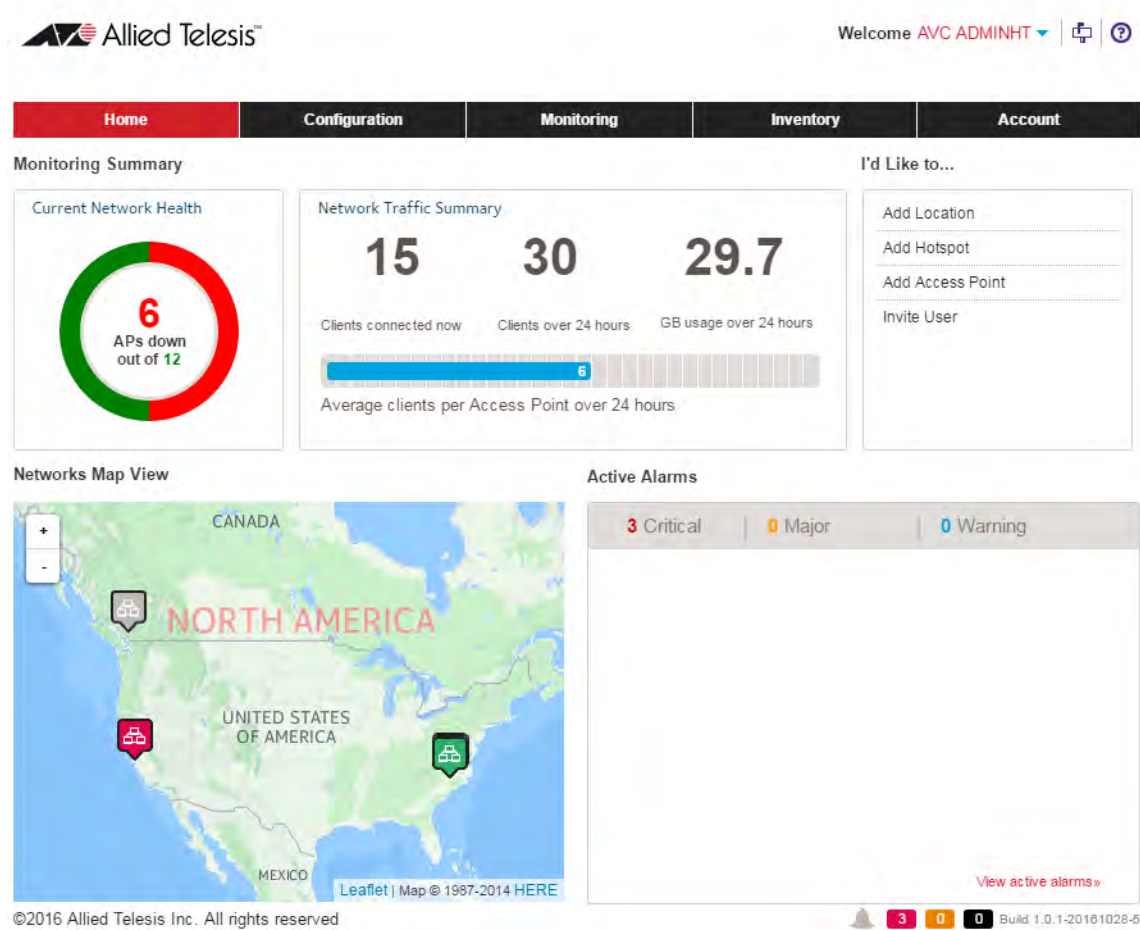


AlliedView Cloud™

□ AT-AP500 Wireless Access Point



User Guide

(Firmware Version 1.1)

Copyright © 2016 Allied Telesis, Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

Allied Telesis and the Allied Telesis logo are trademarks of Allied Telesis, Incorporated. Microsoft and Internet Explorer are registered trademarks of Microsoft, Incorporated. Chrome is a trademark of Google Incorporated. Apple and Safari are registered trademarks of Apple, Incorporated. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

Contents

Preface	15
Safety Symbols Used in this Document	16
Contacting Allied Telesis	17
Chapter 1: Introduction to AlliedView Cloud	19
What is AlliedView Cloud?	20
Architecture	21
AT-AP500 Access Point	23
Structure of Your Wireless Network Information	24
Location Entries	24
Wireless Network Folder	25
Wireless Network Entries	25
Access Points Folder	25
Building Entries	25
Floor Entries	26
Access Point Entries	26
Wireless Network and Access Point Parameters	27
Location Entry Parameters	27
Wireless Network Entry Parameters	28
Building Entry Parameters	30
Floor Entry Parameters	30
Access Point Entry Parameters	30
Wireless Network Examples	32
Building Your Account	39
Account Windows	41
Home	41
Configuration	42
Monitoring	43
Inventory	43
Account	44
User Accounts	46
Licenses and Tokens	47
Starting or Ending Management Sessions	48
Starting a Management Session	48
Ending a Management Session	49
Firmware Version Number	50
Chapter 2: Opening a New AlliedView Cloud Account	51
Introduction to Opening an AlliedView Cloud Account	52
Opening a 24/7 Support Account	53
Opening an AlliedView Cloud Account	57
Activating Your AlliedView Cloud Account	61
Running the Get Started Utility	63
Where to Go Next	72
Chapter 3: Locations	73
Introduction to Locations	74
Viewing Locations	75

Adding Locations	78
Copying Locations	82
Editing a Location's Name or Address	85
Deleting Locations	86
Chapter 4: Location Parameters	87
Introduction to Location Parameters	88
Turning Access Point Radios On or Off	89
Configuring Basic Radio Settings	91
Configuring the Maximum Number of Wireless Clients.....	94
Setting the Local Password for Access Points.....	96
Configuring WMM QoS	98
Chapter 5: Buildings and Floors	101
Introduction to Buildings and Floors.....	102
Viewing the Buildings of a Location	103
Adding Buildings to Locations	104
Changing Building Names	107
Deleting Buildings	108
Viewing the Floors of Buildings.....	109
Adding Floors to Buildings	110
Editing Floors	113
Deleting Floors.....	115
Chapter 6: Access Point Inventory	117
Viewing the Access Point Inventory	118
Introduction to Adding Access Points	120
Adding Access Points with the Configuration Tab	121
Adding Access Points with the Inventory Tab.....	125
Adding Access Points with a CSV File.....	127
Moving Access Points to New Locations	130
Changing Access Points to Unassigned	132
Moving Unassigned Access Points to Locations	133
Setting the Local Password for Unassigned Access Points.....	134
Deleting Access Points from Inventory	136
Chapter 7: Access Point Parameters	137
Introduction to Access Point Parameters	138
Configuring the Syslog Client.....	139
Setting Radio Channels	141
Configuring Radio Transmission Power.....	142
Rebooting Access Points	144
Restoring the Default Settings on Access Points.....	145
Chapter 8: Wireless Networks	147
Viewing Wireless Networks.....	148
Adding Wireless Networks	150
Editing Wireless Network Names and Authentications	155
Editing SSID Broadcasts and Wireless Clients Separation.....	160
Editing VLAN IDs	162
Specifying the 2.4GHz or 5GHz Radios of Wireless Networks	163
Enabling or Disabling Band Steering	164
Enabling or Disabling Wireless Networks	165
Deleting Wireless Networks	166
Chapter 9: Wireless Networks with Captive Portals	167
Introduction to Captive Portals	168
Viewing Captive Portals	170

Captive Portals with Basic Splash Windows	172
Introduction to Captive Portals with Basic Splash Windows	172
Adding Captive Portals with Basic Splash Windows.....	173
Adjusting Artwork in the Image Upload Window	180
Captive Portals with Advanced Splash Windows	183
Introduction to Captive Portal Profiles with Advanced Splash Windows.....	183
Guidelines to Modifying the Advanced Splash Windows	185
Adding a Captive Portal with Advanced Splash Windows	186
Uploading Advanced Splash Windows to a Captive Portal.....	188
Editing Captive Portals	191
Adding Captive Portals to Wireless Networks	193
Removing Captive Portals from Wireless Networks	195
Deleting Captive Portals from Your Account	197
Chapter 10: Wireless Network Hotspots	199
Introduction to Network Hotspots	200
Adding Free-Access Network Hotspots.....	201
Adding a New Captive Portal	203
Copying a Captive Portal	206
Assigning an Existing Captive Portal	209
Editing Network Hotspots	210
Deleting Wireless Network Hotspots	211
Chapter 11: Radio Schedules	213
Introduction to Radio On/Off Schedules	214
Viewing Radio Schedules.....	215
Adding Radio Schedules	217
Adding Radio Schedules to Locations.....	220
Removing Radio Schedules from Locations.....	223
Editing Radio Schedules	224
Deleting Radio Schedules	226
Chapter 12: RADIUS Server Profiles	227
Introduction to RADIUS Server Profiles.....	228
Viewing RADIUS Server Profiles.....	229
Adding RADIUS Server Profiles	231
Adding RADIUS Server Profiles to Locations.....	235
Removing RADIUS Server Profiles from Locations.....	237
Editing RADIUS Server Profiles	238
Deleting RADIUS Server Profiles	240
Chapter 13: Usage Plans	241
Introduction to Usage Plans	242
Viewing Usage Plans.....	243
Adding Usage Plans	245
Editing Usage Plans	248
Adding Usage Plans to Network Components	249
Deleting Usage Plans	250
Chapter 14: Status and Statistics Windows	251
Introduction to the Monitoring Tab Windows	252
Summary Windows.....	255
All Summary Window	255
Location Summary Window	255
Health Summary Window.....	256
Usage Summary Window.....	257
Security Summary Window	258

Wireless Network Summary Window	259
Access Point Summary Window.....	260
AP Details Windows.....	262
Active Alarms Windows	264
Cleared Alarms Windows.....	268
Event Log Windows	271
Hotspot Users Windows.....	273
Details Window	275
Command Log Window.....	277
Chapter 15: Licenses and Tokens	279
Introduction to Licenses and Tokens	280
Viewing Licenses and Tokens	281
Adding New Licenses	283
Chapter 16: Firmware Updates of Access Points	285
Introduction to Access Point Firmware Maintenance	286
Schedule Firmware Upgrades	287
Upgrade When Firmware is Available.....	289
Automatic Upgrades	291
Chapter 17: Accounts and Notifications	293
AlliedView Cloud User Accounts.....	294
Inviting Users to Add AlliedView Cloud Accounts	295
Accepting Invitations and Adding User Accounts	298
Changing User Roles.....	299
Deleting Users	301
Viewing or Changing Your User Profile	302
Viewing or Changing the Organization's Settings.....	304
Checking Application Notifications	305

Figures

Figure 1: AlliedView Cloud Architecture	21
Figure 2: Information Entries and Folders	24
Figure 3: Configuration Example 1	32
Figure 4: Configuration Example 2	33
Figure 5: Configuration Example 3	34
Figure 6: Configuration Example 4	34
Figure 7: Configuration Example 5	35
Figure 8: Configuration Example 6	36
Figure 9: Configuration Example 7	37
Figure 10: Configuration Example 8	38
Figure 11: Home Window	41
Figure 12: Configuration Window	42
Figure 13: Monitoring Window	43
Figure 14: Inventory Window	44
Figure 15: Account Window	45
Figure 16: AlliedView Cloud Window	48
Figure 17: Sign Out Selection	49
Figure 18: Firmware Version Number	50
Figure 19: 24/7 Online Support Web Page	53
Figure 20: Register for an Account Web Page	54
Figure 21: Completion of Registration	55
Figure 22: Change Your Password Prompt	55
Figure 23: My Support Cases Window	56
Figure 24: AlliedView Cloud Window	57
Figure 25: Sign Up Window	58
Figure 26: Sign Up Window with Username and Password Fields	58
Figure 27: Sign Up Window for AlliedView Cloud	59
Figure 28: Sign-Up Was Successful Window	60
Figure 29: New Account Activation Window	61
Figure 30: 90 Days Free Trial Window	61
Figure 31: License Window in the Account Tab	63
Figure 32: Get Started in the Configuration Window	64
Figure 33: Get Started Introductory Window	64
Figure 34: Add Service Location Window in the Get Started Utility	65
Figure 35: Add Wireless Network Window in the Get Started Utility	67
Figure 36: Assign Access Point to Location Window in the Get Started Utility	70
Figure 37: Locations Menu After the Get Started Utility	71
Figure 38: Configuration Tab	75
Figure 39: Location Configuration Settings	76
Figure 40: Configuration Map	77
Figure 41: Add Location Selection in the Choose Action Menu	78
Figure 42: Add Location Window	79
Figure 43: Add Location Confirmation Window	81
Figure 44: Selecting a Location	82
Figure 45: Copy Config Selection in the Choose Action Menu	83

Figure 46: Copy Config Window	83
Figure 47: Delete This Location Selection in the Choose Action Menu	86
Figure 48: Selecting a Location in the Locations Menu	89
Figure 49: Expanding Wireless Radio Area	90
Figure 50: Expanding Load Balancing Area	95
Figure 51: AP Location Management Section for the Local Password for Access Points in a Location.....	96
Figure 52: QoS Section.....	99
Figure 53: Viewing the Buildings of a Location	103
Figure 54: Selecting a Location from the Locations Menu	104
Figure 55: Add Building Selection in the Choose Action Menu.....	104
Figure 56: Add Building Window	105
Figure 57: Add Building Confirmation Window	106
Figure 58: Selecting a Building	107
Figure 59: Building Name Field.....	107
Figure 60: Delete This Building Selection in the Choose Action Menu.....	108
Figure 61: Displaying the Floors of a Building	109
Figure 62: Add Floor Selection in the Choose Action Menu	110
Figure 63: Add Floor Window	111
Figure 64: Add Floor Confirmation Window	112
Figure 65: Selecting a Floor.....	113
Figure 66: Floor Details.....	114
Figure 67: Delete This Floor Selection in the Choose Action Menu.....	115
Figure 68: List of Access Points in the Inventory Tab.....	118
Figure 69: Access Point Identifier	118
Figure 70: Inventory Menu with Locations	119
Figure 71: Access Point Status Information.....	119
Figure 72: Example of Adding an Access Point to a Floor with the Locations Menu.....	121
Figure 73: Add Access Point Selection in the Choose Action Menu.....	122
Figure 74: Add Access Point Window.....	122
Figure 75: Access Point Profile Screen for an Assigned Access Point.....	123
Figure 76: Add Access Point Selection.....	125
Figure 77: Access Point Profile Screen for an Unassigned Access Point.....	126
Figure 78: Add Multiple APs Selection in the Choose Action Menu.....	127
Figure 79: Add Multiple APs Window.....	128
Figure 80: Add Multiple Access Points Window.....	129
Figure 81: Selecting an Access Point in the Locations Menu	130
Figure 82: Location, Building, and Floor Pull-down Menus for Moving Access Points	131
Figure 83: Unassigned Option in the Inventory Menu.....	133
Figure 84: Account Setting in the Account Menu	134
Figure 85: Account Setting for the Local Password for Unassigned Access Points	134
Figure 86: Delete this Access Point Selection in the Choose Action Menu	136
Figure 87: Selecting an Access Point in the Locations Menu	139
Figure 88: Advanced Option in the Access Point Profile Screen	140
Figure 89: Reboot this Access Point Selection in the Choose Action Menu	144
Figure 90: Reboot this Access Point Selection in the Choose Action Menu	145
Figure 91: Selecting a Wireless Network	148
Figure 92: Wireless Network Configuration Screen	149
Figure 93: Selecting Wireless Networks in the Locations Menu	151
Figure 94: Add Wireless Network Selection in the Choose Action Menu.....	151
Figure 95: Add Wireless Network Window.....	152
Figure 96: Selecting a Wireless Network in the Locations Menu	155
Figure 97: Network Name and Authentication Section	156
Figure 98: Security Parameters	160
Figure 99: VLAN Settings Parameter.....	162
Figure 100: Radio Parameters	163

Figure 101: Enabling or Disabling a Wireless Network	165
Figure 102: Delete This Wireless Network Selection in the Choose Action Menu	166
Figure 103: Captive Portal Profiles Selection in the Shared Settings Menu.....	170
Figure 104: Wireless Network with Captive Portal Icon.....	170
Figure 105: Selecting a Wireless Network with a Captive Portal in the Locations Menu	171
Figure 106: Captive Portal Section in a Wireless Network Configuration.....	171
Figure 107: Adjustable Items in the Default Basic Splash Window	172
Figure 108: All Selection in the Locations Menu	174
Figure 109: Add Captive Portal Profile Selection in the Choose Action Menu	174
Figure 110: Add Captive Portal Profile Window	175
Figure 111: Add Captive Portal Profile for a Basic Splash Window	177
Figure 112: Completion of a Captive Portal with a Basic Splash Window.....	180
Figure 113: Upload Image Window	181
Figure 114: Example of the Add Captive Portal Profile Window with Custom Artwork	182
Figure 115: Login Window.....	184
Figure 116: End-user License Agreement Window	184
Figure 117: Successful Login Window	185
Figure 118: Error Window.....	185
Figure 119: Add Captive Portal Profile Window for Advanced Splash Windows.....	187
Figure 120: Warning Prompt	189
Figure 121: Example of the Captive Portal Profile Window with Uploaded Files	190
Figure 122: Edit Captive Portal Profile	191
Figure 123: Selecting a Wireless Network.....	193
Figure 124: Expanding the Captive Portal Configuration Area.....	194
Figure 125: Selecting Captive Portal Profile.....	194
Figure 126: Disable Selection in the Captive Portal Pull-down Menu	196
Figure 127: Delete Captive Portal Profile	197
Figure 128: Selecting a Location.....	201
Figure 129: Add Hotspot (Free) Selection in the Choose Action Menu.....	201
Figure 130: Add Hotspot Window.....	202
Figure 131: Create New Option in the Add Hotspot - Set Access Policy Window.....	203
Figure 132: Add Hotspot - Edit Splash Page Window	205
Figure 133: Add Hotspot - Set Usage Plan Window.....	205
Figure 134: Copy From Existing Option in the Add Hotspot - Set Access Policy Window	207
Figure 135: Use Existing Option in the Add Hotspot - Set Access Policy Window.....	209
Figure 136: Selecting a Wireless Network.....	211
Figure 137: Delete This Wireless Network Selection in the Choose Action Menu	212
Figure 138: Radio On/Off Schedules Selection.....	215
Figure 139: Radio On/Off Schedules Window.....	215
Figure 140: All Selection in the Locations Menu	217
Figure 141: Add Radio Schedule Selection.....	217
Figure 142: Radio On/Off Schedule Window.....	218
Figure 143: Wireless Radio Section	221
Figure 144: Adding a Radio On/Off Schedule to a Location.....	221
Figure 145: Selecting a Radio On/Off Schedule for a Location.....	222
Figure 146: Removing a Radio Schedule from a Location	223
Figure 147: Edit Selected Button.....	224
Figure 148: Edit Selected Schedule Window	224
Figure 149: Delete Selected Button.....	226
Figure 150: Radius Server Profiles Selection in the Shared Settings Menu	229
Figure 151: Radius Server Profile Screen.....	229
Figure 152: All RADIUS Server Profiles Screen.....	230
Figure 153: Radius Server Profile	230
Figure 154: All Selection in the Locations Menu	231
Figure 155: Add Radius Server Profile Selection in the Choose Action Menu	231

Figure 156: Add Radius Server Profile Window.....	232
Figure 157: Confirmation Prompt for Adding a Radius Server Profile.....	234
Figure 158: Selecting a Location In the Locations Menu	235
Figure 159: Radius Server Section in the Location Configuration Settings	236
Figure 160: Removing a RADIUS Server Profile from a Location.....	237
Figure 161: Accounting Server Section for a RADIUS Server Profile	238
Figure 162: Delete This Radius Server Selection in the Choose Action Menu	240
Figure 163: Usage Plan Selection in the Shared Settings Menu	243
Figure 164: Usage Plan Window	243
Figure 165: All Usage Plans Window.....	244
Figure 166: Viewing a Usage Plan.....	244
Figure 167: All Selection in the Locations Menu	245
Figure 168: Add Usage Plan Selection in the Choose Action Menu	245
Figure 169: Add Usage Plan Window	246
Figure 170: Usage Plan Selection in the Shared Settings Menu	248
Figure 171: Delete This Usage Plan Selection in the Choose Action Menu	250
Figure 172: Monitoring Tab and Menus	252
Figure 173: Levels of Monitoring Windows	253
Figure 174: All Summary Window.....	255
Figure 175: Location Summary Window	256
Figure 176: Health Summary Window	257
Figure 177: Usage Summary Window	258
Figure 178: Security Summary Window for a Location.....	259
Figure 179: Wireless Network Summary Window.....	260
Figure 180: Access Point Summary Window.....	261
Figure 181: AP Details Windows in the Monitoring Menu	262
Figure 182: AP Details Window	263
Figure 183: Download Full Details Option in the AP Details Window	263
Figure 184: Active Alarms Windows in the Monitoring Menu.....	264
Figure 185: Active Alarms Window	265
Figure 186: Optional Columns Menu in the Active Alarms Window.....	266
Figure 187: Expanded Alarm Information	266
Figure 188: Download Full Active Alarms Option in the Active Alarms Window	267
Figure 189: Cleared Alarms Windows in the Monitoring Menu	268
Figure 190: Cleared Alarms Selection	269
Figure 191: Download Full Cleared Alarms Option in the Active Alarms Window	270
Figure 192: Event Log Windows in the Monitoring Menu	271
Figure 193: Event Log Selection.....	272
Figure 194: Hotspot Users Windows in the Monitoring Menu	273
Figure 195: Hotspot Users Menu Selections	274
Figure 196: Detail Window in the Monitoring Menu	275
Figure 197: Detail Window at the Access Point Level	276
Figure 198: Command Log Window in the Monitoring Menu.....	277
Figure 199: Licenses Selection in the Account Menu	281
Figure 200: Display Licenses.....	281
Figure 201: License Key Details	282
Figure 202: License Example	283
Figure 203: Add License in the Choose Action Menu.....	283
Figure 204: Add License Window	284
Figure 205: Schedule Firmware Selection in the Account Menu	287
Figure 206: Scheduled Selection in the Firmware Upgrade Menu.....	287
Figure 207: Firmware Upgrade Scheduling Area.....	288
Figure 208: Clicking Firmware Report.....	289
Figure 209: Firmware Report Details	289
Figure 210: Notify Me Selection in the Firmware Upgrade Menu	291

Figure 211: Invite User Selection in the Choose Action Menu	296
Figure 212: Invite User Window	296
Figure 213: Role Pull-down Menu in the Invite User Window	297
Figure 214: Users Selection in the Account Menu	299
Figure 215: User Account Search Icons	299
Figure 216: Delete User Selection in the Choose Action Menu	301
Figure 217: Accessing Your Account Profile	302
Figure 218: My Profile Window.....	302
Figure 219: Account Selection in the Account Menu	304
Figure 220: My Account Window	304
Figure 221: Accessing Application Notifications.....	305

Tables

Table 1. Location Entry Parameters	27
Table 2. Wireless Network Entry Parameters	28
Table 3. Access Point Entry Parameters	30
Table 4. Add Location Window in the Get Started Utility	65
Table 5. Add Wireless Network Window in the Get Started Utility	67
Table 6. Sections in the Location Configuration Window	76
Table 7. Add Location Window	79
Table 8. Basic Radio Settings	92
Table 9. Access Point Parameters	138
Table 10. Syslog Settings	140
Table 11. Sections in the Wireless Network Configuration Screen	149
Table 12. Add Wireless Network Screen	152
Table 13. Network Name and Authentication Section	156
Table 14. SSID Broadcasts and Wireless Client Separation Parameters	161
Table 15. Adjustable Items in the Basic Splash Window	173
Table 16. Add Captive Portal Profile Window	175
Table 17. Add Captive Portal Profile for a Basic Splash Window	178
Table 18. Filenames for Advanced Splash Windows	186
Table 19. Add Hotspot - Add Hotspot Network Window	202
Table 20. Create New Option in the Add Hotspot - Set Access Policy Window	204
Table 21. Copy From Existing Option in the Add Hotspot - Set Access Policy Window	207
Table 22. Radio On/Off Schedule Window	215
Table 23. Add Radio On/Off Schedule Window	218
Table 24. Add Radius Server Profile Screen	232
Table 25. Accounting Server in the Add Radius Server Profile Screen	239
Table 26. Usage Plan Window	244
Table 27. Add Usage Plan Window	246
Table 28. Monitoring Windows	253

Preface

This guide contains instructions on how to configure, manage, and monitor your AlliedView Cloud™ network.

The AlliedView Cloud software has a web browser interface you can access from any workstation with Internet access and an Internet web browser application.

This preface contains the following sections:

- ❑ “Safety Symbols Used in this Document” on page 16
- ❑ “Contacting Allied Telesis” on page 17

Safety Symbols Used in this Document

This document uses the following conventions.

Note

Notes provide additional information.



Caution

Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.



Warning

Warnings inform you that performing or omitting a specific action may result in bodily injury.



Warning

Laser warnings inform you that an eye or skin hazard exists due to the presence of a Class 1 laser device.

Contacting Allied Telesis

If you need assistance with this product, you may contact Allied Telesis technical support by going to the Support & Services section of the Allied Telesis web site at **www.alliedtelesis.com/support**. You can find links for the following services on this page:

- ❑ 24/7 Online Support — Enter our interactive support center to search for answers to your product questions in our knowledge database, to check support tickets, to learn about RMAs, and to contact Allied Telesis technical experts.
- ❑ USA and EMEA phone support — Select the phone number that best fits your location and customer type.
- ❑ Hardware warranty information — Learn about Allied Telesis warranties and register your product online.
- ❑ Replacement Services — Submit a Return Merchandise Authorization (RMA) request via our interactive support center.
- ❑ Documentation — View the most recent installation and user guides, software release notes, white papers, and data sheets for your products.
- ❑ Software Downloads — Download the latest software releases for your managed products.

For sales or corporate information, go to **www.alliedtelesis.com/purchase**.

Chapter 1

Introduction to AlliedView Cloud

This chapter provides an overview of the AlliedView Cloud application. The chapter includes the following sections:

- ❑ “What is AlliedView Cloud?” on page 20
- ❑ “Architecture” on page 21
- ❑ “AT-AP500 Access Point” on page 23
- ❑ “Structure of Your Wireless Network Information” on page 24
- ❑ “Wireless Network and Access Point Parameters” on page 27
- ❑ “Wireless Network Examples” on page 32
- ❑ “Building Your Account” on page 39
- ❑ “Account Windows” on page 41
- ❑ “User Accounts” on page 46
- ❑ “Licenses and Tokens” on page 47
- ❑ “Starting or Ending Management Sessions” on page 48
- ❑ “Firmware Version Number” on page 50

What is AlliedView Cloud?

The AlliedView Cloud is a network cloud application for managing AT-AP500 Access Points. With an AlliedView Cloud account you can manage your wireless networks from any computer with Internet access and an Internet web browser application. It simplifies management of your access points because it lets you organize them into “locations” and manage them as groups, instead of individually. Here are some of the features:

- ❑ Easy to use web browser windows.
- ❑ Get Started utility to simplify the first management session.
- ❑ Simple data structure of locations, wireless networks, buildings, floors, and access points that makes organizing and finding information in your account quick and easy.
- ❑ Windows for displaying status, statistics, alarms, events, and error information on access points, wireless networks, or clients.
- ❑ A range of authentication methods for the wireless access points, including open system, WEP shared key, legacy 802.1x, WPA, and WPA2.
- ❑ Network hotspots for Internet access by wireless clients.
- ❑ Captive portals to add introductory windows to your wireless network hotspots.
- ❑ Radio schedules to limit the times of operations of access points.
- ❑ Usage plans to control the amount of time clients can access wireless networks.
- ❑ Automatic or manual firmware updates of the access points.

Note

This version of the AlliedView Cloud program supports only the AT-AP500 Access Point. Do not use it to manage other types of devices. For the latest information on supported Allied Telesis products, refer to the product's data sheet.

Architecture

Figure 1 shows an example of the AlliedView Cloud architecture of access points and wireless networks.

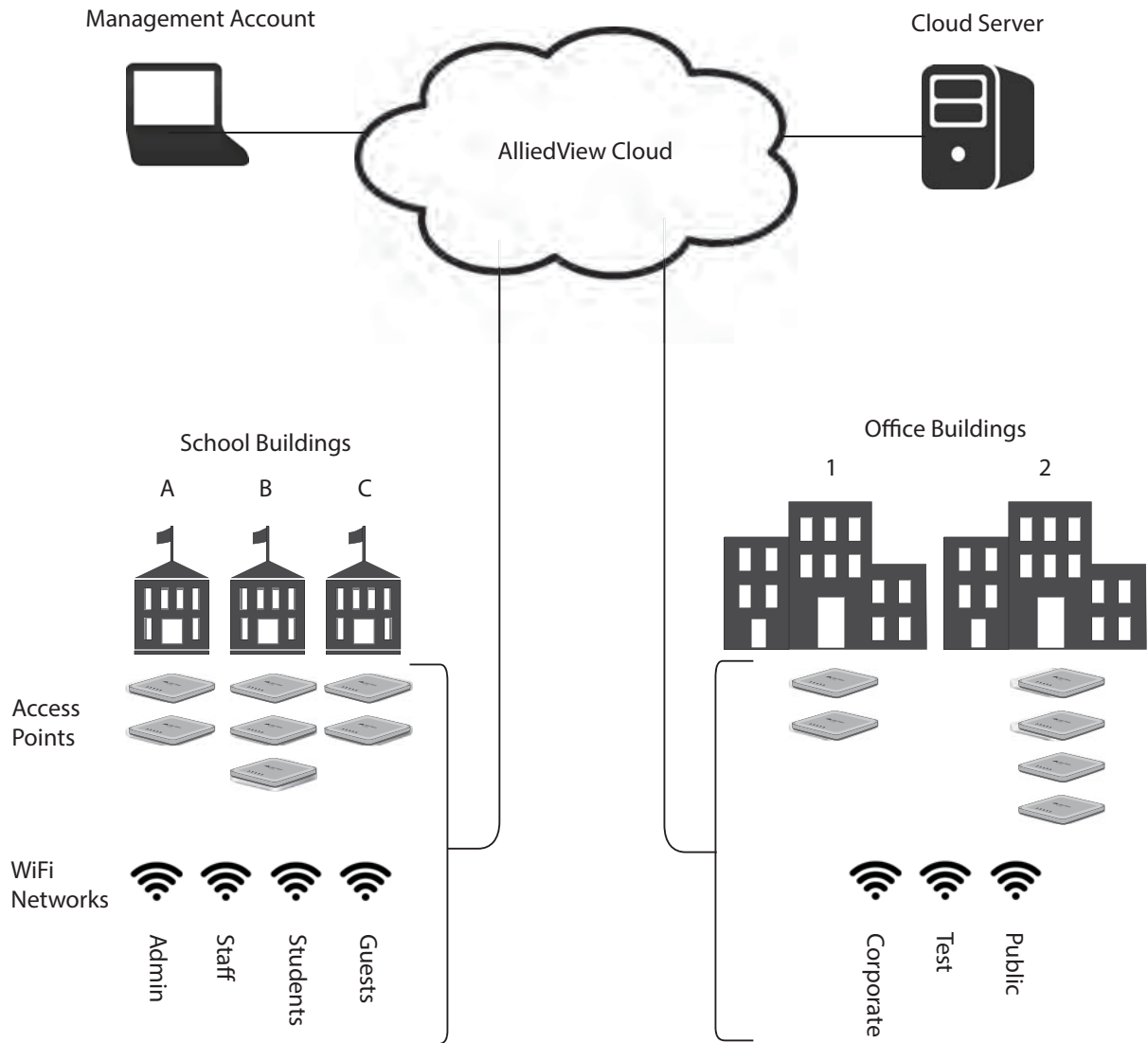


Figure 1. AlliedView Cloud Architecture

In the above example:

- ❑ A school has three buildings. Buildings A and C have two access points each and Building B has three access points. Because the access points are supporting the same four wireless networks (Administration, Staff, Students, and Guests), they are managed as a group in the AlliedView Cloud account.
- ❑ An office location has two buildings. Building 1 has two access

points and Building 2 has four access points. These access points are supporting the three wireless networks, Corporate, Test, and Public, and are managed as another group in the AlliedView Cloud account.

AT-AP500 Access Point

Here are the main features of the AT-AP500 Access Point:

- ☐ Dual concurrent radios: 2.4GHz and 5GHz
- ☐ IEEE 802.11a/b/g/n/ac
- ☐ MIMO with internal omni antennas
- ☐ 2.4GHz maximum capacity of 450Mbps
- ☐ 5GHz maximum capacity of 2,200Mbps
- ☐ One 10/100/1000Base-T Ethernet port with Auto-Negotiation, auto MDI/MDIX, and IEEE 802.3at Power over Ethernet
- ☐ DHCP client
- ☐ Variety of authentication methods, including open system, shared key, legacy 802.1x, WPA and WPA2.
- ☐ RADIUS client and accounting for use with an external RADIUS server.

You have to manage the AT-AP500 Access Point with an AlliedView Cloud account. The device does not support local management.

The AT-AP500 Access Point must have access to the Internet on its LAN port so that it can communicate with the AlliedView Cloud program. The device does not forward wireless network traffic until you add it to your AlliedView Cloud account.

The access point requires a Dynamic Host Control Protocol (DHCP) server to provide it with the following configuration settings:

- ☐ IP address and subnet mask
- ☐ Default gateway address
- ☐ IP address of a Domain Name System (DNS) server (The DNS server must be able to resolve the web address `avcloud.alliedtelesis.com`.)

For further information, refer to the AT-AP500 Access Point Installation Guide.

Structure of Your Wireless Network Information

The information about your access points and wireless networks are stored in folders and entries in your AlliedView Cloud account. There are different types of folders and entries for different types of information. Some of them help you organize the information to make it easier to find the different wireless networks and access points, while others define the actual operating properties of the devices.

The entries and folders are arranged in a defined structure. At the top are “location” entries. They usually represent the physical locations of one or more of your access points. Beneath the locations are your wireless networks and access points. Figure 2 is an example of a location entry with its accompanying folders and entries.

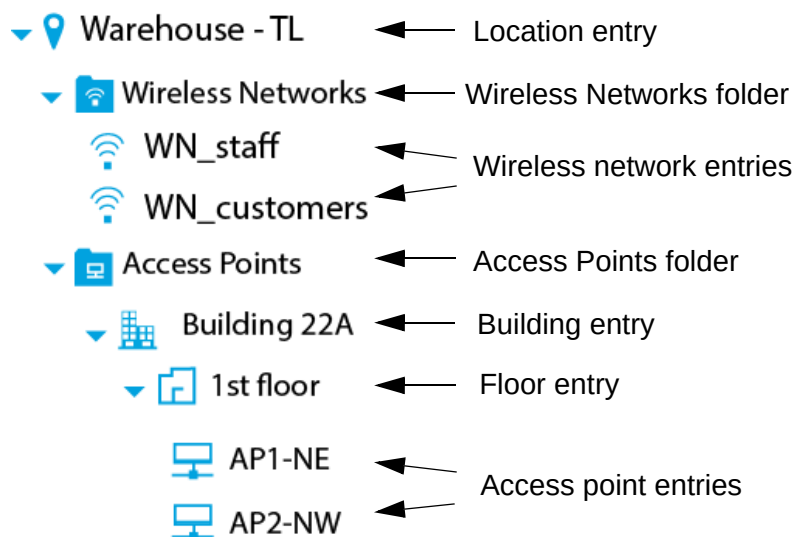


Figure 2. Information Entries and Folders

The entries and folders in the structure are described in the following sections.

Location Entries

At the top of the structure are the location entries of your access points and wireless networks. The location in the example is Warehouse - TL. Locations can consist of part of a building, such as one or two floors, an entire building, or multiple buildings. In some cases, it may be necessary to add more than one location entry to your AlliedView Cloud account for a single physical location, depending on the types and settings of your wireless networks.

Location entry guidelines are listed here:

- ❑ Your account can have any number of location entries.
- ❑ A location entry can have from one to hundreds of access points.

- ❑ A location entry can have up to sixteen wireless networks.
- ❑ Location entries contain some of the operational parameters of your wireless networks and access points, such as radio schedules, radio modes, and load balancing.
- ❑ The access points of a location entry are managed as a group and must have the same wireless networks and operational settings.
- ❑ Access points that need to have different wireless networks or operational settings have to be assigned to different location entries.
- ❑ Location entries can contain wireless networks and access points from different physical locations.

Wireless Network Folder

This folder stores the wireless networks of a location entry. A location entry can have only one Wireless Networks folder, but the folder can have up to sixteen wireless networks. The program automatically adds the folder when you add a location entry to your AlliedView Cloud account.

Wireless Network Entries

These are the individual wireless networks in a location entry. The example location in Figure 2 on page 24 has two wireless network entries, named WN_staff and WN_customers.

Wireless network entries apply to all the access points in a location entry. For example, if a location entry has two access points and four wireless networks, the access points forward traffic of all four networks. If you need access points to support different networks, you must place them in different location entries.

The AT-AP500 Access Point supports a maximum of sixteen wireless networks, eight networks on the 2.4GHz radio and eight on the 5GHz radio. Consequently, the maximum number of networks for a single location entry is sixteen. However, you might want to limit it to eight networks, four for each radio, for best performance.

Access Points Folder

This folder stores your buildings, floors, and access points. Here are the guidelines to this folder:

- ❑ A location entry can have only one Access Points folder.
- ❑ The folder is automatically added when you add a location entry.
- ❑ The folder can contain any number of buildings, floors, or access points.

Building Entries

Location entries have to have at least one building entry. You use building entries to organize your access points to make them easier to find and identify. In some cases, a location and building might be the same thing, in which case the names you give their entries in your account might be very similar. The location entry in the example has only one building, Building 22A.

Here are the building entry guidelines:

- ❑ The Access Points folder can have any number of building entries.
- ❑ Building entries do not have any operational parameters for your wireless networks or access points.

Floor Entries

Buildings have to have at least one floor. As with building entries, you use floor entries to organize your access points. Here are the floor entry guidelines:

- ❑ The Access Points folder can have any number of floor entries.
- ❑ Floor entries do not have any operational parameters for your wireless networks or access points.

Access Point Entries

Beneath the floors in the entries structure are the individual access points. As with the other entries in your account, you can give them names to make them easier to identify. You identify the physical access points by entering their serial numbers into your AlliedView Cloud account. There are several parameters and management functions you can perform on individual access points. However, for the most part, the operating characteristics of the access points are established higher in the information structure, in location and wireless network entries.

Wireless Network and Access Point Parameters

The configuration settings for your wireless networks and access points are set on the entries and folders in your account. The entries and folders have different settings. For example, the IEEE 802.11 wireless mode is set on location entries and applies to all the wireless networks and access points in an entry. In contrast, network authentication is set on the individual wireless network entries and therefore can be different on each network in a location entry. You need to take this into consideration as you plan the assignment of access points and wireless networks to location entries. The basic rule is that access points that are to have the same settings can be assigned to the same location entry, while units with different settings have to be assigned to different location entries.

The following sections describe the wireless network and access point parameters of the entries and folders.

Location Entry Parameters

Table 1 lists the configuration parameters you can set on location entries in your account. The configuration parameters of a location entry apply to all its wireless networks and access points. Access points that need to have different parameter settings have to be assigned to different location entries.

Table 1. Location Entry Parameters

Configuration Parameter	Description
Name and address	Specify a location's name and address, including street, city, state, country, zip code, and time zone.
Radio schedule	Specify the operational times for the radios of the access points in a location entry
Radio status	Turn radios on or off.
RADIUS server profile	Specify a RADIUS server to use for client RADIUS authentication methods.
Load balancing	Specify the maximum number of wireless clients the access points can support on the radios at one time.
Wireless mode	Specify the wireless modes for the 2.4Gz and 5GHz radios. The 2.4GHz radio in the AT-AP500 Access Point has IEEE 802.11b, 11b/g, and 11b/g/n modes. The 5GHz radio has IEEE 802.11a, 11a/n, and 11a/c modes.

Table 1. Location Entry Parameters (Continued)

Configuration Parameter	Description
Channel width	Specifies the channel width of 20 or 40MHz for 2.4GHz radios and 20, 40, or 80MHz for 5GHz radios.
Beacon interval	Specify the time interval, in milliseconds, for transmissions of beacon frames. The access point transmits beacon frames to announce the existence of the wireless network.
DTIM interval	Specify the Delivery Traffic Information Map (DTIM) period. This value specifies how often clients sleeping in low power mode should check the access point for buffered traffic.
WMM QoS and powersave	Enable or disable WiFi Multimedia (WMM) QoS control, which automatically prioritizes data, and WMM powersave, which saves power for battery-operated devices by optimizing data transmission.
AP local password	Specify a password for managing access points without the AlliedView Cloud program. The AT-AP500 Access Point does not support local management, but you still have to assign it a local password.

Wireless Network Entry Parameters

Table 2 lists the configuration parameters you can set on the individual wireless network entries in a location entry. Because these parameters are set on the individual wireless network entries, wireless networks entries in a location entry can have different settings.

Table 2. Wireless Network Entry Parameters

Configuration Parameter	Description
Network Name	Specify a network name, which functions as the SSID for a network.

Table 2. Wireless Network Entry Parameters (Continued)

Configuration Parameter	Description
Network Authentication	Specify the authentication method. The options are listed here: - Open system - Shared key - Legacy 802.1x - WPA with Radius - WPA2 with Radius - WPA/WPA2 with Radius - WPA-PSK - WPA2-PSK - WPA/WPA2-PSK
Data Encryption	Specify data encryption. The available options depend on the authentication method: Here are the options for open system and shared key: - None - 64 bit WEP - 128 bit WEP - 152 bit WEP Legacy 802.1x does not have data encryption. WPA with Radius and WPA-PSK have these data encryption options: - TKIP - TKIP+AES WPA2 with Radius and WPA2-PSK have these data encryption options: - AES - TKIP+AES The only authentication method for WPA/WPA2 with Radius and WPA/WPA2-PSK is TKIP+AES.
Broadcast Network Name (SSID)	Specify whether the access points of a location are to broadcast the SSID. When the access points of a wireless network do not broadcast the SSID, only those wireless clients who know the network name can access it.

Table 2. Wireless Network Entry Parameters (Continued)

Configuration Parameter	Description
Client Security Separation	Specify whether you want the wireless clients of a network to be able to communicate directly with each other through the access points.
VLAN ID	Specify a network's VLAN ID,
Network Radios	Specify whether the access points are to use both 2.4GHz and 5GHz radios or only one radio for a wireless network. For example, if a location has two networks, you might configure it so that the access points use one radio for each network.
Wireless Network Status	Enable or disable wireless networks.
Captive portal	Manage captive portals, which are the introductory windows wireless clients see when accessing hotspots.
Hotspots	Manage hotspots to allow access to the Internet by wireless clients.

Building Entry Parameters

Building entries do not have any operational parameters for access points or wireless networks. Their names are their only parameters.

Floor Entry Parameters

Like building entries, floor entries do not have any operational parameters for access points or wireless networks.

Access Point Entry Parameters

Table 3 lists the parameters for access points. You can set these parameters individually on the access points in a location entry.

Table 3. Access Point Entry Parameters

Configuration Parameter	Description
Syslog	Specify a syslog server to which an access point transmits its log messages.
Radio channel	Specify radio channels for the 2.4GHz and 5GHz radios.
Radio transmission power	Specify a radio transmission power level.
Reboot access point	Reboot an access point.

Table 3. Access Point Entry Parameters (Continued)

Configuration Parameter	Description
Activating the default settings	Return the parameter settings on an access point to the default settings.

Wireless Network Examples

In most cases, the access points in a location entry have to have the same operating parameters and wireless networks. Access points that have to have different operating properties have to be assigned to different location entries in your AlliedView Cloud account. This concept is illustrated in the following examples.

The first example has four access points, AP1 to AP4, and four wireless networks, WN_1 to WN_4. The four access points are to have the same operational settings and support the same four networks. Consequently, you can assign the access points to the same location entry.



Figure 3. Configuration Example 1

As explained in “Location Entry Parameters” on page 27, some of the operational parameters of wireless networks and access points are set in location entries. The parameters include RADIUS server profile, radio modes, WiFi Multimedia QoS control, and radio schedules. (Refer to Table 1 on page 27.) Because access points of a location entry are managed as a group and must have the same settings, access points that need to have different location entry settings have to be assigned to different location entries, as illustrated in the next example.

This example has four access points, AP1 to AP4, and four wireless networks, WN_1 to WN_4. The four access points are to have the same operational settings and support the same wireless networks, with one

difference. AP1 and AP2 are to operate continuously, while AP3 and AP4 only during business hours. Restricting the hours of operations of access points requires a schedule, which, as shown in Table 1 on page 27, is set in location entries. Consequently, two location entries are required. One location entry is for the access points that operate all hours and the other for the units that operate only during business hours.

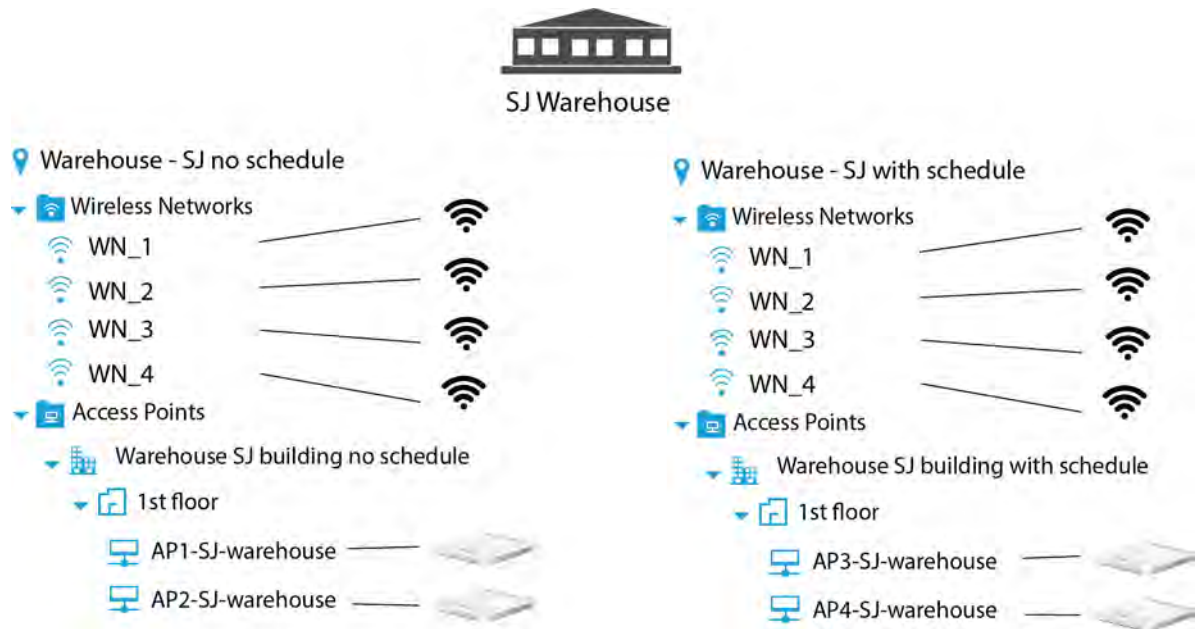


Figure 4. Configuration Example 2

Here is another example of how access points with different location entry parameters have to be assigned to different locations. The example has the same four access points and wireless networks, but AP1 and AP2 are to use load balancing to control the maximum number of permitted wireless clients supported on the radios at one time. AP3 and AP4 are not to use load balancing. Because load balancing is set on location entries, you have to assign the access points to different location entries.

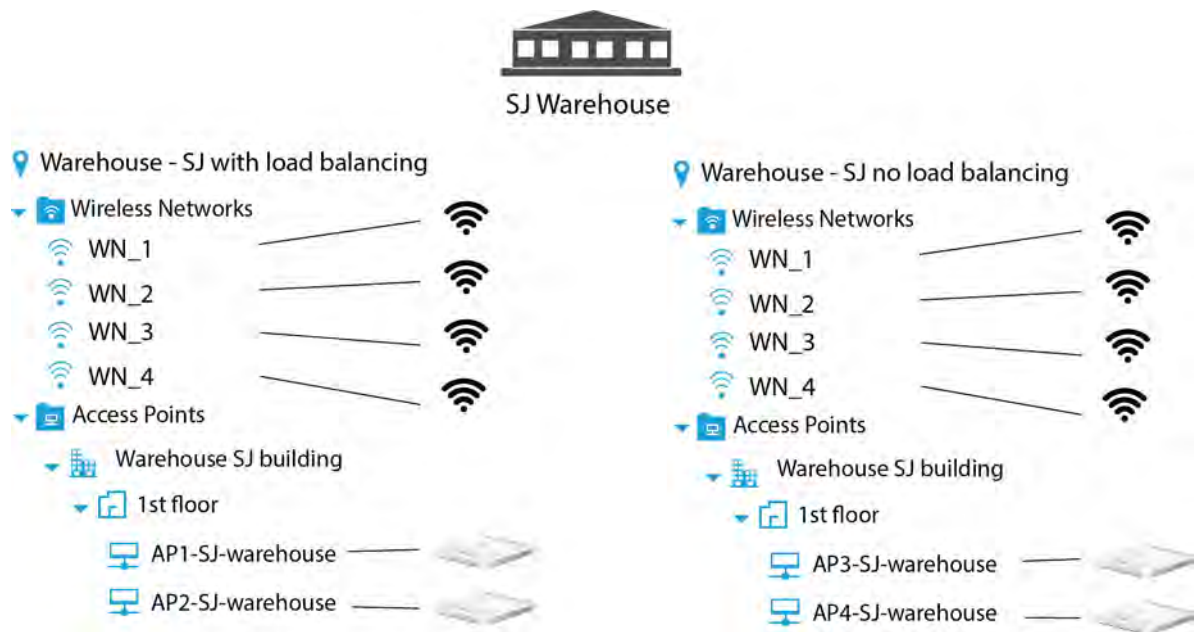


Figure 5. Configuration Example 3

Just as access points of a location entry have to use the same location parameters, they also have to support the same wireless networks. In this example, access points AP1 and AP2 carry four wireless networks, WN_1 to WN_4. Access points AP_3 and AP_4 carry only three of the same networks, WN_1 to WN_3, but not WN4. Because the access points are not supporting the same wireless networks, you have to assign them to different location entries.

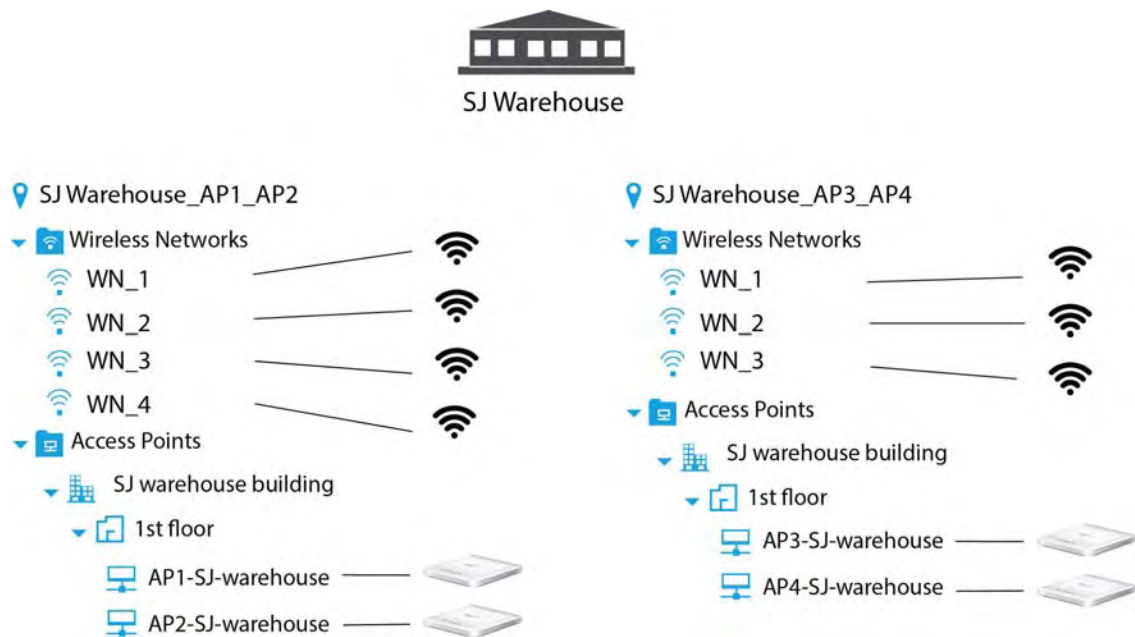


Figure 6. Configuration Example 4

Here is another example. The four access points are supporting four wireless networks. As in the previous example, AP1 and AP2 are supporting networks WN_1 to WN_4, while AP3 and AP4 are supporting WN_1 to WN_3, plus one hotspot network, WN_5. Because the access points are not supporting the same wireless networks they have to be assigned to different location entries.

