks are designed to make access to frequently used features quick and easy.

To view the pages added to ExpertAssist's QuickLinks:

Click the icon in the box on the right hand side of the home page.

Or,
Use the dropdown in the upper frame of every page.

To add a QuickLink:

Click on the QuickLinks icon, which appears on every page.

To remove a QuickLink:

Select **Edit your QuickLinks** command from the drop down menu.

Performance

The performance graph details CPU and memory usage. Data about the physical and committed memory are displayed in an easy to read green and red graph.

Most Recent Accesses

Here you can see information about the users who have most recently accessed the ExpertAssist on this computer.

Current Connections

Here you can see data on any current connections on the host machine.

System Information

Here you can see information on the computer itself, including the current CPU utilization.

Operating System

An overview of the operating system of the accessed machine is displayed here, including when it was installed.

Installed Hotfixes

Here you can see a list of the Hotfixes that have been installed on the machine.

For more information about a particular Hotfix:

Click on the Hotfix name .

Alternatively, you can view the list of installed hotfixes listed with other updates and applications installed on the remote computer on the Installed Applications page available under Performance Monitoring object.

Remote Control

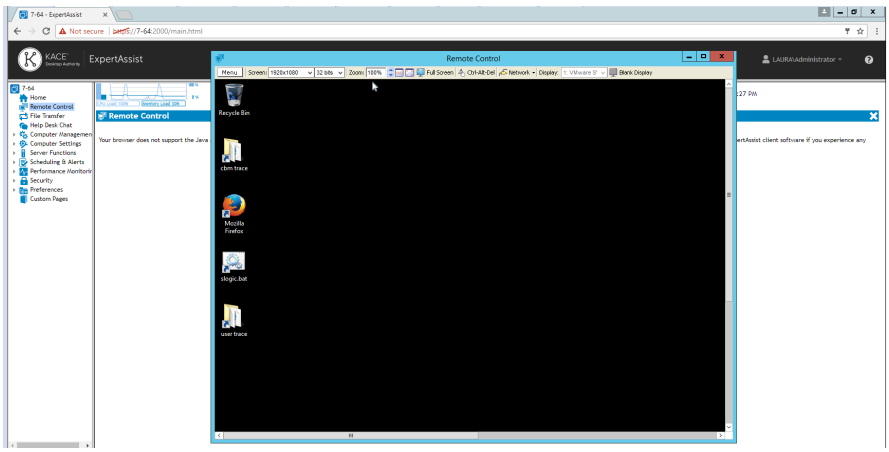
One of the main features of ExpertAssist is its advanced ability to remotely control the computer on which it is installed, thus enabling you to authentically replicate the experience of sitting in front of the host computer — regardless of where you actually are in the world.

When you select Remote Control, a small Java applet is downloaded to the client and will display the screen of the remote computer. Your actions, such as keyboard usage and mouse movement are emulated by ExpertAssist on the screen and on the remote computer. The Java applet downloads automatically.

Depending on your browser settings, you may see a popup window asking you to accept or reject this. You should accept it in order to use Remote Control.

When typing or using your mouse, it will be exactly as if you were sitting in front of the remote machine. The only real difference will be a few ExpertAssist specific tools which appear at the top of the remote control window, detailed below.

Figure 5: The Remote Control window.



Menu Options

In the top left corner of the remote control screen, you will see the menu with the following options:

Send Ctrl-Alt-Del

Pressing Ctrl-Alt-Delete cannot be captured by the applet, but you can still send the combination via this menu item. Selecting this menu item will immediately send the Ctrl-Alt-Del key sequence to the host computer.

Send Special Keys

Certain keystrokes, such as Alt-Tab, cannot be captured by the applet, but you can still send them via this menu item.

Select **Send Special Keys** to gain access to a whole list of special key combinations you might want to send to the host computer.

Transfer Clipboard

Another useful option available from the menu is the ability to transfer your clipboards between machines, thus allowing you to copy from one machine and paste on the other.

The limit is 8 Mbyte in both directions. If the clipboard is larger, you will be notified that clipboard cannot be transferred. It also works with bitmaps.

Below is the example usage of the function:

1. Copy some text on the local machine.
2. Then select **Transfer Clipboard** -> **Local to Host** on the remote screen. Copied text will be placed into clipboard on the host machine.
3. Paste the copied text on a remote machine.
4. The same applies the other way around, but you would select **Host to Local** in order to transfer your clipboard between machines.

Terminal Server Sessions

> **NOTE:** Available when opening a Remote Control session on any operating systems with Terminal Server Sessions support.

The Terminal Server Sessions option lets the user switch between the active Terminal Server sessions.

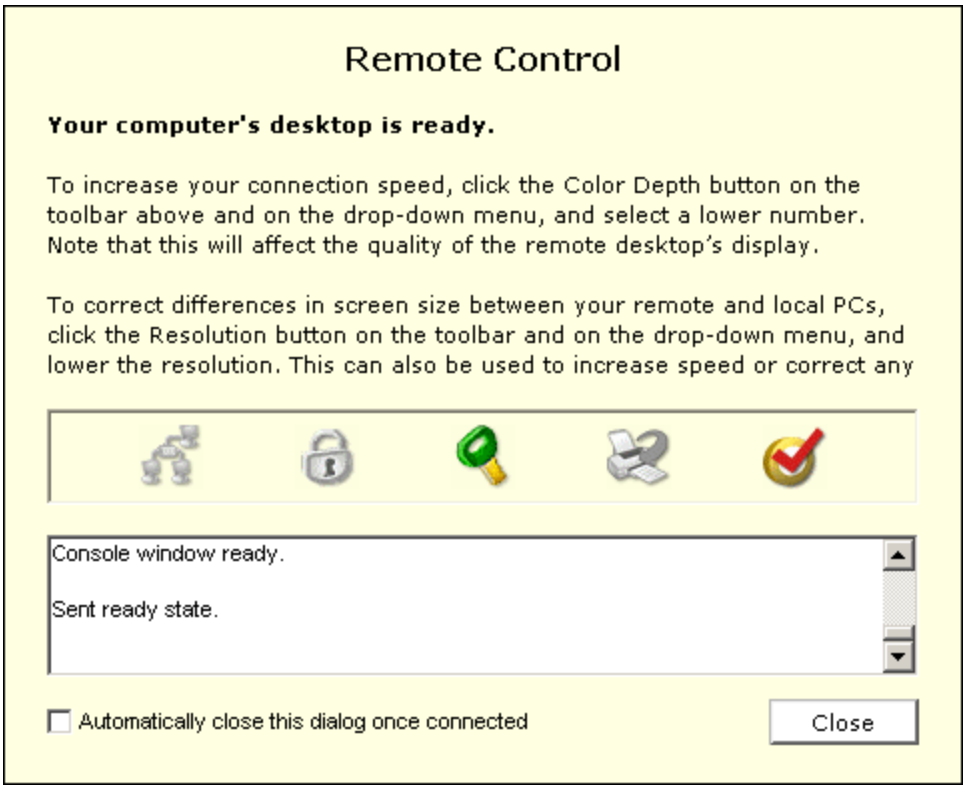
Open Chat

Select Open Chat to initiate a chat session with the remote computer.

View Connection Status dialog

Select View Connection Status dialog to view the status of the connection with the remote computer.

Figure 6: The View Connection Status dialog.



Full Screen

The option detaches the remote window allowing you greater flexibility.

To switch back to the standard ExpertAssist frame:

Select **Exit Full Screen** from the menu.

End Remote Control

Select this menu option to end the Remote Control session.

Screen

Display Properties

You can modify the remote screen's display properties via the menu as well. There are drop-down lists for color quality and screen resolution, as well as a zoom option that allows you to view the screen all the way up to 300% of its original size.

For the best performance during remote control you should set the remote machine's screen resolution down to the lowest, still convenient value.

It is also recommended that you do not use 16-bit (hi-color, 65536 colors) for the remote host's display. Use either 256 colors or true color. Converting 16-bit color bitmaps down to the internal format is rather slow, and has an impact on performance.

Click  to set the dialog size to the same size as the host computer. Click  to fit the host computer dialog within the client's dialog. Click 

to view the host computer in full screen mode.

Ctrl-Alt-Del

Pressing Ctrl-Alt-Delete cannot be captured by the applet, but you can still send the combination via this menu item. Selecting this menu item will immediately send the Ctrl-Alt-Del key sequence to the host computer.

Network

Click Network to select the network type from the given drop-down button list. Select from Modem (56 Kbps), DSL (384 Kbps), WAN (2 Mbps), LAN (10 Mbps) or Auto. Select the network type to optimize the remote control session for the type of network chosen.

Display

Select the Number of Displays for host computers that are using multiple monitors. This will allow the client to switch between the monitors on the host computer during the Remote session.

Blank Display

Click Blank Display to blank the display on the host computer. This is useful for preventing user interaction while remote work is in process.

Remote Notification

When you initiate a remote control session, a notification message will appear on the remote screen. If you do not have full administrative rights on the remote machine, a user sitting there would be invited to decline or accept the remote session, with a default time of 10 seconds before you would be connected automatically. You can configure both the message displayed and the amount of time given to make a decision under the Preferences object. Select Remote Control when a remote session is in progress, a small window in the top right corner of the remote screen is displayed stating who is currently remotely connected to the machine. This message can also be configured under the Preferences object. Select Remote Control.

If the user locked his computer, ExpertAssist can also display the confirmation window over the Windows logon screen, allowing the remote user to accept the remote control session without having to unlock his computer.

ExpertAssist automatically determines if there is an interactive user logged in on the remote computer. If no users are logged in or the remote user has just logged off of the computer, ExpertAssist will determine that nobody is available to answer the Remote Control session confirmation message and skip displaying it. If so, you will be automatically entered the remote control session. This is useful for unassisted remote troubleshooting or resolving remote users' login problems.

> **NOTE:** When the remote control session is started, ExpertAssist will notify the remote user by animating its icon in the notification area of the task bar.

Remote Printing

When connected to the remote machine, and if you have remote printing enabled under Preferences > Remote Control, that machine's default printer will temporarily become that of your local machine. This means that should you choose to print anything from the remote machine, you will receive it on your local printer.

A user sitting at the remote machine would be notified of this change.

Remote Control Preferences

There are a number of special features you can use to configure your remote control sessions under preferences. These are detailed in the Preferences section towards the end of this chapter under the Preferences object. Select Remote Control.

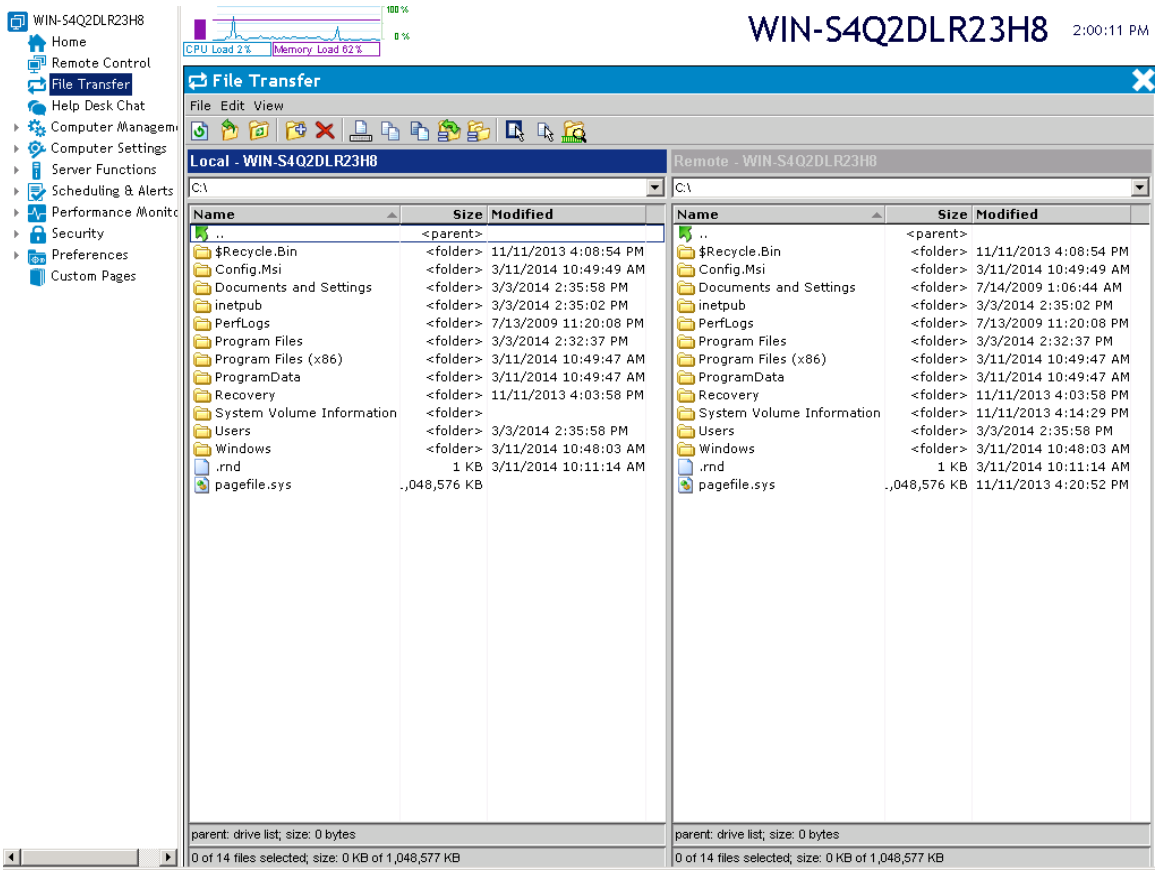
File Transfer

With ExpertAssist File Transfer, you can quickly and securely transfer files between the local and the remote computer. All data transferred between the two computers is compressed and encrypted by the Java applet, so you can be sure that it is secure.

The file transfer screen is divided into two panels:

1. The left hand panel shows the file system of the computer running the web browser.
2. The right panel displays the remote computer's file system.

Figure 7: File Transfer window.



You can use the icons in the toolbar at the top of the screen or your keyboard and mouse to operate the File Transfer applet. There's always an active and inactive panel and you can switch easily between them with the Tab key.

Using the File Transfer applet is very helpful when synchronizing your data. If ExpertAssist notices identical data on the source and destination locations, it will prompt you to choose whether you want to overwrite/update the destination file with the old/new one or skip and continue synchronizing data. It is also possible to apply selected action to all files that will match the same criteria.

The available toolbar buttons are:

 You can refresh the list with the Refresh button, by pressing F5, or by right clicking in the Local or Remote panel and selecting Refresh from the context menu.

 You can go up to the parent directory by clicking on the Up button, by pressing Backspace, or by right clicking on a file or folder and selecting Up from the context menu.

 To go to a different folder click on the Go to folder button, by pressing the CTRL+G key combination, or by right clicking in the Local or Remote panel and selecting Go to folder from the context menu.

 You can create a new folder with the Create folder button or by pressing the CTRL+N key combination, or by right clicking in the Local or Remote panel and selecting Create Folder... from the context menu.

 You can delete a folder or file with the Delete button, by pressing Delete on your keyboard, or by right clicking in the Local or Remote panel and selecting Delete from the context menu.

 You can rename a file or folder with the Rename button, by pressing F2, or by right clicking in the Local or Remote panel and selecting Rename from the context menu.

 You can copy a file or folder with the Copy button, by pressing CTRL+C, or by right clicking in the Local or Remote panel and selecting Copy from the context menu.

 You can move a file or folder with the Move button, by pressing CTRL+X, or by right clicking in the Local or Remote panel and selecting Move from the context menu.

 Synchronize folders by clicking on the Synchronize current folder button or by pressing CTRL+S. Synchronization merges folder contents making sure that each o the synchronized folders contains the most recent version of the file or folder inside.

 Replicate files from the source folder to the destination folder by clicking on the Replicate button or by pressing CTRL+R. Replication replaces target folder contest making sure that the target folder is a bitwise replica of the source folder.

 You can select files with the Select files button or by pressing + (plus) on the number pad.

 You can unselect files via the toolbar Unselect files button or with - (minus) on the number pad.

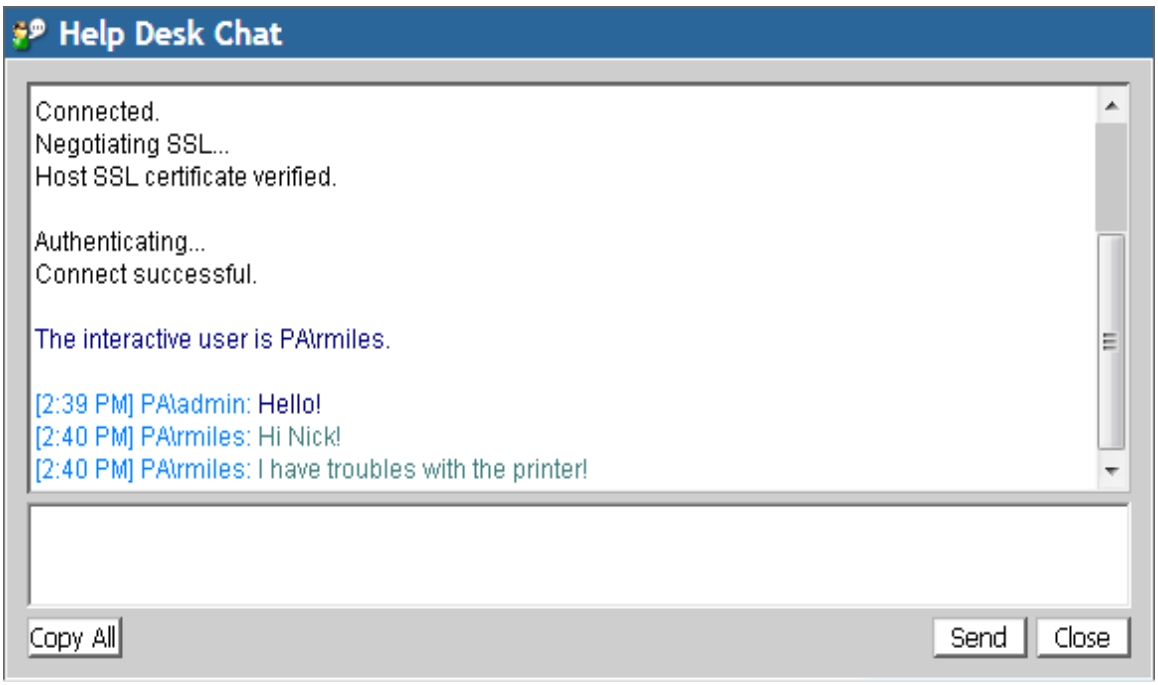
 Select the folder on a remote or local computer and click the Folder size button or press CTRL+F to calculate the size of all contents within the selected folder. Alternatively, right-click the chosen folder and select Folder size from the context menu.

Go directly to the Drive List by right clicking on the active panel and selecting Drive list or by pressing Ctrl+Backspace.

Help Desk Chat

ExpertAssist's Help Desk Chat feature allows you to communicate with the user sitting in front of the remote computer as you would with any instant messenger software. ExpertAssist's advanced diagnostic capabilities can be put to use while you're remotely connected.

Figure 8: Help Desk Chat window.



1. Type text in the lower pane of the chat window.
2. Once typed, click **Send** button or hit **Enter**. The text typed by both yourself and the remote user appears in the upper pane of the chat window.
3. You can distinguish the typed text of yours from that typed by your remote user by different font coloring used for the typed text.
4. Use Ctrl+Enter key combination for entering paragraphs while you type.
5. You can copy and paste text from and to these windows.

This functionality is implemented in a Java applet which is similar to the screen that the remote user will see.

