



USER GUIDE

**cnMaestro c4000 Controller**

**System Release 1.0**



**Accuracy**

While reasonable efforts have been made to assure the accuracy of this document, Cambium Networks assumes no liability resulting from any inaccuracies or omissions in this document, or from use of the information obtained herein. Cambium reserves the right to make changes to any products described herein to improve reliability, function, or design, and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Cambium does not assume any liability arising out of the application or use of any product, software, or circuit described herein; neither does it convey license under its patent rights or the rights of others. It is possible that this publication may contain references to, or information about Cambium products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that Cambium intends to announce such Cambium products, programming or services in your country.

**Copyrights**

This document, Cambium products, and 3<sup>rd</sup> Party software products described in this document may include or describe copyrighted Cambium and other 3<sup>rd</sup> Party supplied computer programs stored in semiconductor memories or other media. Laws in the United States and other countries preserve for Cambium, its licensors, and other 3<sup>rd</sup> Party supplied software certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Cambium, its licensors, or the 3<sup>rd</sup> Party software supplied material contained in the Cambium products described in this document may not be copied, reproduced, reverse engineered, distributed, merged or modified in any manner without the express written permission of Cambium. Furthermore, the purchase of Cambium products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Cambium or other 3<sup>rd</sup> Party supplied software, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.

**Restrictions**

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Cambium.

**License Agreements**

The software described in this document is the property of Cambium and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement.

**High Risk Materials**

Cambium and its supplier(s) specifically disclaim any express or implied warranty of fitness for any high-risk activities or uses of its products including, but not limited to, the operation of nuclear facilities, aircraft navigation or aircraft communication systems, air traffic control, life support, or weapons systems (“High Risk Use”). Any High Risk is unauthorized, is made at your own risk and you shall be responsible for any and all losses, damage or claims arising out of any High-Risk Use.

# Contents

---

|  |           |
|--|-----------|
| <b>Chapter 1: Introduction to cnMaestro c4000 Controller .....</b> | <b>16</b> |
| Overview .....   | 16        |
| cnMaestro c4000 Controller Hardware Features .....                 | 17        |
| cnMaestro c4000 Controller Physical Features .....                 | 17        |
| cnMaestro c4000 Controller LED details .....                       | 18        |
| cnMaestro c4000 Controller Hardware Specifications .....           | 19        |
| cnMaestro c4000 Controller Reset “Button” .....                    | 19        |
| <b>Chapter 2: Installation and Upgrade .....</b>                   | <b>20</b> |
| Mounting cnMaestro c4000 Controller .....                          | 20        |
| Rack Mount .....   | 20        |
| Installing cnMaestro c4000 Controller .....                        | 22        |
| Login to Web UI .....  | 23        |
| Configure Country .....  | 24        |
| Change Default Password .....                                      | 24        |
| Login to web UI with New Password .....                            | 25        |
| Upgrading cnMaestro c4000 Controller .....                         | 25        |
| <b>Chapter 3: Deployment Models .....</b>                          | <b>30</b> |
| cnMaestro c4000 Controller as On-Premises .....                    | 30        |
| cnMaestro c4000 Controller as Tunnel Concentrator .....            | 30        |
| Typical Deployments .....  | 30        |
| Deployment Option 1 .....  | 31        |
| Deployment Option 2 .....  | 31        |
| Deployment Option 3 .....  | 32        |
| Configuring cnMaestro c4000 Controller .....                       | 33        |
| Configuring Management and Data Port .....                         | 33        |
| <b>Chapter 4: UI Navigation .....</b>                              | <b>36</b> |
| Account Type .....   | 36        |
| Access and Backhaul Account .....                                  | 36        |
| Industrial Internet Account .....                                  | 36        |
| Wireless LAN Account .....   | 36        |
| Home Page .....  | 37        |
| Page Structure .....   | 37        |

|   |           |
|---|-----------|
| Page Navigation .....   | 39        |
| Menu .....  | 39        |
| Header .....  | 39        |
| Access and Backhaul Account.....                                      | 39        |
| Overview.....   | 39        |
| Device Tree Navigation.....   | 39        |
| Wireless LAN Account.....   | 44        |
| Overview.....   | 44        |
| System.....   | 44        |
| APs.....  | 44        |
| AP Groups and WLANs.....  | 45        |
| Sites .....   | 45        |
| Side Menu.....  | 45        |
| Section Tabs .....  | 46        |
| System Status.....  | 46        |
| Logout.....   | 47        |
| <b>Chapter 5: Device Onboarding .....</b>                             | <b>48</b> |
| Overview .....  | 48        |
| Device Onboarding and Provisioning .....                              | 48        |
| Onboarding to cnMaestro Cloud Using MSN.....                          | 48        |
| Onboarding to cnMaestro On-Premises .....                             | 49        |
| Pre-Configuration and Approval of Devices (Optional).....             | 50        |
| Device Authentication (Optional).....                                 | 50        |
| Auto-Provisioning .....   | 51        |
| Other Options .....   | 53        |
| Directing Devices to the cnMaestro On-Premises Server Using DHCP..... | 55        |
| Claim using Cambium ID .....  | 57        |
| Claim Through Static URL without Cambium ID and Onboarding Key.....   | 57        |
| Claim Through Static URL with Cambium ID and Onboarding Key.....      | 58        |
| <b>Chapter 6: Network Monitoring.....</b>                             | <b>59</b> |
| Dashboard .....   | 59        |
| KPI (Key Performance Indicators) .....                                | 59        |
| Device Health.....  | 59        |
| Connection Health .....   | 60        |
| Charts and Graphs .....   | 60        |



|   |            |
|---|------------|
| Notifications.....                                  | 61         |
| Overview.....                                       | 61         |
| Events.....   | 62         |
| Alarms.....   | 63         |
| Statistics and Details.....                         | 65         |
| Performance.....                                    | 72         |
| Maps.....   | 80         |
| Map Navigation.....                                 | 82         |
| Mode.....   | 83         |
| Tools.....  | 85         |
| Tower-to-Edge View.....                             | 85         |
| cnPilot Tools.....                                  | 85         |
| cnReach Tools.....                                  | 88         |
| PMP Tools.....                                      | 89         |
| ePMP Tools.....                                     | 91         |
| cnMatrix Tools.....                                 | 94         |
| WIDS.....   | 95         |
| Detecting Rogue APs.....                            | 95         |
| <b>Chapter 7: cnPilot Dashboards.....</b>           | <b>101</b> |
| Device dashboard.....                               | 101        |
| Overview.....                                       | 101        |
| Clients.....  | 103        |
| Network Info.....                                   | 105        |
| Mesh Peers.....                                     | 108        |
| Neighbors.....                                      | 108        |
| Site Dashboard.....                                 | 108        |
| Wi-Fi Devices Availability (Total and Offline)..... | 110        |
| Throughput.....                                     | 110        |
| RF Quality.....                                     | 110        |
| AP Types.....                                       | 110        |
| Top Aps.....  | 111        |
| Channel Distribution by APs.....                    | 111        |
| Radio/WLAN Distribution by Aps.....                 | 111        |
| Clients by SNR.....                                 | 112        |
| Clients by Performance.....                         | 112        |

|  |            |
|--|------------|
| Wireless Clients Graph .....           | 112        |
| Throughput Graph .....                 | 113        |
| Wi-Fi Access Points.....               | 113        |
| Wireless Clients.....                  | 113        |
| Floor Plan .....                       | 114        |
| <b>Chapter 8: Reports.....</b>         | <b>115</b> |
| Generating Reports .....               | 115        |
| Device Report.....                     | 115        |
| Performance Report.....                | 118        |
| Active Alarms Report .....             | 121        |
| Alarms History Report.....             | 122        |
| Events Report .....                    | 122        |
| Clients Report .....                   | 123        |
| Mesh Peers Report.....                 | 124        |
| Remote Upload.....                     | 125        |
| Report Jobs.....                       | 125        |
| <b>Chapter 9: Software Update.....</b> | <b>127</b> |
| Software Update Overview.....          | 127        |
| Create Software Update Job .....       | 128        |
| Software Update Jobs .....             | 132        |
| Abort Software Job.....                | 133        |
| Viewing Running Jobs in Header .....   | 133        |
| cnReach Bulk Software Upgrade.....     | 134        |
| Firmware Versions (OS and Radio).....  | 134        |
| Bulk Upgrade Page.....                 | 134        |
| Upgrade Tracking.....                  | 135        |
| <b>Chapter 10: Inventory.....</b>      | <b>136</b> |
| Inventory Export .....                 | 137        |
| Bulk Move.....                         | 137        |
| Bulk Delete .....                      | 138        |
| Bulk Reboot.....                       | 139        |
| Schedule Reboot .....                  | 139        |
| CSV Configuration Import .....         | 140        |
| Sample Configuration File.....         | 141        |
| Uploading a Configuration File .....   | 141        |

