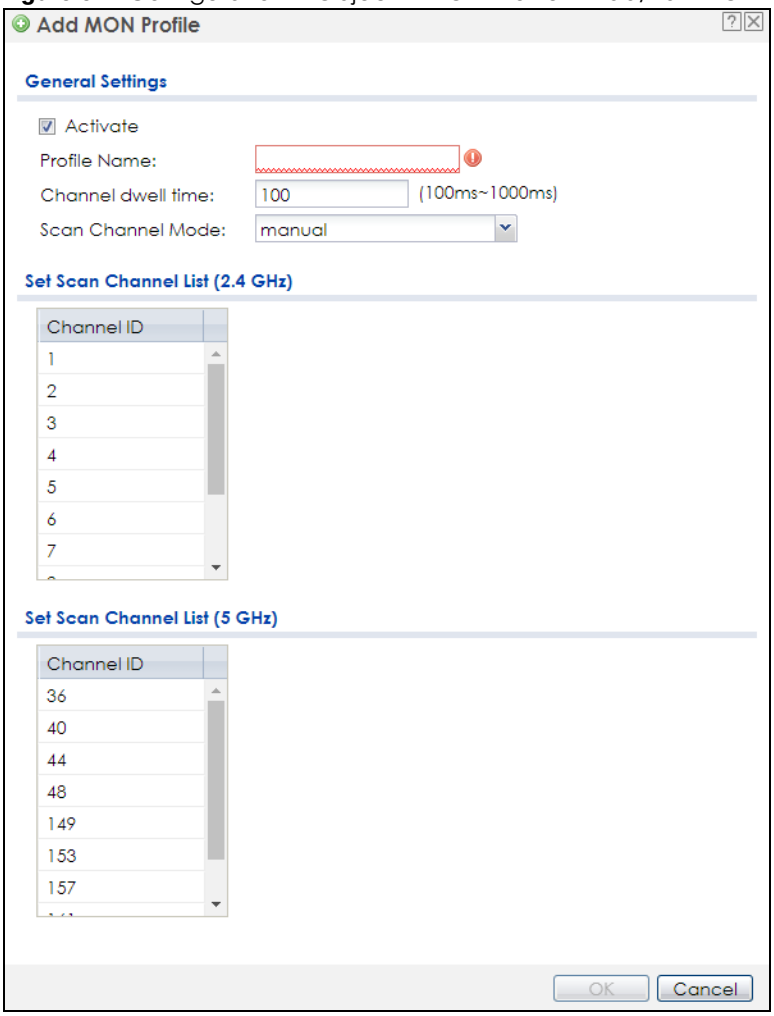
Table 64 Configuration > Object > MON Profile (continued)

LABEL	DESCRIPTION
Object Reference	Click this to view which other objects are linked to the selected monitor mode profile (for example, an AP management profile).
#	This field is a sequential value, and it is not associated with a specific profile.
Status	This field shows whether or not the entry is activated.
Profile Name	This field indicates the name assigned to the monitor profile.

14.2.1 Add/Edit MON Profile

This screen allows you to create a new monitor mode profile or edit an existing one. To access this screen, click the **Add** button or select and existing monitor mode profile and click the **Edit** button. See Section 1.2.3 on page 15 for more information about MON Mode.

Figure 91 Configuration > Object > MON Profile > Add/Edit MON Profile



The following table describes the labels in this screen.

Table 65 Configuration > Object > MON Profile > Add/Edit MON Profile

LABEL	DESCRIPTION
Activate	Select this to activate this monitor mode profile.
Profile Name	This field indicates the name assigned to the monitor mode profile.
Channel dwell time	Enter the interval (in milliseconds) before the Zyxel Device switches to another channel for monitoring.
Scan Channel Mode	Select **auto** to have the Zyxel Device switch to the next sequential channel once the **Channel dwell time** expires. Select **manual** to set specific channels through which to cycle sequentially when the **Channel dwell time** expires. Selecting this options makes the **Scan Channel List** options available.
Set Scan Channel List (2.4 GHz)	Select one or more than one channel to have the Zyxel Device using this profile scan the channel(s) when **Scan Channel Mode** is set to **manual**. These channels are limited to the 2.4 GHz range (802.11 b/g/n/ax).
Set Scan Channel List (5 GHz)	Select one or more than one channel to have the Zyxel Device using this profile scan the channel(s) when **Scan Channel Mode** is set to **manual**. These channels are limited to the 5 GHz range (802.11 a/n/ac/ax). Not all Zyxel Devices support both 2.4 GHz and 5 GHz frequency bands.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

CHAPTER 15
WDS Profile

15.1 Overview

This chapter shows you how to configure WDS (Wireless Distribution System) profiles for the Zyxel Device to form a WDS with other APs.

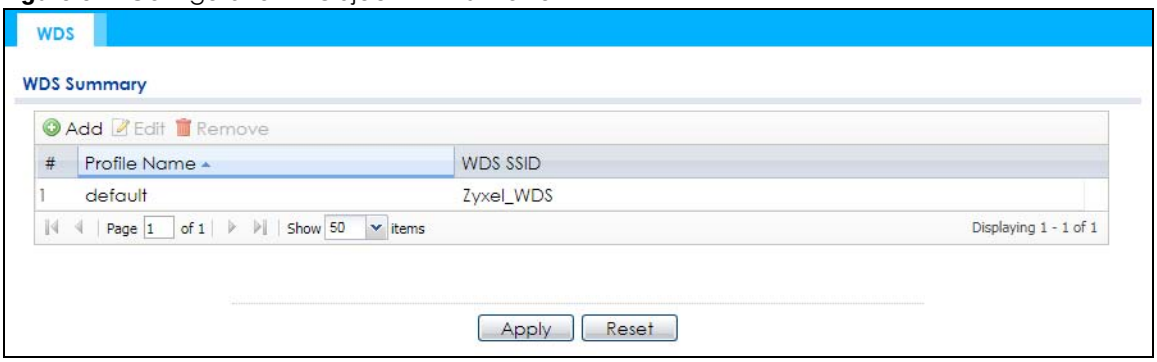
15.1.1 What You Can Do in this Chapter

The **WDS Profile** screen (Section 15.2 on page 153) creates preset WDS configurations that can be used by the Zyxel Device.

15.2 WDS Profile

This screen allows you to manage and create WDS profiles that can be used by the APs. To access this screen, click **Configuration > Object > WDS Profile**.

Figure 92 Configuration > Object > WDS Profile



The following table describes the labels in this screen.

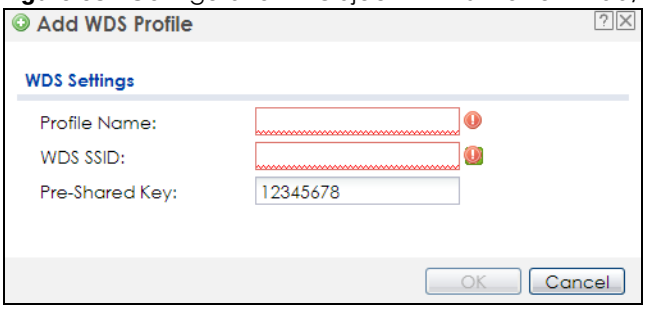
Table 66 Configuration > Object > WDS Profile

LABEL	DESCRIPTION
Add	Click this to add a new profile.
Edit	Click this to edit the selected profile.
Remove	Click this to remove the selected profile.
#	This field is a sequential value, and it is not associated with a specific profile.
Profile Name	This field indicates the name assigned to the profile.
WDS SSID	This field shows the SSID specified in this WDS profile.

15.2.1 Add/Edit WDS Profile

This screen allows you to create a new WDS profile or edit an existing one. To access this screen, click the **Add** button or select and existing profile and click the **Edit** button.

Figure 93 Configuration > Object > WDS Profile > Add/Edit WDS Profile



The following table describes the labels in this screen.

Table 67 Configuration > Object > WDS Profile > Add/Edit WDS Profile

LABEL	DESCRIPTION
Profile Name	Enter up to 31 alphanumeric characters for the profile name.
WDS SSID	Enter the SSID with which you want the Zyxel Device to connect to a root AP or repeater to form a WDS.
Pre-Shared Key	Enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters. The key is used to encrypt the traffic between the APs.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

CHAPTER 16
Certificates

16.1 Overview

The Zyxel Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

16.1.1 What You Can Do in this Chapter

- The **My Certificates** screens (Section 16.2 on page 158) generate and export self-signed certificates or certification requests and import the Zyxel Device's CA-signed certificates.
- The **Trusted Certificates** screens (Section 16.3 on page 165) save CA certificates and trusted remote host certificates to the Zyxel Device. The Zyxel Device trusts any valid certificate that you have imported as a trusted certificate. It also trusts any valid certificate signed by any of the certificates that you have imported as a trusted certificate.

16.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available. The other key is private and must be kept secure.

These keys work like a handwritten signature (in fact, certificates are often referred to as "digital signatures"). Only you can write your signature exactly as it should look. When people know what your signature looks like, they can verify whether something was signed by you, or by someone else. In the same way, your private key "writes" your digital signature and your public key allows people to verify whether data was signed by you, or by someone else.

This process works as follows:

1. Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).
2. Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.
3. Tim uses his private key to sign the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to verify it. Jenny knows that the message is from Tim, and that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim's private key).

5 Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny's public key to verify the message.

The Zyxel Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The Zyxel Device does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The Zyxel Device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

Advantages of Certificates

Certificates offer the following benefits.

- The Zyxel Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

Self-signed Certificates

You can have the Zyxel Device act as a certification authority and sign its own certificates.

Factory Default Certificate

The Zyxel Device generates its own unique self-signed certificate when you first turn it on. This certificate is referred to in the GUI as the factory default certificate.

Certificate File Formats

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.

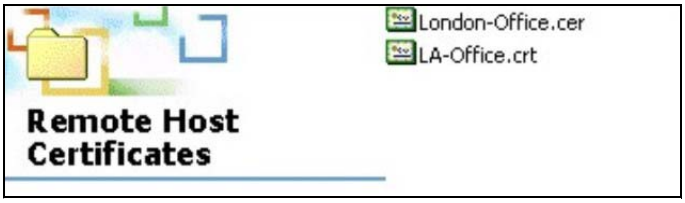
Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

16.1.3 Verifying a Certificate

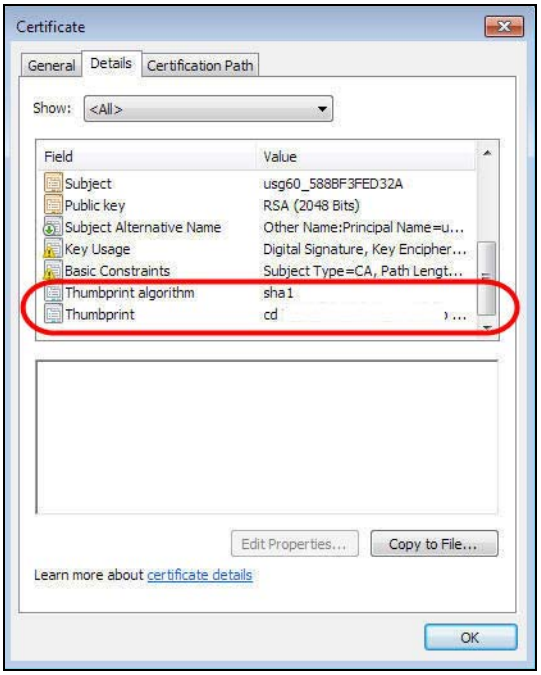
Before you import a trusted certificate into the Zyxel Device, you should verify that you have the correct certificate. You can do this using the certificate's fingerprint. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithm. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

1 Browse to where you have the certificate saved on your computer.

2 Make sure that the certificate has a ".cer" or ".crt" file name extension.



3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

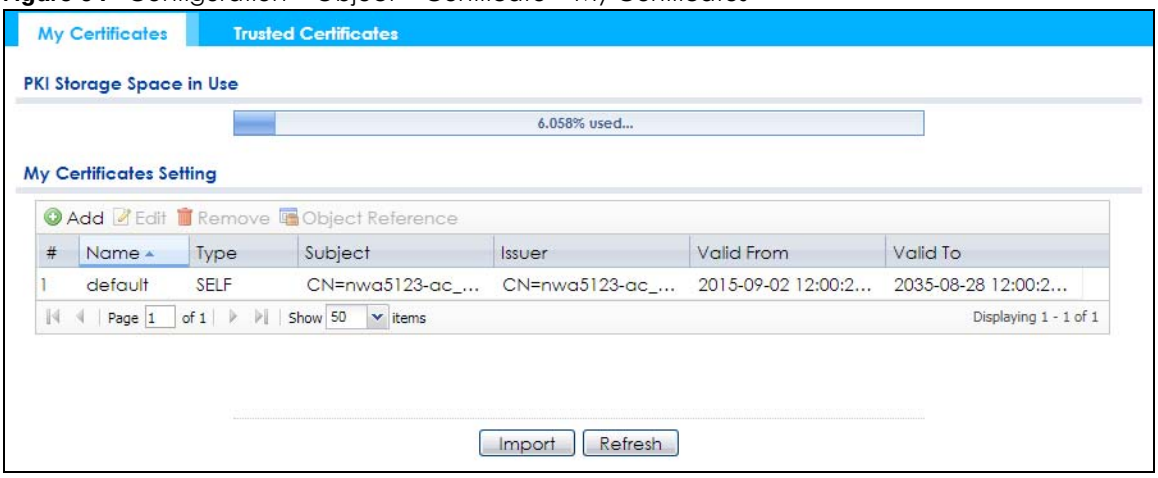


4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may vary based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

16.2 My Certificates

Click **Configuration > Object > Certificate > My Certificates** to open this screen. This is the Zyxel Device's summary list of certificates and certification requests.

Figure 94 Configuration > Object > Certificate > My Certificates



The following table describes the labels in this screen.

Table 68 Configuration > Object > Certificate > My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the Zyxel Device's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Add	Click this to go to the screen where you can have the Zyxel Device generate a certificate or a certification request.
Edit	Double-click an entry or select it and click **Edit** to open a screen with an in-depth list of information about the certificate.
Remove	The Zyxel Device keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
Object Reference	You cannot delete certificates that any of the Zyxel Device's features are configured to use. Select an entry and click **Object Reference** to open a screen that shows which settings use the entry.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Type	This field displays what kind of certificate this is. **REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request. **SELF** represents a self-signed certificate. **CERT** represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.

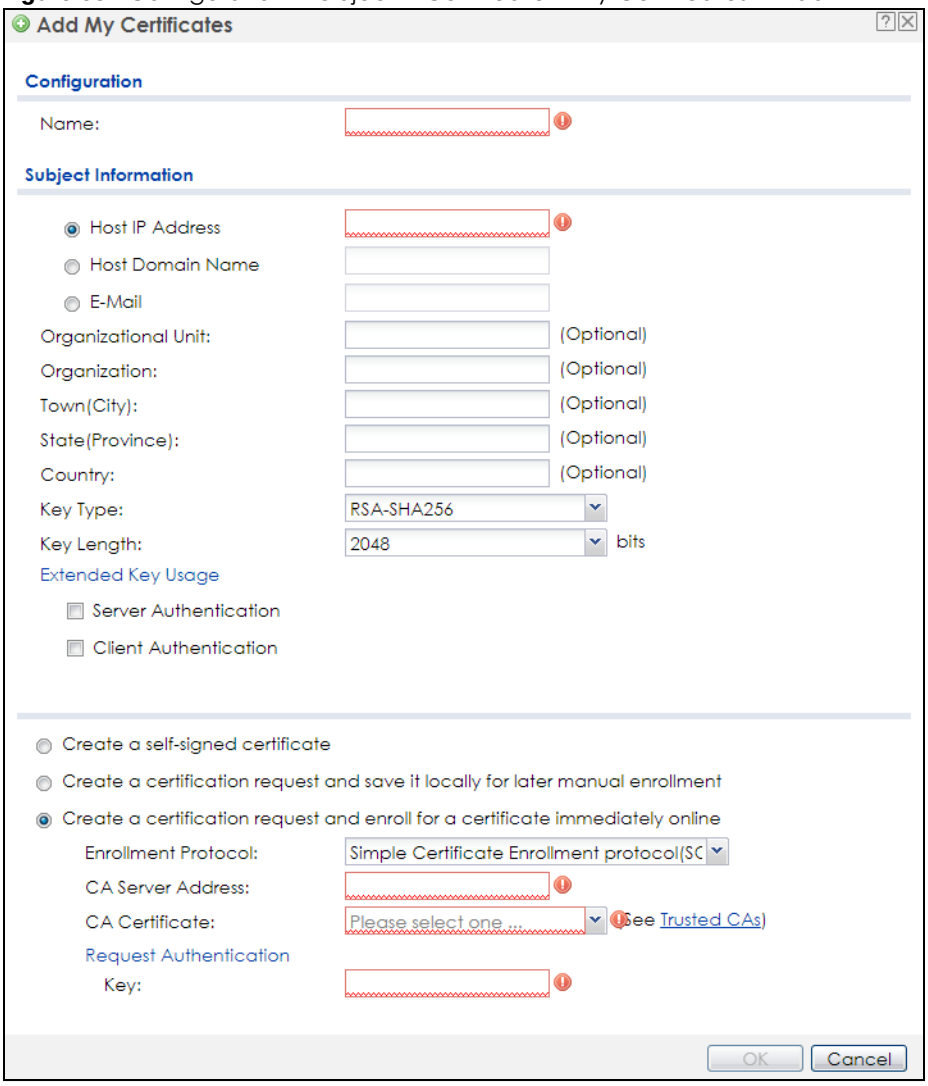
Table 68 Configuration > Object > Certificate > My Certificates (continued)

LABEL	DESCRIPTION
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click **Import** to open a screen where you can save a certificate to the Zyxel Device.
Refresh	Click **Refresh** to display the current validity status of the certificates.

16.2.1 Add My Certificates

Click **Configuration > Object > Certificate > My Certificates** and then the **Add** icon to open the **Add My Certificates** screen. Use this screen to have the Zyxel Device create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

Figure 95 Configuration > Object > Certificate > My Certificates > Add



The following table describes the labels in this screen.

Table 69 Configuration > Object > Certificate > My Certificates > Add

LABEL	DESCRIPTION
Name	Type a name to identify this certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although you must specify a **Host IP Address**, **Host Domain Name**, or **E-Mail**. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information. Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address is for identification purposes only and can be any string. A domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods. An e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.
Organizational Unit	Identify the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Organization	Identify the company or group to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Town (City)	Identify the town or city where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
State (Province)	Identify the state or province where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Country	Identify the nation where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Key Type	The Zyxel Device uses the RSA (Rivest, Shamir and Adleman) public-key encryption algorithm. SHA1 (Secure Hash Algorithm) and SHA2 are hash algorithms used to authenticate packet data. SHA2-256 or SHA2-512 are part of the SHA2 set of cryptographic functions and they are considered even more secure than SHA1. Select a key type from **RSA-SHA256** and **RSA-SHA512**.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (1024 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Extended Key Usage	Select **Server Authentication** to allow a web server to send clients the certificate to authenticate itself. Select **Client Authentication** to use the certificate's key to authenticate clients to the secure gateway.
	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select this to have the Zyxel Device generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select this to have the Zyxel Device generate and store a request for a certificate. Use the **My Certificate Edit** screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the **My Certificate Edit** screen and then send it to the certification authority.

Table 69 Configuration > Object > Certificate > My Certificates > Add (continued)

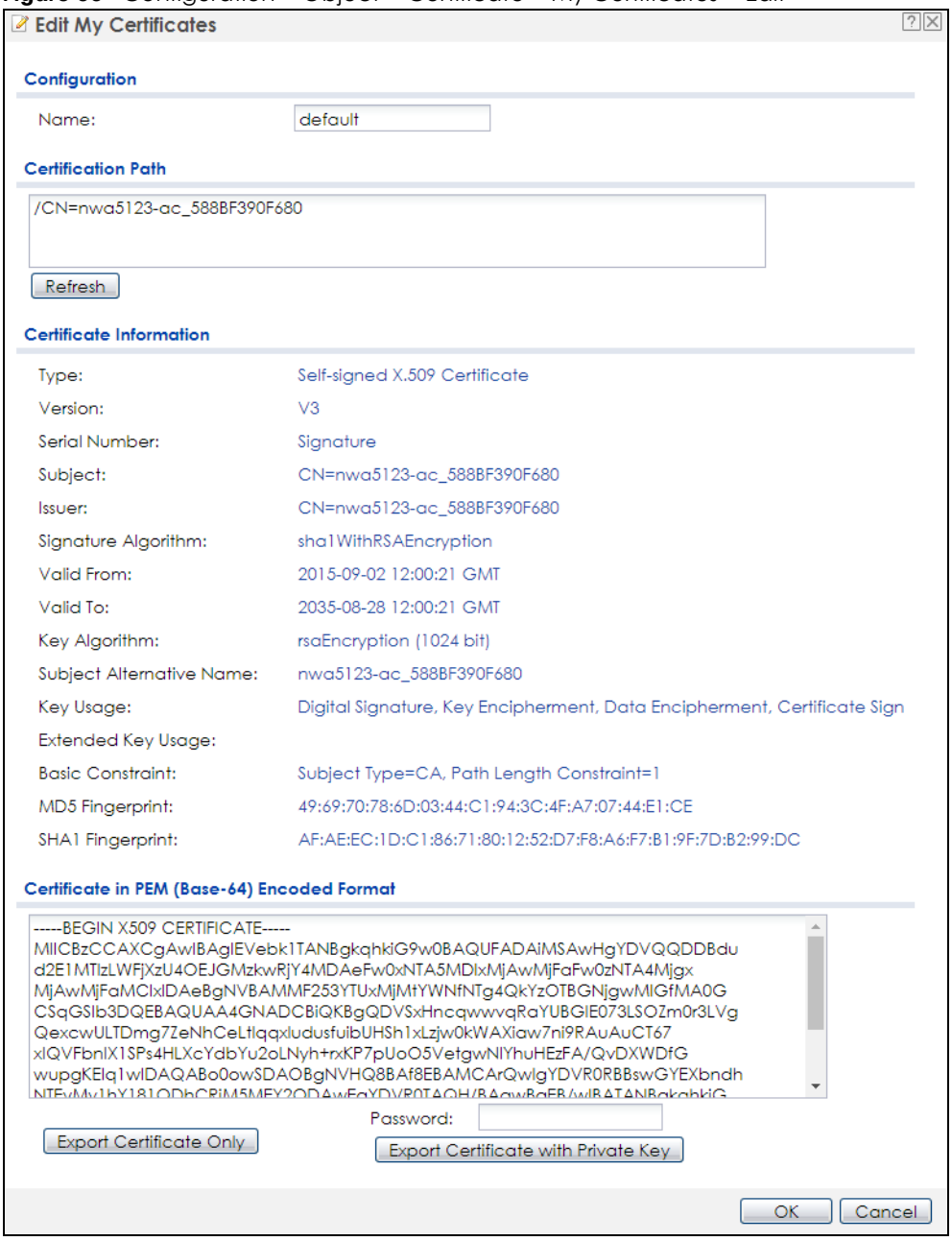
LABEL	DESCRIPTION
Create a certification request and enroll for a certificate immediately online	Select this to have the Zyxel Device generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the **Trusted Certificates** screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the **Reference Number** and **Key** if the certification authority requires them.
Enrollment Protocol	This field applies when you select **Create a certification request and enroll for a certificate immediately online**. Select the certification authority's enrollment protocol from the drop-down list box. **Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. **Certificate Management Protocol (CMP)** is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.
CA Server Address	This field applies when you select **Create a certification request and enroll for a certificate immediately online**. Enter the IP address (or URL) of the certification authority server. For a URL, you can use up to 511 of the following characters. a-zA-Z0-9'()+,/:.=?;!*#@$_%-
CA Certificate	This field applies when you select **Create a certification request and enroll for a certificate immediately online**. Select the certification authority's certificate from the **CA Certificate** drop-down list box. You must have the certification authority's certificate already imported in the **Trusted Certificates** screen. Click **Trusted CAs** to go to the **Trusted Certificates** screen where you can view (and manage) the Zyxel Device's list of certificates of trusted certification authorities.
Request Authentication	When you select **Create a certification request and enroll for a certificate immediately online**, the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the **Reference Number** and the **Key** fields if your certification authority uses the CMP enrollment protocol. Just the **Key** field displays if your certification authority uses the SCEP enrollment protocol. For the reference number, use 0 to 99999999. For the key, use up to 31 of the following characters. a-zA-Z0-9; | `~!@#$%^&*()_+\{}':,./ <>=-
OK	Click **OK** to begin certificate or certification request generation.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

If you configured the **Add My Certificates** screen to have the Zyxel Device enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **Add My Certificates** screen. Click **Return** and check your information in the **Add My Certificates** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the Zyxel Device to enroll a certificate online.

16.2.2 Edit My Certificates

Click **Configuration > Object > Certificate > My Certificates** and then the **Edit** icon to open the **My Certificate Edit** screen. You can use this screen to view in-depth certificate information and change the certificate's name.

Figure 96 Configuration > Object > Certificate > My Certificates > Edit



The following table describes the labels in this screen.

Table 70 Configuration > Object > Certificate > My Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Certification Path	This field displays for a certificate, not a certification request. Click the **Refresh** button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The Zyxel Device does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number. "
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the Zyxel Device.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O), State (ST), and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the **Subject Name** field. "none" displays for a certification request.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate.
Valid From	This field displays the date that the certificate becomes applicable. "none" displays for a certification request.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. "none" displays for a certification request.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the Zyxel Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Extended Key Usage	This field displays for what EKU (Extended Key Usage) functions the certificate's key can be used.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path. This field does not display for a certification request.

Table 70 Configuration > Object > Certificate > My Certificates > Edit

LABEL	DESCRIPTION
MD5 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form. You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export Certificate Only	Use this button to save a copy of the certificate without its private key. Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Password	If you want to export the certificate with its private key, create a password and type it here. Make sure you keep this password in a safe place. You will need to use it if you import the certificate to another device.
Export Certificate with Private Key	Use this button to save a copy of the certificate with its private key. Type the certificate's password and click this button. Click **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
OK	Click **OK** to save your changes back to the Zyxel Device. You can only change the name.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

16.2.3 Import Certificates

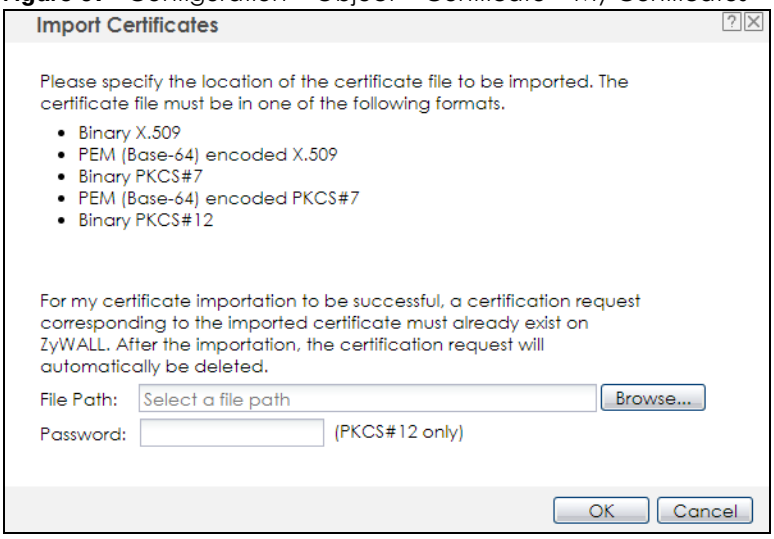
Click **Configuration > Object > Certificate > My Certificates > Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the Zyxel Device.

Note: 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.

The certificate you import replaces the corresponding request in the **My Certificates** screen.

You must remove any spaces in the certificate's filename before you can import it.

Figure 97 Configuration > Object > Certificate > My Certificates > Import



The following table describes the labels in this screen.

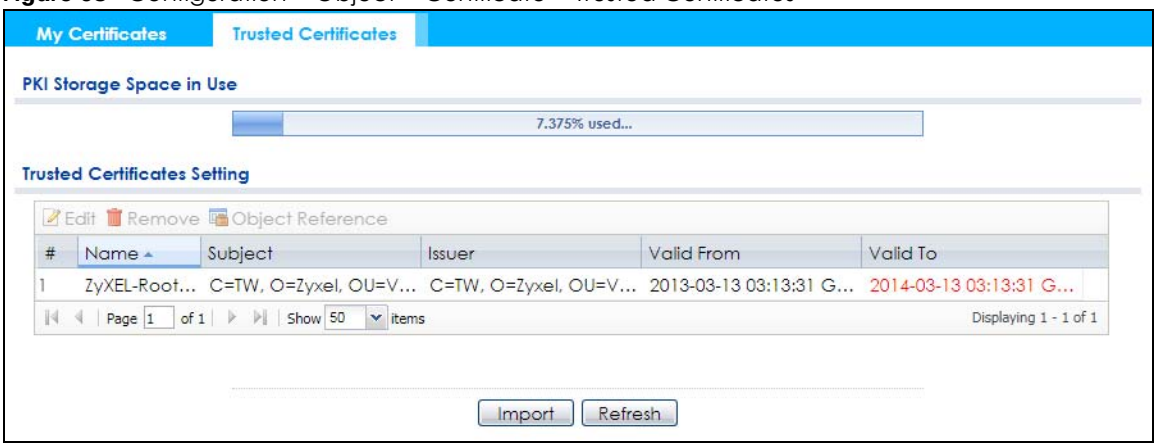
Table 71 Configuration > Object > Certificate > My Certificates > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it. You cannot import a certificate with the same name as a certificate that is already in the Zyxel Device.
Browse	Click **Browse** to find the certificate file you want to upload.
Password	This field only applies when you import a binary PKCS#12 format file. Type the file's password that was created when the PKCS #12 file was exported.
OK	Click **OK** to save the certificate on the Zyxel Device.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

16.3 Trusted Certificates

Click **Configuration > Object > Certificate > Trusted Certificates** to open the **Trusted Certificates** screen. This screen displays a summary list of certificates that you have set the Zyxel Device to accept as trusted. The Zyxel Device also accepts any valid certificate signed by a certificate on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certificates.

Figure 98 Configuration > Object > Certificate > Trusted Certificates



The following table describes the labels in this screen.

Table 72 Configuration > Object > Certificate > Trusted Certificates

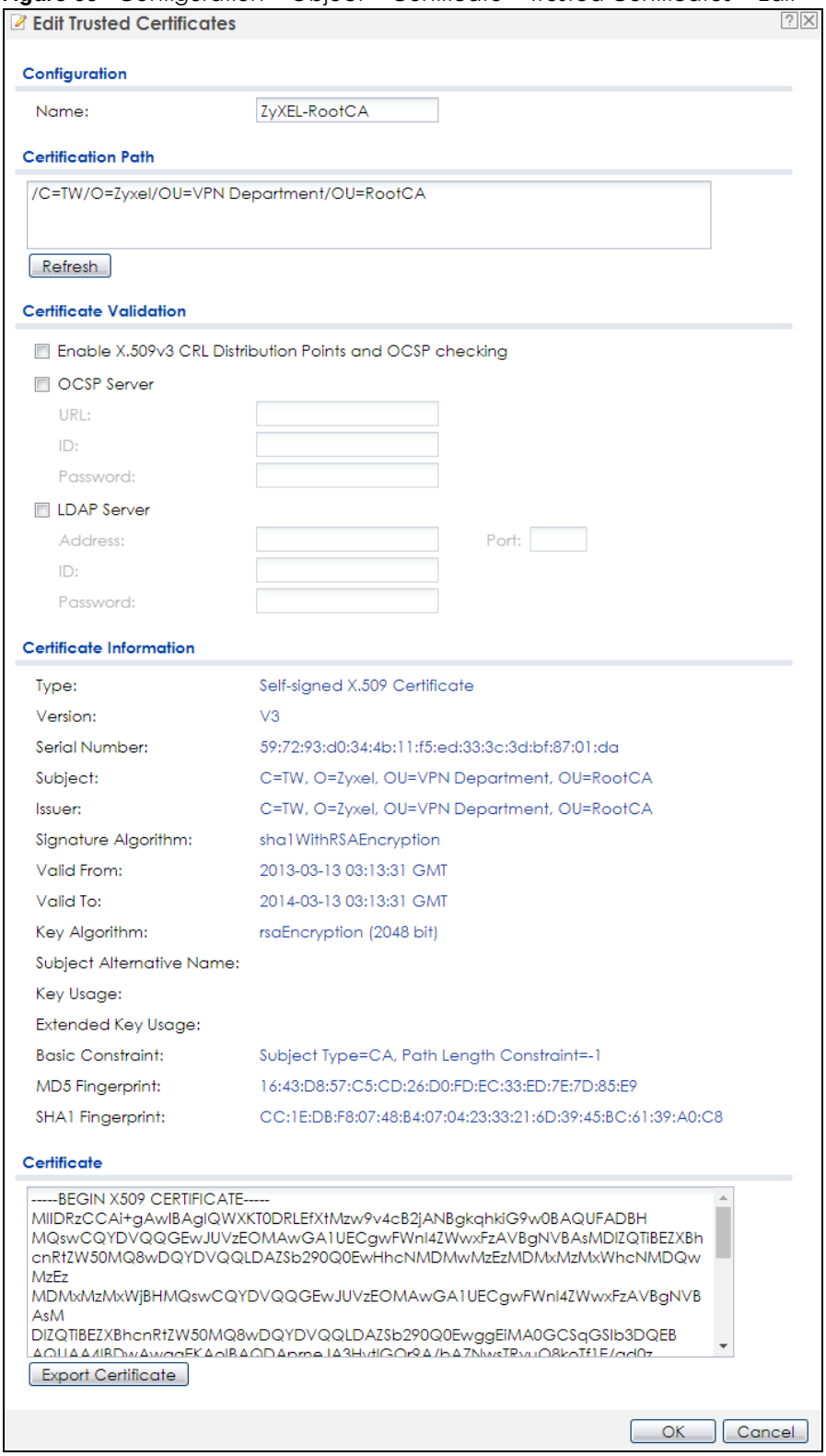
LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the Zyxel Device's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Edit	Double-click an entry or select it and click **Edit** to open a screen with an in-depth list of information about the certificate.
Remove	The Zyxel Device keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
Object Reference	You cannot delete certificates that any of the Zyxel Device's features are configured to use. Select an entry and click **Object Reference** to open a screen that shows which settings use the entry.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click **Import** to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the Zyxel Device.
Refresh	Click this button to display the current validity status of the certificates.

16.3.1 Edit Trusted Certificates

Click **Configuration > Object > Certificate > Trusted Certificates** and then a certificate's **Edit** icon to open the **Trusted Certificates Edit** screen. Use this screen to view in-depth information about the certificate, change the certificate's name and set whether or not you want the Zyxel Device to check a

certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 99 Configuration > Object > Certificate > Trusted Certificates > Edit



The following table describes the labels in this screen.

Table 73 Configuration > Object > Certificate > Trusted Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can change the name. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters.
Certification Path	Click the **Refresh** button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certificate, it may be the only certification authority in the list (along with the end entity's own certificate). The Zyxel Device does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Enable X.509v3 CRL Distribution Points and OCSP checking	Select this check box to have the Zyxel Device check incoming certificates that are signed by this certificate against a Certificate Revocation List (CRL) or an OCSP server. You also need to configure the OSCP or LDAP server details.
OCSP Server	Select this check box if the directory server uses OCSP (Online Certificate Status Protocol).
URL	Type the protocol, IP address and pathname of the OCSP server.
ID	The Zyxel Device may need to authenticate itself in order to assess the OCSP server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the OCSP server (usually a certification authority).
LDAP Server	Select this check box if the directory server uses LDAP (Lightweight Directory Access Protocol). LDAP is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates.
Address	Type the IP address (in dotted decimal notation) of the directory server.
Port	Use this field to specify the LDAP server port number. You must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
ID	The Zyxel Device may need to authenticate itself in order to assess the CRL directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the CRL directory server (usually a certification authority).
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the **Subject Name** field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).