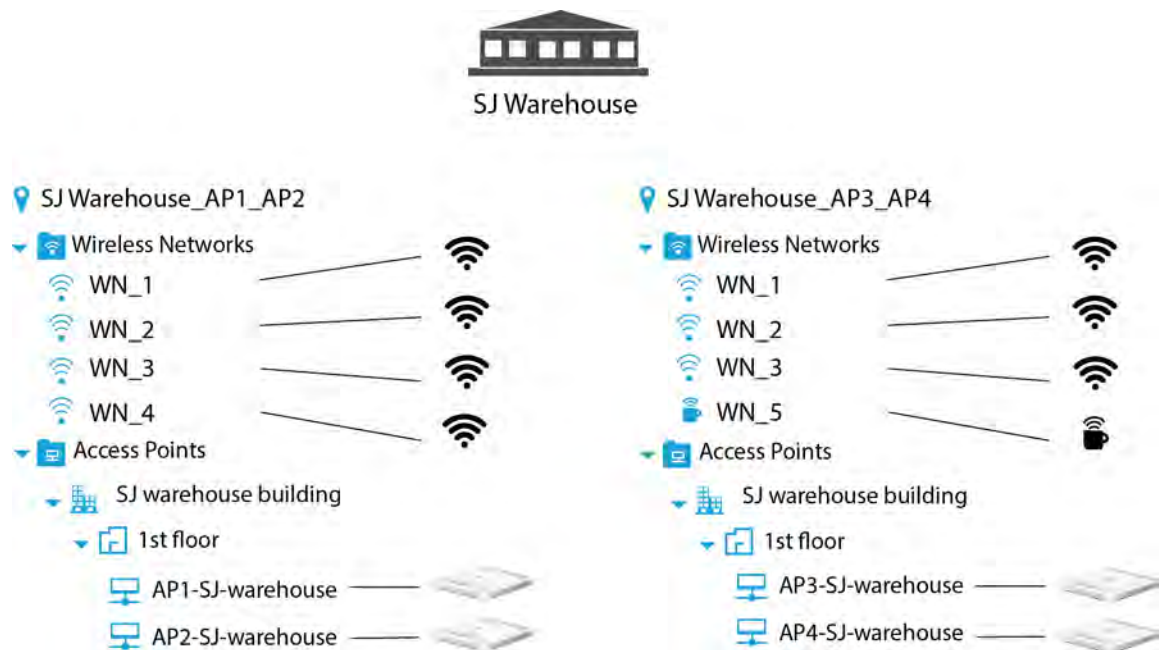


Figure 7. Configuration Example 5

As illustrated in the previous examples, the settings of a location entry and wireless networks apply to all the access points, and that different location entries are needed for devices that need to have different settings or wireless networks. There are, however, a couple parameters you can set on the individual access points themselves. They are listed in Table 3 on page 30 and include syslog server and radio channel. Access points can have different settings for these parameters and still be in the same location entry, so long as all their other settings and wireless networks are the same.

Here is an example. The example shows four access points. The access points have the same settings for their location and wireless network entries. However, access points AP1 and AP2 are to send their syslog messages to syslog_east server and access points AP3 and AP4 are to send their messages to syslog_west server.

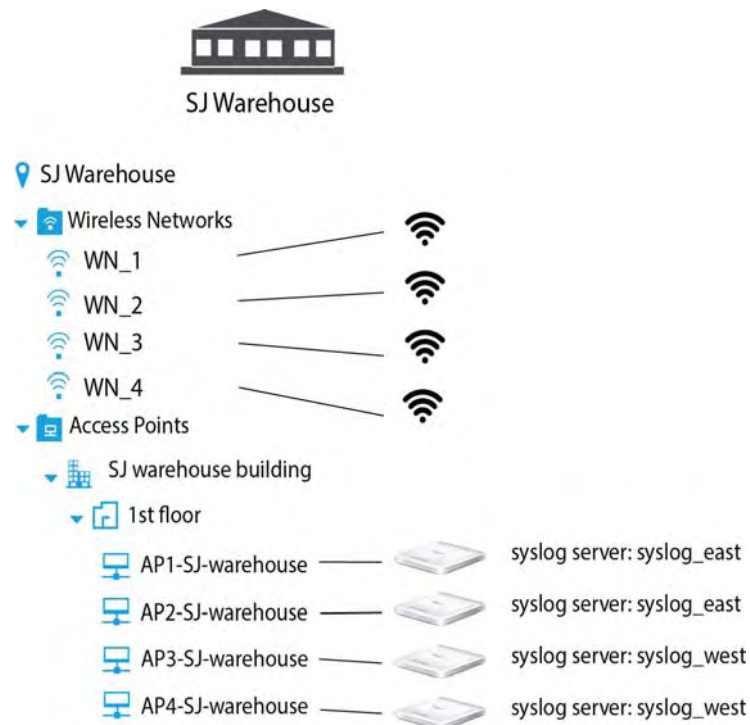


Figure 8. Configuration Example 6

Location entries do not have to correspond to actual physical locations. Consequently, the wireless networks and access points of a location entry do not have to be in the same physical location, as illustrated in this example. There are two locations. Each has two access points. The four wireless networks at each site are exactly the same. In this scenario you have several options. One is to add two locations, one for each site.

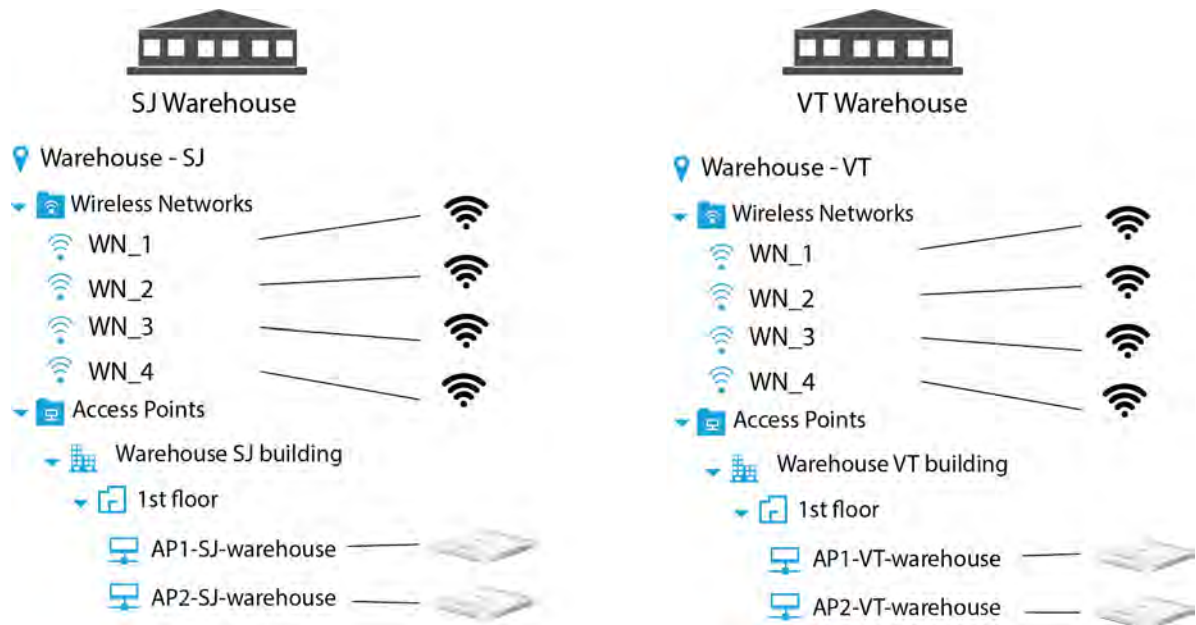


Figure 9. Configuration Example 7

Because the access points are supporting the same four networks, you could add the access points to the same location entry. The illustration in Table 10 on page 38 shows the access points separated by a building entry. The building entry is optional.

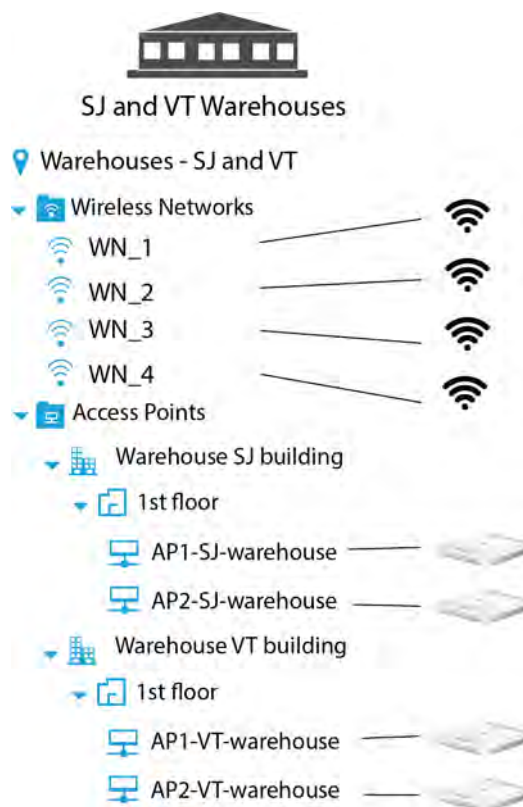


Figure 10. Configuration Example 8

Building Your Account

Before you begin building your AlliedView Cloud account, you have to determine the site requirements for the wireless networks. This usually involves developing a site survey of the offices or buildings. There are many elements to a site survey, but here are some of the main points:

- ❑ Number of access points: You need to determine the number of access points required to provide wireless coverage to the entire site and to handle the number of wireless clients.
- ❑ Number of wireless networks: Determining the number of wireless networks has a variety of variables, including the number of companies or organizations occupying a site and whether networks require different types of authentication.
- ❑ Network operating specifications: You have to decide on the operating specifications of the networks, including 802.11 modes and radio channels.
- ❑ Authentication: You have to determine whether authentication for the wireless clients is required and, if so, which type.
- ❑ Hotspots: You have to decide whether to include hotspots to allow wireless clients access to the Internet through your networks.
- ❑ Usage plans: You can add usage plans to restrict the number of hours wireless clients can access networks.

After you have made the site survey and installed the access points, you are ready to build your AlliedView Cloud account. This involves entering entries for the locations, wireless networks, building, floors, and access points. It is important to remember that, as explained earlier in this chapter, the parameter settings for your access points are set at these three levels:

- ❑ Location entries (refer to Table 1 on page 27.)
- ❑ Wireless network entries (refer to Table 2 on page 28.)
- ❑ Access point entries (refer to Table 3 on page 30.)

Here are the guidelines to assigning access points to location entries:

- ❑ Access points with the same settings in all three levels can be assigned to the same location entry.
- ❑ Access points with different location or wireless network settings have to be assigned to different location entries.
- ❑ Access points with the same location and wireless network settings but different access point entry settings can be assigned to the same location entry or different entries.
- ❑ A location entry can contain access points from different physical

locations.

As you build your account you might wonder whether you should add the location and wireless network entries first before the access points, or the other way around. Actually, you can do it either way, as explained here:

- ❑ If you enter the access points into your account before adding their respective location and wireless network entries, they are stored in the access point inventory with the status of “unassigned,” meaning they are not assigned to any location entries. Their radios are disabled and they do not forward network traffic. After configuring the locations and network entries, you can add them to their appropriate locations from inventory, at which point they begin to forward wireless traffic.
- ❑ If you configure the location and wireless network entries first, the access points immediately begin to forward traffic when you add them to your account and assign them to their respective location entries.

Your account has a Get Started utility that can assist you in building your first location entry, with wireless networks, a building and floor, and access points. The utility is explained in Chapter 2, “Opening a New AlliedView Cloud Account” on page 51. (The utility is only available during the initial management session, after a company or organization opens an AlliedView Cloud account.)

Account Windows

Your AlliedView Cloud account has five main windows.

- ☐ Home
- ☐ Configuration
- ☐ Monitoring
- ☐ Inventory
- ☐ Account

You display the windows by clicking the tabs in the row at the top of the screen. You can view only one window at a time.

Home The Home window displays general status information about the wireless networks and access points.

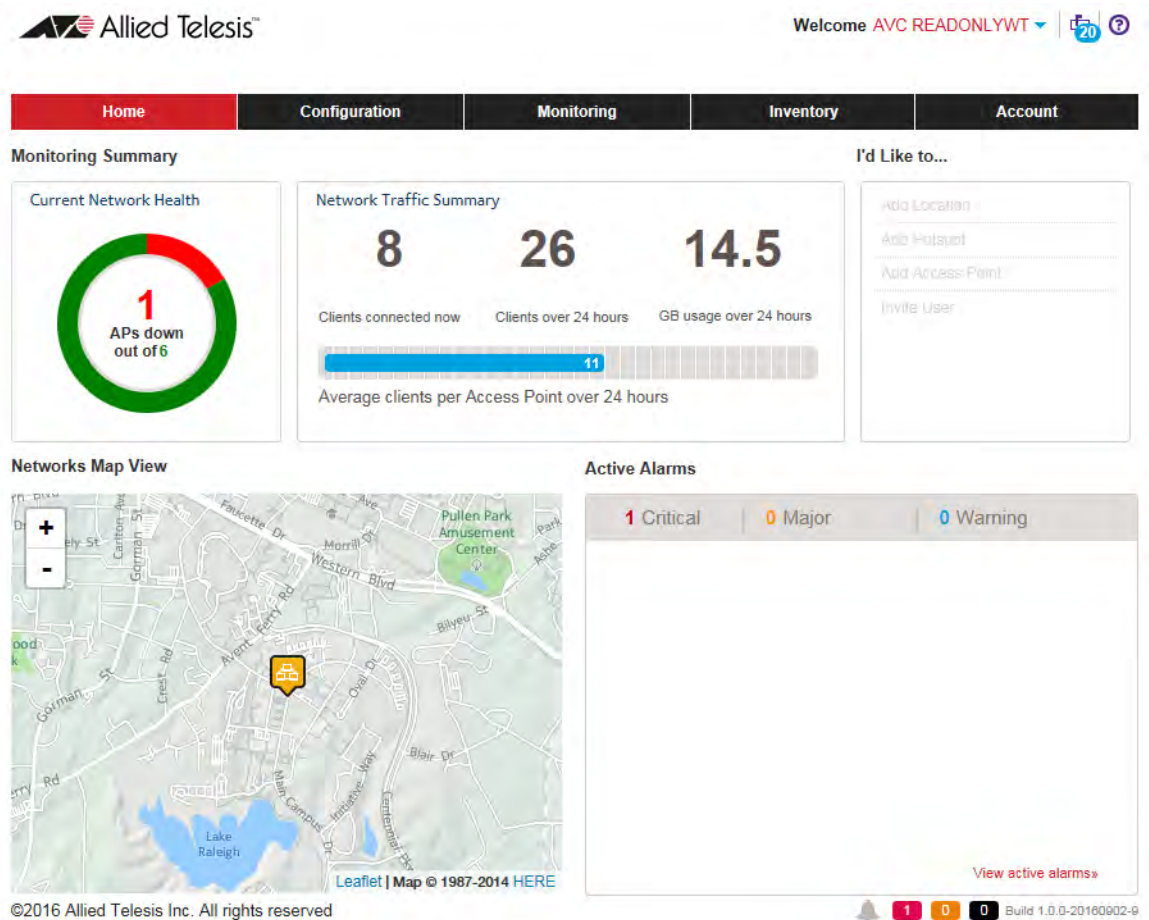


Figure 11. Home Window

Configuration

The Configuration window is where you perform most of your management tasks, such as adding locations, buildings, and floors, as well as configuring wireless networks and access points.

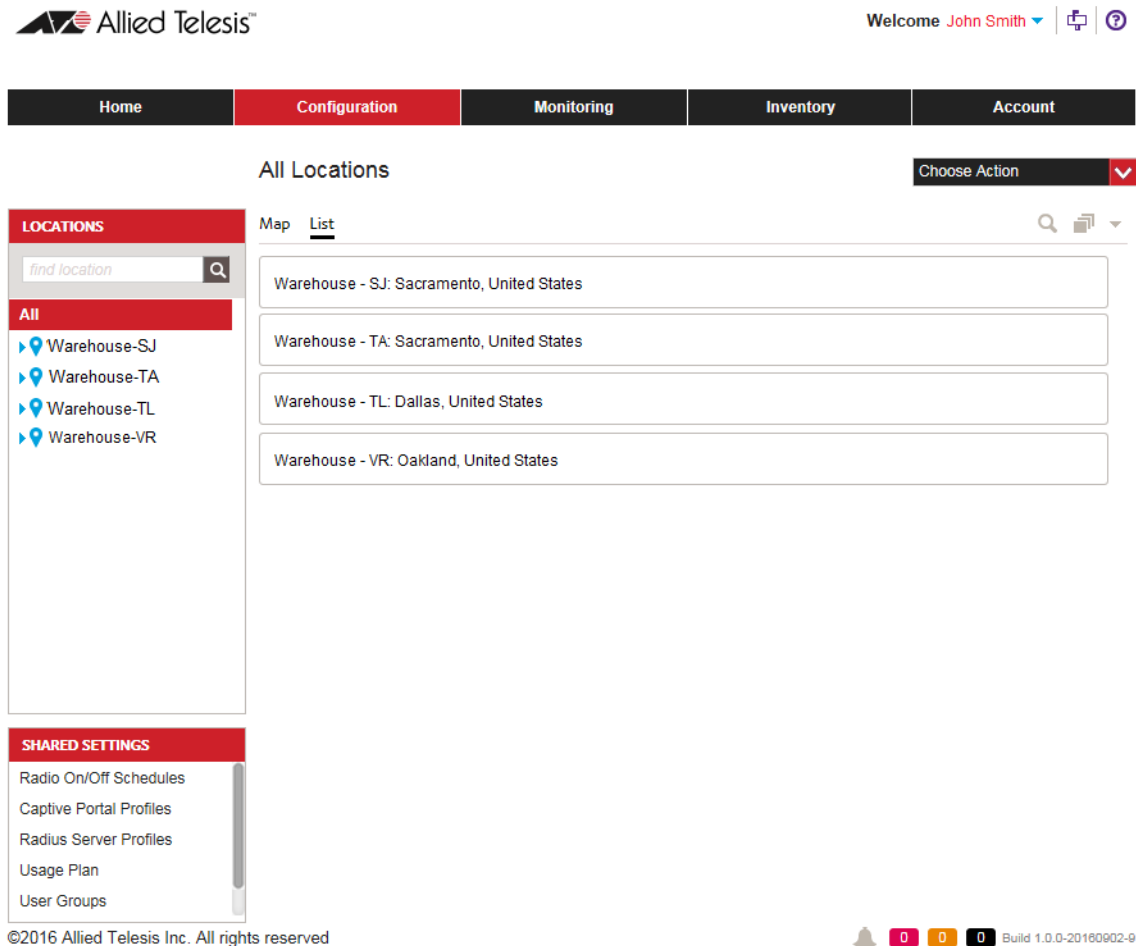


Figure 12. Configuration Window

The parts of the window are described here:

- ❑ The Locations menu on the left side displays the locations, wireless networks, and access points in their hierarchical order. You move through the hierarchy by clicking on the entries. When you select an entry, its configuration settings are displayed in the main section of the window.
- ❑ The Shared Settings menu in the bottom left corner contains selections for configuring features that apply to locations and wireless networks, such as radio schedules and usage plans. The selections in the menu remain the same regardless of the selected entry.
- ❑ The Choose Action menu in the upper right corner of the window contains management functions that change depending on the

selected entry. For instance, the menu displays different selections for a location than a building.

- ❑ The All Locations section typically displays the configuration settings of selected entries. It is in this part of the window that you enter configuration settings.

Monitoring This window displays status information about the wireless networks and access points.

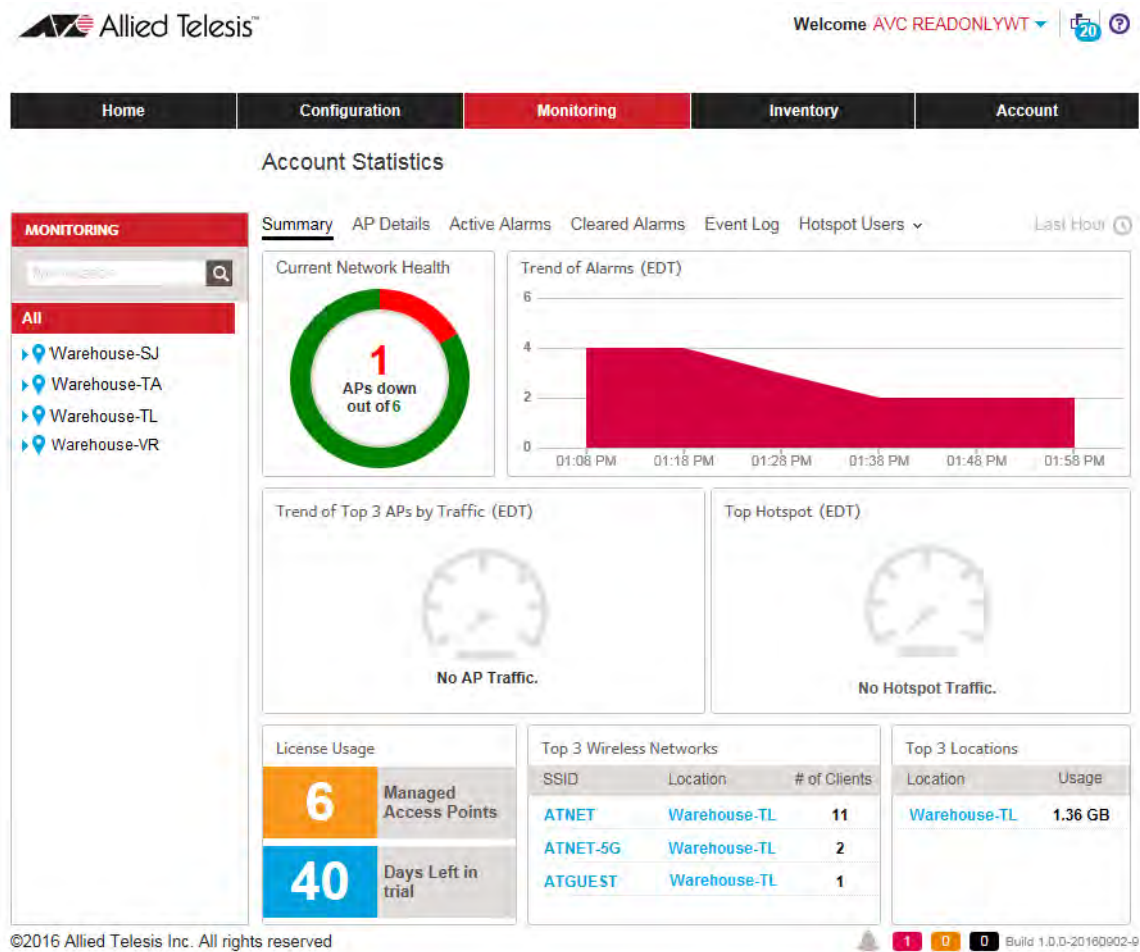


Figure 13. Monitoring Window

Inventory You use this window to add or remove access points from your account. You have to add access points to the inventory before you can manage them with the program.

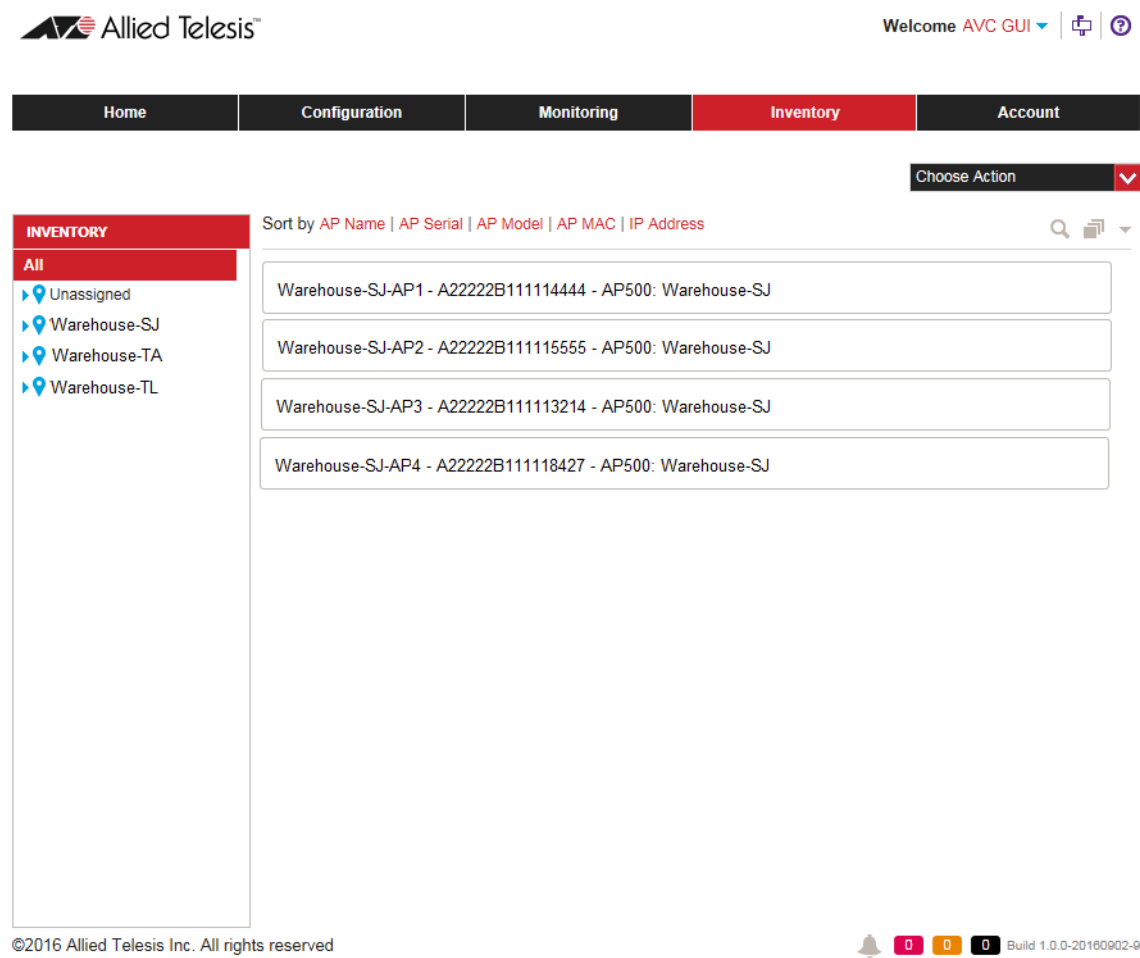


Figure 14. Inventory Window

Account You use this window to configure your account, such as adding managers or access point licenses.

Allied Telesis

Welcome AVC GUI

Home

Configuration

Monitoring

Inventory

Account

My Account

Choose Action

ACCOUNT

Licenses

Users

Account

Settings

Backup/Restore

Company Name

Country

Zip Code

Street Address

City

State

AAA Inc.

United States

95134

11 Highland Rd.

San Jose

California

CANCEL

SAVE

Figure 15. Account Window

User Accounts

There are four types of AlliedView Cloud user accounts. They are listed here:

- ❑ Owner account - The owner account is added when the first person of a company or organization opens an AlliedView Cloud account. A company or organization can have only one owner account and the account cannot be changed or transferred to another account. The person with the owner account can view or manage all entries in the company's AlliedView Cloud account, and invite others to open new AlliedView Cloud user accounts.
- ❑ Admin accounts - Admin accounts, like the owner account, give individuals full access to view or manage all entries in the company's AlliedView Cloud account. Admin accounts also allow users to invite others to open AlliedView Cloud accounts. The difference between owner and admin accounts is that there can be only one owner account while there can be any number of admin accounts.
- ❑ Read-only accounts - Read-only accounts give individuals permission to view the elements but not change any values.
- ❑ Hotspot clerk accounts - Hotspot clerk accounts allow individuals to sell, print, or monitor hotspot vouchers. Only users with hotspot clerk accounts can manage vouchers.

Note

The users described above are not to be confused with wireless or hotspot clients who access your wireless networks.

Licenses and Tokens

To use the AlliedView Cloud program you have to open an account and purchase a license. A license consists of tokens. A token provides management support for one AT-AP500 Access Point for one calendar month. You can add licenses and tokens to your account at any time.

To obtain new licenses and tokens, submit requests through your Allied Telesis 24/7 Support account.

If a license expires and you do not purchase additional licenses, you lose access to the AlliedView Cloud application and your wireless networks as follows:

- ❑ A one-week grace period begins the day after the end of the license period. Your access to the AlliedView Cloud application is limited to the Home window. The access points in the account continue to forward wireless network traffic, with guest access and authentication cloud services, using their last saved configuration settings.
- ❑ After the one-week grace period, the access points are return to the factory default configurations and stop forwarding wireless traffic. However, they are not deleted from the account. The access points begin to forward traffic again if a new license with tokens is added to the account.
- ❑ Thirty days after the end of the grace period, the AlliedView Cloud account is de-activated if no new licenses and tokens are installed.

Starting or Ending Management Sessions

This section contains procedures for starting or ending management sessions with the AlliedView Cloud program. The procedures assume you have obtained an account and run the Get Started utility. For instructions, refer to Chapter 2, "Opening a New AlliedView Cloud Account" on page 51.

Starting a Management Session

To start a management session, do the following:

1. Open your web browser. Supported browsers include Microsoft Internet Explorer, Google Chrome, and Apple Safari.
2. Enter this web address into the URL field of your browser:

avcloud.alliedtelesis.com

The AlliedView Cloud application displays this window.

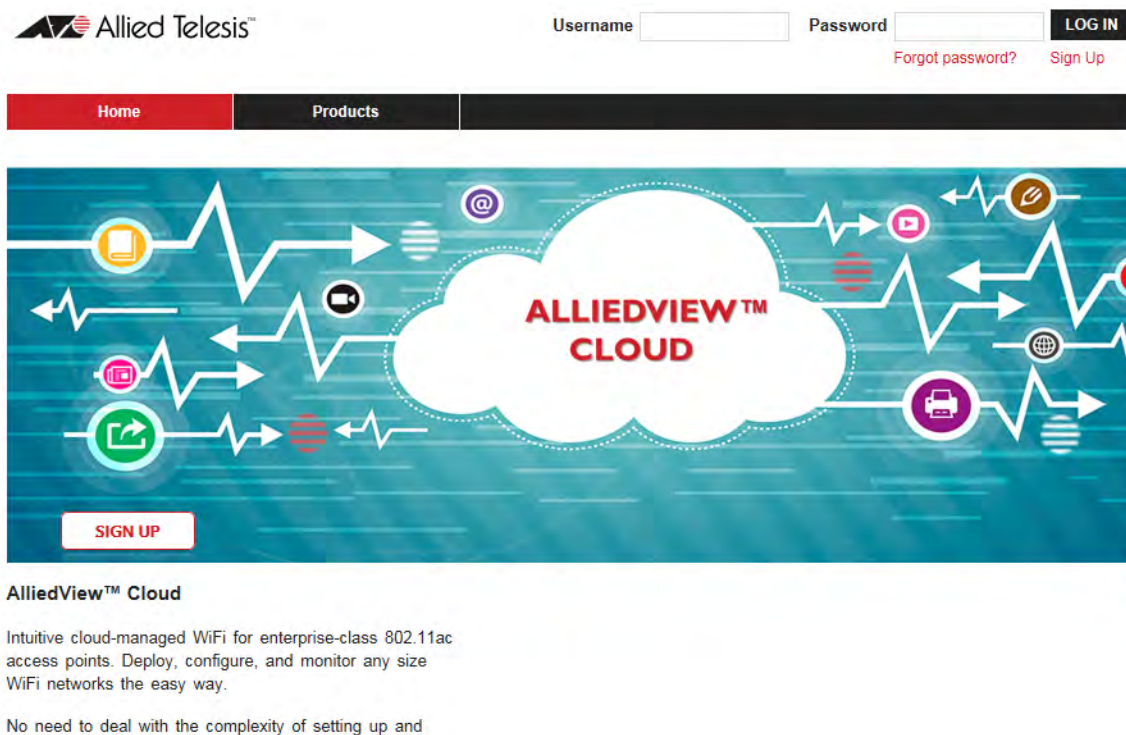


Figure 16. AlliedView Cloud Window

3. Enter your username (email address) and password for your AlliedView Cloud account in the Username and Password fields at the top of the window and click the **LOG IN** button. The username and password are case-sensitive.

You are logged into your AlliedView Cloud account. The program initially displays the Home window. Refer to Figure 11 on page 41.

Ending a Management Session

To end a management session, from any window in the application, hover the cursor over your username in the top right corner and click **Sign Out** from the pop-up menu.

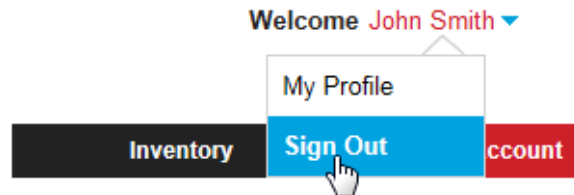


Figure 17. Sign Out Selection

Firmware Version Number

This version of the manual applies to version 1.1 of the AlliedView Cloud program. The version number of the program is displayed in the lower right corners of the application windows. Refer to Figure 18.



Figure 18. Firmware Version Number

Chapter 2

Opening a New AlliedView Cloud Account

This chapter includes the following sections:

- ❑ “Introduction to Opening an AlliedView Cloud Account” on page 52
- ❑ “Opening a 24/7 Support Account” on page 53
- ❑ “Opening an AlliedView Cloud Account” on page 57
- ❑ “Activating Your AlliedView Cloud Account” on page 61
- ❑ “Running the Get Started Utility” on page 63
- ❑ “Where to Go Next” on page 72

Introduction to Opening an AlliedView Cloud Account

There are four steps to opening an AlliedView Cloud account and starting the initial management session:

- ❑ Step 1: Open a 24/7 Support account with Allied Telesis, Inc. You can skip this step if you already have an account. For instructions, refer to “Opening a 24/7 Support Account” on page 53.
- ❑ Step 2: Open a new AlliedView Cloud account using your 24/7 Support account. For instructions, refer to “Opening an AlliedView Cloud Account” on page 57.
- ❑ Step 3: Activate your new AlliedView Cloud account. For instructions, refer to “Activating Your AlliedView Cloud Account” on page 61.
- ❑ Step 4: Run the Get Started utility. For instructions, refer to “Running the Get Started Utility” on page 63.

The steps have to be performed in this order.

Note

The first individual to open an AlliedView Cloud account becomes the owner of all accounts for the company or organization. The owner can invite other individuals to open AlliedView Cloud accounts to assist in managing or monitoring the access points. For a list of supported accounts, refer to “User Accounts” on page 46. There can be only one account owner.

Opening a 24/7 Support Account

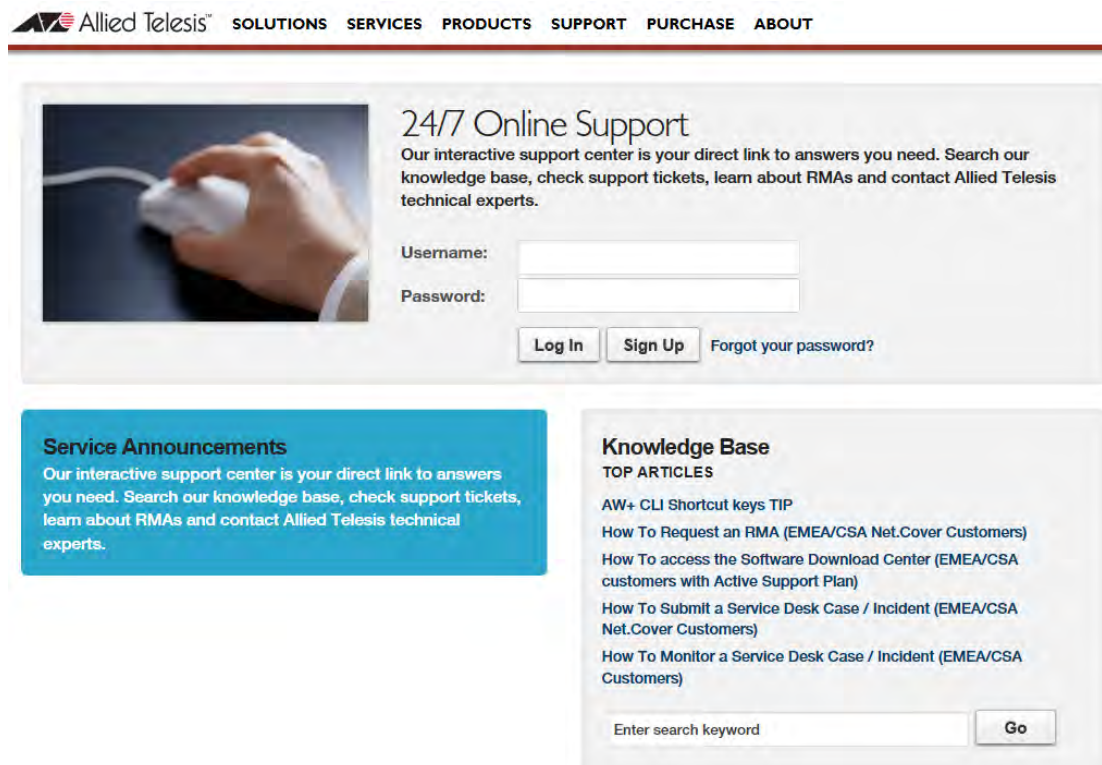
To open an account with AlliedView Cloud, you need to have a 24/7 Support account with Allied Telesis, Inc. If you already have an account, skip this procedure and go to “Opening an AlliedView Cloud Account” on page 57.

To open a 24/7 Support account, do the following:

1. Open your web browser.
2. Enter this web address in the URL field of the browser:

<https://atportal.force.com/Support/CustomerCommunityHome>

Your web browser displays the 24/7 Online Support web page.



24/7 Online Support
Our interactive support center is your direct link to answers you need. Search our knowledge base, check support tickets, learn about RMAs and contact Allied Telesis technical experts.

Username:

Password:

[Forgot your password?](#)

Service Announcements
Our interactive support center is your direct link to answers you need. Search our knowledge base, check support tickets, learn about RMAs and contact Allied Telesis technical experts.

Knowledge Base
TOP ARTICLES

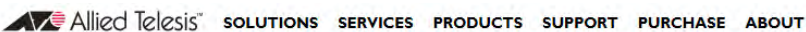
- AW+ CLI Shortcut keys TIP
- How To Request an RMA (EMEA/CSA Net.Cover Customers)
- How To access the Software Download Center (EMEA/CSA customers with Active Support Plan)
- How To Submit a Service Desk Case / Incident (EMEA/CSA Net.Cover Customers)
- How To Monitor a Service Desk Case / Incident (EMEA/CSA Customers)

Enter search keyword

Figure 19. 24/7 Online Support Web Page

3. Click the **Sign Up** button.

The web site displays the Register for an Account web page.





Register for an Account

* All the fields are required.

Users Details	
First Name *	
Last Name *	
Company Name *	
Street *	
City *	
State/Province *	
Zip/Postal Code *	
Country *	-- Select One --
Website *	
Nickname *	
Phone *	+ () -
Email *	
Time Zone *	-- Select One --
Submit Back	

Figure 20. Register for an Account Web Page

4. Fill in the fields for your company and click **Submit**. All fields are required.

Note

The Company Name field becomes the name of your AlliedView Cloud organization account. The owner and all account holders who are invited by the owner to open accounts must enter the same name in the Company Name field when opening 24/7 Support accounts.

Note

The email address you enter in the Email field will be your AlliedView Cloud username.

The program signals the completion of the registration process with this message.

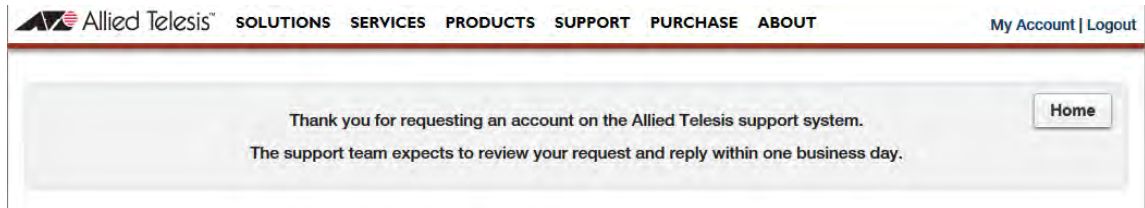


Figure 21. Completion of Registration

Allied Telesis, Inc. sends you an automated email within a few minutes, acknowledging receipt of your registration information.

Another email is sent to you in one business day with a web link. Continue with the next step after you receive the second email.

5. Open the email and click the link.

Your web browser opens and displays this prompt.

 A screenshot of a web browser displaying the 'Change Your Password' prompt. The header shows the Allied Telesis logo. The main heading is 'Change Your Password'. Below this, it says 'Enter a new password for john_smith@aaaindustries.com'. It then lists requirements: 'Your password must have at least: 8 characters, 1 letter, 1 number'. There are two input fields: '* New Password' and '* Confirm New Password'. A 'Change Password' button is at the bottom. At the very bottom, it says 'Password was last changed on 11/2/2016 7:56 AM.'

Figure 22. Change Your Password Prompt

6. Enter a password for your new 24/7 Support account in the New Password field. It must be at least eight characters and have at least one letter and one number. The password is case-sensitive.
7. Reenter the password in the Confirm New Password field.
8. Click **Change Password**.

You are automatically logged into your new 24/7 Support account and this window is displayed:

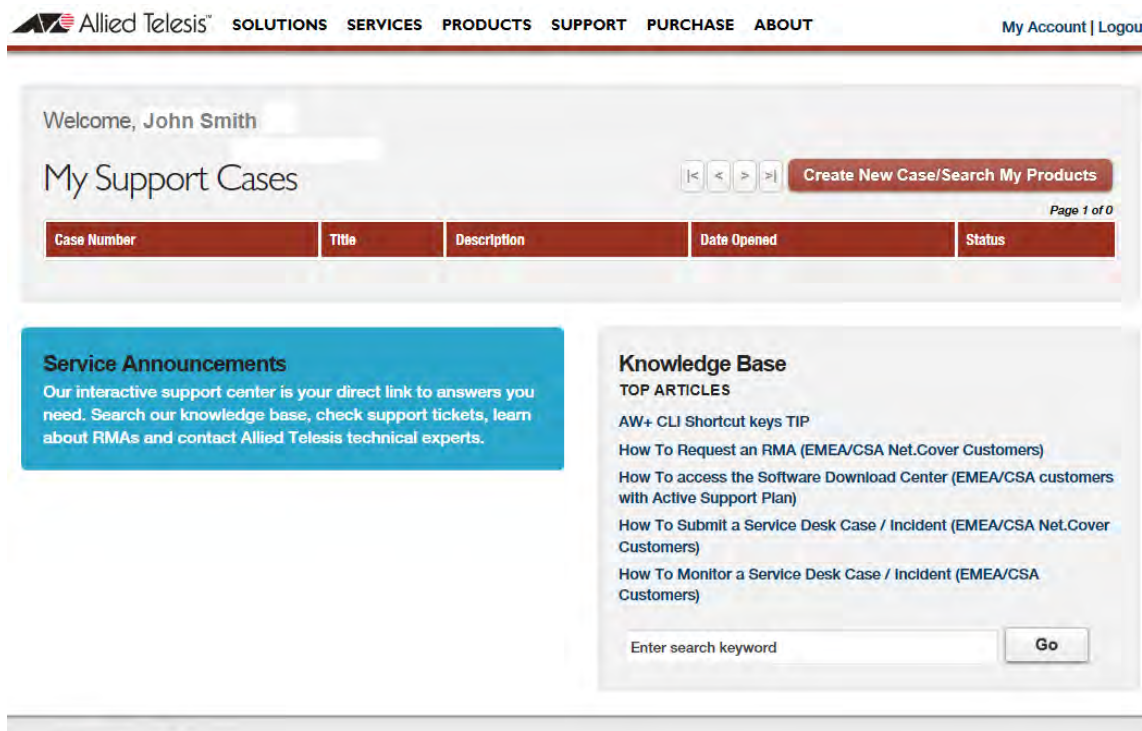


Figure 23. My Support Cases Window

You now have an account with 24/7 Support. Your username is your email address and your password is the password you entered in step 6.

9. Click **Logout** in the upper right corner of the window.

You are now ready to open an account in AlliedView Cloud. For instructions, go to “Opening an AlliedView Cloud Account” on page 57.

Opening an AlliedView Cloud Account

Now that you have a 24/7 Support account, you can open an AlliedView Cloud. To open an account, do the following:

1. Open the web browser on your management workstation.
2. Enter the following address in the URL field of the web browser:

<https://avcloud.alliedtelesis.com>

The following screen is displayed:

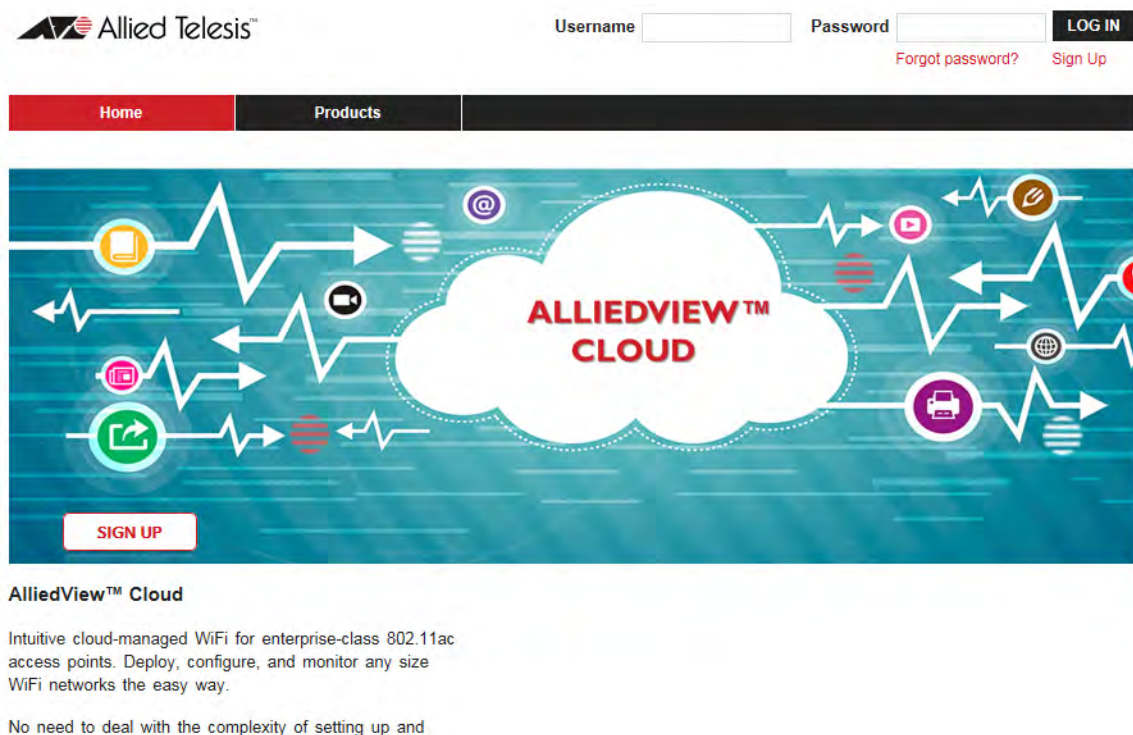
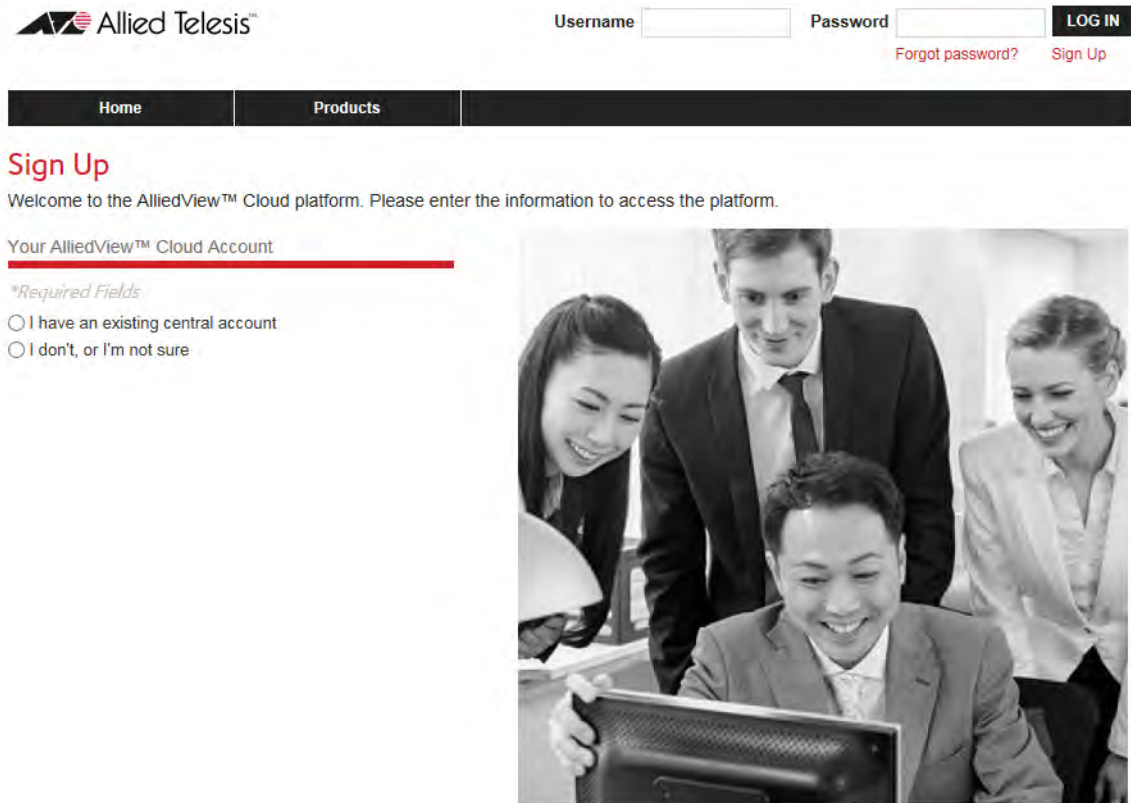


Figure 24. AlliedView Cloud Window

3. Click **Sign Up** in the upper right corner of the window.

The program displays the following window:

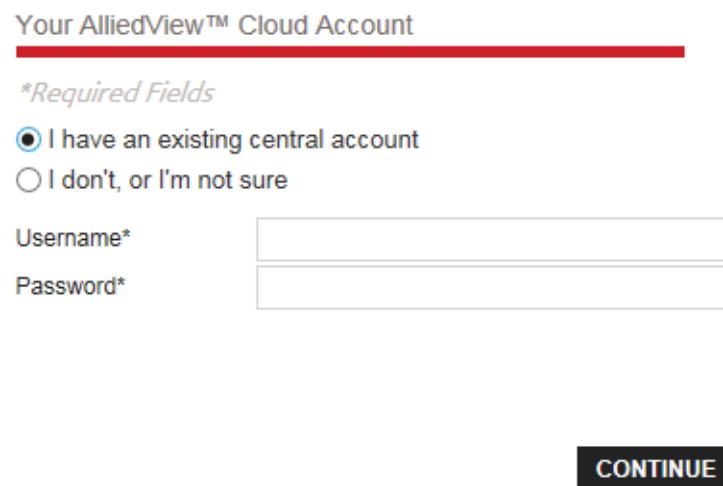


The image shows the Allied Telesis Sign Up window. At the top, there is a navigation bar with the Allied Telesis logo on the left and a login section on the right containing 'Username' and 'Password' input fields, a 'LOG IN' button, and links for 'Forgot password?' and 'Sign Up'. Below the navigation bar is a 'Sign Up' heading in red. Underneath, a welcome message reads: 'Welcome to the AlliedView™ Cloud platform. Please enter the information to access the platform.' The main section is titled 'Your AlliedView™ Cloud Account' and includes a red underline. Below this, there is a section for '*Required Fields' with two radio button options: 'I have an existing central account' and 'I don't, or I'm not sure'. To the right of the text is a black and white photograph of four business professionals (three men and one woman) smiling and looking at a laptop screen.

Figure 25. Sign Up Window

4. Click the dialog circle for **I have an existing central account**.

The window adds Username and Password fields.



