



User's Guide NWA50AX

802.11ax (WiFi6) Dual-Radio PoE Access Point

Default Login Details

| Management IP Address | http://DHCP-assigned IP OR http://192.168.1.2 |
|--------------------------|---|
| User Name | admin |
| Password | 1234 |

Version 6.20 Edition 1, 4/2021



IMPORIANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

This is a User's Guide for a series of products. Not all products support all firmware features. Screenshots and graphics in this book may differ slightly from your product due to differences in your product hardware, firmware, or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Some screens or options in this book may not be available for your product (see the product feature tables in Section 1.4 on page 18).

Related Documentation

• Quic k Start Guide

The Quick Start Guide shows how to connect the Zyxel Device and access the Web Configurator.

• CLIReference Guide

The CUR ference Guide explains how to use the Command-Line Interface (CLI) and CLI commands to configure the Zyxel Device.

Note: It is recommended you use the Web Configurator to configure the Zyxel Device.

• Web Configurator Online Help

Click the help icon in any screen for help in configuring that screen and supplementary information.

• Nebula Control Center User's Guide

This User's Guide shows how to manage the Zyxel Device remotely. The features of these devices can be managed through Nebula Control Center. It also offers features that are not available when the Zyxel Device is in standalone mode (see Section 2.1.2 on page 20).

• NXC Se rie s Use r's G uid e

See this User's Guide for instructions on using the NXC as an AP Controller (AC) for the Zyxel Device. This is used when the Zyxel Device is set to be managed by a Zyxel AC.

• More Information

Go to support.zyxel.com to find other information on the Zyxel Device.



Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this guide.

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

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

Syntax Conventions

- All models in this series may be referred to as the "Zyxel Device" in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Configuration** > **Network** > **IP** Setting means you first click **Configuration** in the navigation panel, then the **Network** sub menu and finally the **IP** Setting tab to get to that screen.

Icons Used in Figures

Figures in this guide may use the following generic icons. The Zyxel Device icon is not an exact representation of your device.

| Zyxe l De vic e | Ro ute r | Swite h | Internet |
|-----------------|----------------|----------------|-------------------|
| Se rve r | De skto p | Laptop | AP C o ntro lle r |
| Printe r | Ne bula Switch | Nebula Gateway | Smart TV. |
| IP Phone | | | |

Contents Overview

| In tro d u c tio n | 12 |
|-----------------------------------|-----|
| AP Management | 20 |
| Hard ware | 28 |
| We b Configurator | 30 |
| Standalone Configuration | 41 |
| Stand a lone Configuration | 42 |
| Dashboard | 44 |
| Se tup Wiza rd | 49 |
| Monitor | 54 |
| Ne two rk | 69 |
| Wire le ss | 75 |
| Use r | 86 |
| AP Pro file | 93 |
| MON Pro file | 117 |
| WDS Pro file | 120 |
| Certific a tes | 122 |
| Syste m | 138 |
| Log and Report | 157 |
| Fle Manager | 167 |
| Diagnostics | 178 |
| LEDs | 180 |
| Reboot | 183 |
| Shutdown | 184 |
| Local Configuration in Cloud Mode | 185 |
| Cloud Mode | 186 |
| Ne two rk | 189 |
| Maintenance | 192 |
| Appendices and Troubleshooting | 197 |
| The ub le sho o ting | 198 |

Table of Contents

| Document Conventions | 3 |
|---|----|
| Contents Overview | 4 |
| Table of Contents | 5 |
| Chapter 1 Introduction | |
| | 10 |
| 1.2 Zwel Device Balag | |
| 1.2 Lyxer Device Roles | |
| 1.2.1 Wim loss Ropo ator | |
| 1.2.2 Where ssile peaker | |
| 1.3 Sample Feature Applications | |
| 1.3.1 MBSSID | 16 |
| 1.3.2 Dua l-Radio | |
| 1.4 ZyxelDevice ProductFeature | |
| Chapter 2 | |
| AP Management | |
| 2.1 Management Mode | 20 |
| 2.1.1 Standalone | 20 |
| 2.1.2 Nebula Control Center | |
| 2.2 Switching Management Modes | |
| 2.3 ZyxelOne Network (ZON) Utility | |
| 2.3.1 Re q uire m e nts | |
| 2.3.2 Run the ZON Utility | |
| 2.4 Ways to Access the Zyxel Device | |
| 2.5 Good Habits for Managing the Zyxel Device | |
| Chapter 3 | |
| Hard ware | |
| 3.1 Zyxel De vice Single LED | |
| 3.1.1 Zyxel Device LED | |
| Chapter 4 | |
| Web Configurator | |
| 4.1 Overview | |
| 4.2 Accessing the WebConfigurator | |
| 4.3 Navigating the Web Configurator | |

| 4.3.1 Title Bar | |
|--|----|
| 4.3.2 Na vig a tio n Pa ne l | 35 |
| 4.3.3 Standalone Mode Navigation Panel Menus | 35 |
| 4.3.4 Cloud Mode Navigation Panel Menus | |
| 4.3.5 Tables and Lists | 38 |
| | |
| | |
| Part I: Standalone Configuration | |
| | |
| Standalone Configuration | 42 |
| | |
| 5.1 O ve rvie w | 42 |
| 5.2 Starting and Stopping the ZyxelDevice | |
| Chapter 6 | |
| Da shb o a rd | 44 |
| | |
| 6.1 Uverview | |
| 6.1.2 Momory Hasso | |
| 0.1.2 Memory Usage | |
| Chapter 7 | |
| Se tup Wiza rd | 49 |
| 7.1 Accessing the Wizard | 49 |
| 7.2 Using the Wizard | 49 |
| 7.2.1 Step 1 Time Settings | 49 |
| 7.2.2 Step 2 Password and Uplink Connection | 50 |
| 7.2.3 Step 3 Radio | 51 |
| 7.2.4 Step 4 SSID | 52 |
| 7.2.5 Summary | 52 |
| Chanten 8 | |
| Monitor | |
| | |
| 8.1 Overvie w | 54 |
| 8.1.1 What You Can Do in this Chapter | 54 |
| 8.2 What You Need to Know | 54 |
| 8.3 Ne two rk Sta tus | 55 |
| 8.3.1 Port Statistic s Graph | |
| 8.4 Radio List | |
| 8.4.1 AP Mode Radio Information | |
| 8.5 Station List | |
| 8.6 WDS Link Info | |
| 8.7 Detected Device | 63 |

| Chapter 9 89 Network. 69 9.1 Overview 69 9.2 P Setting 69 9.3 VIAN 71 9.4 NCC Discovery 73 Chapter 10 75 Wire ss 75 10.1 Overview 75 10.1 Overview 75 10.1 Overview 75 10.1 Overview 75 10.1.1 What You Can Do in this Chapter 75 10.1.2 What You Need to Know 76 10.2 AP Management 76 10.3 Nogue AP 79 10.3.1 Add/Elit Rogue/Friendly List 83 10.4 DCS 83 10.5 Technic al Reference 86 11.1 Overview 86 11.1 Overview 86 11.1 Overview 86 11.1 What You Can Do in this Chapter 86 11.1 What You Can Do in this Chapter 86 11.2 Kadt/Bit User Authentic ation Time out Setting s 91 11.3 Setting 89 12.1 Overview 93 12.1 Overview 93 12.1 Overview <td< th=""><th>8.8 View Log</th><th></th></td<> | 8.8 View Log | |
|---|--|----|
| Network 69 9.1 Overview 69 9.2 IP Setting 69 9.3 VIAN 71 9.4 NCC Discovery 73 Chapter 10 73 Wire less 75 10.1 Overview 75 10.1 Overview 75 10.1 Overview 75 10.1.1 What You Can Do in this Chapter 75 10.1.2 What You Can Do in this Chapter 75 10.1.2 What You Can Do in this Chapter 76 10.2 AP Management 76 10.3 Rogue AP 79 10.3 I Add/Edit Rogue/Friendly List 83 10.4 DCS 83 10.5 The chine al Reference 84 Chapter 11 User User 86 11.1 Overview 86 11.1 Overview 86 11.1 What You Can Do in this Chapter 86 11.1 What You Can Do in this Chapter 86 11.1 What You Can Do in this Chapter 86 11.2 Setting 87 12.3 Exiting 89 13.4 Edit User Authentic ation Time out Settings 91 <th>Chapter 9</th> <th></th> | Chapter 9 | |
| 9.1 Overview 69 9.1.1 What You Can Do in this Chapter 69 9.2 IP Setting 69 9.3 VIAN 71 9.4 NCC Disc overy 73 Chapter 10 75 Wire less 75 10.1 Overview 75 10.1.2 What You Can Do in this Chapter 75 10.1.2 What You Need to Know 76 10.2 AP Manage ment 76 10.3 Rogue AP 79 10.3 I. Add/Edit Rogue/Fiendly List 83 10.4 DCS 83 10.5 The bink al Reference 84 Chapter 11 86 User 86 11.1 Overview 86 11.1 Overview 86 11.1 Overview 86 11.1 Overview 86 11.2 What You Need To Know 86 11.2 What You Need To Know 87 11.3 Editi User 87 11.3 Editi User 87 11.3 Editi User Authentic ation Time out Settings 93 12.1 Overview 93 12.1 What You Can Do in this Chapter 93 < | Ne two rk | |
| 9.1.1 What You Can Do in this Chapter 69 9.2 P Setting 69 9.3 VIAN 71 9.4 NCC Discovery 73 Chapter 10 Wire less 75 10.1 Overvie w 75 10.1.1 What You Can Do in this Chapter 75 10.1.2 What You Red to Know 76 10.2 AP Manage ment 76 10.3 Rogue AP 79 10.3.1 Add/Elit Rogue/Friendly List 83 10.5 Technical Reference 84 Chapter 11 User Setting 11.1 Overview 86 11.1.1 What You Can Do in this Chapter 86 11.1.2 What You Can Do in this Chapter 86 11.1.2 What You Can Do in this Chapter 86 11.2 User Summary 87 11.3 Editit User 89 11.3.1 Editit User Authentic at ion Thme out Settings 91 12.1 Overview 93 | 9.1 Overview | |
| 9.2 IP Setting 69 9.3 VIAN 71 9.4 NCC Discovery 73 Chapter 10 75 Wire less 75 10.1 Overview 75 10.1.1 What You Can Do in this Chapter 75 10.1.2 What You Need to Know 76 10.2 AP Management 76 10.3 Rogue AP 79 10.3.1 Add/Edit Rogue/Friendly List 83 10.4 DCS 83 10.5 Technic al Reference 84 Chapter 11 86 User 86 11.1.1 What You Can Do in this Chapter 86 11.1.1 What You Can Do in this Chapter 86 11.1.2 What You Need To Know 86 11.2 User Summary 87 11.3 Edit User Authentic ation Time out Settings 91 11.3 Edit User Authentic ation Time out Settings 93 12.1 Overview 93 | 9.1.1 What You Can Do in this Chapter | |
| 9.3 VIAN 71 9.4 NCC Discovery 73 Chapter 10 75 10.1 Overview 75 10.1.1 What You Can Do in this Chapter 75 10.1.2 What You Need to Know 76 10.2 AP Management 76 10.3 Rogue AP 79 10.3.1 Add/Edit Rogue/Friendly List 83 10.4 DCS 83 10.5 Technical Reference 84 Chapter 11 86 11.1 Overview 86 11.1.1 What You Can Do in this Chapter 86 11.1.1 What You Can Do in this Chapter 86 11.2 User Summary 87 11.2 User Summary 87 11.3 E ting 89 11.3.1 Edit User Authentic ation Time out Settings 91 11.3.1 Edit User Can Do in this Chapter 93 12.1 Overview 93 12.1 Add/Edit Radio Po file 93 <td>9.2 IP Setting</td> <td></td> | 9.2 IP Setting | |
| 9.4 NCC Discovery 73 Chapter 10 75 Wire less 75 10.1 Overview 75 10.1.1 What You Can Do in this Chapter 75 10.1.2 What You Need to Know 76 10.2 AP Manage ment 76 10.3 Rog ue AP 79 10.3.1 Add/Edit Rog ue/Piendly List 83 10.4 DCS 83 10.5 Technical Reference 84 Chapter 11 86 User 86 11.1 Overview 86 11.1.1 What You Can Do in this Chapter 86 11.1.2 What You Need T& Know 86 11.2 User Sum mary 87 11.3 Edit User Authentic ation Time out Settings 91 11.3 Edit User Authentic ation Time out Settings 93 12.1 Overview 93 12.1 Overview 93 12.1.1 What You Need T& Know 93 12.1 Overview 93 12.1 Overview 93 12.1 Overview 93 12.1.1 What You Can Do in this Chapter 93 12.1 Overview 93 12.2.1 Add/Edit Ra | 9.3 VIAN | |
| Chapter 10 75 Wire less 75 10.1 Overvie w 75 10.1.1 What You Can Do in this Chapter 75 10.1.2 What You Need to Know 76 10.2 AP Manage ment 76 10.3 Rogue AP 79 10.3.1 Add/Edit Rogue/Piendly List 83 10.4 DCS 83 10.5 Technical Reference 84 Chapter 11 86 User 86 11.1 Overvie w 86 11.1.1 What You Can Do in this Chapter 86 11.1.2 What You Need Te Know 86 11.2 User Summary 87 11.2 User Summary 87 11.3 Edit User Authentic ation Time out Settings 91 11.3 Tell it User Authentic ation Time out Settings 91 12.1 Overvie w 93 12.1.2 What You Need Te Know 12.1 Overvie w 93 12.1.2 What You Need Te Know 12.1 Overvie w 93 12.1.3 Tell it User Authentic ation Time out Settings 91 12.3 Sting 93 12.1.1 What You Can Do in this Chapter 93 12.4 Protofic 93 12.1.2 What You Need Te Kn | 9.4 NCC Disc overy | |
| Wire less 75 10.1 Overvie w 75 10.1.1 What You Can Do in this Chapter 75 10.1.2 What You Need to Know 76 10.2 AP Management 76 10.3 Rogue AP 79 10.3.1 Add/Edit Regue/Friendly List 83 10.4 DCS 83 10.5 Technic al Reference 84 Chapter 11 86 User 86 11.1 Overvie w 86 11.1.1 What You Can Do in this Chapter 86 11.1.2 What You Can Do in this Chapter 86 11.2.1 Add/Edit User 87 11.3 Setting 89 11.3.1 Edit User Authentic ation Time out Setting s 91 Chapter 12 93 AP Profile 93 12.1 Overvie w 93 12.1 What You Can Do in this Chapter 93 12.1.1 What You Can Do in this Chapter 93 12.1.2 What You Need To Know 93 12.1.1 What You Can Do in this Chapter 93 12.1.2 What You Need To Know 93 12.1.1 What You Can Do in this Chapter 93 12.1.2 What You Need T | Chapter 10 | |
| 10.1 Overview 75 10.1.1 What You Can Do in this Chapter 75 10.1.2 What You Need to Know 76 10.2 AP Management 76 10.3 Rogue AP 79 10.3.1 Add/Edit Rogue/Friendly List 83 10.4 DCS 83 10.5 Technic al Reference 84 Chapter 11 86 User 86 11.1 Overview 86 11.1.1 What You Can Do in this Chapter 86 11.1.2 What You Need To Know 86 11.2 User Summary 87 11.2 I Add/Edit User 87 11.3 Setting 89 11.3 L Edit User Authentic a tion Time out Settings 91 Chapter 12 93 AP Profile 93 12.1 Doerview 93 12.1 What You Can Do in this Chapter 93 12.1 Overview 93 12.1.1 What You Can Do in this Chapter 93 12.1.2 What You Need To Know 93 12.1.1 What You Can Do in this Chapter 93 12.1.2 What You Need To Know 93 12.2.1 Add/Edit Radio Profile 94 | Wire less | |
| 10.1.1 What You Can Do in this Chapter 75 10.1.2 What You Need to Know 76 10.2 AP Management 76 10.3 Rogue AP 79 10.3.1 Add/Edit Rogue/Friendly List 83 10.4 DCS 83 10.5 Technical Reference 84 Chapter 11 User 11.1 Overview 86 11.1.1 What You Can Do in this Chapter 86 11.2 Wrat You Need To Know 86 11.2 User Summary 87 11.2 User Summary 87 11.3 Setting 89 11.3 Edit User Authentic ation Time out Setting s 91 Chapter 12 AP Profile 93 12.1 Overview 93 12.1.1 What You Can Do in this Chapter 93 12.1 Overview 93 12.1.2 What You Can Do in this Chapter 93 12.1.2 What You Can Do in this Chapter 93 12.1.2 What You Can Do in this Chapter 93 12.1.2 What You Can Do in this Chapter 93 12.1.3 SED 94 12.3 SED | 10.1 Overvie w | |
| 10.1.2 What You Need to Know 76 10.2 AP Management 76 10.3 Rogue AP 79 10.3.1 Add/Edit Rogue/Friendly List 83 10.4 DCS 83 10.5 Te chnic al Reference 84 Chapter 11 User number of the second seco | 10.1.1 What You Can Do in this Chapter | |
| 10.2 AP Management 76 10.3 Rogue AP 79 10.3.1 Add/Edit Rogue/Friendly List 83 10.4 DCS 83 10.5 Technic al Reference 84 Chapter 11 User Set 11.1 Overview 11.1 Overview 11.1 Overview 11.1 What You Can Do in this Chapter 11.2 What You Need Te Know 11.2 User Summary 11.2 User Summary 12.1 Add/Edit User 13.3 Setting 12.1 Overview 12.1 Overview 12.1 Overview 12.1 Overview 12.1 What You Can Do in this Chapter 93 12.1.1 What You Can Do in this Chapter 93 12.1.2 What You Need Te Know 12.1.2 What You Can Do in this Chapter 93 12.1.2 What You Can Do in this Chapter 93 12.1.1 What You Can Do in this Chapter | 10.1.2 What You Need to Know | |
| 10.3 Rogue AP 79 10.3.1 Add/Edit Rogue/Priendly List 83 10.4 DCS 83 10.5 Technic al Reference 84 Chapter 11 User User 86 11.1 Overview 86 11.1.2 What You Can Do in this Chapter 86 11.2 What You Need To Know 86 11.2.1 Add/Edit User 87 11.3 So tting 89 11.3.1 Edit User Authentic ation Time out Setting s 91 Chapter 12 AP Profile 93 12.1 Overview 93 12.1.2 What You Can Do in this Chapter 93 12.1.1 What You Can Do in this Chapter 93 12.1.2 What You Need To Know 93 12.1.2 What You Need To Know 93 12.2 Radio 94 12.2.1 Add/Edit Radio Profile 95 12.3 SSID 100 12.3.1 SSID List 101 12.3.2 Add/Edit SSID Profile 102 12.4 Add/Edit Sec unity Profile 105 12.4.1 Add/Edit S | 10.2 AP Management | |
| 10.3.1 Add/Edit Rogue/Friendly List 83 10.4 DCS 83 10.5 Te chnic al Reference 84 Chapter 11 User User 86 11.1 Overview 86 11.1.1 What You Can Do in this Chapter 86 11.1.2 What You Need To Know 86 11.2.1 What You Need To Know 87 11.3 Setting 89 11.3.1 Edit User Authentic ation Time out Setting s 91 Chapter 12 AP Profile AP Profile 12.1 Overvie w 12.1 Overvie w 12.1 What You Can Do in this Chapter 93 12.1.2 What You Need To Know 12.2 Radio 12.1 What You Need To Know 12.2 Radio 100 12.1 SSID 100 12.1 SSID 12.2 Radio 12.3 SSID 100 12.3 SSID | 10.3 Rogue AP | |
| 10.4 DCS 83 10.5 Te chnic al Reference 84 Chapter 11 User 11.1 Overview 86 11.1.1 What You Can Do in this Chapter 86 11.1.2 What You Need To Know 86 11.2.1 What You Need To Know 86 11.2.1 What You Need To Know 87 11.2.1 Setting 87 11.3.1 Edit User 87 11.3.1 Edit User Authentic ation Time out Setting s 91 Chapter 12 AP Profile 93 12.1 Overview 93 12.1.2 What You Can Do in this Chapter 93 12.1.2 What You Can Do in this Chapter 93 12.1.2 What You Need To Know 93 12.1.2 What You Need To Know 93 12.2.1 Add/Edit Radio Profile 95 12.3 SSID 100 12.3 SSID List 101 12.3.2 Add/Edit SSID Profile 102 12.4 Add/Edit SSID Profile 102 12.4 Add/Edit SSID Profile 105 12.4.1 Add/Edit Sec unity Profile 105 | 10.3.1 Add/Edit Rogue/Friendly List | |
| 10.5 Te chnic al Reference 84 Chapter 11 86 11.1 Overview 86 11.1.1 What You Can Do in this Chapter 86 11.1.2 What You Need To Know 86 11.2.1 Vadd/Edit User 87 11.3.1 Edit User Authentic ation Time out Setting s 91 11.3.1 Edit User Authentic ation Time out Setting s 91 Chapter 12 93 AP Profile 93 12.1 Overview 93 12.1.1 What You Can Do in this Chapter 93 12.1 Overview 93 12.1.2 What You Can Do in this Chapter 93 12.1.3 Setting 93 12.1.4 What You Can Do in this Chapter 93 12.1.3 SiBD Iist 101 12.3 SSID 100 12.3.1 SSID List 101 12.3.2 Add/Edit SSID Profile 102 12.4 1 Add/Edit Sc urity Profile 105 | 10.4 DCS | |
| Chapter 11 User | 10.5 Te c hnic a l Re fe re nc e | |
| Use r | Chanter 11 | |
| 11.1 Overview 86 11.1.1 What You Can Do in this Chapter 86 11.1.2 What You Need To Know 86 11.2 User Summary 87 11.2 User Summary 87 11.2.1 Add/Edit User 87 11.3 Setting 89 11.3.1 Edit User Authentic ation Time out Settings 91 Chapter 12 AP Profile 12.1 Overview 93 12.1.1 What You Can Do in this Chapter 93 12.1.2 What You Need To Know 93 12.1.2 What You Need To Know 93 12.2.1 Add/Edit Ra dio Profile 95 12.3 SSID 100 12.3.1 SSID List 101 12.3.2 Add/Edit SSID Profile 102 12.4 Sec urity List 105 12.4.1 Add/Edit Sec urity Profile 105 | Use r | |
| 11.1 Overview 86 11.2.1 What You Can Do in this Chapter 86 11.1.2 What You Need To Know 86 11.2 User Summary 87 11.2.1 Add/Edit User 87 11.3 Setting 89 11.3.1 Edit User Authentic ation Time out Setting s 91 Chapter 12 AP Profile 12.1 Overview 93 12.1.1 What You Can Do in this Chapter 93 12.1.1 What You Can Do in this Chapter 93 12.2.2 Radio 94 12.3 SSID 100 12.3.1 SSID List 101 12.3.2 Add/Edit SSID Pro file 102 12.4 1 Add/Edit Se curity Pro file 105 | 11.1 Overview | 86 |
| 11.1.2 What You Need To Know 86 11.2 Use r Summary 87 11.2.1 Add/Edit Use r 87 11.3 Setting 89 11.3.1 Edit Use r Authentic ation Time out Setting s 91 Chapter 12 AP Profile 12.1 Overview 93 12.1.1 What You Can Do in this Chapter 93 12.1.2 What You Need To Know 93 12.2.1 Add/Edit Ra dio Profile 93 12.2.1 Add/Edit Ra dio Profile 95 12.3 SSID 100 12.3.1 SSID List 101 12.3.2 Add/Edit SSID Profile 102 12.4 Sec urity List 105 12.4.1 Add/Edit Sec urity Profile 105 | 11.1.1 What You Can Do in this Chapter | 86 |
| 11.2 Use r Sum mary 87 11.2.1 Add/Ed it Use r 87 11.3 Se tting 89 11.3.1 Ed it Use r Authentic a tion Time out Setting s 91 Chapter 12 AP Profile 12.1 Overvie w 93 12.1.1 What You C an Do in this Chapter 93 12.1.2 What You Need To Know 93 12.2.1 Add/Ed it Radio Profile 95 12.3 SSID 100 12.3.1 SSID List 101 12.3.2 Add/Ed it SSID Pro file 102 12.4 Sec urity List 105 12.4.1 Add/Ed it Sec urity Pro file 105 | 11.1.2 What You Need To Know | 86 |
| 11.2.1 Add/Ed it Use r 87 11.3 Setting 89 11.3.1 Ed it Use r Authentic ation Time out Setting s 91 Chapter 12 AP Profile 12.1 Overvie w 93 12.1.1 What You Can Do in this Chapter 93 12.1.2 What You Need To Know 93 12.2.2 Radio 94 12.2.1 Add/Ed it Radio Profile 95 12.3 SSID 100 12.3.1 SSID List 101 12.3.2 Add/Ed it SSID Pro file 102 12.4 Sec unity List 105 12.4.1 Add/Ed it Sec unity Pro file 105 | 11.2 User Summary | 87 |
| 11.3 Setting 89 11.3.1 Edit User Authentic ation Time out Setting s 91 Chapter 12 AP Profile 93 12.1 Overview 93 12.1.1 What You Can Do in this Chapter 93 12.1.2 What You Need To Know 93 12.2 Radio 94 12.2.1 Add/Edit Radio Profile 95 12.3 SSID 100 12.3.1 SSID List 101 12.3.2 Add/Edit SSID Profile 102 12.4 Sec urity List 105 12.4.1 Add/Edit Sec urity Profile 105 | 11.2.1 Ad d/Ed it Use r | |
| 11.3.1 Ed it Use r Authentic ation Time out Setting s 91 Chapter 12 AP Pro file 93 12.1 Overview 93 12.1.1 What You Can Do in this Chapter 93 12.1.2 What You Need To Know 93 12.2 Radio 94 12.2.1 Add/Ed it Radio Pro file 95 12.3 SSID 100 12.3.1 SSID List 101 12.3.2 Add/Ed it SSID Pro file 102 12.4 Sec unity List 105 12.4.1 Add/Ed it Sec unity Pro file 105 | 11.3 Setting | |
| Chapter 12 AP Profile 93 12.1 Overview 93 12.1.1 What You Can Do in this Chapter 93 12.1.2 What You Need To Know 93 12.2 Radio 94 12.2.1 Add/Ed it Radio Profile 95 12.3 SSID 100 12.3.1 SSID List 101 12.3.2 Add/Ed it SSID Profile 102 12.4 Sec urity List 105 12.4.1 Add/Ed it Sec urity Profile 105 | 11.3.1 Ed it Use r Authentic ation Time out Settings | |
| AP Profile 93 12.1 Overview 93 12.1.1 What You Can Do in this Chapter 93 12.1.2 What You Need To Know 93 12.2 Radio 94 12.2.1 Add/Edit Radio Profile 95 12.3 SSID 100 12.3.1 SSID List 101 12.3.2 Add/Edit SSID Profile 102 12.4 Sec urity List 105 12.4.1 Add/Edit Sec urity Profile 105 | Chanter 12 | |
| 12.1 Overview 93 12.1.1 What You Can Do in this Chapter 93 12.1.2 What You Need To Know 93 12.2 Radio 94 12.2.1 Ad d/Ed it Radio Pro file 95 12.3 SSID 100 12.3.1 SSID List 101 12.3.2 Ad d/Ed it SSID Pro file 102 12.4 Sec urity List 105 12.4.1 Ad d/Ed it Sec urity Pro file 105 | AP Pro file | |
| 12.1.1 What You Can Do in this Chapter 93 12.1.2 What You Need To Know 93 12.2 Ra dio 94 12.2.1 Ad d/Ed it Ra dio Pro file 95 12.3 SSID 100 12.3.1 SSID List 101 12.3.2 Ad d/Ed it SSID Pro file 102 12.4 Se c urity List 105 12.4.1 Ad d/Ed it Se c urity Pro file 105 | 12.1 Overview | 93 |
| 12.1.2 What You Need To Know 93 12.2 Ra dio 94 12.2.1 Ad d/Ed it Ra dio Pro file 95 12.3 SSID 100 12.3.1 SSID List 101 12.3.2 Ad d/Ed it SSID Pro file 102 12.4 Se c urity List 105 12.4.1 Ad d/Ed it Se c urity Pro file 105 | 12.1.0 torre w | 93 |
| 12.2 Ra dio | 12.1.2 What You Need To Know | 93 |
| 12.2.1 Ad d/Ed it Ra d io Pro file 95 12.3 SSID 100 12.3.1 SSID List 101 12.3.2 Ad d/Ed it SSID Pro file 102 12.4 Se c urity List 105 12.4.1 Ad d/Ed it Se c urity Pro file 105 | 12.2 Badio | |
| 12.3 SSID 100 12.3.1 SSID List 101 12.3.2 Ad d/Ed it SSID Pro file 102 12.4 Se c urity List 105 12.4.1 Ad d/Ed it Se c urity Pro file 105 | 12.2.1 Add/Edit Badio Profile | 95 |
| 12.3.1 SSID List 101 12.3.2 Ad d/Ed it SSID Pro file 102 12.4 Se c urity List 105 12.4.1 Ad d/Ed it Se c urity Pro file 105 | 12.3 SSID | |
| 12.3.2 Ad d/Ed it SSID Pro file 102 12.4 Se c urity List 105 12.4.1 Ad d/Ed it Se c urity Pro file 105 | 12.3.1 SSID List | |
| 12.4 Se c urity List | 12.3.2 Add/Edit SSID Profile | |
| 12.4.1 Ad d/Ed it Se c unity Pro file | 12.4 Security List | |
| | 12.4.1 Add/Edit Security Profile | |

NWA50AX Use r's Guide

| 12.5 MAC Filte r List | 115 |
|--|-----|
| 12.5.1 Add/Edit MAC Filter Profile | |
| | |
| Unapter 13 MON Profile | 117 |
| | |
| 13.1 Overvie w | |
| 13.1.1 What You Can Do in this Chapter | 117 |
| 13.2 MON Pro file | |
| 13.2.1 Add/Edit MON Profile | |
| Chapter 14 | |
| WDS Pro file | 120 |
| 14.1 Ove wie w | 120 |
| 14.1.1 What You Can Do in this Chanter | 120 |
| 14.2 WDS Pro file | |
| 14.2.1 Add/Edit WDS Pro file | |
| | |
| Chapter 15 | 100 |
| C e runc a te s | 122 |
| 15.1 Overvie w | |
| 15.1.1 What You Can Do in this Chapter | |
| 15.1.2 What You Need to Know | |
| 15.1.3 Venifying a Centificate | |
| $15.2 { m ~My~Ce}$ rtific a te s | |
| 15.2.1 Add My Certific ates | |
| 15.2.2 Ed it My Certific a tes | |
| 15.2.3 Import Certific a tes | 131 |
| 15.3 Truste d Certific a tes | |
| 15.3.1 Ed it Truste d Certific a tes | |
| 15.3.2 Import Trusted Certific ates | |
| 15.4 Te chnic al Reference | |
| Chapter 16 | |
| System | |
| | 100 |
| | |
| 16.1.1 What You Can Do in this Chapter | |
| 16.2 Ho st Name | |
| | |
| 16.3.1 Pre-defined NIP time Servers List | |
| 16.3.2 Time Server Sync hronization | |
| 10.4 WWW Uverview | |
| 16.4.1 Service Access Limitations | |
| 16.4.2 System Imeout | |

NWA50AX Use r's Guide

| 16.4.3 HTPS | |
|---|-----|
| 16.4.4 Configuring WWW Service Control | |
| 16.4.5 HTTPS Example | |
| 16.5 SSH | |
| 16.5.1 How SSH Works | |
| 16.5.2 SSH Implementation on the Zyxel Device | |
| 16.5.3 Requirements for Using SSH | |
| 16.5.4 Configuring SSH | |
| 16.5.5 Examples of Secure Telnet Using SSH | |
| 16.6 FIP | |
| Chapter 17 | |
| Log and Report | 157 |
| 17.1 Overvie w | |
| 17.1.1 What You Can Do In this Chapter | |
| 17.2 Log Setting | |
| 17.2.1 Log Setting Screen | |
| 17.2.2 Ed it System Log Settings | 159 |
| 17.2.3 Edit Remote Server | |
| 17.2.4 Ac tive Log Summary | |
| Chapter 18 | |
| File Manager | 167 |
| 18.1 Overvie w | |
| 18.1.1 What You Can Do in this Chapter | |
| 18.1.2 What you Need to Know | |
| 18.2 Configuration File | |
| 18.2.1 Example of Configuration File Download Using FIP | |
| 18.3 Firmware Package | |
| 18.3.1 Example of Firm ware Up load Using FTP | |
| 18.4 Shell Script | |
| Chapter 19 | |
| Dia g no stic s | |
| 19.1 Overview | |
| 19.1.1 What You Can Do in this Chapter | |
| 19.2 Diagnostics | |
| 19.3 Remote Capture | |
| Chapter 20 | |
| IEDs | |
| 20.1 Overview | |
| 20.1.1 What You Can Do in this Chapter | |

| 20.2 Suppression Screen | |
|--|-----|
| 20.3 Locator Screen | |
| | |
| Chapter 21 Reheat | 189 |
| | |
| 21.1 Overview | |
| 21.1.1 What You Need To Know | |
| 21.2 Reboot | |
| Chapter 22 | |
| Shutdown | |
| | 104 |
| | |
| 22.1.1 what you need to know | |
| 22.2 Shutu 0 w h | |
| | |
| Part II: Local Configuration in Cloud Mode | |
| | |
| Chapter 23 | 100 |
| | |
| 23.1 Overvie w | |
| 23.2 Cloud Mode Web Configurator Screens | |
| 23.3 Da shb o a rd | |
| Chapter 24 | |
| Ne twork | |
| | |
| 24.1 Overvie w | |
| 24.1.1 What You Can Do in this Chapter | |
| 24.2 IP Setting | |
| 24.3 VIAN | |
| Chapter 25 | |
| Maintenance | |
| 25.1 Overvie w | |
| 25.1.1 What You Can Do in this Chapter | |
| 25.2 Shell Script | |
| 25.3 Diagnostics | |
| 25.4 View Log | |
| | |

| Part III: Appendices and | l Trouble shooting | |
|--------------------------|--------------------|--|
| | | |

Chapter 26

| The ubleshooting | |
|--|-----|
| 26.1 Overview | |
| 26.2 Power, Hardware Connections, and LED | |
| 26.3 ZyxelDevice Management, Access, and Login | |
| 26.4 Internet Access | |
| 26.5 WiFi Ne two rk | |
| 26.6 Resetting the Zyxel Device | |
| 26.7 Getting More Throubleshooting Help | |
| Appendix A Importing Certificates | |
| Appendix B IPv6 | |
| Appendix C Customer Support | |
| Appendix D Legal Information | |
| Index | 251 |

C HAPTER 1 Introduction

1.1 Overview

The Zyxel Device can be managed in one of the following methods: remote management through Nebula Control Center (NCC) or local management in Standalone Mode. The Zyxel Device runs in standalone mode by default, but it is recommended to use NCC management if it is available for your device. For more information about Access Point (AP) management, see Section 2.1 on page 20.

Use the ZyxelDevice to set up a wireless network with other $E\!E\!E\,802.11a/b/g/n/ac/ax$ compatible devices in either 2.4 GHz and 5 GHz networks or both at the same time.

When two or more APs are interconnected, this network is called a Wireless Distribution System (WDS). See Section 1.2.2 on page 13 for more information on root and repeater APs and how to set them up.

1.2 Zyxel Device Roles

This section describes some of the different roles that your Zyxel Device can take up within a network. Not all roles are supported by all models (see Section 1.4 on page 18). The Zyxel Device can serve as a:

- Access Point (AP) This is used to a llow wire less clients to connect to the Internet.
- Radio Frequency (RF) monitor An RF monitor searches for rogue APs to help eliminate network threats if it supports monitor mode and rogue APs detection/containment. An RF monitor cannot simultaneously act as an AP.
- Root AP A root AP connects to the gate way or switch through a wired Ethemet connection and has wire less repeaters connected to it to extend its range.
- Wire less repeater A wire less repeater wire lessly connects to a root AP and extends the network's wire less range.

The following figure shows a network setup that uses these different roles to create a secure Wireless Distribution System (WDS). The root AP (\mathbf{Y}) is connected to a network with Internet access and has a wireless repeater (\mathbf{X}) connected to it to expand the wireless network's range. Clients (\mathbf{A} , \mathbf{B} , and \mathbf{C}) can access the wired network through the wireless repeater and/or root AP.

If a client (D) tries to set up his own AP (R) with weak security settings, the network becomes exposed to threats. The RF monitor (M) scans the area to detect all APs, which can help the network administrator discover these rogue APs and remove them or use the NXC to quarantine them.



Figure 1 Sample Network Setup

1.2.1 RootAP

In Root AP mode, you can have multiple SSIDs active for regular wireless connections and one SSID for the connection with a repeater (repeater SSID). Wireless clients can use either SSID to associate with the Zyxel Device in Root AP mode. A repeater must use the repeater SSID to connect to the Zyxel Device in Root AP mode.

When the Zyxel Device is in Root AP mode, repeater security between the Zyxel Device and other repeaters is independent of the security between the wireless clients and the AP or repeater. When repeater security is enabled, both APs and repeaters must use the same pre-shared key. See Section 10.2 on page 76 and Section 14.2 on page 120 formore details.

Unless specified, the term "security settings" refers to the traffic between the wireless clients and the AP. At the time of writing, repeater security is compatible with the Zyxel Device only.

1.2.2 Wire less Repeater

Using Repeater mode, your Zyxel Device can extend the range of the WIAN. In the figure below, the Zyxel Device in Repeater mode (Z) has a wireless connection to the Zyxel Device in Root AP mode (X) which is connected to a wired network and also has a wireless connection to another Zyxel Device in Repeater mode (Y) at the same time. Z and Y act as repeaters that forward traffic between associated wireless clients and the wired IAN. Clients A and B access the AP and the wired network behind the AP through repeaters Z and Y.



Figure 2 Repeater Application

When the Zyxel Device is in Repeater mode, repeater security between the Zyxel Device and other repeater is independent of the security between the wireless clients and the AP or repeater. When repeater security is enabled, both APs and repeaters must use the same pre-shared key. See Section 10.2 on page 76 and Section 14.2 on page 120 formore details.

For NCC managed devices, you only need to enable **AP Smart Mesh** to automatically create wireless links between APs. See the NCC User's Guide formore details.

To set up a WDS in standalone mode APs, do the following steps. You should already have the root AP set up (see the Quick Start Guide for hardware connections).

- 1 Go to Configuration > Object > WDS Profile in your root AP Web Configurator and click Add.
- 2 Enter a profile name, an SSID for the WDS, and a pre-shared key.
- 3 Do steps 1 and 2 for the wireless repeater using the same SSID and pre-shared key.
- 4 Once the security settings of peer sides match one another, the connection between the root and repeater Zyxel Devices is made.

To set up a WDS in NXC managed Zyxel Devices, see the NXC User's Guide.

1.2.3 Radio Frequency (RF) Monitor

The Zyxel Device can be set to work as an RF monitor to discover nearby Access Points. The information it obtains from other APs is used to tag possible rogue APs and quarantine them if the Zyxel Device is managed by the NXC (see Section 2.2 on page 22). If the Zyxel Device's radio setting is set to MON Mode (RF Monitor mode), it will serve as a dedicated RF monitor and its AP clients are disconnected.

The models that do not support **MON Mode** support **Rogue AP Detection** (see Section 10.3 on page 79). **Rogue AP Detection** allows the AP to scan all channels similar to **MON Mode** except that the Zyxel Device still works as an AP while it scans the environment for wireless signals. To see which Zyxel Devices support the RF Monitor feature, see Section 1.4 on page 18.

The Zyxel Device in MON Mode scans a range of WiFichannels that you specify in a MON Profile, either in the 2.4 GHz or 5 GHz band. To scan both bands, you need to set both radio 1 and radio 2 in MON Mode. Once a rogue AP is detected, the network administrator can manually change the network settings to limit its access to the network using its MAC address or have the device physically removed. If the Zyxel Device is managed by an NXC, the network administrator can also use **Rogue AP Containment** through the NXC.

MON Mode in Standalone Mode

To use an RF monitor in standalone mode, do the following steps:

- 1 Create a MON Profile in Configuration > Object > MON Profile > Add. Specify a Channel dwell time to determine how long the RF monitor scans a specific channel before moving to the next one.
- 2 To scan all 2.4 GHz and 5 GHz channels, select auto in Scan Channel Mode. Make sure that the Activate check box is selected and click OK.
- 3 Go to the Configuration > Wireless > APManagement screen and set Radio 1 OPMode (2.4 GHz) and/or Radio 2 OPMode (5 GHz) to MON Mode.
- 4 Select the Radio 1(2) Profile that you created in the previous step. Make sure that the Radio 1(2) Activate check box is selected and click Apply.
- 5 Go to Monitor > Wire less > Detected Device to see a list of APs scanned by the RF monitor.
- 6 Select an AP or APs in the list and click Mark as Rogue AP or Mark as Friendly AP.

MON Mode in NXC-Managed Zyxel Devices

For NXC-managed Zyxel Devices, do the following steps in the NXC Web Configurator.

- 1 Create a MON Profile in CONFIGURATION > Object > MON Profile > Add. Specify a Channel dwell time to determine how long the RF monitor scans a specific channel before moving to the next one.
- 2 To scan all 2.4 GHz and 5 GHz channels, select auto in Scan Channel Mode. Make sure that the Activate check box is selected and click OK.
- 3 Go to the CONFIGURATION > Wireless > AP Management > Mgmt. AP list > Edit screen and/or set Radio 1 OP Mode (2.4 GHz) and Radio 2 OP Mode (5 GHz) to MON Mode.
- 4 Select the Radio 1(2) Profile that you created in the previous step. Select Override Group Radio Setting and click OK.
- 5 Go to MONITOR > Wire less > Detected Device to see a list of APs scanned by the RF monitor.
- 6 Select an AP or APs in the list and click Mark as Rogue AP or Mark as Friendly AP.

7 To quarantine a rogue AP, go to CONFIGURATION > Wireless > Rogue AP, select the APs you want to quarantine, and click Containment. Make sure the Enable Rogue AP Containment check box is selected, and click Apply.

1.3 Sample Feature Applications

This section describes some possible scenarios and topologies that you can set up using your Zyxel Device.

1.3.1 MBSSID

A Basic Service Set (BSS) is the set of devices forming a single wireless network (usually an access point and one or more wireless clients). The Service Set IDentifier (SSID) is the name of a BSS. In Multiple BSS (MBSSID) mode, the Zyxel Device provides multiple virtual APs, each forming its own BSS and using its own individual SSID profile.

You can configure multiple SSID profiles, and have all of them active at any one time.

You can assign different wire less and security settings to each SSID profile. This allows you to compartmentalize groups of users, set varying access privileges, and prioritize network traffic to and from certain BSSs.

To the wire less clients in the network, each SSID appears to be a different access point. As in any wire less network, clients can associate only with the SSIDs for which they have the correct security setting s.

For example, you might want to set up a wire less network in your office where Internet telephony (VoIP) users have priority. You also want a regular wire less network for standard users, as well as a 'guest' wire less network for visitors. In the following figure, **VoIP_SSID** users have QoSpriority, **SSID01** is the wire less network for standard users, and **Guest_SSID** is the wire less network for guest users. In this example, the guest user is forbidden access to the wire d Land Area Network (LAN) behind the AP and can access only the Internet.



1.3.2 Dual-Radio

Some of the Zyxel Device models are equipped with dual wireless radios. This means you can configure two different wireless networks to operate simultaneously.

Note: A different channel should be configured for each WLAN interface to reduce the effects of radio interference.

You could use the 2.4 GHz band for regular Internet surfing and downloading while using the 5 GHz band for time sensitive traffic like high-definition video, music, and gaming.