Computer Management

The Computer Management object allows you to take advantage of a wealth of ExpertAssist administrative features including the File Manager, information on the Processes, Services and Drivers of the remote machine and even a reboot of the remote machine.

File Manager

The File Manager displays a list of all available drives, together with their capacity and available space.

Double-click on the drive names to get into the root directory of that drive, where all files and directories are also links.

Double-click on the name of a subdirectory to get into it and produce a listing.

You can select multiple consecutive files with the Shift key, or non-consecutive files with the CTRL key.

Use the toolbar buttons to copy, delete, or move the selected files.

To work with files:

1. Double-click on the name of a file and the ExpertAssist will send it to your browser.
2. Press the Back button to close the file.
3. Press the Save button to save any changes made to the file.

Table 2: File Manager toolbar buttons.

Click QuickLinks to add your favorite pages to the QuickLinks drop-down list.
Click Refresh to redisplay the File Manager list of files and folders.
Click Parent to go to the Parent folder (move back one folder).
Click Root to go to the root folder of the drive.
Click Browse to open a file browser window.
Click Delete to remove the selected file/folder.
Click Copy to copy selected file/folder to another location. The path to selected file/folder is copied to the clipboard. Copying is performed when you click Paste in the selected destination.
Click Cut to move selected file/folder to another location. The path to selected file/folder is copied to the clipboard. Move is performed when you click Paste in the selected destination.

Click Paste to paste the copied/cut file/folder into the selected destination.
Click Rename to rename the selected file/folder.
The Edit button lets you edit small text files right within your browser. This is useful for changing small configuration or batch files without downloading or uploading.
The Attributes button lets you change file attributes, such as Hidden, Read-Only, etc.
The Permissions button lets you specify NTFS access permissions on the selected objects.
By clicking the Execute button, the ExpertAssist will attempt to launch each selected file on the host.
Click Create to create a new folder.
Clicking the Upload button lets you upload files from your local computer to the current directory of the remote computer using your browser.
Clicking the Download button lets you download the selected file/folder from the remote computer to the local computer. You will be prompted for a download location.
Click the Find button to perform a file search. Use wildcards to find the file/folder by specifying a part of its name.
Click the Sharing button to set the Sharing properties of the current folder.
Click the View button to see the file/folder properties.
Click the Export button to export the displayed table of files and folders into the CSV file.

Fields of the File Manager

The File Manager has the following columns in its view:

Icon

A small icon indicating the file type

Name

File name and extension

Size

File size

Modified

Last modification time

When hovering over a file or folder in the currently selected drive, a tooltip will be displayed containing the following information:

Name

File name and extension

Size

File size

Attributes

File attributes (i.e. read-only, system, etc.)

Created

File creation time

Modified

Last modification time

Accessed

Last time the file/folder was accessed

Permissions

Indicates what actions the user can perform on the object (i.e. read, write, change, etc.)

Owner

The owner of the file/folder

Go

The **Go** field accepts a path name.

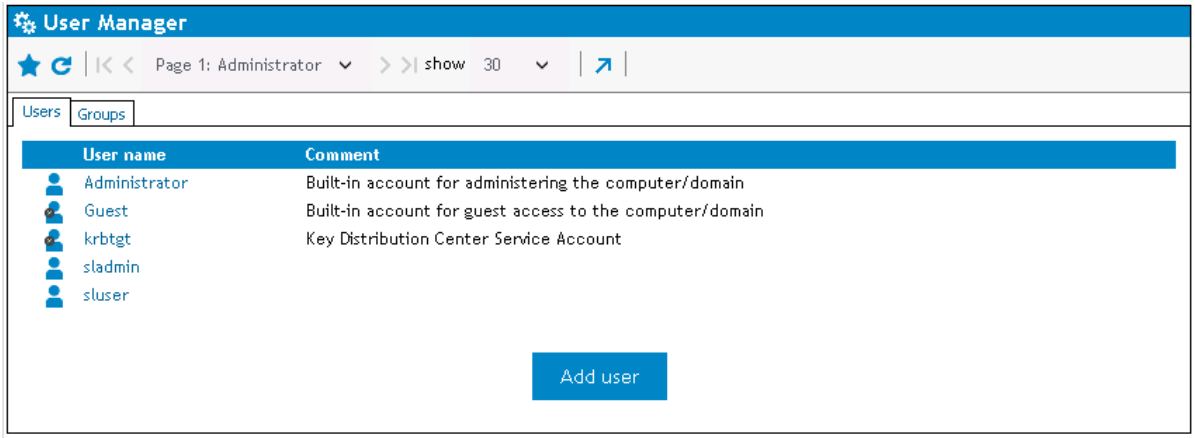
Enter a directory (for example `C:\Windows\System32\Drivers`) and click on the **Go** button. This will immediately take you to the requested location, without having to click your way there. This can be especially helpful over slow connections.

Clicking on the header fields will change the sorting order of the file list to the relevant column.
For example, to sort files by modification time rather than name, simply click on the header field for that column. To sort in descending order, click the header field of the currently active sorting field again.

User Manager

When you click on User Manager under the Computer Management object you will be able to access ExpertAssist's full-blown User Manager. User Manager supports all the features of Windows' built-in User Manager including user and group maintenance.

Figure 9: The User Manager window.



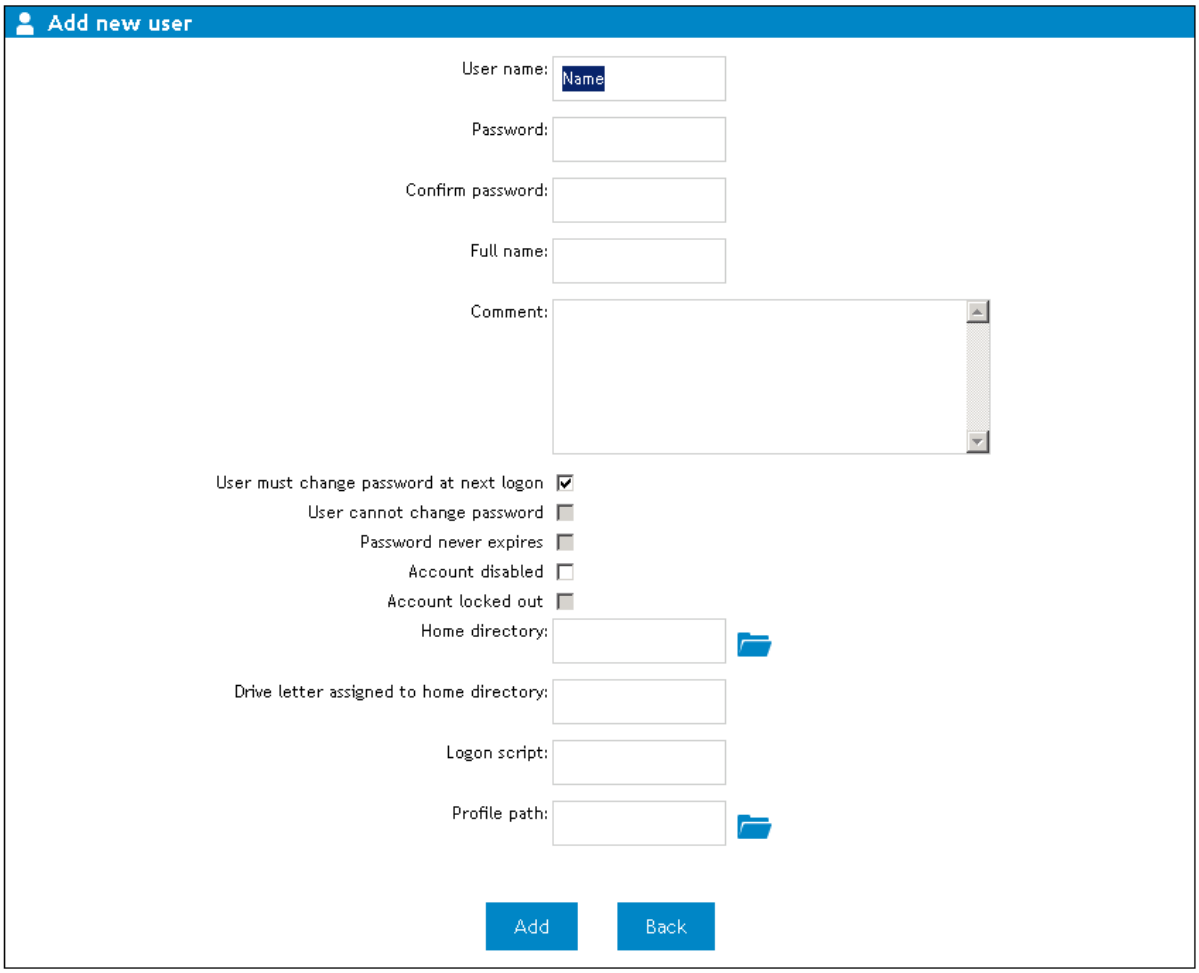
Click **Add user** on the **Users** tab to add a new local user to the computer.

Click on an existing User name to modify the account settings.

On the **Groups** tab, click **Add group** to add a new local group or click on an existing group to manage the group settings.

Add User

Figure 10: The Add User window.



User name

Enter the new user account name.

Password

Enter the user account password.

Confirm password

Type the password again to confirm it.

Full name

Enter the user's display name.

Comment

Enter any text to describe the user account.

User must change password at next logon

Select this box to force the user to reset the password at the next logon.

User cannot change password

Select this box to disallow the password to be changed.

Password never expires

Select this box to enable the password to never expire.

Account disabled

Select this box to disable the selected user account.

Account locked out

Read-only setting that specifies the user account is locked out. This user may not log on to the network.

Home directory

Specify a shared network folder as the home directory.

Drive letter assigned to home directory

Specify the network drive letter to which the home directory will be mapped to.

Logon script

Enter the name of the logon script.

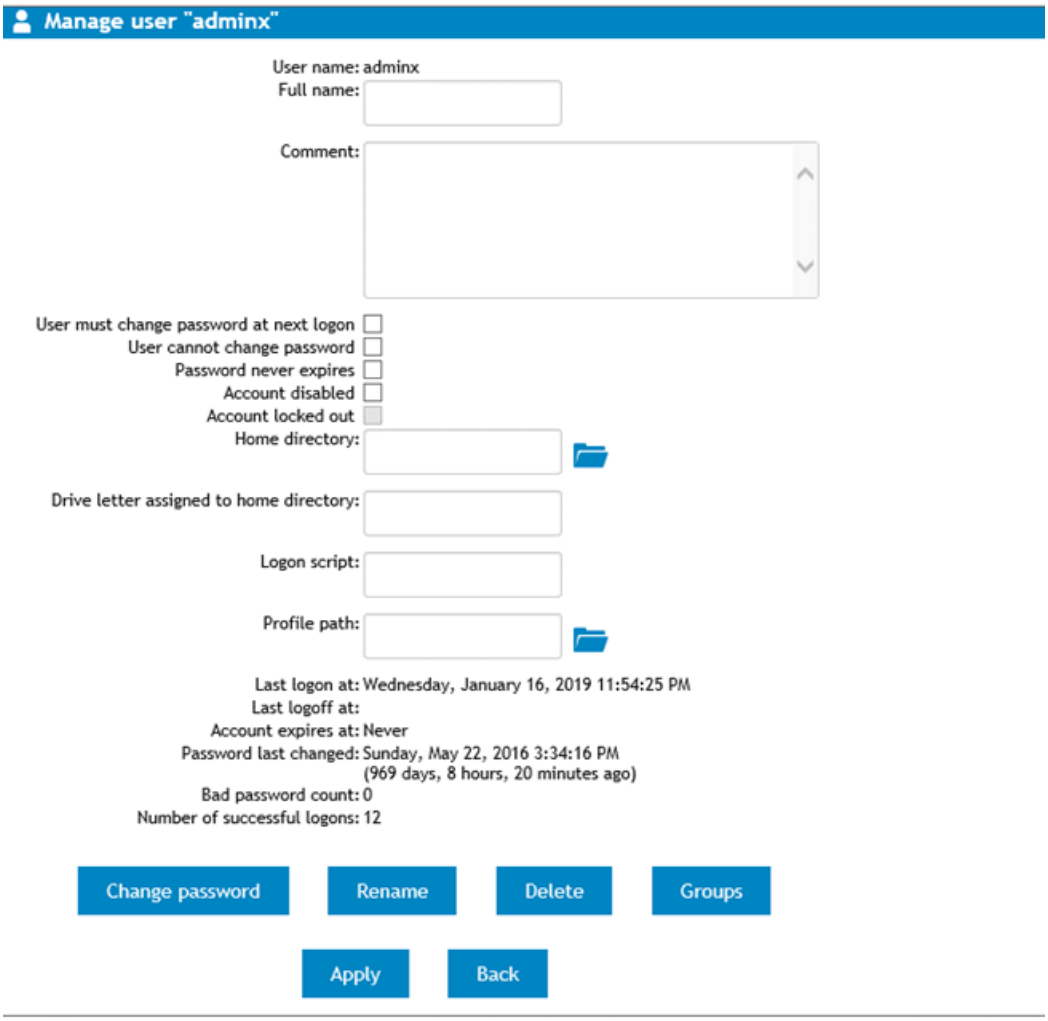
Profile path

Enter the path to the mandatory or roaming user profile.

Manage User

The Manage User dialog presents the same configuration settings as the Add User dialog. The Manage User dialog also presents several different user account statuses—Last logon, Last logoff, Account expires, Password last changed, Bad password count and Number of successful logons.

Figure 11: The Manage User dialog.



Last logon

The date and time of the last time the user logged on to the computer.

Last logoff

The date and time of the last time the user logged off to the computer.

Account expires

The date and time the user account is set to expire.

Password last changed

The date and time of the last time the user password was changed.

Bad password count

A count representing the number of times a bad password was entered during logon.

Number of successful logons

A count representing the number of times a successful logon has occurred.

Apply

Save all changes made to the user account.

Change Password

Modify the current password.

Rename

Change the current user name.

Delete

Delete the user account.

Groups

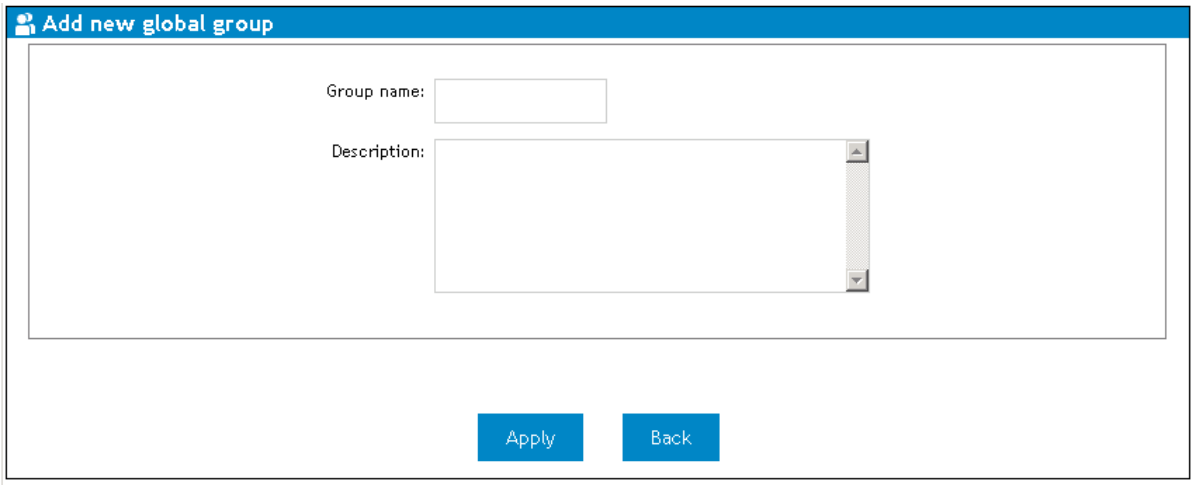
View the local groups the user is a member of.

Back

Go back to the User Manager page.

New Group

Figure 12: The Add New Global Group dialog.



Group name

Enter the name of the new group.

Description

Enter a group description.

Manage Group

The Manage local group dialog displays Group Members and Non-Group Members.

A group can also be renamed or deleted here.

Event Viewer

If you select Event Viewer under the Computer Management object, you can view the NT logs of the remote machine. This feature is very much like Windows Event Viewer snap-in.

(*For Windows 7 and above operating systems*) The Application and Services Logs are also available on the page. You will see a listing of log entries on your screen.

Click on an entry in the list to display its details.

Click the **Export** button to download a CSV file containing a table of the currently shown events.

You can choose to clear the contents of the log file by pressing the **Delete** button in the toolbar.

If you specify a filename, the event log will be backed up before being erased.

You can also have the ExpertAssist send email alerts to a specified email address when log entries matching a given criteria are entered into any of the event logs. For more information on this feature and its uses, select the Scheduling & Alerts object in the navigation pane. See Email Alerts.

Services

When you click on Services under the Computer Management object you will see a list of services running on the remote machine. The Services page displays the names and statuses of all the services installed on the remote machine.

In the list of objects, the status field shows Started, Stopped, etc. ExpertAssist looks through the list of services, and if it finds one that is set to start automatically but is not running, current service status is colored in red. This alerts you to the fact that the service should be running, but isn't.

Click the **Export** button to download a CSV file containing the list of all the services available on the remote computer containing services names, statuses, startup types and description.

To view and/or configure a service:

1. Double-click on the service name to view more details about the selected object and control it.
2. You can change its startup and logon options.
3. When specifying a user account to be used by a service, it must be in DOMAIN\USER form. If you want to use a local user account, you can type .\USER. Be sure to provide this local user account with the right to logon as service.
4. Dependencies can also be viewed by selecting the Dependencies tab.

Processes

When you click on Processes under the Computer Management object, you will see a list of processes running on the remote machine. The Processes page will give you a listing of all processes running on the remote computer.

The list is hierarchical – a parent process will have its child processes listed beneath it, with indentation indicating relationships. Please note that this is for information purposes only, since Windows reuses process IDs.

The following information is available:

- **PID** The internal Windows Process ID.
- **Name** The name of the executable file with full path. This works as a link, and double-clicking on it will give you some very detailed information on the process. On that page, you have the option of changing the priority class for the selected process. This data is arranged on separate tabs for easy viewing.
- **CPU%** Percentage of CPU utilization by process.
- **Priority** The priority class (base priority) of the process.
- **Type** The type of the process (service or interactive).
- **Memory** The amount of total memory (Memory usage plus VM size) in use by the process in kilobytes.
- **Mem%** Percentage of memory usage by process.

The following Process information can be viewed by putting the cursor over the process. They will be displayed in a tooltip.

- **Name** The name of the executable file.
- **Description** The description of the process' file, if given.
- **Version** The version of the file, if given.
- **User Account** The user account that the process is running under.
- **Handle count** The number of object handles the process is using.
- **Threads** The number of threads the process is using.
- **Time Created** The date and time the process was started.
- **CPU Time** The amount of CPU time (d:hh:mm:ss'mss) the process has used.
- **Parent PID** Process identifier of the parent process for the selected process.

The **Refresh** button will retrieve and display the latest process list.

Clicking the **End Process** red button with a white cross will have ExpertAssist kill the process. The process will be terminated immediately.

The CPU utilization function showing process CPU load in CPU% column works in the following manner. It takes two process list samples, two seconds apart, and compares the amount of CPU time used by each process between the two samples to calculate CPU utilization percentages. The total amount displayed can actually be more than 100% on multiprocessor systems, since each processor can be utilized from 0 to 100 per cent. For dual-processor systems, the maximum is 200%, for quadprocessor systems it is 400%, etc.

Click the **Export** button to download a CSV file containing more details on the processes running on the remote computer. The CSV file contains information about the PID, process name, description, CPU time consumed by each of the processes, process image file version, memory usage, number of threads created by the process, the time process has been created, process base priority, and the user account that each of the processes runs under.

