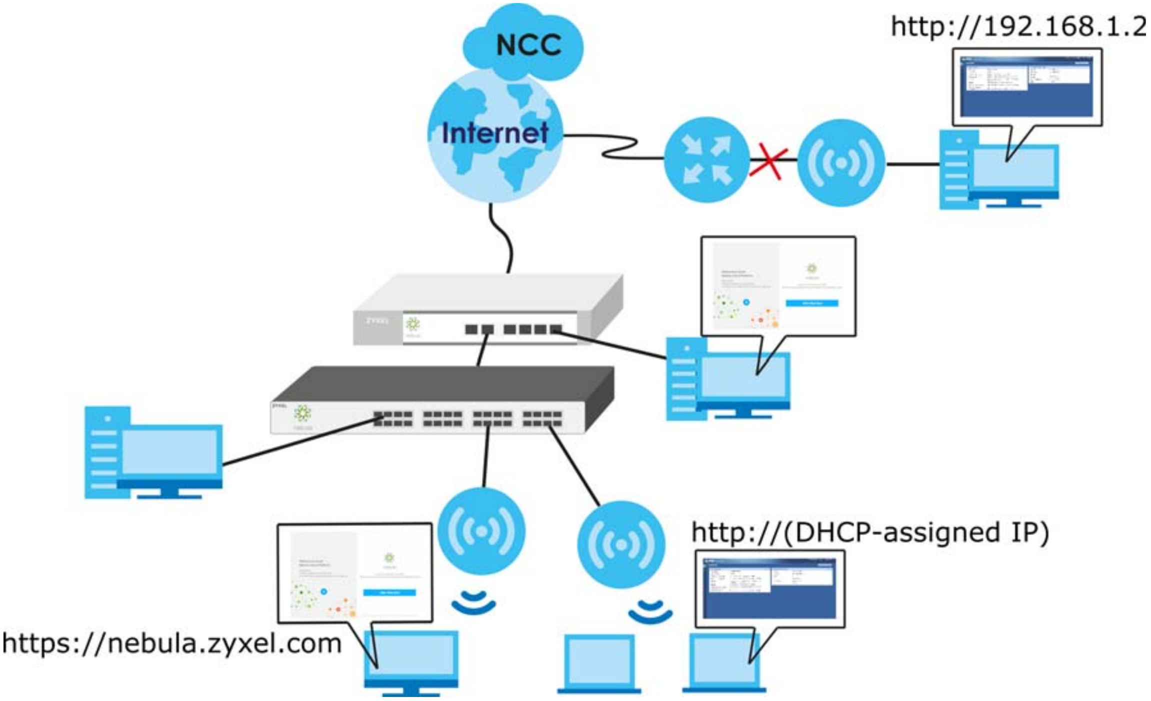
PART II

Local Configuration in Cloud Mode

CHAPTER 25 Cloud Mode

25.1 Overview

The Zyxel Device is managed and provisioned automatically by the *NCC (Nebula Control Center)* when it is connected to the Internet and has been registered in the NCC. If you need to change the Zyxel Device’s VLAN setting or manually set its IP address, access its simplified web configurator (see Chapter 4 on page 52). You can check the NCC's **AP > Monitor > Access Point** screen or the connected gateway for the Zyxel Device's current LAN IP address. Alternatively, disconnect the gateway or disable its DHCP server function and use the Zyxel Device's default static LAN IP address (192.168.1.2).



25.2 Cloud Mode Web Configurator Screens

When your Zyxel Device is managed through NCC, you can access only the following screens through the Web Configurator:

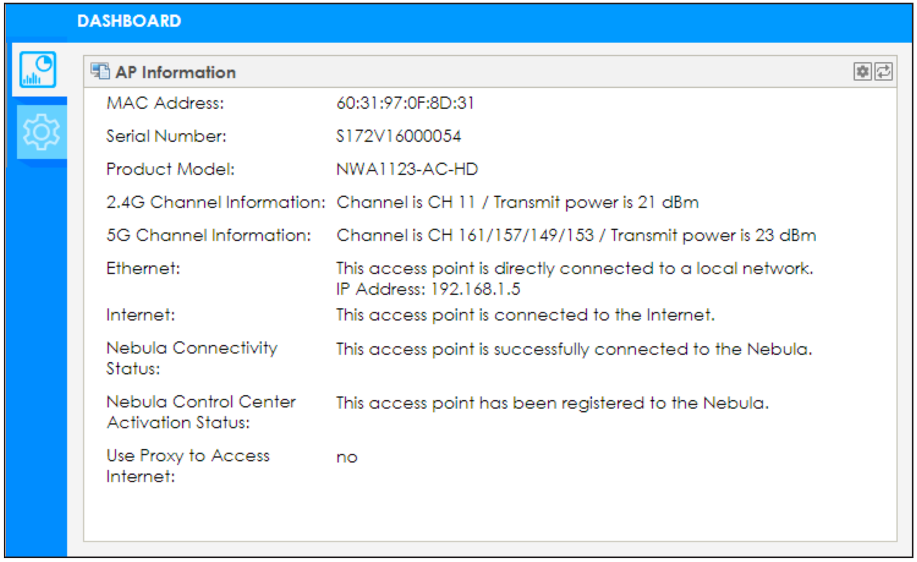
- **Dashboard**
- **Configuration > Network > IP Setting**
- **Configuration > Network > VLAN**

These screens also have fewer options than those in standalone Zyxel Devices. The rest of the Zyxel Device’s features must be configured through the NCC.

CHAPTER 26 Dashboard

This screen displays general AP information, and client information in widgets that you can re-arrange to suit your needs. You can also collapse, refresh, and close individual widgets.

Figure 141 Dashboard



MAC Address: 60:31:97:0F:8D:31
Serial Number: S172V16000054
Product Model: NWA1123-AC-HD
2.4G Channel Information: Channel is CH 11 / Transmit power is 21 dBm
5G Channel Information: Channel is CH 161/157/149/153 / Transmit power is 23 dBm
Ethernet: This access point is directly connected to a local network. IP Address: 192.168.1.5
Internet: This access point is connected to the Internet.
Nebula Connectivity Status: This access point is successfully connected to the Nebula.
Nebula Control Center Activation Status: This access point has been registered to the Nebula.
Use Proxy to Access Internet: no

The following table describes the labels in this screen.

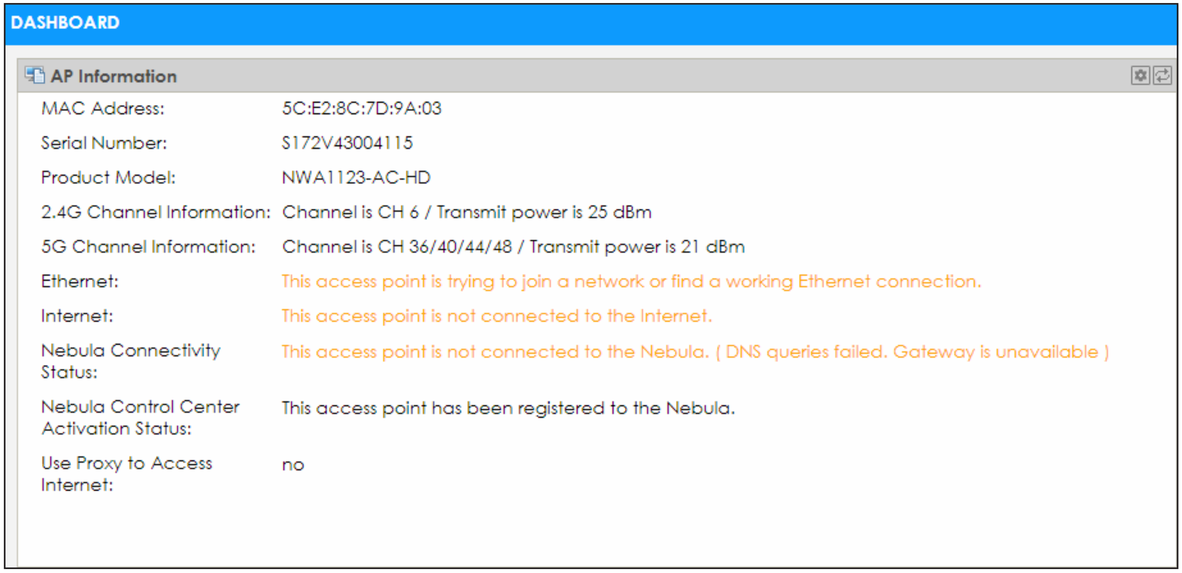
Table 100 Dashboard

LABEL	DESCRIPTION
AP Information	
MAC Address	This field displays the MAC address of the Zyxel Device.
Serial Number	This field displays the serial number of the Zyxel Device.
Product Model	This field displays the model name of the Zyxel Device.
2.4G Channel Information	This field displays the channel number the Zyxel Device is using and its output power in the 2.4 GHz spectrum. This shows **Not activated** if the wireless LAN is disabled.
5G Channel Information	This field displays the channel number the Zyxel Device is using and its output power in the 5 GHz spectrum. This shows **Not activated** if the wireless LAN is disabled.
Ethernet	This field displays whether the Zyxel Device's Ethernet port is connected and the IP address of the gateway to which the Zyxel Device is connected.
Internet	This field displays whether the Zyxel Device is connecting to the Internet.
Nebula Connectivity Status	This field displays whether the Zyxel Device can connect to the Zyxel Nebula Control Center (NCC).

Table 100 Dashboard (continued)

LABEL	DESCRIPTION
Nebula Control Center Activation Status	This field displays whether the Zyxel Device has been registered and can be managed by the NCC.
Use Proxy to Access Internet	This displays whether the NAP uses a proxy server to access the NCC (Nebula Control Center).

If the Zyxel Device cannot connect to the Internet or to NCC, an error message is shown on this screen, as in the following.



DASHBOARD

AP Information

MAC Address: 5C:E2:8C:7D:9A:03

Serial Number: S172V43004115

Product Model: NWA1123-AC-HD

2.4G Channel Information: Channel is CH 6 / Transmit power is 25 dBm

5G Channel Information: Channel is CH 36/40/44/48 / Transmit power is 21 dBm

Ethernet: This access point is trying to join a network or find a working Ethernet connection.

Internet: This access point is not connected to the Internet.

Nebula Connectivity Status: This access point is not connected to the Nebula. (DNS queries failed. Gateway is unavailable)

Nebula Control Center Activation Status: This access point has been registered to the Nebula.

Use Proxy to Access Internet: no

CHAPTER 27
Network

27.1 Overview

This chapter describes how you can configure the management IP address and VLAN settings of your Zyxel Device.

See Section 9.1 on page 95 for information about IP addresses.

Note: Make sure your VLAN settings allow the Zyxel Device to connect to the Internet so you could manage it with NCC.

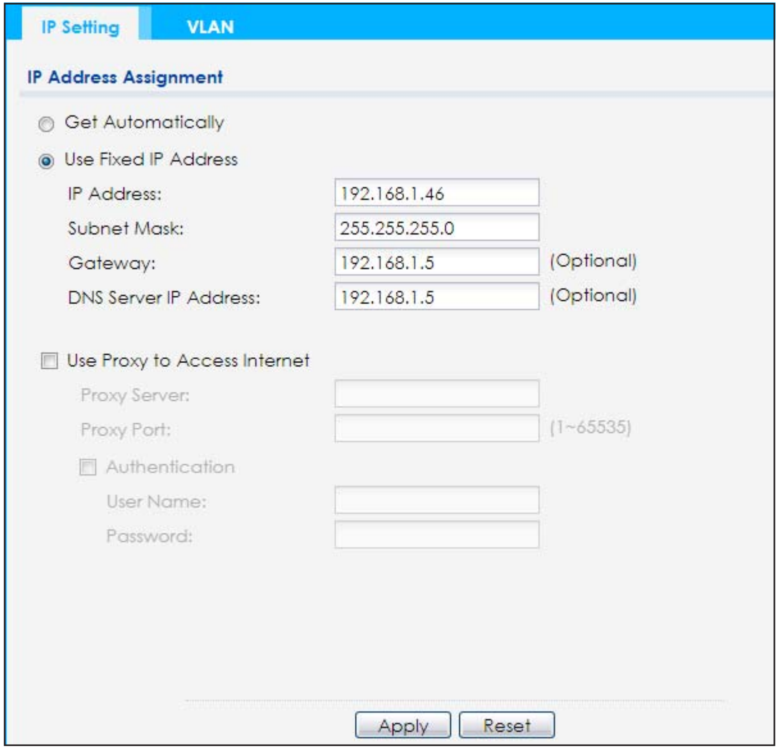
27.1.1 What You Can Do in this Chapter

- The **IP Setting** screen (Section 27.2 on page 232) configures the Zyxel Device's LAN IP address.
- The **VLAN** screen (Section 27.3 on page 234) configures the Zyxel Device's VLAN settings.

27.2 IP Setting

Use this screen to configure the IP address for your Zyxel Device. To access this screen, click **Configuration > Network > IP Setting**.

Figure 142 Configuration > Network > IP Setting



IP Address Assignment

○ Get Automatically

● Use Fixed IP Address

IP Address:	192.168.1.46	
Subnet Mask:	255.255.255.0	
Gateway:	192.168.1.5	(Optional)
DNS Server IP Address:	192.168.1.5	(Optional)

□ Use Proxy to Access Internet

Proxy Server:		
Proxy Port:		(1~65535)

□ Authentication

User Name:	
Password:	

Each field is described in the following table.

Table 101 Configuration > Network > IP Setting

LABEL	DESCRIPTION
IP Address Assignment	
Get Automatically	Select this to make the interface a DHCP client and automatically get the IP address, subnet mask, and gateway address from a DHCP server.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	Enter the IP address of the gateway. The Zyxel Device sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
DNS Server IP Address	Enter the IP address of the DNS server.
Use Proxy to Access Internet	If the Zyxel Device is behind a proxy server, you need to select this option and configure the proxy server settings so that the Zyxel Device can access the NCC through the proxy server.
Proxy Server	Enter the IP address of the proxy server.
Proxy Port	Enter service port number used by the proxy server.
Authentication	Select this option if the proxy server requires authentication before it grants access to the Internet.
User Name	Enter your proxy user name.
Password	Enter your proxy password.

Table 101 Configuration > Network > IP Setting (continued)

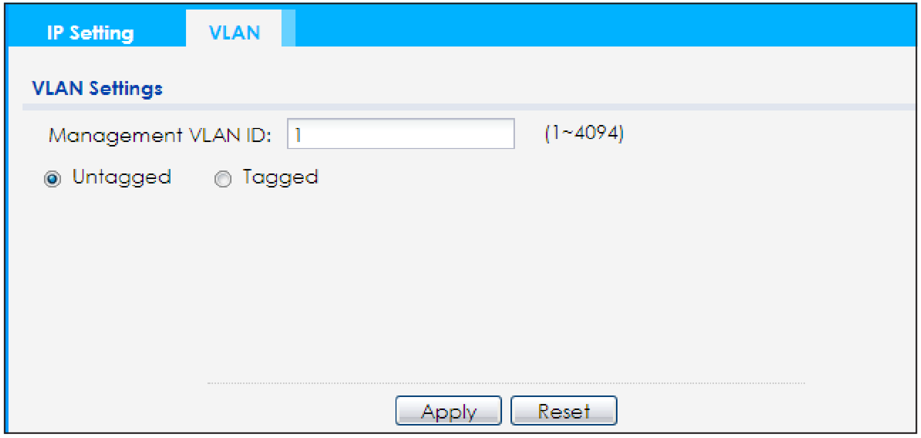
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

27.3 VLAN

This section discusses how to configure the Zyxel Device's VLAN settings. See Section 9.3 on page 99 for more information about VLAN.

Use this screen to configure the VLAN settings for your Zyxel Device. To access this screen, click **Configuration > Network > VLAN**.

Figure 143 Configuration > Network > VLAN



Management VLAN ID: 1 (1~4094)

● Untagged ○ Tagged

Each field is described in the following table.

Table 102 Configuration > Network > VLAN

LABEL	DESCRIPTION
VLAN Settings	
Management VLAN ID	Enter a VLAN ID for the Zyxel Device.
Untagged/ Tagged	Set whether the Zyxel Device adds the VLAN ID to outbound traffic transmitted through its Ethernet port.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

PART III

Appendices and Troubleshooting

CHAPTER 28 Troubleshooting

28.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LED
- Zyxel Device Management, Access, and Login
- Internet Access
- WiFi Network
- Resetting the Zyxel Device

28.2 Power, Hardware Connections, and LED

The Zyxel Device does not turn on. The LED is not on.

1. Make sure you are using the power adapter included with the Zyxel Device or a PoE power injector/switch.
2. Make sure the power adapter or PoE power injector/switch is connected to the Zyxel Device and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adapter or PoE power injector/switch.
4. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
5. If none of these steps work, you may have faulty hardware and should contact your Zyxel Device vendor.

The LED does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 3.2 on page 34.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Disconnect and re-connect the power adapter or PoE power injector to the Zyxel Device.

5 If the problem continues, contact the vendor.

28.3 Zyxel Device Management, Access, and Login

I forgot the IP address for the Zyxel Device.

1 The default IP address (in standalone mode) is 192.168.1.2.

2 If you changed the IP address and have forgotten it, you have to reset the Zyxel Device to its factory defaults. See Section 28.6 on page 243.

3 If your Zyxel Device is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.

4 If the NCC has managed the Zyxel Device, you can also check the NCC's **AP > Monitor > Access Point** screen for the Zyxel Device's current LAN IP address.

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

1 Make sure you are using the correct IP address.

- The default IP address (in standalone mode) is 192.168.1.2.
- If you changed the IP address, use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the Zyxel Device.

2 Check the hardware connections, and make sure the LED is behaving as expected. See the Quick Start Guide and Section 3.2 on page 34.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.

4 Make sure your computer is in the same subnet as the Zyxel Device. (If you know that there are routers between your computer and the Zyxel Device, skip this step.)

- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address.
- If there is no DHCP server on your network, make sure your computer’s IP address is in the same subnet as the Zyxel Device.

5 Reset the Zyxel Device to its factory defaults, and try to access the Zyxel Device with the default IP address. See Section 28.6 on page 243.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the Zyxel Device using another service, such as Telnet. If you can access the Zyxel Device, check the remote management settings to find out why the Zyxel Device does not respond to HTTP.
- If your computer is connected wirelessly, use a computer that is connected to a **LAN**/**ETHERNET** port.

I forgot the password.

1 The default password is **1234**. If the Zyxel Device is connected to the NCC and registered, check the NCC for the password.

2 If this does not work, you have to reset the Zyxel Device to its factory defaults. See Section 28.6 on page 243.

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

1 Make sure you have entered the user name and password correctly. The default password is **1234**. This fields are case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the web configurator while someone is using Telnet to access the Zyxel Device. Log out of the Zyxel Device in the other session, or ask the person who is logged in to log out.

3 Disconnect and re-connect the power adapter or PoE power injector to the Zyxel Device.

4 If this does not work, you have to reset the Zyxel Device to its factory defaults. See Section 28.6 on page 243.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the **Login screen in the web configurator.** Ignore the suggestions about your browser.

I cannot access the Zyxel Device directly anymore after switching to NCC management.

- Check the Zyxel Device IP address and login credentials using the NCC and use them to access the Zyxel Device. Note that the built-in Web Configurator will have limited functionality when managed through NCC.

I enabled **NCC Discovery**, but the Zyxel Device is still in standalone mode.

Make sure your Zyxel Device is registered to the NCC.

The Zyxel Device is already registered with NCC, but it is still in standalone mode; it cannot connect to the NCC.