This image shows the 'Your AlliedView™ Cloud Account' section of the sign-up window. It features a red underline for the title. Below the title, the text '*Required Fields' is displayed. There are two radio button options: 'I have an existing central account' (which is selected with a blue dot) and 'I don't, or I'm not sure'. Below these options are two input fields: 'Username*' and 'Password*'. At the bottom right of the form is a black button with the word 'CONTINUE' in white capital letters.

Figure 26. Sign Up Window with Username and Password Fields

5. Enter your username (email address) and password for your 24/7 Support account.
6. Click **Continue**.

The program displays the Sign Up window for AlliedView Cloud. Some fields are already filled in with information from your 24/7 Support account.

Figure 27. Sign Up Window for AlliedView Cloud

7. Fill in the empty fields in the window.

You can view the terms and conditions of the program by clicking **Terms and Conditions**.

8. After completing the form, click the **SUBMIT** button.

Upon successful sign-up, the following screen is displayed to confirm successful sign-up and request you to check your email to validate the account.

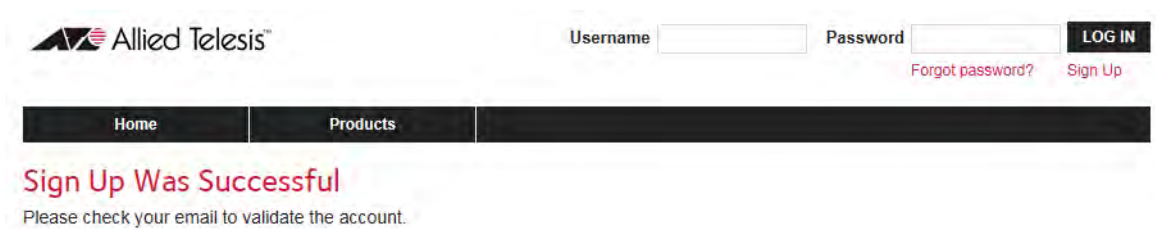


Figure 28. Sign-Up Was Successful Window

9. After receiving the AlliedView Cloud Account Confirmation email, go to “Activating Your AlliedView Cloud Account” on page 61.

Activating Your AlliedView Cloud Account

To activate your new AlliedView Cloud account, do the following.

1. Open the AlliedView Cloud Account Confirmation email you received after signing up for your account.
2. Either click the **here** link in the email or copy and paste the provided HTTPS link into the URL field of your web browser.

The program displays the following window:

The screenshot shows the Allied Telesis login page. At the top, there is a navigation bar with 'Home' and 'Products' links. Below the navigation bar, the main heading is 'New Account Activation' with the subtext 'Please reenter your password to activate your account'. The form contains a 'Username' field with the value 'john_smith@aaaindustries.com' and a 'Password' field. There is a 'Forgot password?' link next to the password field. At the bottom of the form is an 'ACTIVATE' button. In the top right corner, there are links for 'Forgot password?' and 'Sign Up', and a 'LOG IN' button.

Figure 29. New Account Activation Window

3. Enter your account password in the Password field and click the **Activate** button. The password is case-sensitive.

The program displays the following window to indicate that you have successfully opened an AlliedView Cloud account:

The screenshot shows a window titled '90 days left in your free trial'. The text inside reads: 'Your trial to manage the Access Points will expire in 90 days. We encourage you to purchase an AlliedView™ Cloud license to ensure that you can continue to manage your Cloud-based Access Points. If you have any questions, please [contact Allied Telesis Support](#) for additional assistance.' At the bottom of the window, there are two buttons: 'GET STARTED' and 'ADD LICENSE'.

Figure 30. 90 Days Free Trial Window

4. Do one of the following:
 - ❑ To add licenses and tokens to your new account, click the ADD LICENSE button and go to “Adding New Licenses” on page 283.
 - ❑ To run the Get Started utility to begin adding your wireless networks and access points, go to “Running the Get Started Utility” on page 63.

Running the Get Started Utility

This section contains the procedure for running the Get Started utility in your AlliedView Cloud account. The utility allows you to add the following new entries to your account:

- ☐ One location
- ☐ One wireless network
- ☐ Access points

The utility automatically adds one building and one floor, called Building 1 and Floor 1, respectively, and assigns the access points to the floor.

This procedure assumes you are continuing directly from the previous procedure and that the 90 Days Free Trial window in Figure 30 on page 61 is displayed on your screen. If that window is not displayed, perform “Starting a Management Session” on page 48 to log in to your account and then go to step 2 in this procedure.

To run the Get Started utility, do the following:

1. Click the **Get Started** button in the 90 Days Free Trial window.

The utility automatically logs you into your account in the AlliedView Cloud application and displays the License window in the Account tab.

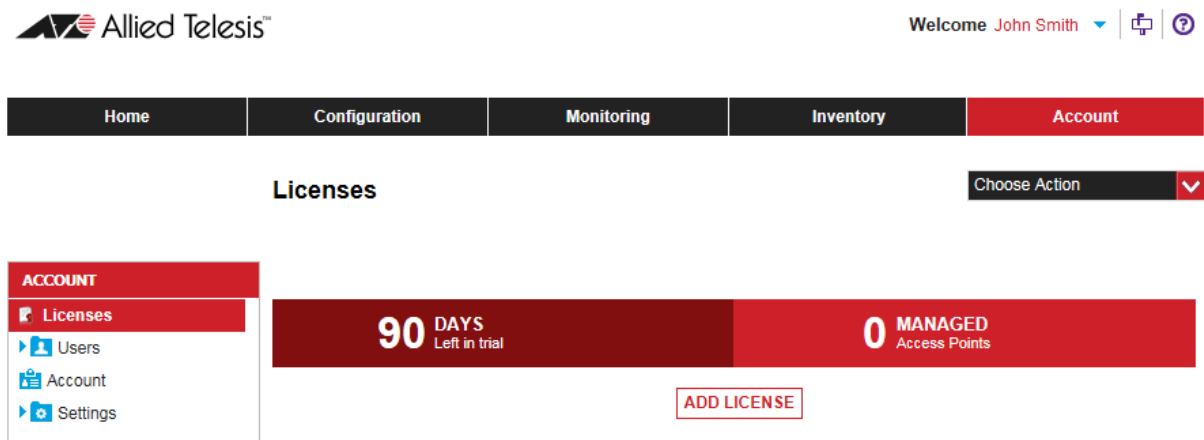


Figure 31. License Window in the Account Tab

2. Click the **Configuration** tab.

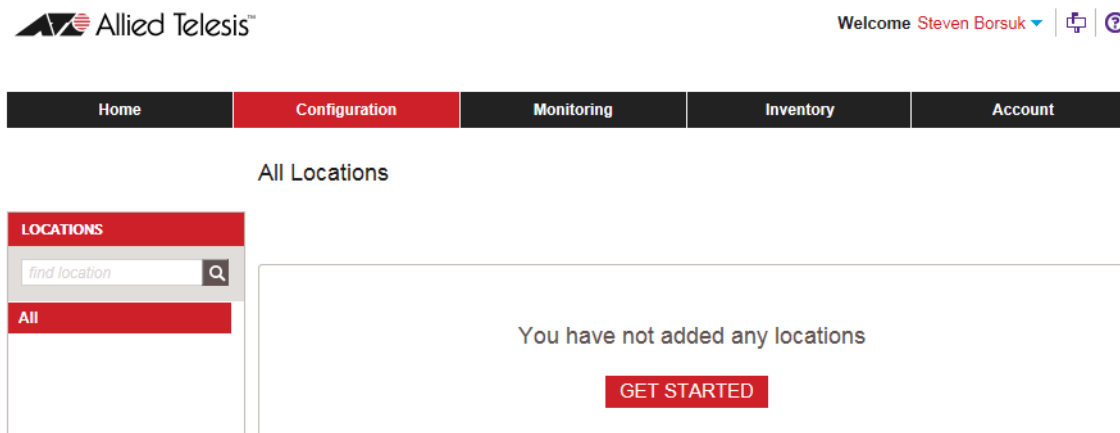


Figure 32. Get Started in the Configuration Window

3. Click the **GET STARTED** button.

The utility displays this introductory window:

Get Started

This Getting Started Wizard will guide you to setup your first wireless network on the Access Point at your location. It takes you through the below listed steps.

- **Add Location**
In this step you will need to enter a name, address and time zone for the location.
- **Add Wireless Network**
In this step you will need to enter a SSID name and select the radio bands to make this network available.
- **Assign Access Points**
In this step you will assign Access Points (APs) to the newly created location.

In case you do not possess the serial number of the Access Point(s), you can always skip the last step and do the AP assignment at a later time from under the Inventory tab by choosing the location for each Access Point. To continue, click Start.

CANCEL **START**

Figure 33. Get Started Introductory Window

4. Click the **START** button.

The utility displays the Add Location window.

Get Started



Add Service Location

Enter details about the location where your Access Points will be deployed for wireless service.

Location Name*
A name for the location

Country*
Value cannot be changed later.

Zip Code

Street Address*

City*

State*

Time Zone*
Value cannot be changed later.

AP Local Password*

CANCEL

NEXT

Figure 34. Add Service Location Window in the Get Started Utility

- Fill in the fields in the Add Service Location window. Parameters marked with an asterisk are required. The fields are defined in Table 4. The wordings of the fields in the window may vary, depending on the selected country.

Table 4. Add Location Window in the Get Started Utility

Field	Description
Location Name	Enter a name for the location. You should make the name as specific as possible so that the location is easy to identify.
Country	Select the country of the location from the pull-down menu. The Country setting is not adjustable on wireless access models sold in the United States. As per FCC regulations, the available wireless channels of wireless products sold in the United States must be fixed to approved channels only. The setting is adjustable on models sold in other countries.

Table 4. Add Location Window in the Get Started Utility (Continued)

Field	Description
Zip Code	Enter the zip code of the location. (Your account automatically determines the City and State from the zip code.)
Street Address	Enter the street address of the location.
City	Enter the city of the location.
State	Enter the state of the location.
Time Zone	Select the time zone of the location from the menu. Use the up and down arrow keys to scroll through the list.
AP Local Password	Enter a management password for the access points of the location. Your AlliedView Cloud account automatically assigns the password to the access points when it detects them. The same password is assigned to all the access points in a location entry. The password can be up to 32 alphanumeric characters. It may not contain spaces or any of these special characters: “, \$, :, <, >, &, *. You use the password as the logon password to the access points if you later decide to manage or troubleshoot them as independent units, without your AlliedView Cloud account. The AT-AP500 Access Point does not support local management, but you must still assign it a password.

Note

The country and time zone cannot be changed after a location is added.

- After filling in the fields in the Add Service Location window, click the **NEXT** button.

The Get Started utility displays the Add Wireless Network window. You use this window to define a wireless network for the access points in the new location.

Get Started



Add Wireless Network

Enter a name for the wireless network that you want to make available at the newly created location.

Network Name*
SSID name

Wireless Network on
Radio bands on which to make this network available

Network Authentication

Data Encryption

Network Key*
Minimum 8 characters, maximum 63 characters.

☒ Show Characters

[BACK](#)
[CANCEL](#)
[NEXT](#)

Figure 35. Add Wireless Network Window in the Get Started Utility

- Fill in the fields in the window. The parameters are defined in Table 5.

Table 5. Add Wireless Network Window in the Get Started Utility

Field	Description
Network Name	Enter a name for the network. The name functions as the SSID for the network. Here are the guidelines: - A network must have a name. - A name can be up to 32 characters. - Spaces are not allowed.

Table 5. Add Wireless Network Window in the Get Started Utility

Field	Description
Wireless Network On	Select the radios for the network from the pull-down menu. The selections are listed here: - 2.4GHz and 5GHz - 2.4GHz - 5GHz For example, if you select 5GHz, the access points of the location will carry the network on their 5GHz radios, but not the 2.4GHz radios. The default settings is 2.4GHz and 5GHz.
Network Authentication	Select the authentication method for the network from the pull-down menu. The options are listed here: - Open System (no authentication) - WPA-PSK - WPA2-PSK - WPA/WPA2-PSK The access points support other authentication methods in addition to the four listed here. However, these are the only ones you can select when you initially add a wireless network. If you want to use one of the other authentication methods, choose one of the four above for now, complete the rest of this procedure, and then perform "Editing Wireless Network Names and Authentications" on page 155 to change the authentication method.

Table 5. Add Wireless Network Window in the Get Started Utility

Field	Description
Data Encryption	Select the data encryption for the network from the pull-down menu. The options are listed here: - AES - TKIP - TKIP+AES The available options depend on the authentication method.
Network Key	Enter a shared secret key of 8 to 63 alphanumeric characters. The key can include special characters.

Note

You can click the Show Characters box to show or hide the network key characters: check the box to show or remove the check mark to hide.

8. After filling in the fields in the Add Wireless Network window, click the **NEXT** button.

The Get Started utility displays the Assign Access Point to Location window. You use this window to add access points to the location.

Get Started

1 Add Service Location — 2 Add Wireless Network — 3 Add Access Point

Assign Access Point To Location

Please populate the table to the right by assigning APs. You can enter AP name/serial number and then click Assign. If you have already added APs to Inventory, you can choose from APs in Inventory to assign.

☒ Assigned Access Points ☐ Skip assignment

Access Points in Inventory

☐	AP Name	Serial Number

or

New Access Point

Name*

A name for the Access Point

Serial Number*

Serial number of Access Point

ASSIGN >>

<< REMOVE

Assigned Access Points

☐	AP Name	Serial Number

BACK
CANCEL
FINISH

Figure 36. Assign Access Point to Location Window in the Get Started Utility

Here are a couple points about this window:

- ☐ The Access Points in Inventory and Assigned Access Points sections are empty because this is the initial management session.
 - ☐ If you do not want to add access points to your account at this time, click the **Skip Assignment** dialog circle and click **FINISH**.
9. To add one or more access points, fill in the New Access Point fields, as follows:
- a. Type a name for the access point in the Name field. Here are the name guidelines:
 - ☐ It can be 2 to 16 characters.
 - ☐ It can contain letters or numbers.
 - ☐ It must have at least one letter.
 - ☐ It must not contain any spaces or special characters.
 - ☐ The only supported special character is the dash (-).
 - ☐ The name cannot end with a dash.

- b. Type the serial number of the access point in the Serial Number field. The serial number can be found on a label on the bottom panel of the access point. The serial number is case sensitive. Letters must be entered in upper or lowercase as they are on the label.

Note

An access point cannot be added without a valid serial number or with the serial number of an access point that has already been added.

- c. Click the **ASSIGN** button. The access point is added to the Assigned Access Points table.
 - d. To add more access points, repeat steps a to c.
10. After entering the access points, click the **FINISH** button.

This completes the Get Started utility. The utility adds the new entries to your account and displays the configuration settings of the new location in the main section of the Configuration window.

11. To confirm the new entries, click on the Wireless Networks and Access Points folders beneath the location's name in the Locations menu in the left column.

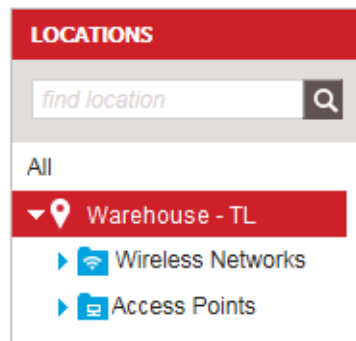


Figure 37. Locations Menu After the Get Started Utility

12. If the access point you added to your account is powered on and connected to the Internet, you can confirm its connection to the AlliedView Cloud program by clicking the **Inventory** tab and examining its identifier in the Inventory window. The identifier, which includes its name, serial number, model name, and location, should display the correct model name. If, instead, the model name is "unknown," the device and the program have not established a connection.
13. For suggestions on what procedures to perform next, refer to "Where to Go Next" on page 72.

Where to Go Next

Here are suggestions on where to go next now that you have completed the Get Started utility.

- ❑ To add more locations, refer to “Adding Locations” on page 78.
- ❑ To add more buildings or floors to locations, refer to “Adding Buildings to Locations” on page 104 or “Adding Floors to Buildings” on page 110.
- ❑ To add more access points to the inventory, refer to Chapter 6, “Access Point Inventory” on page 117.
- ❑ To add more wireless networks, refer to “Adding Wireless Networks” on page 150.
- ❑ To change the authentication method of a new wireless network to no authentication, refer to “Editing Wireless Network Names and Authentications” on page 155.
- ❑ If you want wireless networks of a location to use an authentication method that requires a RADIUS server, you have to add a RADIUS server profile to the location entry before setting the authentication method. For instructions, refer to “Adding RADIUS Server Profiles” on page 231 and “Adding RADIUS Server Profiles to Locations” on page 235. Then change the authentication method of the wireless networks with “Editing Wireless Network Names and Authentications” on page 155.
- ❑ If you want to add a schedule to a location entry to control the hours and days of operations for access point radios, refer to “Adding Radio Schedules” on page 217 and “Adding Radio Schedules to Locations” on page 220.
- ❑ To invite other individuals in your company or organization to open accounts in your AlliedView Cloud organization account, go to “Inviting Users to Add AlliedView Cloud Accounts” on page 295.

Chapter 3

Locations

This chapter includes the following sections:

- ❑ “Introduction to Locations” on page 74
- ❑ “Viewing Locations” on page 75
- ❑ “Adding Locations” on page 78
- ❑ “Copying Locations” on page 82
- ❑ “Editing a Location’s Name or Address” on page 85
- ❑ “Deleting Locations” on page 86

Introduction to Locations

Your AlliedView Cloud account stores wireless access points in groups called “locations” or “location entries.” The access points of a location entry are managed as a group and share the same wireless networks and configuration settings. Beneath location entries are folders for storing the wireless networks and access points. For an example of a location entry and its folders, refer to Figure 2 on page 24. Here are location entry guidelines:

- ❑ Your account can have any number of location entries.
- ❑ A location entry can have from one to hundreds of access points.
- ❑ A location entry can have up to sixteen wireless networks.
- ❑ The access points of a location entry are managed as a group and share the same wireless networks and operational settings.
- ❑ Access points that need to have different wireless networks or operational settings have to be assigned to different location entries.
- ❑ Location entries are managed in the Configuration tab, as shown in Figure 38 on page 75. From the tab you can add or delete location entries as well as configure their parameter settings.
- ❑ Location entries have operational parameters for some of the operating characteristics of your wireless networks and access points. Examples include radio schedules, radio modes, and load balancing. The settings for these parameters apply to all the networks and access points in a location entry. Access points that need to have different settings for their location entry parameters have to be stored in different location entries. For examples, refer to “Wireless Network Examples” on page 32. For information on the parameters, refer to Chapter 4, “Location Parameters” on page 87.
- ❑ Location entries usually represent the physical locations of your access points and wireless networks. For example, they can represent part of a building, an entire building, or multiple buildings.
- ❑ Location entries can contain wireless networks and access points that are located at different physical locations.

Viewing Locations

To view the current locations in your account, click the Configuration tab. The locations are listed in alphabetical order in the main body of the screen as well as in the Locations menu in the left column. The example in Figure 38 has four locations.

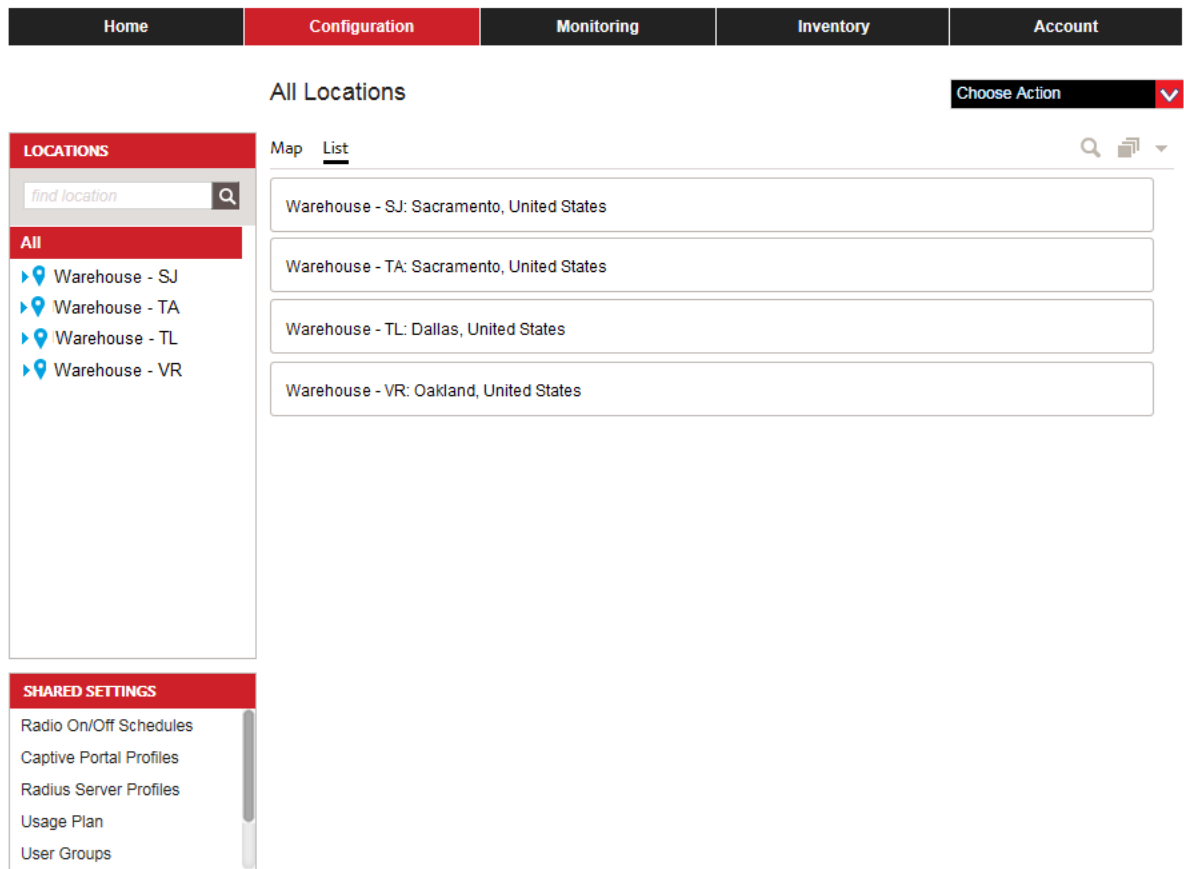


Figure 38. Configuration Tab

If there are many locations and you have trouble finding a specific one, there are two ways you can search for it. One way is with the search tool near the upper right corner of the screen, just below the Choose Action menu. Type in the name of the location you are looking for and press Return. Another way to search for locations is with the Locations menu in the left column. It also has a search feature.

To view the configuration settings of a location, click its name in either the main body of the window or in the Locations menu. The configuration settings are displayed in the main body of the screen. An example is shown in Figure 39 on page 76. By default, the Location Profile section is expanded. To expand other sections, click their arrows.

Map

Details

▼ Location Profile

Location Name

Warehouse - TL

Country

United States

Zip Code

95054

Street Address

22 Walker Dr.

City

San Jose

State*

California

Time Zone

USA-Pacific

▶ Wireless Radio

▶ Load Balancing

▶ Building Access Controls

▶ AP Local Management

▶ Radius Server

▶ QoS

Figure 39. Location Configuration Settings

The sections in the screen are explained in the procedures listed in Table 6.

Table 6. Sections in the Location Configuration Window

Section	Procedure
Location Profile	“Editing a Location’s Name or Address” on page 85
Wireless Radio	“Configuring Basic Radio Settings” on page 91, “Turning Access Point Radios On or Off” on page 89, and “Adding Radio Schedules to Locations” on page 220
Load Balancing	“Configuring the Maximum Number of Wireless Clients” on page 94
AP Local Management	“Setting the Local Password for Access Points” on page 96

Table 6. Sections in the Location Configuration Window (Continued)

Section	Procedure
Radius Server	"Adding RADIUS Server Profiles to Locations" on page 235
QoS	"Configuring WMM QoS" on page 98

By default, the locations are listed by their names. You can also view them in a map by clicking the Map option directly beneath the "All Locations" label. Here is an example.

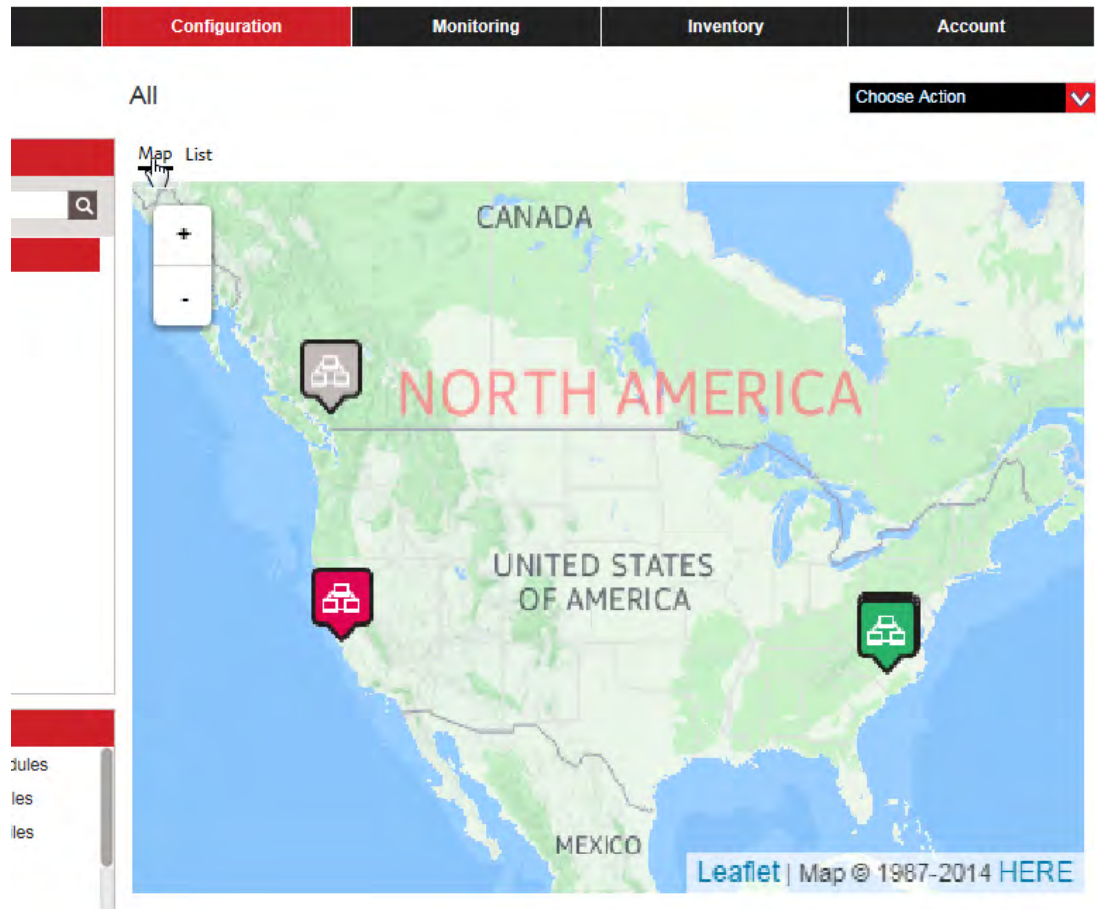


Figure 40. Configuration Map

Adding Locations

This section contains the procedure for adding new locations. A new location requires the following information:

- ❑ Location name
- ❑ Address
- ❑ Country
- ❑ Time zone
- ❑ Password for local management

You can add only one location at a time. To add a new location, do the following:

1. Click the **Configuration** tab:
2. Select **Add Location** from the Choose Action menu.

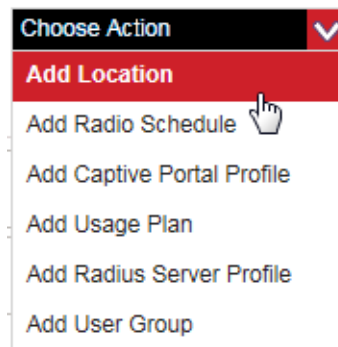


Figure 41. Add Location Selection in the Choose Action Menu

The program displays the Add Location window.

Add Location

Location Name*	
Country*	United States  Value cannot be changed later.
Zip Code	
Street Address*	
City*	
State*	
Time Zone*	Type for auto-suggest Value cannot be changed later.
AP Local Password*	

Figure 42. Add Location Window

- Fill in the fields. Parameters marked with an asterisk are required. The fields are defined in Table 7.

Table 7. Add Location Window

Field	Description
Location Name	Enter a name for the location. You should make the name as specific as possible so that the location is easy to identify.
Country	Select the country of the location from the pull-down menu. The Country setting is not adjustable on wireless access models sold in the United States. As per FCC regulations, the available wireless channels of wireless products sold in the United States must be fixed to approved channels only. The setting is adjustable on models sold in other countries.
Zip Code	Enter the zip code of the location.

Table 7. Add Location Window

Field	Description
Street Address	Enter the street address of the location.
City	Enter the city of the location.
State	Enter the state of the location.
Time Zone	Select the time zone of the location from the menu. Use the up and down arrow keys to scroll through the list. Here are the guidelines to setting the time zone: - You can select only one time zone. - You must select the country before setting the time zone. - The available time zones are determined by the country setting.
AP Local Password	Enter a management password for the access points of the location. The program automatically assigns this password to the access points when it detects them. The same password is assigned to all the access points of a location. The password can be up to 32 alphanumeric characters, It may not contain spaces or any of these special characters: ", \$, :, <, >, &, *. You use this password as the logon password to the access points if you later decide not to use AlliedView Cloud program to manage them, and instead manage them as independent units. The AT-AP500 Access Point does not support local management, but you must still assign it a password.

Note

You cannot change the country or time zone after adding a location.

- After filling in the fields, click **ADD THIS LOCATION**.

The program displays a confirmation window. An example is shown here.

Add Location

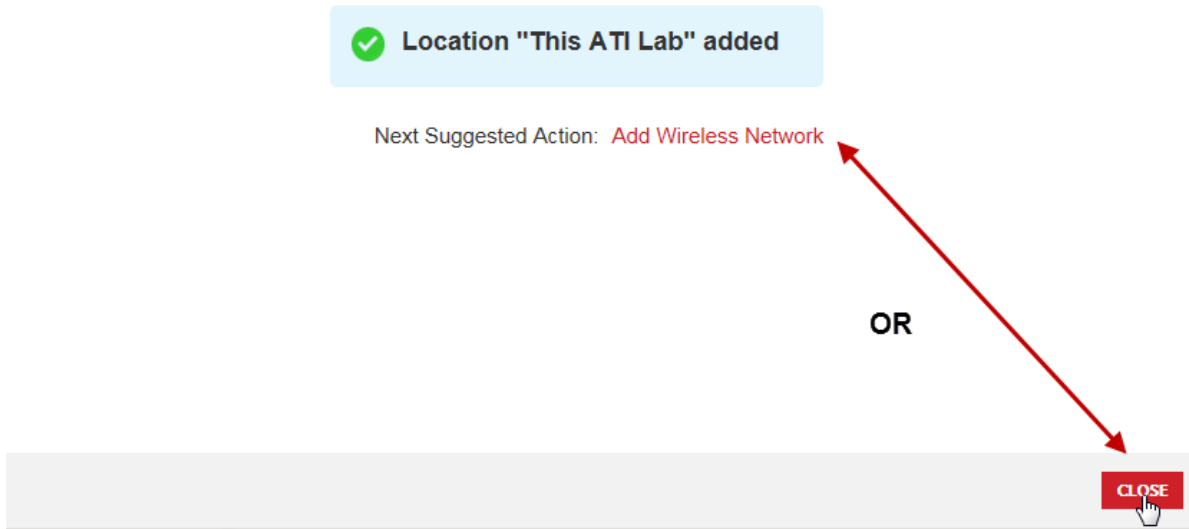


Figure 43. Add Location Confirmation Window

5. Do one of the following:
 - ☐ To add a wireless network to the new location, click **Add Wireless Network**. Go to step 4 in “Adding Wireless Networks” on page 150 for instructions.
 - ☐ To add more locations or perform a different procedure, click **CLOSE**. To add another location, repeat this procedure starting with step 2.

Copying Locations

If two or more locations are to have similar configurations, rather than configuring the locations separately, you can save time and effort by configuring one location and then copying its configuration to the other locations.

Note

Copying the configuration settings to a location overwrites that location's configuration.

To copy an existing location's parameters to other locations, do the following.

1. Click the **Configuration** tab.
2. In the Locations menu in the left margin, click the name of the location whose configuration you want to copy. This is the source location. You can select only one location to be the source location. In the example shown here, the Warehouse - TL location is selected as the location to be copied.

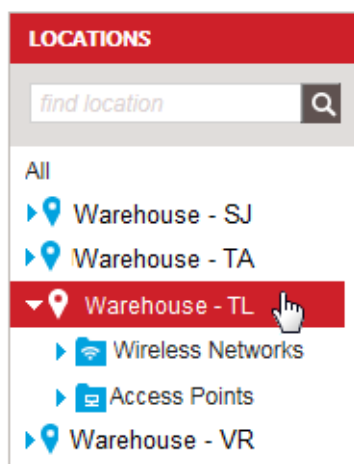


Figure 44. Selecting a Location

The configuration details for the selected location are displayed in the main body of the Configuration tab.

3. Select **Copy Config** from the Choose Action menu:

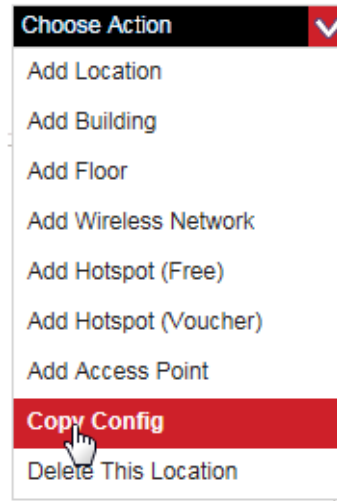


Figure 45. Copy Config Selection in the Choose Action Menu

The program displays the Copy Config window:

Copy Config

WARNING: Configuration for destination location(s) will be REPLACED by the configuration from the source location.

☐ Wireless Radio ☐ Load Balancing ☐ Radio on/off ☐ Auto RF ☐ Building Controls
☐ AP Management ☐ Radius Server ☐ MAC ACL ☐ QoS ☐ Wireless Network

Name

Destination:

☐	Location Name	Address
☐	Building 22A	11 Hillside Rd. Bldg 22A, San Jose, California, United States
☐	Building 22B	11 Hillside Rd. Bldg 22B, San Jose, California, United States
☐	Building 22D	11 Hillside Rd. Bldg 22D, San Jose, California, United States

CANCEL

COPY CONFIG

Figure 46. Copy Config Window

The top area includes the parameter categories you can copy from the source location to the destination locations. The Destination section lists all of the locations, except for the source location.

4. In the top area, click the dialog boxes of the parameters you want to copy from the source location to the destination locations. A parameter is selected when its dialog box has a check mark. The default is no parameters selected.
5. In the Destination area, click the dialog box of the destination location. This is the location to which you want to copy the parameters from the source location. You can select more than one destination location. To copy the parameters to all the locations, click the dialog box next to Location Name in the top row.

If you have trouble finding the correct locations, you can search for them using the Name and search fields in the upper right side of the Copy Config window. Use the Name pull-down field to search by location name or address, and then enter appropriate text string in the search field.

6. Click **COPY CONFIG**.

The program copies the select parameters from the source location to the selected destination locations.

Editing a Location's Name or Address

This section explains how to edit a location's name or address.

Note

You cannot change the country or time zone of a location.

To edit a location's name or address, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left margin or the locations list in the main part of the screen, click the name of the location you want to edit. You can edit only one location at a time.

The program displays the details of the location, with the Location Profile section expanded. An example is shown in Figure 39 on page 76.

3. In the Location Profile area, edit the location name and/or address. The fields are defined in Table 7 on page 79.
4. Click **APPLY** to save your changes or **NO** to cancel the action.

Deleting Locations

This section contains instructions on how to delete locations from your account.

Note

Access points of deleted locations are retained in inventory, with a status of unassigned. Their parameter settings are returned to their default values and their radios are disabled. They stop forwarding network traffic until they are assigned to another location.

To delete a location, do the following.

1. Click the **Configuration** tab.
2. In the Locations menu in the left margin or the locations list in the main part of the screen, click the name of the location you want to delete. You can delete only one location at a time.

The program displays the configuration of the location, with the Location Profile section expanded. An example is shown in Figure 39 on page 76.

3. Select **Delete This Location** from the Choose Action menu:

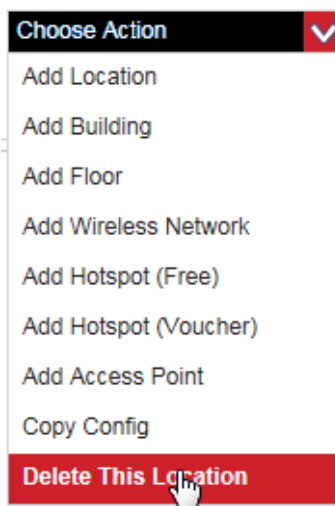


Figure 47. Delete This Location Selection in the Choose Action Menu

The program displays a confirmation prompt.

4. Click **YES** to delete the location or **NO** to cancel the action.
5. Repeat this procedure starting with step 2 to delete more locations.

Chapter 4

Location Parameters

This chapter contains the following sections:

- ❑ “Introduction to Location Parameters” on page 88
- ❑ “Turning Access Point Radios On or Off” on page 89
- ❑ “Configuring Basic Radio Settings” on page 91
- ❑ “Configuring the Maximum Number of Wireless Clients” on page 94
- ❑ “Setting the Local Password for Access Points” on page 96
- ❑ “Configuring WMM QoS” on page 98

Introduction to Location Parameters

This chapter contains procedures on how to set access point parameters in location entries. Because these parameters are controlled from location entries, they apply to all the wireless networks and access points in location entries. If you want wireless networks or access points to have different settings, you must place them in different location entries. The sections in this chapter are briefly described here:

- ❑ “Turning Access Point Radios On or Off” on page 89 - You can use the instructions in this section to turn the radios of the access points at a location on or off. You might turn off the radios if there is a network security risk or to perform network maintenance.
- ❑ “Configuring Basic Radio Settings” on page 91 - This section explains how to configure the wireless mode, channel width, beacon interval, and Delivery Traffic Indication Message (DTIM) interval of the access points.
- ❑ “Configuring the Maximum Number of Wireless Clients” on page 94 - This section contains instructions on how to set the maximum number of wireless clients the access points can support on the radios at one time. This is also referred to as load balancing. You might want to limit the number of clients to prevent network congestion by balancing the clients on both radios.
- ❑ “Setting the Local Password for Access Points” on page 96 - This section explains how to set the local password for access points in a location. You use the password to manage access points locally, without the AlliedView Cloud program. The same password is applied to all the access points in a location. Manually setting the local password is not required. If you do not assign a password, the program automatically generates a password itself.
- ❑ “Configuring WMM QoS” on page 98 - The instructions in this section are used to configure WiFi Multimedia (WMM) QoS control, which automatically prioritizes data with four queues: voice, video, best effort, and background. There are also instructions for WMM Powersave, which saves power for battery-operated devices to optimize data transmission.

Turning Access Point Radios On or Off

This section contains the procedure for turning on or off the 2.4GHz or 5GHz radios in the access points of a location. Here are the guidelines to this procedure:

- ❑ This procedure is performed at the location level and applies to all the access points in a location.
- ❑ You can separately turn the 2.4GHZ and 5GHz radios on or off.

To turn on or off the radios in the access points at a location, perform the following procedure:

1. Click the **Configuration** tab.
2. In the Locations menu in the left margin, click the name of the location with the access points whose radios you want to turn on or off. You can select only one location. This example selects the Warehouse - TL location.

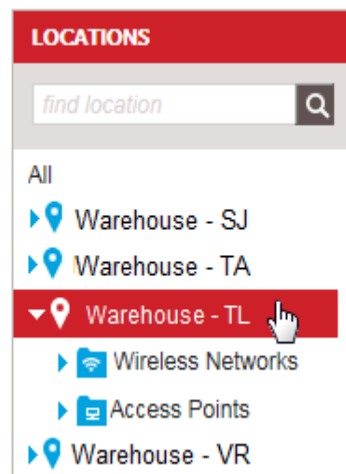


Figure 48. Selecting a Location in the Locations Menu

The program displays the location configuration screen. For an example, refer to Figure 39 on page 76.

3. In the location configuration screen, click the **Wireless Radio** option to expand it.

The Wireless Radio configuration area is displayed:

Wireless Radio

Radio On/Off Setting ?

2.4GHz Radio Always ON ▼

5GHz Radio Always ON ▼

Radio Resource Management

2.4GHz Radio ☐ On ☒ Off

5GHz Radio ☐ On ☒ Off

2.4GHz configuration

Wireless Mode ☐ 11b ☐ 11bg ☒ 11bgn

Channel Width 20MHz ▼

Show Advanced Features

5GHz configuration

Wireless Mode ☐ 11a ☐ 11an ☒ 11ac

Channel Width 40MHz ▼

Figure 49. Expanding Wireless Radio Area

- In the Radio On/Off Setting section, select either **Always ON** to turn on the radios or **Always OFF** to turn them off, from the 2.4GHz Radio or 5GHz Radio pull-down menu,

Note

The Scheduled option in the radio pull-down menus is explained in Chapter 11, “Radio Schedules” on page 213.

- Click **APPLY** to save the changes or **CANCEL** to cancel the action.

Configuring Basic Radio Settings

This section contains the procedure for configuring the following radio settings on the 2.4GHz and 5GHz radios in the access points of a location:

- ☐ Wireless mode
- ☐ Channel width
- ☐ Beacon interval
- ☐ Delivery Traffic Indication Message (DTIM) interval

The parameters are defined in Table 8 on page 92.

This procedure is performed at the location level and affects all the access points in a location.

To configure the basic radio settings of the access points in a location, perform the following procedure:

1. Click the **Configuration** tab.
2. In the Locations menu in the left margin, click the name of the location with the access points whose radios you want to configure. You can select only one location. For an example, refer to Figure 48 on page 89.

The program displays the location configuration screen. For an example, refer to Figure 39 on page 76.

3. In the location configuration area, click the **Wireless Radio** option to expand it.

The program displays the Wireless Radio configuration section. Refer to Figure 49 on page 90.

The Radio On/Off Setting options are explained in “Turning Access Point Radios On or Off” on page 89.

4. Configure the settings in the 2.4GHz Configuration and 5GHz Configuration sections. Refer to Table 8 on page 92.

Table 8. Basic Radio Settings

Basic Radio Setting	Description
Wireless Mode	Specifies the Physical Layer (PHY) standards for the radios. The available modes depend on the radio and country. The modes for the 2.4GHz radio are listed here: - IEEE 802.11b: The access points accept only 802.11b clients. - IEEE 802.11b/g: The access points accept 802.11b and 802.11g clients. - IEEE 802.11b/g/n: The access points accept 802.11b, 802.11g, and 802.11n, clients operating at 2.4GHz. This is the default setting for the 2.4GHz radio. The modes for the 5GHz radio are listed here: - IEEE 802.11a: The access points accept 802.11a clients operating at 5GHz. - IEEE 802.11a/n: The access points accept 802.11n and 802.11a clients operating at 5GHz. - IEEE 802.11a/c: The access points accept 802.11a and 802.11c clients. This is the default setting for the 5GHz radio.
Channel Width	Specifies the channel width of a radio. The wider channels allow for higher data rates, but reduce the number of available channels for other wireless devices. Setting the channel width for the 2.4GHz is only available with the IEEE 802.11b/g/n wireless mode. The options are 20 and 40MHz. The default is 20MHz. Setting the channel width for the 5GHz radio is available with the IEEE 802.11a/n and IEEE 802.11a/c modes. The options are 20 and 40MHz for the IEEE 802.11a/n mode and 20, 40, and 80MHz for the IEEE 802.11a/c mode. The default is 20MHz.

Table 8. Basic Radio Settings

Basic Radio Setting	Description
Beacon interval	Specifies the time interval, in milliseconds, for transmissions of beacon frames. The access point transmits beacon frames to announce the existence of the wireless network. The range is 100 to 1000 milliseconds. The default setting is 100 milliseconds (10 beacon frames per second).
Delivery Traffic Indication Message (DTIM) interval	Specifies the Delivery Traffic Information Map (DTIM) period. This value specifies how often clients sleeping in low power mode should check the access point for buffered traffic. The interval is defined in beacon frames. The range is 1 to 255 beacons frames. The default is 3 beacon frames.

To display the beacon interval and DTIM parameters, click the **Show Advanced Features** link.

- Click **APPLY** to save the changes or **CANCEL** to cancel the action.

Configuring the Maximum Number of Wireless Clients

This section contains instructions on how to set the maximum number of wireless clients the access points can support on the radios at one time. This is referred to as load balancing. The range is 1 to 128 clients. The default is 128 clients per radio. Here are the guidelines to load balancing:

- ❑ Load balancing is applied at the location level and applies to all the access points in a location.
- ❑ The 2.4GHz and 5GHz radios can have different load balancing values.

To configure load balancing on the access points in a location, perform the following procedure:

1. Click the **Configuration** tab.
2. In the Locations menu in the left margin, click the location where you want to configure load balancing. You can configure only one location at a time. For an example, refer to Figure 48 on page 89.

The program displays the location configuration screen. For an example, refer to Figure 39 on page 76.

3. In the location configuration area, click **Load Balancing** to expand the section.

The Load Balancing section is displayed:

Map Details

▶ Location Profile

▶ Wireless Radio

▼ Load Balancing

2.4GHz Max. Wireless Clients

AT-AP500	128	(1 - 128)
----------	----------------------------------	-----------

5GHz Max. Wireless Clients

AT-AP500	128	(1 - 128)
----------	----------------------------------	-----------

▶ Auto RF

▶ Building Access Controls

▶ AP Local Management

▶ Radius Server

▶ MAC-ACL

Figure 50. Expanding Load Balancing Area

4. In the 2.4GHz Max. Wireless Clients and 5GHz Max. Wireless Clients fields, enter the maximum number of clients the radios in the location should support at one time. The range is 1 to 128 clients. The default is 128 clients.
5. Click **APPLY** to save the changes or **CANCEL** to cancel the action.

Setting the Local Password for Access Points

This procedure explains how to set the local password for access points in a location. You use the password to manage access points locally, without the AlliedView Cloud program. The same password is applied to all the access points in a location. Manually setting the local password is not required. If you do not assign a password, the program automatically generates a password itself.

Note

The AT-AP500 Access Point does not support local management, but still must have a local password.

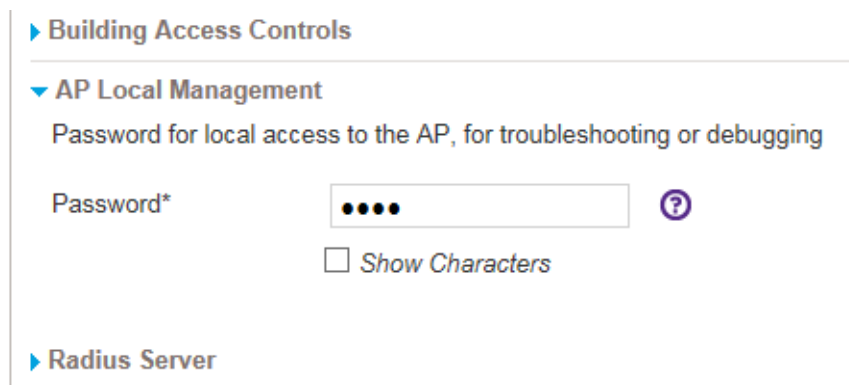
To set the local password for the access points in a location, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left margin or the locations list in the main part of the screen, click the name of the location whose local password you want to change.

The program displays the configuration of the location, with the Location Profile section expanded. An example is shown in Figure 39 on page 76.

3. Click **AP Local Management** to expand the section.

The program displays the prompt for setting the local password for access points.



The screenshot shows a web-based configuration interface. At the top, there is a section titled 'Building Access Controls' with a right-pointing triangle icon. Below it, the 'AP Local Management' section is expanded, indicated by a downward-pointing triangle icon. Under this section, there is a descriptive text: 'Password for local access to the AP, for troubleshooting or debugging'. Below this text is a 'Password*' label followed by a text input field containing four black dots. To the right of the input field is a purple circular help icon with a question mark. Below the input field is a checkbox labeled 'Show Characters'. At the bottom of the visible section, there is another section titled 'Radius Server' with a right-pointing triangle icon.

Figure 51. AP Location Management Section for the Local Password for Access Points in a Location

4. Enter a new local password for the access points. The password can be up to 32 alphanumeric characters, It may not contain spaces or any of these special characters: " , \$, : , < , > , & , * .

You can click the Show Characters box to show or hide the network key characters: check the box to show or remove the check mark to hide.

5. Click **Save** to activate the change or **Cancel** to cancel the procedure.

Configuring WMM QoS

This section describes enabling or disabling WiFi Multimedia (WMM) and WMM Powersave (both enabled by default).

WiFi Multimedia (WMM) QoS control automatically prioritizes data with four queues:

- ☐ Voice: highest
- ☐ Video: second highest
- ☐ Best effort: medium (for example, standard IP application)
- ☐ Background: lowest (for example, FTP)

WMM Powersave saves power for battery-operated devices to optimize data transmission.

Note

WMM must be supported by wireless clients to be effective.

To enable or disable WMM and/or WMM Powersave, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left margin, click the location where you want to configure QoS. You can configure only one location at a time. For an example, refer to Figure 48 on page 89.

The program displays the location configuration screen. For an example, refer to Figure 39 on page 76.

3. Click the **QoS** section to expand it.

The Wireless QoS configuration area is displayed:

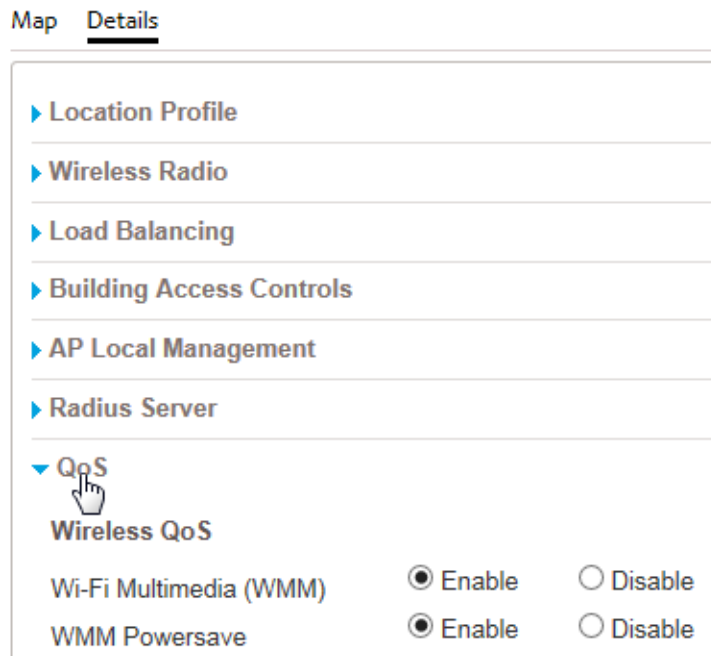


Figure 52. QoS Section

4. Click the WiFi Multimedia (WMM) **Enable** or **Disable** button to enable or disable WMM, respectively.
5. Click the WMM Powersave **Enable** or **Disable** button to enable or disable WMM Powersave, respectively.
6. Click **APPLY** to save the changes or **CANCEL** to cancel the action.

Chapter 5

Buildings and Floors

This chapter includes the following sections:

- ❑ “Introduction to Buildings and Floors” on page 102
- ❑ “Viewing the Buildings of a Location” on page 103
- ❑ “Adding Buildings to Locations” on page 104
- ❑ “Changing Building Names” on page 107
- ❑ “Deleting Buildings” on page 108
- ❑ “Viewing the Floors of Buildings” on page 109
- ❑ “Adding Floors to Buildings” on page 110
- ❑ “Editing Floors” on page 113
- ❑ “Deleting Floors” on page 115

Introduction to Buildings and Floors

Buildings and floors provide you with a way to organize your access points in your account to make them easier to find. They are stored in the Access Points folder in a location entry. A location entry has to have at least one building and one floor. Location entries come with one default building, called Building 1. Location entries do not come with a default floor. However, the application automatically adds one, called Floor 1, the first time you assign an access point to a location entry that does not have any floors.

Building and floor entries do not have to represent actual physical buildings and floors. You can use them in a variety of ways. For instance, you might use them to represent areas of a building or floor.

In this version of the program, buildings and floors do not have any variables or parameters that control access points or wireless networks. Their names are their only variables.

Viewing the Buildings of a Location

This section contains the procedure for viewing the buildings of a location. You can view the buildings of only one location at a time.