Table 73 Configuration > Object > Certificate > Trusted Certificates > Edit (continued)

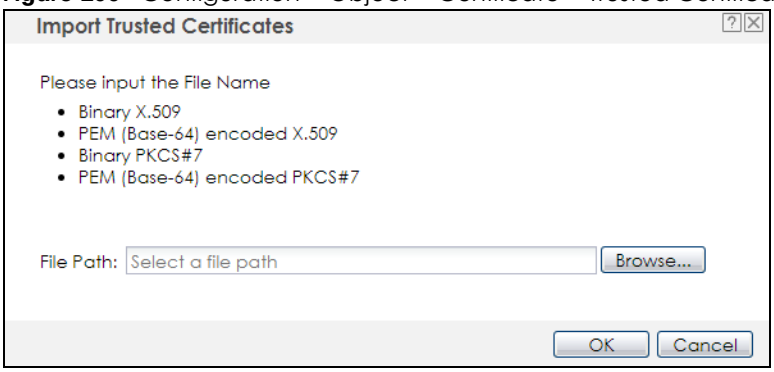
LABEL	DESCRIPTION
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the Zyxel Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the Zyxel Device calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export Certificate	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
OK	Click **OK** to save your changes back to the Zyxel Device. You can only change the name.
Cancel	Click **Cancel** to quit and return to the **Trusted Certificates** screen.

16.3.2 Import Trusted Certificates

Click **Configuration > Object > Certificate > Trusted Certificates > Import** to open the **Import Trusted Certificates** screen. Follow the instructions in this screen to save a trusted certificate to the Zyxel Device.

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

Figure 100 Configuration > Object > Certificate > Trusted Certificates > Import



The following table describes the labels in this screen.

Table 74 Configuration > Object > Certificate > Trusted Certificates > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it. You cannot import a certificate with the same name as a certificate that is already in the Zyxel Device.
Browse	Click **Browse** to find the certificate file you want to upload.
OK	Click **OK** to save the certificate on the Zyxel Device.
Cancel	Click **Cancel** to quit and return to the previous screen.

16.4 Technical Reference

The following section contains additional technical information about the features described in this chapter.

OCSP

OCSP (Online Certificate Status Protocol) allows an application or device to check whether a certificate is valid. With OCSP the Zyxel Device checks the status of individual certificates instead of downloading a Certificate Revocation List (CRL). OCSP has two main advantages over a CRL. The first is real-time status information. The second is a reduction in network traffic since the Zyxel Device only gets information on the certificates that it needs to verify, not a huge list. When the Zyxel Device requests certificate status information, the OCSP server returns a "expired", "current" or "unknown" response.

CHAPTER 17
System

17.1 Overview

Use the system screens to configure general Zyxel Device settings.

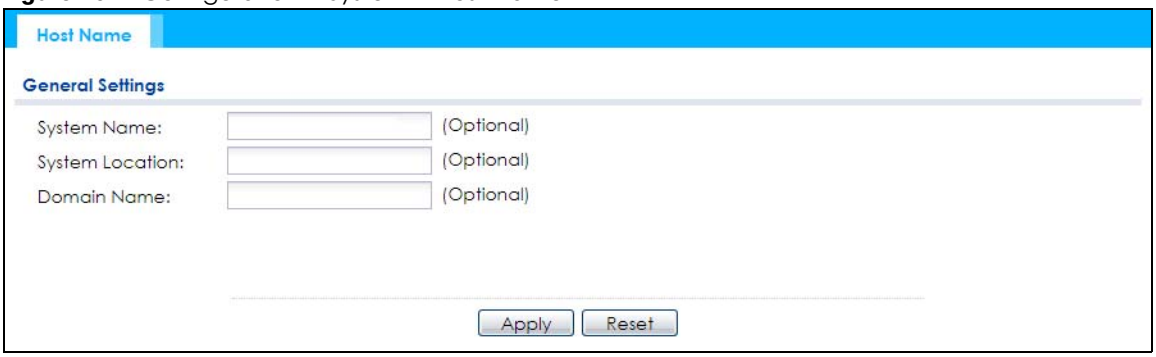
17.1.1 What You Can Do in this Chapter

- The **Host Name** screen (Section 17.2 on page 171) configures a unique name for the Zyxel Device in your network.
- The **Power Mode** screen (Section 17.3 on page 172) configures the Zyxel Device's power settings.
- The **Date/Time** screen (Section 17.4 on page 173) configures the date and time for the Zyxel Device.
- The **WWW** screens (Section 17.5 on page 176) configure settings for HTTP or HTTPS access to the Zyxel Device.
- The **SSH** screen (Section 17.6 on page 184) configures SSH (Secure SHell) for securely accessing the Zyxel Device's command line interface.
- The **Telnet** screen (Section 17.7 on page 188) configures Telnet for accessing the Zyxel Device's command line interface.
- The **FTP** screen (Section 17.8 on page 189) specifies FTP server settings. You can upload and download the Zyxel Device's firmware and configuration files using FTP. Please also see Chapter 19 on page 206 for more information about firmware and configuration files.
- The **SNMP** screens (Section 17.9 on page 190) configure the Zyxel Device's SNMP settings, including profiles that define allowed SNMPv3 access.

17.2 Host Name

A host name is the unique name by which a device is known on a network. Click **Configuration > System > Host Name** to open this screen.

Figure 101 Configuration > System > Host Name



The following table describes the labels in this screen.

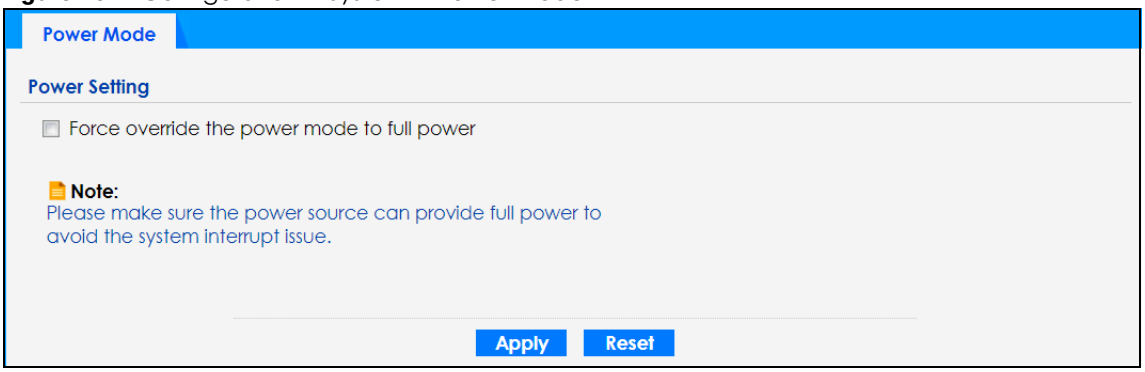
Table 75 Configuration > System > Host Name

LABEL	DESCRIPTION
System Name	Choose a descriptive name to identify your Zyxel Device device. This name can be up to 64 alphanumeric characters long. Spaces are not allowed, but dashes (-) underscores (_) and periods (.) are accepted.
System Location	Specify the name of the place where the Zyxel Device is located. You can enter up to 60 alphanumeric and '()' ,.;?! +-*/= #$%@ characters. Spaces and underscores are allowed. The name should start with a letter.
Domain Name	Enter the domain name (if you know it) here. This name is propagated to DHCP clients connected to interfaces with the DHCP server enabled. This name can be up to 254 alphanumeric characters long. Spaces are not allowed, but dashes "-" are accepted.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

17.3 Power Mode

Use this screen to configure the Zyxel Device's power settings. Click **Configuration > System > Power Mode** to open this screen.

Figure 102 Configuration > System > Power Mode



The following table describes the labels in this screen.

Table 76 Configuration > System > Power Mode

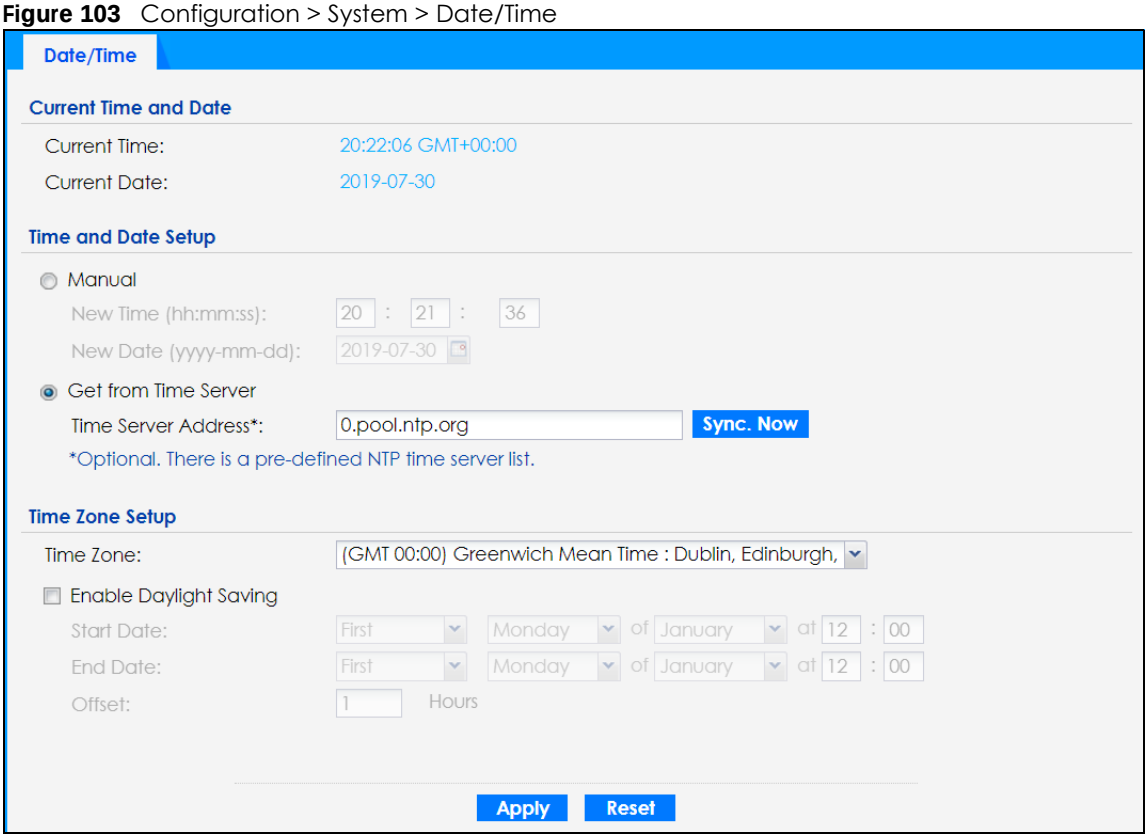
LABEL	DESCRIPTION
Force override the power mode to full power	Select this check box if you are using a PoE injector that does not support PoE negotiation. Otherwise, the Zyxel Device cannot draw full power from the power sourcing equipment. Enable this power mode to improve the Zyxel Device's performance in this situation. Note: Ensure that the power sourcing equipment can supply enough power to the AP to avoid abnormal system reboots. Note: Only enable this if you are using a passive PoE injector that is not IEEE 802.3at/bt compliant but can still provide full power.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

17.4 Date and Time

For effective scheduling and logging, the Zyxel Device system time must be accurate. The Zyxel Device has a software mechanism to set the time manually or get the current time and date from an external server.

To change your Zyxel Device's time based on your local time zone and date, click **Configuration > System > Date/Time**. The screen displays as shown. You can manually set the Zyxel Device's time and date or have the Zyxel Device get the date and time from a time server.

Figure 103 Configuration > System > Date/Time



The following table describes the labels in this screen.

Table 77 Configuration > System > Date/Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the present time of your Zyxel Device.
Current Date	This field displays the present date of your Zyxel Device.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, time zone and daylight saving at the same time, the time zone and daylight saving will affect the new time and date you entered. When you enter the time settings manually, the Zyxel Device uses the new setting once you click **Apply**.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.

Table 77 Configuration > System > Date/Time (continued)

LABEL	DESCRIPTION
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the Zyxel Device get the time and date from the time server you specify below. The Zyxel Device requests time and date settings from the time server under the following circumstances. • When the Zyxel Device starts up. • When you click **Apply** or **Sync. Now** in this screen. • 24-hour intervals after starting up.
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Sync. Now	Click this button to have the Zyxel Device get the time and date from a time server (see the **Time Server Address** field). This also saves your changes (except the daylight saving settings).
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable Daylight Saving	Daylight saving is a period from late spring to fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **at** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **at** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **at** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **at** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Offset	Specify how much the clock changes when daylight saving begins and ends. Enter a number from 1 to 5.5 (by 0.5 increments). For example, if you set this field to 3.5, a log occurred at 6 P.M. in local official time will appear as if it had occurred at 10:30 P.M.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

17.4.1 Pre-defined NTP Time Servers List

When you turn on the Zyxel Device for the first time, the date and time start at 2003-01-01 00:00:00. The Zyxel Device then attempts to synchronize with one of the following pre-defined list of Network Time Protocol (NTP) time servers.

The Zyxel Device continues to use the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

Table 78 Default Time Servers

0.pool.ntp.org
1.pool.ntp.org
2.pool.ntp.org

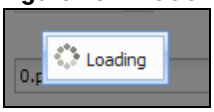
When the Zyxel Device uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the Zyxel Device goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

17.4.2 Time Server Synchronization

Click the **Sync. Now** button to get the time and date from the time server you specified in the **Time Server Address** field.

When the **Loading** message appears, you may have to wait up to one minute.

Figure 104 Loading



The **Current Time** and **Current Date** fields will display the appropriate settings if the synchronization is successful.

If the synchronization was not successful, a log displays in the **View Log** screen. Try re-configuring the **Date/Time** screen.

To manually set the Zyxel Device date and time:

1. Click **System > Date/Time**.
2. Select **Manual** under **Time and Date Setup**.
3. Enter the Zyxel Device's time in the **New Time** field.
4. Enter the Zyxel Device's date in the **New Date** field.
5. Under **Time Zone Setup**, select your **Time Zone** from the list.
6. As an option you can select the **Enable Daylight Saving** check box to adjust the Zyxel Device clock for daylight savings.
7. Click **Apply**.

To get the Zyxel Device date and time from a time server:

1 Click **System > Date/Time**.

2 Select **Get from Time Server** under **Time and Date Setup**.

3 Under **Time Zone Setup**, select your **Time Zone** from the list.

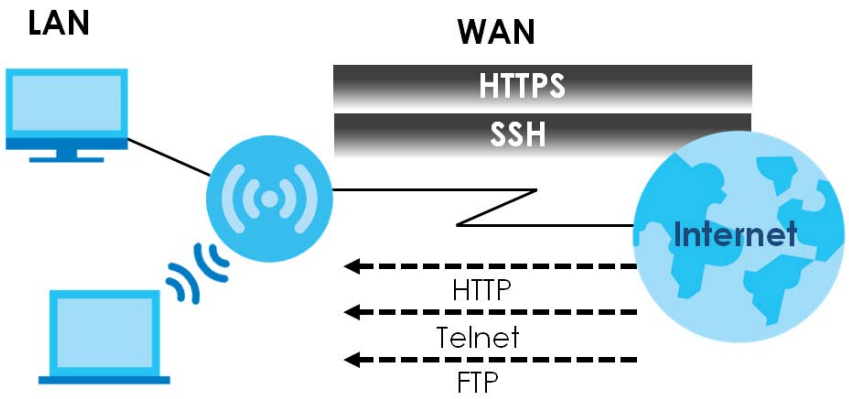
4 Under **Time and Date Setup**, enter a **Time Server Address**.

5 Click **Apply**.

17.5 WWW Overview

The following figure shows secure and insecure management of the Zyxel Device coming in from the WAN. HTTPS and SSH access are secure. HTTP, Telnet, and FTP management access are not secure.

Figure 105 Secure and Insecure Service Access From the WAN



17.5.1 Service Access Limitations

A service cannot be used to access the Zyxel Device when you have disabled that service in the corresponding screen.

17.5.2 System Timeout

There is a lease timeout for administrators. The Zyxel Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

Each user is also forced to log in the Zyxel Device for authentication again when the reauthentication time expires.

You can change the timeout settings in the **User** screens.

17.5.3 HTTPS

You can set the Zyxel Device to use HTTP or HTTPS (HTTPS adds security) for Web Configurator sessions.

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

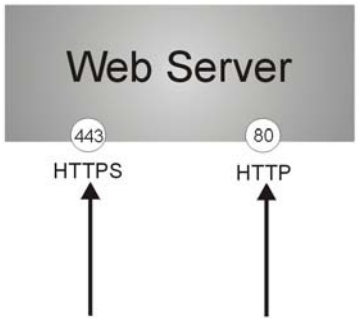
It relies upon certificates, public keys, and private keys (see Chapter 16 on page 155 for more information).

HTTPS on the Zyxel Device is used so that you can securely access the Zyxel Device using the Web Configurator. The SSL protocol specifies that the HTTPS server (the Zyxel Device) must always authenticate itself to the HTTPS client (the computer which requests the HTTPS connection with the Zyxel Device), whereas the HTTPS client only should authenticate itself when the HTTPS server requires it to do so (select **Authenticate Client Certificates** in the **WWW** screen). **Authenticate Client Certificates** is optional and if selected means the HTTPS client must send the Zyxel Device a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the Zyxel Device.

Please refer to the following figure.

1. HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the Zyxel Device's web server.
2. HTTP connection requests from a web browser go to port 80 (by default) on the Zyxel Device's web server.

Figure 106 HTTP/HTTPS Implementation

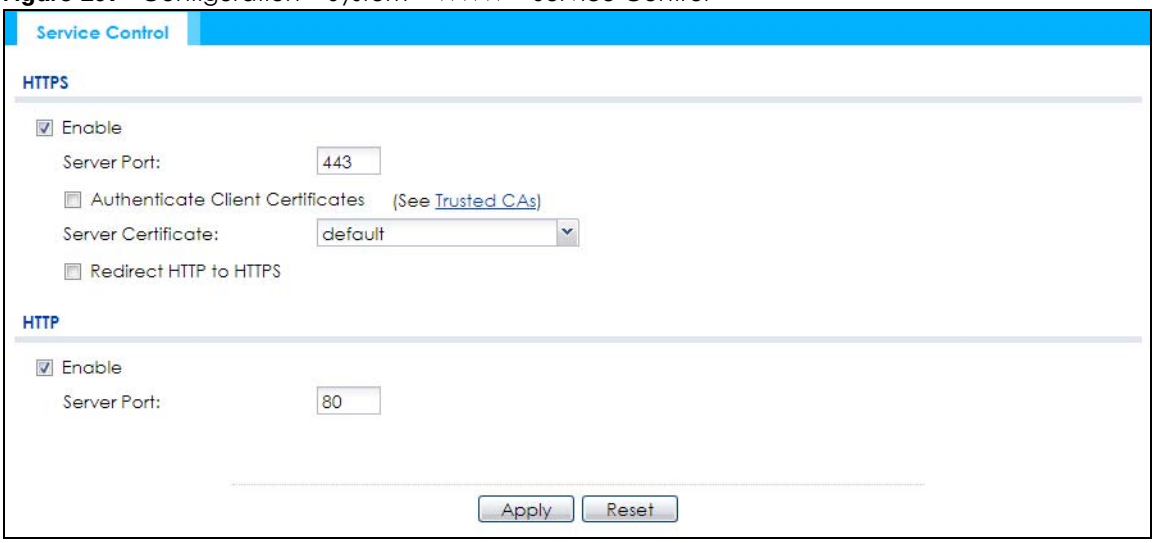


Note: If you disable **HTTP** in the **WWW** screen, then the Zyxel Device blocks all HTTP connection attempts.

17.5.4 Configuring WWW Service Control

Click **Configuration > System > WWW** to open the **WWW** screen. Use this screen to specify HTTP or HTTPS settings.

Figure 107 Configuration > System > WWW > Service Control



The following table describes the labels in this screen.

Table 79 Configuration > System > WWW > Service Control

LABEL	DESCRIPTION
HTTPS	
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the Zyxel Device Web Configurator using secure HTTPs connections.
Server Port	The HTTPS server listens on port 443 by default. If you change the HTTPS server port to a different number on the Zyxel Device, for example 8443, then you must notify people who need to access the Zyxel Device Web Configurator to use "https://Zyxel Device IP Address:**8443**" as the URL.
Authenticate Client Certificates	Select **Authenticate Client Certificates** (optional) to require the SSL client to authenticate itself to the Zyxel Device by sending the Zyxel Device a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the Zyxel Device.
Server Certificate	Select a certificate the HTTPS server (the Zyxel Device) uses to authenticate itself to the HTTPS client. You must have certificates already configured in the **My Certificates** screen.
Redirect HTTP to HTTPS	To allow only secure Web Configurator access, select this to redirect all HTTP connection requests to the HTTPS server.
HTTP	
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the Zyxel Device Web Configurator using HTTP connections.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service to access the Zyxel Device.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

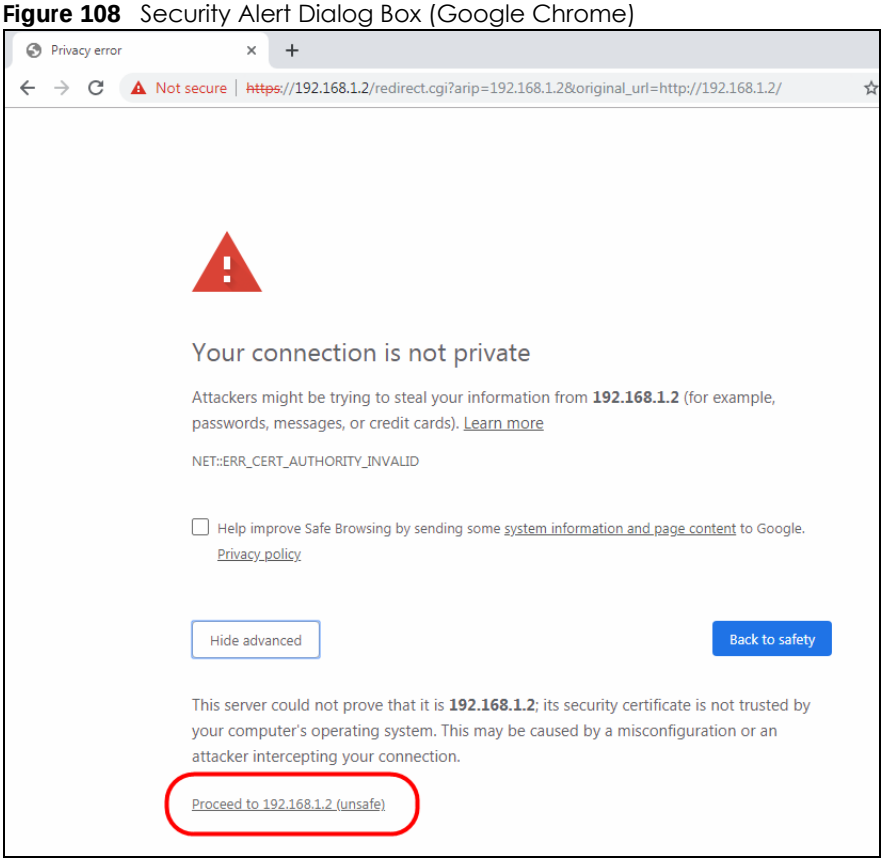
17.5.5 HTTPS Example

If you haven't changed the default HTTPS port on the Zyxel Device, then in your browser enter "https://Zyxel Device IP Address/" as the web site address where "Zyxel Device IP Address" is the IP address or domain name of the Zyxel Device you wish to access.

17.5.5.1 Google Chrome Warning Messages

When you attempt to access the Zyxel Device HTTPS server, you will see the error message shown in the following screen.

Figure 108 Security Alert Dialog Box (Google Chrome)



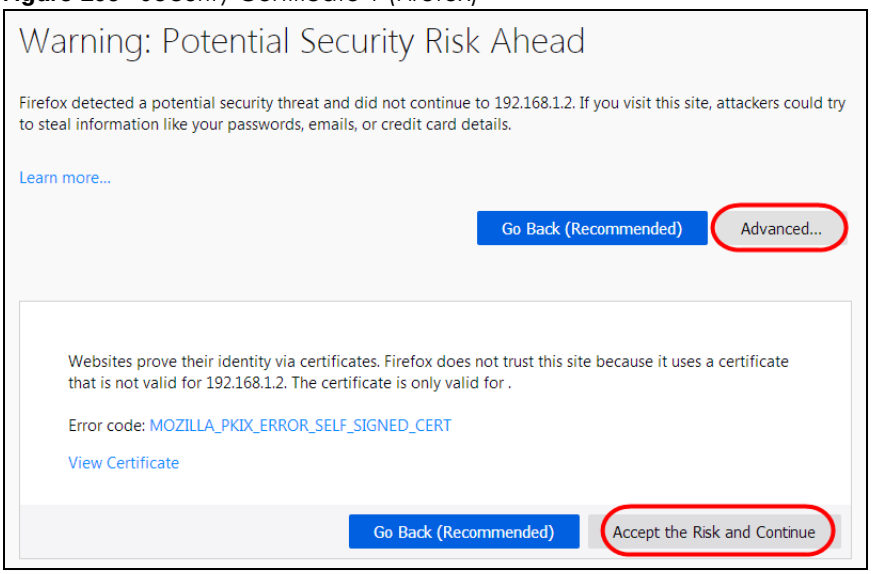
Select **Advanced** > **Proceed to 192.168.1.2 (unsafe)** to proceed to the Web Configurator login screen.

17.5.5.2 Mozilla Firefox Warning Messages

When you attempt to access the Zyxel Device HTTPS server, a Warning screen appears as shown in the following screen. Click **Learn More...** if you want to verify more information about the certificate from the Zyxel Device.

Click **Advanced** > **Accept the Risk and Continue**.

Figure 109 Security Certificate 1 (Firefox)



17.5.5.3 Avoiding Browser Warning Messages

Here are the main reasons your browser displays warnings about the Zyxel Device's HTTPS server certificate and what you can do to avoid seeing the warnings:

- The issuing certificate authority of the Zyxel Device's HTTPS server certificate is not one of the browser's trusted certificate authorities. The issuing certificate authority of the Zyxel Device's factory default certificate is the Zyxel Device itself since the certificate is a self-signed certificate.
- For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
- To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate. Refer to Appendix A on page 249 for details.

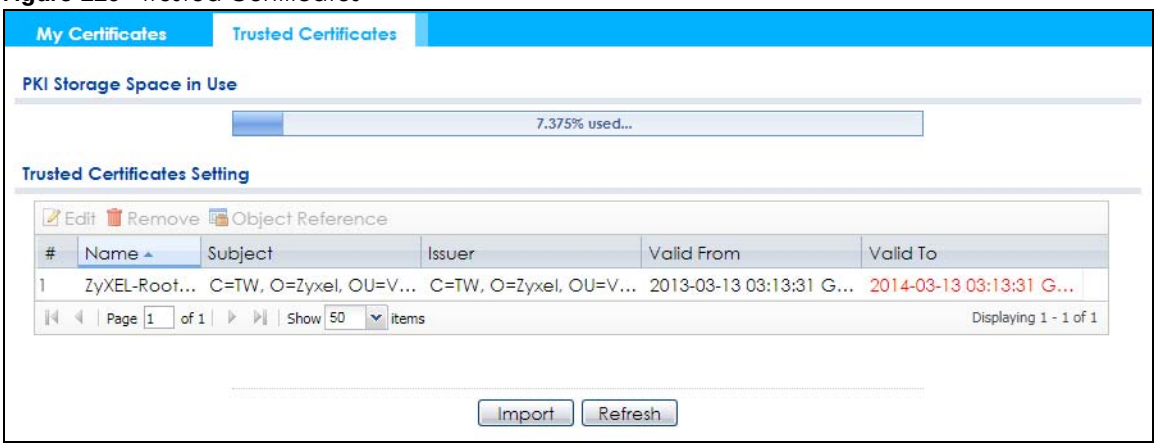
17.5.5.4 Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if **Authenticate Client Certificates** is selected on the Zyxel Device.

You must have imported at least one trusted CA to the Zyxel Device in order for the **Authenticate Client Certificates** to be active (see the Certificates chapter for details).

Apply for a certificate from a Certification Authority (CA) that is trusted by the Zyxel Device (see the Zyxel Device's **Trusted Certificates** Web Configurator screen).

Figure 110 Trusted Certificates



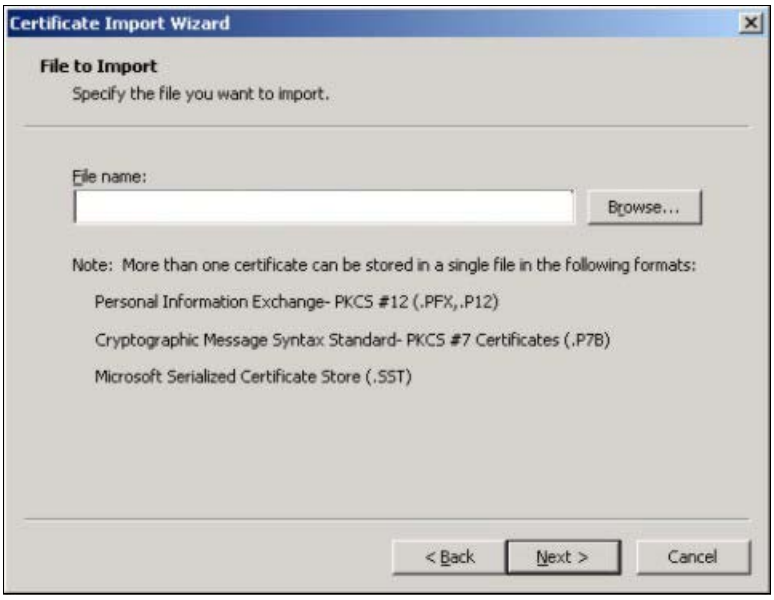
The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

17.5.5.5 Installing a Personal Certificate

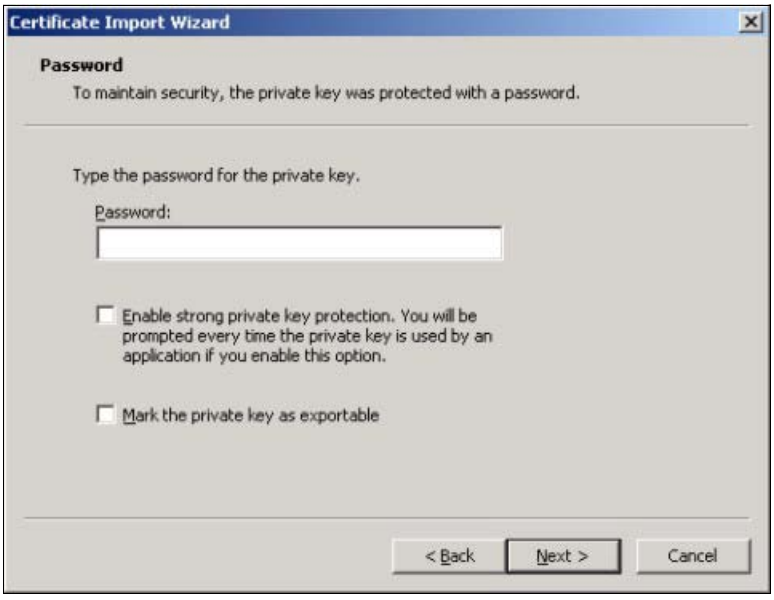
You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next.

1 Click **Next** to begin the wizard.

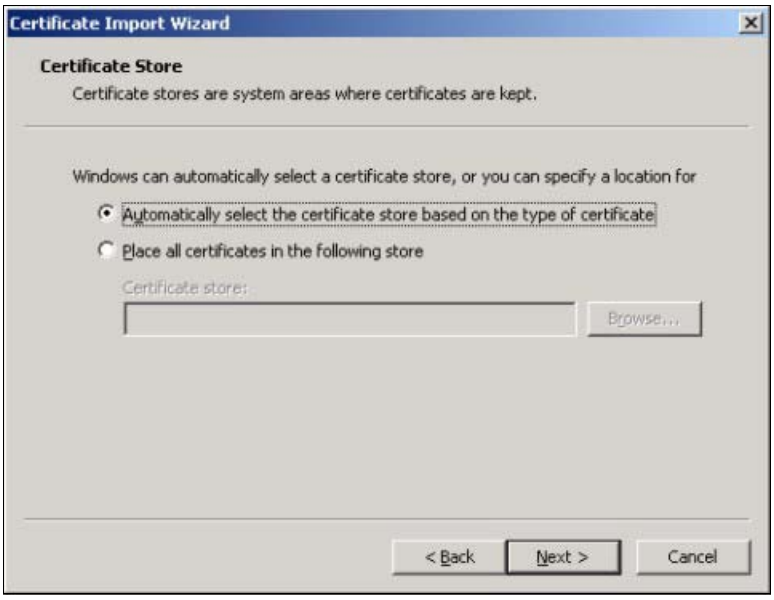
2 The file name and path of the certificate you double-clicked should automatically appear in the **File name** text box. Click **Browse** if you wish to import a different certificate.



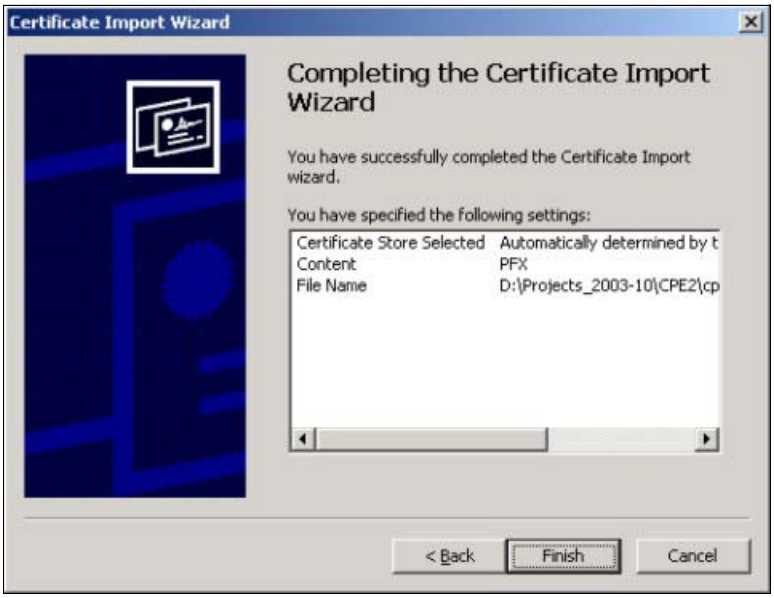
3 Enter the password given to you by the CA.



4 Have the wizard determine where the certificate should be saved on your computer or select **Place all certificates in the following store** and choose a different location.