1. Make sure that NCC Discovery is enabled (see Section 9.6 on page 104).
2. Check your network's firewall/security settings. Make sure the following TCP ports are allowed: 443, 4335, and 6667.
3. Make sure your Zyxel Device can access the Internet.
4. Check your network's VLAN settings (see Section 9.3 on page 99). You may have to change the Management VLAN settings of the Zyxel Device to allow it to connect to the Internet and access the NCC.

   Note: Changing the management VLAN and IP address settings on the Zyxel Device also pushes these changes to the NCC. Do this only if your device cannot otherwise connect to the NCC.

5. Make sure your Zyxel Device doesn't have to go through network authentication such as a captive portal, If your network uses a captive portal, the network administrator may have to create a new VLAN without this requirement. Change your Zyxel Device's management VLAN settings as necessary.

I want to switch from NCC to AC management, but I couldn't find the **AC Discovery** menu in the Zyxel Device web configurator.

1. Unregister the Zyxel Device from the NCC.
2. Reset your Zyxel Device to the factory defaults.
3. Make sure that your Zyxel Device is in the same subnet as the AC, and enable **AC Discovery** in **Configuration** > **Network** > **AC Discovery**.

The Zyxel Device cannot discover the AC.

1. Make sure your Zyxel Device is not registered to NCC.
2. Enable **AC Discovery** in **Configuration** > **Network** > **AC Discovery**.

3 Make sure that the Zyxel Device and the AC are both in the same subnet.

4 If you have to set them up in different subnets, see AC management and IP Subnets on page 97.

I accidentally pressed the Nebula button in the NXC's web configurator. How do I undo it?

1 If the Zyxel Device is not registered with the NCC, register it first.

2 Unregister the Zyxel Device from the NCC.

3 Reset the Zyxel Device to the factory defaults.

Some features I set using the NCC do not work as expected.

1 Make sure your Zyxel Device can access the Internet.

2 Check your network's firewall/security settings. Make sure the following ports are allowed:

- TCP: 443, 4335, and 6667
- UDP: 123

3 After changing your Zyxel Device settings using the NCC, wait 1-2 minutes for the changes to take effect.

I can only see newer logs. Older logs are missing.

When a log reaches the maximum number of log messages (see Section 1.4 on page 19), new log messages automatically overwrite the oldest log messages.

The commands in my configuration file or shell script are not working properly.

- In a configuration file or shell script, use "#" or "!" as the first character of a command line to have the Zyxel Device treat the line as a comment.
- Your configuration files or shell scripts can use "exit" or a command line consisting of a single "!" to have the Zyxel Device exit sub command mode.
- Include `write` commands in your scripts. Otherwise the changes will be lost when the Zyxel Device restarts. You could use multiple `write` commands in a long script.

Note: "exit" or "!'" must follow sub commands if it is to make the Zyxel Device exit sub command mode.

I cannot upload the firmware uploaded using FTP.

The Web Configurator is the recommended method for uploading firmware in standalone mode. For managed Zyxel Devices, using the NCC or AC is recommended. You only need to use FTP if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

28.4 Internet Access

Clients cannot access the Internet through the Zyxel Device.

1. Check the Zyxel Device's hardware connections, and make sure the LEDs are behaving as expected (refer to Section 3.2 on page 34). See the Quick Start Guide and Section 28.2 on page 236.
2. Make sure the Zyxel Device is connected to a broadband modem or router with Internet access and your computer is set to obtain an dynamic IP address.
3. If clients are trying to access the Internet wirelessly, make sure the wireless settings on the wireless clients are the same as the settings on the Zyxel Device.
4. Disconnect all the cables from your Zyxel Device, and follow the directions in the Quick Start Guide again.
5. Reboot the client and reconnect to the Zyxel Device.
6. If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. Look at the LEDs, and check Section 3.2 on page 34. If the Zyxel Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2. Check the signal strength using the NCC, AC, Zyxel Device Web Configurator, or the client device itself. If the signal is weak, try moving the client closer to the Zyxel Device (if possible), and look around to see if there are any devices that might be interfering with the wireless network (microwaves, other wireless networks, and so on).
3. Reboot the Zyxel Device using the web configurator/CLI or the NCC or AC.
4. Check the settings for QoS. If it is disabled, activate it. When enabled, raise or lower the priority for some applications.

5 If the problem continues, contact the network administrator or vendor.

28.5 WiFi Network

I cannot access the Zyxel Device or ping any computer from the WLAN.

1 Make sure the wireless LAN (wireless radio) is enabled on the Zyxel Device.

2 Make sure the radio or at least one of the Zyxel Device's radios is operating in AP mode.

3 Make sure the wireless adapter (installed on your computer) is working properly.

4 Make sure the wireless adapter (installed on your computer) is IEEE 802.11 compatible and supports the same wireless standard as the Zyxel Device's active radio.

5 Make sure your computer (with a wireless adapter installed) is within the transmission range of the Zyxel Device.

6 Check that both the Zyxel Device and your computer are using the same wireless and wireless security settings.

Hackers have accessed my WEP-encrypted wireless LAN.

WEP is extremely insecure. Its encryption can be broken by an attacker, using widely-available software. It is strongly recommended that you use a more effective security mechanism. Use the strongest security mechanism that all the wireless devices in your network support. WPA2 or WPA2-PSK is recommended.

The wireless security is not following the re-authentication timer setting I specified.

If a RADIUS server authenticates wireless stations, the re-authentication timer on the RADIUS server has priority. Change the RADIUS server's configuration if you need to use a different re-authentication timer setting.

I cannot import a certificate into the Zyxel Device.

1 For **My Certificates**, you can import a certificate that matches a corresponding certification request that was generated by the Zyxel Device. You can also import a certificate in PKCS#12 format, including the certificate's public and private keys.

2 You must remove any spaces from the certificate's filename before you can import the certificate.

3 Any certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The Zyxel Device currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.
- Binary PKCS#12: This is a format for transferring public key and private key certificates.The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the Zyxel Device.

Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

Wireless clients are not being load balanced among my Zyxel Devices.

- Make sure that all the Zyxel Devices used by the wireless clients in question share the same SSID, security, and radio settings.
- Make sure that all the Zyxel Devices are in the same broadcast domain.
- Make sure that the wireless clients are in range of the other Zyxel Devices; if they are only in range of a single Zyxel Device, then load balancing may not be as effective.

In the **Monitor > Wireless > AP Information > Radio List** screen, there is no load balancing indicator associated with any Zyxel Devices assigned to the load balancing task.

- Check that the AP profile which contains the load balancing settings is correctly assigned to the Zyxel Devices in question.
- The load balancing task may have been terminated because further load balancing on the Zyxel Devices in question is no longer required.

28.6 Resetting the Zyxel Device

If you cannot access the Zyxel Device by any method, try restarting it by turning the power off and then on again. If you still cannot access the Zyxel Device by any method or you forget the administrator password(s), you can reset the Zyxel Device to its factory-default settings. Any configuration files or shell scripts that you saved on the Zyxel Device should still be available afterwards.

Use the following procedure to reset the Zyxel Device to its factory-default settings. This overwrites the settings in the startup-config.conf file with the settings in the system-default.conf file.

Note: This procedure removes the current configuration.

1. Make sure the Power LED is on and not blinking.
2. Press the **RESET** button and hold it until the Power LED begins to blink. (This usually takes about ten seconds.)
3. Release the **RESET** button, and wait for the Zyxel Device to restart.

   You should be able to access the Zyxel Device in standalone mode using the default settings.

28.7 Getting More Troubleshooting Help

Search for support information for your model at www.zyxel.com for more troubleshooting suggestions.

APPENDIX A
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 Zyxel Device, 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.

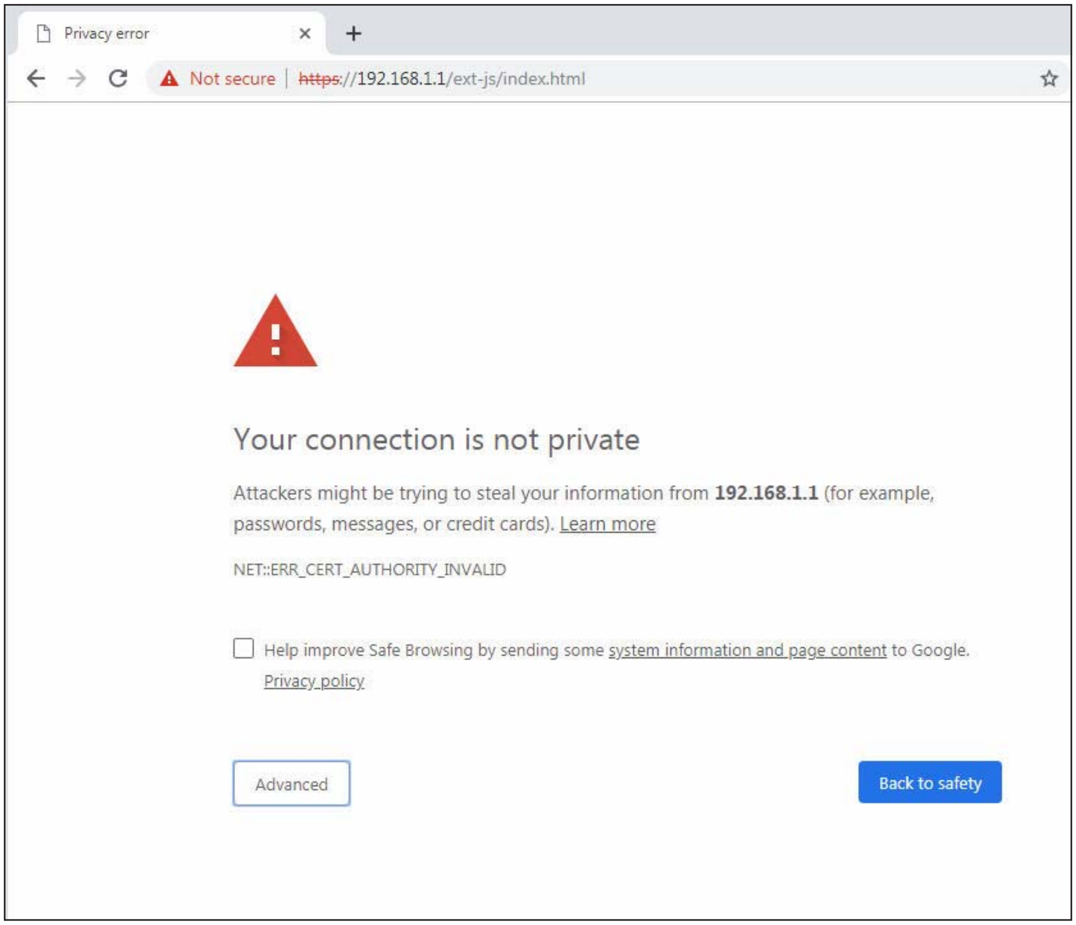
Note: You can see if you are browsing on a secure website if the URL in your web browser's address bar begins with `https://` or there is a sealed padlock icon (🔒) somewhere in the main browser window (not all browsers show the padlock in the same location).

Google Chrome

The following example uses Google Chrome on Windows 7. You first have to store the certificate in your computer and then install it as a Trusted Root CA, as shown in the following tutorials.

Export a Certificate

1 If your device’s Web Configurator is set to use SSL certification, then upon browsing with it for the first time, you are presented with a certification error.



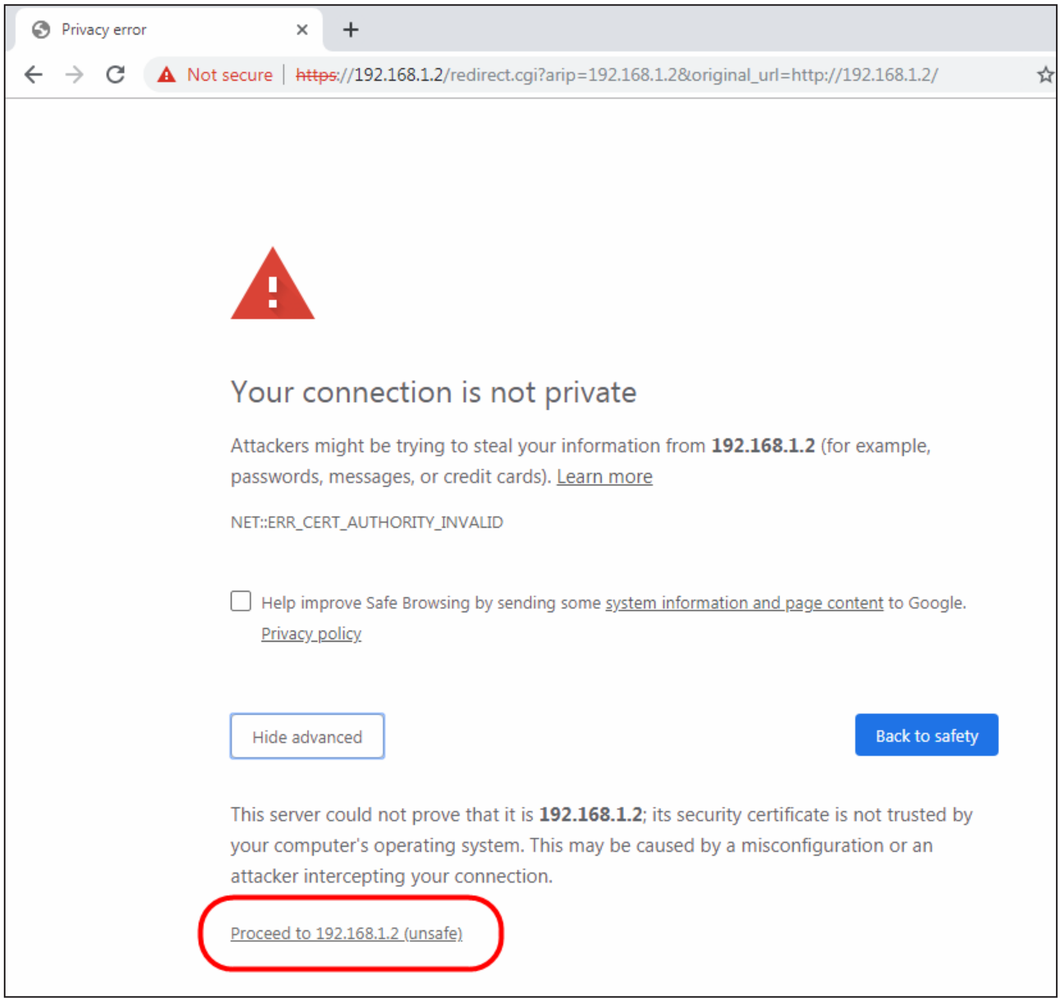
Your connection is not private

Attackers might be trying to steal your information from **192.168.1.1** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

2 Click **Advanced > Proceed to *x.x.x.x* (unsafe)**.


Privacy error
Not secure
~~https~~://192.168.1.2/redirect.cgi?arip=192.168.1.2&original_url=http://192.168.1.2/

Your connection is not private

Attackers might be trying to steal your information from **192.168.1.2** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

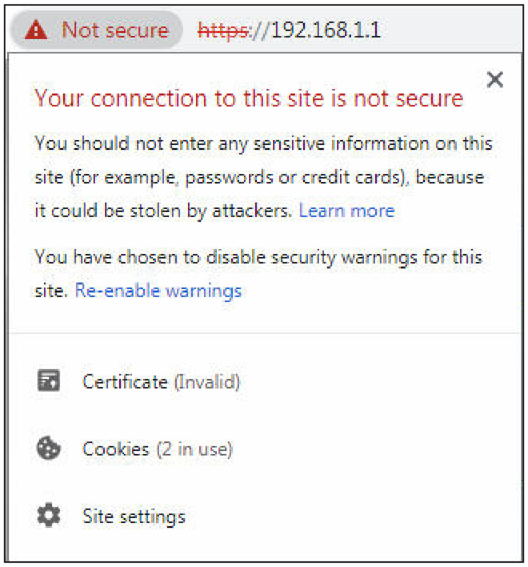
□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

Hide advanced
Back to safety

This server could not prove that it is **192.168.1.2**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.1.2 (unsafe)

3 In the **Address Bar**, click **Not Secure** > **Certificate (Invalid)**.

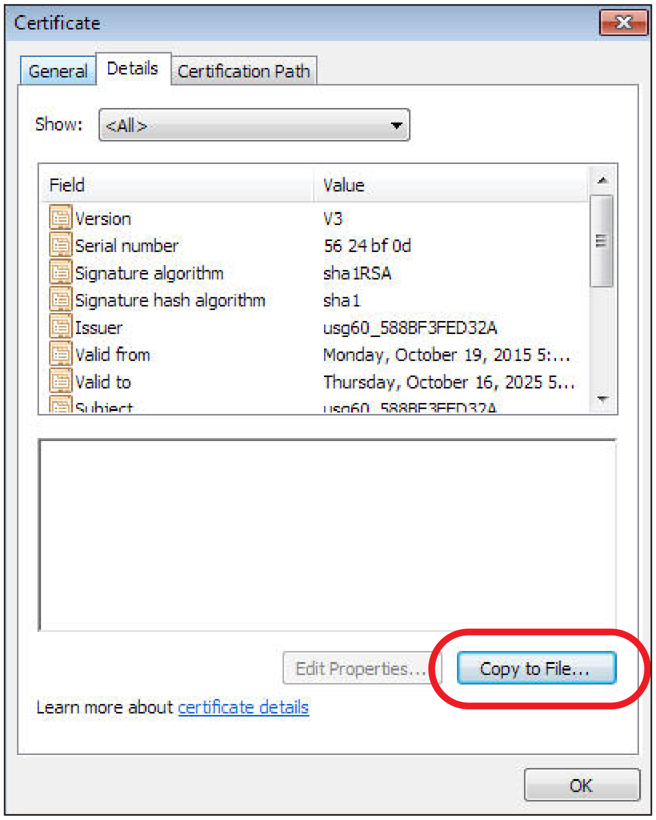


Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

You have chosen to disable security warnings for this site. Re-enable warnings

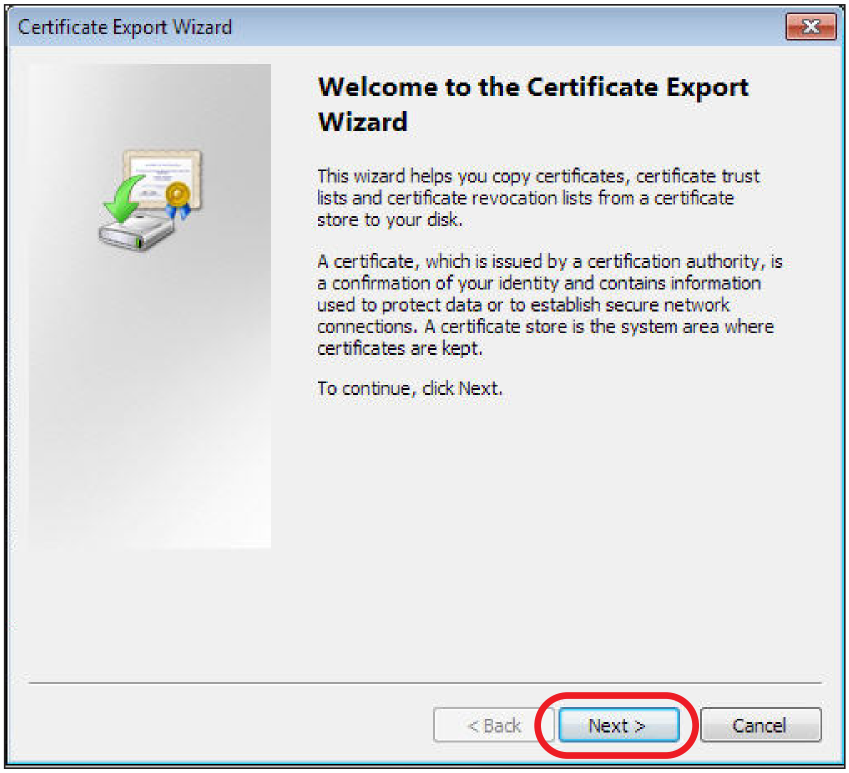
4 In the **Certificate** dialog box, click **Details > Copy to File**.