To view the buildings of a location, do the following:

1. Click the **Configuration** tab.
2. In the Locations column in the left column, click **location name -> Access Points** of the location whose buildings you want to view. This example displays the buildings at the Warehouse - TL location:

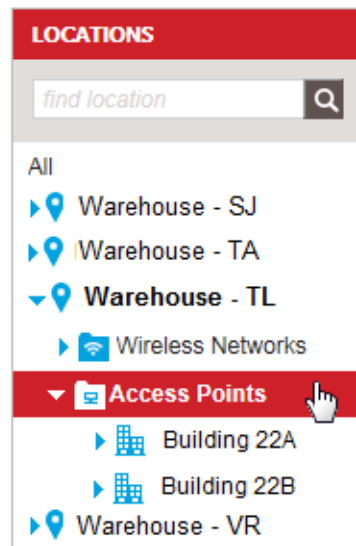


Figure 53. Viewing the Buildings of a Location

The buildings of the location are listed under the Access Points folder.

Adding Buildings to Locations

This section contains the procedure for adding buildings to locations. You have to add a location before adding its buildings. For instructions, refer to “Adding Locations” on page 78.

To add a building to a location, do the following.

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click the name of the location where you want to add the new building. Alternatively, click the name in the All Locations portion of the window. This example shows the selection in the Warehouse - TL location.

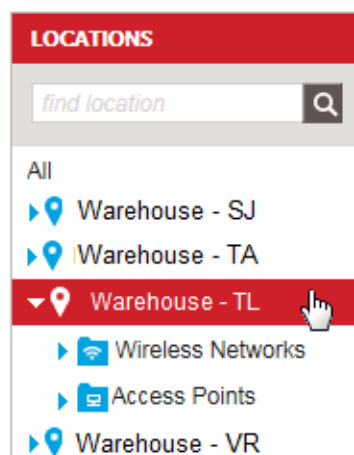


Figure 54. Selecting a Location from the Locations Menu

3. Select **Add Building** from the Choose Action menu.

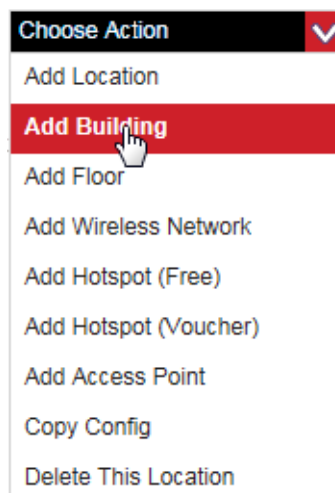


Figure 55. Add Building Selection in the Choose Action Menu

The Add Building window is displayed.

Add Building

Building Name

CANCEL ADD THIS BUILDING

Figure 56. Add Building Window

4. Type a name for the building in the Building Name field.
5. Click **ADD THIS BUILDING**.

The program displays a confirmation window.

Add Building

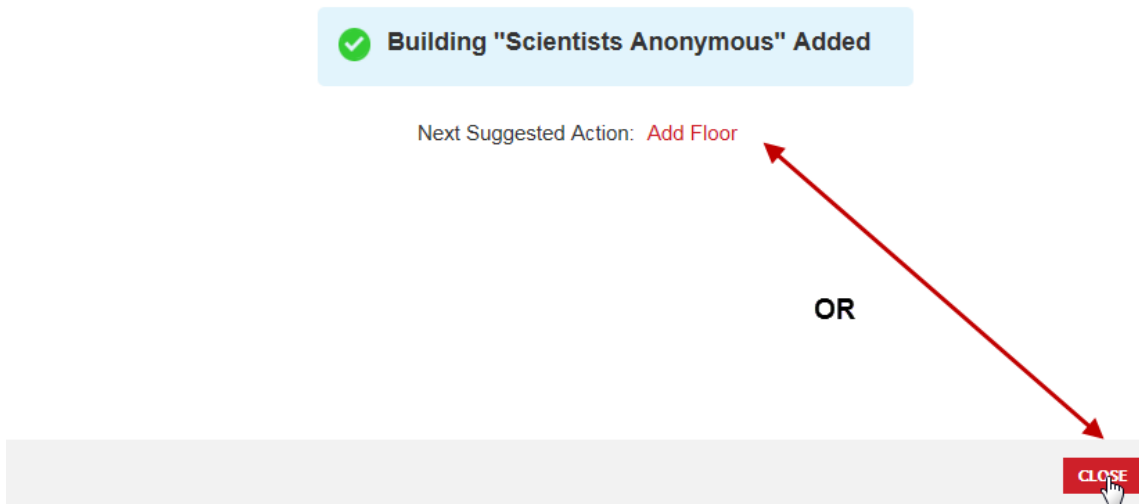


Figure 57. Add Building Confirmation Window

6. Do one of the following:
 - ☐ To add more buildings or perform a different procedure, click **CLOSE**. To add more buildings, repeat this procedure starting with step 2.
 - ☐ To add a floor to the new building, click **Add Floor**. For instructions, go to “Adding Floors to Buildings” on page 110.

Changing Building Names

To change the name of a building, do the following.

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Access Points -> building name
 of the building you want to edit. You can edit only one building at a time. The example here selects Building 22A in the Warehouse - TL location.

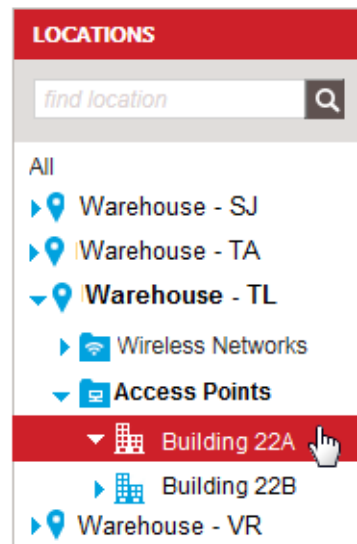


Figure 58. Selecting a Building

The program displays the Building Name field

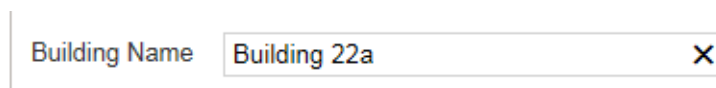


Figure 59. Building Name Field

3. Edit the building name.
4. Click **SAVE** to save the change or **CANCEL** to cancel the action.

Deleting Buildings

To delete a building from your account, do the following.

Note

Access points of deleted buildings are retained in inventory, but their status are changed to unassigned. Their configuration settings are returned to the default values. Their radios are disabled and they stop forwarding traffic. To assign access points to other locations, refer to “Moving Access Points to New Locations” on page 130 or “Moving Unassigned Access Points to Locations” on page 133.

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Access Points -> building name
of the building you want to delete. You can delete only one building at a time. For an example, refer to Figure 58 on page 107.
3. Select **Delete This Building** from the Choose Action menu:

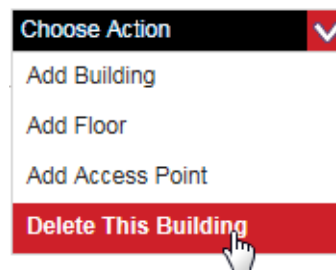


Figure 60. Delete This Building Selection in the Choose Action Menu

The program displays a confirmation window.

4. Click **YES** to delete the building or **NO** to cancel the action.
If you click YES, the program deletes the building.

Viewing the Floors of Buildings

This section explains how to display the floors of a building. To view the names of the floors of a building, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Access Points -> building name
of the building with the floors you want to view. In the example, Building 22A in the Warehouse - TL location has two floors.

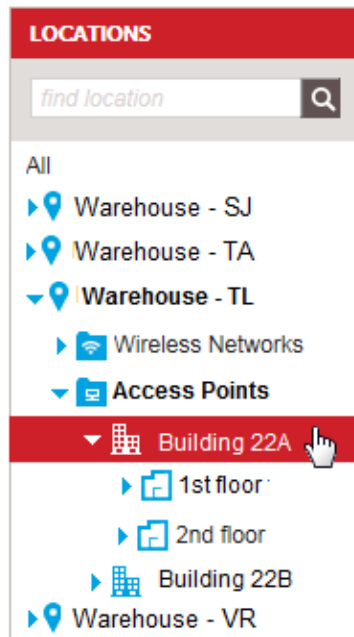


Figure 61. Displaying the Floors of a Building

Adding Floors to Buildings

This section explains how to add floors to buildings. You should add floors before adding access points.

To add a floor to a building, do the following.

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Access Points -> building name
where you want to add the floor. You can add a floor to only one building at a time. For an example, refer to Figure 58 on page 107.
3. Select **Add Floor** from the Choose Action menu:

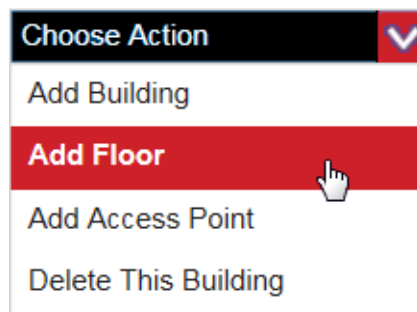


Figure 62. Add Floor Selection in the Choose Action Menu

The program displays the Add Floor window.

Add Floor



Floor Name*

In Building

Scientists Anonymous

CANCEL

Figure 63. Add Floor Window

4. Type a name for the floor in the Floor Name field.
5. If you want to select a different building in the same location for the floor, use the In Building pull-down menu to select the floor. Otherwise, leave the selection as is.

Note

You cannot move a floor to a different building after it is added to a building.

6. Click **ADD THIS FLOOR** to add the floor to the building or **CANCEL** to cancel the action.

A window is displayed confirming the addition of the floor.

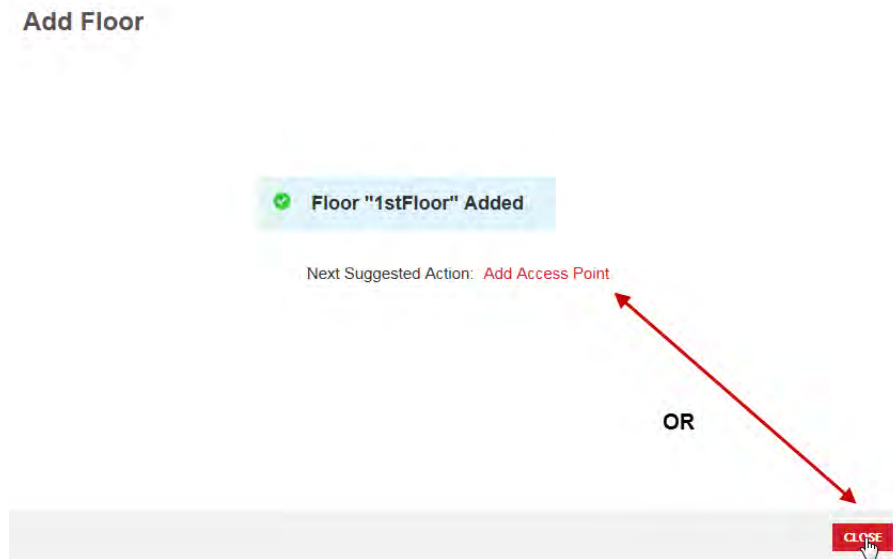


Figure 64. Add Floor Confirmation Window

7. Do one of the following:
- ☐ To add more floors to this building, click **CLOSE** to return to the Building Name window and repeat the procedure starting with step 2.
 - ☐ To move an access point already in inventory to this floor, click **Close** and go to "Moving Access Points to New Locations" on page 130 or "Moving Unassigned Access Points to Locations" on page 133.
 - ☐ To add a new access point to inventory and assign it to this floor, click **Add Access Point**. For instructions, go to "Adding Access Points with the Configuration Tab" on page 121 and start with step 4.

Editing Floors

This section contains the procedure for editing the following floor parameters:

- ❑ Name
- ❑ Width and length

Note

Floor dimensions have no function in this release of the product.

To re-name a floor or change its dimensions, do the following.

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Access Points -> building name -> floor name
 of the floor you want to edit. You can edit only one floor at a time. This example selects the 1st floor in Building 22A.

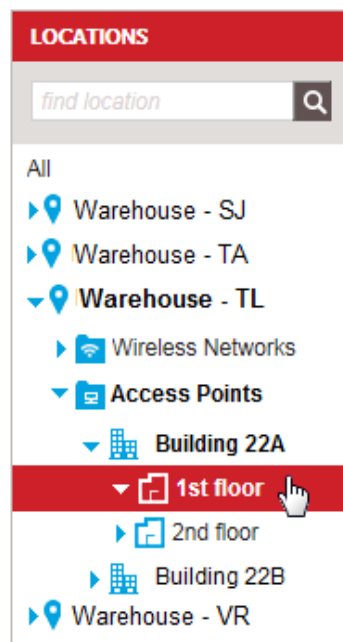
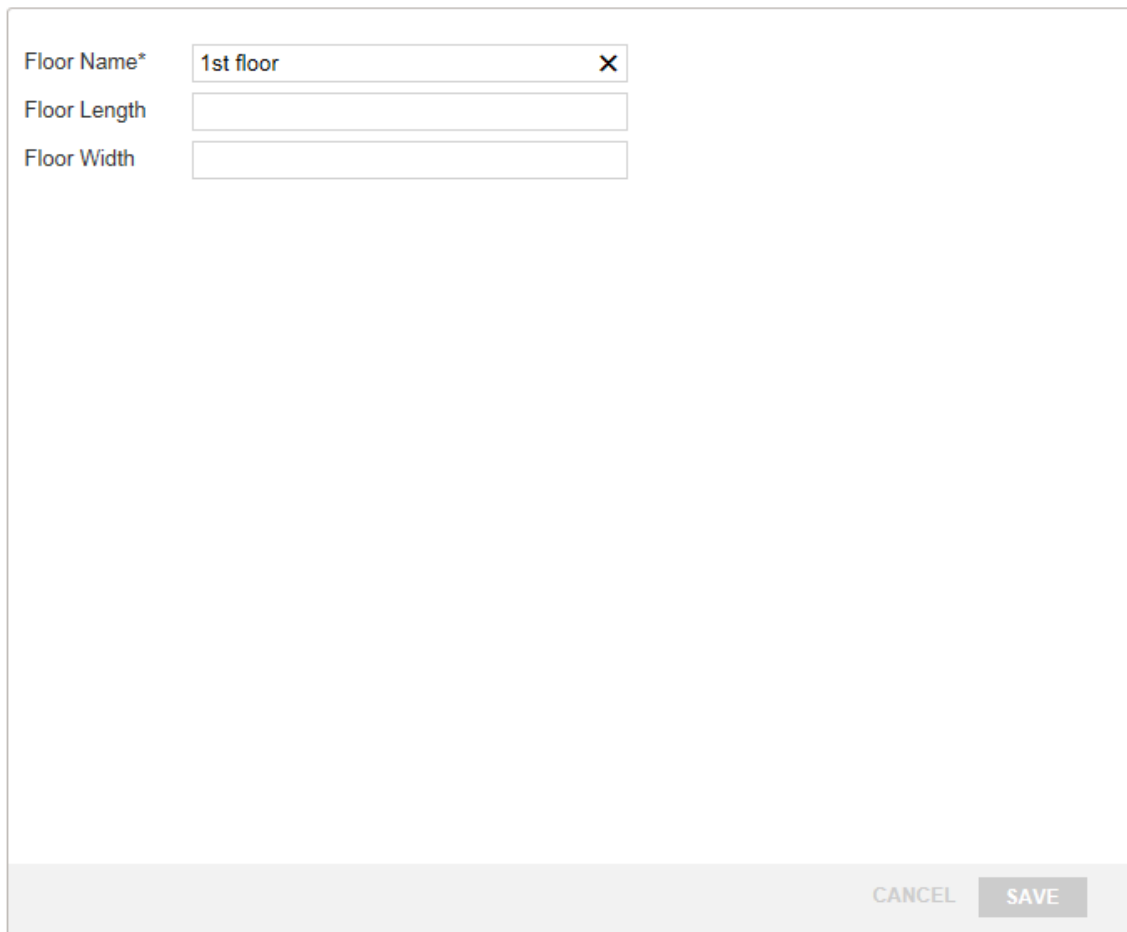


Figure 65. Selecting a Floor

The program displays the Floor Details window.

A dialog box titled "Floor Details" with a light gray background. It contains three input fields: "Floor Name*" with the text "1st floor" and a clear button (X), "Floor Length" which is empty, and "Floor Width" which is empty. At the bottom right, there are two buttons: "CANCEL" and "SAVE".

Floor Name*	1st floor X
Floor Length	
Floor Width	

CANCEL SAVE

Figure 66. Floor Details

3. In the floor configuration area, edit the floor name.
4. If desired, enter the floor length and width, in feet.
5. Click **SAVE** to save your changes or **CANCEL** to cancel the action.

Deleting Floors

To delete a floor, do the following.

Note

Access points of deleted floors are retained in inventory, but their status are changed to unassigned. Their configuration settings are returned to the default values. Their radios are disabled and they stop forwarding traffic. To assign access points to other locations, refer to “Moving Access Points to New Locations” on page 130 or “Moving Unassigned Access Points to Locations” on page 133.

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Access Points -> building name -> floor name
of the floor you want to delete. You can delete only one floor at a time.
For an example, refer to Figure 65 on page 113.
3. Select **Delete This Floor** from the Choose Action menu:

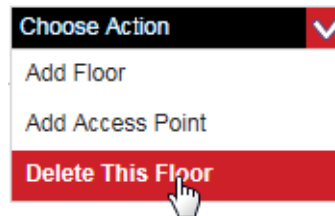


Figure 67. Delete This Floor Selection in the Choose Action Menu

The program displays a confirmation prompt.

4. Click **YES** to delete the floor or **NO** to cancel the action.

If you click YES, the program deletes the floor.

Chapter 6

Access Point Inventory

This chapter includes the following sections:

- ❑ “Viewing the Access Point Inventory” on page 118
- ❑ “Introduction to Adding Access Points” on page 120
- ❑ “Adding Access Points with the Configuration Tab” on page 121
- ❑ “Adding Access Points with the Inventory Tab” on page 125
- ❑ “Adding Access Points with a CSV File” on page 127
- ❑ “Moving Access Points to New Locations” on page 130
- ❑ “Changing Access Points to Unassigned” on page 132
- ❑ “Moving Unassigned Access Points to Locations” on page 133
- ❑ “Setting the Local Password for Unassigned Access Points” on page 134
- ❑ “Deleting Access Points from Inventory” on page 136

Viewing the Access Point Inventory

The inventory is where the AlliedView Cloud program stores the access points in your account. The inventory contains access points that are assigned to locations as well as unassigned units.

To view the inventory, click the Inventory tab. The program displays a list of the access points in your account. An example is shown in Figure 68.

Sort by AP Name | AP Serial | AP Model | AP MAC | IP Address

Warehouse-SJ-AP1 - A22222B111114444 - AP500: Warehouse-SJ
Warehouse-SJ-AP2 - A22222B111115555 - AP500: Warehouse-SJ
Warehouse-SJ-AP3 - A22222B111113214 - AP500: Warehouse-SJ
Warehouse-SJ-AP4 - A22222B111118427 - AP500: Warehouse-SJ

Figure 68. List of Access Points in the Inventory Tab

Access points are identified as shown in Figure 69.

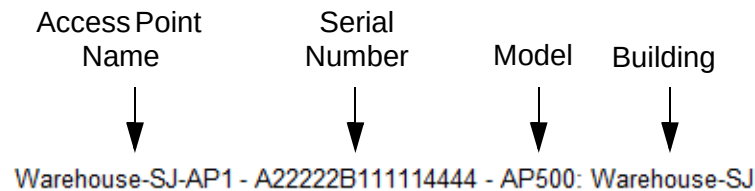


Figure 69. Access Point Identifier

You can sort the devices with the Sort By options above the list, as well as search for devices with the magnify glass option in the upper right corner.

You can also search for access points with the Inventory menu in the left margin of the screen. Refer to Figure 70 on page 119. The menu lists all the locations. Clicking on a location displays the access points of the location in the main body of the screen. The Unassigned option in the menu displays unassigned devices.

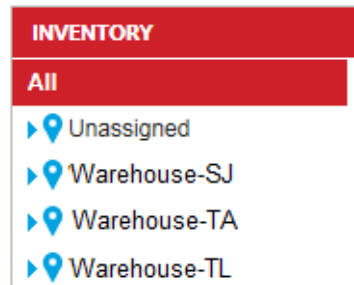


Figure 70. Inventory Menu with Locations

Placing the cursor to the far right of the name displays a small, blue, up arrow. Clicking it displays status information about the device. Figure 71 is an example.



Figure 71. Access Point Status Information

Clicking the name of an access point displays its profile window. For an example, refer to Figure 75 on page 123.

Introduction to Adding Access Points

There are three ways to add access points to your account. Two ways are used to add devices one at a time. The third way is used to add multiple devices. The methods are listed here:

- ❑ “Adding Access Points with the Configuration Tab” on page 121 - You use this method to add one access point at a time. You use the Locations menu in the Configuration tab to move to the building and floor when the device is to be assigned.
- ❑ “Adding Access Points with the Inventory Tab” on page 125 - You can also add one device at a time from the Inventory tab, as explained in this section.
- ❑ “Adding Access Points with a CSV File” on page 127 - If you have a lot of access points to add, you might find it easier to add them to a CSV file and download the file to the program. Access points added in this manner are initially not assigned to any locations. You have to assign them to locations after adding them to the inventory.

Here are the guidelines to adding access points:

- ❑ You can only add access points that have been approved for this program by Allied Telesis. Refer to the product data sheet for a list of approved products.
- ❑ You have to know the serial numbers of the access points. The serial numbers are located on labels on the bottoms of the units.
- ❑ The location, building, and floor where you want to assign an access point should already exist in the program. For instructions, refer to Chapter 3, “Locations” on page 73 and Chapter 5, “Buildings and Floors” on page 101.
- ❑ If you assign an access point to a building that does not have floors, the program automatically adds a floor and assigns the access point to it.
- ❑ You can add access points to the inventory without assigning them to locations by designating them as unassigned.
- ❑ When you add an access point with the Configuration or Inventory tab, the program attempts to communicate with it at the completion of the procedure. If the device is unavailable, the program still adds it to its inventory, but marks its status as “Waiting for connection.”

Adding Access Points with the Configuration Tab

This section contains the procedure for adding new access points to the inventory in your account, with the Locations menu in the Configuration tab. Please review the information in “Introduction to Adding Access Points” on page 120 before performing this procedure.

To add a new access point to the program from the Configuration tab, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left margin, select:
location name - > Access Points - > building name - > floor name
 where you want to add the access point. You can add an access point to only one location and floor. The example here adds an access point to the first floor in Building 22A in the Warehouse - TL location.

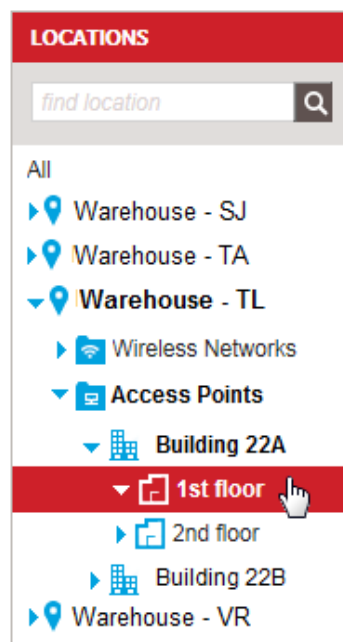


Figure 72. Example of Adding an Access Point to a Floor with the Locations Menu

The program displays the floor profile. For an example, refer to Figure 66 on page 114.

3. Select **Add Access Point** from the Choose Action menu in the upper right corner.

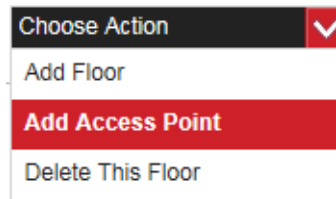


Figure 73. Add Access Point Selection in the Choose Action Menu

The program displays the Add Access Point window:

Add Access Point

NOTE: Please power cycle your Access Point in order to avoid waiting for it to establish connection with this cloud management platform. The AP Local Password for this AP will be set to the AP Local Password for the Location to which it is assigned. If it is not assigned to a Location, the AP Local password will be set to the Account's Default AP Local Password. The default value for this Account's AP Local Password can be changed under Account Settings.

Name*

Serial Number*

Figure 74. Add Access Point Window

4. Type a name for the access point in the Name field. Here are the name guidelines:
 - ☐ It can be 2 to 16 characters.
 - ☐ It can contain letters or numbers.
 - ☐ It must have at least one letter.
 - ☐ It must not contain any spaces or special characters.
 - ☐ The only supported special character is the dash (-).
 - ☐ The name cannot end with a dash.

5. Type the serial number of the access point in the Serial Number field. The serial number can be found on a label on the bottom panel of the access point. The serial number is case sensitive. Letters must be entered in upper or lowercase as they are on the label.

Note

An access point cannot be added without a valid serial number or with the serial number of an access point already in inventory.

6. Click **ADD THIS ACCESS POINT** or **CANCEL** to cancel the action.

The program adds the access point to inventory and the selected floor, and displays the Access Point Profile screen.

▼ Access Point Profile	
Name	AP-3
Serial Number	333393333335
Model	
Hardware Revision	Unknown
Firmware Version	Unknown
MAC Address	Unknown
Location	Warehouse - SJ ▼
Building	Building 1 ▼
Floor	Floor 1 ▼
State	Waiting for connection
Time Since Power Up	Unknown
Date Added	03:49:56PM 03/02/2016 (PST)
Date Provisioned	
Date Located	
Months in Service	< 1
► IP Setting	
► Advanced	

Figure 75. Access Point Profile Screen for an Assigned Access Point

At this point the program attempts to contact the access point. If it succeeds, it updates the following fields in the screen with information from the unit:

- ☐ Hardware Revision

- ☐ Firmware Revision
- ☐ MAC Address
- ☐ Date Provisioned
- ☐ Date Located

If the program is unable to communicate with the access point, it still adds it to the inventory and location.

I

Adding Access Points with the Inventory Tab

This section contains the procedure for adding access points to the program from the Inventory tab. Please review “Introduction to Adding Access Points” on page 120 before performing this procedure.

To add an access point from the Inventory tab, do the following:

1. Click the **Inventory** tab.
2. Select **Add Access Point** from the Choose Action menu:

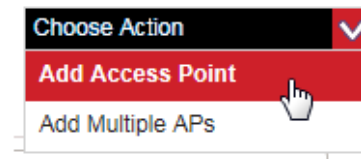


Figure 76. Add Access Point Selection

The program displays the Add Access Point window. For an example, refer to Figure 74 on page 122.

3. Type a name for the access point in the Name field. Here are the name guidelines:
 - ☐ It can be 2 to 16 characters.
 - ☐ It can contain letters or numbers.
 - ☐ It must have at least one letter.
 - ☐ It must not contain any spaces or special characters.
 - ☐ The only supported special character is the dash (-).
 - ☐ The name cannot end with a dash.
4. Type the serial number of the access point in the Serial Number field. The serial number is found on a label on the bottom panel of the access point. The serial number is case sensitive. Letters must be entered in upper or lowercase as they are on the label.

Note

An access point cannot be added without a valid serial number or with the serial number of an access point that is already in the inventory.

5. Click **ADD THIS ACCESS POINT** in the bottom right corner or **CANCEL** to cancel the action.

The program adds the access point and displays the Access Point Profile screen.

The screenshot shows the 'Access Point Profile' screen. It contains a list of fields for an access point named 'Tech-Pubs-ap3'. The 'Serial Number' is 'A22222B111114444'. Most other fields like 'Model', 'Hardware Revision', 'Firmware Version', 'MAC Address', 'State', 'Time Since Power Up', 'Date Added', 'Date Provisioned', and 'Date Located' are 'Unknown'. The 'Location' field is a pull-down menu currently showing 'Unassigned'. The 'Months in Service' is '< 1'. Below the profile fields are three expandable sections: 'IP Setting', 'Advanced', and 'Advanced' (repeated).

▼ Access Point Profile	
Name*	Tech-Pubs-ap3 X
Serial Number	A22222B111114444
Model	
Hardware Revision	Unknown
Firmware Version	Unknown
MAC Address	Unknown
Location	Unassigned ▼
State	Waiting for connection
Time Since Power Up	Unknown
Date Added	02:27:12PM 10/11/2016 (EDT)
Date Provisioned	
Date Located	
Months in Service	< 1
▶ IP Setting	
▶ Advanced	
▶ Advanced	

Figure 77. Access Point Profile Screen for an Unassigned Access Point

At this point the access is not assigned to any location, which is why the Location field in the profile is blank.

6. If you want to add the access point to a location now, use the Location pull-down menu in the profile screen to select the desired location. For instructions, go to step 4 in “Moving Unassigned Access Points to Locations” on page 133.
7. To add more access points, repeat this procedure starting with step 1.

Adding Access Points with a CSV File

This section contains the procedure for adding multiple access points to the program with a CSV file. Please review “Introduction to Adding Access Points” on page 120 before performing this procedure.

You need to create a CSV file with the serial numbers and names of the access points you want to add to the inventory. Here are the guidelines for the CSV file:

- ❑ The serial numbers must be in the left column and the access point names in the right column in the file.
- ❑ The serial numbers can be found on labels on the bottom panels of the access points. Serial numbers are case sensitive. Letters must be entered in upper or lowercase as they are on the labels.
- ❑ The program has a CSV template you can upload to your computer and use to create your file. To obtain the file, perform steps 1 and 2 and then click on the “Download a CSV file template” prompt.

Here are the guidelines to naming access points:

- ❑ A name can be 2 to 16 characters.
- ❑ It can contain letters or numbers.
- ❑ It must have at least one letter.
- ❑ It must not contain any spaces or special characters.
- ❑ The only supported special character is the dash (-).
- ❑ The name cannot end with a dash.

To upload your CSV file to the program, do the following:

1. Click the **Inventory** tab.
2. Select **Add Multiple APs** from the Choose Action menu:

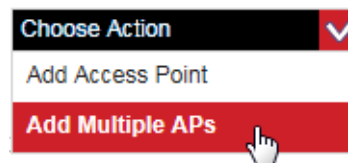


Figure 78. Add Multiple APs Selection in the Choose Action Menu

The program displays the Add Multiple APs window:

Add Multiple APs

1 Upload

2 Confirm & Edit

3 Licensing

Upload multiple Access Points with a CSV file. Not sure how to do that? Use the link to download an example below.

Browse to CSV

☒ My table has header **BROWSE**

[Download a CSV file template](#)

CANCEL

UPLOAD

Figure 79. Add Multiple APs Window

Note

If you want to use the CSV template file in the program, click “Download a CSV file template” and, when prompted, store the file on your computer or network server.

3. If your access points CSV file has a header, check the “My table has a header” box. If it does not have a header, remove the check from the box.

Note

If you are using the CSV template file from the program, leave the check mark because the file has a header.

4. Click **BROWSE** to select the CSV file on your computer or network server.
5. Click **UPLOAD**.

The program checks the file. If the file is in the correct format, it lists the names and serial numbers of the access points in the file on your screen. An example is shown in Figure 80 on page 129.

Note

If you see the message “Your file is wrong format,” try clicking the “My table has header” option to add or remove the check mark, and click **UPLOAD** again.

Add Multiple APs

Please edit any errors and confirm that all of the information uploaded is correct.

No. ↕	Name	Serial No.	Errors ↕	Remove
1	Warehouse-TL-AP1-NW	A22222B111112222		✕
2	Warehouse-TL-AP2-SW	A22222B111113333		✕
3	Warehouse-TL-AP3-N	A22222B111115555		✕

CANCEL
CONFIRM

Figure 80. Add Multiple Access Points Window

6. Review the list for duplicate access points or units with wrong serial numbers or incorrect name formats. You can edit incorrect serial numbers or remove units from the list.
 - ☐ To edit a serial number, edit the number in the Serial No. field.
 - ☐ To remove a unit from the list, click the **X** in the Remove column.
7. Click **CONFIRM** to accept the list or **CANCEL** to cancel the action.

The program displays a list of your tokens.
8. Click **ADD** in the confirmation window to add the access points to the inventory.
9. To assign the access points to locations, refer to “Moving Unassigned Access Points to Locations” on page 133.

Moving Access Points to New Locations

The procedure in this section explains how to move an access point to a new location, building, or floor. To move an access point, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Access Points -> building name -> floor name -> access point name
 of the access point you want to move. You can move only one access point at a time. This example selects the AP1-NW access point in the Warehouse - TL location.

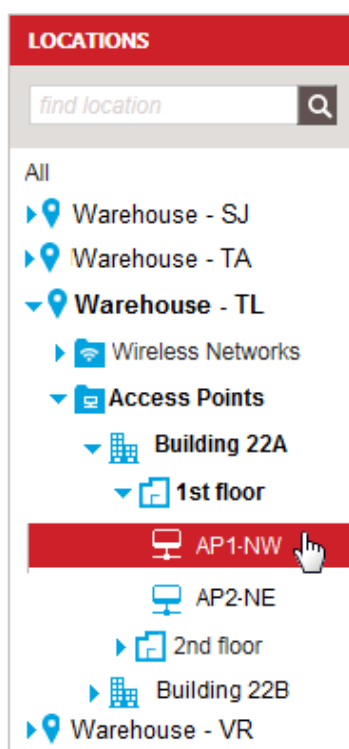


Figure 81. Selecting an Access Point in the Locations Menu

You can also display the profile screen of an access point by clicking the Inventory tab and selecting the access point from the list of units in the Inventory screen.

An example of an access point profile is shown in Figure 75 on page 123.

3. In the Access Point Profile window, use the Location, Building, and Floor pull-down menus to specify the new location for the access point. Refer to Figure 82 on page 131.

Location	Warehouse - SJ	▼
Building	Building 1	▼
Floor	Floor 1	▼

Figure 82. Location, Building, and Floor Pull-down Menus for Moving Access Points

4. Click **Apply** to move the access point to its new location or **Cancel** to cancel the procedure.

If you assign the access point to a building that does not have any floors, the program automatically adds a floor.

5. Repeat this procedure starting with step 2 to move additional access points.

Changing Access Points to Unassigned

If you want to remove an access point from its current location but do not want to assign it to another location, you can mark it as unassigned to retain it in the inventory.

Note

Unassigned access points stop forwarding network traffic. They restore their default configuration settings and disable their radios.

To mark an access point as unassigned, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Access Points -> building name -> floor name -> access point name
of the access point you want to change to unassigned. You can change only one access point at a time. For an example, refer to Figure 81 on page 130.

You can also display the profile screen of an access point by clicking the Inventory tab and selecting the access point from the list of units in the Inventory screen.

An example of a access point profile is shown in Figure 75 on page 123.

3. In the Access Point Profile screen, set the Location field to Unassigned. (The Unassigned selection is listed first in the pull-down menu. It's gray, so it might be hard to see.)
4. Click **Apply** to mark the access point as unassigned or **Cancel** to cancel the procedure.

If you click Apply, the program removes the access point from its current location and marks it as unassigned in the inventory.

5. Repeat this procedure starting to change more access points to unassigned.

Moving Unassigned Access Points to Locations

To move an unassigned access point in inventory to a location, do the following:

1. Click the **Inventory** tab.
2. Click the **Unassigned** option in the Inventory menu in the left column to display a list of unassigned access points.



Figure 83. Unassigned Option in the Inventory Menu

3. From the list of unassigned devices, click the name of the unassigned access point you want to assign to a location. You can move only one access point at a time.

The program displays the Access Point Profile window for the unassigned access point. Refer to Figure 77 on page 126.

4. Use the Location pull-down menu in the Access Point Profile window to select the location for the unassigned access point. You can select only one location for an access point.

The program updates the screen to include Building and Floor options.

5. Use the **Building** and **Floor** pull-down menus to assign the access point to a building and floor at the location.

If you assign the access point to a building that does not have any floors, the program automatically adds a floor.

6. Click **Apply** to assign the access point to the location or **Cancel** to cancel the procedure.

The program moves the access point to the designated location.

7. Repeat this procedure starting with step 1 to move more unassigned access points to locations.

Setting the Local Password for Unassigned Access Points

This procedure explains how to set the local password for unassigned access points. The password, which the program assigns to access points that are not assigned to locations in the inventory, is used to manage access points locally, without the AlliedView Cloud program. The AT-AP500 Access Point does not support local management, but it still must have a local password. Manually setting the local password is not required. If you do not assign a password, the program automatically generates a password itself.

To set the local password for unassigned access points, do the following:

1. Click the **Account** tab.
2. In the Account menu in the left margin, click **Settings -> Account Setting**

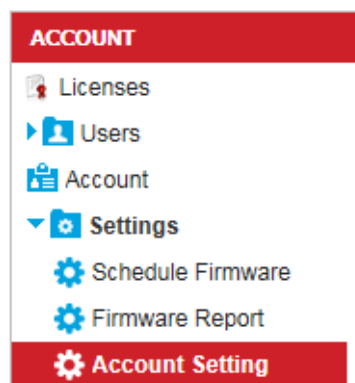


Figure 84. Account Setting in the Account Menu

The program displays the prompt for setting the local password for unassigned access points.

Account Setting Choose Action ▼

Unassigned AP Local Password* ?

☐ Show Characters

CANCEL SAVE

Figure 85. Account Setting for the Local Password for Unassigned Access Points

3. Enter a new local password for unassigned access points. The password can be up to 32 alphanumeric characters, It may not contain spaces or any of these special characters: “, \$, :, <, >, &, *.

You can click the Show Characters box to show or hide the network key characters: check the box to show or remove the check mark to hide.

4. Click **Save** to activate the change or **Cancel** to cancel the procedure.

Deleting Access Points from Inventory

This section contains the procedure for deleting access points from inventory in your account.

Note

Access points stop forwarding network traffic when they are deleted from inventory.

To delete an access point from inventory, do the following:

1. Click the **Inventory** tab.
2. If you want to delete an unassigned access point, click the **Unassigned** option in the Inventory menu in the left column. For an example, refer to Figure 83 on page 133.
3. Click the name of the access point to be deleted.

The program displays the profile page of the access point. An example is shown in Figure 75 on page 123.

You can also display the profile of an access point using the Locations menu in the Configuration tab and selecting the location, building, floor, and access point.

4. Select **Delete This Access Point** from the Choose Action menu:



Figure 86. Delete this Access Point Selection in the Choose Action Menu

The program displays a confirmation message.

5. Click **Yes** to delete the access point or **No** to cancel the procedure.

If you click yes, the program deletes the access point from inventory in your account.

Chapter 7

Access Point Parameters

This chapter includes the following sections:

- ❑ “Introduction to Access Point Parameters” on page 138
- ❑ “Configuring the Syslog Client” on page 139
- ❑ “Setting Radio Channels” on page 141
- ❑ “Configuring Radio Transmission Power” on page 142
- ❑ “Rebooting Access Points” on page 144
- ❑ “Restoring the Default Settings on Access Points” on page 145

Introduction to Access Point Parameters

Most of the operational parameters of your access points and wireless networks are set at location and wireless network levels in your account, and thus affect all the access points at a particular location. However, there are a couple parameters you can set on individual access points. The parameters are listed in Table 9 and explained in the following sections.

Table 9. Access Point Parameters

Management Function or Operational Parameter	Description
Syslog client	The access points have syslog clients that transmit their log messages to syslog servers on your network. You can configure the individual devices to send their message to different servers because each access point has its own client. For instructions, refer to “Configuring the Syslog Client” on page 139
Radio channels	You can configure the access points of a location to use different radio channels. For instructions, refer to “Setting Radio Channels” on page 141
Radio transmission power	You can set the transmission powers of the 2.4GHz and 5GHz radios on the individual access points. For instructions, refer to “Configuring Radio Transmission Power” on page 142.
Rebooting access points	You can reboot individual access points. You might reboot an access point if it is experiencing problems. For instructions, refer to “Rebooting Access Points” on page 144.
Restoring the default settings	You can restore the default settings to individual access points at a location. For instructions, refer to “Restoring the Default Settings on Access Points” on page 145

Configuring the Syslog Client

The access point has a syslog client that it uses to transmit its log messages to a syslog server on your network for storage. The syslog client is configured on individual access points. Consequently, you can configure the access points of a location to send their log messages to different servers.

To configure the syslog client, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Access Points -> building name -> floor name -> access point name
 of the access point you want to configure. You can configure only one access point at a time. This example selects the AP1 NW access point in the Warehouse - TL location.

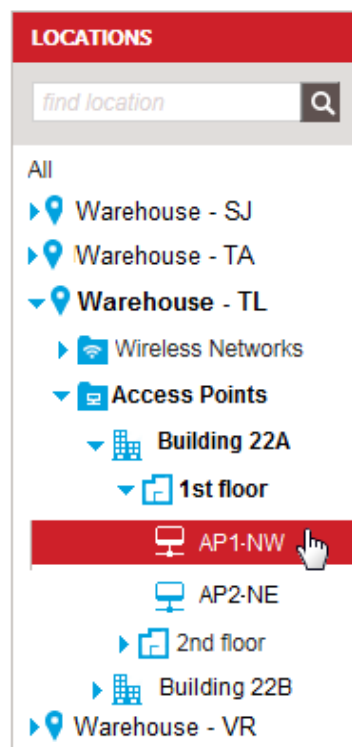


Figure 87. Selecting an Access Point in the Locations Menu

You can also display the profile screen of an access point by clicking the Inventory tab and selecting the access point from the list of units in the Inventory screen.

An example of a profile is shown in Figure 75 on page 123.

- Click the **Advanced** option in the profile to expand it.

▼ **Advanced**

Static Channel

☐ 2.4GHz By AP (--) ▼

☐ 5GHz By AP (--) ▼

Static Tx Power

☐ 2.4GHz By Location (--) ▼

☐ 5GHz By Location (--) ▼

Syslog Settings

Enable Syslog ☐

Server IP Address

Port Number (1 - 65535)

Figure 88. Advanced Option in the Access Point Profile Screen

- Configure the settings in the Syslog Settings section of the screen. Refer to Table 10.

Table 10. Syslog Settings

Parameter	Description
Enable Syslog	Click the dialog box to enable or disable the syslog client. The client is enabled when the dialog box has a check mark and disabled when the dialog box is empty. The default is disabled.
Server IP Address	Enter the IP address of the syslog server on your network. You can specify only one IP address.
Port Number	Enter the protocol port number for your syslog server. The default is 514.

- Click **Apply** to activate your change or **Cancel** to cancel the procedure.

If you click Apply, the access point uses the syslog client to send its log messages to the server as messages are generated. The client does not send any messages already stored in the log.

Setting Radio Channels

Unlike most access point settings, which are set at the location level and thus apply to all the devices in a location, the channels for the 2.4GHz and 5GHz radios can be set on the individual access points themselves, thereby making it possible for radios in the same location to use different channels. Radio channels can be set two ways. The access points can set them automatically, which is the default, or you can set them manually. When an access sets its channels automatically, it listens on the available channels and selects the one with the least traffic.

To set the channels of the 2.4GHz and 5GHz radios in an access point, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Access Points -> building name -> floor name -> access point name
to display the profile screen of the access point you want to configure. You can configure only one access point at a time. For an example refer to Figure 87 on page 139.

You can also display the profile screen of an access point by clicking the Inventory tab and selecting the access point from the list of units in the Inventory screen.

The program displays the access point profile. An example is shown in Figure 75 on page 123.

3. Click the **Advanced** option in the profile to expand it. Refer to Figure 88 on page 140.
4. In the Static Channel section of the Advanced option, configure the 2.4GHz and 5GHz settings, as needed. Here are the guidelines:
 - ☐ To manually set a radio channel, click the dialog box of the radio to add a check mark to it, and then use the pull-down menu to select the desired channel for the radio. You can select only one channel for each radio.
 - ☐ To have the access point set a radio channel automatically, click the dialog box of the radio to remove the check mark. This is the default setting. The pull-down menus are disabled.
5. Click **Apply** to activate your change or **Cancel** to cancel the procedure.

Configuring Radio Transmission Power

This section explains how to configure the transmission powers of the radios in the individual access points of a location. The possible selections are listed here:

- ☐ Full power
- ☐ Half power
- ☐ Quarter power
- ☐ Eighth power
- ☐ Minimal power

High transmission power levels are more cost-effective than low power settings because the access points have a greater range. This reduces the number of access points required to cover a particular area.

Low transmission power settings can be useful in reducing overlap and interference between access points or increasing security by limiting the wireless signals to a physical location.

To set the radio transmission power of the 2.4GHz and 5GHz radios, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Access Points -> building name -> floor name -> access point name
 to display the profile screen of the access point you want to configure. You can configure only one access point at a time. For an example refer to Figure 87 on page 139.

You can also display the profile screen of an access point by clicking the Inventory tab and selecting the access point from the list of units in the Inventory screen.

The program displays the access point profile. An example is shown in Figure 75 on page 123.

3. Click the **Advanced** option in the profile to expand it. Refer to Figure 88 on page 140.
4. In the Static Tx Power section, do one of the following:
 - ☐ To set the power for a radio manually, click the dialog box of the radio to add a check mark to it, and then use the pull-down menu to select the desired power setting for the radio. You can select only one power level for a radio.

- ❑ To set a radio to full possible power, click the dialog box of the radio to remove the check mark. This is the default setting. The pull-down menus are disabled.
5. Click **Apply** to activate your change or **Cancel** to cancel the procedure.

Rebooting Access Points

This section contains instructions on how to reboot access points. You can reboot only one access point at a time.



Caution

Rebooting an access point can be disruptive to your wireless network. When reset, an access point does not forward network traffic for several minutes while it initializes its operating system and configuration settings.

To reboot an access point, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Access Points -> building name -> floor name -> access point name
to display the profile screen of the access point you want to reboot. You can reboot only one access point at a time. For an example, refer to Figure 87 on page 139.

The program displays the access point profile. An example is shown in Figure 75 on page 123.

You can also display the profile screen of an access point by clicking the Inventory tab and selecting the access point from the list of units in the Inventory screen.

3. Select **Reboot This Access Point** from the Choose Action menu:

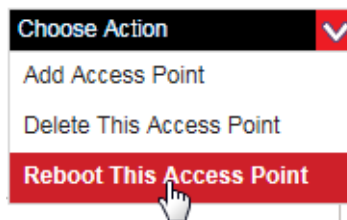


Figure 89. Reboot this Access Point Selection in the Choose Action Menu

The program displays a confirmation message.

4. Click **Yes** to reboot the access point or **No** to cancel the procedure.

If you click yes, allow several minutes for the access point to reboot and re-connect to the AlliedView Cloud application.

Restoring the Default Settings on Access Points

This section contains instructions on how to restore the default settings on access points. Please review the following items before performing this procedure:

- ❑ An access point whose settings are returned to their default values waits to receive its current configuration settings from the AlliedView Cloud program before forwarding network traffic again.
- ❑ There is no functional value to performing this procedure on unassigned access points in inventory; their settings are already at the default values.

To restore the default settings on an access point, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Access Points -> building name -> floor name -> access point name
 to display the profile screen of the access point whose configuration settings to you want to restore to the default settings. You can restore the default settings of only one access point at a time. For an example, refer to Figure 87 on page 139.

The program displays the Access Point Profile screen. An example of a profile is shown in Figure 75 on page 123.

You can also display the profile screen of an access point by clicking the Inventory tab and selecting the access point from the list of units in the Inventory screen.

3. Select **Reset This Access Point to Factory** from the Choose Action menu:

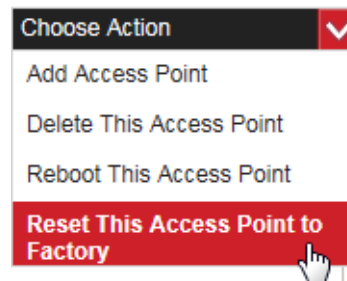


Figure 90. Reboot this Access Point Selection in the Choose Action Menu

The program displays a confirmation message.

4. Click **Yes** to restore the default settings to the access point or **No** to cancel the procedure.

If you select Yes, the access point returns its settings to the default values, reconnects with the AlliedView Cloud program, and waits to receive its current configuration settings from the program. It begins to forward network traffic again after it receives its settings.

Chapter 8

Wireless Networks

This chapter includes the following sections:

- ❑ “Viewing Wireless Networks” on page 148
- ❑ “Adding Wireless Networks” on page 150
- ❑ “Editing Wireless Network Names and Authentications” on page 155
- ❑ “Editing SSID Broadcasts and Wireless Clients Separation” on page 160
- ❑ “Editing VLAN IDs” on page 162
- ❑ “Specifying the 2.4GHz or 5GHz Radios of Wireless Networks” on page 163
- ❑ “Enabling or Disabling Band Steering” on page 164
- ❑ “Enabling or Disabling Wireless Networks” on page 165
- ❑ “Deleting Wireless Networks” on page 166

Viewing Wireless Networks

To view the settings of a wireless network, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Wireless Networks -> network name
of the wireless network whose settings you want to view. You can view the settings of only one network at a time. This example selects the WN_area_1 network in the Warehouse - TL location.

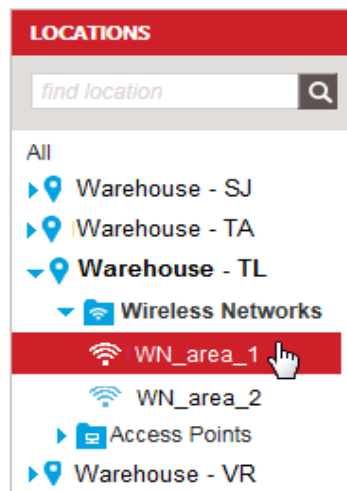


Figure 91. Selecting a Wireless Network

The program displays the configuration screen of the selected network. The following example shows the configuration settings for the WN_area_1 wireless network.

▼ **Network Name and Authentication**

Network Name

Status ☒ Enable ☐ Disable

Network Authentication ▼

Data Encryption ▼

Network Key

☐ Show Characters

Radius Server Profiles *Not Set*

▶ **Security**

▶ **VLAN Settings**

▶ **Radio**

▶ **Captive Portal**

Figure 92. Wireless Network Configuration Screen

The screen has five sections. The Network Name and Authentication section is expanded and the other sections are collapsed. The sections of the screen are explained in the procedures listed in Table 12.

Table 11. Sections in the Wireless Network Configuration Screen

Section	Procedure
Network Name and Authentication	"Editing Wireless Network Names and Authentications" on page 155 and "Enabling or Disabling Wireless Networks" on page 165
Security	"Editing SSID Broadcasts and Wireless Clients Separation" on page 160
VLAN Settings	"Editing VLAN IDs" on page 162
Radio	"Specifying the 2.4GHz or 5GHz Radios of Wireless Networks" on page 163
Captive Portal	"Adding Captive Portals to Wireless Networks" on page 193

Adding Wireless Networks

This section contains instructions on how to add new wireless networks to locations in your account. Please review the following guidelines before performing the procedure:

- ❑ You can add only one wireless network at a time.
- ❑ You have to add the location for a wireless network first. For instructions, refer to “Adding Locations” on page 78.
- ❑ A location can have more than one wireless network.
- ❑ The AT-AP500 Access Point supports up to four wireless networks on its 2.4GHz radio and four networks on its 5GHz radio, for a total of eight networks.
- ❑ If the network authentication method for a wireless network requires a RADIUS server, you must add a RADIUS server profile to the location first. For instructions, refer to “Adding RADIUS Server Profiles” on page 231 and “Adding RADIUS Server Profiles to Locations” on page 235.
- ❑ The access points support a variety of network authentication methods. However, you can choose only open system (no authentication), WPA-PSK, WPA2-PSK, or WPA/WPA2-PSK for authentication when you initially add a network. If you want to use one of the other authentication methods, choose one of these three during the initial configuration and then perform “Editing Wireless Network Names and Authentications” on page 155 to change the authentication method.
- ❑ If you want to add a wireless network as a hotspot, you should first review the information in “Introduction to Network Hotspots” on page 200.

To add a wireless network to a location, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Wireless Networks
 where you want to add the wireless network. You can add a network to only one location at a time. This example selects Wireless Networks at the Warehouse - TL location.