5 Click **Finish** to complete the wizard and begin the import process.

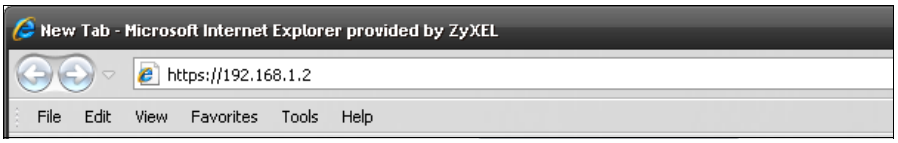


6 You should see the following screen when the certificate is correctly installed on your computer.

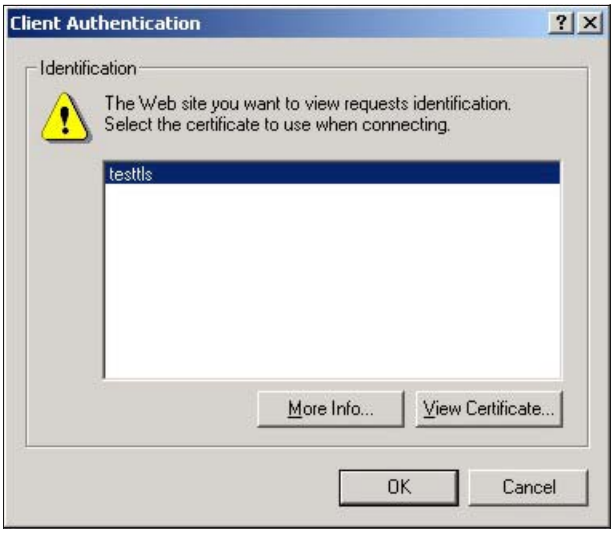
17.5.5.6 Using a Certificate When Accessing the Zyxel Device

To access the Zyxel Device via HTTPS:

1 Enter 'https://Zyxel Device IP Address/' in your browser's web address field.



2 When **Authenticate Client Certificates** is selected on the Zyxel Device, the following screen asks you to select a personal certificate to send to the Zyxel Device. This screen displays even if you only have a single certificate as in the example.



3 You next see the Web Configurator login screen.

17.6 SSH

You can use SSH (Secure SHell) to securely access the Zyxel Device's command line interface.

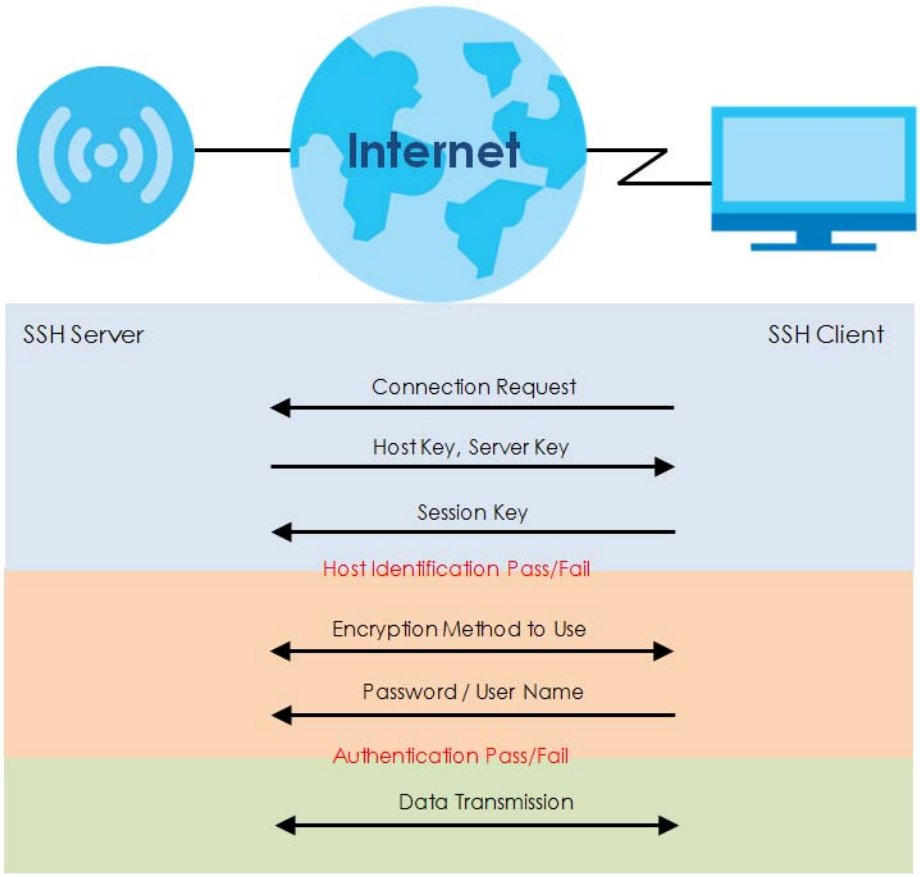
SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. In the following figure, computer B on the Internet uses SSH to securely connect to the Zyxel Device (A) for a management session.

Figure 111 SSH Communication Over the WAN Example

17.6.1 How SSH Works

The following figure is an example of how a secure connection is established between two remote hosts using SSH v1.

Figure 112 How SSH v1 Works Example



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

17.6.2 SSH Implementation on the Zyxel Device

Your Zyxel Device supports SSH versions 1 and 2 using RSA authentication and four encryption methods (AES, 3DES, Archfour, and Blowfish). The SSH server is implemented on the Zyxel Device for management using port 22 (by default).

17.6.3 Requirements for Using SSH

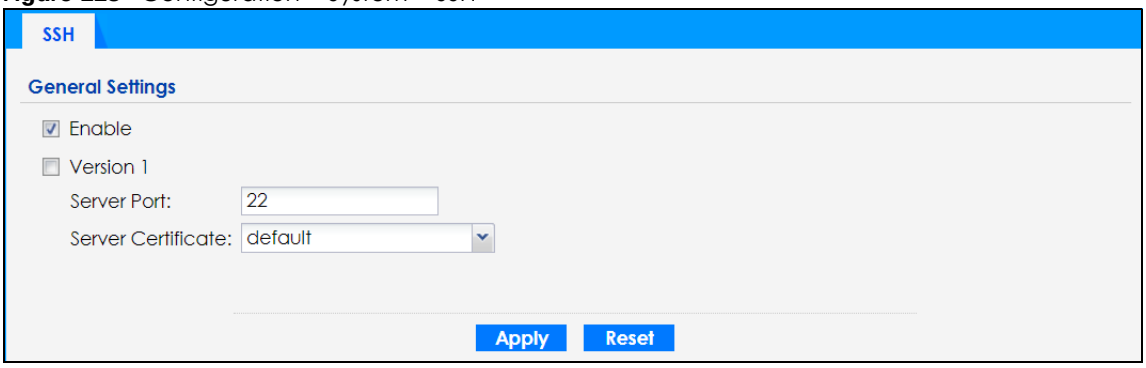
You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the Zyxel Device over SSH.

17.6.4 Configuring SSH

Click **Configuration > System > SSH** to open the following screen. Use this screen to configure your Zyxel Device's Secure Shell settings.

Note: It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

Figure 113 Configuration > System > SSH



The following table describes the labels in this screen.

Table 80 Configuration > System > SSH

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the Zyxel Device CLI using this service. Note: The Zyxel Device uses only SSH version 2 protocol.
Version 1	Select the check box to have the Zyxel Device use both SSH version 1 and version 2 protocols. If you clear the check box, the Zyxel Device uses only SSH version 2 protocol.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the Zyxel Device for SSH connections. You must have certificates already configured in the **My Certificates** screen.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

17.6.5 Examples of Secure Telnet Using SSH

This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the Zyxel Device. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user's guide.

17.6.5.1 Example 1: Microsoft Windows

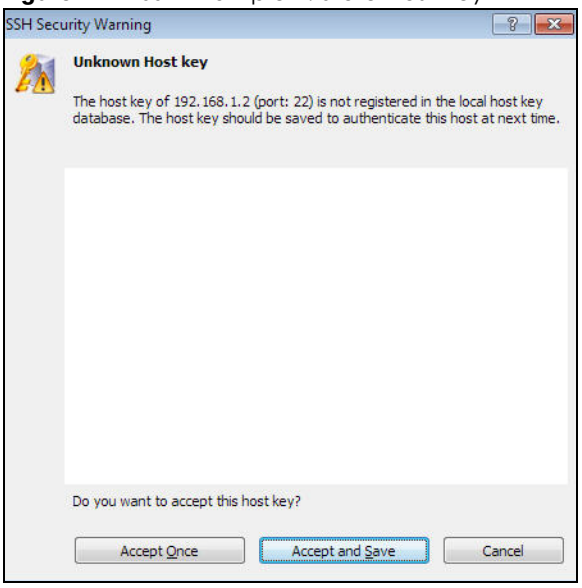
This section describes how to access the Zyxel Device using the Secure Shell Client program.

1 Launch the SSH client and specify the connection information (IP address, port number) for the Zyxel Device.

2 Configure the SSH client to accept connection using SSH version 2.

3 A window displays prompting you to store the host key in you computer. Click **Yes** to continue.

Figure 114 SSH Example 1: Store Host Key



Enter the password to log in to the Zyxel Device. The CLI screen displays next.

17.6.5.2 Example 2: Linux

This section describes how to access the Zyxel Device using the OpenSSH client program that comes with most Linux distributions.

1 Test whether the SSH service is available on the Zyxel Device.

Enter "`telnet 192.168.1.2 22`" at a terminal prompt and press [ENTER]. The computer attempts to connect to port 22 on the Zyxel Device (using the default IP address of 192.168.1.2).

A message displays indicating the SSH protocol version supported by the Zyxel Device.

Figure 115 SSH Example 2: Test

```
$ telnet 192.168.1.2 22
Trying 192.168.1.2...
Connected to 192.168.1.2.
Escape character is '^]'.
SSH-1.5-1.0.0
```

2 Enter "`ssh -2 192.168.1.2`". This command forces your computer to connect to the Zyxel Device using SSH version 1. If this is the first time you are connecting to the Zyxel Device using SSH, a message displays prompting you to save the host information of the Zyxel Device. Type "`yes`" and press [ENTER].

Then enter the password to log in to the Zyxel Device.

Figure 116 SSH Example 2: Log in

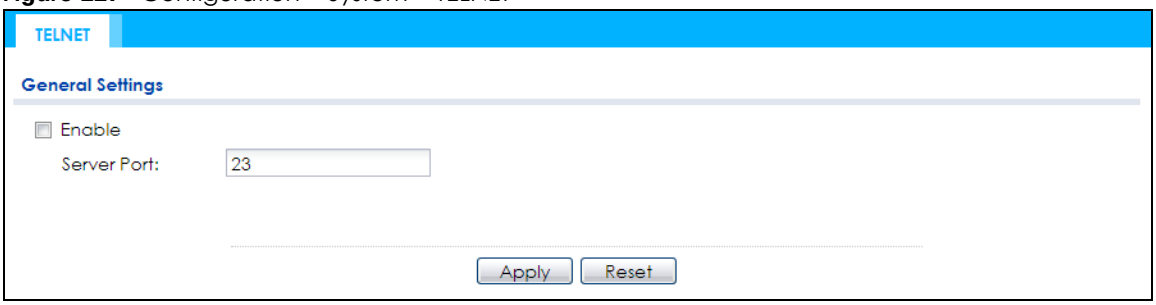
```
$ ssh -2 192.168.1.2
The authenticity of host '192.168.1.2 (192.168.1.2)' can't be established.
RSA1 key fingerprint is 21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.2' (RSA1) to the list of known hosts.
Administrator@192.168.1.2's password:
```

3 The CLI screen displays next.

17.7 Telnet

You can use Telnet to access the Zyxel Device's command line interface. Click **Configuration > System > TELNET** to configure your Zyxel Device for remote Telnet access. Use this screen to enable or disable Telnet and set the server port number.

Figure 117 Configuration > System > TELNET



The following table describes the labels in this screen.

Table 81 Configuration > System > TELNET

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the Zyxel Device CLI using this service.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.

Table 81 Configuration > System > TELNET (continued)

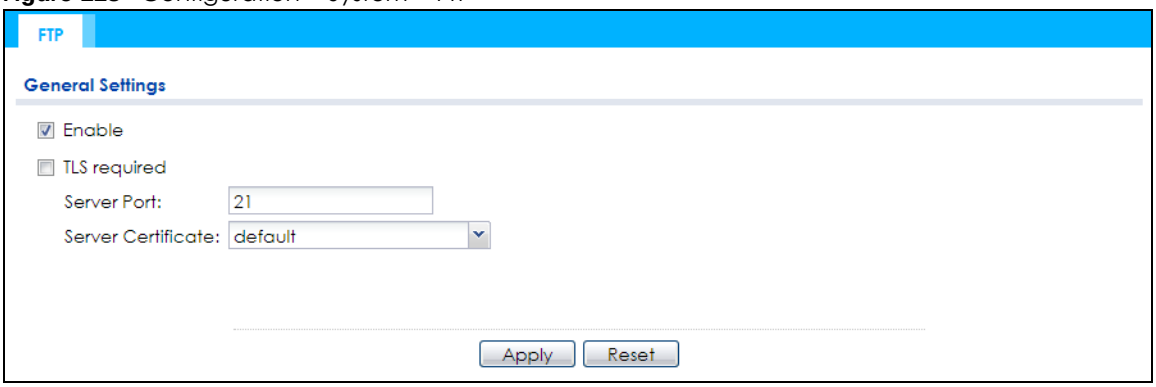
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

17.8 FTP

You can upload and download the Zyxel Device's firmware and configuration files using FTP. To use this feature, your computer must have an FTP client. See Chapter 19 on page 206 for more information about firmware and configuration files.

To change your Zyxel Device's FTP settings, click **Configuration > System > FTP** tab. The screen appears as shown. Use this screen to specify FTP settings.

Figure 118 Configuration > System > FTP



The following table describes the labels in this screen.

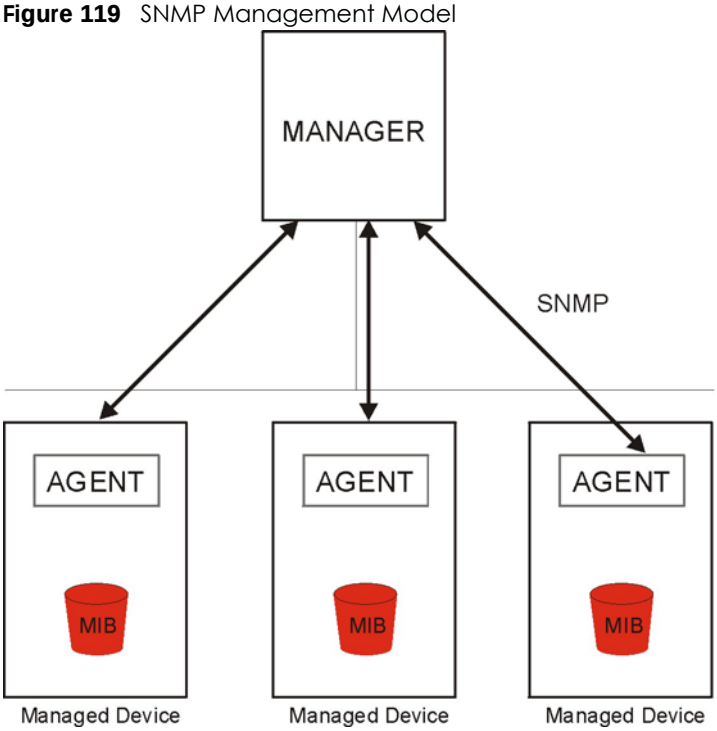
Table 82 Configuration > System > FTP

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the Zyxel Device using this service.
TLS required	Select the check box to use FTP over TLS (Transport Layer Security) to encrypt communication. This implements TLS as a security mechanism to secure FTP clients and/or servers.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the Zyxel Device for FTP connections. You must have certificates already configured in the **My Certificates** screen.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

17.9 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your Zyxel Device supports SNMP agent functionality, which allows a manager station to manage and monitor the Zyxel Device through the network. The Zyxel Device supports SNMP version one (SNMPv1), version two (SNMPv2c), and version three (SNMPv3). The next figure illustrates an SNMP management operation.

Figure 119 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the Zyxel Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.

- Trap - Used by the agent to inform the manager of some events.

17.9.1 Supported MIBs

The Zyxel Device supports MIB II that is defined in RFC-1213 and RFC-1215. The Zyxel Device also supports private MIBs (ZYXEL-ES-CAPWAP.MIB, ZYXEL-ES-COMMON.MIB, ZYXEL-ES-ZyXELAPMgmt.MIB, ZYXEL-ES-PROWLAN.MIB, ZYXEL-ES-RFMGMT.MIB, ZYXEL-ES-SMI.MIB, and ZYXEL-ES-WIRELESS.MIB) to collect information about CPU and memory usage and VPN total throughput. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance. You can download the Zyxel Device's MIBs from www.zyxel.com.

17.9.2 SNMP Traps

The Zyxel Device will send traps to the SNMP manager when any one of the following events occurs.

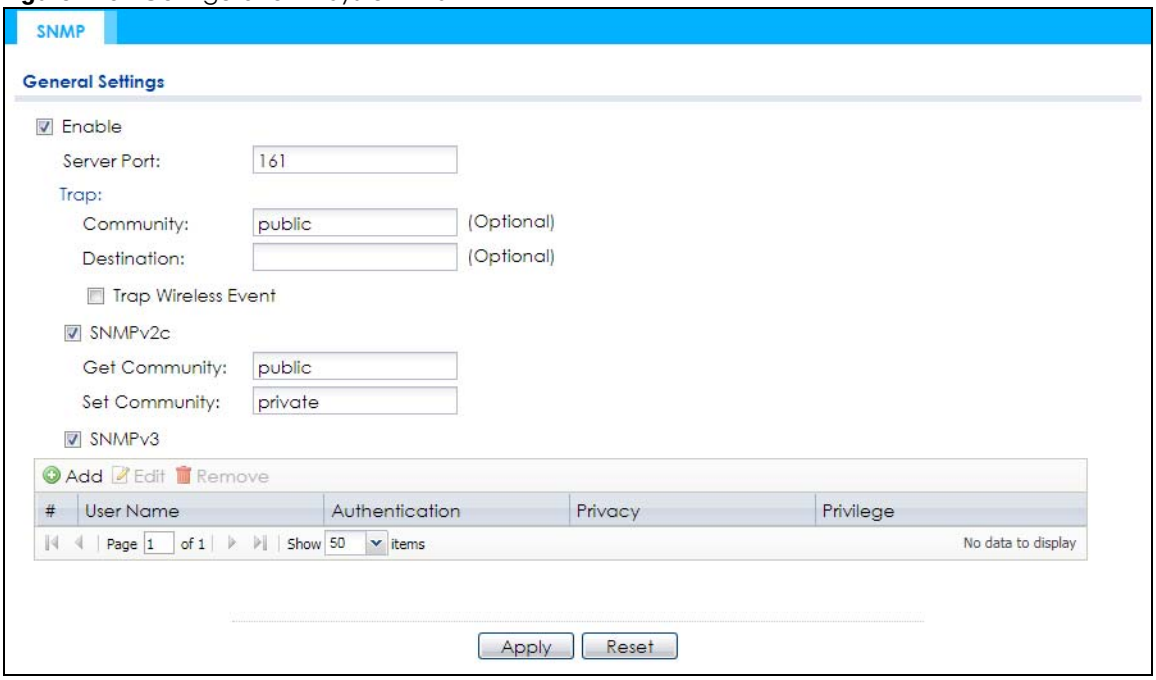
Table 83 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.

17.9.3 Configuring SNMP

To change your Zyxel Device's SNMP settings, click **Configuration > System > SNMP** tab. The screen appears as shown. Use this screen to configure your SNMP settings. You can also configure user profiles that define allowed SNMPv3 access.

Figure 120 Configuration > System > SNMP



The following table describes the labels in this screen.

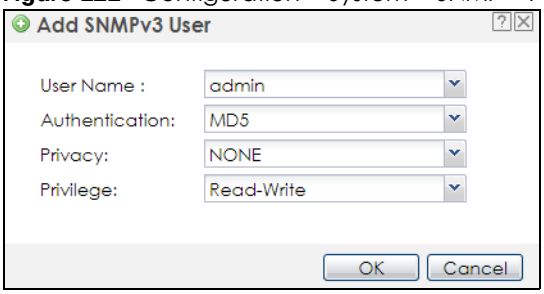
Table 84 Configuration > System > SNMP

LABEL	DESCRIPTION
Enable	Select the check box to allow or disallow users to access the Zyxel Device using SNMP.
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
Trap Wireless Event	Select this to have the Zyxel Device send a trap to the SNMP manager when a wireless client is connected to or disconnected from the Zyxel Device.
SNMPv2c	Select this to allow SNMP managers using SNMPv2c to access the Zyxel Device.
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is private and allows all requests.
SNMPv3	Select this to allow SNMP managers using SNMPv3 to access the Zyxel Device.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to be able to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so. Note that subsequent entries move up by one when you take this action.
#	This the index number of an SNMPv3 user profile.
User Name	This is the name of the user for which this SNMPv3 user profile is configured.
Authentication	This field displays the type of authentication the SNMPv3 user must use to connect to the Zyxel Device using this SNMPv3 user profile.
Privacy	This field displays the type of encryption the SNMPv3 user must use to connect to the Zyxel Device using this SNMPv3 user profile.
Privilege	This field displays whether the SNMPv3 user can have read-only or read and write access to the Zyxel Device using this SNMPv3 user profile.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

17.9.4 Adding or Editing an SNMPv3 User Profile

This screen allows you to add or edit an SNMPv3 user profile. To access this screen, click the **Configuration > System > SNMP** screen's **Add** button or select a SNMPv3 user profile from the list and click the **Edit** button.

Figure 121 Configuration > System > SNMP > Add



The following table describes the labels in this screen.

Table 85 Configuration > System > SNMP

LABEL	DESCRIPTION
User Name	Select the user name of the user account for which this SNMPv3 user profile is configured.
Authentication	Select the type of authentication the SNMPv3 user must use to connect to the Zyxel Device using this SNMPv3 user profile. Select **MD5** to require the SNMPv3 user's password be encrypted by MD5 for authentication. Select **SHA** to require the SNMPv3 user's password be encrypted by SHA for authentication.
Privacy	Select the type of encryption the SNMPv3 user must use to connect to the Zyxel Device using this SNMPv3 user profile. Select **NONE** to not encrypt the SNMPv3 communications. Select **DES** to use DES to encrypt the SNMPv3 communications. Select **AES** to use AES to encrypt the SNMPv3 communications.
Privilege	Select whether the SNMPv3 user can have read-only or read and write access to the Zyxel Device using this SNMPv3 user profile.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

CHAPTER 18
Log and Report

18.1 Overview

Use the system screens to configure daily reporting and log settings.

18.1.1 What You Can Do In this Chapter

- The **Email Daily Report** screen (Section 18.2 on page 194) configures how and where to send daily reports and what reports to send.
- The **Log Setting** screens (Section 18.3 on page 196) specify which logs are e-mailed, where they are e-mailed, and how often they are e-mailed.

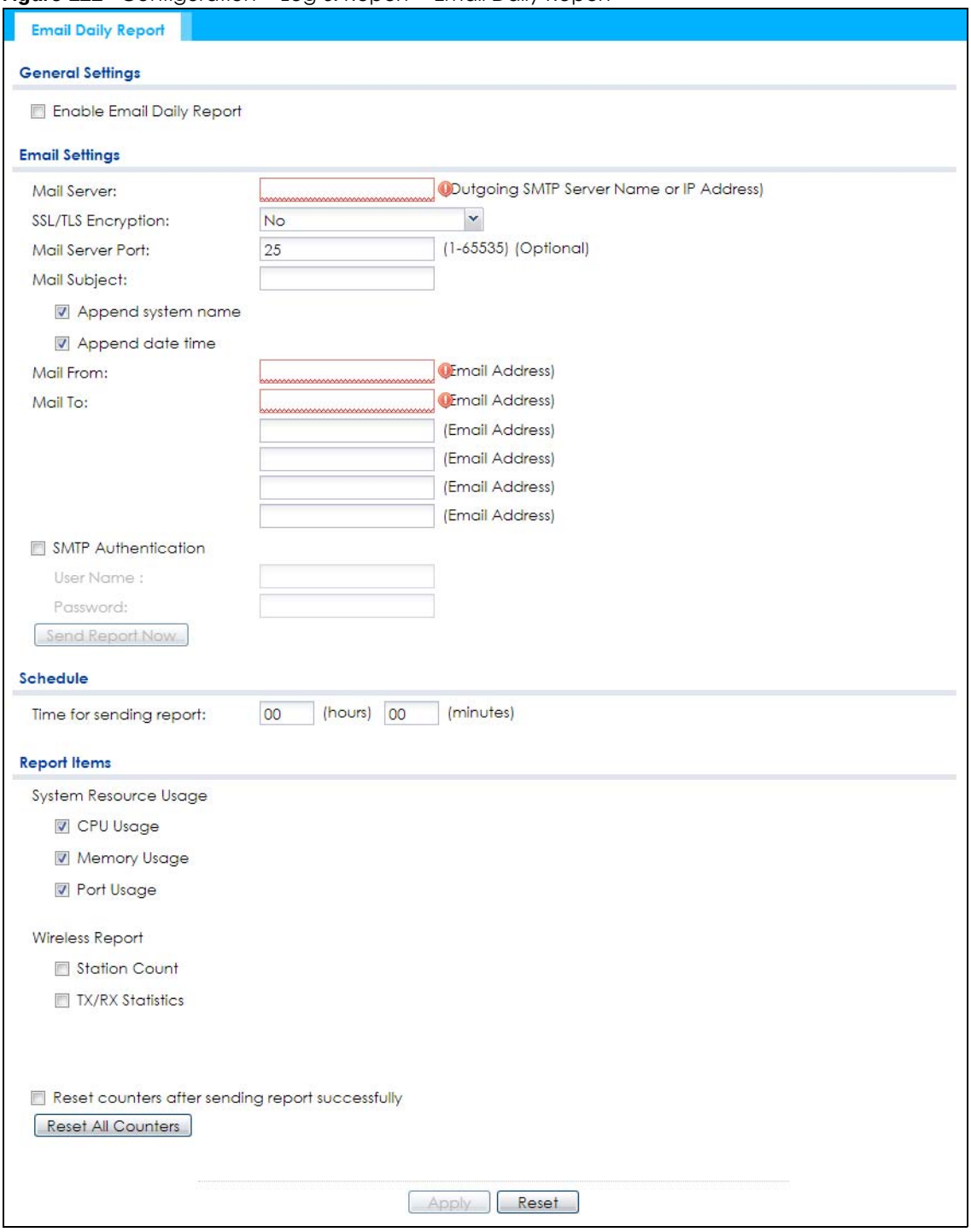
18.2 Email Daily Report

Use this screen to start or stop data collection and view various statistics about traffic passing through your Zyxel Device.

Note: Data collection may decrease the Zyxel Device's traffic throughput rate.

Click **Configuration > Log & Report > Email Daily Report** to display the following screen. Configure this screen to have the Zyxel Device e-mail you system statistics every day.

Figure 122 Configuration > Log & Report > Email Daily Report



The following table describes the labels in this screen.

Table 86 Configuration > Log & Report > Email Daily Report

LABEL	DESCRIPTION
Enable Email Daily Report	Select this to send reports by e-mail every day.
Mail Server	Type the name or IP address of the outgoing SMTP server.

Table 86 Configuration > Log & Report > Email Daily Report (continued)

LABEL	DESCRIPTION
SSL/TLS Encryption	Select **SSL/TLS** to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) if you want encrypted communications between the mail server and the Zyxel Device. Select **STARTTLS** to upgrade a plain text connection to a secure connection using SSL/TLS. Select **No** to not encrypt the communications.
Mail Server Port	Enter the same port number here as is on the mail server for mail traffic.
Mail Subject	Type the subject line for the outgoing e-mail. Select **Append system name** to add the Zyxel Device's system name to the subject. Select **Append date time** to add the Zyxel Device's system date and time to the subject.
Mail From	Type the e-mail address from which the outgoing e-mail is delivered. This address is used in replies.
Mail To	Type the e-mail address (or addresses) to which the outgoing e-mail is delivered.
SMTP Authentication	Select this check box if it is necessary to provide a user name and password to the SMTP server.
User Name	This box is effective when you select the **SMTP Authentication** check box. Type the user name to provide to the SMTP server when the log is e-mailed.
Password	This box is effective when you select the **SMTP Authentication** check box. Type the password to provide to the SMTP server when the log is e-mailed.
Send Report Now	Click this button to have the Zyxel Device send the daily e-mail report immediately.
Time for sending report	Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.
Report Items	Select the information to include in the report. Select **Reset counters after sending report successfully** if you only want to see statistics for a 24 hour period.
Reset All Counters	Click this to discard all report data and start all of the counters over at zero.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

18.3 Log Setting

These screens control log messages and alerts. A log message stores the information for viewing (for example, in the **Monitor > View Log** screen) or regular e-mailing later, and an alert is e-mailed immediately. Usually, alerts are used for events that require more serious attention, such as system errors and attacks.

The Zyxel Device provides a system log and supports e-mail profiles and remote syslog servers. The system log is available on the **View Log** screen, the e-mail profiles are used to mail log messages to the specified destinations, and the other four logs are stored on specified syslog servers.

The **Log Setting** tab also controls what information is saved in each log. For the system log, you can also specify which log messages are e-mailed, where they are e-mailed, and how often they are e-mailed.

For alerts, the **Log Setting** screen controls which events generate alerts and where alerts are e-mailed.

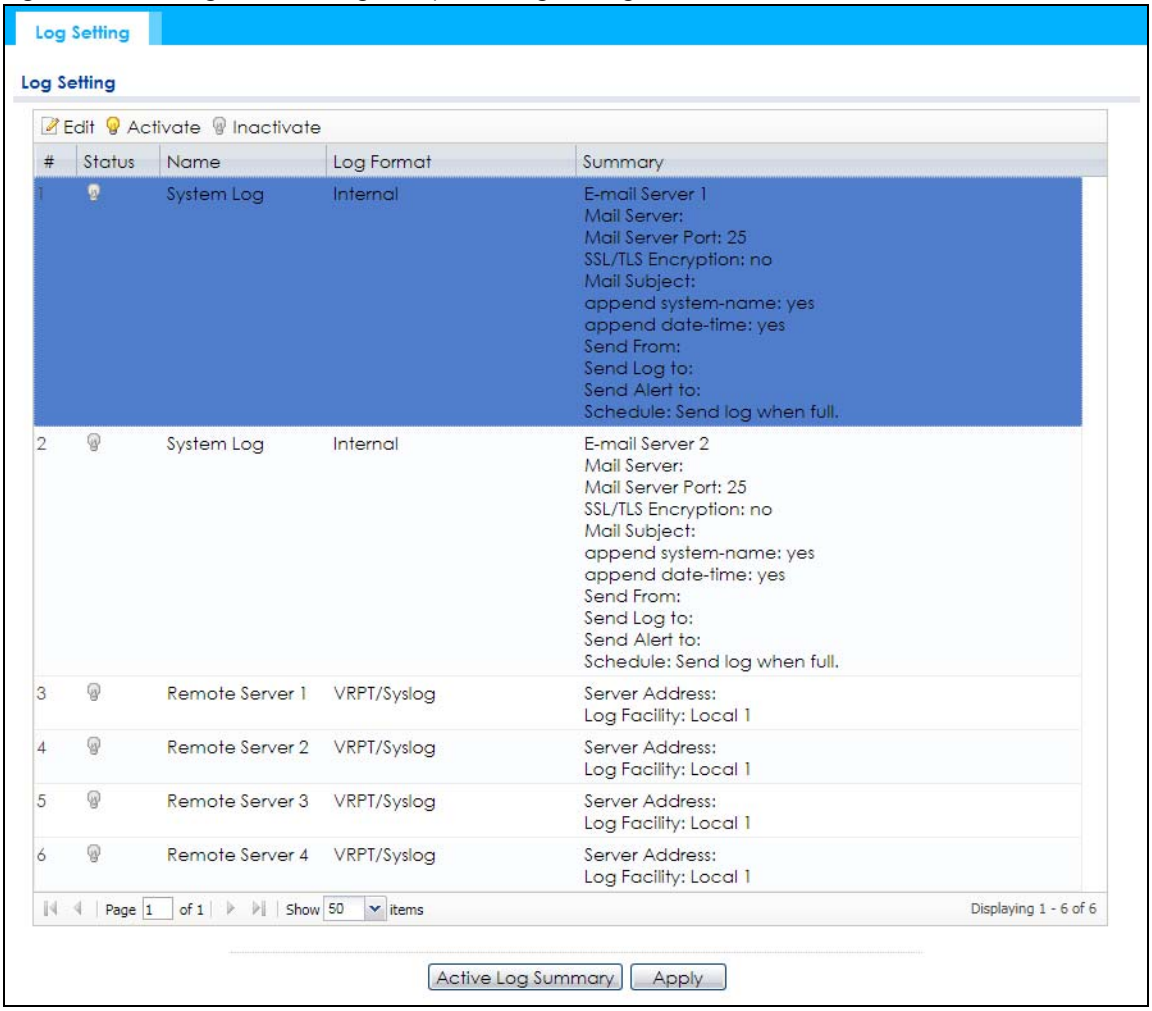
The **Log Setting** screen provides a summary of all the settings. You can use the **Edit Log Setting** screen to maintain the detailed settings (such as log categories, e-mail addresses, server names, etc.) for any log.

Alternatively, if you want to edit what events is included in each log, you can also use the **Active Log Summary** screen to edit this information for all logs at the same time.

18.3.1 Log Setting Screen

To access this screen, click **Configuration > Log & Report > Log Setting**.

Figure 123 Configuration > Log & Report > Log Setting



The following table describes the labels in this screen.

Table 87 Configuration > Log & Report > Log Setting

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	This field is a sequential value, and it is not associated with a specific log.
Status	This field shows whether the log is active or not.
Name	This field displays the name of the log (system log or one of the remote servers).