Field	Value
Version	V3
Serial number	56 24 bf 0d
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	usg60_588BF3FED32A
Valid from	Monday, October 19, 2015 5:...
Valid to	Thursday, October 16, 2025 5...
Subject	usg60_588BF3FED32A

Learn more about certificate details

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



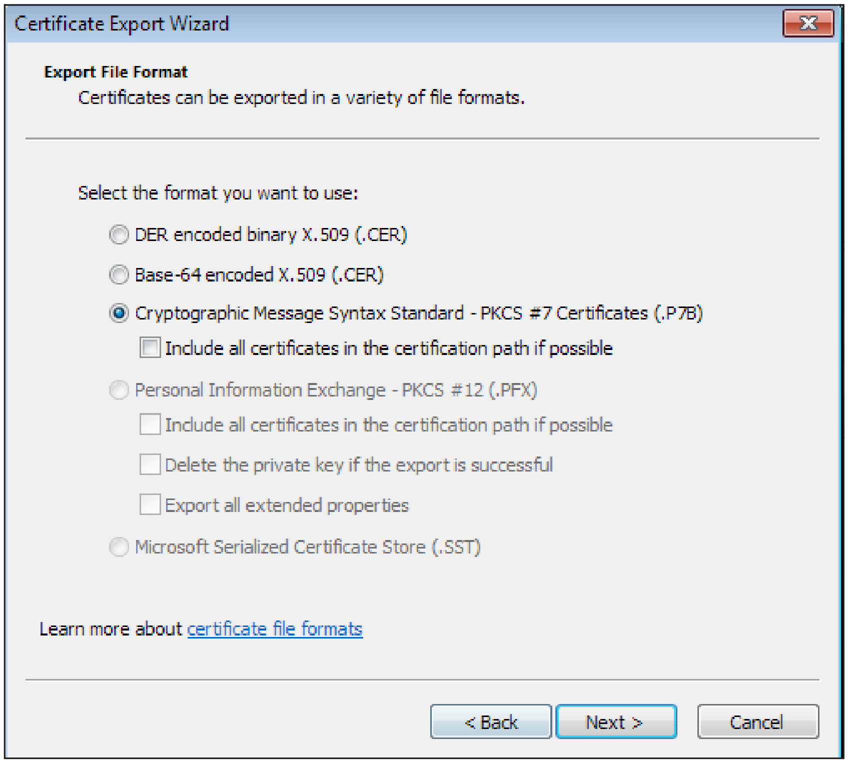
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

6 Select the format and settings you want to use and then click **Next**.



Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

● Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

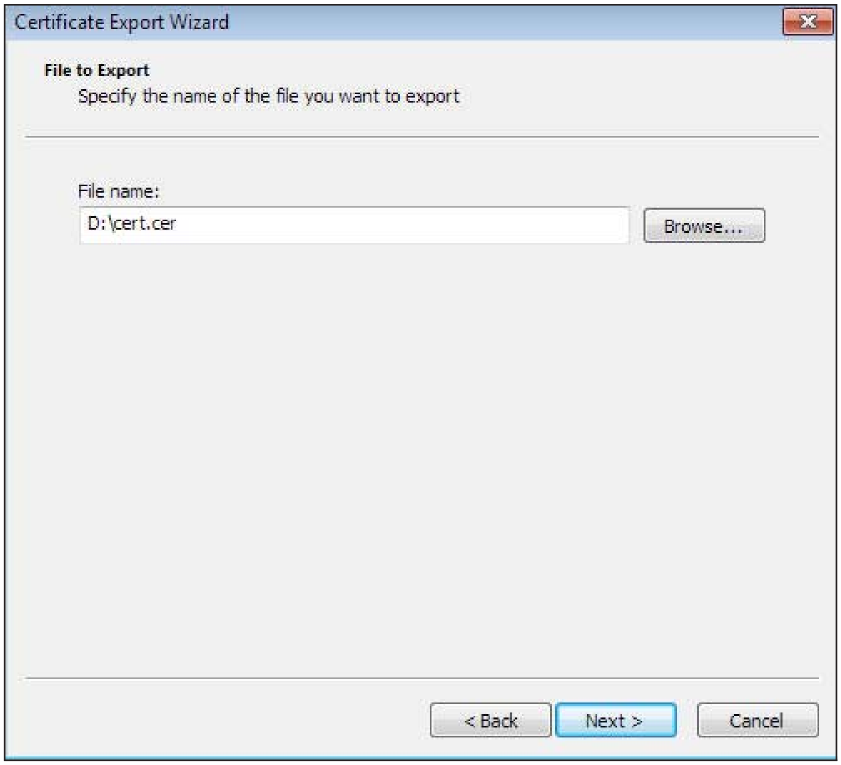
□ Delete the private key if the export is successful

□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

7 Type a filename and specify a folder to save the certificate in. Click **Next**.

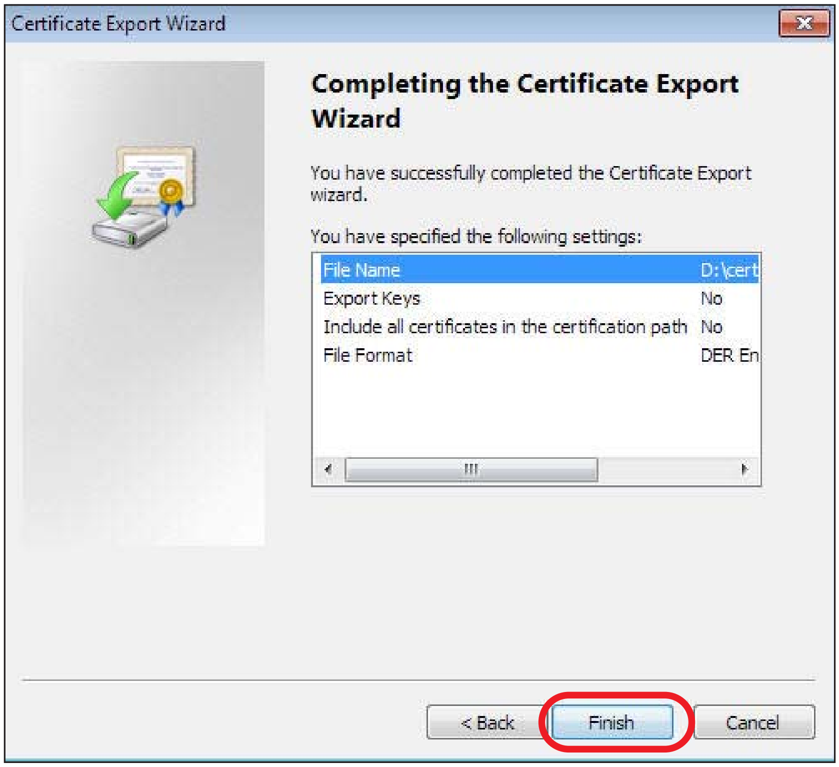


Certificate Export Wizard

File to Export
Specify the name of the file you want to export

File name:
D:\cert.cer

8 In the **Completing the Certificate Export Wizard** screen, click **Finish**.



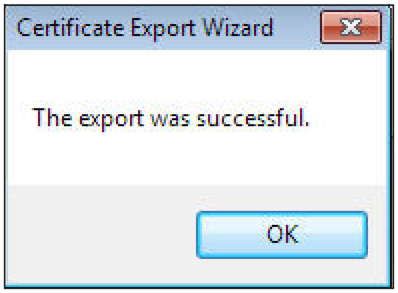
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	D:\cert
Export Keys	No
Include all certificates in the certification path	No
File Format	DER En

9 Finally, click **OK** when presented with the successful certificate export message.

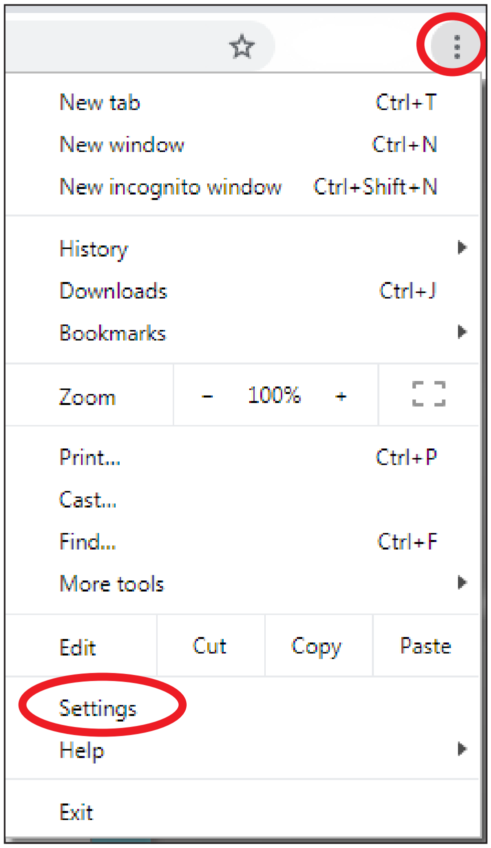


The export was successful.

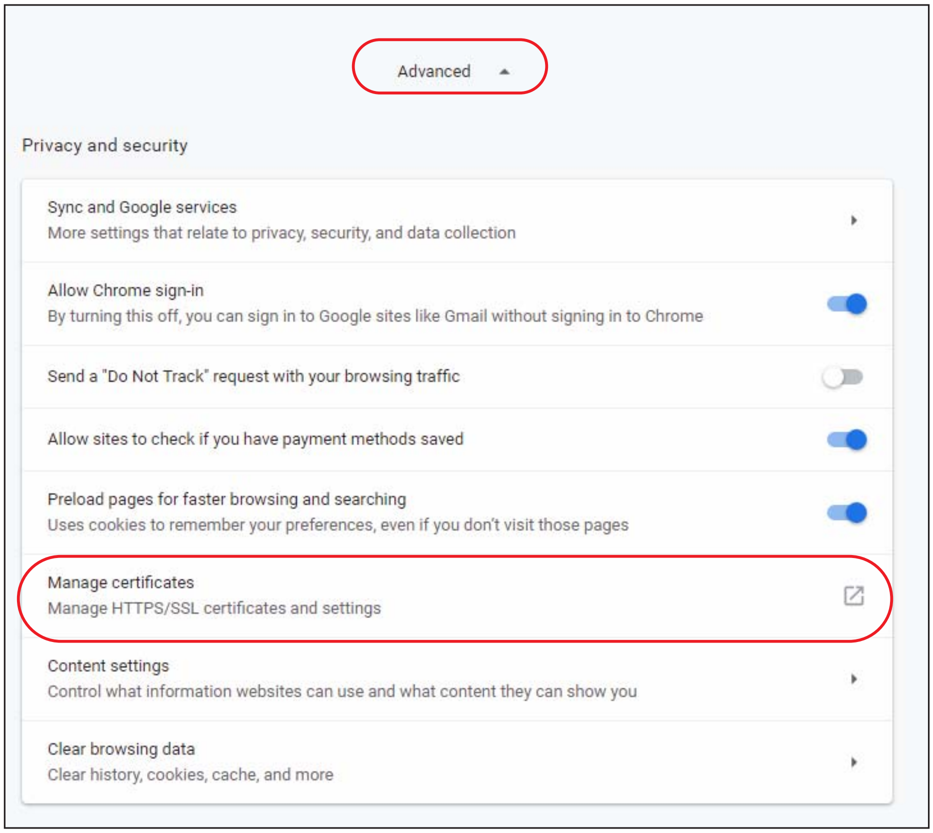
Import a Certificate

After storing the certificate in your computer (see Export a Certificate), you need to install it as a trusted root certification authority using the following steps:

1 Open your web browser, click the menu icon, and click **Settings**.



2 Scroll down and click **Advanced** to expand the menu. Under **Privacy and security**, click **Manage certificates**.



Advanced

Privacy and security

Sync and Google services
More settings that relate to privacy, security, and data collection

Allow Chrome sign-in
By turning this off, you can sign in to Google sites like Gmail without signing in to Chrome

Send a "Do Not Track" request with your browsing traffic

Allow sites to check if you have payment methods saved

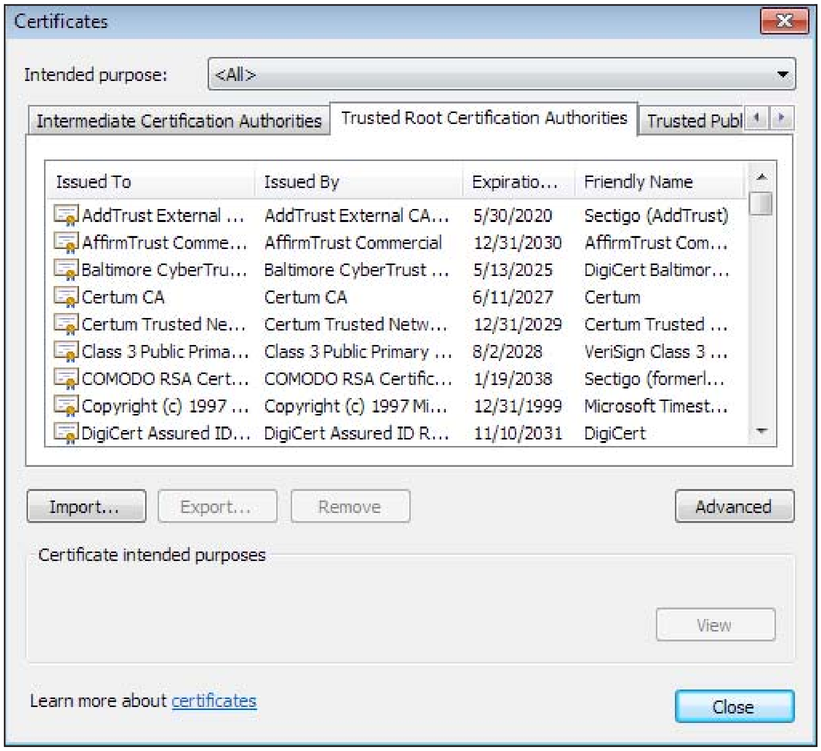
Preload pages for faster browsing and searching
Uses cookies to remember your preferences, even if you don't visit those pages

Manage certificates
Manage HTTPS/SSL certificates and settings

Content settings
Control what information websites can use and what content they can show you

Clear browsing data
Clear history, cookies, cache, and more

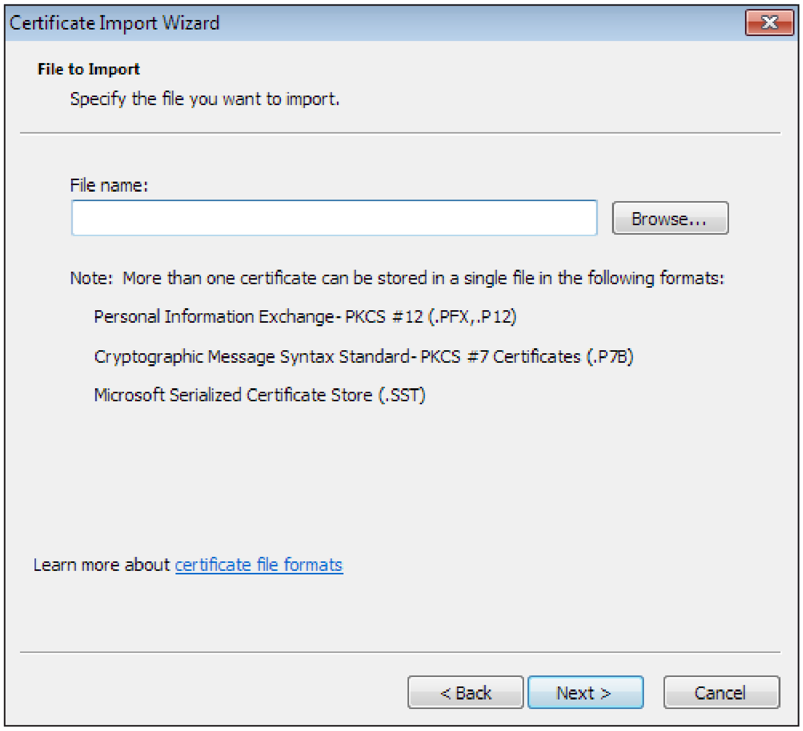
3 In the **Certificates** pop-up screen, click **Trusted Root Certification Authorities**. Click **Import** to start the **Certificate Import Wizard**.