1.4 Zyxel Device Product Feature

The following table lists the features of the Zyxel Device..

|--|

| FEATURES | NWA50AX |
|---|--|
| Supported Wire less Standards | IEEE 802.11a IEEE802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11a c IEEE802.11a x |
| Supported Frequency Bands | 2.4 G Hz 5 G Hz |
| Available Security Modes | None WEP WPA2-MIX WPA2-PSK WPA2-PSK-MIX Enhanced-open WPA3-personal |
| Number of SSID Profiles | 64 |
| Number of Wire less Radios | 2 |
| Monitor Mode & Rogue APs Containment ^A | No |
| Rogue AP Detection | Yes |
| WDS (Wire le ss Distribution System) - Root AP & Repeater Modes | Ye s |
| Tunnel Forwarding Mode | No |
| La ye r-2 Iso la tio n | No |
| Supported PoEStandards | IEEE 802.3a t |
| PowerDetection | Yes |
| Exte malAntennas | No |
| Inte mal Ante nna s | Yes |

NWA50AX Use r's Guide

| FEATURES | NWA50AX |
|--------------------------------|--------------------------------------|
| Antenna Switch | No |
| Console Port | 4-Pin Se ria l |
| LED Locator | Yes |
| LED Suppression | Yes |
| AC (AP Controller) Discovery | No |
| Ne b ula Fle x PRO | No |
| NCC Disc overy | Yes |
| 802.11r Fast Roaming Support | Yes |
| 802.11k/v Assisted Roaming | Yes |
| Blue to o th Low Energy (BLE) | No |
| USB Port for BLE | No |
| Ethe me t Storm Control | No |
| Gwunding | No |
| PowerJack | Yes |
| Maximum number of log messages | $512 \mathrm{event} \log \mathrm{s}$ |

A. For NXC managed devices only. See the NXC User's Guide for details.

C HAPTER 2 AP Management

2.1 Management Mode

The Zyxel Device is a unified AP and can be managed by the NCC or work as a standalone device. We recommend you use NCC to manage multiple APs (see the NCC User's Guide).

The following table shows the default IP addresses and firm ware upload methods for different management modes.

Table 2 Zyxel Device Management Mode Comparison

| MANAGEMENTMODE | DEFAULT IP ADDRESS | UPIO AD FIRM WARE VIA |
|-----------------------|------------------------------------|-----------------------------|
| Nebula Control Center | Dynamic | NCC Portal |
| Standalone | Dynamic or Static (192.168.1.2) | Built-in Web Config ura tor |

When the ZyxelDevice is in standalone mode and connects to a DHCP server, it uses the IP address assigned by the DHCP server. Otherwise, the ZyxelDevice uses the default static management IP address (192.168.1.2). You can use the NCC Discovery screen to allow the ZyxelDevice to be managed by the NCC.

When the Zyxel Device is managed by the NCC, it acts as a DHCP client and obtains an IP address from the NCC. It can be configured ONLY by the NCC. To change the Zyxel Device back to standalone mode, use the **Reset** button to restore the default configuration. Alternatively, you need to check the NCC for the Zyxel Device's IP address and use FIP to upload the default configuration file at conf/ system-default.conf to the Zyxel Device and reboot the device.

2.1.1 Standalone

When working in standalone mode, the Zyxel Device is configured mainly with its built-in Web Configurator. You can only connect to and set up one Zyxel Device at a time in this mode.

See Chapter 5 on page 42 for detailed information about the standalone Web Configuratorscreens.

2.1.2 Nebula Control Center

In this mode, which is also called cloud mode, you can manage and monitor the Zyxel Device through the Zyxel Nebula cloud-based network management system. This means you can manage devices remotely without the need of connecting to each device directly. It offers many features to better manage and monitor not just the Zyxel Device, but yournetwork as a whole, including supported

Note: Not all models can be managed by NCC or an AC. See Section 1.4 on page 18 to check whether your product supports the se.

switches and gateways. Yournetwork can also be managed through yoursmartphone using the Nebula Mobile app. See Section 23.1 on page 186 for an example NCC managed network topology.

NCC allows different levels of management. You can configure each device on its own or configure a set of devices together as a site. You can also monitor groups of sites called organizations, as shown below.

| Table 3 NCC Managemen | t Le ve ls |
|-----------------------|------------|
|-----------------------|------------|

| Org a niza tio n | | | |
|------------------|------------|------------|------------|
| Site | e A | Site | e B |
| Device A-1 | Device A-2 | Device B-1 | Device B-2 |

It graphically presents your device/network statistics and shows an overview of your network topology, as shown in the following figure. It also sends reports, alerts, and notifications for events, such as when a site goes offline.

Figure 5 Traffic Monitoring Graph From NCC



NWA50AX Use r's Guide

See the NCC (Nebula Control Center) User's Guide for how to configure Nebula managed devices. See Chapter 24 on page 189 if you want to change the Zyxel Device's VIAN setting or manually set its IP address.

Note: Make sure your network fire wall allows TCP ports 443, 4335, and 6667 as well as UDP port 123 so the device can connect to and sync with the NCC.

2.2 Switching Management Modes

The Zyxel Device is in standalone mode by default, with NCC and/or AC discovery enabled.

Standalone-to-NCC

Register the Zyxel Device at the NCC website and then tum on the Zyxel Device. Make sure that NCC **Discovery** is enabled (see Section 9.4 on page 73). The NCC manages the Zyxel Device automatically when it is discovered.

NCC-to-Standalone

Unregister the Zyxel Device from the NCC organization/site. Reset the Zyxel Device to factory defaults (see Section 26.6 on page 205).

2.3 ZyxelOne Network (ZON) Utility

ZON Utility is a program designed to help you deploy and manage a network more efficiently. It detects devices automatically and allows you to do basic settings on devices in the network without having to be nearit.

The ZON Utility issues requests via Zyxel Discovery Protocol(ZDP) and in response to the query, the device responds back with basic information including IP address, firmware version, location, system and model name in the same broadcast domain. The information is then displayed in the ZON Utility screen and you can perform tasks like basic configuration of the devices and batch firmware upgrade in it. You can download the ZON Utility at www.zyxel.com and install it on your computer (Windows operating system).

2.3.1 Requirements

Before installing the ZON Utility on your PC, please make sure it meets the requirements listed below.

Operating System

At the time of writing, the ZON Utility is compatible with:

- Windows 7 (both 32-bit / 64-bit versions)
- Windows 8 (both 32-bit / 64-bit versions)
- Windows 8.1 (both 32-bit / 64-bit versions)
- Window 10 (both 32-bit / 64-bit versions)

- Note: To check for your Windows operating system version, right-click on My Computer > Properties. You should see this information in the General tab.
- Note: It is suggested that you install Npcap, the packet capture library for Windows operating systems, and remove WinPcap or any other installed packet capture tools before you install the ZON utility.

Hardware

Here are the minimum hardware requirements to use the ZON Utility on your PC.

- Core i3 processor
- 2 G B RAM
- 100 MB free hard disk
- WXGA (Wide XGA 1280x800)

2.3.2 Run the ZON Utility

- 1 Double-click the ZON Utility to run it.
- 2 The first time you run the ZON Utility, you will see if your device and firm ware version support the ZON Utility. Click the OK button to close this screen.

| efter for the tob | le fo ensure your device fim | ware a supporting the 20H utility. |
|-------------------|------------------------------|---|
| Trobert | Serves and Bodier | Firmulari Detail |
| | WAC6530 series | From V4.30 • WADESOD-E AASD-8 • WADESOD-E AASE 0 • WADESOD-B AASE 0 • WADESOD-B AASE 0 • WADESOD-B AASE 0 • WADESOD-B ABSO 0 • WADESOD 0 • |
| | WAC\$300 serves | From V5.10 • WACKINGO-S ABOL B |
| | INAC6160 series | From V4.21 • WADD103D-6 AA0H.1 |
| | NXI42006-N series | From V2.23 • NWA3150-N UJA 8 • NWA3150-N UJA 8 |

If you want to check the supported models and firmware versions later, you can click the Show information about ZON icon in the upper right hand comer of the screen. Then select the Supported **model and firm ware version** link. If your device is not listed here, see the device release notes for ZON utility support. The release notes are in the firm ware zip file on the Zyxel web site.



| Eyel One Nerwork Unit | S | | | | | | | | Sol State Date |
|-----------------------|------|-----------|--------------|----------------|---------------|---------|--------------|-----|----------------|
| | ZYXE | iL. | | | | | | 4 | e 0 |
| | (8) | Θ. 0 | 9 ® | 0 📾 | (6 5) | 39 | (6) | 8 B | ۲ |
| + | | 1 | (i) | C145- | of the second | 172 | -)) | |]ece |
| | | x23100.04 | VALUE/ARTICL | NEICED | 145.145.1.1 | 50,401 | | | |
| -9 | - | 810750.24 | SA BLAND | BAIRBARAT_ | YTZ-ME.C. | (1A,555 | W12H | | |
| 20° | - | 10000000 | watel(AADE)) | 5.6410-0017.6A | (rg.iag.i.) | 1248,84 | 0108 | | _ |

3 Select a network adapter to which your supported devices are connected.



4 Click the Go button for the ZON Utility to discover all supported devices in your network.



5 The ZON Utility screen shows the devices discovered.

Figure 10 ZON Utility Screen

| Contract Site Network Lifes | | | | | - | Colored (press, res |
|-----------------------------|---------------------------------------|------------------------------|-----------------|-----------------|-----------|----------------------|
| | ZYXEL | | | | | 9 8 0 |
| | 10 20 3 | 45 80 | 6 7 79 | 12 NO | 10~ 119 | 188 180 |
| | I had a work | (many local | and dama | Consultant of | | |
| | | wanter alters | 1584-175-1883.5 | (SA)IR | | |
| | · · · · · · · · · · · · · · · · · · · | 10.2014422.00. Ex 10.00 | Tat., HEIMELL | 10,000 | 100 | |
| NOP 1 | - XOSE708-48 | VERSIANDERS, ENTRE | PAR - 1421162-1 | 1240,04 | F102 | |
| 3 | | an interaction of the basis. | anal million | abless into the | and shine | |

- 6 Select a device and then use the icons to perform actions. Some functions may not be available for your devices.
 - Note: You must know the selected device admin password before taking actions on the device using the ZON utility icons.

Figure 11 Password Prompt

| Password Authe | ntiation in the second | 100.25 |
|----------------|---|--------|
| ZYXEL | | |
| 0 | Please enter the administration postward to proceed. | |
| বি | Device | |
| | Password | |
| | | _ |
| | Carce | |

The following table describes the iconsnumbered from left to right in the ZON Utility screen.

| ICON | DESC RIPIIO N |
|-------------------------------------|---|
| 1 IP Config ura tion | Change the selected device's IP address. |
| 2 Renew IP Address | Update a DHCP-assigned dynamic IP address. |
| 3 Reboot Device | Use this ic on to restart the selected device(s). This may be useful when trouble shooting or upgrading new firm ware. |
| 4 Reset Configuration to Default | Use this ic on to reload the fac tory-default configuration file. This means that you will lose all previous configurations. |
| 5 Locator LED | Use this icon to locate the selected device by causing its locator LED to blink. |
| 6 Web GUI | Use this to access the selected device Web Configurator from your browser. You will need a usemame and password to log in. |
| 7 Firm ware Upgrade | Use this ic on to upgrade new firm ware to selected device(s) of the same model. Make sure you have downloaded the firm ware from the Zyxelwebsite to your computer and unzipped it in advance. |
| 8 Change Password | Use this ic on to change the admin password of the selected device. You must know the current admin password before changing to a new one. |

Table 4 ZON Utility Icons

| ICON | DESC RIPIIO N |
|------------------------------|--|
| 9 Configure NCC Discovery | You must have Internet access to use this feature. Use this icon to enable ordisable the Nebula Control Center (NCC) discovery feature on the selected device. If it is enabled, the selected device will try to connect to the NCC. Once the selected device is connected to and has registered in the NCC, it will go into the Nebula cloud management mode. |
| 10 ZAC | Use this icon to run the ZyxelAPC onfigurator of the selected AP. |
| 11 Clearand Rescan | Use this icon to clear the list and discoverall devices on the connected network again. |
| 12 Save Config uration | Use this icon to save configuration changes to permanent memory on a selected device. |
| 13 Setting s | Use this icon to select a network adapter for the computer on which the ZON utility is installed, and the utility language. |

| Table 4 | ZO N Utility | Ic ons | (continue | d) |
|---------|--------------|--------|-----------|----|
|---------|--------------|--------|-----------|----|

The following table describes the fields in the ZON Utility main screen.

| LABEL | DESC RIPTIO N |
|-------------------|---|
| Туре | This field displays an icon of the kind of device discovered. |
| Model | This field displays the model name of the discovered device. |
| Firm ware Version | This field displays the firm ware version of the discovered device. |
| MAC Address | This field displays the MAC address of the disc overed device. |
| IP Address | This field displays the IP address of an internal interface on the discovered device that first received an ZDP discovery request from the ZON utility. |
| System Name | This field displays the system name of the discovered device. |
| Lo c a tio n | This field displays where the discovered device is. |
| Status | This field displays whether changes to the discovered device have been done successfully. As the Zyxel Device does not support IP Configuration , Renew IP address and Flash Locator LED , this field displays "Update failed", "Not support Renew IP address" and "Not support Flash Locator LED" respectively. |
| NCC Disc overy | This field displays if the discovered device supports the Nebula ControlCenter(NCC) discovery feature. If it's enabled, the selected device will try to connect to the NCC. Once the selected device is connected to and has registered in the NCC, it'll go into the Nebula cloud management mode. |
| Se nial Number | Enter the admin password of the discovered device to display its serial number. |
| Hardware Version | This field displays the hardware version of the discovered device. |

Table 5 ZON Utility Fields

2.4 Ways to Access the Zyxel Device

You can use the following ways to configure the Zyxel Device.

Web Configurator

The Web Configurator allows easy Zyxel Device setup and management using an Internet browser. If your Zyxel Device is managed by the NCC or an AC, use this only for trouble shooting if you cannot connect to the Internet. This User's Guide provides information about the Web Configurator.

NCC

This is the primary means by which you manage the Zyxel Device in cloud (NCC) mode. With the NCC, you can remotely manage and monitor the Zyxel Device through a cloud-based network management system. See the NCC User's Guide for more information.

ZON Utility

ZyxelOne Network (ZON) Utility is a utility tool that assists you to set up and maintain network devices in a simple and efficient way. You can download the ZON Utility at www.zyxel.com and install it on your computer (Windows operating system). For more information on ZON Utility see Section 2.3 on page 22.

Command-Line Interface (CLI)

The CHallows you to use text-based commands to configure the Zyxel Device. You can access it using remote management (for example, SSH or Telnet) or via the console port. See the Command Reference Guide for more information.

File Transfer Protocol (FIP)

This protocol can be used for firm ware upgrades and configuration backup and restore.

2.5 Good Habits for Managing the Zyxel Device

Do the following things regularly to make the Zyxel Device more secure and to manage it more effectively.

- Change the password often. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the Zyxel Device becomes unstable or even crashes. If you forget your password, you will have to reset the Zyxel Device to its factory default settings. If you backed up an earlier configuration file, you will not have to totally re-configure the Zyxel Device; you can simply restore your last configuration.

C HA PTER 3 Hardware

See the Quick Start Guide for hard ware installation and connections.

3.1 Zyxel Device Single LED

The LED of the ZyxelDevice can be controlled by using the suppression feature such that the LEDs stay lit (ON) or OFF after the ZyxelDevice is ready. Refer to Chapter 20 on page 180 for the LED Suppression and Locator menus in standalone mode.

3.1.1 Zyxel Device LED

Figure 12 NWA50AX LED



The following are the LED descriptions for your Zyxel Device.

| COLOR | | STATUS | DESC RIPTIO N | | |
|---------|-------------|--|--|--|--|
| 1 | Amber | Blinks amberfor 1 second and green for 1 second | The Zyxel Device is booting up or is connecting with NCC. | | |
| | Green | a lte ma tive ly. | | | |
| | Amber | Blinksamberandgreen | The Zyxel Device is discovering the NCC or an AC. | | |
| 1 | Green | altematively 3 times and then tums solid green for 3 seconds. | | | |
| | Amber | Blinksamberandgreen | The Zyxel Device is managed by an AC but the uplink is | | |
| ţ | Green | altematively 2 times and then tums solid green for 3 seconds. | 1d disconnected. or 3 | | |
| | Green | Slow Blinking (On for 1 second, Off for 1 second) | The wire less module of the Zyxel Device is disabled or fails, the Zyxel Device is using default wire less settings, or the Zyxel Device is configured to be managed by NCC but is not yet registered with the NCC. | | |
| | Green | Steady On | The Zyxel Device is ready for use, the Zyxel Device's wire less interface is activated, and/or wire less clients are connected to the Zyxel Device. | | |
| | Bright Blue | Steady On | The Zyxel Device's wire less interface is activated, but the re are no wire less clients connected. | | |
| | Blue | Slow Blinking (Blink for 1 time, Off for 1 second) | The Zyxel Device is performing a Channel Availability Check (CAC) with Dynamic Frequency Selection (DFS) to monitora channel forradar signals. | | |
| | Re d | On | The Zyxel Device failed to boot up or is experiencing system failure. | | |
| | | Fa st Blinking (On for 50 millise c o nd s, Off for 50 millise c o nd s) | The Zyxel Device is undergoing firm ware upgrade. | | |
| | | Slow Blinking (Blink for 3 times, Off for 3 seconds) | The Uplink port of the Zyxel Device in standalone mode is disconnected. | | |

Table 6 Zyxel Device LED

C HAPTER 4 Web Configurator

4.1 Overview

The Web Configurator is an HIML based management interface that allows easy system setup and management via internet browser. Use a browser that supports HIML5, such Internet Explorer 11, Mozilla Fire fox, or Google Chrome. The recommended screen resolution is 1024 by 768 pixels.

In order to use the Web Configurator you need to allow:

- Web browserpop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

4.2 Accessing the Web Configurator

- 1 Make sure your Zyxel Device hard ware is properly connected. See the Quick Start Guide.
- 2 If the ZyxelDevice and yourcomputerare not connected to a DHCP server, make sure yourcomputer's IP address is in the range between "192.168.1.3" and "192.168.1.254".
- 3 Browse to the ZyxelDevice's DHCP-assigned IP address or http://192.168.1.2. The Login screen appears. If you are in NCC mode, check the NCC's AP> Monitor> Access Point screen for the ZyxelDevice's LAN IP address.

| ZYXEL | | Q English • |
|-------|---------|-------------|
| Er: | NWA50AX | ik Login. |
| | 0 | 1 |
| | 0 | _ |
| | | |
| | Login | 1 |

If a Zyxel Device is in standalone mode and supports NCC, the login page displays as shown in the following figure.

| ZYXEL | Q Engl | ah w |
|----------------------------|-------------------------------|----------|
| Texteet Lines February Pro | SUAX | |
| and and the second | and the set of many second in | |
| 0 | | |
| 0 | | |
| | | |
| | | |
| 1 | 1 02020 | enter la |
| | nigo | |

Click **Nebula Mode** to show the following screen. Here, you can watch a tutorial for using the Zyxel Nebula ControlCenter(NCC) or access the link to the NCC, as shown in the following figure. Otherwise, continue with the next step. The NCC is a cloud-based network management system that allows you to

remotely manage and monitor the Zyxel Device (see Section 2.1.2 on page 20).



If you want to return to the login page, click Standalone Mode and follow the next steps.

- 4 Enter the user name (default: "admin") and password (default: "1234"). If the Zyxel Device is being managed or has been managed by the NCC, check the NCC's Site-Wide > Configure > General setting screen for the Zyxel Device's current password.
- 5 Select the language you prefer for the Web Configurator. Click Login.
- 6 The wizard screen opens when the Zyxel Device is accessed for the first time or when you reset the Zyxel Device to its default factory setting s.
- 7 If you logged in using the default user name and password, the Update Admin Info screen appears. Otherwise, the dashboard appears.

| ZYXEL | NWA |
|----------------------------------|---|
| As a security precision | Update Admin Info Bon, if is highly incomminded that you change the admin password. |
| New Pasiyword Confim Password | max. 43 aptignument, printable chiatochen and no spacet(|
| | Apply Ignore |

The **Update Admin Info** screen appears every time you log in using the default username and default password. If you change the password for the default useraccount, this screen does not appear anymore.

4.3 Navigating the Web Configurator

The following summarizes how to navigate the Web Configurator from the **Dashboard** screen. The following figures show the **Dashboard** screen for standalone mode and for cloud (NCC) mode. The screen is different for standalone mode and cloud (NCC) mode and may vary slightly for different mode ls.



| XEL Investigate | AC | 0 0 | | 0.0 | - 12 - |
|---|-------------|--|--|---------|--------|
| C. Server & Normalian Server & Server Server Lasonaria Serve | c | Claims Inter Science corres Electric confirm Electric con | allara International a sub- apres (Jonerica) (SLAPSH) Do Do Doc Marine Na | - | - |
| Annual Insta | 827 | A CONTRACTOR | * finally | Sol dei | 1010 |
| A "Shared Magness and tota tota tota tota | 8/11 1/4 | C All Labor Tonic The Constant States C All Labored Tonic C The Constant States | - | | 11 M |

Figure 14 The Web Configurator's Main Screen for Cloud Mode

| et de la companya de | | | |
|--|--|---|--|
| 197 Internation - MAC Assess Setter Konder: Restauf Varians Ard Diserve Internation 30 Diserve Internation 20 Diserve Internation Restaur Connectivity 20 Diserve Internation Assess Connectivity 20 Diserve Internation Assess Connectivity 20 Diserve Internation Assess Connectivity 20 Diserve Internation 20 Diserve Internation | NUM FINE FEDD 1201658000108 NWASSAR Charles & Child / Internet press \$211000 Desma & Child Workshold, Takawat press \$30 Market Society and Takens Access \$30 Market Society and Takens Access Access \$30 Market Society and Takens Access Access Takens Market Society and Takens Access Access Access Access Market Society and Takens Access Access Access Access Market Society Access Access Access Access Access Market Society Access Access Access Access Market Society Access Access Access Access Access Access Market Access Access Access Access Access Access Access Market Access Access Access Access Access Access Access Market Access Acce | c | |

The Web Configurator's main screen is divided into these parts:

- A Title Bar
- B Navigation Panel
- C Main Window

4.3.1 Title Bar

The title barprovides some useful links that a lways appear over the screens below, regardless of how deep into the Web Configuratoryou navigate. If your Zyxel Device is in NCC mode, not all icons will be available in the Title Bar.

Figure 15 Title Bar



The iconsprovide the following functions.

| IABEL | DESC RIPHO N |
|----------|---|
| Wiza rd | Click this to open the wizard. See Chapter 7 on page 49 for more information. |
| He lp | Click this to open the help page for the cument screen. |
| Fo rum | C lick this to go to Zyxel Biz User Forum, where you can get the latest Zyxel Device information and have conversations with other people by posting your messages. |
| Site Map | Click this to see an overview of links to the Web Configuratorscreens. |
| сп | Click this to open a popup window that displays the Clicommands sent by the Web Configurator. |
| Logout | Click this to log out of the Web Configurator. |
| ne b ula | Click this to open the NCC web site login page in a new tab or window. |

Site Map

Click **Site MAP** to see an overview of links to the Web Configuratorscreens. Click a screen's link to go to that screen.

| 👗 Sile Map | | | 28 |
|----------------|---|-----|----|
| C Monitor | | | 8 |
| Network Status | Wireless AP Information Station info Detected Device | Log | |
| Configuration | | | Ð |
| 1 Maintenance | | | Ð |

Figure 16 Site Map

СЦMessages

Click **CU** to look at the CU commands sent by the Web Configurator. These commands appear in a popup window, such as the following.

Figure 17 CUMessages

| Tă CII | (*)() |
|--------------|--------|
| Cea | |
| ### Ctistori | |
| | |
| | 1 |
| | |
| | |
| | |
| | |
| | Candel |

Click Clear to remove the currently displayed information.

Note: See the Command Reference Guide for information about the commands.

4.3.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure Zyxel Device features. Click the arrow in the middle of the right edge of the navigation panel to hide the navigation panel menus or drag it to resize them. The following sections introduce the Zyxel Device's navigation panel menus and their screens.



4.3.3 Standalone Mode Navigation Panel Menus

The following are the screens available in standalone mode. Note that some screens may not be available for your Zyxel Device model. See Section 1.4 on page 18 to see which features your Zyxel Device model supports.

Dashboard

The dashboard displays general device information, system status, system resource usage, and interface status in widgets that you can re-arrange to suit your needs.

For details on the Dashboard's features, see Chapter 6 on page 44.

Monitor Menu

The monitor menu screens display status and statistics information.

| FO LDER OR LINK | TAB | FUNCTION |
|-----------------------|--------------------------|---|
| Ne twork Status | Ne two rk Sta tus | Display general IAN interface information and packet statistics. |
| Wire le ss | | |
| AP Inform a tio n | Radio List | Display information about the radios of the connected APs. |
| Station Info | Station List | Display information about the connected stations. |
| WDS Link Info | WDS Link Info | Disp lay statistic s a bout the Zyxel Device's WDS (Wireless Distribution System) connections. |
| De te c te d De vic e | De te c te d De vic e | Display information about suspected rogue APs. |
| Log | View Log | Disp la y log entries for the Zyxel Device. |

Table 8 Monitor Menu Screens Summary

Configuration Menu

Use the configuration menu screens to configure the Zyxel Device's features.

| FO LDER OR LINK | TAB | FUNCTION |
|------------------|---------------------------|--|
| Ne two rk | IP Setting | $Configure$ the $I\!PaddressfortheZyxelDeviceEthemetinterface$. |
| | VIAN | Manage the Ethemet interface VIAN settings. |
| | NCC Disc overy | Configure proxy server settings to access the NCC. |
| Wire le ss | | |
| AP Management | WIAN Setting | Manage the Zyxel Device's general wireless settings. |
| Rogue AP | Rogue/Friendly AP List | Configure how the Zyxel Device monitors for rogue APs. |
| DCS | DCS | Configure dynamic wire less channel se le ction. |
| O b je c t | - | |
| Use r | Use r | Create and manage users. |
| | Setting | Manage default settings for all users, general settings for user sessions, and rules to force user authentication. |
| AP Pro file | Ra d io | C reate and manage wireless radio settings files that can be associated with different APs. |
| | SSID | C reate and manage wire less SSID, security, MAC filtering, and layer-2 iso lation files that c an be associated with different APs. |
| MON Pro file | MON Pro file | C reate and manage rogue AP monitoring files that can be associated with different APs. |

Table 9 Configuration Menu Screens Summary

NWA50AX Use r's Guide
| FO LDER OR LINK | ТАВ | FUNC TIO N |
|-----------------|--------------------------|---|
| WDS Pro file | WDS | Create and manage WDS profiles that can be used to connect to different APs in WDS. |
| C e rtific a te | My Certific a te s | Create and manage the Zyxel Device's certificates. |
| | Truste d Certific a te s | Import and manage certificates from trusted sources. |
| Syste m | | |
| Ho st Na me | Ho st Name | Configure the system and domain name for the Zyxel Device. |
| Power Mode | PowerMode | Configure the Zyxel Device's powersettings. |
| Da te / Tim e | Date/Time | Configure the current date, time, and time zone in the Zyxel Device. |
| WWW | Service Control | Configure HTIP, HTIPS, and general authentication. |
| SSH | SSH | Configure SSH server and SSH service setting s. |
| FIP | FIP | Configure FIP server setting s. |
| Log & Report | | |
| Log Setting | Log Setting | Configure the system log, e-mail logs, and remote syslog servers. |

Table 9 Configuration Menu Screens Summary (continued)

Maintenance Menu

Use the maintenance menu screens to manage configuration and firm ware files, run diagnostics, and reboot or shut down the Zyxel Device.

| FO LDER O R LINK | ТАВ | FUNC TIO N |
|------------------|--------------------|---|
| File Manager | Configuration File | Manage and upload configuration files for the Zyxel Device. |
| | Firmware Package | View the current firm ware version and to up load firm ware. |
| | Shell Script | Manage and run shell script files for the Zyxel Device. |
| Dia g no stic s | Diagnostics | Collect diagnostic information. |
| LEDs | Suppression | Enable this feature to keep the LEDs off after the Zyxel Device starts. |
| | Locator | Enable this feature to see the actual location of the Zyxel Device between several devices in the network. |
| Antenna | Antenna Switch | Change antenna orientation for the radios. |
| Reboot | Reboot | Re start the Zyxel De vice. |
| Shutdown | Shutdown | Tum off the Zyxel Device. |

Table 10 Maintenance Menu Screens Summary

4.3.4 Cloud Mode Navigation Panel Menus

If your Zyxel Device is in NCC mode, you only need to use the Web Configurator for trouble shooting if your Zyxel Device cannot connect to the Internet.

Dashboard

The dashboard displays general Zyxel Device information, and AP information in widgets that you can re-arrange to suit your needs.

For details on the Dashboard's features, see Chapter 23 on page 187.

Configuration Menu

Use the configuration menu screens to configure the Zyxel Device's features.

| FOIDERORUNK | TAB | FUNCTION |
|--|------|--|
| Ne two nk IP Setting Configure the IP address for the Zyxel Device Ethemet int | | Configure the IP address for the Zyxel Device Ethemet interface. |
| | VIAN | Manage the Ethemet interface VIAN settings. |

| Table | 11 | Configur | a tio n | Menu | Screens | Summar |
|--------|----|-------------|----------|--------|------------|--------|
| 10.010 | | c c ning un | a 010 11 | nic na | 2010 0 110 | Sammar |

4.3.5 Tables and Lists

The Web Configurator tables and lists are quite flexible and provide several options for how to display their entries.

4.3.5.1 Manipulating Table Display

Here are some of the ways you can manipulate the Web Configurator tables.

1 Click a column heading to sort the table's entries according to that column's criteria.

| 0 | Add (11) | R Consider Q Achieley Q Reactivity | Section 1 (non-section | |
|---|----------|------------------------------------|------------------------|--|
| - | Shahin | Chatte Hame ->> | frequency hand | |
| | 9 | Wb_Radio_24G | 2.43 | |
| | 4 | Wtr_Rode_SG | 50 | |
| 5 | 9 | detoutt | 2.4G | |
| 6 | | ciedoult2 | 50 | |

- 2 Click the down arrow next to a column heading for more options about how to display the entries. The options available vary depending on the type of fields in the column. Here are some examples of what you can do:
 - Sort in a scending alphabetic alorder
 - Sort in descending (reverse) alphabetic al order
 - Select which columns to display
 - Group entries by field
 - Show entries in groups
 - Filter by mathematic aloperators (<, >, or =) or searching for text.

| I Viz Radio 24G 11 Sort Ascending MBSS 2 Viz Radio 3G 11 Sort Descending MBSS | |
|--|----|
| 2 Vitz, Radio_5G 11 Sort Descending MBSS | D |
| | D |
| default TR. Columns IV Status | |
| 4 Q default2 Center Ru Trib Dates IV Profile Nar | 00 |

3 Select a column heading cell's right border and drag to re-size the column.

| 0 400 | Concern & Withham & Letters | A | |
|------------|-----------------------------|----------------|---------------------|
| 51000 | Profile Harro - | Highersoy Band | Ciperating Mode |
| 9 | Witz_Rocko_24G | L4G | MBSSID |
| | Wiz_Rodio_5G | G | MBSSID |
| Q. | default | 2.4G | MBSSID |
| | detault2 | 00 | M833ID |
| # * Poge I | of t + H Show III as here | V | Displaying 1 - # of |

4 Select a column heading and drag and drop it to change the column order. A green check mark displays next to the column's title when you drag the column to a valid new location.

| and the second second | TYN THE WHITE EXT. | THE REAL PROPERTY AND INC. | CONTRACTOR OF MANAGE |
|-----------------------|--|----------------------------|--|
| Contention - | Interesting to the second seco | Litrationary again | and a state of the |
| | default2 | 5G | M Profee Marriel |
| | detault | 2.4G | A4BSSID |
| · • | Wiz_Radio_5G | 5G | MBSSID |
| 9 | Wiz Radio 24G | 2.4G | MBSSID |

5 Use the icons and fields at the bottom of the table to navigate to different pages of entries and control how many entries display at a time.

| D Add Tim 1 | Remaines & Addressin & Ameri | Sector Council Robosiness | |
|-------------|------------------------------|---------------------------|-----------------|
| status - | Inuttie Name | Requercy band | Casesuling Mode |
| Q. | delauit2 | 5G | MBSRD |
| | thoteb | 2.4G | MBSSID |
| | Wiz_Radio_5G | 5G | MBSSID |
| 0 | Witz Radio 24G | 2.4G | M6SSD |

4.3.5.2 Working with Table Entries

The tables have icons for working with table entries. A sample is shown next. You can often use the [Shift] or [Ctrl] key to select multiple entries to remove, activate, or deactivate.

| Fig ure | 19 | Common | Table | k ons |
|----------|----|------------|---------|--------------|
| I In all | 10 | 0011111011 | 10 0 10 | TO O HID |

| Alund - con | Memorye A working a rudo | tivale Coject Reference | |
|-------------|--------------------------|-------------------------|---------------|
| | Proble Name | Troquency Band | Operating Mod |
| 9 | Wiz, Radio, 24G | 2,4G | MBSSID |
| 0 | Wiz_Rodio_SG | 5G | M8SSID |
| 9 | default | 2.4G | MBISHD |
| 9 | default2 | 5G | MBSSID |
| ¥. | test | 5G | MBSSID |

Here are descriptions for the most common table icons.

Table 12 Common Table Lons

| LABEL | DESC RIPTIO N |
|--------------------------|---|
| Add | Click this to create a new entry. For features where the entry's position in the numbered list is important (features where the Zyxel Device applies the table's entries in order like the fire wall for example), you can select an entry and click Add to create a new entry after the selected entry. |
| Ed it | Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings. In some tables you can just click a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied. |
| Remove | To remove an entry, select it and click Remove . The Zyxel Device confirms you want to remove it before doing so. |
| Ac tiva te | To tum on an entry, select it and click Activate. |
| Ina c tiva te | To tum off an entry, se lect it and click Inactivate . |
| O b je c t Re fe re nc e | Select an entry and click Object Reference to open a screen that shows which settings use the entry. |

PART I Standalone Configuration

C HAPTER 5 Standalone Configuration

5.1 Overview

The Zyxel Device is in standalone mode by default. Use the web configurator to manage and configure the Zyxel Device directly. As shown in the following figure, wire less clients can connect to the Zyxel Device (A) to access network resources.



5.2 Starting and Stopping the Zyxel Device

Here are some of the ways to start and stop the Zyxel Device.

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

| MEIHO D | DESC RIPIIO N |
|-------------------------------|---|
| Tuming on the power | A cold start occurs when you tum on the power to the Zyxel Device. The Zyxel Device powers up, checks the hardware, and starts the system processes. |
| Rebooting the Zyxel Device | A warm start (without powering down and powering up again) occurs when you use the Reboot button in the Reboot screen or when you use the reboot command. The Zyxel Device writes all cached data to the local storage, stops the system processes, and then does a warm start. |

Table 13 Starting and Stopping the ZyxelDevice

NWA50AX Use r' s $\operatorname{Guid} e$

| MEIHO D | DESC RIPIIO N |
|---|---|
| Using the RESETbutton | If you press the RESET button on the back of the Zyxel Device, the Zyxel Device sets the configuration to its default values and then reboots. See Section 26.6 on page 205 for more information. |
| Clicking Maintenance > Shutdown > Shutdown or using the shutdown command | Clicking Maintenance > Shutdown > Shutdown or using the shutdown command writes all cached data to the local storage and stops the system processes. Wait for the Zyxel Device to shutdown and then manually turn offorremove the power. It does not turn off the power. |
| Disconnecting the power | Poweroffoccurs when you turn off the power to the ZyxelDevice. The ZyxelDevice simply turns off. It does not stop the system processes or write cached data to local storage. |

Table 13 Starting and Stopping the ZyxelDevice

The Zyxel Device does not stop or start the system processes when you apply configuration files or run shell scripts although you may temporarily lose access to network resources.

C HAPTER 6 Dashboard

6.1 Overview

This screen displays general device information, system status, system resource usage, and interface status in widgets that you can re-arrange to suit your needs. You can also collapse, refresh, and close individual widgets.

| ANOTO REC. | | | | | |
|--|--|------|--|---|-----------------------|
| E Barris Elementation Deliter Valens Tychen Joshidan Matel Valens Delit Garlesen Matt Assensi Range Hersuger Vertige | NUMBER NUM NUM NUM NUM NUM NUM NUM NUM NUM NUM | | C Names Halos Synteen Labore Current Carlos Tone Compet Carlos Tone Soul Tonico Manager Series Manager Soula | SDAY M Sector Lower and J SC States States States Age | B / C |
| Jahl Revision Lagrant Paris. | 108 | | W prevent a little but story | 7/11-1-1 | 100 million |
| C Arrent Arrent of | | | 10 1000Ad | C 240010000 | CONTRACT Same |
| i Halimage Barrany tengat Marrany tengat Marri tenga | 198. 1998 | | RTACIONALIZATIONE Alternational Inclusione at Alternation Alternational | - | *** |
| - | 14 | | and and all the second second | | and the second second |
| A Disease Property | | 10.0 | Concession and the second | 0.000 | and the second |
| ere hut hut | THE MA HA | 100A | A ¹ Anti du avente du re- | | ALC: NOT DR |
| | 1 240 AF76 | - | | | |

| Table | 14 | Dashboard |
|--------|----|------------|
| La D L | TI | Dasinovaiu |

| LABEL | DESC RIPTIO N | |
|-----------------------------|---|--|
| WidgetSettings (A) | Use this link to re-open closed widgets. Widgets that are already open appeargrayed out. | |
| Refresh Time Setting (B) | Set the interval for refreshing the information displayed in the widget. | |
| Re fre sh No w (C) | Click this to update the widget's information immediately. | |
| Close Widget(D) | Click this to close the widget. Use Widget Settings to re-open it. | |
| Device Information | | |
| System Name | This field displays the name used to identify the Zyxel Device on any network. Click the icon to open the screen where you can change it. | |
| System Location | This field displays the location of the Zyxel Device. Click the icon to open the screen where you can change it. | |
| ModelName | This field displays the model name of this Zyxel Device. | |
| Se ria l Num b e r | This field displays the serial number of this Zyxel Device. | |

| IABEL | DESC RIPTIO N | | |
|---------------------------------|--|--|--|
| MAC Address Range | This field displays the MAC addresses used by the Zyxel Device. Each physical port or wire less radio has one MAC address. The first MAC address is assigned to the Ethernet IAN port, the second MAC address is assigned to the first radio, and so on. | | |
| Firm ware Version | This field displays the version number and date of the firm ware the Zyxel Device is currently running. Click the icon to open the screen where you can upload firm ware. | | |
| Last Firmware Upgrade Status | This field displays whether the latest firm ware update was successfully completed. | | |
| Last Firmware Upgrade | This field displays the date and time when the last firm ware update was made. | | |
| System Re so urc e s | | | |
| C PU Usa g e | This field displays what percentage of the Zyxel Device's processing capability is currently being used. Hoveryourcursorover this field to display the Show CPU Usage icon that takes you to a chart of the Zyxel Device's recent CPU usage. | | |
| Memory Usage | This field displays what percentage of the Zyxel Device's RAM is currently being used. Hover your cursor over this field to display the Show Memory Usage ic on that takes you to a chart of the Zyxel Device's recent memory usage. | | |
| Fla sh Usa g e | This field displays what percentage of the Zyxel Device's onboard flash memory is currently being used. | | |
| Ethe met Neighbor | | | |
| Local Port (Description) | This field displays the port of the Zyxel Device, on which the neighboring device is discovered. | | |
| ModelName | This field displays the model name of the discovered device. | | |
| System Name | This field displays the system name of the discovered device. | | |
| FW Version | This field displays the firm ware version of the disc overed device. | | |
| Port (De sc rip tio n) | This field displays the discovered device's port which is connected to the Zyxel Device. | | |
| ₽ | This field displays the IP address of the discovered device. Click the IP address to access and manage the discovered device using its Web Configurator. | | |
| MAC | This field displays the MAC address of the disc overed device. | | |
| WDS (Wire le ss Distrib ut | ion System) Up link/Downlink Status | | |
| MAC Address | This field displays the MAC address of the root AP or repeater to which the Zyxel Device is connected using WDS. | | |
| Ra d io | This field displays the radio number on the root AP or repeater to which the Zyxel Device is connected using WDS. | | |
| Channel | This field displays the channel number on the root AP or repeater to which the Zyxel Device is connected using WDS. | | |
| SSID | This field displays the name of the wire less network to which the Zyxel Device is connected using WDS. | | |
| Se c urity Mod e | This field displays which secure encryption methods is being used by the Zyxel Device to connect to the root AP or repeater using WDS. | | |
| Link Status | This field displays the RSSI (Received Signal Strength Indicator) and transmission/reception rate of the wire less connection in WDS. | | |
| Syste m Sta tus | Syste m Sta tus | | |
| Syste m Up tim e | This field displays how long the Zyxel Device has been running since it last restarted or was turned on. | | |
| Cument Date/ Time | This field displays the cument date and time in the Zyxel Device. The format is yyyy-mm-dd hh:mm:ss. | | |
| Cument Login User | This field displays the user name used to log in to the current session, the amount of reauthentic ation time remaining, and the amount of lease time remaining. | | |

Table 14 Dashboard (continued)

| Table 14 Das | ıboard (c | ontinue d) |
|--------------|-----------|------------|
|--------------|-----------|------------|

| IABEL | DESC RIPTIO N |
|----------------------------------|--|
| Bo o t Sta tus | This field displays details a bout the Zyxel Device's startup state. |
| | OK - The Zyxel Device started up successfully. |
| | Firm ware update OK - A firm ware update was successful. |
| | Problematic configuration after firm ware update - The application of the configuration failed after a firm ware upgrade. |
| | System default configuration - The Zyxel Device successfully applied the system default configuration. This occurs when the Zyxel Device starts for the first time or you intentionally reset the Zyxel Device to the system default setting s. |
| | Fallback to lastgood configuration - The Zyxel Device was unable to apply the startup- config.conf configuration file and fell back to the lastgood.conf configuration file. |
| | Fallback to system default configuration - The Zyxel Device was unable to apply the lastgood.conf configuration file and fell back to the system default configuration file (system-default.conf). |
| | Booting in progress - The Zyxel Device is still applying the system configuration. |
| Management Mode | This shows whether the Zyxel Device is set to work as a stand alone AP. |
| Interface Status Summary | If an Ethemet interface does not have any physical ports associated with it, its entry is displayed in light gray text. Click the Detail ic on to go to a (more detailed) summary screen of interface statistics. |
| Name | This field displays the name of each interface. |
| Sta tus | This field displays the cument status of each interface. The possible values depend on what type of interface it is. |
| | Inactive - The Ethemet interface is disabled. |
| | Down - The Ethemet interface is enabled but not connected. |
| | Speed / Duplex - The Ethemet interface is enabled and connected. This field displays the port speed and duplex setting (Full or Half). |
| VID | This field displays the VIAN ID to which the interface belongs. |
| IP Add n⁄ Ne tm a sk | This field displays the cument IP address and subnet mask assigned to the interface. If the IP address is 0.0.0.0, the interface is disabled ordid not receive an IP address and subnet mask via DHCP. |
| IP Assig nment | This field displays how the interface gets its IP address. |
| | Static - This interface has a static IP address. |
| | DHCP Client - This interface gets its IP address from a DHCP server. |
| Ac tio n | If the interface has a static IP address, this shows n/a. |
| | If the interface has a dynamic IP address, use this field to get or to update the IP address for the interface. Click Renew to send a new DHCP request to a DHCP server. |
| WIAN Interface Status Summary | This d isp la ys sta tus info m a tio n fo r the WIAN interface. |
| Status | This d isp lays whe the rornot the WIAN interface is activated. |
| MAC Address | This displays the MAC address of the radio. |
| Ra d io | This indicates the radio number on the Zyxel Device. |
| Band | This indicates the wire less frequency band currently being used by the radio. |
| | This shows - when the radio is in monitor mode. |
| OP Mode | This indic ates the radio's operating mode. Operating modes are AP (MBSSID), MON (monitor), Root AP or Repeater . |

NWA50AX Use r's Guide

| IABEL | DESC RIPIIO N | | |
|-------------------|--|--|--|
| Channel | This indicates the channel number the radio is using. | | |
| Antenna | This indicates the antenna orientation for the radio (Wallor Ceiling). | | |
| | This field is not a vailable if the Zyxel Device does not allow you to a djust antenna orientation for the Zyxel Device's radio(s) using the web configuratorora physical switch. Refer to Section 1.4 on page 18 to see if your Zyxel Device has an antenna switch. | | |
| Sta tio n | This d isp la ys the number of wire less c lients connected to the Zyxel Device. | | |
| AP Information | This shows a summary of connected wire less Access Points (APs). | | |
| All Sensed Device | This sections displays a summary of all wire less devices detected by the network. Click the link to go to the Monitor > Wire less > Detected Device screen. | | |
| Un-Classifie d AP | This displays the number of detected unclassified APs. | | |
| Rogue AP | This displays the number of detected rogue APs. | | |
| Friendly AP | This displays the number of detected friendly APs. | | |

Table 14 Dashboard (continued)

6.1.1 CPU Usage

Use this screen to look at a chart of the Zyxel Device's recent CPU usage. To access this screen, click CPU Usage in the dashboard.