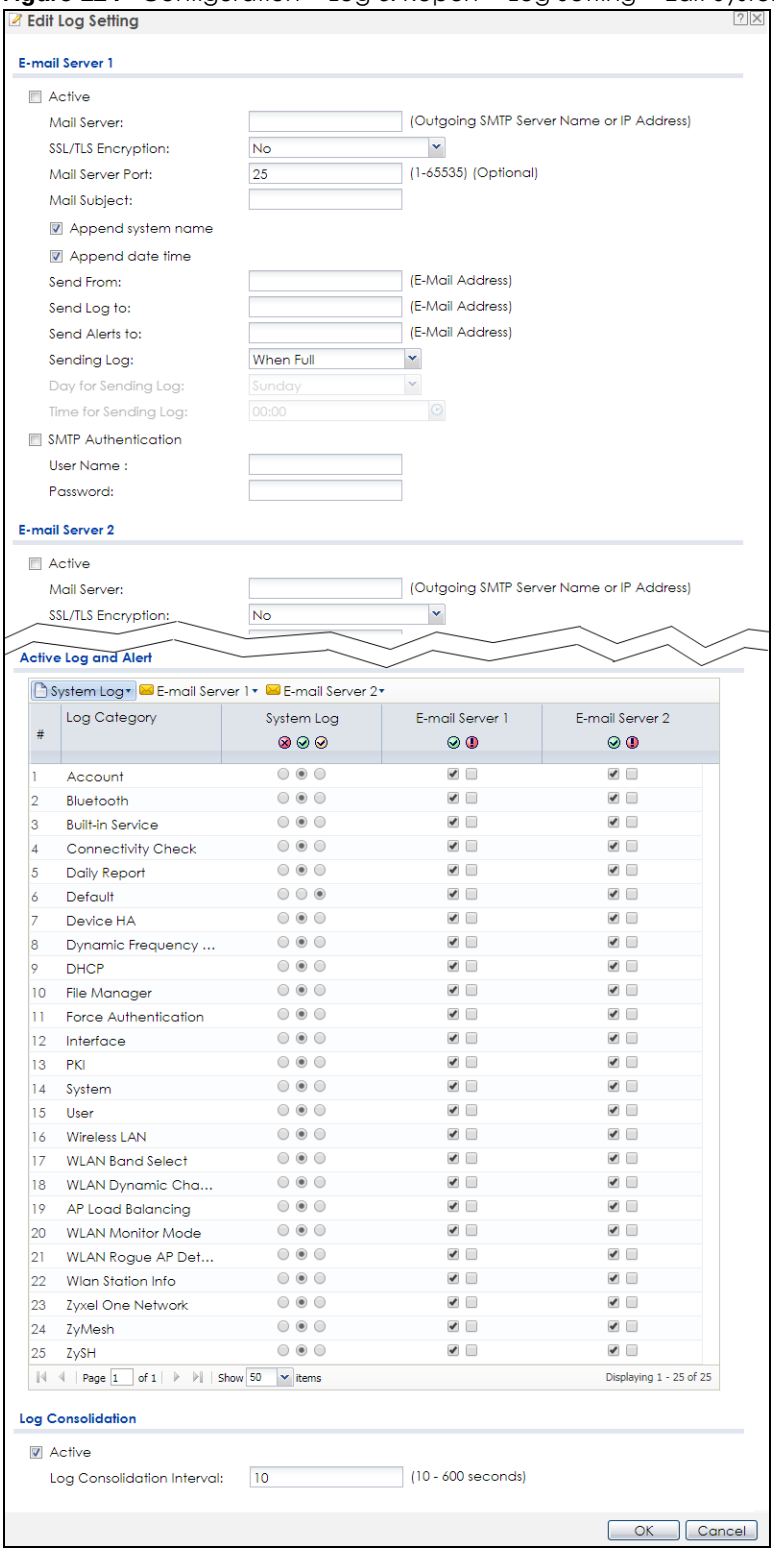
Table 87 Configuration > Log & Report > Log Setting (continued)

LABEL	DESCRIPTION
Log Format	This field displays the format of the log. **Internal** - system log; you can view the log on the **View Log** tab. **VRPT/Syslog** - Zyxel's Vantage Report, syslog-compatible format. **CEF/Syslog** - Common Event Format, syslog-compatible format.
Summary	This field is a summary of the settings for each log.
Active Log Summary	Click this button to open the **Active Log Summary** screen.
Apply	Click this button to save your changes (activate and deactivate logs) and make them take effect.

18.3.2 Edit System Log Settings

This screen controls the detailed settings for each log in the system log (which includes the e-mail profiles). Select a system log entry in the **Log Setting** screen and click the **Edit** icon.

Figure 124 Configuration > Log & Report > Log Setting > Edit System Log Setting



The following table describes the labels in this screen.

Table 88 Configuration > Log & Report > Log Setting > Edit System Log Setting

LABEL	DESCRIPTION
E-Mail Server 1/2	
Active	Select this to send log messages and alerts according to the information in this section. You specify what kinds of log messages are included in log information and what kinds of log messages are included in alerts in the **Active Log and Alert** section.
Mail Server	Type the name or IP address of the outgoing SMTP server.
SSL/TLS Encryption	Select **SSL/TLS** to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) if you want encrypted communications between the mail server and the Zyxel Device. Select **STARTTLS** to upgrade a plain text connection to a secure connection using SSL/TLS. Select **No** to not encrypt the communications.
Mail Server Port	Enter the same port number here as is on the mail server for mail traffic.
Mail Subject	Type the subject line for the outgoing e-mail. Select **Append system name** to add the Zyxel Device's system name to the subject. Select **Append date time** to add the Zyxel Device's system date and time to the subject.
Send From	Type the e-mail address from which the outgoing e-mail is delivered. This address is used in replies.
Send Log To	Type the e-mail address to which the outgoing e-mail is delivered.
Send Alerts To	Type the e-mail address to which alerts are delivered.
Sending Log	Select how often log information is e-mailed. Choices are: **When Full**, **Hourly and When Full**, **Daily and When Full**, and **Weekly and When Full**.
Day for Sending Log	This field is available if the log is e-mailed weekly. Select the day of the week the log is e-mailed.
Time for Sending Log	This field is available if the log is e-mailed weekly or daily. Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.
SMTP Authentication	Select this check box if it is necessary to provide a user name and password to the SMTP server.
User Name	This box is effective when you select the **SMTP Authentication** check box. Type the user name to provide to the SMTP server when the log is e-mailed.
Password	This box is effective when you select the **SMTP Authentication** check box. Type the password to provide to the SMTP server when the log is e-mailed.
Active Log and Alert	
System log	Use the **System Log** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not log any information for any category for the system log or e-mail any logs to e-mail server 1 or 2. **enable normal logs** (green check mark) - create log messages and alerts for all categories for the system log. If e-mail server 1 or 2 also has normal logs enabled, the Zyxel Device will e-mail logs to them. **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information for all categories. The Zyxel Device does not e-mail debugging information, even if this setting is selected.

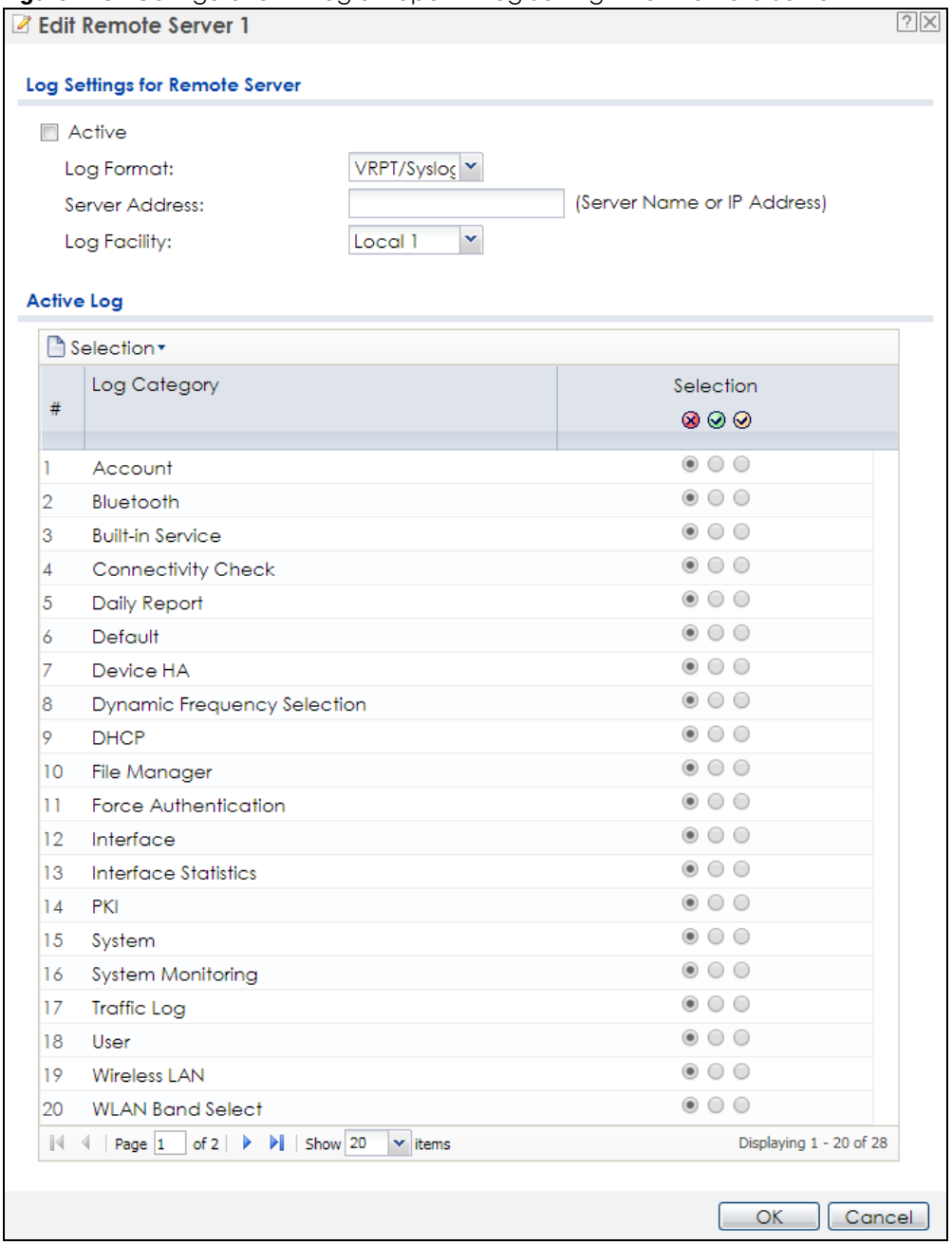
Table 88 Configuration > Log & Report > Log Setting > Edit System Log Setting (continued)

LABEL	DESCRIPTION
E-mail Server 1	Use the **E-Mail Server 1** drop-down list to change the settings for e-mailing logs to e-mail server 1 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your e-mail server 1 settings. **enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 1. **enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 1.
E-mail Server 2	Use the **E-Mail Server 2** drop-down list to change the settings for e-mailing logs to e-mail server 2 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your e-mail server 2 settings. **enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 2. **enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 2.
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
System log	Select which events you want to log by **Log Category**. There are three choices: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green check mark) - create log messages and alerts from this category **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information from this category; the Zyxel Device does not e-mail debugging information, however, even if this setting is selected.
E-mail Server 1	Select whether each category of events should be included in the log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in **E-Mail Server 1**. The Zyxel Device does not e-mail debugging information, even if it is recorded in the **System log**.
E-mail Server 2	Select whether each category of events should be included in log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in **E-Mail Server 2**. The Zyxel Device does not e-mail debugging information, even if it is recorded in the **System log**.
Log Consolidation	
Active	Select this to activate log consolidation. Log consolidation aggregates multiple log messages that arrive within the specified **Log Consolidation Interval**. In the **View Log** tab, the text "[count=*x*]", where *x* is the number of original log messages, is appended at the end of the **Message** field, when multiple log messages were aggregated.
Log Consolidation Interval	Type how often, in seconds, to consolidate log information. If the same log message appears multiple times, it is aggregated into one log message with the text "[count=*x*]", where *x* is the number of original log messages, appended at the end of the **Message** field.
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

18.3.3 Edit Remote Server

This screen controls the settings for each log in the remote server (syslog). Select a remote server entry in the **Log Setting** screen and click the **Edit** icon.

Figure 125 Configuration > Log & Report > Log Setting > Edit Remote Server



The following table describes the labels in this screen.

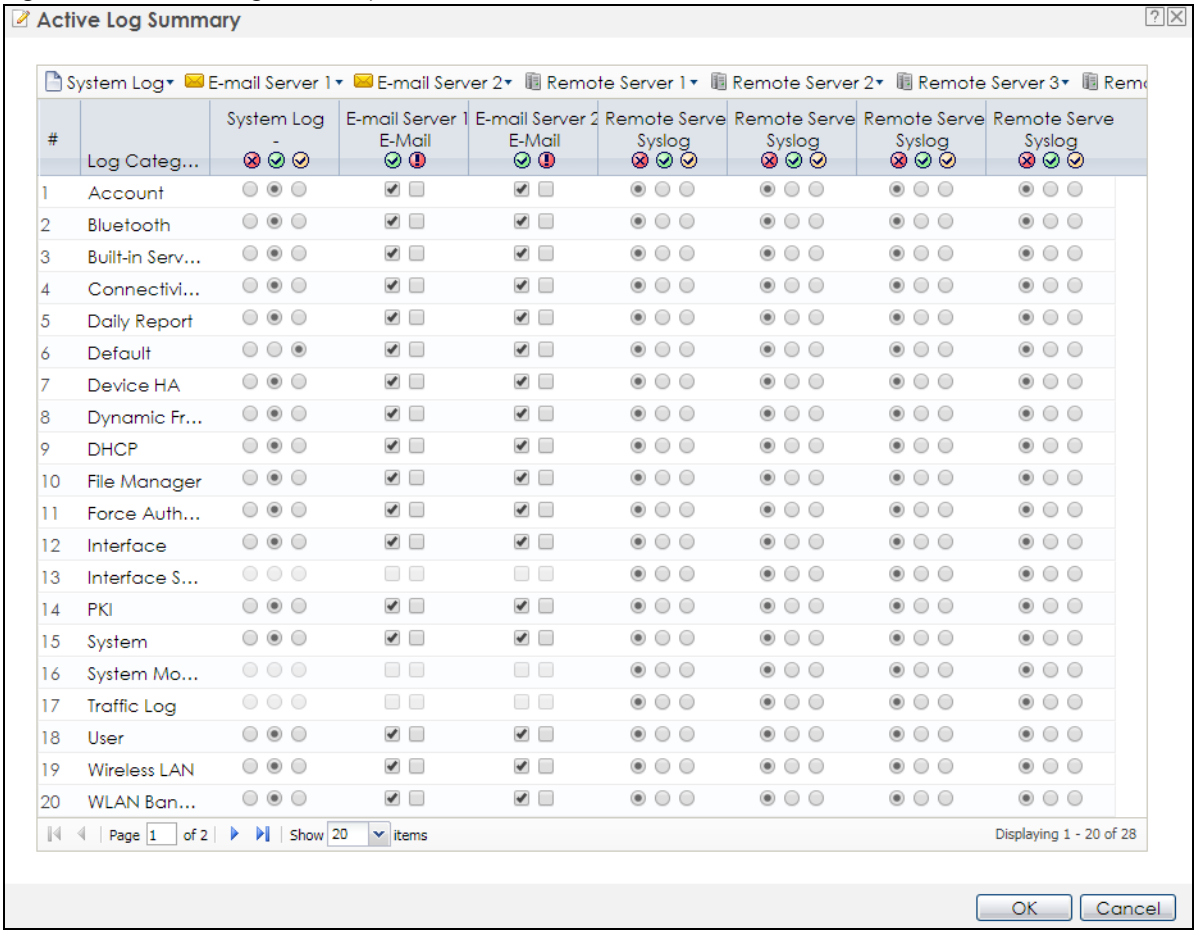
Table 89 Configuration > Log & Report > Log Setting > Edit Remote Server

LABEL	DESCRIPTION
Log Settings for Remote Server	
Active	Select this check box to send log information according to the information in this section. You specify what kinds of messages are included in log information in the **Active Log** section.
Log Format	This field displays the format of the log information. It is read-only. **VRPT/Syslog** - Zyxel's Vantage Report, syslog-compatible format. **CEF/Syslog** - Common Event Format, syslog-compatible format.
Server Address	Type the server name or the IP address of the syslog server to which to send log information.
Log Facility	Select a log facility. The log facility allows you to log the messages to different files in the syslog server. Please see the documentation for your syslog program for more information.
Active Log	
Selection	Use the **Selection** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not send the remote server logs for any log category. **enable normal logs** (green check mark) - send the remote server log messages and alerts for all log categories. **enable normal logs and debug logs** (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
Selection	Select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green checkmark) - log regular information and alerts from this category **enable normal logs and debug logs** (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

18.3.4 Active Log Summary

This screen allows you to view and to edit what information is included in the system log, e-mail profiles, and remote servers at the same time. It does not let you change other log settings (for example, where and how often log information is e-mailed or remote server names). To access this screen, go to the **Log Setting** screen, and click the **Active Log Summary** button.

Figure 126 Active Log Summary



This screen provides a different view and a different way of indicating which messages are included in each log and each alert. (The **Default** category includes debugging messages generated by open source software.)

The following table describes the fields in this screen.

Table 90 Configuration > Log & Report > Log Setting > Active Log Summary

LABEL	DESCRIPTION
Active Log Summary	If the Zyxel Device is set to controller mode, the AC section controls logs generated by the controller and the AP section controls logs generated by the managed APs.
System log	Use the **System Log** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not log any information for any category for the system log or e-mail any logs to e-mail server 1 or 2. **enable normal logs** (green check mark) - create log messages and alerts for all categories for the system log. If e-mail server 1 or 2 also has normal logs enabled, the Zyxel Device will e-mail logs to them. **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information for all categories. The Zyxel Device does not e-mail debugging information, even if this setting is selected.

Table 90 Configuration > Log & Report > Log Setting > Active Log Summary (continued)

LABEL	DESCRIPTION
E-mail Server 1	Use the **E-Mail Server 1** drop-down list to change the settings for e-mailing logs to e-mail server 1 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your e-mail server 1 settings. **enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 1. **enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 1.
E-mail Server 2	Use the **E-Mail Server 2** drop-down list to change the settings for e-mailing logs to e-mail server 2 for all log categories. Using the **System Log** drop-down list to disable all logs overrides your e-mail server 2 settings. **enable normal logs** (green check mark) - e-mail log messages for all categories to e-mail server 2. **enable alert logs** (red exclamation point) - e-mail alerts for all categories to e-mail server 2.
Remote Server 1~4	For each remote server, use the **Selection** drop-down list to change the log settings for all of the log categories. **disable all logs** (red X) - do not send the remote server logs for any log category. **enable normal logs** (green check mark) - send the remote server log messages and alerts for all log categories. **enable normal logs and debug logs** (yellow check mark) - send the remote server log messages, alerts, and debugging information for all log categories.
#	This field is a sequential value, and it is not associated with a specific address.
Log Category	This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software.
System log	Select which events you want to log by **Log Category**. There are three choices: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green checkmark) - create log messages and alerts from this category **enable normal logs and debug logs** (yellow check mark) - create log messages, alerts, and debugging information from this category; the Zyxel Device does not e-mail debugging information, however, even if this setting is selected.
E-mail Server 1 E-mail	Select whether each category of events should be included in the log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in **E-Mail Server 1**. The Zyxel Device does not e-mail debugging information, even if it is recorded in the **System log**.
E-mail Server 2 E-mail	Select whether each category of events should be included in log messages when it is e-mailed (green check mark) and/or in alerts (red exclamation point) for the e-mail settings specified in **E-Mail Server 2**. The Zyxel Device does not e-mail debugging information, even if it is recorded in the **System log**.
Remote Server 1~4 Syslog	For each remote server, select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are: **disable all logs** (red X) - do not log any information from this category **enable normal logs** (green checkmark) - log regular information and alerts from this category **enable normal logs and debug logs** (yellow check mark) - log regular information, alerts, and debugging information from this category
OK	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

CHAPTER 19
File Manager

19.1 Overview

Configuration files define the Zyxel Device's settings. Shell scripts are files of commands that you can store on the Zyxel Device and run when you need them. You can apply a configuration file or run a shell script without the Zyxel Device restarting. You can store multiple configuration files and shell script files on the Zyxel Device. You can edit configuration files or shell scripts in a text editor and upload them to the Zyxel Device. Configuration files use a .conf extension and shell scripts use a .zysh extension.

19.1.1 What You Can Do in this Chapter

- The **Configuration File** screen (Section 19.2 on page 207) stores and names configuration files. You can also download and upload configuration files.
- The **Firmware Package** screen (Section 19.3 on page 212) checks your current firmware version and uploads firmware to the Zyxel Device.
- The **Shell Script** screen (Section 19.4 on page 214) stores, names, downloads, uploads and runs shell script files.

19.1.2 What you Need to Know

The following terms and concepts may help as you read this chapter.

Configuration Files and Shell Scripts

When you apply a configuration file, the Zyxel Device uses the factory default settings for any features that the configuration file does not include. When you run a shell script, the Zyxel Device only applies the commands that it contains. Other settings do not change.

These files have the same syntax, which is also identical to the way you run CLI commands manually. An example is shown below.

Figure 127 Configuration File / Shell Script: Example

```
# enter configuration mode
configure terminal
# change administrator password
username admin password 4321 user-type admin
#configure default radio profile, change 2GHz channel to 11 & Tx output
power # to 50%
wlan-radio-profile default
2g-channel 11
output-power 50%
exit
write
```

While configuration files and shell scripts have the same syntax, the Zyxel Device applies configuration files differently than it runs shell scripts. This is explained below.

Table 91 Configuration Files and Shell Scripts in the Zyxel Device

Configuration Files (.conf)	Shell Scripts (.zysh)
• Resets to default configuration. • Goes into CLI **Configuration** mode. • Runs the commands in the configuration file.	• Goes into CLI **Privilege** mode. • Runs the commands in the shell script.

You have to run the aforementioned example as a shell script because the first command is run in **Privilege** mode. If you remove the first command, you have to run the example as a configuration file because the rest of the commands are executed in **Configuration** mode.

Comments in Configuration Files or Shell Scripts

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.

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

In the following example lines 1 and 2 are comments. Line 7 exits sub command mode.

```
! this is from Joe
# on 2010/12/05
wlan-ssid-profile default
ssid Joe-AP
qos wmm
security default
!
```

Errors in Configuration Files or Shell Scripts

When you apply a configuration file or run a shell script, the Zyxel Device processes the file line-by-line. The Zyxel Device checks the first line and applies the line if no errors are detected. Then it continues with the next line. If the Zyxel Device finds an error, it stops applying the configuration file or shell script and generates a log.

You can change the way a configuration file or shell script is applied. Include `setenv stop-on-error off` in the configuration file or shell script. The Zyxel Device ignores any errors in the configuration file or shell script and applies all of the valid commands. The Zyxel Device still generates a log for any errors.

19.2 Configuration File

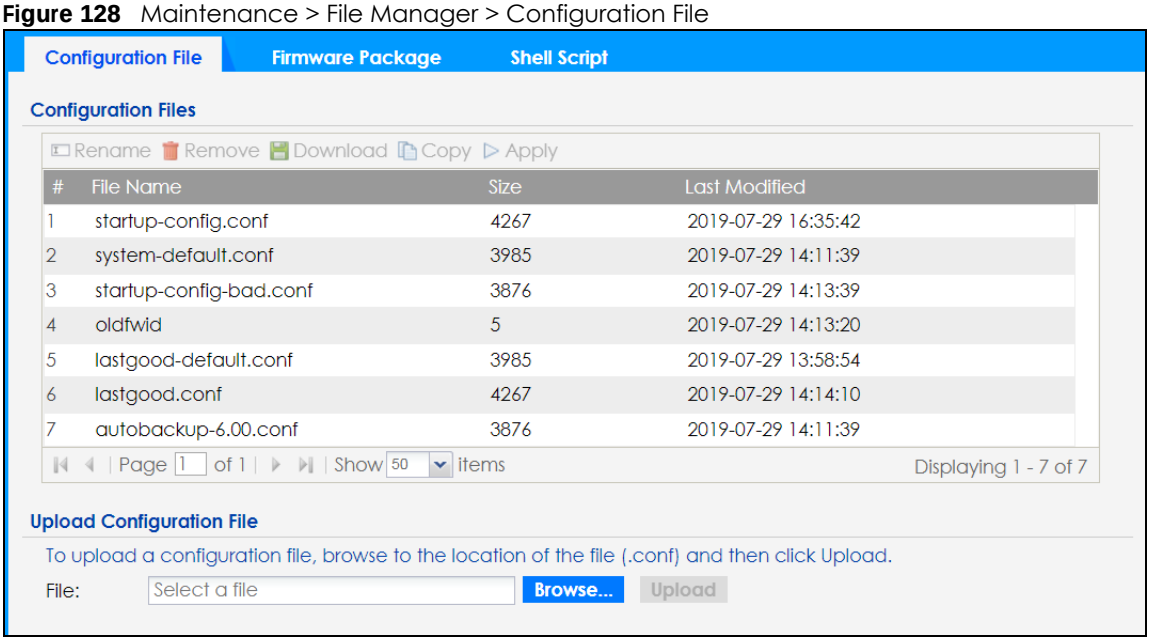
Click **Maintenance > File Manager > Configuration File** to open this screen. Use the **Configuration File** screen to store, run, and name configuration files. You can also download configuration files from the Zyxel Device to your computer and upload configuration files from your computer to the Zyxel Device.

Once your Zyxel Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making further configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Configuration File Flow at Restart

- If there is not a **startup-config.conf** when you restart the Zyxel Device (whether through a management interface or by physically turning the power off and back on), the Zyxel Device uses the **system-default.conf** configuration file with the Zyxel Device's default settings.
- If there is a **startup-config.conf**, the Zyxel Device checks it for errors and applies it. If there are no errors, the Zyxel Device uses it and copies it to the **lastgood.conf** configuration file as a back up file. If there is an error, the Zyxel Device generates a log and copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file. If there isn't a **lastgood.conf** configuration file or it also has an error, the Zyxel Device applies the **system-default.conf** configuration file.
- You can change the way the **startup-config.conf** file is applied. Include the `setenv-startup stop-on-error off` command. The Zyxel Device ignores any errors in the **startup-config.conf** file and applies all of the valid commands. The Zyxel Device still generates a log for any errors.

Figure 128 Maintenance > File Manager > Configuration File



Do not turn off the Zyxel Device while configuration file upload is in progress.

The following table describes the labels in this screen.

Table 92 Maintenance > File Manager > Configuration File

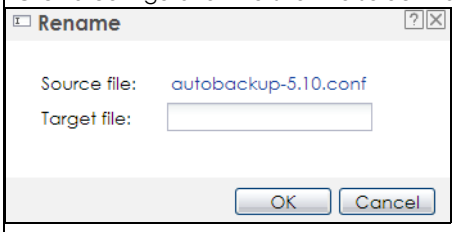
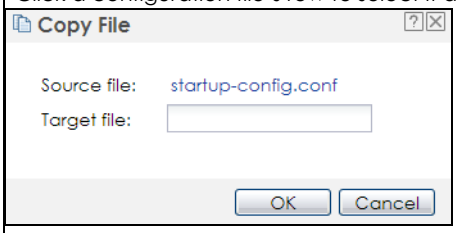
LABEL	DESCRIPTION
Rename	Use this button to change the label of a configuration file on the Zyxel Device. You can only rename manually saved configuration files. You cannot rename the **lastgood.conf**, **system-default.conf** and **startup-config.conf** files. You cannot rename a configuration file to the name of another configuration file in the Zyxel Device. Click a configuration file's row to select it and click **Rename** to open the **Rename File** screen.  Specify the new name for the configuration file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Remove	Click a configuration file's row to select it and click **Remove** to delete it from the Zyxel Device. You can only delete manually saved configuration files. You cannot delete the **system-default.conf**, **startup-config.conf** and **lastgood.conf** files. A pop-up window asks you to confirm that you want to delete the configuration file. Click **OK** to delete the configuration file or click **Cancel** to close the screen without deleting the configuration file.
Download	Click a configuration file's row to select it and click **Download** to save the configuration to your computer.
Copy	Use this button to save a duplicate of a configuration file on the Zyxel Device. Click a configuration file's row to select it and click **Copy** to open the **Copy File** screen.  Specify a name for the duplicate configuration file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.

Table 92 Maintenance > File Manager > Configuration File (continued)

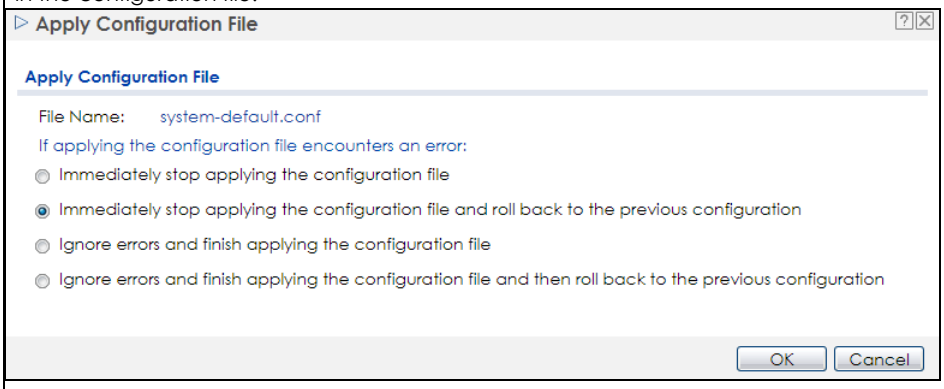
LABEL	DESCRIPTION
Apply	Use this button to have the Zyxel Device use a specific configuration file. Click a configuration file's row to select it and click **Apply** to have the Zyxel Device use that configuration file. The Zyxel Device does not have to restart in order to use a different configuration file, although you will need to wait for a few minutes while the system reconfigures. The following screen gives you options for what the Zyxel Device is to do if it encounters an error in the configuration file.  **Immediately stop applying the configuration file** - this is not recommended because it would leave the rest of the configuration blank. If the interfaces were not configured before the first error, the console port may be the only way to access the Zyxel Device. **Immediately stop applying the configuration file and roll back to the previous configuration** - this gets the Zyxel Device started with a fully valid configuration file as quickly as possible. **Ignore errors and finish applying the configuration file** - this applies the valid parts of the configuration file and generates error logs for all of the configuration file's errors. This lets the Zyxel Device apply most of your configuration and you can refer to the logs for what to fix. **Ignore errors and finish applying the configuration file and then roll back to the previous configuration** - this applies the valid parts of the configuration file, generates error logs for all of the configuration file's errors, and starts the Zyxel Device with a fully valid configuration file. Click **OK** to have the Zyxel Device start applying the configuration file or click **Cancel** to close the screen
#	This column displays the number for each configuration file entry. This field is a sequential value, and it is not associated with a specific address. The total number of configuration files that you can save depends on the sizes of the configuration files and the available flash storage space.
File Name	This column displays the label that identifies a configuration file. You cannot delete the following configuration files or change their file names. The **system-default.conf** file contains the Zyxel Device's default settings. Select this file and click **Apply** to reset all of the Zyxel Device settings to the factory defaults. This configuration file is included when you upload a firmware package. The **startup-config.conf** file is the configuration file that the Zyxel Device is currently using. If you make and save changes during your management session, the changes are applied to this configuration file. The Zyxel Device applies configuration changes made in the Web Configurator to the configuration file when you click **Apply** or **OK**. It applies configuration changes made via commands when you use the `write` command. The **lastgood.conf** is the most recently used (valid) configuration file that was saved when the Zyxel Device last restarted. If you upload and apply a configuration file with an error, you can apply lastgood.conf to return to a valid configuration.
Size	This column displays the size (in KB) of a configuration file.

Table 92 Maintenance > File Manager > Configuration File (continued)

LABEL	DESCRIPTION
Last Modified	This column displays the date and time that the individual configuration files were last changed or saved.
Upload Configuration File	The bottom part of the screen allows you to upload a new or previously saved configuration file from your computer to your Zyxel Device You cannot upload a configuration file named **system-default.conf** or **lastgood.conf**. If you upload **startup-config.conf**, it will replace the current configuration and immediately apply the new settings.
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .conf file you want to upload. The configuration file must use a ".conf" filename extension. You will receive an error message if you try to upload a fie of a different format. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

19.2.1 Example of Configuration File Download Using FTP

The following example gets a configuration file named startup-config.conf from the Zyxel Device and saves it on the computer.

1. Connect your computer to the Zyxel Device.
2. The FTP server IP address of the Zyxel Device in standalone mode is 192.168.1.2, so set your computer to use a static IP address from 192.168.1.3 ~192.168.1.254.
3. Use an FTP client on your computer to connect to the Zyxel Device. For example, in the Windows command prompt, type `ftp 192.168.1.2`. Keep the console session connected in order to see when the firmware recovery finishes.
4. Enter your user name when prompted.
5. Enter your password as requested.
6. Use "cd" to change to the directory that contains the files you want to download.
7. Use "dir" or "ls" if you need to display a list of the files in the directory.
8. Use "get" to download files. Transfer the configuration file on the Zyxel Device to your computer. Type `get` followed by the name of the configuration file. This examples uses `get startup-config.conf`.

```
C:\>ftp 192.168.1.2
Connected to 192.168.1.2.
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 5 allowed.
220-Local time is now 21:28. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 600 minutes of inactivity.
User (192.168.1.2:(none)): admin
331 User admin OK. Password required
Password:
230 OK. Current restricted directory is /
ftp> cd conf
250 OK. Current directory is /conf
ftp> ls
200 PORT command successful
150 Connecting to port 5001
lastgood.conf
startup-config.conf
system-default.conf
226 3 matches total
ftp: 57 bytes received in 0.33Seconds 0.17Kbytes/sec.
ftp> get startup-config.conf
200 PORT command successful
150 Connecting to port 5002
226-File successfully transferred
226 0.002 seconds (measured here), 1.66 Mbytes per second
ftp: 2928 bytes received in 0.02Seconds 183.00Kbytes/sec.
ftp>
```

9 Wait for the file transfer to complete.

10 Enter "quit" to exit the ftp prompt.

19.3 Firmware Package

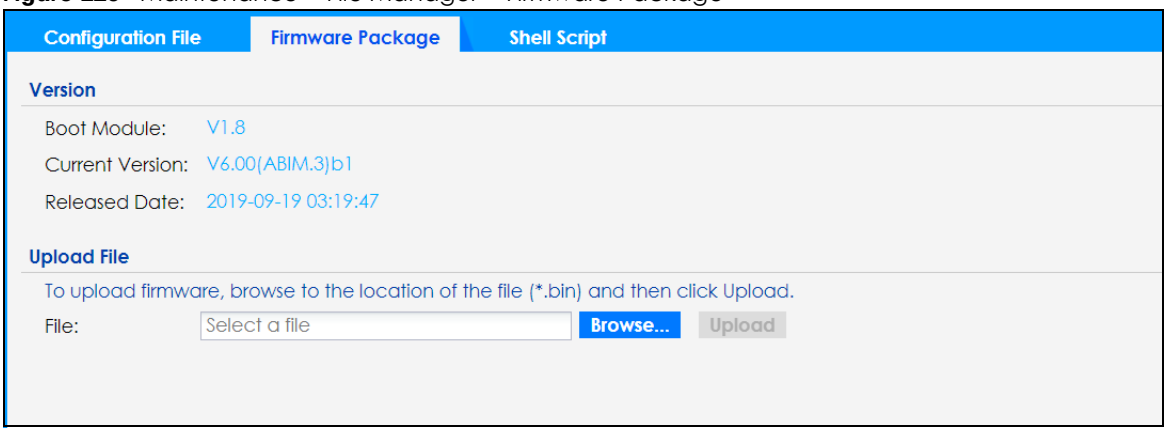
Click **Maintenance > File Manager > Firmware Package** to open this screen. Use the **Firmware Package** screen to check your current firmware version and upload firmware to the Zyxel Device.

Note: The Web Configurator is the recommended method for uploading firmware. You only need to use the command line interface 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.

Find the firmware package at www.zyxel.com in a file that (usually) uses a .bin extension.

The firmware update can take up to five minutes. Do not turn off or reset the Zyxel Device while the firmware update is in progress!

Figure 129 Maintenance > File Manager > Firmware Package



The following table describes the labels in this screen.

Table 93 Maintenance > File Manager > Firmware Package

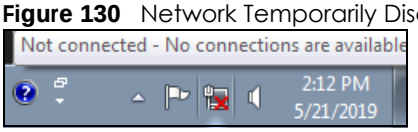
LABEL	DESCRIPTION
Boot Module	This is the version of the boot module that is currently on the Zyxel Device.
Current Version	This is the firmware version and the date created.
Released Date	This is the date that the version of the firmware was created.
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the Zyxel Device again.

Note: The Zyxel Device automatically reboots after a successful upload.

The Zyxel Device automatically restarts causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 130 Network Temporarily Disconnected



After five minutes, log in again and check your new firmware version in the **Dashboard** screen.

19.3.1 Example of Firmware Upload Using FTP

This procedure requires the Zyxel Device's firmware. Download the firmware package from www.zyxel.com and unzip it. The firmware file uses a .bin extension, for example, "600ABFH0C0.bin". Do the following after you have obtained the firmware file.

1 Connect your computer to the Zyxel Device.

2 The FTP server IP address of the Zyxel Device in standalone mode is 192.168.1.2, so set your computer to use a static IP address from 192.168.1.3 ~192.168.1.254.