|  |            |
|--|------------|
| <b>Chapter 11: Fixed Wireless Configuration .....</b>    | <b>144</b> |
| Overview .....   | 144        |
| Configuration Templates .....                            | 144        |
| Configuration Variables .....                            | 145        |
| Macros .....   | 146        |
| Variable Caching.....                                    | 146        |
| Device Type-Specific Configurations .....                | 146        |
| Variable Validation.....                                 | 146        |
| Sample Templates.....                                    | 146        |
| Template File Creation.....                              | 147        |
| Template .....   | 147        |
| Configuration Update.....                                | 147        |
| Device Selection .....                                   | 147        |
| Device Type.....   | 148        |
| Device Table.....  | 148        |
| Configuration Upgrade Steps.....                         | 149        |
| Jobs.....  | 150        |
| Onboarding Configuration Update .....                    | 151        |
| <b>Chapter 12: Wireless LAN Configuration.....</b>       | <b>152</b> |
| cnPilot Home and Enterprise.....                         | 152        |
| Configure cnPilot using cnMaestro c4000 Controller ..... | 152        |
| Create an AP Group .....                                 | 157        |
| Pre-Defined Overrides.....                               | 161        |
| User-Defined Overrides (Advanced) .....                  | 162        |
| User-Defined Variables (Advanced) .....                  | 162        |
| Factory Reset.....                                       | 163        |
| Association ACL .....                                    | 164        |
| Overview.....  | 164        |
| Configuring Association ACL.....                         | 164        |
| <b>Chapter 13: Services .....</b>                        | <b>167</b> |
| API Client .....   | 167        |
| Overview.....  | 167        |
| API Clients.....   | 167        |
| cnPilot GRE Tunnels.....                                 | 168        |
| Overview.....  | 168        |

|   |            |
|---|------------|
| Configuring L2GRE/EoGRE Tunnel Concentrator .....             | 168        |
| Access Control List (ACL) Configuration.....                  | 169        |
| cnPilot Guest Access .....                                    | 171        |
| Configuration .....   | 171        |
| SMS Authentication.....                                       | 182        |
| <b>Chapter 14: Appliance.....</b>                             | <b>197</b> |
| User Management .....   | 197        |
| Authentication.....   | 197        |
| Local Users.....  | 197        |
| Authentication Servers.....                                   | 204        |
| Session Management .....                                      | 214        |
| Jobs.....   | 215        |
| Configuration Update .....                                    | 215        |
| Software Update Jobs.....                                     | 216        |
| Reports.....  | 217        |
| Actions.....  | 217        |
| Server .....  | 218        |
| Dashboard.....  | 218        |
| Monitoring.....   | 220        |
| Settings .....  | 221        |
| Operations .....  | 225        |
| Diagnostics .....   | 229        |
| SSL Certificates.....   | 230        |
| Software Images.....  | 235        |
| Network.....  | 237        |
| Statistics.....   | 237        |
| Configuration .....   | 238        |
| Data Port solution for L2GRE deployment.....                  | 244        |
| Tools.....  | 246        |
| Access Control List (ACL) .....                               | 250        |
| Synchronize (Sync) Configuration .....                        | 252        |
| Manual Synchronization.....                                   | 253        |
| <b>Chapter 15: RADIUS Proxy .....</b>                         | <b>254</b> |
| Overview .....  | 254        |
| Minimum cnMaestro c4000 Controller Version Requirements ..... | 254        |

|  |            |
|--|------------|
| RADIUS Proxy Configuration.....                  | 254        |
| <b>Appendix: Windows DHCP.....</b>               | <b>256</b> |
| Configuring Option 60.....                       | 256        |
| Windows DHCP Server Configuration.....           | 256        |
| Configuring Option 43.....                       | 257        |
| Windows DHCP Server Configuration.....           | 257        |
| Configuring Option 15.....                       | 258        |
| Windows DHCP Server Configuration.....           | 258        |
| Configuring Vendor Class Identifiers.....        | 259        |
| Configuring the Policies at the SCOPE Level..... | 260        |
| <b>Appendix: Network Port Requirements.....</b>  | <b>264</b> |
| Network Port Requirements for Inbound.....       | 264        |
| Network Port Requirements for Outbound.....      | 264        |
| <b>Cambium Networks.....</b>                     | <b>265</b> |
| Feedback.....                                    | 265        |
| Contacting Cambium Networks.....                 | 265        |



# List of Figures

---

|   |    |
|---|----|
| Figure 1: cnMaestro c4000 Controller Front View .....                         | 17 |
| Figure 2: cnMaestro c4000 Controller Back View.....                           | 17 |
| Figure 3: Installing cnMaestro c4000 Controller.....                          | 23 |
| Figure 4 Controller on public IP address.....                                 | 31 |
| Figure 5 Controller and AP in private subnet in different VLAN.....           | 32 |
| Figure 6 Controller and AP in the same VLAN .....                             | 33 |
| Figure 7 cnMaestro c4000 Controller home page.....                            | 37 |
| Figure 8 cnMaestro c4000 Controller page structure.....                       | 38 |
| Figure 9 Device Tree navigation.....  | 40 |
| Figure 10 Wi-Fi AP Groups .....   | 42 |
| Figure 11 Map Navigation .....  | 43 |
| Figure 12 Node search .....   | 44 |
| Figure 13 APs.....  | 44 |
| Figure 14 Management page.....  | 45 |
| Figure 15 AP Groups.....  | 45 |
| Figure 16 Logout.....   | 47 |
| Figure 17 Onboarding to cnMaestro cloud using MSN .....                       | 49 |
| Figure 18 Onboarding to cnMaestro On-Premises.....                            | 49 |
| Figure 19 Pre-Configuration and Approval of Devices.....                      | 50 |
| Figure 20 Device Authentication .....   | 51 |
| Figure 21 Auto-Provisioning .....   | 52 |
| Figure 22 Claiming the device using MAC address (ESN).....                    | 53 |
| Figure 23 Claiming the device using Serial Number (MSN) .....                 | 54 |
| Figure 24 Claim the device using MAC address.....                             | 55 |
| Figure 25 Claim the device using MSN.....                                     | 55 |
| Figure 26 DHCP option 43.....   | 56 |
| Figure 27 DHCP option 15 .....  | 56 |
| Figure 28 Claim through static URL without Cambium ID and onboarding key..... | 58 |
| Figure 29 Claim through static URL with Cambium ID and onboarding key .....   | 58 |
| Figure 30 Key performance indicators .....                                    | 59 |
| Figure 31 Device Health.....  | 60 |
| Figure 32 Connection Health .....   | 60 |

|  |     |
|--|-----|
| Figure 33 Charts and Graphs .....                                  | 61  |
| Figure 34 Alarm Acknowledge .....                                  | 64  |
| Figure 35 Alarm History .....                                      | 65  |
| Figure 36 Map Street View .....                                    | 81  |
| Figure 37 Map Satellite View.....                                  | 82  |
| Figure 38 AP Configuration Page.....                               | 84  |
| Figure 39 Sector Visualization.....                                | 84  |
| Figure 40 Tower-to-Edge View .....                                 | 85  |
| Figure 41 cnPilot Tools .....                                      | 86  |
| Figure 42 cnReach Tools .....                                      | 89  |
| Figure 43 PMP Tools .....  | 91  |
| Figure 44 ePMP Tools.....  | 93  |
| Figure 45 Dashboard > Overview Page.....                           | 102 |
| Figure 46 R-Series: Device Dashboard > Wired Clients Page.....     | 103 |
| Figure 47 R-Series: Device Dashboard > Wireless Clients Page ..... | 103 |
| Figure 48 E-Series: Device Dashboard > Wireless Clients Page ..... | 104 |
| Figure 49 E-Series: Device Dashboard > Wired Clients Page.....     | 105 |
| Figure 50 R-Series: Device Dashboard > Network Info Page.....      | 106 |
| Figure 51 E-Series: Device Dashboard > Network Info Page .....     | 107 |
| Figure 52 PTP: Device Dashboard > Network Info Page.....           | 108 |
| Figure 53 Device Dashboard > Mesh Peers Page.....                  | 108 |
| Figure 54 Device Dashboard > Neighbors Page .....                  | 108 |
| Figure 55 Site Dashboard.....                                      | 109 |
| Figure 56 cnMatrix performance report .....                        | 119 |
| Figure 57 cnPilot performance report.....                          | 119 |
| Figure 58 cnReach Performance Report .....                         | 120 |
| Figure 59 ePMP performance report .....                            | 120 |
| Figure 60 PMP performance report .....                             | 121 |
| Figure 61 PTP performance report.....                              | 121 |
| Figure 62 Active alarms report .....                               | 122 |
| Figure 63 Alarms history report.....                               | 122 |
| Figure 64 Events report.....                                       | 123 |
| Figure 65 Clients report.....                                      | 123 |
| Figure 66 Mesh peers report.....                                   | 124 |
| Figure 67 Scheduling reports .....                                 | 125 |