Double-clicking a process will show you more detail about the selected process. Threads, DLLs, open files and registry keys used by the selected process can also be viewed.

Drivers

When you click on Drivers under the Computer Management object, you will see a list of drivers running on the remote machine. The Drivers page displays the names and statuses of all the drivers installed on the remote machine.

Double-clicking on the driver name will show you more detail about the selected object.

Dependencies can be viewed by selecting the Dependencies tab.

In the list of objects, the status field shows Started, Stopped, etc.

ExpertAssist looks through the list of drivers, and if it finds one that is set to start automatically but is not running, current driver status is colored in red. This alerts you to the fact that the driver should be running, but isn't.

Click the **Export** button to download a CSV file containing the list of all the drivers available on the remote computer containing services names, statues, startup types and description.

Registry Editor

The Registry Editor enables you to edit the registry of the remote computer using ExpertAssist. First, the registry roots (HKCR, HKCU, HKLM, etc.) are displayed.

Drill down into registry roots by clicking the plus sign (+) next to them or clicking twice on their names.

Registry keys are links that open up that key for you. Key values are also displayed here, with their name, type and value.

You can edit values that are of either text (REG_SZ, REG_EXPAND_SZ or REG_MULTI_SZ), integer (REG_ DWORD), binary (REG_BINARY), and other value types.

Using the toolbar buttons at the top of every page you can add a subkey or delete the currently selected key. You can add a value, delete it or set its access permissions.

Command Prompt

You can access a command prompt from within your browser by selecting Command Prompt under the Computer Management object. The Telnet client, written as a Java applet, provides encryption and data compression for security and speed. The Telnet server included with ExpertAssist lets you access a command prompt on a remote computer from terminal emulator software or a web browser.

Use the **Mark**, **Copy**, and **Paste** buttons at the bottom of the screen as the corresponding Windows Command Prompt commands.

Use the CB (clipboard) button to display the content that you have just copied into the Command Prompt window of EA:

1. Click **CB** to open the clipboard window with data copied from the Command Prompt window.
2. (*If the Clipboard window is open*) Click the **Refresh** button of the Clipboard window to display the most recent data sent to clipboard.
3. Click **Send** and then **Paste** to paste the data from the clipboard into the Command Prompt.

You can either use the Java Telnet client that's part of ExpertAssist, or any other terminal emulator you like. There are several reasons to stick with ExpertAssist's client:

It's secure - it uses the same encryption that's employed by the remote control module. You must be connected to ExpertAssist though HTTPS in your browser to enable the channel encryption. It's fast, since it uses

sophisticated data compression to achieve high throughput. Furthermore, you don't have to keep a Telnet port (23 by RFC defaults) open on a remote machine. The Command Prompt client allows you to work directly through the port you use to connect to ExpertAssist (2000 by default). And finally, it lets you transfer keystrokes that terminal emulators don't handle, such as the Alt key. You can also use your mouse in console applications that support it.

If you decide to use a terminal emulator instead, you will need to start the Telnet server and connect to the Telnet port (23).

To start the Telnet server:

1. Set ExpertAssist to allow the Telnet connections. This can be done on the Telnet Sever configuration page under the Preferences object.
2. You can change the default listen ports in the configuration dialogs to any port available on the remote computer.
3. When a connection is initiated from a terminal emulator, you will be asked to log on.

   This is handled automatically by telnet clients, so you need to enter your username and password in the standalone client itself. ExpertAssist's built-in client, on the other hand, automatically logs you on to the remote computer telnet session using the credentials specified when logging to the ExpertAssist.

   With standalone Telnet clients, you need to enter your credentials in clear text during the session. You are asked for your username, password, and domain. Specify your Active Directory domain as the domain if you want to authenticate on the remote computer using your domain credentials. Otherwise, specify the remote computer's name to authenticate using SAM credentials (local to the remote computer).
4. After successfully logging in, you will be asked if you want full console support if you had the Ask console parameters checkbox set on the Telnet Server page. If you answer with No, you will only be able to use stream-mode programs - applications that take over the whole console window, like Edit.com, the Far file manager, etc. will not work. To answer No, press the 'n' key on the keyboard. However, if you are only planning to use command-line utilities, you can safely say No to this question. You will be taken directly to the command prompt.
5. (*If you answered Yes to the previous question*) You will be asked to specify the console window size. To answer Yes, press the 'y' key on the keyboard. A default value is provided for you. You should make sure that the terminal emulator you are using supports it and is set to the size you enter here.
6. Finally, if you have an ANSI compliant terminal emulator, you can choose to use ANSI color support during the session.
7. Should you disconnect your terminal emulator, or go to a different page in the browser window containing the Telnet client applet, all applications you have running in the Telnet session are left active.

   You can reconnect to this Telnet session by simply logging in (or loading the applet) again. There is a timeframe for this though: if you do not reconnect within an hour, all your telnet applications, including the command shell, are terminated. You can change the timeout value from the default one hour to anything you like under Preferences object on the Telnet Server configuration page.
8. To close the Telnet session, type Exit at the command prompt.

Reboot

When you click on Reboot under the Computer Management object, you will see the following reboot options. There are five choices.

 **Restart ExpertAssist** Restarts the ExpertAssist services. It does not reboot the remote machine. This is useful if you change settings like the listening port and have no physical access to the machine in order to restart the service.

 **Normal Reboot** Closes all processes and reboots the remote machine in an orderly fashion.

 **Emergency Reboot** Does not allow applications and other processes to terminate gracefully, so you might lose unsaved data. Windows will, however, shut down nicely and flush all outstanding file operations to disk. This can be useful if there are hung processes that prevent Windows from shutting down normally.

 **Hard Reboot** Reboots as quickly as possible. This option will not allow Windows to terminate gracefully, so you might lose unsaved data. This may help if the remote computer hangs. Since rebooting is immediate (just like pressing the reset button) you will not receive any feedback from ExpertAssist when clicking this button.

 **Scheduled Reboot** This allows you to schedule a date and time to automatically reboot the remote computer which you are currently managing. This is useful if the reboot is not urgent and can take place during off-peak hours.

Monitor Host Screen

On this page you can safely monitor the remote computer's screen. This allows you to watch what the remote user is doing on his computer without the risk of interfering with the user's work.

Update Now

Remote computer or a remote user logged into the remote computer can be assigned a number of Group Policy objects.

(*For Desktop Authority Manager users*) These settings can be much more sophisticated if the remote computer, user, OU where they have a membership group or other Active Directory objects were assigned an action via Desktop Authority Manager. To lessen the load on the computers, both the IntelliSense and the Desktop Authority client component apply their policies on a regular basis with a strictly defined update interval. ExpertAssist allows you to force applications of both types of policies to get them applied to the remote computer or user immediately upon your request.

Group Policy Update

Group Policies are updated on a timed interval. By default, the background refresh interval is set to 90 minutes with a time offset of 0 to 30 minutes. This time offset allows avoiding collisions when several computers could request a Group Policy refresh at the same time. The larger the time offset, the more unlikely the collision in refresh requests and the more the latency.

To force a Group Policy update for both computer and user policies on the remote computer immediately without waiting for an automatic group policy application:

1. Click the **Group Policy Update** button to refresh local and Active Directory based Group Policy settings, including security settings at the current time. This will force Group Policy settings to re-apply on a

remote computer even if there has been no change to the Group Policy settings.

2. (*If there are any client-side extensions (such as Software Installation) enabled in any Group Policy Object to be re-applied on the computer*) Reboot the remote computer to re-apply client-side extensions (if necessary). Click the **Reboot** button when the Group Policy is updated.

   Don't click the **Reboot** button if you don't need to re-apply the client-side extensions.

Computer Settings

In addition to the administrative features available under Computer Management, you can also view and modify a number of settings on the remote machine, from Environment Variables to Automatic Priorities.

Environment Variables

Here you can view and make changes, if necessary, to System Environment Variables on the remote machine. Windows environment variables that are defined by you or by programs are listed, such as a path where files are located. These are the variables that are effective for all users logged into the computer.

Click the **Export** button to download a CSV file containing the list system environment variables available on the remote computer.

Virtual Memory

This option allows you to change virtual memory settings on the remote computer:

1. Simply enter an initial (minimum) or maximum size for the paging file next to a drive listed above.

   Entering zero values both for the minimum and maximum size will set the paging file size to a minimum allowed for the current remote computer configuration.
2. Click the **Apply** button. Entering zero values both for the minimum and maximum size will set the paging file size to a minimum allowed for the current remote computer configuration.
3. You will need to reboot the computer for any changes to take effect.

User Account Control

NOTE: *Available only if managing EA hosts running Windows 7 and above operating systems*

Use the options available on the page to configure the User Account Control (UAC) Settings of the remote computer.

To modify the UAC settings of the remote computer:

1. Select the desired option to configure the UAC settings:
   a. Use the **Settings for administrators** section to configure UAC settings that will apply when an administrator-level user is logged into the remote computer.

b. Use the **Settings for users** section to configure UAC settings that will apply when a non-administrator user is logged into the remote computer.

   The availability of the user-specific settings depend on the configuration of the **Settings for administrator** section.

2. Click **Apply**.
3. Click the **Normal Reboot** button that will show immediately after you click **Apply** to reboot the remote computer in order for the changes to take effect. The remote computer will restart immediately.

   Or,
   use the Reboot section to perform other types of reboot.

Time

This option allows you to edit the time on the remote computer:

1. Simply enter the correct values
2. Click the Apply button.

NOTE: The time is displayed according to the time zone settings of the remote computer.

Automatic Logon

This option lets you enable or disable Windows autologon feature.

Enabling autologon will cause the remote computer to bypass the logon screen after system startup and log in with the username and password specified here.

Using Enabled autologon is a potential security risk: the username and password are stored in the registry in clear-text format.

Shared Resources

This function gives a detailed report of all shared resources on the remote computer, including shared folders, administrative shares, and printers etc.

The Path link (in the right hand pane)

The link to the Path in the right hand pane of the window takes you to the directory in File Manager.

The Connections list shows open connections and number of open files, if any.

Locked files are listed in the Files list.

To forcibly close these connections and files:

Click on the **Close** button.

Access permissions active on the object can also be listed and changed to your needs. Accept permissions for administrative shares are not shown since permissions cannot be set on them.

The **Delete** button removes sharing from the object.

To download a CSV file containing the list of all network shared resources available on the remote computer:

Click the **Export** button in the left-hand frame of the page.

To download a CSV file containing detailed information for the currently selected shared resource:

Click the **Export** button in the right-hand frame of the page.

Automatic Priorities

Automatic Priorities lets you direct ExpertAssist to automatically change process priorities. If you have ever wanted to run a backup on your server without impacting performance or archive a huge directory structure using zip/WinZip on a live web server without putting additional load on the machine you will find this feature useful. Likewise if you have ever wanted your workstation to be responsive while you browse the web on your workstation during a lengthy compile, you may set the browser process to have a higher priority than the compiler.

To set the priorities:

1. When you click on Automatic Priorities, you are taken to a page that shows you a list of executables and their target priorities. By default, the list is empty, so you will need to click on the Create button,  , in the toolbar.
2. On the dialogue that comes up, enter the name of the executable, and select the target priority from the drop-down list.

   The name of the executable is without paths, so, for WinZip it is `WINZIP.EXE`, for the Microsoft C compiler it's `CL.EXE`, etc.

   The target priority is usually Normal. This puts your process in the same priority class as the screen saver, meaning that it will only get a chance to make any progress if it does not compete for CPU power with the processes with a higher priority class.

   You can also select a target CPU or a CPU core for the process. This allows you to divide processes amongst CPUs on an SMP machine to suit your needs.
3. Click on **Add** and you are taken back to the previous list that is now showing your executable's name and the priority class you selected.

If there are entries in the list, ExpertAssist will scan the process list on your machine every ten seconds, looking for the process names you entered. If ExpertAssist finds one and its priority class does not match the one you specified it will be changed to your preference.

Click the **Export** button to download a CSV file containing the list of custom process priority management rules to your local computer.

Server Functions

Under Server Functions you can find all the pages you'll need to make use of ExpertAssist's powerful FTP capabilities.

ExpertAssist comes with an extremely versatile FTP server. You can set up an unlimited amount of FTP servers on one computer, each with its unique IP address and port combination. You can create users and groups for your FTP server, or you can use the built-in Windows accounts for rights management.

If logging has been enabled on the Log Settings page of the Preferences object, the FTP Server will log all user activity to the main ExpertAssist log file (`DesktopAuthority.log`).

FTP Configuration

The options for creating and managing the settings for your FTP servers, users and groups are arranged into three tabs.

FTP Servers

In order to create a new virtual FTP server on your machine:

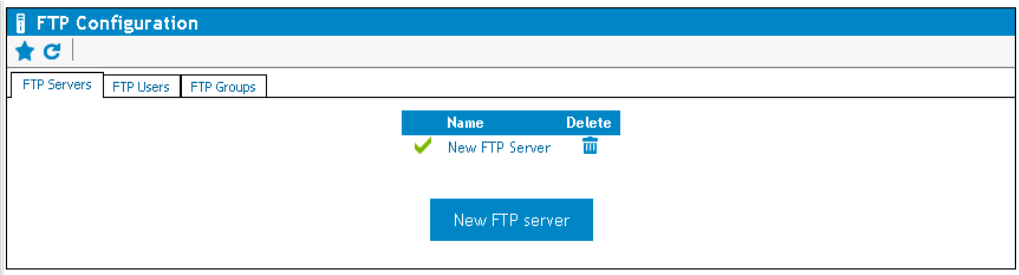
1. You need to define at least one virtual FTP server on the FTP Servers tab of the FTP Configuration screen.

   If no FTP servers are defined then this screen will be blank, except for the **New FTP server** button.

   Use the link to know details on the available options.

2. Once you have defined a new server they will be listed in a table.

   Figure 13: The FTP Servers list.



To delete a server:

Click on the red box in the delete column to the right of a given server.

To start/stop the server:

Click on the status indicator to the left of the virtual server.

Status indicators

1. A green circle status indicator indicates that the server is running.
2. A red one shows that it is stopped. This may be either because it was stopped manually, it has been disabled, or it was not able to start due to an error.
3. When you stop an FTP server on this screen its status will change to Disabled. This means that when you reboot the computer the server will not be started automatically.
4. Likewise, if you start a stopped or disabled FTP server it will be Enabled, and it will start automatically on rebooting.

FTP Server Configuration options

Name

The name of the virtual FTP server. This is for reference purposes only. You can call your server whatever you want. This is what will be displayed on the FTP Configuration page, the login message from the FTP server, and so on.

TCP/IP port to listen on

The port in use by the virtual FTP server. The default is the standard FTP port, 21.

TCP/IP address to listen on

The IP address to use. You can select one item from the list. If you select All available interfaces the virtual FTP server will listen on all assigned IP addresses.

IP Filter

The IP Filtering drop-down list lets you specify the IP addresses from which to accept connections. By default, the clients can come from any IP address. The IP filtering engine is the same as that used by ExpertAssist itself. Please see the section on IP filtering under Security for more information.

If a server is enabled, it will start automatically with ExpertAssist. If disabled, you will need to start it manually.

Port range for passive data

Enter a range of ports to use for passive FTP data transfers. These ports will be used on FTP server when the client is connecting in passive mode (PASV command). Passive mode is needed if the FTP client is connecting from behind the firewall and the FTP server cannot establish incoming connection to the client.

IP address of the network interface connecting to NAT router

Select the corresponding IP address from the drop-down list for the network interface in the same subnet with the NAT router. This should be the network interface that allows connecting from the FTP server to NAT router.

Subnet mask of the network interface connecting to NAT router

Enter the subnet mask for the network interface in the same subnet with the NAT router.

External address of NAT router

Enter the external IP address for the NAT router.

The server is enabled

Select this box to indicate if the FTP server is enabled. This has the same meaning as clicking the green circle status indicator on the FTP Servers tab.

Use Implicit SSL encryption

Select this checkbox to use implicit SSL encryption (passive security). Implicit security provides and “always-on” mode security when you don’t have to bother about turning the SSL security mode on FTP server each time you connect to FTP server. Once the implicit SSL encryption is enabled, you can connect to a FTP as usual and you will always have your connection encrypted through the SSL.

Root directory

The root directory for the virtual FTP server. If you leave this field blank the drive list will be used as the root.

Resolve shell links

If you enable this option, shell links (.lnk files) pointing to directories will be displayed as directories, enabling you to use Unix and NTFS file system hard links.

Download bandwidth limit

The global download speed limit for the server. No matter how fast users are accepting data, the server will not send it any faster than the speed specified here.

Upload bandwidth limit

The global upload limit to the server. No matter how fast users are sending data, the server will not accept it any faster than the speed specified here.

> **NOTE:** The following FTP server configuration pages will become available as buttons at the bottom of the page: Security, Windows Users, Welcome, ODBC

Security

The Security configuration page lets you specify various security and connection-related options.

Table 3: FTP Server Security options.

Maximum number of simultaneous connections	The maximum number of simultaneous connections to the FTP server. Setting it to zero means that there are no limits.
Maximum number of failed login attempts	If a user fails to log in with this many tries the connection will be dropped and the user’s originating IP will be locked out on FTP server.
Login timeout	The maximum number of seconds the user can take to log in until control connection will be closed by FTP server.
No transfer timeout	The connection will be considered idle and will terminate after the specified number of seconds have elapsed on an open connection without a file transfer

	or directory listing.
Stalled transfer timeout	This is the amount of time a file transfer can spend without sending or receiving any data before it is considered stalled and thus terminated.
Allow keep-alives	FTP clients use various commands to keep the connection from being idle. When enabled, FTP commands such as CWD, PWD or the ubiquitous NOOP will reset the No transfer timeout counter (described above). If disabled, only an actual file transfer or a directory listing will reset the counter.
Thread priority	You can select the priority of the threads servicing users for the FTP server. If you are running an FTP server on an otherwise busy host computer it might be a good idea to set the priority to a lower value than the default Normal setting.
Allow unsecured FTP connections	If this option is disabled the FTP client must support and utilize SSL. Client connected though unsecure FTP will get error 524 Only secure authentication is allowed.
Allow data connections to go to different IPs than that of the control connection (enable FXP, basically)	The FTP protocol uses two connections: The control connection and the data connection. The data connection is where all the raw data is sent, the control connection is used to send commands to the server and receive replies. Normally data connections are set up to the same IP address as that of the control connection, but in order to facilitate server-to-server file transfers it may be desirable to allow data connections to go to different IP addresses. If you are not using server-to-server transfers you can safely disable this option.
Quoted password changes	This determines whether the parameters of the SITE PSWD command are in quotes or simply surrounded by a space. (SITE PSWD oldpwd newpwd vs. SITE PSWD "oldpwd" "newpwd"). Which form is used depends on the targeted FTP client.

Anti-hammer filter

This feature is similar to ExpertAssist's IP address lockout settings. By default if 4 trials to establish more simultaneous data connections than it is allowed from an IP address occur within one minute, the IP address will be locked out for one hour. When the client IP gets locked out, the FTP client receives an error response 421 Connection rejected. Service available in 01:00:00 from the server.

Enabled	Select this box to enable the anti-hammer filter.
Number of invalid attempts before locking out	You can change the number of bad login attempts from 4 to anything you want.
Reset invalid attempt counter after	You can modify the time before the invalid attempt count is reset to zero.
Lock out for	You can choose the duration for which the user is locked out after the specified number of invalid attempts has been made.

Windows Users

You can connect to the newly defined FTP server with any FTP client, but you are not able to log in until you have created a new FTP user and give them access to the server or you can allow any Windows NT user to access the new virtual FTP server.

