ZyWALL SSL 10

Integrated SSL-VPN Appliance

User's Guide

Version 2.00
12/2008
Edition 1

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to log into a network over secure connections through the ZyWALL. You should have at least a basic knowledge of computer usage.

Related Documentation

- Web Configurator Online Help

  Embedded web help for descriptions of individual screens and supplementary information.
- ZyXEL Web Site

  Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The ZyWALL SSL 10 may be referred to as the "ZyWALL", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyWALL icon is not an exact representation of your device.

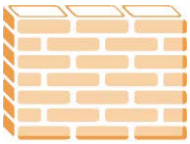
ZyWALL 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 

Table of Contents

List of Figures

PART I
Remote User Access

1 Introduction

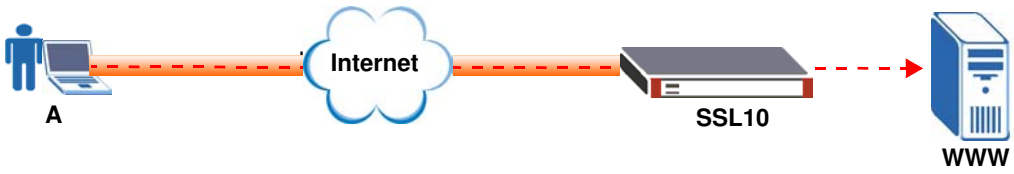
This chapter introduces secure network access and gives an overview of the remote user screens on the ZyWALL.

1.1 Overview

The ZyWALL provides secure connections to network resources such as applications, files, intranet sites or e-mails through web-based interface using Microsoft Outlook Web Access (OWA). No additional computer configuration or software installation is required.

The following figure shows a network example where a remote user (**A**) logs into the ZyWALL (**SSL10**) from the Internet to access a web server (**WWW**) on the local network.

Figure 1 Network Example



1.1.1 Network Resource Access Methods

As a remote user, you can access resources on the ZyWALL's local network using one of the following methods.

- Using a web browser

  Once you have successfully logged in through the ZyWALL, you can access any intranet site, web-based applications or web-based e-mails using a supported web browser. You do not have to install or pre-launch any application on your computer.
- Using the ZyWALL SecuExtender client

  Once you have successfully logged into the ZyWALL, the ZyWALL automatically loads the ZyWALL SecuExtender client program to your computer. With the ZyWALL SecuExtender, you can access servers, remote desktops and manage files as if you were on the local network. See Chapter 4 on page 33 for more on the ZyWALL SecuExtender.

1.1.2 System Requirements

The following lists the browser and computer system requirements for remote user access.

- Internet Explorer 5.5 with Microsoft XML (MSXML) service pack installed or 6.0 and above
- Netscape 7.2 and above
- Firefox 1.0 and above
- Mozilla 1.7.3 and above
- Windows 2000 Professional, Windows 2003, Windows XP Home/Professional (with service pack 2 and above), Windows Vista, or Linux.
- Sun Java Virtual Machine (JVM) installed with a minimum version of 1.4.2_07 for Netscape/Mozilla/Firefox and 1.4.2_02 for Internet Explorer and Linux computers.
- Java enabled in Internet Explorer on Windows computers.

1.1.3 Information You Need

Your network administrator should provide the following information that allows you to log in and access network resources.

- Domain name or IP address of the ZyWALL.
- Login account user name and password
- Specific computer requirements. For example, if you must use Windows XP with service pack 2, etc.
- If also required, the user name and/or password to access the network resource.

1.1.4 Certificate

Your computer establishes an HTTPS connection to the ZyWALL to access the login screen. If instructed by your network administrator, you must install or import a certificate (provided by the ZyWALL or your network administrator).

Refer to Appendix B on page 69 for more information.

1.2 Remote User Login

This section shows you how to access and log into the network through the ZyWALL. Example screens for Internet Explorer are shown.

1 Open a web browser and enter the web site address or IP address of the ZyWALL. For example, “http://sslvpn.mycompany.com”.

Figure 2 Enter the Address in a Web Browser

2 Click **OK** or **Yes** if a security screen displays.

Figure 3 Login Security Screen

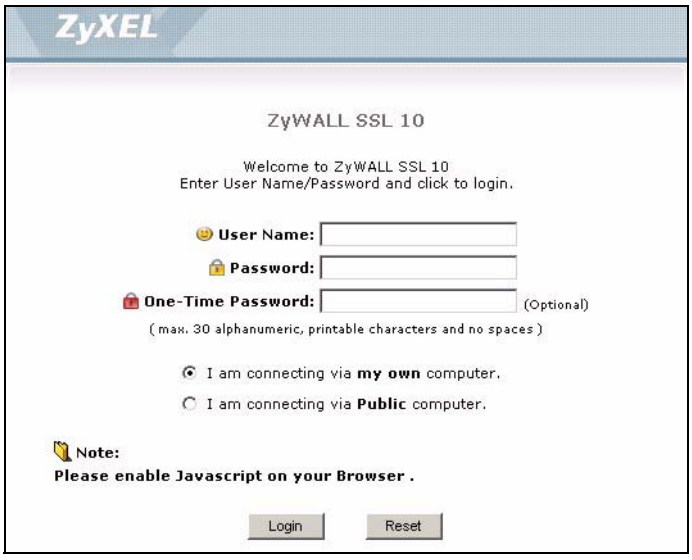
3 A login screen displays. Enter the user name and password of your login account. If a token password is also required, enter it in the **One-Time Password** screen.

Select **I am connecting via my own computer** if you log in using your personal computer.

If you are using a public computer to log in, select **I am connecting via Public computer**. The ZyWALL automatically clears history information from your browser cache after you log out. This prevents anyone from obtaining information that may be stored in the browser cache.

Click **Login**.

Figure 4 Login Screen



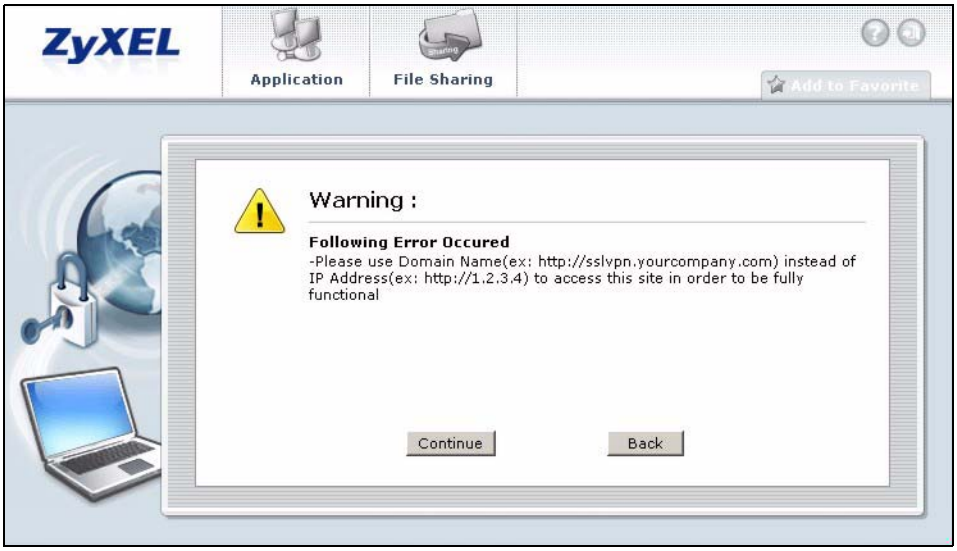
4 After the login is successful, your computer starts establishing a secure connection to the ZyWALL. This may take up to two minutes.

5 Download the installation software if you are prompted to upgrade the JVM. Click the link to access the Sun Java software web site. It is recommended you select the **Offline Installation** option.

Figure 5 Software Upgrade Prompt

6 If the following warning screen displays, click **Continue**.

Figure 6 Login Warning Message



7 The ZyWALL SecuExtender icon displays in the system tray.

Figure 7 ZyWALL SecuExtender Icon

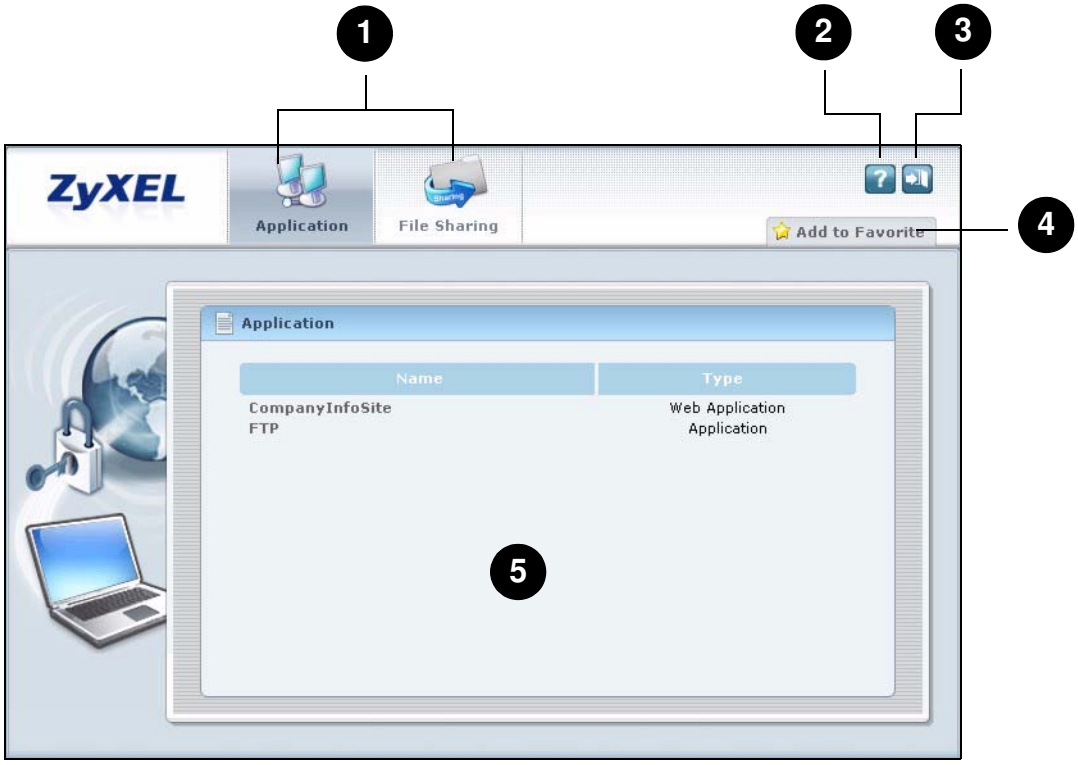
8 When the list of available resources displays in the **Application** screen, you have successfully logged into the network. See Figure 8 on page 19.

Available resource links vary depending on how the network administrator configures the ZyWALL.

1.3 Remote User Screen

This section describes the main elements in the remote user screens.

Figure 8 Remote User Screen



The following table describes the various parts of a remote user screen.

Table 1 Remote User Screen Overview

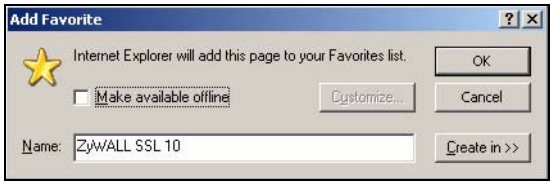
#	DESCRIPTION
1	Click on a menu tab to go to the **Application** or **File Sharing** screen.
2	Click this icon to display the on-line help window.
3	Click this icon to log out and terminate the secure connection.
4	Click **Add to Favorite** to create a bookmark for the ZyWALL in your web browser.
5	This part of the screen displays a list of the resources available to you. In the **Application** screen, click on a link to access or display the access method. In the **File Sharing** screen, click on a link to open a file or directory.

1.4 Bookmark

To bookmark the ZyWALL, click **Add to Favorite**. This lets you use the bookmark to access the ZyWALL instead of entering the ZyWALL's address every time.

1. In any remote user screen, click **Add to favorite**.
2. A descriptive name is entered in the **Name** field. You can accept the default or enter a name.
3. Click **OK** to create a bookmark in your web browser.

Figure 9 Add Favorite



1.5 Logout

To properly terminate a connection, click on the Logout icon in any remote user screen.

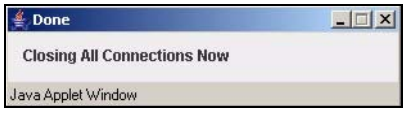
If you selected **I am connecting via Public computer** in the login screen, history information in your browser cache is also erased once you log out.

1. Click the **Logout** icon in any remote user screen.
2. A prompt window displays. Click **OK** to continue.

Figure 10 Logout: Prompt

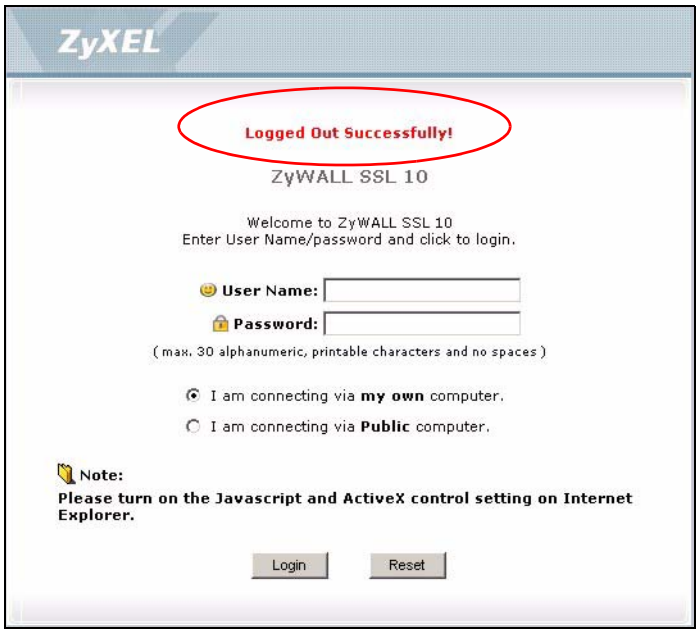
3. An information screen displays. This indicates that all connections have been successfully terminated.

Figure 11 Logout: Information Window



4. The login screen displays with the "Logged out successfully!" message.

Figure 12 Logout: Successful



2

Application

This chapter describes the Application screen you use to access an application on the network.

2.1 Overview

Depending on the configuration of your network administrator, you can use the Application screen to perform the following:

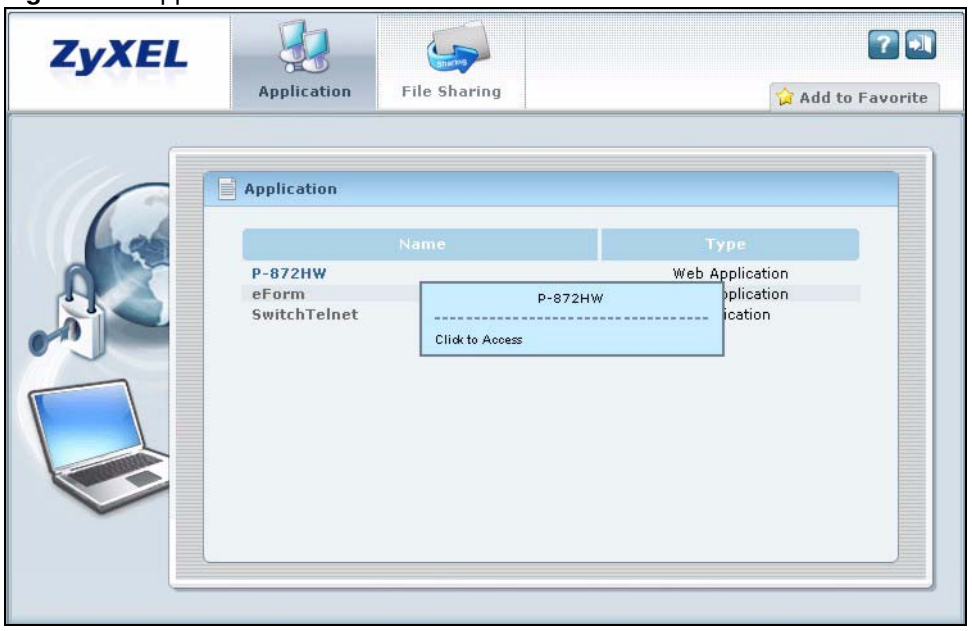
- Access a web-based application (such as a web site and e-mail).
- Display additional information on how to access a non-web based application (such as FTP).

2.1.1 The Application Screen

Click the **Application** tab to display the screen. The **Name** field displays the descriptive name for an application. The **Type** field displays **Web Application** to indicate a web-based application or **Application** for a non-web based application.

You can move your mouse over a link to display help information on how to access an application. The following shows an example.

Figure 13 Application

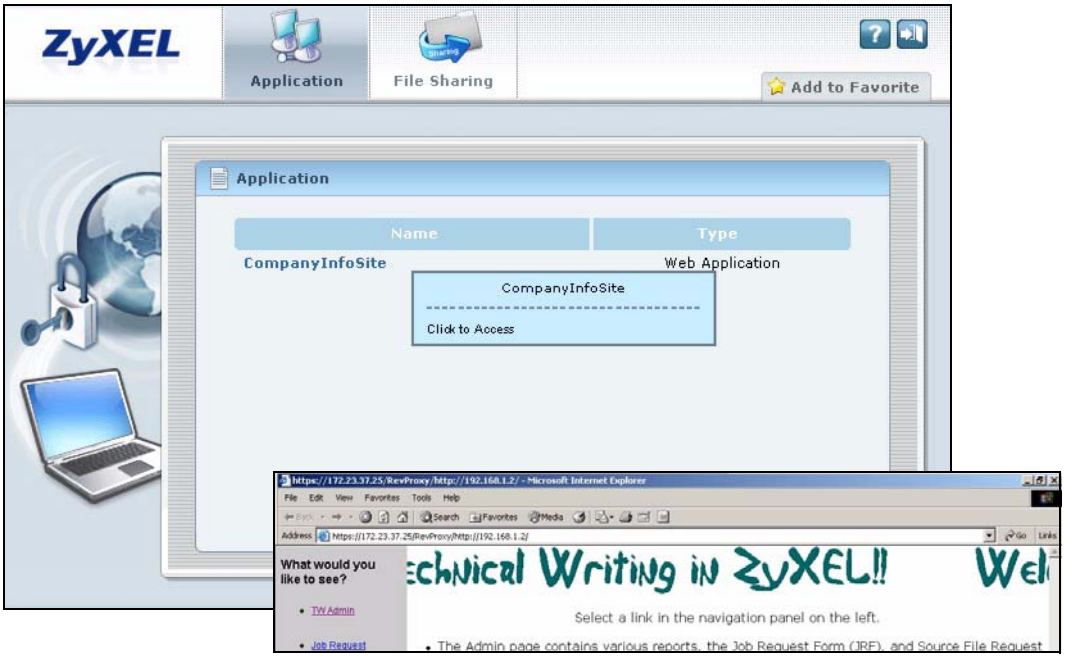


2.2 Accessing a Web-based Application

To access a web-based application, simply click a link in the **Application** screen to display the web screen in a separate browser window.

The following shows an example.

Figure 14 Application: Access Web-based Application



2.3 Accessing a Non-Web Based Application

To access a non-web based application, move your mouse over the link in the **Application** screen to display the access information.

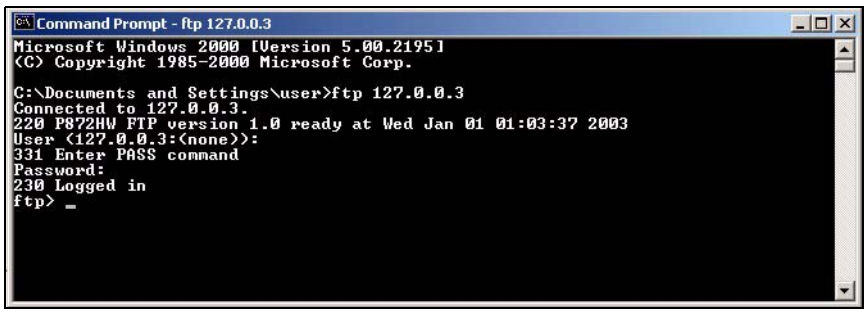
The following example shows you how to establish an FTP connection to a switch for device management.

1 In the **Application** screen, move your mouse over a link to display the pop-up information window.

Figure 15 Application: Access Non-Web based Application

2 Launch an FTP application and connect to the IP address provided. The following figure shows an example using Windows Command Prompt.

Figure 16 Application: Telnet Example



3

File Sharing

This chapter describes the **File Sharing** screen you use to access files on a Windows or Linux file server.

3.1 Overview

Use the **File Sharing** screen display and access shared files/folders on a file server.