|  |     |
|--|-----|
| Figure 68 Report jobs .....  | 126 |
| Figure 69 Software Update Overview .....                                     | 127 |
| Figure 70 Software Update Dashboard (cnPilot Enterprise AP) .....            | 128 |
| Figure 71 Software Update Dashboard (cnMatrix) .....                         | 129 |
| Figure 72 Scheduling Software Update Job .....                               | 129 |
| Figure 73 Retry Software Update .....  | 130 |
| Figure 74 Abort Software Job.....  | 133 |
| Figure 75 Bulk upgrade package.....  | 135 |
| Figure 76 Upgrade tracking .....   | 135 |
| Figure 77 Inventory - Access and Backhaul View.....                          | 136 |
| Figure 78 Inventory - Wi-Fi View .....                                       | 137 |
| Figure 79 Bulk Move.....   | 138 |
| Figure 80 Bulk Delete .....  | 138 |
| Figure 81 Bulk Reboot.....   | 139 |
| Figure 82 Import Device Configuration .....                                  | 140 |
| Figure 83 Sample configuration file .....                                    | 141 |
| Figure 84 Basic Template Configuration Flow.....                             | 144 |
| Figure 85 Sample ePMP Template.....  | 145 |
| Figure 86 Variable Usage .....   | 146 |
| Figure 87 Abort Configuration.....   | 149 |
| Figure 88 API Clients.....   | 167 |
| Figure 89 Configuring L2GRE/EoGRE Tunnel Concentrator.....                   | 168 |
| Figure 90 Logs and Statistics.....   | 169 |
| Figure 91 ACL Configuration .....  | 170 |
| Figure 92 MAC Layer ACL .....  | 170 |
| Figure 93 IP Layer ACL .....   | 170 |
| Figure 94 Transport Layer ACL .....  | 171 |
| Figure 95 Free access type configuration .....                               | 174 |
| Figure 96 Adding Users .....   | 198 |
| Figure 97 Changing Password.....   | 203 |
| Figure 98 List of Authentication Servers.....                                | 205 |
| Figure 99 Appliance > Add Authentication Server Type > Active Directory..... | 208 |
| Figure 100 Appliance > Add Authentication Server Type > LDAP .....           | 210 |
| Figure 101 Secondary Server Authentication.....                              | 212 |
| Figure 102 Session Management > Sessions .....                               | 215 |

|   |     |
|---|-----|
| Figure 103 Appliance > Jobs > Configuration update.....                           | 216 |
| Figure 104 Appliance > Jobs > Software update.....                                | 217 |
| Figure 105 Appliance > Jobs > Reports.....  | 217 |
| Figure 106 Appliance > Jobs > Actions.....  | 218 |
| Figure 107 Appliance > Server > Dashboard.....                                    | 220 |
| Figure 108 Appliance > Server > Monitoring.....                                   | 221 |
| Figure 109 Appliance > Server > Settings.....                                     | 225 |
| Figure 110 Alliance > Server > Operations > Reboot.....                           | 225 |
| Figure 111 Appliance > Server > Operations > Restore.....                         | 227 |
| Figure 112 Initiating upgrade.....  | 228 |
| Figure 113 Technical Support Dump.....  | 229 |
| Figure 114 Logging Level.....   | 229 |
| Figure 115 Services.....  | 230 |
| Figure 116 SSL Error Message.....   | 230 |
| Figure 117 Managing Device Software Images.....                                   | 235 |
| Figure 118 Automatically Update Device Software.....                              | 237 |
| Figure 119 Appliance > Network > Statistics.....                                  | 238 |
| Figure 120 Appliance > Network > Configuration > Management Port.....             | 240 |
| Figure 121 Appliance > Network > Configuration > Data Port.....                   | 240 |
| Figure 122 Appliance > Network > Configuration > Switched Virtual Interfaces..... | 241 |
| Figure 123 Appliance > Network > Configuration > Static Routes.....               | 241 |
| Figure 124 Management port in Access mode - DHCP.....                             | 242 |
| Figure 125 Management port in Access mode - Static.....                           | 242 |
| Figure 126 Data port in Access mode.....  | 243 |
| Figure 127 Data port in Trunk mode.....   | 243 |
| Figure 128 Single-port solution for Cambium GRE.....                              | 244 |
| Figure 129 Two-port solution for Cambium GRE.....                                 | 245 |
| Figure 130 Appliance > Network > Tools.....                                       | 247 |
| Figure 131 Appliance > Network > Tools > Ping Hostname.....                       | 248 |
| Figure 132 Appliance > Network > Tools > Ping IP.....                             | 248 |
| Figure 133 Appliance > Network > Tools > Trace Route Hostname.....                | 249 |
| Figure 134 Appliance > Network > Tools > Trace Route IP.....                      | 249 |
| Figure 135 Appliance > Network > Tools > Packet capture.....                      | 250 |
| Figure 136 ACL policy configuration.....  | 251 |
| Figure 137 GRE inter tunnel ACL configuration.....                                | 251 |

|  |     |
|--|-----|
| Figure 138 Ethernet ACL policies .....                     | 252 |
| Figure 139 SVI ACL policies.....                           | 252 |
| Figure 140 RADIUS Proxy on cnMaestro c4000 Controller..... | 254 |
| Figure 141 RADIUS Proxy Configuration .....                | 255 |



# List of Tables

---

|   |     |
|---|-----|
| Table 1 Front view components .....                                 | 17  |
| Table 2 Back view components .....                                  | 18  |
| Table 3 cnMaestro c4000 Controller LED details.....                 | 18  |
| Table 4 Hardware specifications .....                               | 19  |
| Table 5 Reset.....  | 19  |
| Table 6 Mounting steps.....   | 20  |
| Table 7 Structured Hierarchy Nodes.....                             | 40  |
| Table 8 Tree menu .....   | 42  |
| Table 9 Section Tabs.....   | 46  |
| Table 10 System status icon .....                                   | 47  |
| Table 11 Auto-Provisioning parameter details.....                   | 52  |
| Table 12 Notification parameters.....                               | 61  |
| Table 13 Event Severity .....                                       | 62  |
| Table 14 Alarm Life Cycle .....                                     | 63  |
| Table 15 Alarm Severity.....  | 63  |
| Table 16 Alarm Types.....   | 64  |
| Table 17 Device Statistics .....                                    | 65  |
| Table 18 Performance.....   | 72  |
| Table 19 Mode .....   | 83  |
| Table 20 cnReach Tools.....   | 88  |
| Table 21 PMP Tools.....   | 89  |
| Table 22 ePMP Tools .....   | 91  |
| Table 23 Parameters Displayed in Device Table .....                 | 130 |
| Table 24 Parameters displayed in Software Update Jobs tab.....      | 132 |
| Table 25 Error list .....   | 142 |
| Table 26 Parameters Displayed in the Device Table.....              | 148 |
| Table 27 Parameters displayed in the Configuration Update tab.....  | 150 |
| Table 28 Parameters displayed in configuring data tunnel page ..... | 169 |
| Table 29 Free Access Type Parameters .....                          | 175 |
| Table 30 Voucher Access Type Parameters .....                       | 177 |
| Table 31 Splash Page Parameters.....                                | 180 |
| Table 32 Sessions Parameters .....                                  | 182 |

|  |     |
|--|-----|
| Table 33 Role-Mappings .....   | 198 |
| Table 34 TACACS+ Parameters .....                                    | 205 |
| Table 35 RADIUS Parameters .....                                     | 207 |
| Table 36 Active Directory Parameters .....                           | 208 |
| Table 37 LDAP Parameters .....                                       | 210 |
| Table 38 Appliance > Server > Dashboard parameters .....             | 218 |
| Table 39 Configure: Appliance > Server > Monitoring parameters ..... | 220 |
| Table 40 Appliance > Server > Settings parameters .....              | 221 |
| Table 41 Configuring CSR Parameters .....                            | 233 |
| Table 42 Appliance > Network > Configuration parameters .....        | 238 |
| Table 43 Configure: Appliance > Network > Tools parameters .....     | 246 |
| Table 44 Inbound Port Details .....                                  | 264 |
| Table 45 Outbound Port Details .....                                 | 264 |

# Chapter 1: Introduction to cnMaestro c4000 Controller

---

This chapter covers the following topics:

- [Overview](#)
- [cnMaestro c4000 Controller Hardware Features](#)

## Overview

cnMaestro c4000 Controller is an On-Premises hardware appliance for onboarding, management, and monitoring of Cambium products. cnMaestro c4000 Controller can be used as a GRE tunnel concentrator for cnPilot device.