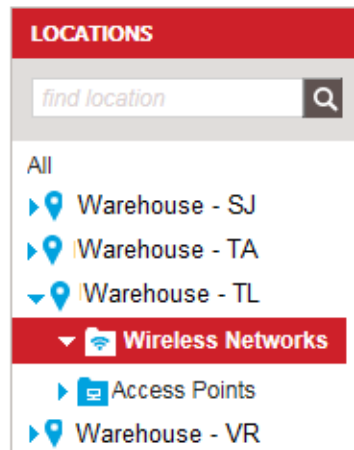


Figure 93. Selecting Wireless Networks in the Locations Menu

3. Select **Add Wireless Network** from the Choose Action menu in the upper left corner:

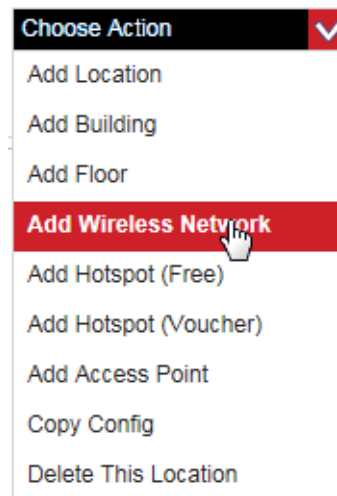


Figure 94. Add Wireless Network Selection in the Choose Action Menu

The program displays the Add Wireless Network window:

Add Wireless Network

Enter details for the new wireless network that you would like to make available at this location. Please note that you can configure advanced authentication types including 'WPA with RADIUS' by directly editing this wireless network after completing this wizard

Network Name*

Wireless Network on ▼

Network Authentication ▼

Data Encryption ▼

Network Key*
Minimum 8 characters, maximum 63 characters.
☒ Show Characters

CANCEL

Figure 95. Add Wireless Network Window

4. Fill in the fields in the window. The parameters are defined in Table 12.

Table 12. Add Wireless Network Screen

Field	Description
Network Name	Enter a name for the network. The name functions as the SSID for the network. Here are the guidelines: - A network must have a name. - A name can be up to 32 characters. - Spaces are not allowed.

Table 12. Add Wireless Network Screen (Continued)

Field	Description
Wireless Network On	Select the radios for the network from the pull-down menu. The selections are listed here: - 2.4GHz and 5GHz - 2.4GHz - 5GHz For example, if you select 5GHz, the access points of the location will carry the network on their 5GHz radios, but not the 2.4GHz radios. The default settings is 2.4GHz and 5GHz.
Network Authentication	Select the authentication method for the network from the pull-down menu. The options are listed here: - Open System (no authentication) - WPA-PSK - WPA2-PSK - WPA/WPA2-PSK The access points support other authentication methods in addition to the four listed here. However, these are the only ones you can select when you initially add a wireless network. If you want to use one of the other authentication methods, choose one of the four above for now, complete the rest of this procedure, and then perform "Editing Wireless Network Names and Authentications" on page 155 to change the authentication method.

Table 12. Add Wireless Network Screen (Continued)

Field	Description
Data Encryption	Select the data encryption for the network from the pull-down menu. The options are listed here: - AES - TKIP - TKIP+AES The available options depend on the authentication method:
Network Key	Enter a shared secret key of 8 to 63 alphanumeric characters. The key can include special characters.

You can click the Show Characters box to show or hide the network key characters as you enter them.

5. Click **ADD THIS WIRELESS NETWORK** to add the network or **CANCEL** to cancel the action.

The program displays the configuration window for the new wireless network. For an example, refer to Figure 92 on page 149.

6. Do one of the following:
 - ☐ To add more wireless networks to locations, repeat this procedure starting with step 2.
 - ☐ To change the authentication method of the new wireless network, refer to “Editing Wireless Network Names and Authentications” on page 155 and start with step 3.

Note

If the authentication method requires a RADIUS server, you must add a RADIUS server profile to the location before editing the wireless network. For instructions, refer to “Adding RADIUS Server Profiles” on page 231 and “Adding RADIUS Server Profiles to Locations” on page 235.

Editing Wireless Network Names and Authentications

This section explains how to edit the following attributes of wireless networks:

- ☐ Name
- ☐ Authentication method
- ☐ Encryption method
- ☐ Enable or disable status

You must assign a RADIUS server profile to a location before using the following authentication methods in wireless networks:

- ☐ Legacy 802.1x
- ☐ WPA with Radius
- ☐ WPA2 with Radius
- ☐ WPA and WPA2 with Radius

For instructions, refer to “Adding RADIUS Server Profiles” on page 231 and “Adding RADIUS Server Profiles to Locations” on page 235.

To edit a wireless network, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Wireless Networks -> network name
of the wireless network you want to edit. This example selects the WN_area_1 network in the Warehouse - TL location.

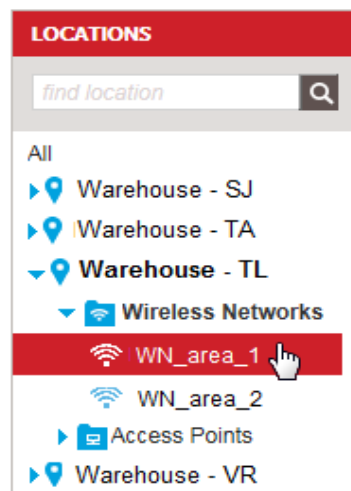


Figure 96. Selecting a Wireless Network in the Locations Menu

The program displays the configuration screen for the network, with the Network Name and Authentication section expanded:

▼ Network Name and Authentication

Network Name

Warehouse_TL_wireless_network

Status

☒ Enable

☐ Disable

Network Authentication

WPA/WPA2-PSK▼

Data Encryption

TKIP+AES▼

Network Key

●●●●●●●●

☐ Show Characters

Radius Server Profiles

Not Set

▶ Security

▶ VLAN Settings

▶ Radio

▶ Captive Portal

Figure 97. Network Name and Authentication Section

3. Edit the fields in the Network Name and Authentication section, as needed. The fields are defined in Table 13.

Table 13. Network Name and Authentication Section

Field	Description
Network Name	Enter a name for the network. The name functions as the SSID for the network. Here are the name guidelines: - A network must have a name. - A name can be up to 32 characters. - Spaces are not allowed.

Table 13. Network Name and Authentication Section

Field	Description
Status	Enable or disable the wireless network. The options are listed here: Enable -Enables the network. This is the default setting. Disable - Disables the network.
Network Authentication	Select the authentication method for the network from the pull-down menu. A network can have only one authentication method. The options are listed here: - Open system (no authentication) - Shared key - Legacy 802.1x - WPA with Radius - WPA2 with Radius - WPA/WPA2 with Radius - WPA-PSK - WPA2-PSK - WPA/WPA2-PSK

Table 13. Network Name and Authentication Section

Field	Description
Data Encryption	Select the data encryption for the network from the pull-down menu. The available options depend on the authentication method. Here are the options for open system and shared key: - None - 64 bit WEP - 128 bit WEP - 152 bit WEP Legacy 802.1x does not have data encryption. WPA with Radius and WPA-PSK have these data encryption options: - TKIP - TKIP+AES WPA2 with Radius and WPA2-PSK have these data encryption options: - AES - TKIP+AES The only authentication method for WPA/ WPA2 with Radius and WPA/WPA2-PSK is TKIP+AES.
Network Key	Enter a shared secret key of 8 to 63 alphanumeric characters. The key can include special characters.

Table 13. Network Name and Authentication Section

Field	Description
Keys 1, 2, 3, and 4	Enter up to four WEP keys in the fields numbered 1 to 4 for open system or shared key authentication. The order of the keys has be the same on the access point and clients. The keys must be entered in hexadecimal. Here are the guidelines: - A hexadecimal key can contain the letters A to F and numbers 0 to 9. - The key length of 64 bits requires 10 hexadecimal characters. - The key length of 128 bits requires 26 hexadecimal characters. - The key length of 152 bits requires 32 hexadecimal characters.

4. Click **APPLY** to save the changes or **CANCEL** to cancel the action.

Editing SSID Broadcasts and Wireless Clients Separation

This procedure explains how to configure the following network parameters:

- ❑ Network SSID broadcasts - You can configure wireless networks not to broadcast their SSIDs so that only wireless clients who know the SSIDs can gain access to them.
- ❑ Wireless clients separation - You can configure networks to maintain separation between the wireless clients so that they cannot directly communicate with each other through the access points.

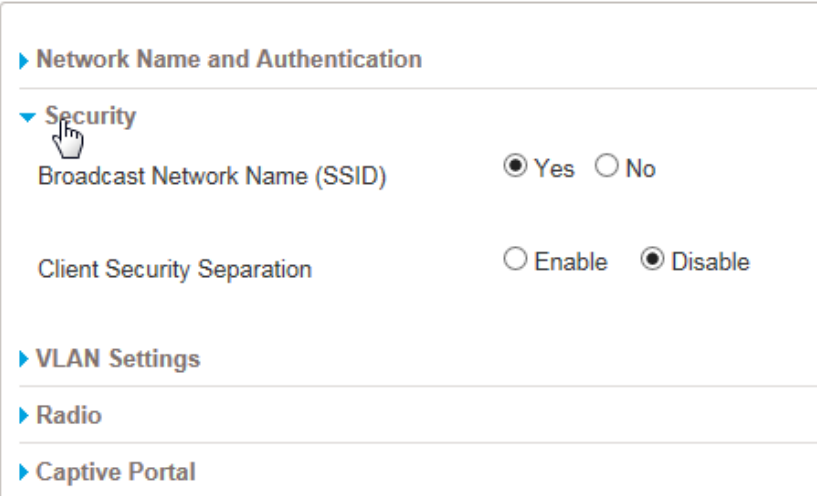
To configure these security parameters, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click: **location name** -> **Wireless Networks** -> **network name** of the network you want to edit. You can edit only one network at a time. For an example, refer to Figure 96 on page 155.

The program displays the configuration screen for the wireless network. For an example, refer to Figure 92 on page 149.

3. Click **Security** to expand the Security area.

The program displays the Security parameters:



▶ Network Name and Authentication

▼ Security

Broadcast Network Name (SSID) ☒ Yes ☐ No

Client Security Separation ☐ Enable ☒ Disable

▶ VLAN Settings

▶ Radio

▶ Captive Portal

Figure 98. Security Parameters

4. Adjust the security parameters as needed. Refer to Table 14 on page 161.

Table 14. SSID Broadcasts and Wireless Client Separation Parameters

Parameter	Description
Broadcast Network Name (SSID)	Controls whether the access points in a location are to broadcast the SSID of a wireless network. When the Yes dialog box is checked, the access points transmit the SSID to advertise the wireless network to clients. When the No dialog box is checked, the access points do not transmit the SSID. Clients who want to connect to a network that is not advertised have to know its name. The default setting is Yes.
Client Security Separation	Enables or disables client isolation. When client isolation is enabled, the wireless clients of a network cannot communicate directly with each other through the access points. However, the clients can communicate with clients in other networks and with the wired LAN. The default setting is disabled.

5. Click **APPLY** to save the changes or **CANCEL** to cancel the action.

Editing VLAN IDs

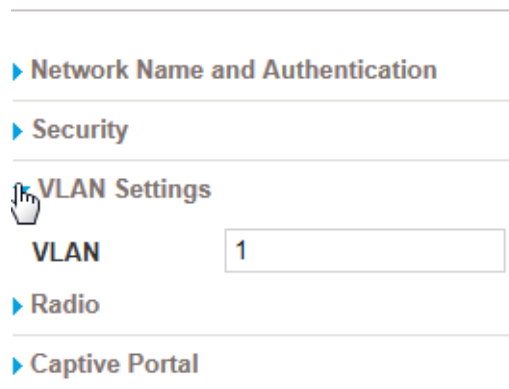
This section explains how to set a WiFi network's VLAN ID. A wireless network can have only one VLAN ID. To edit a network's VLAN ID, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Wireless Networks -> network name
of the network you want to edit. You can edit only one network at a time. For an example, refer to Figure 96 on page 155.

The program displays the configuration screen for the wireless network. For an example, refer to Figure 92 on page 149.

3. Click **VLAN Settings** to expand the VLAN Settings parameter.

The program displays the VLAN Settings parameter:



▶ Network Name and Authentication

▶ Security

▶ **VLAN Settings**

VLAN

▶ Radio

▶ Captive Portal

Figure 99. VLAN Settings Parameter

4. Enter a new VLAN ID in the VLAN field. The default is VID 1.
5. Click **APPLY** to save the changes or **CANCEL** to cancel the action.

Specifying the 2.4GHz or 5GHz Radios of Wireless Networks

The access points have 2.4GHz and 5GHz radios. You can configure networks to use either both radios in the access points or only one radio. At the default settings, the access points use both radios for wireless networks. In some cases, however, you might want the access points to use only one radio for a network, rather than both. For example, if a location has two networks, you might configure it so that the access points use one radio for each network.

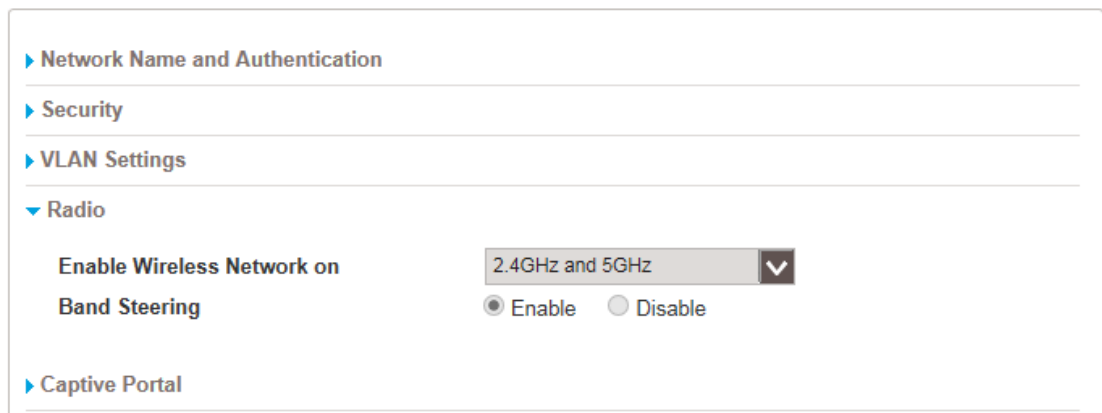
To select the radios for a wireless network, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Wireless Networks -> network name
of the network you want to edit. You can edit only one network at a time. For an example, refer to Figure 96 on page 155.

The program displays the configuration screen for the wireless network. For an example, refer to Figure 92 on page 149.

3. Click **Radio** to expand the Radio parameters.

The program displays the Radio parameters:



The screenshot shows a configuration interface with several expandable sections: Network Name and Authentication, Security, VLAN Settings, Radio, and Captive Portal. The 'Radio' section is currently expanded, revealing two settings. The first is 'Enable Wireless Network on', which has a dropdown menu currently displaying '2.4GHz and 5GHz'. The second is 'Band Steering', which has two radio buttons: 'Enable' (which is selected) and 'Disable'.

Figure 100. Radio Parameters

4. Select the radios for the network. The options are listed here:
 - ☐ 2.4GHz and 5GHz
 - ☐ 2.4GHz
 - ☐ 5GHz
5. Click **APPLY** to save the changes or **CANCEL** to cancel the action.

Enabling or Disabling Band Steering

Band steering is used to reduce network congestion on the 2.4GHz radio on wireless networks that use both 2.4GHz and 5GHz radios. It directs some wireless clients who support both radios to associate on the 5GHz radio rather than the 2.4GHz radio to balance the traffic loads between the radios.

Note

The feature is only available on wireless networks that use both 2.4GHz and 5GHz radios.

To enable or disable band steering, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Wireless Networks -> network name
of the network you want to edit. You can edit only one network at a time. For an example, refer to Figure 96 on page 155.

The program displays the configuration screen for the wireless network. For an example, refer to Figure 92 on page 149.

3. Click **Radio** to expand the Radio parameters.

The program expands the Radio section. Refer to Figure 100 on page 163.

4. For the Band Steering option, click **Enable** to enable band steering on the wireless network or **Disable** to disable it. The default setting is disabled.

Note

You cannot enable band steering on a wireless network that uses only one radio. A network has to be using both 2.4GHz and 5GHz radios for you to enable band steering. For instructions, refer to "Specifying the 2.4GHz or 5GHz Radios of Wireless Networks" on page 163.

5. Click **APPLY** to save the changes or **CANCEL** to cancel the action.

Enabling or Disabling Wireless Networks

This section contains the procedure for enabling or disabling wireless networks. When a wireless network is disabled, the access points of the location stop forwarding its traffic. You might disable a wireless network for security purposes or when performing network maintenance. The default setting for wireless networks is enabled.

To enable or disable a wireless network, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Wireless Networks -> network name
of the network you want to enable or disable. You can edit only one network at a time. For an example, refer to Figure 96 on page 155.

The program displays the configuration screen for the wireless network. For an example, refer to Figure 92 on page 149.

3. If it is not already expanded, click **Network Name and Authentication** to display its parameters.
4. In the Network Name and Authentication section, click either the **Enable** or **Disable** dialog circle for the Status parameter.

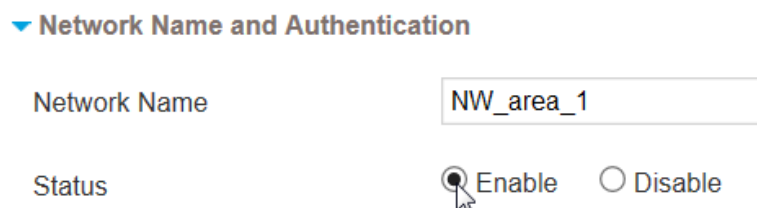


Figure 101. Enabling or Disabling a Wireless Network

5. Click **APPLY** to save the changes or **CANCEL** to cancel the action.

Note

Wireless access points immediately stop forwarding traffic of disabled networks.

Deleting Wireless Networks

This section contains the procedure for deleting wireless networks from your account. Deleting wireless networks that have captive portals or usage plans does not delete the portals or plans. They remain in your account.

To delete a wireless network, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Wireless Networks -> wireless network
of the network you want to delete. You can delete only one network at a time. For an example, refer to Figure 96 on page 155.
3. Select **Delete This Wireless Network** from the Choose Action menu in the upper left corner:



Figure 102. Delete This Wireless Network Selection in the Choose Action Menu

The program displays a confirmation prompt.

4. Click **YES** to delete the wireless network or **NO** to cancel the action.

If you click Yes, the network is deleted from the program.

Chapter 9

Wireless Networks with Captive Portals

This chapter includes the following sections:

- ❑ “Introduction to Captive Portals” on page 168
- ❑ “Viewing Captive Portals” on page 170
- ❑ “Captive Portals with Basic Splash Windows” on page 172
- ❑ “Captive Portals with Advanced Splash Windows” on page 183
- ❑ “Editing Captive Portals” on page 191
- ❑ “Adding Captive Portals to Wireless Networks” on page 193
- ❑ “Removing Captive Portals from Wireless Networks” on page 195
- ❑ “Deleting Captive Portals from Your Account” on page 197

Introduction to Captive Portals

Captive portals are the introductory windows that clients see when connecting to wireless network hotspots. They usually identify the network owners and may contain terms of use of the sites. They might also require that clients provide information, such as their email addresses, prior to gaining access to networks.

Listed here are the properties and operating characteristics you need to consider when planning for captive portals:

- ❑ **Type of captive portal:** This version of the AlliedView Cloud program supports two types of captive portals. The first is called “Click Through.” Wireless clients who connect to a network with this type of captive portal only have to click on a Continue button in the introductory window to access a network. The other type is called “Click Through with Email.” Clients who access networks with this type of portal have to enter their email addresses to gain access.
- ❑ **Type of splash window:** The splash window refers to the introductory window clients see when accessing a wireless network through a captive portal. There are two types of splash windows, basic and advanced. The basic version has only one introductory window while the advanced version has four windows.
- ❑ **Usage plan:** You can add usage plans to captive portals to limit the amount of time clients can access your network hotspots. For example, you might add a usage plan that limits access to a hotspot by clients to two hours a day and only during regular business hours. For further information, refer to Chapter 13, “Usage Plans” on page 241.
- ❑ **Redirect to a web page:** Captive portals can redirect wireless clients to a specific web page.
- ❑ **End-user license agreement (EULA):** Captive portals can contain end-user license agreements, also referred to as terms of use agreements.

Note

Adding a captive portal to a wireless network automatically activates client isolation. Wireless clients on networks with captive portals cannot communicate directly with each. However, they can communicate with clients in other networks and with the wired LAN.

A network hotspot consists of the following components:

- ❑ Wireless network
- ❑ Captive portal

❑ Usage plan (optional)

You can add hotspots to your AlliedView Cloud account a couple ways. One way is to add the components individually. You can add them in any order. A wireless network automatically becomes a hotspot as soon as you add a captive portal to it.

The other way is by performing the instructions in Chapter 10, “Wireless Network Hotspots” on page 199. The chapter explains how to add the three components all at the same time. The instructions have you add a wireless network to a location, then a captive portal to the network, and finally a usage plan.

You can also combine the two methods. For instance, you might add the captive portal and usage plan separately and then use the instructions in the hotspot chapter to add them to a new wireless network.

The two methods have one important difference. Adding the components individually works whether you are adding a new wireless network hotspot to a location or changing an existing network to a hotspot. The instructions in Chapter 10, “Wireless Network Hotspots” on page 199, however, add a new wireless network as the hotspot. Consequently, you should use those instructions only when you want to add new wireless networks to locations and designate them as hotspots. You cannot use the instructions to convert existing wireless networks into hotspots.

Viewing Captive Portals

To view or change the settings of a captive portal, use the Captive Portal Profiles selection in the Shared Settings menu in the Configuration window. To view captive portal profiles, do the following:

1. Click the **Configuration** tab.
2. Select **Captive Portal Profiles** from the Shared Settings menu in the left margin:

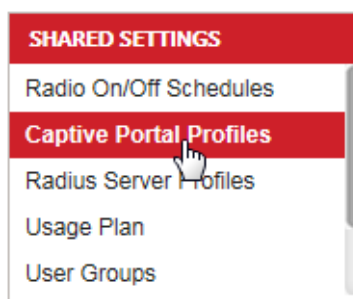


Figure 103. Captive Portal Profiles Selection in the Shared Settings Menu

The program displays a list of the names of the current captive portal profiles in the main part of the window.

3. To view the configuration settings of a captive portal, click its name. You can view only one captive portal at a time.

The captive portal profile is displayed in the main section of the window.

To learn which captive portal is currently assigned to a wireless network, use the Locations menu and select the network. Networks with captive portals are easy to identify in the menu because they have the symbol in Figure 104.



Figure 104. Wireless Network with Captive Portal Icon

To determine which captive portal is assigned to a wireless network, do the following:

1. Click the **Configuration** tab.

- In the Locations menu in the left column, click:
location name -> Wireless Networks -> network name
 of the wireless network with the captive portal you want to view. This example selects the WN_area_1 network in the Warehouse - TL location.

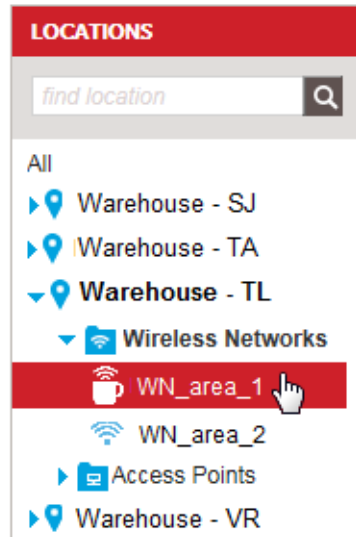


Figure 105. Selecting a Wireless Network with a Captive Portal in the Locations Menu

The network profile is displayed in the main section of the window.

- Click **Captive Portal** to expand the section.

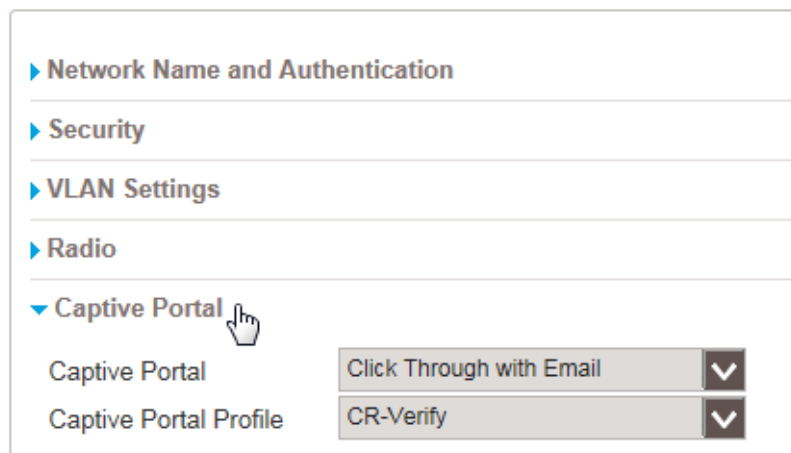


Figure 106. Captive Portal Section in a Wireless Network Configuration

The Captive Portal Profile field displays the name of the captive portal currently assigned to the wireless network.

Captive Portals with Basic Splash Windows

This section contains background information on captival portals with basic splash windows and instructions on how to add them to your account. For instructions on how to add captival portals to wireless networks, refer to “Adding Captive Portals to Wireless Networks” on page 193.

Introduction to Captive Portals with Basic Splash Windows

Your account comes with two default basic splash windows, one for each type of authentication. The default window for Click Through with Email authentication is shown in Figure 107. The figure identifies the adjustable items in the window. The default window for Click Through authentication looks the same, except it does not have a field for entering an email address. You can use the default windows the way they are or you can customize them for your company or organization.

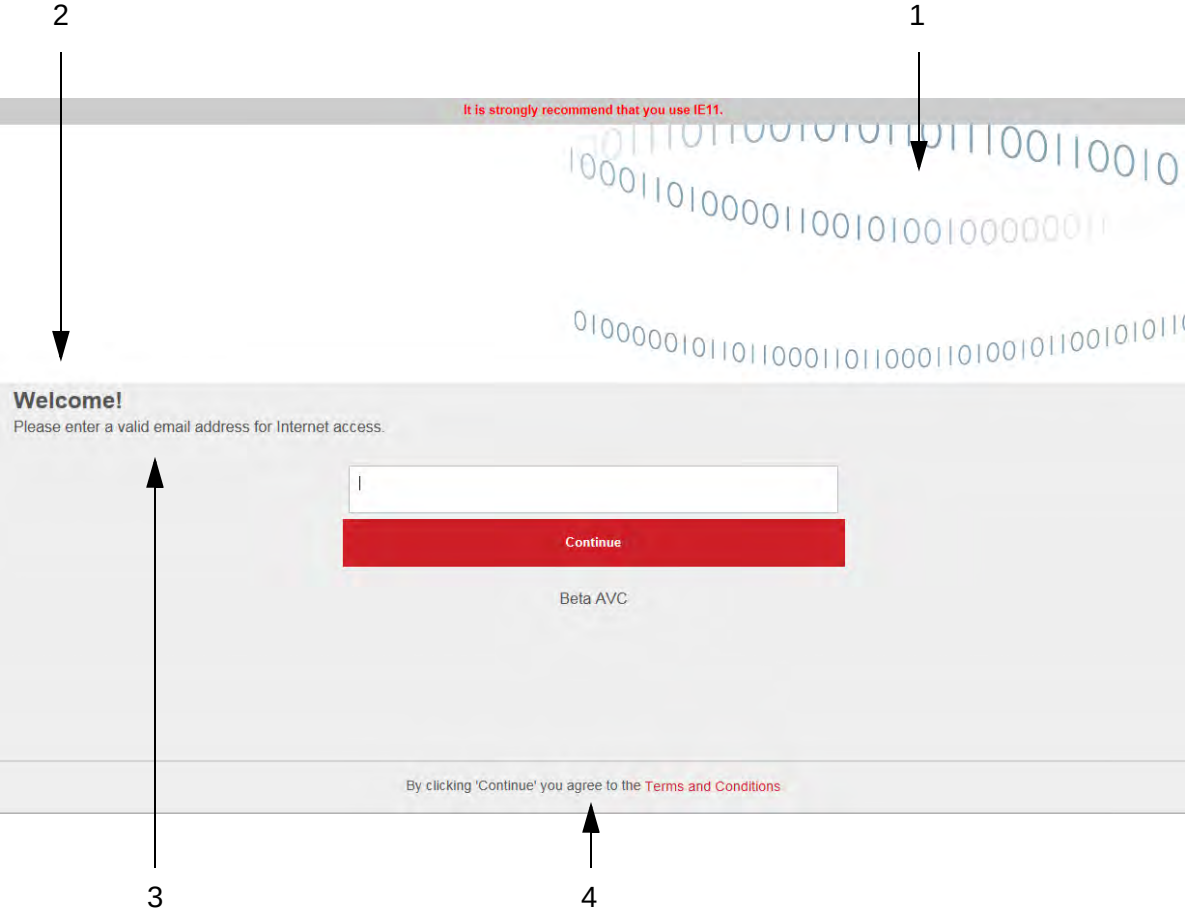


Figure 107. Adjustable Items in the Default Basic Splash Window

The adjustable items in the splash window are defined in Table 15 on page 173.

Table 15. Adjustable Items in the Basic Splash Window

Text	Description
1	This is a background image. You can use the default image or replace it with one of your own. The basic splash window can have only one background image. Here are the image requirements: - Maximum image size is 640 pixels wide by 300 pixels high. - Supported file formats are PNG, GIF, JPEG, JPG, and BMP. - Maximum file size is 10 MB. You can control the alignment of the image in the splash window as left, center, or right. The default is right.
2	This is the header title for the splash window. The default is "Welcome!".
3	This is introductory text. The default text depends on the authentication method.
4	Your splash window can include an end-user license agreement (EULA). Your account has a default agreement you can edit or replace. This prompt is not included in the splash window if you choose not to include an EULA.

After adding a basic splash window, perform "Adding Captive Portals to Wireless Networks" on page 193 to assign it to a wireless network.

Adding Captive Portals with Basic Splash Windows

This section contains instructions on how to add a new captive portal with a basic splash window to your account. For background information, refer to "Introduction to Captive Portals with Basic Splash Windows" on page 172.

To add a captive portal with a basic splash window to your account, do the following:

1. Click the **Configuration** tab.
2. If it is not already selected, select **All** in the Locations menu in the left column.

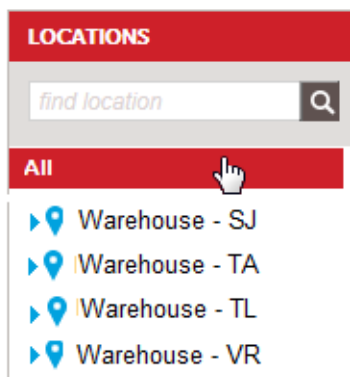


Figure 108. All Selection in the Locations Menu

3. Select **Add Captive Portal Profile** in the Choose Action menu:

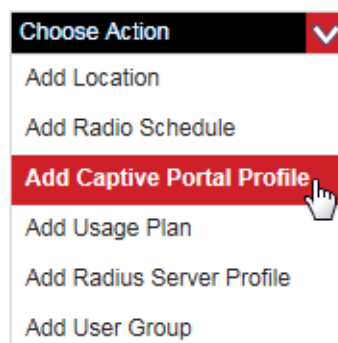


Figure 109. Add Captive Portal Profile Selection in the Choose Action Menu

The program displays the Add Captive Portal Profile window:

Add Captive Portal Profile



Profile Name

Authentication ▼

Usage Plan ▼

Client separation will be enabled on this network.

☐ Redirect users to a specified website after login

CANCEL

NEXT

Figure 110. Add Captive Portal Profile Window

- Fill in the fields. The fields are defined in Table 16.

Table 16. Add Captive Portal Profile Window

Parameter	Description
Profile Name	Enter a name for the captive portal profile.
Authentication	Select the authentication for the profile. The choices are listed here: - Click Through: Wireless clients can click through the captive portal without any authentication. - Click Through With Email: Wireless clients must provide email addresses before clicking through.
Usage Plan	Select a usage plan for the captive portal from the pull-down menu. Setting a usage plan is optional. A captive portal can have only one usage plan. If you do not want the captive portal to have a usage plan, select No Policy, the default. For further information, refer to Chapter 13, "Usage Plans" on page 241.

Table 16. Add Captive Portal Profile Window (Continued)

Parameter	Description
Redirect users to a specified website after login	Specify whether wireless clients are to be redirected to a specific web site after accessing the captive portal. The options are listed here: - No check mark: The wireless clients are not redirected to a specific web site. This is the default. - Check mark: Clients are redirected to a specific website. Type the website address in the field that the program displays when the box is checked. You can enter only one web site address.

5. After filling in the profile, click **NEXT**.

The program displays a window for configuring the splash window:

Add Captive Portal Profile

1 Add Captive Portal Profile
 2 Customize CP Profile

☒ Basic
 ☐ Advanced

RESET
PREVIEW

Image

Header

Text

EULA



Maximum image size is 640px wide by 300px tall.
 Accepted image formats are PNG, GIF, JPEG, JPG and BMP.
 Max image size is 10 MB.

Alignment ☐ left ☐ center ☒ right
 UPLOAD

Header

Welcomel

Text

Please click Continue for free Internet access.

EULA

☒ On ☐ Off

This usage agreement governs your use of the Internet services provided. The use of this hotspot is voluntarily given and may be rescinded without advanced notice. The user is not entitled to any compensation for damages, real or imagined, incurred while using the hotspot.

The user agrees not to:

- 1) Transmit or participate in the transmission of materials in violation of local or national laws and regulations.
- 2) Send large quantities of unsolicited email (spam).
- 3) Restrict or hinder the free usage of this hotspot by other users
- 4) Attack another user, website or service provider with a denial of service attack or otherwise.
- 5) Invade the privacy of anyone on the network regardless of motivation
- 6) Resell access to this hotspot
- 7) Defraud the provider of any due payment for services and access rendered

No technical support is given by the hotspot provider.

CANCEL
ADD WITH BASIC MODE

Figure 111. Add Captive Portal Profile for a Basic Splash Window

6. If it is not selected already, click the **Basic** dialog circle in the top left corner of the window to select basic splash window.
7. Configure the settings in the window. Refer to Table 17 on page 178.

Table 17. Add Captive Portal Profile for a Basic Splash Window

Parameter	Description
Basic - Advanced	Specify the type of splash window. The selections are listed here: - Basic: Add a basic splash window. This is the default setting. This procedure is for adding a basic splash window; so be sure this option is selected. - Advanced: Add an advanced splash window. For instructions, refer to “Captive Portals with Advanced Splash Windows” on page 183.
Image	Displays the background image for the splash window.
Alignment	Specify the alignment of the background artwork at the top of the splash window. The options are listed here: - Left: Align the artwork with the left edge of the window. - Center: Align the artwork in the center of the window. - Right: Align the artwork with the right edge of the window.

Table 17. Add Captive Portal Profile for a Basic Splash Window

Parameter	Description
UPLOAD button	Use this button to replace the current splash artwork with your own artwork. To add your own artwork, click the Browse button, and, when prompt, locate the file on your computer or network server, and then click Open. The program displays the artwork in the Upload Image window. For instructions on how to use the window, refer to “Adjusting Artwork in the Image Upload Window” on page 180. The guidelines for the image are listed here: - Maximum image size is 640 pixels wide by 300 pixels high. - Accepted file formats are PNG, GIF, JPEG, JPG, and BMP. - Maximum file size is 10 MB.
Header	Enter a header title for the splash window. The default is “Welcome!”.
Text	Enter the body text for the splash window. The default text changes depending on the authentication method selected in step 4.
EULA	Enable or disable the end-user license agreement with the On or Off options, respectively. If you choose to include the EULA in the splash window, edit or replace the default end-user license agreement.
RESET button	Use this button if you want to return the settings in the window to their default values.
PREVIEW button	Use this button to preview your splash window.

- If you replaced the default artwork with custom art and want to preview it in the captive portal window, click the **PREVIEW** button.

9. When you are satisfied with the window, click **ADD WITH BASIC MODE** to add the captive portal to your account or **CANCEL** to cancel the procedure.

The captive portal is added to your account. Its name, authentication method, and other information are displayed in a window similar to Figure 112.

Captive Portal Profile: area 2a

CUSTOMIZE
CANCEL
SAVE

Profile Name

Authentication ▼

Usage Plan ▼

Client separation will be enabled on this network.

☐ Redirect users to a specified website after login

Figure 112. Completion of a Captive Portal with a Basic Splash Window

10. Do one of the following:

- ☐ To add the captive portal to a wireless network, go to “Adding Captive Portals to Wireless Networks” on page 193.
- ☐ To modify the captive portal you just added, click the **CUSTOMIZE** button and return to step 7.
- ☐ To add another captive portal with a basic splash window to your account, repeat this procedure.

Adjusting Artwork in the Image Upload Window

This section explains how to use the Image Upload window to replace the default artwork file for the basic splash window with your own artwork. The window is displayed after you click the Upload button and select your artwork file. An example of the window is shown in Figure 113.

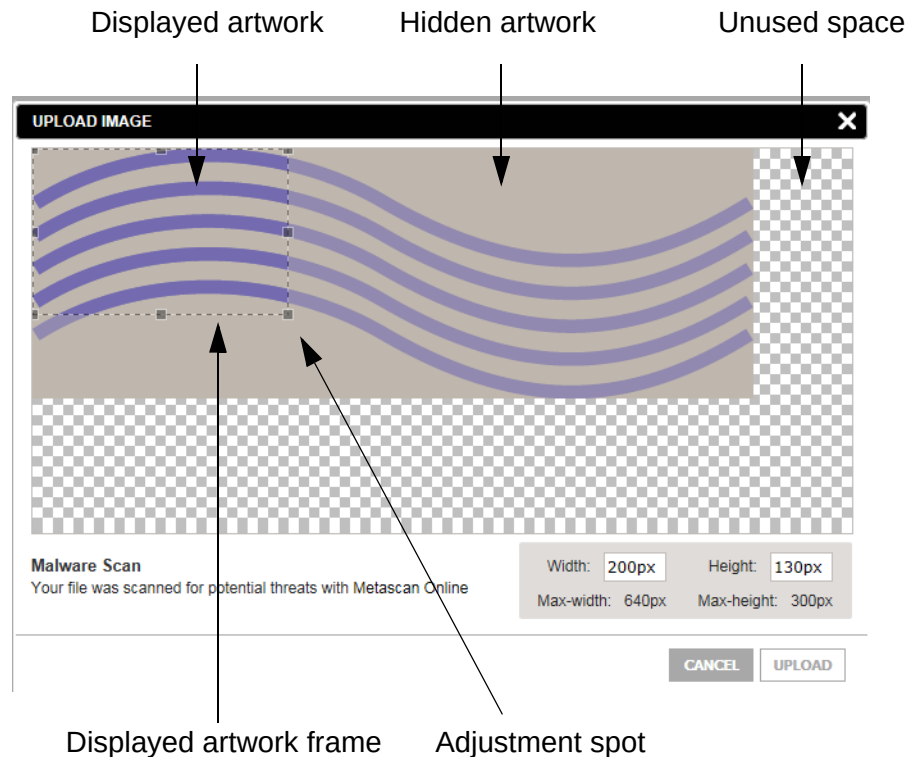


Figure 113. Upload Image Window

Please review the following about the window:

- ❑ If the window is displaying only part of your artwork, the artwork is too large. To include the whole image, reduce its size with your artwork program and upload it again.
- ❑ If there is unused space, you can make the image larger with your artwork program and then upload it again.
- ❑ You can use the window to designate the amount of artwork to include in the splash window. You can designate all or part of it. This is controlled with the displayed artwork frame. Artwork within the frame is displayed in the splash window while artwork outside it is hidden.
- ❑ The displayed artwork frame has a default value of 200 pixels wide by 130 pixels high. To adjust the frame to include more or less of the artwork in the splash window, place the cursor over one of the adjustment spots and drag the frame to resize it, as needed. (You cannot adjust the frame by entering new numbers in the Width and Height fields in the bottom right corner of the window.)
- ❑ When you are satisfied with the artwork, click the Upload button in the Image Upload window to add it to the Add Captive Portal Profile window. Figure 114 is an example of the Add Captive Portal Profile window with custom artwork.

- ❑ When you are satisfied with the artwork, return to step 7 in the previous procedure.

Add Captive Portal Profile

1

Add Captive Portal Profile

2

Customize CP Profile

☒ Basic

☐ Advanced

Image

Header

Text



Maximum image size is 640px wide by 300px tall.

Accepted image formats are PNG, GIF, JPEG, JPG and BMP.

Max image size is 10 MB.

Alignment ☐ left ☐ center ☒ right

UPLOAD

Welcome!

Please click Continue for free Internet access.

CANCEL

ADD WITH BASIC MODE

Figure 114. Example of the Add Captive Portal Profile Window with Custom Artwork

Captive Portals with Advanced Splash Windows

This section contains background information on captive portals with advanced splash windows and instructions on how to add them to your account. For instructions on how to add captive portals to wireless networks, refer to “Adding Captive Portals to Wireless Networks” on page 193.

Introduction to Captive Portal Profiles with Advanced Splash Windows

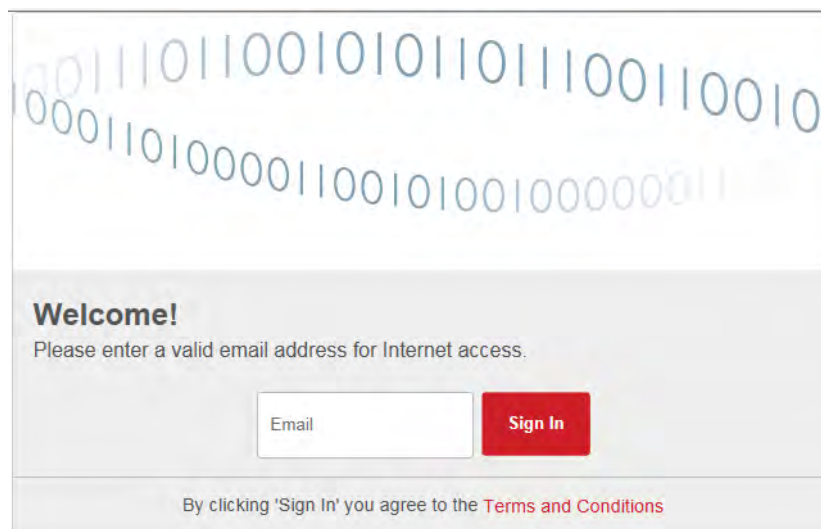
Captive portals are introductory windows to your wireless networks. The windows, which clients see when they first connect to a network, typically identify the network owners and may contain other information.

There are two types of captive portals, basic and advanced. The main difference between them is the number of windows that wireless clients see when they connect to your networks. As explained in “Captive Portals with Basic Splash Windows” on page 172, a basic splash window has only one window. In comparison, advanced splash windows have the four windows listed here:

- ☐ Login
- ☐ End-user license agreement
- ☐ Successful login
- ☐ Error

Your account has advanced splash window templates you can download and use to build your own windows. There are two sets of templates, one for each authentication method. There is one set for Click Through authentication and another for Click Through with Email authentication.

Figure 115 on page 184 illustrates the default login window. This is the first window wireless clients see when they connect to a wireless network that has an captive portal with advanced splash windows. The window in the figure is for Click Through with Email authentication. The window for Click Through authentication does not have the field for an email address and the button says Continue.

A login window with a decorative header of binary code. The main content area has a light gray background and contains the text "Welcome!" followed by "Please enter a valid email address for Internet access." Below this is a white text input field labeled "Email" and a red "Sign In" button. At the bottom, a thin gray bar contains the text "By clicking 'Sign In' you agree to the [Terms and Conditions](#)".

Welcome!

Please enter a valid email address for Internet access.

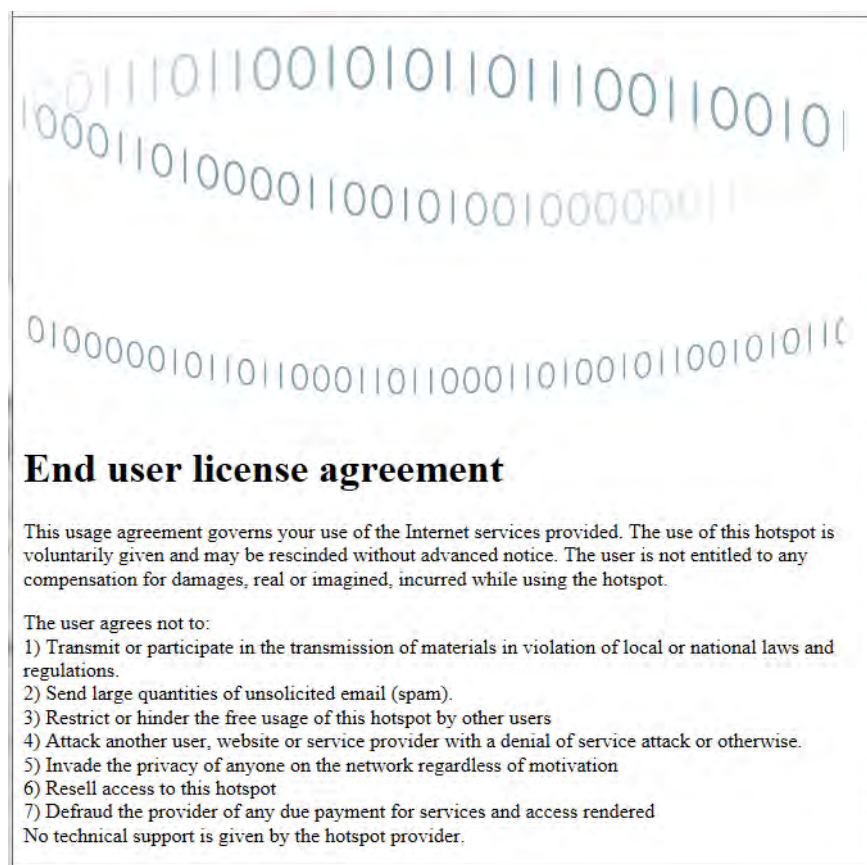
Email

Sign In

By clicking 'Sign In' you agree to the [Terms and Conditions](#)

Figure 115. Login Window

Clients who click on the Terms and Conditions link at the bottom of the login window see the end-user license agreement. The default window is shown Figure 116.

A window titled "End user license agreement" with a decorative header of binary code. The text explains that the usage agreement governs the use of Internet services and that the use is voluntarily given. It lists seven items the user agrees not to do: 1) Transmit or participate in the transmission of materials in violation of local or national laws and regulations, 2) Send large quantities of unsolicited email (spam), 3) Restrict or hinder the free usage of this hotspot by other users, 4) Attack another user, website or service provider with a denial of service attack or otherwise, 5) Invade the privacy of anyone on the network regardless of motivation, 6) Resell access to this hotspot, and 7) Defraud the provider of any due payment for services and access rendered. It concludes with "No technical support is given by the hotspot provider."

End user license agreement

This usage agreement governs your use of the Internet services provided. The use of this hotspot is voluntarily given and may be rescinded without advanced notice. The user is not entitled to any compensation for damages, real or imagined, incurred while using the hotspot.

The user agrees not to:

- 1) Transmit or participate in the transmission of materials in violation of local or national laws and regulations.
- 2) Send large quantities of unsolicited email (spam).
- 3) Restrict or hinder the free usage of this hotspot by other users
- 4) Attack another user, website or service provider with a denial of service attack or otherwise.
- 5) Invade the privacy of anyone on the network regardless of motivation
- 6) Resell access to this hotspot
- 7) Defraud the provider of any due payment for services and access rendered

No technical support is given by the hotspot provider.

Figure 116. End-user License Agreement Window

When clients click the Continue button in the login window, they see the successful login window, shown in Figure 117.

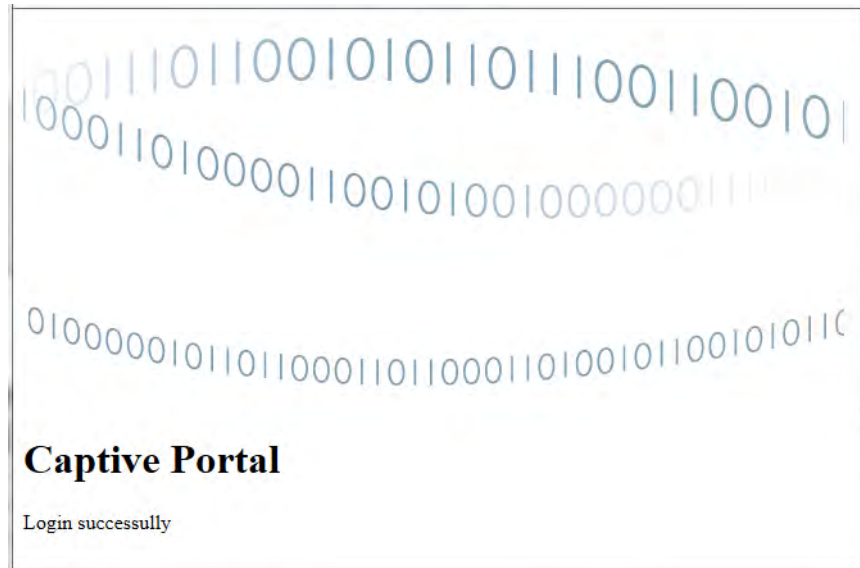


Figure 117. Successful Login Window

The error window in Figure 118 is displayed for wireless clients who are denied access to your networks.

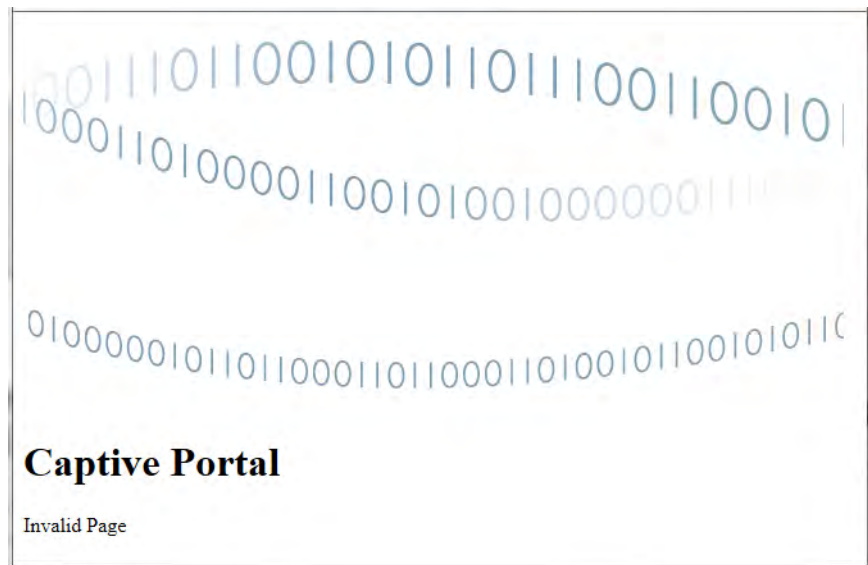


Figure 118. Error Window

Guidelines to Modifying the Advanced Splash Windows

Here are the guidelines to modifying the template files for the advanced splash windows:

- ☐ You cannot have more than four splash windows.
- ☐ You can have only one artwork file for the windows.

- ❑ The artwork file must be in PNG format.
- ❑ The artwork filename must be “default.png”. The characters must be lowercase.
- ❑ You must not change the filenames of the splash windows. The window and filenames are listed in Table 18. The filename must be lowercase.

Table 18. Filenames for Advanced Splash Windows

Window	Filename
Login window	login.html
End-use license agreement	eula.html
Successful login	success.html
Error	error.html

- ❑ If you do not want the end-user license agreement window, remove the terms and conditions line from the bottom of the login window when you edit its HTML file.

Note

Allied Telesis recommends changing only the artwork and text in the HTML files. The windows might not function properly if you change the cascading style sheet or the format of the HTML files or tags

Adding a Captive Portal with Advanced Splash Windows

This section contains instructions on how to add a new captive portal with advanced splash windows to your account. You can perform this procedure whether or not you have already modified the window templates. The procedure includes instructions on how to download the templates to your computer so that you can modify them. For background information, refer to “Introduction to Captive Portal Profiles with Advanced Splash Windows” on page 183.

To add a new captive for advanced splash windows, do the following:

1. Click the **Configuration** tab.
2. If it is not already selected, select **All** in the Locations menu in the left column. Refer to Figure 108 on page 174.
3. Select **Add Captive Portal Profile** from the Choose Action menu (see Figure 109 on page 174).

The program displays the Add Captive Portal Profile window. Refer to Figure 110 on page 175.

4. Fill in the fields in the Add Captive Portal Profile window. The fields are defined in Table 16 on page 175.
5. Click **NEXT**.

The program displays the Add Captive Portal Profile window for a basic splash screen. Refer to Figure 111 on page 177.

6. Click the **Advanced** dialog circle.

Add Captive Portal Profile

The screenshot shows the 'Add Captive Portal Profile' window. At the top right, a progress bar indicates two steps: 1. Add Captive Portal Profile (current) and 2. Customize CP Profile. Below the title bar, there are two radio buttons: 'Basic' and 'Advanced'. The 'Advanced' radio button is selected, and a mouse cursor is pointing at it. Below the radio buttons, there is a text prompt: 'Use these templates to customize your own pages.' To the right of this prompt are two buttons: 'DOWNLOAD TEMPLATES' and 'UPLOAD FILE'. The main content area is divided into three sections: 'Image', 'HTML', and 'CSS'. The 'Image' section shows 'default.png'. The 'HTML' section lists four files: 'login.html', 'error.html', 'success.html', and 'eula.html', each with a 'PREVIEW' button to its right. The 'CSS' section is currently empty. At the bottom of the window, there are two buttons: 'CANCEL' and 'ADD WITH ADVANCED MODE'.