You can also perform the following actions:

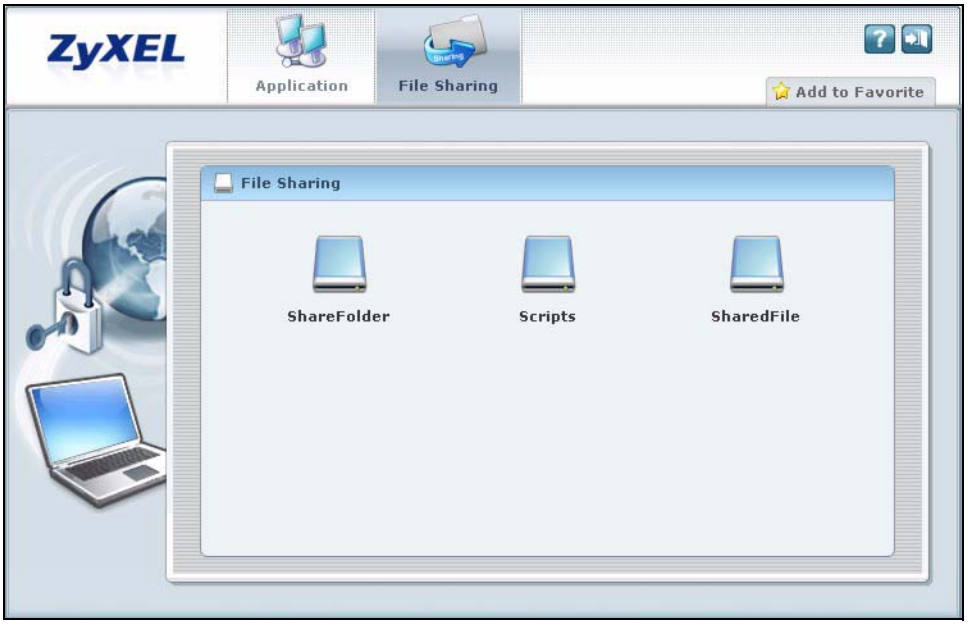
- Access a folder.
- Open a file (if your web browser cannot open the file, you are prompted to download it).
- Save a file to your computer.
- Create a new folder.
- Rename a file or folder.
- Delete a file or folder.
- Upload a file.

Available actions you can perform in the **File Sharing** screen vary depending on the rights granted to your user account on the file server.

3.2 Main File Sharing Screen

The first **File Sharing** screen displays the name(s) of the shared folder(s) available. The following figure shows an example with three file shares.

Figure 17 File Sharing

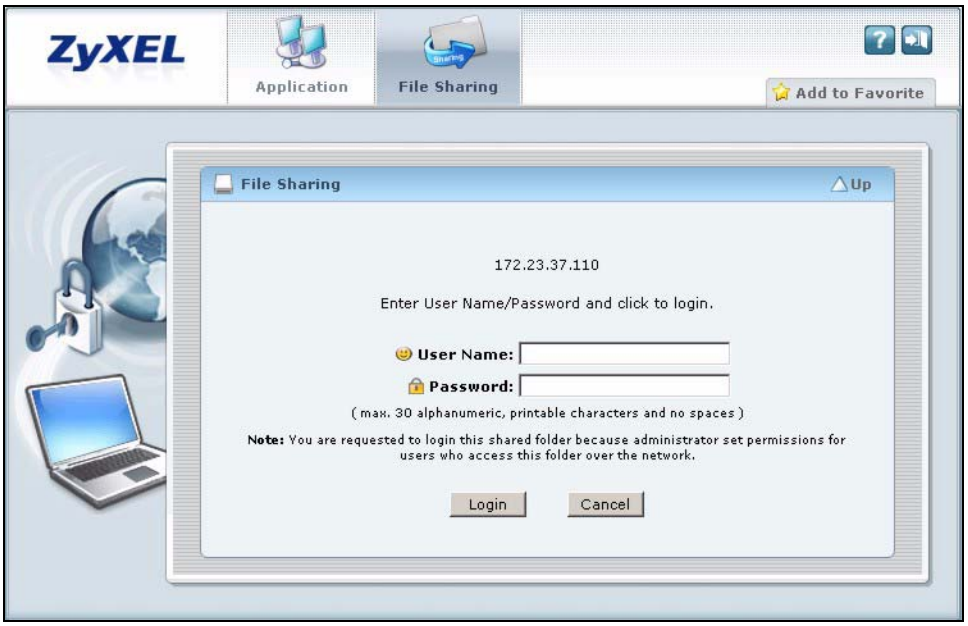


3.3 Opening a File or Folder

You can open a file if the file extension is recognized by the web browser and the associated application is installed on your computer.

1. Log in as a remote user and click the **File Sharing** tab.
2. Click on a file share icon.
3. If an access user name and password are required, a screen displays as shown in the following figure. Enter the account information and click **Login** to continue.

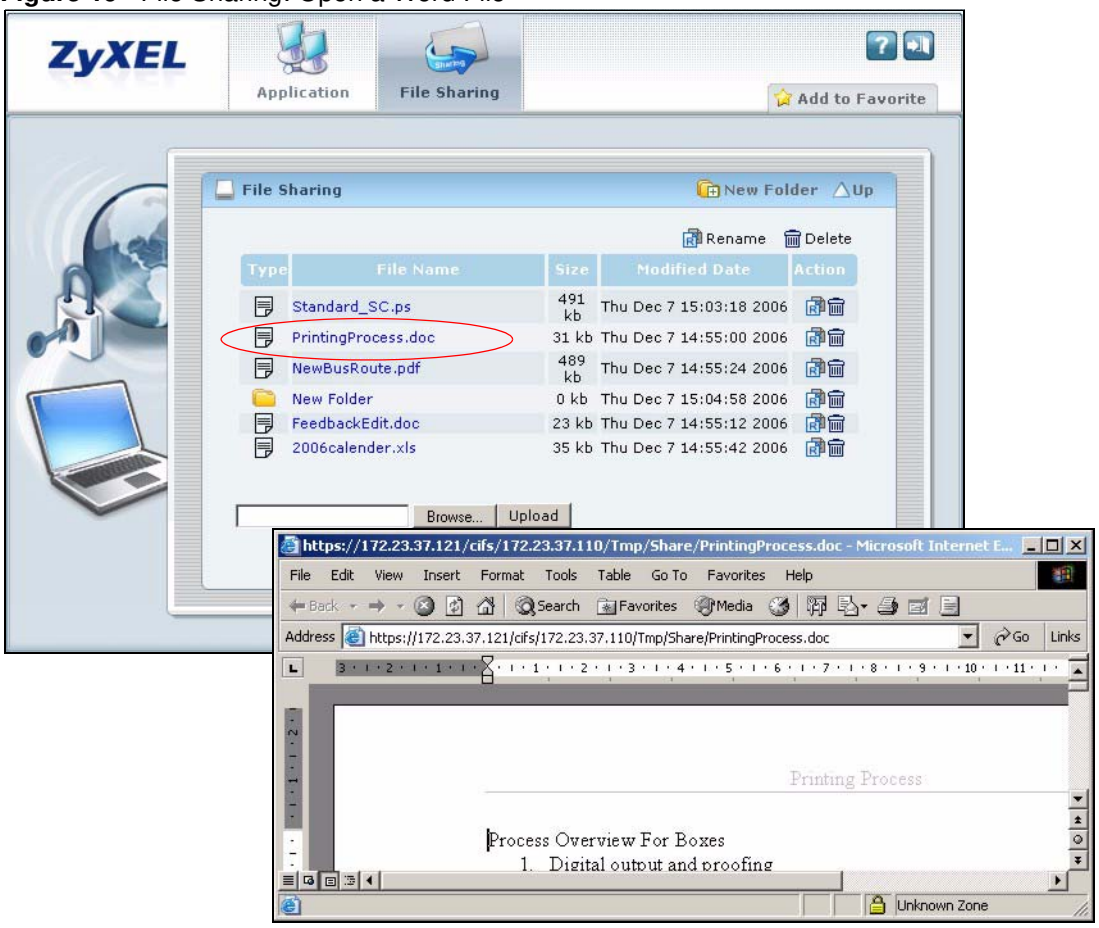
Figure 18 File Sharing: Enter Access User Name and Password



4 A list of files/folders displays. Click on a file to open it in a separate browser window. You can also click a folder to access it.

For this example, click on a .doc file to open the Word document.

Figure 19 File Sharing: Open a Word File



3.3.1 Downloading a File

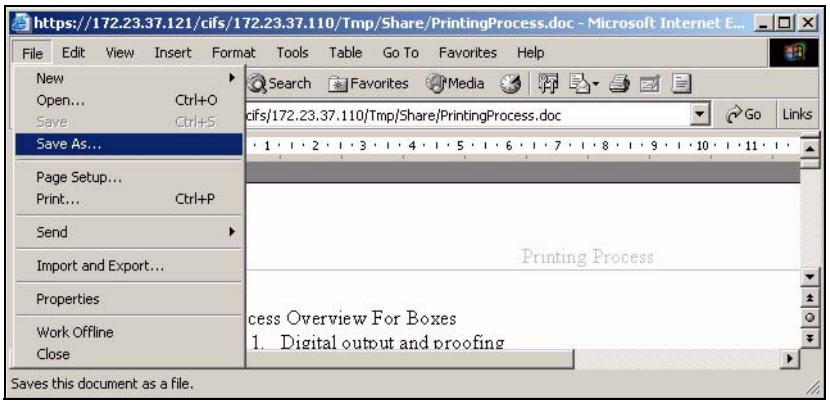
You are prompted to download a file which cannot be opened using a web browser.

You can follow the on-screen instruction to download and save the file to your computer. Then launch the associated application to open the file.

3.3.2 Saving a File

After you have opened a file in a web browser, you can save a copy of the file by clicking **File > Save As** and follow the on-screen instruction.

Figure 20 File Sharing: Save a Word File



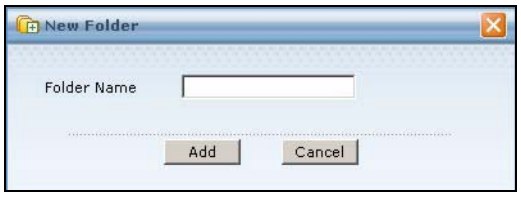
3.4 Creating a New Folder

To create new folder in the file share location, click the **New Folder** icon.

Specify a descriptive name for the folder. You can enter up to 128 characters (“a-z”, “A-Z”, “0-9”, “-”, “_”, with spaces allowed). Then click **Add**.

Make sure the length of the folder name does not exceed the maximum allowed on the file server.

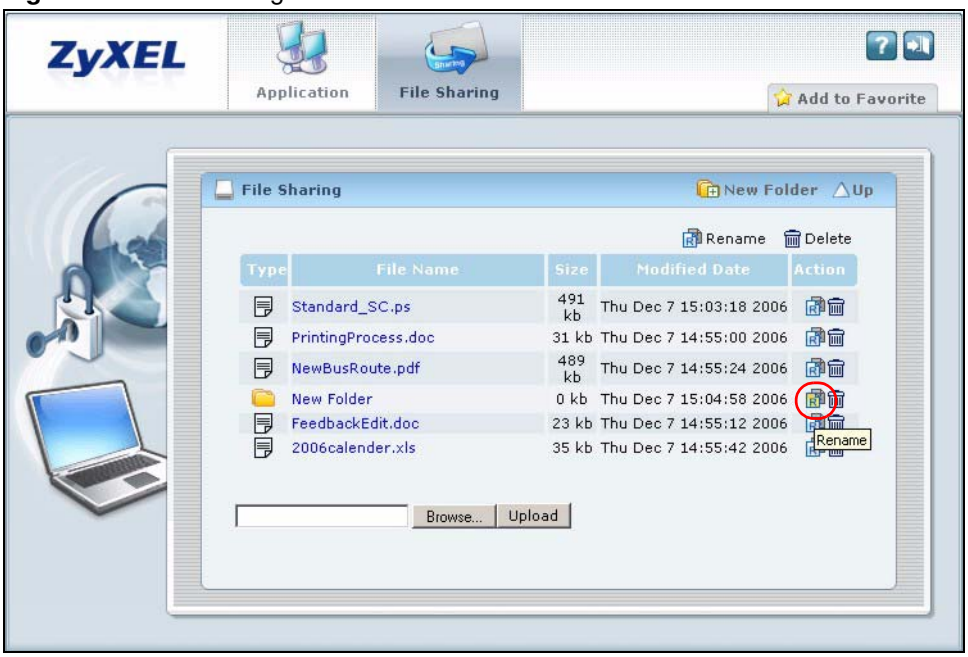
Figure 21 File Sharing: Save a Word File



3.5 Renaming a File or Folder

To rename a file or folder, click the **Rename** icon next to the file/folder.

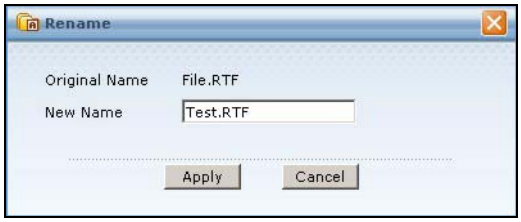
Figure 22 File Sharing: Rename



A popup window displays. Specify the new name and/or file extension in the field provided. You can enter up to 128 characters (“a-z”, “A-Z”, “0-9”, “-”, “_”, with spaces allowed). Then click **Apply**.

Make sure the length of the name does not exceed the maximum allowed on the file server.
You may not be able to open a file if you change the file extension.

Figure 23 File Sharing: Rename



3.6 Deleting a File or Folder

To delete a file or folder, click the Delete icon next to the file/folder and then OK in a prompt screen that displays.

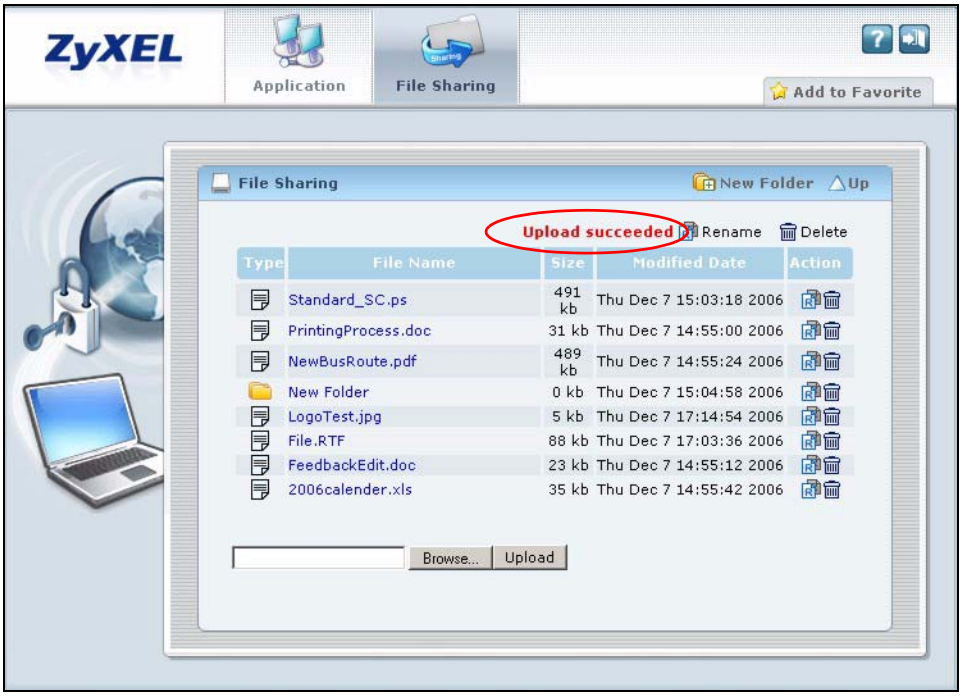
Figure 24 File Sharing: Delete Prompt

3.7 Uploading a File

Follow the steps below to upload a file to the file server.

1. Log into the remote user screen and click the **File Sharing** tab.
2. Specify the location and/or name of the file you want to upload. Or click **Browse** to locate it.
3. Click **Upload** to send the file to the file server.
4. After the file is uploaded successfully, you should see the name of the file and the message in the screen.

Figure 25 File Sharing: File Upload



Uploading a files with the same name and file extension replaces the existing file on the file server. No warning message is displayed.

4

ZyWALL SecuExtender

The ZyWALL automatically loads the ZyWALL SecuExtender client program to your computer after a successful login. The ZyWALL SecuExtender lets you:

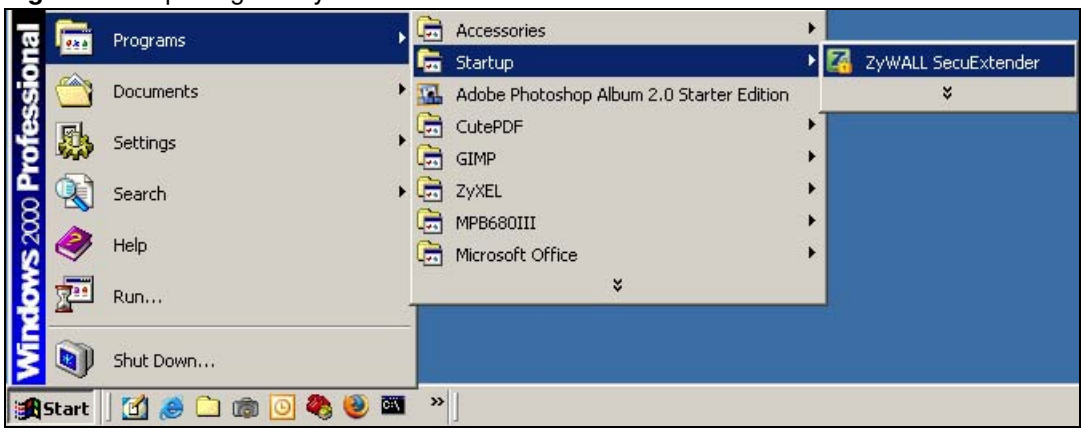
- Access servers, remote desktops and manage files as if you were on the local network.
- Use applications like e-mail, file transfer, and remote desktop programs directly without using a browser. For example, you can use Outlook for e-mail instead of the ZyWALL's web-based e-mail.
- Use applications, even proprietary applications, for which the ZyWALL does not offer SSL application objects.

The applications must be installed on your computer. For example, to use the VNC remote desktop program, you must have the VNC client installed on your computer.

4.1 Connecting Using the ZyWALL SecuExtender

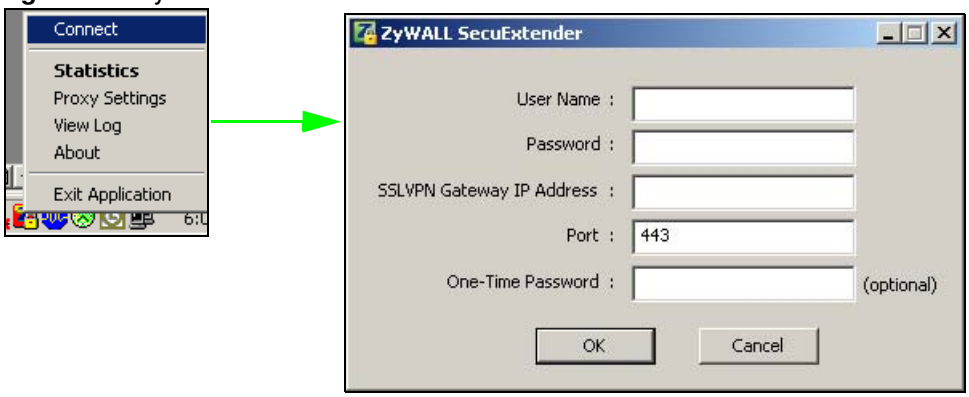
1 If the ZyWALL SecuExtender icon is not already displayed in the system tray, click **Start > Programs > Startup > ZyWALL SecuExtender** to open it.

Figure 26 Opening the ZyWALL SecuExtender



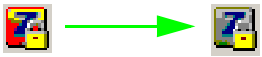
2 Right-click the ZyWALL SecuExtender icon in the system tray and select **Connect** to open the **Connect** screen. Use this screen to access and log into the network through the ZyWALL.

Figure 27 ZyWALL SecuExtender Connect Screen



3 The ZyWALL SecuExtender icon color changes from red to gray after the SSL VPN tunnel is built.

Figure 28 ZyWALL SecuExtender Icon

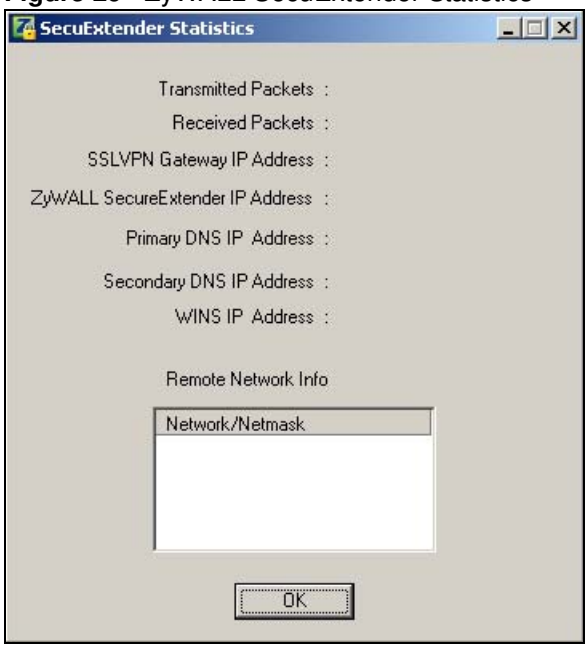


4 Now you can use another application to access resources behind the ZyWALL.

4.2 Statistics

Right-click the ZyWALL SecuExtender icon in the system tray and select **Statistics** to open the **Statistics** screen. Use this screen to view the ZyWALL SecuExtender's statistics.