The difference between FTP users and NT users is simple. NT users are pre-existing users in the Windows local SAM user database and Active Directory. Creating and managing local users from SAM database is done either via the HTML-based User Manager included in ExpertAssist, or the User Accounts applet that comes with Windows. You cannot explicitly tell the FTP server the directories and files to which the user has access, but Windows access rights will be enforced. If a user can access a file below the server's root directory locally or over the network, he will be able to do so via FTP as well. If a user has no rights to a file or a directory, he will not be able to access the object with FTP either. This is enforced by the FTP server by having the thread servicing the user impersonate him towards the operating system as soon as login is complete.

FTP users, on the other hand, are created and managed within the FTP configuration pages. You can tell the server which files or folders the user can access, where he can read from, where he can write to. When an FTP user logs on, the thread servicing the user is executing under the LocalSystem account by default. This is rather undesirable, so you can specify an NT user account on a per-server basis that will be impersonated when servicing FTP users. We will return to FTP users later in this chapter, when discussing the content of the FTP Users tab.

The Windows account which the FTP users will impersonate under can be defined by specifying a username, domain and password for an existing Windows account using the corresponding fields on the Windows Users page. This is used when an FTP user logs on: the thread servicing the user will be impersonating this account towards the operating system. If you enter an incorrect username or an incorrect password here, the FTP user will receive a 'Login incorrect' message from the FTP server, even if he enters his credentials correctly.

To grant access to a Windows NT user or group on the FTP server, select its name in the list on the right and click the Apply button. To revoke access from a user or a group, select its name in the list on the left, and click the Apply button.

To list user accounts from a domain rather than from the local computer, enter the domain's name in the 'default domain' field and click the Apply button.

Now that you have granted access to an NT user, you can use an FTP client to connect and log in to the FTP server. The user will have access to all files and directories below the server's root directory. However, on an NTFS file system, NT access restrictions will apply. For example, if the user does not have the rights to read or write in a certain directory, he will not be able to do so via FTP either. The FTP server enforces this in a very effective way: the thread servicing the user will impersonate him towards the operating system as soon as login is successful.

Welcome

The Welcome configuration page allows you to view and modify the welcome message for your users:

The first message the user will see when they log in will be the ExpertAssist welcome banner. If you do not wish to let the outside world know which FTP server you are running, you can disable this via the checkbox at the bottom of this window.

The next message the user will see looks like this by default:

Welcome to the _!SERVER_NAME!_ FTP server,
running on _!OS_VERSION!_.
The server has been up for _!SERVER_UPTIME!_.
Data downloaded: _!BYTES_DOWN!_
Data uploaded: _!BYTES_UP!_
Sessions serviced: _!TOTAL_LOGINS!_

You can change this to anything you like, or leave it blank if you'd prefer no login message for your users. If you disable both the banner and the welcome note, the FTP Server will just send 'Welcome' whenever somebody connects to the FTP port. This is because the FTP specification requires a server to send a code and some text when a connection is established.

By default, the post-login message looks like this:

Welcome, _!USER_NAME!_, to _!SERVER_NAME!_.
Your last successful login was at _!LAST_LOGIN!_.
Good logins so far: _!GOOD_LOGINS!_.
Bad logins so far: _!BAD_LOGINS!_.
You have uploaded _!BYTES_UP!_ and downloaded
_!BYTES_DOWN!_ in your previous sessions.

User logged in.

The final line reading User logged in cannot be customized, as this is a requirement of FTP protocol. The rest you can change to suit your preferences, or leave blank.

The following variables can be inserted into the welcome messages, and they will be automatically replaced with their corresponding values:

_!SERVER_NAME!_

The name of the FTP server.

_!OS_VERSION!_

The operating system and its version.

_!SERVER_UPTIME!_

The amount of time the server has been up.

_!BYTES_UP!_ and _!BYTES_DOWN!_

The amount of data uploaded and downloaded. These variables behave differently when used in the pre-login or post-login messages. In the pre-login message, they represent a server-wide value, while in the post-login message they represent the amount of data transferred by the user.

_!TOTAL_LOGINS!_

The number of successful logins to the FTP server. Only valid in the pre-login message.

_!GOOD_LOGINS!_ and _!BAD_LOGINS!_

The number of logins and unsuccessful login attempts for the user logging in. Only valid in the post-login message.

_!LAST_LOGIN!_

The last successful login by the user. Only valid in the post-login message.

These welcome messages are server-wide settings, and apply to all users and groups. When you specify a welcome message for an FTP group or an FTP user, it will override the post-login message defined here.

ODBC

The ODBC option allows you to specify a database as a source of user information.

With this configuration page you can set up a database to contain user information. This can be any database type: Oracle, SQL Server, Microsoft Access, or even a plain text file. You need to create an ODBC data source

that refers to this database so that ExpertAssist can access it. The data source must be a so-called System Data Source, as this is the only ODBC source available to processes running in the system context.

NOTE: The data source should be of the System DSN type.

NOTE: On 64-bit Windows environments please use the Microsoft SQL system or SNAC drivers as these are the only ODBC providers available for System data sources.

When you have your database and ODBC data source ready, we advise you to test it by querying it with a tool that supports ODBC queries, such as a spreadsheet program or the Windows built-in ODBC Data Source Administrator tool.

NOTE: On 64-bit Windows please make sure to use the 64-bit ODBC Data Source Administrator tool. It is available under the %systemroot%\system32 folder.

You should have all user information available in one table. If you already have a user database and user information is in separate tables, you should set up a query within your database that contains all user-related fields. ExpertAssist only reads from the database.

Suppose that you have a user database in a data source called FTPUsers. The user information is present in a database table called Users. A database SQL login called ea is able to read from the Users table. You should also supply the password for this user.

ODBC Data source settings

Use ODBC

Set this checkbox to enable the use of ODBC.

Data source name

Enter the name of the System DNS created using the ODBC Data Source Administrator tool to be used as the data source.

Login name

Enter the User Name that is used to access the ODBC data source.

Password

Enter the Password that is used to access the ODBC data source.

Connect timeout

The amount of time to wait while establishing a connection before ending the connection attempt.

User information table name

Enter the name of the database table that the ODBC data source will use.

Column names for user properties

User name

Enter database table field (column) name storing the users' login names.

Password

Enter database table field (column) name storing the users' passwords.

Home Directory

Enter database table field (column) name storing the users' home directory path here. Users have full access to their home directory, but have neither read nor write permissions outside of it. The path can be an absolute path (such as z:\ftp\users\~john) or it can be relative to the server root (such as /users/~john).

Quota

Optional) The quota field will restrict user from storing more data in his home directory and its subdirectories than the number of bytes specified here.

Download/Upload Bandwidth

Optional) These fields restrict download/upload speed. They are optional, and should be an integer number specifying bytes per second.

Disabled

Optional) Enter database table field (column) name storing the user's status. Within the database this field should store an integer value. When the value is non-zero, the user is disabled and cannot log in.

Maximum number of simultaneous connections

Optional) Enter database table field (column) name that specifies the maximum simultaneous connections to this FTP server for a user.

Maximum number of simultaneous connections per IP address

Optional) Enter database table field (column) name that specifies the maximum number of simultaneous connections per unique IP address for a user.

Welcome Message

(*Optional*) Enter database table field (column) name storing a custom welcome message for the user.

FTP Users

If you click on the FTP Configuration page under the Server Functions object and select the FTP Users tab, you can view, create or modify your existing FTP users. These are only defined in ExpertAssist and unlike Windows NT users they do not exist outside of the FTP server.

As on the FTP Users tab, users are shown in a table, with a delete column to the right.

Below this is the New FTP user button.

New FTP User

To create a new FTP user, click on the **New FTP user** button on the **FTP Users** tab of the **FTP Configuration** page.

Enter the desired username and password on the Settings for FTP user page. You can also specify upload and download speed limits for the user. If not set to zero (meaning disabled) these options override the global FTP server settings.

You can also enable or disable their ability to change this password, and select an IP from the IP filter drop-down list.

Click **Apply** to create the user.

When you create a new user the following options become available:

Groups
Permissions
Ratio
Disable
Home/Quota
Max Connections
Welcome
Permissions Report

The newly created user cannot log in yet: you have to assign permissions to them for an FTP server and a path so that the user is able to use the account.

Groups

This configuration page lets you specify the FTP groups to which the user belongs. For more details on FTP groups, please see the next section.

Selecting a group that the user is a member of and clicking the **Apply** button will remove the user from that group. Selecting a group that the user is not a member of and clicking the **Apply** button will add the user to that group.

The Back button takes you back to the Settings for FTP user page.

Permissions

This configuration page lets you edit users' access rights to directories. To grant access to a directory on a server, select the virtual server from the server list, select the type of rights you wish to assign to the user, enter the path to the directory and click the **Apply** button.

The path you specify can be a full path, containing a drive letter, or a path relative to the server's root directory. If you assign rights to a path that is not within the server's root directory, the setting will have no effect at all.

The following rights are possible:

L – Show directory contents.
Allows the user to list the contents of the directory.

R – Read file.
Download files from the directory.

C – Create subdirectories.
Create new directories in the directory.

D – Delete/rename file.
Delete or rename a file or a directory. Also required to be able to overwrite files.

W – Create/modify file.
Create a new file and/or write data to it.

Full access.
All of the above.

The rights you specify for a directory are automatically inherited by its subdirectories, unless you specify different rights for them.

The following method is used when checking access rights to a directory:

The current virtual server's access list is enumerated for the current user.

When the directory closest to the directory in question is found, the access rights specified for that directory is used. For example, if the user has LRW rights for C:\Work, he has LR rights for C:\Work\CPP, and the directory in question is C:\Work\CPP\Project1, only LR rights are returned – meaning that the user can only list and read files, but not write to them.

If an NT user is specified on the Windows Users configuration page for the server to run FTP accounts under, further Windows NT-enforced restrictions might apply, based on file system permissions. This configuration page is available from the Settings for FTP server page.

You can also make the user member of one or more groups, and these groups can also be members of one or more groups. For an explanation of this scenario, please see the FTP Groups section.

Ratio

This configuration page lets you edit the upload/download ratio settings for users. The upload/download ratio lets you control how much data the user has to upload before he can download anything.

If the Upload ratio is set to 1, and the Download ratio is set to 5, the user can download 5 bytes for every byte uploaded. If it were the other way around, the user would have to upload 5 bytes to be able to download one. You can enter any positive integer number in either of these fields.

There are four possible settings for the Ratio type:

1. None. The user is a normal user, and can download any file he has read access to, without having to upload first.
2. Per session. When the user logs in, his counters are zeroed. Should he lose connection while uploading or downloading, any remaining credits he has will be lost.
3. Per user. The user's credits are remembered over sessions. It is not recommended if you want several users to share the same account.
4. Per IP address. Even if the user loses connection, his credits are remembered, if he logs in again from the same IP address. This does not cause a problem, even if the user account is shared by hundreds of concurrent users.

The Per IP ratio expiration time setting allows you to expire the per-IP credits after a certain amount of time. If the user logs back from the same IP address after not visiting the server for this much time, he will have to start over building up his credits.

The ratio setting applies to all virtual FTP servers.

To let the user download files without uploading, you can specify a starting credit. The amount given is in kilobytes – the user will be able to download the specified amount of data without uploading.

Disable

The following configuration page lets you explicitly disable (or ban) a user on a virtual FTP server. Disabled users cannot log in, even if they have rights on an FTP server. You can also disable a connected user from the FTP status page.

Home/Quota

This configuration page lets you specify home directories for the user. A home directory is basically the entry point for a user on an FTP server. When the user logs in, he will find himself in the directory you specify here. If no home directory is specified, he will be logged in to the server's root directory. The user can move out from his home directory if he has rights to an outside directory. You can use a full path, starting with a drive letter, when specifying home directories – or you can enter a relative path to the server's root directory.

You should make sure that the user has rights to his entry point on the server – either to his home directory, or if the home directory is not specified, to the root directory of the server. If the user has no rights to the entry point,

he will not be able to log in. If the user's home directory is specified above the server's root, the user will not be able to log in.

You can specify quotas for your users. Quotas are only enforced on home directories, and apply to all files contained in the home directory and its subdirectories. If a user has rights to upload files outside of his home directory, he will be able to do so without restrictions – quotas only apply to the home directory and its contents.

The ExpertAssist can help to enforce disk quotas for user accounts. When a user starts to upload a file, the FTP server quickly scans the contents of the directory to determine if the user is below or above the quota. If the quota is not exceeded, the upload can be started – however, the FTP server will interrupt the transfer as soon as the file being uploaded starts to exceed the specified quota.

Home directory quotas are entirely optional, by leaving the field empty you choose not to limit the amount of data that can be stored on the server by the user.

Maximum Connections

You can specify the maximum number of simultaneous connections for a user account on this configuration page. By default, a user account can be used to log in any number of times, until exhausting the maximum number of connections for the virtual FTP server, or exhausting the resources of the computer.

Simply select the server on the right, enter the number of maximum simultaneous connections in the **Count** field and click the **Apply** button.

To remove a limitation, select it in the list on the left and click the **Apply** button.

You can also limit the number of simultaneous connections to be established by the user from a single IP address. The Per IP field serves this purpose. When left blank, or a zero is entered, this limitation is disabled and the user can establish that many connections as defined in the Count field. If you enter a numeric value, a single computer can be used to log in that many times with the account.

It is a good idea to limit certain user accounts (for example the Anonymous account) this way. An overall maximum connection limit defined in the Count field ensures that the server cannot be overloaded by thousands of Anonymous users, and a Per IP limitation makes sure that no single user can take up all available connections.

Welcome

You can compose a custom welcome message for the user in this window.

Welcome, _!USER_NAME!_, to _!SERVER_NAME!_.
Your last successful login was at _!LAST_LOGIN!_.
Good logins so far: _!GOOD_LOGINS!_.
Bad logins so far: _!BAD_LOGINS!_.
You have uploaded _!BYTES_UP!_ and downloaded
_!BYTES_DOWN!_ in your previous sessions.
!QUOTA!

Messages specified here override any post-login message specified for the virtual FTP server. In this case, messages specified for any groups the user belongs to will be disregarded as well. See the equivalent section on welcome messages above for the available variables.

Permissions Report

The permissions report can be retrieved for any FTP user. It will list all FTP servers, and all the rights a user has on the given server.

This report can be useful if you have a more complicated setup of groups and users, and would like to see what exactly the user can do on the system, and from where these rights come.

FTP Groups

If you click on the **FTP Groups** tab on the **FTP Configuration** page under the **Server Functions** object, you can easily control the resources available to your FTP users. As on the FTP Servers and FTP Users tabs, groups are shown in a table, with a Delete column to the right.

To add a new FTP Group click on **New FTP group**.

General Group Settings

You can make a group a member of another group, thus bringing in any permissions or restrictions for its member users from the parent group.

Selecting a group in the Member of list and clicking the Apply button will remove it from that group. Selecting a group in the Not member of list and clicking the Apply button will add the group to it.

You can also specify a welcome message for a group. Whenever a member logs in, he will see this message instead of the server's general welcome message.

Permissions

With this configuration page you can specify the rights to servers and directories.

The configuration page works very much like the Permissions configuration page within the FTP Users tab. For a basic description please see the appropriate section of this document.

There are some scenarios, however, that might require further explanation.

Suppose the following, rather complicated scenario:

- User1 is member of Group1.
- Group1 is member of Group2 and Group3. In the Member of list for the Group1, Group2 is shown first and Group3 is shown second.
- User1 is granted LR access to C:\, and LRW access to C:\Work.
- Group1 is granted full access to C:\, LR access to C:\Work, and LRWD access to C:\Work\CPP.
- Group2 is granted LR access to C:\Work\CPP and full access to C:\Work\CPP\Project1
- Group3 is granted LR access to C:\Work\CPP\Project1

So, what exactly User1 can do in the aforementioned directories?

- C:\

He has LR rights. He was explicitly granted LR rights to this directory, and this overrides anything else.

- C:\TEMP

He has LR rights. He was explicitly granted LR rights to the directory closest to this one (C:\), and no groups that he is a member of, directly or indirectly, specify anything else for the C:\TEMP directory.

- C:\Work

LRW rights again. See the first case.

- C:\Work\CPP

LRWD, because Group1 has LRWD rights. Even though Group2, which Group1 is a member of, specifies LR access for this directory, Group1 is the least indirect object that specifies actual rights for the directory. Group2 is one more indirection away, with User1 only being a member of it because he is a member of Group1, and is therefore overridden by Group1.

- C:\Work\CPP\Project1

Full access. Both Group2 and Group3 are two indirections away, they both specify access rights to the same directory, so the deciding factor between Group2 and Group3 is that Group2 is the first one in the Member of list of the Group1.

FTP Status

When you click on **FTP Status** under **Server Functions**, you can view the current status of each of your virtual FTP servers consolidated into a table.

For each server, it provides a listing of all current connections and their current activity. The fields in the list are:

Icon

This field shows a small icon, representing the current status of the connection. A green checkmark indicates a ready, or idle connection. An hourglass indicates a connection currently in the process of logging in or becoming ready. An up or down arrow indicates uploading or downloading.

User name

The name of the user associated with the connection. For NT users, it is in an AUTHORITY\ACCOUNT form. For FTP users, it's simply the username. For connections not yet logged in, it's N/A.

Control IP

The IP address of the FTP control connection. This is where commands from FTP client to virtual FTP server are sent from.

Downloaded

Bytes downloaded during this connection.

Uploaded

Bytes uploaded during this connection.

Data IP

The IP address of the FTP data connection, if applicable. This is where data is sent via from or to.

Path

The path and name of the file currently being uploaded or downloaded, if any.

Speed

The speed of the upload or download process.

Bytes left

The amount of data left from the transfer operation. Only applies to download transfers, since the FTP protocol does not let the server know the size of the file being uploaded in advance.

Est. time left

The estimated time remaining from the transfer operation. Only applies to download transfers, for the same reason as the previous item.

Kick

This button kicks the user out – in other words, terminates the connection.

Ban

This button kicks and then bans the user from the FTP server. Only applies to FTP users, and not to NT users. The Disabled configuration page for the banned user will show him as disabled on the server he was banned from.

Ban user IP

This option first kicks the user from the server in question, then adds an IP filtering rule to the IP Filtering page under the Security object and sets the created rule to the IP filter drop-down list on the Settings for FTP user for the banned user. That will prevent him from logging in again from the IP address in question. He will have the ability to log in from other IP addresses (depending on IP filtering setup) and the IP address will only be disabled for this user.

Ban server IP

This button kicks the user, then adds an IP filtering rule to the IP Filtering page under the Security object and sets the created rule to the IP filter drop-down list on the Settings for FTP server for the banned server. That will cause the server not to accept connections from the IP address in question at all. No matter which user is logging onto the FTP server from the banned IP. The user will be able to log in from other IP addresses.

Anti-hammering

Information for each server is also shown, where applicable. It is in the following format:

IP address

The address the attempted connection came from.

Expires at

The time when the information will be discarded – users will be able to establish connections from the IP address at this time again.

Delete

Clicking this button will remove the anti-hammering information from the FTP server's memory, thus making the IP address available for logins, had it been locked out.

The Refresh button refreshes the contents of the screen to reflect any changes, while the Back button goes back to the main FTP settings screen.

FTP Statistics

If you click on **FTP Statistics** under **Server Functions**, in the table you can view per-server and per-user statistics, such as the last login, number of logins, bytes sent and received, etc.

The red button Delete button in the Reset table column will reset or delete statistics kept on that object.

Port Forwarding Config

ExpertAssist also comes with Port Forwarding Server. This allows you to forward one or more TCP ports on one computer to another so that separate networks can be bridged.