Figure 21 Dashboard > CPUUsage

| Ta b le | 15 | Da shb o a rd | > | C PU Usa g | e |
|---------|----|---------------|---|------------|---|
|---------|----|---------------|---|------------|---|

| LABEL | DESC RIPTIO N |
|----------------------|---|
| % | The y-axis represents the percentage of CPU usage. |
| time | The x-axis shows the time period over which the CPU usage occurred. |
| Re fre sh Inte rva l | Enter how often you want this window to be automatically updated. |
| Re fre sh No w | Click this to update the information in the window right away. |

6.1.2 Memory Usage

Use this screen to look at a chart of the Zyxel Device's recent memory (RAM) usage. To access this screen, click **Memory Usage** in the dashboard.



Figure 22 Dashboard > Memory Usage

| IABEL | DESC RIPIIO N |
|----------------------|---|
| % | The y-axis represents the percentage of RAM usage. |
| time | The x-axis shows the time period over which the RAM usage occumed |
| Re fre sh Inte rva l | Enter how often you want this window to be automatically updated. |
| Re fre sh No w | Click this to update the information in the window right away. |

Table 16 Dashboard > Memory Usage

C HA PTER 7 Se tup Wiza rd

7.1 Accessing the Wizard

When you log into the Web Configurator for the first time or when you reset the Zyxel Device to its default configuration, the wizard screen displays.

Note: If you have already configured the wizard screens and want to open it again, click the Wizard icon on the upper right comer of any Web Configurators creen.

7.2 Using the Wizard

This wizard helps you configure the Zyxel Device IP address, change time zone, daylight saving and radio settings, and edit an SSID profile to change general wire less and wire less security settings.

7.2.1 Step 1 Time Settings

Use this screen to configure the Zyxel Device's country code, time zone and daylight saving time.

- Country Code: Select the country where the Zyxel Device is located.
- Note: The country code field is not available and you cannot change the country code if the Zyxel Device products comply with the U.S. laws, policies and regulations and are to be sold to the U.S. market.
- Time Zone: Select the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
- Enable Daylight Saving: Select the option if you use Daylight Saving Time. Configure the day and time when Daylight Saving Time starts and ends.
- Offset a llows you to specify how much the clock changes when daylight saving begins and ends. Enter a number from 1 to 5.5 (by 0.5 increments).

Click Next to proceed. Click Cancel to close the wizard without saving.

| Figure 23 | Wizard : Tim e | Se tting s |
|-----------|----------------|------------|
|-----------|----------------|------------|

| Wiscrid Sett | ing | |
|--------------|---------------|--|
| step 1 | Weicomet | o the Setup Wizard |
| | Time Settings | |
| 1002 | Time Zone: | (GMT+0500) Beijing, Hang Kang, Perth, Singapare, Tapel 👘 |
| - | E Encipie Do | ylight saving |
| | - 20pt (Amp | 전 김 그는 친 그는 친 삶을 |
| 1904 | | Englishers, St. |
| 1000 | | |
| | | |
| | | Tite Next Canoel |

7.2.2 Step 2 Password and Uplink Connection

Use this screen to configure the Zyxel Device's system password and IP address.

Change Password: Enter a new password and retype it to confirm.

Uplink Connection: Select Auto (DHCP) if the Zyxel Device is connected to a router with the DHCP server enabled. You then need to check the router for the IP address assigned to the Zyxel Device in order to access the Zyxel Device's Web Configurator again.

O the rwise, se lect **Static IP** when the Zyxel Device is NOT connected to a routeroryou want to assign it a fixed IP address. You will need to manually enter.

- the Zyxel Device's IP address and subnet mask.
- the \mathbb{I} address of the router that helps forward traffic.
- a DNS server's IP address. The Domain Name System (DNS) maps a domain name to an IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

Click **Prev** to return to the previous screen. Click **Next** to proceed. Click **Cancel** to close the wizard without saving.

| ig: t | Change Password | | |
|-------|-------------------|--------------|---------|
| | Hew Potoword: | | |
| | Confirm Password | ****** | |
| Ξ, | Uplink Connection | | |
| | () Auto(DHCP) | Static P | |
| | | (P Address | 0.6.0.0 |
| | | Subnet Mosic | 0000 |
| 4 | | Cateway: | 0.0.0 |
| | | Cr45 Server: | 8655 |
| ÷3 | | | |
| | | | |

Figure 24 Wizard: Change Password and Uplink Connection

7.2.3 Step 3 Radio

Use this screen to configure the Zyxel Device's radio transmitter(s).

- Channel Selection: Select Auto to have the Zyxel Device automatically choose a radio channel that has least interference. Otherwise, select Manual and specify a channel the Zyxel Device will use in the 2.4 GHz or 5 GHz wire less LAN. The options vary depending on the frequency band and the country you are in.
- Maximum Output Power. Enter the maximum output power of the Zyxel Device. If there is a high density of APs in an area, decrease the output power of the Zyxel Device to reduce interference with other APs.

Note: Reducing the output poweralso reduces the Zyxel Device's effective broadcast radius.

Click **Prev** to return to the previous screen. Click **Next** to proceed. Click **Cancel** to close the wizard without saving.

| 30903/1 | Rodio | |
|---------|-----------------------|--------------------|
| | Bond. | 2.40Hz |
| Ship 2 | Channel Width | 20//Hz |
| | Channel Selection: | Auto O Monuol |
| Step 5 | Maximum Output Pawer: | 30 dBm(0-30) |
| | Bondt | 3GHt |
| Dep 4 | Channel Wildm: | 20/40/80MHz = |
| | Channel Selection: | Auto 6 Manual 2005 |
| See. | Maximum Output Power: | 20 dBm(0-30) |
| | | |
| | | Rent Mark Course |

Figure 25 Wizard: Radio

NWA50AX Use r's Guide

7.2.4 Step 4 SSID

Use this screen to enable, disable oredit an SSID profile.

Select an SSID profile and click the **Status** switch to turn it on or off. To change an SSID profile's settings, such as the SSID (WiFinetwork name) and WiFipassword, double-click the SSID profile entry from the list. See Section 7.2.4.1 on page 52 for more information.

Note: You cannot add or remove an SSID profile after running the setup wizard.

| 10-11 | 2 | | | | | |
|------------|-------|--------|--------|---------------|-----------|-------|
| 24021 | \$510 | 0 | | | | |
| | C | analue | 2011) | Security Mode | Hand Made | W.AND |
| State of C | 1 | (COL) | Zynai | WPAD-Perional | Dual Band | |
| | 2 | - | Zynei | WPA2-Personal | Dual Bond | 1 |
| Nex.3 | 3 | | Ζγκιφί | WFA2-Fenonal | DualBand | 1 |
| | 4 | œ | Zyna | WPA3-Renonal | Dual Band | 3 |
| | 1 | 0 | Zynai | WEA2-Personal | Dud Band | 1 |
| 100.000 | | 0 | Dyneli | WPA3-Personal | Dud Bond | 1 |
| | 9 | | Zyne | WPA2-Personal | Dua Band | 3 |
| Daniel. | 0. | | Zyonei | WPAD-Personal | Dud Band | .1 |

7.2.4.1 Ed it SSID Profile

Use this screen to configure an SSID profile.

The screen varies depending on the security type you selected.

- SSID: Enter a descriptive name of up to 32 printable characters for the wire less IAN.
- VIAN ID: Enter a VIAN ID for the Zyxel Device to use to tag traffic originating from this SSID.

Band Mode: Select the wire less band which this profile should use. 2.4 GHz is the frequency used by IEEE 802.11b/g/n wire less clients. 5 GHz is the frequency used by IEEE 802.11ac/a/n wire less clients.

- Security Type: Select WPA2 to add security on this wire less network. Otherwise, select OPEN to allow any wire less client to associate this network without authentication.
- Personal: If you set Security Type to WPA2 and select Personal, enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.

ClickOK to proceed. Click Cancel to close the screen without saving.

7.2.5 Summary

Use this screen to check whether what you have configured is correct. Click **Save** to apply your settings and complete the wizard setup. Otherwise, click **Prev** to return to the previous screen or click **Cancel** to close the wizard without saving.

| Waged Set | fing | | | | | 100 |
|-----------|------------------|--------|----------------------|------------------|----------|--------|
| Desil | Summary | | | | | 1 |
| | Time Jone: | 7540 | ideath twing king ka | ing Perti Ingawa | n Topper | |
| Part | Daylight Saving: | Deal | | | | |
| | Management (P) | Until | P | | | |
| Sec.1 | ₽ Address | -50.03 | | | | |
| | Subriet Matic | E G BA | | | | |
| 1.11 | Conewoy: | 803 | | | | 18. |
| Card of | Crid Server: | -00.04 | 1 | | | |
| | 2.40 Fode: | date | | | | |
| - | 5G Radia; | (Auto | | | | |
| Date 2 | \$90 | | | | | |
| | 4 200A | 2147 | Secondly Morde | Torst Mode | VSA(III) | 1.1 |
| | - | | | | 141 | T 70 |
| | | | | Prev | Save 0 | Isocel |

Figure 27 Wizard: Summary

C HAPTER 8 Monitor

8.1 Overview

Use the Monitor screens to check status and statistics information.

8.1.1 What You Can Do in this Chapter

- The Network Status screen (Section 8.3 on page 55) displays general IAN interface information and packet statistics.
- The AP Information > Radio List screen (Section 8.4 on page 57) displays statistics about the wire less radio transmitters in the Zyxel Device.
- The Station Info screen (Section 8.5 on page 61) displays statistics pertaining to the associated stations.
- The WDS Link Info screen (Section 8.6 on page 62) displays statistics about the Zyxel Device's WDS (Wire less Distribution System) connections.
- The Detected Device screen (Section 8.7 on page 63) displays information about suspected rogue APs.
- The View Log screen (Section 8.8 on page 66) displays the Zyxel Device's cument log messages. You can change the way the log is displayed, you can e-mail the log, and you can also clear the log in this screen.

8.2 What You Need to Know

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

Rogue AP

Rogue APs are wire less access points operating in a network's coverage area that are not under the control of the network's administrators, and can open up holes in a network's security. See Chapter 13 on page 117 for details.

Friendly AP

Friendly APs are otherwireless access points that are detected in yournetwork, as well as any others that you know are not a threat (those from neighboring networks, for example). See Chapter 13 on page 117 for details.



8.3 Network Status

Use this screen to look at general Ethemet interface information and packet statistics. To access this screen, click Monitor > Network Status.

| Figure 28 | Mo nito r > | Ne two rk | Status |
|-----------|-------------|-----------|--------|
|-----------|-------------|-----------|--------|

| Nome | | itatus | VID | IP Addr/N | 4etmask | | IP Assignme | int i | Action |
|--------------------------------|------------|------------|------------|-----------|------------------|------------|-------------|-------|----------|
| UPLINK | | 1000M/Full | 1 | 172.16.40 |).29 / 255.255.3 | 252.0 | DHCP clien | t | Renew |
| vé interfac | e Summary | | | | | | | | |
| Name | Statu | 5 | PA | ddress | | | | Actio | n |
| UPUNK | 1000 | M/Full | UN | LOCAL fe8 | 0::becf:4fff:fe5 | i6:be03/64 | | n/a | |
| ort Statistics Poll Interva | s Table | 5 S | econds Set | interval | Stop | | | | |
| Switch to t | Status | Ъr₽kts | RoPids | Tx Boast | Rx Boast | Collisions | Тх | Rx | Up Time |
| Name | | E 1000 | 40206 | 28 | 12604 | 0 | 0 | 635 | 01:43:51 |
| Nome UPUNK | 1000M/Full | 5490 | 100 800 10 | | | | | | |

| LABEL | DESC RIPIIO N |
|---|---|
| Interface Summary IPv6 Interface Summary | Use the Interface Summary section for IPv4 network settings. Use the IPv6 Interface Summary section for IPv6 network settings if you connect your Zyxel Device to an IPv6 network. Both sections have similar fields as described below. |
| Name | This field displays the name of the physical Ethemet port on the Zyxel Device. |
| Sta tus | This field displays the cument status of each physical port on the Zyxel Device. |
| | Down - The port is not connected. |
| | Speed / Duplex - The port is connected. This field displays the port speed and duplex setting (Full or Half). |
| VID | This field displays the VIAN ID to which the port belongs. |
| IP Ad d n/ Ne tm a sk IP Ad d re ss | This field displays the cument IP address (and subnet mask) of the interface. If the IP address is 0.0.0.0 (in the IPv4 network) or:: (in the IPv6 network), the interface does not have an IP address yet. |
| IP Assig nm ent | This field displays how the interface gets its IPv4 address. |
| | Static - This interface has a static IPv4 address. |
| | DHCPClient - This interface gets its IPv4 address from a DHCP server. |
| Ac tio n | Use this field to get or to update the IP address for the interface. Click Renew to send a new DHCP request to a DHCP server. If the interface cannot use one of the se ways to get or to update its IP address, this field displays n / a . |
| Port Sta tistic s Ta b le | |
| Poll Interval | Enter how often you want this window to be updated automatically, and click Set Interval. |

Table 17 Monitor > Network Status

| LABEL | DESC RIPIIO N |
|---------------------------|--|
| Set Interval | Click this to set the Poll Interval the screen uses. |
| Sto p | Click this to stop the window from updating automatically. You can start it again by setting the Poll Interval and clicking Set Interval . |
| Switch to Graphic View | Click this to display the port statistics as a line graph. |
| Name | This field displays the name of the interface. |
| Status | This field displays the cument status of the physical port. |
| | Down - The physical port is not connected. |
| | Speed / Duplex - The physical port is connected. This field displays the port speed and duplex setting (Full or Half). |
| TxPkts | This field displays the number of packets transmitted from the Zyxel Device on the physical port since it was last connected. |
| RxPkts | This field displays the number of packets received by the Zyxel Device on the physical port since it was last connected. |
| Tx Bc a st | This field displays the number of broadcast packets transmitted from the Zyxel Device on the physical port since it was last connected. |
| Rx Bc a st | This field displays the number of broadcast packets received by the Zyxel Device on the physical port since it was last connected. |
| C o llisio n s | This field displays the number of collisions on the physical port since it was last connected. |
| Tx | This field displays the transmission speed, in bytes per second, on the physical port in the one-second interval before the screen updated. |
| Rx | This field displays the reception speed, in bytes per second, on the physical port in the one- second interval before the screen updated. |
| Up Time | This field displays how long the physical port has been connected. |
| System Up Time | This field displays how long the Zyxel Device has been running since it last restarted or was tumed on. |

Table 17 Monitor > Network Status (continued)

8.3.1 Port Statistics Graph

Use the port statistics graph to look at a line graph of packet statistics for the Ethemet port. To view, click Monitor > Network Status and then the Switch to Graphic View button.

| senerci semingi | | and the second second | |
|-------------------|-----------|-------------------------------|-----|
| Refresh Interval: | 5 minutes | Robesh Now | |
| fort Usage | | | |
| Port Selection/ | UPLINK 🔄 | Switch To Grid View | |
| 21 Hape 12 | -0 | Last quarter 2709-07-29 16146 | 1 |
| 10.9 | | | |
| 18.8 | | | 12 |
| 14.7 | | | |
| 12.6 | | | 11. |
| 19.5 | | | |
| 8,4 | | | |
| K.3 | | | A |
| 4.2 - | | | 10 |
| 2.1 | | | 1 |

Figure 29 Monitor > Network Status > Switch to Graphic View

The following table describes the labels in this screen.

| LABEL | DESC RIPTIO N |
|------------------------|--|
| Re fre sh Interval | Enter how often you want this window to be automatically updated. |
| Re fre sh No w | Click this to update the information in the window right away. |
| Port Se le c tio n | Select the Ethemet port for which you want to view the packet statistics. |
| Switch to Grid View | Click this to display the port statistics as a table. |
| Kbps/Mbps | The y-axis represents the speed of transmission or reception. |
| Tim e | The x-axis shows the time period over which the transmission or reception occurred. |
| TX | This line represents traffic transmitted from the Zyxel Device on the physical port since it was last connected. |
| RX | This line represents the traffic received by the Zyxel Device on the physical port since it was last connected. |
| La st Up d a te | This field displays the date and time the information in the window was last updated. |

Table 18 Monitor > Network Status > Switch to Graphic View

8.4 Radio List

Use this screen to view statistics for the Zyxel Device's wireless radio transmitters. To access this screen, click Monitor > Wireless > AP Information > Radio List.

| 21 | fore inflor | reation | | | | | | | | | |
|----|-------------|---------|---------|-------|------|----------|---------|------------|------|--------|-------------------|
| 27 | lood. | Itean- | Chan | 5000- | sta. | . Upload | Down! | MAC Adds | NED: | CP MD- | AF / WOS Profile |
| Ŷ | - | 2.4G | 1 | 25 | 0 | .0 | \$70310 | 80:31:97:0 | 1 | AP M | default / default |
| 9 | ÷ . | SG | 161/1 | 29 | 0 | 0 | 668418 | 60:31:97:0 | 2. | AP [M | defouit2 / def |
| 14 | F (Page | i arti | F H. Sh | W TD | 200 | 100 | | | | | Deploying 1-2.012 |

Figure 30 Monitor > Wire less > AP Information > Radio List (for Zyxel Device that supports WDS)



| <u>- 1</u> | | | | | | | | | | | | |
|------------|--------|-----------|--------|--------|--------|----------|------|------------|-------|----------|-----------|--------------|
| 1 | Und. | functions | Chan- | mornii | 30341 | species. | DOWE | MAC ACLE | Radi) | Of Model | dicate. | Charrie Ulli |
| 9 | (#) | 2.4G | 1 | 23 | 0 | 9 | 9 | 00:13:4970 | 1 | AF (M81 | detca./ft | 125 |
| | + | 50 | :157/1 | 26 | 0 | 0 | 0. | 00:13:49:0 | 2 | AP (MIS | defol/ff2 | 15 |
| 1 | Filipp | or i i | H Sho | | durns. | | | 44 | | | | Dumming 1-21 |

Table 19 Monitor > Wire less > AP Information > Radio List

| LABEL | DESC RIPTIO N |
|------------------|--|
| More Information | Click this to view additional information about the selected radio's wireless traffic and station count. Information spans a 24 hour period. |
| Status | This displays whether or not the radio is enabled. |
| Lo a d ing | This indicates the AP's load balance status (Underload or Overload) when load balancing is enabled on the Zyxel Device. Otherwise, it shows - when load balancing is disabled or the radio is in monitor mode. |
| MAC Address | This displays the MAC address of the radio. |
| Ra d io | This indicates the radio number on the Zyxel Device to which it belongs. |
| OP Mode | This indic a testhe radio's operating mode. Operating modes are AP (MBSSID), MONIOR, Root AP or Repeater. |
| AP/WDS Pro file | This indicates the AP profile name and WDS profile name to which the radio belongs. |
| | This field is a vailable only on the Zyxel Device that supports WDS. |
| Pro file | This indicates the AP profile name to which the radio belongs. |
| | This field is a vailable only on the Zyxel Device that does not support WDS. |
| Frequency Band | This indicates the wire less frequency band currently being used by the radio. |
| | This shows - when the radio is in monitor mode. |
| Channel | This indic a tes the radio's channel ID. |
| Transmit Power | This displays the output power of the radio. |
| Sta tio n | This displays the number of wire less clients connected to this radio on the Zyxel Device. |

| IABEL | DESC RIPTIO N |
|-----------------------------|---|
| Up lo a d | This displays the total number of packets received by the radio. |
| Download | This displays the total number of packets transmitted by the radio. |
| C ha nne l Utiliza tio n | This indicates how much IEEE 802.11 traffic the radio can receive on the channel. It displays what percentage of the radio's channel is currently being used. |

Table 19 Monitor > Wire less > AP Information > Radio List (continued)

8.4.1 AP Mode Radio Information

This screen a llows you to view a selected radio's SSID details, wire less traffic statistics and station count for the preceding 24 hours. To access this window, select a radio and click the **More Information** button in the **Radio List** screen.



Figure 32 Monitor > Wire less > AP Information > Radio List > More Information

The following table describes the labels in this screen.

| Table 20 Monitor> | Wire less $> A$ | P Information > | Radio | List > More | Information |
|-------------------|-----------------|-----------------|-------|-------------|-------------|
|-------------------|-----------------|-----------------|-------|-------------|-------------|

| IABEL | DESC RIPIIO N |
|---------------|---|
| SSID De ta il | This list shows information about all the wire less clients that have connected to the specified radio over the preceding 24 hours. |
| # | This is the items sequential number in the list. It has no bearing on the actual data in this list. |

NWA50AX Use r's Guide

60

| LABEL | DESC RIPIIO N |
|-----------------------|--|
| SSID Name | This displays an SSID associated with this radio. There can be up to eight maximum. |
| BSSID | This displays a BSSID a ssociated with this radio. The BSSID is tied to the SSID. |
| Se c urity Mo d e | This displays the security mode in which the SSID is operating. |
| VIAN | This displays the VIAN ID a ssociated with the SSID. |
| Tra ffic Sta tistic s | This graph displays the overall traffic information of the radio over the preceding 24 hours. |
| Kbps/Mbps | This y-axis represents the amount of data moved across this radio in megabytes per second. |
| Tim e | This x-axis represents the amount of time over which the data moved across this radio. |
| Station Count | This graph displays the connected station information of the radio over the preceding 24 hours |
| Sta tio ns | The y-axis represents the number of connected stations. |
| Tim e | The x-axis shows the time period over which a station was connected. |
| La st Up d a te | This field displays the date and time the information in the window was last updated. |
| ОК | C lick this to c lose this window. |
| Cancel | C lick this to c lose this window. |

Table 20 Monitor > Wire less > AP Information > Radio List > More Information (continued)

8.5 Station List

Use this screen to view statistics pertaining to the associated stations (or "wire less clients"). Click Monitor > Wire less > Station Info to access this screen.

| Figure 33 | Mo nito r > | Wire $le ss >$ | Sta tio n | Info |
|-----------|-------------|----------------|-----------|------|
|-----------|-------------|----------------|-----------|------|

| State | fion List | | | | | | | | | | |
|-------|-----------|-----------|---------|------------|----------|------------|----------|------------|-----------|----------|-----------------|
| | PNL- | MAC ALL | 11(121) | Capitolity | 000111e. | 100 Notes | Sicomr - | April 18.5 | Visition: | To Fight | Access. |
| 17 | 172 | 00:19:00: | 1 | 802.11b/g | N/A | 2yxel-6E03 | Open | -35d8m | 54M | 54M | 19:58:40 |
| 11 | 4. (P00) | | ्य आ | ow 10 (#18 | HITS. | | | | | DIN | aaying 1 - 1 af |
| | | | | | | Roberth | 12 | | | | |

| IABEL | DESC RIPTIO N |
|--------------------|---|
| # | This is the station's index number in this list. |
| IP Address | This is the station's IP address. |
| MAC Address | This is the station's MAC address. |
| Ra d io | This is the radio number on the Zyxel Device to which the station is connected. |
| C a p a b ility | This displays the supported standard currently being used by the station or the standards supported by the station. |
| 802.11 Fe a ture s | This displays whether the station supports IEEE802.11r, IEEE 802.11k, IEEE 802.11v or none of the above (N/A) . |

Table 21 Monitor > Wire less > Station Info

| IABEL | DESC RIPIIO N |
|-----------------------|--|
| SSID Name | This indicates the name of the wire less network to which the station is connected. A single AP can have multiple SSIDs or networks. |
| Se c urity Mode | This indic a tes which secure encryption methods is being used by the station to connect to the network. |
| Sig nal Strength | This is the RSSI (Received Signal Strength Indicator) of the station's wire less connection. |
| Tx Ra te | This is the maximum transmission rate of the station. |
| Rx Ra te | This is the maximum reception rate of the station. |
| Asso c ia tio n Tim e | This d isp lays the time the station first a ssoc ia ted with the Zyxel Device's wire less network. |
| Re fre sh | Click this to refresh the items displayed on this page. |

Table 21 Monitor > Wire less > Station Info (continued)

8.6 WDS Link Info

Use this screen to view the WDS traffic statistics between the ZyxelDevice and a root AP or repeaters. See Section 1.2 on page 12 to know more about WDS. Click **Monitor > Wire less > WDS Link Info** to access this screen.

| 03 0 | plink teto | | | |
|------|--|----------------------------|--------------|--|
| 2 | MAC Adams - Radio SSD Name | Security Max. Signal Stren | iter Protein | Autocidition firms |
| 11.1 | Page 1 of 1 # #1 Show 00. #1/her | <u>u</u> | | No data to diplay |
| DS D | ownlink Info | | | |
| os D | ownlink Info MAIC Accres • Ro., 1500 Name Se | corthySignal/SHSkillate | ta Rate | Association time |
| DS D | ownlink Info MAID Access + Ro., 1500 Marriel Se Frage (of) + R (Show 10Ber | corthy Signal St. Scillate | ta Role | Association time No data to display |

Figure 34 Monitor > Wire less > WDS Link Info

Ta b le 22 Monitor > Wire le s
s > WDS Link Info

| IABEL | DESC RIPIIO N |
|------------------|---|
| WDS Up link Info | Uplink refers to the WDS link from the repeaters to the root AP. |
| WDS Downlink | Downlink refers to the WDS link from the root AP to the repeaters. |
| Into | When the Zyxel Device is in root AP mode and connected to a repeater, only the downlink information is displayed. |
| | When the Zyxel Device is in repeatermode and connected to a root AP directly or via another repeater, the uplink information is displayed. |
| | When the Zyxel Device is in repeatermode and connected to a root AP and other repeater(s), both the uplink and downlink information would be displayed. |
| # | This is the index number of the mot AP or repeater in this list. |

| IABEL | DESC RIPIIO N |
|-----------------------|---|
| MAC Address | This is the MAC address of the mot AP or repeater to which the Zyxel Device is connected using WDS. |
| Ra d io | This is the radio number on the root AP or repeater to which the Zyxel Device is connected using WDS. |
| SSID Name | This indicates the name of the wireless network to which the Zyxel Device is connected using WDS. |
| Se c unity Mode | This indicates which secure encryption methods is being used by the Zyxel Device to connect to the root AP or repeater using WDS. |
| Sig nal Strength | This is the RSSI (Received Signal Strength Indicator) of the wire less connection in WDS. |
| Tx Ra te | This is the maximum transmission rate of the root AP or repeater to which the Zyxel Device is connected using WDS. |
| Rx Ra te | This is the maximum reception rate of the root AP or repeater to which the Zyxel Device is connected using WDS. |
| Asso c ia tio n Tim e | This displays the time the Zyxel Device first a ssociated with the wire less network using WDS. |
| Re fre sh | Click this to refresh the items displayed on this page. |

Table 22 Monitor > Wire less > WDS Link Info (continue d)

8.7 Detected Device

Use this screen to view information about sumounding APs which you could mark as Rogue or Friendly. Click **Monitor > Wireless > Detected Device** to access this screen. Not all Zyxel Devices support monitor mode (see Section 1.4 on page 18). For more information about Rogue APs, see Section 10.3 on page 79.

Note: If the Zyxel Device supports monitor mode, the radio or at least one of the Zyxel Device's radio must be set to monitor mode (in the **Wireless > AP Management** screen) in order to detect other wireless devices in its vicinity.

If the Zyxel Device does not support monitor mode, tum on rogue AP detection in the **Configuration > Wire less > Rogue AP** screen to detect other APs.

| 2 | Mark al | Bogue AP 😋 | Mark a | s Friendly AP | | | | | | |
|----|---------|--------------|--------|--------------------|--------------|------------|------|---------|---------|----------------------|
| | Stot | Device: | Role | MAC Address | 55ID Nome | Chame | 907 | Securit | Descrip | Lost Seen: |
| | V | infrastruc | | 00:02:6F:12:34:56 | VIDEOTRON | 10 | HEFE | WP | | Mon Jul |
| | 8 | infrastruc | | 00/02/CFIAF/6P/DC | 5001-85662 | 8 | IFFE | TOP | | Mon J.A |
| | 9 | Infrastruc | | 001334911166/8C | Zy_private | 5 | HEEE | WP | | Mon Jul_ |
| | | Infrastruc | | 00:12:49:F1:28:88 | 13431.2041.2 | 5 | ITTE | WP | | Mon Mi |
| | 8 | Infrastruc | | 00:17:16:44:33:70 | 100000/2 | 10 | EFF. | WP | | Mon Jul |
| | 9 | infrastruc | | 00.19:CB(1):44:DD | wpo | 10 | IFFE | 16P | | Mon 3.6 |
| | 9 | Intrastruc | | 00(25:36:AC)25:78 | 416H/v2 | ÷ | | WEP | | Mon J.d |
| | 0 | Information | | 100.00.18 CO ADEs | TYPE AND | 3 | - | WPar | _ | Adon Jul |
| | 9 | Intraitruc | 6 | 00:AAI58:01:23.40 | ZYONAL AF | | IEEE | WP | | Mon Jul |
| n' | | infrastruc | | 02:11:22:33:44:88 | aisfbre_334, | 8 | IEEE | TEP | | Mon Jul |
| ř. | 8 | Infrastruc | | 02:17:16:44:32:70 | eennnu722 | 10 | IEEE | WP | | Mon Jul_ |
| ż | | infrostruc | | 02:AA58:11:23:40 | HT_API | á. | IEEE | None | | Mon Mi |
| 5 | 9 | infrastruc | | 02:AA:88:21123140 | HT_AP2 | 4 | HEFE | None | | Mon Jul |
| 4 | | Infrastruc | | 021AA-58-31123140 | HT_AP3 | <i>ź</i> . | EFE | None | | Mon 3.4 |
| \$ | | infrastruc | | 04:8F:8D:0A:ED:10 | VIDEOTRON | 5 | HEFE | WP | | Mon Jul_ |
| 6 | | infrastruc | | 10:11:12:13:14:00 | 00,00,71 | 5 | ITTE | WP | | Mon M |
| Ť. | V | Intrastruc | | 10-78-EF-C\$-AC-85 | Elsa_999999 | 11 | IFFE | WP | | Man Jul |
| n. | | infrostruc | | 14(91:82:16:24(9A | TO_BH | 11 | ETT | WP | | Mon Jul |
| 9 | 8 | Whatbuc | | 14:91:82:81:AA:21 | Kell/55553 | 9 | EEE. | WP | | Mon Jul_ |
| Π. | | litification | | 14:91:82:82:30:99 | Kel/%8.0%3 | 8 | IEEE | WP | | Mon 3,4 |
| 6 | 1 Page | 1 1 1 1 1 | H m | a 21 w tens | | | | | 00 | flowig 1 - 20 of 225 |

| | the seat | | | | | | | | |
|-------|---------------------|----------------|--------------------|---------------|-------|-------|---------------------|-----------|---------------------|
| 09 | ue AP: | | | | | | | | |
| hip | ected rogue AP | - 20 | | | | | | | |
| frier | adly AP1 | 1 | | | | | | | |
| (m-t | lanified API | 310 | | | | | | | |
| Det | ect Now | | | | | | | | |
| efeic | ted Device | | | | | | | | |
| • | hark as Rogue Al | F 🗢 Mark as Fi | landly AP | -North - | | | | | |
| | Role | Clossfield by | MAC Address | SBD Nome | Chonn | 802 | Secim | Desofipue | contineen |
| | | | ADEACE/C/BIOS | 2,115_010 | 4 | MEE | WP | | Alter av |
| 12 | | | 5C:F4:A8:A8:59:05 | VIDEOTION | 153 | ·EEE | WP | | Man Jul |
| 23 | | | 80/82/DC/8P/55/8E | Next_106 | 36 | IEEE | WP | | Man Jul |
| 24 | | | 90:EF:68:FB:27:21 | 6315_55 | 1.57 | EEE | WP | | Man Jul. |
| 25 | | | 10/7EEF/CSIAC-85 | E8d_99999 | 11. | ·IEEE | WP | | Man Jul |
| 24 | | | 5A:47:F3:91:12;68 | Unizyx_WLAN | 1 | HEEE | WP_{**} | | Man Julie |
| 27 | | | 80:31:97:10:8P#5 | Plapfics00049 | + | HEEE | WP | | Thu Jon |
| 28 | Suspected t | Hidden \$\$1D | 10/4/00/19:00 | | 153 | -ETT | WP | | Mon Juline |
| 9 | Heridty AP | | 60:31:97:70:38:81 | Nebula Ac | 1 | 1666 | WP | | Mon Jului |
| 30 | | | 10/74/00/99:03:81 | ADHBU_5G | 36. | HEEE | $WP_{\tau\tau\tau}$ | | Mon Julie |
| 31 | | | -60(51:97:7D(38:2A | \$5KD1 | 45 | HEE | None | | Mon Juli. |
| 52 | | | 45:48/11/07:AC | IVXE_CSO | 36 | HEE | WP_{i-i} | | Mon Julier |
| 25 | | | A2:88:08:70 //8:89 | LYXEL_CSO | 6 | 1000 | WP | | Mars Avi |
| 54 | Suspected n | Hidden \$510 | 72:EC:A3:74:C8:57 | | 157 | 1222 | $WP_{\rm red}$ | | Thu Jono |
| 15. | Suspected t | Hidden SSID | 1C:74(0D:#P:D0: | | 161 | 1000 | WP | | Mon Millio |
| 56. | | | 5A:47:F3:91:12:69 | Unitys_ASA | 1 | (EEE | WP | | Mon Juline |
| 37 | Suspected r | Hidden \$\$1D | 10:74:00#FiD284 | | 161 | 1666 | WP | | thu John |
| 16 | | | 80/82/DC/C2/15/00 | 2101745,88 | 4 | (ETT | WP | | Mon Julie |
| 99 | | | 62:91:97:73:65:92 | e-Nebula | 44 | HEEE | None | | Mon Al |
| 40 | | | E8:37:7A:86:E7:19 | ZyXEL86871 | 149 | (EEE | WF | | Thu Jon |
| 14 | 4 Project 2 Torn 10 | P. H. Show 7 | 20 int family | | | | | Date | 10 10 10 - 40 of 24 |

Figure 36 Monitor > Wire less > Detected Device (for Zyxel Device that does not support Monitor mode)

The following table describes the labels in this screen.

| IABEL | DESC RIPTIO N |
|-----------------------|---|
| Discovered APs | |
| Rogue AP | This shows how many devices are detected as rogue APs. |
| Suspected rogue AP | This shows how many devices are detected as possible rogue APs based on the classification rule (s) in Section 10.3 on page 79. |
| Friendly AP | This shows how many devices are detected as friendly APs. |
| Un-c la ssifie d AP | This shows how many devices are detected, but have not been classified as either Rogue or Friendly by the Zyxel Device. |
| De te c t No w | Click this button for the Zyxel Device to scan for APs in the network. |
| De te c te d De vic e | |

Table 23 Monitor > Wire less > Detected Device

NWA50AX Use r's Guide

| LABEL | DESC RIPIIO N |
|------------------------|---|
| Markas Rogue AP | Click this button to mark the selected AP as a rogue AP. For more on managing rogue APs, see the Configuration > Wireless > Rogue AP screen (Section 10.3 on page 79). |
| Mark as Friendly AP | Click this button to mark the selected AP as a friendly AP. For more on managing friendly APs, see the Configuration > Wireless > Rogue AP screen (Section 10.3 on page 79). |
| # | This is the detected device's index number in this list. |
| Status | This indicates the detected device's status. |
| De vic e | This indicates the type of device detected. |
| Ro le | This indicates the detected device's role (such as friendly or rogue). |
| C la ssifie d b y | This indicates the detected device's classification rule. |
| MAC Address | This indicates the detected device's MAC address. |
| SSID Name | This indicates the detected device's SSID. |
| Channel₪ | This indicates the detected device's channel ID. |
| 802.11 Mode | This indicates the 802.11 mode $(a/b/g/n/ac/ax)$ transmitted by the detected device. |
| Se c urity | This indicates the encryption method (if any) used by the detected device. |
| De sc rip tio n | This displays the detected device's description. For more on managing friendly and rogue APs, see the Configuration > Wireless > Rogue AP screen (Section 10.3 on page 79). |
| La st Se e n | This indicates the last time the device was detected by the Zyxel Device. |
| Re fre sh | Click this to refresh the items displayed on this page. |

Table 23 Monitor > Wire less > Detected Device (continued)

8.8 View Log

Log messages are stored in two separate logs, one for regularlog messages and one for debugging messages. In the regularlog, you can look at all the log messages by selecting **All Logs**, or you can select a specific category of log messages (for example, user). You can also look at the debugging log by selecting **Debug Log**. All debugging messages have the same priority.

To access this screen, click Monitor > Log. The log is displayed in the following screen.

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.

The Web Configurator saves the filter settings once you click **Search**. If you leave the **View Log** screen and return to it later, the last filter settings would still apply.



| lupidy ource Addr ource Interf rotocok earch. Email Log | enz ace Now 2 Ref | All an an | logs in v M v M | Priority: Destination / Destination it Keyword: | kddress: | олу | <u>ii</u> |
|--|-------------------------|-----------------|----------------------------|--|-----------------------|-----------------|-----------|
| ource Ada ource Interf ratocok earch. Email Log | ens ace Now 2 Ref | an | * 18 * 18 | Destination A Destination is Keyword: | kddress: nterface: | | |
| arce interf atocsk earch | now 2 Ref | an | v Mil v Mil | Destination it Keyword: | recohern | Louis | |
| earch | Now 2 Rel | an | v 🔄 | Keyward: | | DALLA, CONTRACT | 100 |
| earch Emicil Log | Now 2 Rel | hanh | | | | 1 | |
| Entel Log | Now 2 Rel | hainhi - | | | | | |
| - Time | | a menta y | 🧳 ClearLog | | | | |
| | 111 | Qui | Mesoge | | Source | Destination | Note |
| 1 2017-07 | -03 05 | ¥ | Administrator admin from | n http/https has lo | 172,17.1.1 | 172.56.1.4 | Account: |
| 2 2017-07 | -83 04: | - | Station: 88:53.AC:14:70:8 | 6 has deauth by \$1 | | | |
| 3 2017-07 | 03 041 | U | Administrator admin from | n http:/https:hasibe | 172.17.1.1 | 172.56.1.4 | Account: |
| 4 2017-07 | -83 04/ | - | Station: 40:40:87.90;98.0 | D has deauth by 1 | | | |
| 5 2917-07 | 03 04: | | Station: 88:53:AC:14:73:8 | 6 has associated a | | | |
| £ 2017-07 | -03.04/ | 1= | Station: 2C PD:A2:99:3F:0 | 2 has deauth by \$7 | | | |
| 7 2017-07 | 03 04: | int. | Station: 2C/F0:A2:93:5Fit | 2 has associated a | | | |
| 8 2017-07 | 00.041 | | Station: 2C F0:A2:93:3F:0 | 2 has deouth by ST | | | |
| # 2017-07 | -03 63 | 1.0 | Station: 20.90;A2:93:35:0 | 2 has deauth by \$1 | | | |
| 10 2017-07 | -03.05 | - | Station: 2C P0:A2:93:3Fi0 | 2 has deauth by D | | | |
| 11 2017-07 | 03 03 | 1 | Station: 40:40:47:00:98:0 | D has associated | | | |
| 12 2017-07 | -03.03: | - | Station: 10:78:21:5F/Fi8 | has deauth by \$1 | | | |
| 13 2017-07 | -03 031 | in. | Station: 20:90;A2:93:5F:0 | 2 has disaspe by 5 | | | |
| 14 2017-07 | -03 03 | - | Station: 2C PD:A2:93:5F:0 | 2 has associated o | | | |
| 15 2017-07 | -03 03 | inak (| Station: 2C#0;A2:95:5F:0 | 2 has deouth by D | | | |
| 16 2017-07 | -03 03 | 1- | Station: 2C PD:A2:93;3Fi0 | 2 has associated a | | | |
| 17 2017-07 | -03.03/ | - | Station: 10:78:21:8F/FF:81 | has deased by 5 | | | |
| 18 2017-07 | -03 03 | 110 | Station: 10:78:21:85/F9.81 | har-associated and | | | |
| 19 2017-07 | -03 03 | | Station: 10:78:21:8PFF:81 | has deouth by D | | | |

Figure 37 Monitor > Log > View Log

| Ta b le | 24 | Moni | or> | Log | > | Vie w | Log |
|---------|----|------|-----|-----|---|-------|-----|
|---------|----|------|-----|-----|---|-------|-----|

| LABEL | DESC RIPIIO N |
|--------------------|---|
| Show Filter / Hide | Click this button to show or hide the filter setting s. |
| Filte r | If the filter settings are hidden, the Display, Email Log Now, Refresh, and Clear Log fields are available. |
| | If the filter setting s are shown, the Display, Priority, Source Address, Destination Address, Source Interface, Destination Interface, Protocol, Keyword, and Search fields are available. |
| Disp la y | 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 . |
| Prio rity | 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 , emor , wam , notice , and info , from highest priority to lowest priority. This field is read-only if the Category is Debug Iog . |
| 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. |

| LABEL | DESC RIPIIO N |
|--------------------------------|---|
| De stina tio n Ad d re ss | 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. |
| De stina tio n Inte rfa c e | This displays when you show the filter. Select the destination interface of the packet that generated the log message. |
| Pro to c o l | This d isp lays when you show the filter. Se lect a service protocol whose log messages you would like to see. |
| Ke yw o rd | 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. |
| Se a rc h | This displays when you show the filter. Click this button to update the log using the cument filter settings. |
| Email Log Now | Click this button to send log messages to the Active e-mailaddresses specified in the Send Log To field on the Configuration > Log & Report > Log Settings screen. |
| Re fre sh | Click this to update the list of logs. |
| ClearLog | 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. |
| Tim e | This field displays the time the log message was recorded. |
| Prio rity | This field displays the priority of the log message. It has the same range of values as the Priority field above. |
| C a te g o ry | This field displays the log that generated the log message. It is the same value used in the Display and (other) Category fields. |
| Me ssa g e | 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. |
| So urc e | 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. |
| De stina tio n | This field displays the destination IP address and the port number of the event that generated the log message. |
| De stina tio n Inte rfa c e | This field displays the destination interface of the packet that generated the log message. |
| Pro to c o l | 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. |

Table 24 Monitor > Log > View Log (continued)

C HAPTER 9 Network

9.1 Overview

This chapterdescribes how you can configure the management IP address and VIAN settings of your Zyxel Device.

The Internet Protocol (IP) address identifies a device on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.





The figure above illustrates one possible setup of your Zyxel Device. The gate way IP address is 192.168.1.1 and the managed IP address of the Zyxel Device is 192.168.1.2 (default), but if the Zyxel Device is assigned an IP address by a DHCP server, the default (192.168.1.2) will not be used. The gate way and the Zyxel Device must belong in the same IP subnet to be able to communicate with each other.

9.1.1 What You Can Do in this Chapter

- The IP Setting screen (Section 9.2 on page 69) configures the Zyxel Device's LAN IP address.
- The VIAN screen (Section 9.3 on page 71) configures the Zyxel Device's VIAN settings.
- The NCC Discovery screen (Section 9.4 on page 73) configures the Zyxel Device's Nebula Control Center (NCC) discovery setting s.