Certificates
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced
Certificate intended purposes
View
Learn more about certificates
Close

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
AddTrust External ...	AddTrust External CA...	5/30/2020	Sectigo (AddTrust)
AffirmTrust Comme...	AffirmTrust Commercial	12/31/2030	AffirmTrust Com...
Baltimore CyberTru...	Baltimore CyberTrust ...	5/13/2025	DigiCert Baltimor...
Certum CA	Certum CA	6/11/2027	Certum
Certum Trusted Ne...	Certum Trusted Netw...	12/31/2029	Certum Trusted ...
Class 3 Public Prima...	Class 3 Public Primary ...	8/2/2028	VeriSign Class 3 ...
COMODO RSA Cert...	COMODO RSA Certific...	1/19/2038	Sectigo (formerl...
Copyright (c) 1997 ...	Copyright (c) 1997 Mi...	12/31/1999	Microsoft Timest...
DigiCert Assured ID...	DigiCert Assured ID R...	11/10/2031	DigiCert

4 Click **Next** when the wizard pops up, and then on the following screen click **Browse**.


Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
Browse...
Learn more about certificate file formats
< Back
Next >
Cancel

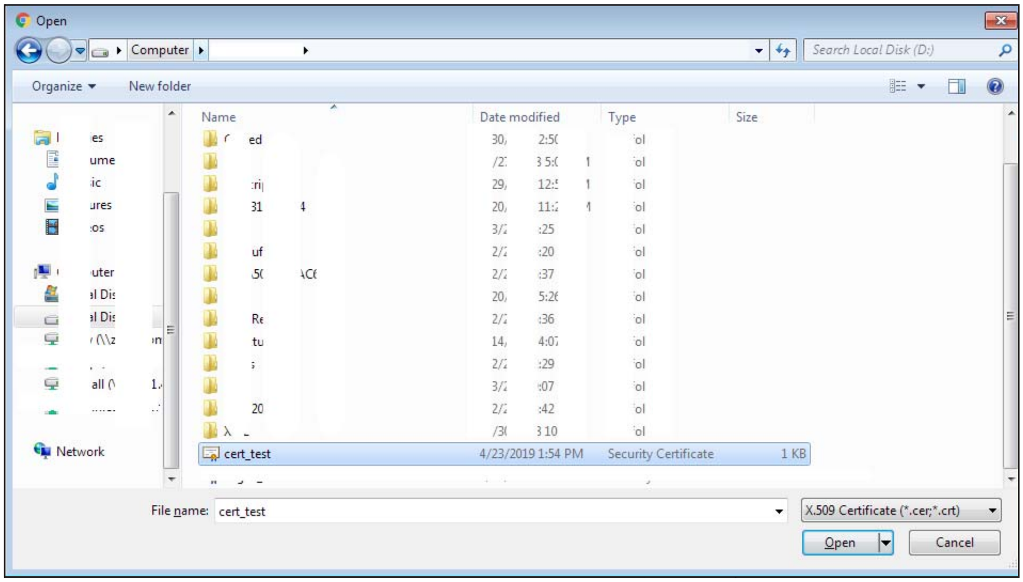
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

5 Select the certificate file you want to import and click **Open**.

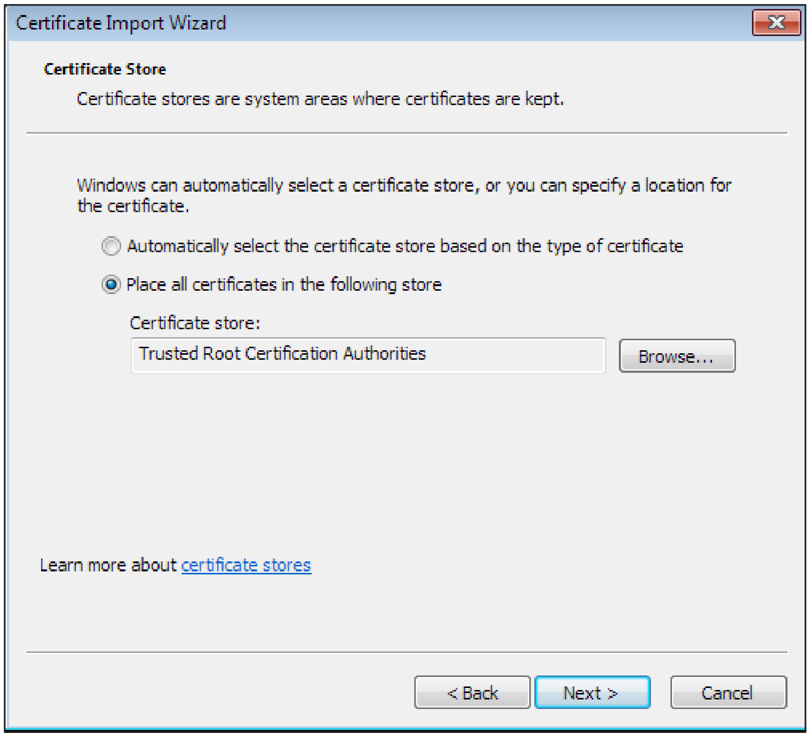


cert_test 4/23/2019 1:54 PM Security Certificate 1 KB

File name: cert_test

X.509 Certificate (*.cer;*.crt)

6 Click **Next.**



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

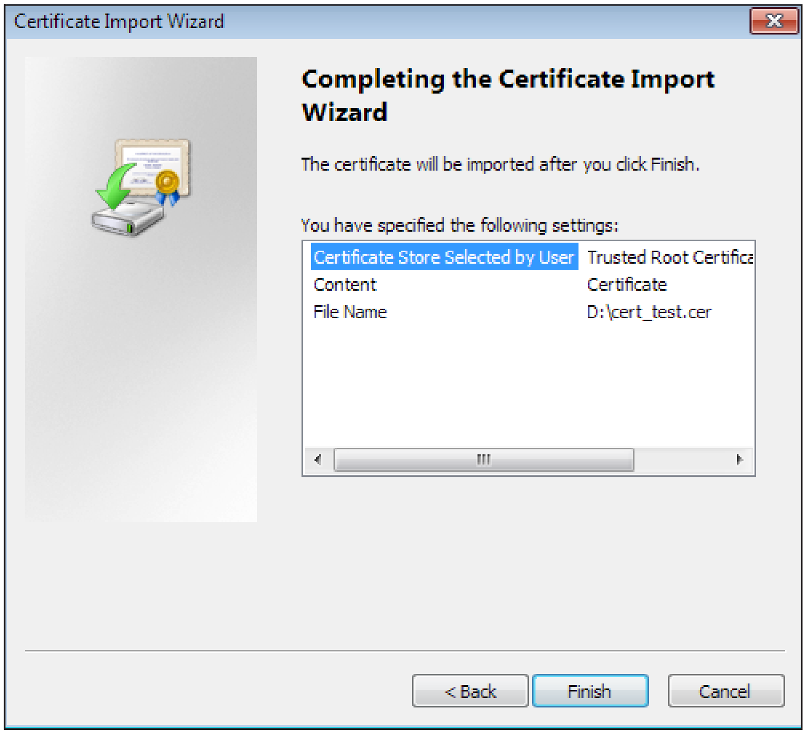
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

7 Confirm the settings displayed and click **Finish**.



Certificate Import Wizard

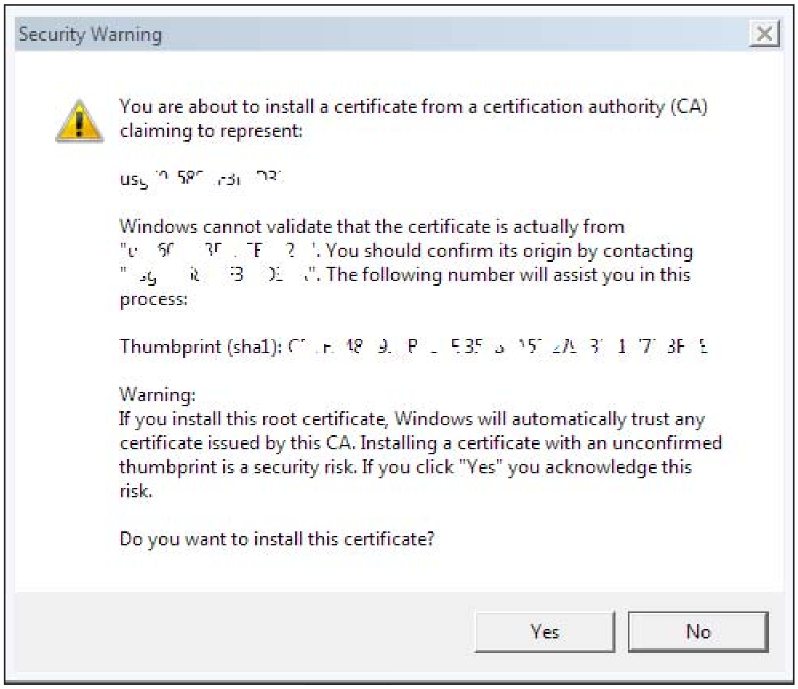
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certifica
Content	Certificate
File Name	D:\cert_test.cer

8 If presented with a security warning, click **Yes**.



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

usg [illegible]

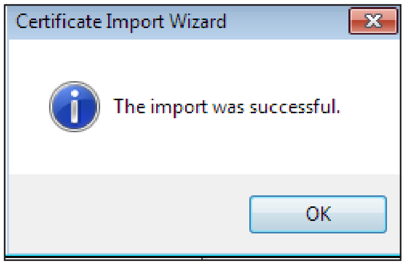
Windows cannot validate that the certificate is actually from "[illegible]". You should confirm its origin by contacting "[illegible]". The following number will assist you in this process:

Thumbprint (sha1): [illegible]

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

9 Finally, click **OK** when you are notified of the successful import.



Certificate Import Wizard

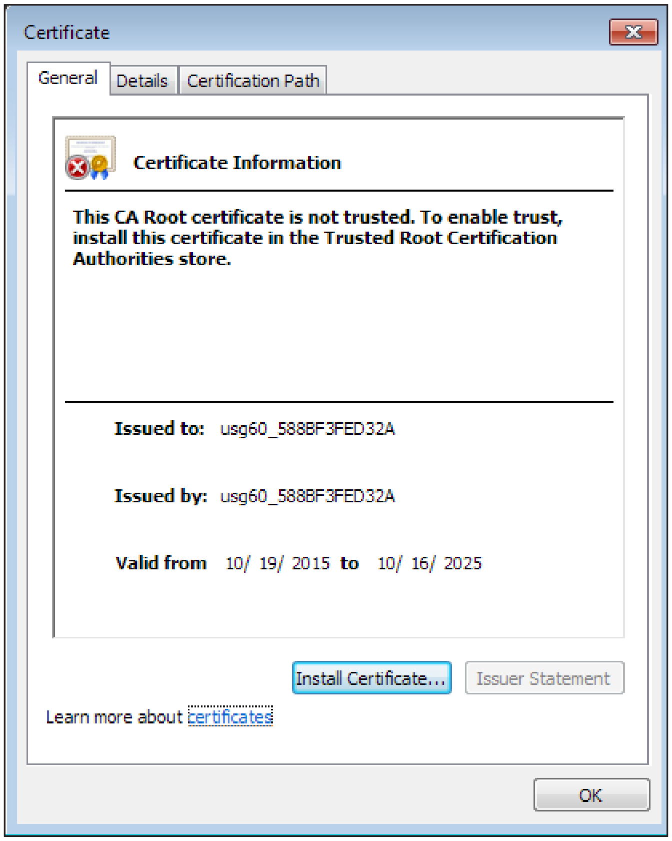
The import was successful.

Install a Stand-Alone Certificate File

Rather than installing a public key certificate using web browser settings, you can install a stand-alone certificate file if one has been issued to you.

1 Double-click the public key certificate file.

2 Click **Install Certificate**.



Certificate

Certificate Information

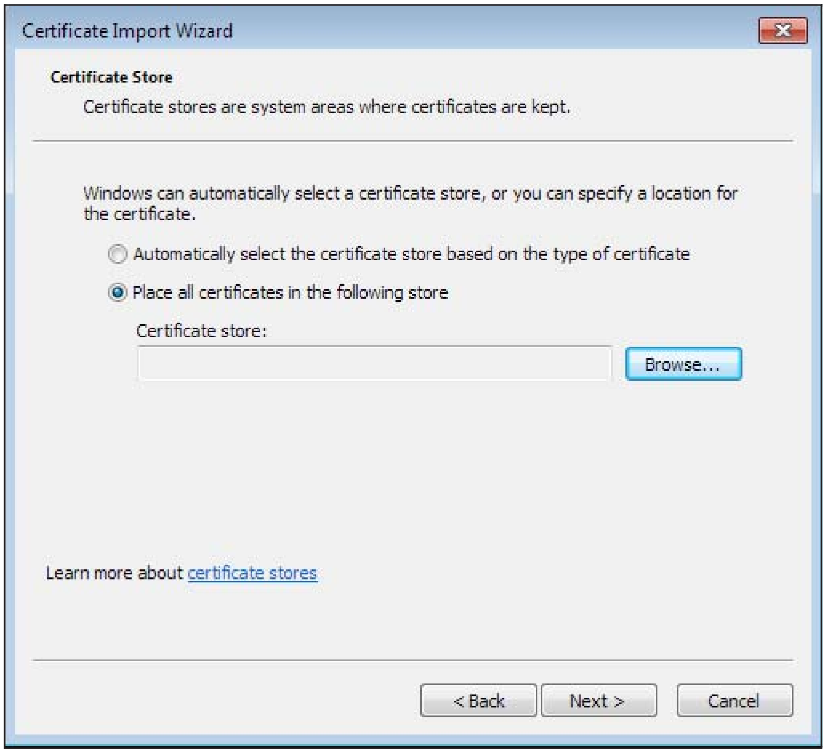
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: usg60_588BF3FED32A

Issued by: usg60_588BF3FED32A

Valid from 10/ 19/ 2015 to 10/ 16/ 2025

3 Click **Next** on the first wizard screen, click **Place all certificates in the following store**, and click **Browse**.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

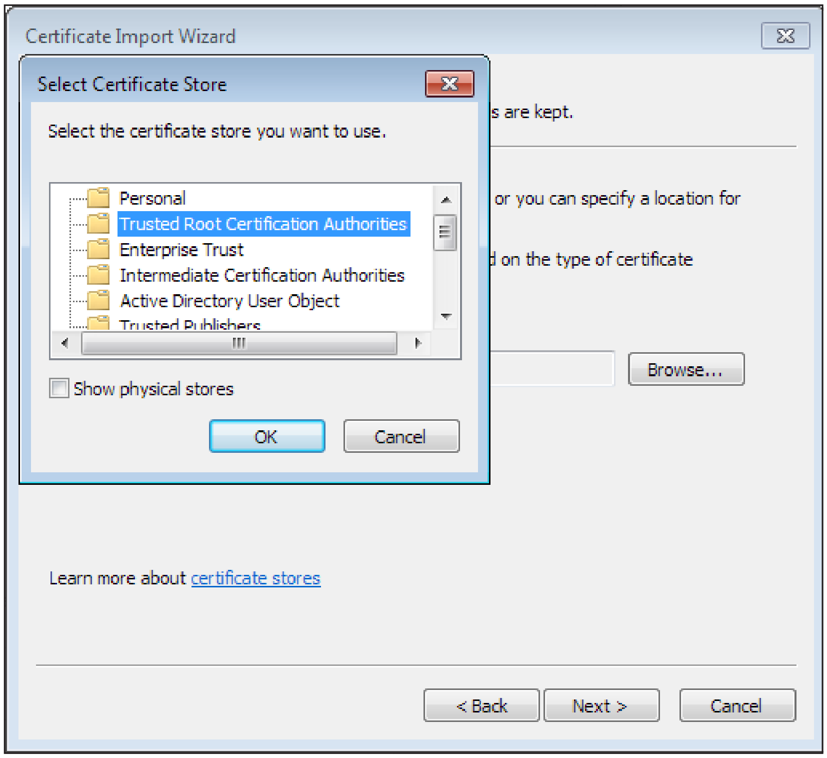
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

4 Select **Trusted Root Certificate Authorities** > **OK**, and then click **Next**.



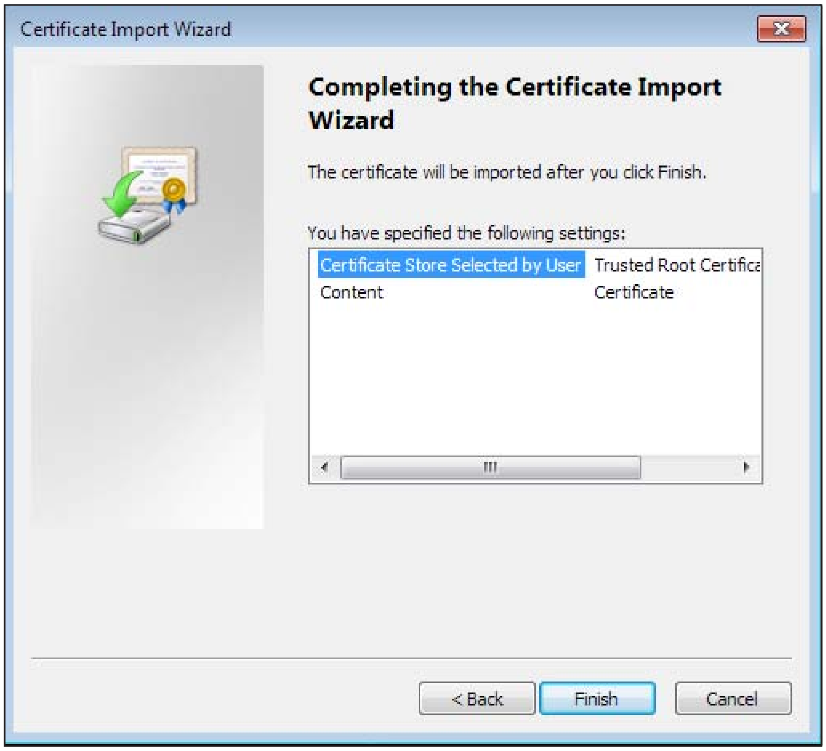
Certificate Import Wizard

Select Certificate Store

Select the certificate store you want to use.

Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
□ Show physical stores
OK
Cancel
s are kept.
or you can specify a location for
d on the type of certificate
Browse...
Learn more about certificate stores
< Back
Next >
Cancel

5 Confirm the information shown on the final wizard screen and click **Finish**.



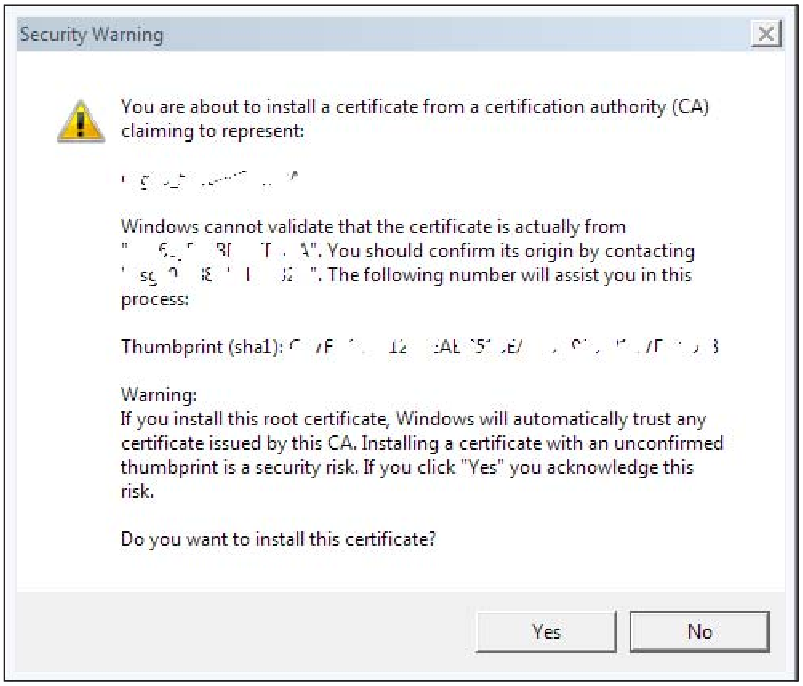
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certifica
Content	Certificate

6 If presented with a security warning, click **Yes**.



You are about to install a certificate from a certification authority (CA) claiming to represent:

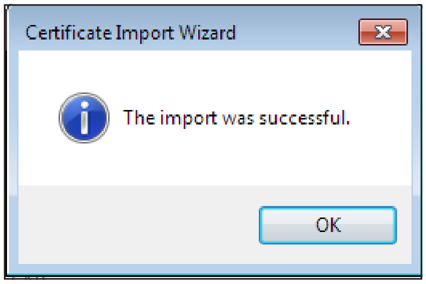
Windows cannot validate that the certificate is actually from " 6 3I T A". You should confirm its origin by contacting " sg 8 I J2 ". The following number will assist you in this process:

Thumbprint (sha1): C /F 12 :AE 5 E/ /F 3

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

7 Finally, click **OK** when you are notified of the successful import.



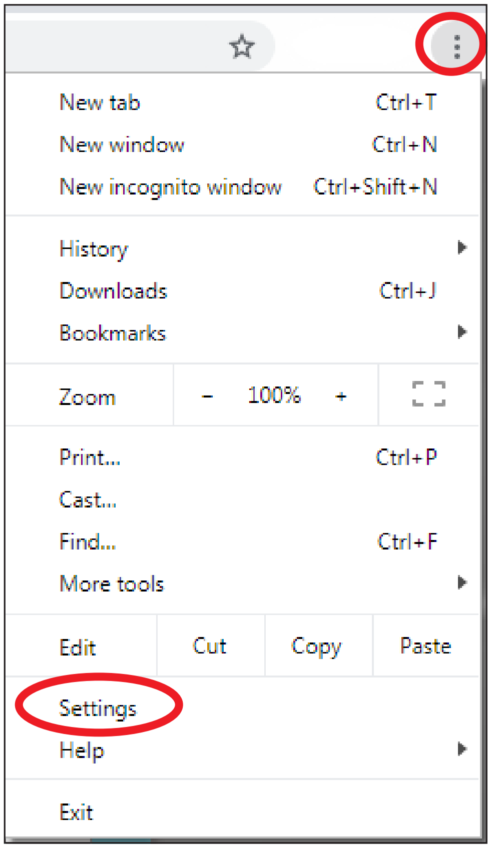
Certificate Import Wizard

The import was successful.