3 Use an FTP client on your computer to connect to the Zyxel Device. For example, in the Windows command prompt, type `ftp 192.168.1.2`. Keep the console session connected in order to see when the firmware recovery finishes.

4 Enter your user name when prompted.

5 Enter your password as requested.

6 Enter "hash" for FTP to print a `#' character for every 1024 bytes of data you upload so that you can watch the file transfer progress.

7 Enter "bin" to set the transfer mode to binary.

8 Transfer the firmware file from your computer to the Zyxel Device. Type `put` followed by the path and name of the firmware file. This examples uses `put C:\ftproot\Zyxel Device_FW\600ABFH0C0.bin`.

```
C:\>ftp 192.168.1.2
Connected to 192.168.1.2.
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 5 allowed.
220-Local time is now 21:28. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 600 minutes of inactivity.
User (192.168.1.2:(none)): admin
331 User admin OK. Password required
Password:
230 OK. Current restricted directory is /
ftp> hash
Hash mark printing On  ftp: (2048 bytes/hash mark) .
ftp> bin
200 TYPE is now 8-bit binary
ftp> put C:\ftproot\Zyxel Device_FW\600ABFH0C0.bin
```

9 Wait for the file transfer to complete.

10 Enter "quit" to exit the ftp prompt.

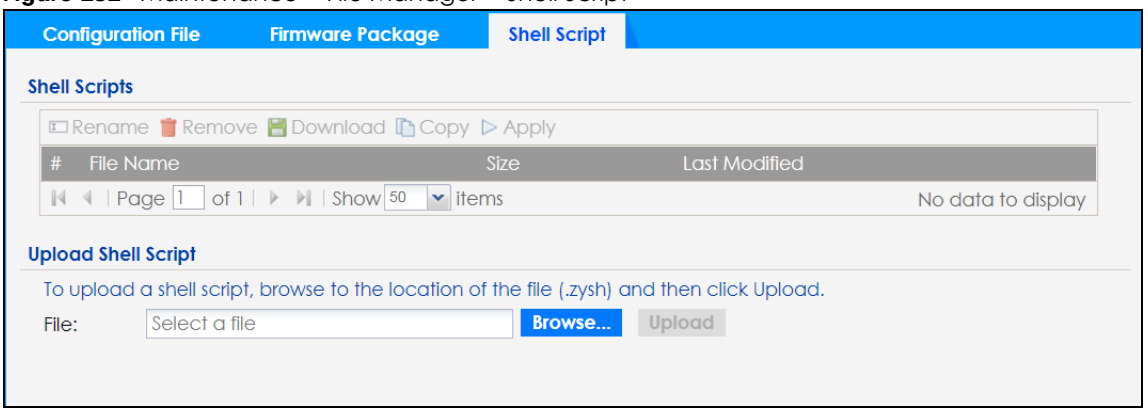
19.4 Shell Script

Use shell script files to have the Zyxel Device use commands that you specify. Use a text editor to create the shell script files. They must use a ".zysh" filename extension.

Click **Maintenance > File Manager > Shell Script** to open this screen. Use the **Shell Script** screen to store, name, download, upload and run shell script files. You can store multiple shell script files on the Zyxel Device at the same time.

Note: You should include `write` commands in your scripts. If you do not use the `write` command, the changes will be lost when the Zyxel Device restarts. You could use multiple `write` commands in a long script.

Figure 131 Maintenance > File Manager > Shell Script



Each field is described in the following table.

Table 94 Maintenance > File Manager > Shell Script

LABEL	DESCRIPTION
Rename	Use this button to change the label of a shell script file on the Zyxel Device. You cannot rename a shell script to the name of another shell script in the Zyxel Device. Click a shell script's row to select it and click **Rename** to open the **Rename File** screen. Specify the new name for the shell script file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Remove	Click a shell script file's row to select it and click **Delete** to delete the shell script file from the Zyxel Device. A pop-up window asks you to confirm that you want to delete the shell script file. Click **OK** to delete the shell script file or click **Cancel** to close the screen without deleting the shell script file.
Download	Click a shell script file's row to select it and click **Download** to save the configuration to your computer.
Copy	Use this button to save a duplicate of a shell script file on the Zyxel Device. Click a shell script file's row to select it and click **Copy** to open the **Copy File** screen. Specify a name for the duplicate file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Apply	Use this button to have the Zyxel Device use a specific shell script file. Click a shell script file's row to select it and click **Apply** to have the Zyxel Device use that shell script file. You may need to wait awhile for the Zyxel Device to finish applying the commands.
#	This column displays the number for each shell script file entry.
File Name	This column displays the label that identifies a shell script file.
Size	This column displays the size (in KB) of a shell script file.
Last Modified	This column displays the date and time that the individual shell script files were last changed or saved.
Upload Shell Script	The bottom part of the screen allows you to upload a new or previously saved shell script file from your computer to your Zyxel Device.
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.

Table 94 Maintenance > File Manager > Shell Script (continued)

LABEL	DESCRIPTION
Browse...	Click **Browse...** to find the .zysh file you want to upload.
Upload	Click **Upload** to begin the upload process. This process may take up to several minutes.

CHAPTER 20
Diagnostics

20.1 Overview

Use the diagnostics screen for troubleshooting.

20.1.1 What You Can Do in this Chapter

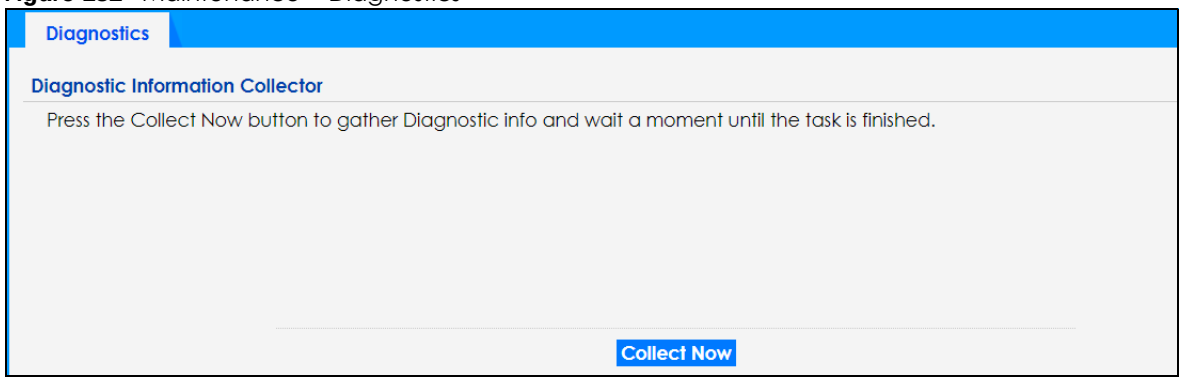
The **Diagnostics** screen (Section 20.2 on page 217) generates a file containing the Zyxel Device's configuration and diagnostic information if you need to provide it to customer support during troubleshooting.

20.2 Diagnostics

This screen provides an easy way for you to generate a file containing the Zyxel Device's configuration and diagnostic information. You may need to generate this file and send it to customer support during troubleshooting. All categories of settings and shell script files stored on the Zyxel Device will be included in the diagnostic file.

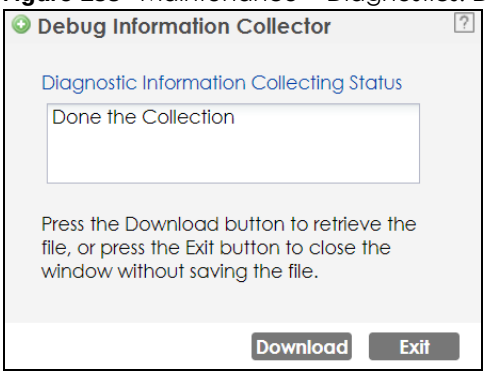
Click **Maintenance > Diagnostics** to open the **Diagnostics** screen. Click **Collect Now** to have the Zyxel Device create a new diagnostic file.

Figure 132 Maintenance > Diagnostics



The **Debug Information Center** screen then displays showing whether the collection is in progress, was successful, or has failed. When the data collection is done, click **Download** to save the most recent diagnostic file to a computer.

Figure 133 Maintenance > Diagnostics: Debug Information Collector



CHAPTER 21
LEDs

21.1 Overview

The LEDs of your Zyxel Device can be controlled such that they stay lit (ON) or OFF after the Zyxel Device is ready. There are two features that control the LEDs of your Zyxel Device - **Locator** and **Suppression** (see Section 1.4 on page 19).

21.1.1 What You Can Do in this Chapter

- The **Suppression** screen (Section 21.2 on page 219) allows you to set how you want the LEDs to behave after the Zyxel Device is ready.
- The **Locator** screen (Section 21.3 on page 220) allows users to see the actual location of the Zyxel Device between several devices in the network.

21.2 Suppression Screen

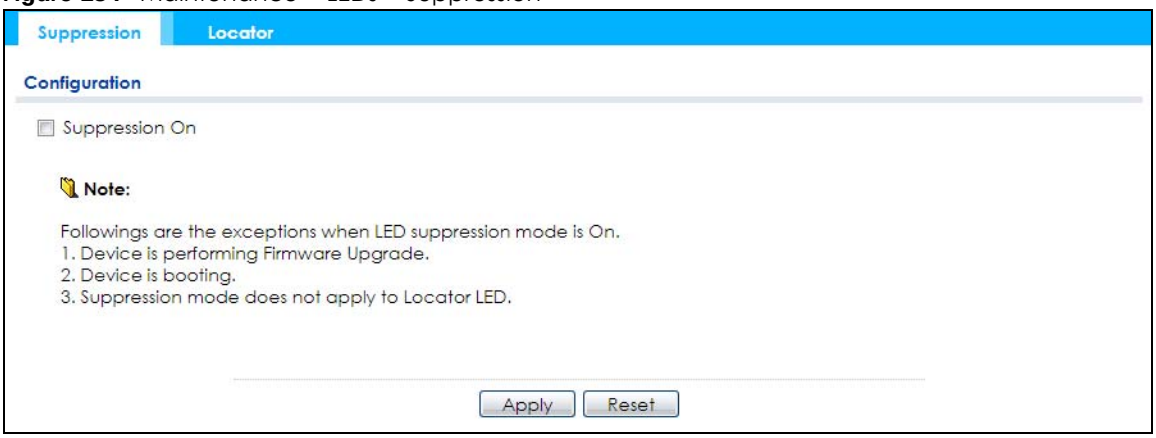
The LED Suppression feature allows you to control how the LEDs of your Zyxel Device behave after it's ready. The default LED suppression setting of your AP is different depending on your Zyxel Device model.

You can go to the **Maintenance** > **LEDs** > **Suppression** screen to see the default LED behavior and change the LED suppression setting. After you make changes in the suppression screen, it will be stored as the default when the Zyxel Device is restarted. See (Section 3.2 on page 34) for information on default values for different models.

Note: When the Zyxel Device is booting or performing firmware upgrade, the LEDs will light up regardless of the setting in LED suppression.

To access this screen, click **Maintenance** > **LEDs** > **Suppression**.

Figure 134 Maintenance > LEDs > Suppression



The following table describes fields in the above screen.

Table 95 Maintenance > LED > Suppression

LABEL	DESCRIPTION
Suppression On	If the **Suppression On** check box is checked, the LEDs of your Zyxel Device will turn off after it's ready. If the check box is unchecked, the LEDs will stay lit after the Zyxel Device is ready.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

21.3 Locator Screen

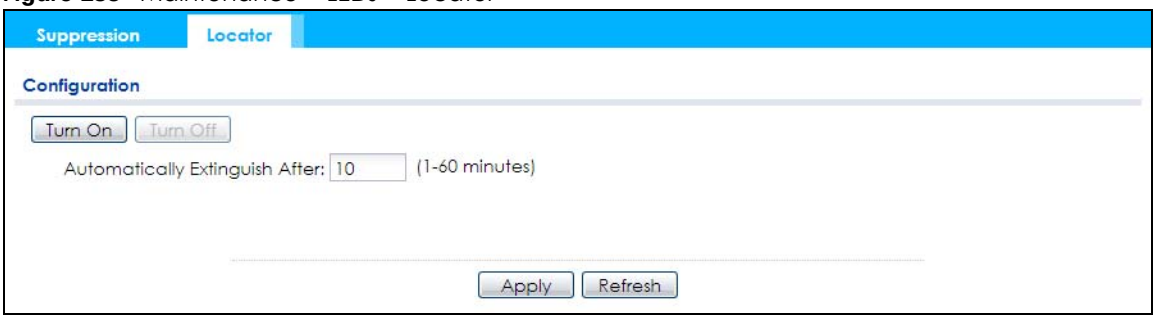
The Locator feature identifies the location of your Zyxel Device among several devices in the network. You can run this feature and set a timer in this screen.

To run the locator feature, enter a number of minutes and click **Turn On** button to have the Zyxel Device find its location. The Locator LED will start to blink for the number of minutes set in the **Locator** screen. The default setting is 10 minutes. While the locator is running, the turn on button will gray out and return after it's finished. If you make changes to the time default setting, it will be stored as the default when the Zyxel Device restarts.

Note: The Locator feature is not affected by the Suppression setting.

To access this screen, click **Maintenance** > **LEDs** > **Locator**.

Figure 135 Maintenance > LEDs > Locator



The following table describes fields in the above screen.

Table 96 Maintenance > LED > Locator

LABEL	DESCRIPTION
Turn On Turn Off	Click **Turn On** button to activate the locator. The Locator function will show the actual location of the Zyxel Device between several devices in the network. Otherwise, click **Turn Off** to disable the locator feature.
Automatically Extinguish After	Enter a time interval between 1 and 60 minutes to stop the locator LED from blinking. Default is 10 minutes.
Apply	Click **Apply** to save changes in this screen.
Refresh	Click **Refresh** to update the information in this screen.

CHAPTER 22
Antenna Switch

22.1 Overview

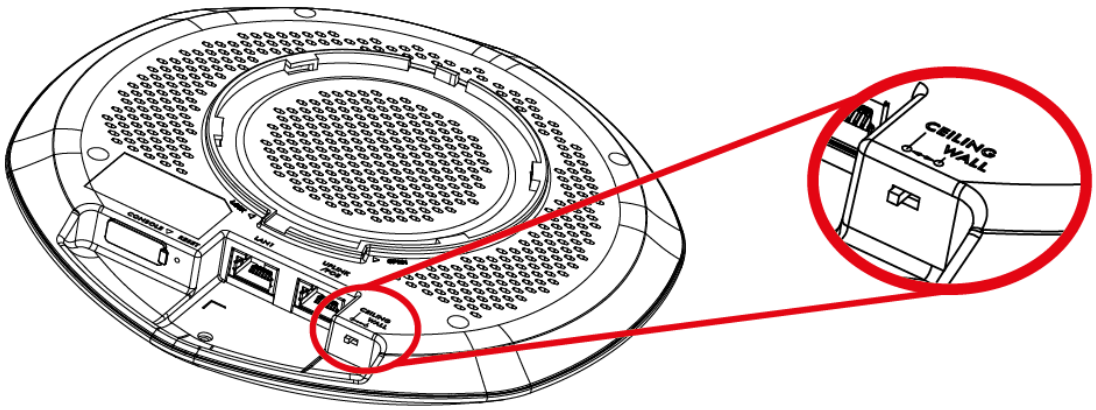
Use this screen to adjust coverage depending on the orientation of the antenna.

22.1.1 What You Need To Know

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

On the Zyxel Device that comes with internal antennas and also has an antenna switch, you can adjust coverage depending on the antenna orientation for the Zyxel Device radios using the web configurator, the command line interface (CLI) or a physical switch. Check Section 1.4 on page 19 to see if your Zyxel Device has an antenna switch.

Figure 136 WAC Physical Antenna Switch



Note: With the physical antenna switch, you apply the same antenna orientation settings to both radios. You can set the radios to have different settings while using the web configurator or the command line interface.

Note: The antenna switch in the web configurator has priority over the physical antenna switch after you **Enable Software Control** in the **Maintenance > Antenna** screen. By default, software control is disabled.

22.2 Antenna Switch Screen

To access this screen, click **Maintenance** > **Antenna**.

The screen varies depending on whether the Zyxel Device has a physical antenna switch or allows you to change antenna orientation settings on a per-radio basis or on a per-AP basis.

Figure 137 Maintenance > Antenna > Antenna Switch (Per Radio)

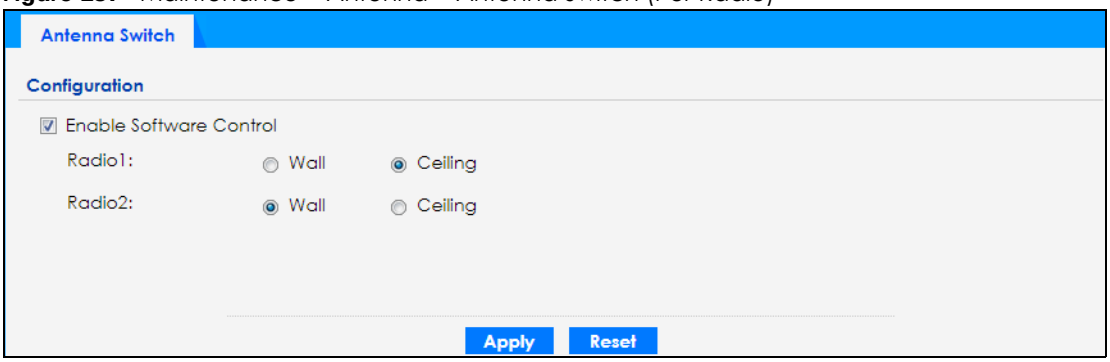
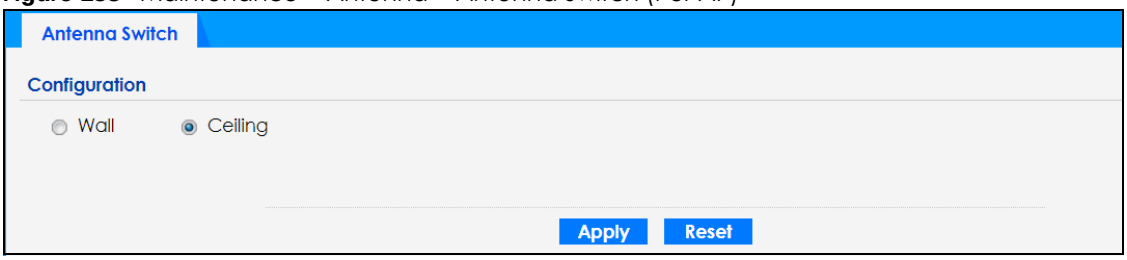


Figure 138 Maintenance > Antenna > Antenna Switch (Per AP)



If the Zyxel Device has a physical antenna switch, select the **Enable Software Control** option to use the Web configurator to adjust coverage depending on each radio's antenna orientation for better coverage.

Select **Wall** if you mount the Zyxel Device to a wall. Select **Ceiling** if the Zyxel Device is mounted on a ceiling. You can switch from **Wall** to **Ceiling** if there are still wireless dead zones, and vice versa.

Click **Apply** to save your changes or click **Reset** to return the screen to its last-saved settings.

CHAPTER 23
Reboot

23.1 Overview

Use this screen to restart the Zyxel Device.

23.1.1 What You Need To Know

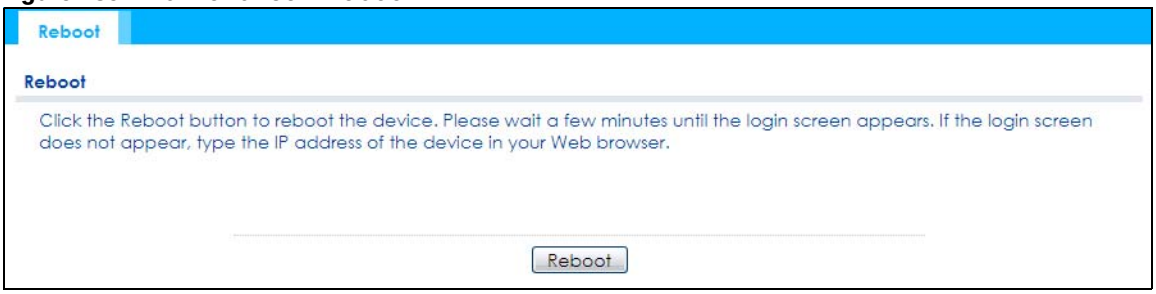
If you applied changes in the Web configurator, these were saved automatically and do not change when you reboot. If you made changes in the CLI, however, you have to use the `write` command to save the configuration before you reboot. Otherwise, the changes are lost when you reboot.

Reboot is different to reset; reset returns the Zyxel Device to its default configuration.

23.2 Reboot

This screen allows remote users can restart the Zyxel Device. To access this screen, click **Maintenance** > **Reboot**.

Figure 139 Maintenance > Reboot



Click the **Reboot** button to restart the Zyxel Device. Wait a few minutes until the login screen appears. If the login screen does not appear, type the IP address of the Zyxel Device in your Web browser.

You can also use the CLI command `reboot` to restart the Zyxel Device.

CHAPTER 24
Shutdown

24.1 Overview

Use this screen to shut down the Zyxel Device.

Always use Maintenance > Shutdown > Shutdown or the `shutdown` command before you turn off the Zyxel Device or remove the power. Not doing so can cause the firmware to become corrupt.

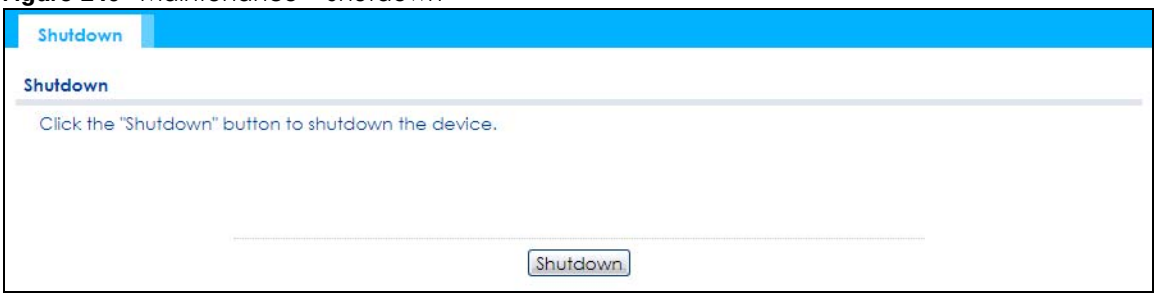
24.1.1 What You Need To Know

Shutdown writes all cached data to the local storage and stops the system processes. Shutdown is different to reset; reset returns the Zyxel Device to its default configuration.

24.2 Shutdown

To access this screen, click **Maintenance** > **Shutdown**.

Figure 140 Maintenance > Shutdown



Click the **Shutdown** button to shut down the Zyxel Device. Wait for the Zyxel Device to shut down before you manually turn off or remove the power. It does not turn off the power.

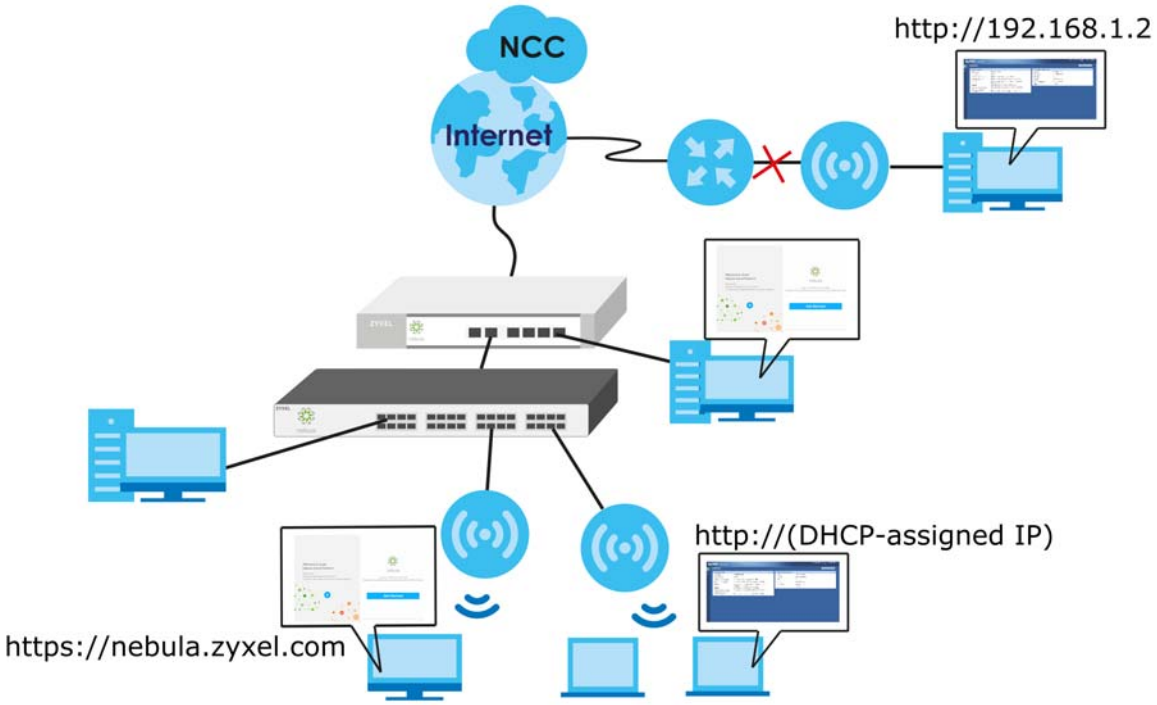
You can also use the CLI command `shutdown` to shut down the Zyxel Device.

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 53). You can check the NCC's **Access Point > Monitor > Access Points** 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**
- **Maintenance > Shell Script**
- **Maintenance > Diagnostics**

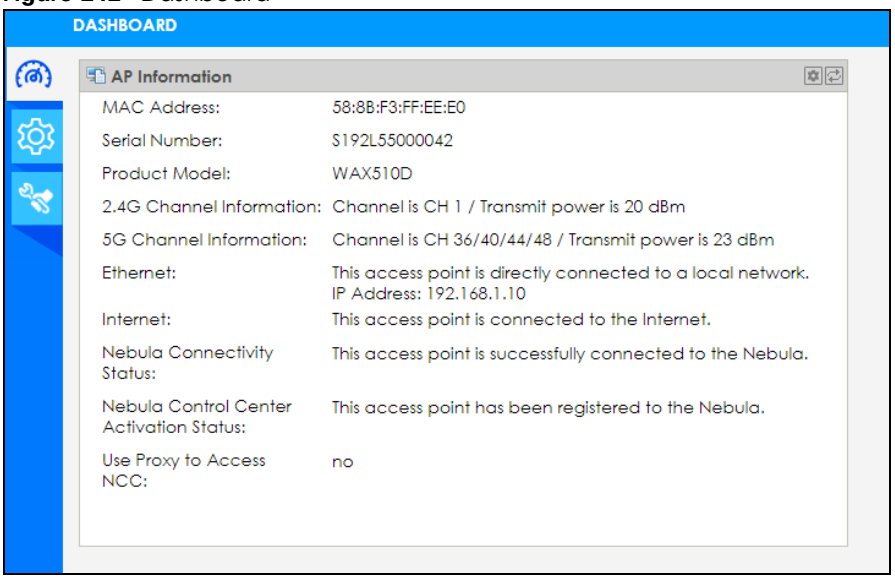
- **Maintenance > Log**

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



The following table describes the labels in this screen.

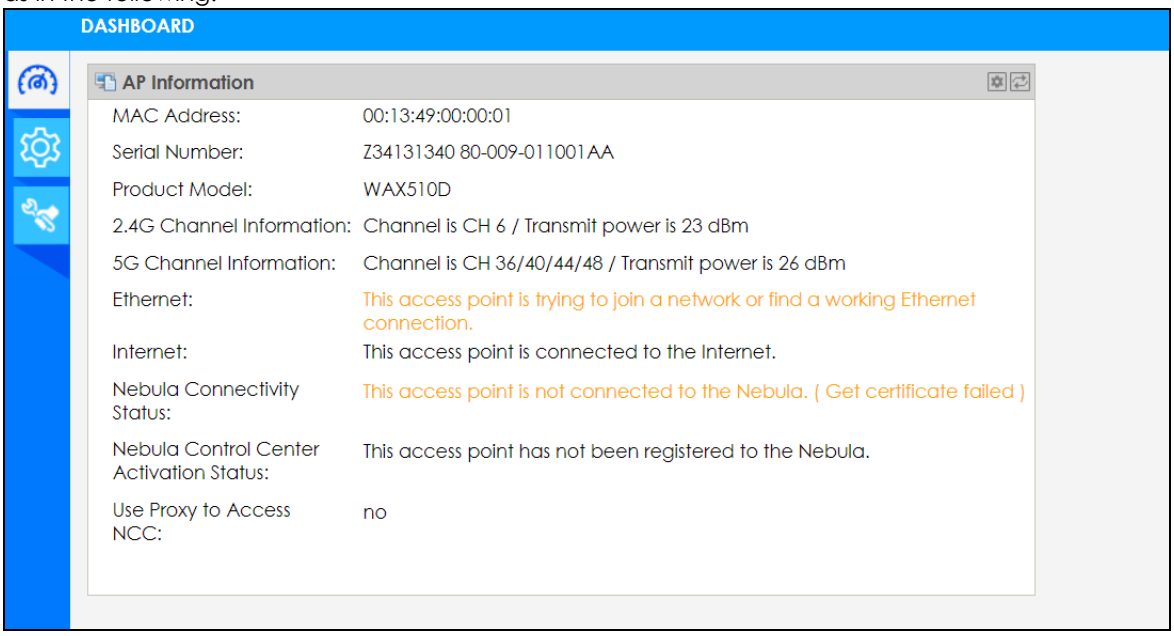
Table 97 Dashboard

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 97 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 NCC	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.



CHAPTER 27
Network

27.1 Overview

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

See Section 9.1 on page 94 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.

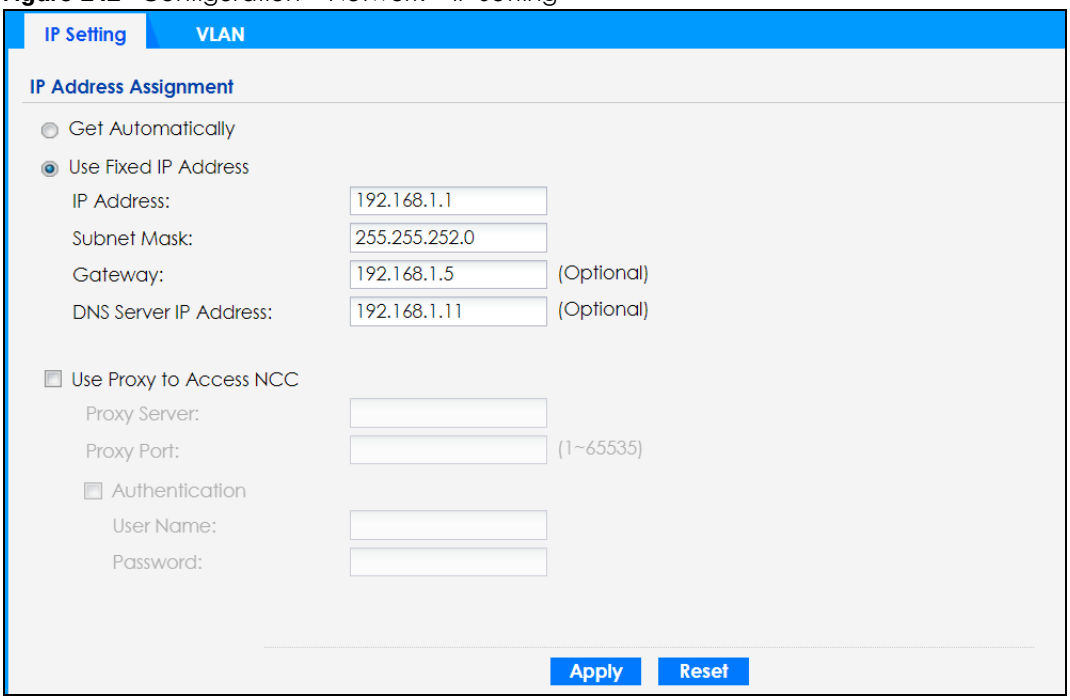
27.1.1 What You Can Do in this Chapter

- The **IP Setting** screen (Section 27.2 on page 231) configures the Zyxel Device's LAN IP address.
- The **VLAN** screen (Section 27.3 on page 233) 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



Each field is described in the following table.

Table 98 Configuration > Network > IP Setting

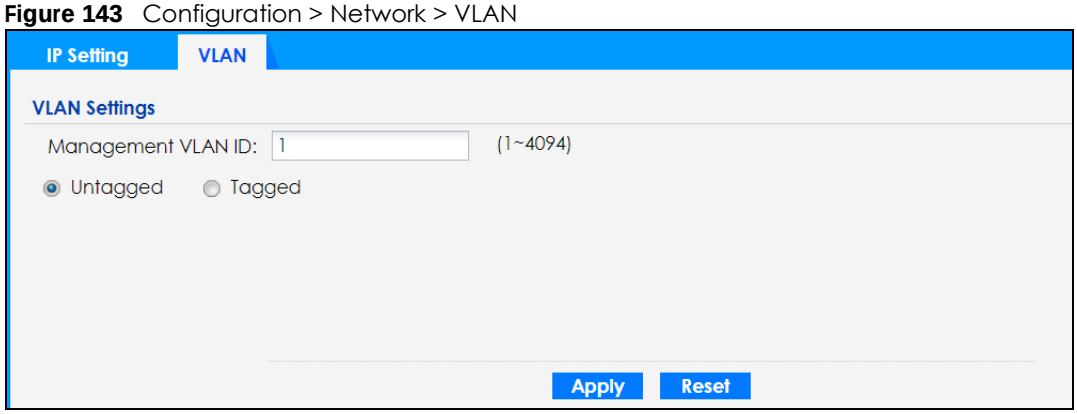
LABEL	DESCRIPTION
IP Address Assignment	
Get Automatically	Select this to make the interface a DHCP client and automatically get the IP address, subnet mask, and gateway address from a DHCP server.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
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.
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 98 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



Each field is described in the following table.

Table 99 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.

CHAPTER 28
Maintenance

28.1 Overview

When the Zyxel Device is set to work in cloud mode, the **Maintenance** screens let you mange shell script files on the Zyxel Device, generate a diagnostic file, or view log messages.

See Chapter 19 on page 206 for information about shell scripts.

28.1.1 What You Can Do in this Chapter

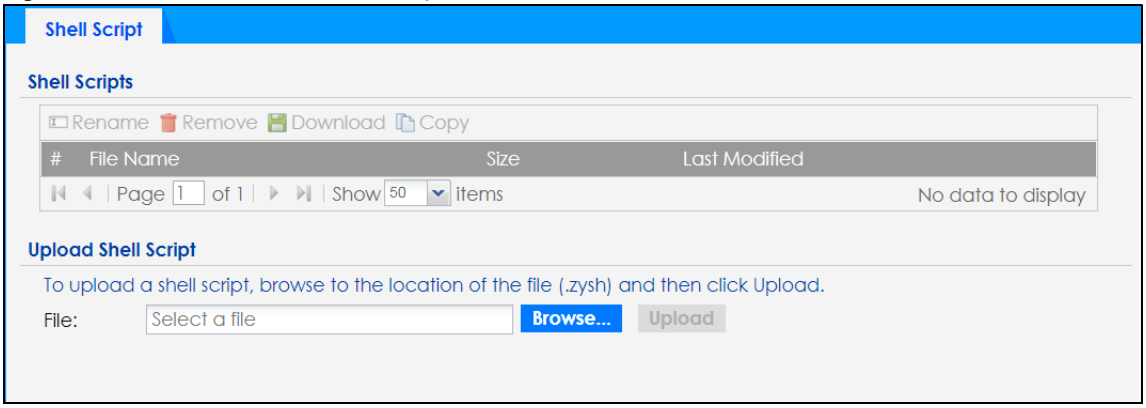
- The **Shell Script** screen (Section 28.2 on page 234) stores, names, downloads, and uploads shell script files.
- The **Diagnostics** screen (Section 28.3 on page 235) generates a file containing the Zyxel Device's configuration and diagnostic information if you need to provide it to customer support during troubleshooting.
- The **Log > View Log** screen (Section 28.4 on page 236) displays the Zyxel Device's current log messages when it is disconnected from the NCC.