Figure 29 ZyWALL SecuExtender Statistics



The following table describes the labels in this screen.

Table 2 ZyWALL SecuExtender Statistics

LABEL	DESCRIPTION
Transmitted Packets	This is how many packets the computer has sent through the SSL VPN connection.
Received Packets	This is how many packets the computer has received through the SSL VPN connection.
SSLVPN Gateway IP Address	This is the IP address of the ZyWALL.
ZyWALL SecuExtender IP Address	This is the IP address the ZyWALL assigned to this remote user computer for an SSL VPN connection.
Primary DNS Address	This is the DNS server address for the SSL VPN connection. DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. Your computer uses the DNS server specified here to resolve domain names for resources you access through the SSL VPN connection.
Secondary DNS Address	This is the backup DNS server address for the SSL VPN connection.
WINS IP Address	This is the IP address of the WINS (Windows Internet Naming Service) server for the SSL VPN connection. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Remote Network Info	This is the network (including netmask) that you can access through the SSL VPN connection.
OK	Click **OK** to close the screen.

4.3 Proxy Settings

If the environment to which you connect requires it, you can have the SSL VPN connection from the ZyWALL SecuExtender to the ZyWALL go through an HTTPS proxy server.

Right-click the ZyWALL SecuExtender icon in the system tray and select **Proxy Settings** to open the **Proxy Settings** screen. Use this screen to configure the ZyWALL SecuExtender to use an HTTPS proxy server.

Figure 30 Proxy Settings

The following table describes the labels in this screen.

Table 3 Proxy Settings

LABEL	DESCRIPTION
Enable Proxy	Select this to use HTTPS proxy for the SSL VPN connection to the ZyWALL.
Use IE's Proxy Settings	Click this if you have already configured the settings for using HTTPS proxy in Internet Explorer. Otherwise fill in the fields below.
IP Address	Specify the IP address of the HTTPS proxy server.
Port	Specify the HTTPS proxy server's listening port number.
User Name	Enter your user name for using the HTTPS proxy server.
Password	Enter your password for using the HTTPS proxy server.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to close the screen.

4.4 View Log

If you have problems with the ZyWALL SecuExtender, customer support may request you to provide information from the log. Right-click the ZyWALL SecuExtender icon in the system tray and select **View Log** to open a notepad file of the ZyWALL SecuExtender's log.

Figure 31 ZyWALL SecuExtender Log

```
[24/11/2008-18:04:26] checking status of service as the user has admin
privilege
[24/11/2008-18:04:48] Error in HttpQuerycookie :12002
[24/11/2008-18:04:48] Unable to get Cookie information.
[24/11/2008-18:06:32] LoginAndConnect() Failed
[24/11/2008-18:09:29] INITDIALOG of UserDlg and setting defaults
[24/11/2008-18:37:59] checking status of service as the user has admin
privilege
[24/11/2008-18:38:53] Error occured while sending the request, Error code:
12038, Ignoring...
[24/11/2008-18:38:53] Error Description: SSL certificate common name (host
name field) is incorrect
[24/11/2008-18:38:53] Error in HttpQuerycookie :0
[24/11/2008-18:38:53] cookie from tray :d398c6f690a7af3b34bc98d2023e3ac5
[24/11/2008-18:38:53] login success
[24/11/2008-18:38:53] Creating sslPrg SUCCESS
[24/11/2008-18:38:53] Winsock successfully initiated in FtmTray
[24/11/2008-18:38:53] Port number of progbar: 2681
[24/11/2008-18:38:53] TRAY Reading UDP port from registry: count 0
[24/11/2008-18:38:53] Logged in user has admin privileges
[24/11/2008-18:38:53] Received port from registry is: 1027
[24/11/2008-18:38:53] Progbar successfully set port num to registry
[24/11/2008-18:38:53] Socket created successfully in FtmTray
```

PART II Troubleshooting, Appendices and Index

The appendices provide general networking information. Some information may not apply to your ZyWALL.

5

Troubleshooting

This chapter provides tips to solve common problems. You should contact your network administrator if a problem persists.

I forgot my account user name and/or password.

- Your account information is provided by your network administrator. If you have forgotten this information, contact your network administrator for assistance.

I cannot see or access the **Login** screen in the web configurator.

1. Make sure you enter the correct IP address or domain name of the ZyWALL. Check with your network administrator to verify this information.
2. Make sure your computer meets the system requirements. See Section 1.1.2 on page 16.
3. Make sure your computer meets any other requirements specified by your network administrator. This may include the version of your operating system, service pack, etc.
4. If there is a DHCP server on your network, make sure your computer is using a dynamic IP address.
5. If the problem continues, contact the network administrator.

I can see the **Login** screen, but I cannot log in to the ZyWALL.

- Make sure you have entered the user name and password exactly as provided by your network administrator. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- You cannot log in to the web configurator if someone has already logged in using the same user account. In this case, inform that person to log out or contact your network administrator for assistance.

The connection is slow or intermittent.

- Transmission speed varies depending on your network connection to the ZyWALL and the traffic load. Check with your network administrator and ask for more bandwidth assigned to you.

I cannot access a web site (on Mondays).

- Check that the web site is available for access.
- Check that the network administrator has not blocked you from accessing the web site during specific times.

I cannot access a non-web based application.

- Check that the application is available for access.
- Make sure you have following the instruction in the pop-up information window to access the application.
- If required, make sure you enter the access account information correctly.

I cannot access a file share.

- Check that the file server is configured properly and is available for access.
- If required, make sure you enter the access account information correctly.
- Contact your network administrator for assistance if the problem persists.

I cannot open a file.

- If your web browser cannot open a file, you are prompted to download it to your computer. You can then launch the appropriate application to open the file.

I cannot rename/delete/upload a file and/or folder.

- You must have read/write access rights for the file share. Check with your network administrator for this information.

A

Setting Up Your Computer's IP Address

Your specific ZyXEL device may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

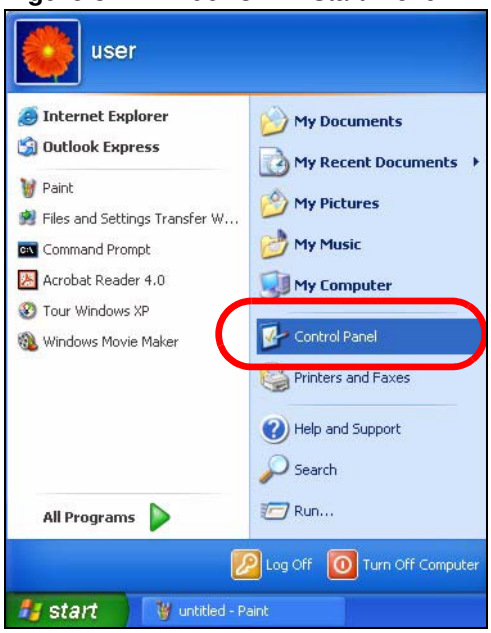
In this appendix, you can set up an IP address for:

Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

1 Click **Start** > **Control Panel**.

Figure 32 Windows XP: Start Menu

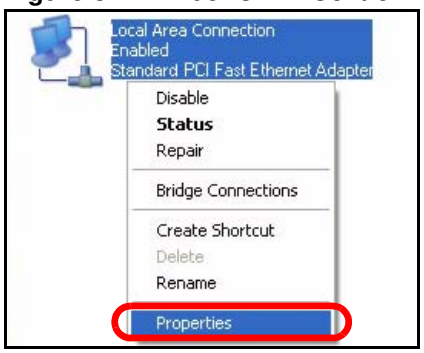


2 In the **Control Panel**, click the **Network Connections** icon.

Figure 33 Windows XP: Control Panel

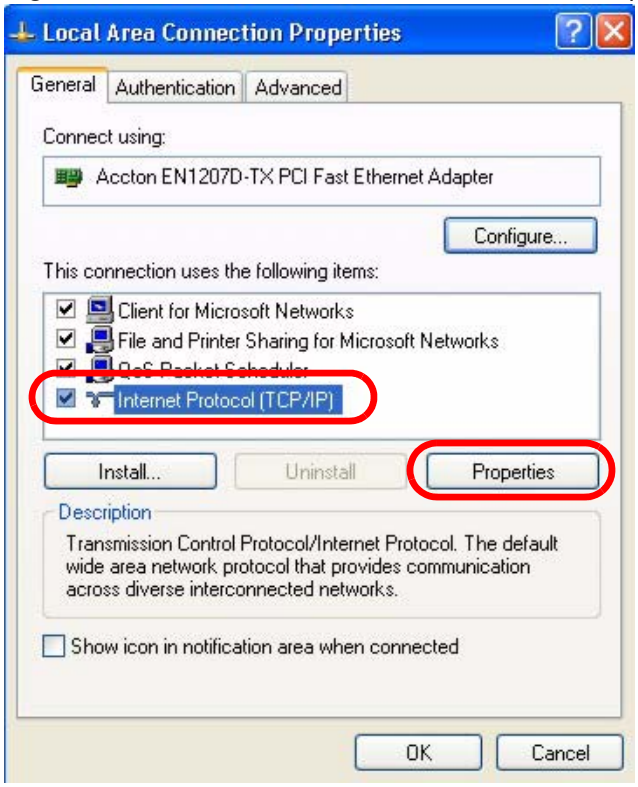
3 Right-click **Local Area Connection** and then select **Properties**.

Figure 34 Windows XP: Control Panel > Network Connections > Properties



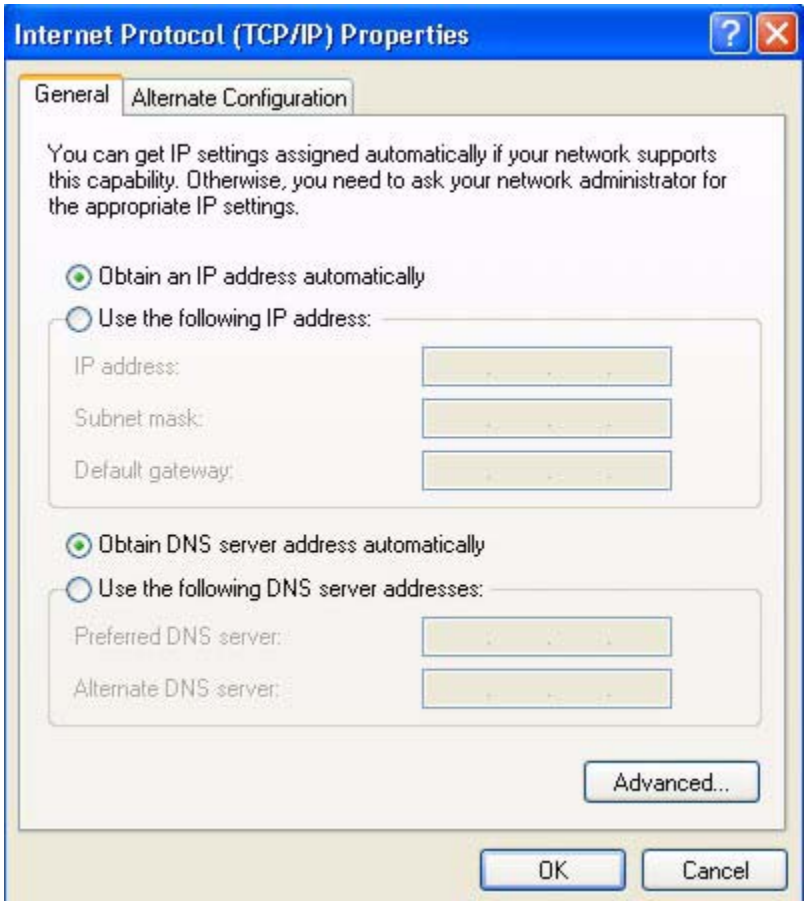
4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

Figure 35 Windows XP: Local Area Connection Properties



5 The **Internet Protocol TCP/IP Properties** window opens.

Figure 36 Windows XP: Internet Protocol (TCP/IP) Properties



6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.

7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start > All Programs > Accessories > Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

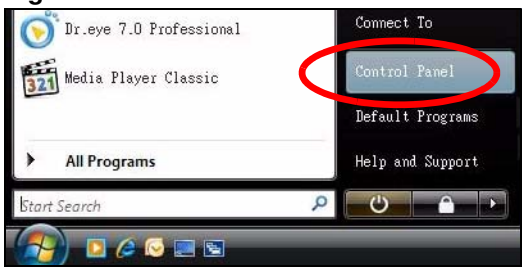
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows Vista

This section shows screens from Windows Vista Professional.

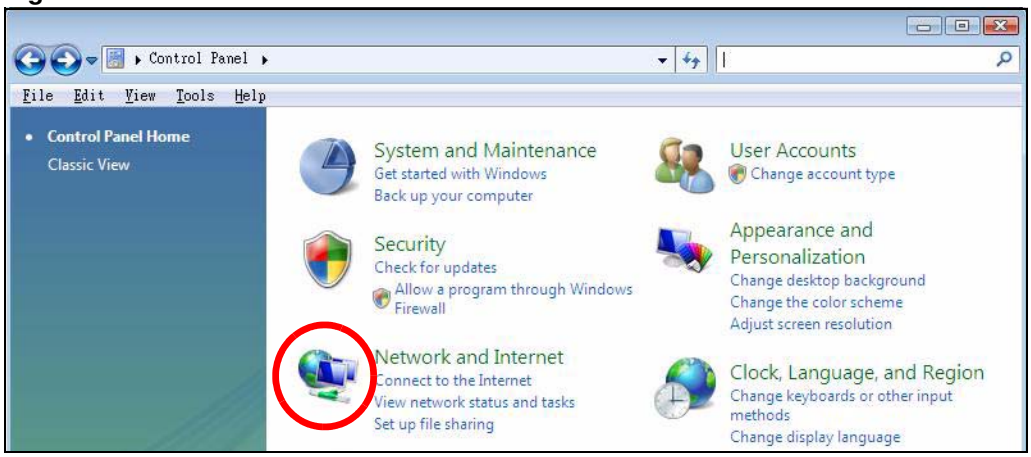
1 Click **Start** > **Control Panel**.

Figure 37 Windows Vista: Start Menu



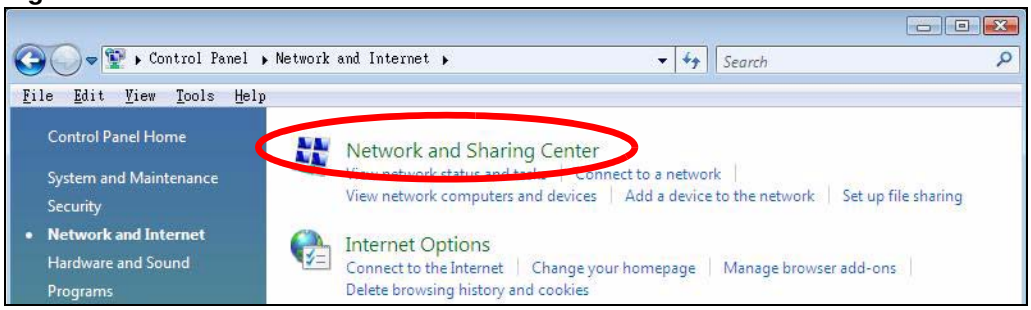
2 In the **Control Panel**, click the **Network and Internet** icon.

Figure 38 Windows Vista: Control Panel



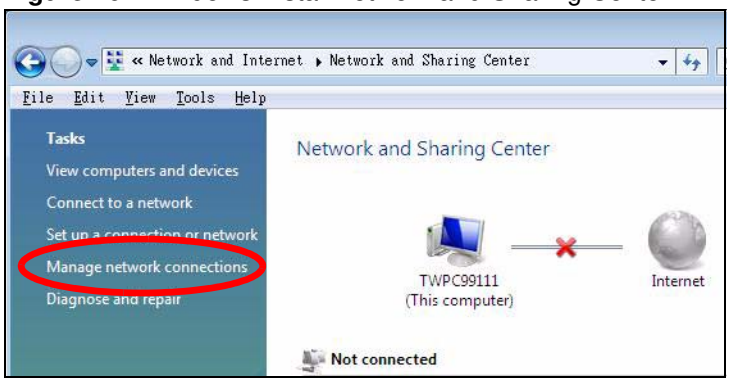
3 Click the **Network and Sharing Center** icon.

Figure 39 Windows Vista: Network And Internet



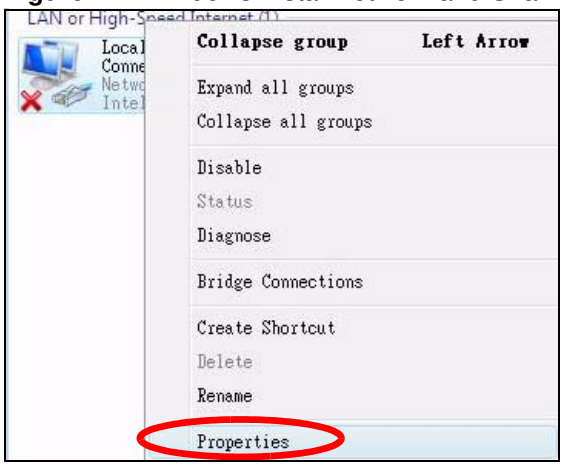
4 Click **Manage network connections**.

Figure 40 Windows Vista: Network and Sharing Center



5 Right-click **Local Area Connection** and then select **Properties**.

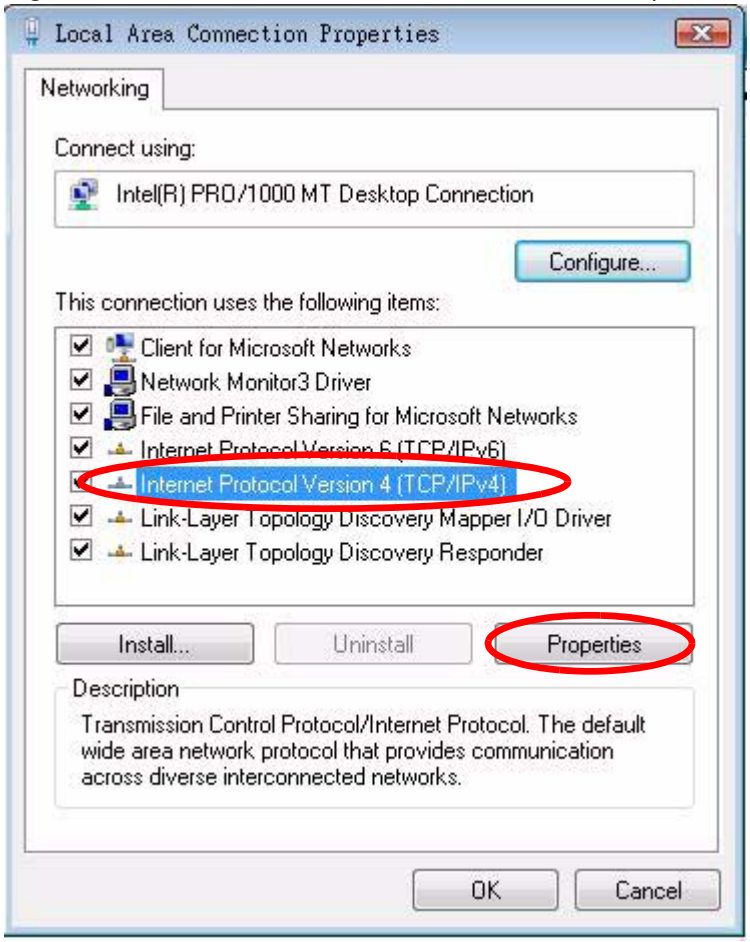
Figure 41 Windows Vista: Network and Sharing Center



During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

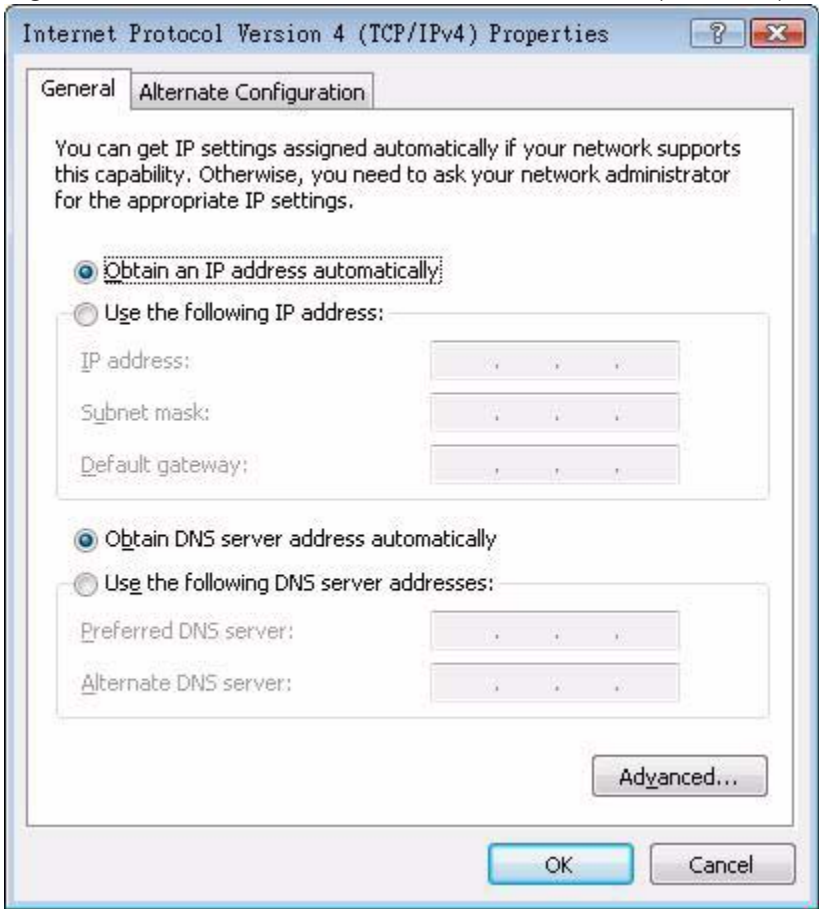
6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 42 Windows Vista: Local Area Connection Properties



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 43 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.Click **Advanced**.