Before getting into the details of how you would configure your Port Forwarding Server (PFS) we will look at how it works. Picture the following scenario:

You have a Local Area Network (LAN), connected to the Internet with a firewall / proxy server. The computers on the LAN all have non-Internet IP addresses, and they connect to the outside world via the proxy server.

If you have ExpertAssist installed on any computer on the LAN — say, the fileserver — you would be able to access it from within the LAN without any problems. However, it is not accessible from the Internet.

If you set up ExpertAssist and PFS on the firewall, so that a certain port (say, 3000) on the firewall is forwarded to the fileserver's IP address and ExpertAssist port (2000 by default), accessing port 3000 on the firewall will let you access ExpertAssist on the fileserver. Both from within the LAN and from the outside as well.

When you click on the Port Forwarding Config page under the Server Functions object in the tree you can set up the above scenario. In order to look at the interface for this feature we will look at some more possible scenarios.

Imagine, for example, the following situation:

The firewall's Internet IP address is 145.236.120.227
The firewall's LAN IP address is 192.168.0.2
The fileserver's LAN IP address is 192.168.0.10. ExpertAssist is installed on both computers, and is listening on port 2000.
The IP addresses used in the foregoing are for demonstration purposes only.

What we need to do is simple: map port 3000 on the firewall computer to port 2000 on the fileserver. Having called up the Port Forwarding Config page from the tree you can now add a new rule by clicking the Create forwarding rule button.

The Protocol drop-down list in the In group should have TCP selected in it. Other protocols (SSL, CSSL) will be discussed later. The IP Address drop-down list in the In group can be set to an * (asterisk) meaning that the port will be forwarded from all IP addresses of the firewall. If you want to use a single IP address instead of all assigned ones, select it here. The Port edit box in the Incoming group can be anything not already in use on the computer – in our case it is 3000.

The Protocol drop-down list in the Out group should have TCP selected in it. The IP Address edit box in the Out group will be 192.168.0.10 (or the actual DNS address of the host), and the Port edit box will be 2000. The Defer and the Timeout values can be left to their defaults. These will be explained later.

The Description field lets you specify a remark associated with the port forwarding item. This will be displayed in the table on the Port Forwarding Config page.

If you fill out the dialog and click the **Apply** button, the item will be listed on the Port Forwarding Config page.

That's really all there is to it. Your first port forwarding item has now been configured.

Advanced Options

You can edit a port forwarding item by double clicking it, or by selecting on it and clicking on the Modify Rule button.

You can specify IP address restrictions for the item from the IP address filter profile drop-down list. This works exactly like the Quest ExpertAssist IP Filtering feature, only it restricts incoming connections to the corresponding port forwarding item only. For more information, please read the documentation on IP Filtering.

Timeout

This setting lets you specify how long the PFS will hold a connection open with no data going through it in either direction. When the amount of time specified here is reached and the connection is idle, both ends of the connection will be closed gracefully.

Defer

This setting lets you specify a timeout value for a special condition. When one end of the connection has been closed, but the other is still open, PFS will wait this much time for the open end of the connection to be closed. It will then close the connection itself.

Protocol (In and Out)

These fields let you specify SSL or CSSL as well as TCP. To translate SSL connections to TCP or TCP to SSL, and thus behave as an SSL proxy for applications that are not SSL-enabled, simply set one end to SSL and the other end to TCP.

There are situations when SSL encryption would be a very nice thing to have, but neither the client nor the server support it. In this case, you can use two installations of Quest ExpertAssist: one to translate the connection from TCP to SSL, the other to translate it back from SSL to TCP.

Let's suppose that you are using a laptop with a dialup account, and your email software does not support SSL. Let's also suppose that your corporate mail server does not support SSL either. If you still want to keep your email secure, you can install Quest ExpertAssist both on your laptop and on the email server, and set up a port forwarding item on both computers.

On your laptop, you would need to do the following:

- Create a port forwarding item with the incoming IP address as 127.0.0.1 (the loopback address), the incoming port as 3110, the incoming protocol is TCP. The outgoing IP address or host name would be set to that of your email server, the outgoing port would be set to 3110, and the outgoing protocol would be SSL.
- Change your email client's preferences so that the POP3 server is 127.0.0.1 and the port is 3110.

On the mail server, you would need to only create one port forwarding item, with the incoming IP address set to your mail server's Internet IP address, the incoming port would be 3110, and the incoming protocol would be SSL. The outgoing IP address would be the same (the mail server's Internet IP address), the outgoing port would be 110 (the standard POP3 port), and the outgoing protocol would be set to TCP.

If you performed the above three steps, starting up your email client and checking for mail would actually go through two port forwarding servers; the first one being on your own computer, encrypting all data before it's sent to the mail server. The mail server's port forwarding server would receive the encrypted data, and decrypt it before sending it on to the actual mail server software. Data flowing in the other direction would be also seamlessly encrypted and decrypted.

However, if you have two Quest ExpertAssist Port Forwarding Servers talking to each other, you could also utilize the proprietary CSSL protocol instead of using plain SSL. CSSL, which stands for Compressed SSL, would also seamlessly compress and decompress your data as well as encrypt and decrypt it - to keep to the above example, making your mail arrive much faster over a dialup connection. (And also, to properly finish the laptop/email example, you would also have to create one additional port forwarding item on both computers for the SMTP protocol that is used to send email as opposed to receiving it. This runs on port 25 by default.)

Click the **Export** button to download a CSV file containing the list of custom port forwarding rules to your local computer.

Port Forwarding Status

If you have configured your Port Forwarding Server as in the examples above, you will be able to view the status of your Port Forwarding connections by clicking on Port Forwarding Status page under Server Functions object in the tree.

Click the Export button to download a CSV file containing detailed information about port forwarding operations for each of the port forwarding rules created on the Port Forwarding Config page.

Active Directory

This page allows the browsing of the Active Directory nodes using LDAP.

Scheduling and Alerts

Under Scheduling & Alerts, you can make use of ExpertAssist's scripting capabilities, as well as set up a service to send you email alerts when certain events occur on the remote machine.

This powerful feature of the ExpertAssist enables you to monitor the system based on the performance data collected.

You can also define conditions, and actions to be performed. A condition and an associated action are known as a rule.

System Monitoring

Use the System Monitoring page under Scheduling & Alerts object in the tree to make changes and create new rules.

A rule has the following structure:

```
<rule name> (delay)
{ <condition> { <action1> } else { <action2> } }
```

The action can consist of several statements – they have to be separated with a semicolon.

Such as:

```
MemUsageAboveFor(70%, 20m)
  {
  SendMail("administrator@company.com","Memory usage on [MACHINE]","High memory
utilization!\n" "(Max: [MAX_USAGE])");
  SendMessage("administrator","High memory utilization on [MACHINE]!\n" "(Max:
[MAX_USAGE])");
  }
```

You can enable or disable certain rules right on the System Monitoring page.

The **Edit rules** button lets you edit the monitoring rules in your browser.

For example:

```
"Check Memory Usage" (10m)
{
MemUsageAboveFor(70%, 20m)
 {
 SendMail("administrator@company.com","Memory usage on [MACHINE]","High memory
utilization!\n""(Max: [MAX_USAGE])");
 }
else
 {
 SendMail("administrator@company.com","Memory usage back to normal","See topic.");
```

```
  }
}
```

The above rule executes every 10 minutes (delay), and checks the condition MemUsageAboveFor. In the above scenario, if the memory utilization is above 70% for 20 minutes or more, the condition becomes true, and action1 is executed.

The action, in this case, will send an email to administrator@company.com describing what has happened. The rule will keep checking the condition every 10 minutes after the condition has become true. If it's still true, it does nothing – but if it becomes false (that is, the emergency situation is resolved) it executes action2. In that case, ExpertAssist will email the administrator to let him know that the problem has been resolved.

NOTE: There is one special rule that can – and should – be defined: it's called ERROR. If something goes wrong while performing actions – for example, when the user Administrator is not logged on and the above actions are executed, SendMessage will fail – ERROR is executed, allowing you to customize error-handling behavior.

NOTE: You can use any of the built-in and/or custom written PowerShell scripts in your monitoring scripts to implement a PowerShell-based customized auditing and background monitoring actions.

The monitoring script runs like a trigger. If it invokes the PowerShell script, it first initializes the $POWERSHELL_RES variable to 0. This state is then handled as the 'previous state'. Then the ExpertAssist monitoring script engine compares this state to the state known as the 'current state' that is set when execution of the PowerShell script is finished. If executing the PowerShell script changes the state and the current state is different to the previous state, monitoring script triggers and executes the branch depending on the trigger value. The trigger in this case is the value of the $POWERSHELL_RES variable. If executing the PowerShell script returned the $POWERSHELL_RES variable set to 1, the monitoring script condition (main script branch) is executed following the monitoring script function declaration. If executing the PowerShell script returned the $POWERSHELL_RES variable set to 1, the monitoring script ELSE condition (else script branch) is executed. Thus, if the previous state has the $POWERSHELL_RES of 0 and executing the script returned the $POWERSHELL_RES set to 0, monitoring script will not trigger. If executing the script returned $POWERSHELL_RES set to 1, it indicates a trigger and the main script branch is executed since the variable value is 1. The table below shows the value of the $POWERSHELL_RES variable on a particular state and the script branch that will be executed within the monitoring script.

Table 4: The $POWERSHELL_RES variable.

Previous State	Current State	What is Executed
0	0	The states do not differ. Nothing is executed. Waiting for a trigger during the script execution delay.
Not a 0	Not a 0	The states do not differ. Nothing is executed. Waiting for a trigger during the script execution delay.
0	Not a 0	Tigger. Current state has changed and the $POWERSHELL_RES has been set to some value that is not a zero. Executing the main script branch.
Not a 0	0	Tigger. Current state has changed and the $POWERSHELL_RES has been set to zero. Executing the else script branch.

Email Alerts

When log entries matching a certain criteria are entered into any of the event logs you can have ExpertAssist send you email alerts to an email address of your choice.

Email alerts will not work until you configure your SMTP server under Preferences > Network.

Once you've set that up, you can configure email alerts according to the following criteria:

Enabled

Enables/Disables the event alert

Event Log Name

The event log to watch.

Event Type

Can be Error, Warning, Error & Warning, Information, Audit Success, Audit Failure, or All types.

Event Source

Type in the source of the message you want to be alerted on. For example, Security, Disk, etc. This field is optional.

Event Category

Type in the category of the message as it would appear in the event log. This field is optional.

Event ID

Type in the event code as it would appear in the event log. This field is optional.

Email

The email address the notifications are sent out to. You can only specify a single email address per entry, so if you want several people to receive these messages you should specify a group alias here.

Task Scheduler

The Task Scheduler gives you a simple interface to NT's Scheduler. In order to be able to view, add and delete tasks, the Schedule service must also be running.

On the main page, you can see a list of all currently scheduled tasks. The table shows you the following:

- The name of the task;
- The command to be executed;
- The time of the day the command is to be run;
- Whether the last run of the job ended successfully.

To remove a task from the list:

Select it and click on the **Delete** button in the toolbar.

To add a new scheduled task:

Click on the **Create new task** button.

To view/modify the attributes of your existing tasks:

1. Double click a task. The page with task attributes will open.
   Or,
   Use the Change attributes button in the toolbar.
2. Use the attributes organized under three tabs, with the headings Task, Settings and Schedule.

To download a CSV file containing the currently displayed table of scheduled tasks available on the remote computer:

Click the **Export** button.

Scripts

> **NOTE:** All scripts require you have PowerShell 1.x command line shell installed on the remote computer. You may download the installation package for your version of Windows on the manufacturer's site at http://microsoft.com/powershell.

This page in ExpertAssist provides an extension interface in which you can create custom PowerShell scripts that interact with the remote system, ExpertAssist and the remote user.

ExpertAssist comes shipped with a set of scripts that allow you to perform some typical administrative tasks on the remote computer. You may use them as a basis for your custom scripts, or you may create your own scripts from scratch as well.

Table 5: Pre-defined scripts description.

Script	Description
CheckCDrive	Checks and lists a free space left on C drive on a remote computer
dainclude	Include file. Contains supplementary methods used in interactive scripts to output data back from a remote computer to the ExpertAssist page on the local computer.
Email	Sends a message via a defined mail relay and outputs back the result into the ExpertAssist page
File	Gets a hexadecimal dump of the file specified and outputs it back to the ExpertAssist page
Ping	Pings the remote computer where ExpertAssist is running on
Processes	Queries the remote computer processes and their properties. Outputs collected info arranged into a table back to the ExpertAssist page.
Services	Queries the remote computer services and drivers, and their properties. Outputs collected info arranged into a table back to the ExpertAssist page.
WatchProcess	Watches the state of the specified process and notifies you if it's not running.

There are three kinds of scripts you can create:

- Interactive
- Quiet
- Hybrid

Interactive scripts display their output on HTML pages, returning script output back to your right within the ExpertAssist's Scripts page. An example for an interactive script is the `File.ps1` script, which is installed with ExpertAssist. These scripts do not have to return a value from their main function. They communicate with the user via the htmlBeginOutptut(), htmlEndOutput().

> **NOTE:** You can locate this and other built-in PowerShell scripts (*.ps1) within the ExpertAssist program folder on the remote computer.

A **Quiet** script is one that is usually called from the System Monitoring script. It does not display output. A return value is required at the end of the main function.

A skeleton example for a Quiet script is here:

```
& {$POWERSHELL_RES = 1;}
```

This script does not do anything useful. It simply sets the $POWERSHELL_RES variable to 1, meaning that a problem has occurred.

By default, PowerShell is initialized with the $POWERSHELL_RES variable set to 0. When using PowerShell scripts in monitoring scripting, setting $POWERSHELL_RES to something other than 0 allows the ExpertAssist to automatically execute the action followed by the monitoring script function declaration.

In the example above setting the $POWERSHELL_RES variable to 1 will indicate to the ExpertAssist built-in monitoring script compiler that the PowerShell interpreter has failed executing the script. This enables the monitoring script compiler invoking the PowerShell script to trigger and execute the 'else' branch of the monitoring script.

Hybrid scripts, on the other hand, are executable interactively and also return a value at the end of their main function. Hybrid scripts check the return value of the htmlBeginOutput() function, and if it's a zero value, the script is run in non-interactive mode.

These PowerShell scripts can be invoked from the System Monitoring scripts via the PowerShell() function call. This function takes the name of the PowerShell script name you want to invoke for monitoring as an input parameter. For example, if you want to regularly send notifications to your inbox, you can invoke the Email script written in PowerShell right from the monitoring script. This can be done by passing the PowerShell script name to the PowerShell() function:

```
PowerShell(Email)
```

See the MonitoringScript.txt file in the ExpertAssist program folder for an example.

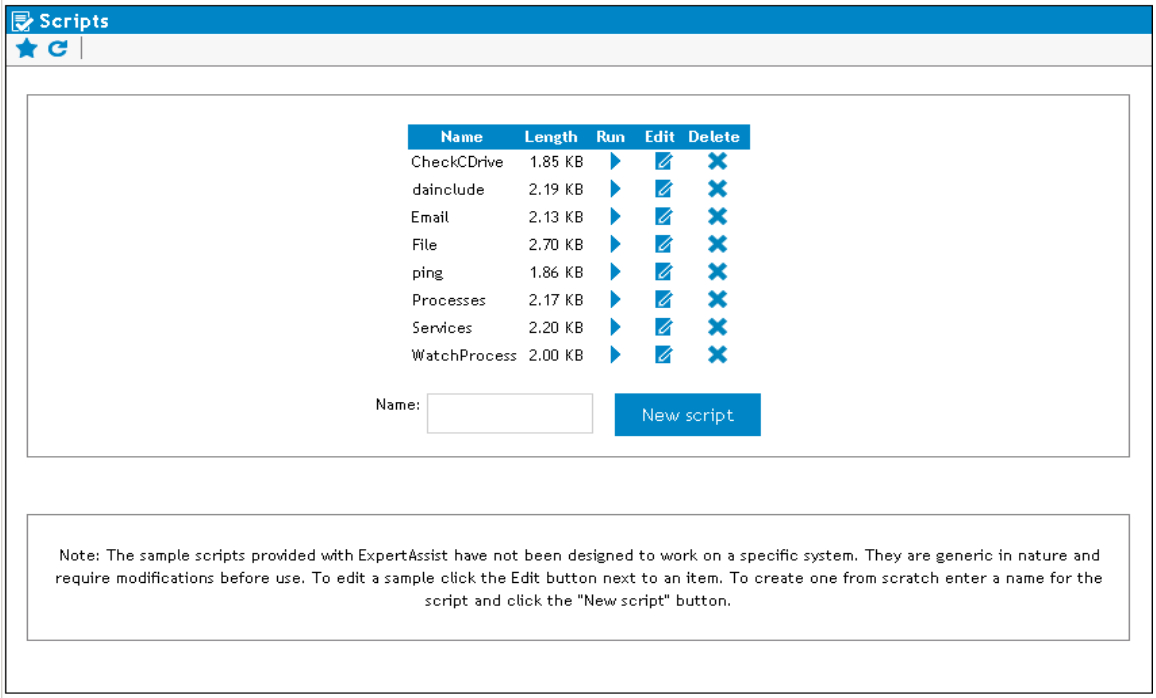
> **NOTE:** The Small() call can be used as an alias for the PowerShell() function. This function has been left for compatibility to allow you to re-use your monitoring scripts without having to rewrite them for the new PowerShell scripts.

For the PowerShell scripting language reference, please see the Owner's Manual available for downloading at http://www.microsoft.com/technet/scriptcenter/topics/winpsh/manual/default.mspx.

To run a script:

Click the script's Run icon to execute it immediately. ExpertAssist will show the notification message on the Scripting page during the script runtime to indicate that the script is being executed on the remote computer.

Figure 14: The script is being executed.



The Length column shows the size of the PowerShell script.

To edit and save changes made to the PowerShell source code of the script:

1. Click the **Edit** button in the Edit column in the row for a particular script.
2. When opened, make changes to your script just as you do it within the PowerShell ISE / shell.
3. Click **Save** to commit changes. Or click **Cancel** to discard changes made to the script during editing and return back to the script list page.

The **Delete** command removes the script. Confirm script deletion by clicking OK in the message box or click Cancel to skip deleting the script.

Deleting the script will permanently delete the script *.ps1 file from the remote computer!

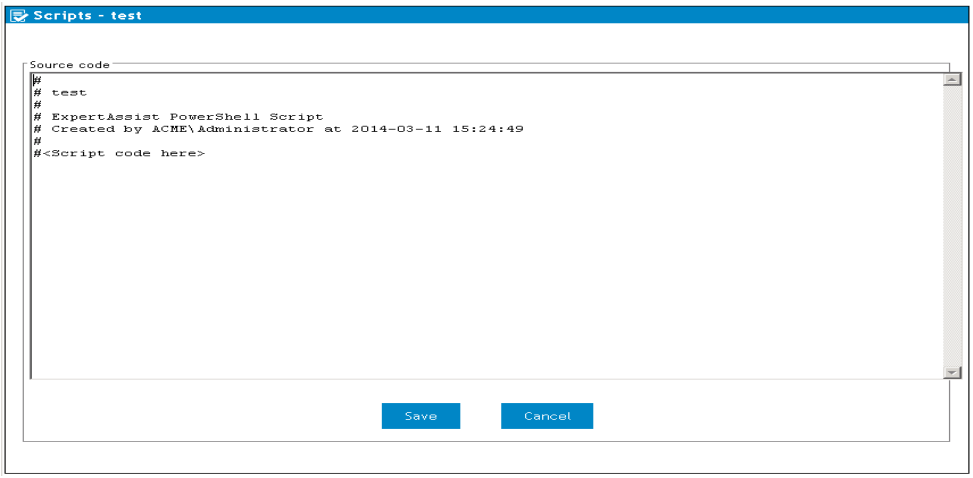
To create a new script, enter its desired name in the Name field and click the New script button.