28.2 Shell Script

Use shell script files to have the Zyxel Device use commands that you specify. Use a text editor to create the shell script files. They must use a ".zysh" filename extension.

Click **Maintenance > Shell Script** to open this screen. Use the **Shell Script** screen to store, name, download, and upload shell script files. You can store multiple shell script files on the Zyxel Device at the same time.

Figure 144 Maintenance > Shell Script



Each field is described in the following table.

Table 100 Maintenance > Shell Script

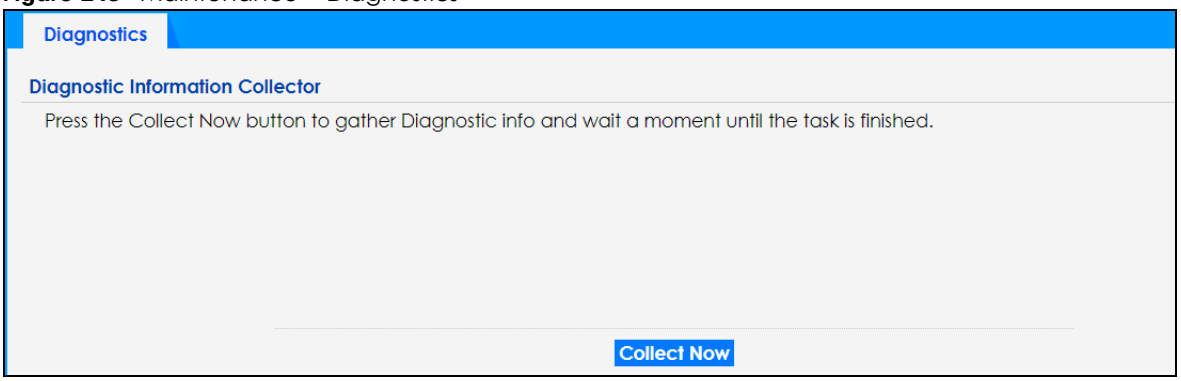
LABEL	DESCRIPTION
Rename	Use this button to change the label of a shell script file on the Zyxel Device. You cannot rename a shell script to the name of another shell script in the Zyxel Device. Click a shell script's row to select it and click **Rename** to open the **Rename File** screen. Specify the new name for the shell script file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
Remove	Click a shell script file's row to select it and click **Delete** to delete the shell script file from the Zyxel Device. A pop-up window asks you to confirm that you want to delete the shell script file. Click **OK** to delete the shell script file or click **Cancel** to close the screen without deleting the shell script file.
Download	Click a shell script file's row to select it and click **Download** to save the configuration to your computer.
Copy	Use this button to save a duplicate of a shell script file on the Zyxel Device. Click a shell script file's row to select it and click **Copy** to open the **Copy File** screen. Specify a name for the duplicate file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-). Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file.
#	This column displays the number for each shell script file entry.
File Name	This column displays the label that identifies a shell script file.
Size	This column displays the size (in KB) of a shell script file.
Last Modified	This column displays the date and time that the individual shell script files were last changed or saved.
Upload Shell Script	The bottom part of the screen allows you to upload a new or previously saved shell script file from your computer to your Zyxel Device.
File	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .zysh file you want to upload.
Upload	Click **Upload** to begin the upload process. This process may take up to several minutes.

28.3 Diagnostics

This screen provides an easy way for you to generate a file containing the Zyxel Device's configuration and diagnostic information. You may need to generate this file and send it to customer support during troubleshooting. All categories of settings and shell script files stored on the Zyxel Device will be included in the diagnostic file.

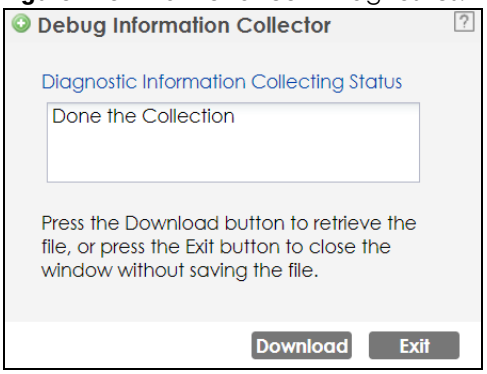
Click **Maintenance > Diagnostics** to open the **Diagnostics** screen. Click **Collect Now** to have the Zyxel Device create a new diagnostic file.

Figure 145 Maintenance > Diagnostics



The **Debug Information Center** screen then displays showing whether the collection is in progress, was successful, or has failed. When the data collection is done, click **Download** to save the most recent diagnostic file to a computer.

Figure 146 Maintenance > Diagnostics: Debug Information Collector



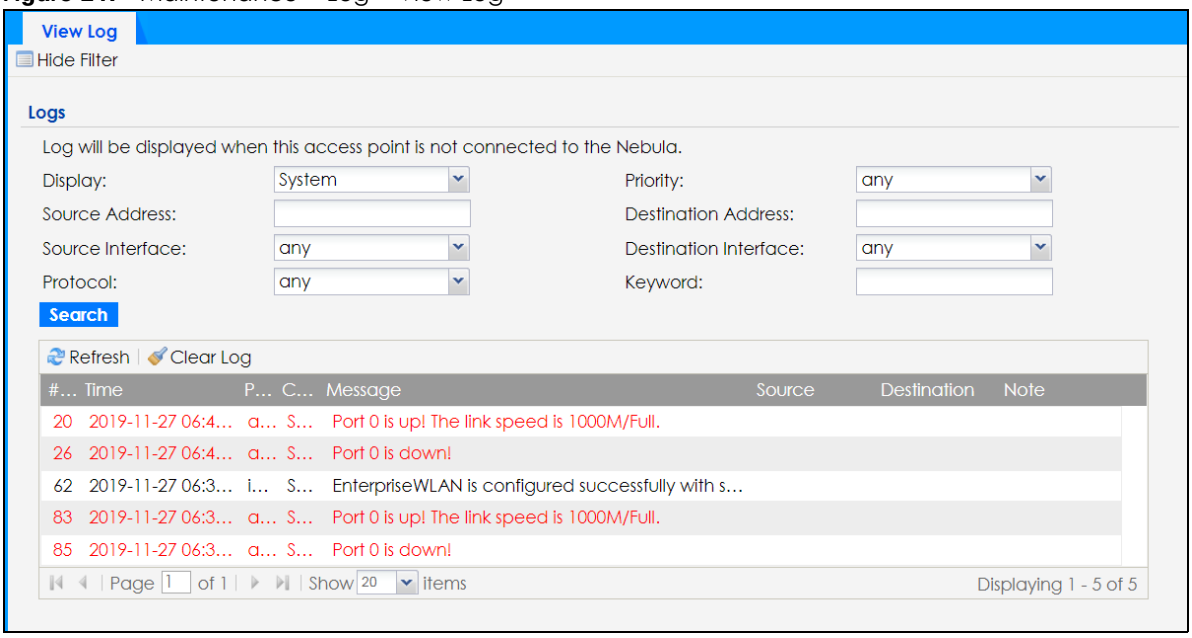
28.4 View Log

The NCC periodically gathers log files from the devices being managed by it. Before the NCC pulls logs from the Zyxel Device or when the Zyxel Device is disconnected from the NCC, you can use this screen to view its current log messages. To access this screen, click **Maintenance > Log**.

Note: When a log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

Events that generate an alert (as well as a log message) display in red. Regular logs display in black. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 147 Maintenance > Log > View Log



The following table describes the labels in this screen.

Table 101 Maintenance > Log > View Log

LABEL	DESCRIPTION
Show Filter / Hide Filter	Click this button to show or hide the filter settings. If the filter settings are hidden, the **Display**, **Email Log Now**, **Refresh**, and **Clear Log** fields are available. If the filter settings are shown, the **Display**, **Priority**, **Source Address**, **Destination Address**, **Source Interface**, **Destination Interface**, **Protocol**, **Keyword**, and **Search** fields are available.
Display	Select the category of log message(s) you want to view. You can also view **All Logs** at one time, or you can view the **Debug Log**.
Priority	This displays when you show the filter. Select the priority of log messages to display. The log displays the log messages with this priority or higher. Choices are: **any**, **emerg**, **alert**, **crit**, **error**, **warn**, **notice**, and **info**, from highest priority to lowest priority. This field is read-only if the **Category** is **Debug Log**.
Source Address	This displays when you show the filter. Type the source IP address of the incoming packet that generated the log message. Do not include the port in this filter.
Destination Address	This displays when you show the filter. Type the IP address of the destination of the incoming packet when the log message was generated. Do not include the port in this filter.
Source Interface	This displays when you show the filter. Select the source interface of the packet that generated the log message.
Destination Interface	This displays when you show the filter. Select the destination interface of the packet that generated the log message.
Protocol	This displays when you show the filter. Select a service protocol whose log messages you would like to see.
Keyword	This displays when you show the filter. Type a keyword to look for in the **Message**, **Source**, **Destination** and **Note** fields. If a match is found in any field, the log message is displayed. You can use up to 63 alphanumeric characters and the underscore, as well as punctuation marks ()' ,:;?! +-*/= #$% @ ; the period, double quotes, and brackets are not allowed.
Search	This displays when you show the filter. Click this button to update the log using the current filter settings.

Table 101 Maintenance > Log > View Log (continued)

LABEL	DESCRIPTION
Refresh	Click this to update the list of logs.
Clear Log	Click this button to clear the whole log, regardless of what is currently displayed on the screen.
#	This field is a sequential value, and it is not associated with a specific log message.
Time	This field displays the time the log message was recorded.
Priority	This field displays the priority of the log message. It has the same range of values as the **Priority** field above.
Category	This field displays the log that generated the log message. It is the same value used in the **Display** and (other) **Category** fields.
Message	This field displays the reason the log message was generated. The text "[count=*x*]", where *x* is a number, appears at the end of the **Message** field if log consolidation is turned on and multiple entries were aggregated to generate into this one.
Source	This field displays the source IP address and the port number in the event that generated the log message.
Source Interface	This field displays the source interface of the packet that generated the log message.
Destination	This field displays the destination IP address and the port number of the event that generated the log message.
Destination Interface	This field displays the destination interface of the packet that generated the log message.
Protocol	This field displays the service protocol in the event that generated the log message.
Note	This field displays any additional information about the log message.

PART III
Appendices and Troubleshooting

CHAPTER 29
Troubleshooting

29.1 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

29.2 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.

29.3 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 29.6 on page 247.

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 29.6 on page 247.

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 29.6 on page 247.

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 29.6 on page 247.

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 103).
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 98). 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 96.

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.

29.4 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 29.2 on page 240.
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.

29.5 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.

29.6 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.

29.7 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.

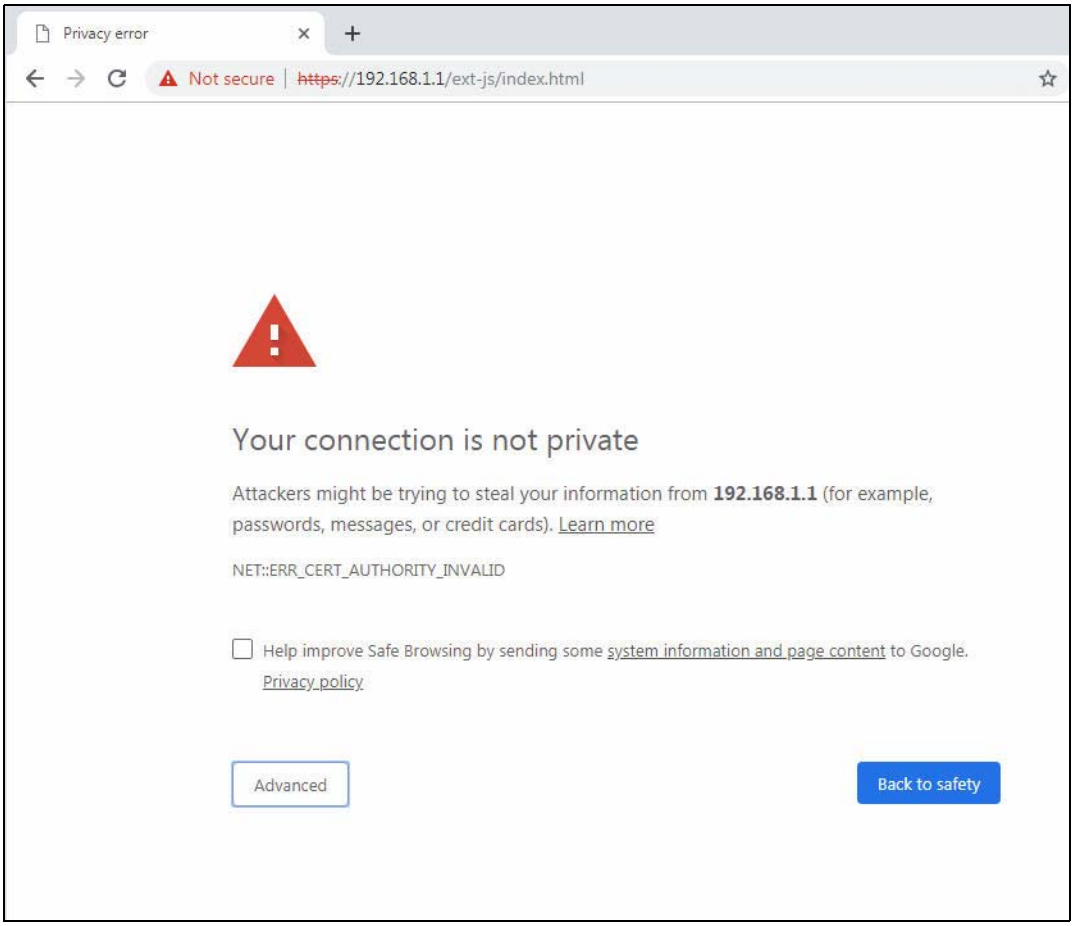
Note: You can see if you are browsing on a secure website if the URL in your web browser's address bar begins with `https://` or there is a sealed padlock icon ( ) somewhere in the main browser window (not all browsers show the padlock in the same location).

Google Chrome

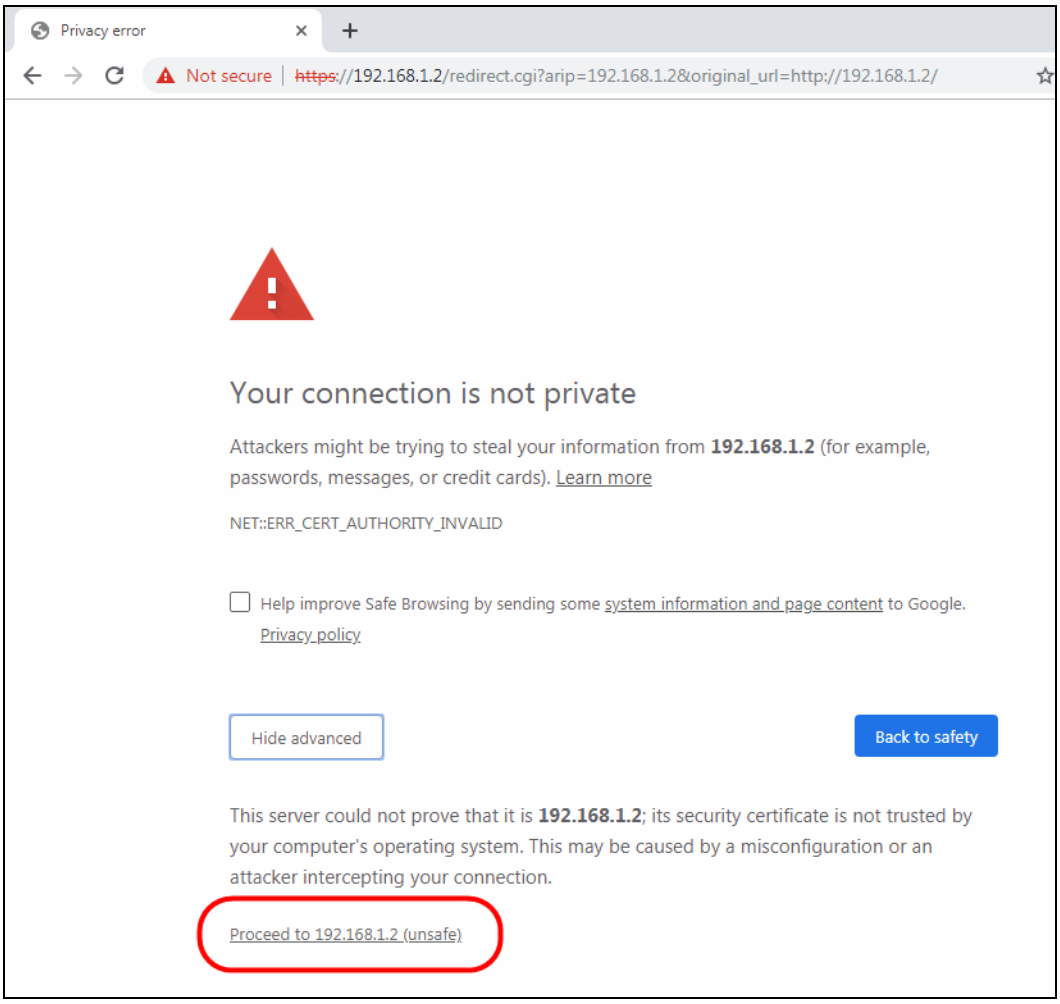
The following example uses Google Chrome on Windows 7. You first have to store the certificate in your computer and then install it as a Trusted Root CA, as shown in the following tutorials.

Export a Certificate

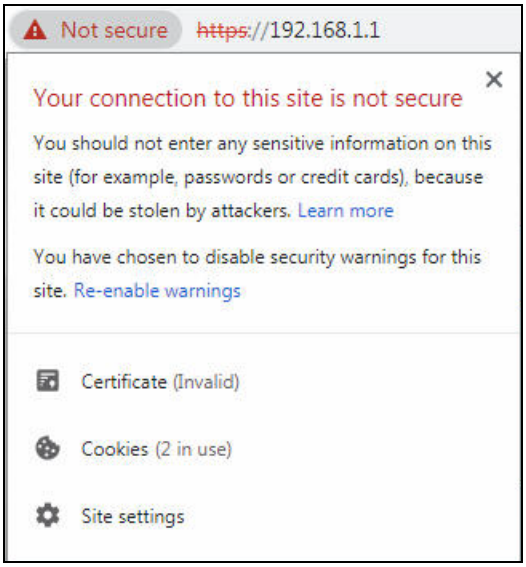
1 If your device's Web Configurator is set to use SSL certification, then upon browsing with it for the first time, you are presented with a certification error.



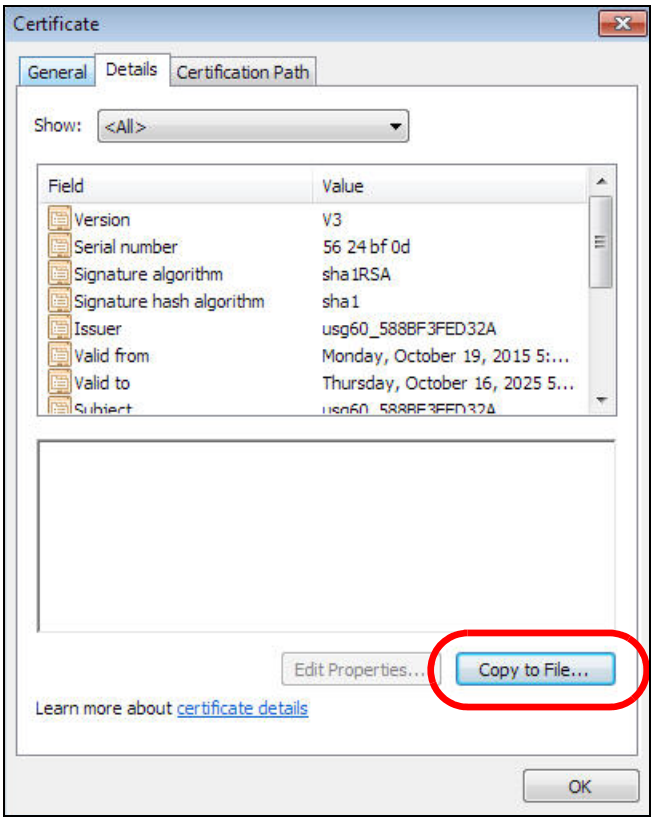
2 Click **Advanced > Proceed to *x.x.x.x* (unsafe)**.



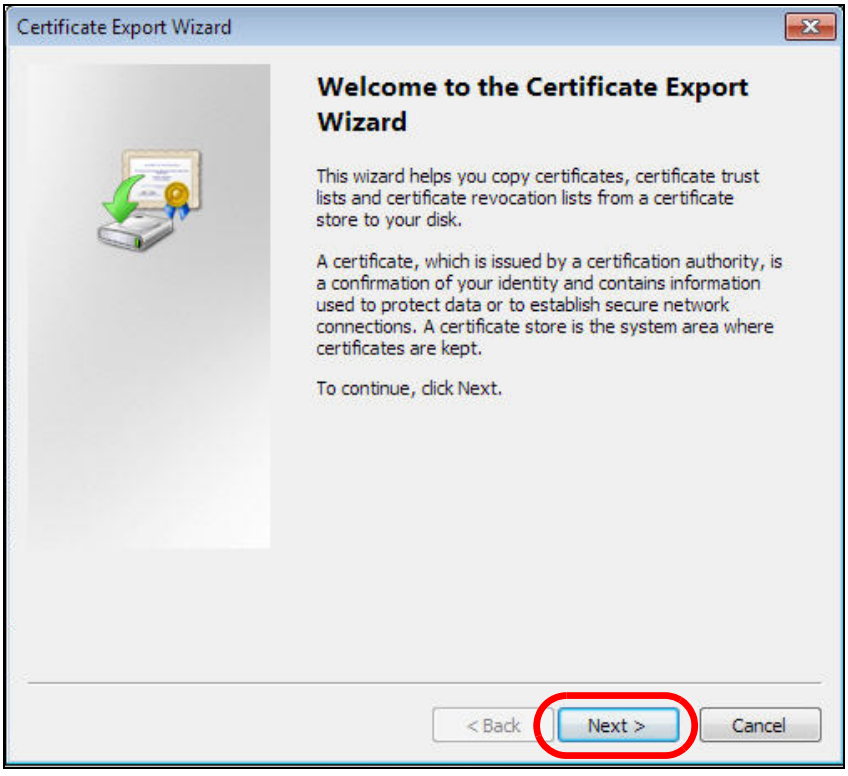
3 In the **Address Bar**, click **Not Secure** > **Certificate (Invalid)**.



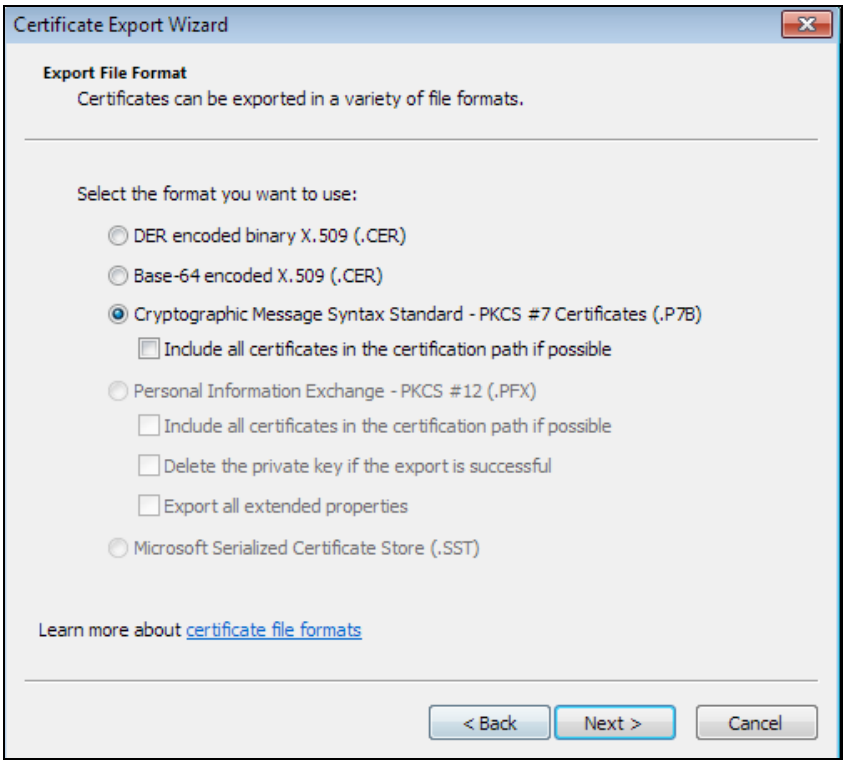
4 In the **Certificate** dialog box, click **Details > Copy to File**.



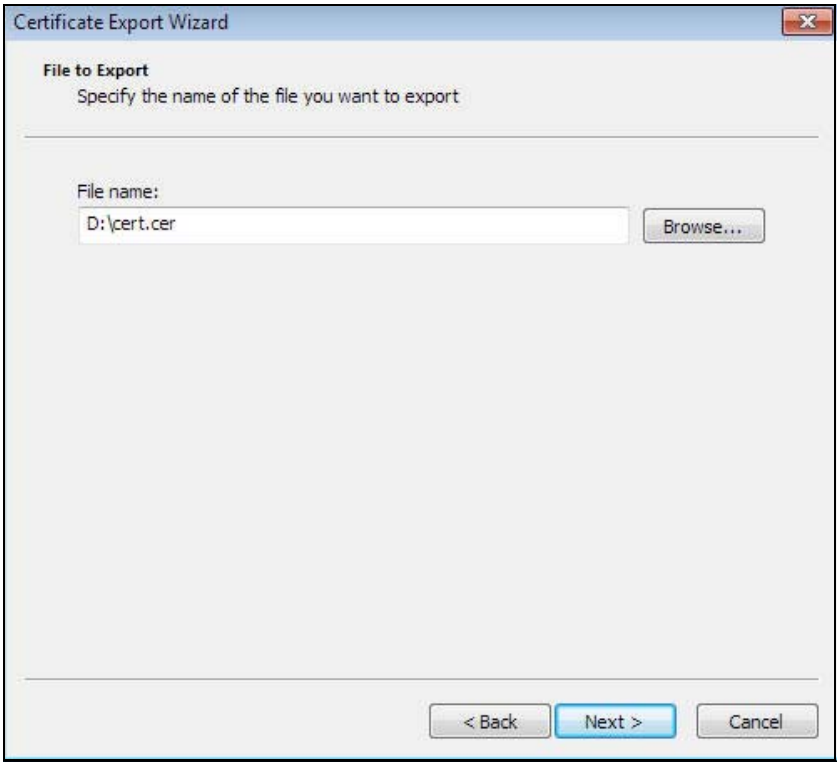
5 In the **Certificate Export Wizard**, click **Next**.



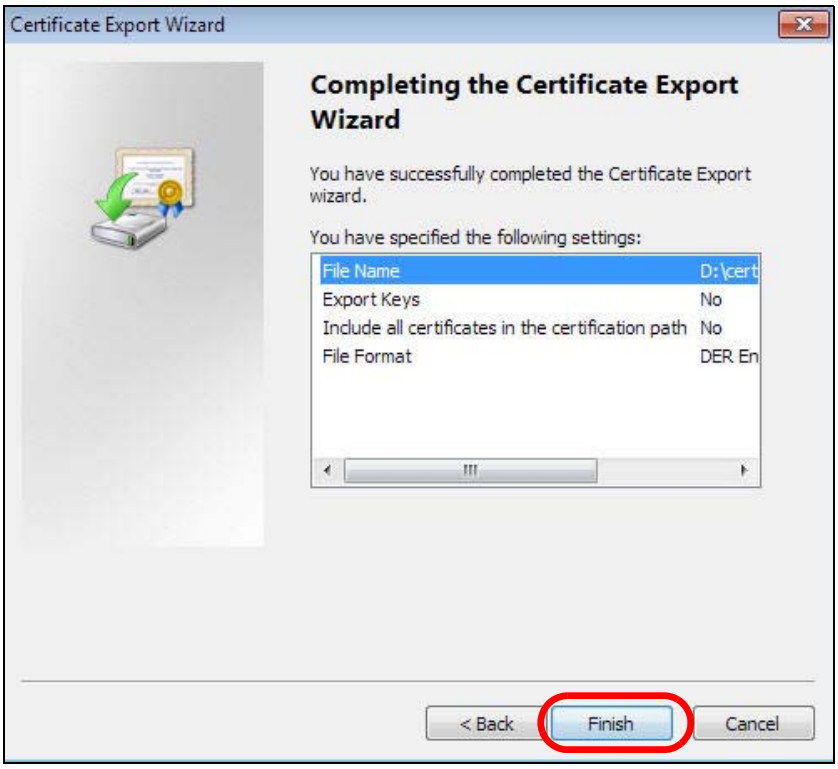
6 Select the format and settings you want to use and then click **Next**.



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



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

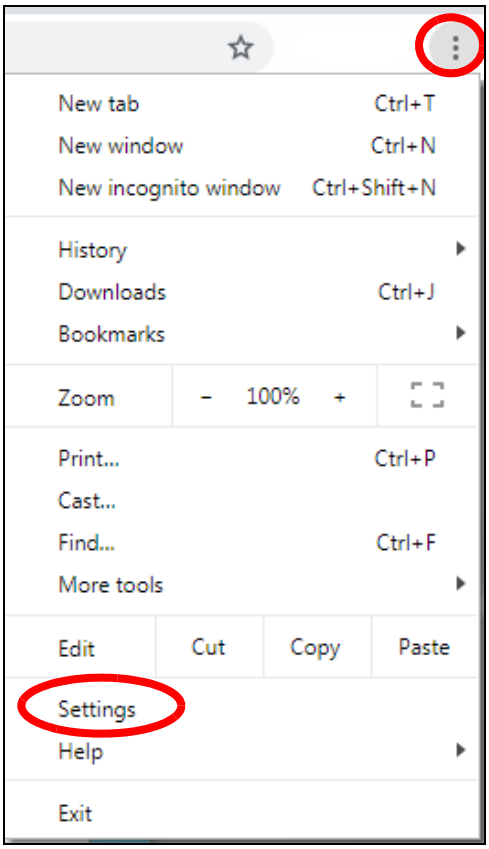


9 Finally, click **OK** when presented with the successful certificate export message.

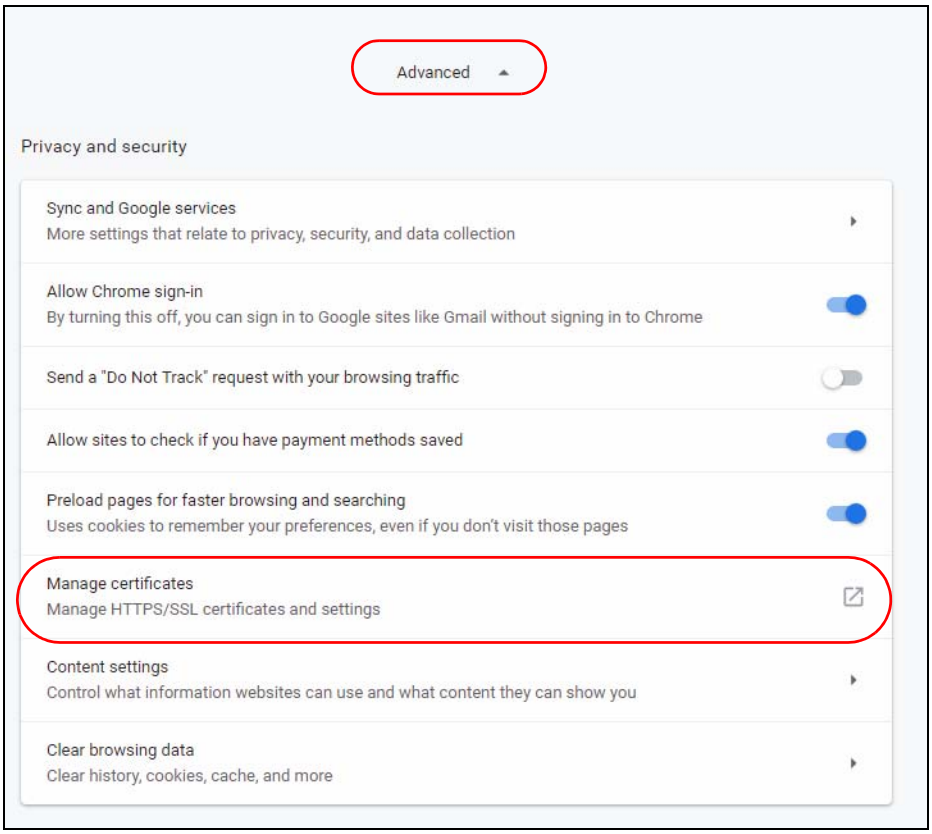
Import a Certificate

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:

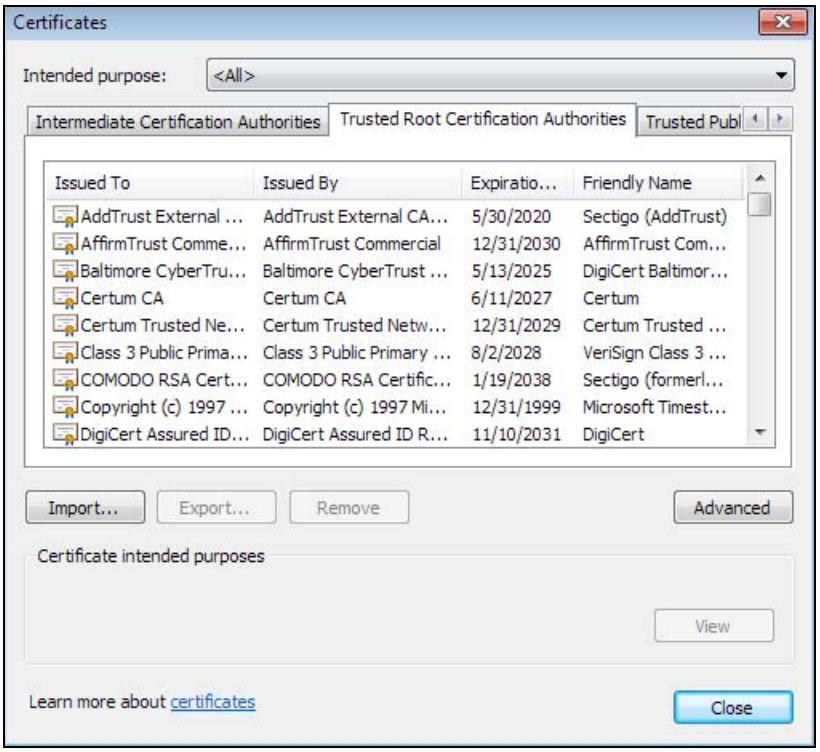
1 Open your web browser, click the menu icon, and click **Settings**.