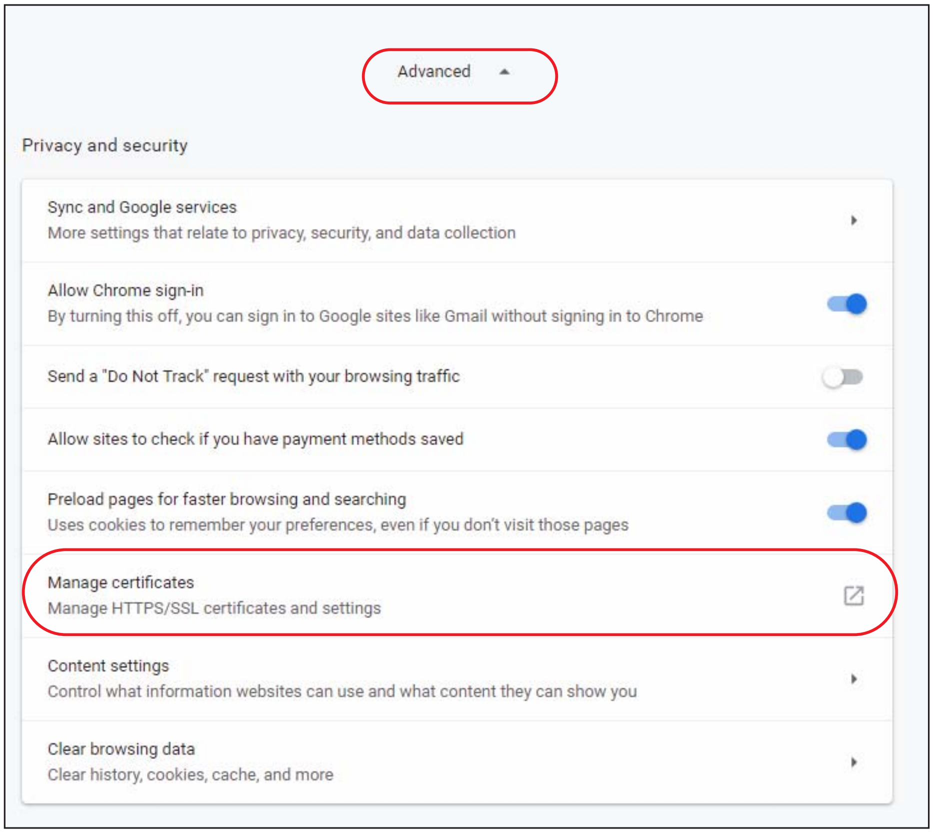
Remove a Certificate in Google Chrome

This section shows you how to remove a public key certificate in Google Chrome on Windows 7.

1 Open your web browser, click the menu icon, and click **Settings**.



2 Scroll down and click **Advanced** to expand the menu. Under **Privacy and security**, click **Manage certificates**.



Privacy and security

Sync and Google services
More settings that relate to privacy, security, and data collection

Allow Chrome sign-in
By turning this off, you can sign in to Google sites like Gmail without signing in to Chrome

Send a "Do Not Track" request with your browsing traffic

Allow sites to check if you have payment methods saved

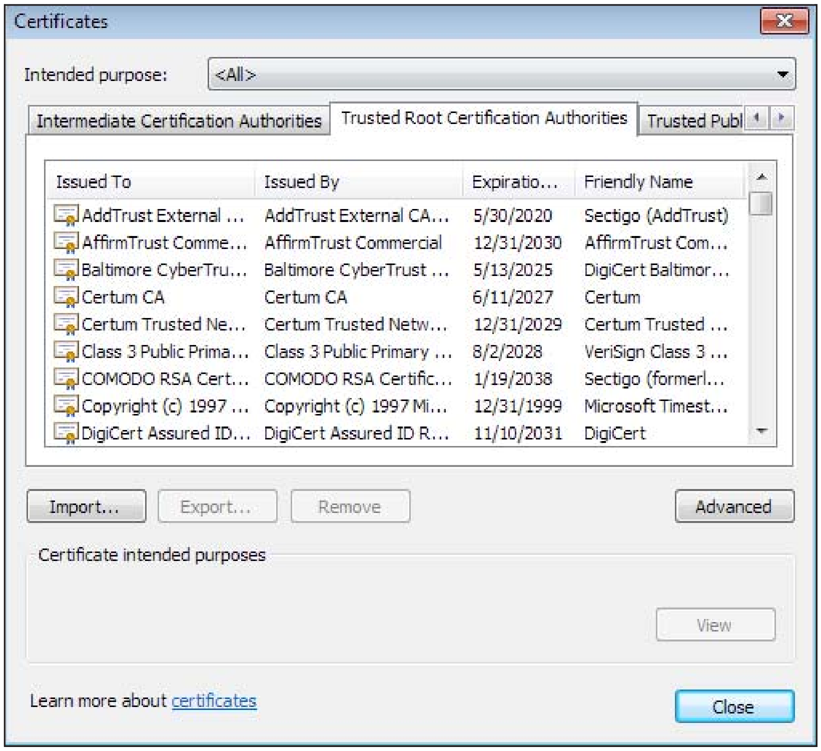
Preload pages for faster browsing and searching
Uses cookies to remember your preferences, even if you don't visit those pages

Manage certificates
Manage HTTPS/SSL certificates and settings

Content settings
Control what information websites can use and what content they can show you

Clear browsing data
Clear history, cookies, cache, and more

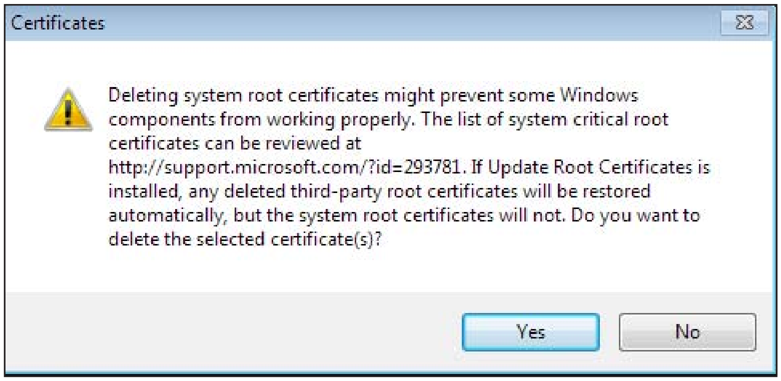
3 In the Certificates pop-up screen, click **Trusted Root Certification Authorities**.


Certificates
Intended purpose:
<All>
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ

Issued To	Issued By	Expiratio...	Friendly Name
AddTrust External ...	AddTrust External CA...	5/30/2020	Sectigo (AddTrust)
AffirmTrust Comme...	AffirmTrust Commercial	12/31/2030	AffirmTrust Com...
Baltimore CyberTru...	Baltimore CyberTrust ...	5/13/2025	DigiCert Baltimor...
Certum CA	Certum CA	6/11/2027	Certum
Certum Trusted Ne...	Certum Trusted Netw...	12/31/2029	Certum Trusted ...
Class 3 Public Prima...	Class 3 Public Primary ...	8/2/2028	VeriSign Class 3 ...
COMODO RSA Cert...	COMODO RSA Certific...	1/19/2038	Sectigo (formerl...
Copyright (c) 1997 ...	Copyright (c) 1997 Mi...	12/31/1999	Microsoft Timest...
DigiCert Assured ID...	DigiCert Assured ID R...	11/10/2031	DigiCert

4 Select the certificate you want to remove and click **Remove**.

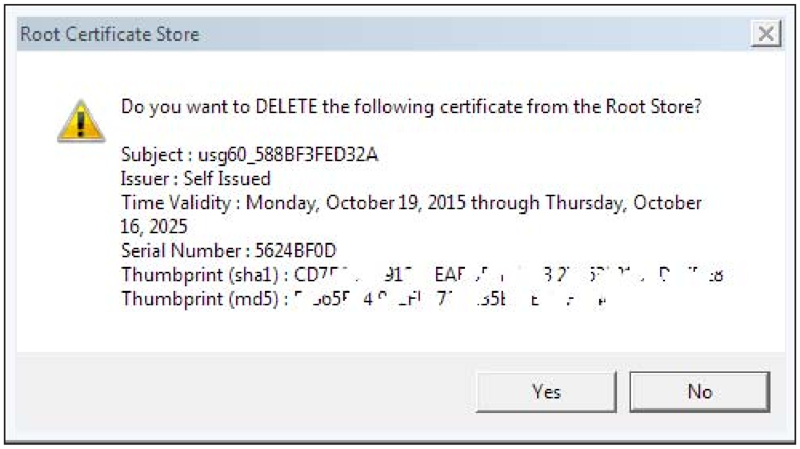
5 Click **Yes** when you see the following warning message.



Certificates

Deleting system root certificates might prevent some Windows components from working properly. The list of system critical root certificates can be reviewed at http://support.microsoft.com/?id=293781. If Update Root Certificates is installed, any deleted third-party root certificates will be restored automatically, but the system root certificates will not. Do you want to delete the selected certificate(s)?

6 Confirm the details displayed in the warning message and click **Yes**.



Root Certificate Store

Do you want to DELETE the following certificate from the Root Store?

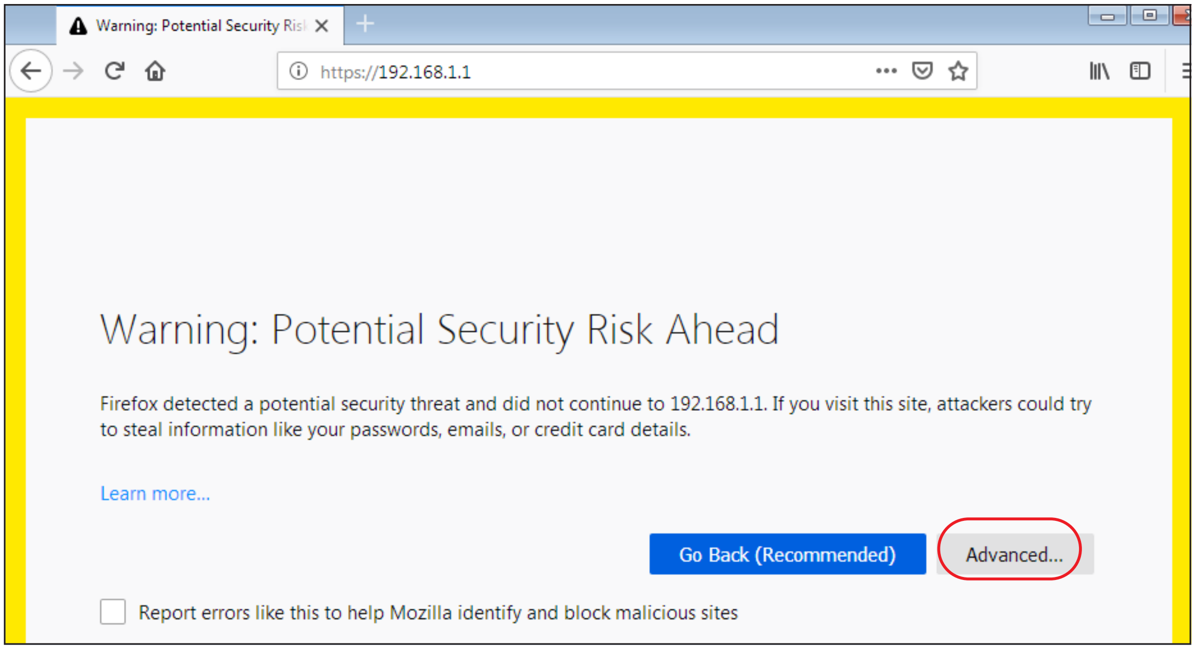
Subject : usg60_588BF3FED32A
Issuer : Self Issued
Time Validity : Monday, October 19, 2015 through Thursday, October 16, 2025
Serial Number : 5624BF0D
Thumbprint (sha1) : [redacted]
Thumbprint (md5) : [redacted]

Firefox

The following example uses Mozilla Firefox on Windows 7. You first have to store the certificate in your computer and then install it as a Trusted Root CA, as shown in the following tutorials.

Export a Certificate

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. Click **Advanced**.

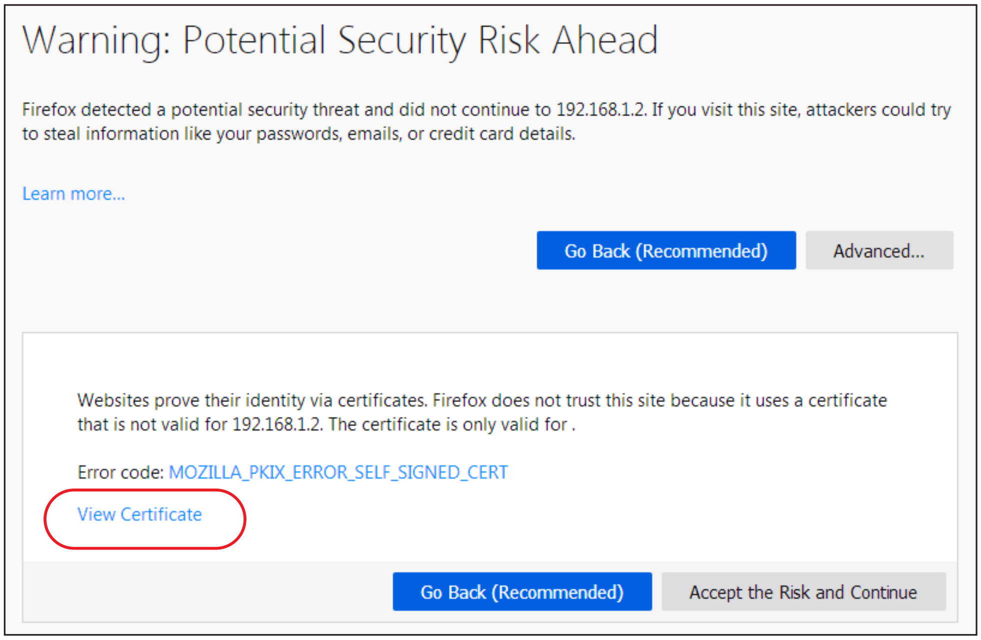


Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 192.168.1.1. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

□ Report errors like this to help Mozilla identify and block malicious sites

2 Click **View Certificate.**



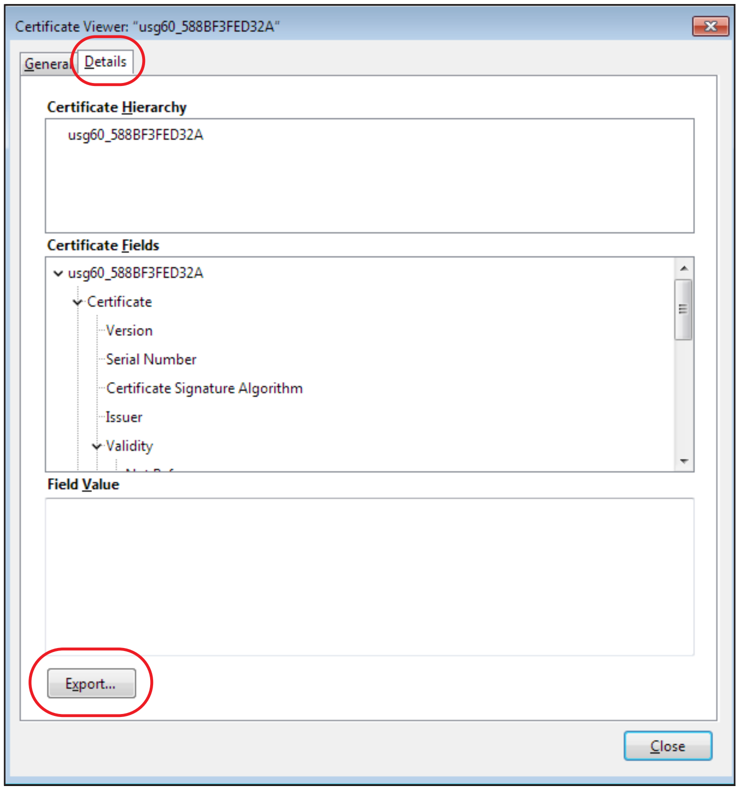
Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 192.168.1.2. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for 192.168.1.2. The certificate is only valid for .

Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

3 Click **Details** > **Export.**



Certificate Viewer: “usg60_588BF3FED32A”

Certificate Hierarchy

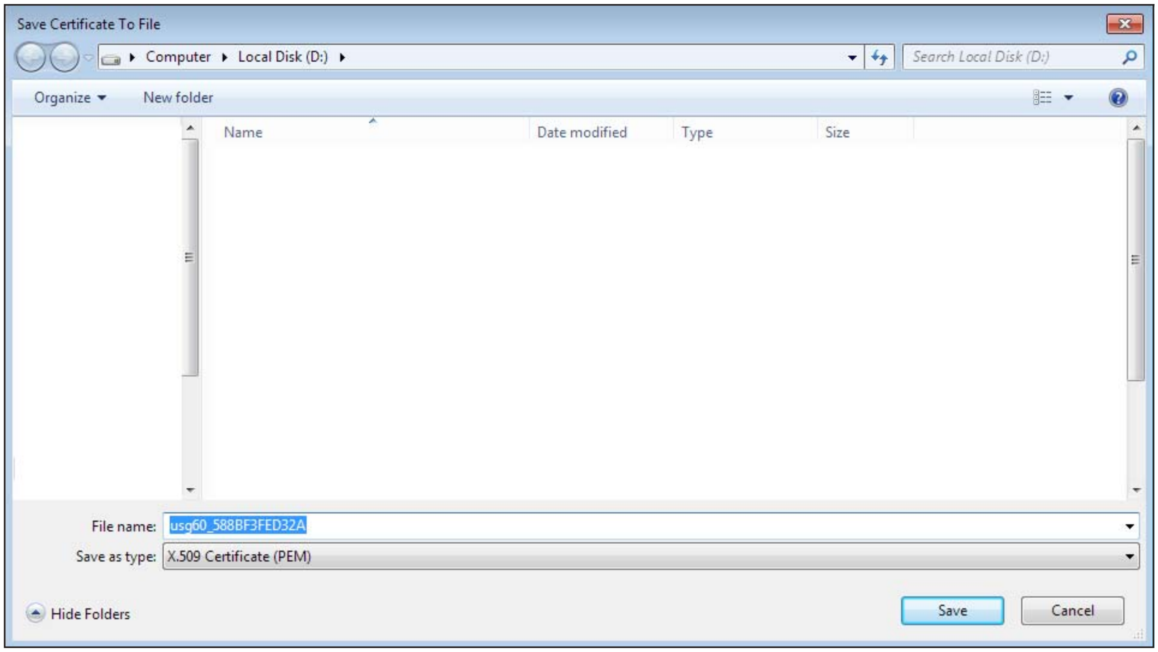
usg60_588BF3FED32A

Certificate Fields

```
usg60_588BF3FED32A
  Certificate
    Version
    Serial Number
    Certificate Signature Algorithm
    Issuer
    Validity
```