## cnMaestro c4000 Controller hardware features

### cnMaestro c4000 Controller physical features

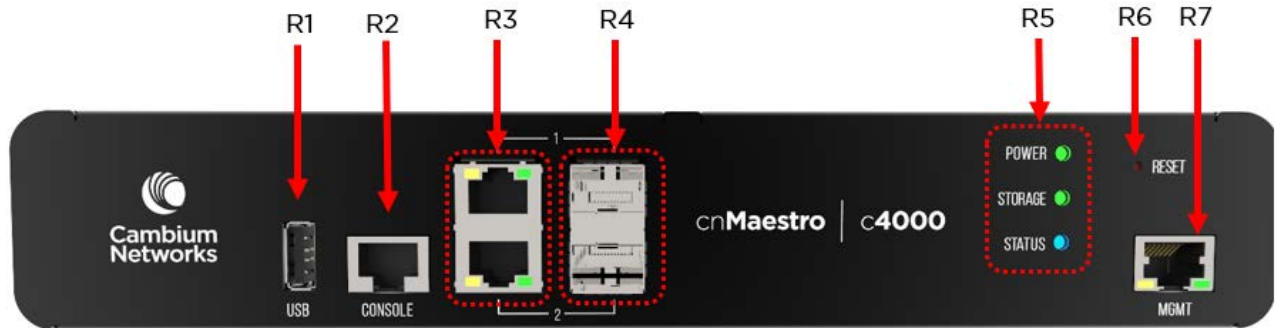


Figure 1: cnMaestro c4000 Controller Front View

Table 1 Front view components

| Item | Component                                 | Qty |
|------|---|-----|
| R1   | USB 2.0 Type A Port                       | 1   |
| R2   | Console Port                              | 1   |
| R3   | 1 Gigabit Ethernet Interfaces (Data Port) | 2   |
| R4   | 1 Gigabit SFP Ports (Data Port)           | 2   |
| R5   | Multi-purpose LEDs                        | 3   |
| R6   | Reset Button                              | 1   |
| R7   | Management Port                           | 1   |



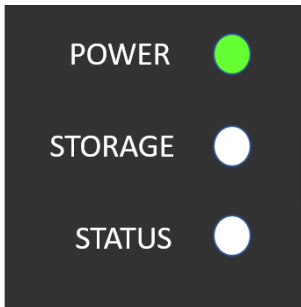
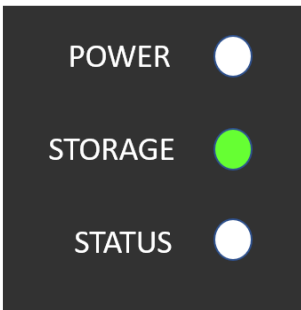
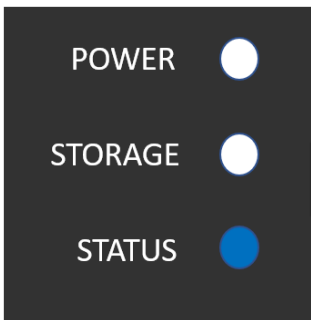
Figure 2: cnMaestro c4000 Controller Back View

Table 2 Back view components

| Item | Component       | Qty |
|------|-----------------|-----|
| R8   | Kensington Lock | 1   |
| R9   | DC Power In     | 1   |

## cnMaestro c4000 Controller LED details

Table 3 cnMaestro c4000 Controller LED details

| LED Name | LED   | Color          | Behaviour | Status Indication                 |
|----------|---|----------------|-----------|-----------------------------------|
| Power    |   | Green          | Steady On | Power On                          |
| Storage  |  | Green          | Blinking  | Represents Storage Activity       |
| Status   |  | Amber          | Steady On | The device is booting state       |
|          |   | Blue           | Steady On | The successful boot of the device |
|          |   | Blue and Amber | Blinking  | Factory Reset in progress         |



## cnMaestro c4000 Controller Hardware Specifications

**Table 4 Hardware specifications**

| Category            | Specification            |
|---------------------|--------------------------|
| Power supply        | 115vac/230VAC            |
| MTBF (Hours)        | 320,415 hours (GB, 30C)  |
| Weight              | 2.3 kg                   |
| Dimensions          | 255mm x 191.2 mm x 44 mm |
| CPU speed           | C2758, 2.4GHz            |
| Rack mountable      | Yes                      |
| Temperature ranges  | 0 - 40C                  |
| Operating humidity  | 95%@40C                  |
| Storage temperature | -20°C to - 80°C          |
| Memory              | 8GB                      |
| CPU cores           | 8                        |

## cnMaestro c4000 Controller Reset “Button”

**Table 5 Reset**

| Action                        | Behaviour     |
|-------------------------------|---------------|
| Press and release             | Reboot        |
| Press and hold for 10 seconds | Factory reset |

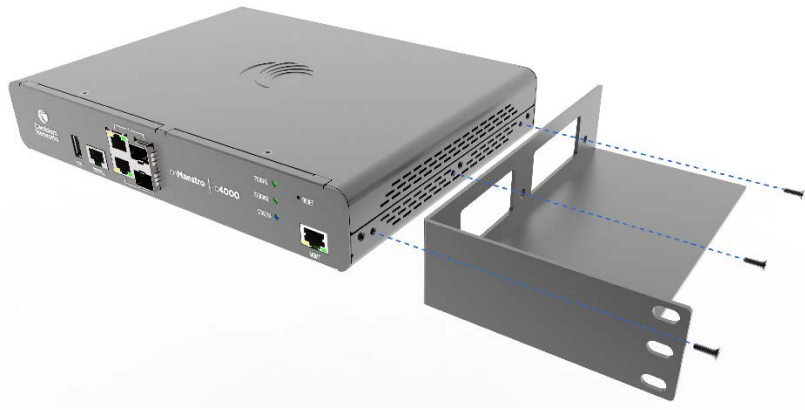

## Chapter 2: Installation and Upgrade

### Mounting cnMaestro c4000 Controller

Follow the below steps for mount cnMaestro c4000 Controller on a rack:

#### Rack Mount

Table 6 Mounting steps

|  |  |
|--|--|
| <p><b>Step 1:</b></p> <p>Fix the right-side mounting bracket to cnMaestro c4000 Controller using 3x M2 screws.</p> |   |
| <p><b>Step 2:</b></p> <p>Fix the Left-side mounting bracket to cnMaestro c4000 Controller using 3x M2 screws.</p>  |  |

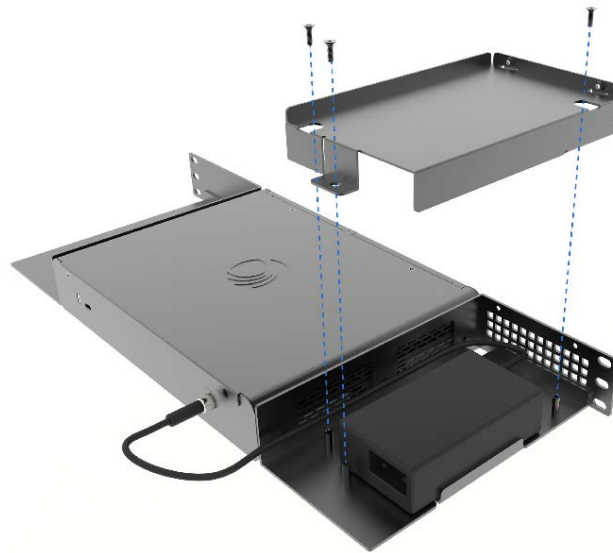
**Step 3:**

Place the power adapter on the Left-side mounting bracket.



**Step 4:**

Place the adapter top cover on the Left-side mounting bracket holding the power adaptor inside by using 3x M2 screws from the top.



**Step 5:**

Using 2x M2 screws, assemble the adaptor top cover to the Left-side mounting bracket from the front as shown in the figure.

**Step 6:**

If you are using a universal 19-inch cabinet, snap a TAR M6 square cage nut into the top and bottom holes of the location where you will be installing the rail plate as shown.



## Installing cnMaestro c4000 Controller

Power ON the cnMaestro c4000 Controller. POWER LED will glow after powering ON and wait for 2 minutes to boot up the device completely.

- The controller comes with a default factory image.
- To upgrade the controller with the latest software image, setup the management port connectivity as shown in [Figure 3](#).

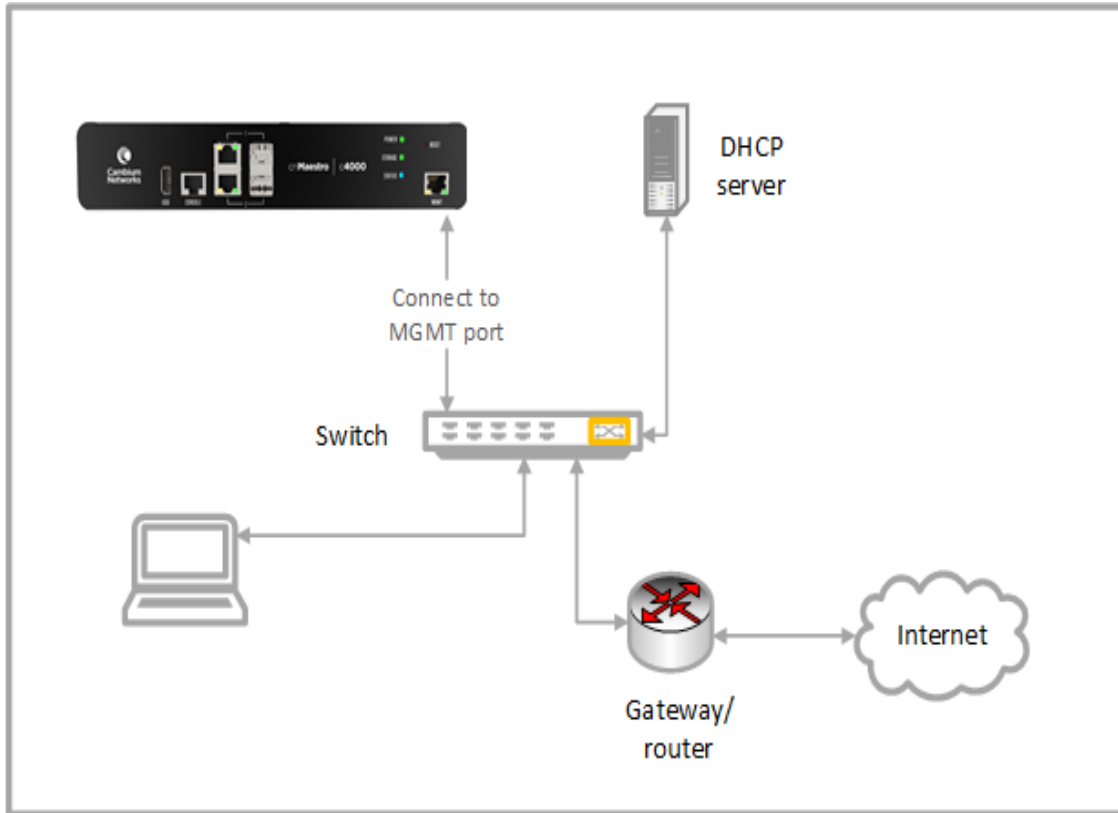


Figure 3: Installing cnMaestro c4000 Controller

## Login to Web UI

Open the browser and login to controller UI as `http(s)://<IP address>` with default credentials as below:

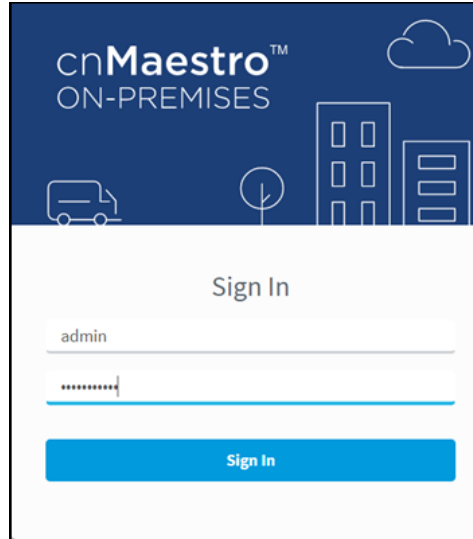
- Username: admin
- Password: admin



### Note

cnMaestro c4000 Controller will try to get a DHCP IP. In the case of DHCP failure, the default fallback IP is 192.168.0.1.





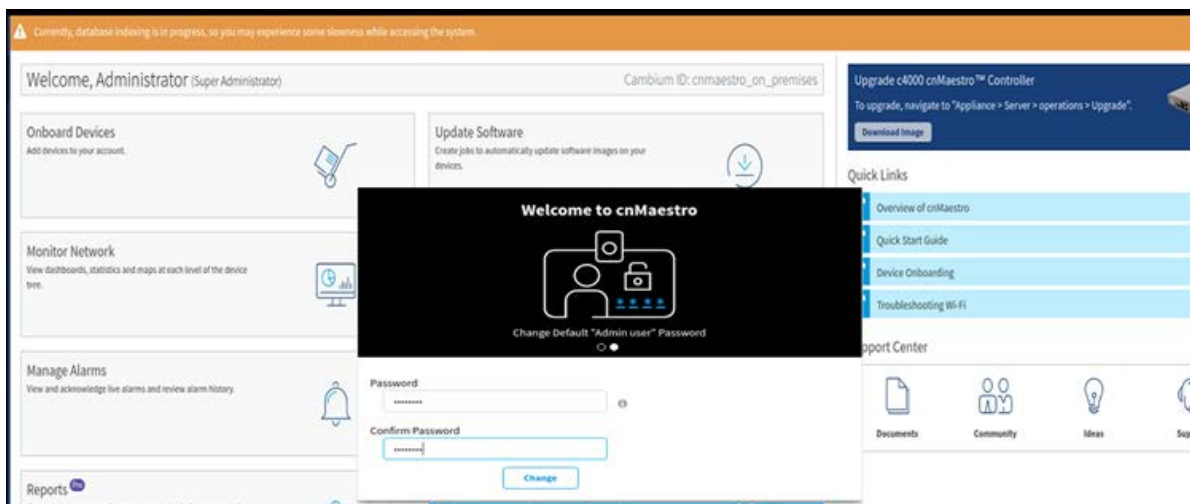
## Configure Country

After login a pop-up window will appear to configure country. This is mandatory to continue configuring the system as per the requirements.



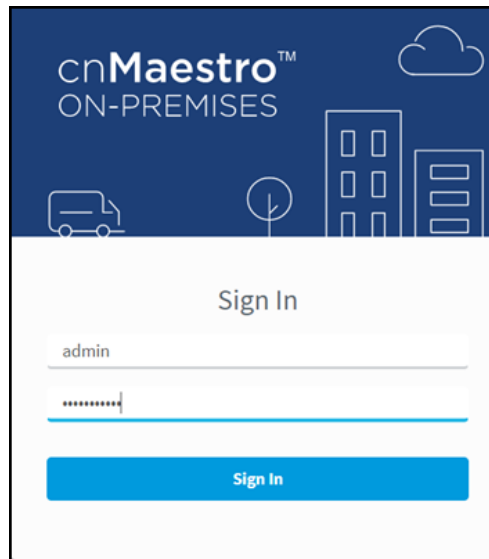
## Change Default Password

After login, a window will appear prompting the user to change the default password.



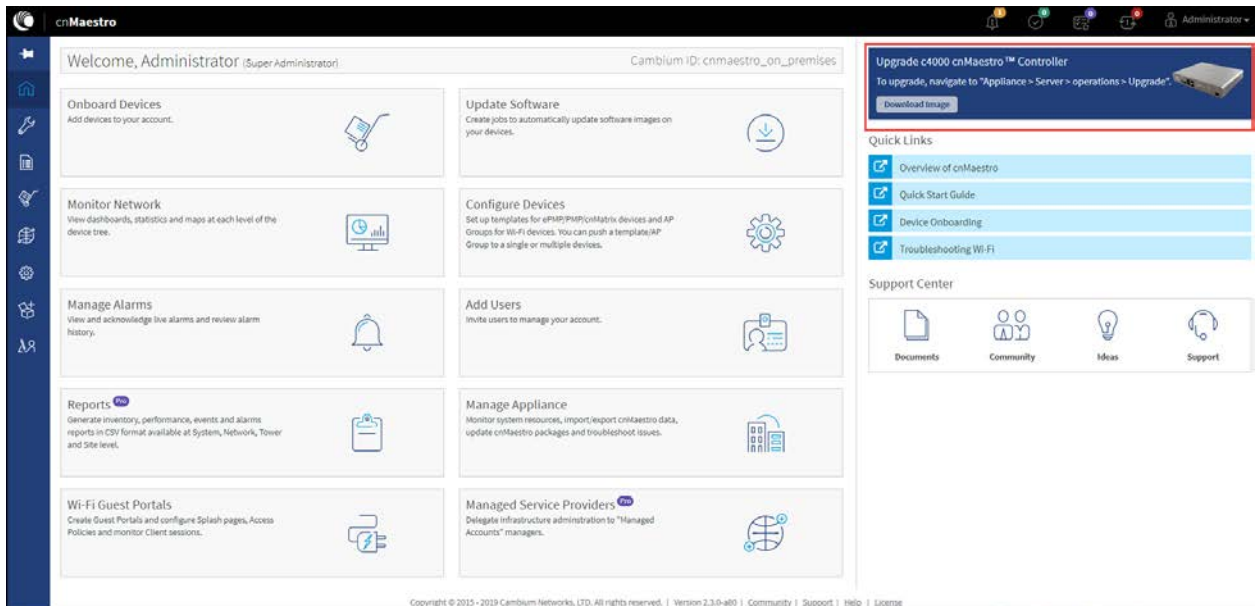
## Login to web UI with New Password

It will redirect to login page again. Login with the default username (admin) and new password.