9.2 IP Setting

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



| IP Setting VLAN | NCC Bloovery |
|--|--------------------------------|
| IP Address Assignment | |
| · Get Automatically | |
| () Use Read IP Address | |
| P Address | |
| Scienced Married | |
| Commun. | 1000 - California |
| Distance P Address | |
| IPvs Address Assignment | |
| El Engole Stoleies Addres | Auto-configuration(RLAAC) |
| Unk-Local Addreal | NetDor Softwith Hert (Tably 44 |
| Pvs Address/Prefix Lengths | jOpfonali |
| Gateway | [Opfional] |
| Matric: | (0-15) |
| EI CHOPvil Client | |
| | |
| Di Nacional Address DHORVA Request Option | |
| 25 Doit haven | |
| 25 Million Statements | |
| | |
| | |
| | Apply Resol |

Figure 39 Configuration > Network > IP Setting

 Each field is described in the following table.

| | Table 25 | Configu | ra tio n > | Ne two rk > | IP Setting |
|--|----------|---------|------------|-------------|------------|
|--|----------|---------|------------|-------------|------------|

| LABEL | DESC RIPTIO N | | |
|---|---|--|--|
| IP Address Assignment | | | |
| Get Automatically | Select this to make the interface a DHCP client and automatically get the IP address, subnet mask, and gate way address from a DHCP server. | | |
| Use Fixed IP Address | Select this if you want to specify the IP address, subnet mask, and gate way manually. | | |
| IP Ad d re ss | Enter the \mathbb{P} address for this interface. | | |
| Sub ne t Ma sk | 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 gate way. The Zyxel Device sends packets to the gate way when it does not know how to route the packet to its destination. The gate way should be on the same network as the interface. | | |
| DNS Server IP Address | Enter the IP address of the DNS server. | | |
| IPv6 Address Assignment | | | |
| Enable Stateless Address Auto- configuration (SIAAC) | Se le c t this to e nable IPv6 state less auto-configuration on the Zyxel Device. The Zyxel Device will generate an IPv6 address itself from a prefix obtained from an IPv6 router in the network. | | |
| Link-Local Address | This displays the IPv6 link-local address and the network prefix that the Zyxel Device generates itself for the LAN interface. | | |

| IABEL | DESC RIPTIO N | |
|--------------------------------|--|--|
| IPv6 Address/ Prefix Length | Enter the IPv6 address and the prefix length for the LAN interface if you want to use a static IP address. This field is optional. | |
| | The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address. | |
| Gateway | Enter the IPv6 address of the default outgoing gate way using colon (:) hexadecimal notation. | |
| Me tric | Enter the priority of the gate way (if any) on the LAN interface. The Zyxel Device decides which gate way to use based on this priority. The lower the number, the higher the priority. If two ormore gate ways have the same priority, the Zyxel Device uses the one that was configured first. Enterzero to set the metric to 1024 for IPv6. | |
| DHC Pv6 C lie nt | Select this option to set the Zyxel Device to actas a DHC Pv6 client. | |
| DUID | This field displays the DHC P Unique ID entifier (DUID) of the Zyxel Device, which is unique and used for identification purposes when the Zyxel Device is exchanging DHC Pv6 messages with others. See Appendix Bon page 230 formore information. | |
| Request Address | Select this option to get an IPv6 address from the DHC Pv6 server. | |
| DHC Pv6 Request Options | Select this option to determine what additional information to get from the DHC Pv6 server. | |
| DNS Server | Select this option to obtain the IP address of the DNS server. | |
| NTP Server | Select this option to obtain the IP address of the NTP server. | |
| Apply | Click Apply to save your changes back to the Zyxel Device. | |
| Re se t | Click Reset to return the screen to its last-saved settings. | |

Table 25 Configuration > Network > \mathbb{IP} Setting (continued)

9.3 VIAN

This section discusses how to configure the Zyxel Device's VIAN settings.

Note: Mis-configuring the management VIAN settings in your Zyxel Device can make it in a c c e ssible. If this happens, you will have to reset the Zyxel Device.





In the figure above, to access and manage the Zyxel Device from computer **A**, the Zyxel Device and switch **B**'s ports to which computer **A** and the Zyxel Device are connected should be in the same VIAN.

A Vitual Local Area Network (VIAN) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VIAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

VIAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VIAN, all broadcasts are confined to a specific broadcast domain.

IEEE 802.1Q Tag

The EEE 802.1Q standard defines an explicit VIAN tag in the MAC header to identify the VIAN membership of a frame across bridges. A VIAN tag includes the 12-bit VIAN ID and 3-bit user priority. The VIAN ID associates a frame with a specific VIAN and provides the information that devices need to process the frame across the network.

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

The screen varies depending on whether the Zyxel Device has an extra Ethemet port (except the uplink port).

| IP Setting | VLAN | | |
|---------------|----------|-------------|--|
| VLAN Settings | | | |
| Management | VLAN ID: | 1 (1~4094) | |
| As Native Vi | LAN 🔒 | | |
| | | | |
| | | | |
| | | Apply Reset | |

Each field is described in the following table.

| LABEL | DESC RIPIIO N | | | |
|-------------------------------|---|--|--|--|
| VIAN Setting s | VIAN Setting s | | | |
| Management VLAN ID | Entera VIAN ID for the Zyxel Device. | | | |
| As Native VLAN | Select this option to treat this VIAN ID as a VIAN created on the Zyxel Device and not one assigned to it from outside the network. | | | |
| IAN Setting | | | | |
| Port Setting | | | | |
| Ed it | Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings. In some tables you can just click a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied. | | | |
| Ac tiva te / Ina c tiva te | To tum on an entry, select it and click Activate . To tum off an entry, select it and click Inactivate . | | | |
| # | This is the index number of the port. | | | |

Table 26 Configuration > Network > VIAN

NWA50AX Use r's Guide
| LABEL | DESC RIPIIO N |
|-------------------------------|---|
| Status | This field indicates whether the port is enabled (a yellow bulb) or not (a gray bulb). |
| Po rt | This field displays the name of the port. |
| PVID | This field displays the port number of the VLAN ID. |
| VIAN Config ura tio n | |
| Add | C lick this to create a new entry. For features where the entry's position in the numbered list is important (features where the Zyxel Device applies the table's entries in order like the SSID for example), you can select an entry and click Add to create a new entry after the selected entry. |
| Ed it | Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings. In some tables you can just click a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied. |
| Re m o ve | To remove an entry, select it and click Remove . The Zyxel Device confirms you want to remove it before doing so. |
| Ac tiva te / Ina c tiva te | To tum on an entry, select it and click Activate . To tum off an entry, select it and click Inactivate . |
| # | This is the index number of the VIAN ID. |
| Status | This field indicates whether the VLAN is enabled (a yellow bulb) or not (a gray bulb). |
| Name | This field displays the name of each VIAN. |
| VID | This field displays the VIAN ID. |
| Member | This field displays the VIAN membership to which the port belongs. |
| Apply | Click Apply to save your changes back to the Zyxel Device. |
| Re se t | Click Reset to return the screen to its last-saved settings. |

Table 26 Configuration > Network > VIAN (continued)

9.4 NCC Discovery

You can manage the ZyxelDevice through the ZyxelNebula ControlCenter(NCC). Use this screen to configure the proxy server settings if the ZyxelDevice is behind a proxy server.

To a c c e ss this sc re e n, c lic k Configuration > Network > NCC Discovery.

| IP Setting YUAN | MCC Discovery |
|-------------------------|--|
| Nebula Control Center 5 | lative |
| internet: | This docume point is connected to the information |
| Netwas Connectivity: | The second part is All correction [1] for installing (the definition of the) [|
| lebula Carital Center D | acovery letting |
| if trape | |
| (ii) Use Proxy to Ac | DEW MOC |
| Proxy Server: | 0 |
| Proxy Port | Q -45535 |
| E Authenticatio | n |
| der ware | |
| | |
| | |
| | TALAN STATE |

Figure 42 Configuration > Network > NCC Discovery

Each field is described in the following table.

| Table 27 | Configura | tio n > N | le twork > | NCC | Disc o ve rv |
|----------|-------------|-----------|------------|-----|--------------|
| | o o mig ana | | | | |

| LABEL | DESC RIPIIO N | |
|----------------------------|--|--|
| Nebula Control Center Sta | tus | |
| Inte me t | This field displays whether the Zyxel Device can connect to the Internet. | |
| Nebula Connectivity | This field displays whether the Zyxel Device can connect to the Zyxel Nebula Control Center (NCC). | |
| Ne bula Control Center Dis | c o ve ry Se tting | |
| Ena b le | Select this option to tum on NCC discovery on the Zyxel Device. The Zyxel Device will try to discover the NCC and go into NCC management mode when it is connected to the Internet and has been registered in the NCC. | |
| | If NCC discovery is disabled, the Zyxel Device will not discover the NCC and remain in standalone operation. | |
| Use Proxy to Access NCC | If the ZyxelDevice is behind a proxy server, you need to select this option and configure the proxy server settings so that the ZyxelDevice can access the NCC through the proxy server. | |
| Pro xy Se rve r | Enter the IP address of the proxy server. | |
| Pro xy Po rt | Enter the service port number used by the proxy server. | |
| Authentication | Select this option if the proxy server requires authentication before it grants access to the NCC. | |
| Use r Na m e | Enteryourproxy username. | |
| Pa ssw o rd | Enteryourproxy password. | |
| Apply | Click Apply to save yourchanges back to the Zyxel Device. | |
| Re se t | Click Reset to return the screen to its last-saved settings. | |

C HAPTER 10 Wire less

10.1 Overview

This c hapterdiscusses how to configure the wire less network settings in your Zyxel Device.

The following figure provides an example of a wire less network.





The wire less network is the part in the blue circle. In this wire less network, devices **A** and **B** are called wire less clients. The wire less clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your Zyxel Device is the AP.

10.1.1 What You Can Do in this Chapter

- The **AP Management** screen (Section 10.2 on page 76) allows you to manage the Zyxel Device's general wire less settings.
- The Rogue AP sc reen (Section 10.3 on page 79) allows you to assign APs either to the rogue AP list or the friendly AP list.
- The Load Balancing screen (Section 10.4 on page 83) allows you to configure network traffic load balancing between the APs and the Zyxel Device.
- The DCS screen (Section 10.4 on page 83) allows you to configure dynamic radio channel selection.

10.1.2 What You Need to Know

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

Station / Wire less Client

A station or wire less client is any wire less-capable device that can connect to an AP using a wire less signal.

Dynamic Channel Selection (DCS)

Dynamic Channel Selection (DCS) is a feature that allows an AP to automatically select the radio channel which it broadcasts. For more information, see Section 10.5 on page 84.

10.2 APManagement

Use this screen to manage the Zyxel Device's general wireless settings. Click **Configuration > Wireless > APManagement** to access this screen.

| WLAN Set | ing | | |
|---|------------|-----------------|------------------------|
| COrecte ne | w Cbject+ | | |
| Andio 1 Set | ing | | |
| W. Rode 1 | Activate | | |
| Rodit 1 0 | F Node: | # AP.Mode (b) I | toot Alt 🕐 Neperater 🌘 |
| Rode 1 Pr | offie: | deficult | |
| Misk Outp | ut Power. | 35 | dim (0-30) |
| MILLOD Self | Ings | | |
| | a Protec | | |
| 1 : ::::::::::::::::::::::::::::::::::: | faut | OF | |
| 2: sh | abie | 0 | |
| 3 39 | abie | 0 | |
| 4 dis | abie | 0 | |
| 5 di | abie | 0 | |
| 4. 68 | abie | 0 | |
| 7 de | obie | 0 | |
| 8. da | abie | 0 | |
| | | | |
| Rodio 2 Self | ing | | |
| IV Rodio 3 | 2 Activaté | | |
| Rodo 2 O | P \$Acde: | # AP Mode: () 3 | ioot AF 🕐 Repeater 🌘 |
| Rodio 271 | ofie: | defourt2 | 2 0 E 0 |
| Max Outp | UT Powert | 30 | dlim (0-00) |
| MISSID Set | Ingt | | |
| Contraction of the | . Itali | | |
| 1 :::::: | foult | 0 # | |
| 2 dis | dDie . | 0 | |
| 3 de | abie | 0 | |
| 4 di | obie | 0 | |
| 8 dis | able | 0 | |
| + de | 0010 | 0 | |
| 7 de | obie | 0 | |
| 8 clo | 900 | 0 | |
| | | | |
| | | | A COMPANY OF COMPANY |
| | | | Apply Reset |

Figure 44 Configuration > Wire less > AP Management

Each field is described in the following table.

Table 28 Configuration > Wireless > AP Management

| LABEL | DESC RIPTIO N |
|------------------|--|
| Radio 1 Setting | |
| Radio 1 Activate | Select the check box to enable the Zyxel Device's first (default) radio. |

| IABEL | DESC RIPIIO N |
|-------------------------------|---|
| Radio 1 OP Mode | Select the operating mode for radio 1. |
| | AP Mode means the radio can receive connections from wire less clients and pass their data traffic through to the Zyxel Device to be managed (or subsequently passed on to an upstream gate way for managing). |
| | MON Mode means the radio monitors the broadcast area for other APs, then passes their information on to the Zyxel Device where it can be determined if those APs are friendly or rogue. If a radio is set to this mode it cannot receive connections from wire less clients (see Section 1.2.3 on page 14). |
| | Root AP means the radio acts as an AP and also supports the wireless connections with other APs (in repeater mode) to form a WDS (Wireless Distribution System) to extend its wireless network. |
| | Repeater means the radio can establish a wireless connection with other APs (in either not AP or repeater mode) to form a WDS. |
| Radio 1 Profile | Select the radio profile the radio uses. |
| | Note: You can only apply a 2.4G AP radio profile to radio 1. Otherwise, the first radio will not be working. |
| Radio 1 WDS Profile | This field is a vailable only when the radio is in Root AP or Repeater mode. |
| | Select the WDS profile the radio uses to connect to a mot AP or repeater. |
| Up link Se le c tio n Mada | This field is a vailable only when the radio is in Repeater mode. |
| houe | Select AUIO to have the Zyxel Device automatically use the settings in the applied WDS profile to connect to a root AP or repeater. |
| | Select Manual to have the Zyxel Device connect to the mot AP or repeater with the MAC address specified in the Radio 1 Uplink MAC Address field. |
| Max Output Power | Enter the maximum output power (between 0 to 30 dBm) of the Zyxel Device in this field. If there is a high density of APs in an area, decrease the output power of the Zyxel Device to reduce interference with other APs. |
| | Note: Reducing the output power also reduces the Zyxel Device's effective broadcast radius. |
| MBSSID Settings | |
| Ed it 🤘 | C lic k Edit ic on (📷) to open a screen where you can modify the entry's settings. In some tables you can just c lic k a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied. |
| # | This field shows the index number of the SSID |
| SSID Pro file | This field displays the SSID profile that is a ssociated with the radio profile. |
| Radio 2 Setting | |
| Radio 2 Activate | This displays if the Zyxel Device has a second radio. |
| | Select the check box to enable the Zyxel Device's second radio. |

Table 28 Configuration > Wire less > AP Management (continued)

| LABEL | DESC RIPIIO N |
|-----------------------|---|
| Radio 2 OP Mode | This displays if the Zyxel Device has a second radio. Select the operating mode for radio 2. |
| | AP Mode means the radio can receive connections from wire less clients and pass their data traffic through to the Zyxel Device to be managed (or subsequently passed on to an upstream gate way for managing). |
| | MON Mode means the radio monitors the broadcast area for other APs, then passes their information on to the Zyxel Device where it can be determined if those APs are friendly or rogue. If a radio is set to this mode it cannot receive connections from wire less clients (see Section 1.2.3 on page 14). |
| | Root AP means the radio acts as an AP and also supports the wireless connections with other APs (in repeater mode) to form a WDS to extend its wireless network. |
| | Repeater means the radio can establish a wireless connection with other APs (in either not AP or repeater mode) to form a WDS. |
| Radio 2 Profile | This displays if the Zyxel Device has a second radio. Select the radio profile the radio uses. |
| | Note: You can only apply a 5G AP radio profile to radio 2. Otherwise, the second radio will not be working. |
| Radio 2 WDS Profile | This field is a vailable only when the radio is in Root AP or Repeater mode. |
| | Select the WDS profile the radio uses to connect to a root AP or repeater. |
| Up link Se le c tio n | This field is a vailable only when the radio is in Repeater mode. |
| Mode | Select AUIO to have the Zyxel Device automatically use the settings in the applied WDS profile to connect to a root AP or repeater. |
| | Select Manual to have the Zyxel Device connect to the mot AP or repeater with the MAC address specified in the Radio 2 Uplink MAC Address field. |
| Max Output Power | Enter the maximum output power(between 0 to 30 dBm) of the Zyxel Device in this field. If there is a high density of APs in an area, decrease the output power of the Zyxel Device to reduce interference with other APs. |
| | Note: Reducing the output power also reduces the Zyxel Device's effective broadcast radius. |
| MBSSID Settings | |
| Ed it 🥤 | Click Edit () to open a screen where you can modify the entry's settings. In some tables you can just click a table entry and edit it directly in the table. For those types of tables small red triangles display for table entries with changes that you have not yet applied. |
| # | This field shows the index number of the SSID |
| SSID Pro file | This field shows the SSID profile that is a ssociated with the radio profile. |
| Apply | Click Apply to save your changes back to the Zyxel Device. |
| Re se t | Click Reset to return the screen to its last-saved settings. |

Table 28 Configuration > Wire less > AP Management (continued)

10.3 Rogue AP

Use this screen to enable **Rogue AP Detection** and import/export a rogue or friendly AP list in a txt file. Click **Configuration > Wire less > Rogue AP** to access this screen.

Rogue APs

A rogue AP is a wire less access point operating in a network's coverage area that is not under the control of the network administrator, and which can potentially open up holes in a network's security.

In the following example, a corporate network's security is compromised by a rogue AP (**R**G) set up by an employee at his workstation in order to allow him to connect his note book computer wire lessly (**A**). The company's legitimate wire less network (the dashed ellipse **B**) is well-secured, but the rogue AP uses inferior security that is easily broken by an attacker (**X**) running readily available encryption-cracking software. In this example, the attacker now has access to the company network, including sensitive data stored on the file server (**C**).





Friendly APs

If you have more than one AP in your wire less network, you should also configure a list of "friendly" APs. Friendly APs are wire less access points that you know are not a threat. It is recommended that you export (save) your list of friendly APs often, especially if you have a network with a large number of access points. Exported lists show MAC addresses in txt file format separated by line breaks.

Rogue AP Detection

This feature allows the Zyxel Device to monitor the WiFi signals for otherwire less APs (see also Section 1.2.3 on page 14). Detected APs will appear in the Monitor > Wire less > Detected Device screen, where the Zyxel Device will abel APs with the criteria you select in Suspected Rogue AP Classification Rule as a suspected rogue. The APs which you mark as eitherrogue or friendly APs in the Monitor > Wire less > Detected Device screen will appear in the Wire less > Rogue AP screen. See Section 1.4 on page 18 to

know which models support Rogue AP Detection.

Note: Enabling **Rogue AP Detection** might affect the performance of wireless clients a ssociated with the Zyxel Device.

Figure 46 Configuration > Wire less > Rogue AP (for Zyxel Devices that support Monitor mode)

| Add Add | | | | |
|-----------------------------|----------------------------|-------------------------|----------|---------------------|
| · Pole - | MAC Address | Oexcription | | |
| 1 rogue-op | 00:A0.C5:01:23:45 | togu ee xamt | sie | |
| 14 4 Page 1 July 1 4 | Shiw 52 (W) Items | | | Displaying 1:1 if 1 |
| Friendly AP Ust Importing/E | porting | | | |
| Pile Potte Select o the p | oth for Fillendly AP Call. | Brown | Eporting | |
| | | | | |
| | | | | |

| segve, minning wy and | | |
|---|------------------|----------------------|
| ogue AP Detection Setting | | |
| 9) Enoble Rogue AP Detection | | |
| uspected Rogue AP Classification Rule | | |
| I Weak Security (Open WEP, WPA-PSK) | | |
| 2 Hidden SSD | | |
| 12 SSID Keyword | | |
| Q Add all Tall 8 Femilian | | |
| a SSID Keyword | | |
| 1 tect | | |
| ogue/Friendly AF List | | |
| O Add 21:0 9 Fermine | | |
| * Role - MAC Address | Description | |
| 1 Menaty-ap 60:31:97:70:58:51 | | |
| 2 rogue-op 00:40.C5:01:23:45 | example | 00000000 |
| 11 1 Page 1 of 1 2 21 Show 10 (Millions | | Dialeying 1 - 2 of 2 |
| ague AF List Importing/Exporting | | |
| File Futhi Levent in Me purty for Rogue AP List | Browne Exporting | |
| | | |
| sendly AP List importing/Exponing | | |
| Fie Path: Telect o Ne path for triendly AP UP | Browse. Sporting | |
| | | |
| | America | |

Figure 47 Configuration > Wire less > Rogue AP (for Zyxel Devices that support Rogue AP Detection)

Each field is described in the following table.

Table 29 Configuration > Wire less > Rogue AP

| LABEL | DESC RIPHO N |
|---|--|
| Rogue AP Detection Set | ting |
| Enable Rogue AP Detection | Select this check box to detect Rogue APs in the network. |
| Suspected Rogue AP Classification Rule | Select the check boxes (Weak Security (Open, WEP, WPA-PSK), Hidden SSID , SSID Keyword) of the characteristics an AP should have for the Zyxel Device to mark it as a Rogue AP. |
| Add | Click this to add an SSID Keyword. |
| Ed it | Select an SSID Keyword and click this button to modify it. |
| Re m o ve | Select an existing SSID keyword and click this button to delete it. |
| # | This is the SSID Keyword's index number in this list. |
| SSID Keyword | This field displays the SSID Keyword. |
| Rogue/Friendly AP List | |
| Add | Click this button to add an AP to the list and assign it either friendly or rogue status. |
| Ed it | Select an AP in the list to edit and reassign its status. |
| Remove | Select an AP in the list to remove. |
| # | This field is a sequential value, and it is not a ssociated with any interface. |

NWA50AX Use r's Guide

| LABEL | DESC RIPHO N |
|---|---|
| Ro le | This field indicates whether the selected AP is a rogue-ap or a friendly-ap . To change the AP's role, click the Edit button. |
| MAC Address | This field indicates the AP's radio MAC address. |
| De sc rip tio n | This field displays the AP's description. You can modify this by clicking the Edit button. |
| Rogue/Friendly AP List Importing/Exporting | The se controls allow you to export the current list of rogue and friendly APs or import existing lists. |
| File Path / Browse / Importing | Enter the file name and path of the list you want to import or click the Browse button to locate it. Once the File Path field has been populated, click Importing to bring the list into the Zyxel Device. |
| Exporting | Click this button to export the current list of eitherm que APs or friendly APS |
| Lapoining | |
| Apply | Click Apply to save your changes back to the Zyxel Device. |
| Re se t | C lick Reset to return the screen to its last-saved settings. |

Table 29 Configuration > Wire less > Rogue AP(continued)

10.3.1 Add/Edit Rogue/Friendly List

Click Add or select an AP and click the Edit button in the Configuration > Wireless > Rogue AP table to display this screen.

Figure 48 Configuration > Wire less > Rogue AP > Add/Edit Rogue/Friendly AP List

| Edit Rogue/Friendly Al | P List | ? X |
|-------------------------------|----------|-----------------------------|
| MAC: Description: Role: | Rogue AP | (Optional) © Friendly AP |
| | | OK Cancel |

 Each field is described in the following table.

| LABEL | DESC RIPIIO N |
|-----------------|---|
| MAC | Enter the MAC address of the AP you want to add to the list. A MAC address is a unique hardware identifier in the following hexadec imal format: xx:xx:xx:xx:xx:xx where xx is a hexadec imal number separated by colons. |
| De sc rip tio n | Enter up to 60 characters for the AP's description. Spaces and underscores are allowed. |
| Ro le | Selecteither Rogue AP or Friendly AP for the AP's role. |
| ОК | Click OK to save your changes back to the Zyxel Device. |
| Cancel | Click Cancel to close the window with changes unsaved. |

10.4 DCS

Use this screen to configure dynamic radio channelselection (see Dynamic ChannelSelection (DCS) on page 76). Click **Configuration > Wireless > DCS** to access this screen.

| Figure | 49 | Configura | tion > | Wire $ e ss >$ | DCS |
|---------|----|-------------|----------|----------------|-----|
| 1,5 410 | | 0 0 mig and | 010 11 - | 11 HO 10 DD - | PON |

| DCS | |
|------------------|--|
| General Sellings | |
| DCS Now | |
| | |
| Apply Reset | |

Each field is described in the following table.

| IABEL | DESC RIPIIO N |
|----------|---|
| DCS No w | Click this to have the Zyxel Device scan for and select an available channel immediately. |
| Apply | Click Apply to save your changes back to the Zyxel Device. |
| Re se t | Click Reset to return the screen to its last-saved settings. |

10.5 Technical Reference

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

Dynamic Channel Selection

When numerous APs broadcast within a given area, they introduce the possibility of heightened radio interference, especially if some or all of them are broadcasting on the same radio channel. If the interference becomes too great, then the network administrator must open his AP configuration options and manually change the channel to one that no other AP is using (or at least a channel that has a lower level of interference) in order to give the connected stations a minimum degree of interference. Dynamic channel selection frees the network administrator from this task by letting the AP do it automatically. The AP can scan the area around it looking for the channel with the least amount of interference.

In the 2.4 GHz spec trum, each channel from 1 to 13 is broken up into discrete 22 MHz segments that are spaced 5 MHz apart. Channel 1 is centered on 2.412 GHz while channel 13 is centered on 2.472 GHz.



Figure 50 An Example Three-Channel Deployment

Three channels are situated in such a way as to create almost no interference with one another if used exclusively: 1, 6 and 11. When an AP broadcasts on any of the se 3 channels, it should not interfere with neighboring APs as long as they are also limited to same trio.



Figure 51 An Example Four-ChannelDeployment

However, some regions require the use of other channels and often use a safety scheme with the following four channels: 1, 4, 7 and 11. While they are situated sufficiently close to both each other and the three so-called "safe" channels (1,6 and 11) that interference becomes inevitable, the severity of it is dependent upon other factors: proximity to the affected AP, signal strength, activity, and so on.

Finally, there is an alternative four channel scheme for EISI, consisting of channels 1, 5, 9, 13. This offers significantly less overlap that the other one.

Figure 52 An Alternative Four-Channel Deployment



C HAPTER 11 User

11.1 Overview

This chapterdescribes how to set up user accounts and user settings for the Zyxel Device.

11.1.1 What You Can Do in this Chapter

- The Userscreen (see Section 11.2 on page 87) provides a summary of all user accounts.
- The Setting screen (see Section 11.3 on page 89) controls default settings, login settings, loc kout settings, and other user settings for the Zyxel Device.

11.1.2 What You Need To Know

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

UserAccount

A use raccount defines the privileges of a user logged into the Zyxel Device. Use raccounts are used in controlling access to configuration and services in the Zyxel Device.

UserTypes

These are the types of user accounts the Zyxel Device uses.

| TYPE | ABILITIES | LOGIN METHOD(S) |
|--------------------|---|-----------------------|
| Admin Users | | |
| admin | Change Zyxel Device configuration (web, CLI) | WWW, TEINET, SSH, FIP |
| limite d -a d m in | Look at Zyxel Device configuration (web, CLI) | WWW, TELNET, SSH |
| | Perform basic diagnostics (CLD) | |
| Ac c e ss Use rs | | |
| use r | Used for the embedded RADIUS server and SNMPv3 user a c c e ss | |
| | Browse user-mode commands (CLI) | |

Table 32 Types of User Accounts

Note: The default **admin** account is always authenticated locally, regardless of the authentication method setting.



11.2 User Summary

The User screen provides a summary of all user accounts. To access this screen click Configuration > Object > User.

Figure 53 Configuration > Object > User

| Add sitter # hereas 18 | Chilaide Waldenryce | |
|------------------------|---------------------|------------------------|
| I - User Nome | UserType | Description |
| odmin | odmin | Administration account |
| I Page 1 Mill # 11 19 | ov EI (* terre | Districting 1 < 3 of 5 |

The following table describes the labels in this screen.

| LABEL | DESC RIPIIO N |
|--------------------------|---|
| Add | Click this to create a new entry. |
| Ed it | Double-click an entry or select it and click Edit to open a screen where you can modify the entry's setting s. |
| Remove | To remove an entry, select it and click Remove . The Zyxel Device confirms you want to remove it before doing so. |
| O b je c t Re fe re nc e | Select an entry and click Object Reference to open a screen that shows which settings use the entry. |
| # | This field is a sequential value, and it is not a ssociated with a specific user. |
| Use r Na m e | This field displays the username of each user. |
| Use r Typ e | This field displays type of user this account was configured as. admin - this user can look at and change the configuration of the Zyxel Device limited-admin - this user can look at the configuration of the Zyxel Device but not to change it user - this user has access to the Zyxel Device's services but cannot look at the configuration |
| De sc rip tio n | This field displays the description for each user. |

Table 33 Configuration > Object > User

11.2.1 Add/Edit User

The UserAdd/Edit screen allows you to create a new useraccount ore dit an existing one.

11.2.1.1 Rules for User Names

Entera username from 1 to 31 characters.

The user name can only contain the following characters:

- Alphanumeric A-z 0-9 (there is no unicode support)
- _ [und e rsc o re s]

• - [d a she s]

The first character must be alphabetical (A-Za-z), an underscore (_), or a dash (-). Other limitations on user names are:

- Usernames are case-sensitive. If you enter a user'bob' but use 'BOB' when connecting via CIFS or FIP, it will use the account settings used for 'BOB' not 'bob'.
- Usernames have to be different than usergroup names.
- Here are the reserved user names:

| • | a d m | • | a d m in | • | any | • | b in | • | daemon |
|---|----------------|---|-----------------|---|--------|---|----------|---|------------|
| • | debug | • | device haecived | • | ftp | • | games | • | halt |
| • | ld a p -use rs | • | lp | • | mail | • | news | • | no b o d y |
| • | operator | • | ra d ius-use rs | • | ro o t | • | shutdown | • | sshd |
| • | sync | • | uuc p | • | zyxel | | | | |

To access this screen, go to the Userscreen, and click Add or Edit.

| User Name 1 | odmin1 | |
|--------------|--------|--|
| User Type: | U507 🛩 | |
| Posyword: | | |
| Retype: | | |
| Description: | | |
| | | |
| | | |
| | | |
| | | |

Figure 54 Configuration > Object > User > Add/Edit A User

The following table describes the labels in this screen.

Table 34 Config uration > User > User > Add/Edit A User

| LABEL | DESC RIPIIO N |
|-----------------|---|
| Use r Na m e | Type the username for this useraccount. You may use 1-31 alphanumeric characters, underscores(_), ordashes (-), but the first character cannot be a number. This value is case- sensitive. Usernames have to be different than usergroup names, and some words are reserved. |
| Use r Typ e | Select what type of user this is. Choices are: |
| | • admin - this user can look at and change the configuration of the Zyxel Device |
| | • limited-admin - this usercan look at the configuration of the Zyxel Device but not to change it |
| | • user-this is used for embedded RADIUS server and SNMPv3 user access |
| Pa ssw o rd | Enter the password of this user account. It can consist of 4 - 63 alphanumeric characters. |
| Re typ e | Re-enter the password to make sure you have entered it correctly. |
| De sc rip tio n | Enter the description of each user, if any. You can use up to 60 printable ASC II characters. Default descriptions are provided. |

NWA50AX Use r's Guide

| IABEL | DESC RIPIIO N | | | | |
|-----------------------------------|--|--|--|--|--|
| Authentication TimeoutSettings | This field is not a vailable if the user type is user . | | | | |
| - | If you want to set a uthentic ation time out to a value other than the default settings, select Use Manual Settings then fill your preferred values in the fields that follow. | | | | |
| Le a se Tim e | This field is not a vailable if the user type is user . | | | | |
| | Enter the number of minutes this user has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the Web Configurator. | | | | |
| Reauthentication | This field is not a vailable if the user type is user . | | | | |
| ime | Type the number of minutes this user can be logged into the Zyxel Device in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike Lease Time , the user has no opportunity to renew the session without logging out. | | | | |
| ОК | Click OK to save your changes back to the Zyxel Device. | | | | |
| Cancel | Click Cancel to exit this screen without saving your changes. | | | | |

Table 34 Configuration > User > User > Add/Edit A User(continued)

11.3 Setting

This screen controls default settings, log in settings, loc kout settings, and other user settings for the Zyxel Device.

To access this screen, login to the Web Configurator, and click Configuration > Object > User > Setting.

| elouit Authentication Timeout Settings | | | |
|---|----------------------|-----------------------|--------------------------|
| 12 to a | | | |
| UserType | Lease Time | Reauthentication Time | |
| 1 admin | 1440 | 1440 | |
| 2 Emiled-admin | 1440 | 1440 | |
| 3 user | | 12 | |
| TALA TARGET AND A DUAL TRADE OF THE | 876- | | Contrained 1 - 1 - 1 - 1 |
| Unit the number of simultaneous logar | s for administration | account | |
| Madmum number per administration iccount | 1. | (1-64) | |
| Jser Lookout Settings | | | |
| The second second second | | | |
| III Enable logon retry limit | | 11.000 | |
| Maximum refry count: | 3 | (1-99) | |
| Enable logion retry Rmit | | 12.000 | |

Figure 55 Configuration > Object > User > Setting

The following table describes the labels in this screen.

| IABEL | DESC RIPTIO N | | | |
|---|--|--|--|--|
| Use r De fa ult Se tting | • | | | |
| De fa ult Authentic a tion Time out Settings | The se authentic ation time out settings are used by default when you create a new user account. They also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentic ation time out settings. | | | |
| Ed it | Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings. | | | |
| # | This field is a sequential value, and it is not associated with a specific entry. | | | |
| Use r Typ e | The se are the kinds of user account the Zyxel Device supports. admin - this user can bok at and change the configuration of the Zyxel Device limited-admin - this user can bok at the configuration of the Zyxel Device but not to change it user - this is used for embedded RADIUS server and SNMPv3 user access | | | |
| Le a se Tim e | This is the default lease time in minutes for each type of user account. It defines the number of minutes the user has to renew the current session before the user is logged out. Admin users renew the session every time the main screen refreshes in the Web Configurator. | | | |
| Re a uthe ntic a tio n Tim e | This is the default reauthentication time in minutes for each type of user account. It defines the number of minutes the user can be logged into the Zyxel Device in one session before having to log in again. Unlike Lease Time, the user has no opportunity to renew the session without logging out. | | | |

Table 35 Configuration > Object > User > Setting

NWA50AX Use r's Guide

| IABEL | DESC RIPIIO N |
|--|---|
| Limit the number of simultaneous logons for administration account | Se le c t this c he c k box if you want to set a limit on the number of simultaneous log ins by admin use is. If you do not se le c t this, admin use is c an log in as many times as the y want at the same time using the same or different IP addresses. |
| Maximum numberper administration account | This field is effective when Limit for a dministration account is checked. Type the maximum number of simultaneous log ins by each admin user. |
| Use r Lo c ko ut Se tting s | |
| Enable logon retry limit | Select this check box to set a limit on the number of times each user can log in unsuccessfully (for example, wrong password) before the IP address is locked out for a specified amount of time. |
| Maximum retry count | This field is effective when Enable logon retry limit is checked. Type the maximum number of times each user can log in unsuccessfully before the IP address is locked out for the specified lockout period . The number must be between 1 and 99. |
| Lockoutpeniod | This field is effective when Enable logon retry limit is checked. Type the number of minutes the user must wait to try to login again, if logon retry limit is enabled and the maximum retry count is reached. This number must be between 1 and 65,535 (about 45.5 days). |
| Apply | Click Apply to save the changes. |
| Re se t | Click Reset to return the screen to its last-saved settings. |

Table 35 Configuration > Object > User > Setting (continued)

11.3.1 Edit User Authentic ation Time out Settings

This screen allows you to set the default authentic ation timeout settings for the selected type of user account. These default authentic ation timeout settings also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentic ation timeout settings.

To access this screen, go to the **Configuration > Object > User > Setting** screen, selectone of the **Default Authentication Timeout Settings** entry and click the **Edit** icon.

Figure 56 User > Setting > Edit User Authentic ation Time out Settings

| - T | | |
|------------------------|----|----------------------------------|
| 18 10118 | 40 | (D-1440 minutes, 0 is unimited) |
| uthenitcotion Time: 14 | 40 | (0-1440 minutes, 0 is unlimited) |

The following table describes the labels in this screen.

| IABEL | DESC RIPHO N | | | |
|---------------------------------|---|--|--|--|
| Use r Typ e | This read-only field identifies the type of user account for which you are configuring the default settings. | | | |
| | • admin - this user can look at and change the configuration of the Zyxel Device. | | | |
| | • limited-admin-this user can look at the configuration of the Zyxel Device but not to change it. | | | |
| Le a se Tim e | Enter the number of minutes this type of user account has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. | | | |
| | Ad min users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the Renew button on their screen. If you allow access users to renew time automatically, the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires. | | | |
| Re a uthe ntic a tio n Tim e | Type the number of minutes this type of user account can be logged into the Zyxel Device in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike Lease Time , the user has no opportunity to renew the session without logging out. | | | |
| ОК | Click OK to save your changes back to the Zyxel Device. | | | |
| Cancel | Click Cancel to exit this screen without saving your changes. | | | |

Table 36 User > Setting > Edit User Authentic ation Time out Settings

C HAPTER 12 AP Pro file

12.1 Overview

This chapter shows you how to configure preset profiles for the Zyxel Device.

12.1.1 What You Can Do in this Chapter

- The Radio screen (Section 12.2 on page 94) creates radio configurations that can be used by the APs.
- The SSID screen (Section 12.3 on page 100) configures three different types of profiles for your networked APs.

12.1.2 What You Need To Know

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

Wire le ss Pro file s

At the heart of all wire less AP configurations on the Zyxel Device are profiles. A profile represents a group of saved settings that you can use a cross any number of connected APs. You can set up the following wire less profile types:

- Radio This profile type defines the properties of an AP's radio transmitter. You can have a maximum of 64 radio profiles on the Zyxel Device.
- SSID This profile type defines the properties of a single wire less network signal broadcast by an AP. Each radio on a single AP can broadcast up to 8 SSIDs. You can have a maximum of 64 SSID profiles on the Zyxel Device.
- Security This profile type defines the security settings used by a single SSID. It controls the encryption method required for a wireless client to associate itself with the SSID. You can have a maximum of 64 security profiles on the Zyxel Device.
- MAC Filtering This profile provides an additional layer of security for an SSID, allowing you to block accessorallow access to that SSID based on wire less client MAC addresses. If a client's MAC address is on the list, then it is either allowed ordenied, depending on how you set up the MAC Filter profile. You can have a maximum of 64 MAC filtering profiles on the Zyxel Device.

SSID

The SSID (Service Set IDentifier) is the name that identifies the Service Set with which a wire less station is a ssociated. Wire less stations a ssociating to the access point (AP) must have the same SSID. In other words, it is the name of the wire less network that clients use to connect to it.



WEP

WEP (Wire d Equivalent Privacy) encryption scrambles all data packets transmitted between the AP and the wire less stations associated with it in order to keep network communications private. Both the wire less stations and the access points must use the same WEP key for data encryption and decryption.

WPA2

WPA2 (IEEE 802.11i) is a wire less security standard that defines strongerencryption, authentication and key management than WPA. Key differences between WPA2 and WEP are improved data encryption and user authentication.

IEEE 802.1x

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wire less stations and encryption key management. Authentication is done using an external RADIUS server.

IEEE 802.11k/v Assisted Roaming

IEEE 802.11k is a standard for radio resource management of wireless IANs, which allows clients to request neighbor lists from the connected AP and discover the best available AP when roaming. An 802.11k neighbor list can contain up to six BSSIDs with the highest RCPI (Received Channel Power Indicator) value in both bands (5 GHz and 2.4 GHz, in the ratio of 4:2).

The IEEE 802.11v BSS Transition Management feature lets an AP automatically provide load information of the neighbor APs to clients. It helps the Zyxel Device steerclients to a suitable AP for better performance or load balancing.

12.2 Radio

This screen allows you to create radio profiles for the Zyxel Device. A radio profile is a list of settings that an Zyxel Device can use to configure its radio transmitter(s). To access this screen click **Configuration > Object > AP Profile**.