Field Value

4 Type a filename and click **Save**.



Save Certificate To File

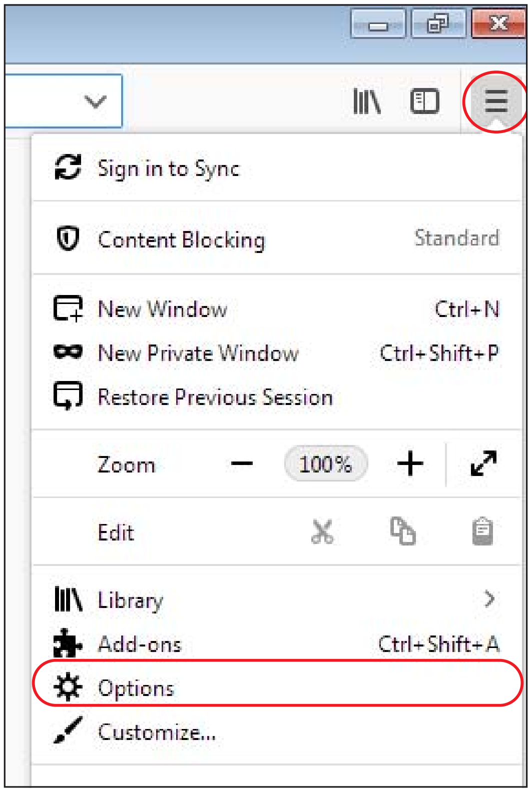
File name: usg60_588BF3FED32A

Save as type: X.509 Certificate (PEM)

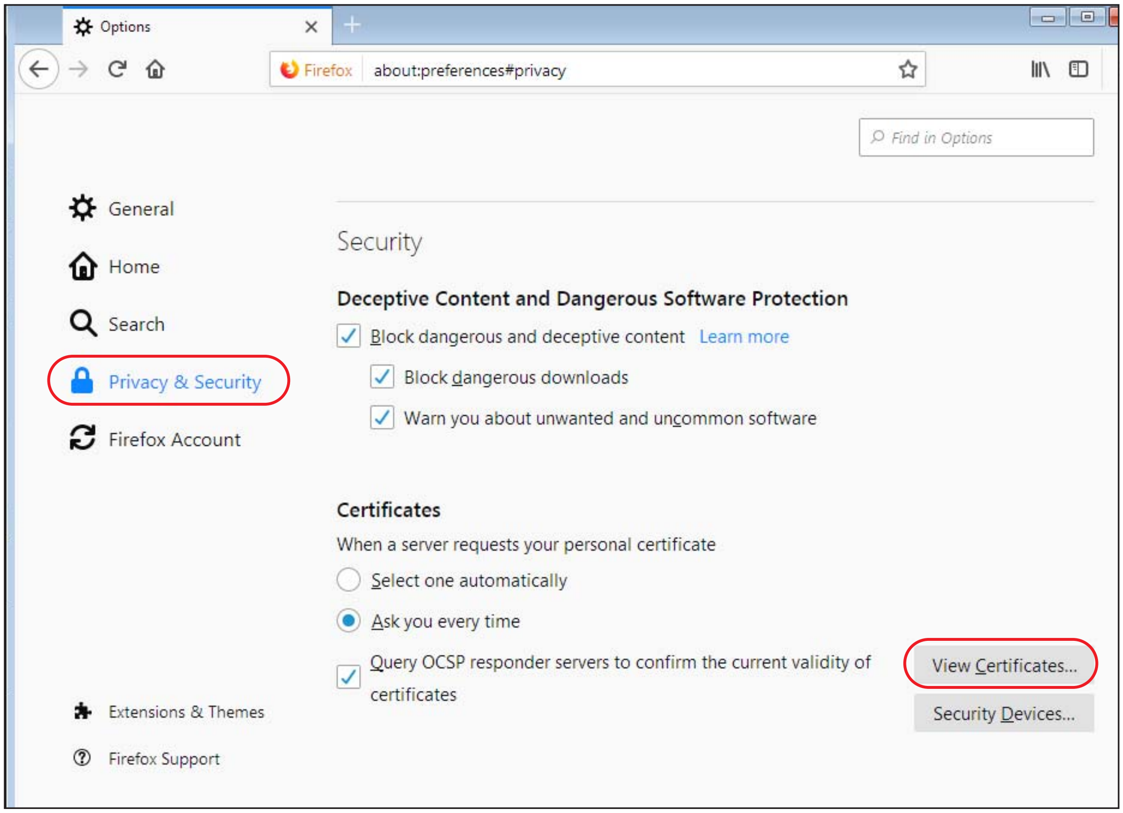
Import a Certificate

After storing the certificate in your computer, you need to import it in trusted root certification authorities using the following steps:

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



2 In the **Options** page, click **Privacy & Security**, scroll to the bottom of the page, and then click **View Certificates**.



Security

Deceptive Content and Dangerous Software Protection

☑ Block dangerous and deceptive content Learn more

☑ Block dangerous downloads

☑ Warn you about unwanted and uncommon software

Certificates

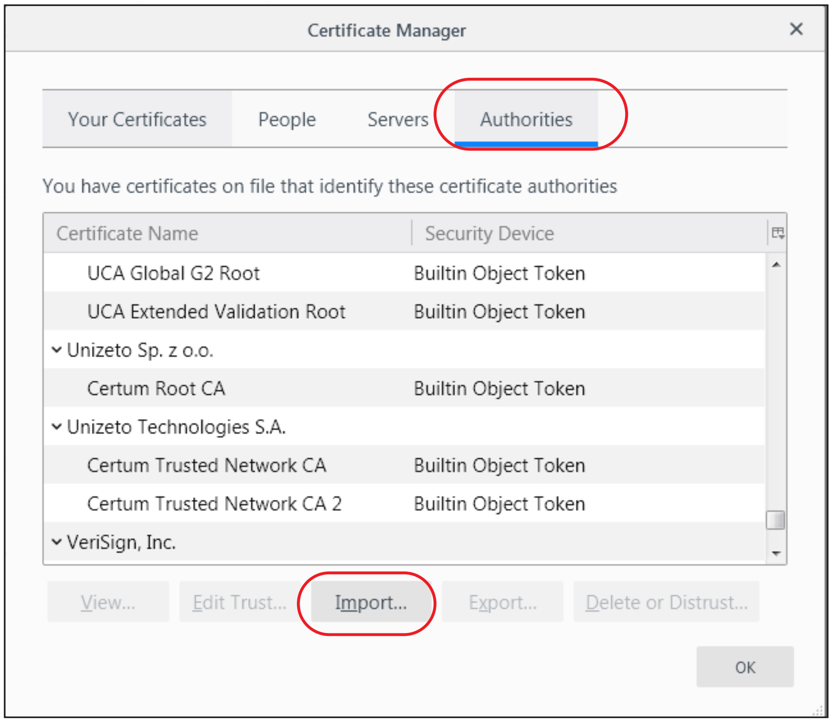
When a server requests your personal certificate

○ Select one automatically

● Ask you every time

☑ Query OCSP responder servers to confirm the current validity of certificates

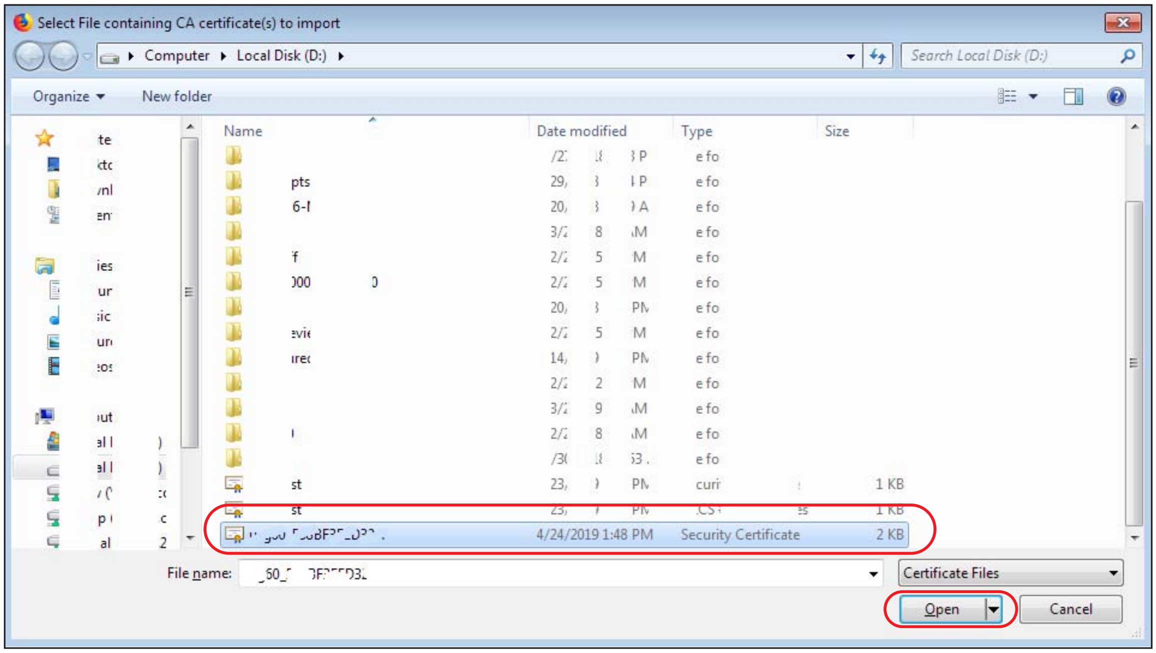
3 In the **Certificate Manager**, click **Authorities** > **Import**.



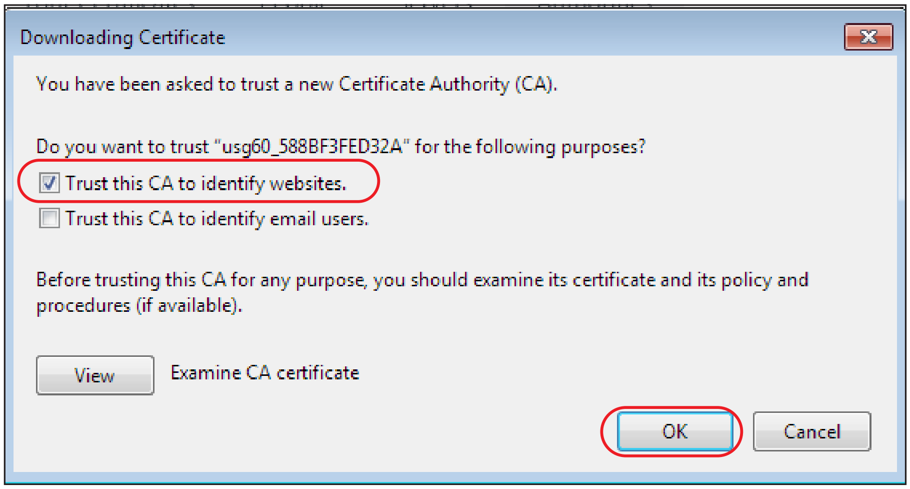
You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
UCA Global G2 Root	Builtin Object Token
UCA Extended Validation Root	Builtin Object Token
˅ Unizeto Sp. z o.o.	
Certum Root CA	Builtin Object Token
˅ Unizeto Technologies S.A.	
Certum Trusted Network CA	Builtin Object Token
Certum Trusted Network CA 2	Builtin Object Token
˅ VeriSign, Inc.	

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



5 Select **Trust this CA to identify websites** and click **OK**.


Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "usg60_588BF3FED32A" for the following purposes?

☑ Trust this CA to identify websites.

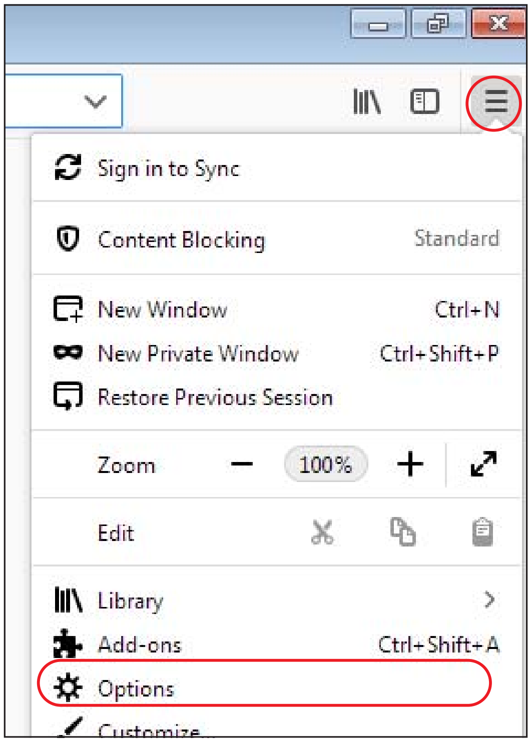
□ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

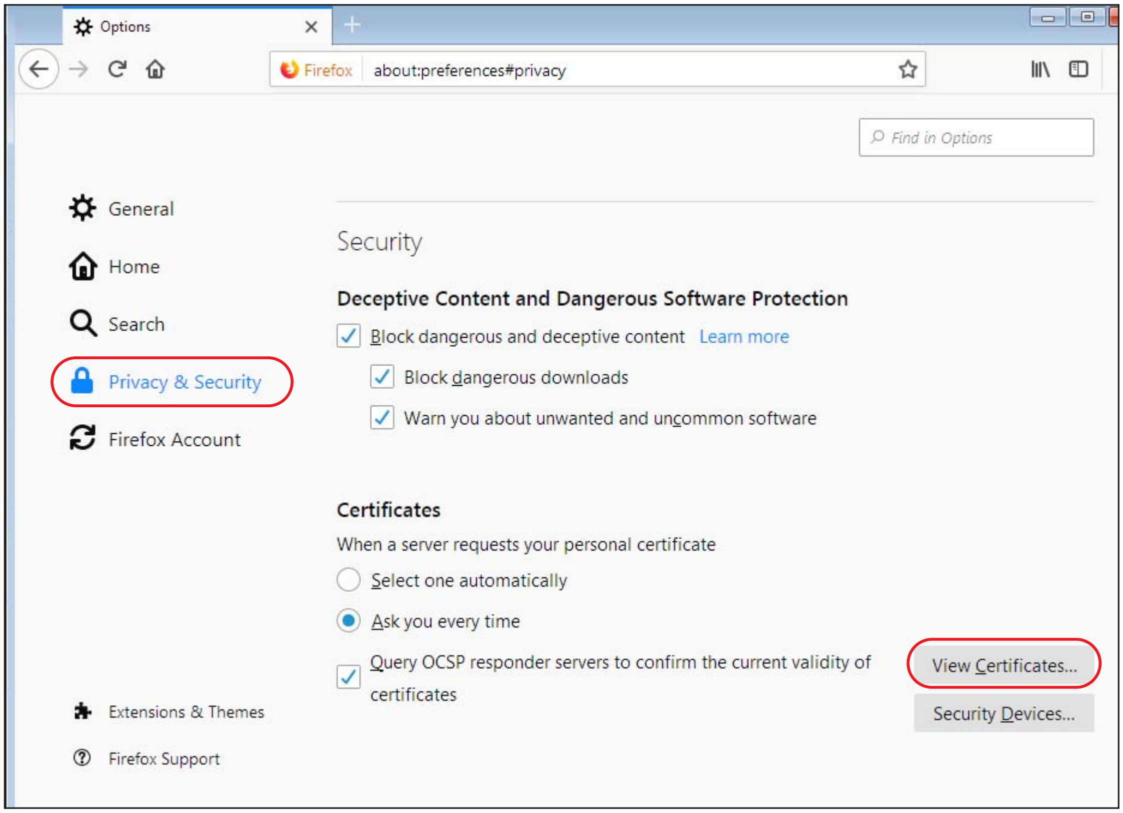
Removing a Certificate in Firefox

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

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



2 In the **Options** page, click **Privacy & Security**, scroll to the bottom of the page, and then click **View Certificates**.



Security

Deceptive Content and Dangerous Software Protection

☑ Block dangerous and deceptive content Learn more

☑ Block dangerous downloads

☑ Warn you about unwanted and uncommon software

Certificates

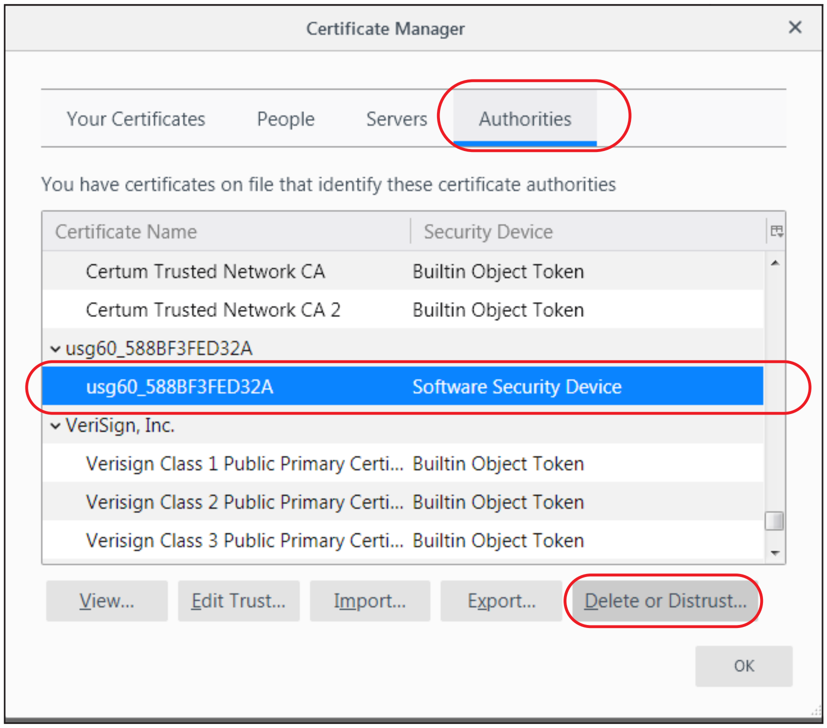
When a server requests your personal certificate

○ Select one automatically

● Ask you every time

☑ Query OCSP responder servers to confirm the current validity of certificates

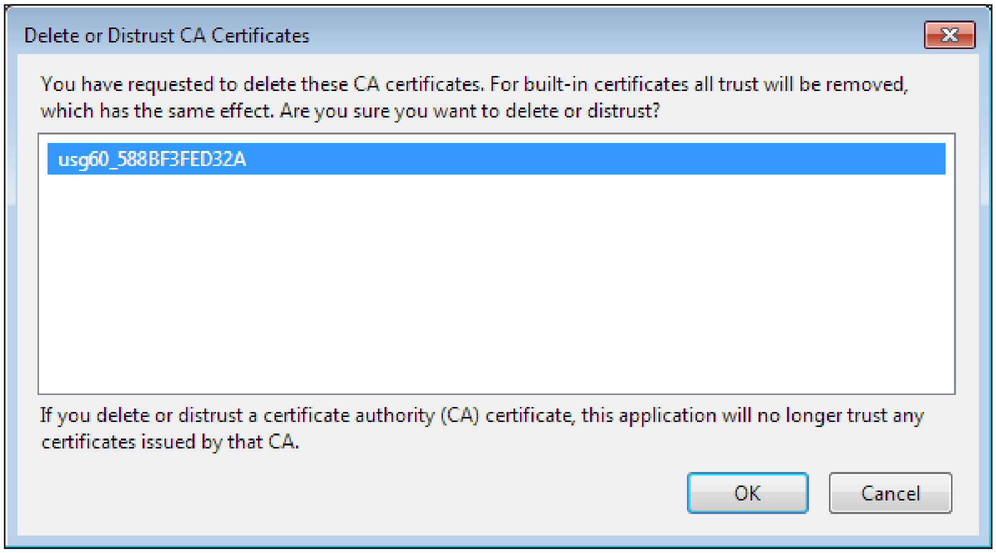
3 In the **Certificate Manager**, click **Authorities** and select the certificate you want to remove, Click **Delete or Distrust**.