## Upgrading cnMaestro c4000 Controller


1. Navigate to the home page of cnMaestro c4000 controller UI.



2. Click on the **Download Image** button.

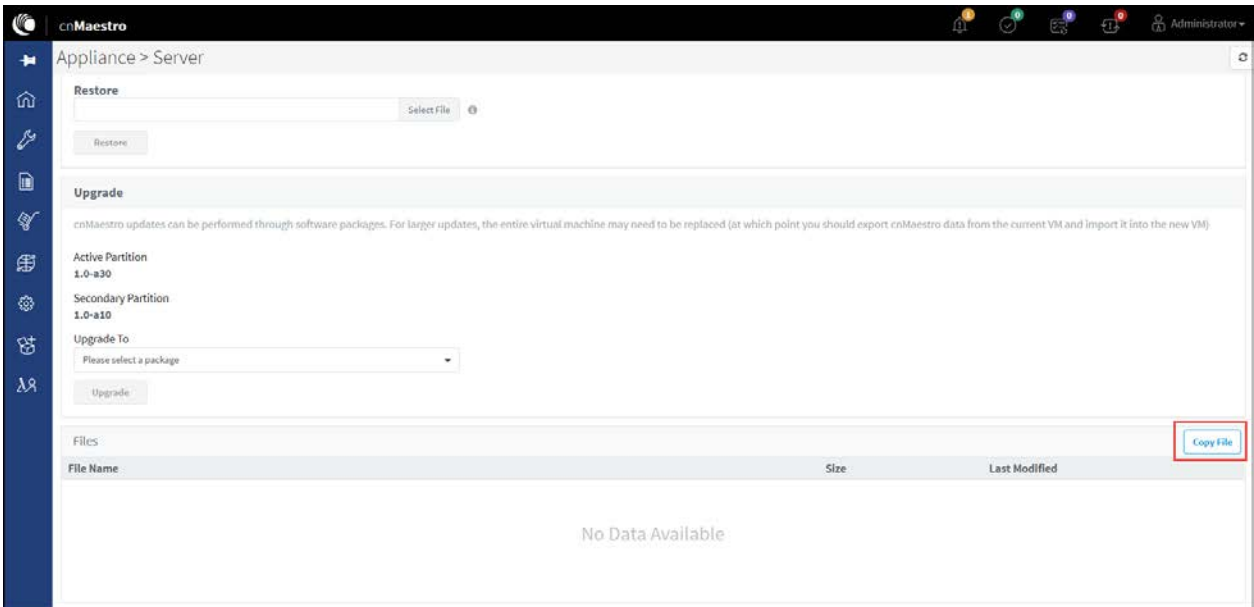
**Upgrade c4000 cnMaestro™ Controller**  
 To upgrade, navigate to "Appliance > Server > operations > Upgrade".

[Download Image](#)

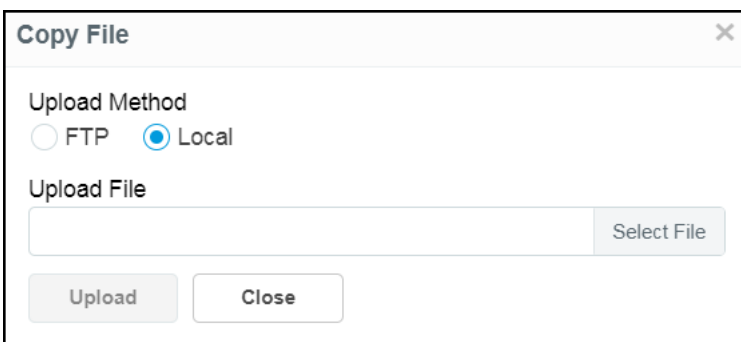


It directs the user to the Cambium Support page. The user can login to the Support Site and download the cnMaestro c4000 Controller image.

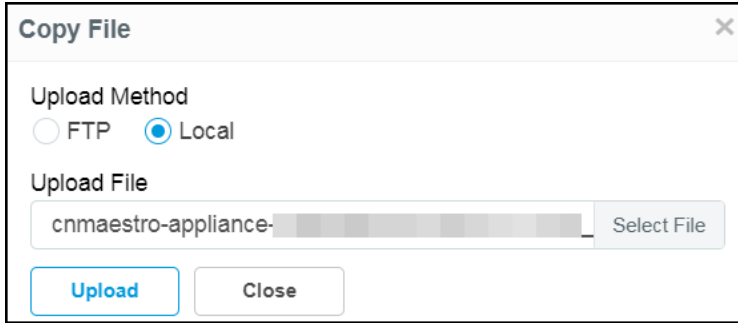
3. Once the download is complete, navigate to the **Appliance > Server > Operations** page in the UI.
4. Navigate to **File** and click **Copy File** button.



5. **Copy File** window will pop-up. Choose the **Local** radio button.

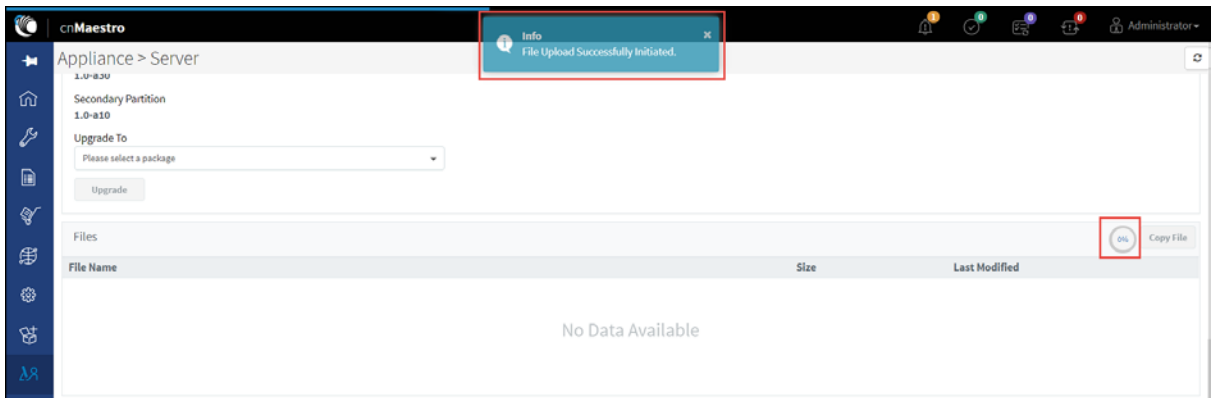


6. Click **Select File** to browse and select the downloaded cnMaestro c4000 Controller image.

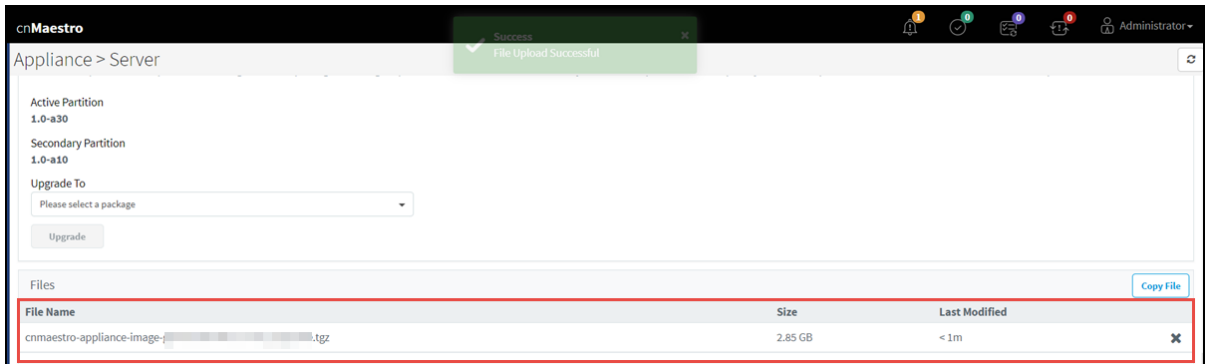


7. Click the **Upload** button to upload the selected cnMaestro c4000 Controller image.

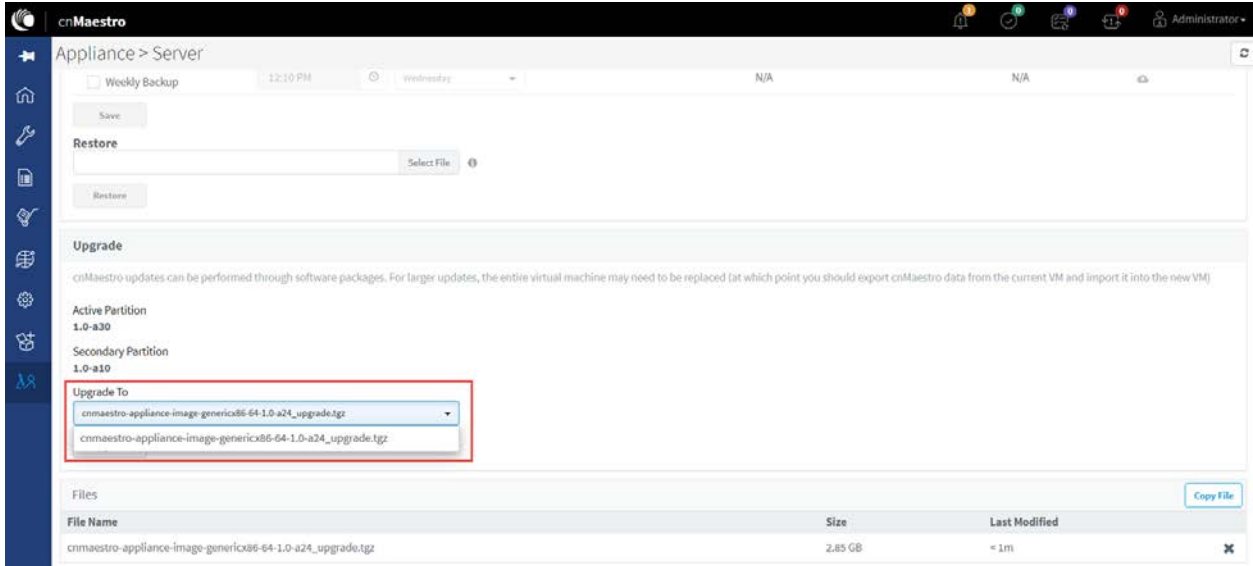
You can view the status of the upload in the UI as displayed below:



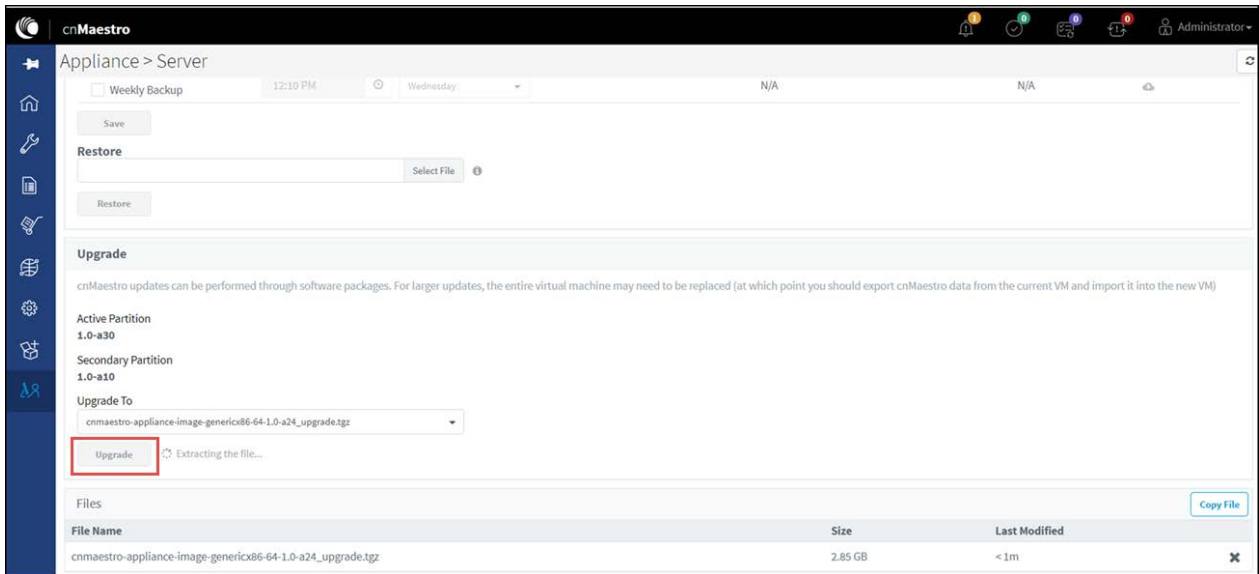
8. Once the upload is successful, the cnMaestro c4000 Controller image file will be displayed under **File Name** in the UI.



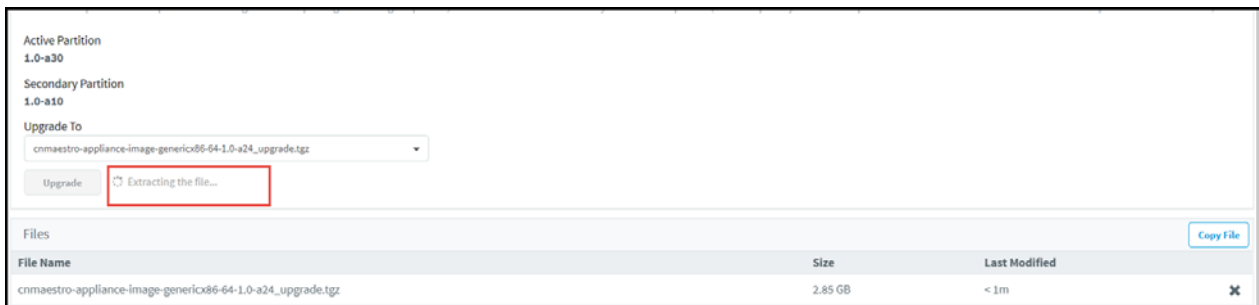
9. Under **Upgrade**, choose the uploaded cnMaestro c4000 Controller image from the drop-down list.



10. Click the **Upgrade** button.



11. You can also view the status of the upgrade as shown below:



12. Once the upgrade is successful, click on the link next to the **Upgrade** button for rebooting the device.

cnMaestro

Appliance > Server

Weekly Backup:  12:23 PM Wednesday N/A N/A

Save

Restore

Select File

Restore

**Upgrade**

cnMaestro updates can be performed through software packages. For larger updates, the entire virtual machine may need to be replaced [at which point you should export cnMaestro data from the current VM and import it into the new VM]

Active Partition  
1.0-a30

Secondary Partition  
1.0-a10

Upgrade To  
cnmaestro-appliance-image-genericx86-64-1.0-a30\_upgrade.tgz

Upgrade Upgrade process has been completed. [Reboot](#) the device.

Files Copy File

| File Name   | Size    | Last Modified |
|---|---------|---------------|
| extract   | 4.00 KB | 0d 0h 2m      |
| cnmaestro-appliance-image-genericx86-64-1.0-a30_upgrade.tgz | 2.68 GB | < 1m          |

## Chapter 3: Deployment Models

---

This chapter covers the following topics:

- [cnMaestro c4000 Controller as On-Premises](#)
- [cnMaestro c4000 Controller as Tunnel Concentrator](#)
- [Typical Deployments](#)
- [Configuring cnMaestro c4000 Controller](#)

### cnMaestro c4000 Controller as On-Premises

This is like cnMaestro on-premise deployment. More information regarding onboarding, management, the configuration can be found in the following chapters.

### cnMaestro c4000 Controller as Tunnel Concentrator

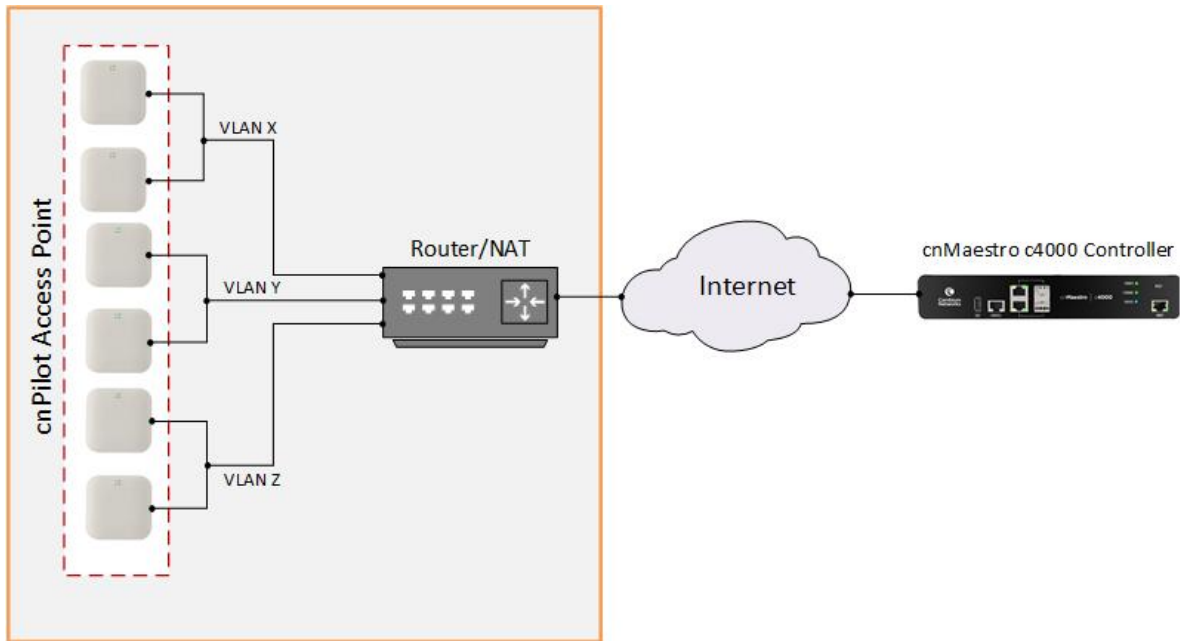
Layer 2 Generic Routing Encapsulation (L2GRE) is a tunnel protocol for encapsulating multicast, broadcast, and L2 packets between a GRE-capable device and an end-point. cnMaestro c4000 Controller supports L2GRE in UDP encapsulation as per RFC 8086. It is capable of operating as a L2GRE concentrator in parallel with all functionalities of cnMaestro on-premises. L2GRE supported by cnMaestro c4000 Controller is proprietary to Cambium Networks. Only cnPilot devices L2GRE tunnel can be terminated to cnMaestro c4000 Controller.

### Typical Deployments

This section illustrates some typical deployment for the cnMaestro c4000 Controller. Following deployment options assumes cnMaestro c4000 Controller is configured as both Tunnel concentrator and cnMaestro on-premises with tunnel traffic segregated based on VLANs on the data ports.

## Deployment Option 1

In this deployment option, the APs are in the private network whereas the cnMaestro c4000 Controller is deployed with a public IP.