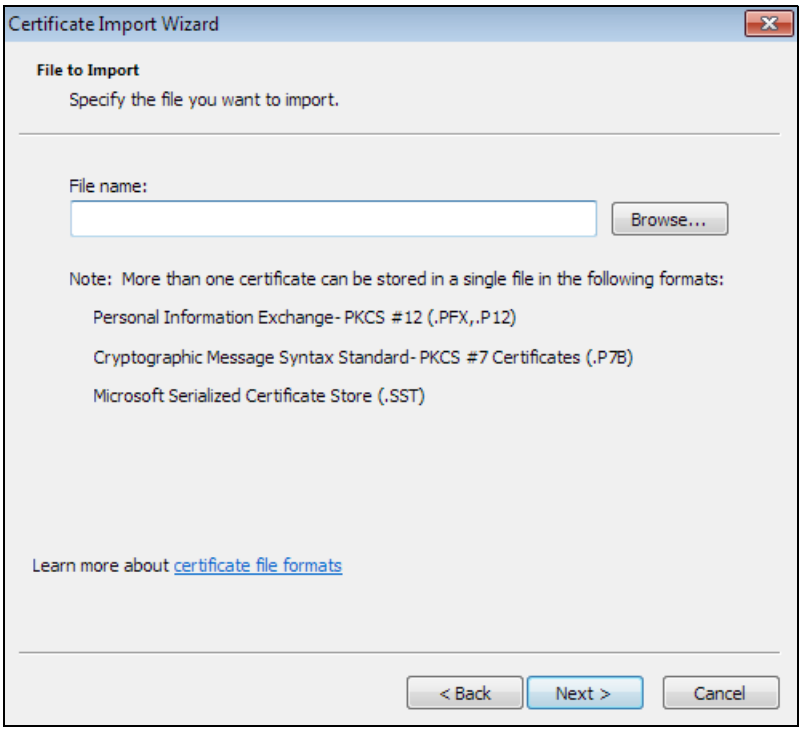
2 Scroll down and click **Advanced** to expand the menu. Under **Privacy and security**, click **Manage certificates**.



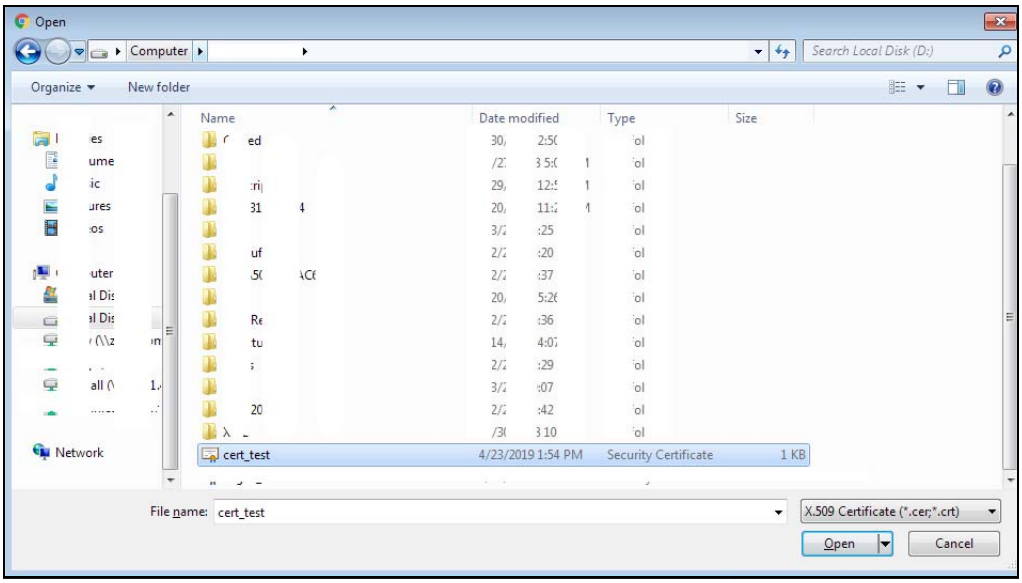
3 In the **Certificates** pop-up screen, click **Trusted Root Certification Authorities**. Click **Import** to start the **Certificate Import Wizard**.



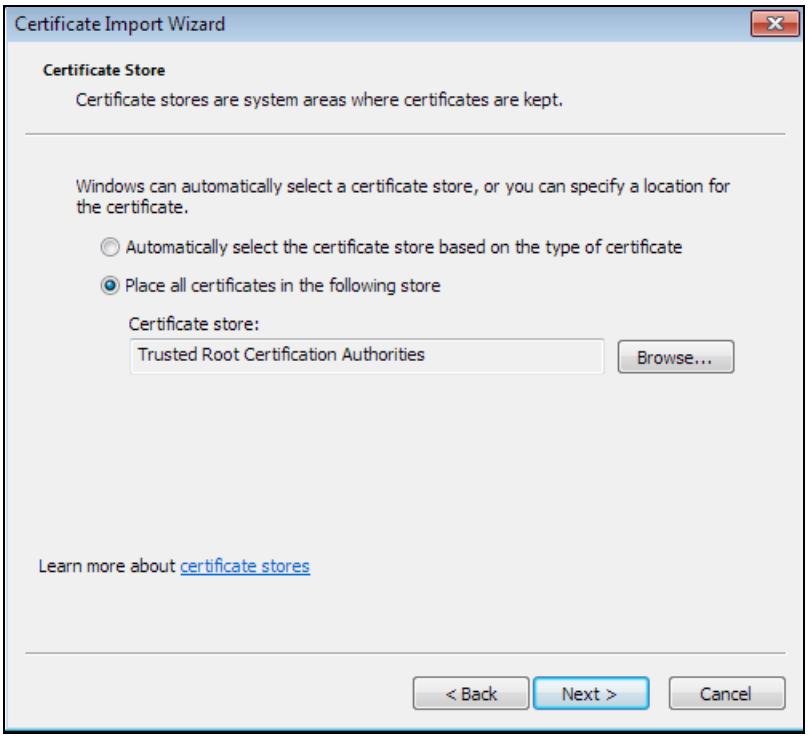
4 Click **Next** when the wizard pops up, and then on the following screen click **Browse**.



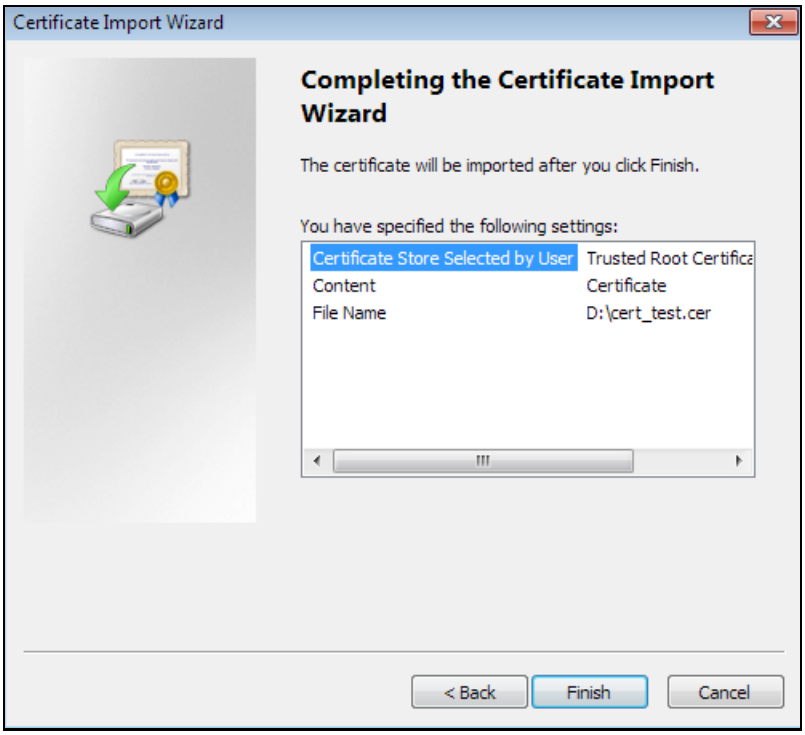
5 Select the certificate file you want to import and click **Open**.



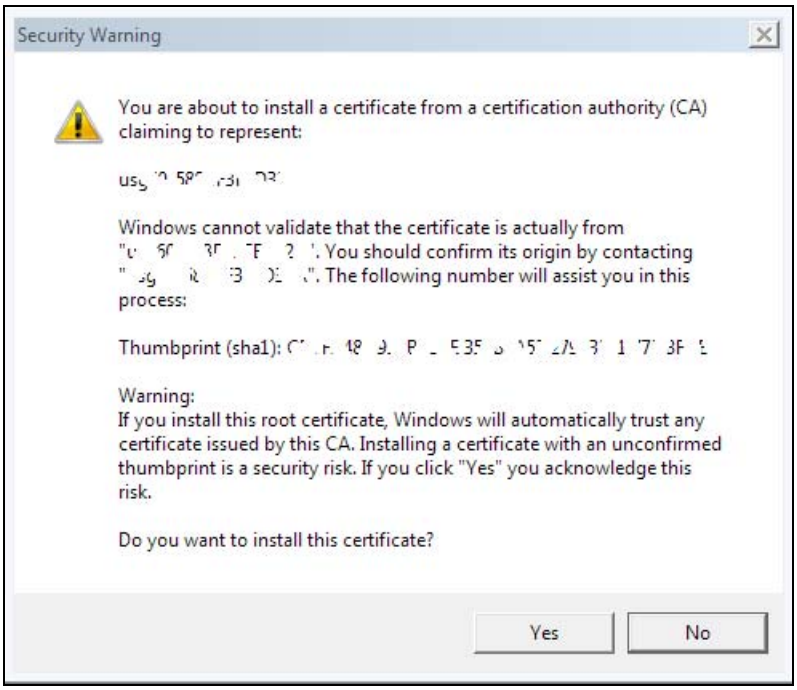
6 Click **Next.**



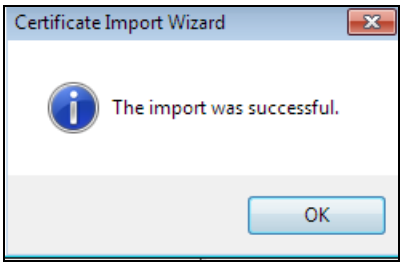
7 Confirm the settings displayed and click **Finish**.



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



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

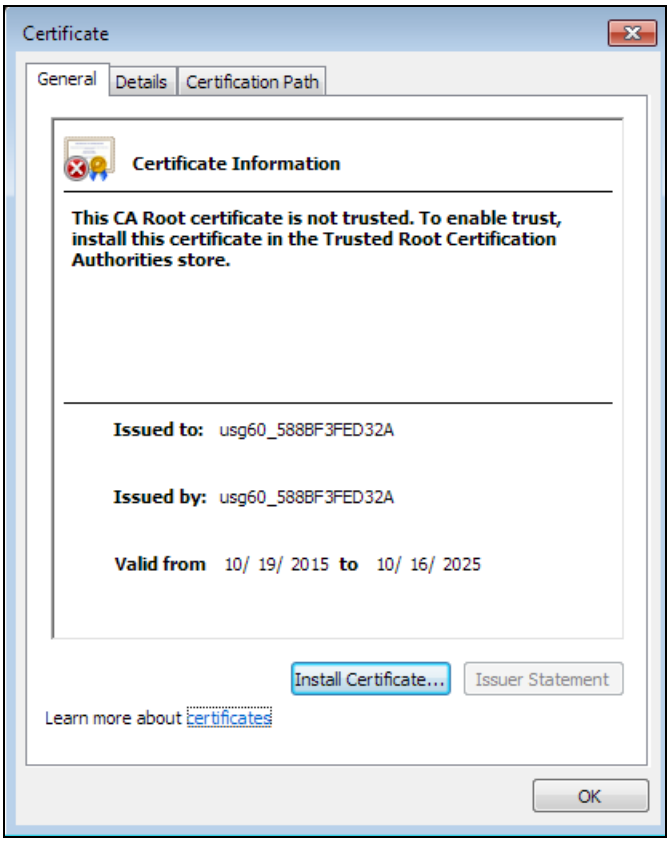


Install a Stand-Alone Certificate File

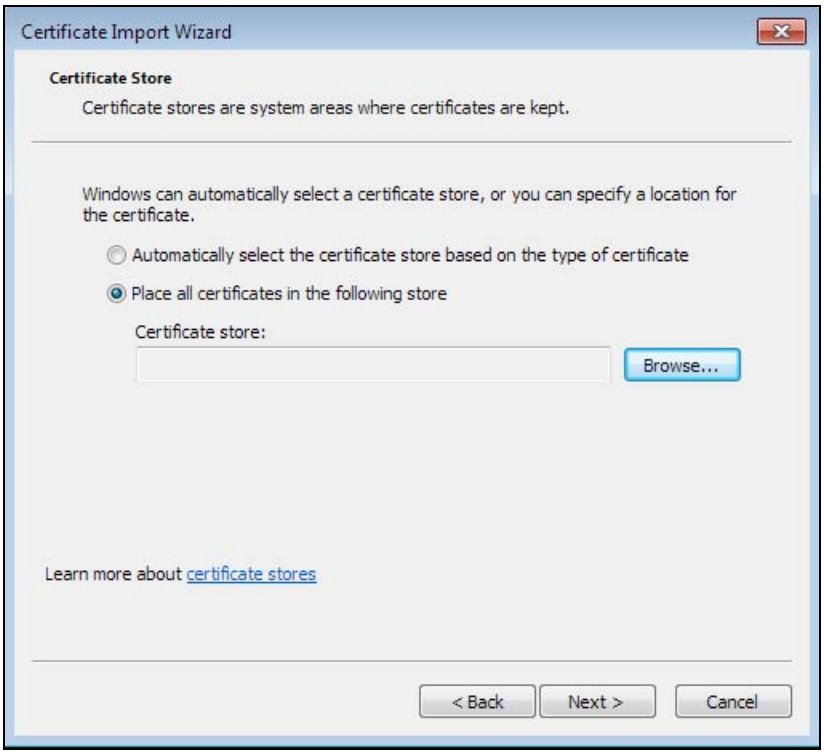
Rather than installing a public key certificate using web browser settings, you can install a stand-alone certificate file if one has been issued to you.

1 Double-click the public key certificate file.

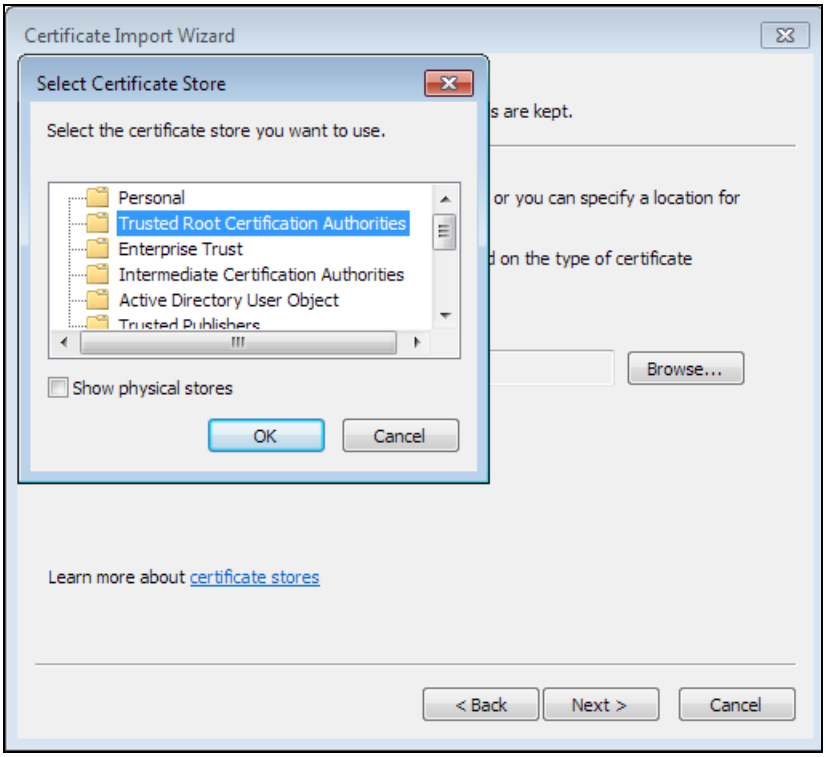
2 Click **Install Certificate**.



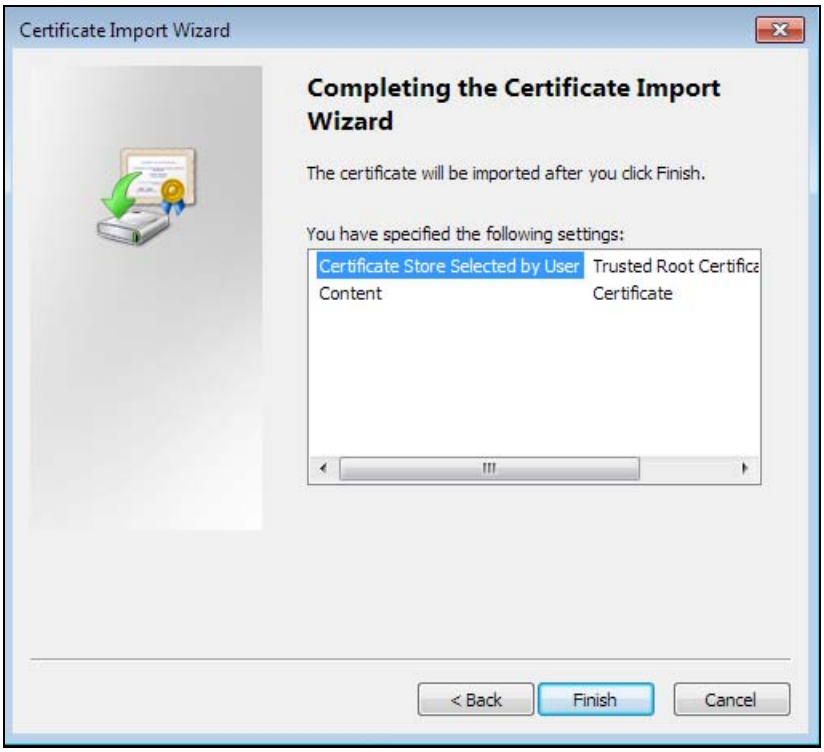
3 Click **Next** on the first wizard screen, click **Place all certificates in the following store**, and click **Browse**.



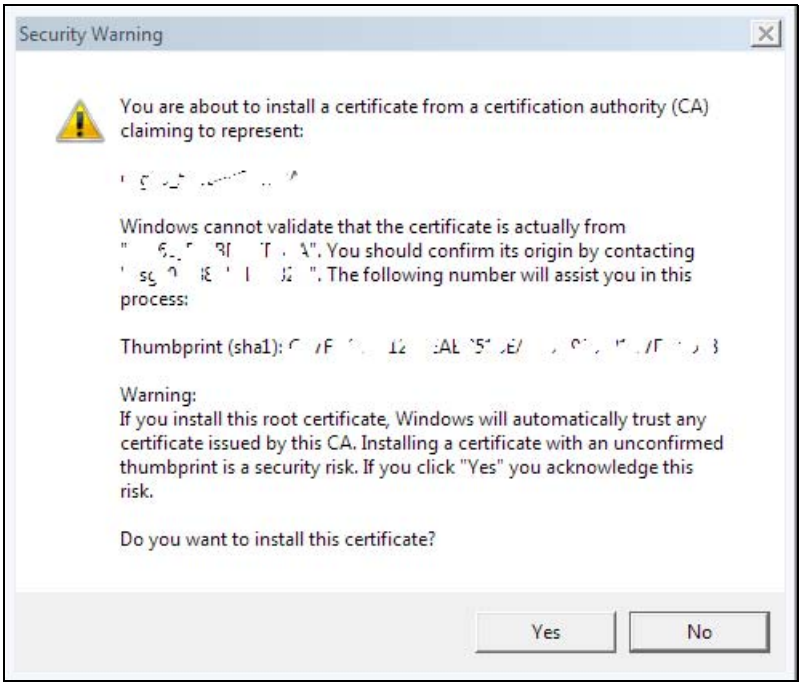
4 Select **Trusted Root Certificate Authorities** > **OK**, and then click **Next**.



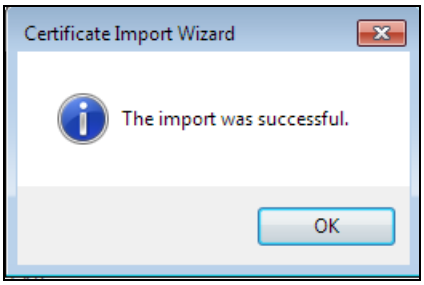
5 Confirm the information shown on the final wizard screen and click **Finish**.



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



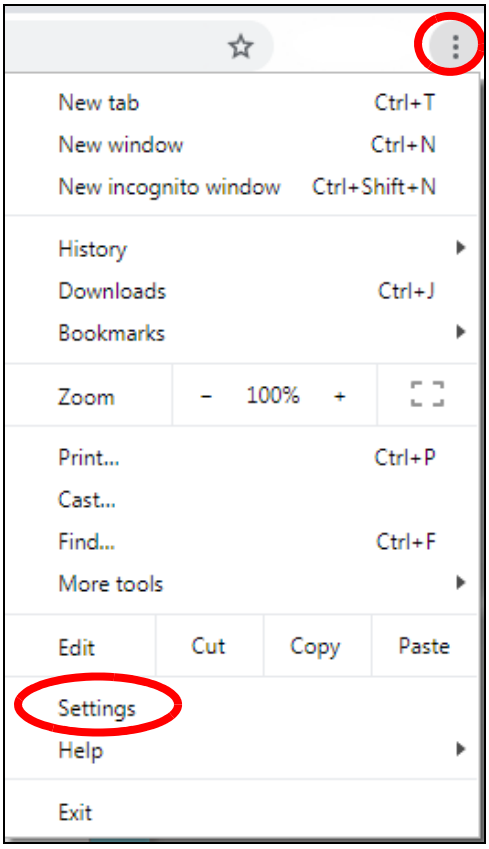
7 Finally, click **OK** when you are notified of the successful import.



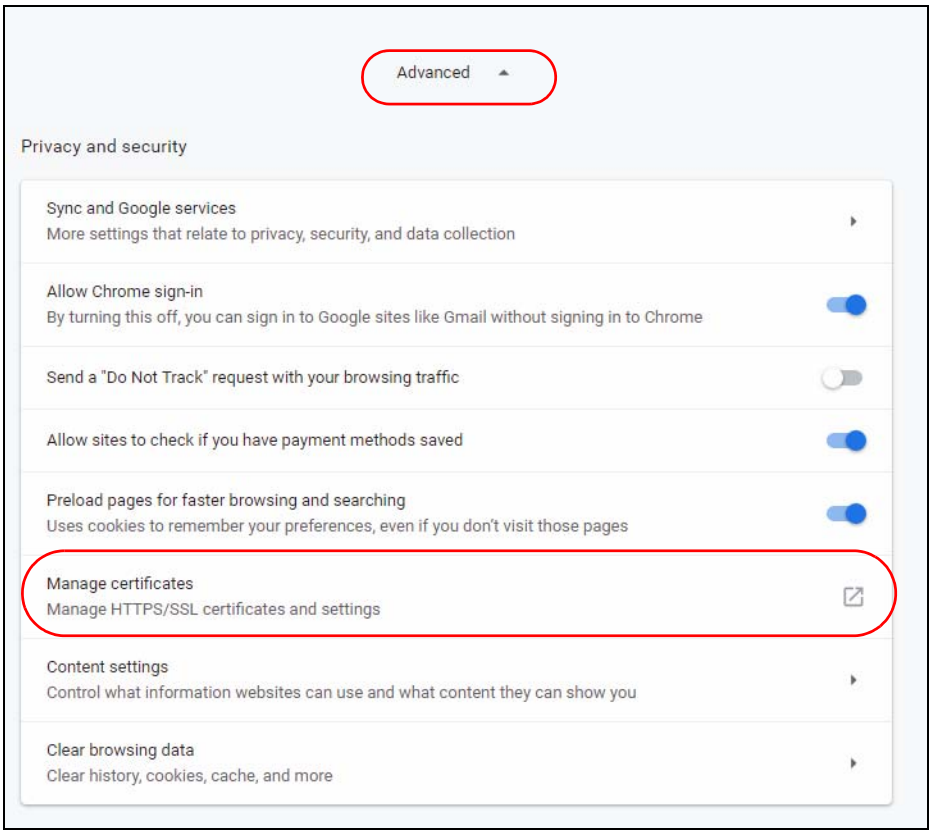
Remove a Certificate in Google Chrome

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

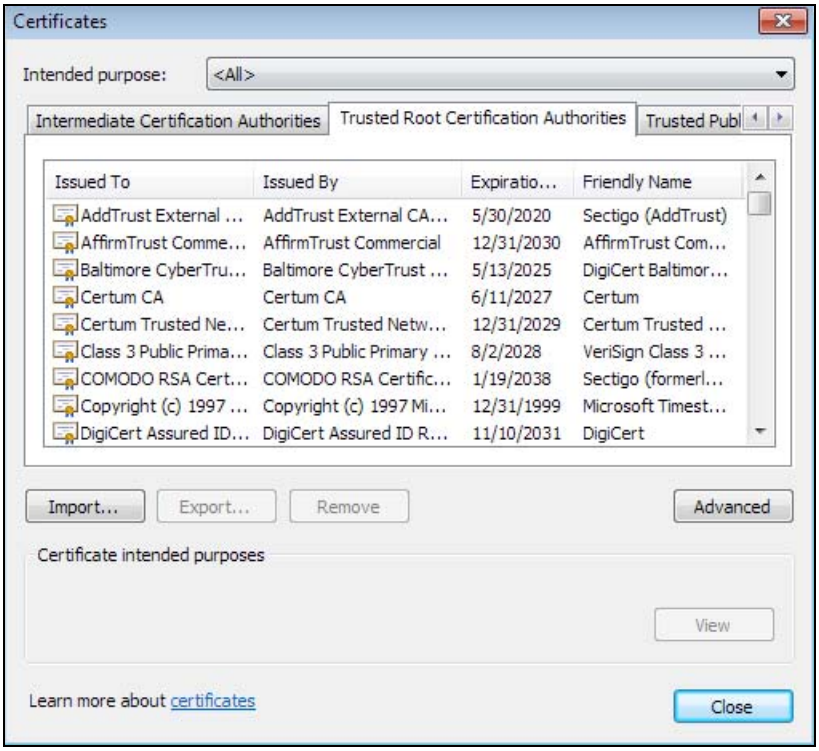
1 Open your web browser, click the menu icon, and click **Settings**.



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

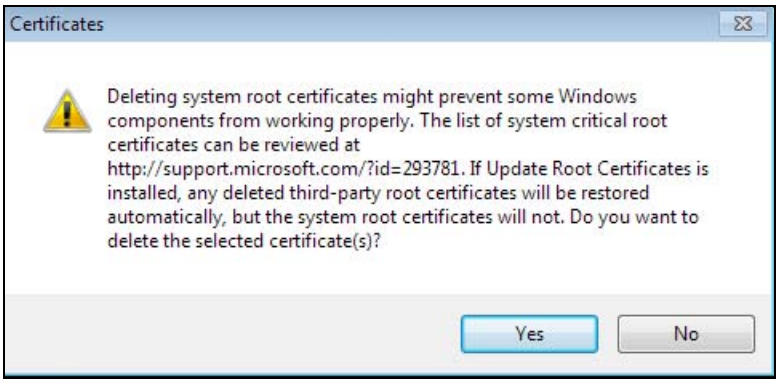


3 In the Certificates pop-up screen, click **Trusted Root Certification Authorities**.

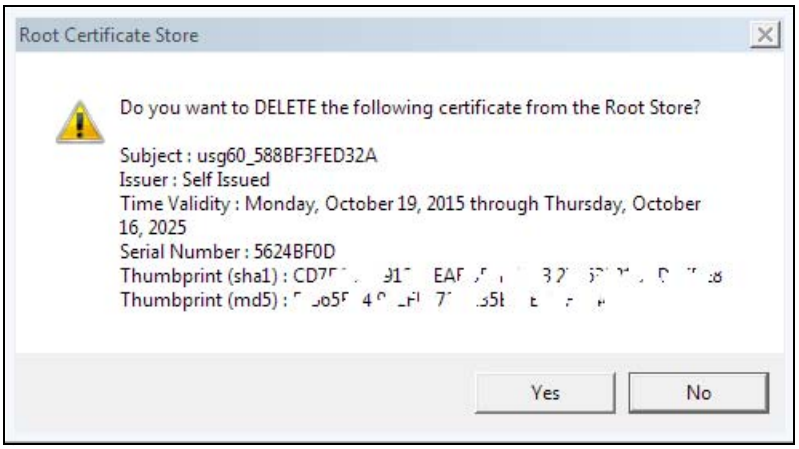


4 Select the certificate you want to remove and click **Remove**.

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



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

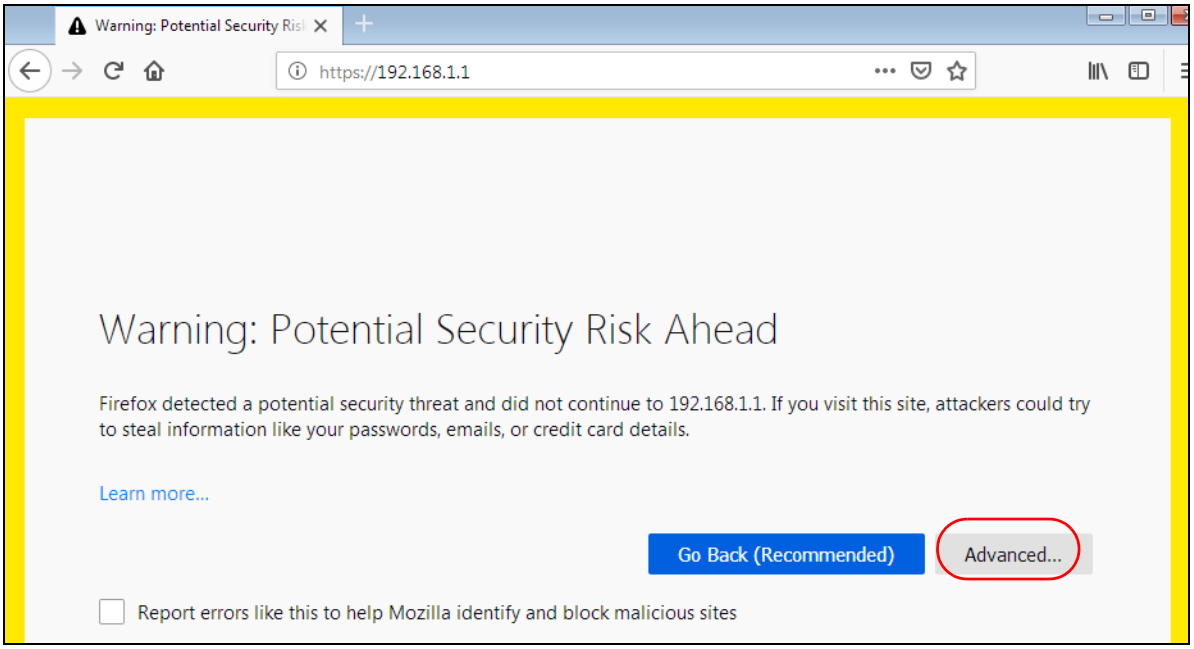


Firefox

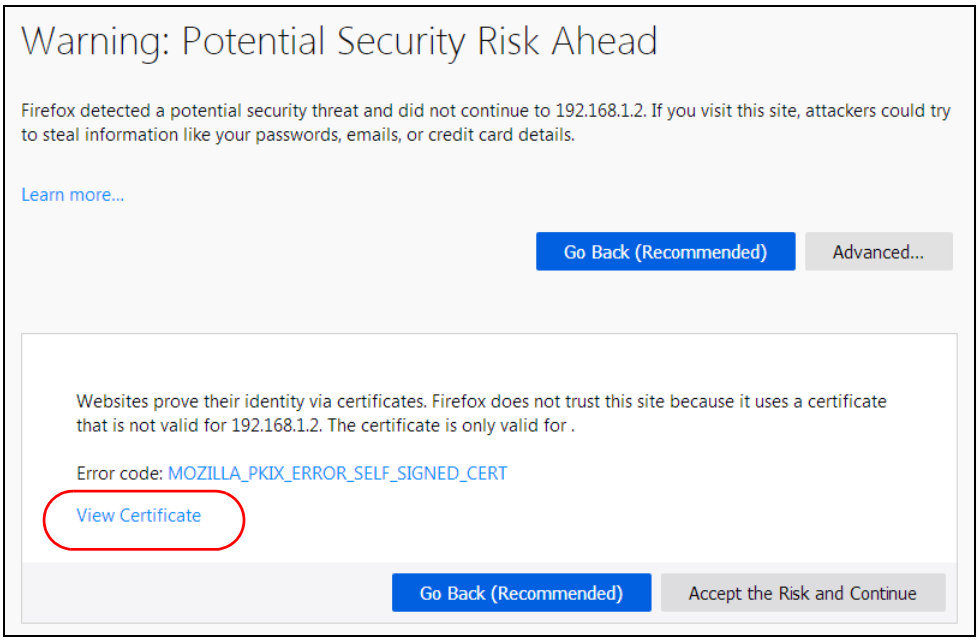
The following example uses Mozilla Firefox on Windows 7. You first have to store the certificate in your computer and then install it as a Trusted Root CA, as shown in the following tutorials.

Export a Certificate

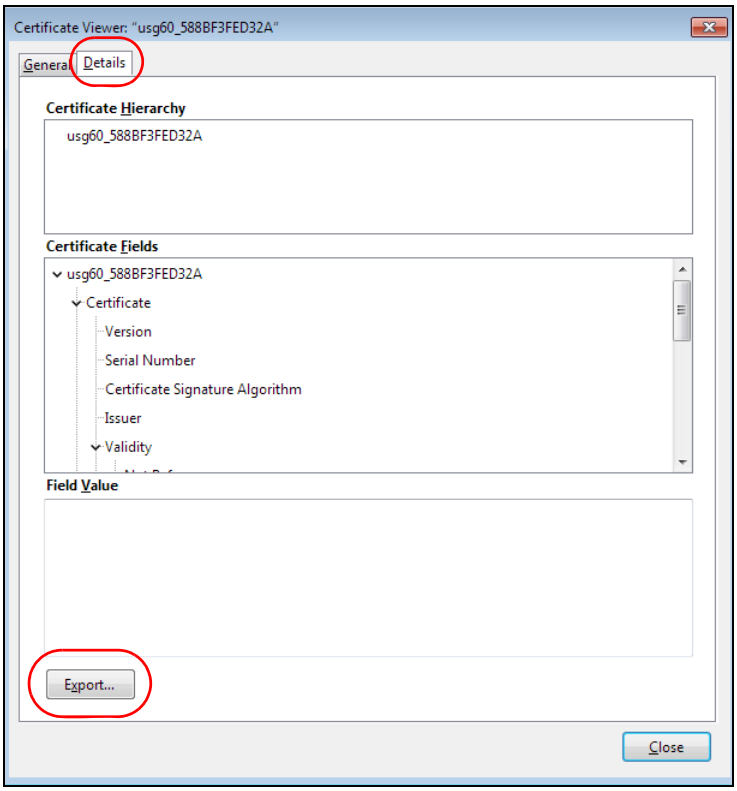
1 If your device's Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error. Click **Advanced**.