Note: You can have a maximum of 32 radio profiles on the Zyxel Device.

| 0 | Add 21ml 8 | Participa @ Section @ marifulate (\$60 | Rend Ratiniance | |
|----|------------|--|-----------------|-----------------|
| | Statue | Profile Name - | Frequency Band | |
| | 9 | Wiz_Radio_24G | 2.4G | |
| | | Wiz_Radio_5G | ðG | |
| | 9 | default | 2.4G | |
| | 4 | default2 | 8G | |
| 11 | i Page 1 u | F1 > P1 Show 10 W Apres | | Deging 1-4 of 4 |

Figure 57 Configuration > Object > AP Profile > Radio

The following table describes the labels in this screen.

| IABEL | DESC RIPTIO N | | |
|---------------------|---|--|--|
| Add | Click this to add a new radio profile. | | |
| Ed it | Click this to edit the selected radio profile. | | |
| Remove | Click this to remove the selected radio profile. | | |
| Ac tiva te | To tum on an entry, se lect it and click Activate. | | |
| Ina c tiva te | To turn off an entry, se lect it and click Inactivate. | | |
| Object Reference | Click this to view which otherobjects are linked to the selected radio profile. | | |
| # | This field is a sequential value, and it is not associated with a specific user. | | |
| Status | This field shows whether or not the entry is activated. | | |
| | A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active. | | |
| Profile Name | This field indicates the name assigned to the radio profile. | | |
| Frequency Band | This field indicates the frequency band which this radio profile is configured to use. | | |
| Apply | Click Apply to save your changes back to the Zyxel Device. | | |
| Re se t | Click Reset to return the screen to its last-saved settings. | | |

Table 37 Configuration > Object > AP Profile > Radio

12.2.1 Add/Edit Radio Profile

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

| Add Rodio Profile | | | | | 182 |
|----------------------------------|---|-------------------------|----------------|------------|----------|
| and the second second second | | | | | |
| General Settings | | | | | |
| ill Activate | | | | | |
| Picke Nome | - AND | | | | |
| 80111 Band: | 17.00 | | | | |
| Chaoriel Wildlo | 20/40/805/Hz | 2 | | | |
| Codousi teature | # 001 11 | Maruai | - O. | | |
| III Brook DCt Cleri Aware | | | | | |
| III Brocke & Girls DRL Aware | | | | | |
| E Grid Chornel Selector Mer | 194 | 2 | | | |
| () Tele interval | | | | | |
| # Schedule | | | | | |
| liohTime: | 123.00 | | | | |
| Weec Slove | (# Manual | a in treasure | E Westerd | 28 | |
| | il Print | ny III fricas | W Saturday | | |
| | W Junda | al case | | | |
| | | | | | |
| Advanced Settings | | | | | |
| Quart Intenial | # Proff | O Sorg | | | |
| W Brottle A-MPDU Apprepation | | | | | |
| III Erable A-Mttll: Apprepation | | | | | |
| #15/C12 Treemod | 2242 | (0-0347) | | | |
| Beccor manor | 100 | (40ma-1000ma) | | | |
| DTW | 1.1 | 71-0551 | | | |
| 11 Exceedigral Treehold | | | | | |
| Station Signal Threehold | -82 | alim (20/08), | | | |
| Democrate Station Threehold | 1. 48 | 100+100-108 | | | |
| C Allow Station Connection | ofter Multiple Battle | | | | |
| Itoton Rany Count | 1.1 |)) = (00) | | | |
| 11 Alow 812. Th/oc stations and | 0 | | | | |
| III Blockel DPS charmen in press | ince drappy | | | | |
| If Engine 800.71g | | | | | |
| Madicast Settings | | | | | |
| Tramamilian Mode | 10.000 | triblest a fe | ed Autoor Kine | | |
| Muticod Rate Mook | ** 01 | 012 014 | 0.24 0.34 | 04 05 | |
| | - Contraction | come of the | and the second | 1.11 ×3 | |
| Magman WCAH Rate Cornel Serie | | | | | |
| | | CONTRACTOR OF THE OWNER | ON ON | 6.40 miles | 4 |
| | | | | | - |
| | | | | C. Carro | Citilian |

Figure 58 Configuration > Object > AP Profile > Radio > Add/Edit

The following table describes the labels in this screen.

| LABEL | DESC RIPTIO N |
|----------------------------------|---|
| Hide / Show Advanced Settings | Click this to hide or show the Advanced Settings in this window. |
| General Settings | |
| Ac tiva te | Select this option to make this profile active. |
| Profile Name | Enter up to 31 alphanumeric characters to be used as this profile's name. Spaces and underscores are allowed. |
| 802.11 Band | Select whether this radio would use the 2.4 GHz or 5 GHz band. |

| Table 38 | Configuration | > Object > | A P Pro file . | > Radio | ~ | $\Delta d d / F d t$ |
|----------|----------------|------------|----------------|---------|---|----------------------|
| lable so | Coming una uon | | AP Prome - | | ~ | Add/ Edit |

| Table 38 (| Config ura tio | n > Object | > AP Pro file | > Ra d io > | • Add/Edit (continued) |
|------------|----------------|------------|---------------|-------------|------------------------|
| | | | | | |

| LABEL | DESC RIPTIO N |
|----------------------------|---|
| 802.11 Mode | Se le c t how to le t wire le ss c lie nts c o nne c t to the AP. |
| | If 802.11 Band is set to 2.4G: |
| | • 11b/g: a lows either IEEE 802.11b or IEEE 802.11g compliant WIAN devices to a ssociate with the Zyxel Device. The Zyxel Device adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices. |
| | • 11n: a llows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WIAN devices to a ssociate with the Zyxel Device. |
| | • 11ax: a lows IEEE802.11b, IEEE802.11g, IEEE802.11n, and IEEE802.11ax compliant WIAN devices to associate with the Zyxel Device. If the WIAN device isn't compatible with 802.11ax, the Zyxel Device will communicate with the WIAN device using 802.11n, and so on. |
| | ff 802.11 Band is set to 5G : |
| | • 11a: a llows only IEEE 802.11a compliant WIAN devices to associate with the Zyxel Device. |
| | • 11n: a lows both IEEE802.11n and IEEE802.11a compliant WIAN devices to associate with the Zyxel Device. |
| | • 11ac: a lows IEEE802.11n, IEEE802.11a, and IEEE802.11ac compliant WIAN devices to a ssociate with the Zyxel Device. If the WIAN device isn't compatible with 802.11ac, the Zyxel Device will communicate with the WIAN device using 802.11n, and so on. |
| | • 11ax: allows IEEE802.11n, IEEE802.11a, IEEE802.11ac, and IEEE802.11ax compliant WIAN devices to associate with the ZyxelDevice. If the WIAN device isn't compatible with 802.11ax, the ZyxelDevice will communicate with the WIAN device using 802.11ac, and so on. |
| C hannel Width | Se le c t the channel b and width you want to use for your wire less network. |
| | Se le c t 20 MHz if you want to lessen radio interference with other wire less devices in your neighborhood. |
| | Se lect 20/40 MHz to a llow the Zyxel Device to choose the channel b and width (20 or 40 MHz) that has least interference. |
| | Se le c t 20/40/80 to a llow the Zyxel Device to choose the channel band width ($20 \text{ or } 40 \text{ or } 80$) that has least interference. This option is available only when you select 11ac or 11ax in the 802.11 Mode field. |
| | Note: If the environment has poor signal-to-noise ratio (SNR), the Zyxel Device will switch to a lower bandwidth. |
| Channel Selection | This is the radio channel which the signal will use for broadcasting by this radio profile. |
| | • DCS: Choose Dynamic ChannelSelection to have the ZyxelDevice choose a radio channel that has least interference. |
| | • Manual: Choose from the available radio channels in the list. If your Zyxel Device is outdoor type, be sure to choose non-indoors channels. |
| Enable DCS Client Aware | Select this to have the Zyxel Device switch channels only when there are no clients connected to it. If there is a client connected, the Zyxel Device will not switch channels but generate a log. The Zyxel Device tries to scan and switch channels again at the end of the specified time intervalor at the scheduled time. |
| | If you disable this then the Zyxel Device switches channels immediately regardless of any client connections. In this instance, clients that are connected to the Zyxel Device when it switches channels are dropped. |
| Enable DCS Client Aware | This field is a vailable when you set Channel Selection to DCS. |
| | Select this to have the Zyxel Device switch channels only when there are no clients connected to it. If there is a client connected, the Zyxel Device will not switch channels but generate a log. The Zyxel Device tries to scan and switch channels again at the end of the specified time intervalor at the scheduled time. |
| | If you disable this then the Zyxel Device switches channels immediately regardless of any client connections. In this instance, clients that are connected to the Zyxel Device when it switches channels are dropped. |

NWA50AX Use r's Guide

| LABEL | DESC RIPTIO N |
|---|--|
| 2.4 GHz Channel Salaction Mathad | This field is a vailable when you set Channel Selection to DCS. |
| | Select how you want to specify the channels the Zyxel Device switches between for 2.4 GHz operation. |
| | Select auto to have the Zyxel Device display a 2.4 GHz Channel Deployment field you can use to limit channel switching to 3 or 4 channels. |
| | Select manual to select the individual channels the Zyxel Device switches between. |
| | Note: The method is automatically set to auto when no channel is selected or any one of the previously selected channels is not supported. |
| C ha nne l ID | This field is a vailable only when you set Channel Selection to DCS and set 2.4 GHz Channel Selection Method to manual. |
| | Select the channels that you want the Zyxel Device to use. |
| 2.4 G Hz Channel De p lo ym e nt | This is a vailable when you set Channel Selection to DCS and the 2.4 GHz Channel Selection Method is set to auto . |
| | Select Three-Channel Deployment to limit channel switching to channels 1,6, and 11, the three channels that are sufficiently attenuated to have almost no impact on one another. In other words, this allows you to minimize channel interference by limiting channel-hopping to the se three "safe" channels. |
| | Se le ct Four-Channel De ployment to limit channel switching to four channels. Depending on the country domain, if the only allo wable channels are 1-11 then the Zyxel Device uses channels 1, 4, 7, 11 in this configuration; otherwise, the Zyxel Device uses channels 1, 5, 9, 13 in this configuration. Four channel de ployment expands your pool of possible channels while keeping the channel interference to a minimum. |
| Enable 5 GHz DFS Aware | This field is a vailable only when you select 5G in the 802.11 Band field, set Channel Selection to DCS and set 5 GHz Channel Selection Method to auto. |
| | Select this if your APs are operating in an area known to have RADAR devices. This allows the Zyxel Device to downgrade its frequency to below 5 GHz in the event RADAR signal is detected, thus preventing it from interfering with that signal. |
| | Enabling this forces the AP to select a non-DFS channel. |
| 5 G Hz Channel Se le c tion Me tho d | Select how you want to specify the channels the Zyxel Device switches between for 5 GHz operation. |
| | Select Auto to have the Zyxel Device automatically select the best channel. |
| | Select manual to select the individual channels the Zyxel Device switches between. |
| | Note: The method is automatically set to auto when no channel is selected or any one of the previously selected channels is not supported. |
| Channel ID | This field is a vailable only when you set Channel Selection to DCS and set 5 GHz Channel Selection Method to manual. |
| | Select the channels that you want the Zyxel Device to use. |
| Time Interval | Select this option to have the Zyxel Device survey the other APs within its broadcast radius at the end of the specified time interval. |
| DCSTime Interval | This field is a vailable when you set Channel Selection to DCS and select the Time Interval option. |
| | Enter a number of minutes. This regulates how often the Zyxel Device surveys the other APs within its broad cast radius. If the channel on which it is currently broad casting suddenly comes into use by another AP, the Zyxel Device will then dynamically select the next available clean channel or a channel with lower interference. |

Table 38 Configuration > Object > AP Profile > Radio > Add/Edit (continued)

| IABEL | DESC RIPTIO N |
|-----------------------------|--|
| Sc he d ule | Select this option to have the Zyxel Device survey the other APs within its broadcast radius at a specific time on selected days of the week. |
| Start Time | Specify the time of the day (in 24-hour format) to have the Zyxel Device use DCS to automatically scan and find a less-used channel. |
| Week Days | Select each day of the week to have the Zyxel Device use DCS to automatically scan and find a less-used channel. |
| Advanced Settings | |
| Guard Interval | This field is a vailable only when the channel width is $20/40MHz$ or $20/40/80MHz$ and the 802.11 Mode is either $11n$ or $11ac$. |
| | Set the guard interval for this radio profile to either short or long. |
| | The guard interval is the gap introduced between data transmission from users in order to reduce interference. Reducing the interval increases data transferrates but also increases interference. Increasing the interval reduces data transferrates but also reduces interference. |
| Enable A-MPDU | This field is not available when you set 802.11 Mode to $11a$ or $11b/g$. |
| Aggregation | Select this to enable A-MPDU aggregation. |
| | Message Protocol Data Unit (MPDU) aggregation collects Ethemet frames along with their 802.11n headers and wraps them in a 802.11n MAC header. This method is useful for increasing bandwidth throughput in environments that are prone to high error rates. |
| Enable A-MSDU | This field is not available when you set 802.11 Mode to $11a$ or $11b/g$. |
| Aggiegation | Select this to enable A-MSDU aggregation. |
| | Mac Service Data Unit (MSDU) aggregation collects Ethemet frames without any of their 802.11n headers and wraps the header-less payload in a single 802.11n MAC header. This method is useful for increasing bandwidth throughput. It is also more efficient than A-MPDU except in environments that are prone to high emorrates. |
| RIS/ C IS Thre sho ld | Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) be fore it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions). |
| | A wire less client sends an RIS for all packets larger than the number (of bytes) that you enter here. Set the RIS/CIS equal to or higher than the fragmentation threshold to turn RIS/CIS off. |
| Be a c o n Inte rva l | When a wire lessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the Zyxel Device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. A high value helps save current consumption of the access point. |
| D'IIM | De live ry Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255. |
| Enable Signal Threshold | Select the check box to use the signal threshold to ensure wire less clients receive good throughput. This allows only wire less clients with a strong signal to connect to the AP. |
| | Clear the check box to not require wire less clients to have a minimum signal strength to connect to the AP. |
| Station Signal Threshold | Set a minimum client signal strength. A wire less client is allowed to connect to the AP only when its signal strength is stronger than the specified threshold. |
| | -20 dBm is the strongest signal you can require and -105 is the weakest. |

Table 38Configuration > Object > AP Profile > Radio > Add/Edit (continued)

| LABEL | DESC RIPTIO N |
|---|---|
| Disa sso c ia te Sta tio n Thre sho ld | Set a minimum kick-off signal strength. When a wire less client's signal strength is lower than the specified threshold, the Zyxel Device disconnects the wire less client from the AP. |
| | -20 dBm is the strongest signal you can require and -105 is the weakest. |
| Allow Station Connection after Multiple Retries | Select this option to allow a wireless client to try to associate with the AP again after it is disconnected due to weak signal strength. |
| Sta tio n Re try C o unt | Set the maximum number of times a wireless client can attempt to re-connect to the AP |
| Allow 802.11n/ ac/ax stations only | Se le c t this option to a llow only 802.11 n/ac/ax c lients to connect, and reject 802.11a/b/g c lients. |
| Blacklist DFS | This field is a vailable if 802.11 Band is set to 5G and Channel Selection is set to DCS. |
| pre sence of radar | Enable this to temporarily blacklist the wire less channels in the Dynamic Frequency Selection (DFS) range whenever a radar signal is detected by the Zyxel Device. |
| Enable 802.11d | Clear the checkbox to prevent the AP from broadcasting a country code, also called a country Information Element (IE), in beacon frames. This makes the AP incompatible with 802.11d networks and devices. |
| | 802.11d is a WiFi network specification that allows the AP to broadcast a country code to WiFi client. The country code indicates where the AP is located. If WiFi clients are unable to connect to the AP due to an incompatible country code, you should disable 802.11d. |
| Multic a st Se tting s | |
| Tra nsmissio n Mode | Specify how the Zyxel Device handles wire less multicast traffic. |
| | Se le ct Multic a st to Unic a st to broadcast wire less multic a st traffic to all of the wire less clients as unic a st traffic. Unic a st traffic dynamic ally changes the data rate based on the application's bandwidth requirements. The retransmit mechanism of unic ast traffic provides more reliable transmission of the multicast traffic, although it also produces duplicate packets. |
| | Select Fixed Multicast Rate to send multicast traffic to all wireless clients at a single data rate. You must know the multicast application's bandwidth requirements and set it in the following field. |
| Multic a st Ra te (Mb p s) | If you set Transmission Mode to Fixed Multic ast Rate , select a data rate at which the Zyxel Device transmits multic ast packets to wire less clients. For example, to deploy 4 Mbps video, select a fixed multic ast rate higher than 4 Mbps. |
| WLAN Rate Control Setting | Sets the minimum data rate that 2.4G hz WiFi c lients can connect at, in Mbps. At the time of write, a llowed values are: 1, 2,5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54. |
| | Sets the minimum data rate that 5Ghz WiFiclients can connect at, in Mbps. At the time of write, allowed values are: 6,9, 12, 18, 24, 36, 48, 54. |
| | Increasing the minimum data rate can reduce network overhead and improve WiFi network performance in high density environments. However, WiFi clients that do not support the minimum data rate will not be able to connect to the AP. |
| OK | Click OK to save your changes back to the Zyxel Device. |
| Cancel | Click Cancel to exit this screen without saving your changes. |

Table 38 Configuration > Object > AP Profile > Radio > Add/Edit (continued)

12.3 SSID

The SSID screens allow you to configure three different types of profiles for your networked APs: an SSID list, which can assign specific SSID configurations to your APs; a security list, which can assign specific

encryption methods to the APs when allowing wire less clients to connect to them; and a MAC filter list, which can limit connections to an AP based on wire less clients MAC addresses.

12.3.1 SSID List

This screen a lows you to create and manage SSID configurations that can be used by the APs. An SSID, or Service Set IDentifier, is basically the name of the wireless network to which a wireless client can connect. The SSID appears as readable text to any device capable of scanning for wireless frequencies (such as the WiFi adapter in a laptop), and is displayed as the wireless network name when a person makes a connection to it.

To access this screen click Configuration > Object > AP Profile > SSID > SSID List.

Note: You cannot add or remove an SSID profile after running the setup wizard.

| Figure 59 | $C \circ nfig uration > O b ject > AP Profile > SSID > SSID List (Default)$ | |
|-----------|---|--|
| | | |

| 5550 B | it Secu | ntry List M | AC filter Ust | | | | |
|--------|--------------------|-------------|----------------|--------|-----------|--------|--------------------|
| D Sun | nmory | | | | | | |
| D AD | a 2147 8 (* | New Botest | Internet | | | | |
| - F | Falle Nation + | 1000 | Security Peola | Laon - | WACTUMPAS | VLAN E | |
| 1.1 | iefault | Alt26-lext | thursleib. | WMW. | disable | 1 | |
| 1. 1 | Page Fiot | F P P Stow | an (w) Steeps | | | | Diskoying 1 . 1 of |

| - | | market first | Art Dillor Link | | | | |
|------|---------------|---------------|-----------------|---------|--------------|-------|--|
| | 100 | econtry can a | AAC PROFILE | | | | |
| ID I | lummary | | | | | | |
| 1 | East Colject | Reference | | | | | |
| | (TOTAL INCOME | - 110 | Socurity Hotel | 001 | MMC Claima - | VIAND | |
| | W2.110.1 | Typet | We_SEC_Profil_, | WMM | chable | 1 | |
| E | WE,310,2 | Zynori | Walsec_Profil | Weater | distrike | 1 | |
| | W2_55ED_3 | Zynet | We_SEC_Profil | WMM | disatsie | 1 | |
| | W2,350,4 | 29000 | WILSEC_Profil | WMM | disciple | | |
| ł. | W2_SSE_5 | 2 yiel | Wajsed_Profil | WMM | dhobie | 1 | |
| | W2,550_6 | Zyssel | Wa_SEC_Profil | WMM | ditoble | 1 | |
| 0 | W2_330_7 | Zyroet | Wa_SEC_Profil | WMMA | choole | 1 | |
| | W2,STELS | Zynel | We_SEC_Profil_, | WMM | ditable | 1 | |
| | ctadea.it | 2-mmi-8021-A | claim # | 100.064 | chickie | 1 | |

Figure 60 Configuration > Object > AP Profile > SSID > SSID List (After wizard setup)

The following table describes the labels in this screen.

| | Table 39 | Config ura tion | > Object > | AP Pro file | > SSID > | SSID List |
|--|----------|-----------------|------------|-------------|----------|-----------|
|--|----------|-----------------|------------|-------------|----------|-----------|

| IABEL | DESC RIPTIO N |
|-------|--|
| Add | Click this to add a new SSID profile. |
| | This button is not a vailable after you configure the Zyxel Device using the wizard. |
| Ed it | C lick this to edit the selected SSID profile. |

| LABEL | DESC RIPIIO N |
|--------------------------|---|
| Remove | Click this to remove the selected SSID profile. |
| | This button is not a vailable after you configure the Zyxel Device using the wizard. |
| Object Reference | Click this to view which otherobjects are linked to the selected SSID profile (for example, radio profile). |
| # | This field is a sequential value, and it is not a ssociated with a specific user. |
| Profile Name | This field indicates the name assigned to the SSID profile. |
| SSID | This field indicates the SSID name as it appears to wireless clients. |
| Se c urity Pro file | This field indicates which (if any) security profile is a ssociated with the SSID profile. |
| QoS | This field indicates the QoS type associated with the SSID profile. |
| MAC Filtering Profile | This field indicates which (if any) MAC filter Profile is a ssociated with the SSID profile. |
| VIAN ID | This field indicates the VIAN ID associated with the SSID profile. |

Table 39 Configuration > Object > AP Profile > SSID > SSID List (continued)

12.3.2 Add/Edit SSID Profile

This screen allows you to create a new SSID profile ore dit an existing one. To access this screen, click the Add button or select a SSID profile from the list and click the Edit button.

| | | _ | | | 0 | | | |
|---|--|----------------------|---------------------------------|--|--|---|--|--|
| SIDI. | | 2yxel | | | | | | |
| ecurity Ptofile: | | deto | ult . | | 0 | 0 | 10 | |
| AAC Filtering Pro | oflec | dijat | de | | 1 | 0 | | |
| Sol: | | WINN | À | | 2 | | | |
| tote Limiting Pe | er Station | Iraffic | Eate | ie | | | | |
| Downlink: | | 0 | | mope 🗮 | (0+1) | 0,0161 | (betimbre | |
| Uplink: | | Ô | | mope | 10-14 | 0. 0 is : | (betimized) | |
| (LAN ID: | | 1 | | | pi- | 4094) | | |
| 1 RECEILING ARE | ined #oc | ming | | | | | | |
| Schedule 550 | 5 | | | | | | | |
| § Schedule 550 Sunday: |) (enable | | tem: | 00:00 . (*) | for: | 24:00 | 17 | |
| 5 Schedule 556 Sundayi Mandayi | enable enable | NON . | hom: | 00:00 1 | for: for: | 24:00 24:00 | | |
| Schedule 550 Sunday: Monday: Tuesday: | enable enable enable | 10.10.10 | tom: tom: | 00:00 * 00:00 * 00:00 * | 50. 50. 50. | 24:00 24:00 24:00 | | |
| Eschedule 550 Sundayi Mandayi Tuesdayi Wednesday: | enable enable enable enable | N IN IN IN | tom tom tom | 00:00 m 00:00 m 00:00 m | 5 5 5 5 | 24:00 24:00 24:00 24:00 | 1 (1 (1 (1 (1 (1 (1 (1 (1 (1 (1 (1 (1 (1 | |
| Schedule SSC Sunday: Monday: Tuesday: Wednesday: Thursday: | enable enable enable enable enable | IN SECTOR DOTATION | kom kom kom | 00:00 = 00:00 = 00:00 = 00:00 = | 2 2 2 2 2 | 24:00 24:00 24:00 24:00 24:00 | | |
| § Schedule 550 Sunday: Manday: Tuesday: Wednesday: Thursday: Priday: | enable enable enable enable enable enable | INCIRCIPATING INCIRC | kom hom hom kom | 00:00 00 | fo: fo: fo: fo: fo: fo: | 24:00 24:00 24:00 24:00 24:00 24:00 | | |
| 6 Schedule 550 Sunday: Ntonday: Tuesday: Wednesday: Thursday: Priday: Saturday: | enable enable enable enable enable enable enable | | kom kom kom kom kom | 00:00 * 00:00 * 00:00 * 00:00 * 00:00 * 00:00 * | | 24:00 24:00 24:00 24:00 24:00 24:00 24:00 | | |

Figure 61 Configuration > Object > AP Profile > SSID > SSID List > Add/Edit SSID Profile (NWA50AX)

The following table describes the labels in this screen.

| Table 40 Co | onfiguration | >Object> | AP Pro file | > SSID > | SSID List > | Add/Edit | SSID Pro file |
|-------------|--------------|----------|-------------|----------|-------------|----------|---------------|
|-------------|--------------|----------|-------------|----------|-------------|----------|---------------|

| LABEL | DESC RIPTIO N |
|---------------------|--|
| Createnew Object | Select an object type from the list to create a new one associated with this SSID profile. |
| Profile Name | Enterup to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed. |
| SSID | Enter the SSID name for this profile. This is the name visible on the network to wire less clients. Enter up to 32 characters, spaces and underscores are allowed. |
| Se c urity Pro file | Select a security profile from this list to a ssociate with this SSID. If none exist, you can use the Create new Object menu to create one. |
| | Note: It is highly recommended that you create security profiles for all of your SSIDs to enhance your network security. |

| LABEL | DESC RIPIIO N |
|--------------------------------------|---|
| MAC Filtering Profile | Select a MAC filtering profile from the list to a ssociate with this SSID. If none exist, you can use the Create new Object menu to create one. |
| | MAC filtering a llows you to limit the wire less clients connecting to your network through a particular SSID by wire less client MAC addresses. Any clients that have MAC addresses not in the MAC filtering profile of a llowed addresses are denied connections. |
| | The disable setting means no MAC filtering is used. |
| QoS | Select a Quality of Service (QoS) access category to associate with this SSID. Access categories minimize the delay of data packets across a wireless network. Certain categories, such as video orvoice, are given a higher priority due to the time sensitive nature of their data packets. |
| | QoSaccesscategories are as follows: |
| | disable: Tums off QoS for this SSID. All data packets are treated equally and not tagged with access categories. |
| | WMM: Enables automatic tagging of data packets. The Zyxel Device assigns access categories to the SSID by examining data as it passes through it and making a best guess effort. If something looks like video traffic, for instance, it is tagged as such. |
| | WMM_VOICE: All wire less traffic to the SSID is tagged as voice data. This is recommended if an SSID is used for activities like placing and receiving VoIP phone calls. |
| | WMM_VIDEO : All wire less traffic to the SSID is tagged as video data. This is recommended for activities like video conferencing. |
| | WMM_BEST_EFFORE All wire less traffic to the SSID is tagged as "best effort," meaning the data travels the best route it can without displacing higher priority traffic. This is good for activities that do not require the best bandwidth throughput, such as surfing the Internet. |
| | WMM_BACKG ROUND: All wire less traffic to the SSID is tagged as low priority or "background traffic", meaning all other access categories take precedence over this one. If traffic from an SSID does not have strict throughput requirements, then this access category is recommended. For example, an SSID that only has network printers connected to it. |
| Rate Limiting | |
| Do w nlink | Define the maximum incoming transmission data rate (either in mbps or kbps) on a per-station basis. |
| Uplink | De fine the maximum outgoing transmission data rate (either in mbps or kbps) on a per-station basis. |
| VLAN ID | Enter a VIAN ID for the Zyxel Device to use to tag traffic originating from this SSID. |
| Hidden SSID | Se le ct this if you want to "hide" your SSID from wire less clients. This tells any wire less clients in the vic inity of the AP using this SSID profile not to display its SSID name as a potential connection. Not all wire less clients respect this flag and display it anyway. |
| | When a SSID is "hidden" and a wire less client cannot see it, the only way you can connect to the SSID is by manually entering the SSID name in your wire less connection setup screen(s) (the se vary by client, client connectivity software, and operating system). |
| Enable Intra-BSS Traffic Blocking | Select this option to prevent crossover traffic from within the same SSID on the Zyxel Device. |
| Enable U-APSD | Se le c t this option to enable Unschedule d Automatic Power Save Delivery (U-APSD), which is a lso known as WMM-Power Save. This helps increase battery life for battery-powered wire less clients connected to the Zyxel Device using this SSID profile. |
| 802.11k/v Assiste d Ro a ming | Se le ct this option to enable IEEE 802.11k/v assisted roaming on the Zyxel Device. When the connected clients request 802.11k neighbor lists, the Zyxel Device will response with a list of neighbor APs that can be candidates for roaming. |
| Schedule SSID | Select this option and set whether the SSID is enabled ordisabled on each day of the week. You also need to select the hourand minute (in 24-hourformat) to specify the time period of each day during which the SSID is enabled/enabled. |

Table 40 Configuration > Object > AP Profile > SSID > SSID List > Add/Edit SSID Profile (continued)

NWA50AX Use r's Guide

| | Table 40 | Configuration > | > Object > AP | Pro file > SSID > | SSID List > Ad d | Ed it SSID Pro file | (continue d |
|--|----------|-----------------|---------------|-------------------|------------------|---------------------|-------------|
|--|----------|-----------------|---------------|-------------------|------------------|---------------------|-------------|

| IABEL | DESC RIPIIO N |
|--------|---|
| ОК | Click OK to save your changes back to the Zyxel Device. |
| Cancel | Click Cancel to exit this screen without saving your changes. |

12.4 Security List

This screen allows you to manage wire less security configurations that can be used by your SSIDs. Wire less security is implemented strictly between the AP broadcasting the SSID and the stations that are connected to it.

To access this screen click Configuration > Object > AP Profile > SSID > Security List.

Note: You can have a maximum of 32 security profiles on the Zyxel Device.

Figure 62 Configuration > Object > AP Profile > SSID > Security List (NWA50AX)

| lodio | SSID | | | |
|-------------|---------------|-----------------|--------------|-------------------|
| SSID List | Security List | MAC File | r Liat | |
| curity Sumr | mary | | | |
| Q Add 21 | int Blancin S | Colient fullion | 14 Sec. 19 | |
| · Puster | Norme - | | Toourly Mode | 1 |
| defou | ή. | | Open | |
| 14 - 8 Proc | A LINET & A | Thow It is | Terco | Depaying 1+1 of 1 |

The following table describes the labels in this screen.

| Table 41 | Configuration > | Object> | AP Pro file | > SSID : | > Se c urity List |
|----------|-----------------|---------|-------------|----------|-------------------|
|----------|-----------------|---------|-------------|----------|-------------------|

| LABEL | DESC RIPIIO N |
|---------------------|--|
| Add | Click this to add a new security profile. |
| Ed it | C lick this to edit the selected security profile. |
| Remove | Click this to remove the selected security profile. |
| Object Reference | Click this to view which otherobjects are linked to the selected security profile (for example, SSID profile). |
| # | This field is a sequential value, and it is not a ssociated with a specific user. |
| Pro file Name | This field indicates the name assigned to the security profile. |
| Se c unity Mode | This field indicates this profile's security mode (if any). |

12.4.1 Add/Edit Security Profile

This screen allows you to create a new security profile ore ditan existing one. To access this screen, click the **Add** button or select a security profile from the list and click the **Edit** button.

Note: These screens' options change based on the Security Mode selected.

Figure 63 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile > Security Mode: none (NWA50AX)

| O Edit Security Profile defaul | £ | | 12156 |
|--------------------------------|---------|----------------------|--------------|
| Hide Advanced Selfings | | | |
| General Settings | | | |
| Profile Home. | data di | | |
| Security Mode: | none | 16 | |
| Authentication Settings | | | |
| Advance | | | |
| ide fimedult: | 200 | 30-2000 seconds | |
| Advance Ide fimeovit | 200 | 1 (30-30000 seconds) | |
| ide timedut: | 300 | 10-2000 tecondti | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | I STORES |
| | | | Records Ave. |

The following table describes the labels in this screen.

Ta b le 42 Config ura tion > O b je c t > AP Profile > SSID > Se c unity List > Ad d/ Ed it Se c unity Profile > Se c unity Mode: none

| LABEL | DESC RIPTIO N | | | | |
|--------------------|--|--|--|--|--|
| General Settings | | | | | |
| Profile Name | Enterup to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed. | | | | |
| Security Mode | Select a security mode from the list: none, enhanced-open, wep, wpa2, wpa2-mix or wpa3. | | | | |
| | enhanced-open uses Opportunistic Wire less Encryption (OWE) which encrypts the wire less connection when possible. | | | | |
| Advance | | | | | |
| Note: Click on the | Show Advanced Settings button to show the fields describe below. | | | | |
| Id le Timeout | Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued. | | | | |
| ОК | Click OK to save your changes back to the Zyxel Device. | | | | |
| Cancel | Click Cancel to exit this screen without saving your changes. | | | | |

Figure 64 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile > Security Mode: enhanced-open

| C Edit Security Profile default | | | 1100 |
|---------------------------------|----------------------|--------------------|--------|
| Show Advanced Settings | | | |
| General Settings | | | |
| Profile Nome: | defout | | |
| Security Mode: | enhanced-oper | 1 | |
| Authentication Settings | | | |
| 2 Transform Marche | | | |
| Adyonce | | | |
| Idle timeout: | 300 | (30-30000 seconds) | |
| SI Monopement Northe Public | iction is Ophonia ia | Paralent. | |
| | | 1/2/2011/201 | |
| | | | |
| | | | |
| | | | |
| | | OK | Cancel |

The following table describes the labels in this screen.

| Table 43 | Configuration > Object > | AP Pro file > 5 | SSID > Se c urity | List > Add/ | 'Ed it Se c urity | Pro file > S | se c urity |
|----------|--------------------------|-------------------|-------------------|-------------|-------------------|--------------|------------|
| Mode: en | ıhanced-open | | | | | | |

| IABEL | DESC RIPTIO N | | | |
|--------------------------|---|--|--|--|
| General Settings | | | | |
| Profile Name | Enterup to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed. | | | |
| Se c unity Mode | Select a security mode from the list: none, enhanced-open, wep, wpa2, wpa2-mix or wpa3. | | | |
| | enhanced-open uses Opportunistic Wire less Encryption (OWE) which encrypts the wire less connection when possible. | | | |
| Authentic ation Settings | | | | |
| Transition Mode | Enable this for backwards compatibility. This option is only available if the Security Mode is wpa3 or enhanced-open. This creates two virtual APs (VAPs) with a primary (wpa3 or enhanced-open) and fallback (wpa2 or none) security method. | | | |
| | If the Security Mode is wpa3, enabling this will force Management Frame Protection to be set to Optional. If this is disabled or if the Security Mode is enhanced-open, Management Frame Protection will be set to Required. | | | |
| Ad vanc e | | | | |
| Note: Clickon the Sho | wAdvanced Settings button to show the fields describe below. | | | |
| Idle Timeout | Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued. | | | |

| IABEL | DESC RIPTIO N |
|--|--|
| Ma na g e m e nt Fra m e Pro te c tio n | This field is a vailable only when you select wpa2 in the Security Mode field and set Cipher Type to aes . |
| | Data frames in 802.11 WLANs can be encrypted and authentic ated with WEP, WPA or WPA2. But 802.11 management frames, such as beacon/probe response, association request, association response, de-authentic ation and disassociation are always unauthentic ated and unencrypted. IEEE 802.11 w Protected Management Frames allows APs to use the existing security mechanisms (encryption and authentic ation methods defined in IEEE 802.11 ii WPA/WPA2) to protect management frames. This helps prevent wire less Do S attacks. Select the check box to enable management frame protection (MFP) to add security to 802.11 management frames. |
| | Select Optional if you do not require the wireless clients to support MFP. Management frames will be encrypted if the clients support MFP. |
| | Se le c t Require d and wire less c lients must support MFP in order to join the Zyxel Device's wire less network. |
| ОК | Click OK to save your changes back to the Zyxel Device. |
| Cancel | Click Cancel to exit this screen without saving your changes. |

 $\label{eq:star} \begin{array}{ll} Table \ 43 & Configuration > Object > AP \ Profile > SSID > Security \ List > Add/Edit Security \ Profile > Security \ Mode: enhanced-open (continued) \end{array}$

Figure 65 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile > Security Mode: wep (NWA50AX)

| Edit Security Profile default | | | 141 |
|--|---|--|-----|
| Hae Advanced Settings | | | |
| General Selfings | | | |
| Profile Nome: | Select. | | |
| Security Mode: | wep | 15 | |
| Authentication Settings | | | |
| Authenlication Type: | open | 8 | |
| Keysength: | WEP-64 | | |
| 44-bit Enter 3 ASCI character 125-bit Enter 13 ASCI character | t or 10 hexadecimid of tes or 26 hexadecimic | cractes (G-F, 'A-F) for each key (1-4), characters (D-F, 'A-F) for each key (1-4) | |
| Key 1 | - | 0 | |
| () Key 2 | | | |
| © Kay-3 | | | |
| C Fay 4 | | | |
| E Advance ide timeout: | 300 | [30-30000 seconds] | _ |
| 1 | | | |
| | | | |
| | | | |
| | | | |
| | | | |
Table 44 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile > Security Mode: we p

| LABEL | DESC RIPTIO N |
|--------------------------|--|
| General Settings | |
| Pro file Name | Enterup to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed. |
| Se c unity Mode | Select a security mode from the list: none, enhanced-open, wep, wpa2, wpa2-mix or wpa3. |
| | enhanced-open uses Opportunistic Wire less Encryption (OWE) which encrypts the wire less connection when possible. |
| Authentic ation Settings | |
| Authentic ation Type | Select a WEP authentic ation method. Choices are Open or Share key. |
| Key Length | Select the bit-length of the encryption key to be used in WEP connections. |
| | If you select WEP-64: |
| | • Enter 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x11AA22BB33) for each Key used. |
| | or |
| | • Enter 5 ASC II characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for each Key used. |
| | If you select WEP-128: |
| | • Enter 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x00112233445566778899AABBCC) for each Key used. |
| | or |
| | • Enter 13 ASC II c haracters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey 12345678) for each Key used. |
| Ke y 1~4 | Based on your Key Length selection, enter the appropriate length hexadecimalor ASC II key. |
| Ad vanc e | |
| Note: Click on the Sho | wAdvanced Settings button to show the fields describe below. |
| Idle Timeout | Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued. |
| ОК | Click OK to save your changes back to the Zyxel Device. |
| Cancel | Click Cancel to exit this screen without saving your changes. |

Figure 66 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile > Security Mode: wpa2 (NWA50AX)

| Hide Advanced Settings Oeneral Settings Profile Home: Security Mode: Authenflootion Settings Pre-Shared Keyt Oeneral Keyt | |
|--|--|
| Oenerol Sellings Profile reame: Security Mode: Authenflootion Sellings • Pershared Reyt | |
| Profile Home: Security Mode: Authenfloction Settings Pre-Shored Keyt | |
| Security Mode: wpo2 Authenflootion Settings | |
| Authenfloction Settings | |
| Penonat Pre-Graned Keyt | |
| Pe-Dicred Keyl | |
| and a lot of the | |
| (4) Advorce | |
| Cipher Type: Des m | |
| Ide tmeput: 300 (30-3000 second) | |
| Group Key Updote Timer: 30000 (Ro-30000 seconds) | |
| Management frame thatection | |

The following table describes the labels in this screen.

 $\label{eq:star} \begin{array}{ll} \mbox{Ta b le 45} & \mbox{C on fig ura tio } n > \mbox{O b je c t > AP Pro file > SSID > Se c unity List > AAd d/Ed it Se c unity Pro file > Se c unity Mo de : wp a 2 \end{array}$

| IABEL | DESC RIPIIO N |
|------------------------------|---|
| General Settings | · |
| Profile Name | Enterup to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only formanagement purposes. Spaces and underscores are allowed. |
| Se c unity Mode | Select a security mode from the list: none, enhanced-open, wep, wpa2, wpa2-mix or wpa3. |
| | enhanced-open uses Opportunistic Wire less Encryption (OWE) which encrypts the wire less connection when possible. |
| Authentic ation Settings | |
| Pe rso na l | This field is a vailable when you select the wpa2, wpa2-mix or wpa3 security mode. |
| | Select this option to use a Pre-Shared Key (PSK) with WPA2 encryption or Simultaneous Authentication of Equals (SAE) with WPA3 encryption. |
| Pre-Shared Key | Enter a pre-shared key of between 8 and 63 case-sensitive ASC II characters (including spaces and symbols) or 64 hexadecimal characters. |
| Ad vanc e | · |
| Note: Clickon the Sho | w Advanced Settings button to show the fields describe below. |

| LABEL | DESC RIPIIO N |
|--------------------------------|---|
| C ip her Typ e | Select an encryption cipher type from the list. |
| | • auto - This automatically chooses the best available cipherbased on the cipherin use by the wire less client that is attempting to make a connection. |
| | • aes - This is the Advanced Encryption Standard encryption method. It is a more recent development over TKIP and considerably more robust. Not all wireless clients may support this. |
| Idle Timeout | Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued. |
| Group Key Update Timer | Enter the interval (in seconds) at which the AP updates the group WPA2 encryption key. |
| Pre-Authentication | Se le c t Enable to a llow pre-authentic a tion. O the rwise, se le c t Disable. |
| Management Frame Protection | This field is a vailable only when you select wpa2 in the Security Mode field and set Cipher Type to aes . |
| | Da ta frames in 802.11 WIANs can be encrypted and authentic ated with WEP, WPA or WPA2. But 802.11 management frames, such as beacon/pmbe msponse, association request, association ne sponse, de-authentic ation and disassociation are always unauthentic ated and unencrypted. IEEE 802.11 w Protected Management Frames allows APs to use the existing security mechanisms (encryption and authentic ation methods defined in IEEE 802.11 ii WPA/WPA2) to protect management frames. This helps prevent wire less Do S attacks. |
| | Select the checkbox to enable management frame protection (MFP) to add security to 802.11 management frames. |
| | Select Optional if you do not require the wireless clients to support MFP. Management frames will be encrypted if the clients support MFP. |
| | Se le c t Require d and wire less c lients must support MFP in order to join the Zyxel Device's wire less network. |
| OK | Click OK to save your changes back to the Zyxel Device. |
| Cancel | Click Cancel to exit this screen without saving your changes. |

Table 45 Configuration > Object > AP Profile > SSID > Security List > AAdd/Edit Security Profile > Security Mode: wpa2(continued)

| Figure 67 | Configuration > Object > | AP Pro file > SSID > | > Security List > | Add/Edit Security | Pro file > Se c urity |
|-----------|--------------------------|----------------------|-------------------|-------------------|-----------------------|
| Mode | : wpa2-mix (NWA50AX) | | | | |

| | | | Hate Advanced Settings |
|--------------|--|---------------------|--|
| | | | General Infines |
| | | | General senings |
| | | and a second | Polienone |
| | | (wpc2-mil | Security Mode: |
| | | | Authentication Lettings |
| | | | # Fetond |
| | 0 | | Pre-Dhored Key: |
| | | OHE | Advance Cloher Type: |
| diji | [30-30000 seconds] | 300 | ide firreout: |
| daj | iji0-30000 seconda | 20000 | Group Key update Timer: |
| diji diji | (30-30000 seconds (30-30000 seconds | 040 300 30000 | Cipher Type. Idle timeout: Group Key update Timer. |

 $\label{eq:approx} \begin{array}{ll} \mbox{Ta b le } 46 & \mbox{C on fig ura tio } n > \mbox{O b je c } t > \mbox{AP Pro file } > \mbox{SSID } > \mbox{Se c unity List } > \mbox{AAd } d/\mbox{Ed it Se c unity Pro file } > \mbox{Se c unity Mo de : } wp a 2-mix \end{array}$

| IABEL | DESC RIPIIO N |
|--------------------------|--|
| General Settings | |
| Profile Name | Enterup to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed. |
| Se c unity Mode | Select a security mode from the list: none, enhanced-open, wep, wpa2, wpa2-mix or wpa3. |
| | enhanced-open uses Opportunistic Wire less Encryption (OWE) which encrypts the wire less connection when possible. |
| Authentic ation Settings | |
| Pe rso na l | This field is a vailable when you select the wpa2 , wpa2-mix or wpa3 security mode. |
| | Select this option to use a Pre-Shared Key (PSK) with WPA2 encryption or Simultaneous Authentication of Equals (SAE) with WPA3 encryption. |
| 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. |
| Advanc e | |

Note: Clickon the Show Advanced Settings button to show the fields describe below.

| Table 46 | Configuration > Object > | AP Pro file $>$ | \sim SSID > | Se c urity | List > A | AAdd/] | Ed it Se c urity | Pro file > | Se c urity |
|----------|---------------------------|-----------------|---------------|------------|----------|--------|------------------|------------|------------|
| Mode: wp | o a 2-mix (c o ntinue d) | | | | | | | | |

| LABEL | DESC RIPTIO N | |
|---------------------------|--|--|
| C ip he r Typ e | Select an encryption ciphertype from the list. | |
| | • auto - This automatically chooses the best available cipherbased on the cipherin use by the wire less client that is attempting to make a connection. | |
| | • aes - This is the Advanced Encryption Standard encryption method. It is a more recent development over TKIP and considerably more robust. Not all wireless clients may support this. | |
| Id le Timeout | Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued. | |
| Group Key Update Timer | Enter the interval (in seconds) at which the AP updates the group WPA2 encryption key. | |
| Pre -Authe ntic a tio n | Se le c t Enable to allow pre-authentic ation. O the rwise, se le c t Disable. | |
| ОК | Click OK to save your changes back to the Zyxel Device. | |
| Cancel | Click Cancel to exit this screen without saving your changes. | |

Figure 68 Configuration > Object > AP Profile > SSID > Security List > Add/Edit Security Profile > Security Mode: wpa3 (NWA50AX)

| G Edil Security Profile default | | | 32 |
|-------------------------------------|----------------|---|-------|
| Hide Advanced Settings | | | |
| General Lettings | | | |
| Profile razmai | (better | | |
| Jecuity Mode: | (wpc3 | | |
| Authentication Settings | | | |
| # Penondi | | | |
| Pre-Chored Key: | 1 | 0 | |
| 35 Northine artists. | | | |
| - Advance | | Constant of the second | |
| ide triedut: | 200 | [35-30000 tecontti] | |
| Group Key Update Timer: | 30000 | [30-30000 seconds] | |
| the difference of the second second | ar & Carrent - | The second se | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | Cunod |

Table 47 Configuration > Object > AP Profile > SSID > Security List > AAdd/Edit Security Profile > Security Mode: wpa3

| IABEL | DESC RIPTIO N |
|------------------|--|
| General Settings | |
| Profile Name | Enterup to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed. |

| IABEL | DESC RIPHO N |
|--------------------------------|--|
| Se c unity Mode | Select a security mode from the list: none, enhanced-open, wep, wpa2, wpa2-mix or wpa3. |
| | enhanced-open uses Opportunistic Wire less Encryption (OWE) which encrypts the wire less connection when possible. |
| Authentic ation Settings | |
| Pe rso na l | This field is a vailable when you select the wpa2 , wpa2-mix or wpa3 security mode. |
| | Se lect this option to use a Pre-Shared Key (PSK) with WPA2 encryption or Simultaneous Authentication of Equals (SAE) with WPA3 encryption. |
| 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. |
| Tra nsitio n Mo d e | Enable this for backwards compatibility. This option is only available if the Security Mode is wpa3 or enhanced-open. This creates two virtual APs (VAPs) with a primary (wpa3 or enhanced-open) and fallback (wpa2 or none) security method. |
| | If the Security Mode is wpa3, enabling this will force Management Frame Protection to be set to Optional. If this is disabled or if the Security Mode is enhanced-open, Management Frame Protection will be set to Required. |
| Advanc e | |
| Note: Click on the Sho | wAdvanced Settings button to show the fields describe below. |
| Idle Timeout | Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued. |
| Group Key Update Timer | Enter the interval (in seconds) at which the AP updates the group WPA2 encryption key. |
| Pre -Authe ntic a tio n | Se le c t Enable to allow pre-authentication. O the rwise, se le c t Disable. |
| Management Frame Protection | This field is a vailable only when you select wpa2 in the Security Mode field and set Cipher Type to aes. |
| | Data frames in 802.11 WIANs can be encrypted and authentic ated with WEP, WPA or WPA2. But 802.11 management frames, such as beacon/probe response, association request, association response, de-authentic ation and disassociation are always unauthentic ated and unencrypted. IEEE 802.11w Protected Management Frames allows APs to use the existing security mechanisms (encryption and authentic ation methods defined in IEEE 802.11i WPA/WPA2) to protect management frames. This helps prevent wire less Do S attacks. |
| | Select the checkbox to enable management frame protection (MFP) to add security to 802.11 management frames. |
| | Select Optional if you do not require the wireless clients to support MFP. Management frames will be encrypted if the clients support MFP. |
| | Se le c t Require d and wire less c lients must support MFP in order to join the Zyxel Device's wire less network. |
| ОК | Click OK to save your changes back to the Zyxel Device. |
| Cancel | Click Cancel to exit this screen without saving your changes. |

 $\label{eq:stable_stab$

12.5 MAC Filter List

This screen allows you to create and manage security configurations that can be used by your SSIDs. To access this screen click **Configuration > Object > AP Profile > SSID > MAC Filter List**.