9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start > All Programs > Accessories > Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

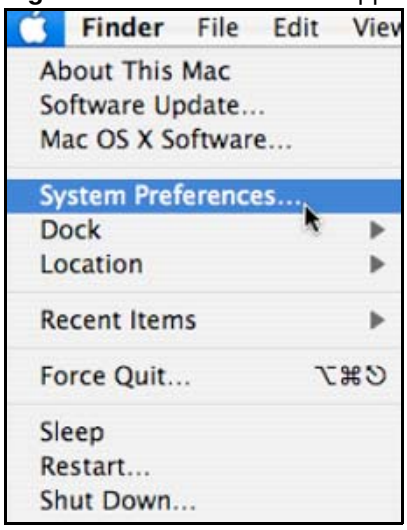
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Mac OS X: 10.3 and 10.4

The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

1 Click **Apple** > **System Preferences**.

Figure 44 Mac OS X 10.4: Apple Menu

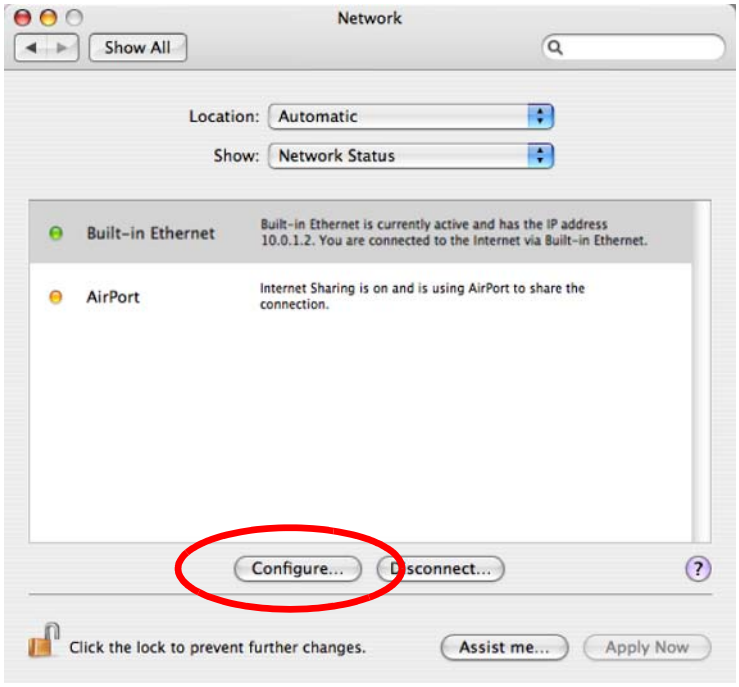


2 In the **System Preferences** window, click the **Network** icon.

Figure 45 Mac OS X 10.4: System Preferences

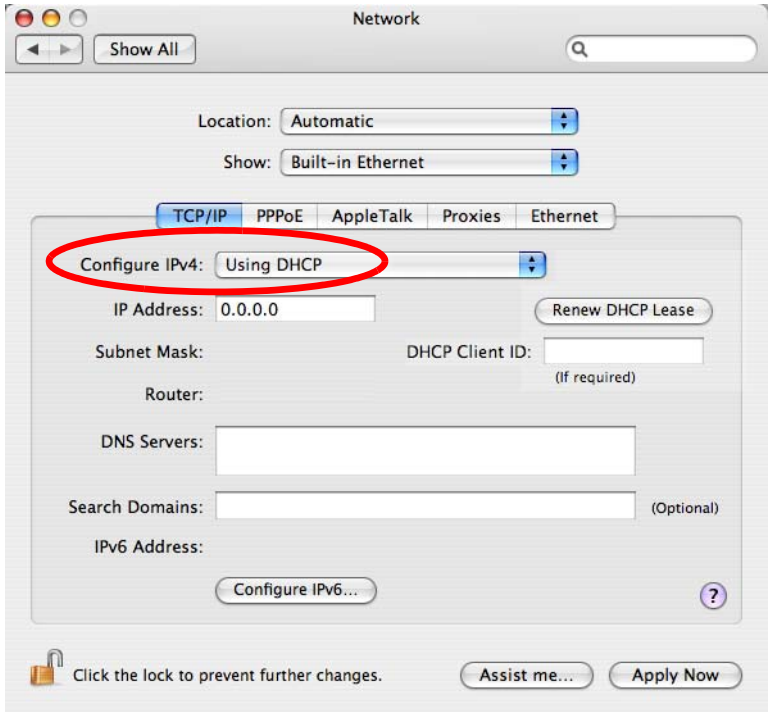
3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure.**

Figure 46 Mac OS X 10.4: Network Preferences



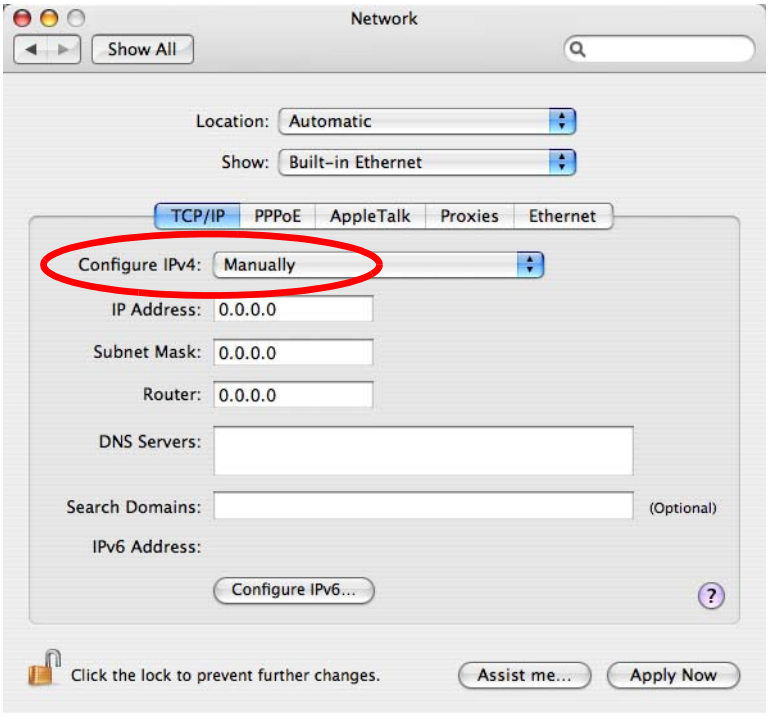
4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.

Figure 47 Mac OS X 10.4: Network Preferences > TCP/IP Tab.



5 For statically assigned settings, do the following:
- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.
- In the **Subnet Mask** field, type your subnet mask.
- In the **Router** field, type the IP address of your device.

Figure 48 Mac OS X 10.4: Network Preferences > Ethernet

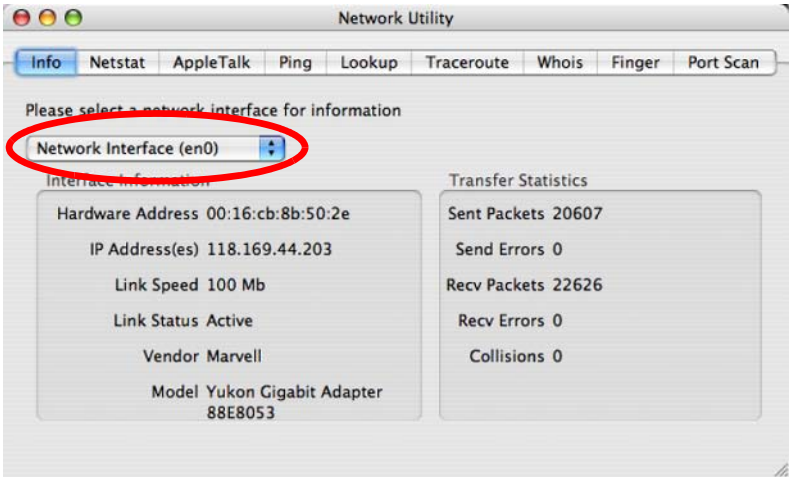


Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

Figure 49 Mac OS X 10.4: Network Utility

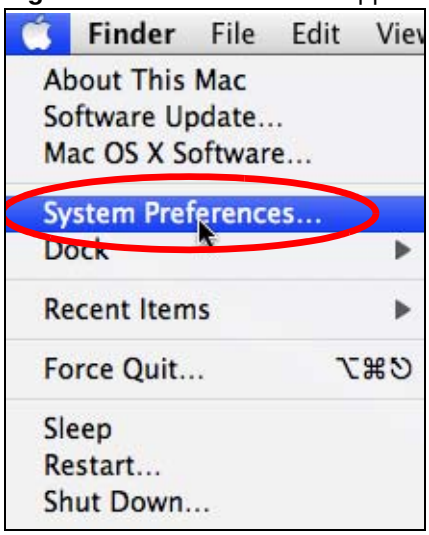


Mac OS X: 10.5

The screens in this section are from Mac OS X 10.5.

1 Click **Apple** > **System Preferences**.

Figure 50 Mac OS X 10.5: Apple Menu

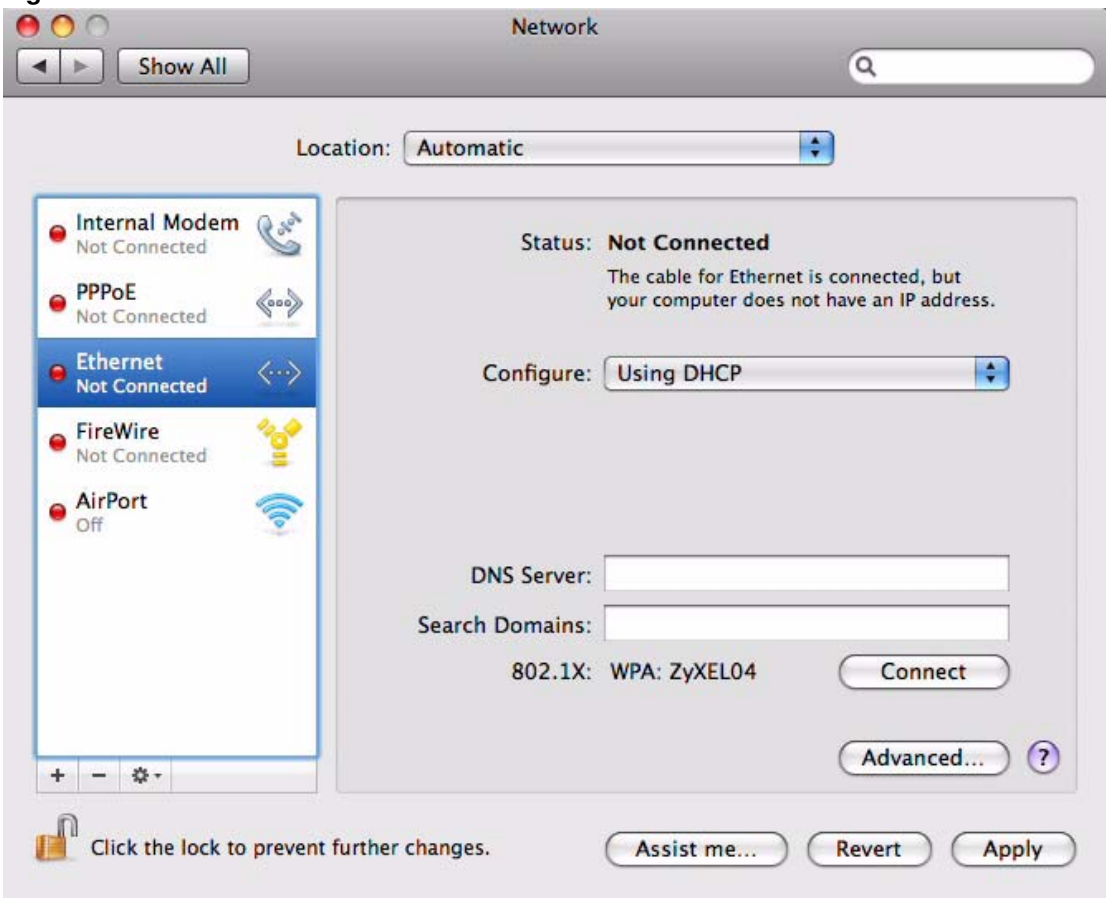


2 In **System Preferences**, click the **Network** icon.

Figure 51 Mac OS X 10.5: Systems Preferences

3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.

Figure 52 Mac OS X 10.5: Network Preferences > Ethernet

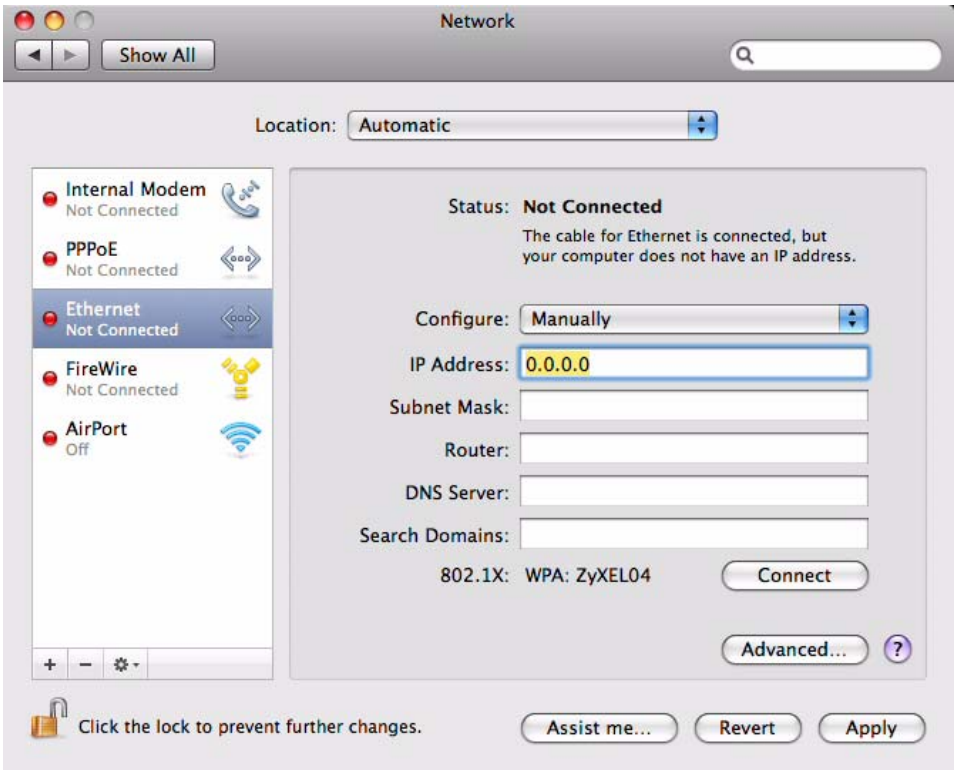


4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.
- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.
- In the **Router** field, enter the IP address of your ZyWALL.

Figure 53 Mac OS X 10.5: Network Preferences > Ethernet

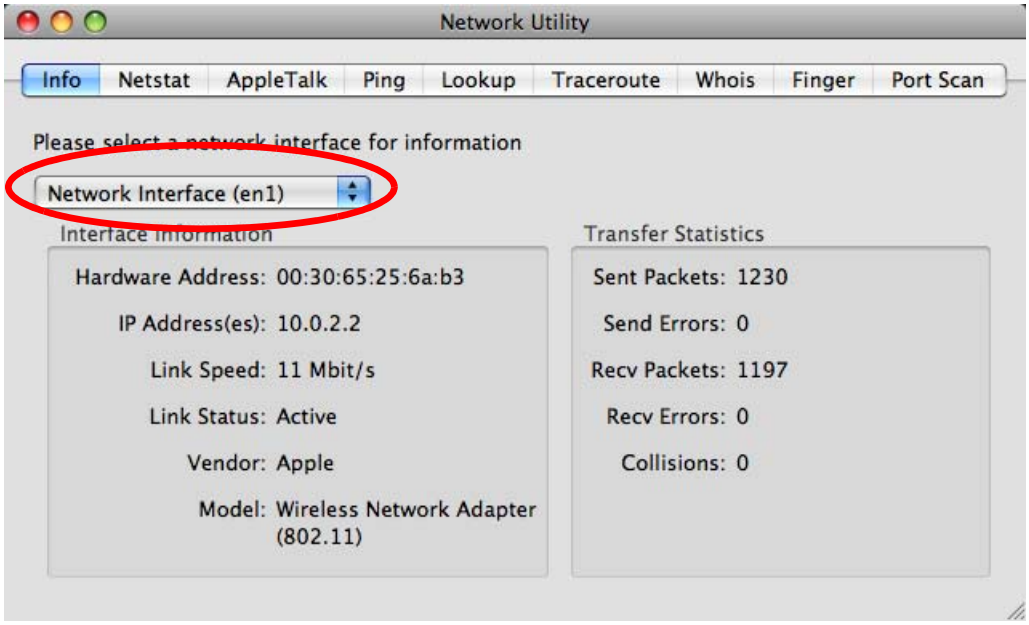


6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 54 Mac OS X 10.5: Network Utility



Linux: Ubuntu 8 (GNOME)

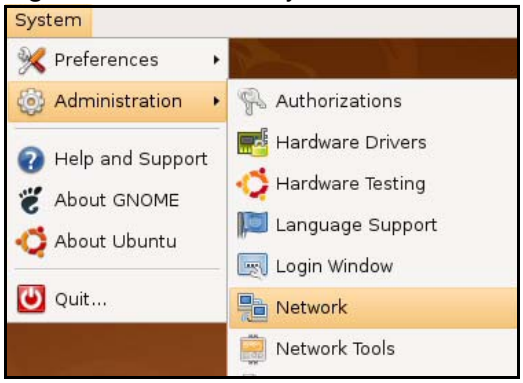
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

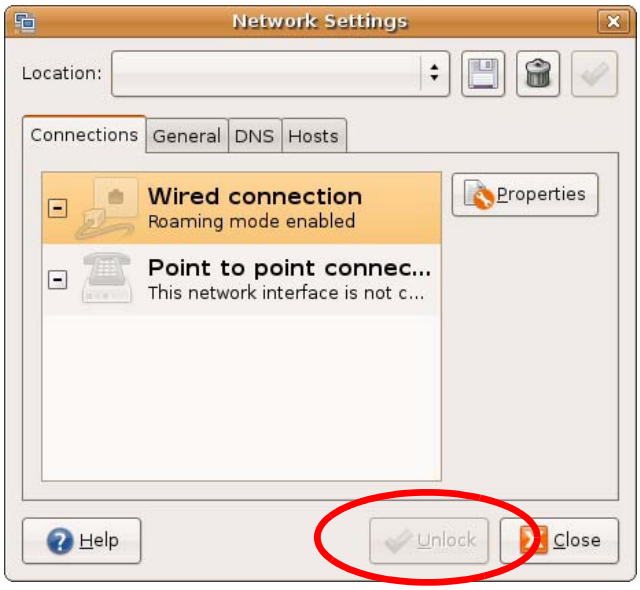
1 Click **System > Administration > Network**.