Figure 119. Add Captive Portal Profile Window for Advanced Splash Windows

7. Do one of the following:
 - ☐ If you need to download the advanced splash window templates so that you can modify them, continue with the next step.
 - ☐ If you already modified the window templates and are ready to upload them to your new captive portal, go to “Uploading Advanced Splash Windows to a Captive Portal” on page 188 and start with step 5.
8. Click the **DOWNLOAD TEMPLATES** button.

Note

The DOWNLOAD TEMPLATES button does not work after you have uploaded one or more files to a captive portal. The button only works before files are uploaded.

9. When prompted, save the zip file with the HTML templates to a folder on your computer or a network server.

Your account has templates for Click Through authentication and Click Through with Email authentication. The template downloaded to your computer depends on the authentication method you selected in the Add Captive Portal Profile window, in step 4.

The filenames of the zip files are listed here:

- ☐ Click Through - cp_template_click_through.zip
- ☐ Click Through with Email - cp_template_click_through_email.zip

10. Click the **ADD WITH ADVANCED MODE** button to add the new captive portal to your account or the **CANCEL** button to cancel the procedure

The profile is displayed in the Configuration area.

11. After modifying the splash window templates, perform “Uploading Advanced Splash Windows to a Captive Portal” on page 188 to add them to the captive portal.

Uploading Advanced Splash Windows to a Captive Portal

Please review the following guidelines before uploading advanced splash windows to a captive portal:

- ☐ You have to upload the files one at a time. Do not upload the files in a zip file.
- ☐ The filename of the artwork file must be default.png.
- ☐ The correct filenames for the HTML files are listed in Table 18 on page 186.

When you are finished modifying the templates for advanced splash windows and are ready to upload them to a captive portal, do the following:

1. Click the **Configuration** tab.
2. Select **Captive Portal Profiles** in the Shared Settings menu in the lower left column. Refer to Figure 103 on page 170.

The program displays a list of the names of the current captive portal profiles in the main part of the window.

3. Click the name of the captive portal for the advanced splash windows. You can select only one captive portal.

The window displays the first profile page of the selected captive portal. An example is shown in Figure 112 on page 180.

4. Click the **CUSTOMIZE** button.

The window displays the second profile page of the selected captive portal. An example is shown in Figure 119 on page 187.

5. Click the **UPLOAD** button.
6. When prompted, select the artwork or HTML template file you want to upload from your computer or network server to the captive portal. You can upload only one file at a time.

The program displays the warning prompt in Figure 120.

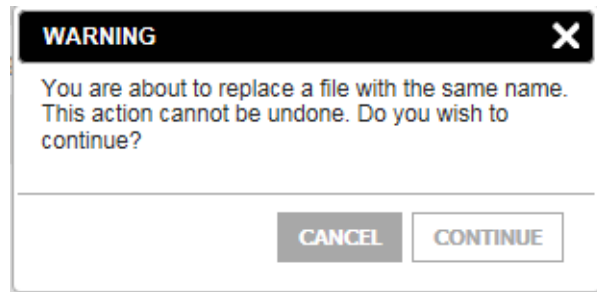


Figure 120. Warning Prompt

7. Click the **Continue** button.

The file is uploaded to the captive portal. A check mark and date are added to the file in the window.

8. To preview a modified window, click the corresponding **PREVIEW** button.
9. Repeat steps 5 to 8 to upload additional files.

An example of the window with three uploaded files is shown in Figure 121 on page 190.

Captive Portal Profile: tech pubs cp1

BACK CANCEL DELETE **SAVE**

☐ Basic ☒ Advanced

Use these templates to customize your own pages. **DOWNLOAD TEMPLATES** **UPLOAD FILE**

Image			
default.png	12/07/2016		✓

HTML			
login.html	12/07/2016	PREVIEW	✓
error.html		PREVIEW	
success.html	12/07/2016	PREVIEW	✓
eula.html		PREVIEW	

CSS			
style.css			

Figure 121. Example of the Captive Portal Profile Window with Uploaded Files

10. After uploading the files, click the **SAVE** button.

Note

The **DOWNLOAD TEMPLATES** button is deactivated after you update one or more files to a captive portal.

Editing Captive Portals

To edit a captive portal, do the following:

1. Click the **Configuration** tab.
2. Select **Captive Portal Profiles** from the Shared Settings menu in the left margin: Refer to Figure 103 on page 170.

The program displays a list of the names of the current captive portal profiles in the main part of the screen.

3. Click the name of the profile you want to edit. You can edit only one captive portal at a time.

The program displays the first window of the captive portal profile. Figure 122 shows an example of a captive portal profile with Click Through authentication.

Captive Portal Profile: CP-Warehouse

CUSTOMIZE **CANCEL** **SAVE**

Profile Name

Authentication ▼

Usage Plan ▼

Client separation will be enabled on this network.

☐ Redirect users to a specified website after login

Figure 122. Edit Captive Portal Profile

4. Edit parameters as needed.
5. Click the **SAVE** button if you make changes to this window.
6. To change the basic or advanced splash windows, click the **CUSTOMIZE** button.
 - ❑ For instructions on modifying a basic splash window, refer to Table 17 on page 178 in “Adding Captive Portals with Basic Splash Windows” on page 173.
 - ❑ For instructions on modifying a captive portal with advanced splash windows, refer to “Uploading Advanced Splash Windows to a Captive Portal” on page 188.

7. Click the **SAVE** button to implement your changes or the **CANCEL** button to cancel the action.

Adding Captive Portals to Wireless Networks

This procedure explains how to add captive portals to wireless networks. Networks with captive portals function as network hotspots for wireless clients. The procedure assumes you have already added the captive portals to your account. If you have not added the captive portals, refer “Captive Portals with Basic Splash Windows” on page 172 or “Captive Portals with Advanced Splash Windows” on page 183 for instructions. You can assign a captive portal to more than one wireless network.

To add a captive portal to a wireless network, do the following:

1. Click the **Configuration** tab.
2. In the Location column in the left column, click:
location name -> Wireless Networks -> network name
of the wireless network where you want to add the captive portal. You can add a captive portal to only one network at a time. This example selects the WN_area_1 network in the Warehouse - TL location.

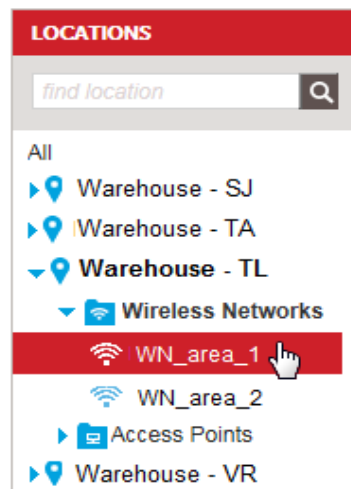


Figure 123. Selecting a Wireless Network

The program displays the wireless network configuration screen. For an example, refer to Figure 92 on page 149.

3. Click **Captive Portal** in the wireless network configuration screen to expand the section.

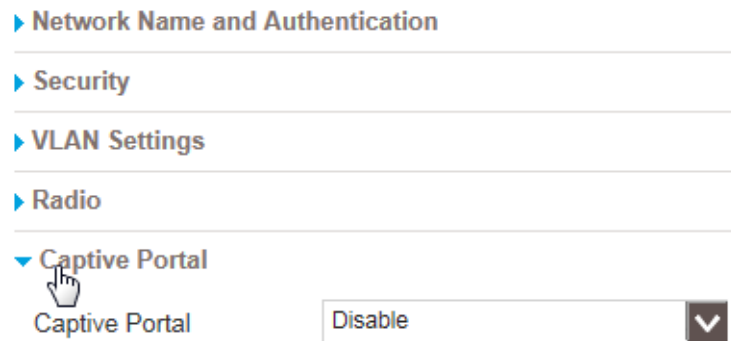


Figure 124. Expanding the Captive Portal Configuration Area

- Using the Captive Portal pull-down menu, select the desired type of captive portal for the wireless network. The options are **Click Through** and **Click Through with Email**. The default setting is Disable.

The program adds the Captive Portal Profile pull-down menu to the section.

- Select the desired captive portal from the Captive Portal Profile pull-down menu. You can select only one profile.

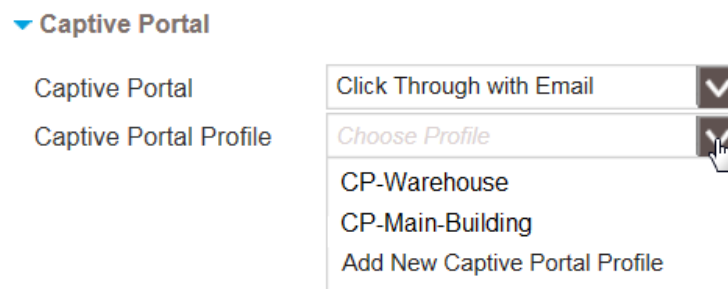


Figure 125. Selecting Captive Portal Profile

Note

The Add New Captive Portal Profile selection in the pull-down menu is used to add new captive portals to your account. For instructions, refer to “Captive Portals with Basic Splash Windows” on page 172 or “Captive Portals with Advanced Splash Windows” on page 183.

- Click **APPLY** to add the captive portal to the wireless network or **CANCEL** to cancel the action.

A wireless network begins to function as a hotspot as soon as you add a captive portal to it. Wireless clients who connect to it see the introductory windows in the captive portal on their screens.

Removing Captive Portals from Wireless Networks

This section contains the procedure for removing captive portals from wireless networks. Please review the following information before performing the procedure:

- ❑ A wireless network stops functioning as a hotspot when you remove its captive portal.
- ❑ Captive portals removed from all their wireless networks remain in your account so that you can assign them to other networks. If you want to delete a captive portal from your account, refer to “Deleting Captive Portals from Your Account” on page 197.

To remove a captive portal from a wireless network, do the following:

1. Click the **Configuration** tab.
2. In the Locations column in the left column, click:
location name -> Wireless Networks -> network name
of the wireless network whose captive portal you want to remove. You can remove a captive portal from only one network at a time. For an example, refer to Figure 123 on page 193. (Wireless networks with captive portals are identified with the icon in Figure 104 on page 170.)

The program displays the wireless network configuration screen. For an example, refer to Figure 92 on page 149.

3. Click **Captive Portal** in the wireless network configuration screen to expand the section. For an example, refer to Figure 106 on page 171.
4. From the Captive Portal pull-down menu, select **Disable**.

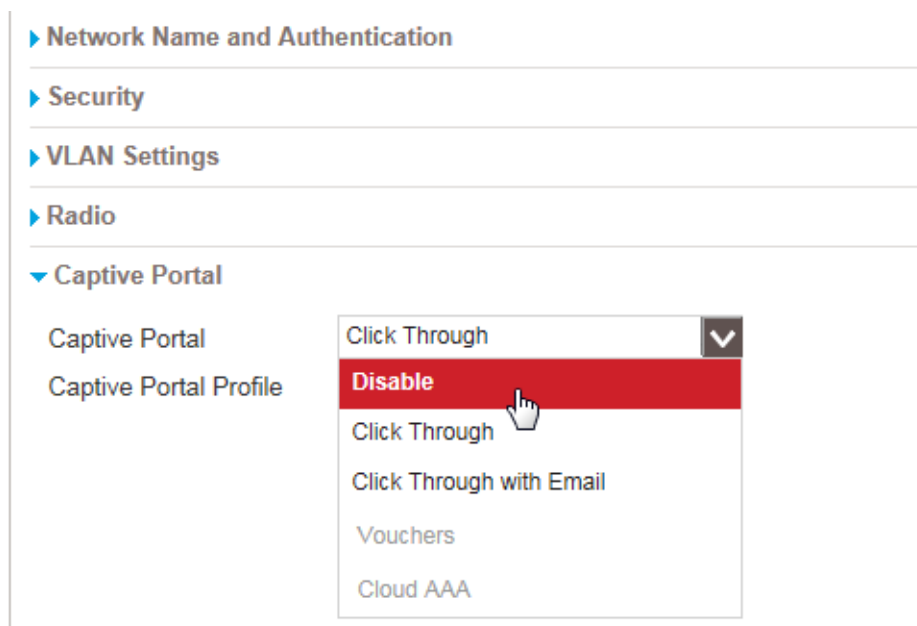


Figure 126. Disable Selection in the Captive Portal Pull-down Menu

5. Click **APPLY** to remove the captive portal from the network or **CANCEL** to cancel the action.

Deleting Captive Portals from Your Account

This section contains the procedure for deleting captive portals from your account.

Note

You cannot delete captive portals that are assigned to wireless networks. You must remove them from all networks before deleting them. For instructions, refer to “Removing Captive Portals from Wireless Networks” on page 195.

To delete a captive portal from your account, do the following:

1. Click the **Configuration** tab.
2. Select **Captive Portal Profiles** from the Share Settings menu in the lower left corner.

The main section of the window displays the names of the captive portals.

3. Click the name of the captive portal you want to delete. You can delete only one captive portal at a time.

The program displays the captive portal details. For an example, refer to Figure 122 on page 191.

4. Select **Delete This Captive Portal Profile** from the Choose Action menu in the upper right corner:

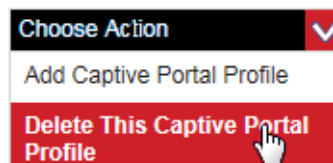


Figure 127. Delete Captive Portal Profile

The program displays a confirmation prompt.

5. Click **YES** to delete the captive portal from your account or **NO** to cancel the action.

Chapter 10

Wireless Network Hotspots

This chapter contains instructions on how to manage wireless network hotspots. This chapter includes the following sections:

- ❑ “Introduction to Network Hotspots” on page 200
- ❑ “Adding Free-Access Network Hotspots” on page 201
- ❑ “Editing Network Hotspots” on page 210
- ❑ “Deleting Wireless Network Hotspots” on page 211

Introduction to Network Hotspots

You use network hotspots to provide wireless clients with Internet access through your wireless networks. They consist of the following components:

- ❑ Wireless network
- ❑ Captive portal - A wireless network hotspot must have a captive portal. It contains the windows that wireless clients see when they initially access your hotspots. When adding a hotspot, you have the option of using an existing captive portal or building a new one. A wireless network automatically becomes a hotspot as soon as you add a captive portal to it. Please review “Introduction to Captive Portals” on page 168 for background information before adding network hotspots.
- ❑ Usage plan - Network hotspots can have usage plans. By adding a usage plan to a hotspot you can limit the amount of time that wireless clients can access your networks. When adding a hotspot, you have the option of using an existing usage plan or building a new one. Please review “Introduction to Usage Plans” on page 242 for background information. Usage plans for hotspots are optional.

This version of the program supports the following types of network hotspots:

- ❑ Click Through - free access in which users click a Continue button.
- ❑ Click Through with Email - free access in which users enter an email address, then click a Continue button.

You can add hotspots to your AlliedView Cloud account a couple ways. One way is with the instructions in this chapter. They explain how to add the three components all at the same time. You add a wireless network to a location, then a captive portal to the network, and finally a usage plan.

You can also add the components individually to your account. You can add them in any order.

You can also combine the two methods. For instance, you might add the captive portal and usage plan separately and then use the instructions in this chapter to add them to a new wireless network.

The two methods have one important difference. Adding the components individually works whether you are adding a new wireless network hotspot to a location or changing an existing network to a hotspot. The instructions in this chapter, however, create a new wireless network as the hotspot. Consequently, you should use these instructions when you want to add new wireless networks to locations and designate them as hotspots. You cannot use the instructions to convert existing wireless networks into hotspots.

Adding Free-Access Network Hotspots

To add a free-access network hotspot to the access points of a location in your account, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left margin or the locations list in the main part of the screen, click the name of the location for the hotspot. You can assign a network hotspot to only one location. This example selects the Warehouse - TL location.

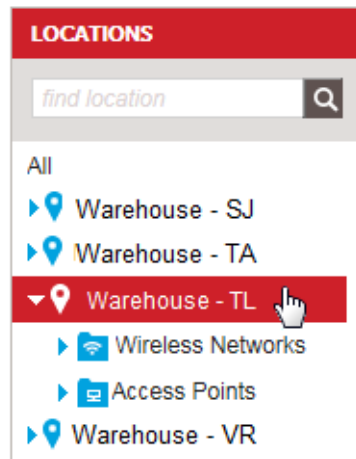


Figure 128. Selecting a Location

Your account displays the details of the location. An example is shown in Figure 39 on page 76.

3. Select **Add Hotspot (Free)** from the Choose Action menu:

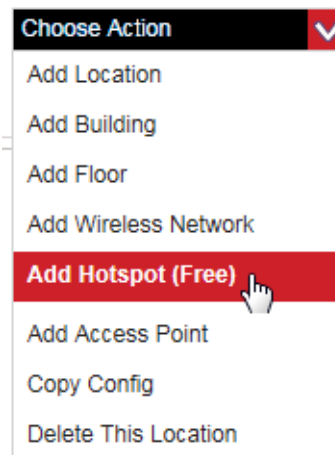


Figure 129. Add Hotspot (Free) Selection in the Choose Action Menu

The program displays the Add Hotspot window:

Add Hotspot

1

Add Hotspot Network

2

Set Access Policy

3

Edit Splash Page

4

Set Usage Plans

Add Hotspot Network

Enter a name for your hotspot and select which radio bands to make this hotspot available. The entered name will be used as the SSID name that users will connect to. This network will be created with OPEN authentication. Please note that you can configure other authentication types by directly editing this wireless network after completing this wizard.

Hotspot Name*

Wireless Network on

2.4GHz and 5GHz

CANCEL

NEXT

Figure 130. Add Hotspot Window

4. Fill in the fields in the window. Refer to Table 19.

Table 19. Add Hotspot - Add Hotspot Network Window

Parameter	Description
Hotspot Name	Enter a name for the new hotspot. The name acts as the service set identifier (SSID) for the network hotspot,
Wireless Network On	Use the Wireless Network on pull-down menu to specify the radios for the hotspot. The default is both 2.4GHz and 5GHz radios.

5. Click **NEXT**.

The program displays the Add Hotspot - Set Access Policy window.

Add Hotspot



Set Access Policy

Set access policy for your hotspot by configuring a Captive Portal Profile. You can either create a new profile, copy from an existing profile or use existing profile.

Captive Portal ☒ Create New ☐ Copy From Existing ☐ Use Existing

Captive Portal Profile

Authentication

Client separation will be enable on this network

☐ Redirect users to a specified website after login

Figure 131. Create New Option in the Add Hotspot - Set Access Policy Window

You use this window to specify the captive portal for the hotspot. A hotspot must have a captive portal. You can add a new captive portal, add a new portal by copying an existing portal, or assign an existing portal to the network hotspot.

6. Do one of the following:
 - ☐ To build a new captive portal for the network hotspot, go to “Adding a New Captive Portal”.
 - ☐ To add a new captive portal for the network hotspot by copying and modifying an existing portal, refer to “Copying a Captive Portal” on page 206.
 - ☐ To assign an existing captive portal to the network hotspot, refer to “Assigning an Existing Captive Portal” on page 209.

Adding a New Captive Portal

To add a new captive portal to your account for the network hotspot, do the following:

1. If it is not already selected, click the **Create New** dialog circle in the Add Hotspot - Set Access Policy window.
2. Configure the window settings. Refer to Table 20 on page 204.

Table 20. Create New Option in the Add Hotspot - Set Access Policy Window

Parameter	Description
Captive Portal Profile	Enter a name for the new captive portal for the hotspot.
Authentication	Specify the authentication method for the wireless clients of the hotspot. The pull-down menu has these selections: - Click Through: Clients can access the hot spot without any authentication, by clicking the Continue button. - Click Through with Email: Clients have to provide email addresses to access the hotspot.
Redirect users to a specified website after login	Specify whether wireless clients are to be redirected to a specific web site after accessing the hotspot. The options are listed here: - No check mark: The wireless clients are not redirected to a specific web site. This is the default. - Check mark: Clients are redirected to a specific website. Type the website address in the field that the program displays when the box is checked. You can enter only one web site address.

3. After editing the window, click **NEXT**.

Your screen displays the Add Hotspot - Edit Splash Page, for adding a new basic or advanced captive portal. The window is functionally identical to the Add Captive Portal Profile in Figure 111 on page 177.

Figure 132. Add Hotspot - Edit Splash Page Window

4. Add a new basic or advanced splash window to your account, for the network hotspot. For directions, refer to “Captive Portals with Basic Splash Windows” on page 172 or “Captive Portals with Advanced Splash Windows” on page 183.
5. After configuring the captive portal for the network hotspot, click **NEXT**.

Your screen displays the Add Hotspot - Set Usage Plan window.

Figure 133. Add Hotspot - Set Usage Plan Window

6. Do one of the following:

- ☐ If you do not want to assign a usage plan to the network hotspot, click the **No** dialog circle. This is the default setting.
- ☐ To add a new usage plan to your account for the network hotspot, click the **Yes** and **Create New** dialog circles. Fill in the displayed fields. For instructions, refer to Table 27 on page 246.
- ☐ To assign the network hotspot a new usage plan based on an existing plan, click the **Yes** and **Copy From Existing** dialog circles. Select the existing plan to be copied and edit the displayed fields. For instructions, refer to Table 27 on page 246.
- ☐ To assign the network hotspot an existing usage plan, click the **Yes** and **Use Existing** dialog circles. Select the existing plan from the pull-down menu.

7. Click **ADD THIS HOTSPOT**.

The new network hotspot is added to the Wireless Network folder of the selected location. The configuration settings of the wireless network are displayed in the main section of the window. The sections are explained in the procedures listed in Table 12 on page 152. The network hotspot is now active on the access points of the location.

Copying a Captive Portal

To add a new captive portal to your account for the network hotspot by copying an existing portal, do the following:

1. Click the **Copy From Existing** dialog circle in the Add Hotspot - Set Access Policy window.

The program displays the window in Figure 134 on page 207.

Add Hotspot



Set Access Policy

Set access policy for your hotspot by configuring a Captive Portal Profile. You can either create a new profile, copy from an existing profile or use existing profile.

Captive Portal ☐ Create New ☒ Copy From Existing ☐ Use Existing

Based on ▼

Captive Portal Profile

Authentication ▼

Client separation will be enable on this network

☐ Redirect users to a specified website after login

BACK

CANCEL

NEXT

Figure 134. Copy From Existing Option in the Add Hotspot - Set Access Policy Window

2. Configure the window settings. Refer to Table 21.

Table 21. Copy From Existing Option in the Add Hotspot - Set Access Policy Window

Parameter	Description
Based On	Use the pull-down menu to select the existing captive portal you want to copy.
Captive Portal Profile	Enter a name for the new captive portal for the hot spot.
Authentication	Specify the authentication method for the wireless clients of the hotspot. The pull-down menu has these selections: - Click Through: Clients can access the hot spot without any authentication, by clicking the Continue button. - Click Through with Email: Clients have to provide email addresses to access the hotspot.

Table 21. Copy From Existing Option in the Add Hotspot - Set Access Policy Window (Continued)

Parameter	Description
Redirect users to a specified website after login	Specify whether wireless clients are to be redirected to a specific web site after accessing the hotspot. The options are listed here: - No check mark: The wireless clients are not redirected to a specific web site. This is the default. - Check mark: Clients are redirected to a specific website. Type the website address in the field that the program displays when the box is checked. You can enter only one web site address.

3. After editing the window, click **NEXT**.

Your screen displays the Add Hotspot - Set Usage Plan window, shown in Figure 133 on page 205. The information in the window varies depending on whether the captive portal you copied has a usage plan.

4. Do one of the following:
- ☐ If you do not want to assign a usage plan to the network hotspot, click the **No** dialog circle. This is the default setting.
 - ☐ To add a new usage plan to your account for the network hotspot, click the **Yes** and **Create New** dialog circles. Fill in the displayed fields. For instructions, refer to Table 27 on page 246.
 - ☐ To assign the network hotspot a new usage plan based on an existing plan, click the **Yes** and **Copy From Existing** dialog circles. Select the existing plan to be copied and edit the displayed fields. For instructions, refer to Table 27 on page 246.
 - ☐ To assign the network hotspot an existing usage plan, click the **Yes** and **Use Existing** dialog circles. Select the existing plan from the pull-down menu.
5. Click **ADD THIS HOTSPOT** to add the new wireless network hotspot or **CANCEL** to cancel the procedure.

The new network hotspot is added to the Wireless Network folder of the selected location. The configuration settings of the wireless network are displayed in the main section of the window. The sections are explained in the procedures listed in Table 12 on page 152. The network hotspot is now active on the access points of the location.

Assigning an Existing Captive Portal

To assign an existing captive portal to the new network hotspot, do the following:

1. Click the **Copy From Existing** dialog circle in the Add Hotspot - Set Access Policy window.

The program displays the window in Figure 135.

Add Hotspot



Set Access Policy

Set access policy for your hotspot by configuring a Captive Portal Profile. You can either create a new profile, copy from an existing profile or use existing profile.

Captive Portal ☐ Create New ☐ Copy From Existing ☒ Use Existing

Use

This Hotspot will use the setting in "CP-Test-AVCupgrade".

Usage Plan will be set to "None".

You cannot edit the web page or usage plan.

BACK
CANCEL
ADD THIS HOTSPOT

Figure 135. Use Existing Option in the Add Hotspot - Set Access Policy Window

2. In the Use pull-down menu, select the existing captive portal you want to assign to the wireless network hotspot.
3. Click **ADD THIS HOTSPOT** to add the new wireless network hotspot or **CANCEL** to cancel the procedure.

The new network hotspot is added to the Wireless Network folder of the selected location. The configuration settings of the wireless network are displayed in the main section of the window. The sections are explained in the procedures listed in Table 12 on page 152. The network hotspot is now active on the access points of the location.

Editing Network Hotspots

A network hotspot consists of a wireless network, captive portal, and an optional usage plan. You have to edit the components separately. The following lists references to editing the components.

- ❑ For instructions on how to edit wireless networks, refer to Chapter 8, “Wireless Networks” on page 147.
- ❑ For instructions on how to edit captive portals, refer to “Editing Captive Portals” on page 191.
- ❑ For instructions on how to edit usage plans, refer to “Editing Usage Plans” on page 248.

Deleting Wireless Network Hotspots

This section contains the procedure for deleting wireless network hotspots from your account. Deleting a network hotspot does not delete its captive portal or usage plan. They remain in your account.

To delete a network hotspot from your account, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left column, click:
location name -> Wireless Networks -> network name
 of the network hotspot you want to delete. You can delete only one network hotspot at a time. This example selects the WN_area_1_hs network in the Warehouse - TL location.

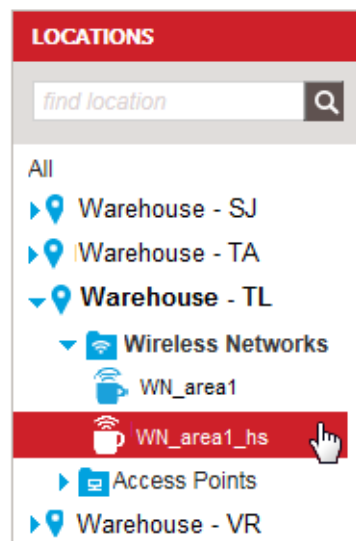


Figure 136. Selecting a Wireless Network

The program displays the configuration screen of the selected network. An example is shown in Figure 92 on page 149.

3. Select **Delete This Wireless Network** from the Choose Action menu in the upper left corner:



Figure 137. Delete This Wireless Network Selection in the Choose Action Menu

The program displays a confirmation prompt.

4. Click **YES** to delete the network hotspot or **NO** to cancel the action.

If you click Yes, the network is deleted from your account.

Chapter 11

Radio Schedules

This chapter contains the following sections:

- ❑ “Introduction to Radio On/Off Schedules” on page 214
- ❑ “Viewing Radio Schedules” on page 215
- ❑ “Adding Radio Schedules” on page 217
- ❑ “Adding Radio Schedules to Locations” on page 220
- ❑ “Removing Radio Schedules from Locations” on page 223
- ❑ “Editing Radio Schedules” on page 224
- ❑ “Deleting Radio Schedules” on page 226

Introduction to Radio On/Off Schedules

You use radio schedules to control the times of operations of the radios in the access points at locations in your wireless networks. Radio schedules are useful in restricting the radios of access points to operate only during certain hours or days of the week. Radios in access points at locations without schedules operate continuously, 24 hours a day and seven days a week.

Here are the guidelines for radio schedules:

- ☐ Radio schedules are applied to location entries in your account and so control all the access points of the networks in a location.
- ☐ A location can have only one radio schedule.
- ☐ You can apply a radio schedule to more than one location.
- ☐ A radio schedule applies to both the 2.4GHz and 5GHz radios in the access points. You cannot assign different schedules to the radios.
- ☐ A schedule cannot specify different hours for different days of the week.

Viewing Radio Schedules

To view the current radio schedules, perform the following procedure:

1. Click the **Configuration** tab.
2. Select **Radio On/Off Schedules** from the SHARED SETTINGS menu:

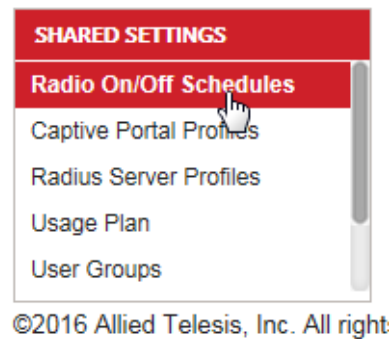


Figure 138. Radio On/Off Schedules Selection

The program displays the Radio On/Off Schedules window.

Radio On/Off Schedules

 A screenshot of the 'Radio On/Off Schedules' window. At the top right is a button labeled 'ADD SCHEDULE'. Below it is a table with the following columns: a checkbox, 'Name', 'On/Off', 'Day', 'Radio On Time', and 'Radio Off Time'. There are two rows of data: 'default' and 'Weekly'. Below the table are two buttons: 'DELETE SELECTED' and 'EDIT SELECTED'.

☐	Name	On/Off	Day	Radio On Time	Radio Off Time
☐	default	On	MTuWThFSaSu	01:00 AM	11:30 PM
☐	Weekly	On	SaSu	06:00 AM	07:00 PM

Figure 139. Radio On/Off Schedules Window

The columns in the window are defined Table 22.

Table 22. Radio On/Off Schedule Window

Column	Description
Name	Displays the name of the schedule.

Table 22. Radio On/Off Schedule Window (Continued)

Column	Description
On/Off	Displays the status of the schedule. The possible states are listed here: On - The schedule is enabled. Off - The schedule is disabled. To enable or disable schedules, refer to “Editing Radio Schedules” on page 224.
Day	Displays the days of the week when the schedule is enabled. Here are the abbreviations of the days: M - Monday Tu - Tuesday W - Wednesday Th - Thursday F - Friday Sa - Saturday Sun - Sunday The radios of access points are active on days that are not included in schedules.
Radio OnTime	Displays the time when the access points turn on the radios.
Radio Off Time	Displays the time when the access points turn off the radios.

Adding Radio Schedules

To add a radio schedule to your account, do the following:

1. Click the **Configuration** tab.
2. If it is not already selected, select **All** in the Locations menu in the left column.

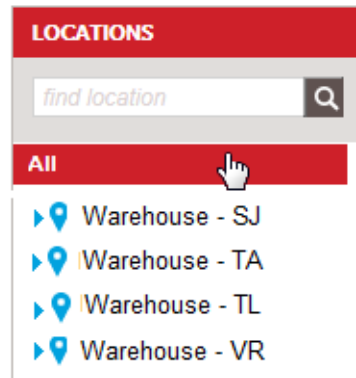


Figure 140. All Selection in the Locations Menu

3. Select **Add Radio Schedule** from the Choose Action menu:

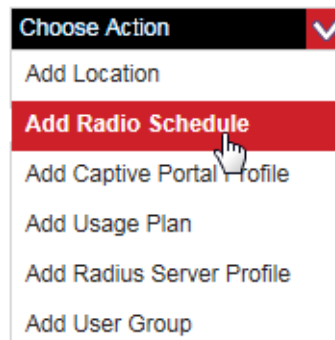


Figure 141. Add Radio Schedule Selection

The program displays the Add Radio On/Off Schedule window:

Add Radio On/Off Schedule

Schedule Name

Schedule On

☐ M ☐ T ☐ W ☐ T ☐ F ☒ S ☒ S

Radio On time

07 : 00 AM

(hrs:mins)

Radio OFF time

11 : 30 AM

(hrs:mins)

Figure 142. Radio On/Off Schedule Window

Another way to display the window is by selecting **Radio On/Off Schedule** from the Shared Settings menu in the lower left corner and then clicking the **ADD SCHEDULE** button in the Radio On/Off Schedule window.

- 4. Configure the parameters in the window for the new radio schedule. Refer to Table 23.

Table 23. Add Radio On/Off Schedule Window

Parameter	Description
Name	Enter a name for the new schedule.
Schedule On	Add check marks to the dialog boxes of the days of the week when the schedule is to be active. The schedule is enabled on days that have check marks and disabled on days that do not have check marks. The radios in access points are active on days when a schedule is disabled. For example, if you check the dialog boxes for Monday through Friday to enable a schedule on those days, and leave Saturday and Sunday unchecked, the radios will be active on those two days.
Radio On Time	Specify the time when the access points are to turn on the radios. The time is specified in hours and minutes.
Radio Off Time	Specify the time when the access points are to turn off the radios. The time is specified in hours and minutes.

5. Click the **ADD THIS RADIO ON/OFF** button to add the schedule or **CANCEL** to cancel the action.

The new schedule is added to the Radio On/Off Schedules window. Refer to Figure 139 on page 215.

6. To add the new radio schedule to a location, go to “Adding Radio Schedules to Locations” on page 220.

Adding Radio Schedules to Locations

This section contains the procedure for adding radio schedules to locations. Here are the guidelines:

- ❑ A location can have only one radio schedule.
- ❑ You can assign a schedule to more than one location.
- ❑ You can add a schedule to only one location at a time.

For instructions on how to add a radio schedule, refer to “Adding Radio Schedules” on page 217.

To add a radio schedule to a location, perform the following procedure:

1. Click the **Configuration** tab.
2. Select the location for the radio schedule by clicking its name in the All Locations portion of the window or in the Locations column in the left column. You can select only one location.

The program displays the details of the location, with the Location Profile section expanded. An example is shown in Figure 39 on page 76.

3. In the location configuration area, click the **Wireless Radio** option to expand it.

The program displays the Wireless Radio configuration section. Refer to Figure 143 on page 221.

Wireless Radio

Radio On/Off Setting ?

2.4GHz Radio Always ON ▼

5GHz Radio Always ON ▼

Radio Resource Management

2.4GHz Radio ☐ On ☒ Off

5GHz Radio ☐ On ☒ Off

2.4GHz configuration

Wireless Mode ☒ 11b ☐ 11bg ☐ 11bgn

Channel Width 20MHz ▼

Show Advanced Features

5GHz configuration

Wireless Mode ☐ 11a ☐ 11an ☒ 11ac

Channel Width 40MHz ▼

Figure 143. Wireless Radio Section

- In the Radio On/Off Setting section, select **Scheduled** from either the 2.4GHz Radio or 5GHz Radio pull-down menu. Refer to Figure 144.

Radio On/Off Setting ?

2.4GHz Radio Scheduled ▼

5GHz Radio Always ON

Schedule Profile Always OFF

Scheduled

Figure 144. Adding a Radio On/Off Schedule to a Location

The window adds the Schedule Profile pull-down menu to the Radio On/Off Setting area.

5. Select the desired radio on/off schedule for the location from the Schedule Profile pull-down menu. You can select only one schedule. Refer to Figure 145.

Radio On/Off Setting ?

2.4GHz Radio	Scheduled
5GHz Radio	Scheduled
Schedule Profile	Not Set
2.4GHz configuration	default
Wireless Mode	Weekly

Figure 145. Selecting a Radio On/Off Schedule for a Location

Note

You cannot select different schedules for the 2.4GHz and 5GHz radios. The radios must use the same schedule.

6. Click **APPLY** to save the changes or **CANCEL** to cancel the action.

If you click Apply, the radio schedule is now active on the access points at the location.

Removing Radio Schedules from Locations

To remove a radio schedule from a location, perform the following procedure:

1. Click the **Configuration** tab.
2. Select the location with the radio schedule to be removed by clicking its name in the All Locations portion of the window or in the Locations column in the left column. You can select only one location.

The program displays the details of the location, with the Location Profile section expanded. An example is shown in Figure 39 on page 76.

3. In the location configuration area, click the **Wireless Radio** option to expand it.

The program displays the Wireless Radio configuration section. Refer to Figure 143 on page 221.

4. In the Radio On/Off Setting section, select from the 2.4GHz Radio or 5GHz Radio pull-down menu either **Always ON** if you want the radios to operate continuously or **Always OFF** if you want to turn off the radios. Refer to Figure 146.

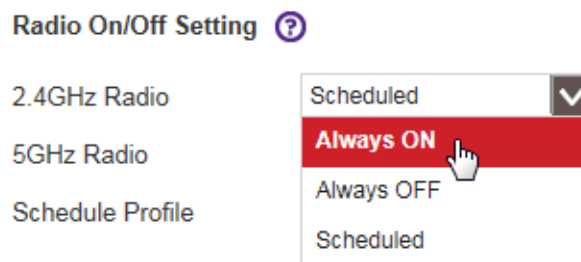


Figure 146. Removing a Radio Schedule from a Location

5. Click **APPLY** to remove the radio schedule from the location or **CANCEL** to cancel the action.

If you click Apply to remove the schedule, the access points at the location now operate continuously or shut off, depending on whether you selected Always ON or Always OFF in step 4.

Editing Radio Schedules

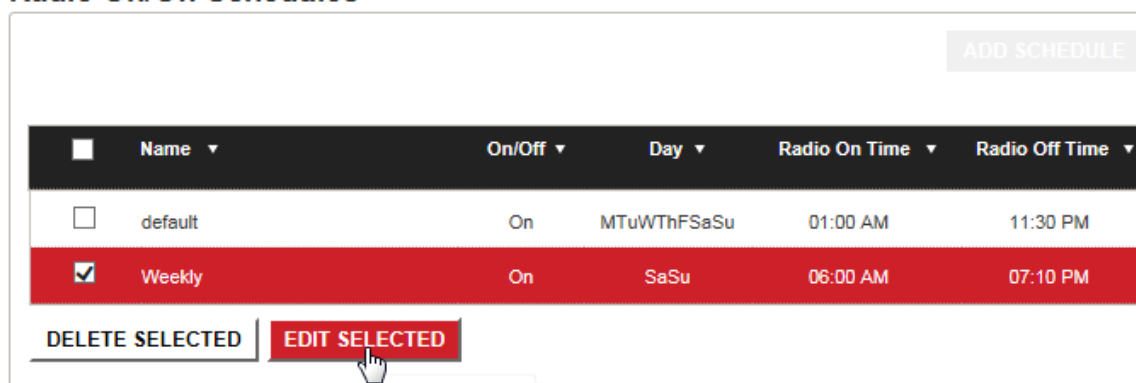
To edit a radio schedule's name or times, do the following:

1. Click the **Configuration** tab.
2. Select **Radio On/Off Schedules** from the Shared Settings menu. Refer to Figure 138 on page 215.

The program displays the Radio On/Off Schedules window (see Figure 139 on page 215).

3. Check the dialog box of the schedule you want to edit. You can edit only one schedule at a time.
4. Click the **EDIT SELECTED** button.

Radio On/Off Schedules

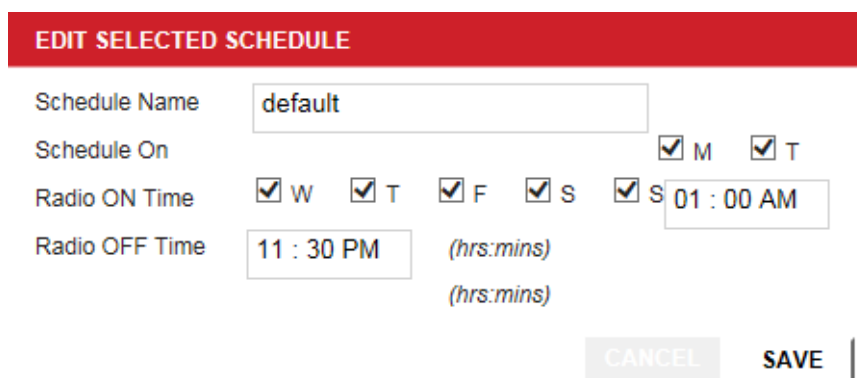


☐	Name ▾	On/Off ▾	Day ▾	Radio On Time ▾	Radio Off Time ▾
☐	default	On	MTuWThFSaSu	01:00 AM	11:30 PM
☒	Weekly	On	SaSu	06:00 AM	07:10 PM

DELETE SELECTED EDIT SELECTED

Figure 147. Edit Selected Button

The EDIT SELECTED SCHEDULE window is displayed:



EDIT SELECTED SCHEDULE

Schedule Name

Schedule On ☒ M ☒ T ☐ W ☐ T ☐ F ☐ S ☐ S

Radio ON Time ☒ W ☒ T ☒ F ☒ S ☒ S

Radio OFF Time (hrs:mins)

CANCEL SAVE

Figure 148. Edit Selected Schedule Window

5. Edit the schedule name, days, and radio on/off times as needed. Refer to Table 23 on page 218.
6. Click **SAVE** to activate your changes or **CANCEL** to cancel the action.

Deleting Radio Schedules

This section contains the procedure for deleting radio schedules from your account. You cannot delete radio schedules while they are assigned to location entries. They have to be removed from all location assignments before you can delete them. For instructions, refer to “Removing Radio Schedules from Locations” on page 223.

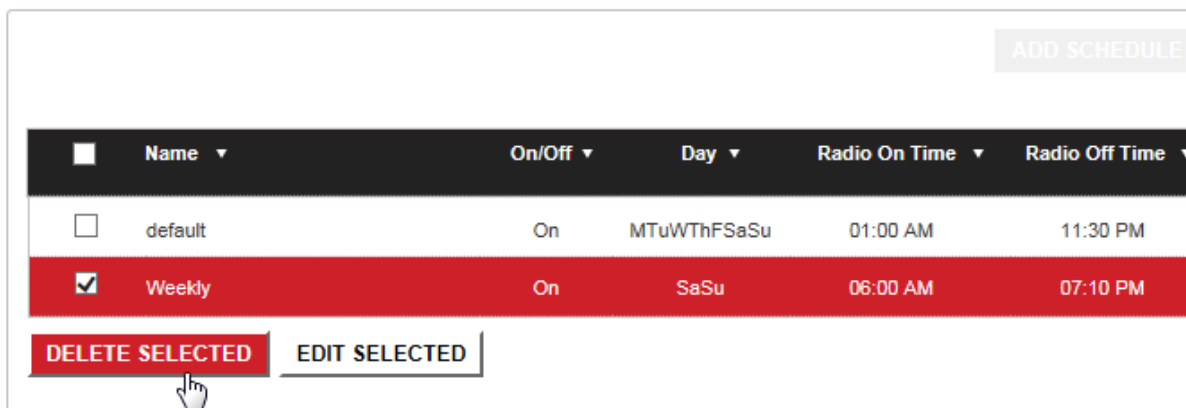
To delete a radio on/off schedule, do the following:

1. Click the **Configuration** tab.
2. Select **Radio On/Off Schedules** from the Shared Settings menu. Refer to Figure 138 on page 215.

The program displays the Radio On/Off Schedules window (see Figure 139 on page 215).

3. Check the dialog box of the schedule you want to delete. You can delete multiple schedules at the same time. To select all schedules, click the Name dialog box in the heading.
4. Click the **DELETE SELECTED** button.

Radio On/Off Schedules



ADD SCHEDULE

☐	Name ▾	On/Off ▾	Day ▾	Radio On Time ▾	Radio Off Time ▾
☐	default	On	MTuWThFSaSu	01:00 AM	11:30 PM
☒	Weekly	On	SaSu	06:00 AM	07:10 PM

DELETE SELECTED EDIT SELECTED

Figure 149. Delete Selected Button

A confirmation prompt is displayed.

5. Click **YES** to delete the schedule or **NO** to cancel the action.

Chapter 12

RADIUS Server Profiles

This chapter includes the following sections:

- ❑ “Introduction to RADIUS Server Profiles” on page 228
- ❑ “Viewing RADIUS Server Profiles” on page 229
- ❑ “Adding RADIUS Server Profiles” on page 231
- ❑ “Adding RADIUS Server Profiles to Locations” on page 235
- ❑ “Removing RADIUS Server Profiles from Locations” on page 237
- ❑ “Editing RADIUS Server Profiles” on page 238
- ❑ “Deleting RADIUS Server Profiles” on page 240

Introduction to RADIUS Server Profiles

RADIUS server profiles are required for the following authentication methods:

- ❑ Legacy 802.1x
- ❑ WPA with RADIUS
- ❑ WPA2 with RADIUS
- ❑ WPA & WPA2 with RADIUS

RADIUS server profiles contain the IP addresses of RADIUS authentication servers on your network. The profiles are used by the access points to communicate with the servers to authenticate wireless clients who are accessing your wireless network through locations that are using one or more of the above authentication methods.

RADIUS server profiles are not required if you are not using the above authentication methods.

Here are the guidelines to RADIUS server profiles.

- ❑ After adding a RADIUS server profile, you have to assign it to the location with wireless networks that need it to authenticate clients. For instructions, refer to “Adding RADIUS Server Profiles to Locations” on page 235.
- ❑ You can assign a RADIUS server profile to more than one location.
- ❑ A profile can specify primary and secondary RADIUS servers. The program uses the secondary server of a profile only if a primary server is unavailable. Specifying a secondary server is optional.
- ❑ Profiles can also include RADIUS accounting servers. However, you cannot define the accounting servers when you initially add profiles. You define the accounting servers by editing the profiles.
- ❑ RADIUS server profiles can be deleted, but not disabled.

Viewing RADIUS Server Profiles

To view RADIUS server profiles, do the following:

1. Click the **Configuration** tab.
2. Select **Radius Server Profiles** from the Shared Settings menu in the lower left corner:

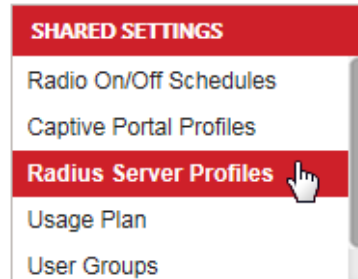


Figure 150. Radius Server Profiles Selection in the Shared Settings Menu

If there are no profiles, the program displays the Radius Server Profile window:

Radius Server Profile

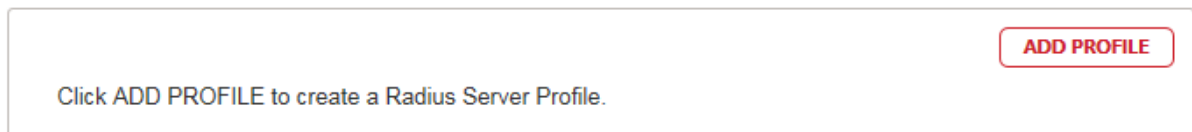


Figure 151. Radius Server Profile Screen

To add a profile, click **ADD PROFILE** and go to step 4 in “Adding RADIUS Server Profiles” on page 231.

If your account already has profiles, it lists their names in the All Radius Server Profiles window.

All Radius Server Profiles

Choose Action



Warehouse SF RADIUS profile

Warehouse TA RADIUS profile

Warehouse TL RADIUS profile

Warehouse VR RADIUS profile

Figure 152. All RADIUS Server Profiles Screen

3. To view or edit the settings of a profile, click its name in the list. The settings are described in Table 24 on page 232.

Radius Server Profile: Warehouse SF RADIUS Profile

CANCEL SAVE

Profile Name Warehouse SF RADIUS F

▼ Authentication Server

Primary Authentication Server

IP Address 149.123.55.64

Port Number 1812

Shared Secret ●●●●●●●●

Secondary Authentication Server

IP Address

Port Number 1812

Shared Secret

Authentication Setting

Reauthentication Time 3600 seconds

☐ Update global key every 1800 seconds

► Accounting Server

Figure 153. Radius Server Profile

Adding RADIUS Server Profiles

This procedure explains how to add RADIUS server profiles. For background information, refer to “Introduction to RADIUS Server Profiles” on page 228. To add a RADIUS server profile, do the following:

1. Click the **Configuration** tab.
2. If it is not already selected, select **All** in the Locations menu in the left column.

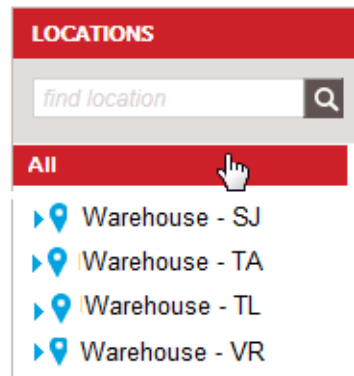


Figure 154. All Selection in the Locations Menu

3. Select **Add Radius Server Profile** from the Choose Action menu in the upper right corner:

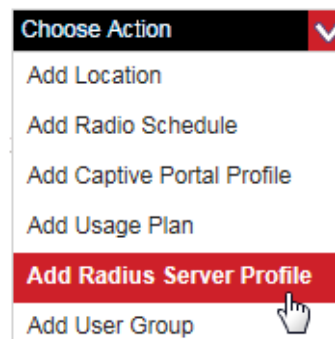


Figure 155. Add Radius Server Profile Selection in the Choose Action Menu

The program displays the Add Radius Server Profile window:

Add Radius Server Profile

Profile Name

Primary Authentication Server

IP Address

Port Number

1812

Shared Secret

Secondary Authentication Server

IP Address

Port Number

1812

Shared Secret

Authentication Setting

Reauthentication Time

3600

seconds

☐ Update global key every

seconds

CANCEL

Add This Radius Profile

Figure 156. Add Radius Server Profile Window

4. Fill in the fields. The fields are defined in Table 24.

Note

Defining a secondary RADIUS server is optional.

Table 24. Add Radius Server Profile Screen

Parameter	Description
Profile Name	Enter a name for the profile. The name can be up to 30 alphanumeric characters. Spaces are allowed.
Primary Authentication Server	
IP Address	Enter the IPv4 address of the primary RADIUS server.
Port Number	Enter the RADIUS port number of the primary RADIUS server. The range is 0 to 65535. The default is 1812.

Table 24. Add Radius Server Profile Screen

Parameter	Description
Shared Secret	Enter the shared secret key of the primary RADIUS server. The key can be up to 64 characters and can consist of letters, numbers, and special characters. The key is case-sensitive. It must be entered the same here and on the server.
Secondary Authentication Server	
IP Address	Enter the IPv4 address of the secondary RADIUS server.
Port Number	Enter the RADIUS port number of the secondary RADIUS server. The range is 0 to 65535. The default is 1812.
Shared Secret	Enter the shared secret key of the secondary RADIUS server. The key can be up to 64 characters and can consist of letters, numbers, and special characters. The key is case-sensitive. It must be entered the same here and on the server.
Authentication Setting	
Reauthentication Time	Enter the amount of time, in seconds, at which wireless clients must re-authenticate. The default is 3600 seconds. Entering 0 disables re-authentication.
Update Global Key Every dialog box	Add a check mark to the dialog box if you want the program to periodically update the global key.
Update Global Key Every	Enter the amount of time, in seconds, at which the global key is updated. The default is 1800 seconds.

- Click **ADD THIS RADIUS PROFILE** to add the profile or **CANCEL** to cancel the action.

The program displays a confirmation window.