Note: You can have a maximum of 32 MAC filtering profiles on the Zyxel Device.

Figure 69 Configuration > Object > AP Profile > SSID > MAC Filter List

| and the second second | | | | |
|-----------------------|----------------|-------------------|------------------------|--------------------|
| 15ID LM | Tecurty lat | MAC Filler List | Lutyer-2 Isolation 104 | |
| IAC Filter List Sum | mary | | | |
| Q Add 2 top 1 | Annes States | distantion of the | | |
| · Profile Nam | | | Filer Action | |
| 19 4 Paper & La | ft P Pi Show M | 0 m dens | | No data to English |

The following table describes the labels in this screen.

| LABEL | DESC RIPIIO N |
|---------------------|---|
| Add | Click this to add a new MAC filtering profile. |
| Ed it | Click this to edit the selected MAC filtering profile. |
| Remove | Click this to remove the selected MAC filtering profile. |
| Object Reference | Click this to view which otherobjects are linked to the selected MAC filtering profile (for example, SSID profile). |
| # | This field is a sequential value, and it is not a ssociated with a specific user. |
| Pro file Name | This field indicates the name assigned to the MAC filtering profile. |
| Filte r Ac tio n | This field indic a tes this profile's filter a c tion (if a ny). |

Table 48 Configuration > Object > AP Profile > SSID > MAC Filter List

12.5.1 Add/Edit MAC Filter Profile

This screen allows you to create a new MAC filtering profile ore ditan existing one. To access this screen, click the **Add** button or select a MAC filter profile from the list and click the **Edit** button.

Note: Each MAC filtering profile can include a maximum of 512 MAC addresses.

| AGO MAC HIE | Prune | | |
|----------------|----------------------|-------------|----------------------|
| Profile Name: | | 0 | |
| Filter Action: | deny | 15 | |
| Q Add = 1 | Parriera | | |
| # MAC - | | Description | |
| 21 8 Page 1 | af 2 / / Dave HI | T BETA | too date to display |
| 21 1 Page 1 | st to in the pass of | * 1874 | and react to bedrate |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Figure 70 Configuration > Object > AP Profile > SSID > MAC Filter List > Add/Edit MAC Filter Profile

| IABEL | DESC RIPTIO N |
|------------------|---|
| Profile Name | Enterup to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only formanagement purposes. Spaces and underscores are allowed. |
| Filte r Ac tio n | Select a llow to permit the wire less client with the MAC addresses in this profile to connect to the network through the associated SSID; select deny to block the wire less clients with the specified MAC addresses. |
| Add | Click this to add a MAC address to the profile's list. |
| Ed it | C lick this to edit the selected MAC address in the profile's list. |
| Remove | C lick this to remove the selected MAC address from the profile's list. |
| # | This field is a sequential value, and it is not a ssociated with a specific user. |
| MAC | This field specifies a MAC address associated with this profile. You can click the MAC address to make it editable. |
| De sc rip tio n | This field displays a description for the MAC address associated with this profile. You can click the description to make it editable. Enterup to 60 characters, spaces and underscores allowed. |
| ОК | Click OK to save your changes back to the Zyxel Device. |
| Cancel | Click Cancel to exit this screen without saving your changes. |

| Table 49 | Config ura tion > | • O b je c t > AP Pro file | > SSID $>$ MAC | C Filte r List > | • Ad d/Ed it MAC | Filte r Pro file |
|----------|-------------------|----------------------------|----------------|------------------|------------------|------------------|
|----------|-------------------|----------------------------|----------------|------------------|------------------|------------------|

C HAPTER 13 MON Profile

13.1 Overview

This screen allows you to set up monitor mode configurations that allow your Zyxel Device to scan for otherwireless devices in the vicinity. Once detected, you can use the **Wireless > MON Mode** screen (Section 10.3 on page 79) to classify them as eitherrogue or friendly.

Not all Zyxel Devices support monitor mode and rogue APs detection.

13.1.1 What You Can Do in this Chapter

The **MON Profile** screen (Section 13.2 on page 117) creates preset monitor mode configurations that can be used by the Zyxel Device.

13.2 MON Profile

This screen allows you to create monitor mode configurations that can be used by the APs. To access this screen, log into the Web Configurator, and click **Configuration > Object > MON Profile**.

Figure 71 Configuration > Object > MON Profile

| Add | Geldent 12 Pe | empine 🔮 Applantes 🔮 beputting to 🍱 (bep | and A phone many |
|------|---------------|--|------------------|
| \$6 | ofut : | Profile Name - | |
| | R | default | |
| 1.93 | Page 1 of 1 | r 1) Show 32 (w) days | Charanying 1 - 1 |

The following table describes the labels in this screen.

| IABEL | DESC RIPIIO N |
|---------------|---|
| Add | Click this to add a new monitor mode profile. |
| Ed it | Click this to edit the selected monitor mode profile. |
| Remove | Click this to remove the selected monitor mode profile. |
| Ac tiva te | To tum on an entry, se lect it and click Activate. |
| Ina c tiva te | To tum off an entry, se lect it and click Inactivate. |

Table 50 Configuration > Object > MON Profile

NWA50AX Use r's Guide

| IABEL | DESC RIPTIO N |
|---------------------|--|
| Object Reference | C lick this to view which otherobjects are linked to the selected monitormode 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. |
| Pro file Name | This field indicates the name assigned to the monitor profile. |

Table 50 Configuration > Object > MON Profile (continued)

13.2.1 Add/Edit MON Profile

This screen allows you to create a new monitor mode profile ore ditan 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 14 for more information about MON Mode.

Figure 72 Configuration > Object > MON Profile > Add/Edit MON Profile

| Seneral Settings | | |
|---|------------------|--------|
| () Activate | | |
| Profile Name: | • | |
| Channel dwell time | 100 (100me-1000m | 111 |
| Scan Channel Mod | e manual | |
| let Scon Channel Ust | (2.4 GHz) | |
| Chonnel ID | | |
| 1 | 2 | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 42 | | |
| Set Scan Channel List | (5 GHz) | |
| Chonnel ID | | |
| 36 | | |
| 40 | | |
| 44 | | |
| 43 | | |
| 149 | | |
| 153 | 6 | |
| 157 | 4. | |
| 1 + + + · · · · · · · · · · · · · · · · | 9 | |
| | | |
| | | Concel |

| 8 | |
|-------------------------------------|---|
| IABEL | DESC RIPIIO N |
| Ac tiva te | Se le c t this to a c tiva te this monitor mode profile. |
| Pro file Name | This field indicates the name assigned to the monitor mode profile. |
| Channeldwell time | Enter the interval (in millise c ond s) 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. |
| | Se le c t manual to set specific channels through which to cycle sequentially when the Channel dwell time expires. Se le c ting this options makes the Scan Channel List options a vailable. |
| Set Scan Channel List (2.4 G Hz) | Selectone 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. |
| | The sechannels are limited to the 2.4 GHz range (802.11 b/g/n/ax). |
| Set Scan Channel List (5 G Hz) | Selectone 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. |
| | The se 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. |
| ОК | Click OK to save your changes back to the Zyxel Device. |
| Cancel | Click Cancel to exit this screen without saving your changes. |

Table 51 Configuration > Object > MON Profile > Add/Edit MON Profile

C HAPTER 14 WDS Profile

14.1 Overview

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

14.1.1 What You Can Do in this Chapter

The WDS Profile screen (Section 14.2 on page 120) creates preset WDS configurations that can be used by the Zyxel Device.

14.2 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 73 | Conf | ig ura tio n | 1 > C |) biect > | WDS Pro | file |
|-----------|------|--------------|-------|-----------|---------|------|
| | | | | | | |

| Add af bitt 🛢 feiticile | | |
|-----------------------------|--------------|----------------------|
| Profile Nome + | WDS SHD | |
| default | 2yvel_WD8 | |
| 1.1 Page 1 July 1 - 11 Show | 12 (m) heres | Deplecing 5 - 5 of 5 |

| IABEL | DESC RIPTIO N |
|--------------|--|
| Add | Click this to add a new profile. |
| Ed it | C lick this to edit the selected profile. |
| Remove | Click this to remove the selected profile. |
| # | This field is a sequential value, and it is not a ssociated 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. |

Table 52 Configuration > Object > WDS Profile

14.2.1 Add/Edit WDS Profile

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

| Figure 74 | Config ura tion > | Object> | WDS Pro file > | · Add/Edit V | VDS Pro file |
|-----------|-------------------|---------|----------------|--------------|--------------|
|-----------|-------------------|---------|----------------|--------------|--------------|

| Add WDS Profile | | | ?)X |
|-----------------|----------|------|-------|
| WDS Settings | | | |
| Profile Name: | | | |
| WD\$ \$SID: | | | |
| Pre-Shared Key: | 12345678 | | |
| | | | |
| | | OK C | ancel |

| LABEL | DESC RIPIIO N |
|----------------|--|
| Profile Name | Enterup to 31 alphanumeric characters for the profile name. |
| WDS SSID | Enter the SSID with which you want the Zyxel Device to connect to a mot 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. |
| ОК | Click OK to save your changes back to the Zyxel Device. |
| Cancel | Click Cancel to exit this screen without saving your changes. |

| Table 53 | Configuration > | Object> | WDS Pro file > | Add/Edit | WDS Pro file |
|------------|------------------|---------|---------------------|----------|----------------|
| 10.010 000 | o o mig and no m | | 11 2 10 1 10 1 10 1 | | 11 20 2 10 100 |

C HAPTER 15 Certific a tes

15.1 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.

15.1.1 What You Can Do in this Chapter

- The My Certificates screens (Section 15.2 on page 125) generate and export self-signed certificates or certification requests and import the Zyxel Device's CA-signed certificates.
- The **Thusted Certific ates** screens (Section 15.3 on page 132) save CA certific ates and trusted remote host certific ates to the Zyxel Device. The Zyxel Device trusts any valid certific ate that you have imported as a trusted certific ate. It also trusts any valid certific ate signed by any of the certific ates that you have imported as a trusted certific ate.

15.1.2 What You Need to Know

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

When using public-key cryptology for a uthentication, 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.

The se keys work like a hand written 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 herown 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.

Certific ation 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, so ftware, 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 actas 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 IIU-Trecommendation 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 PKC S# 7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKC S # 7 file is used to transfera 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 PKC S#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKC S#7 certificate into a printable form.

- Binary PKC S# 12: This is a format for transferring public key and private key certificates. The private key in a PKC S # 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 PKC S # 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.

15.1.3 Verifying a Certificate

Be fore 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.

| prifficate. | | 1 |
|--|--|-------|
| Seneral Dennis (Cethudon Pa Storit (1821- | • | |
| Perc Subject Rubic cary El Subject Alternative Name Mary Angel | Telus ungle_thirtrations SSA (1946 RH) Office Takes Pringer Takeshi Digite Spreads, Nex Brighter School Takeshi Levit | |
| Thumbert agorthm Thumbert | afw⊑ म¦ ।. | |
| | | |
| Learn mine skout o r thinks an a | Sinhamin.) [Deckfe | ba.cl |
| | | QI. |

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 HTIPS connection.

15.2 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 75 | Configuration > | Object> | Certific a te | > My | Certific a te s |
|-----------|-----------------|---------|---------------|------|-----------------|
| | | | | | |

| | | 1000 | | s.000% sound | | |
|----|----------------|---------------|-----------------|---------------|--------------------|----------------------|
| G | ertificates Se | etting | | | | |
| 07 | dd Phile | E farmeren | Chart Selemate | | | |
| • | Nomex | Type | Subject | Incer | Valid from | Volid To |
| | default | SELF | CN=niva5123-ac | CN4nwa5123-ac | 3015-09-02 12:00:2 | 2035-08-38 12:00-2 |
| 4 | 1 Page 3 | 1 1 1 1 1 1 1 | Show 50 m merus | | | Digloring 5 - 1 of 1 |

| IABEL | DESC RIPTIO N |
|----------------------------|---|
| PKIStorage Space in Use | This bard isplays 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. |
| Ed it | 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 certific ates unless you specific ally delete them. Up loading a new firm ware or default configuration file does not delete your certific ates. To remove an entry, select it and click Remove . The Zyxel Device confirms you want to remove it before doing so. Subsequent certific ates move up by one when you take this action. |
| O b je c t Re fe re nc e | 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. |
| Туре | 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 54 Configuration > Object > Certificate > My Certificates

| IABEL | DESC RIPTIO N |
|------------|---|
| Issue r | 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. |
| Re fre sh | C lick Refire sh to display the current validity status of the certificates. |

Table 54 Configuration > Object > Certificate > My Certificates (continued)

15.2.1 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.

| Add My Certificates | | | ?× |
|--|----------------------------|--------------------------------------|--------|
| Configuration | | | |
| Name: | | | |
| Subject Information | | | |
| Host IP Address | | | |
| Host Domain Name | | | |
| E-Mail | | | |
| Organizational Unit: | | (Optional) | |
| Organization: | | (Optional) | |
| Town(City): | | (Optional) | |
| State(Province): | | (Optional) | |
| Country: | | (Optional) | |
| Key Type: | RSA-SHA256 | * | |
| Key Length: | 2048 | ✓ bits | |
| Extended Key Usage | | | |
| Server Authentication | | | |
| Client Authentication | | | |
| | | | |
| Create a self-signed certificat | te | | |
| Create a certification request | t and save it locally for | later manual enrollment | |
| Create a certification request | t and enroll for a certifi | cate immediately online | |
| Enrolment Protocol: | Simple Certificate | Enrollment protocol(\$C 🗶 | |
| CA Server Address: | | | |
| CA Certificate: | Please selectione. | Gee Trusted CAs) | |
| Request Authentication | | | |
| Kery: | | | |
| | | | |
| | | OK | Cancel |

NWA50AX Use r's Guide

| Table 55 | Configuration > | Object> | Certific a te | > My Certific a tes > | Add |
|----------|-----------------|---------|---------------|-----------------------|-----|
| | 0 | | | | |

| LABEL | DESC RIPIIO N |
|--|---|
| Name | Type a name to identify this certificate. You can use up to 31 alphanumeric and ;'~!@#\$%^&()_+[]{}',=- characters. |
| Subject Information | Use the se 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 ore- mail address. Type the IP address (in dotted decimal notation), domain name ore-mail address in the field provided. The domain name ore-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 add ress can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore. |
| Org a niza tio na l 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. |
| Org a niza tio n | Identify the company orgroup to which the certificate ownerbelongs. 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 orprovince 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. |
| Кеу Туре | 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. |
| | Selecta 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 a uthenticate 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. |
| C reate a self-signed c ertificate | 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 | 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. |
| manualenrollment | Copy the certification request from the My Certificate Edit screen and then send it to the certification authority. |

| LABEL | DESC RIPIIO N |
|--|--|
| Create a certification request and enroll for | Select this to have the Zyxel Device generate a request for a certificate and apply to a certification authority for a certificate. |
| a centificate immediatelyonline | 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. |
| Enro llm e nt Pro to c o l | 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 (IEIF) 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-ZO-9'()+,/:.=?;!*#@\$_%- |
| CA Certific a te | 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 Thusted Certificates screen. Click Thusted CAs to go to the Thusted 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 yourcertification authority uses the CMP enrollment protocol. Just the Key field displays if yourcertification 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-ZO-9; `~!@#\$%^&*()_+\{}':,./ <>=- |
| ОК | Click OK to beg in certificate or certification request generation. |
| Cancel | Click Cancel to quit and return to the My Certificates screen. |

| Table 55 | Config ura tion > | >Object> | • Certificate > | > My | Certific a tes > | ·Add | (continued) |
|----------|-------------------|----------|-----------------|------|------------------|------|-------------|
|----------|-------------------|----------|-----------------|------|------------------|------|-------------|

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 **Retum** button that takes you back to the Add My Certificates screen. Click **Retum** 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.

15.2.2 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 7 | 77 | Configuration > | ·Object> | Certific a te | > M | v Certificates≥ | > Ed it |
|----------|----|--------------------|-------------|-----------------|-------|----------------------------------|---------|
| ing une | •• | c o mig ana no n , | 0 0 0 0 0 0 | C C I ULLO U UC | · ••• | <i>y</i> 0010110 0 00 0 <i>y</i> | 1.0.10 |

| onfiguration | |
|--------------------------------|---|
| Nome: | default |
| ertification Path | |
| CN=nwa5123-ac_5888F390F | 680 |
| Refresh | |
| ertificate Information | |
| Type: | Self-signed X.509 Certificate |
| Venion: | V3 |
| Serial Number: | Signature |
| Subject: | CN=nwa5123-ac_5888F390F680 |
| Issuer: | CN=nwa5123-ac_5888F390F680 |
| Signature Algorithm: | sha1WithRSAEncryption |
| Valid From: | 2015-09-02 12:00:21 GMT |
| Valid To: | 2035-08-28 12:00:21 GMT |
| Key Algorithm: | rscEncryption (1024 bit) |
| Subject Alternative Name: | rwa5123-ac_5888F390F680 |
| Key Usage: | Digital Signature, Key Encipherment, Data Encipherment, Certificate Sign |
| Extended Key Usage: | |
| Basia Constraint: | Subject Type=CA. Path Length Constraint=1 |
| MD5 Fingerprint: | 49:69:70:78:6D:03:44:C1:94:3C:4F:A7:07:44:E1:CE |
| SHA1 Fingerprint: | AF:AE:EC:1D:C1:86:71:80:12:52:D7:#8:A6:F7:81:9F:7D:82:99:DC |
| ertificate in PEM (Base-64) En | coded Format |
| | kITANBgkqhkiG9w08AQUFADAIWSAwHgYDVQQDD8du RJY4MDAeFw0xNTA5MDkMJAwMJFoFw0zNTA4Mjgx WMP253YTUxMjMHYWNHNTg4QkYzOT8GNjgwMiGfMA0G DC8IQK8gQDVSxHncqwwvqRoYU8GE073JS0Zm0r3LVg pludusfuIbUHSh1xLgw0kWAXiaw7n19RAuAuCT67 LNyh+oxKP7pUaOSVetgwNIYhwHExFA/QvDXWD1G AO8gNVHQ88A48EBAMCArQwigYDVR0R888wQYEXbndh Y2OD4wEoYDV90TAQH/8Acm&oF8/w/8ATAN8akabkiQ Possword: Export Certificate with Private Key |

| Table 56 | Configuration > | • Object > Certificate | > My Certific a tes > Ed i |
|----------|-----------------|------------------------|----------------------------|
| | | | |

| LABEL | DESC RIPIIO N |
|------------------------------------|---|
| Name | This field displays the identifying name of this certificate. You can use up to 31 alphanumeric and ;'~ $!@#$ %/^&()_+[]{',.=- characters. |
| Certific a tion Path | This field displays for a certificate, not a certification request. |
| | C lick 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 certific ation authority is one that you have imported as a trusted certific ation authority, it may be the only certific ation authority in the list (along with the certific ate itself). If the certific ate is a self-signed certific ate, the certific ate itself is the only one in the list. The Zyxel Device does not trust the certific ate and displays "Not trusted" in this field if any certific ate on the path has expired or been revoked. |
| Re fre sh | C lick Refiesh to display the certification path. |
| C e rtific a te Info rm a tio n | The se read-only fields display detailed information about the certificate. |
| Тур е | 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 IIU-TX.509 recommendation that defines the formats for public-key certificates. |
| Ve rsio n | This field displays the X.509 version number. |
| Se ria l Num b e r | 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 (SI), and Country (C). |
| Issue r | 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. |
| Simple turn Almenithm | none displays for a certification request. |
| Valid En m | This field displays the type of a gonthin that was used to sign the certificate. |
| | 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 Altemative 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. |

| IABEL | DESC RIPIIO N |
|---|---|
| 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 Certific a te 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 . |
| Pa ssw o rd | 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 . |
| ОК | 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. |

Table 56 Configuration > Object > Certificate > My Certificates > Edit

15.2.3 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 PKC S# 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 78 (| Configuration | > O b je c t > C e rtif | icate > My Certific | cates > Import |
|-------------|---------------|-------------------------|---------------------|----------------|
|-------------|---------------|-------------------------|---------------------|----------------|

| Import Ce | rtificates | 700 |
|---|--|-------|
| Please spe certificate Binary PEM (t Binary PEM (t Binary | city the location of the certificate file to be imported. The file must be in one of the following formats. X.509 Base-64] encoded X.509 PKCS#7 Base-64] encoded PKCS#7 PKCS#12 fficate importation to be successful, a certification request | |
| correspond ZyWALL, Af automatic | ding to the imported certificate must already exist an ter the importation, the certification request will ally be deleted. | |
| File Path: | Select a file path Browse | |
| Password: | (PKCS#12 only) | |
| | OK C | ancel |

| Table 57 | Configuration | > Object > | Certificate > | My Cer | tific a tes > Import |
|----------|---------------|------------|---------------|---------|----------------------|
| | | - 00,000 | | 11, 001 | meanes, mpon |

| IABEL | DESC RIPIIO N | |
|-------------|--|--|
| File Path | Type in the location of the file you want to upload in this field orclick Browse to find it. | |
| | You cannot import a certificate with the same name as a certificate that is already in the Zyxel Device. | |
| Bro w se | Click Browse to find the certificate file you want to upload. | |
| Pa ssw o rd | This field only applies when you import a binary PKC S# 12 format file. Type the file's password that was created when the PKC S # 12 file was exported. | |
| ОК | Click OK to save the certificate on the Zyxel Device. | |
| Cancel | Click Cancel to quit and return to the My Certificates screen. | |

15.3 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 79 Configuration > Object > Centricate > Invited Centricate | Figure 79 | Configuration > | Object> | Certificate > | Truste d | Certific a te s |
|---|-----------|-----------------|---------|---------------|----------|-----------------|
|---|-----------|-----------------|---------|---------------|----------|-----------------|

| | and a share a | | 7.325% resid. | | |
|------|------------------|----------------------------|-------------------|-----------------------|------------------------|
| vate | d Certificates S | etting | | | |
| 160 | int Thermore | Control Rathmence | | | |
| | Nome « | Subject | fatuer | Vold from | Vold to |
| | ZyXE-floot | CHTW. OrZynel. OURV | CHTW. OHIVEL OUNV | 2915-03-13 03:13:01 G | 2014-03-13-03-13-01 (5 |
| 24. | 1 Page 1 uf | L. P. P. Show III (W. Harr | | | Displaying 1-1 of 3 |

| LABEL | DESC RIPTIO N | |
|----------------------------|--|--|
| PKIStorage Space in Use | This bard isplays 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. | |
| Ed it | 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 certific ates unless you specific ally delete them. Up loading new firm ware or default configuration file does not delete your certific ates. To remove an entry, select it and click Remove . The Zyxel Device confirms you want to remove it before doing so. Subsequent certific ates 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. | |
| Issue r | 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 a Expire d! 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. | |
| Re fre sh | Click this button to display the current validity status of the certificates. | |

Table 58 Configuration > Object > Certificate > Trusted Certificates

15.3.1 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

a utho rity.

| Configuration ZyXEL-RootCA Certification Path //////////////////////////////////// | |
|--|---|
| Name: ZyKELRootCA Certification Path //C=TW/O=Zyxel/OU=VPN Department/OU=RootCA //C=TW/O=Zyxel/OU=VPN Department/OU=RootCA //Enable X.30Pv3 CRL Distribution Points and OCSP checking OCSP Server URL: D: Pathword: Serial Information Type: Self-signed X.509 Certificate Vealon: V3 Serial Number: S97:293:a00:34:4b:11:15:ed:33:33:3:3:3:0:1687:01:a0 Subject: C=TW, O=2ywel, OU=VPN Department, OU=RootCA Signature Algorithm: saEbnoryption Valid From: saEbnoryption Valid From: | |
| Certification Path //C=TW/O=Zysel/OU=VTPN Department/OU=RootCA //C=TW/O=Zysel/OU=VTPN Department/OU=RootCA //Endote Validation Indition Validation Indition Validation Indition Validation OCSP Server UR: ID: Password: ID: Password: ID: Password: ID: Password: Password: ID: Password: Safal Number: Safal Safa 332:336:344:3711:15:ed:332:336:341:87:01:40 Subject: C=TW, O=2ysel, OU=VTN Department, OU=RootCA Sagnature Algorithm: safal WiH#SAEncryp | |
| /C=TW/O=2yxel/OU=VPN Department/OU=RootCA Refrest: Certificate Validation In table X.30Pv3 CRL Distribution Points and OCSP checking OCSP Server UR: D: Password: Certificate Information Type: Self-signed X.50P Certificate Version: V3 Serial Number: 59:72:93:x00:34:4b:11:15:ed:33:3c:3d:b1:87:01:da Subject: C=TW, O=2yxel, OU=VPN Department, OU=RootCA Issuer: C=TW, O=2yxel, OU=VPN Department, OU=RootCA Subject: C=TW, O=2yxel, OU=VPN Department, OU=RootCA Subject Alemative Name: xeaDecryption (2048 bit) Subject Alemative Name: xeaDecryption (2048 bit) Subject Alemative Name: Subject Type=CA, Path Length Constroint=-1 <td< td=""><td></td></td<> | |
| Reference Enclobe X.509-V3 CRL Distribution Points and OCSP checking OCSP Server URL: ID: Password: Version: V3 Serial Number: Serial Number: Subject: C=TW, O=2ysel, OU=VPN Department, OU=RootCA Issee: C=TW, O=2ysel, OU=VPN Department, OU=RootCA Issee: C=TW, O=2ysel, OU=VPN Department, OU=RootCA Vaid From: 2014-03-13 03:13:01 GMT Vaid From: 2014-03-13 03:13:01 GMT Vaid From: sefer.cppfion (2048 bit) Subject Alternative Name: Subject Type=CA, Path Length Constraint=-1 | |
| Certificate Validation | |
| Enoble X:509V3 CRL Distribution Points and OCSP checking OCSP Server URL: ID: Password: ID: Address: ID: Password: ID: Password: Post: | |
| OCSP Server URL: ID: Possword: ILDAP Server Address: ID: Possword: ID: Possword: Port: Possword: Port: Possword: Post: Possword: Post: Possword: | |
| UB1: | |
| ID: | |
| Possword: | |
| LDAP Server Address: LD: Possword: Certificate Information Possword: Certificate Information Type: Self-signed X.30? Certificate Version: V3 Serial Number: S9:72:93:d0:34:4b:11:f5:ed:33:3c:3dbbf87:01:d0 Subject: C=TW, O=2yxel, OU=VPN Department, OU=RootCA Issuer: C=TW, O=2yxel, OU=VPN Department, OU=RootCA Vaild From: 2013-03-13:03:13:31 GMT Vaild To: 2014-03-13:03:13:31 GMT Vaild To: 2014-03-13:03:13:31 GMT Subject Alternative Name: Key Usage: Extended Key Usage: Estended Key Usage: Basic Constraint: Subject Type=CA, Path Length Constraint=-1 MD5 Fingerprint: CC1EDEF8:07:48:B4:07:04:23:33:21:3D:39:40:c81 CertHicate CertHicate <td< td=""><td></td></td<> | |
| Address: | |
| ID: Possword: Certificate Information Type: Self-signed X.509 Certificate Vesion: V3 Serial Number: S97293:d0:34:4b:11:f5:ed:33:30:30:db/bf/87:01:d0 Subject: C=TW, O=2yxel, OU=VPN Department, OU=RootCA Issuer: C=TW, O=2yxel, OU=VPN Department, OU=RootCA Signature Algorithm: sha1WithR5AEncryption Vaid From: 2013-03-13:03:13:31 GMT Vaid To: 2014-03-13:03:13:31 GMT Vaid To: 2014-03-13:03:13:31 GMT Key Algorithm: rsaEncryption (2048 bit) Subject Alternative Name: rsaEncryption (2048 bit) Subject Alternative Name: subject Type=CA, Path Length Constraint=-1 MD5 Fingerprint: 14:43:08:57:C5:CD:26:00:FD:EC:33:2D:7E:7D:85:E9 SHA1 Fingerprint: CC:1EDB:58:07:48:B4:07:04:23:33:21:5D:39:45:8C:51:39:A0:CB Certificate | |
| Possword: | |
| Type: Self-signed X.509 Certificate Vesion: V3 Serial Number: 59:72:93:d0:34:40:11:15:ed:33:30:3d:bf:87:01:d0 Subject: C=TW, O=2yxel, OU=VPN Department, OU=RootCA Issuer: C=TW, O=2yxel, OU=VPN Department, OU=RootCA Issuer: C=TW, O=2yxel, OU=VPN Department, OU=RootCA Signature Algorithm: sha1WithRSAEncryption Valid From: 2013-03-13 03:13:31 GMT Valid To: 2014-03-13 03:13:31 GMT Subject Alternative Name: Key Usage: Extended Key Usage: Extended Key Usage: Bail: Constraint: Subject Type=CA, Path Length Constraint=-1 MD5 Pingerprint: 16:43:D8:57:C5:CD:24:D0:FD:EC:33:2D:7E:7D:85:E9 SH1 Fingerprint: CC:1EDB:F8:07:48:B4:07:04:23:33:21:sD:39:43:BC:81:39:40:C8 CettBicate | |
| Type: Self-signed X.509 Certificate Version: V3 Serial Number: 59:72:93:d0:34:4b:11:t5:ed:33:3c:3d:bbf87:01:da Subject: C=TW, O=2yxel, OU=VPN Department, OU=RootCA Issuer: C=TW, O=2yxel, OU=VPN Department, OU=RootCA Issuer: C=TW, O=2yxel, OU=VPN Department, OU=RootCA Signature Algorithm: sha1WithRSAEncryption Valid From: 2013-03-13:03:13:31 GMT Valid For: 2014-03-13:03:13:31 GMT Valid To: 2014-03-13:03:13:31 GMT Key Algorithm: rsaEncryption (2048 bit) Subject Alternative Name: rsaEncryption (2048 bit) Subject Constraint: Subject Type=CA, Path Length Constraint=-1 MD5 Fingerprint: 14:43:D8:57:C5:CD:24:00:FD:EC:33:ED:7E:7D:85:E9 SHA1 Fingerprint: CC:1ED8:F8:07:48:B4:07:04:23:33:21:5D:39:45:BC:61:39:40:CB Certificate rmBErCC Alt-rgAwiBAgiQWXKTDBRLETXIMaw9v4cB2]ANBgkcphkiO9v08AQUFADBH MDR:vCQ1DVQQGEwJUV2EOMAwGA1UECgwFWinI42WwsF2AVBghVBAMDI2QTIBEZ:Bhr crR12WS0MQ8wDQYDVQQLDA2Sb290Q0EwHeeNMDVMM2EWMABAMDI2QTIBEZ:Bhr crR12WS0M | |
| Version: V3 Serial Number: 59:72:93:d0:34:4b:11:f5:ed:33:3c:3dtbf:87:01:da Subject: C=TW, O=Zyxel, OU=VPN Department, OU=RootCA Issuer: C=TW, O=Zyxel, OU=VPN Department, OU=RootCA Issuer: C=TW, O=Zyxel, OU=VPN Department, OU=RootCA Signature Algorithm: sha1WithRSAEncryption Vaild From: 2013-03-13:03:13:31 GMT Vaild To: 2014-03-13:03:13:31 GMT Vaild To: 2014-03-13:03:13:31 GMT Key Algorithm: rsaEncryption (2048 bit) Subject Alternative Name: sabiped Type=CA, Path Length Constraint=-1 MD5 Fingerprint: 14:43:D8:57:C5:CD:24:00:FD:EC:33:ED:7E:7D:85:E9 SHA1 Fingerprint: CC:1ED8:F8:07:48:B4:07:04:23:33:21:6D:39:45:BC:61:39:A0:C8 setEctate | |
| Serial Number: 59:72:93:d0:34:4b:11:f5:ed:33:3c:3dibf:87:01:da Subject: C=TW, O=Zyxel, OU=VPN Department, OU=RootCA Issuer: C=TW, O=Zyxel, OU=VPN Department, OU=RootCA Signature Algorithm: sha1WithRSAEncryption Valid From: 2013-03-13:03:13:31 GMT Valid To: 2014-03-13:03:13:31 GMT Key Algorithm: soEncryption (2048 bit) Subject Alternative Name: Key Usage: Extended Key Usage: | |
| Subject: C=TW, O=2yxel, OU=VPN Department, OU=RootCA Issuer: C=TW, O=2yxel, OU=VPN Department, OU=RootCA Signature Algorithm: sha1WithRSAEncryption Valid From: 2013-03-13 03:13:31 GMT Valid Ta: 2014-03-13 03:13:31 GMT Valid Ta: 2014-03-13 03:13:31 GMT Key Algorithm: rsaEncryption (2048 bit) Subject Alternative Name: rsaEncryption (2048 bit) Subject Alternative Name: subject Type=CA, Path Length Constraint=-1 MD5 Fingerprint: 14:43:D8:57:C5:CD:24:0DFD:EC:33:ED:7E:7D:85:E9 SHA1 Fingerprint: CC:1ED8:F8:07:48:B4:07:04:23:33:21:5D:39:45:8C:61:39:A0:C8 CettRicate | |
| Issuer: C=TW. O=2yxel. OU=VPN Department. OU=RootCA Signature Algorithm: sha1WithRSAEncryption Valid From: 2013-03-13 03:13:31 GMT Valid To: 2014-03-13 03:13:31 GMT Valid To: 2014-03-13 03:13:31 GMT Key Algorithm: rsaEncryption (2048 bit) Subject Alternative Name: Key Usage: Extended Key Usage: | |
| Signature Algorithm: sha1WithRSAEncryption Vaild From: 2013-03-13 03:13:31 GMT Vaild To: 2014-03-13 03:13:31 GMT Key Algorithm: rsaEncryption (2048 bit) Subject Alternative Name: | |
| Valid From: 2013-03-13 03:13:31 GMT Valid To: 2014-03-13 03:13:31 GMT Key Algorithm: isaEncryption (2048 bit) Subject Alternative Name: Key Usage: Extended Key Usage: Extended Key Usage: Basic Constraint: Subject Type=CA, Path Length Constraint=-1 MD5 Pingerprint: 14:43:08:57:C5:CD:24:00:FD:EC:33:ED:7E:7D:85:E9 SHA1 Fingerprint: CC:1ED8:F8:07:48:84:07:04:23:33:21:6D:39:45:8C:61:39:A0:C8 Cetificate | |
| Vaild To: 2014-03-13 03:13:31 GMT Key Algorithm: rsaEncryption (2048 bit) Subject Alternative Name: Key Usage: Extended Key Usage: Extended Key Usage: Basic Constraint: Subject Type=CA, Path Length Constraint=-1 MD5 Pingerprint: 14:43:08:57:C5:CD:24:00:FD:EC:33:ED:7E:7D:85:E9 SHA1 Pingerprint: CC:1ED8:F8:07:48:84:07:04:23:33:21:6D:39:45:8C:61:39:A0:C8 Certificate | |
| Key Algorithm: rsaEncryption (2048 bit) Subject Alternative Name: | |
| Subject Alternative Name: Key Usage: Extended Key Usage: Basic Constraint: Subject Type=CA, Path Length Constraint=-1 MD5 Pingerprint: 16:43:D8:57:C5:CD:24:D0:FD:EC:33:ED:7E:7D:85:E9 SHA1 Pingerprint: CC:1ED8:F8:07:48:84:07:04:23:33:21:6D:39:45:8C:61:39:A0:C8 CC:1ED8:F8:07:48:84:07:04:23:33:21:6D:39:45:8C:61:39:A0:C8 CC:1ED8:F8:07:48:84:07:04:23:33:21:6D:39:45:8C:61:39:A0:C8 CC:1ED8:F8:07:48:84:07:04:23:33:21:6D:39:45:8C:61:39:A0:C8 CC:1ED8:F8:07:48:84:07:04:23:33:21:6D:39:45:8C:61:39:A0:C8 CC:1ED8:F8:07:48:84:07:04:23:33:21:6D:39:45:8C:61:39:A0:C8 CC:1ED8:F8:07:48:84:07:04:23:33:21:6D:39:45:8C:61:39:A0:C8 CC:1ED8:F8:07:48:84:07:04:23:33:21:6D:39:45:8C:61:39:A0:C8 CC:1ED8:F8:07:48:84:07:04:23:33:21:6D:39:45:8C:61:39:A0:C8 CC:1ED8:F8:07:48:84:07:04:23:33:21:6D:39:45:8C:61:39:A0:C8 CC:1ED8:F8:07:48:84:07:04:23:33:21:6D:39:45:8C:61:39:A0:C8 CC:1ED8:F8:07:48:84:07:04:23:33:21:6D:39:45:8C:61:39:A0:C8 CC:1ED8:F8:07:48:84:07:04:23:33:21:6D:39:45:8C:61:39:A0:C8 CC:1ED8:F8:07:48:84:07:04:23:33:21:6D:39:45:8C:61:39:A0:C8 CC:1ED8:F8:07:48:84:07:04:23:20:00; MDM:M2M:W[BHMQswCQYDVQQLDA25b:29:00; MDM:M2M:W[BHMQswCQYDVQQCBWJUV2EOMAwGA1UECgwFW:nI4ZWwwFzAV8gNV8 AM DI2GT8E2:/8b:cn8f2W8:0cgYDVQQLDA25b:29:00; MDM:M2M:W[BHMQswCQYDVQQLDA25b:29:00; MDM:M2M:W[BHMQswCQYDVQQLDA25b:29:00; MDM:M2M:W[BHMQswCQYDVQQLDA25b:29:00; MDM:M2M:W[BHMQswCQYDVQQLDA25b:29:00; MDM:M2M:W[BHMQswCQYDVQQLDA25b:29:00; MDM:M2M:W[BHMQswCQYDVQQLDA25b:29:00; MDM:M2M:W[BHMQswCQYDVQQLDA25b:29:00; MDM:M2M:W[BHMQswCQYDVQQLDA25b:29:00; MDM:M2M:W[BHMQswCQYDVQQLDA25b:29:00; MDM:M2M:M2M:W[BHMQswCQYDVQQLDA25b:29:00; MDM:M2M:M2M:W[BHMQswCQYDVQQLDA25b:29:00; MDM:M2M:M2M:M2M:M2M:M2M:M2M:M2M:M2M:M2M: | |
| Key Usage: Extended Key Usage: Basic Constraint: Subject Type=CA, Path Length Constraint=-1 MD5 Fingerprint: 14:43:D8:57:C5:CD:24:D0:FD:EC:33:ED:7E:7D:85:E9 SHA1 Fingerprint: CC:1EDB:F8:07:48:B4:07:04:23:33:21:6D:39:45:BC:61:39:A0:CB CC:1EDB:F8:07:48:B4:07:04:23:33:21:6D:39:45:BC:61:39:A0:CB CC:1EDB:F8:07:48:B4:07:04:23:33:21:6D:39:45:BC:61:39:A0:CB CC:1EDB:F8:07:48:B4:07:04:23:33:21:6D:39:45:BC:61:39:A0:CB CC:1EDB:F8:07:48:B4:07:04:23:33:21:6D:39:45:BC:61:39:A0:CB CC:1EDB:F8:07:48:B4:07:04:23:33:21:6D:39:45:BC:61:39:A0:CB CC:1EDB:F8:07:48:B4:07:04:23:33:21:6D:39:45:BC:61:39:A0:CB CC:1EDB:F8:07:48:B4:07:04:23:33:21:6D:39:45:BC:61:39:A0:CB CC:1EDB:F8:07:48:B4:07:04:23:33:21:6D:39:45:BC:61:39:A0:CB CC:1EDB:F8:07:48:B4:07:04:23:33:21:6D:39:45:BC:61:39:A0:CB CC:1EDB:F8:07:48:B4:07:04:23:33:21:6D:39:45:BC:61:39:A0:CB CC:1EDB:F8:07:48:B4:07:04:23:33:21:6D:39:45:BC:61:39:A0:CB CC:1EDB:F8:07:48:B4:07:04:23:33:21:6D:39:45:BC:61:39:A0:CB CC:1EDB:F8:07:48:B4:07:04:23:33:21:6D:39:45:BC:61:39:A0:CB CC:1EDB:F8:07:48:B4:07:04:23:32:20:02 CC:1EDB:F8:07:48:B4:07:04:23:32:20 CC:1EDB:F8:07:48:B4:07:04:23:32:20 CC:1EDB:F8:07:48:B4:07:04:23:22 CD:1A:44:BD:v::04:vo:07:04:04:25:22 CD:1A:44:BD:v::04:vo:07:04:23:20 CD:2D:2D:2D:2D:2D:2D:2D:2D:2D:2D:2D:2D:2D | |
| Extended Key Usoge: Basic Constraint: Subject Type=CA, Path Length Constraint=-1 MD5 Fingerprint: 14:43:D8:57:C5:CD:24:D0:FD:EC:33:ED:7E:7D:85:E9 SHA1 Fingerprint: CC:1ED8:F8:07:48:84:07:04:23:33:21:6D:39:45:8C:61:39:A0:C8 Certificate | |
| Basic Constraint: Subject Type=CA, Path Length Constraint=-1 MD5 Fingerprint: 14:43:D8:57:C5:CD:24:D0:FD:EC:33:ED:7E:7D:85:E9 SHA1 Fingerprint: CC:1ED8:F8:07:48:84:07:04:23:33:21:6D:39:45:8C:61:39:A0:C8 Cetificate | |
| MD5 Fingerprint: 14:43:D8:57:C5:CD:24:D0:FD:EC:33:ED:7E:7D:85:E9 SHA1 Fingerprint: CC:1ED8:F8:07:48:B4:07:04:23:33:21:6D:39:45:BC:61:39:A0:C8 certificate BEGIN X509 CERTIFICATE MIDE:2CCAI+gAwiBAgiQWIXKT0DRLEN:Max/9v4cB2jAN8gkohkiG9v08AQUFAD8H MQswCQYDVQQGewJUV2EOMAwGA1UECgwFWniA2WwxFzAV8gNV8AsMDI2QTBEZXBh cnRtZWS0MQ8wDQYDVQQLDAZ5b290Q0EwHhcNMDMwMzEzMDMxMzMWhcNMDQw M2Ez MDM:M2M:WjBHMQswCQYDVQQCBwJUV2EOMAwGA1UECgwFWniA2WwxFzAV8gNV8 AsM DI2QTBEZX8hcnRtZW50MQ8wDQYDVQQLDAZ5b290Q0EwggBIMA0GCSqGSib3DQ6B ACILIAA.HID:wdwcoff&AcilB-CDCApress JA3b:d1COr8A.fba2NextBitsuC0Ked918(acide) | |
| SHA1 Fingerprint: CC:1ED8:F8:07:48:84:07:04:23:33:21:6D:39:45:8C:61:39:A0:C8 CertificateBEGIN X509 CERTIFICATE MIDR:CCAI+gAw/BAgIQWXKT0DRLEXIM/aw9v4c82]AN8gkohkiG9w08AQUFAD8H MQswCQYDVQQGewJUV2EOMAwGA1UECgwFWnI42WwxFzAV8gNV8AsMDI2QT8EZX8h cRR12WS0MQ8wDQYDVQQLDA25b290Q06wHhcNMDMwMzEzMDMxMzMvWhcNMDQw MzEz MDM:MzMvWjBHMQswCQYDVQQGEwJUV2EOMAwGA1UECgwFWnI42WwxFzAV8gNV8 AsM DI2QT8EZX8hcnRfzW50MQ8wDQYDVQQLDA25b290Q06wggBIMA0GCSqG5b3DQ68 +C114A:480DwawcofKAxi8ACDAcreae.143b;46C024A;5b290Q06wggBIMA0GCSqG5b3DQ68 +C114A:480DwawcofKAxi8AcDAcreae.143b;46C024A;5b290Q06wgBIMA0GC54A;5b290Q68wgBIMA0GC54A;5b290068;550;550068;550;550068;550;550068;550;550068;550;550068;550;550068;550;550068;550;550068;550068;5500;5500 | |
| Certificate Certificate MIDEscCAI+gAw/BAgiQWXX10DRLEIXIMzw9v4c82jAN8gkqhkiG9v08AQUFAD8H MQtwCQ1DVQQGEwJUV2EOMAwGA1UECgwFWni42WwxFzAV8gNV8AaMDI2QT8EZX8h cnRt2W50MQ8wDQYDVQQLDA25b290Q0EwHhcNMDMwMzt2MDMxMzMvWhcNMDQw MzEz MDMxMzMxWj8HMQswCQYDVQQGEwJUV2EOMAwGA1UECgwFWni42WwxFzAV8gNV8 AsM DI2QT8E2X8hcnRt2W50MQ8wDQYDVQQLDA25b290Q0EwggBMA0GCSqGSib3DQ68 ACUL4A485DwawcofKAci8aCDAccesa143bc4GCx8A4ba2NavcBibyc0kof31E/codbz * | |
| BEGIN X509 CERTIFICATE MIDR2CCAI+gAwiBAgiQWXX10DRLEIXIMzw9v4c82jAN8gkqhkiO9w08AQUFAD8H MQswCQYDVQQGEwJUV2EOMAwQA1UECgwFWnHzWwrFzAV8gNV8AsMDI2QT8EZXBh cnR12W50MQ8wDQYDVQQLDAISb290Q0EwHhcNMDMwMzEzMDMxMzW/WhcNMDQw MzEz MDMxMzMxWjBHMQswCQYDVQQGEwJUV2EOMAwGA1UECgwFWnHzWwrFzAV8gNV8 AsM DI2QT8EZX8hcnRtzW50MQ8wDQYDVQQLDAISb290Q0EwggEMA0GCSqGSib3DQE8 x | |
| MDMdMzMxWijBHMQswCQYDVQQGEwJUVzEOMAwGA1UECgwFWnI4ZWwoFzAV8gNV8 AsM DIQT8E2/8hcnRtZW50MQ8wDQYDVQQLDA2Sb290Q0EwggBMA0GCSqGSib3DQE8 ACII4A.485DwAwsoFKAci8.4CDAcces.a.143tb.45COr8.4.0ba7NwsTExxC0AcoR11E.codbr * | |
| | , |
| Export Certificate | |

| able of Computation / Object / Centilicate / Indied Centilicates / Ed | Table 59 | Config ura tion | > Object > | Certificate > | > Truste d | Certificates > | Edit |
|---|----------|-----------------|------------|---------------|------------|----------------|------|
|---|----------|-----------------|------------|---------------|------------|----------------|------|

| LABEL | DESC RIPIIO N |
|--|---|
| Name | This field displays the identifying name of this certificate. You can change the name. You can use up to 31 alphanumeric and ;'~!@#\$%^&()_+[]{}',.=- characters. |
| C e rtific a tio n Pa th | C lick the Refresh button to have this read-only text box display the end entity's certific ate and a list of certific ation a uthority certific ates that shows the hierarchy of certific ation a uthorities that valid ate the end entity's certific ate. If the issuing certific ation a uthority is one that you have imported as a trusted certific ate, it may be the only certific ation a uthority in the list (along with the end entity's own certific ate). The Zyxel Device does not trust the end entity's certific ate and displays "Not trusted" in this field if any certific ate on the path has expired or been revoked. |
| Re fre sh | Click Refiesh to display the certification path. |
| Enable X.509v3 CRL Distribution Points and OCSP checking | Se le ct 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 IDAP 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. |
| D | The Zyxel Device may need to authentic ate itself in order to assess the OCSP server. Type the log in name (up to 31 ASC II c haracters) from the entity maintaining the server (usually a certific ation authority). |
| Pa ssw o rd | Type the password (up to 31 ASC II c haracters) from the entity maintaining the OCSP server (usually a certification authority). |
| IDAP Server | Se le c t this c he c k box if the dire c tory server uses IDAP (Lightweight Dire c tory Access Protocol). IDAP 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. |
| Po rt | Use this field to specify the IDAP server port number. You must use the same server port number that the directory server uses. 389 is the default server port number for IDAP. |
| D | The Zyxel Device may need to authentic ate itself in order to a ssess the CRL directory server. Type the log in name (up to 31 ASC II characters) from the entity maintaining the server (usually a certification authority). |
| Pa ssw o rd | Type the password (up to 31 ASC II c haracters) from the entity maintaining the CRL directory server (usually a certific ation authority). |
| C e rtific a te Info rm a tio n | The se read-only fields display detailed information about the certificate. |
| Туре | 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 IIU-TX.509 recommendation that defines the formats for public-key certificates. |
| Ve rsio n | This field displays the X.509 vension number. |
| Senial Number | This field displays the certific a te's identific a tion number given by the certific a tion 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). |
| Issue r | 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. |
| Sig na ture Algorithm | This field displays the type of a lgorithm that was used to sign the certific ate. Some certific ation a uthorities use rsa-pkc s1-sha 1 (RSA public-private key encryption a lgorithm and the SHA1 hash a lgorithm). O thercertific ation a uthorities may use rsa-pkc s1-md 5 (RSA public-private key encryption a lgorithm and the MD5 hash a lgorithm). |