You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
Certum Trusted Network CA	Builtin Object Token
Certum Trusted Network CA 2	Builtin Object Token
⌄ usg60_588BF3FED32A	
usg60_588BF3FED32A	Software Security Device
⌄ VeriSign, Inc.	
Verisign Class 1 Public Primary Certi...	Builtin Object Token
Verisign Class 2 Public Primary Certi...	Builtin Object Token
Verisign Class 3 Public Primary Certi...	Builtin Object Token

4 In the following dialog box, click **OK**.



You have requested to delete these CA certificates. For built-in certificates all trust will be removed, which has the same effect. Are you sure you want to delete or distrust?

usg60_588BF3FED32A

If you delete or distrust a certificate authority (CA) certificate, this application will no longer trust any certificates issued by that CA.

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

APPENDIX B
IPv6

Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

Table 103 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a "public IP address" in IPv4. A global unicast address starts with a 2 or 3.

Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to “0.0.0.0” in IPv4.

Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to “127.0.0.1” in IPv4.

Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

Table 104 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP severs on a local site.

The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

Table 105 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

Table 106

MAC	00	:	13	:	49 : 12	:	34	:	56

Table 107

EUI-64	02	:	13	:	49 :	FF	:	FE	: 12	:	34	:	56

Stateless Autoconfiguration

With stateless autoconfiguration in IPv6, addresses can be uniquely and automatically generated. Unlike DHCPv6 (Dynamic Host Configuration Protocol version six) which is used in IPv6 stateful autoconfiguration, the owner and status of addresses don't need to be maintained by a DHCP server. Every IPv6 device is able to generate its own and unique IP address automatically when IPv6 is initiated on its interface. It combines the prefix and the interface ID (generated from its own Ethernet MAC address, see Interface ID and EUI-64) to form a complete IPv6 address.

When IPv6 is enabled on a device, its interface automatically generates a link-local address (beginning with fe80).

When the interface is connected to a network with a router and the Zyxel Device is set to automatically obtain an IPv6 network prefix from the router for the interface, it generates [1]another address which combines its interface ID and global and subnet information advertised from the router. This is a routable global IP address.

DHCPv6

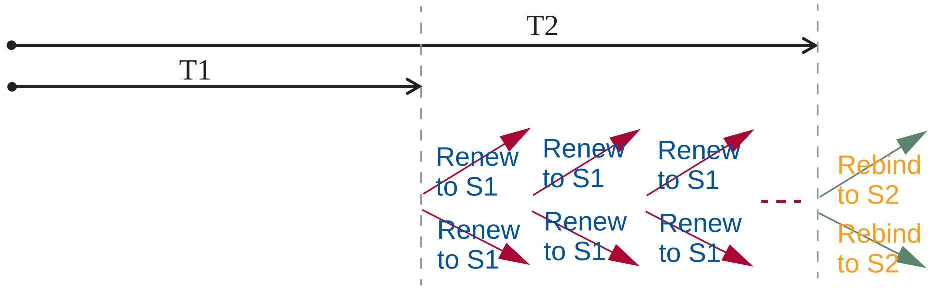
The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

[1] In IPv6, all network interfaces can be associated with several addresses.

Each DHCP client and server has a unique DHCP Unique IDentifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.
The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Zyxel Device uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the Zyxel Device passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor’s reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor’s link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being “reachable” means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Zyxel Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Zyxel Device configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Zyxel Device also sends out a neighbor solicitation message. When the Zyxel Device receives a neighbor advertisement in response, it stores the neighbor’s link-layer address in the neighbor cache. When the Zyxel Device uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router’s information to the neighbor cache, prefix list and destination cache. The Zyxel Device creates an entry in the default router list cache if the router can be used as a default router.

When the Zyxel Device needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Zyxel Device uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is onlink, the address is considered as the next hop. Otherwise, the Zyxel Device determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Zyxel Device looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Zyxel Device cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example - Enabling IPv6 on Windows XP/2003/Vista

By default, Windows XP and Windows 2003 support IPv6. This example shows you how to use the `ipv6 install` command on Windows XP/2003 to enable IPv6. This also displays how to use the `ipconfig` command to see auto-generated IP addresses.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.1.46
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : fe80::2d0:59ff:feb8:103c%4
        Default Gateway . . . . . . . . . : 10.1.1.254
```

IPv6 is installed and enabled by default in Windows Vista. Use the `ipconfig` command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

Example - Enabling DHCPv6 on Windows XP

Windows XP does not support DHCPv6. If your network uses DHCPv6 for IP address assignment, you have to additionally install a DHCPv6 client software on your Windows XP. (Note: If you use static IP addresses or Router Advertisement for IPv6 address assignment in your network, ignore this section.)

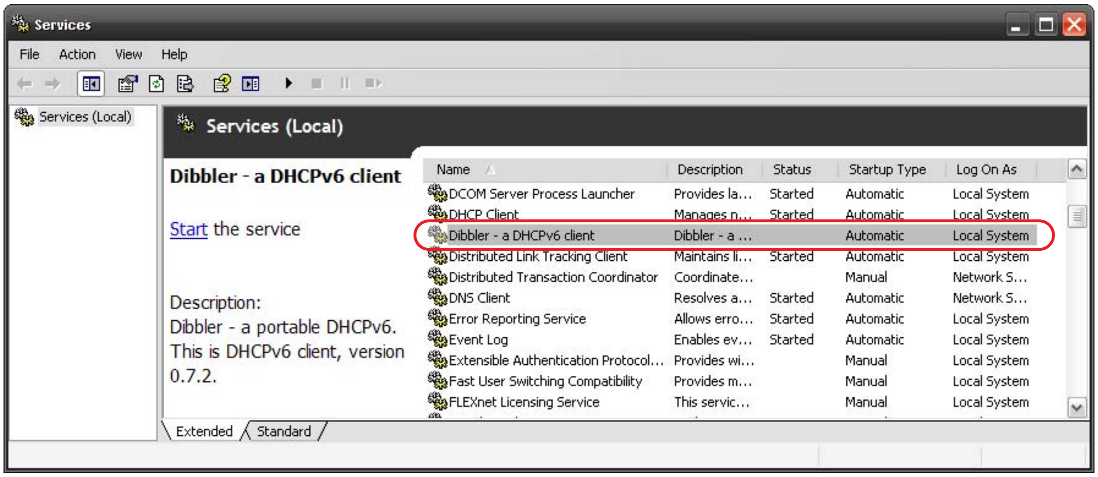
This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:

1 Install Dibbler and select the DHCPv6 client option on your computer.

2 After the installation is complete, select **Start** > **All Programs** > **Dibbler-DHCPv6** > **Client Install as service**.

3 Select **Start** > **Control Panel** > **Administrative Tools** > **Services**.

4 Double click **Dibbler - a DHCPv6 client**.



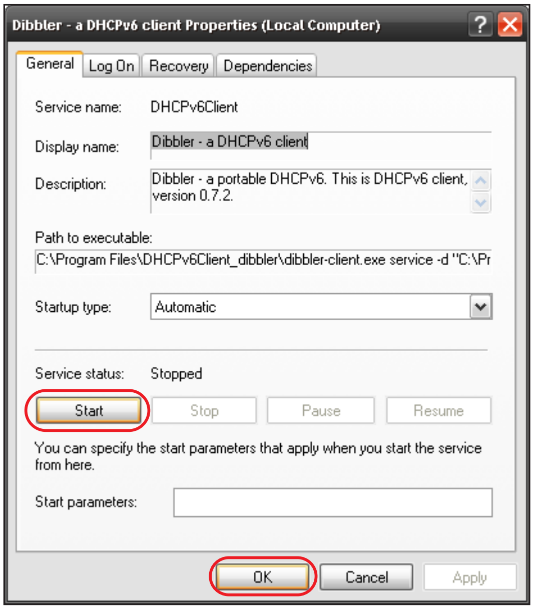
Dibbler - a DHCPv6 client

Start the service

Description:
Dibbler - a portable DHCPv6. This is DHCPv6 client, version 0.7.2.

Name	Description	Status	Startup Type	Log On As
DCOM Server Process Launcher	Provides la...	Started	Automatic	Local System
DHCP Client	Manages n...	Started	Automatic	Local System
Dibbler - a DHCPv6 client	Dibbler - a ...		Automatic	Local System
Distributed Link Tracking Client	Maintains li...	Started	Automatic	Local System
Distributed Transaction Coordinator	Coordinate...		Manual	Network S...
DNS Client	Resolves a...	Started	Automatic	Network S...
Error Reporting Service	Allows erro...	Started	Automatic	Local System
Event Log	Enables ev...	Started	Automatic	Local System
Extensible Authentication Protocol...	Provides wi...		Manual	Local System
Fast User Switching Compatibility	Provides m...		Manual	Local System
FLEXnet Licensing Service	This servic...		Manual	Local System

5 Click **Start** and then **OK**.



Service name: DHCPv6Client

Display name: Dibbler - a DHCPv6 client

Description: Dibbler - a portable DHCPv6. This is DHCPv6 client, version 0.7.2.

Path to executable:
C:\Program Files\DHCPv6Client_dibbler\dibbler-client.exe service -d "C:\Pr

Startup type: Automatic

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

6 Now your computer can obtain an IPv6 address from a DHCPv6 server.

Example - Enabling IPv6 on Windows 7

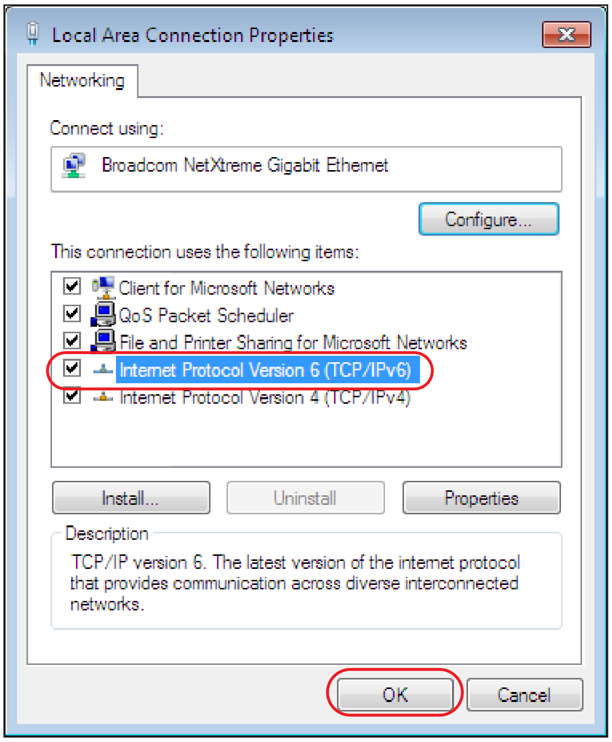
Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

1 Select **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.

2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.

3 Click **OK** to save the change.



Connect using:

Broadcom NetXtreme Gigabit Ethernet

This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)

Description

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

4 Click **Close** to exit the **Local Area Connection Status** screen.

5 Select **Start** > **All Programs** > **Accessories** > **Command Prompt**.

6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . : 172.16.100.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:feaa:7125%11
                                       172.16.100.254
```

APPENDIX C
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.

See *https://www.zyxel.com/homepage.shtml* and also *https://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml* for the latest information.

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.

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications Corporation
- http://www.zyxel.com

Asia

China

- Zyxel Communications (Shanghai) Corp.
  Zyxel Communications (Beijing) Corp.
  Zyxel Communications (Tianjin) Corp.
- https://www.zyxel.com/cn/zh/

India

- Zyxel Technology India Pvt Ltd
- https://www.zyxel.com/in/en/

Kazakhstan

- Zyxel Kazakhstan
- https://www.zyxel.kz

Korea

- Zyxel Korea Corp.
- http://www.zyxel.kr

Malaysia

- Zyxel Malaysia Sdn Bhd.
- http://www.zyxel.com.my

Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

Philippines

- Zyxel Philippines
- http://www.zyxel.com.ph

Singapore

- Zyxel Singapore Pte Ltd.
- http://www.zyxel.com.sg

Taiwan

- Zyxel Communications Corporation
- https://www.zyxel.com/tw/zh/

Thailand

- Zyxel Thailand Co., Ltd
- https://www.zyxel.com/th/th/

Vietnam

- Zyxel Communications Corporation-Vietnam Office
- https://www.zyxel.com/vn/vi

Europe

Belarus

- Zyxel BY
- https://www.zyxel.by

Belgium

- Zyxel Communications B.V.
- https://www.zyxel.com/be/nl/

- https://www.zyxel.com/be/fr/

Bulgaria

- Zyxel България
- https://www.zyxel.com/bg/bg/

Czech Republic

- Zyxel Communications Czech s.r.o
- https://www.zyxel.com/cz/cs/

Denmark

- Zyxel Communications A/S
- https://www.zyxel.com/dk/da/

Estonia

- Zyxel Estonia
- https://www.zyxel.com/ee/et/

Finland

- Zyxel Communications
- https://www.zyxel.com/fi/fi/

France

- Zyxel France
- https://www.zyxel.fr

Germany

- Zyxel Deutschland GmbH
- https://www.zyxel.com/de/de/

Hungary

- Zyxel Hungary & SEE
- https://www.zyxel.com/hu/hu/

Italy

- Zyxel Communications Italy
- https://www.zyxel.com/it/it/

Latvia

- Zyxel Latvia
- https://www.zyxel.com/lv/lv/

Lithuania

- Zyxel Lithuania
- https://www.zyxel.com/lt/lt/

Netherlands

- Zyxel Benelux
- https://www.zyxel.com/nl/nl/

Norway

- Zyxel Communications
- https://www.zyxel.com/no/no/

Poland

- Zyxel Communications Poland
- https://www.zyxel.com/pl/pl/

Romania

- Zyxel Romania
- https://www.zyxel.com/ro/ro

Russia

- Zyxel Russia
- https://www.zyxel.com/ru/ru/

Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- https://www.zyxel.com/sk/sk/

Spain

- Zyxel Communications ES Ltd
- https://www.zyxel.com/es/es/

Sweden

- Zyxel Communications
- https://www.zyxel.com/se/sv/

Switzerland

- Studerus AG
- https://www.zyxel.ch/de
- https://www.zyxel.ch/fr

Turkey

- Zyxel Turkey A.S.
- https://www.zyxel.com/tr/tr/

UK

- Zyxel Communications UK Ltd.
- https://www.zyxel.com/uk/en/

Ukraine

- Zyxel Ukraine
- http://www.ua.zyxel.com

South America

Argentina

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

Brazil

- Zyxel Communications Brasil Ltda.
- https://www.zyxel.com/br/pt/

Colombia

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

Ecuador

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

South America

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

Middle East

Israel

- Zyxel Communications Corporation
- http://il.zyxel.com/

Middle East

- Zyxel Communications Corporation
- https://www.zyxel.com/me/en/

North America

USA

- Zyxel Communications, Inc. - North America Headquarters
- https://www.zyxel.com/us/en/

Oceania

Australia

- Zyxel Communications Corporation
- https://www.zyxel.com/au/en/

Africa

South Africa

- Nology (Pty) Ltd.
- https://www.zyxel.com/za/en/

APPENDIX D
Legal Information

Copyright

Disclaimers

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.

Your use of the Zyxel Device is subject to the terms and conditions of any related service providers.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Regulatory Notice and Statement

UNITED STATES of AMERICA

The following information applies if you use the product within USA area.

FCC EMC Statement

- This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
  (1) This device may not cause harmful interference, and
  (2) this device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications 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 according to 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 or television reception, which is found 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:
  - Reorient or relocate the receiving antenna
  - Increase the separation between the devices
  - Connect the equipment to an outlet other than the receiver's
  - Consult a dealer or an experienced radio/TV technician for assistance

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC Radiation Exposure Statement

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter. This transmitter must be at least 30 cm (WAC6553D-E) from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Country Code selection feature to be disabled for products marketed to the US/CANADA.
- Operation of this device is restricted to indoor use only, except for relevant user's manual mention that this device can be installed into the external environment. (WAC6553D-E is a device for outdoor use.)

BRAZIL

The following applies if you use the product within Brazil.

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

CANADA

The following information applies if you use the product within Canada area.

Innovation, Science and Economic Development Canada ICES Statement

CAN ICES-3 (B)/NMB-3(B)

Innovation, Science and Economic Development Canada RSS-GEN & RSS-247 Statement

- This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.
- This radio transmitter (2468C-NWA5123AC (NWA1123-AC v2), 2468C-NWA5123ACHD (NWA1123-AC HD), 2468C-WAC5302DS (NWA1302-AC), 2468C-NWA5123AC (NWA5123-AC), 2468C-NWA5123ACHD (NWA5123-AC HD), 2468C-WAC6502DE (WAC6502D-S, WAC6502D-E), 2468C-WAC6503DS (WAC6503D-S), 2468C-WAC6552DS (WAC6552D-S), 2468C-WAC6553DE (WAC6553D-E), 2468C-WAC6303DS (WAC6303D-S), 2468C-WAC6103DI (WAC6103D-I), 2468C-WAC5302DS (WAC5302D-S), 2468C-WAX650S (WAX650S)) has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed, are strictly prohibited for use with this device.

Antenna Information

ANTENNA MODEL	NO.	TYPE	CONNECTOR	2.4 G GAIN	5G GAIN	REMARK
NWA1123-ACv2	1	PIFA	UFL	3.08		
	2	PIFA	UFL	3.07		
	3	PIFA	UFL		4.06 (5150~5250 MHz) 3.79 (5725~5850 MHz)	
	4	PIFA	UFL		3.99 (5150~5250 MHz) 3.78 (5725~5850 MHz)	
NWA1123-AC HD	1	PIFA	I-PEX	3 (2400-2483.5 MHz)		
	2	PIFA	I-PEX	3 (2400-2483.5 MHz)		
	3	Monopole	I-PEX		4 (5150-5250 MHz) 4 (5725-5850 MHz)	
	4	Monopole	I-PEX		4 (5150-5250 MHz) 4 (5725-5850 MHz)	
	5	Monopole	I-PEX		4 (5150-5250 MHz) 4 (5725-5850 MHz)	
NWA1302-AC	1	Loop	I-PEX	5.82 (2400-2483.5 MHz)		
	2	Loop	I-PEX	5.02 (2400-2483.5 MHz)		
	3	PIFA	I-PEX		5 (5150-5250 MHz) 5 (5250-5350 MHz) 5 (5470-5725 MHz) 5 (5725-5850 MHz)	
NWA5123-AC	1	PIFA	U.FL	3.08 (2400-2483.5 MHz)		
	2	PIFA	U.FL	3.07 (2400-2483.5 MHz)		
	3	PIFA	U.FL		4.06 (5150-5250 MHz) 3.91 (5725-5850 MHz)	
	4	PIFA	U.FL		3.99 (5150-5250 MHz) 3.79 (5725-5850 MHz)	
NWA5123-AC HD	1	PIFA	I-PEX	3 (2400-2483.5 MHz)		
	2	PIFA	I-PEX	3 (2400-2483.5 MHz)		
	3	Monopole	I-PEX		4 (5150-5250 MHz) 4 (5725-5850 MHz)	
	4	Monopole	I-PEX		4 (5150-5250 MHz) 4 (5725-5850 MHz)	
	5	Monopole	I-PEX		4 (5150-5250 MHz) 4 (5725-5850 MHz)	
WAC6502D-E		Dipole	RSMA	5	7	
WAC6502D-S		Dipole	IPEX	4	6	
WAC6503D-S		Dipole	IPEX	4	6	
WAC6553D-E		Dipole	N type	4.5	7	
WAC6103D-I	1	PIFA	U.FL	3.28		Ceiling Mounted: Antenna 1, 2, 3 Wall Mounted: Antenna 1, 2, 4
	2	PIFA	U.FL	3.37		
	3	PIFA	U.FL	3.15		
	4	Dipole	U.FL	4.33		
	5	Loop	U.FL		4.38 (5150-5250 MHz) 4.23 (5725-5850 MHz)	Ceiling Mounted: Antenna 5, 6, 7 Wall Mounted: Antenna 5, 6, 8
	6	Loop	U.FL		4.31 (5150-5250 MHz) 4.22 (5725-5850 MHz)	
	7	Loop	U.FL		4.38 (5150-5250 MHz) 4.36 (5725-5850 MHz)	
	8	Dipole	U.FL		5.12 (5150-5250 MHz) 5.20 (5725-5850 MHz)	

ANTENNA MODEL	NO.	TYPE	CONNECTOR	2.4 G GAIN	5G GAIN	REMARK
WAC5302D-S	1	Loop	I-PEX	5.82 (2400-2483.5 MHz)		
	2	Loop	I-PEX	5.02 (2400-2483.5 MHz)		
	3	PIFA	I-PEX		5 (5150-5250 MHz) 5 (5250-5350 MHz) 5 (5470-5725 MHz) 5 (5725-5850 MHz)	
WAC6303D-S	1	Direction	U.FL	1.12 (2400-2483.5 MHz)		
	2	Direction	U.FL		1.29 (5150-5250 MHz) 1.07 (5725-5850 MHz)	
WAC6552D-S SECTX-DB r2.0	1	Direction	I-PEX	0.8 (2400-2483.5 MHz)	4.22 (5150-5250 MHz) 5.34 (5725-5850 MHz)	
WAX650S		Direction	U.FL	0 (2400-2483.5 MHz)	3.51 (5150-5250 MHz) 4.22 (5250-5350 MHz) 4.61 (5470-5725 MHz) 4.68 (5725-5850 MHz)	

If the product with 5G wireless function operating in 5150-5250 MHz and 5725-5850 MHz, the following attention must be paid,

- The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and
- Where applicable, antenna type(s), antenna model(s), and the worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.23 of RSS 247 shall be clearly indicated.