Add Radius Server Profile

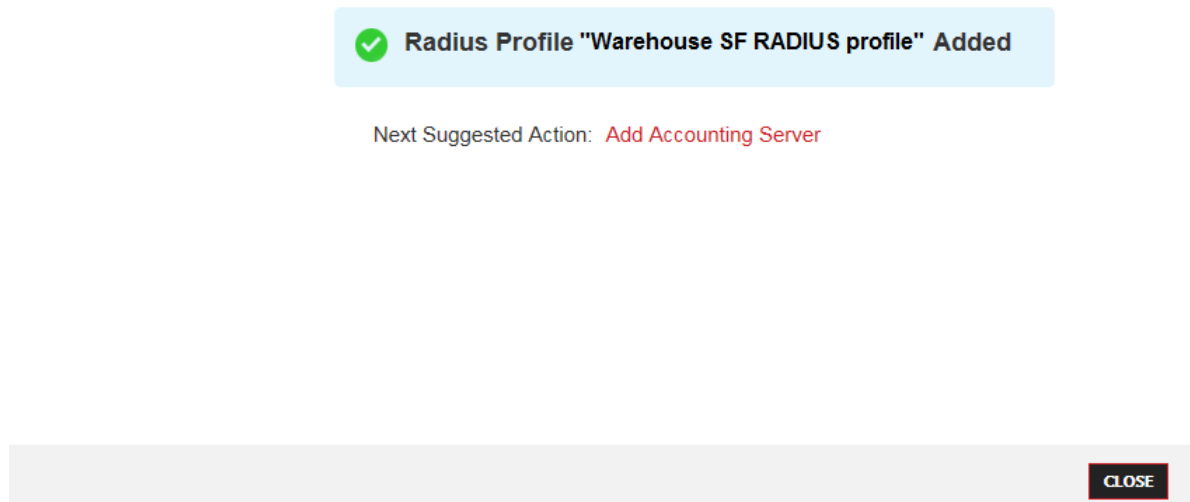


Figure 157. Confirmation Prompt for Adding a Radius Server Profile

6. Do one of the following:
 - ☐ To add more profiles or perform a different procedure, click **Close**. To add more profiles, repeat this procedure starting with step 2.
 - ☐ To add an accounting server to the profile, click **Add Accounting Server**. For instructions, go to step 5 in “Editing RADIUS Server Profiles” on page 238.
7. To add the profile to a location, refer to “Adding RADIUS Server Profiles to Locations” on page 235.

Adding RADIUS Server Profiles to Locations

This section contains the procedure for adding RADIUS server profiles to locations. You can add a RADIUS server profile to more than one location.

To add a RADIUS server profile to a location, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left margin, click the name of the location where you want to add a RADIUS server profile. This example selects the Warehouse-TL location.

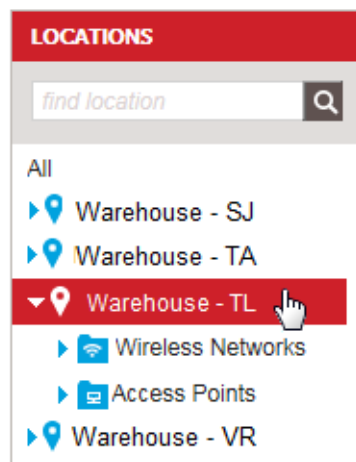


Figure 158. Selecting a Location In the Locations Menu

The program displays the details of the location, with the Location Profile section expanded. An example is shown in Figure 39 on page 76.

3. Click **Radius Server** to expand the section.

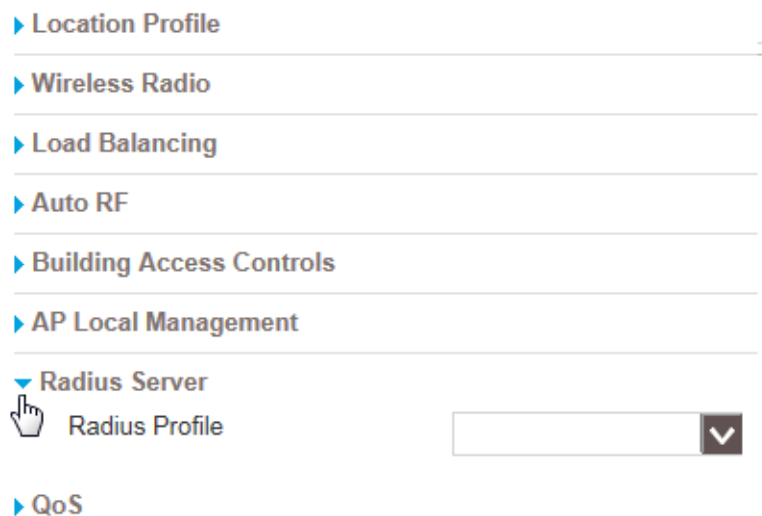


Figure 159. Radius Server Section in the Location Configuration Settings

4. From the Radius Profile pull-down menu, select the RADIUS server profile for the location. You can select only one profile.

Note

If you want to remove a profile from a location without assigning another one, select Not Set from the Radius Profile pull-down menu.

5. Click **APPLY** to add the server profile to the location or **Cancel** to cancel the action.

Removing RADIUS Server Profiles from Locations

This section contains the procedure for removing RADIUS server profiles from locations.

Note

You cannot remove a RADIUS server profile from a location that has one or more wireless networks that are using RADIUS authentication. You must first either delete the wireless networks from the location or change them to non-RADIUS authentication. For instructions, refer to “Deleting Wireless Networks” on page 166 or “Editing Wireless Network Names and Authentications” on page 155. You can also remove a RADIUS server profile from a location by assigning it a different server profile. For instructions, refer to “Adding RADIUS Server Profiles to Locations” on page 235.

To remove a RADIUS server profile from a location, do the following:

1. Click the **Configuration** tab.
2. In the Locations menu in the left margin, click the name of the location where you want to remove a RADIUS server profile. For an example, refer to Figure 158 on page 235.

The program displays the details of the location, with the Location Profile section expanded. An example is shown in Figure 39 on page 76.

3. Click **Radius Server** to expand the section. Refer to Figure 159 on page 236.
4. From the Radius Profile pull-down menu, select the **Not Set** option. Refer to Figure 160.

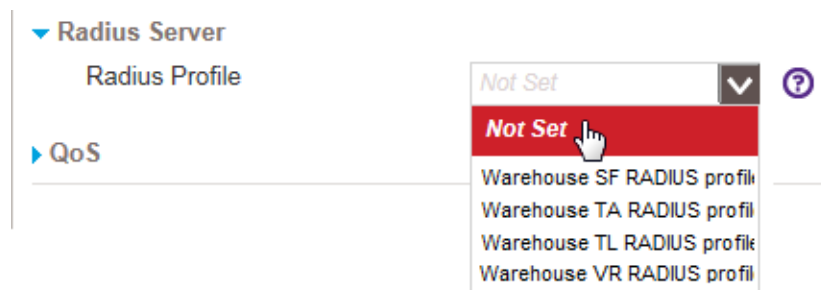


Figure 160. Removing a RADIUS Server Profile from a Location

5. Click **APPLY** to remove the RADIUS server profile from the location or **Cancel** to cancel the action.

Editing RADIUS Server Profiles

To edit a RADIUS server profile, do the following:

- 1. Click the **Configuration** tab.
- 2. Select **Radius Server Profiles** from the Shared Settings menu in the lower left corner of the window: Refer to Figure 150 on page 229.

The program displays the All Radius Server Profiles screen. Refer to Figure 152 on page 230.

- 3. Click the name of the RADIUS server profile you want to edit. You can edit only one profile at a time.

The program displays the configuration settings of the selected RADIUS server profile. Refer to Figure 153 on page 230.

- 4. Edit the profile parameters, as needed. Refer to Table 24 on page 232.
- 5. Click **SAVE** to save your changes or **CANCEL** to cancel the action.
- 6. To edit the accounting parameters, click **Accounting Server** to expand its section.

Profile Name

Warehouse SF RADIUS F

► Authentication Server

▼ Accounting Server

Primary Accounting Server

IP Address

Port Number

1813

Shared Secret

Secondary Accounting Server

IP Address

Port Number

1813

Shared Secret

Figure 161. Accounting Server Section for a RADIUS Server Profile

- 7. Edit the parameters. Refer to Table 25 on page 239.

Table 25. Accounting Server in the Add Radius Server Profile Screen

Field	Description
Primary Accounting Server	
IP Address	Enter the IPv4 address of the primary accounting server.
Port Number	Enter the RADIUS accounting port number of the primary server. The range is 0 to 65535. The default is 1813.
Shared Secret	Enter the shared secret key of the primary RADIUS accounting server. The key can be up to 64 characters and can consist of letters, numbers, and special characters. The key is case-sensitive. It must be entered the same here and on the server.
Secondary Accounting Server	
IP Address	Enter the IPv4 address of the secondary RADIUS accounting server.
Port Number	Enter the RADIUS port number of the secondary RADIUS accounting server. The range is 0 to 65535. The default is 1813.
Shared Secret	Enter the shared secret key of the secondary RADIUS accounting server. The key can be up to 64 characters and can consist of letters, numbers, and special characters. The key is case-sensitive. It must be entered the same here and on the server.

8. Click **SAVE** to save your changes or **CANCEL** to cancel the action.
9. To add the profile to a location, refer to “Adding RADIUS Server Profiles to Locations” on page 235.

Deleting RADIUS Server Profiles

To delete a RADIUS server profile, do the following:

1. Click the **Configuration** tab.
2. Select **Radius Server Profiles** from the Shared Setting menu in the lower left corner of the window Refer to Figure 150 on page 229.
3. Select the profile you want to delete from the list. You can delete only one profile at a time.
4. Select **Delete This Radius Server** from the Choose Action menu.



Figure 162. Delete This Radius Server Selection in the Choose Action Menu

The program displays a confirmation window.

5. Click **YES** to delete the profile or **NO** to cancel the action.

Chapter 13

Usage Plans

This chapter includes the following sections:

- ❑ “Introduction to Usage Plans” on page 242
- ❑ “Viewing Usage Plans” on page 243
- ❑ “Adding Usage Plans” on page 245
- ❑ “Editing Usage Plans” on page 248
- ❑ “Adding Usage Plans to Network Components” on page 249
- ❑ “Deleting Usage Plans” on page 250

Introduction to Usage Plans

You use usage plans to limit the amount of time that wireless clients can access your wireless networks through network elements, such as hotspots or captive portals. Usage plans specify the maximum number of hours that clients can access your network. Access points deny access to clients who have exceeded the maximum number of hours stated in usage plans.

You can use usage plans to control the following attributes:

- ❑ Maximum number of hours of permitted access by the day, week, month, or year.
- ❑ Maximum number of concurrent connections by wireless clients.

You assign usage plans to captive portals.

Here are the guidelines to usage plans:

- ❑ Usage plans can specify one or both of the following restrictions:
 - Maximum time limit of permitted access by clients.
 - Maximum number of simultaneous connections per client.
- ❑ You can apply a usage plan to more than one captive portal.
- ❑ You cannot delete usage plans while they are assigned to network objects. You have to remove them from their network assignments before deleting them.

Viewing Usage Plans

This section contains the procedure for displaying a list of the names of the current usage plans in your account and for displaying their configuration settings. It does not explain how to view the assignments of usage plans to captive portals. For that you have to display the configuration settings of captive portals. For instructions, refer to “Viewing Captive Portals” on page 170.

To view the existing usage plans, do the following:

1. Click the **Configuration** tab.
2. Select **Usage Plan** from the Shared Settings menu in the lower left corner of the window:

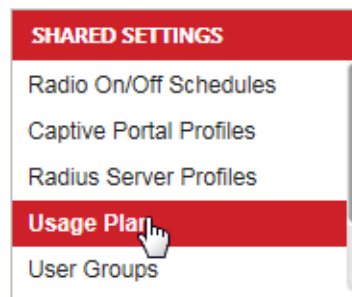


Figure 163. Usage Plan Selection in the Shared Settings Menu

If there are no plans, the program displays the window in Figure 164:

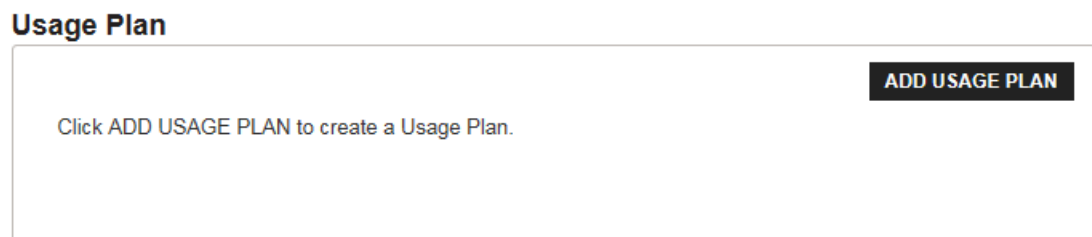


Figure 164. Usage Plan Window

To add a new plan, click Add Usage Plan and go to “Adding Usage Plans” on page 245.

If the program has usage plans, it lists them in the All Usage Plans window. Refer to Figure 165 on page 244.

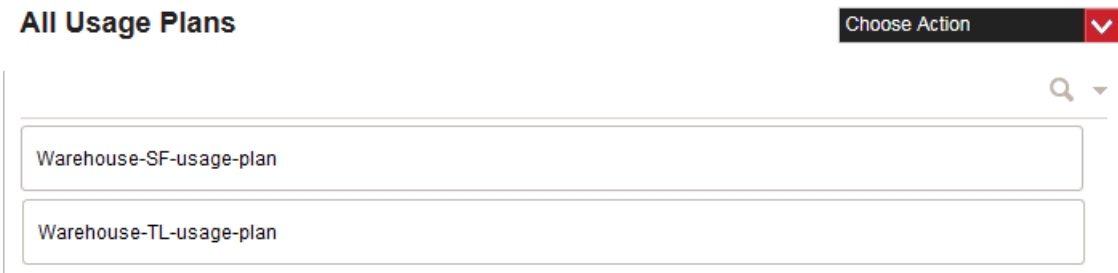


Figure 165. All Usage Plans Window

- 3. To display plan details, click a plan's name. You can view only one plan at a time.

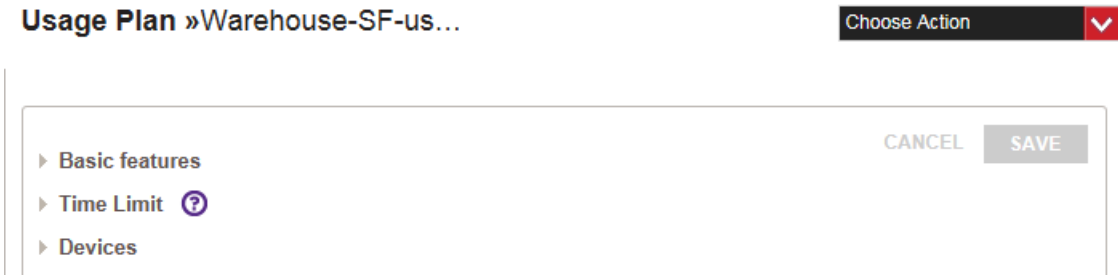


Figure 166. Viewing a Usage Plan

The sections in the window are described in Table 26. For more information about the parameters, refer to Table 27 on page 246.

Table 26. Usage Plan Window

Parameter	Description
Basic Features	Contains the plan's name.
Time Limit	Contains the number of permitted hours and the start and end times of permitted access.
Devices	Contains the maximum number of simultaneous connections per wireless client.

Adding Usage Plans

To add a new usage plan to your account, do the following:

1. Click the **Configuration** tab.
2. If it is not already selected, select **All** in the Locations menu in the left margin of the window.

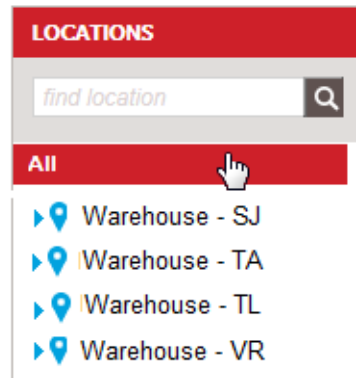


Figure 167. All Selection in the Locations Menu

3. Select **Add Usage Plan** from the Choose Action menu in the upper left corner of the window:

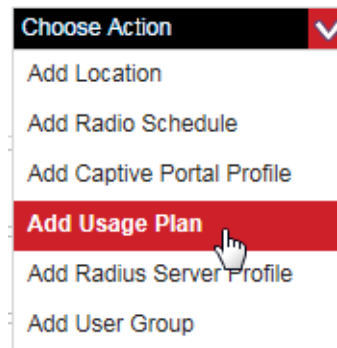


Figure 168. Add Usage Plan Selection in the Choose Action Menu

The program displays the Add Usage Plan window:

Add Usage Plan

Usage Plan Name

▼ Time Limit

Limit access to

Not Set

Hours per

Month

▼

Permitted access hours

12 : 00

AM

▼

to

12 : 00

AM

▼

► Devices

CANCEL

ADD THIS USAGE PLAN

Figure 169. Add Usage Plan Window

4. Fill in the fields of the plan. The fields are defined in Table 27.

Table 27. Add Usage Plan Window

Parameter	Description
Usage Plan Name	Enter a name for the plan.
Limit access to	Type the number of permitted hours and then select Day , Week , Month , or Year from the drop-down menu.
Permitted access hours	Specify the start and end times of permitted access.
Devices Allow concurrent connections (per username or voucher)	Enter the maximum number of simultaneous connections per user.

5. After filling in the plan, click **ADD THIS USAGE PLAN** to add the plan to your account or **CANCEL** to cancel the action.

6. To assign the plan to a wireless component, such as a hotspot or captive portal, refer to “Adding Usage Plans to Network Components” on page 249.

Editing Usage Plans

To edit an existing usage plan in your account, do the following:

1. Click the **Configuration** tab.
2. Select **Usage Plan** from the Shared Settings menu in the lower left corner of the window:

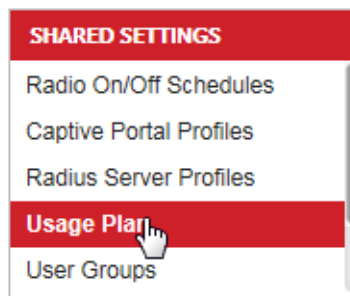


Figure 170. Usage Plan Selection in the Shared Settings Menu

The names of the current usage plans are listed in the main section of the window. Refer to Figure 165 on page 244.

3. Select the desired usage plan from the list. You can edit only one plan at a time.

The configuration settings of the plan are displayed in the main section of the window. For an example, refer to Figure 166 on page 244.

4. Edit the fields. Refer to Table 27 on page 246.
5. After editing the plan, click **SAVE** to save your change or **CANCEL** to cancel the action.
6. To assign the plan to a wireless component, such as a hotspot or captive portal, refer to “Adding Usage Plans to Network Components” on page 249.

Adding Usage Plans to Network Components

For instructions on how to apply usage plans to network components, refer to the following sections:

- ❑ To add a usage plan to a captive portal profile with a basic splash screen, refer to “Captive Portals with Basic Splash Windows” on page 172 or “Editing Captive Portals” on page 191.
- ❑ To add a usage plan to a captive portal profile with an advanced splash screen, refer to “Captive Portals with Advanced Splash Windows” on page 183 or “Editing Captive Portals” on page 191.
- ❑ To assign a usage plan to a network hotspot, refer to “Adding Free-Access Network Hotspots” on page 201.

Deleting Usage Plans

This section contains the steps for deleting usage plans from your account.

Note

You cannot delete usage plans that are currently assigned to wireless components, such as hotspots or captive portals. You must remove them from all assignments before deleting them.

To delete a usage plan, do the following:

1. Click the **Configuration** tab.
2. Select **Usage Plan** from the Shared Services menu in the lower left corner of the window. Refer to Figure 163 on page 243.
3. Select the usage plan you want to delete from the displayed list. You can delete only one plan at a time.
4. Select **Delete This Usage Plan** from the Choose Action menu.

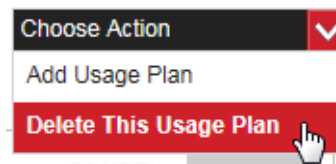


Figure 171. Delete This Usage Plan Selection in the Choose Action Menu

The program displays a confirmation window.

5. Click **YES** to delete the plan or **NO** to cancel the action.

Chapter 14

Status and Statistics Windows

This chapter describes how to view status and statistics about the wireless networks and access points in your account. This chapter includes the following sections:

- ❑ “Introduction to the Monitoring Tab Windows” on page 252
- ❑ “Summary Windows” on page 255
- ❑ “AP Details Windows” on page 262
- ❑ “Active Alarms Windows” on page 264
- ❑ “Cleared Alarms Windows” on page 268
- ❑ “Event Log Windows” on page 271
- ❑ “Hotspot Users Windows” on page 273
- ❑ “Details Window” on page 275
- ❑ “Command Log Window” on page 277

Introduction to the Monitoring Tab Windows

The Monitoring tab has more than two dozen windows with status information or statistics for you to use to monitor your wireless networks or access points. The windows are displayed with the Monitoring menu in the left column in the Monitoring tab. The tab and menus are identified in Figure 172.

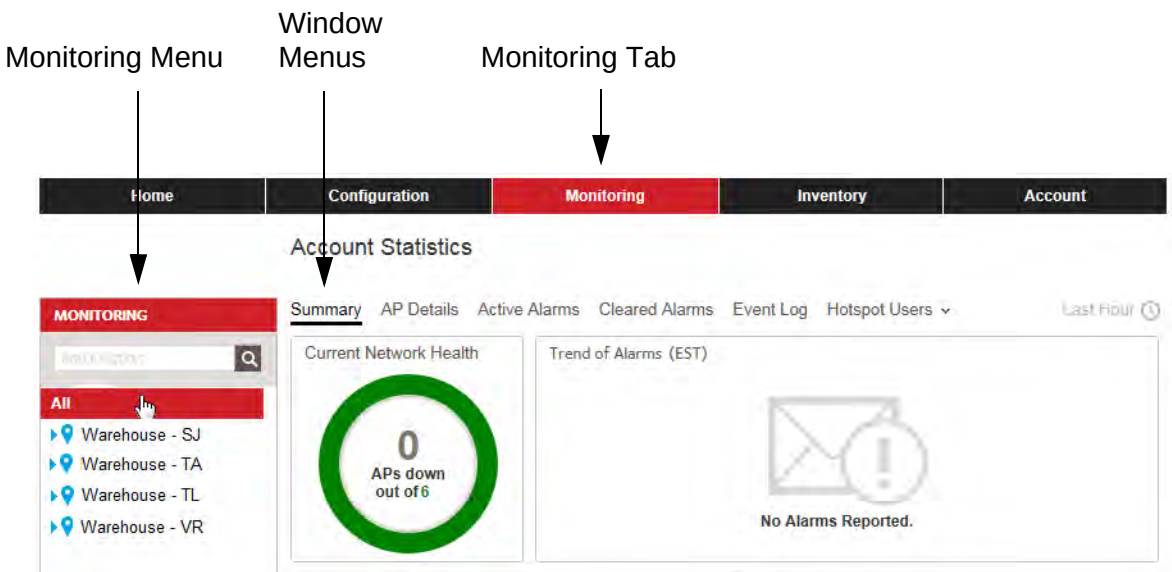


Figure 172. Monitoring Tab and Menus

The windows are grouped into the seven levels identified in Figure 173 on page 253.

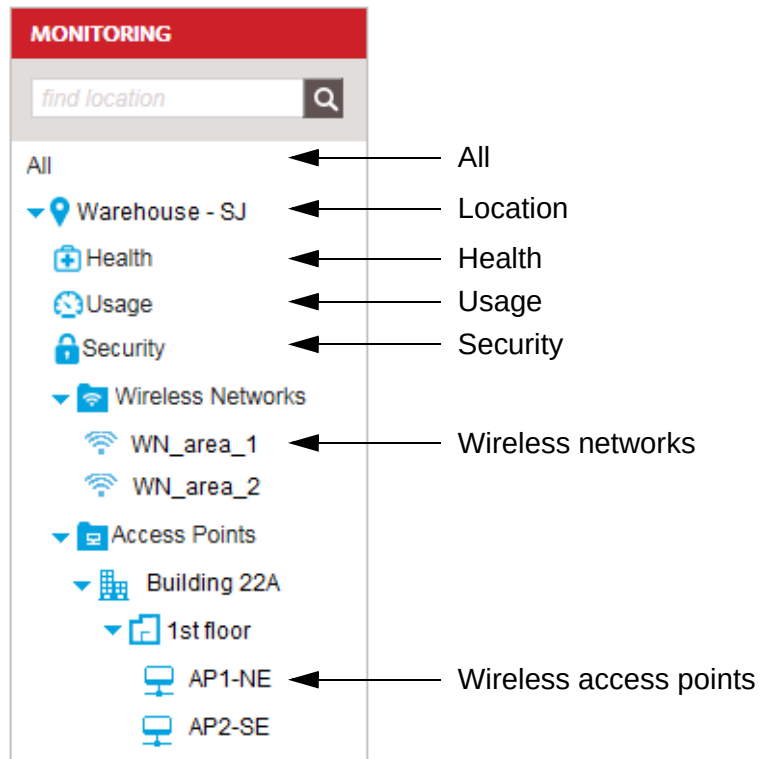


Figure 173. Levels of Monitoring Windows

Each level has multiple monitoring windows. Table 28 on page 253 lists the levels and windows.

Table 28. Monitoring Windows

Level	Monitoring Window
All	Summary
	AP Details
	Active Alarms
	Cleared Alarms
	Event Log
	Hotspot Users
Location	Summary

Table 28. Monitoring Windows (Continued)

Level	Monitoring Window
Health	Summary
	AP Details
	Active Alarms
	Cleared Alarms
	Command Log
	Event Log
Usage	Summary
	Client Details
	Hotspot Users
Security	Summary
	Neighbor Details
Wireless Networks	Summary
	Clients
	Event Log
	Hotspot Users
Wireless Access Points	Summary
	Clients
	Details
	Active Alarms
	Cleared Alarms
	Event Log

Some windows are found in multiple levels. They display different information depending on the level. For example, the event log window, which displays operating and status messages, is found in four levels. The window in the All level displays the event messages for all wireless networks and access points in your account, while the same window in the wireless access points level displays the events for selected access points.

Summary Windows

All the levels in the Monitoring menu have Summary windows.

All Summary Window

The All Summary window provides an overview of all the wireless networks and access points in your account.

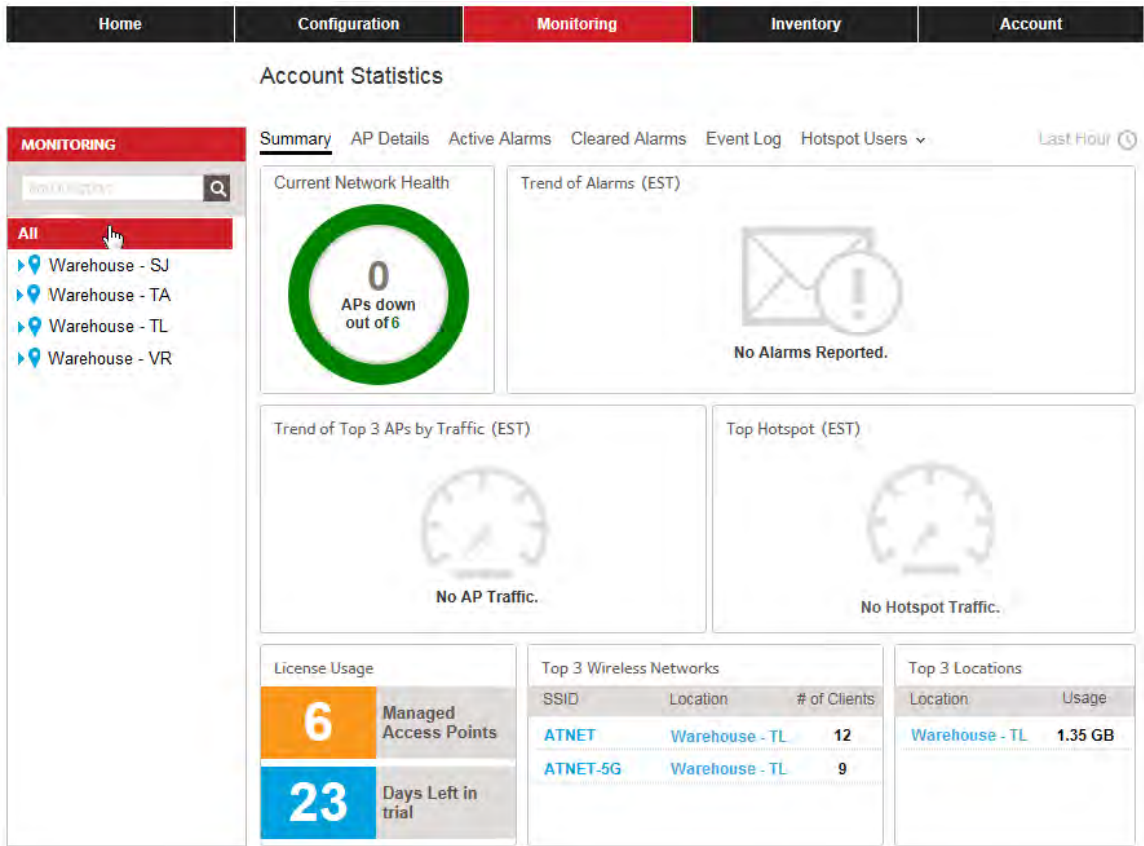


Figure 174. All Summary Window

Location Summary Window

A location Summary window provides an overview of the status and traffic packet trends of the access points of a selected location entry. The window is displayed by selecting a location entry in the Monitoring menu.

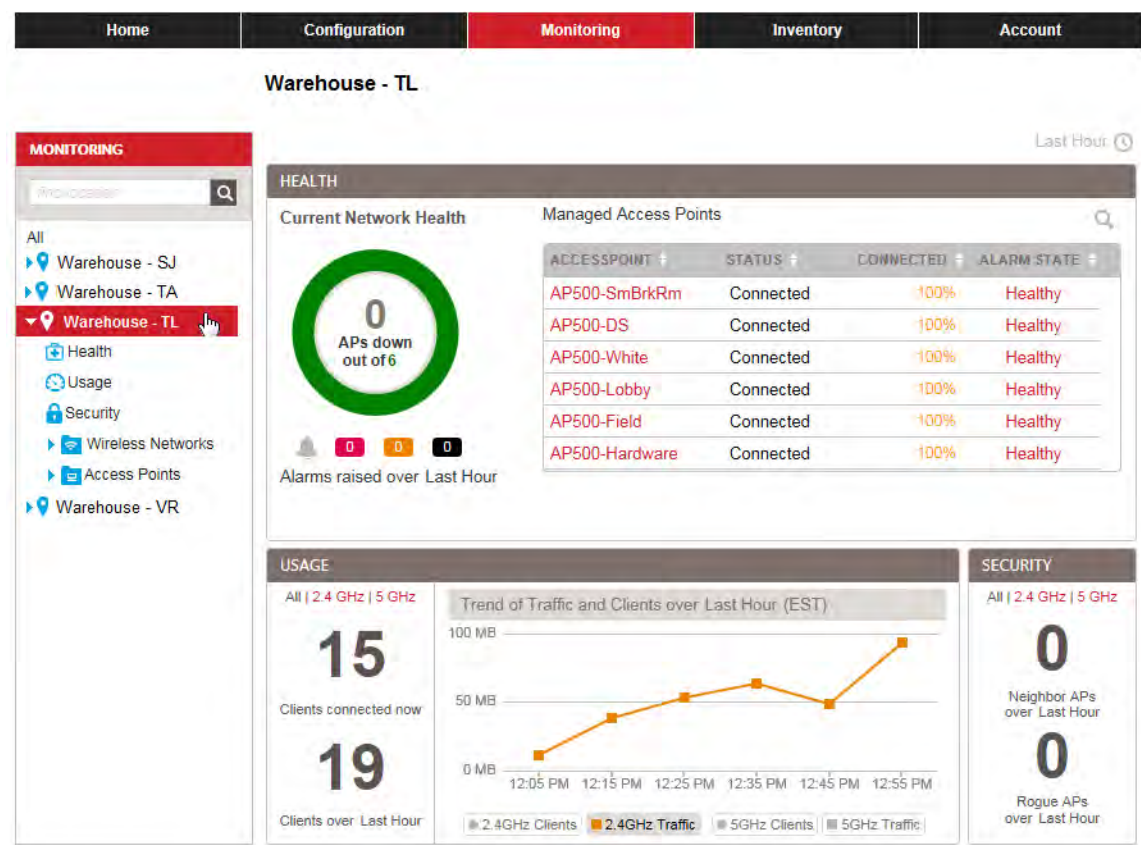


Figure 175. Location Summary Window

Health Summary Window

The Health Summary window displays overall status and statistics information on the wireless networks and access points of a selected location.

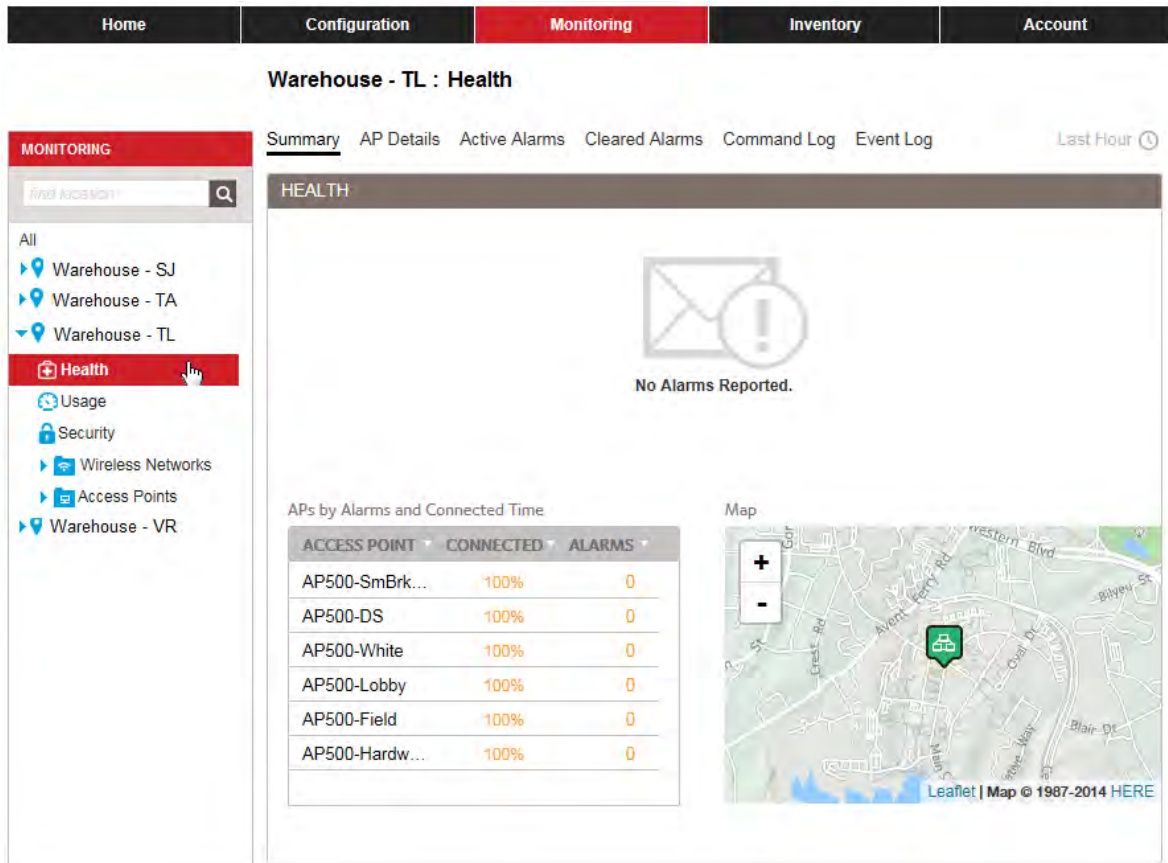


Figure 176. Health Summary Window

Usage Summary Window

The Usage Summary window provides a usage summary, client details, and hotspot usage.

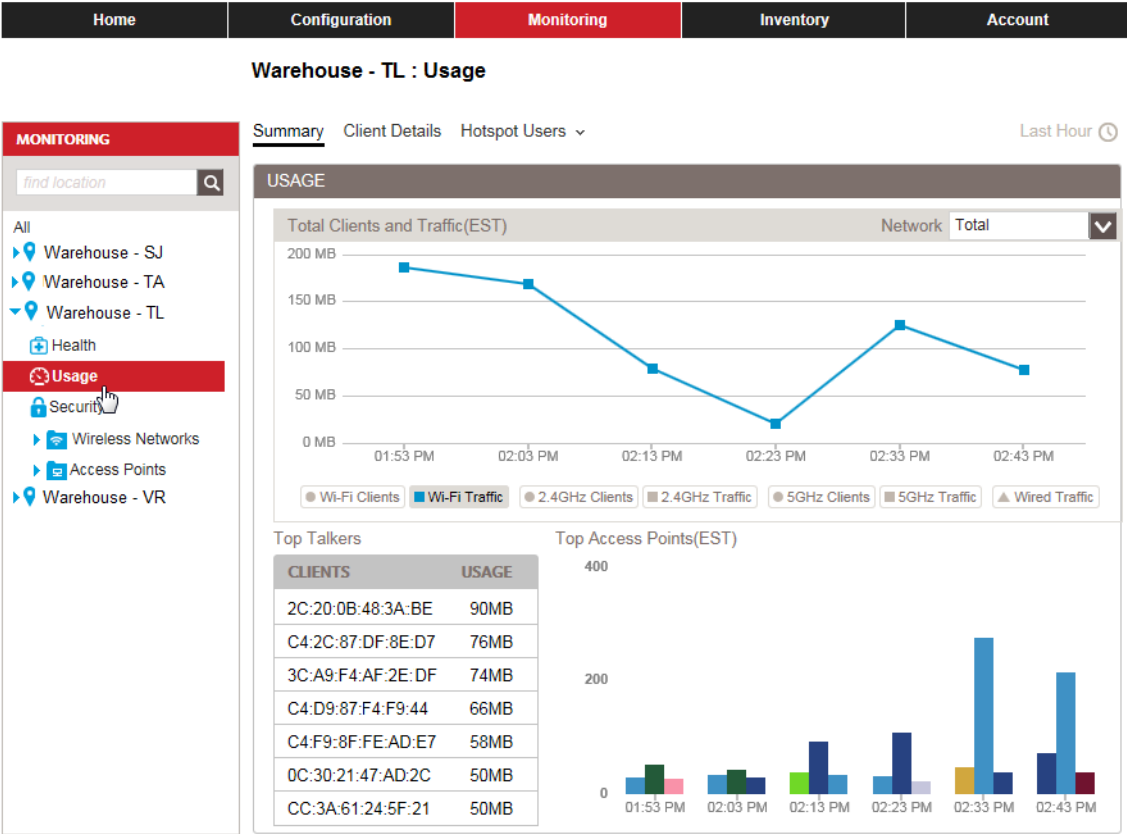


Figure 177. Usage Summary Window

**Security
Summary
Window**

The Security Summary window provides information about rogue and neighboring access points for a location. The example in Figure 178 on page 259 displays the Security Summary for the Warehouse - TL location.

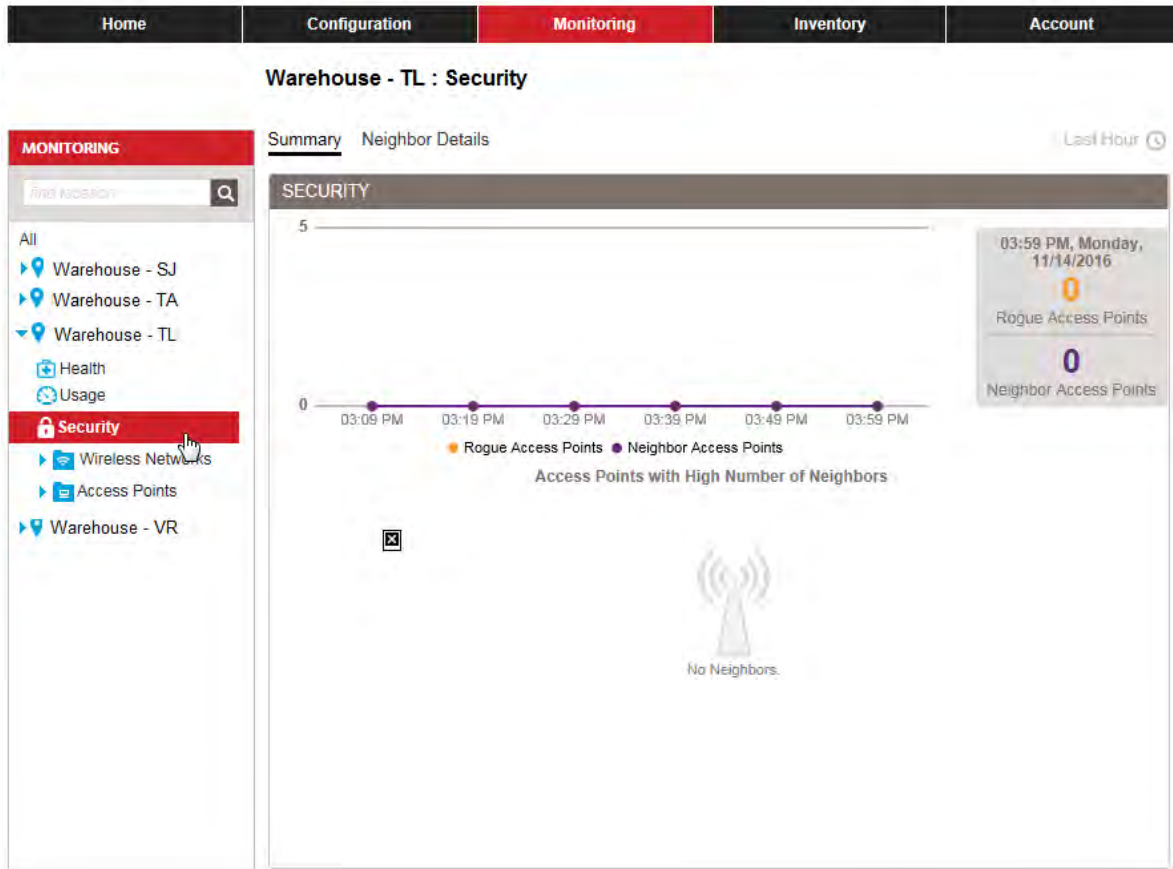


Figure 178. Security Summary Window for a Location

Wireless Network Summary Window

The wireless network Summary window displays status or statistics about a wireless network in your account. You can view only one wireless network at a time. The example in Figure 179 on page 260 displays the Summary window for the WN_area1 wireless network in the Warehouse - TL location.

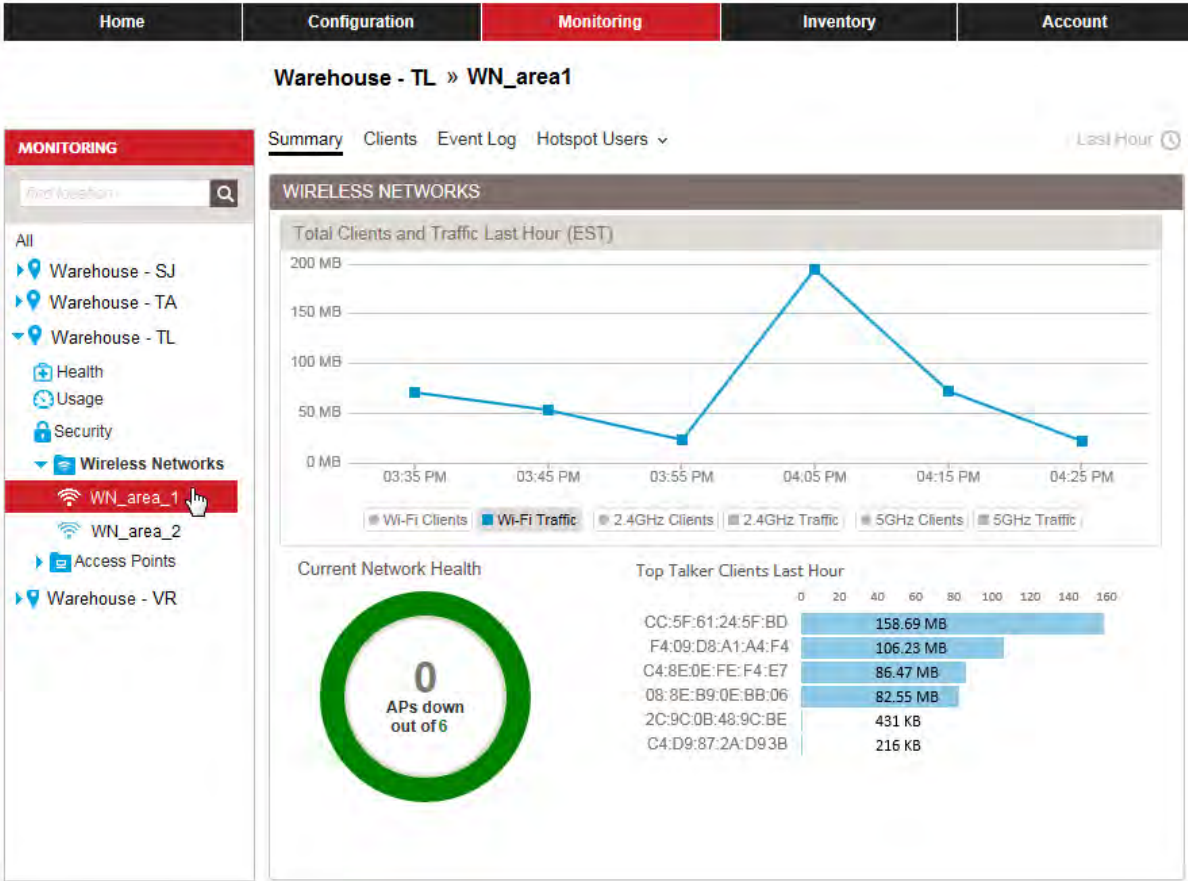


Figure 179. Wireless Network Summary Window

**Access Point
Summary
Window**

An access point Summary window displays status or statistics about individual access points in your account. The example in Figure 180 on page 261 displays the Summary window for the AP1-NW access point in Building 1 of the Warehouse - TL location.

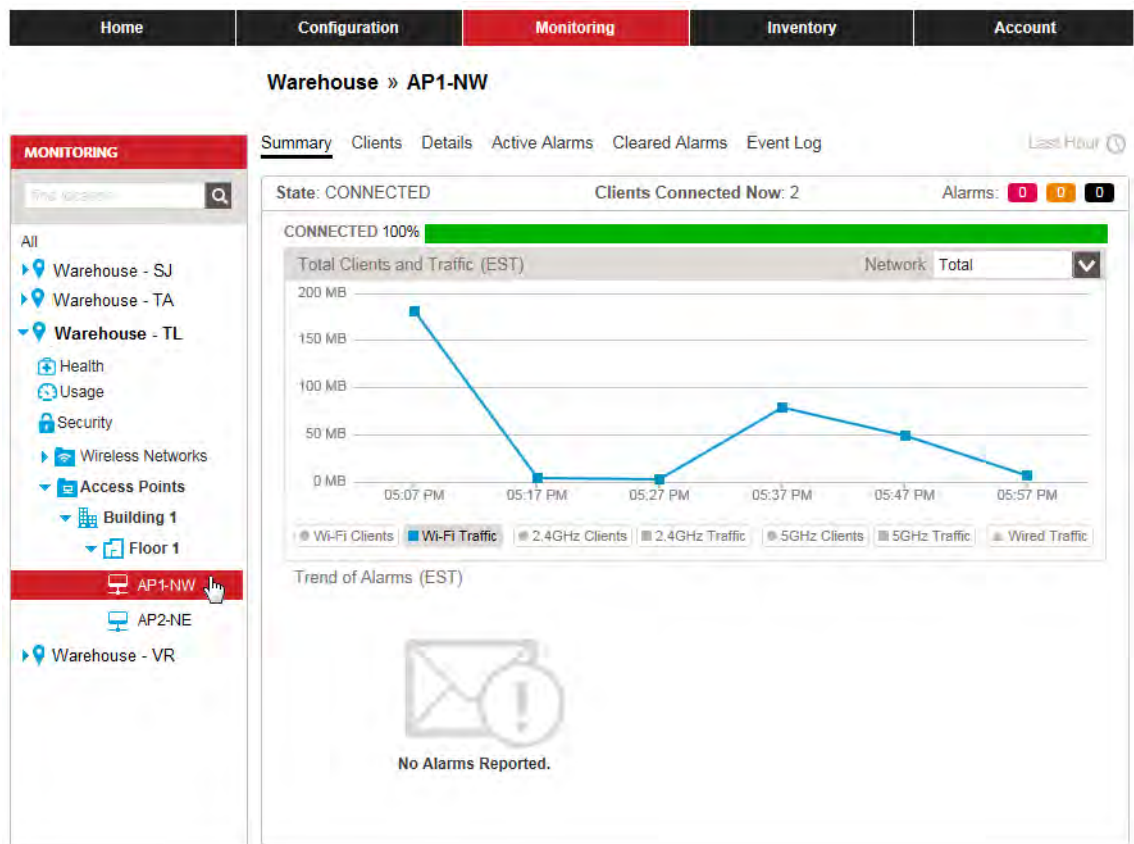


Figure 180. Access Point Summary Window

AP Details Windows

The AP Details windows display the following information about the access points in your account:

- ☐ Name
- ☐ Status
- ☐ Alarm state
- ☐ Uptime
- ☐ Model
- ☐ Number of neighbors
- ☐ IP address
- ☐ Channels
- ☐ Number of wireless clients per radio

AP Details windows are available from these two levels in the Monitoring menu.

- ☐ All - Displays details for all access points in your account.
- ☐ Health - Displays details for the access points in a location.

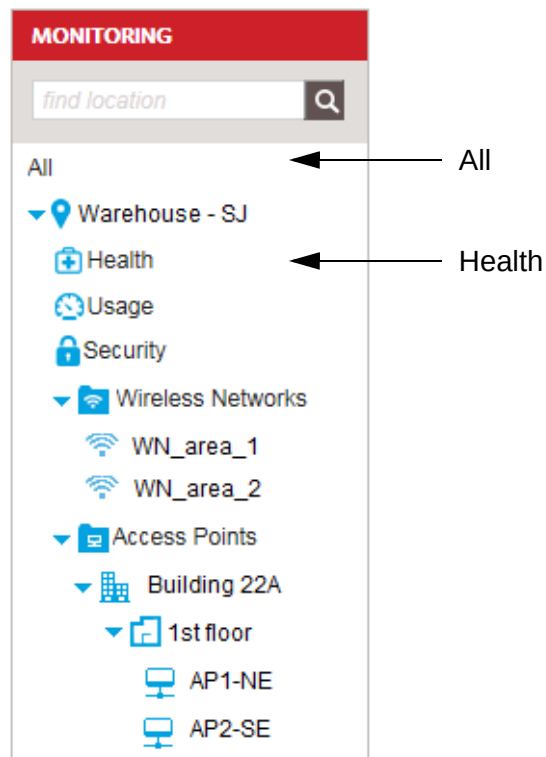


Figure 181. AP Details Windows in the Monitoring Menu

An example of the AP Details window at the All level is shown in Figure 193.

Account Statistics

MONITORING

Summary **AP Details** Active Alarms Cleared Alarms Event Log Hotspot Users ▾ Last Hour ⌚

find location 🔍

All

- Warehouse - SJ
- Warehouse - TA
- Warehouse - TL
- Warehouse - VR

MANAGED ACCESS POINTS

Download Full Details

No.	Name ▾	Status ▾	Alarm State ▾	AP Uptime ▾	MAC ▾
		Select... ▾	Healthy ▾		
1	AP500-D2	Disconnected	Healthy	Unknown	6C:0B:84:E4:A0:20
2	SouthLab	Healthy	Healthy	6d:2h:14m	6C:0B:84:C5:AB:...
3	ProtoType-AP500	Healthy	Healthy	0d:0h:1m	6C:0B:84:C5:AC:...

Figure 182. AP Details Window

You need to use the horizontal scroll bar at the bottom of the window to view all the columns.

You can use the fields beneath the column titles to screen the table by a selected attribute. For example, entering the name of an access point in the Name column displays the information for that device.

To download the table as a CSV file, click the Download Full Details option in the upper left corner of the window and follow the prompts. Refer to Figure 183.

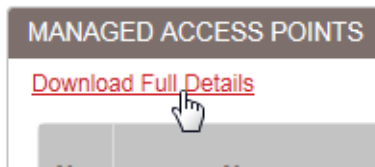


Figure 183. Download Full Details Option in the AP Details Window

Active Alarms Windows

Active alarms windows store messages of unresolved events from the access points. The windows are available from the three monitoring levels listed here.

- ❑ All - Displays the active alarms for all access points in your account.
- ❑ Health - Displays the active alarms for the access points in a selected location.
- ❑ Access point - Displays the active alarms for a selected access point.