Script creation example

Suppose, you want to create a script that will check to see the printer drivers available on the remote computer to help you troubleshoot printing errors. Of course, you would like to have this script output the results back to you elegantly wrapped in a table.

1. In the **Name** field type something like Get-PrinterDrivers.
2. Click the **New script** button, and ExpertAssist will automatically open the new blank script file for you.

Figure 15: The new blank script file.



> **NOTE:** It is recommended that you use PowerShell naming convention when defining cmdlet verb names http://msdn.microsoft.com/en-us/library/ms714428.aspx. Please make sure to not use spaces for script names. You can use spaces in commentary headers within the scripts though.

The time stamp is given in the UTC.

3. Put the cursor at the beginning of the #<Script code here> line, press Shift+End and start typing the script. Since we want to create an interactive script, we want ExpertAssist to automatically wrap the output into a table. To do that, we need to load ExpertAssist built-in functions preparing formatted output into the runtime. This is done by declaring the dainclude.ps1 file:

```
. .\dainclude
```

> **NOTE:** Make sure to have two dots and space between (. .) before the backslash (\). You may use slash (/) as well.

4. Next, we want the output table to have its title. The dainclude file contains the function htmlBeginOutput that indicates the start of the output data and creates the title. Let us name it according to the script name.

```
htmlBeginOutput -title "Printer Drivers";
```

5. Following this line we want to prepare table columns. To query printer drivers on the remote compute we will use the Win32_PrinterDriver WMI class. We have to open MSDN or use the Get-Member cmdlet to retrieve the class properties. When done, we can select ones that fit our needs. For out test purposes, let's select the following ones:

```
Name

Driver Path

Configuration File

Data File

Dependent Files

Help File

Supported Platform
```

To prepare the columns, we invoke the htmlBeginTable function and pass the properties that we want to check on the remote computer.

```
htmlBeginTable "Name" "Driver Path" "Configuration File"`

"Data File" "Dependent Files" "Help File" "Supported Platform";
```

> **NOTE:** You can use the backtick (`) to denote escape sequence and indicate line continuation. Please see Get-Help about_escape_character for more information.

6. Once we formed the table header, we can start to retrieve the data from the WMI. TO work with WMI we will use the Get-WMIObject cmdlet or its GWMI alias. Since the querying the Win32_PrinterDriver class returns an array, we will need to walk though it to select each of the desired properties passing the output to the ForEach-Object cmdlet via the pipe (|). Type the following on a new line:

```
Gwmi Win32_PrinterDriver | ForEach-Object {
```

7. Now we need to form the table row. To do that, type:

```
write-host "<tr>"
```

8. This is where we start to feed the table row with data using the <td> tag and selecting the properties found in the Win32_PrinterDriver class. Add the following line by line:

```
write-host "<td>" $_.Name "</td>"

write-host "<td>" $_.DriverPath"</td>"

write-host "<td>" $_.ConfigFile "</td>"

write-host "<td>" $_.DataFile "</td>"

write-host "<td>" $_.DependentFiles "</td>"

write-host "<td>" $_.HelpFile"</td>"

write-host "<td>" $_.SupportedPlatform"</td>"
```

9. Once all the properties are selected, we have to close the row and end the loop by adding a line:

```
write-host "</tr>"

}
```

10. That is almost it and we are a couple of lines before finishing. All is left to do is to finish the table by invoking the htmlEndTable function (which is available in the dainclude.ps1) and terminate the output using the htmlEndOutput:

```
htmlEndTable

htmlEndOutput
```

If we sum up, we will get this script:

```
#

# Printer Drivers

#

# ExpertAssist PowerShell Script

# Created by PM\Gluon at 2009-06-10 18:33:54

#

. .\dainclude


htmlBeginOutput -title "Printer Drivers";

htmlBeginTable "Name" "Driver Path" "Configuration File" "Data File" "Dependent
Files" "Help File" "Supported Platform";


Gwmi Win32_PrinterDriver | ForEach-Object {

    write-host "<tr>"

    write-host "<td>" $_.Name "</td>"

    write-host "<td>" $_.DriverPath"</td>"

    write-host "<td>" $_.ConfigFile "</td>"

    write-host "<td>" $_.DataFile "</td>"

    write-host "<td>" $_.DependentFiles "</td>"

    write-host "<td>" $_.HelpFile"</td>"

    write-host "<td>" $_.SupportedPlatform"</td>"

    write-host "</tr>"

}


htmlEndTable

htmlEndOutput
```

11. Click the **Save** button to create the script.

12. Locate the newly created script in the script table on the Scripts page and click the Printer Drivers script name for ExpertAssist to execute it.
13. When finished, ExpertAssist will return a neat table listing all the printer drivers found on the remote computer and their details.

Performance Monitoring

The pages under Performance Monitoring allow you access to the performance data collected by ExpertAssist. Descriptions for each of the pages can be found below.

CPU Load

This page has a number of graphs and a table.

The graphs show CPU utilization with various sampling rates.

Please note that ExpertAssist needs time to gather performance data for these graphs. If you have just installed the software, it is likely that only the right-hand side of the first graph will show you meaningful information.

If you have multiple CPUs in your computer, you will see separate graphs for each one, as well as a set of graphs showing you the total CPU load.

The sampling rate for the first graph is 2 seconds, so the graph spans less than an hour. This is useful to see what's happening right now on the machine. If you move your mouse over a line in one of the graphs, the tooltip that pops up tells you exactly when the sample was taken..

The Most CPU-Intensive Processes table at the bottom shows the processes that take up most of the processor time. This table is weighted, so younger processes that take up a lot of processing time come closer to the top. Processing time is counted like PROCESSOR_SECONDS divided by PROCESS_AGE_SECONDS. Thus, it shows how much the current process has consumed from the overall CPU time. So, if you see a sudden spike on the graph you can check the table and immediately find out which process is eating up processor time.

Clicking on an item in the ID column will display the relevant data on that process, organized under seven separate tabs (General, Windows, Threads, Services hosted, DLLs, Open Files, and Registry Keys In Use).

Memory Load

This option will present you with four graphs similar to those on the CPU Load page. These display the memory utilization on the machine.

Disk Space

Graphs displaying the disk space utilization per logical disk are available under this menu item. You also can observe the total disc space utilization on the remote computer.

Drive & Partition Info

This page displays all physical drives in the remote computer and their partition tables. This data is organized onto two separate tabs for Physical Drives and Partitions, and Logical Drives.

To download a CSV file containing the currently displayed drive and partition layout table

When on the Physical Drives and Partitions tab, click the **Export** button .

Open TCP/IP Ports

This option will present you with a listing of all open IP endpoints on the computer.

You can specify the following settings:

- Whether you'd like to see the ports that are listening for connections, ports that have been connected to another computer, and ports in various stages of being connected and disconnected.
- Have ExpertAssist resolve IP addresses appearing in the list of hostnames.

NOTE: Resolving IP addresses can take a considerable amount of time.

Network

The data displayed under Network is organized under two configuration pages, Inbound Network Traffic and Outbound Network Traffic.

NOTE: ExpertAssist needs time to gather performance data for these graphs. If you have just installed the software, it is likely that only the right-hand side of the first graph will show you meaningful information.

Use the section as described below:

1. Clicking each configuration page button, Inbound/Outbound Network Traffic, takes you to a page with a number of graphs.
2. The graphs show network traffic at various sampling rates.
3. The sampling rate for the first graph is 2 seconds, so the graph spans less than an hour.
4. This is useful to see what's happening right now. If you move your mouse over a line in one of the graphs, the tooltip that pops up tells you exactly when the sample was taken.
5. Other graphs plot the Network Traffic with sampling rates of 10 seconds, 5 minutes, and 1 hour.

PCI Information

If you click on PCI Information you can view all devices connected to the PCI bus or buses in the system.

Open Files

This option will show a listing of all files currently open on the remote computer, along with the names of the processes using them.

The processes list is clickable, so you can view data on the processes, and if necessary, kill them.

Registry Keys in Use

Under Registry Keys in Use you can view a list of all registry keys currently open on the remote computer. As with open files, you can also see the names of the processes that use them.

The processes list is clickable, so you can view data on the processes, and if necessary, kill them.

DLLs in Use

Here you can view a listing of all currently loaded dynamic link libraries and the processes that use them.

The processes list is clickable, so you can view data on the processes, and if necessary, kill them.

EA Connections

Selecting this page will display all current connections currently being served by ExpertAssist. It will display the IP address and host name of the remote computer, the type of connection and the name of the Windows user associated with the connection.

The connection type can be one of the following:

ExpertAssist Desktop Icon

Connections opened by ExpertAssist's icon in the notification area.

Browser (HTTP)

A typical browser connection requesting a page.

Remote Control

A Java remote control client.

File Transfer

Connection performed via File Manager applet

EAtelnet

Connections opened by ExpertAssist built-in telnet client available via the Command Prompt page under the Computer Management object.

Performance Viewer

The Java applet above the menu, displaying CPU and memory utilization.

Session Monitor

Connection established by Session Monitor that shows management sessions.

Telnet

Connections to ExpertAssist's built-in Telnet Server performed via standalone telnet client (such as Windows built-in telnet console application).

FTP Client

Connections to the Virtual FTP Server

Telnet Connections

Selecting this option will display all current Telnet connections currently being served by ExpertAssist. This includes the connections opened via the built-in Command Prompt telnet client as well as those that are served by built-in Telnet Server and opened using some standalone telnet client. It will display the IP address of the connected client, the connection protocol, and the name of the Windows user established the connection. This will be the user whose credentials were used by a remote client to authenticate within ExpertAssist. You can also see the time the connection has been started on, emulation type, console window size (if applicable), and when will the session recovery timeout expire (if applicable).

Additionally, you can terminate the established connection. Clicking the red button in the Lose column will disconnect the client but leave the session open until the session recovery timeout expires.

You can kill the connection by terminating the connection session if you click the red button in the Kill column.

Installed Applications

Typically, you can view applications installed on a remote computer using the Add or Remove Programs. However, this requires you choose Start|Control Panel|Add or Remove Programs right on the remote computer or press <Windows Logo> + <R>, type appwiz.cpl and press <Enter>. Whilst you can do that from the Remote Control applet, it is much easier to do that from the Installed Application page. It will save your traffic, and allow you export the retrieved list of all the applications, hotfixes, service packs to your local computer right from the browser. If some of the applications installed on the remote computer is failing, you can review the list and locate the faulting one.

To remove the application:

1. If necessary, you can remove the application by copying the string present in the Uninstall String for the application. This string is only displayed if supported by the application itself.
2. To uninstall the application, open the Command Prompt page under the Computer Management object, paste the copied string and hit <Enter>.

Please note that Command Prompt runs applications non-interactively (technically, in another Window Station).

When uninstalling applications by executing the uninstall string in the Command Prompt window, make sure to use switches that will force the uninstall to run quietly without requiring remote user input. Use /quiet switch when executing the spuninst.exe:

```
"C:\Windows\$NtUninstallKBXXXX$\spuninst\spuninst.exe" /quiet
```

Alternatively,

1. You can write a custom PowerShell script that will execute the uninstall script. For example, suppose that you have to uninstall a KBXXXXX update that has the following in the Uninstall Script:

   ```
   C:\Windows\$NtUninstallKBXXXX$\spuninst\spuninst.exe
   ```

2. Copy this string from the page. Now you can write the following single-line script and execute it with ExpertAssist:

   ```
   & env:windir\`$NtUninstallKBXXXX`$\spuninst\spuninst.exe
   ```

3. Executing this will automatically run the Software Update Removal wizard on the remote computer.

   > **NOTE:** Use escape sequences to enable PowerShell correctly handle special symbols like dollar sign ($). Use the backwards apostrophe (`).

   Please refer to Scripts to find out more about PowerShell scripting functionality integrated into the ExpertAssist.

Manipulating installed applications from the page is even easier that doing so from the Control Panel applet. For example, simply hovering your mouse over the row with a particular application in the list will display support information for the application-something that would usually require you clicking the link.

Security

The pages items under Security object allow you access to ExpertAssist's various enhanced security features.

Access Control

Here you can control who has access to Quest ExpertAssist.

The upper portion of this page lists users already granted access to Quest ExpertAssist (if any).

The **Add** button lets you specify a Windows user or group, and their permissions within the Quest ExpertAssist.

The red **Delete** button next to each entry in the list will remove that user or group from the access list.

The following list details the options available for an entry in the permission list.

Table 6: Permission list options.

Permission	Type*	Description
Login	[R]	Anyone with any sort of access to Quest ExpertAssist is implicitly granted Login access. This allows for looking at the Home page, viewing the expiration date of your password on the Security > Windows Password and logging out. This is a basic permission. Users who do not have this permission cannot log in and will not be able to use other permissions should they have it assigned to them.
Configuration	[R][W][D]	Users have access to Server Functions > FTP capabilities, Performance Monitoring > Telnet Connections, Security > IP configurations and Access Control, and Preferences object. Keep this in mind this grants users access control to modifying user permissions in Quest ExpertAssist.
Scripts	[R][W][D]	Users can execute, create, change or delete scripts on Scheduling & Alerts > Scripting. Users should have appropriate permissions on a remote machine to be able to create, change, or delete scripts.
Event Viewer	[R][D]	Allows the use of the Event Viewer page under Computer Management.
File System	[R][W][D]	Allows the use of the File Transfer object, Computer Management > File Manager, Computer Settings > Shared Resources, and Security

Permission	Type*	Description
		> EA Logs. Users should have appropriate permissions on a remote machine to be able to copy, modify files to remote machine, and view shared resources.
Registry	[R][W][D]	Allows for editing and compacting of the registry under Computer Management, and viewing Performance Monitoring > Installed Applications.
Performance Data	[R]	Ability to view performance and system information data under Performance Monitoring.
Processes	[R][W][D]	Allows you view processes, service and drivers, on a remote computer, change their settings and statuses in Computer Management object. Allows create and manage tasks via Scheduling & Alerts > Task Scheduler. Users can also view open files, registry keys, TCP/IP ports, and DLLs in use on the remote computer.
Reboot	[W]	Allows rebooting the computer and restarting the ExpertAssist service on the Computer Management > Reboot page.
Remote Control	[R][W][D]	Allows use of the Java-based Remote Control. You can also talk to interactive user via Help Desk Chat.
User/Group Accounts	[R][W][D]	Allows the use of the User Manager page found under the Computer Management object. Users should have appropriate permissions on the remote computer to be able to create and modify local users and groups.
System Configuration	[R][W][D]	Allows the user to view and change environment variables, set virtual memory settings and time, enable automatic logon via Computer Settings object. Provides access to Server Functions > Active Directory page and allows you view network and drive partition info pages using the Performance Monitoring object. Users should have appropriate permissions on the remote computer. The user should be registered with Active Directory to be able to use Active Directory page features.
Telnet (EA Client)	[R]	Allows the user to use the ExpertAssist built-in proprietary secured telnet client found on Server Functions > Command Prompt page.
Telnet	[R]	Allows access to the machine via Telnet using any standalone terminal emulator.
Full Control	Adds all possible permissions to a user. It is recommended to have at least one account that has Full Control capabilities.	
Force “Personal Edition”	Enable users to get the user interface of EA Personal Edition when logged on. The interface provides access to a limited set of features. Though any EA feature can still be used by referring to it with its URL. The setting does not affect the Administrator-level users.	

Permission	Type*	Description
Interface		
IP Filter		Assign an IP filter profile to the user, and specify which IP addresses can or cannot be connected from.

*

[R] Read Access
[W] Write (Update) Access
[D] Delete (Remove) Access

You can select individual permissions, or specify Full Control.

You can also restrict the user to an IP address or a network by creating an IP Filter on the IP Filtering page under the Security object.

You can also restrict a certain user to an IP address or an IP address range. Please remember that access rights are cumulative: if Group X has full access to Quest ExpertAssist and is not bound to an IP address and User Z is a member of that group, he will always have full access, even if you bind him to a specific IP address or network. To allow a user or group access from two or more IP addresses or networks, simply grant them the same permissions several times, but with different IP restrictions.

Access rights are cumulative. That is, if Group A has access to the Event Viewer, and Group B has access to the File Manager, a user who is a member of both groups will have access to both modules.

If the machine is a domain controller, the user accounts and groups that appear are listed from its domain. If the computer is not a domain controller, local users and groups are displayed. You can specify where to list accounts from by typing the name of the domain or the computer in the input field and clicking the List accounts button.

Access rights are stored under the registry key HKEY_LOCAL_MACHINE\SOFTWARE\DesktopAuthority\V5\Permissions\ in binary form. This data is basically stored in a particular key with the name of the Security Identifiers (SIDs) of the groups or users. The particular key contains registry parameters that define the access mask associated with SID, and the specific IP Filter applied. Each created IP Filter and its IP address restrictions are stored under the HKEY_LOCAL_MACHINE\SOFTWARE\DesktopAuthority\V5\IPFilter\Profiles\. By default, any data under the HKEY_LOCAL_MACHINE\SOFTWARE\ key can only be changed by Administrators, PowerUsers, or the SYSTEM account.

There are a few options on the lower part of the Access Control page. Here you can enable or disable the following features:

Allow full control to administrators

This is enabled by default. It adds Full Control permission to all administrators of the computer. If you turn it off, only users explicitly granted permission to use Quest ExpertAssist will have access.

NT LAN Manager authentication

Enable/Disable NTLM authentication. For those of you concerned about security, Quest ExpertAssist supports the Windows Challenge/Response type authentication. You must use Internet Explorer to take advantage of this feature. You need not worry about exposing your password to eavesdroppers if you are using HTTPS to secure all communications between your browser and Quest ExpertAssist.

Save user name in a cookie

Finally, you can configure Quest ExpertAssist to remember your user name in a cookie.

Any Access Control permissions set locally on a workstation will be overwritten by the permissions specified in the Remote Control tab of the Desktop Authority Manager.

Configuration Permissions and Registry Permission

Special care needs to be taken with a few of the above options. Users with access to Security > Access Control page (Configuration permission) and Computer Management > Registry Editor page (Registry permission) can also access and change the Quest ExpertAssist configuration data, including users' permissions. However, the Registry permission can be considered safe, since the administrator can change permissions on the HKLM\Software\DesktopAuthority key and protect it from unwanted access. Users who can Create/Edit Scripts can also create programs in the Small language that run on the remote computer. These scripts will be run under the account of the person starting the script from the Scripting page – except when a Small program is called from the system monitoring script. In this case, the program is run under the LocalSystem account.

Reboot Permissions, Remote Control Permissions, Processes Permissions

With the exception of the objects and pages that the user is given access within the Quest ExpertAssist by applying Reboot, Remote Control and Processes permissions to them, user's Windows account permissions is used by Quest ExpertAssist on the remote computer. For example, you can grant someone access to the File Manager page within the Quest ExpertAssist, but they will only be able to access files and directories their Windows user account has permissions to on the remote computer. The same goes for the Registry Editor, User Manager, etc.

The above exception for objects and pages that can be accessed having the Reboot, Remote Control and Processes permissions applied within Quest ExpertAssist is made to provide you maximum control over your system. The Quest ExpertAssist uses the all-powerful LocalSystem account to perform the tasks via these objects and pages. For example, not even an Administrator has sufficient rights to terminate a service process - but with Quest ExpertAssist performing this action under the LocalSystem account, any process can be terminated. Remote Control is another exception. When you are remotely controlling the system with Quest ExpertAssist, you have access to the mouse and the keyboard of the system. If nobody is logged on interactively, you will need to use the Windows logon screen to gain access to the desktop, typing in a username or password, possibly different than the one you are accessing Quest ExpertAssist with. If there is a user logged on to the host computer, you will be working under this user account.