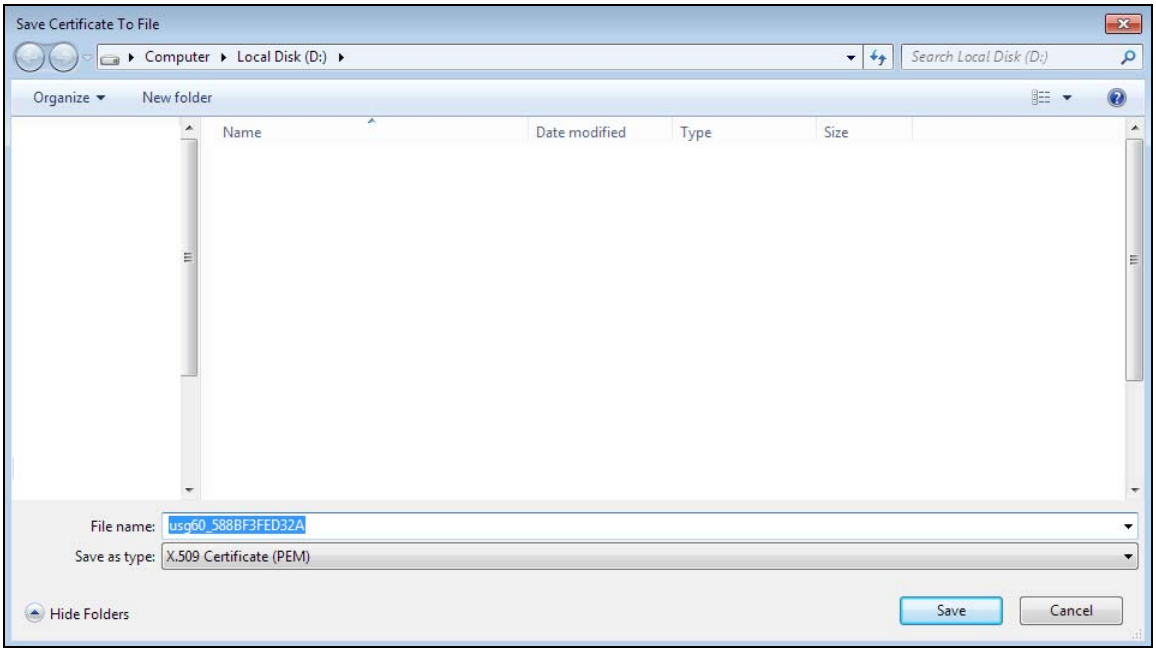
2 Click **View Certificate.**



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



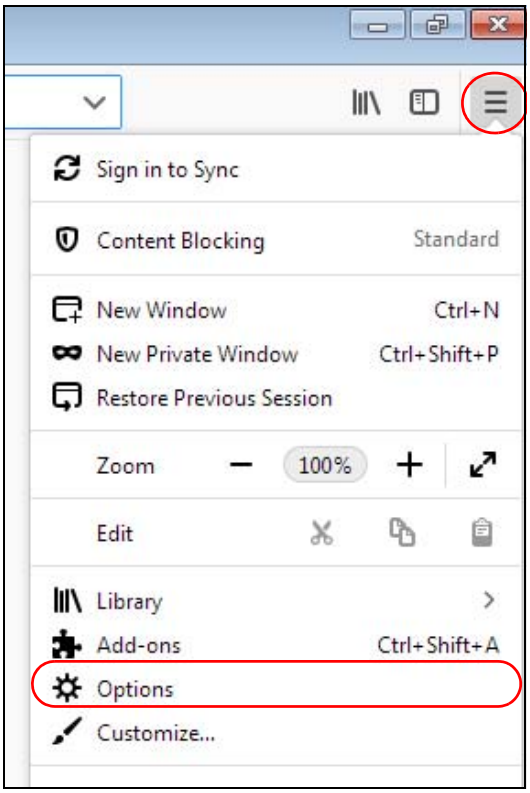
4 Type a filename and click **Save**.



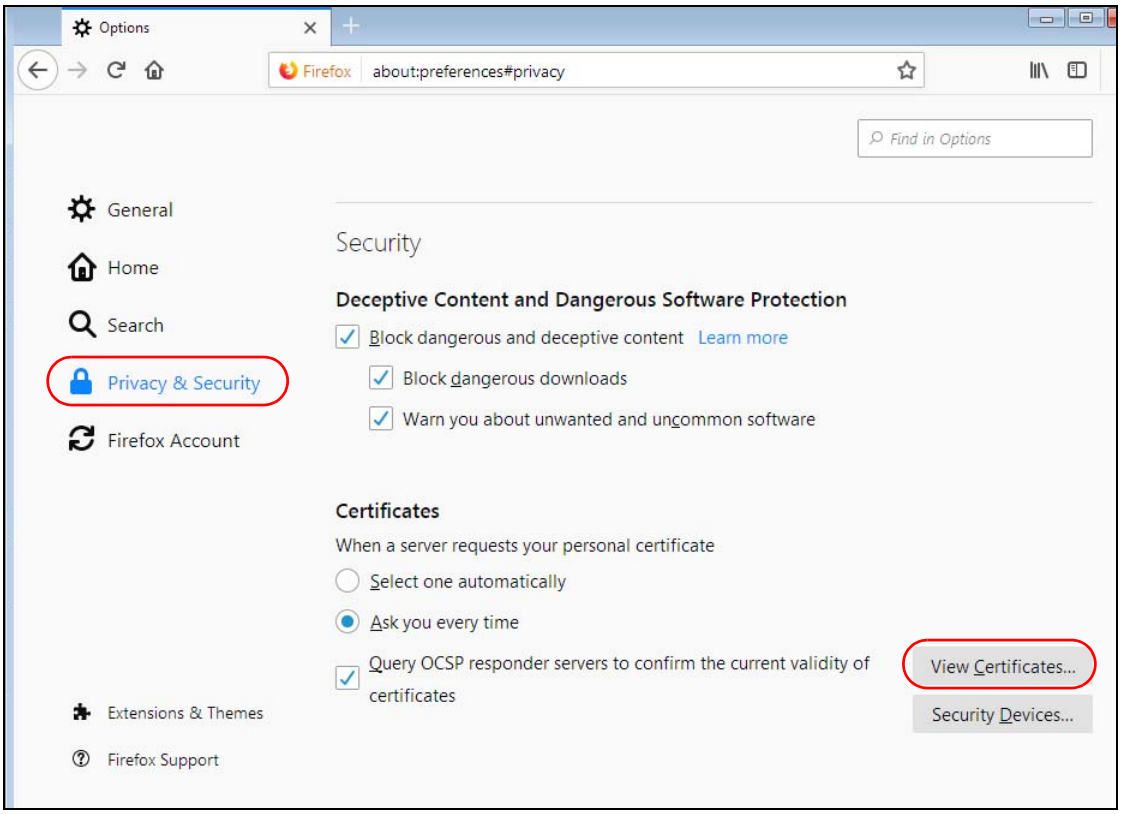
Import a Certificate

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

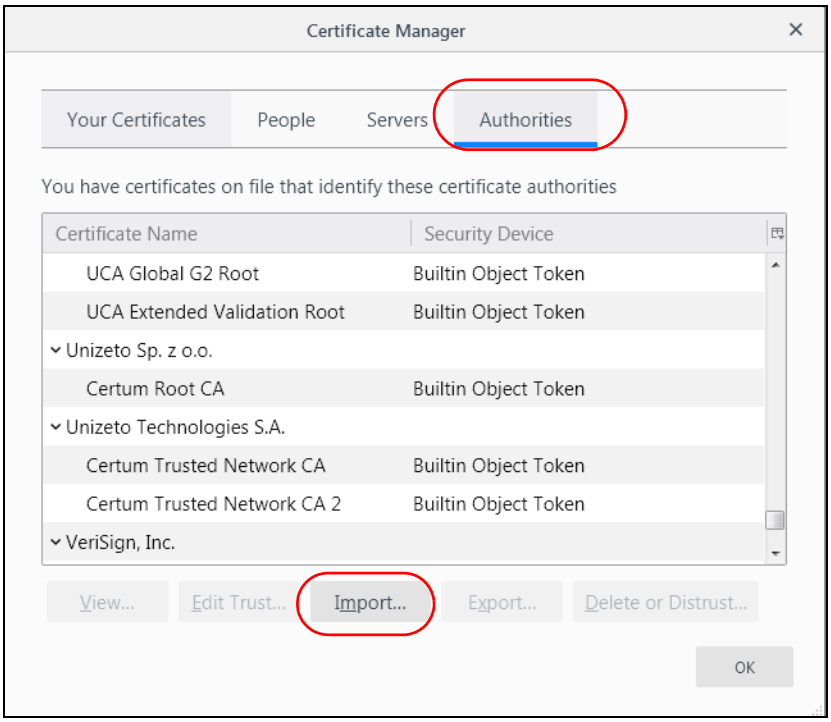
1 Open **Firefox** and click **Tools > Options**.



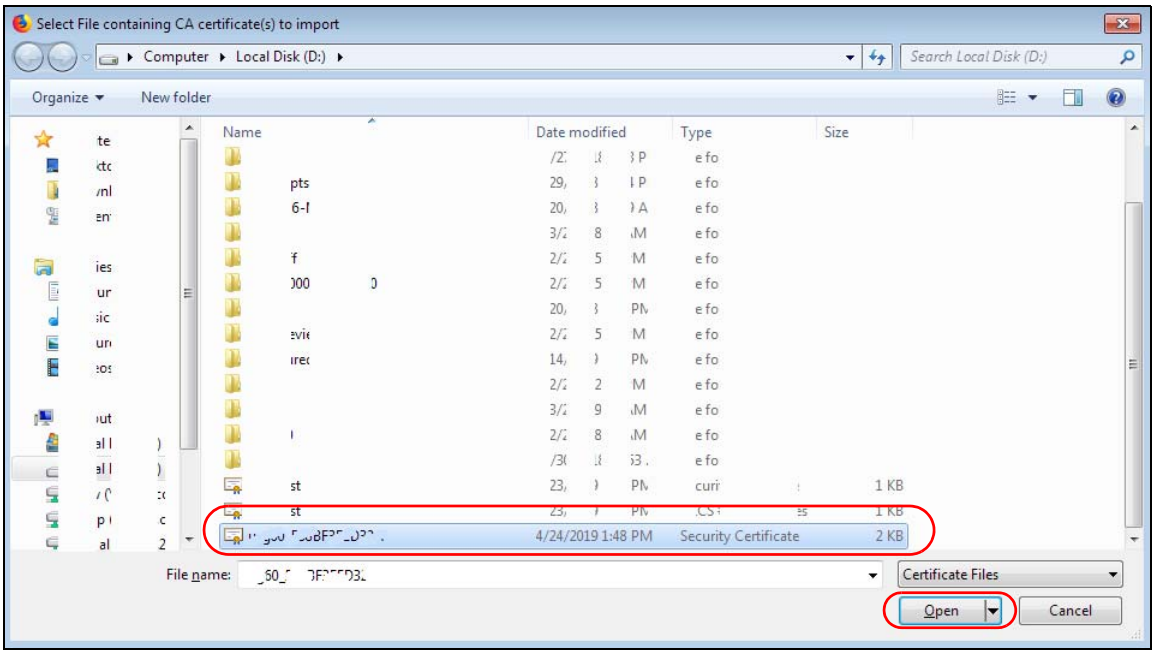
2 In the **Options** page, click **Privacy & Security**, scroll to the bottom of the page, and then click **View Certificates**.



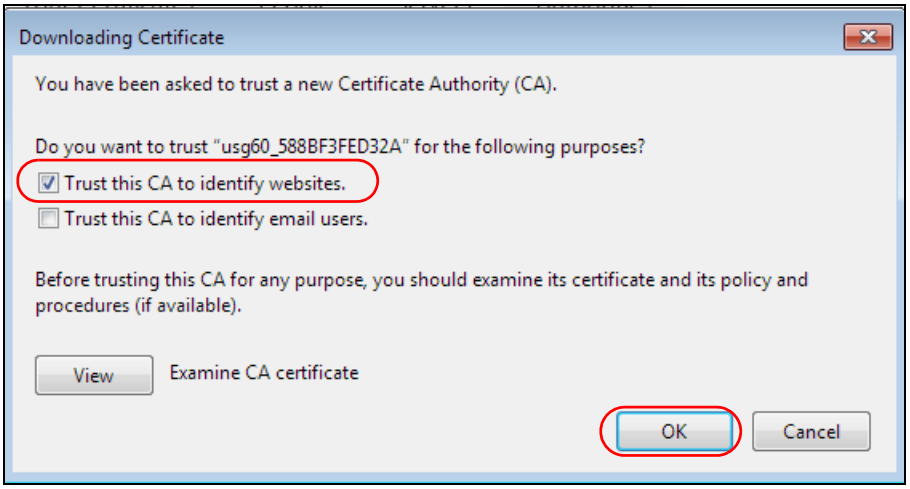
3 In the **Certificate Manager**, click **Authorities** > **Import**.



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



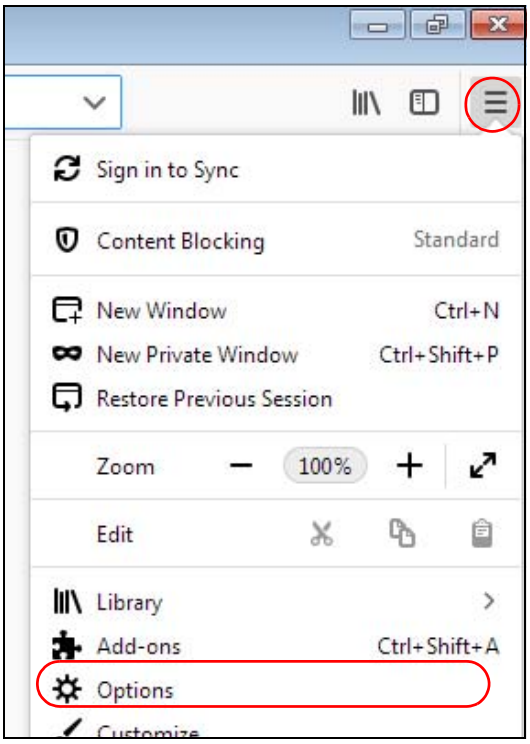
5 Select **Trust this CA to identify websites** and click **OK**.



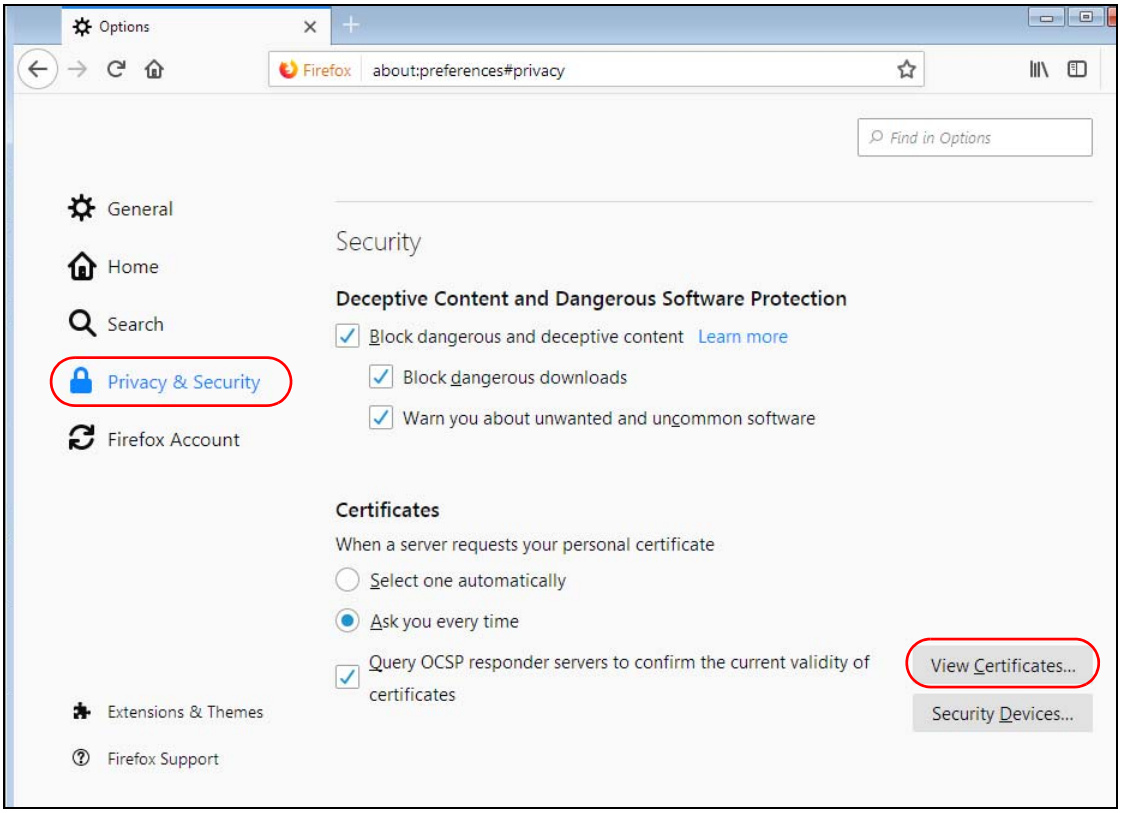
Removing a Certificate in Firefox

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

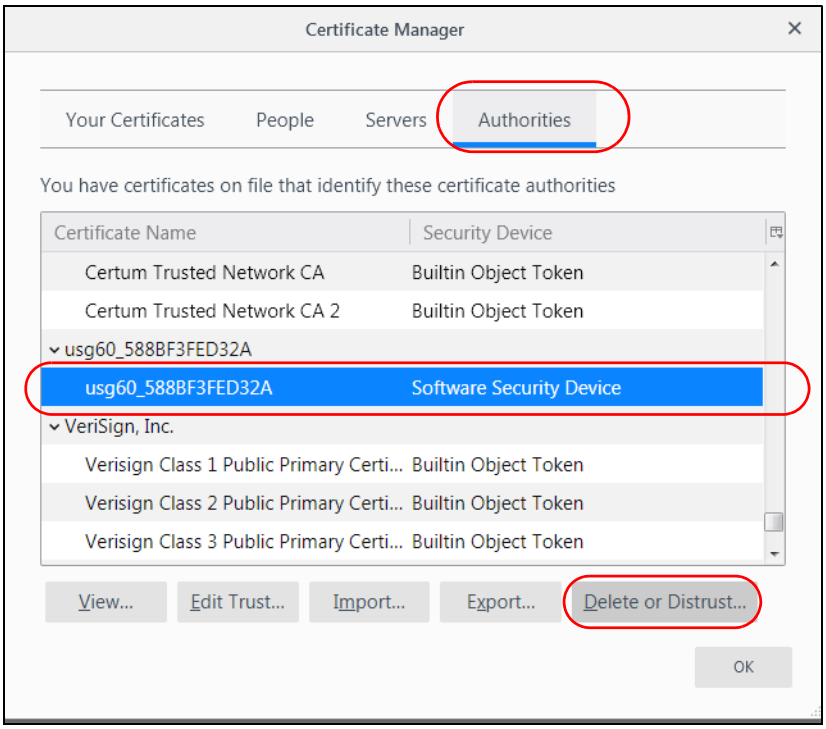
1 Open **Firefox** and click **Tools > Options**.



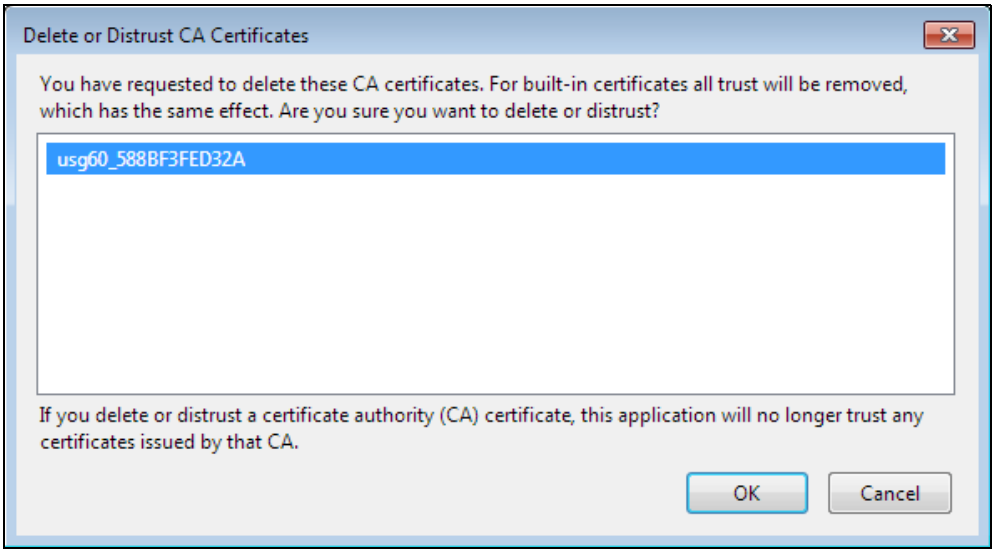
2 In the **Options** page, click **Privacy & Security**, scroll to the bottom of the page, and then click **View Certificates**.



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



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



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 102 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 103 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 104 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 105

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

Table 106

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

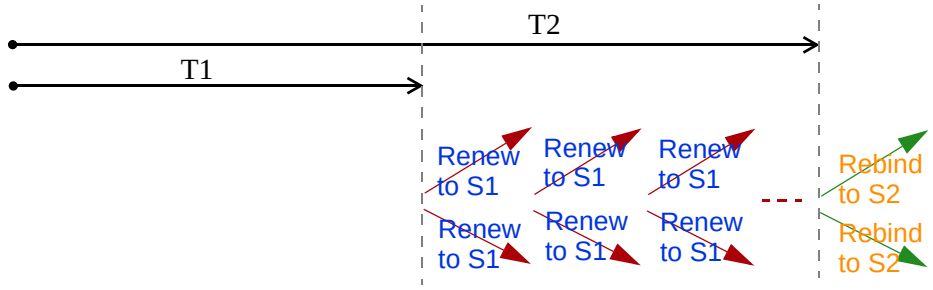
The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

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.)

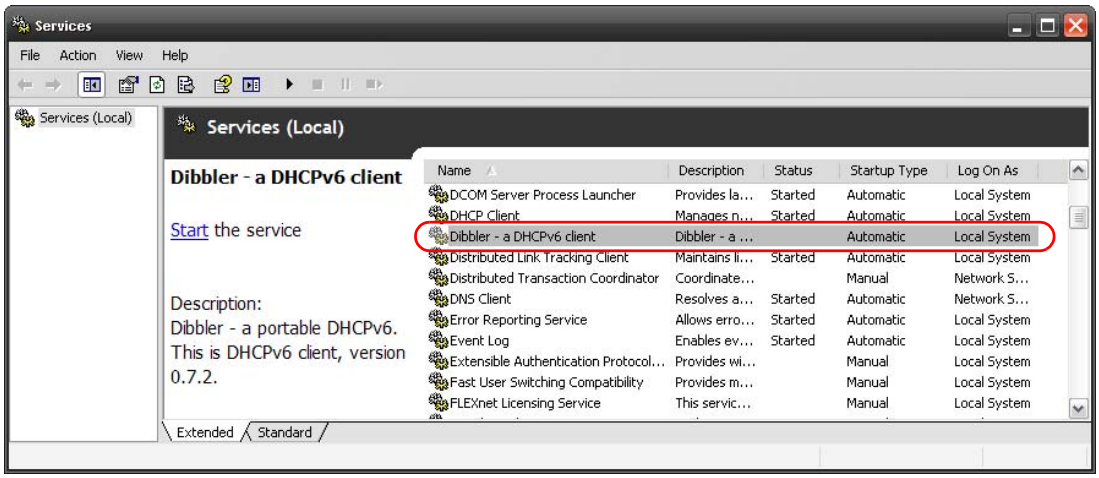
This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:

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

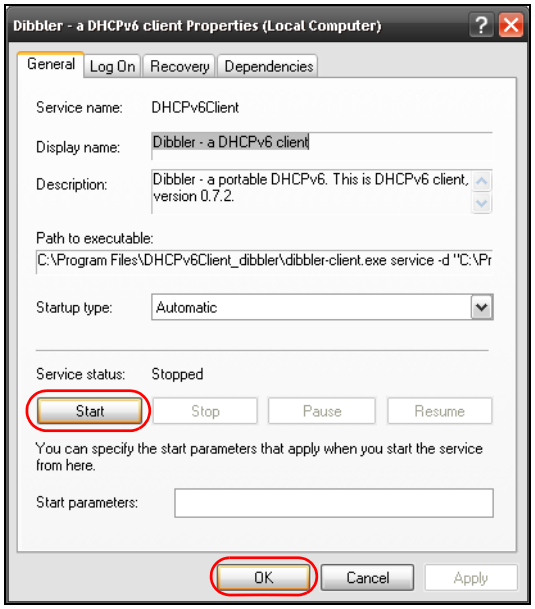
2 After the installation is complete, select **Start** > **All Programs** > **Dibbler-DHCPv6** > **Client Install as service**.

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

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



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



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

Example - Enabling IPv6 on Windows 7

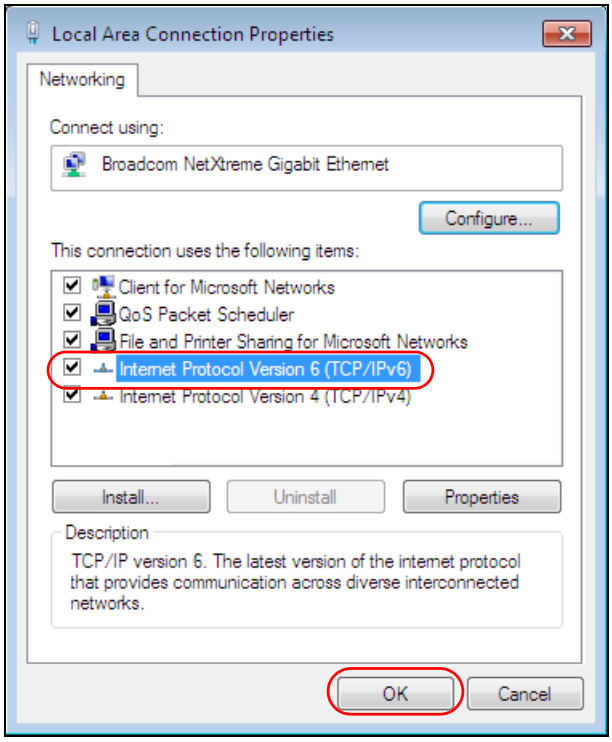
Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

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.



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

Copyright © 2019 by Zyxel Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel Communications Corporation.

Published by Zyxel Communications Corporation. All rights reserved.

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.

WAX650S

- The band 2,400 MHz to 2,483.5 MHz is 91.2 mW,
- The band 5,150 MHz to 5,350 MHz is 177.01 mW,
- The band 5,470 MHz to 5,725 MHz is 899.5 mW.

Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС. **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 cerinţele esenţiale 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

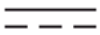
為了您的安全，請先閱讀以下警告及指示：

- 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

Symbols

Numbers

802.11k **20**, **22**, **23**
802.11r **20**, **22**, **23**
802.11v **20**, **22**, **23**

A

AC. See AP Controller
access **53**
access privileges **17**
access users **123**
  see also users **123**
admin users **123**
  multiple logins **128**
  see also users **123**
alerts **196**, **200**, **201**, **203**, **204**, **205**
antenna switch **222**
AP Controller **20**, **21**, **23**, **26**
applications
  MBSSID **17**
  Repeater **14**
Assisted Roaming. See 802.11k/v

B

backing up configuration files **208**
Basic Service Set
  see BSS
Bluetooth
  BLE. See Bluetooth Low Energy
  advertisements **121**
  advertising settings **122**
  BLE **120**
  Bluetooth Low Energy **20**, **22**, **23**, **120**
  Bluetooth Smart **120**
  iBeacon **120**
  iBeacon ID **120**
  major **120**
  minor **120**
  UUID **120**
  UUID format **122**
boot module **213**
BSS **17**

C

CA
  and certificates **156**
CA (Certificate Authority), see certificates
CAPWAP **94**
CEF (Common Event Format) **198**, **203**
Certificate Authority (CA)
  see certificates
Certificate Management Protocol (CMP) **161**
Certificate Revocation List (CRL) **156**
  vs OCSP **170**
certificates **155**
  advantages of **156**
  and CA **156**
  and FTP **189**
  and HTTPS **177**
  and SSH **186**
  and WWW **178**
  certification path **156**, **163**, **168**
  expired **156**
  factory-default **156**
  file formats **156**
  fingerprints **164**, **169**
  importing **159**
  not used for encryption **156**
  revoked **156**
  self-signed **156**, **160**

serial number 163, 168
storage space 158, 166
thumbprint algorithms 157
thumbprints 157
used for authentication 156
verifying fingerprints 157
certification requests 160, 161
certifications
viewing 298
channel 18
CLI 32, 57
button 57
messages 57
popup window 57
Reference Guide 2
cold start 65
commands 32
sent by Web Configurator 57
Common Event Format (CEF) 198, 203
comparison table 19, 21, 22
configuration
information 217, 235
configuration files 206
at restart 208
backing up 208
downloading 209
downloading with FTP 189
editing 206
how applied 207
lastgood.conf 208, 210
managing 207
startup-config.conf 210
startup-config-bad.conf 208
syntax 206
system-default.conf 210
uploading 211
uploading with FTP 189
use without restart 206
contact information 281
cookies 53
copyright 287
CPU usage 68, 70
current date/time 68, 173
daylight savings 174
setting manually 175
time server 176
customer support 281

D

date 173
daylight savings 174
DCS 106
DHCP 172
and domain name 172
diagnostics 217, 235
disclaimer 287
domain name 172
dual radios 18
dual-radio application 18
dynamic channel selection 106

E

e-mail
daily statistics report 194
encryption 14
ESSID 246
Extended Service Set IDentification 130

F

Fast Roaming. See 802.11r
FCC interference statement 287
file extensions
configuration files 206
shell scripts 206
file manager 206
Firefox 53
firmware
and restart 212
boot module, see boot module
current version 68, 213
getting updated 212
uploading 212, 213
uploading with FTP 189
flash usage 68
FTP 32, 189
and certificates 189
with Transport Layer Security (TLS) 189

G

Guide
CLI Reference 2

H

HTTP
over SSL, see HTTPS
redirect to HTTPS 178
vs HTTPS 177
HTTPS 177
and certificates 177
authenticating clients 177
avoiding warning messages 180
example 178
vs HTTP 177
with Internet Explorer 179
with Netscape Navigator 179
HyperText Transfer Protocol over Secure Socket Layer, see HTTPS

I

IEEE 802.1x 131
interface
status 69
interfaces
as DHCP servers 172
interference 18
Internet Explorer 53
Internet Protocol version 6, see IPv6
IP Address 94, 231
gateway IP address 94
IP subnet 94
IPv6 273
addressing 273
EUI-64 275
global address 273
interface ID 275
link-local address 273
Neighbor Discovery Protocol 273
ping 273
prefix 273
prefix length 273
stateless autoconfiguration 275
unspecified address 274

J

Java
permissions 53
JavaScripts 53

K

key pairs 155

L

lastgood.conf 208, 210
layer-2 isolation 147
example 147
MAC 148
LED suppression 219
LEDs 34
Blinking 43, 45, 47, 49, 51
load balancing 106
Locator LED 220
log messages
categories 201, 203, 204, 205
debugging 91
regular 91
types of 91
logout
Web Configurator 57
logs
e-mail profiles 196
e-mailing log messages 93, 200
formats 198
log consolidation 201
settings 196
syslog servers 196
system 196
types of 196

M

MAC address
range 68
Management Information Base (MIB) 190, 191
Management Mode
CAPWAP and DHCP 95
management mode 24
Management, NCC 24
Management, Standalone 24
managing the device
good habits 32
using FTP. See FTP.
MBSSID 17
memory usage 68, 71
messages
CLI 57
mode, default 24
model name 67
My Certificates, see also certificates 158

N

NCC. See Nebula Control Center
Nebula Control Center 24
Netscape Navigator 53
Network Time Protocol (NTP) 175

O

objects
certificates 155
users, account
user 123
Online Certificate Status Protocol (OCSP) 170
vs CRL 170
overview 13, 65, 227

P

pop-up windows 53
power off 66
power on 65
product registration 299
Public-Key Infrastructure (PKI) 156
public-private key pairs 155

R

radio 18
Radio Frequency monitor 13
reboot 65, 224
vs reset 224
Reference Guide, CLI 2
registration
product 299
remote management
FTP, see FTP
Telnet 188
WWW, see WWW
reports
daily 194
daily e-mail 194
reset 247
vs reboot 224
vs shutdown 225
RESET button 66, 247
restart 224
RF interference 18
RF monitor. See Radio Frequency Monitor
RFC
2510 (Certificate Management Protocol or CMP) 161
Rivest, Shamir and Adleman public-key algorithm (RSA) 160
RSA 160, 168, 169
RSSI threshold 137

S

SCEP (Simple Certificate Enrollment Protocol) 161
screen resolution 53
Secure Socket Layer, see SSL
serial number 68

service control
and users 176
limitations 176
timeouts 176
Service Set 130
Service Set Identifier
see SSID
shell scripts 206
downloading 215, 235
editing 214, 234
how applied 207
managing 214, 234
syntax 206
uploading 216, 235
shutdown 66, 225
vs reset 225
Simple Certificate Enrollment Protocol (SCEP) 161
Simple Network Management Protocol, see SNMP
SNMP 190
agents 190
Get 190
GetNext 190
Manager 190
managers 190
MIB 190, 191
network components 190
Set 190
Trap 191
traps 191
versions 190
SSH 184
and certificates 186
client requirements 186
encryption methods 186
for secure Telnet 187
how connection is established 185
versions 186
with Linux 187
with Microsoft Windows 187
SSID 17
SSID profile
pre-configured 17
SSID profiles 17
SSL 177
starting the device 65
startup-config.conf 210
if errors 208
missing at restart 208
present at restart 208
startup-config-bad.conf 208
station 106
statistics
daily e-mail report 194
status 229
stopping the device 65
supported browsers 53
syslog 198, 203
syslog servers, see also logs
system log, see logs
system name 67, 172
system uptime 68
system-default.conf 210

T

Telnet 188
with SSH 187
time 173
time servers (default) 175
trademarks 287
Transport Layer Security (TLS) 189
troubleshooting 217, 235
Trusted Certificates, see also certificates 165

U

upgrading
firmware 212
uploading
configuration files 211
firmware 212
shell scripts 214, 234
usage
CPU 68, 70
flash 68
memory 68, 71
onboard flash 68
user authentication 123
user name
rules 124

user objects 123
users 123
access, see also access users
admin (type) 123
admin, see also admin users
and service control 176
currently logged in 69
default lease time 127, 129
default reauthentication time 127, 129
lease time 126
limited-admin (type) 123
lockout 128
reauthentication time 126
types of 123
user (type) 123
user names 124

V

Vantage Report (VRPT) 198, 203
Virtual Local Area Network 99
VLAN 99
introduction 99
VRPT (Vantage Report) 198, 203

W

warm start 65
warranty 298
note 298
WDS 14
Web Configurator 31, 53
access 53
requirements 53
supported browsers 53
WEP (Wired Equivalent Privacy) 131
wireless channel 246
wireless client 106
Wireless Distribution System (WDS) 14
wireless LAN 246
Wireless network
overview 105
wireless network
example 105
wireless profile 130
layer-2 isolation 130
MAC filtering 130
radio 130
security 130
SSID 130
wireless security 17, 246
wireless station 106
Wizard Setup 73
WLAN interface 18
WPA2 131
WWW 177
and certificates 178
see also HTTP, HTTPS 177

Z

ZDP 27
ZON Utility 27
ZyXEL Discovery Protocol 27