Figure 55 Ubuntu 8: System > Administration Menu



2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.

Figure 56 Ubuntu 8: Network Settings > Connections



3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

Figure 57 Ubuntu 8: Administrator Account Authentication

4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

Figure 58 Ubuntu 8: Network Settings > Connections

5 The **Properties** dialog box opens.

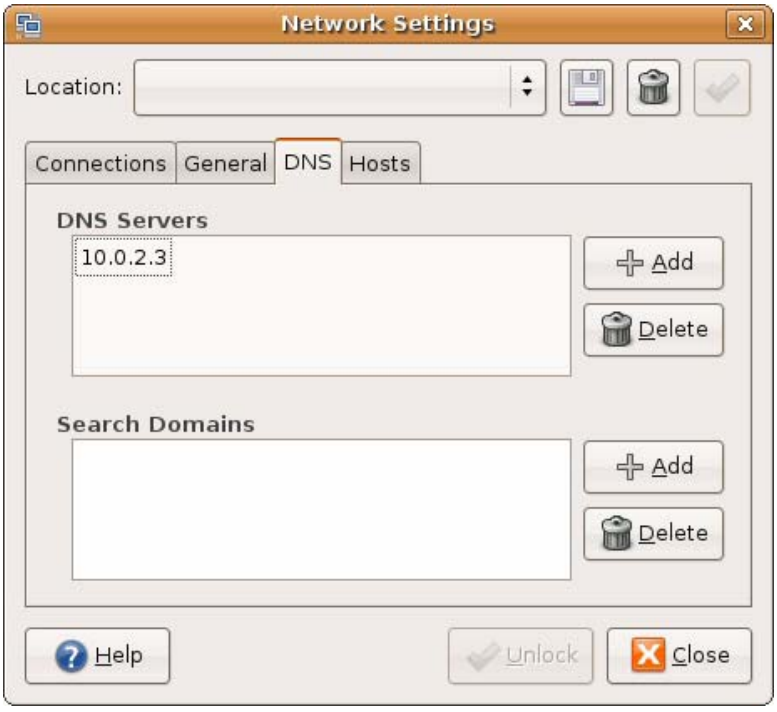
Figure 59 Ubuntu 8: Network Settings > Properties

- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

Figure 60 Ubuntu 8: Network Settings > DNS

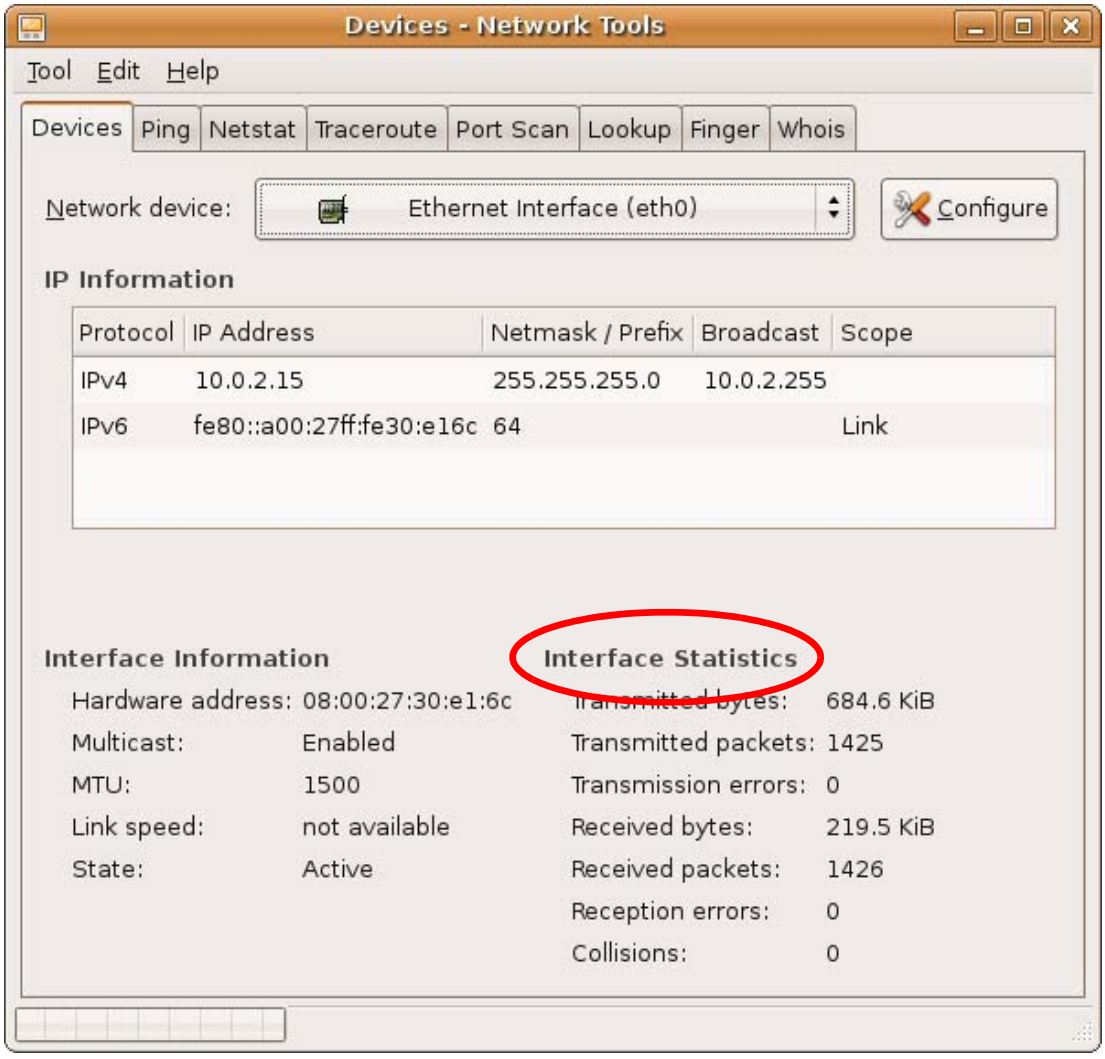


8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices** tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 61 Ubuntu 8: Network Tools



Linux: openSUSE 10.3 (KDE)

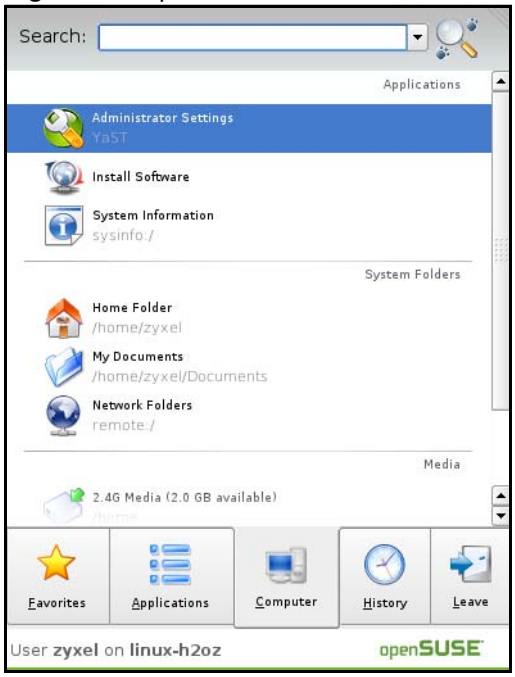
This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in the KDE:

1 Click **K Menu > Computer > Administrator Settings (YaST)**.

Figure 62 openSUSE 10.3: K Menu > Computer Menu

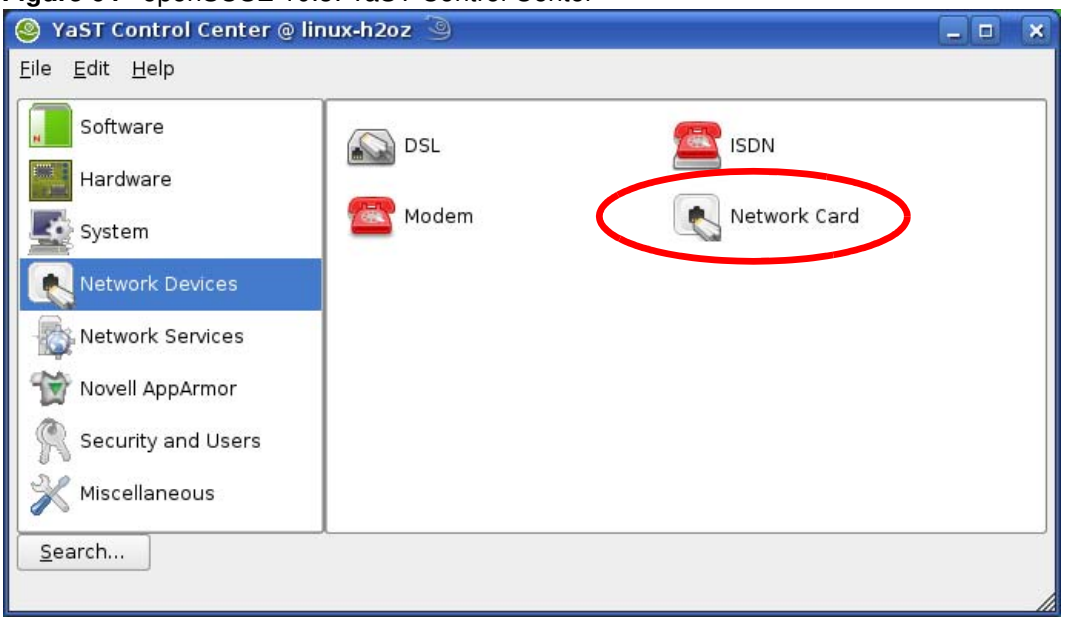


2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

Figure 63 openSUSE 10.3: K Menu > Computer Menu

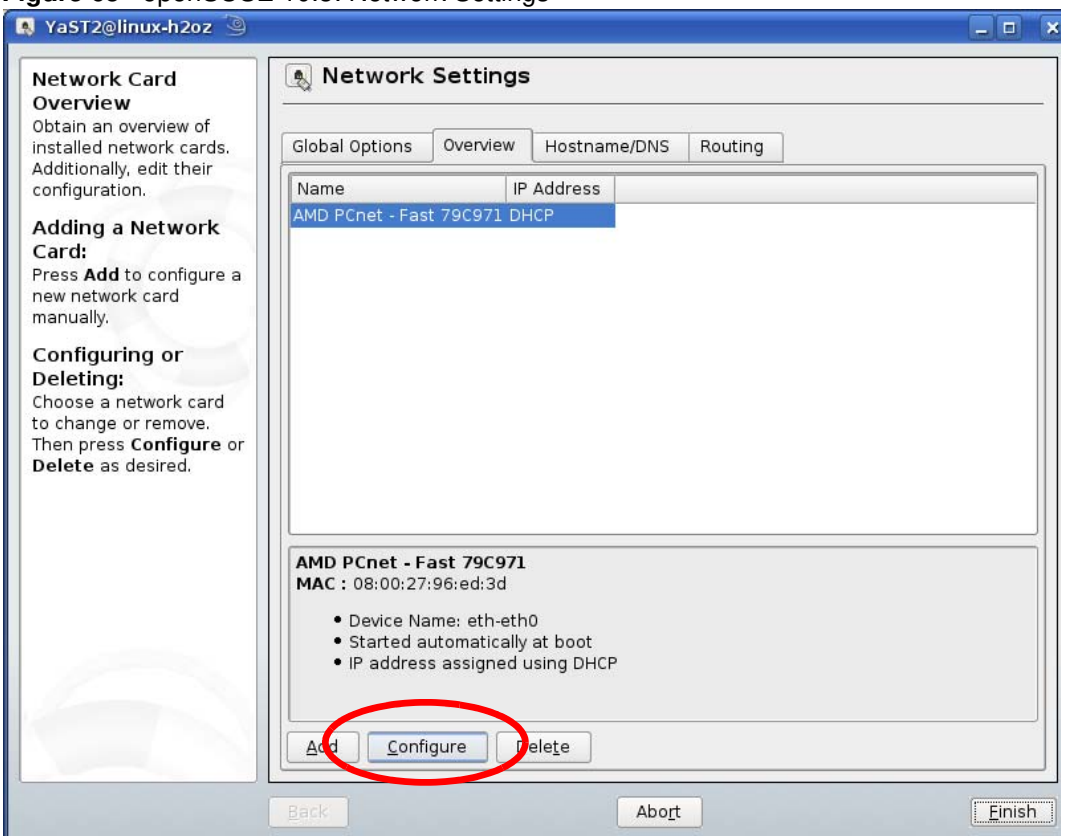
3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

Figure 64 openSUSE 10.3: YaST Control Center



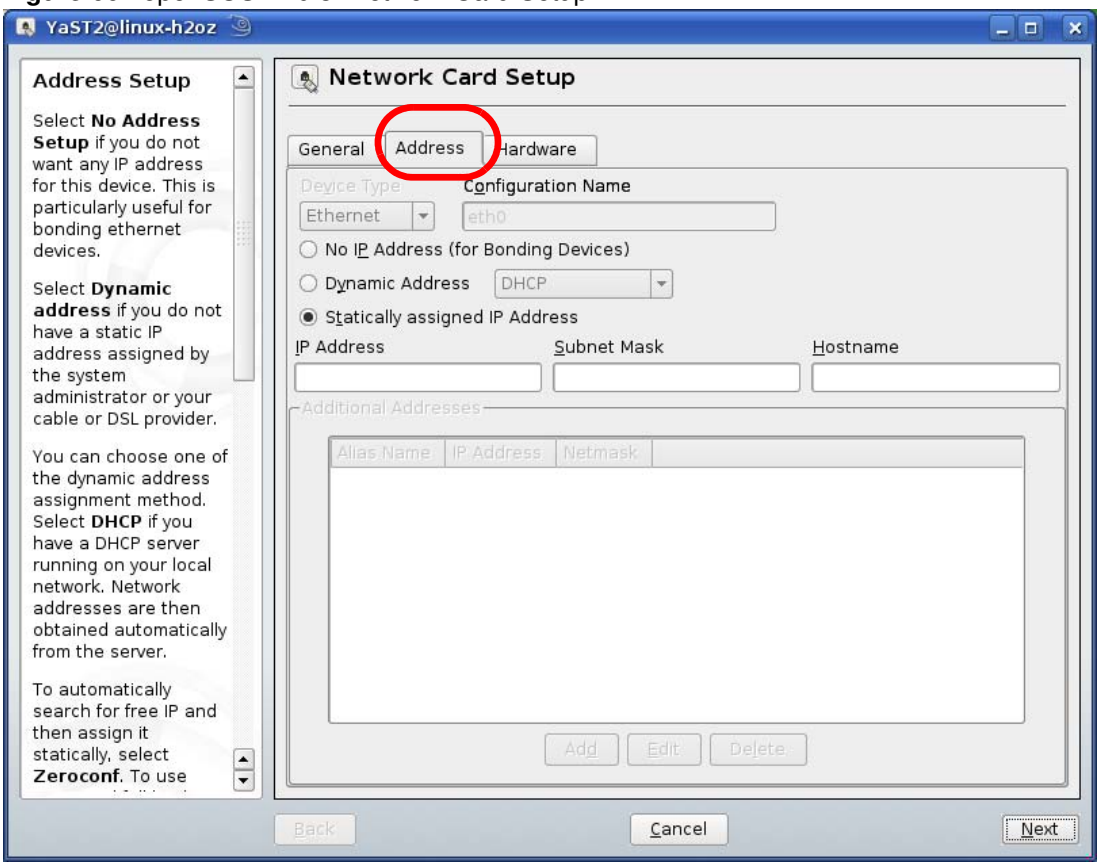
4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

Figure 65 openSUSE 10.3: Network Settings



5 When the **Network Card Setup** window opens, click the **Address** tab

Figure 66 openSUSE 10.3: Network Card Setup

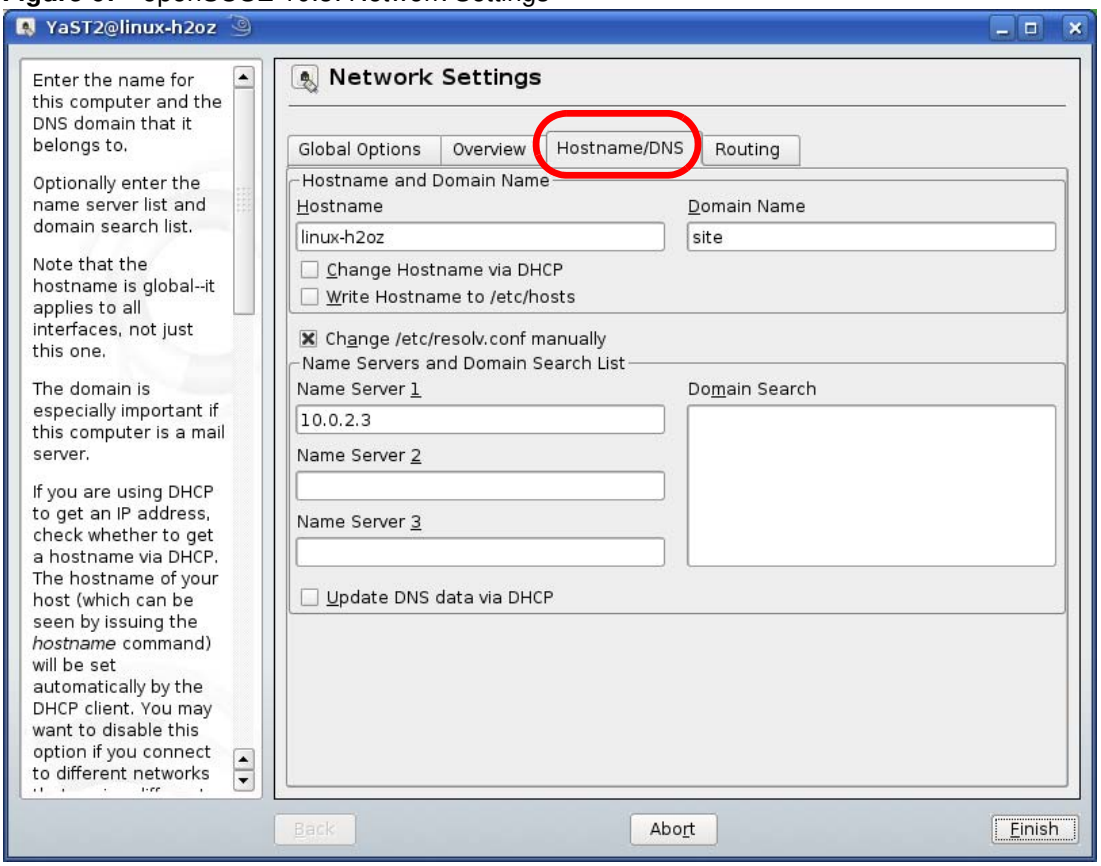


6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.
Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.

7 Click **Next** to save the changes and close the **Network Card Setup** window.

8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

Figure 67 openSUSE 10.3: Network Settings

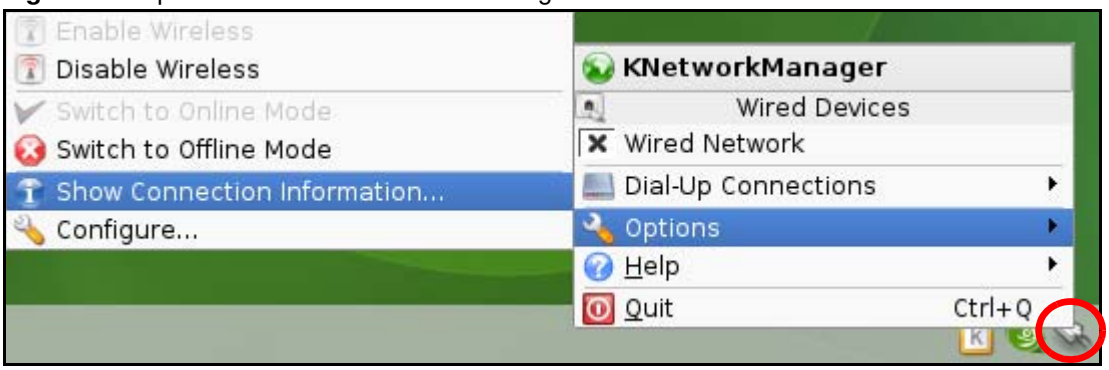


9 Click **Finish** to save your settings and close the window.

Verifying Settings

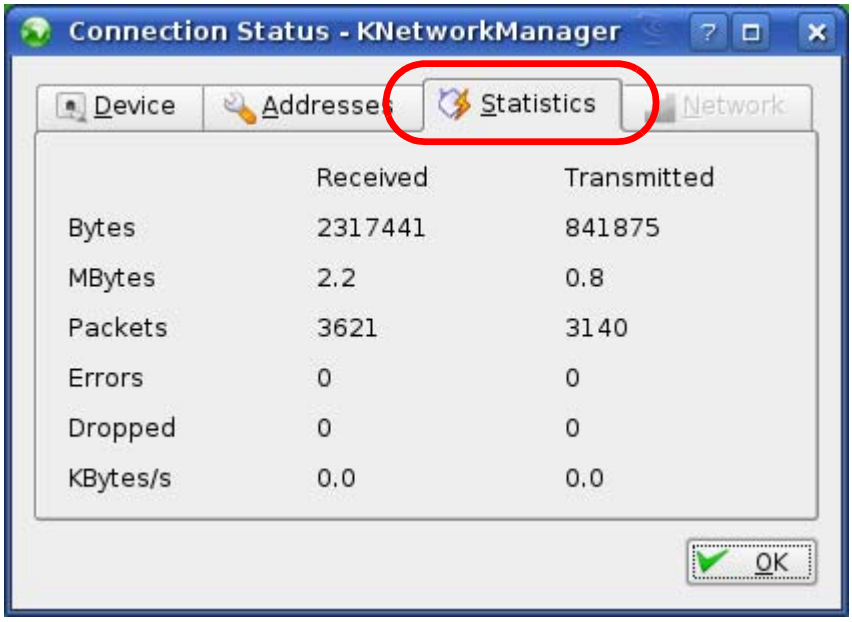
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 68 openSUSE 10.3: KNetwork Manager



When the **Connection Status - KNetwork Manager** window opens, click the **Statistics tab** to see if your connection is working properly.