IP Address Lockout

With ExpertAssist's IP Address Lockout feature you can detect and temporarily lock out potential intruders.

This security precaution allows you to configure two specific types of filter. These are called the Denial of Service Filter and the Authentication Attack Filter. The first is a precaution against unwanted intruders who slow your remote machine to a halt by continuously requesting the same service. The second locks out those who persistently try to get past your log-in screen without authorization.

The configuration for each is identical, although the default values differ due to the differences in the kind of attack they are designed to prevent.

Active

By ticking this checkbox you will enable this feature. This can be useful if your server is exposed to the Internet. IP Lockout will prevent people from gaining access to the administrator username and password using brute-force methods, or from tying up your services through relentless requests.

Number of invalid attempts before locking out

Specify the number of login attempts before a lockout occurs.

Reset invalid attempt counter after

After the amount of time specified in this box elapses, the invalid attempt count of the offending IP address will be reset to zero.

Lock out for

If there were a number of bad login attempts from the same IP address, as specified in the second field, within the time period specified in the reset count field, all attempted connections from the offending IP address will be rejected for the amount of time given here.

Bad login attempts and lockouts are logged in the DesktopAuthority.log file if you have logging enabled. Bad login attempts are also logged into User Management Logs.

IP Filtering

With ExpertAssist's IP address filtering feature you can specify exactly which computers are allowed to access ExpertAssist on your system.

The simple interface on the Security > IP Filtering page lets you maintain IP address restrictions.

If the Profiles list is empty, then filtering is disabled.

How IP Filtering works

When an IP address is checked against a list, ExpertAssist goes from the first element of the list to the last, comparing the IP address against the item. If the item is a single IP address, it only matches the remote IP if they are equal. If the item is an IP address with a subnet mask, a logical AND operation is performed on the subnet mask and the remote IP address, and the result is checked against the item's network address to see if the remote IP address is in fact on the network. If the item is a wildcard, the remote IP address is converted to its dotted textual representation and the two strings are compared.

When a match is found, ExpertAssist checks if it should allow or deny the connection, based on the allow/deny flag belonging to it. This result is then used to decide whether to let the connection proceed.

If no match is found, then the connection is allowed. If you would like all connections to be denied by default, except for those in the list, enter a DENY:* line as the last item on the list.

It is not possible for you to lock yourself out by accident when setting up IP address restrictions from afar, i.e. you can't enter a DENY:* clause into an empty list.

To add an IP Filtering:

1. Select the existing IP Filter and click **Edit**.
   Or,
   Type in the new IP Filter name in the **Name** edit box and click **Add**.
2. The **Move Up**, **Delete**, and **Move Down** buttons on the IP Filtering page for the selected filter let you manage already entered filters. Select one item in the list, and move it up or down with the appropriate buttons, or remove it altogether.
3. The **Address** and **Subnet** fields let you specify a new filtering item. You can enter the following:
   - A single IP address
   - An IP address with a subnet mask, essentially granting or denying access for a whole network.
   - An IP address with wildcards and no subnet mask. Accepted wildcards are an asterisk (*) that matches any number of characters, or a question mark (?), that matches a single character only.

4. The Allow and Deny options in the **Type** drop-down list let you specify whether you want to allow or deny access to the IP address or addresses entered.

Whenever a new connection is established to ExpertAssist, the remote IP address is checked against the filter or filters in the list, and access is granted or denied accordingly. The IP filters that you set up here apply to every connection received by ExpertAssist, except for those aimed at the Virtual FTP Server. To specify IP address restrictions specific to this module you will need to use its specific IP filtering options.

Examples

Example 1.

Allow connections from IP address 215.43.21.12 and the network 192.168.0.0/16, and deny all other connections:

```
ALLOW:215.43.21.12
ALLOW:192.168.0.0  (255.255.0.0)  -OR-  ALLOW:192.168.*
DENY:*
```

Example 2.

Allow connections from IP address 215.43.21.12 and the network 192.168.0.0/16, but not from the address 192.168.0.12, and deny everything else:

```
ALLOW:215.43.21.12
DENY:192.168.0.12
ALLOW:192.168.0.0  (255.255.0.0)  -OR-  ALLOW:192.168.*
DENY:*
```

Please note that denying the connection from 192.168.0.12 comes before allowing connections to the 192.168.0.0/16 network. This is because if ExpertAssist was to find the ALLOW item first, it would let IP address 192.168.0.12 through, since it matches the condition. To prevent this, we make sure that the address 192.168.0.12 is checked before the network to which it belongs.

Example 3.

Allow all connections, except those coming from 192.168.0.12:

```
DENY:192.168.0.12
```

Example 4.

Deny all connections from the network 192.168.0.0/16 except for the subnet 192.168.12.0/24, and allow all other connections:

```
ALLOW:192.168.12.0 (255.255.255.0) -OR- ALLOW:192.168.12.*
DENY:192.168.0.0 (255.255.0.0) -OR- DENY:192.168.*
```

Yet again, ordering is crucial.

EA Logs

Here is where you view the ExpertAssist log files.

The active log file is at the top of the list and is named `DesktopAuthority.log`. Older logs are stored with the naming convention DAYYYYMMDD.log. For example, the ExpertAssist log file for June 1st 2018 would be called DA20180601.log.

You can enable or disable logging to text files as you will, but ExpertAssist will always log the following events to the Windows Application Log:

1. Service Start/Stop
2. Login/Logout

3. Remote Control Start/Stop
4. Telnet Login/Logout

The Application Log is used because of security considerations.

In addition, service start and stop events are always written to the `DesktopAuthority.log` file, no matter whether logging is enabled or disabled. You can modify the settings for these logs under the Log Settings page of the Preferences section.

The last entry in the log file list is Download all logs in one compressed file. Click this to create and download a single zipped package with all the log files above.

User Management Log

Use the **User Management Log** section to view the logs of the activities performed during each remote management session on the EA host you are currently managing via EA. These activities are, for example, a registry key creation, stopping/running services, remote control session data, etc. (To view the overall EA activities logs, use the EA Logs page.)

The user management logs feature the following:

- Store the records of the activities performed during remote management sessions during the period specified in the corresponding settings – 30 days by default.
- Are presented in a special secure ExpertAssist's own file format — SLOG files;
- Are saved on an EA host (by default, to an EA installation directory: %ProgramFiles%\DesktopAuthority\useractions, or %ProgramFiles(x86)%\DesktopAuthority\useractions).
- Are stored encrypted on an EA host, so use the User Management Log page to read the logs' content.
- Are secured and protected from changes outside of EA. The standard RSA 8000 based digital signature schema is used for the security purposes. The modified or anyhow corrupted logs are marked as invalid.

To view logs:

1. In the navigation pane of the EA Management Window, go **Security** -> **User Management Log**. The list of available SLOG log files will be shown on the page to the right in a table. Some of the columns are detailed below.

   Table 7: User Management logs data.

Table Heading	Explanation
ID	The active log (DesktopAuthority.slog) is on top of the list. The active log logs activities performed during the period when the EA services were started and stopped. The log for the oldest session is at the bottom of the list.
Name	• The DesktopAuthority.slog file is the active log.

Table Heading	Explanation
	• Older logs are named according to the following convention DAYYYYMMDD_HHMMSS.slog. For example, the user management log file for June 1st, 2018, will be entitled **DA20180601_132125.slog**.
Validity	Icon that indicates an SLOG file is invalid, i.e. modified (by other means than the EA application) or anyhow corrupted.

2. Click on an SLOG log file you need. The selected log's details will be shown in the table below the logs list.
   The most recent records are always on top of the list.

To filter logs:

You can filter logs by the following data:

- the user logged in to run the EA management session;
- the date they were created or modified;
- the validity of the logs.

To filter the list of logs:

1. Use the desired field to set values to filter the logs' list.

   For the **User** field, use the following format:
   DomainName\UserName

   For the **Date from** and **Date to** fields, either use the calendar that will show when you click on the field, or enter the date manually in the following format;
   YYYY-MM-DD.
2. Click **Apply**. The list of logs will change accordingly.

SSL Setup

If you set up SSL support for ExpertAssist, all traffic between the host and the remote computer will be encrypted using industry-strength 128-bit ciphers, protecting your passwords and data. The SSL certificates generated here are used for accessing the HTML-based administration module via HTTPS, and are also used by all virtual FTP servers to secure connections if using a suitable client. Because the SSL protocol is considered insecure as it is vulnerable to the POODLE attack, ExpertAssist in fact uses high secure TLS protocol. Make sure to enable the TLS 1.1 or 1.2 protocol in the browser for the computer where you will be connecting to the remote compute from.

Setting up SSL support for ExpertAssist is done in four easy steps:

1. First, you must set up your Certificate Authority (CA). Select the Create a self-signed certificate item in the list at the top for the page and click the Continue button. This step will allow you to start creating a CA certificate, valid for nine years, and self-sign it. All of that you can do on the next page.

2. On the next page simply fill out the form at the bottom of the page specifying your country code, your organization and your name. Some default values are provided here from your computer's registry. This will configure the CA selected from the list at the top of the page. If you are creating a new CA, select the Create new CA.

As the second step on this page, you need to create the server certificate. Simply fill out the form at the bottom and click the Continue button to proceed. ExpertAssist will generate a certificate request, and sign it with the Certificate Authority selected at the top of the page. The certificate created this way will be valid for ten years. Click Continue at the bottom.

3. The third step is optional: you can now install the CA certificate in your browser. This will suppress the message you'd otherwise get about the unknown Certificate Authority every time you make a secure connection to ExpertAssist. Click on the button to download the generated certificate to your computer so that you can install it in your browser.

That's it. You are now ready to make a secure connection to ExpertAssist. Simply use a URL in the form of https://my.machine.here:2000.

You can use the same CA certificate on several machines, but you can't use the same server certificate in more than one place.

To use one CA certificate on a network of NT machines:

1. Perform step one on the first machine.
2. Copy the files CACert.pem, CAKey.pem and CACert.der in the ExpertAssist directory to the other machines.
3. Continue SSL setup from step two on all other boxes. You only have to perform step three once in this case.

FIPS Compliant Cryptography

You can enable ExpertAssist to comply with Federal Information Processing Standard (FIPS) 140-1 cryptography policies. When enabled, ExpertAssist will accept only those connections from remote clients that comply with FIPS policies and use strong cipher suite of strong encryption algorithms TLS_RSA_WITH_3DES_EDE_CBC_SHA. In effect, this enables both the client (a computer where you access the remote computer from) and the server (remote computer where ExpertAssist runs on) organize a highly secure channel using the Transport Layer Security (TLS) protocol. Once the TLS is used and enabled to choose from the FIPS 140-1 standard's security algorithms suite, this makes the strict use of certain algorithms for implementing certain operations.

Table 8: FIPS 140-1 standard's security algorithms.

Algorithm	Usage
Triple DES (3DES)	Used to encrypt TLS traffic
Rivest, Shamir, and Adelman (RSA)	Public key algorithm used for exchanging TLS keys and authentication
Secure Hashing Algorithm 1 (SHA-1)	Used for TLS hashing

To inform the ExpertAssist that it should use only FIPS 140-1 compliant algorithms:

1. Enable the following security policy for the remote computer within either Local Security Policy (LSP) or as a part of Group Policy **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**.

   This policy can be enabled under the Configuration\Windows Settings\Security Settings\Local Policies\Security Options\ path for the LSP or Group Policy object (GPO).

   > **NOTE:** To enable ExpertAssist using the FIPS 140-1 standard this security policy should be enabled on the remote computer where the ExpertAssist runs.

2. When this policy is applied to the remote computer, you have to enable your client browser to use the TLS 1.1/1.2 protocol when accessing that remote computer. This enables your client browser to use that limited cipher suite of the algorithms that are required by the FIPS enabled remote computer. In other words, both the remote computer and your local computer should be able to use the only the FIPS compliant set of security algorithms. Enabling the FIPS security policy on the remote computer forces the ExpertAssist to accept only those connections and only from those clients that connect over the TLS protocol, and then apply cipher set restrictions on it. Enabling the client browser to use the TLS protocol you trigger the browser to negotiate the requirements determined by ExpertAssist.

   By default the TLS protocol supports the following cipher suites:

   - TLS_RSA_WITH_RC4_128_MD5
   - TLS_RSA_WITH_RC4_128_SHA
   - TLS_RSA_WITH_3DES_EDE_CBC_SHA
   - TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
   - TLS_RSA_WITH_DES_CBC_SHA
   - TLS_DHE_DSS_WITH_DES_CBC_SHA
   - TLS_RSA_EXPORT1024_WITH_RC4_56_SHA
   - TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA
   - TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA
   - TLS_RSA_EXPORT_WITH_RC4_40_MD5
   - TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
   - TLS_RSA_WITH_NULL_MD5
   - TLS_RSA_WITH_NULL_SHA

   Enabling usage of TLS in the browser (the client), you enable it to work with all the specified cipher suites. Enabling the FIPS security policy on your remote computer you force the ExpertAssist (the server) to narrow the cipher suite scope down to the single FIPS compliant suite: TLS_RSA_WITH_ 3DES_EDE_CBC_SHA.

   > **NOTE:** If you see the 'Internet Explorer cannot display the page' when connecting to the remote computer enabled with FIPS policy this may indicate your browser does not have the TLS enabled. Make sure to enable the TLS 1.1/1.2 protocols in the browser for the computer where you will be connecting to the remote computer from.

To enable your browser use the TLS protocol:

1. Tools|Internet Options in your browser and switch to the Advanced tab of the Internet Options dialog box.
2. Scroll the Settings list to the very end and set the Use TLS 1.1 and Use TLS 1.2 checkboxes in the Security settings section.

You can enable the TLS 1.1/1.2 automatically on your client computers using Desktop Authority Manager functionality to apply registry changes.

To do that, set it to create the SecureProtocols REG_DWORD value under the HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings key on your client computers. Then set the SecureProtocols value to the corresponding mask. The following masks are available:

To do that, set it to create the SecureProtocols REG_DWORD value under the HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings key on your client computers. Then set the SecureProtocols value to the corresponding mask. The following mask is available:

Protocol	Mask (Decimal)	Mask (Hexadecimal)
TLSv1.1/TLSv1.2	2560	0xa00

If you want set all your clients to have both TLS 1.1 and TLS 1.2 enabled in their browsers, set the mask to 2560 (decimal) or 0xa00 (hexadecimal).

Once you connect with your browser from your local computer to the remote computer running ExpertAssist and enabled with FIPS policy, ExpertAssist will ask your browser to negotiate the TLS/SSL channel using the TLS_RSA_WITH_3DES_EDE_CBC_SHA suite. Since you enabled your browser to use the TLS, this cipher suite will be selected to organize a secure communication channel (a so called Schannel) matching the FIPS 140-1 standard between your computer and the remote computer.

NOTE: Please refer to http://msdn.microsoft.com/en-us/library/aa380123(VS.85).aspx for more information about the Schannel provider and its cipher suites.

NOTE: Since the FIPS policy is configured in the Computer Configuration part of the GPO and applied per computer object, enabling this policy will affect all the users and applications running on the remote computer.

NOTE: Some of the web sites that require you use secure HTTPS connection may not be FIPS compliant because they generally use the SSL3 protocol which uses a non-FIPS compliant MD5 hashing algorithm. Please see the following KB http://support.microsoft.com/kb/811834 to find out how you could enable the remote computer user to work with such sites if necessary.

Windows Password

Select Windows Password to change the current user's windows password. You must be able to enter the old password before it can be updated.

Preferences

Appearance

If you select Appearance page under the Preferences object, you can tailor the look of ExpertAssist to your liking.

General Settings

Display perfviewer applet at the top of the screen

Enable/Disable the Java applet showing the current processor and memory utilization in the top frame.

Enable Tooltips

If you grow bored of the tooltips displayed by ExpertAssist, you can turn them off here.

Enable Icons

You can turn off most of the icons displayed on pages.

Default number of items per page for long lists

The number of records displayed per page on those where there are long lists (such as on the Event Viewer page).

Default number of items per WAP page

Most of the WAP devices out there have very small screens and limited memory. Also, some gateways might enforce size restrictions on the WML documents they compile for their devices. This configuration setting lets you specify the number of records to appear per WAP screen, where applicable. Such screens belong to the Services, Processes, and Drivers page.

Systray Settings

Display the ExpertAssist icon in the System Tray

If you don't want the ExpertAssist icon to be displayed in the notification area (system tray), you can disable it here. Right-clicking on this icon gives you access to a wealth of extra information, including a log of recent events and detailed performance data graphs. The computer must be restarted for this change to take effect.

Custom Pages

ExpertAssist is able to act as a simple HTTP daemon and serve files from the computer to the Web.

If you specify the root directory for the HTTP daemon, and the default index file, it will display the default index file from the web root specified.

Simply leave the directory field empty if you don't want to use custom pages.

Network

Here you can configure your ExpertAssist connection settings, your SMTP settings, and even Dynamic IP Support.

General Settings

The General Settings group allows you to change various connection and data transport related options.

TCP/IP port to listen on

Specify the port you want ExpertAssist to use. This takes effect when the service is restarted.

TCP/IP address to listen on

Specify the IP address you want ExpertAssist to use for incoming connections. Your machine can have several IP addresses assigned to it, and ExpertAssist can listen on all of those addresses or just the one you specify here. This takes effect when the service is restarted.

IP filter profile to use

Here you can select from a drop-down list of specified IP addresses. You will first need to set this up under Security > IP Filtering

You must restart the ExpertAssist service before the changes take effect.

Accept unsecured HTTP connections (non-SSL)

If this checkbox is unchecked and SSL transport has been set up (Security > SSL Setup) then only HTTPS connections will be allowed.

Broken proxy server mask

This is a rather obscure name for a setting provided to work around a rather obscure problem.

Some proxy servers request pages from web servers using several IP addresses. This can cause ExpertAssist to bounce you back to the login page after you click the Login button. If you are not affected by this problem, you should not change this setting. However, if you experience this problem, please read the following section carefully.

When you log in, your browser is assigned a session identifier in a cookie. For security reasons, this cookie is only valid when sent from the IP address from which the login originated. Were it not so, an eavesdropping attacker would be able to copy your cookie and gain access to all ExpertAssist resources to which you have access.

Some proxy servers use several IP addresses when requesting data from a remote computer. If this is the case with your proxy server, ExpertAssist sees the original IP address and session identifier as valid, but requests

originating from other IP addresses (even if accompanied by a valid cookie) are replied to with the login page. The login page breaks out of frames, and displays itself in your browser - and you are prompted to log in again. A possible workaround is to keep logging in as many times as necessary - most proxy servers only use a few - maybe half a dozen - IP addresses. Once all the IP addresses are logged in, you will no longer be bounced to the login page.

ExpertAssist has had a setting called Proxy Problem Fixer. This is essentially a mask that can be applied to IP addresses. Suppose your proxy server uses the following IP addresses to request pages from servers:

192.168.0.33, 192.168.0.34, 192.168.0.35, 192.168.0.36, 192.168.0.37, 192.168.0.38

In this scenario, if you look at the IP addresses in binary form, you can see that only the last three bits are different:

11000000.10101000.00000000.00100001

11000000.10101000.00000000.00100010

11000000.10101000.00000000.00100011

11000000.10101000.00000000.00100100

11000000.10101000.00000000.00100101

11000000.10101000.00000000.00100110

This means that the largest number that can be represented on three bits (111 binary = 7 decimal) has to be masked from the IP addresses when checking them against each other to verify the validity of the session identifier cookie.

ExpertAssist provides a subnet mask-like setting for this purpose. By default, it is set to 255.255.255.255 - this means that no bits are masked off. Given the above scenario, we need to mask off the three least significant bits, thus we subtract 7 (binary form: 111) from 255.255.255.255, which leaves us with 255.255.255.248. By entering this value in the Proxy Problem Fixer field, we are telling ExpertAssist to ignore the last three bits.