NWA50AX Use r's Guide

| LABEL | DESC RIPTIO N |
|----------------------------|---|
| 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 a heady 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 Altemative Name | This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL). |
| Ke y Usa g e | 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 Finge nprint | 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. |
| C e rtific a te | This mead-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 Certific a te | 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 . |
| ОК | 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. |

Table 59 Configuration > Object > Certificate > Trusted Certificates > Edit (continued)

15.3.2 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 file name before you can import the certificate.

| Import Trusted Certificates | [<u>*</u>][8] |
|--|-----------------|
| Please Input the File Name • Binary X.307 • FEM (Base-64) encoded X.307 • Binary PKCS#7 • PEM (Base-64) encoded PKCS#7 | |
| File Path: Select of file path | (Browner) |
| | OK Concel |

Figure 81 Configuration > Object > Certificate > Trusted Certificates > Import

Table 60 Configuration > Object > Certificate > Trusted Certificates > Import

| IABEL | DESC RIPIIO N |
|-----------|--|
| File Path | Type in the location of the file you want to upload in this field orclick Browse to find it. |
| | You cannot import a certificate with the same name as a certificate that is already in the Zyxel Device. |
| Bro w se | 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 retum to the previous screen. |

15.4 Technical Reference

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

OCSP

OCSP (Online Certific ate Status Protocol) allows an applic ation or device to check whether a certific ate is valid. With OCSP the Zyxel Device checks the status of individual certific ates instead of downloading a Certific ate 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 certific ates that it needs to verify, not a huge list. When the Zyxel Device requests certific ate status information, the OCSP server returns a "expired", "current" or "unknown" response.

C HAPTER 16 System

16.1 Overview

Use the system screens to configure general Zyxel Device settings.

16.1.1 What You Can Do in this Chapter

- The Host Name screen (Section 16.2 on page 138) configures a unique name for the Zyxel Device in your network.
- The Date/Time screen (Section 16.3 on page 139) configures the date and time for the Zyxel Device.
- The WWW screens (Section 16.4 on page 143) configure settings for HTIP or HTIPS access to the Zyxel Device.
- The SSH screen (Section 16.5 on page 151) configures SSH (Secure SHe II) for secure ly accessing the Zyxel Device's command line interface.
- The Telnet screen (Section 16.6 on page 155) configures Telnet for accessing the Zyxel Device's command line interface.
- The FIP screen (Section 16.6 on page 155) specifies FIP server settings. You can upload and download the Zyxel Device's firmware and configuration files using FIP. Please also see Chapter 18 on page 167 for more information about firmware and configuration files.

16.2 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.

| Hast Norma | | |
|--|--|--|
| General Settings | | |
| System Name: System Location: Domain Name: | (Opfional) (Opfional) (Opfional) | |
| | ApplyReset | |

Figure 82 Configuration > System > Host Name

| IABEL | DESC RIPIIO N |
|-----------------|--|
| 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. |
| Re se t | Click Reset to return the screen to its last-saved settings. |

Table 61 Configuration > System > Host Name

16.3 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 orget 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.

| Lunem time and Date | |
|---|---|
| Current Time: | 2022266-GMT+00:00 |
| Current Date: | 2019-02-30 |
| Time and Date Setup | |
| Manual | |
| New Tree processes | |
| New Date how mm att. | |
| | |
| Get from Time Server | |
| Get from Time Server Time Server Address*: | 0.pool.ntp.org |
| Get from Time Server Time Server Address*: "Optional. There is a pre-de | 0.pool.ntp.org Sync. Now fine: NIP time server list. |
| Get from Time Server Time Server Address*: *Optional. There is a pre-de Ime Zone Setup | D.poot.ntp.org Sync. Now Inner NIP time server list. |
| Get from Time Server Time Server Address*: *Optional. There is a pre-de time Zone Setup Time Zone: | 0.pool.ntp.org Sysc. Now fined NIP time server list. (GMI 00:00) Greenwich Mean Time : Dublin, Edinburgh, (m) |
| Get from Time Server Time Server Address*: *Optional. There is a pre-de time Zone Setup Time Zone: Enacle Daylight Saving | 0.poot.ntp.org |
| Get from Time Server Time Server Address*: *Optional. There is a pre-de time Zone Setup Time Zone: El Enacle Daylight Saving Time Todae | 0.pool.ntp.org |
| Get from Time Server Time Server Address*: *Optional. There is a pre-de time Zone Setup Time Zone: El Enacle Daylight Saving Time Zone: El Enacle Daylight Saving Time Zone: | 0.poot.ntp.org |

Figure 83 Configuration > System > Date / Time

The following table describes the labels in this screen.

| Table 62 | Config ura tion | > Syste m | > Date / Time |
|-----------|-------------------|---|---------------|
| 10.010 01 | o o ning unu no n | ~ | Dave, mile |

| LABEL | DESC RIPTIO N | | | |
|--------------------------|--|--|--|--|
| Current Time and Date | | | | |
| Cument Time | This field displays the present time of your Zyxel Device. | | | |
| Cument 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 serveror 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 . | | | |
| New Date (yyyy-mm-dd) | This field displays the last updated date from the time serveror 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. | | | |

NWA50AX Use r's Guide

| LABEL | DESC RIPTIO N | |
|---------------------------|---|--|
| 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 . No w | Click this button to have the Zyxel Device get the time and date from a time server (see the Time ServerAddress 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. | |
| | Se le c t 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. GMTor UIC). 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 GMTor UIC (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. GMTor UIC). 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 hourahead of GMTor UIC (GMT+1). | |
| O ffse t | Specify how much the clock changes when daylight saving begins and ends. | |
| | Entera 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. | |
| Re se t | Click Reset to return the screen to its last-saved settings. | |

Table 62 Configuration > System > Date/Time (continued)

16.3.1 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 NIP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

| Table 63 | De fa ult Time | Servers |
|----------|----------------|---------|
| | | |

| 0.poolntp.org |
|---------------|
| 1.poolntp.org |
| 2.poolntp.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.

16.3.2 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.



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. Thy re-configuring the Date/Time screen.

To manually set the Zyxel Device date and time:

- 1 Clic k 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 saving s.
- 7 C lic k Apply.

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

- 1 Clic k 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.

16.4 WWW Overview

The following figure shows secure and insecure management of the Zyxel Device coming in from the WAN. HTIPS and SSH access are secure. HTIP, Telnet, and FIP management access are not secure.

Figure 85 Secure and Insecure Service Access From the WAN



16.4.1 Service Access Limitations

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

16.4.2 System Timeout

There is a lease time out for administrators. The Zyxel Device automatically logs you out if the management session remains idle for longer than this time out 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 a uthentication again when the reauthentication time expires.

You can change the time out settings in the Userscreens.

16.4.3 HTIPS

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

HTTPS (HyperText Transfer Protocolover 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 re lies upon certificates, public keys, and private keys (see Chapter 15 on page 122 for more information).

HTIPS 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 HTIPS server (the Zyxel Device) must always authenticate itself to the HTIPS client (the computer which requests the HTIPS connection with the Zyxel Device), whereas the HTIPS client only should authenticate itself when the HTIPS server requires it to do so (select Authenticate Client Certificates in the WWW screen). Authenticate Client Certificates is optional and if selected means the HTIPS 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 HTIPS connection requests from an SSL-aware web browsergo 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 86 HTTP/HTTPS Implementation



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

16.4.4 Configuring WWW Service Control

Click **Configuration > System > WWW** to open the **WWW** screen. Use this screen to specify HTIP or HTIPS setting s.
| Figure 87 | Config uration | > Syste m > | · WWW > | Service Control |
|-----------|----------------|-------------|---------|-----------------|
|-----------|----------------|-------------|---------|-----------------|

| Service Control | | | |
|-------------------------|------------------------|---------|--|
| HITPS | | | |
| 2 Enable | | | |
| Server Port: | 442 | | |
| E Authenticate Client (| Certificates (See Init | ed Géti | |
| Server Certificate: | defoult | | |
| C Redirect HTTP to HTTP | \$ | | |
| HTTP | | | |
| 12 Enoble | | | |
| Server Port: | 60 | | |
| | | | |
| | | | |
| | | Apply | |

| IABEL | DESC RIPTIO N | | | | |
|-------------------------------------|---|--|--|--|--|
| HTIPS | HTIPS | | | | |
| En a b le | Select the check box to a low ordisallow 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 HTIPs connections. | | | | |
| Se rve r Po t | The HTIPS server listens on port 443 by default. If you change the HTIPS 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 SSLclient to authenticate itself to the ZyxelDevice by sending the ZyxelDevice a certificate. To do that the SSLclient must have a CA-signed certificate from a CA that has been imported as a trusted CA on the ZyxelDevice. | | | | |
| Se rve r C e rtific a te | Select a certificate the HTIPS server (the Zyxel Device) uses to authenticate itself to the HTIPS client. You must have certificates already configured in the My Certificates screen. | | | | |
| Redirect HTIP to HTIPS | To allow only secure Web Configurator access, select this to redirect all HTIP connection requests to the HTIPS server. | | | | |
| HTTP | | | | | |
| Ena b le | Select the check box to allow ordisallow 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 HTIP connections. | | | | |
| Se rve r Po rt | 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. | | | | |
| Re se t | Click Reset to return the screen to its last-saved settings. | | | | |

Table 64 Configuration > System > WWW > Service Control

16.4.5 HTIPS Example

If you have not changed the default HTIPS port on the Zyxel Device, then in your browserenter "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.

16.4.5.1 Google Chrome Warning Messages

When you attempt to access the Zyxel Device HTIPS server, you will see the emormessage shown in the following screen.

```
Figure 88 Security Alert Dialog Box (Google Chrome)
```



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

16.4.5.2 Mozilla Fire fox Warning Messages

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

ClickAdvanced > Accept the Risk and Continue.

| Fig ure | 89 | Se c uritv | Certific a te | 1 | (Fire fo x) |
|---------|----|------------|---------------|---|-------------|
| ing unc | 00 | Se c unity | | - | (1 10 10 A) |

| Warning: Potential Security Risk Ahead |
|--|
| Firefox detected a potential security threat and did not continue to 192.168.1.2. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details. |
| Leam more |
| Go Back (Recommended) Advanced |
| |
| Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for 192.168.1.2. The certificate is only valid for . |
| Error code: MOZILLA_PKDK_ERROR_SELF_SIGNED_CERT |
| View Certificate |
| Go Back (Recommended) Accept the Risk and Continue |

16.4.5.3 Avoiding Browser Warning Messages

Here are the main reasons your browserd isplays warnings about the Zyxel Device's HTIPS server certificate and what you can do to avoid seeing the warnings:

- The issuing certific ate authority of the ZyxelDevice's HTTPS server certific ate is not one of the browser's trusted certific ate authorities. The issuing certific ate authority of the ZyxelDevice's factory default certific ate is the ZyxelDevice itself since the certific ate is a self-signed certific ate.
- 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 206 for details.

16.4.5.4 Enrolling and Importing SSLC lient 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 **Tiusted Certificates** Web Configuratorscreen).

Figure 90 Trusted Certificates

| | | and the second s | 2.329% institu- | | |
|-----|------------------|--|---------------------|-----------------------|-----------------------|
| tie | d Certificates S | etting | | | |
| 61 | at Branner | Control Reference | | | |
| | Nome « | Subject | hitser | Volid Rom | Vold To |
| | ZyXEL-Root | CHTW. OrZynel. OURV | CHTW. CHEVINEL OUNV | 2915-03-13-03:13:01 G | 2014-03-13-03-13/3/ G |
| 4.1 | f I fage 12 Luft | LT # PS Show III (million | | | Distance (-1 of) |

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).

16.4.5.5 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.

| Elle name: | |
|--------------------------------|-----------------|
| Ī | Browse. |
| Microsoft Serialized Certifica | da Store (.531) |
| | |

3 Enter the password given to you by the CA.

| × |
|--------|
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| Cancel |
| |

4 Have the wizard determine where the certificate should be saved on your computeror 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.

| Certificate Impost Waard | Completing the P Wizard Too have second-by comp estant. You have specified the follo | Certificate Import | IX |
|--------------------------|--|---|----|
| | Certificate Store Selected Content Pile Name | Automatically determined by T PFX D: Wrogents_2003-10(CPE2)cp | |
| | * | Frish Carea | |

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



16.4.5.6 Using a Certificate When Accessing the Zyxel Device

To access the Zyxel Device via HTIPS:

1 Enter 'https://ZyxelDevice IPAddress/' in yourbrowser'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.

16.5 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 Bon the Internet uses SSH to secure ly connect to the Zyxel Device (A) for a management session.

Figure 91 SSH Communication Over the WAN Example



16.5.1 How SSH Works

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



Figure 92 How SSH v1 Works Example

1 Ho st Id e ntific a tio n

The SSH c lient sends a connection request to the SSH server. The server identifies itself with a host key. The c lient 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 Authentic ation 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.

16.5.2 SSH Implementation on the Zyxel Device

Yo ur 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).

16.5.3 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.

16.5.4 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 FIP when you configure SSH for secure connections.

| Figure 93 | Config ura tion | > Syste m $>$ SSF | I |
|-----------|-----------------|-------------------|---|
|-----------|-----------------|-------------------|---|

| 55 | н | v | |
|-----|---------------------|---------|-------------|
| Ger | neral Settings | | |
| X | Enable | | |
| | Version 1 | | |
| | Server Port: | 22 | |
| | Server Certificate: | default | * |
| | | | |
| | | | |
| | | | Apply Reset |

The following table describes the labels in this screen.

| IABEL | DESC RIPTIO N |
|--------------------------|---|
| Ena b le | Select the check box to allow ordisallow the computer with the IP address that matches the IP address(es) in the Service Control table to access the Zyxel Device CII 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. |
| Se rve r Po rt | 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 mote management. |
| Se rve r C e rtific a te | Select the certificate whose comesponding 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. |
| Re se t | Click Reset to return the screen to its last-saved settings. |

Table 65 Configuration > System > SSH

16.5.5 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.

16.5.5.1 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 94 SSH Example 1: Store Host Key

| 2945en | aley Warning | | 1 DOM |
|--------|--|--|------------------|
| 54 | Unknown Hest key | | |
| PH | The host key of 262, 168, 1,2 detabase. The host key should | (part) 12) is mit regetered in the is dies seried to authenticate this ho | et at rest time. |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | Do you want to accept their to | act key i | |
| | Accest Qrea | Acoust and Save | Secul |

Enter the password to log in to the Zyxel Device. The Clisc reen displays next.

16.5.5.2 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 a vailable 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 95 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 96 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 sc re e n d isp la ys next.

16.6 FIP

You can upload and download the Zyxel Device's firmware and configuration files using FIP. To use this feature, your computer must have an FIP client. See Chapter 18 on page 167 for more information about firmware and configuration files.

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

| Figure 97 | Config ura tion | > Syste m | > | FIF |
|-----------|-----------------|-----------|---|-----|
|-----------|-----------------|-----------|---|-----|

| ETP . | | | |
|---------------------|---------|-------|--|
| General Settings | | | |
| 12 Enoble | | | |
| El 1LS required | | | |
| Server Port: | 21 | | |
| Server Certificate: | defoult | 100 | |
| | | | |
| | | | |
| | | Apply | |

| IABEL | DESC RIPIIO N |
|--------------------------|--|
| Ena b le | Select the check box to a low ordisa low 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 re quire d | Select the check box to use FIP over TLS (Tansport Layer Security) to encrypt communication. |
| | This implements TLS as a security mechanism to secure FIP clients and/or servers. |
| Se rve r Po rt | 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. |
| Se rve r C e rtific a te | Select the certific ate whose comesponding private key is to be used to identify the Zyxel Device for FIP connections. You must have certific ates already configured in the My Certific ates screen. |
| Apply | Click Apply to save yourchanges back to the Zyxel Device. |
| Re se t | Click Reset to return the screen to its last-saved settings. |

CHAPTER 17 Log and Report

17.1 Overview

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

17.1.1 What You Can Do In this Chapter

• The Log Setting screens (Section 17.2 on page 157) specify which logs are e-mailed, where they are e-mailed, and how often they are e-mailed.

17.2 Log Setting

The se screens control log messages and a lerts. A log message stores the information for viewing (for example, in the **Monitor > View Log** screen) or regulare-mailing later, and an a lert is e-mailed immediately. Usually, a lerts 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 a lerts, the Log Setting screen controls which events generate a lerts and where a lerts 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, servernames, 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.

17.2.1 Log Setting Screen

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

| 1 | Salt Q Ac | tivate 🐨 Inactivate | | | |
|---|-----------|---------------------|-------------|---|--------------------|
| | Status | Nome | Log Format | Summary. | |
| | | Sustaine Long | Prince | E-must Server 1 food Server Form 25 Most Server Form 25 XSLTIS Environment in Most Subject Insperiod collections yes oppowned dollections yes Send Form Send Form Send Aler for Send Aler for Send Aler for Send Aler for | |
| | ę. | System Log | Internal | E-mail Server 2 Mail Server Mail Server Part: 35 SSL/TL3 Encryption: na Mail Subject: append system-name: yes append date-time: yes Send From Send From Send Jug to: Send Aust to: Schedule: Send log when full. | |
| | Ψ. | Remote Server 1 | VRP1/Syslog | Server Address: Log Facility: Local 1 | |
| | 9 | Remate Server 2 | VRPE/Syslog | Server Address Log Facility: Local I | |
| | Ψ. | Remote Server 3 | VRPT/Systag | Servet Address: Log Facility: Local 1 | |
| | 9. | Remote Server 4 | VRP1/Syslag | Server Address Log Facility: Local 1 | |
| | 1 Page 1 | Tofat a shi she | 10 W. Kerni | | Denving 1 - 8 of 9 |

Figure 98 Configuration > Log & Report > Log Setting

| Table 67 | Config ura tion | > Lo g | & Report > Log | Setting |
|----------|-----------------|--------|--|---------|
| | | . 0 | ··· ·· · · · · · · · · · · · · · · · · | , |

| LABEL | DESC RIPTIO N |
|---------------|---|
| Ed it | Double-click an entry or select it and click Edit to open a screen where you can modify the entry's setting s. |
| Ac tiva te | To tum on an entry, se lect it and click Activate. |
| Ina c tiva te | To tum off an entry, se lect it and click Inactivate. |
| # | This field is a sequential value, and it is not a ssociated 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). |
| Log Format | This field displays the format of the log. |
| | Internal - system log; you can view the log on the View Log tab. |
| | VRPV 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. |

| IABEL | DESC RIPTIO N |
|-----------------------|--|
| 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. |

Table 67 Configuration > Log & Report > Log Setting (continued)

17.2.2 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.

| med Server 1 | | | |
|-----------------------------------|------------------------|-----------------------|-------------------------|
| D Active | | | |
| Ailud Selver: | | (Dutgoing M/IP Serv | W TONY & ST 7 AUDITOR |
| 38, 7.5 Enzyphon | 140 | 8 | |
| Abull Lerver Purts | 28 | 11-4553111 (Ophumut) | |
| Moti Sumech | | | |
| III Apparid surfammente | | | |
| E Addrenal choise filmer | | | |
| Sarva France | | EAter Address | |
| Secret on its | | EALS ADDALL | |
| Tarrel Black Im- | | GARAT Ackinett | |
| Encolored and | State P. F. | | |
| the set if not | The section of | | |
| | | | |
| A CARDINAL PROPERTY AND | | | |
| S MALANDARY COMPANY | | -70 | |
| Inter FLOME | | | |
| Pressind | | | |
| not lancer 3 | | | |
| Action . | | | |
| Abait Samer: | | (Outgoing Skiff' Serv | er Tizzne or P Asideen) |
| SIL/f13 Enmysflori | 1940 | | |
| | | | 2 |
| fire log soid Apert | | | ~~~ |
| Summings #5-mailtane | r i t 📕 5-cosi Sever 3 | 14 | |
| Leg Cetegrey | System Log. | Sentimet. | EventServer 2 |
| | | 9.4 | |
| Arrent | | # 51 | |
| Batterie | 0.00 | 411 | 4.1 |
| Bullio Jackina | 0.00 | 8.0 | |
| Correctively Chart | 0.00 | W 11 | 9.0 |
| Delli Raneri | 0.4.0 | # 11 | |
| Fadar di | 0.0.4 | 4.0 | 4.0 |
| Davina Hit | 0.00 | *0 | |
| Dennis Remains | 0.00 | #11 | |
| Dec. | 0.00 | 4.1 | |
| the Diversion | | 410 | |
| I Room & Annalisation | 0.00 | A 12 | |
| 1 madeira | 0.00 | 20 | 9.1 |
| a menosar | 0.4.0 | | |
| A holom | | | |
| a litera | | * 0 | |
| a Mineskin I dia | 0.0.0 | | |
| 7 Mill Black Council | 0.00 | | |
| A DECKA Common Char | | | |
| and a series in the second second | 0.00 | 8.0 | |
| 1 101 all block of the liter | 0.00 | 20 | 8.0 |
| Walk Rome 18 Tel | 0.0.0 | 14.10 | |
| Win Delan Mr. | 0.0.0 | | |
| 1 August Otto Income | 0.00 | *0 | |
| A Long the resident | 0.00 | 8.0 | |
| 19 Subel | 0.00 | 8.0 | |
| N. C. Pasell Laffacts. In . B. | and the second | | Desirates 1 (10 of 10 |
| | CONTRACTOR STATE | | 11.1 |
| Carrobitation | | | |
| Active . | | | |
| Jug Consolidation High-of | 198 | 110-800 seconds | |
| | | | |
| | | | 06 IF-6 |

Figure 99 Configuration > Log & Report > Log Setting > Edit System Log Setting

Table 68 Configuration > Log & Report > Log Setting > Edit System Log Setting

| LABEL | DESC RIPTIO N |
|-------------------------|--|
| E-Ma il Se rve r 1/2 | |
| Ac tive | 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 Enc ryp tio n | Select SSL/ILS 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 STARTIES to upgrade a plain text connection to a secure connection using SSL/ILS. |
| | Select No to not encrypt the communic ations. |
| Mail Server Port | Enter the same port number here as is on the mail server for mail traffic. |
| Ma il Subje c t | 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. Choicesare: 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 ordaily. 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. |
| Use r Na m e | 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. |
| Pa ssw o rd | 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 | |
| Syste m lo g | 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. |

| IABEL | DESC RIPIIO N |
|-------------------------------|---|
| E-m a il Se rve r 1 | Use the E-Mail Server1 drop-down list to change the settings fore-mailing logs to e-mail server1 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 checkmark) - 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-m a il Se rve r 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 checkmark) - 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 a ssociated 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. |
| Syste m lo g | 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-m a il 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 a lerts (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-m a il Se rve r 2 | Select whether each category of events should be included in log messages when it is e- mailed (green check mark) and/or in a lerts (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 | |
| Ac tive | Select this to activate log consolidation. Log consolidation aggregates multiple log messages that a nive 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. |
| ОК | 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. |

Table 68 Configuration > Log & Report > Log Setting > Edit System Log Setting (continued)

17.2.3 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 100 Configuration > Log & Report > Log Setting > Edit Remote Server

| Log Formati VRPT/Sydor w Server Address: | - | A | | |
|--|------|-----------------------------|---------------------------|-----------------------------|
| Log Farman (VMF/13)d0(1) Server Address: | - | ME UYO | | |
| server Address: Log Facility: Local I Selection* Local I Selection Local I Selection Local I Selection Local I Selection Local I Selection Local I Selection Confective Lag Local I Selection | - 5 | og Formati | ARE1/3/sio[12] | |
| Local 1 Mail Selection* Selection * Collegery Selection * Account * * * * * * * * * * * * * * * * * * * | 5 | erver Address: | Contraction of the second | (server Nome or IP Address) |
| Colspan Log Colegary Selection * Contegary Selection 1 Account * 0 0 2 Bluetooth * 0 0 2 Bluetooth * 0 0 2 Bluetooth * 0 0 3 Built-in Service * 0 0 4 Connectivity Check * 0 0 5 Dolly Report * 0 0 4 Default * 0 0 5 Dolly Report * 0 0 6 Dynamic Frequency Selection * 0 0 7 Device HA * 0 0 8 Dynamic Frequency Selection * 0 0 9 DHCP * 0 0 10 Free Authentication * 0 0 11 Force Authentication * 0 0 12 Interface * 0 0 13 Interface * 0 0 14 PN * 0 0 15 System Monitoring * 0 0 16 User * 0 0 17 Traffic Log * 0 0 18 <td>Ł</td> <td>og Foicility:</td> <td>Local 1 M</td> <td></td> | Ł | og Foicility: | Local 1 M | |
| Selection* Log Cotegory Selection * Account * • • • • • 1 Account * • • • • • 2 Sluetooth • • • • • • 2 Sluetooth • • • • • • 3 Built-in Service • • • • • • 4 Connectivity Check • • • • • • 5 Doly Report • • • • • • 4 Defauit • • • • • • 5 Doly Report • • • • • • 6 Defauit • • • • • • 7 Device HA • • • • • • 8 Dynamic Frequency Selection • • • • • • 9 DHCP • • • • • 10 File Manager • • • • • • 11 Force Authentication • • • • • • 12 Interface • • • • • 13 Interface Statistica • • • • • 14 PN • • • • • 15 System Monitoring • • • • • • 16 System Monitoring • • • • • • 17 Trofic Log • • • • • | cliv | e log | | |
| Log Cotegory Selection I Account Image: Comparison of the selection I Account Image: Comparison of the selection I Built-In Service Image: Comparison of the selection I Connectivity Check Image: Comparison of the selection I Defoult Image: Comparison of the selection I Dynamic Frequency Selection Image: Comparison of the selection I Force Authentication Image: C | D | Selection + | | |
| * • • • • • • • • • • • • • • • • • • • | | Log Category | | Selection |
| 1 Account ************************************ | * | | | |
| 2 Bluetooth * 6 0 3 Bult-In Service * 6 0 4 Connectivity Check * 6 0 5 Doly Report * 6 0 6 Defoult * 6 0 7 Defoult * 6 0 8 Dynamic Frequency Selection * 6 0 9 DHCP * 6 0 10 File Manager * 6 0 11 Force Authentication * 6 0 12 Interfoce * 6 0 13 Interfoce Statistics * 6 0 14 PQ * 6 0 15 System Monitoring * 6 0 16 System Monitoring * 6 0 17 Traffic Log * 6 0 18 User * 6 0 19 Wreless LAN * 6 0 | T | Account | | *00 |
| Built-in Service • • • • • • • Connectivity Check • • • • • • Daily Report • • • • • • • Default • • • • • • • • Default • • • • • • • • Default • • • • • • • • • • • • • • • • • • • | 2 | Bluetooth | | * 0 0 |
| 4 Connectivity Check # 0 0 5 Doly Report # 0 0 4 Default # 0 0 7 Device HA # 0 0 8 Dynamic Frequency Selection # 0 0 9 DHCP # 0 0 10 File Manager # 0 0 11 Force Authentication # 0 0 12 Interface # 0 0 13 Interface Statistica # 0 0 14 PK0 # 0 0 15 System # 0 0 16 System Monitoring # 0 0 17 Traffic Log # 0 0 18 User # 0 0 | 2 | Bullt-In Service | | *00 |
| 5 Dolly Report • • • • • • • • • • • • • • • • • • • | i. | Connectivity Check | | *00 |
| b Default • • • • • • • • • • • • • • • • • • • | 5 | Dolly Report | | |
| 7 Device HA # 0 0 8 Dynamic Frequency Selection # 0 0 9 DHCP # 0 0 10 File Manager # 0 0 11 Force Authentication # 0 0 12 Interface # 0 0 13 Interface Statistica # 0 0 14 PN # 0 0 15 System # 0 0 16 System Monitoring # 0 0 17 Traffic Log # 0 0 18 User # 0 0 19 Wreleis LAN # 0 0 | 6 | Defoult | | |
| B Dynamic Frequency Selection • • • • • • • • • • • • • • • • • • • | 7 | Device HA | | * 0 0 |
| 9 DHCP • 0 0 10 File Manager • 0 0 11 Force Authentication • 0 0 12 Interface • 0 0 13 Interface Statistica • 0 0 14 FN0 • 0 0 15 System • 0 0 16 System Monitoring • 0 0 17 Traffic Log • 0 0 18 User • 0 0 19 Wireless CAN • 0 0 | ŧ.; | Dynamic Frequency Selection | | |
| 10 File Manager # 0 0 11 Force Authentication # 0 0 12 Interface # 0 0 13 Interface Statistics # 0 0 14 PN # 0 0 15 System # 0 0 16 System Monitoring # 0 0 17 Traffic Log # 0 0 18 User # 0 0 19 Wreless LAN # 0 0 | 9 | DHCP | | * 0 0 |
| 11 Force Authentication • • • • • • 12 Interface • • • • • • 13 Interface Statistica • • • • • • 14 FN0 • • • • • • 15 System • • • • • • 16 System Monitoring • • • • • 17 Traffic Log • • • • • 18 User • • • • • 19 Wreless LAN • • • • • | 10 | Rie Monoger | | * 0 0 |
| 12 Interface • • • • • • 13 Interface Statistics • • • • • • 14 FN0 • • • • • • 15 System • • • • • • 16 System Monitoring • • • • • • 17 Traffic Log • • • • • • 18 User • • • • • 19 Wreless LAN • • • • • | 11 | Force Authentication | | *00 |
| 13 Interface Statistics # 0 0 14 PK0 # 0 0 15 System # 0 0 16 System Monitoring # 0 0 17 Traffic Log # 0 0 18 User # 0 0 19 Wreless LAN # 0 0 | 12 | Interface | | * 0 0 |
| 14 PK0 # 0 0 15 System # 0 0 16 System Monitoring # 0 0 17 Traffic Log # 0 0 18 User # 0 0 19 Wreien LAN # 0 0 10 With At Rend Scient # 0 0 | 15 | Interlace Statistics | | *00 |
| 15 System # 0 0 16 System Monitoring # 0 0 17 Traffic Log # 0 0 18 User # 0 0 19 Wreless LAN # 0 0 | 14 | PKI | | * 6 6 |
| 16 System Monitoring # 0 0 17 Traffic Log # 0 0 18 User # 0 0 14 Wreless LAN # 0 0 10 Wild Millioned Scient # 0 0 | 15 | System | | |
| 17 Traffic Log # 0 0 18 User # 0 0 14 Wreless LAN # 0 0 15 User # 0 0 | 61 | System Monitoring | | *00 |
| 18 User # 0 0 19 Wrelets LAN # 0 0 10 Wild Millered Scient # 0 0 | 17. | Traffic Log | | .00 |
| IF Wreien CAN #00 | 18 | User | | |
| Wild Stal Banad Calant | 14 | Wheless LAN | | *00 |
| 20 WLAX band select | 30 | WLAN Band Select | | |

| Table 69 | Configuration > L | og & Report > Log | g Setting > Ed it Remote Server | |
|----------|-------------------|-------------------|---------------------------------|--|
| | 0 | | 8 8 | |

| IABEL | DESC RIPIIO N |
|----------------------|--|
| Log Settings for Ren | mote Server |
| Ac tive | Se le c t this c he c k box to send log information a c c ording 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. |
| | VRPV Syslog - Zyxel's Vantage Report, syslog-compatible format. |
| | CEF/Syslog - Common Event Format, syslog-compatible format. |
| Se rve r Addre ss | 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 | |
| Se le c tio n | 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 checkmark) - 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, a lerts, 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. |
| Se le c tio n | 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 checkmark) - log regular information, alerts, and debugging information from this category |
| ОК | 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. |

17.2.4 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.

| | Log Cafeg | System Log | E-moll Server E-Mol D | E-mail Server E-Mail | Permote Serve Systeg | flemote Serve Syslog @@@@ | Remote Serve | Remote Serve Syslog |
|-------|---------------|------------|-----------------------------|-------------------------|-------------------------|---------------------------------|--------------|------------------------|
| | Account | 0.8.0 | 8.0 | 8.0 | 800 | *00 | 800 | 800 |
| | Bluetootti | 080 | 10 10 | 8.0 | +00 | #00 | *00 | |
| 1. | Built-In Serv | 080 | 8.0 | 8.0 | 800 | 800 | 800 | 800 |
| £., | Connectful | 0.8.0 | 10 M | 8.0 | | *00 | | 800 |
| 1 | Daily Report | 0.8.0 | 8.0 | 8.0 | 800 | 800 | 800 | 800 |
| 67 | Default | 00.8 | 10 M | 8.0 | | *00 | | .00 |
| 1.1.1 | Device HA | 080 | 80 | 8.0 | 800 | *00 | 800 | 800 |
| | Dynamic Fr | 0.8.0 | 10 (B) | 10.00 | | | | 800 |
| | DHCF | 080 | 8.0 | 8.0 | 800 | *00 | 800 | 800 |
| 0 | Re Manager | 0.00 | 10 M | 10.00 | | | *00 | 800 |
| it. | Force Auth | 080 | 80 | 8.0 | * 0 0 | 800 | 800 | 800 |
| 12 | Interface | 0.80 | 10.06 | 10.00 | | | *00 | 800 |
| 1.5 | Interface 1 | | | | 800 | 800 | 80.0 | 800 |
| 4 | PIC | 0.00 | 10.56 | 10.00 | | | *00 | 800 |
| 5 | System | 080 | 80 | 9.0 | * 0 0 | 800 | 80.0 | 800 |
| 16 | System Mo | | | | | #00 | *00 | 800 |
| 2 | Traffic Log | | | | * 0 0 | 800 | 800 | 800 |
| 0. | User | 0.00 | 10.56 | 10.0 | | #00 | *00 | 800 |
| | Wreless LAN | 080 | 8.0 | 8.0 | *00 | 800 | 800 | 800 |
| 20 | WLAN Ban | 0.00 | 10 M | 8.0 | | | | 800 |
| 11.1 | Page 1 473 | A 44 10mm | 20 - 0 - 0 - 02 | | | | | Displaying 5 - 30 of 2 |

| Fig ure | 101 | Ac tive | 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 70 | Configuration > Iog | g & Report > log | Setting > Active log Summary | |
|----------|---------------------|------------------|-------------------------------|--|
| | Company month in a | s a rapono ing | setting - ne live ing summary | |

| LABEL | DESC RIPTIO N |
|-----------------------|--|
| 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 (m d 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 checkmark) - 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 (ye llow 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. |

| IABEL | DESC RIPIIO N |
|-----------------------------|--|
| E-mail Server 1 | Use the E-Mail Server1 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 checkmark) - 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 dmp-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. |
| | e nable normal logs (green checkmark) - 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 normallogs (green checkmark) - send the remote server log messages and alerts for all log categories. |
| | enable normal logs and debug logs (ye llow checkmark) - send the remote server log messages, a lerts, 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 (ye llow check mark) - create log messages, a lerts, 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 a lerts (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 a lerts (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 memote 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 normallogs (green checkmark) - log regular information and alerts from this category |
| | enable normal logs and debug logs (ye llow check mark) - log regular information, a lerts, and debugging information from this category |
| OK | Click this to save your changes and return to the previous screen. |
| Cancel | C lick this to return to the previous screen without saving your changes. |

| Table 70 | Config ura tion > | ۰ Log | & Report > Log | Setting $>$ Active | Log Summary (c | ontinue d) |
|----------|-------------------|-------|----------------|--------------------|----------------|------------|
|----------|-------------------|-------|----------------|--------------------|----------------|------------|

NWA50AX Use r's Guide

CHAPTER 18 File Manager

18.1 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 up load them to the Zyxel Device. Configuration files use a .confextension and shell scripts use a .zysh extension.

18.1.1 What You Can Do in this Chapter

- The **Configuration File** screen (Section 18.2 on page 168) stores and names configuration files. You can also download and upload configuration files.
- The Firm ware Package screen (Section 18.3 on page 173) checks your current firm ware version and up loads firm ware to the Zyxel Device.
- The Shell Script screen (Section 18.4 on page 175) stores, names, downloads, uploads and runs shell script files.

18.1.2 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.

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

Figure 102 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.

| | 5 |
|---|---|
| Configuration Files (.conf) | She ll Sc rip ts (.zysh) |
| Resets to default configuration. Goes into CII Configuration mode. Runs the commands in the configuration file. | Goes into C LI Privile ge mode. Runs the commands in the shell script. |

Table 71 Configuration Files and Shell Scripts in the Zyxel Device

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.