Figure 69 openSUSE: Connection Status - KNetwork Manager



B

Importing Certificates

This appendix shows you how to import public key certificates into your web browser.

Public key certificates are used by web browsers to ensure that a secure web site is legitimate. When a certificate authority such as VeriSign, Comodo, or Network Solutions, to name a few, receives a certificate request from a website operator, they confirm that the web domain and contact information in the request match those on public record with a domain name registrar. If they match, then the certificate is issued to the website operator, who then places it on the site to be issued to all visiting web browsers to let them know that the site is legitimate.

Many ZyXEL products, such as the NSA-2401, issue their own public key certificates. These can be used by web browsers on a LAN or WAN to verify that they are in fact connecting to the legitimate device and not one masquerading as it. However, because the certificates were not issued by one of the several organizations officially recognized by the most common web browsers, you will need to import the ZyXEL-created certificate into your web browser and flag that certificate as a trusted authority.

You can see if you are browsing on a secure website if the URL in your web browser's address bar begins with `https://` or there is a sealed padlock icon () somewhere in the main browser window (not all browsers show the padlock in the same location.)

In this appendix, you can import a public key certificate for:

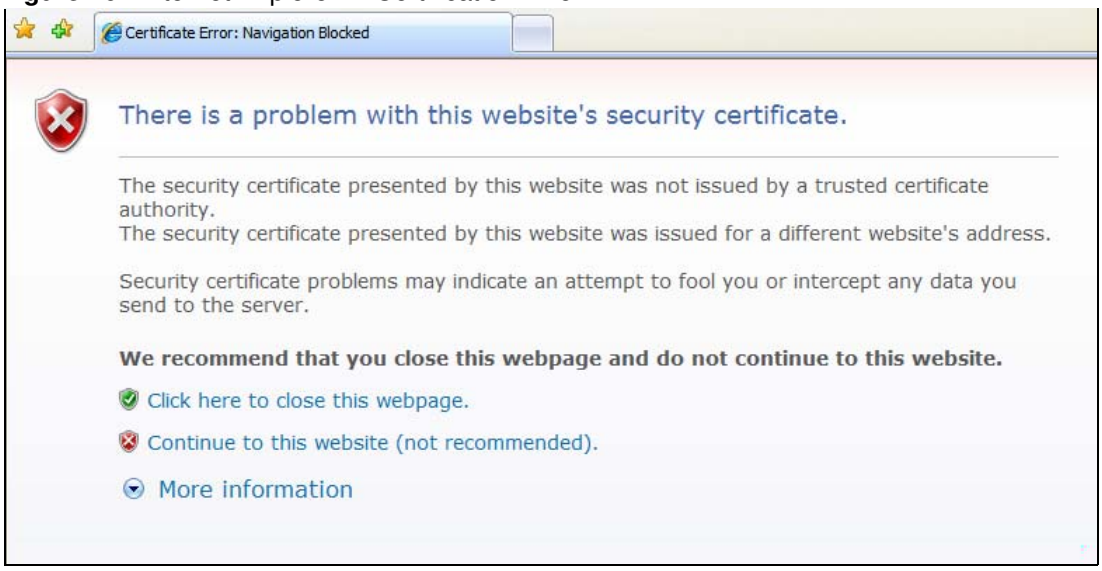
- Internet Explorer on page 70
- Firefox on page 78
- Opera on page 83
- Konqueror on page 89

Internet Explorer

The following example uses Microsoft Internet Explorer 7 on Windows XP Professional; however, they can also apply to Internet Explorer on Windows Vista.

1 If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

Figure 70 Internet Explorer 7: Certification Error

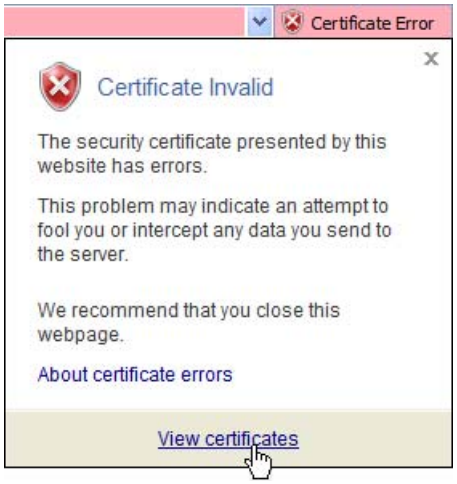


2 Click **Continue to this website (not recommended)**.

Figure 71 Internet Explorer 7: Certification Error

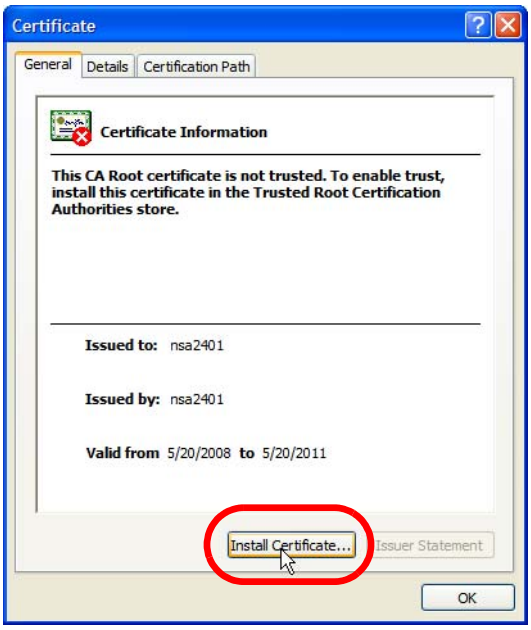
3 In the **Address Bar**, click **Certificate Error** > **View certificates**.

Figure 72 Internet Explorer 7: Certificate Error



4 In the **Certificate** dialog box, click **Install Certificate**.

Figure 73 Internet Explorer 7: Certificate

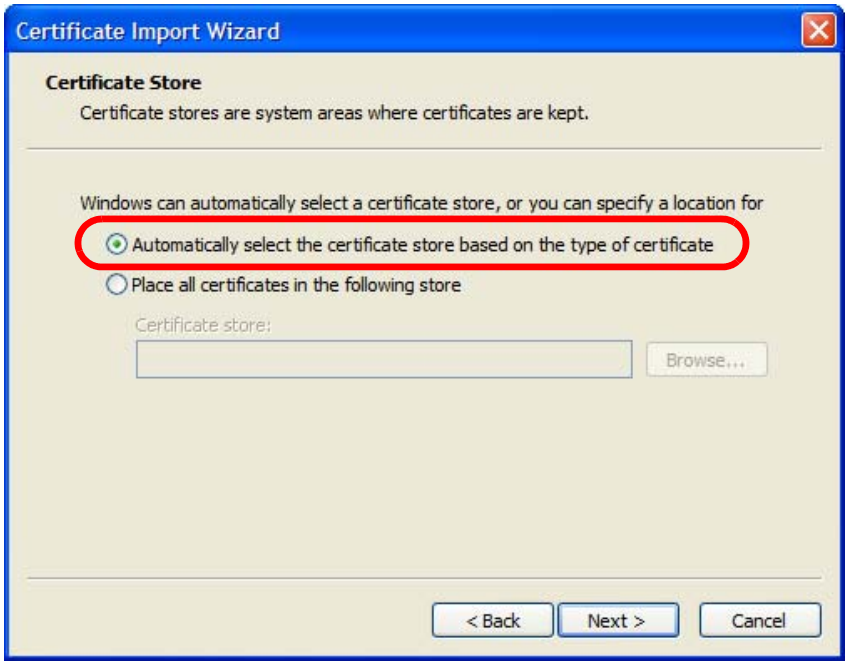


5 In the **Certificate Import Wizard**, click **Next**.

Figure 74 Internet Explorer 7: Certificate Import Wizard

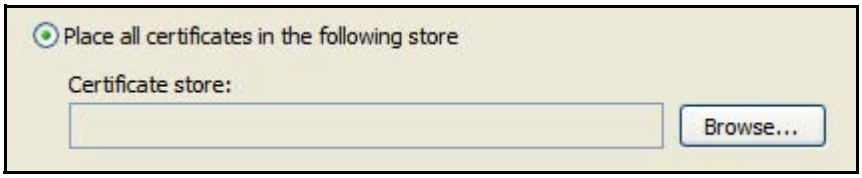
6 If you want Internet Explorer to **Automatically select certificate store based on the type of certificate**, click **Next** again and then go to step 9.

Figure 75 Internet Explorer 7: Certificate Import Wizard



7 Otherwise, select **Place all certificates in the following store** and then click **Browse**.

Figure 76 Internet Explorer 7: Certificate Import Wizard

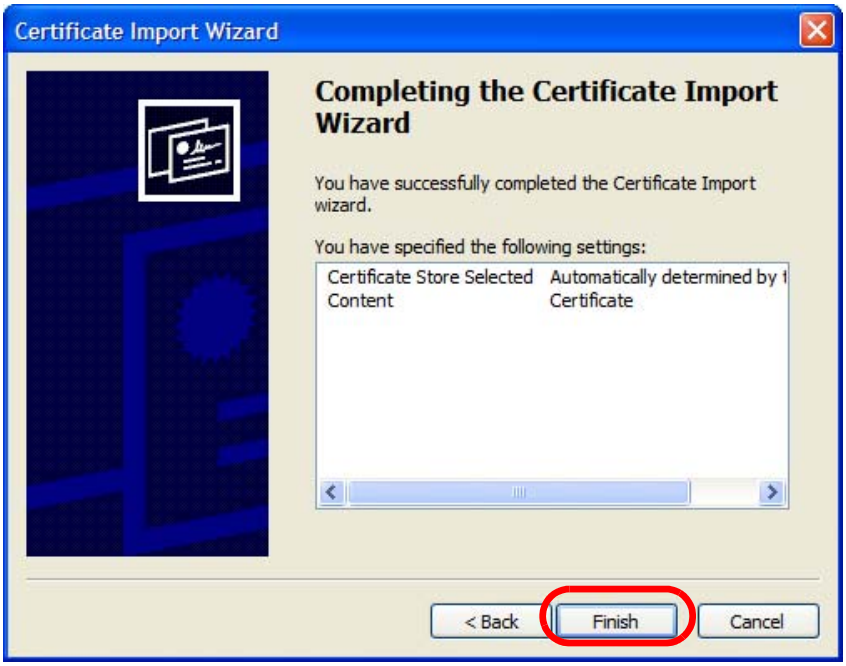


8 In the **Select Certificate Store** dialog box, choose a location in which to save the certificate and then click **OK**.

Figure 77 Internet Explorer 7: Select Certificate Store

9 In the **Completing the Certificate Import Wizard** screen, click **Finish**.

Figure 78 Internet Explorer 7: Certificate Import Wizard



10 If you are presented with another **Security Warning**, click **Yes**.

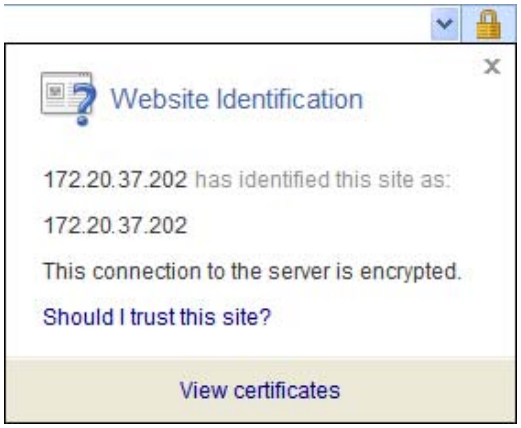
Figure 79 Internet Explorer 7: Security Warning

11 Finally, click **OK** when presented with the successful certificate installation message.

Figure 80 Internet Explorer 7: Certificate Import Wizard

12 The next time you start Internet Explorer and go to a ZyXEL web configurator page, a sealed padlock icon appears in the address bar. Click it to view the page's **Website Identification** information.

Figure 81 Internet Explorer 7: Website Identification



Installing a Stand-Alone Certificate File in Internet Explorer

Rather than browsing to a ZyXEL web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

1 Double-click the public key certificate file.

Figure 82 Internet Explorer 7: Public Key Certificate File

2 In the security warning dialog box, click **Open**.

Figure 83 Internet Explorer 7: Open File - Security Warning

3 Refer to steps 4-12 in the Internet Explorer procedure beginning on page 70 to complete the installation process.

Removing a Certificate in Internet Explorer

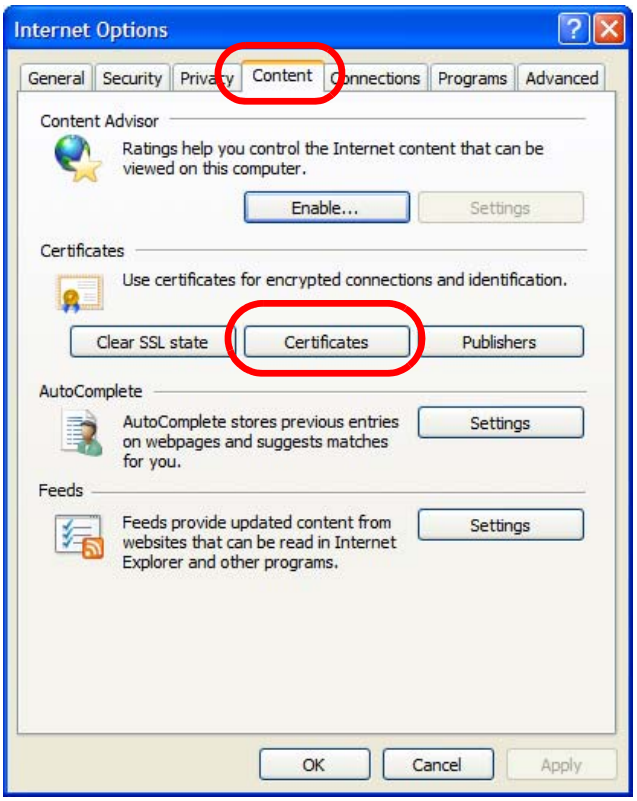
This section shows you how to remove a public key certificate in Internet Explorer 7.

1 Open **Internet Explorer** and click **Tools > Internet Options**.

Figure 84 Internet Explorer 7: Tools Menu

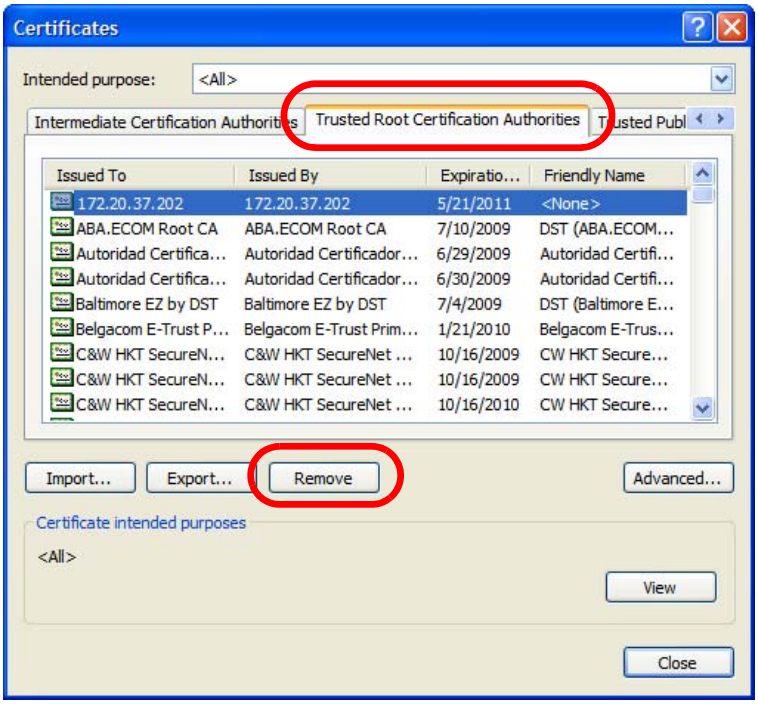
2 In the **Internet Options** dialog box, click **Content** > **Certificates**.

Figure 85 Internet Explorer 7: Internet Options



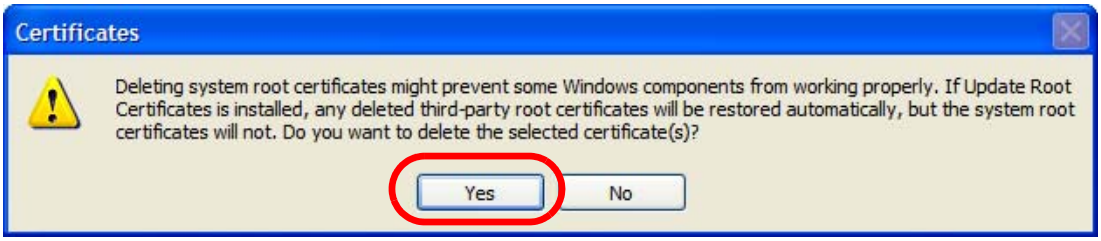
3 In the **Certificates** dialog box, click the **Trusted Root Certificates Authorities** tab, select the certificate that you want to delete, and then click **Remove**.

Figure 86 Internet Explorer 7: Certificates



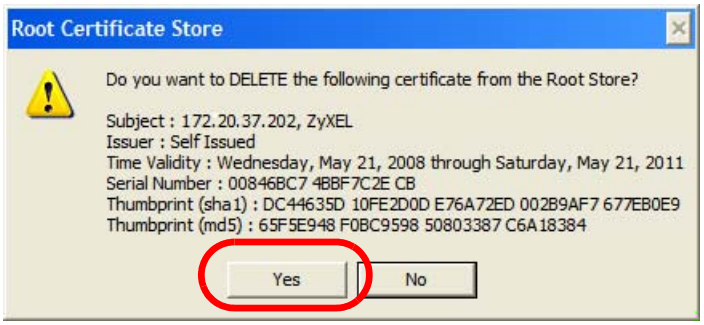
4 In the **Certificates** confirmation, click **Yes**.

Figure 87 Internet Explorer 7: Certificates



5 In the **Root Certificate Store** dialog box, click **Yes**.

Figure 88 Internet Explorer 7: Root Certificate Store



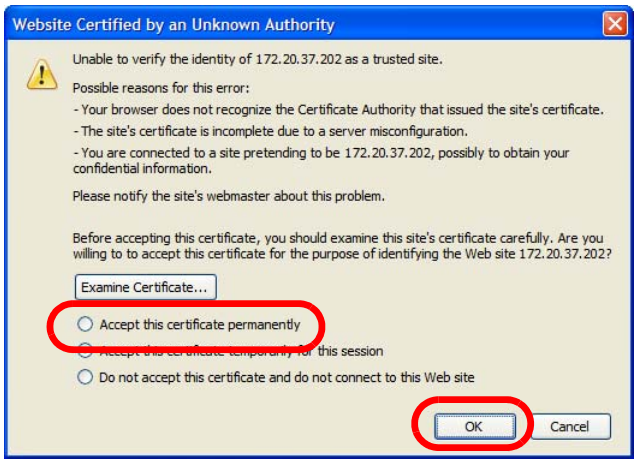
6 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

Firefox

The following example uses Mozilla Firefox 2 on Windows XP Professional; however, the screens can also apply to Firefox 2 on all platforms.