This is a rather tedious way of getting around the problem, but short of reconfiguring the proxy server to use only one IP address, there is no easier solution. The latter is the recommended solution, since allowing several IP addresses to share the same session identifier can be a security risk. It is not really significant when you only mask off a few (three or four) bits, but if you need to decrease more and more significant bits of the IP addresses, you are putting yourself in a risky situation.

Of course, the risk can be decreased by protecting the cookie with SSL - but this requires that you request the login page with the HTTPS protocol and do not rely on the Use SSL switch that appears when it is requested via unsecured HTTP.

Maximum number of servicing threads

Here you can specify the maximum number of threads ExpertAssist can spawn to service client connections. You must restart the ExpertAssist service before the changes take effect.

Idle time allowed

Here you can specify the idle time allowed on a connection before the user is automatically logged out.

ExpertAssist is a highly configurable tool, meaning that you can change its settings to suit your individual remote administration needs and desires.

Stalled transfer timeout

In the ExpertAssist File Transfer applet, files can be copied to and from the remote computer. If the file transfer is halted for the duration of the timeout value the file transfer will be canceled.

File Transfer Download Bandwidth Limit

Enter the download bandwidth to be used for file transfers. This is entered in the form of kbits/sec. A bandwidth limit of 0 will disable this setting.

File Transfer Upload Bandwidth Limit

Enter the download bandwidth to be used for file transfers. This is entered in the form of kbits/sec. A bandwidth limit of 0 will disable this setting.

Force HTTP Tunneling

Force all java applets to use HTTP protocol instead of a direct socket connection.

SMTP Settings

If you want to configure ExpertAssist to send you email alerts you need to enter your SMTP server settings here.

SMTP server address

The IP address of the SMTP server that email will be sent through.

SMTP user name

If the SMTP server requires authentication, enter the user name here. Leave this field blank if the SMTP server does not require authentication.

SMTP password

If the SMTP server requires authentication, enter the password here. Leave this field blank if the SMTP server does not require authentication.

Default sender address

Enter a default email address for the SMTP server to use.

Test email recipient

To test the SMTP server settings, enter a test message here and click Send test message. An email will be sent through the SMTP server.

Dynamic IP Support

ExpertAssist can send you an email message pointing to the IP address of your remote host every time it starts up. Use this if your host has a dynamic IP address.

Email recipient

Enter the email address of the user who will receive the IP address change email. To disable this feature, leave this field blank.

Check every

Enter the time interval for when IP addresses should be checked for change.

Colors

Here you can modify the colors used by ExpertAssist.

This is done using the standard hexadecimal code used by HTML.

Simply enter the '#' symbol followed by the appropriate six-digit code and click **Apply** to see the change.
For example, the pale blue color used for backgrounds in the default color settings for ExpertAssist is #8abdf0.

Predefined color schemes can be selected from the options in the **Scheme** drop down menu at the bottom of the screen. Click **Apply** after selecting a theme.

You can restore the default colors by clicking **Restore** at the bottom of the page.

Log Settings

ExpertAssist's log settings are fully configurable. Here you can modify the general settings for ExpertAssist, ODBC and the Syslog settings. In order to view the logs themselves you would go to Security > EA Logs.

General Settings

Keep log files for this many days

At midnight ExpertAssist rotates its log files and deletes old, unneeded ones. The value you enter here determines how old log files can grow before they are deleted. If you set this to zero, the files will never be deleted, unless you do it manually.

Directory for log files

You can also specify the directory for storing these log files. If you leave this blank, they will be stored in ExpertAssist's installation folder, by default.

ODBC Messages

Send log events to ODBC data source

Set this checkbox to use the specified ODBC data source to send events to. Click the Click here to configure the ODBC data source link to configure the data source.

Syslog Settings

With ExpertAssist you can also modify the syslog settings. Here you can modify the syslog settings and specify the syslog hostname or IP address, transport protocol (UDP or TCP), syslog port numbers for UDP and TCP, as well as the facility code to report. Click Apply to update your settings.

User Management Log

Use the option to set the number of days within which theUser Management Log will be stored on an EA host machine - 30 days by default. Once the time specified elapses, logs will be deleted from the EA host.

You must Reboot before the changes take effect.

ODBC Messages

Specify an ODBC Data Source and table to write messages to. The messages are written to this database via a script defined on Scripting and System Monitoring pages.

Data Source

Enter the Data Source name that will enable the database connection.

User Name

Enter the User Name that is used to access the tables using the specified DSN.

Password

Enter the Password that is used to access the tables using the specified DSN.

Table Name

Enter the Table that the script will write messages to.

Time Stamp

Enter the name of the timestamp or text field from the database that will be used for the time stamp. Maximum 20 characters.

Computer Name

Enter the name of the text field from the database that will be used to hold the computer name. Maximum 16 characters.

Message

Enter the name of the text field from the database that will be used message. Maximum 250 characters.

Log Level

Enter the name of the text field from the database that will be used for the severity of the message. Maximum 10 characters.

Module

Enter the name of the text field from the database that will be used for the originating module. Maximum 20 characters.

Facility

Enter the name of the text field from the database that will be used for the originating facility. Maximum 20 characters.

Client

Enter the name of the text field from the database that will be used to hold the address and name of the client. Maximum 100 characters.

Write test message

Enter a message to send to the ODBC data source in order to test the data source connection. Click the Write test message button to send the test message.

Remote Control

Here you can view and modify a number of options available during real-time remote control sessions. This includes the general settings, security, audible notification, interactive user permissions, and the remote printing feature.

General Settings

Use mirror display driver

ExpertAssist provides a mirror display driver to be used on the remote computer. This display driver provides a faster and less CPU-intensive remote control session. Select this checkbox to use the mirror display driver. Clear this checkbox to disable the use of the mirror driver.

Change the color depth of the remote machine to the one selected in the Remote Control session

By default, ExpertAssist processes the captured screen image using software color dithering. This allows the ExpertAssist to 'virtually' change the color bit depth on the remote computer thus decreasing the traffic between the remote computer and your local computer. If a remote computer has a current bit depth set to 32 bit and you choose to change it to, say, 8 bit by choosing this depth from the corresponding drop-down list within the Remote Control applet, it will result in changing the bit depth within the applet only. Only the remote computer screen displayed on your local computer will change the bit dept. It will not physically change the color bit depth on the remote computer. Indeed, ExpertAssist converts the captured screen picture on the remote computer dithering the picture on-the-fly from 32 bit to 8 bit and sends it in such a way to the browser of your local computer.

NOTE: Dithering, also known as halftoning, allows to reduce the color palette table without affecting the image quality by smoothing the visibility of quantization errors that appear when converting the depth. Since the effect is color bit depth reduction, ExpertAssist suggests to choose from the drop-down list only those values that are less or equal to bit depth set on the remote computer.

Setting this checkbox on is only necessary if you really want to change the bit depth physically right on the remote computer (but not only on the screen capture that is being transferred to your local computer).

NOTE: You can further boost remote control processing speeds by forcing Windows to not re-draw windows while you are dragging them. On the remote computer, open the System Properties dialog box and switch to Advanced tab. In the Performance box click Settings, select the Custom radio button and check the Show window contents while dragging checkbox off. This will enable ExpertAssist to draw the window box while you are dragging a window on the remote computer effectively reducing traffic and boosting processing speeds.

Automatically disable wallpaper

Select this checkbox to disable the wallpaper (or background desktop image) on the host computer when a remote control session is started. Clear this checkbox to view the image during the remote session.

Automatic clipboard transfer maximum size

The ExpertAssist provides the ability to transfer clipboards between host and client machines, allowing the ability to copy from one machine and paste on the other. Specify the maximum number of kilobytes (KB) that can be transferred between machines. The default size is 1024 KB. Transferring significantly larger amounts may cause slowdowns. The maximum limit is 5 Mbytes in both directions. If the clipboard is larger than the maximum limit nothing will be transferred.

Idle time allowed

Specify the number of minutes a remote host may be inactive for. If a period of inactivity is determined, the client will automatically be disconnected from the remote session.

Auto panning

If the host computer's display area is larger than that which the remote control client can display only a part of the screen is shown and you can use scrollbars to view the required area of the remote display. With this option enabled, the screen is automatically scrolled for you when the mouse nears the edge of the current display area.

Maximum number of screen updates per second

Specify the number of times the screen is updated per second.

Control-Alt-Del Hotkey

Select an alternate hotkey to use from the drop list. Choose from Ctrl-Alt-Insert, Ctrl-Alt-F12 and Ctrl-Alt-F1.

Security

Disable host keyboard and mouse

Select this checkbox to disable the host's keyboard and mouse during the remote session. This will prevent the host user from using the keyboard or mouse while the remote control session is in progress. Clear this checkbox to enable the host's keyboard and mouse during the remote control session.

Blank the host's monitor

Select this checkbox to blank the display on the host computer during a remote control session. This is useful for preventing user interaction while remote work is in process.

Lock console when connection broken

Select this checkbox to lock the console in order to protect open files, if, due to a network error, the Java remote control client loses its connection to the server. Clear this checkbox to leave console as is when the connection is broken.

Lock console when connection times out

Select this checkbox to lock the console in order to protect open files, if the connection times out. Clear this checkbox to leave client as is when the connection times out.

Always lock console when remote control disconnects

Select this checkbox to lock the console when the remote session ends. Clear this checkbox to leave client as is when the remote session ends.

Audible Notification

Beep when the remote control session starts or ends

Select this checkbox to have an audible beep on the host computer when a remote control session is initiated or ended.

Beep continuously during remote control

Select this checkbox to have a periodic audible beep on the host computer during the remote control session.

Beep interval

Specify an interval for the periodic beep during the remote control session. The beep interval is specified in seconds.

Interactive User's Permission

Ask for permission from interactive user

If you turn this option off, you will disable the icon, and also any attempts to notify the local user when someone is accessing the computer remotely. When this option is off, none of the other settings in this configuration screen apply. This option, when disabled, basically tells ExpertAssist not to bother starting rmgui.exe, the software that sits in the system tray and communicates with the user. Disabling this option will also disable the Chat function.

Default answer for confirmation message

Yes or No. When someone tries to gain remote control access to the computer, and the interactive user does not answer the query, the remote control session will either proceed or not, depending on this setting.

Time allowed for the interactive user to give permission

This is the amount of time specified before the notification message times out.

Text to display to the user

This is the text that will be presented to the user in the remote control confirmation dialogue box. The string '%USER%' will be substituted by the name of the user who is attempting the remote control operation.

Display a warning message during Remote Control

Do not ask for permissions for technicians with Full Control (or Remote Control D) access rights

Select this checkbox to allow all administrators access to start a remote management session without waiting for a confirmation from a remote interactive user. Clear this checkbox to disable administrators default automatic

access to remotely control workstations without a remote user confirmation. Explicit permissions must be granted to users who will have access to start a remote management session.

Remote Printing

Enable Remote Printing

Here you can enable or disable ExpertAssist's ability to print remotely.

Telnet Server

This page allows you to view and modify Telnet related options. For a complete explanation of the Telnet server, please see Computer Management.

TCP/IP port to listen on / address to listen on

Here you can specify which port / address you want ExpertAssist to listen on for telnet connections. This defaults to the standard telnet port of 23, and all available interfaces. Changes take effect when ExpertAssist services are restarted.

Accept ExpertAssist connections (secure)

Allow the ExpertAssist's built-in terminal emulator connections to the remote computer. If disabled, the built-in Java client available via Computer Management|Command Prompt page cannot be used to access Telnet.

Accept Telnet connections

Specify whether telnet connections will be accepted from the standalone telnet clients on the specified TCP/IP port. If disabled you will only be able to telnet the remote computer using the ExpertAssist's built-in terminal emulator via Computer Management|Command Prompt page.

Show login banner

Enable or disable the logon message sent by the ExpertAssist's Telnet Server when a connection is established. The logon message includes the version of the operating system and ExpertAssist.

If you do not want to let anybody who connects to the Telnet ports know the version of the operating system and ExpertAssist, disable this option.

Maximum simultaneous connections

Here you can specify the maximum number of connections to the Telnet Server. It's a good idea to set a reasonable limit, especially on computers connected to the Internet. Every new connection uses resources on the computer.

Timeouts

Login/Idle/Session recovery timeout

Here you can set the login timeout (number of seconds the user may remain idle during the login process), the idle timeout (number of seconds the user may remain idle during a Telnet session) and the session recovery

timeout. When a Telnet connection is broken ungracefully (that is, the user does not type exit at the command prompt) it is possible to reconnect to the session and continue work where it was left off for a period of time. You can specify the amount of time for which you want the lost telnet session to remain available. Any and all running programs started by the user in the Telnet session will be available when the session is resumed.

Telnet Client Default Parameters

Here you can specify the default parameters for the ExpertAssist's built-in Telnet client . This client is available from the Command Prompt page under the Computer Management object.

Columns

Specify the number of columns to be used in the Telnet client window. This number determines the width of the window.

Rows

Specify the number of rows to be used in the Telnet client window. This number determines the height of the window.

Console mode

Select the Console mode from the drop-down list. Select from Stream, Full (ANSI colors) and Full (monochrome).

Ask console parameters

Select this checkbox to allow the system to prompt the user for the console parameters.

Custom Pages

ExpertAssist is able to act as a simple HTTP daemon and serve files from a specified directory. The default Custom Page path and index file is defined in the Custom Pages section on the Appearance page of the Preferences section. All other custom pages are reached from a link on the Custom HTTP default index file.

WAP and PDA Interface

ExpertAssist supports limited access via wireless devices using the Wireless Application Protocol (WAP). These devices are usually mobile phones, with limited screen size, limited memory, and limited processor capacity. For this reason, they do not understand HTML – pages displayed on WAP devices are written in WML, which is based on XML. Graphics are simple black-and-white images.

When you access ExpertAssist via the WAP interface, you are prompted to log in. Enter your username and password using the phone's controls then click the OK link. If ExpertAssist does not recognize your WAP device as such, it might cause your WAP browser to display a message regarding unknown content, a compile error, or something similar. In this case, you can edit the contents of the WapClients.cfg file found in your ExpertAssist folder to make the user agent known as a WAP device. Further information on the format of the file is found inside. It is a plain text file and can be edited using any text editor.

Security Precautions

With HTTP and the browser interface, you have a fairly simple job securing your communication: simply create an SSL certificate, install the certificate in your browser, and use HTTPS as the protocol.

With the WAP interface, things are more difficult, since your phone does not directly communicate with ExpertAssist. WAP devices connect to a WAP gateway that acts like an intelligent proxy server:

- The phone issues a request to the gateway. The phone and the gateway communicate via UDP (connectionless IP).
- The gateway issues an HTTP or HTTPS request to ExpertAssist and waits for the reply.
- The gateway compiles the received WML into bytecode and sends it to the phone.

While this is of no concern when browsing WAP pages for stock quotes or weather forecasts, it raises two issues when a secure connection is required:

1. The phone must be able to communicate with the gateway via a secure channel. This is done via the WTLS protocol that requires that the phone 'trusts' the gateway – that is, it has its WTLS certificate installed.
2. The gateway must be able to communicate with ExpertAssist via HTTPS. This requires that the gateway 'trust' the ExpertAssist installation in question – it should have its certificate installed.

When using a commercial gateway (such as the ones provided by cell phone companies) the first issue is usually not a problem. However, your cell phone provider will probably not install your self-generated ExpertAssist certificates, so the secure connection between the gateway and ExpertAssist will not be established.

When accessing ExpertAssist from your phone, always use the HTTPS protocol by specifying HTTPS:// in the beginning of the URL. This will encrypt the data sent and received between the gateway and the ExpertAssist installation.

Here is a brief description of how to configure a Nokia7110 to use a WAP gateway:

1. Select the Services menu. Select Settings. The 7110 allows you to store 5 different sets of WAP connection settings. Highlight the current settings, or one of the unused settings on the phone, and select Options. Select Edit to edit the selected settings.
2. Homepage should be set to the ExpertAssist installation you most frequently access - or any other WML page. You can use the Bookmarks feature of the phone to store your ExpertAssist URLs.
3. Connection Type should be set to Continuous.
4. Connection Security should be set to On, this will encrypt the data sent and received between the phone and the gateway.
5. Bearer must be set to Data.
6. Dial-up number must be set to the phone number of your dial-in server.
7. IP Address must be set to the address of your WAP gateway.
8. Authentication type can be set to either Normal or Secure, depending on the configuration of your dial-in server. This setting specifies how the username and password are sent to the dial-in server, and does not have any affect on actual WAP communications.
9. Data call type can be set to either Analogue or ISDN, depending on your mobile operator network and the type of dial-in connection that you will be using.
10. Data call speed can normally be left to Autobauding.
11. User name specifies the user name associated with your dial-up connection.
12. Password specifies the password associated with your dial-up connection.
13. Once you have configured all of your settings, use Back to return to the previous level of menus, and then Activate your configuration.

Info Screen

You will be greeted with an Info screen that displays some essential information about the computer.

At the bottom of this screen (and at the bottom of every screen) you will find the main menu that allows you to select ExpertAssist functions accessible via the WAP interface.

The Menu

The menu, at the bottom of the screen looks like the image on the left (only partially shown):

Here is the complete list of menu options:

1. Main Menu
2. Services
3. Drivers
4. Processes
5. Performance Monitoring
6. Reboot
7. Event Viewer
8. Logout

A link to this menu is present at the bottom of every page displayed by ExpertAssist.

Services

You see a listing of all installed services, with their status next to them. Selecting a service takes you into a menu that allows you to control that service:

On the services listing page, near the end, you can request different parts of the list.

Drivers

Looks and behaves exactly like the Services page.

Processes

The Processes page has three options, as shown in the image on the left.

The first two will let you see a listing similar to the Services or Drivers lists – next to the process name you will see either the CPU time used by the process or the Memory in use by the process, depending on your selection:

Selecting a process will display detailed information about it, such as the executable name with full path, the parent process, if available, the creation time, CPU time, pagefile and physical memory usage, as in the image on the left.

You also have the option of killing a process here.

The third option in the Processes menu is the Create Process one. This will present you with the following dialogue:

Filling out this form and submitting it launches a new process under the user account of the person using the WAP device. You can use this for a variety of tasks, such as executing batch files:

Executable Name: cmd.exe

Optional Parameters: /C c:\backup\startbackup.cmd

This will launch the command interpreter, which, in turn, will launch the startbackup.cmd batch file in the c:\backup directory.

Performance Monitoring

On the performance pages, you can view graphs on the CPU, memory, and disk space utilization. The main menu looks like the image on the left.

By selecting either of these options, you are presented with three graphs, each with a different sampling rate – just like in the main ExpertAssist performance charts.

The CPU load represents the total CPU load on multiprocessor machines. The memory load includes physical and virtual memory. The disk space utilization chart represents the total for all hard disks in the computer.

Reboot

This option presents you with a menu similar to that found in the HTML interface.

The first three selections reboot the computer. Normal reboot shuts down all applications. Emergency reboot kills all processes then shuts down and restarts the system in an orderly fashion. You might lose data in your running applications. Hard reboot is just like pressing the reset button or toggling the power switch: use this only as a last resort!

The last selection restarts the ExpertAssist service.

Event Viewer

This option enables you to view ExpertAssist's event viewer. You will be given a list of event viewer options.

Logout

This menu option ends your ExpertAssist session.

It is not strictly necessary to manually log out – your session will eventually time out after the time period specified in the ExpertAssist configuration elapses.

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build communitydriven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit https://www.quest.com/company/contact-us.aspx or call +1-949-754-8000.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions

- Chat with support engineers online
- View services to assist you with your product