If the product with 5G wireless function operating in 5250-5350 MHz and 5470-5725 MHz, the following attention must be paid.

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit.
- L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage; (2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Le présent émetteur radio (2468C-NWA5123AC (NWA1123-AC v2), 2468C-NWA5123ACHD (NWA1123-AC HD), 2468C-WAC5302DS (NWA1302-AC), 2468C-NWA5123AC (NWA5123-AC), 2468C-NWA5123ACHD (NWA5123-AC HD), 2468C-WAC6502DE (WAC6502D-S, WAC6502D-E), 2468C-WAC6503DS (WAC6503D-S), 2468C-WAC6552DS (WAC6552D-S), 2468C-WAC6553DE (WAC6553D-E), 2468C-WAC6303DS (WAC6303D-S), 2468C-WAC6103DI (WAC6103D-I), 2468C-WAC5302DS (WAC5302D-S), 2468C-WAX650S (WAX650S)) a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

Informations Antenne

MODÈLE D'ANTENNE	NB.	TYPE	CONNECTEUR	2.4 G GAIN	5G GAIN	REMARQUE
NWA1123-ACv2	1	PIFA	UFL	3.08		
	2	PIFA	UFL	3.07		
	3	PIFA	UFL		4.06 (5150~5250 MHz) 3.79 (5725~5850 MHz)	
	4	PIFA	UFL		3.99 (5150~5250 MHz) 3.78 (5725~5850 MHz)	
NWA1123-AC HD	1	PIFA	I-PEX	3 (2400-2483.5 MHz)		
	2	PIFA	I-PEX	3 (2400-2483.5 MHz)		
	3	Monopole	I-PEX		4 (5150-5250 MHz) 4 (5725-5850 MHz)	
	4	Monopole	I-PEX		4 (5150-5250 MHz) 4 (5725-5850 MHz)	
	5	Monopole	I-PEX		4 (5150-5250 MHz) 4 (5725-5850 MHz)	
NWA1302-AC	1	Loop	I-PEX	5.82 (2400-2483.5 MHz)		
	2	Loop	I-PEX	5.02 (2400-2483.5 MHz)		
	3	PIFA	I-PEX		5 (5150-5250 MHz) 5 (5250-5350 MHz) 5 (5470-5725 MHz) 5 (5725-5850 MHz)	
NWA5123-AC	1	PIFA	U.FL	3.08 (2400-2483.5 MHz)		
	2	PIFA	U.FL	3.07 (2400-2483.5 MHz)		
	3	PIFA	U.FL		4.06 (5150-5250 MHz) 3.91 (5725-5850 MHz)	
	4	PIFA	U.FL		3.99 (5150-5250 MHz) 3.79 (5725-5850 MHz)	
NWA5123-AC HD	1	PIFA	I-PEX	3 (2400-2483.5 MHz)		
	2	PIFA	I-PEX	3 (2400-2483.5 MHz)		
	3	Monopole	I-PEX		4 (5150-5250 MHz) 4 (5725-5850 MHz)	
	4	Monopole	I-PEX		4 (5150-5250 MHz) 4 (5725-5850 MHz)	
	5	Monopole	I-PEX		4 (5150-5250 MHz) 4 (5725-5850 MHz)	
WAC6502D-E		Dipole	RSMA	5	7	
WAC6502D-S		Dipole	IPEX	4	6	
WAC6503D-S		Dipole	IPEX	4	6	
WAC6553D-E		Dipole	N type	4.5	7	
WAC6103D-I	1	PIFA	U.FL	3.28		Ceiling Mounted: Antenna 1, 2, 3 Wall Mounted: Antenna 1, 2, 4
	2	PIFA	U.FL	3.37		
	3	PIFA	U.FL	3.15		
	4	Dipole	U.FL	4.33		
	5	Loop	U.FL		4.38 (5150-5250 MHz) 4.23 (5725-5850 MHz)	Ceiling Mounted: Antenna 5, 6, 7 Wall Mounted: Antenna 5, 6, 8
	6	Loop	U.FL		4.31 (5150-5250 MHz) 4.22 (5725-5850 MHz)	
	7	Loop	U.FL		4.38 (5150-5250 MHz) 4.36 (5725-5850 MHz)	
	8	Dipole	U.FL		5.12 (5150-5250 MHz) 5.20 (5725-5850 MHz)	

MODÈLE D'ANTENNE	NB.	TYPE	CONNECTEUR	2.4 G GAIN	5G GAIN	REMARQUE
WAC5302D-S	1	Loop	I-PEX	5.82 (2400-2483.5 MHz)		
	2	Loop	I-PEX	5.02 (2400-2483.5 MHz)		
	3	PIFA	I-PEX		5 (5150-5250 MHz) 5 (5250-5350 MHz) 5 (5470-5725 MHz) 5 (5725-5850 MHz)	
WAC6303D-S	1	Direction	U.FL	1.12 (2400-2483.5 MHz)		
	2	Direction	U.FL		1.29 (5150-5250 MHz) 1.07 (5725-5850 MHz)	
WAC6552D-S SECTX-DB r2.0	1	Direction	I-PEX	0.8 (2400-2483.5 MHz)	4.22 (5150-5250 MHz) 5.34 (5725-5850 MHz)	
WAX650S		Direction	U.FL	0 (2400-2483.5 MHz)	3.51 (5150-5250 MHz) 4.22 (5250-5350 MHz) 4.61 (5470-5725 MHz) 4.68 (5725-5850 MHz)	

Lorsque la fonction sans fil 5G fonctionnant en 5150-5250 MHz and 5725-5850 MHz est activée pour ce produit, il est nécessaire de porter une attention particulière aux choses suivantes

- Les dispositifs fonctionnant dans la bande de 5 150 à 5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;
- Lorsqu'il y a lieu, les types d'antennes (s'il y en a plusieurs), les numéros de modèle de l'antenne et les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, énoncée à la section 6.2.2.3 du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit, il est nécessaire de porter une attention particulière aux choses suivantes.

- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

Industry Canada radiation exposure statement

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 22cm (NWA1123-AC HD, NWA5123-AC HD) between the radiator and your body.

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 30 cm (WAC6553D-E) between the radiator and your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé.Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé.Cet équipement doit être installé et utilisé avec un minimum de 22 cm (NWA1123-AC HD, NWA5123-AC HD) de distance entre la source de rayonnement et votre corps.

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé.Cet équipement doit être installé et utilisé avec un minimum de 30 cm (WAC6553D-E) de distance entre la source de rayonnement et votre corps.

Caution:

(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

(ii) the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall comply with the e.i.r.p. limit; and

(iii) the maximum antenna gain permitted for devices in the band 5725-5825 MHz shall comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate.

(iv) Users should also be advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

(v) WAC6553D-E is an outdoor device and only uses 5G Band 4 (5725-5850 MHz).

Avertissement:

(i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

(ii) le gain maximal d'antenne permis pour les dispositifs utilisant les bandes 5250-5350 MHz et 5 470-5 725 MHz doit se conformer à la limite de p.i.r.e.;

(iii) le gain maximal d'antenne permis (pour les dispositifs utilisant la bande 5725-5825 MHz) doit se conformer à la limite de p.i.r.e. spécifiée pour l'exploitation point à point et non point à point, selon le cas.

(iv) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

(v) WAC6553D-E est un appareil exterieur et seulement utilise 5G Bane 4 (5725-5850 MHz).

EUROPEAN UNION

The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED)

- Compliance information for 2.4GHz and/or 5GHz wireless products relevant to the EU and other Countries following the EU Directive 2014/53/EU (RED). And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) without any limitation except for the countries mentioned below table:
- In the majority of the EU and other European countries, the 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5GHz wireless LANs.
- If this device for operation in the band 5150-5350 MHz, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20 cm between the radio equipment and your body.
- The maximum RF power operating for each band as follows:

NWA1123-ACv2 and NWA5123-AC

- The band 2,400 MHz to 2,483.5 MHz is 97.95 mW,
- The band 5,150 MHz to 5,350 MHz is 199.07 mW,
- The band 5,470 MHz to 5,725 MHz is 743.02 mW.

WAC6503D-S

- The band 2,400 MHz to 2,483.5 MHz is 99.54 mW,
- The band 5,150 MHz to 5,350 MHz is 183.65 mW,
- The band 5,470 MHz to 5,725 MHz is 941.89 mW.

WAC6502D-E and WAC6502D-S

- The band 2,400 MHz to 2,483.5 MHz is 94.19 mW,
- The band 5,150 MHz to 5,350 MHz is 194.98 mW,
- The band 5,470 MHz to 5,725 MHz is 986.28 mW.

WAC6553D-E

- The band 2,400 MHz to 2,483.5 MHz is 92.26 mW,
- The band 5,150 MHz to 5,350 MHz is 198.61 mW,
- The band 5,470 MHz to 5,725 MHz is 995.41 mW.

NWA1123-AC PRO and WAC6103D-I

- The band 2,400 MHz to 2,483.5 MHz is 92.68 mW,
- The band 5,150 MHz to 5,350 MHz is 192.75 mW,
- The band 5,470 MHz to 5,725 MHz is 966.05 mW.

NWA1302-AC and WAC5302D-S

- The band 2,400 MHz to 2,483.5 MHz is 93.33 mW,
- The band 5,150 MHz to 5,350 MHz is 192.31 mW,
- The band 5,470 MHz to 5,725 MHz is 391.74 mW.

NWA1123-AC HD and NWA5123-AC HD

- The band 2,400 MHz to 2,483.5 MHz is 97.274 mW,
- The band 5,150 MHz to 5,350 MHz is 198.61 mW,
- The band 5,470 MHz to 5,725 MHz is 995.40 mW.

WAC6303D-S

- The band 2,400 MHz to 2,483.5 MHz is 194.09 mW,
- The band 5,150 MHz to 5,350 MHz is 198.61 mW,
- The band 5,470 MHz to 5,725 MHz is 995.41 mW.

WAC6552D-S

- The band 2,400 MHz to 2,483.5 MHz is 93.11 mW,
- The band 5,150 MHz to 5,350 MHz is 198.61 mW,
- The band 5,470 MHz to 5,725 MHz is 914.11 mW.

NWA1123AX, WAX510D and WAX650S

- The band 2,400 MHz to 2,483.5 MHz is 93.11 mW,
- The band 5,150 MHz to 5,350 MHz is 198.61 mW,
- The band 5,470 MHz to 5,725 MHz is 914.11 mW.

Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/EC. **National Restrictions** • The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details. • Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens. • Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.
Español (Spanish)	Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE..
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU. **National Restrictions** • In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage. • I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EU põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EU.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/EU.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/EU.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/EU.
Italiano (Italian)	Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/EU. **National Restrictions** • This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details. • Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.
Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/EU būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. **National Restrictions** • The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details. • 2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/EU Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/EU.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/EU.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU.

Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale şi alte prevederi relevante ale Directivei 2014/53/EU.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EU.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 2014/53/EU.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.

2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CR	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Sweden	SE
Ireland	IE	Switzerland	CH
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Professional installation instruction (WAC6553D-E)

Please be advised that due to the unique function supplied by this product, the device is intended for use with our interactive entertainment software and licensed third-party only. The product will be distributed through controlled distribution channel and installed by trained professional and will not be sold directly to the general public through retail store.

1 Installation personal

This product is designed for specific application and needs to be installed by a qualified personal who has RF and related rule knowledge. The general user shall not attempt to install or change the setting.

2 Installation location

The product shall be installed at a location where the radiating antenna can be kept 30 cm from nearby person in normal operation condition to meet regulatory RF exposure requirement.

3 External antenna

Use only the antennas which have been approved by Zyxel Communications Corporation. The non-approved antenna(s) may produce unwanted spurious or excessive RF transmitting power which may lead to the violation of FCC/IC limit and is prohibited.

4 Installation procedure

Please refer to user's manual for the detail.

5 Warning

Please carefully select the installation position and make sure that the final output power does not exceed the limit set force in relevant rules. The violation of the rule could lead to serious federal penalty.

Instructions d'installation professionnelle (WAC6553D-E)

Veuillez noter que l'appareil etant dedie a une fonction unique, il doit etre utilise avec notre logiciel proprietaire de divertissement interactif . Ce produit sera propose par un reseau de distribution controle et installe par des professionels; il ne sera pas propose au grand public par le reseau de la grande distribution.

1 Installation

Ce produit est destine a un usage specifique et doit etre installe par un personnel qualifie maitrisant les radiofrequences et les regles s'y rapportant. L'installation et les reglages ne doivent pas etre modifies par l'utilisateur final.

2 Emplacement d'installation

En usage normal, afin de respecter les exigences reglementaires concernant l'exposition aux radiofrequences, ce produit doit etre installe de facon a respecter une distance de 30 cm entre l'antenne emettrice et les personnes.

3 Antenn externe.

Utiliser uniiquement les antennes approuvees par le fabricant. L'utilisation d'autres antennes peut conduire a un niveau de rayonnement essentiel ou non essentiel depassant les niveaux limites definis par FCC/IC, ce qui est interdit.

4 Procedure d'installation

Consulter le manuel d'utilisation.

5 Avertissement

Choisir avec soin la position d'installation et s'assurer que la puissance de sortie ne depasse pas les limites en vigueur. La violation de cette regle peut conduire a de serieuses penalites federales.

Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- This device (WAC6553D-E, WAC6552D-S) must be grounded by qualified service personnel. Never defeat the ground conductor or operate the device in the absence of a suitably installed ground conductor. Contact the qualified service personnel if you are uncertain that suitable grounding is available.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,
  - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;
  - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

Environment statement

ErP (Energy-related Products) (NWA1123-ACv2, NWA1123-AC HD, NWA5123-AC, NWA5123-AC HD, WAC6502D-E, WAC6502D-S, and WAC6503D-S)

Zyxel products put on the EU market in compliance with the requirement of the European Parliament and the Council published

Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called

as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

Network standby power consumption < 8W, and/or

Off mode power consumption < 0.5W, and/or

Standby mode power consumption < 0.5W.

For wireless setting, please refer to the chapter about wireless settings for more detail.

European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

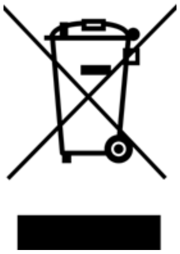
Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.



台灣

以下訊息僅適用於產品銷售至台灣地區
第十二條 經型式認證合格之低功率射頻電機，非經許可，公司，商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信法規定作業之無線電通信。 低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
無線資訊傳輸設備避免影響附近雷達系統之操作。

電磁波曝露量 MPE 標準值 1mW/cm2，送測產品 (NWA1123-ACv2) 實測值為：0.316 mW/cm2 本產品使用時建議應距離人體 20 cm
電磁波曝露量 MPE 標準值 1mW/cm2，送測產品 (NWA1123-AC PRO) 實測值為：0.448 mW/cm2 本產品使用時建議應距離人體 20 cm
電磁波曝露量 MPE 標準值 1mW/cm2，送測產品 (NWA1123-AC HD) 實測值為：0.685 mW/cm2 本產品使用時建議應距離人體 20 cm
電磁波曝露量 MPE 標準值 1mW/cm2，送測產品 (NWA1302-AC) 實測值為：0.109 mW/cm2 本產品使用時建議應距離人體 20 cm
電磁波曝露量 MPE 標準值 1mW/cm2，送測產品 (NWA5123-AC) 實測值為：0.316 mW/cm2 本產品使用時建議應距離人體 20 cm
電磁波曝露量 MPE 標準值 1mW/cm2，送測產品 (WAC6503D-S) 實測值為：0.744 mW/cm2 本產品使用時建議應距離人體 20 cm
電磁波曝露量 MPE 標準值 1mW/cm2，送測產品 (WAC6502D-S) 實測值為：0.320 mW/cm2 本產品使用時建議應距離人體 20 cm
電磁波曝露量 MPE 標準值 1mW/cm2，送測產品 (WAC6502D-E) 實測值為：0.403 mW/cm2 本產品使用時建議應距離人體 20 cm
電磁波曝露量 MPE 標準值 1mW/cm2，送測產品 (WAC6553D-E) 實測值為：0.539 mW/cm2 本產品使用時建議應距離人體 30 cm
電磁波曝露量 MPE 標準值 1mW/cm2，送測產品 (WAC6103D-I) 實測值為：0.448 mW/cm2 本產品使用時建議應距離人體 20 cm
電磁波曝露量 MPE 標準值 1mW/cm2，送測產品 (WAC5302D-S) 實測值為：0.109 mW/cm2 本產品使用時建議應距離人體 20 cm
電磁波曝露量 MPE 標準值 1mW/cm2，送測產品 (NWA5123-AC HD) 實測值為：0.685 mW/cm2 本產品使用時建議應距離人體 20 cm
電磁波曝露量 MPE 標準值 1mW/cm2，送測產品 (WAC6303D-S) 實測值為：0.349 mW/cm2 本產品使用時建議應距離人體 20 cm

無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。
無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中。
無線資訊傳輸設備必須具備安全功能，以保護未經授權之一方任意更改軟體進而避免發射機操作於非經認證之頻率、輸出功率、調變形式或其他射頻參數設定。
使用無線產品時，應避免影響附近雷達系統之操作。
高增益指向性天線只得應用於固定式點對點系統。

專業安裝警語： (WAC6553D-E)
以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區
本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

安全警告

為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
- 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座 (如：北美 / 台灣電壓 110V AC，歐洲是 230V AC)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  - 對永久連接之設備， 在設備外部須安裝可觸及之斷電裝置；
  - 對插接式之設備， 插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
∿	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
⎓	Direct current (DC): DC if the unidirectional flow or movement of electric charge carriers.
⏚	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
⧈	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. 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 your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. If you cannot find it there, contact your vendor or Zyxel Technical Support at support@zyxel.com.tw.

To obtain the source code covered under those Licenses, please contact your vendor or Zyxel Technical Support at support@zyxel.com.tw.

Index