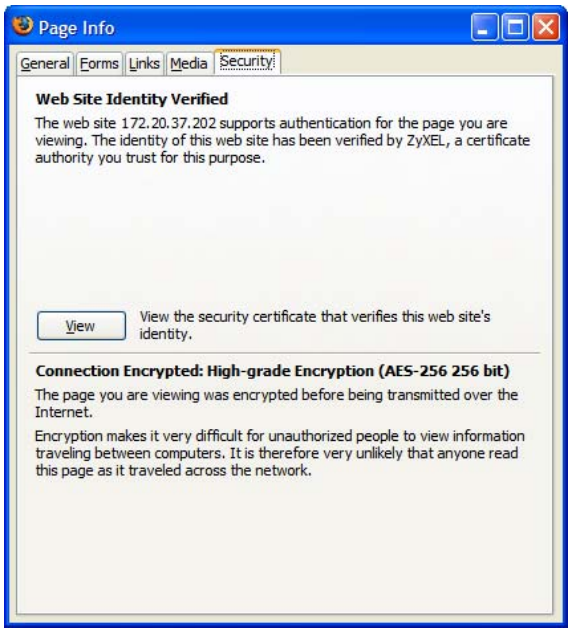
1. If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.
2. Select **Accept this certificate permanently** and click **OK.**

Figure 89 Firefox 2: Website Certified by an Unknown Authority



3. The certificate is stored and you can now connect securely to the web configurator. A sealed padlock appears in the address bar, which you can click to open the **Page Info > Security** window to view the web page's security information.

Figure 90 Firefox 2: Page Info

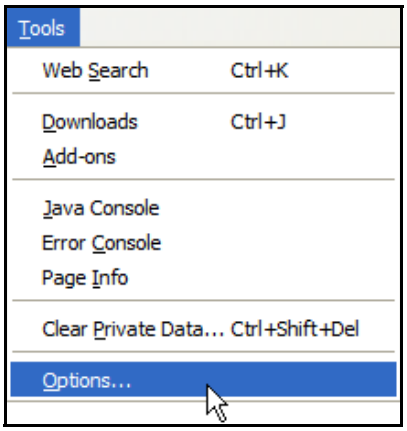


Installing a Stand-Alone Certificate File in Firefox

Rather than browsing to a ZyXEL web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

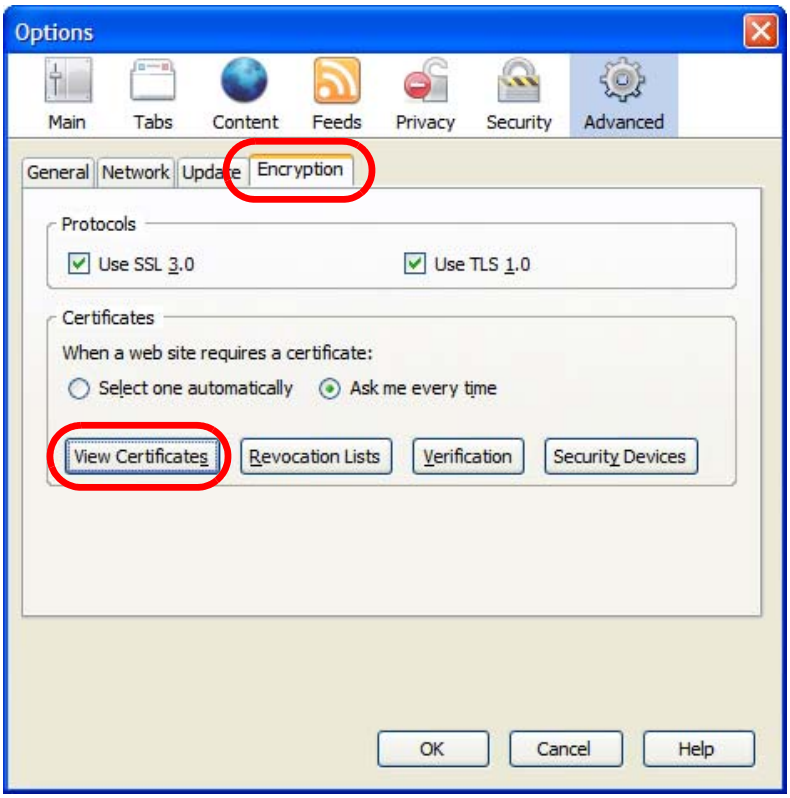
1 Open **Firefox** and click **Tools > Options**.

Figure 91 Firefox 2: Tools Menu



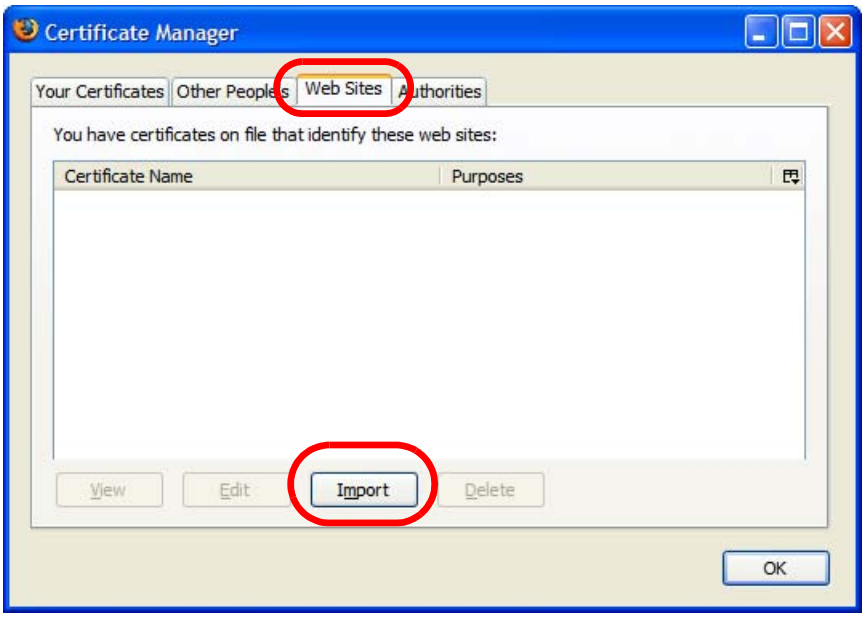
2 In the **Options** dialog box, click **Advanced > Encryption > View Certificates**.

Figure 92 Firefox 2: Options



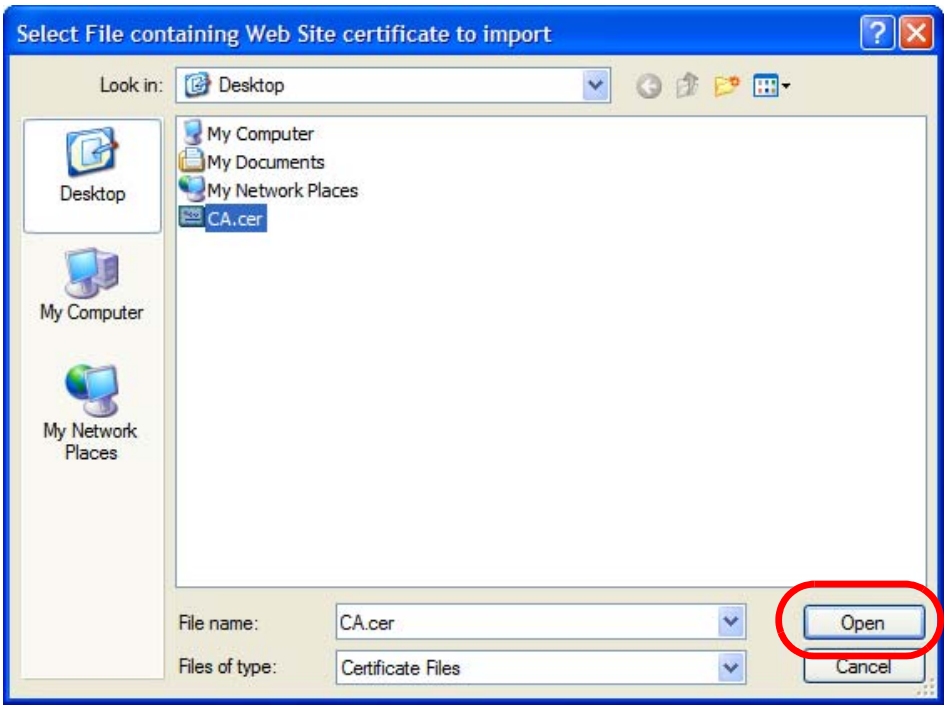
3 In the **Certificate Manager** dialog box, click **Web Sites** > **Import**.

Figure 93 Firefox 2: Certificate Manager



4 Use the **Select File** dialog box to locate the certificate and then click **Open**.

Figure 94 Firefox 2: Select File



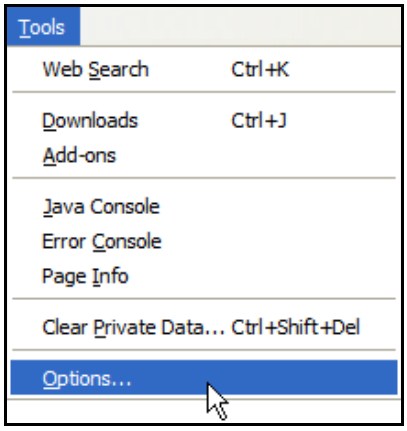
5 The next time you visit the web site, click the padlock in the address bar to open the **Page Info > Security** window to see the web page's security information.

Removing a Certificate in Firefox

This section shows you how to remove a public key certificate in Firefox 2.

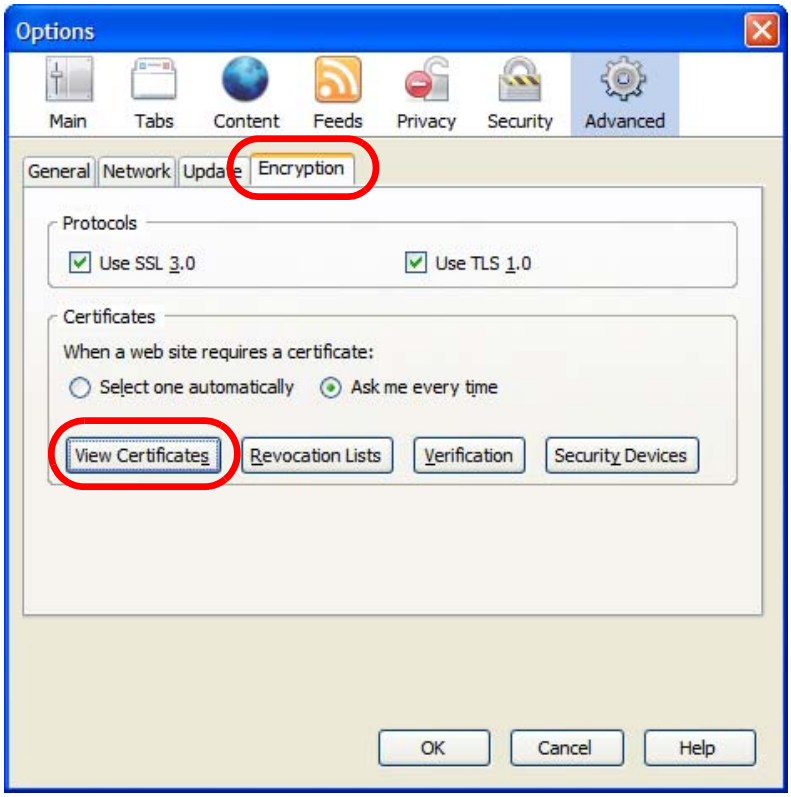
1 Open **Firefox** and click **Tools** > **Options**.

Figure 95 Firefox 2: Tools Menu



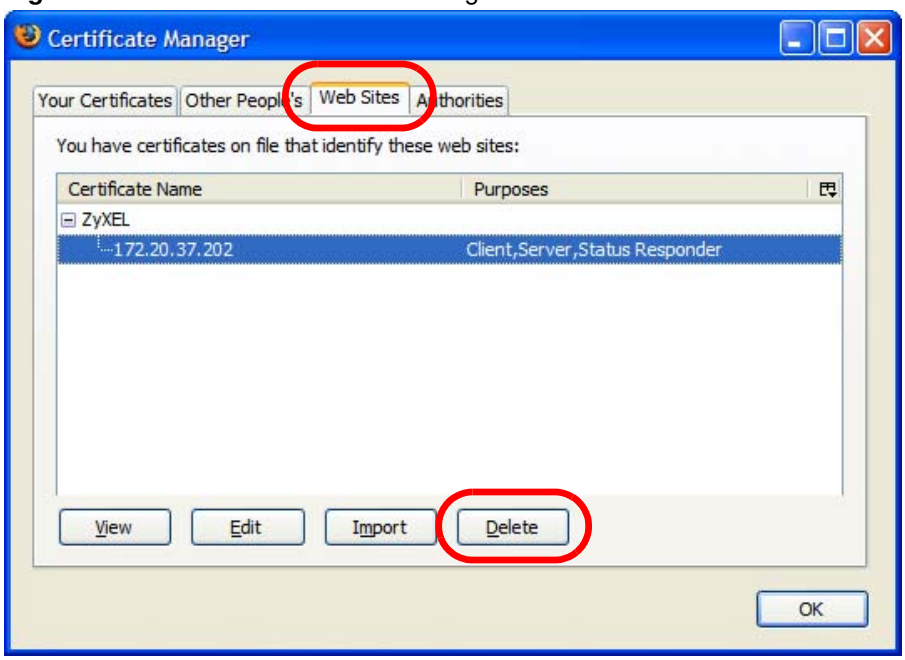
2 In the **Options** dialog box, click **Advanced** > **Encryption** > **View Certificates**.

Figure 96 Firefox 2: Options



3 In the **Certificate Manager** dialog box, select the **Web Sites** tab, select the certificate that you want to remove, and then click **Delete**.

Figure 97 Firefox 2: Certificate Manager



4 In the **Delete Web Site Certificates** dialog box, click **OK**.

Figure 98 Firefox 2: Delete Web Site Certificates

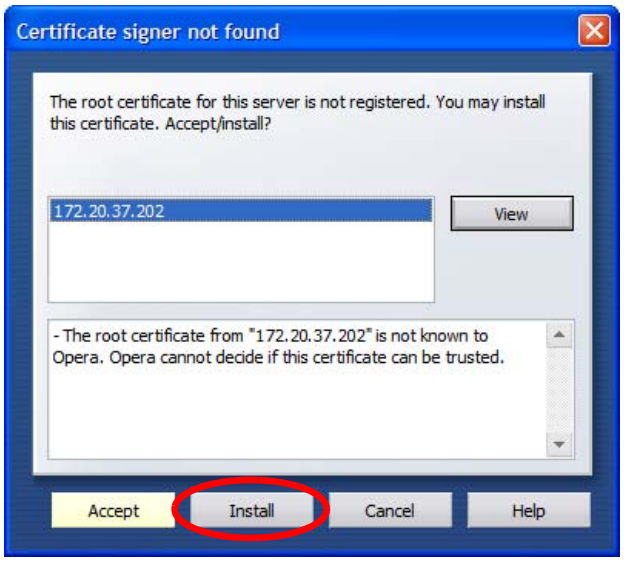
5 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

Opera

The following example uses Opera 9 on Windows XP Professional; however, the screens can apply to Opera 9 on all platforms.

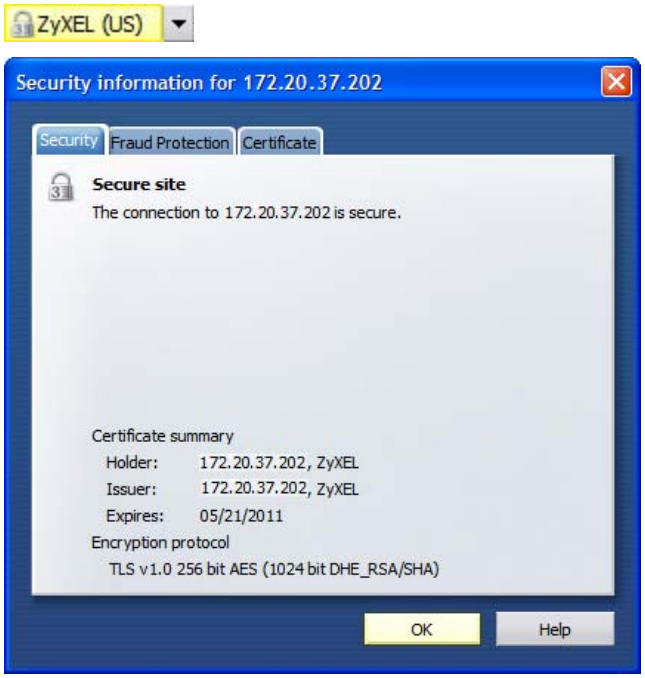
1. If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.
2. Click **Install** to accept the certificate.

Figure 99 Opera 9: Certificate signer not found



3. The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

Figure 100 Opera 9: Security information

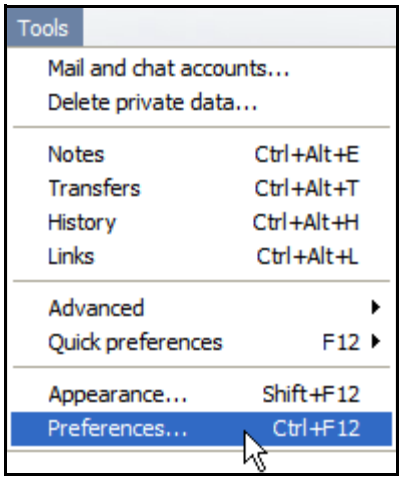


Installing a Stand-Alone Certificate File in Opera

Rather than browsing to a ZyXEL web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

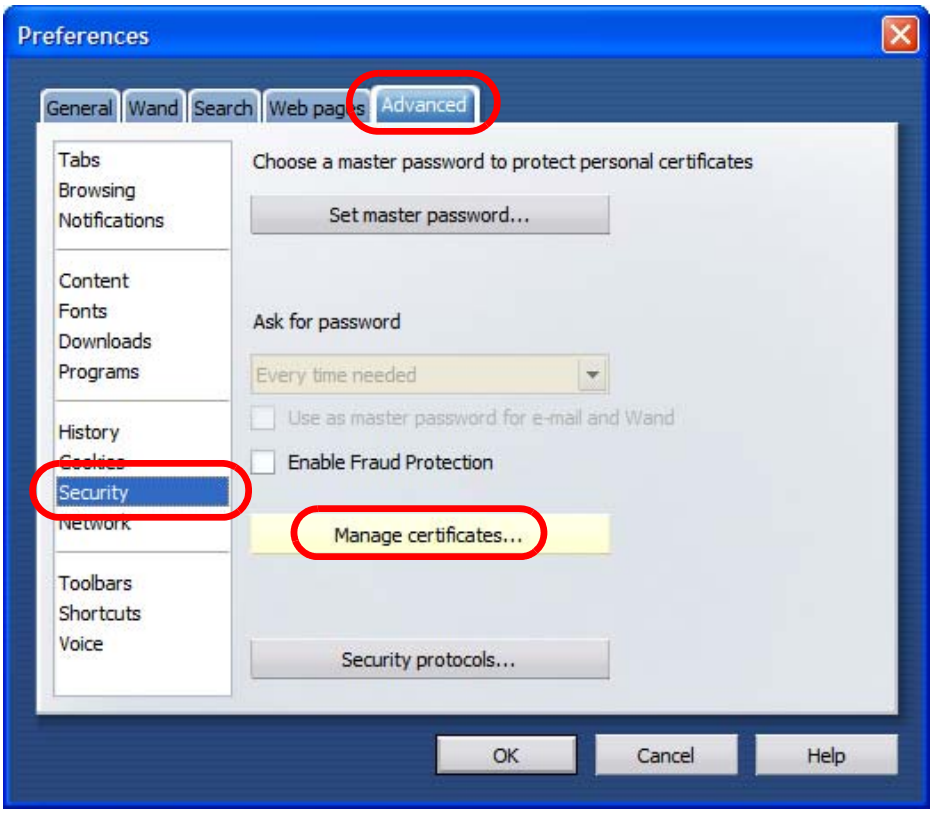
1 Open **Opera** and click **Tools** > **Preferences**.