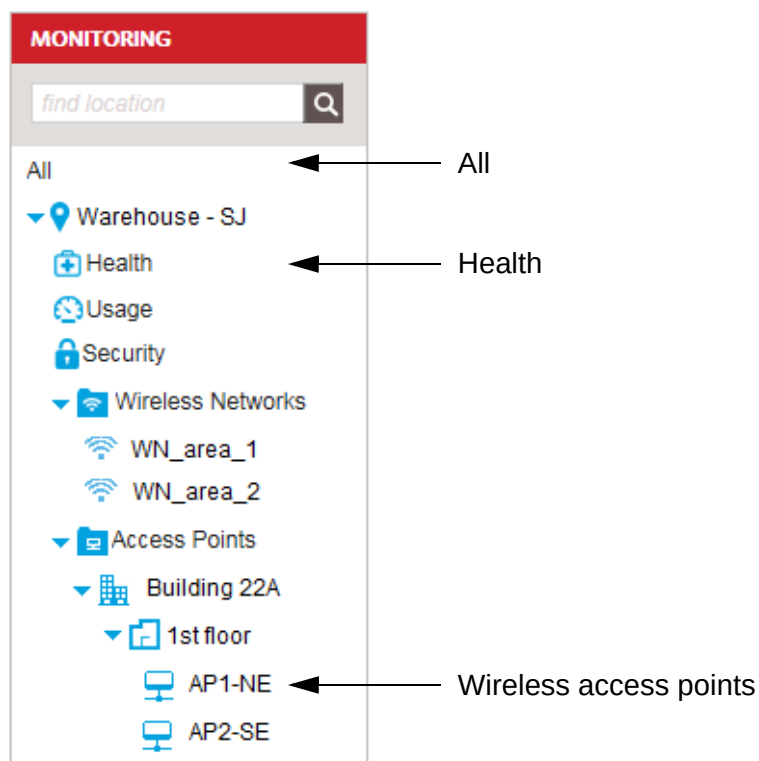


Figure 184. Active Alarms Windows in the Monitoring Menu

An example of the Active Alarms window at the All level is shown in Figure 185 on page 265.

The screenshot shows the 'Active Alarms' window. The top navigation bar includes 'Home', 'Configuration', 'Monitoring' (highlighted), 'Inventory', and 'Account'. Below this is the 'Account Statistics' section with a 'Choose Action' dropdown. The main content area has tabs for 'Summary', 'AP Details', 'Active Alarms' (selected), 'Cleared Alarms', 'Event Log', and 'Hotspot Users'. A 'Last Hour' filter is also present. On the left, there's a 'MONITORING' sidebar with a search bar and a list of locations: Warehouse-SJ, Warehouse-TA, Warehouse-TL, and Warehouse-VR. The main table is titled 'Download Full Active Alarms' and has columns: Acknowledged, Title, Source, and Location Name. The table contains two rows of data, both showing 'AP disconnected unexpectedly' as the title, with different MAC addresses in the Source column and 'Warehouse-TA' as the Location Name. Both are marked as 'No' in the Acknowledged column.

	Acknowledged	Title	Source	Location Name
☐	No	AP disconnected unexpectedly	AP 6C:0B:84:D4:12:3B	Warehouse-TA
☐	No	AP disconnected unexpectedly	AP 6C:0B:84:D4:12:98	Warehouse-TA

Figure 185. Active Alarms Window

The window has these columns:

- ☐ Acknowledged - Whether you or another administrator has acknowledged the alarm.
- ☐ Title - Alarm title.
- ☐ Source - The IP address of the access point that was the source of the alarm.
- ☐ Location Name - The name of the location entry containing the access point that was the source of the alarm.
- ☐ Severity - The severity of the alarm. The severity can be critical, major, or minor.
- ☐ Alarm Time - Time and day when the alarm occurred.

You need to use the horizontal scroll bar at the bottom of the window to view all the columns.

You can add these optional columns to the window:

- ☐ Raised By - The event that caused the alarm.
- ☐ Cleared By - The event that has to occur to clear the alarm.
- ☐ Count - The number of times the same access point has experienced the alarm.
- ☐ Acknowledged By - The administrator who acknowledged the alarm.
- ☐ Acknowledge Time - The time and day when the alarm was acknowledged.

To add or remove optional columns, place the cursor anywhere in the header of the table and right click to display the optional column menu. Refer to Figure 186 on page 266.

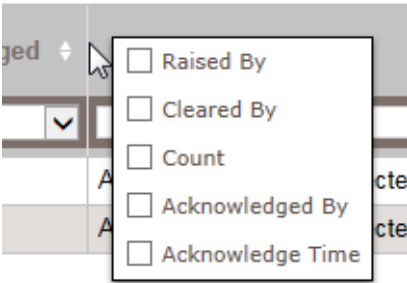


Figure 186. Optional Columns Menu in the Active Alarms Window

Adding a check mark to a dialog box adds an optional column to the window and removing a check mark removes a column. The default is no optional columns. Optional columns are added to the far right in the window.

You can use the fields beneath the column titles to screen the table by a selected attribute. For example, entering the MAC address of an access point in the Source column displays the information only for that device.

You can view additional information about an alarm by clicking its arrow in the second column in the window. Refer to Figure 187.

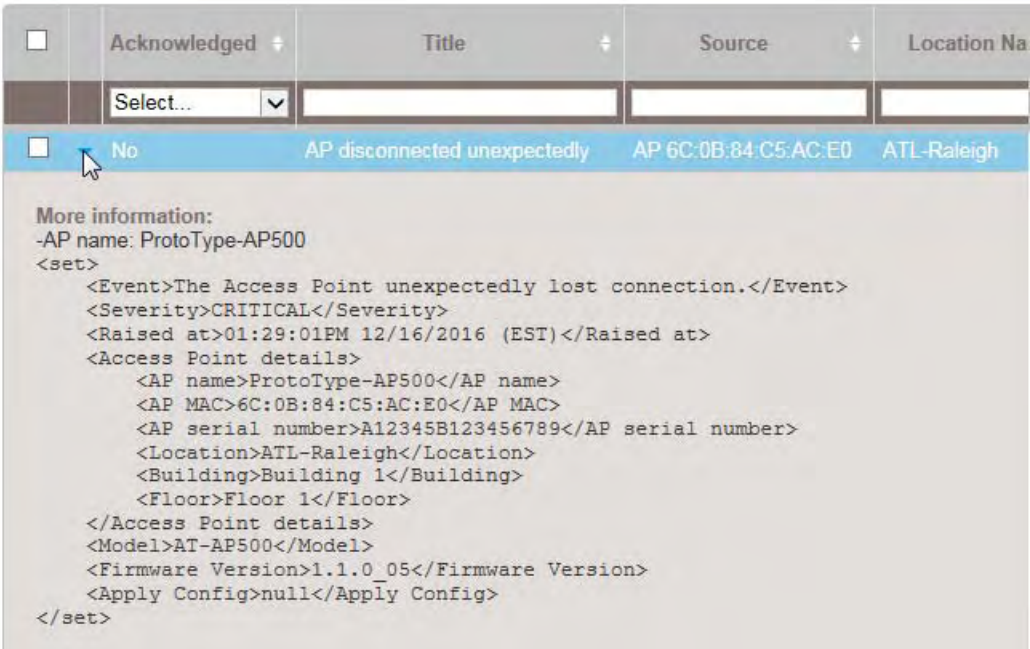


Figure 187. Expanded Alarm Information

To download the table as a CSV file, click the Download Full Active Alarms option in the upper left corner of the window and follow the prompts. Refer to Figure 188 on page 267.

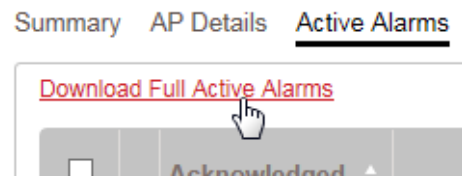


Figure 188. Download Full Active Alarms Option in the Active Alarms Window

Cleared Alarms Windows

Cleared alarms windows display resolved active alarms. The windows are available from these three levels in the Monitoring menu.

- ❑ All - Displays cleared alarms for all access points in your account.
- ❑ Health - Displays cleared alarms for the access points in a selected location.
- ❑ Access point - Displays cleared alarms for a selected access point.

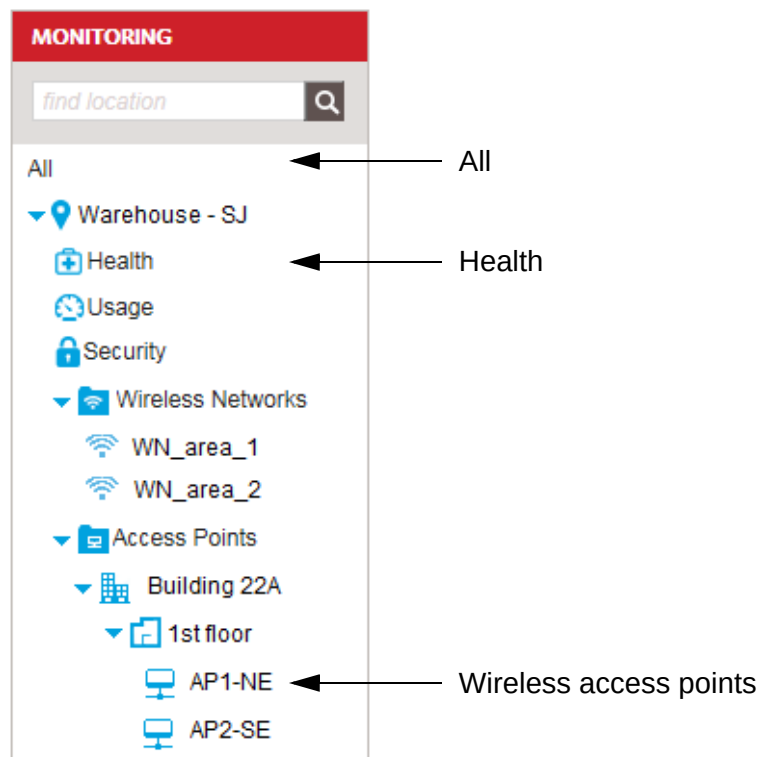


Figure 189. Cleared Alarms Windows in the Monitoring Menu

An example of the Cleared Alarms window from the All level is shown in Figure 190 on page 269.

Account Statistics Choose Action

Summary AP Details Active Alarms **Cleared Alarms** Event Log Hotspot Users ▾ Last Hour

MONITORING

find location

All

- Warehouse-SJ
- Warehouse-TA
- Warehouse-TL
- Warehouse-VR

Download Full Cleared Alarms

☐	Title	Source	Location Name	Severity
☐	AP disconnected unexpectedly	AP 6C:0B:84:D4:12:3B	Warehouse-TA	Critical
☐	AP disconnected unexpectedly	AP 6C:0B:84:D4:12:98	Warehouse-TA	Critical

Figure 190. Cleared Alarms Selection

The window has these columns:

- ☐ Title - Alarm title.
- ☐ Source - The IP address of the access point that was the source of the alarm.
- ☐ Location Name - The name of the location entry containing the access point that was the source of the alarm.
- ☐ Severity - The severity of the alarm. The severity can be critical, major, or minor.
- ☐ Alarm Time - Time and day when the alarm occurred.

You need to use the horizontal scroll bar at the bottom of the window to view all the columns.

You can add these optional columns to the window:

- ☐ Raised By - The event that caused the alarm.
- ☐ Cleared By - The event that has to occur to clear the alarm.
- ☐ Count - The number of times the same access point has experienced the alarm.
- ☐ Acknowledged By - The administrator who acknowledged the alarm.
- ☐ Acknowledge Time - The time and day when the alarm was acknowledged.

To add or remove optional columns, place the cursor anywhere in the header of the table and right click to display the optional column menu. Refer to Figure 186 on page 266. Adding a check mark to a dialog box adds an optional column to the window and removing a check mark removes a column. The default is no optional columns. Optional columns are added to the far right in the window.

You can use the fields beneath the column titles to filter the table by a

selected attribute. For example, entering the MAC address of an access point in the Source column displays the information only for that device.

To view additional information about an alarm, click its arrow in the left column. For an example, refer to Figure 187 on page 266.

To download the table as a CSV file, click the Download Full Cleared Alarms option in the upper left corner of the window and follow the prompts. Refer to Figure 191.

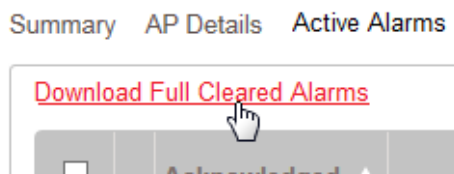


Figure 191. Download Full Cleared Alarms Option in the Active Alarms Window

Event Log Windows

Event log windows display operational messages from the access points in your AlliedView Cloud account. You can use the message to determine the status of the devices as well as troubleshoot problems. The messages are grouped into the following categories:

- ☐ Critical
- ☐ Warning
- ☐ Informational
- ☐ Debug

Event log windows are available from the following four levels in the Monitoring menu:

- ☐ All - Displays the events for all the access points in your account.
- ☐ Health - Displays the events for the wireless networks and access points in a selected location.
- ☐ Wireless networks - Displays the events for a selected wireless network.
- ☐ Wireless access points - Displays the events for an access point.

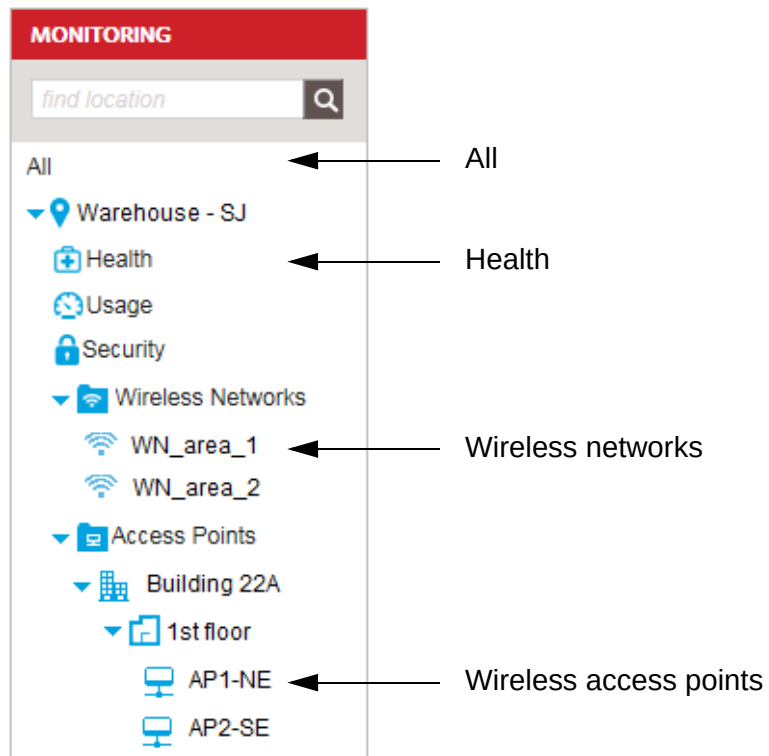


Figure 192. Event Log Windows in the Monitoring Menu

The Event Log option is shown in Figure 193 on page 272.

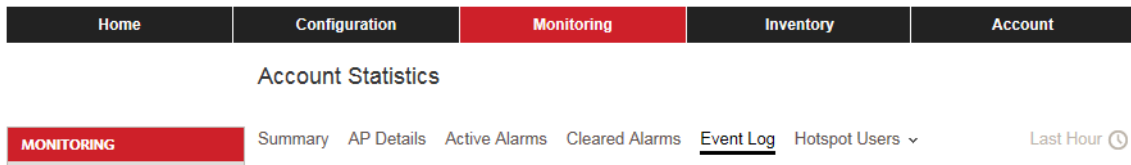


Figure 193. Event Log Selection

Here are the guidelines to event log windows:

- ❑ Event logs are available for connected access points, which are access points your AlliedView Cloud account can actively detect and manage.
- ❑ Event log windows do not contain messages from disconnected devices, which are access points that your account cannot detect, possibly because of a communication problem or because they are off-line.
- ❑ Event long windows are also not available for access points that are not assigned to a location.

Hotspot Users Windows

The Hotspot User windows display the wireless clients and activity statistics of your hotspots. The Hotspot Users monitoring windows are found at these levels in the Monitoring menu:

- ☐ All - Displays hotspot usage and client activity for all hotspots in your account.
- ☐ Usage - Displays hotspot usage and client activity for a selected location.
- ☐ Wireless networks - Displays hotspot usage and client activity for a selected wireless network.

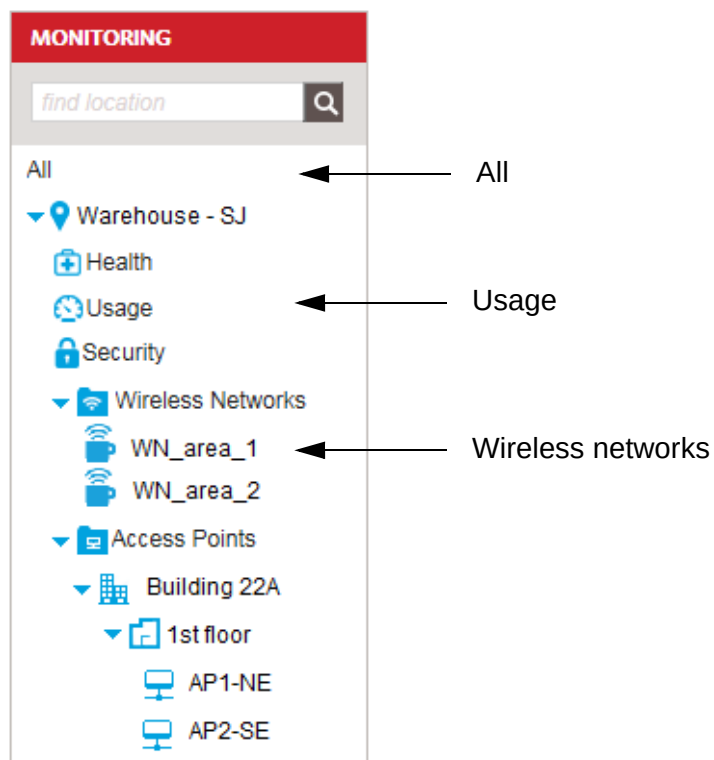


Figure 194. Hotspot Users Windows in the Monitoring Menu

The Hotspot Usage selection displays hotspot usage in trend graphs for any captive portal type for your account. These graphs display the connected time for paid and free captive portal access. You can also check paid and free number of devices and traffic.

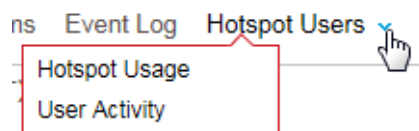


Figure 195. Hotspot Users Menu Selections

Details Window

The Details window displays the following information about the individual access points in your account:

- ❑ IP configuration settings and other detailed information.
- ❑ LAN statistics (for example, number of receive and transmit packets on the LAN port).
- ❑ Wireless statistics (for example, packet information).

The Details monitoring window is only available from individual access points in the Monitoring menu.

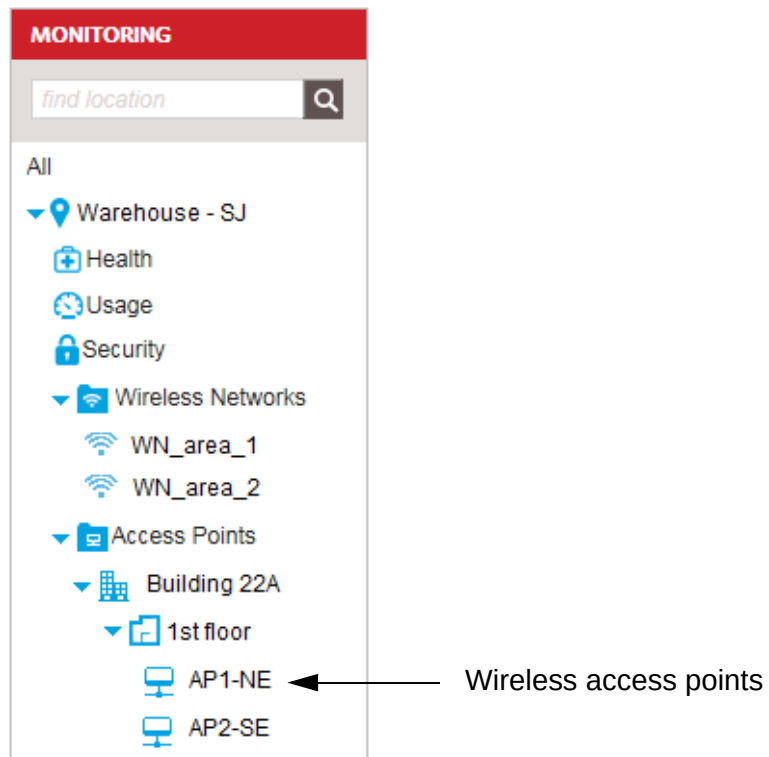
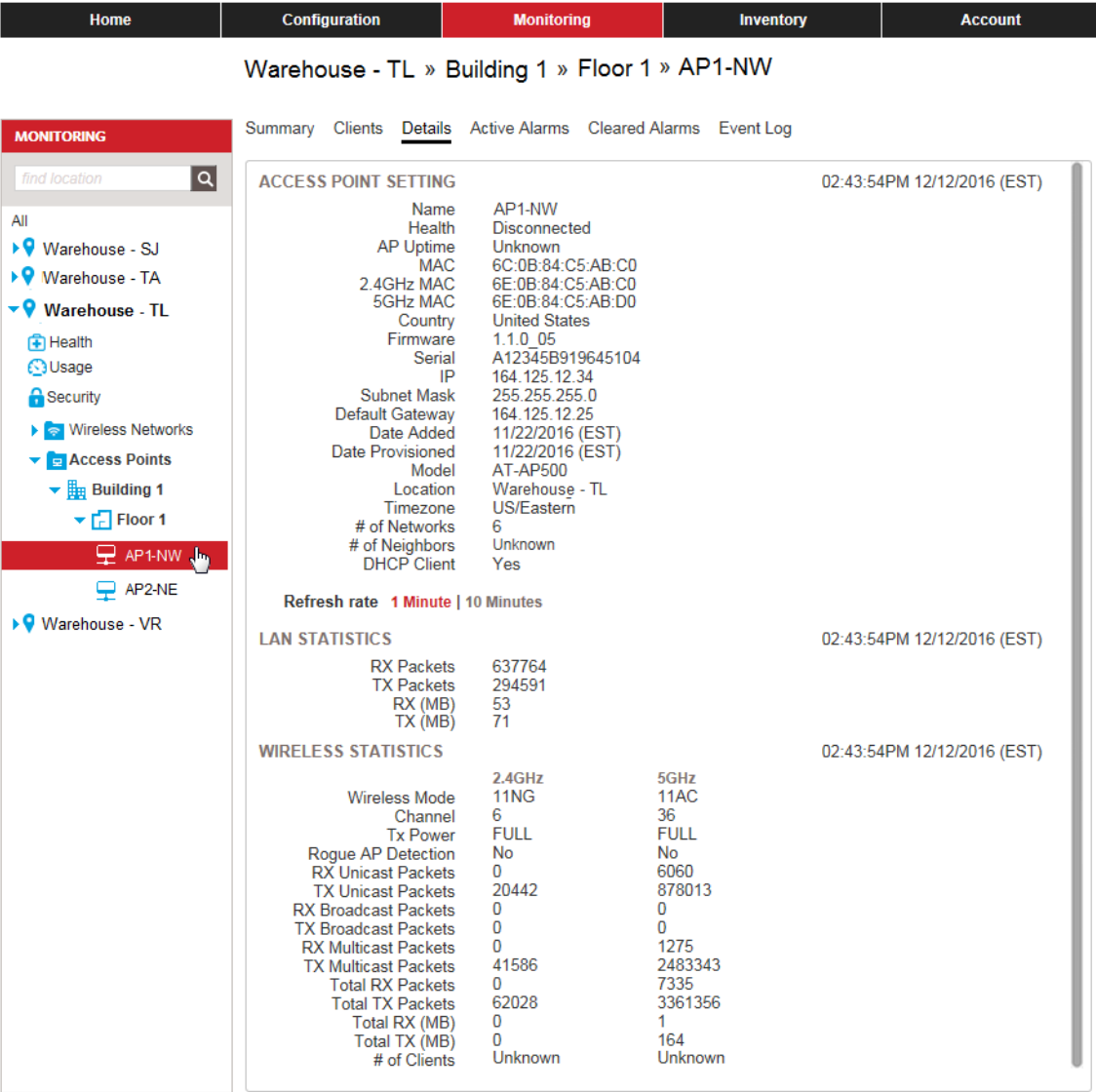


Figure 196. Detail Window in the Monitoring Menu

An example of the Details window is shown in Figure 197 on page 276.



Command Log Window

Your changes to the configuration settings of access points are stored in the command log window of your AlliedView Cloud account. You can use the window to determine the status of your changes, such as whether they were successfully implemented by the access points, as well as view a history of your changes. Here are the guidelines to the command log window:

- ❑ The command log window is only available from the Health level of in the Monitoring menu of a location entry. Consequently, it displays the configuration changes for all the access points of a selected location.
- ❑ The command log stores commands of connected access points, which are access points the AlliedView Cloud has detected. It does not store commands of disconnected access points or access points that are not assigned to a location.

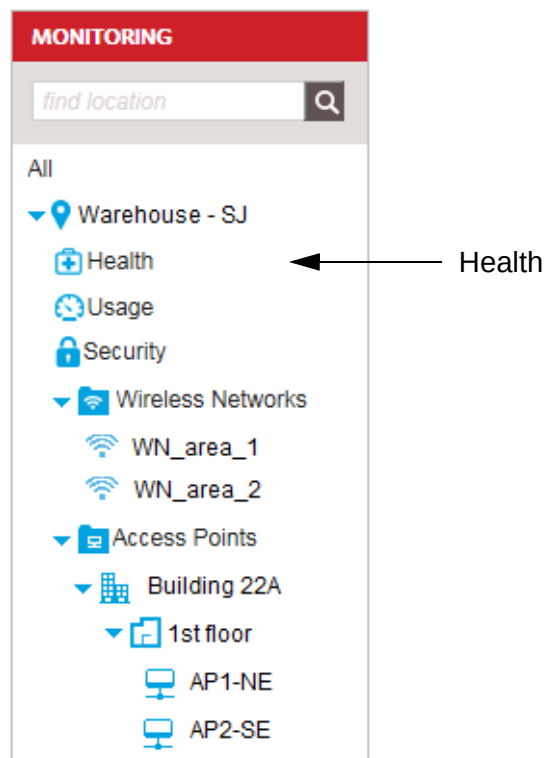


Figure 198. Command Log Window in the Monitoring Menu

Chapter 15

Licenses and Tokens

This chapter describes license tokens, adding licenses to an account, and displaying license information.

This chapter includes the following sections:

- ❑ “Introduction to Licenses and Tokens” on page 280
- ❑ “Viewing Licenses and Tokens” on page 281
- ❑ “Adding New Licenses” on page 283

Introduction to Licenses and Tokens

The AlliedView Cloud application requires a license and tokens. One token provides one calendar month of cloud support for one access point. New licenses can be purchased and added to your account at any time.

To obtain new licenses and tokens, submit requests through your Allied Telesis 24/7 Support account.

If you do not purchase licenses for the AlliedView Cloud application, you lose access to it and your wireless networks, as follows:

- ❑ A one-week grace period begins the day after the end of the license period. You can only access the Home page monitoring summary. For one week, access points retain their configurations and continue to provide wireless connectivity, including guest access and authentication cloud services.
- ❑ The one-week grace period ends after seven days. The access points are reset to the factory default configurations and the radios are disabled. However, the access points remain in the account. Adding a new license re-activates the account and access points.
- ❑ Thirty days after the end of the grace period, the AlliedView Cloud account is de-activated.

Viewing Licenses and Tokens

To display the current licenses and tokens in your account, do the following:

1. Click the **Account** tab.
2. In the Account menu in the left margin, select **Licenses**.

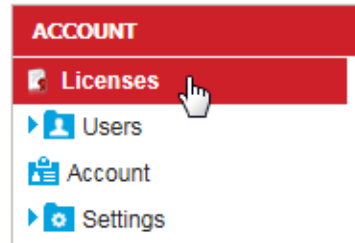


Figure 199. Licenses Selection in the Account Menu

The screen displays the licenses, license renewal date, remaining tokens, and the average number of tokens used per month.

115 TOKENS Available		DEC 2016 Renewal	74 TOKENS Used This Month
Sort by Date Added Status License Key Tokens Remaining SKU			
	QT05ODE3MjU2Ny0zCkM9MQpLPTk5MC0xMjMtNDU2NzgK	Used Up	
	QT05ODE3MjU2Ny0zCkM9MQpLPTk5MC0xMjMtNDU2NzgK	Used Up	
	QT1BbGxpZWQgVGVsZXNpcwpDPTEwMDAKSz0xMjM0NTY	In Use	

Figure 200. Display Licenses

3. Click the license key to check a license's details.

115 TOKENS
Available

DEC 2016
Renewal

74 TOKENS
Used This Month

Sort by [Date Added](#) | [Status](#) | [License Key](#) | [Tokens Remaining](#) | [SKU](#)

QT05ODE3MjU2Ny0zCkM9MQpLPTk5MC0xMjMtNDU2NzgK

Used Up

QT05ODE3MjU2Ny0zCkM9MQpLPTk5MC0xMjMtNDU2NzgK

Used Up

QT1BbGxpZWQgVGVsZXNpcwpDPTEwMDAKSz0xMjM0NT

In Use

Status: In Use
SKU: 1234567890

Date Added: 2016-05-19 (PDT)
Date Activated: 2016-05-19 (PDT)

Token Remaining: 868
Token Used: 132

No.	AP Serial	Date Used
1	A00019B000000000B00	10:37:15AM 05/19/2016 (PDT)
2	A00020B000000000B00	10:37:16AM 05/19/2016 (PDT)

Figure 201. License Key Details

The screen displays the license status, SKU, date activated, and remaining and used tokens.

Adding New Licenses

To add a new license to your account, do the following:

1. Submit a request for a new license and tokens through your Allied Telesis 24/7 Support account.
2. When you receive the new license from Allied Telesis, store it on your computer or a network server.
3. Open the file as an ASCII text file with a word processor.

Figure 202 is an example of a license.

```
-----BEGIN LICENSE KEY-----
nnnnnnnnnnQz0xCks9OTkwLTEyMy00NTY30ApMPTMKVD0xNDc5MjM1ODM5MDc3ClY9MgpTPW8rZH1hM3:
hOeXFmS1V4Z2pJUncxQVp5QzZpQWZoaTJVdUhjUl1h2VmNnnnnnnnnnwNWErNVpaajV1RWcrQ0JwQ2Na:
YnBscWkyWEJOWXVtdHRYZ0xKRWtXbXZSR0p3OUd1NTb21mMXEWVidk1Vd1Q1SlZrQi91VTArbU11c2:
d4WjYxNk5QMUplTnnnnnnnnnZZbzE0L2ZUN1ZkYm55cWU4ak91UnlNS0hrcEnnnnnnnnn11Z2ZCFFFm:
VFU5MHA4T0J1R3FJdWINTb21mMXEU0FzZFZXMG00d3ZHQnhBWURETnhPbyETWZaR2xoTDRHSzFRWH:
dHaTJxVHFCOXZuZVd5TzVjMHRvY2ZSeVZEdW9peFNuQm5KQzFjZDB4Zm1Ma2FwNFVjTG50SEgyNWZF:
ODNzTFRidlJmU1lFenl1NE9MVlNTb21mMXExSXBtSXBnVUtsM3Rjnnnnnnnn
-----END LICENSE KEY-----
```

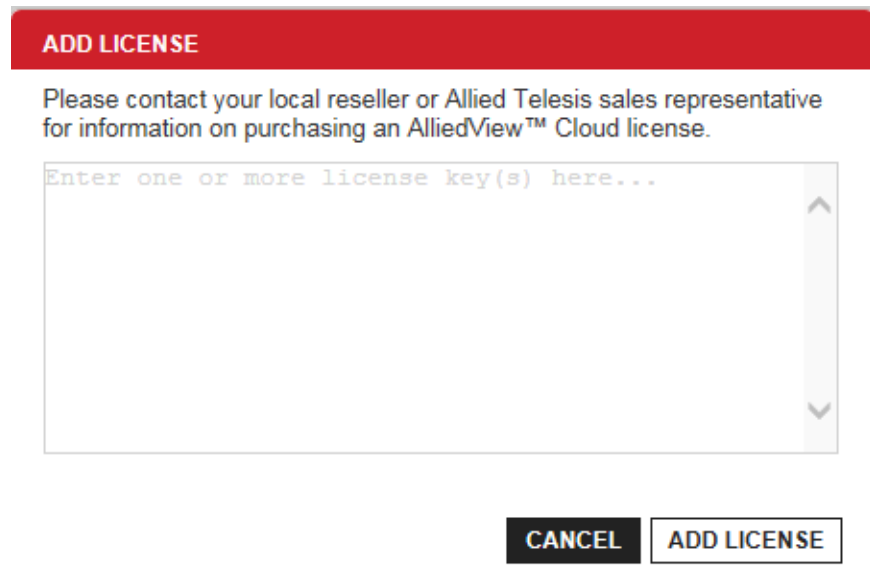
Figure 202. License Example

4. Copy the license. Do not include the BEGIN LICENSE KEY or END LICENSE KEY text.
5. If you have not started a management session with your AlliedView Cloud account yet, start a session now.
6. Click the **Account** tab.
7. In the Account menu in the left margin, select **Licenses**. Refer to Figure 199 on page 281.
8. Select **Add License** from the Choose Action menu.



Figure 203. Add License in the Choose Action Menu

The program displays the Add License window:



ADD LICENSE

Please contact your local reseller or Allied Telesis sales representative for information on purchasing an AlliedView™ Cloud license.

Enter one or more license key(s) here...

CANCEL **ADD LICENSE**

Figure 204. Add License Window

9. In the Add License window, paste in the license key you copied in step 4.

10. Click the **ADD LICENSE** button.

The license is validated, and the application displays the license(s), number of available tokens, license renewal date, and average number of tokens used per month.

11. Repeat this procedure to add more licenses.

Chapter 16

Firmware Updates of Access Points

This chapter describes maintaining the access point firmware. The chapter includes the following sections:

- ❑ “Introduction to Access Point Firmware Maintenance” on page 286
- ❑ “Schedule Firmware Upgrades” on page 287
- ❑ “Upgrade When Firmware is Available” on page 289
- ❑ “Automatic Upgrades” on page 291

Introduction to Access Point Firmware Maintenance

Allied Telesis, Inc. may periodically release new firmware for the access points. You are notified about releases with messages in the Notification Center.

You can manage access point firmware upgrades in one of the following ways:

- ❑ Let AlliedView Cloud automatically upgrade the firmware. The program automatically upgrades all access points in the cloud seven days after new firmware becomes available. This is the default.
- ❑ Schedule firmware upgrades. You might want to limit upgrades to non-business hours so as to prevent
- ❑ Upgrade access point firmware as soon as it is available.

This chapter describes the following:

- ❑ “Schedule Firmware Upgrades” to schedule firmware upgrades for specified times or days.
- ❑ “Upgrade When Firmware is Available” on page 289 to upgrade firmware as soon as it is available.
- ❑ “Automatic Upgrades” on page 291 to return to automated upgrades.

Schedule Firmware Upgrades

The AlliedView Cloud program has a schedule that you can use to control when it can upgrade the firmware on your access points. By configuring the schedule for non-business hours, you can prevent the program from updating firmware during business hours, and interrupting wireless network service.

To configure a schedule, do the following:

1. Click the **Account** tab.
2. From the Account menu in the left margin, click **Settings -> Schedule Firmware**

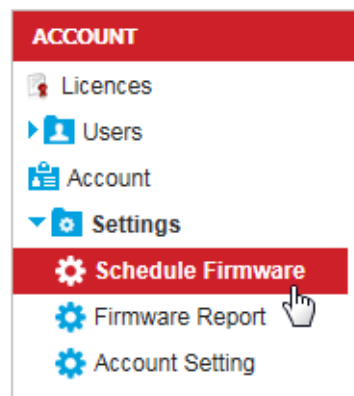


Figure 205. Schedule Firmware Selection in the Account Menu

3. Select **Scheduled** from the Firmware Upgrade pull-down menu:

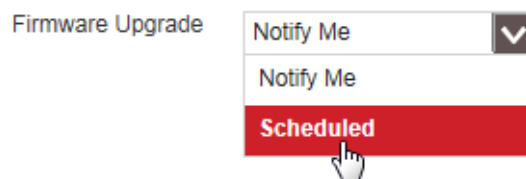
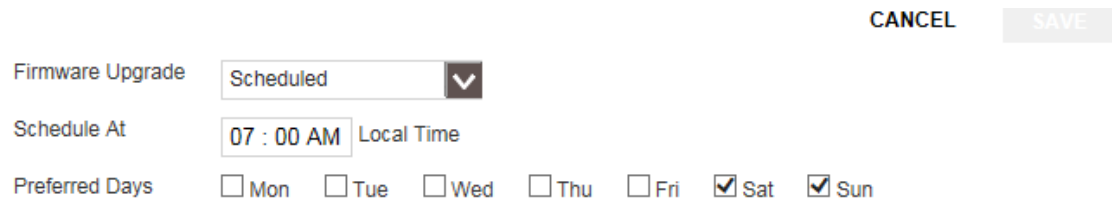


Figure 206. Scheduled Selection in the Firmware Upgrade Menu

The program displays the scheduling area:



The image shows a web interface for scheduling a firmware upgrade. At the top right are two buttons: 'CANCEL' and 'SAVE'. Below these are three rows of settings. The first row, 'Firmware Upgrade', has a dropdown menu set to 'Scheduled'. The second row, 'Schedule At', has a time input field showing '07 : 00 AM' and a 'Local Time' label. The third row, 'Preferred Days', has checkboxes for each day of the week: Mon, Tue, Wed, Thu, Fri, Sat, and Sun. The checkboxes for Saturday and Sunday are checked.

Firmware Upgrade	Scheduled	▼
Schedule At	07 : 00 AM	Local Time
Preferred Days	☐ Mon	☐ Tue
	☐ Wed	☐ Thu
	☐ Fri	☒ Sat
		☒ Sun

Figure 207. Firmware Upgrade Scheduling Area

4. In the Schedule At field, set the time when an upgrade can begin: select the hour setting, then use up and down arrow keys to set the time. Repeat for the minute and AM/PM settings.
5. In the boxes next to Preferred Days, check the boxes of the days when upgrades are allowed.
6. Click **SAVE** to activate your changes or **CANCEL** to cancel the action.

Upgrade When Firmware is Available

If you received a notification message about new firmware and want to upgrade access points right now, do the following:

1. Click the **Account** tab.
2. From the Account menu in the left margin, click **Settings -> Firmware Report**:

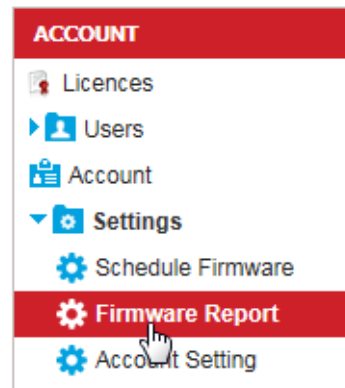


Figure 208. Clicking Firmware Report

3. In the Firmware Report Screen, click an access point under the Model column.

A window appears with more detailed information.

[RELEASE NOTES](#)

Firmware Version: 0.0.2_12 (Test)

AP Model: AT-AP500

Release Date: 06/21/2016 (PDT)

Started: 05:39 AM 06/22/2016 (PDT)

► Summary

Upgrade Progress

Show Location All Location ▼

Access Point Name	Queued	Downloading	Upgrading	Complete
AP500-Bench				Up To Date
AP500-SouthLab				Completed
AP500-Desk				Completed

Figure 209. Firmware Report Details

4. To check release notes on the access point, click **RELEASE NOTES**. Otherwise, skip to Step 5.
5. Click **UPGRADE NOW**.

The screen shows the upgrade process. The upgrade status is shown when the upgrade is finished.

Automatic Upgrades

To change from scheduled upgrades to automatic upgrades, do the following:

1. Click the **Account** tabs.
2. From the Account menu in the left margin, click **Settings** -> **Schedule Firmware** as shown in Figure 205 on page 287.
3. Select **Notify Me** from the Firmware Upgrade pull-down menu:

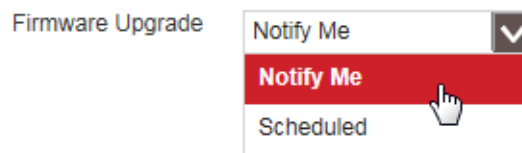


Figure 210. Notify Me Selection in the Firmware Upgrade Menu

4. Click **SAVE** to activate your changes or **CANCEL** to cancel the action.

Chapter 17

Accounts and Notifications

This chapter describes managing user accounts, editing the organization's name and address, and checking AlliedView Cloud notifications.

This chapter includes the following sections:

- ❑ “AlliedView Cloud User Accounts” on page 294
- ❑ “Inviting Users to Add AlliedView Cloud Accounts” on page 295
- ❑ “Accepting Invitations and Adding User Accounts” on page 298
- ❑ “Changing User Roles” on page 299
- ❑ “Deleting Users” on page 301
- ❑ “Viewing or Changing Your User Profile” on page 302
- ❑ “Viewing or Changing the Organization's Settings” on page 304
- ❑ “Checking Application Notifications” on page 305

AlliedView Cloud User Accounts

There are four types of AlliedView Cloud user accounts. They are listed here:

- ❑ Owner account - The owner account is added when the first person of a company or organization opens an AlliedView Cloud account. A company or organization can have only one owner account and the account cannot be changed or transferred to another account. The person with the owner account can view or manage all elements in the company's AlliedView Cloud account, and invite others to open new AlliedView Cloud accounts.
- ❑ Admin accounts - Admin accounts, like the owner account, give individuals full access to view or manage all elements in the company's AlliedView Cloud account. Admin accounts also allow users to invite others to open AlliedView Cloud accounts. The difference between owner and admin accounts is that there can be only one owner account while there can be any number of admin accounts.
- ❑ Read-only accounts - Read-only accounts give individuals permission to view the elements but not change any values.
- ❑ Hotspot clerk accounts - Hotspot clerk accounts allow individuals to manage hotspot vouchers. Only users with hotspot clerk accounts can manage vouchers.

Note

Users must have Allied Telesis 24/7 Support Accounts before they can add their own AlliedView Cloud accounts. For instructions, refer to "Opening a 24/7 Support Account" on page 53.

Inviting Users to Add AlliedView Cloud Accounts

This section contains the procedure for inviting other individuals in your company or organization to open their own AlliedView Cloud accounts so they can assist you in managing network devices. You can assign users a role of admin, read-only, or hotspot clerk. The roles are described in “AlliedView Cloud User Accounts” on page 294.

Note

Only users with owner or admin accounts can invite other individuals to open AlliedView Cloud accounts. Read-only or hotspot clerk account holders cannot invite others to open accounts.

Please perform the following steps before inviting a user to add an AlliedView Cloud account:

1. Instruct the user to perform “Opening a 24/7 Support Account” on page 53.

Note

When users are filling in the Company Name field in the Register for an Account window, they must be sure to enter exactly the same company or organization name that the owner entered when opening the first AlliedView Cloud account.

Note

Users must have Allied Telesis 24/7 Support accounts before being invited to add their own AlliedView Cloud accounts.

2. After the user has completed the procedure for opening a support account, instruct the user to send you his username (email address) of the account.

After receiving the username, perform the next procedure to invite the user to open an AlliedView Cloud account.

To invite a user to open an AlliedView Cloud account, do the following:

1. Click the **Account** tab.
2. Select **Invite User** from the Choose Action menu:



Figure 211. Invite User Selection in the Choose Action Menu

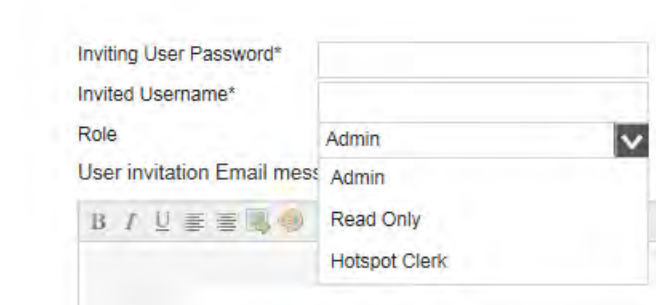
The program displays the Invite User window.

Invite User

Figure 212. Invite User Window

3. In the Inviting User Password field, enter your account password.
4. In the Invited Username field, enter the username (email address) of the 24/7 Support account of the user you are inviting to access the program.
5. From the Role pull-down menu, select one of the following:
 - ☐ **Admin:** Allows the user to view and configure all information in the account.
 - ☐ **Read Only:** Allows the user to view but not configure the information in the account.
 - ☐ **Hotspot clerk:** Allows the user to manage vouchers, but blocks the user from configuring or viewing the account.

Invite User



The screenshot shows the 'Invite User' window with the following fields and controls:

- Inviting User Password***: A text input field.
- Invited Username***: A text input field.
- Role**: A pull-down menu currently showing 'Admin' with a dropdown arrow.
- User invitation Email message**: A text area with a rich text editor toolbar (Bold, Italic, Underline, Bulleted List, Numbered List, Link, Image) and a 'Send' button.

The role pull-down menu is open, displaying the following options:

- Admin
- Admin
- Read Only
- Hotspot Clerk

Figure 213. Role Pull-down Menu in the Invite User Window

6. If desired, edit the text in the email.
7. Click **INVITE THIS USER** to activate your changes or **CANCEL** to cancel the action.

After you click **INVITE THIS USER**, the program sends an email invitation to the user.

Accepting Invitations and Adding User Accounts

This procedure is for users who have received invitations from the owner or an admin account holder to open their own AlliedView Cloud accounts. Users perform this procedure after opening Allied Telesis 24/7 Support accounts and receiving email invitations.

To open your own AlliedView Cloud account after receiving an invitation, do the following:

1. Open the AlliedView Cloud invitation email.
2. Click the **here** link.

The Invited User Sign Up screen is displayed.

3. Enter your password from your Allied Telesis 24/7 Support account (under your email address).
4. Enter your personal information in the **Information** area.
5. To see the terms and conditions:
 - a. Click the **Terms and Conditions** link.

The program displays the Terms and Conditions window.

- b. Click **CLOSE WINDOW**.
6. Click **Sign Up**.

If the sign-up is successful, the application sends a confirmation email.

7. Open the confirmation email.
8. Click the **here** link.

The program displays the New Account Activation screen.

9. Enter your password from your Allied Telesis 24/7 Support account.
10. Click **ACTIVATE**.

You are logged into your AlliedView Cloud account and the Home tab is displayed on your screen.

This completes the procedure for opening a new account.

Changing User Roles

This procedure explains how to change the roles of AlliedView Cloud account holders. Please review the following before performing the procedure:

- ☐ Only the owner or an administrator can change the role of a user.
- ☐ The role of the owner cannot be changed.
- ☐ An administrator cannot change his own role. The owner or another administrator must change it for him.

To edit the role of a user, do the following:

1. Click the **Account** tab.
2. In the Account menu in the left margin, click **Users**:

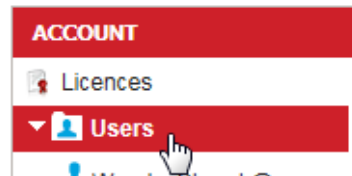


Figure 214. Users Selection in the Account Menu

The program displays the user accounts in alphabetical order.

3. Do one of the following to select a user:
 - ☐ If there are a small number of user accounts, click the user listed in the main area of the Account Users screen.
 - ☐ If there are a large number of user accounts, use the Search icons in the upper right of the main area of the Account Users screen to narrow the search (see Figure 215). Then click the account in the main area.

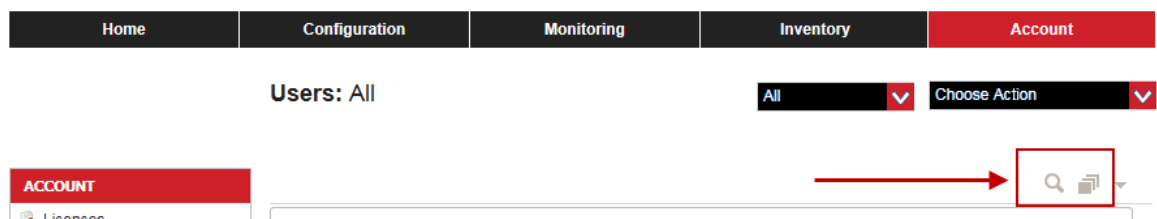


Figure 215. User Account Search Icons

4. Select one of the following from the Role menu:
 - ☐ **Admin:** Allows the user to view and configure all information in the

account.

- ☐ **Read Only:** Allows the user to view but not configure the information in the account.
 - ☐ **Hotspot clerk:** Allows the user to manage vouchers, but blocks the user from configuring or viewing the account.
5. Click **SAVE** to activate your changes or **CANCEL** to cancel the action.

Deleting Users

To delete a user account from your organization's account, do the following:

1. Click the **Account** tab.
2. In the Account menu in the left margin, click **Users** (see Figure 214 on page 299).
3. Select a user to delete (refer to “Changing User Roles” on page 299 for details on selecting a user). You can delete only one user at a time.
4. Select **Delete User** from the Choose Action menu:



Figure 216. Delete User Selection in the Choose Action Menu

The program deletes the selected user.

Viewing or Changing Your User Profile

Your user profile contains general information about your account, such as your username and address. Each account holder is responsible for maintaining his or her own profile. An account holder cannot view or edit a profile belonging to someone else.

To view or change your user profile, do the following:

- 1. From any window in the account, hover the cursor over your username next to Welcome.
- 2. Click **My Profile**.



Figure 217. Accessing Your Account Profile

Your profile is displayed.

User: John Smith

Choose Action

CANCEL

SAVE

▼ User Profile

Name

John Smith

Username

john_smith@aaainc.com

Email

john_smith@aaainc.com

Role

Admin

Phone

(408) 555-5555

Country

United States

▼

► Change Password

► User Preferences

Figure 218. My Profile Window

The window has the following four sections:

- ❑ User Profile: This section contains your name, username, email address, role, phone number, and country. The only adjustable

properties are your phone number and country. To change other properties, use your Allied Telesis 24/7 Support account.

- ☐ **Change Password:** You cannot change your password from your AlliedView Cloud account. To change it, change your password to your Allied Telesis 24/7 Support account. Both accounts use the same password.
 - ☐ **User Preferences:** You can use the options in this section to set the time zone or control whether you want to receive email alerts for access point alarms or firmware updates.
3. To change your phone number or country, enter the new information in the fields in the User Profile section of the window.
 4. To change user preferences, do the following:
 - a. Click **User Preferences** to expand the User Preferences section.
 - b. Use the Time Zone menu to select a different time zone.
 - c. To prevent automatic email notifications, check the following boxes under Email Notifications:
 - Don't send alarm notifications
 - Don't send new firmware notifications
 5. Click **SAVE** to activate your changes or **CANCEL** to cancel the action.

Viewing or Changing the Organization's Settings

To view or change your organization's address in your account, do the following:

1. Click the **Account** tab.
2. If it is not already selected, click the **Account** option in the Account menu in the left margin.

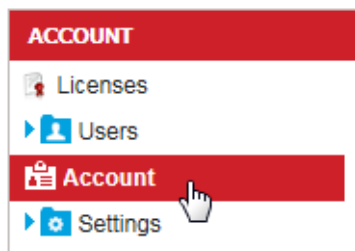


Figure 219. Account Selection in the Account Menu

The program displays the My Account window.

My Account

Choose Action ▼

Company Name	AAA Industries
Country	United States ▼
Zip Code	95134
Street Address	11 Hillside Drive
City	San Jose
State	California

Figure 220. My Account Window

3. Change the address, as needed. You cannot change the Company Name.
4. Click **SAVE** to activate your changes or **CANCEL** to cancel the action.

Checking Application Notifications

You can check application notifications to see if new firmware is available and firmware-upgrade-related events. These notifications are categorized by the following severity levels: Critical, Warning, and Info.

You can also mark the notifications as read. AlliedView Cloud automatically deletes application notifications after 30 days.

To check application notifications, do the following:

1. From any screen in the application, check the mailbox next to the user name in the upper right corner. If there are unread application notifications, a number appears on the mailbox indicating the number of notifications.
2. Click the mailbox:



Figure 221. Accessing Application Notifications

A list of application notifications appears containing information such as the type of notification (for example, new firmware), severity, and date.

- ☐ To select a monitoring period other than the default, click the icon at the upper right of the screen, then select one of the following periods from the menu: **Last Hour**, **Last 24 Hours**, **Last 7 Days**, or **Last 30 Days**.
 - ☐ To check details on a notification, click the triangle left of the notification or any field in any column. To hide details, click the triangle or field again.
 - ☐ Use the slider at the right of the screen to see more rows.
 - ☐ Use the table headings to sort information.
 - ☐ You can search for an item and narrow displayed information by typing in a field below a heading or selecting from a menu below a heading.
3. To mark all notifications as read, select **Mark All as Read** from the Choose Action menu. The number in the mailbox icon is cleared.