18.2 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 backon), the Zyxel Device uses the system-default.conf configuration file with the Zyxel Device's default setting s.
- 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** config uration file as a back up file. If there is an error, the Zyxel Device generates a log and copies the **startup-config.conf** config uration file to the **startup-config-bad.conf** config uration file and tries the existing **lastgood.conf** config uration file. If there isn't a **lastgood.conf** config uration file or it also has an error, the Zyxel Device applies the **system-default.conf** config uration file.
- You can change the way the startup-config.conf file is applied. Include the setenv-startup stopon-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.

| Ni konstran 🗮 Parri | eve 🛃 Dovisional 🔂 Cap | r Dr Apply | | |
|---------------------|------------------------|------------|---------------------|----------------------|
| # The Nome | | 500 | Last ModRed | |
| startup-config | cont | 4267 | 2019-07-29 16:35:42 | |
| 2 system-defaul | Loonf | 3965 | 2019-07-29 14:11:39 | |
| a startup-config | -bad.coni | 3876 | 2019-07-29 14:13:39 | |
| a olativid | | 3 | 2019-07-29 14:13:20 | |
| 5 lastgood-defo | ult.conf | 3985 | 2019-07-29 13:58:54 | |
| 6 kastgood.cont | | 4267 | 2019-07-29 14:14:10 | |
| 1 autobackup-6 | .00.cont | 3876 | 2019-07-29 14:11:29 | |
| II - Page Life | f1 + + + 3how 30 (m) | terns | 1 | Daplaying 1 - 7 of 7 |
| | | | | |

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

| Table 72 Maintenance > File Manager > Configuration | File |
|---|------|
|---|------|

| IABEL | DESC RIPTIO N |
|---------------|---|
| 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. |
| | Source file: outobackup-5.10.con/ Target file: |
| | OK Concel |
| | Spec ify the new name for the configuration file. Use up to 25 c haracters (including a-zA-Z0-9;'~!@#%^&()_+[]{',.=-}. |
| | C lic k OK to save the duplic ate orc lic k Cancel to c lose the screen without saving a duplic ate of the configuration file. |
| Remove | C lick a configuration file's row to select it and c lick 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. |
| Do w n lo a d | Click a configuration file's row to select it and click Download to save the configuration to your computer. |
| Сору | 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. |
| | Copy File |
| | Source Re: stortup-config.con/ Torget Re: |
| | CK Cancel |
| | Specify a name for the duplicate configuration file. Use up to 25 c haracters (including a-zA-ZO-9;'~!@#%^&()_+[]{',.=-). |
| | Click OK to save the duplicate orclick Cancel to close the screen without saving a duplicate of the configuration file. |

| lable 12 Maintenance > rile Manager > Configuration rile (continued) | Table 72 | Ma inte na nc e | > File | Manager> | Config ura ti | on File | (continued) |
|--|----------|-----------------|--------|----------|---------------|---------|-------------|
|--|----------|-----------------|--------|----------|---------------|---------|-------------|

| IABEL | DESC RIPTIO N |
|-----------|--|
| Apply | Use this button to have the Zyxel Device use a specific configuration file. |
| | C lick a configuration file's row to select it and c lick 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. |
| | > Apply Configuration File |
| | Apply Configuration File |
| | File Name: system-default.conf |
| | If applying the configuration file encounters an error: |
| | Immediately stop applying the configuration file |
| | Immediately stop applying the configuration file and roll back to the previous configuration |
| | Ignore errors and finish applying the configuration file |
| | Ignore errors and finish applying the configuration file and then roll back to the previous configuration |
| | |
| | OK Cancel |
| | 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. |
| | C lic k OK to have the Zyxel Device start applying the configuration file or c lic k Cancel to c lose the screen. |
| # | This column displays the number for each configuration file entry. This field is a sequential value, and it is not a ssociated 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 de le te 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. |

| IABEL | DESC RIPHO N |
|--------------------------------------|---|
| La st Mo d ifie d | This column displays the date and time that the individual configuration files were last changed or saved. |
| Up lo a d C o nfig ura tio n File | The bottom part of the screen allows you to up load a new or previously saved configuration file from your computer to your Zyxel Device. |
| | You cannot up load a configuration file named system-default.confor lastgood.conf. |
| | If you up load 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 orclick Browse to find it. |
| Browse | C lick Browse to find the .conf file you want to upload. The configuration file must use a ".conf" filename extension. You will receive an enormessage if you try to upload a fie of a different format. Remember that you must decompress compressed (.zip) files before you can upload them. |
| Up lo a d | Click Upload to begin the upload process. This process may take up to two minutes. |

Table 72 Maintenance > File Manager > Configuration File (continued)

18.2.1 Example of Configuration File Download Using FIP

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 FIP 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 FIP 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 firm ware recovery finishes.
- 4 Enteryourusername when prompted.
- 5 Enteryour 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.

18.3 Firmware Package

Click Maintenance > File Manager > Finnware Package to open this screen. Use the Finnware 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 CUR ference Guide for how to determine if you need to recover the firmware and how to recover it.

Find the firm ware package at www.zyxelcom in a file that (usually) uses a .b in extension.

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

| Figure 104 | Ma inte na nc e | > File | Manager> | Firmware | Package |
|------------|-----------------|--------|----------|----------|---------|
|------------|-----------------|--------|----------|----------|---------|

| Configuration File | e Firmware Package Shell Script | |
|--------------------|---|----------------------|
| Version | | |
| Boot Module: | V1.8 | |
| Current Version: | V6.00(ABIM.3)51 | |
| Released Date: | 2019-09-19 03:19:47 | |
| Upload File | | |
| To upload firmwo | are, browse to the location of the file (*.bin) and | I then click Upload. |
| File: | Select a file Bro | wse Upload |
| | | |
| | | |

| Table 73 | Maintenance > | File | Manager> | Firmware | Package |
|----------|---------------|------|----------|----------|---------|
|----------|---------------|------|----------|----------|---------|

| IABEL | DESC RIPIIO N |
|--------------------|--|
| Boot Module | This is the version of the boot module that is currently on the Zyxel Device. |
| Curre nt Versio n | This is the firm ware version and the date created. |
| Re le a se d Da te | This is the date that the version of the firm ware 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 | C lic k Browse to find the .b in file you want to up load. Remember that you must decompress compressed (.zip) files before you can up load them. |
| Up lo a d | Click Upload to begin the upload process. This process may take up to two minutes. |

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

Note: The Zyxel Device automatically reboots after a successful up load.

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

Figure 105 Network Temporarily Disconnected



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

18.3.1 Example of Firmware Upload Using FIP

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

- 1 Connect your computer to the Zyxel Device.
- 2 The FIP 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 FIP 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 firm ware recovery finishes.
- 4 Enteryourusername when prompted.
- 5 Enteryour password as requested.
- 6 Enter "hash" for FIP 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 Thansfer the firm ware file from your computer to the Zyxel Device. Type put followed by the path and name of the firm ware 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.

18.4 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 yourscripts. 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 106 Maintenance > File Manager > Shell Script

| Contractor | 10011110 | emware Pockage | sum scubi | | |
|---|--|-----------------|-----------------------|--|--------------------|
| heli Scriph | 10 - C | | | | |
| Cilinian | ie 🕿 Nersowi 🕿 | Developer Brook | D/A006/ | | |
| the second se | | | | and the second sec | |
| # ffic? | 4CMTNF | | 3040 | Last Modified | |
| # 1961 14 4 1 P | age 1 of 1 3 | H Show in 😐 🕯 | 500 1016 | Last Modified | No data to dipicy |
| IA 4 P | age (1of 1> 8 Script | 21 210W 28 💌 8 | - 1040 10778 | Last Modified | No data to dipiay |
| pload She | upper ogenitien of the second It is shell script, or | H Show H M In | of the file (29th) of | nd then click Upload | No data to dipilay |

 Each field is described in the following table.

Table 74 Maintenance > File Manager > Shell Script

| LABEL | DESC RIPIIO N |
|----------------------------|---|
| 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 a nother 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 c haracters (including a -zA-ZO-9;'~ $!@#$ %%&()_+[]{',=-). |
| | Click OK to save the duplicate orclick 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. |
| Do w nlo a d | Click a shell script file's row to select it and click Download to save the configuration to your computer. |
| Сору | 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 c haracters (including a -zA-Z0-9;'~ $!@#$ %%&()_+[]{}',=-). |
| | Click OK to save the duplicate orclick 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. |
| La st Mo d ifie d | This column displays the date and time that the individual shell script files were last changed or saved. |
| Up lo a d She ll Script | The bottom part of the screen allows you to upload a new orpreviously 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 orclick Browse to find it. |

| IABEL | DESC RIPIIO N |
|-----------|--|
| Browse | Click Browse to find the .zysh file you want to upload. |
| Up lo a d | Click Upload to begin the upload process. This process may take up to several minutes. |

C HAPTER 19 Diagnostics

19.1 Overview

Use the diag no stics screen for trouble shooting.

19.1.1 What You Can Do in this Chapter

The **Diagnostics** screen (Section 19.2 on page 178) generates a file containing the Zyxel Device's configuration and diagnostic information if you need to provide it to customer support during trouble shooting.

19.2 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 trouble shooting. All categories of settings and shell script files stored on the Zyxel Device will be included in the diagnostic file.

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

Figure 107 Maintenance > Diagnostics> 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 108 Maintenance > Diagnostics: Debug Information Collector



19.3 Remote Capture

Use this screen to capture network traffic going through the Zyxel Device connected to the Zyxel gate way or ZyWAIL, and output the captured packets to a packet analyzer (also known as network or protocol analyzer) such as Wire shark.

Click Maintenance > Diagnostics > Remote Capture to open the Remote Capture screen.

Figure 109 Maintenance > Diagnostics> Remote Capture

| Diagnostias | Remote Capture | | | | |
|------------------------------------|----------------|------------|--|--|--|
| Remote Copture | | | | | |
| Server Fort: | 2002 | | | | |
| Wireless Monitor Interface Support | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | Stort Stop | | | |

The following table describes the labels in this screen.

| Table | 75 | Mainte nance 🔅 | > | Dia g no stic s> | Re m o te | Capture |
|-------|----|----------------|---|------------------|-----------|---------|
|-------|----|----------------|---|------------------|-----------|---------|

| IABEL | DESC RIPTIO N |
|----------------|---|
| Se rve r Po rt | Enter the number of the server port you want the packet analyzer to connect to in order to capture traffic going through the Zyxel Device. The default port number is 2002. |
| Sta rt | Click this button to allow the packet analyzer to start capturing traffic going through the Zyxel Device. |
| Sto p | Click this button to stop the packet analyzer from capturing traffic going through the Zyxel Device. |

C HAPTER 20 LEDs

20.1 Overview

The LEDs of your ZyxelDevice can be controlled such that they stay lit (ON) or OFF after the ZyxelDevice is ready. There are two features that control the LEDs of your ZyxelDevice - Locator and Suppression (see Section 1.4 on page 18).

20.1.1 What You Can Do in this Chapter

- The Suppression screen (Section 20.2 on page 180) allows you to set how you want the LEDs to behave after the Zyxel Device is ready.
- The Locatorscreen (Section 20.3 on page 181) allows users to see the actual location of the Zyxel Device between several devices in the network.

20.2 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 > IEDs > Suppression** screen to see the default IED behavior and change the IED 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 3.1 on page 28) for information on default values for different models.

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

To a c c e ss this sc re e n, c lic k Maintenance > LEDs > Suppression.
| Figure 110 | Ma inte na nc e | > LEDs $>$ | Suppression |
|------------|-----------------|------------|-------------|
|------------|-----------------|------------|-------------|

| Suppression | Location |
|--|--|
| Configuration | |
| El Suppression | On Ch |
| Note: | |
| Followings o 1, Device is 2. Device is 3. Suppression | te the exceptions when LED suppression mode is On. serforming Firmware Upgrade: soofing. In made does not apply to Locator LED. |

The following table describes fields in the above screen.

| IABEL | DESC RIPIIO N |
|----------------|--|
| Suppression On | If the Suppression On checkbox 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. |
| Re se t | Click Reset to return the screen to its last-saved settings. |

Table 76 Maintenance > LED > Suppression

20.3 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 locatorfeature, enter a number of minutes and click **Tum On** button to have the Zyxel Device find its locator. 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 tum 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 a c c e ss this sc re e n, c lic k Mainte nance > LEDs > Locator.

Figure 111 Maintenance > LEDs > Locator

| Counciliant Cleavier | |
|--|--|
| Configuration | |
| [Jum Oni] [Jum Citi] | |
| Automatically Edinguish Alter; 10 (1-50 minuter) | |
| | |
| | |
| Apply Retrem | |

The following table describes fields in the above screen.

| IABEL | DESC RIPTIO N |
|-----------------------------------|---|
| Tum On Tum Off | Click Thum On button to activate the locator. The Locator function will show the actual location of the Zyxel Device between several devices in the network. |
| | O the rwise, c lick Tum 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. |
| Re fre sh | Click Refresh to update the information in this screen. |

Table 77 Maintenance > LED > Locator

CHAPTER 21 Reboot

21.1 Overview

Use this screen to restart the Zyxel Device.

21.1.1 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.

21.2 Reboot

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

Figure 112 Maintenance > Reboot

| Taboof | |
|---|--|
| apoci | |
| Click the Reboard buttom to reboard the device. Please wolf a few minutes until the tagin screen appears. If the tagin screen does not appear, type the IP address of the device in your Web browser. | |
| Report | |

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 CII command reboot to restart the Zyxel Device.

C HAPTER 22 Shutdown

22.1 Overview

Use this screen to shut down the Zyxel Device.

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

22.1.1 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.

22.2 Shutdown

To a c c e ss this sc re e n, c lic k Mainte nance > Shutdown.

| Fig ure | 113 | Ma inte na nc e | > | Shutdowr | ı |
|---------|-----|-----------------|---|----------|---|
|---------|-----|-----------------|---|----------|---|

| Shuhlows | |
|---|----------|
| Shutdown | |
| Ctol: the "Shutdown" button to shutdown the device. | |
| Shund | priviti. |

Click the **Shutdown** button to shut down the Zyxel Device. Wait for the Zyxel Device to shut down before you manually tum 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

C HAPTER 23 Cloud Mode

23.1 Overview

The Zyxel Device is managed and provisioned automatically by the *NCC (Ne bula 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 VIAN setting or manually set its IP address, access its simplified web configurator (see Chapter 4 on page 30). You can check the NCC's Access Point > Monitor > Access Points screen or the connected gate way for the Zyxel Device's current IAN IP address. Alternatively, disconnect the gate way or disable its DHCP server function and use the Zyxel Device's default static IAN IP address (192.168.1.2).





23.2 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 > VIAN

- 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.

23.3 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 115 Dashboard

| AP information | (80) |
|--|--|
| MAC Address | 58.88.F3.FF.EE.E0 |
| Seriol Number: | 3192555009042 |
| Product Model: | WAKSTOD |
| 2.40 Channel Informatio | on: Channel's CH 7 / Transmit power is 20 dBm |
| 30 Channel Information | Channel's CH 36/40/44/48 / Transmit power is 23 dBm |
| Ethemet | This access point is directly connected to a local network, IP Address 192,1ab.1.10 |
| intenat: | This access point is connected to the internet. |
| Nebula Connectivity Status: | This access point is successfully connected to the Nebula. |
| Nebula Control Center Activation Status | This access point has been registered to the Nebula. |
| Use Proxy to Access NCC: | na |

The following table describes the labels in this screen.

| | LABEL | DESC RIPTIO N |
|---|---|---|
| ĺ | AP Information | |
| | MAC Address | This field displays the MAC address of the Zyxel Device. |
| ĺ | Se ria l Num b e r | This field displays the serial number of the Zyxel Device. |
| ĺ | 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 IAN 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 a c tiva ted if the wire less IAN is disabled. |
| | Ethe me t | This field displays whether the Zyxel Device's Ethemet port is connected and the IP address of the gate way to which the Zyxel Device is connected. |
| ĺ | Inte me t | This field displays whether the Zyxel Device is connecting to the Internet. |
| | Ne b ula C o nne c tivity Sta tus | This field displays whether the Zyxel Device can connect to the Zyxel Nebula Control Center (NCC). |

Table 78 Dashboard

Table 78 Dashboard (continued)

| IABEL | DESC RIPTIO N |
|---|---|
| Nebula Control Center Activation Status | This field displays whether the Zyxel Device has been registered and can be managed by the NCC. |
| Use Pro xy to Ac c e ss NC C | This displays whether the NAP uses a proxy server to access the NCC (Nebula Control Center). |



| AP Information | 兼項 |
|--|---|
| MAC Address: | 00:13:49:00:00:01 |
| Setal Number: | Z34131340 80-009-011001AA |
| Product Model: | WAXSTOD |
| 2.4G Channel Information: | Channel is CH 6 / Transmit power is 23 dBm |
| 5G Channel Information: | Channel is CH 36/40/44/48 / Transmit power is 26 dBm |
| Etsemeti | tria access point is trying to join a welwark or find is waiting lithernet connection. |
| Internet: | This access point is connected to the Internet. |
| Nebula Connectivity Status: | We access point & not conversient to the Netsola. (Get pertillance taked) |
| Nebula Control Center Activation Status | This access point has not been nigistered to the Nebula. |
| Use Proxy to Access NCC: | no |

C HAPTER 24 Network

24.1 Overview

This chapterdescribes how you can configure the management IP address and VIAN settings of your Zyxel Device in cloud mode.

See Section 9.1 on page 69 for information about IP addresses.

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

24.1.1 What You Can Do in this Chapter

- The IP Setting screen (Section 24.2 on page 189) configures the Zyxel Device's LAN IP address.
- The VIAN screen (Section 24.3 on page 191) configures the Zyxel Device's VIAN settings.

24.2 IP Setting

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

| IP Setting VIAN | | |
|---------------------------|---------------|-------------|
| P Address Assignment | | |
| Get Automatically | | |
| Like Fixed IP Address | | |
| IP Address: | 192.165.1.1 | |
| Subnet Mask: | 255.255.252.0 | |
| Gateway: | 192.168.1.5 | (Optional) |
| DNS Server IP Address: | 192.168.1.11 | (Optional) |
| E Use Proxy to Access NCC | | |
| Provy hervers | | |
| Présny Points | | 0.469300 |
| #2 Avimentication? | | |
| Over Name: | | |
| Prevatoria: | | |
| | | |
| | | Apply Reset |

Figure 116 Configuration > Network > IP Setting

 $\label{eq:eq:charge} Each field is described in the following table.$

| Table 79 | C o nfig ura t | io n > Ne two rk > | IP Setting |
|----------|----------------|--------------------|------------|
| | | | |

| LABEL | DESC RIPIIO N |
|---------------------------------|--|
| IP Address Assignment | |
| Get Automatically | Select this to make the interface a DHCP client and automatically get the IP address, subnet mask, and gate way address from a DHCP server. |
| Use Fixed IP Address | Select this if you want to specify the IP address, subnet mask, and gate way manually. |
| IP Ad d re ss | Enter the \mathbb{I} address for this interface. |
| Sub ne t Ma sk | 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 ZyxelDevice is behind a proxy server, you need to select this option and configure the proxy server settings so that the ZyxelDevice can access the NCC through the proxy server. |
| Pro xy Se rve r | Enter the IP address of the proxy server. |
| Pro xy Po rt | Enterservice port number used by the proxy server. |
| Authentication | Select this option if the proxy server requires a uthentication before it grants access to the Internet. |
| Use r Name | Enteryourpmoxy username. |
| Pa ssw o rd | Enteryourproxy password. |
| Apply | Click Apply to save your changes back to the Zyxel Device. |
| Re se t | Click Reset to return the screen to its last-saved settings. |

24.3 VIAN

This section discusses how to configure the Zyxel Device's VIAN settings. See Section 9.3 on page 71 for more information about VIAN.

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

Figure 117 Configuration > Network > VLAN

| IP Setting | VLAN |
|---------------|------------|
| VLAN Settings | |
| Management | VLAN ID: 1 |
| Untagged | Tagged |
| | |
| | |
| | |
| | |
| | |

Each field is described in the following table.

| IABEL | DESC RIPTIO N |
|-----------------------|---|
| VIAN Settings | |
| Management VLAN ID | Entera VIAN ID for the Zyxel Device. |
| Untagged/ Tagged | Set whether the Zyxel Device adds the VIAN ID to outbound traffic transmitted through its Ethemet port. |
| Apply | Click Apply to save your changes back to the Zyxel Device. |
| Re se t | Click Reset to return the screen to its last-saved settings. |

Table 80 Configuration > Network > VLAN

C HAPTER 25 Maintenance

25.1 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 18 on page 167 for information about shell scripts.

25.1.1 What You Can Do in this Chapter

- The Shell Script screen (Section 25.2 on page 192) stores, names, downloads, and up loads shell script files.
- The **Diagnostics** screen (Section 25.3 on page 193) generates a file containing the Zyxel Device's configuration and diagnostic information if you need to provide it to customer support during trouble shooting.
- The Log > View Log screen (Section 25.4 on page 194) displays the Zyxel Device's current log messages when it is disconnected from the NCC.

25.2 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" file name 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.

| ren acris | | | | |
|-----------|---|------------------------------|---------------------------|---------------------|
| Clint | zisi 🕱 karoove 🔡 Dowersoo | R BCODY | | |
| | 1 Martini | 300 | Last Modified | |
| 14.4.1 | Fage 1 of 1 > 41 Show | w si 👻 densi | | No rista to display |
| | | | | |
| | | | | |
| nicad Si | tell Script | | | |
| no uplo | ell Script ad a shell script, browse to th | e location of the file (.2)s | hý and thên click Upload. | |

Figure 118 Maintenance > Shell Script

192

Each field is described in the following table.

| Mole of Mu | |
|-------------------------|---|
| IABEL | DESC RIPIIO N |
| 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 c haracters (including a -zA-Z0-9; $\sim !@#$ \$%^&()_+[]{}',.=-). |
| | Click OK to save the duplicate orclick 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. |
| Do w n lo a d | C lick a shell script file's row to select it and c lick Download to save the configuration to your computer. |
| Сору | 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 orclick 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. |
| La st Mo d ifie d | This column displays the date and time that the individual shell script files were last changed or saved. |
| Up load Shell Script | The bottom part of the screen allows you to upload a new orpreviously 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 orclick Browse to find it. |
| Browse | Click Browse to find the .zysh file you want to upload. |
| Up lo a d | Click Upload to begin the upload process. This process may take up to several minutes. |

Table 81 Maintenance > Shell Script

25.3 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 trouble shooting. 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.





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 120 Maintenance > Diagnostics: Debug Information Collector



25.4 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.

| Fig ure | 121 | Ma inte na nc e | > | Log | > \ | ∕ie w | Log |
|---------|-----|------------------|---|-----|-----|-------|-----|
| rig uic | 141 | ma ma na na na c | - | шg | - | | шg |

| 2 | | | | | |
|--|--|--|--|------------|--------|
| ga | | | | | |
| cog will be deplayed Display: Source Address | System | et li not connecte | Ptionty: Destination Address: | ary | - |
| in ana interface. | any | (T) | Destination interface: | any | 5 |
| and the state of the second | | | | | |
| Profocot Search | any | 10 | Keyword: | | |
| Profucat Search Refresh @ Clear | any | | Keyword: | Dertrato | n hole |
| Profucció Leccol 2 Refreim - de Clear I 15 Cline 20 2019 11-07 Doix | any P., C., Areas , G., 3., Parton | Copt Ther Rns: speece | Keyword: perfice rs icconvFue | Derbrato | n hole |
| Profucció Meteoria 21 Retream - de Clear I 20 2019 11-27 04-4 24 2019-11-27 04-4 | any P. C. A-mo a. 3. Parton a. 5. Parton | opt The Drit speed | Keyword: Donnes Ph 1000m/Fue | Destruto | n hole |
| Profucció Arcocch 2 Retream de Clear I 20 2019 11-27 04-4 34 2019-11-27 04-4 42 2019-11-27 04-3 | any A. C. A-10 a. 3. Partol a. 5. Partol b. 5. Enterpr | Copt The Pricipeeo Copt The Pricipeeo Cooking SelWLAN & configu | Keyword: Stringe Ph ICCOM/Fue Med successfully with t | Destinatio | n Noe |
| Profucció Leocch 20 Retrein de Clear 20 2019 11-27 04-4 24 2019 11-27 04-4 42 2019 11-27 04-3 10 2019 11-27 04-3 | any P. C. A | Contract The This speed spewich is configurately the The This speed | Keyword: CORCE IN ICCORVELS Med NUCCESSFUTY WITH N IN ICCORVELS. | Destinatio | n Nole |

The following table describes the labels in this screen.

| Table 82 | Ma inte na nc e | > Log | > Vie | wLog |
|----------|-----------------|-------|-------|------|
| | | | | |

| LABEL | DESC RIPIIO N |
|--------------------------------|--|
| 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 |
| | a vallable. If the filter settings are shown, the Display, Priority, Source Address, Destination Address, Source Interface, Destination Interface, Protocol, Keyword, and Search fields are available. |
| Disp la y | 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 . |
| Prio rity | 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, emor, wam, 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. |
| De stina tio n Ad d re ss | 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. |
| De stina tio n Inte rfa c e | This displays when you show the filter. Select the destination interface of the packet that generated the log message. |
| Pro to c o l | This displays when you show the filter. Select a service protocol whose log messages you would like to see. |
| Ke yword | 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. |
| Se a rc h | This displays when you show the filter. Click this button to update the log using the current filter settings. |

NWA50AX Use r's Guide

| LABEL | DESC RIPIIO N |
|--------------------------------|---|
| Re fre sh | Click this to update the list of logs. |
| ClearLog | $C \hbox{ lic }k \hbox{ this }b \hbox{ utto }n \hbox{ to }c \hbox{ lear the }w \hbox{ hole }\log , \hbox{ regard } \hbox{ less }o \hbox{ f }w \hbox{ hat } \hbox{ is }c \hbox{ umently }d \hbox{ isp } \hbox{ layed }on \hbox{ the }sc \hbox{ reen.}$ |
| # | This field is a sequential value, and it is not a ssociated with a specific log message. |
| Tim e | This field displays the time the log message was recorded. |
| Prio rity | This field displays the priority of the log message. It has the same range of values as the Priority field above. |
| C a te g o ry | This field displays the log that generated the log message. It is the same value used in the Display and (o the r) Category fields. |
| Me ssa g e | 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. |
| So urc e | 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. |
| De stina tio n | This field displays the destination IP address and the port number of the event that generated the log message. |
| De stina tio n Inte rfa c e | This field displays the destination interface of the packet that generated the log message. |
| Pro to c o l | This field displays the service protocol in the event that generated the log message. |
| No te | This field displays any additional information about the log message. |

Table 82 Maintenance > Log > View Log (continued)

PART II Appendices and Trouble shooting

C HAPTER 26 Trouble shooting

26.1 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 Ne two rk
- Resetting the Zyxel Device

26.2 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 PoEpower injector's witch.
- 2 Make sure the poweradapterorPoEpowerinjector/switch is connected to the ZyxelDevice and plugged in to an appropriate powersource. Make sure the powersource is turned on.
- 3 Disconnect and re-connect the power adapter or PoEpower 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 3.1 on page 28.
- 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 PoEpower injector to the Zyxel Device.
- 5 If the problem continues, contact the vendor.

26.3 Zyxel Device Management, Access, and Login

If orgot the IP address for the Zyxel Device.

- 1 The default in-band IP address in standalone mode is http://DHCP-assigned IP (when connecting to a DHCP server) or 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 26.6 on page 205.
- 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 IAN IP address.

Icannot see or access the Login screen in the Web Configurator.

- 1 Make sure you are using the correct IP address.
 - The default **P** 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 trouble shooting 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 3.1 on page 28.
- 3 Make sure your Internet browser does not block pop-up windows and has Java Scripts and Java enabled.
- 4 Make sure your computer is in the same subnet as the Zyxel Device. (If you know that there are noters 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 26.6 on page 205.

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

Advanced Suggestions

- Thy 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 wire lessly, use a computer that is connected to a IAN/EIHERNET port.

If orgot 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 26.6 on page 205.

Ican see the Login screen, but Icannot 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 PoEpower injector to the Zyxel Device.
- 4 If this does not work, you have to reset the Zyxel Device to its factory defaults. See Section 26.6 on page 205.

Icannot use FIP to upload / download the configuration file. / Icannot use FIP to upload new firm ware.

See the trouble shooting suggestions for I cannot see or access the Login screen in the Web Configurator. Ignore the suggestions about your browser.

Icannot access the Zyxel Device directly anymore after switching to NCC management.

• Check the Zyxel Device IP address and log in 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 e na b le d NCC Discovery, b ut the Zyxel Device is still in standalone mode.

Make sure your Zyxel Device is registered to the NCC.

The Zyxel Device is a heady 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 9.4 on page 73).
- 2 Checkyournetwork's fire wall/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 VIAN settings (see Section 9.3 on page 71). You may have to change the Management VIAN settings of the Zyxel Device to allow it to connect to the Intermet and access the NCC.
 - Note: Changing the management VIAN 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 does not 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 VIAN without this requirement. Change your Zyxel Device's management VIAN settings as necessary.

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 fire wall 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.

Ican only see newer logs. Older logs are missing.

When a log reaches the maximum number of log messages (see Section 1.4 on page 18), 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.

Icannot upload the firmware uploaded using FIP.

The Web Configurator is the recommended method for uploading firmware in standalone mode. For managed ZyxelDevices, using the NCC or AC is recommended. You only need to use FIP if you need to recover the firmware. See the CURe ference Guide for how to determine if you need to recover the firmware and how to recover it.

26.4 Internet Access

 $C \ \text{lients cannot access the Intermet through the Zyxel Device}.$

- 1 Check the Zyxel Device's hardware connections, and make sure the LEDs are behaving as expected (refer to Section 3.1 on page 28). See the Quick Start Guide and Section 26.2 on page 198.
- 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 c lients are trying to access the Internet wire lessly, make sure the wire less settings on the wire less c lients 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.

NWA50AX Use r's Guide

- 1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 3.1 on page 28. 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 wire less network (microwaves, otherwire less 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.

26.5 WiFi Network

Icannot access the Zyxel Device orping any computer from the WIAN.

- 1 Make sure the wire less IAN (wire less 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 wire less adapter (installed on your computer) is working properly.
- 4 Make sure the wire less adapter (installed on your computer) is EEE 802.11 compatible and supports the same wire less standard as the Zyxel Device's active radio.
- 5 Make sure your computer (with a wire less 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 wire less and wire less security setting s.

Hackers have accessed my WEP-encrypted wire less IAN.

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 wire less security is not following the re-authentication timer setting I specified.

If a RADIUS server authentic ates wire less stations, the re-authentic ation timer on the RADIUS server has priority. Change the RADIUS server's configuration if you need to use a different re-authentic ation timer setting.

Icannot 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 PKC S# 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 IIU-Trecommendation 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 PKC S# 7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKC S # 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 PKC S# 7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKC S# 7 certificate into a printable form.
 - Binary PKC S# 12: This is a format for transferring public key and private key certificates. The private key in a PKC S # 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 PKC S # 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.

Wire less 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 wire less 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 > Wire less > AP Information > Radio List screen, there is no load balancing indicator a ssociated with any Zyxel Devices assigned to the load balancing task.

• Check that the AP profile which contains the load balancing settings is comectly 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.

26.6 Resetting the Zyxel Device

If you cannot access the Zyxel Device by any method, try restarting it by tuming 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.

26.7 Getting More Trouble shooting Help

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





A PPENDIX 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 Zyxelproducts, such as the ZyxelDevice, issue the irown public key certificates. These can be used by web browsers on a IAN 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 URLin your web browser's address barbegins with https:// or there is a sealed padlockicon (

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, c lic k Not Secure > Certificate (Invalid).



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

| eid | Value | |
|--------------------------|-------------------------------|---|
| Verson | 43 | Ŀ |
| Serial number | 95 24 bf 0d | Ę |
| Signature algorithm | shasRSA | l |
| Sgnature flash eigorithm | stua 3 | |
| laver | usg60_\$888F.9FED32A | |
| Valid from | Monday, October 19, 2015 Sten | |
| Valid to | Thursday, October 16, 2025 S | |
| To Atlant | UNAGE REPORTED TO A | 2 |
| | | |

5 In the Certificate Export Wizard, click Next.

| Certificate Export Waard | |
|--------------------------|--|
| | <section-header> Welcome to the Certificate Export Wizard This ward helps you copy certificates, certificate trust iss and certificate revocation lists from a certificate to your dist. A certificate, which is issued by a certification authority, is confirmation of your identity and contains information used to protect data or to establish secure network cornectors. A certificate store is the system area where certificates are kept. To continue, cloir Next.</section-header> |
| | < Back Next > Cancel |

NWA50AX Use r's Guide

209

 ${\bf 6} \quad {\rm Se}\,{\rm le}\,c\,t\,{\rm the}\,\,fo\,{\rm mat}\,and\,\,{\rm setting}\,s\,yo\,u\,\,want\,to\,\,use\,\,and\,\,{\rm the}\,n\,c\,lic\,k\,\,{\bf Ne\,xt}.$

| Certificate Esport Wizard | X |
|--|------|
| Export File Format Certificates can be exported in a variety of file formats. | |
| Select the format you want to use: | |
| () DER encoded binary X.509 (,CER) | |
| () Base-64 encoded X. 509 (,CER) | |
| Cryptographic Message Syntax Standard - PKCS #7 Certificates (,P76) Circlede all certificates in the certification path if possible | |
| Personal Information Exchange - PKCS #12 (JPFX) Include all certificates in the certification path if possible | |
| Delete the private key if the export is successful | |
| Espurt all estimated properties | |
| C Mcrosoft Serulated Certificate Stare (.507) | |
| Learn more about <u>constituate. Re formata</u> | |
| < Back Next > Ca | ncel |

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

| Specify the name of the file | you want to export |
|------------------------------|--------------------|
| File name: | |
| D:\cert.cer | Stowse |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

NWA50AX Use r's Guide

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

| Comple Wizard | eting the C | ertificate l | Export |
|-------------------------------------|-----------------------------------|-------------------|------------------------------|
| You have s wittend. | uccessfully comp | eted the Certific | ale Export |
| Export Ke Indude al File Form | rya I certificates in th at | e certification p | No No ath No DER En |
| (*)- | | | |

9 Finally, click OK when presented with the successfulcertificate export message.



Import a Certificate

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

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



2 Sc to ll down and c lick Advanced to expand the menu. Under Privacy and security, c lick Manage certificates.

| Advanced + | |
|---|-----|
| vacy and security | |
| Sync and Boogle services. More settings that retails to privacy, settienty, and data collection | |
| Allow Obrome sign-in By turning this off, you can sign in to Google altes like Omeil without signing in its Dironwe | -0 |
| Send a 'Do Not Track' request with your browsing traffic | 0.0 |
| Allow after to check if you have payment methods saved | |
| Preised pages for faster browsing and searching Uses cookies to remember your preferences, even if you don't start those pages | |
| Manage contributes Manage HTTPS/SSS, partificates and settings | Ø |
| Content settings Control what information websites can use and what content they can show you | |
| Clear browning data | |

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

| Issued To | Issued By | Exprato | Friendly Name | |
|--|--|--|--|---------|
| AddThust External AffirmThust Comme Baltimore CyberThu ICertum CA ICertum Trusted Ne ICertum Trus | AddTrust External CA AffirmTrust Converced Baltanore CyberTrust Certum CA Certum Trusted Netw Class 3 Public Primary COMODO RSA Certific Copyright (c) 1997 M DigCert Assured 10 R | 5/30/2020 12/31/2030 5/13/2025 6/11/2027 12/31/3029 8/2/2028 1/19/2038 12/31/1999 11/10/2031 | Sectigo (AddThu AffirmTrust Corr DigiCert Soltmon Certum Certum Trusted VerSign Class 3 Sectigo (formert Microsoft Timest DigiCert | |
| noort | Renive | | [::A | dvences |

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.

| 3.65 | 100 | Computer | | | | | | | +14+ Gard | Lealing St. | P |
|--------|--------|-----------|-------------|-----|----------|--------|-----|----------------------|------------|--------------------|------|
| Digett | | Rea Align | - | | | | | | | - 10 + 13 | - 60 |
| | | | Thereise. | | (Data to | attat | | Type | die . | | |
| - | | | 1.14 | | | 26 | | - | | | |
| 1 | time. | | | | | 1.54 | | | | | |
| | - | 100 | | | - 28. | 445 | ٥. | 14 | | | |
| | 1000 | | | | | 100 | 3.0 | | | | |
| | | | - | | | 100 | | 14 | | | |
| | | | | | - 25 | 100 | | 14 | | | |
| | uter - | | | 101 | | 一些 | | 14 | | | |
| - 44 | 41.530 | | | | - 28 | 2.08 | | - 14 | | | |
| 1.00 | (CD) | 1.14 | · · · · · | | | 188. | | 10 | | | |
| 9 | +014- | - H | - h. | | 14. | 4(0) | | 14 | | | |
| | 1000 | | 5.0 | | 26 | 119. | | - M | | | |
| S. | 417 | - 4(j) | - 20 | | - 25 | 127 | | 1.9 | | | |
| - | | - 48 | a | | 25 | -42 | | | | | |
| | | - 13 | | | /8 | 130 | | | | | |
| · tim | look. | - 11 | - vet.tem | | 4.95.8 | 101.54 | M.) | Secondy Terrificants | 1.16 | | |
| | | | | | | | | | | | - |
| | | (Fires | ene iertind | | | | | | · (8.309-C | (In-their) elsings | |

6 Click Next.

| Certificate Import Wizard |
|--|
| Certificate Store Certificate stores are system areas where certificates are kept. |
| Windows can automatically select a certificate store, or you can specify a location for the certificate. |
| Automatically select the certificate store based on the type of certificate |
| Pace all certificates in the following store |
| Certificate store: |
| Trusted Root Certification Authorities Browse |
| Learn more about <u>pertificate storing</u> |
| < Back Next > Cancel |

7 Confirm the settings displayed and click Finish.

| Certificate Import Wizard | | | | | | |
|---------------------------|--|-----------------------------------|--|--|--|--|
| | Completing the Wizard | Certificate Import | | | | |
| 4 | The certificate will be exported after you click Finish. | | | | | |
| ~ | Certificate Thre Selecte | Olin Liter Trusted Root Certifica | | | | |
| | Content File Name | Certificate Dt/cert_test_cer | | | | |
| | | | | | | |
| | (e)m | | | | | |
| | | | | | | |
| | | | | | | |
| | < Back | Finish Cancel | | | | |

 $\label{eq:second} \textbf{B} \quad \text{ If } p \, \text{re sented } with \ a \ \text{sec unity } w \, a \, \text{ming} \,, \, c \ \text{lic} \ k \, \textbf{Ye s}.$

| Security, V | /among | × |
|-------------|--|---|
| | You are about to install a certificate from a certification authority (CA) claiming to represent: $u_{S_{2}} \stackrel{q}{\rightarrow} \stackrel{q}{\rightarrow}$ | |
| | Do you want to install this certificate? | |
| | Ves No | |
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.



 $\label{eq:chi} 2 \qquad C \mbox{ lic } k \mbox{ Install } C \mbox{ ertific a te} \,.$

| SH. | cate Information |
|---|--|
| This CA Root install this ce Authorities of | certificate is not trusted. To enable trust, rtificate in the Trusted Root Certification tare. |
| | NE 340 |
| | |
| Issued b | ex ung60_5888F3FED33A |
| Issued b | y: usg60_5888P3PED32A |
| Valid fro | m 10/ 19/ 2015 to 10/ 16/ 2025 |
| | |

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

| nicescindion nicesci | |
|---|---|
| Certificate Store Certificate stores are system areas wh | ere certificates are kept. |
| Windows can automatically select a can the certificate. | tificate store, or you can specify a location for |
| C Automatically select the certification | te store based on the type of certificate |
| Place all certificates in the follow | ing store |
| Certificate store: | |
| | Browse |
| | |
| | |
| | |
| | |
| | |
| een nore shoul no bit als shoes | |
| .mern more about <u>the tificalle stares</u> | |
| wern more about <u>se tificale stares</u> | |
| .mern more about <u>nertificalle staren</u> | |

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

| ert Certhrate Store | |
|---|-----------------------------------|
| elect the certificate store you want t | o use. |
| Personal | or you can specify a location for |
| Enterprise Trust | t on the type of sertificate |
| Active Directory User Object | /frontes |
| Thister Publishers | |
| Show physical stores | Browse |
| ок | Cancel |
| | |
| | |
| earn more about <u>certificate stores</u> | |
| | |
| | |

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

| Centificate Import Wizard | | 1 | | | |
|---------------------------|--|---------------------------------------|--|--|--|
| <u></u> | Completing the Certificate Import Wizard The certificate will be imported after you tick Firish. You have specified the following settings: | | | | |
| | Content Content | Trusted Root Certifica Certificate | | | |
| | < Beck | fraith Cancel | | | |

6 If presented with a security warning, click Yes.

| Security \ | Warning | × |
|------------|--|---|
| Å | You are about to install a certificate from a certification authority (CA) claiming to represent: 'I | |
| | ' si | |
| | Warning: If you initial this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk. | |
| | Do you want to install this certificate? | |
| | Yes No. | 1 |

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 Sc roll down and c lick Advanced to expand the menu. Under Privacy and security, c lick Manage certificates.

| Advancent + | |
|--|----|
| tracy and security | |
| Sync and Dodgle services More settings that retain to privacy, security, and data collection | |
| Allow Chrome sign-in By turning this off, you can sign in to Google Alles like Omail without signing in to Dironw | -0 |
| Send a 'Do Not Track' request with your browsing traffic | 30 |
| Allow also to check if you have payment methods saved | -0 |
| Preised pages for factor browsing and searching Uses cookies to remember your preferences, even if you don't stud those pages | - |
| Manage certificates Manage HTTPS/SSL certificates and settings | ß |
| Content settings Content what information websites can use and what content they can show you | |
| Clear browning data Clear history, capilier, cache, and more | i. |

3 In the Certific a tespop-up screen, click Trusted Root Certific a tion Authorities.

| Issued To | lesued By | Expirato | Friendly Name | |
|--|---|--|---|------|
| AddThust External JAffirmThust Comme JBalthore CyberThu ICertum CA Cleer Lim Trusted He Cleer 3 Public Prima IComODO RSA Cert ICopyright (c) 1997 IDigiCert Assured 20 | AddTrust External CA AffirmTrust Commercial Baltanore CyberTrust Gertum Crusted Netw Class 3 Public Primary COMODO RSA Certific Copyright (c) 1997 M DigiCert Assured 20 R | 5/30/2020 12/31/2030 5/13/2025 6/11/2027 12/31/3029 8/2/3028 1/19/2038 12/31/1999 11/10/2031 | Sectigo (AddThust) AffirmThust Com DigCert Baltinor Certum Certum Trusted VerSign Class 3 Sectigo (formerl Microsoft Timest DigCert | |
| Insortine (Econt., | Renive. | | Adva | nced |

NWA50AX Use r's Guide

- 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.



Fire fo x

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 SSLcentification, then the first time you browse to it you are presented with a certification error. Click Advanced.



 $\label{eq:click} 2 \quad C \operatorname{lic} k \operatorname{\mathbf{Vie}} w \operatorname{\mathbf{Certific}} a \operatorname{\mathbf{te}}.$

| Warning: Potential Security Risk Ahead |
|---|
| Firefox detected a potential security threat and did not continue to 192.168.1.2. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details. |
| Learn more |
| Go Back (Recommended) Advanced |
| |
| Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for 192.168.1.2. The certificate is only valid for . Error code: MOZILLA_PKDC_ERROR_SELF_SIGNED_CERT |
| View Certificate |
| Go Back (Recommended) Accept the Risk and Continue |

 $\textbf{3} \qquad C \ \text{lic} \ k \ \textbf{De ta ils} > \textbf{Export.}$

| Certificate (Secondary | |
|----------------------------------|---|
| ungh0_5880F3FE012A | |
| Certificate Tielde | |
| w usig60_5888F5FED32A | 3 |
| + Certificate | |
| Versitett | 1 |
| Serial Rumber | |
| Certificate Signature Algorithms | |
| lotuet | |
| ~ Validity | |
| Tield Value | |
| Egent | |

4 Type a filename and click Save.

| Sever Constitute To File | | | | | 1.2020 | | - |
|----------------------------------|----------------------|------|------------|------|-------------|--------------------|-------|
| OO ILa + Comp | vien 🔹 Lacuel Disk (| • 10 | | | • • • • • • | h Lassi (hiri (d)/ | ,p |
| -Digertite - Navida | MMC . | | | | | 83 | |
| | Name | | Exempleted | Tate | 304 | | 1 × 1 |
| File name Serie to type: [13] | 29 Cemilicate (1914) | | | | | | |
| in Hide Folders | | | | | | AVE CON | • |

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 Fire fox 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.

| Certifi | icate Manager | × |
|--------------------------------------|-----------------------------------|----|
| Your Certificates Poople | Servers Authorities | |
| You have orthicates on his that idea | hty these certificate authorities | |
| Certificate Name | Security Device | |
| UCA Global G2 Root | Builtin Object Token | ~ |
| UCA Extended Validation Boot | Builtin Object Token | |
| ≥ Unizeto Sp. z o.o. | | |
| Certum Root CA | Builtin Object Token | |
| × Unizeto Lechnologies S.A. | | |
| Certum Trusted Network CA | Builtin Object Token | |
| Certum Trusted Network CA 2 | Builtin Object Token | |
| ≥ VenSign, Inc. | | - |
| View <u>E</u> dit Trust Im | port Esport Qelete or Distrust | L |
| | | СК |

NWA50AX Use r's Guide