Figure 101 Opera 9: Tools Menu



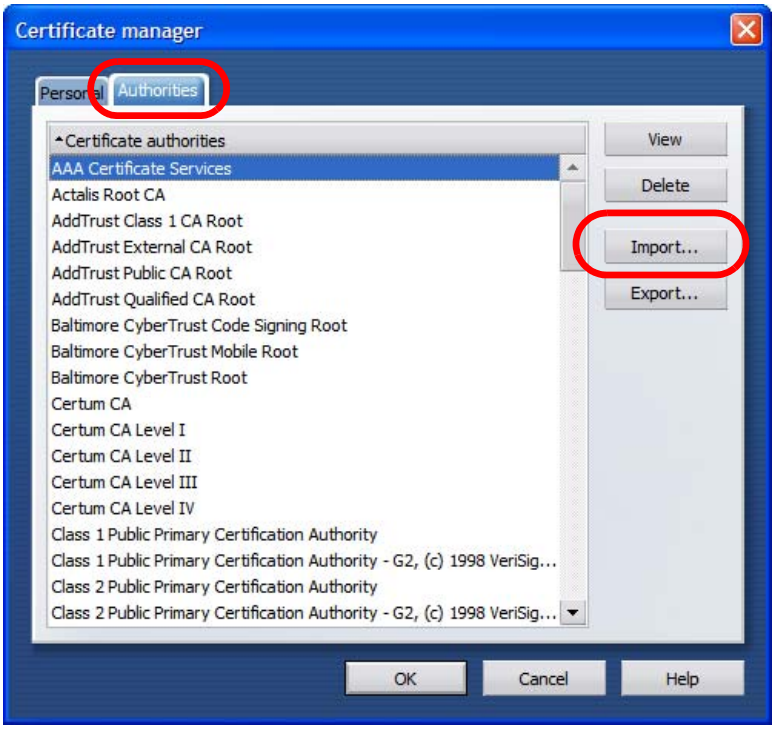
2 In **Preferences**, click **Advanced** > **Security** > **Manage certificates**.

Figure 102 Opera 9: Preferences



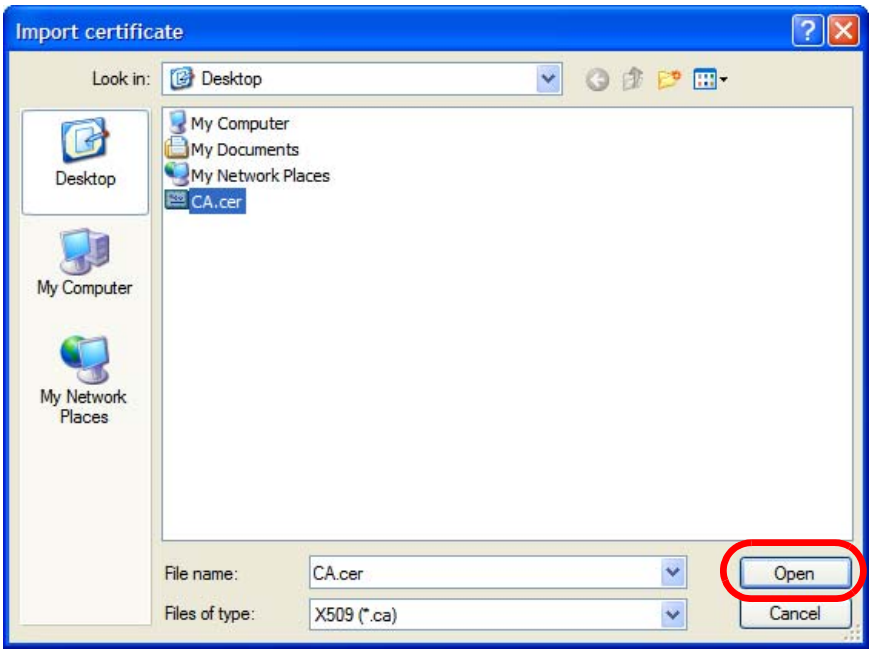
3 In the **Certificates Manager**, click **Authorities** > **Import**.

Figure 103 Opera 9: Certificate manager



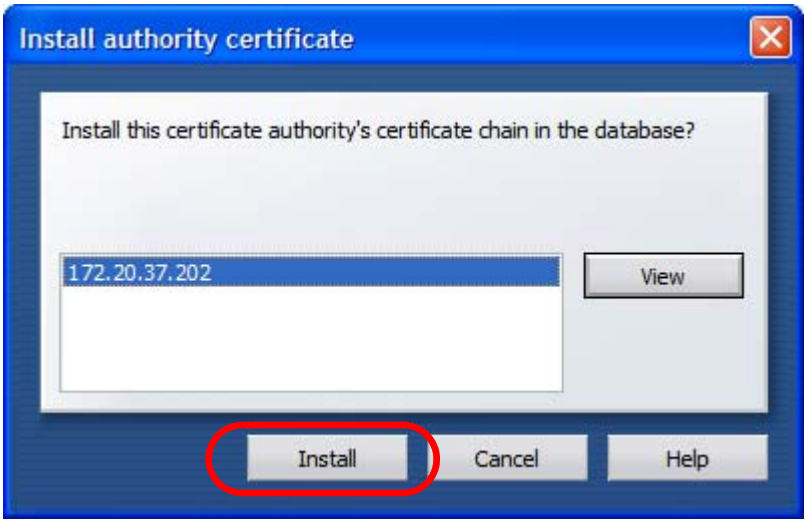
4 Use the **Import certificate** dialog box to locate the certificate and then click **Open.**

Figure 104 Opera 9: Import certificate



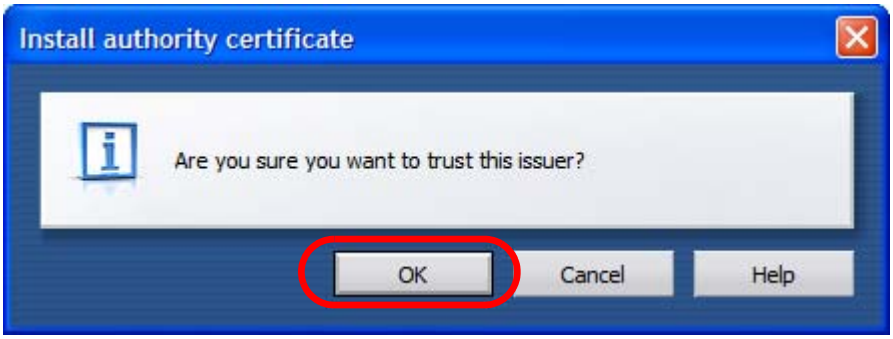
5 In the **Install authority certificate** dialog box, click **Install**.

Figure 105 Opera 9: Install authority certificate



6 Next, click **OK**.

Figure 106 Opera 9: Install authority certificate



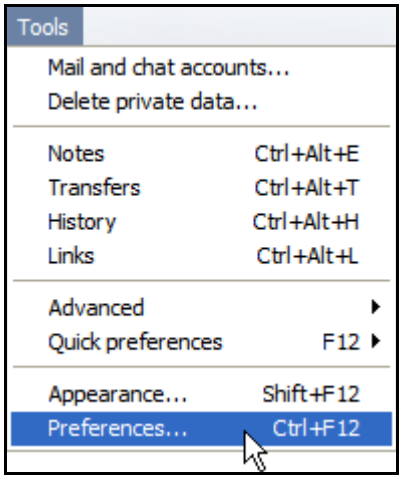
7 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

Removing a Certificate in Opera

This section shows you how to remove a public key certificate in Opera 9.

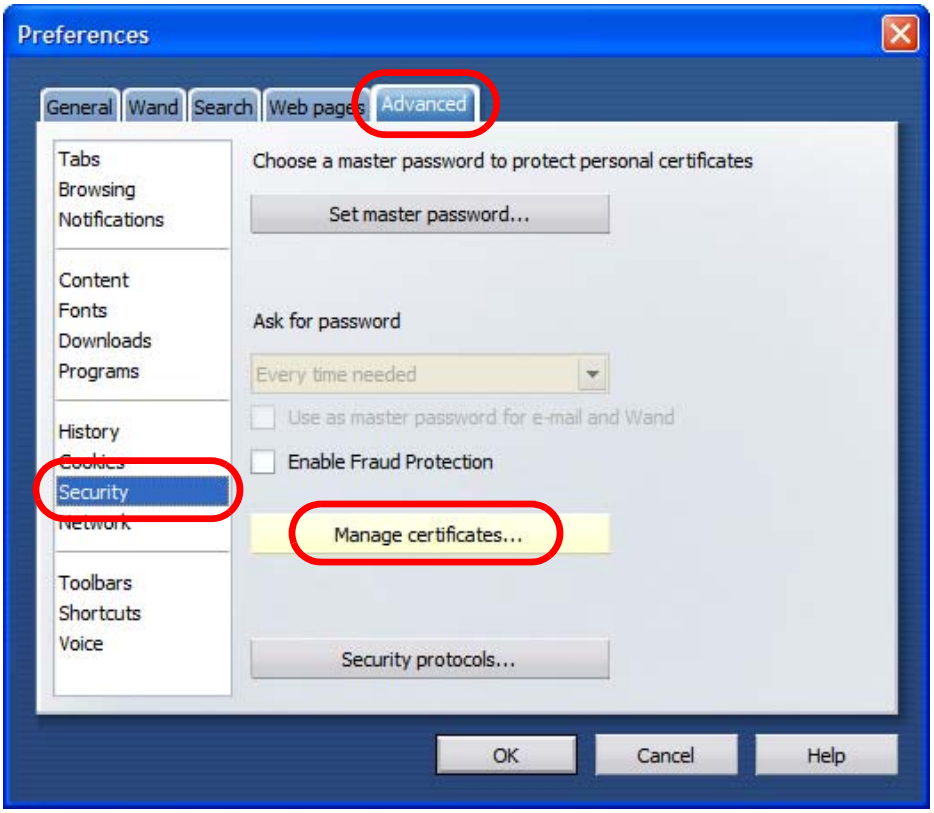
1 Open **Opera** and click **Tools** > **Preferences**.

Figure 107 Opera 9: Tools Menu



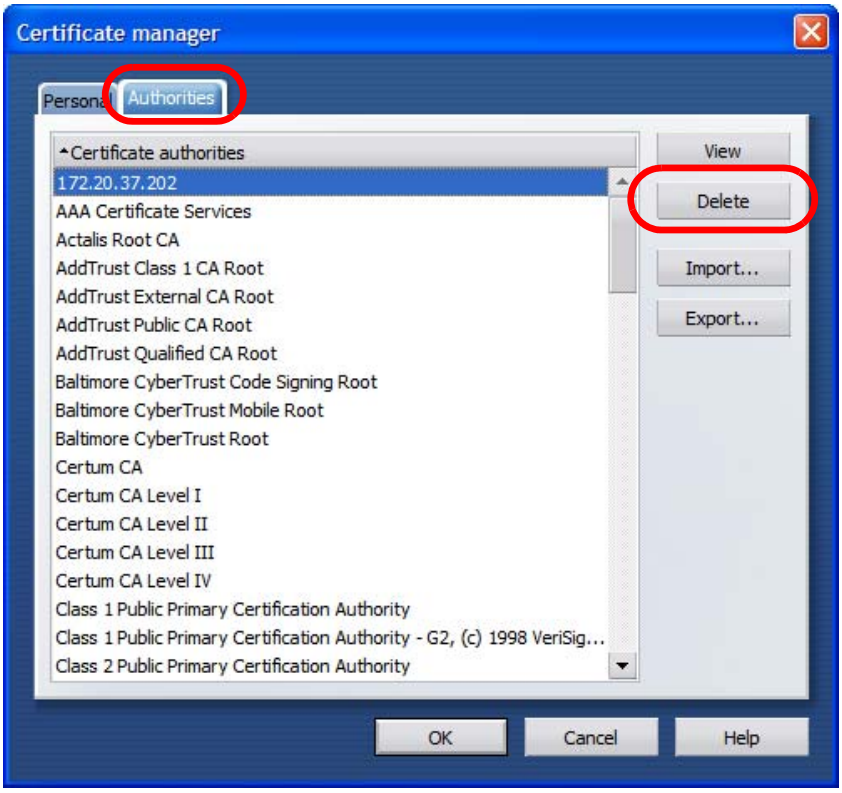
2 In **Preferences**, **Advanced** > **Security** > **Manage certificates**.

Figure 108 Opera 9: Preferences



3 In the **Certificates manager**, select the **Authorities** tab, select the certificate that you want to remove, and then click **Delete**.

Figure 109 Opera 9: Certificate manager



4 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

There is no confirmation when you delete a certificate authority, so be absolutely certain that you want to go through with it before clicking the button.

Konqueror

The following example uses Konqueror 3.5 on openSUSE 10.3, however the screens apply to Konqueror 3.5 on all Linux KDE distributions.

1. If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.
2. Click **Continue**.

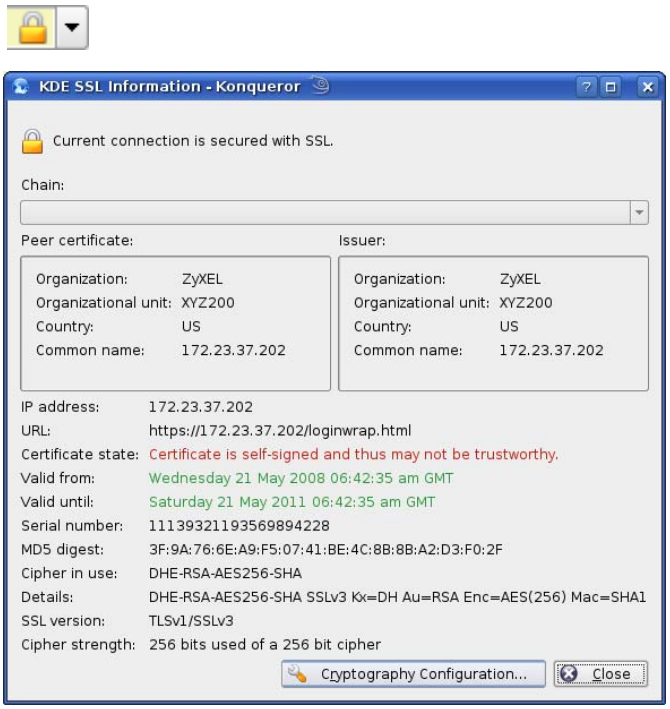
Figure 110 Konqueror 3.5: Server Authentication

3. Click **Forever** when prompted to accept the certificate.

Figure 111 Konqueror 3.5: Server Authentication

4. Click the padlock in the address bar to open the **KDE SSL Information** window and view the web page's security details.

Figure 112 Konqueror 3.5: KDE SSL Information



Installing a Stand-Alone Certificate File in Konqueror

Rather than browsing to a ZyXEL web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

1 Double-click the public key certificate file.

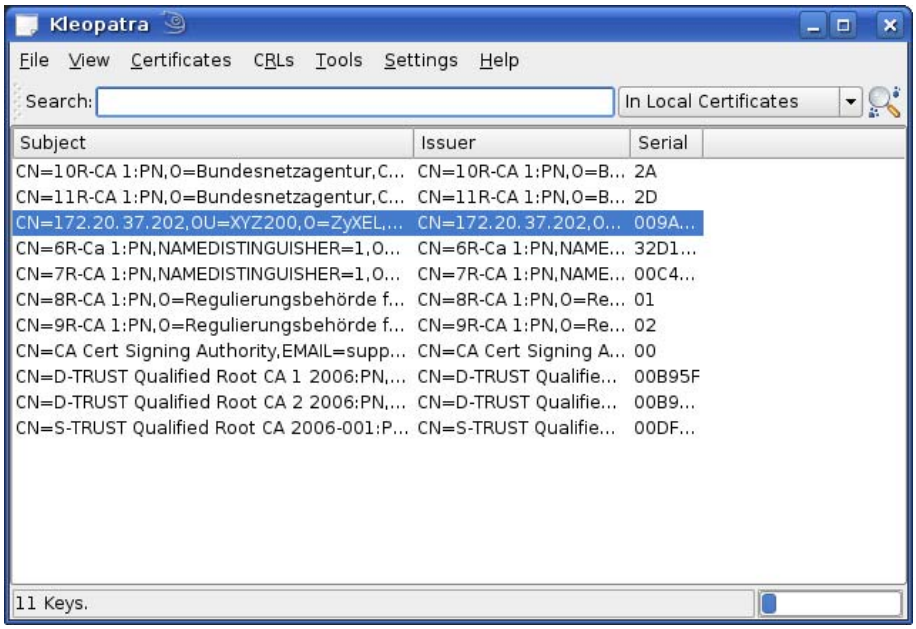
Figure 113 Konqueror 3.5: Public Key Certificate File

2 In the **Certificate Import Result - Kleopatra** dialog box, click **OK**.

Figure 114 Konqueror 3.5: Certificate Import Result

The public key certificate appears in the KDE certificate manager, **Kleopatra**.

Figure 115 Konqueror 3.5: Kleopatra



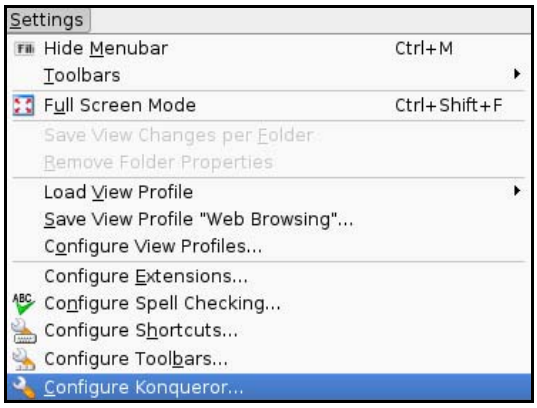
3 The next time you visit the web site, click the padlock in the address bar to open the **KDE SSL Information** window to view the web page's security details.

Removing a Certificate in Konqueror

This section shows you how to remove a public key certificate in Konqueror 3.5.

1 Open **Konqueror** and click **Settings > Configure Konqueror**.

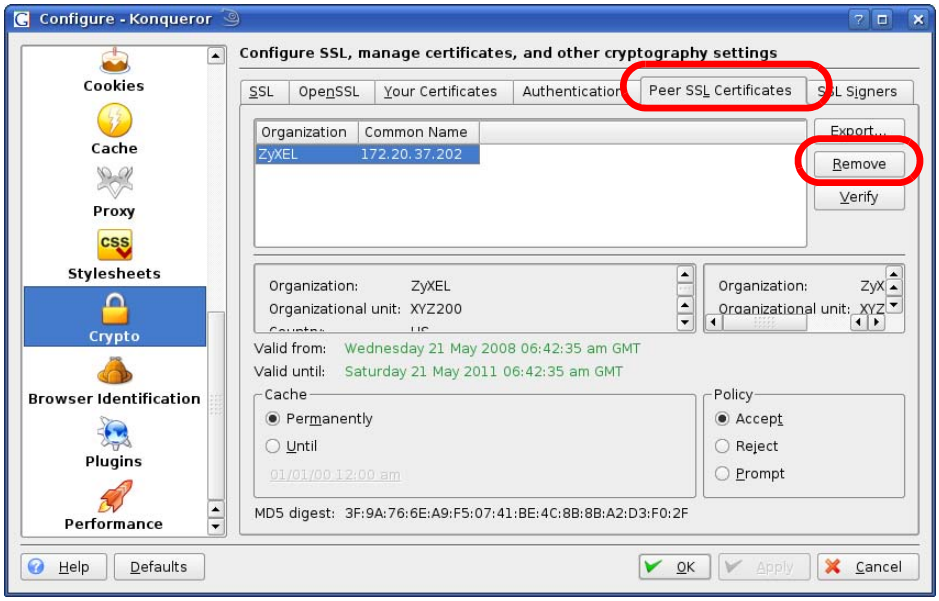
Figure 116 Konqueror 3.5: Settings Menu



2 In the **Configure** dialog box, select **Crypto**.

3 On the **Peer SSL Certificates** tab, select the certificate you want to delete and then click **Remove**.

Figure 117 Konqueror 3.5: Configure



4 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

There is no confirmation when you remove a certificate authority, so be absolutely certain you want to go through with it before clicking the button.

C

Legal Information

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.

3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4 Consult the dealer or an experienced radio/TV technician for help.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1 Go to http://www.zyxel.com.
2 Select your product on the ZyXEL home page to go to that product's page.
3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

D

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. Regional offices are listed below (see also http://www.zyxel.com/web/contact_us.php). Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

"+" is the (prefix) number you dial to make an international telephone call.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

China - ZyXEL Communications (Beijing) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-010-82800646
- Fax: +86-010-82800587
- Address: 902, Unit B, Horizon Building, No.6, Zhichun Str, Haidian District, Beijing
- Web: http://www.zyxel.cn

China - ZyXEL Communications (Shanghai) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-021-61199055
- Fax: +86-021-52069033

- Address: 1005F, ShengGao International Tower, No.137 XianXia Rd., Shanghai
- Web: http://www.zyxel.cn

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

North America

- Support E-mail: support@zyxel.com
- Support Telephone: +1-800-978-7222
- Sales E-mail: sales@zyxel.com
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Taiwan

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-2-27399889
- Fax: +886-2-27353220
- Web: http://www.zyxel.com.tw
- Address: Room B, 21F., No.333, Sec. 2, Dunhua S. Rd., Da-an District, Taipei

Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Turkey

- Support E-mail: cso@zyxel.com.tr
- Telephone: +90 212 222 55 22
- Fax: +90-212-220-2526
- Web: http:www.zyxel.com.tr
- Address: Kaptanpasa Mahallesi Piyalepasa Bulvari Ortadogu Plaza N:14/13 K:6 Okmeydani/Sisli Istanbul/Turkey

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 0845 122 0301 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)