**Figure 4 Controller on public IP address**

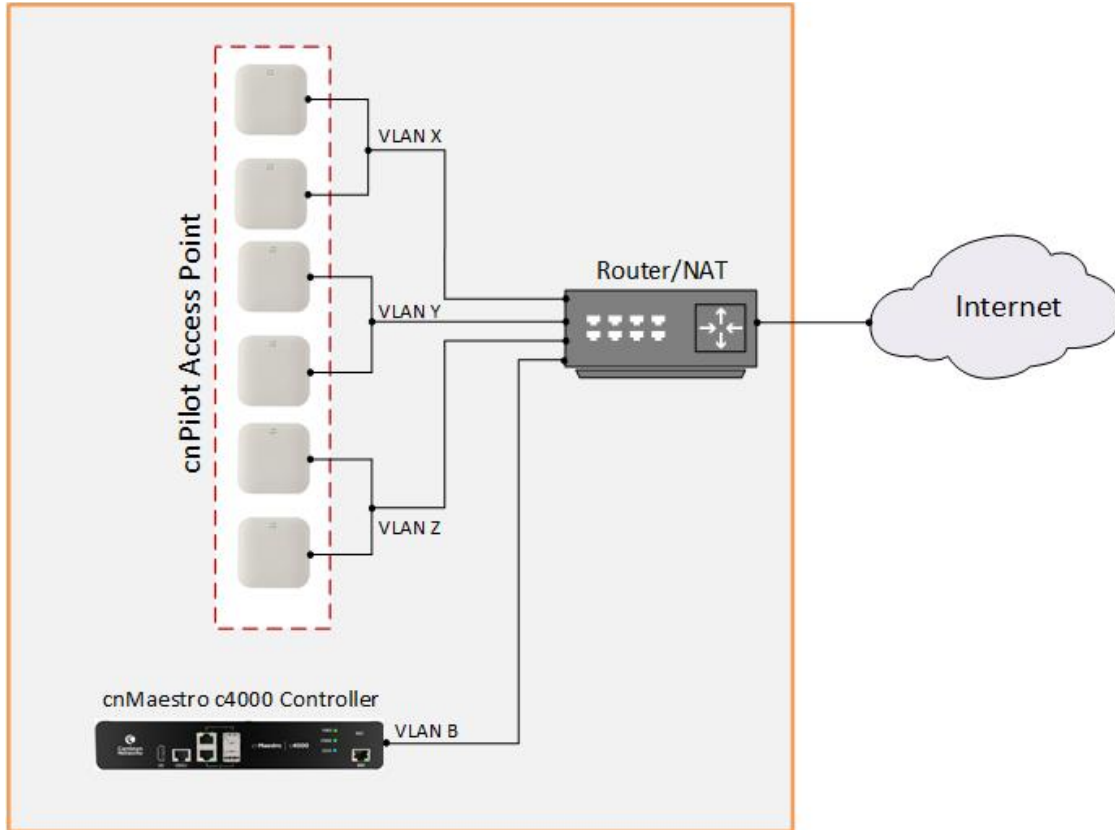
For this deployment following must be enabled/configured:

- UDP port 4754 should be allowed in the network for cnPilot devices to establish a tunnel with cnMaestro c4000 Controller.
- R3 ports of cnMaestro c4000 Controller must be connected to the Internet.
- Network to which Aps are connected should be routable to cnMaestro c4000 Controller.

## Deployment Option 2

In this deployment option, the Aps and cnMaestro c4000 Controller in the private network.





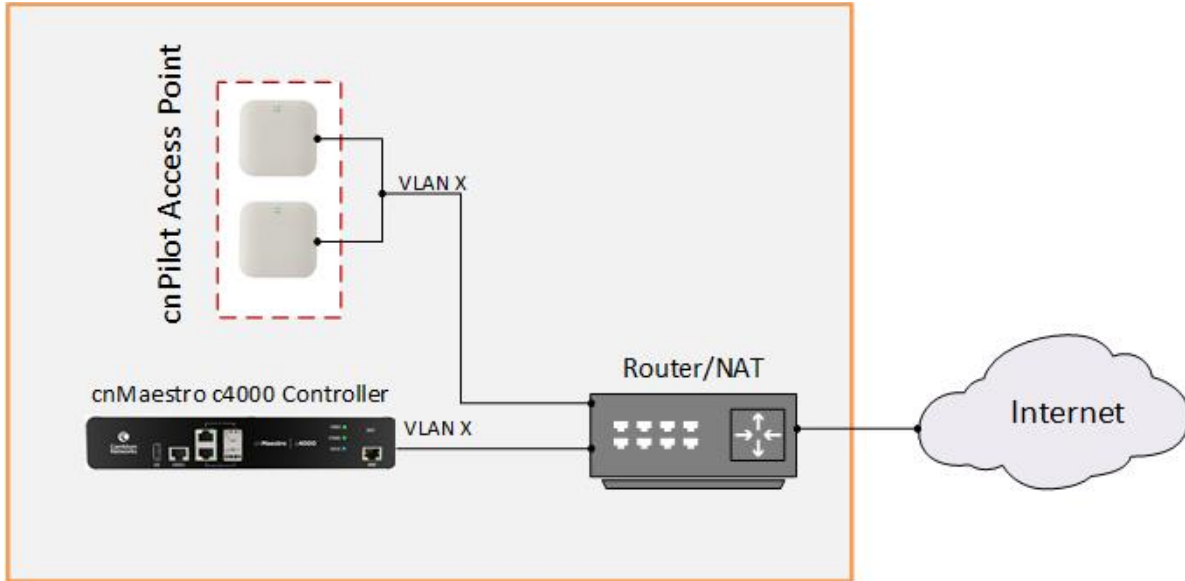
**Figure 5 Controller and AP in private subnet in different VLAN**

For this deployment following must be enabled/configured:

- UDP port 4754 should be allowed in the network for cnPilot devices to establish a tunnel with cnMaestro c4000 Controller.
- R3 ports of cnMaestro c4000 Controller must be connected to the private network.
- The network to which APs are connected should be routable to cnMaestro c4000 Controller.
- cnMaestro c4000 controller can be configured either with multiple SVIs based on AP VLANs or as an Access port and reachable from APs subnet.

### Deployment Option 3

In this deployment option, the APs and cnMaestro c4000 Controller in the private network.



**Figure 6 Controller and AP in the same VLAN**

For this deployment following must be enabled/configured:

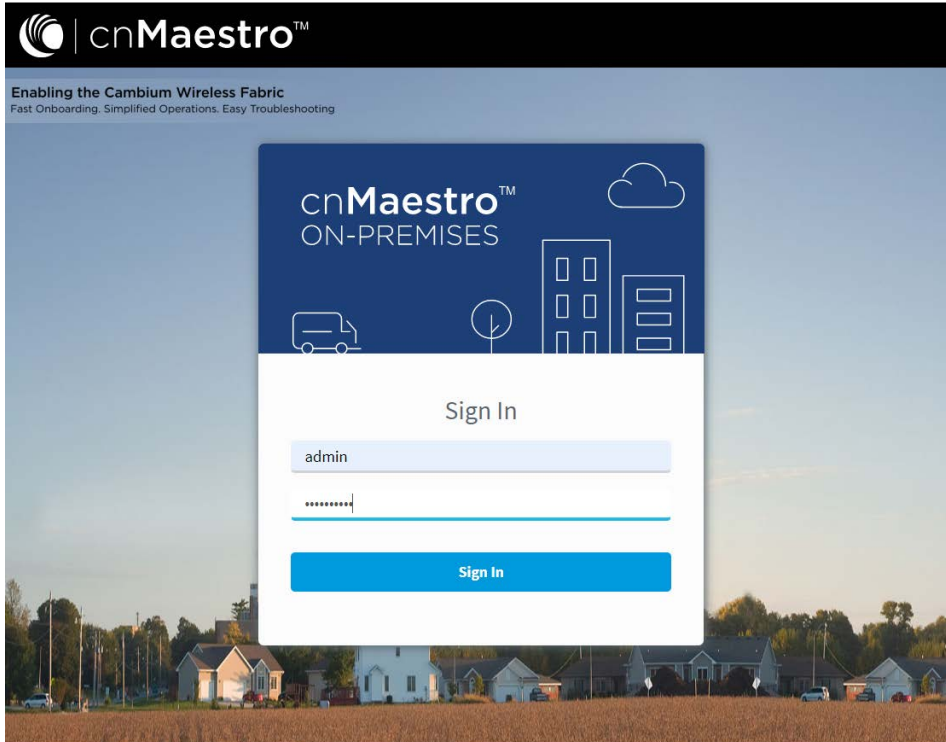
- UDP port 4754 should be allowed in the network for cnPilot devices to establish a tunnel with cnMaestro c4000 Controller.
- R3 ports of cnMaestro c4000 Controller must be connected to the private network.
- The network to which APs are connected should be reachable to cnMaestro c4000 Controller.

## Configuring cnMaestro c4000 Controller

Once the installation is done based on the requirement, it is necessary to configure cnMaestro c4000 Controller for management and data access.

### Configuring Management and Data Port

1. Login to cnMaestro c4000 Controller with credentials configured during [Installing cnMaestro c4000 Controller](#).



2. Navigate to **Network > Appliance > Configuration > Management Port** to configure IP mode of the management interface.

| Name | IP Address | Admin Status | MTU  | Description      |
|------|------------|--------------|------|------------------|
| mgmt | dhcp       | Up           | 1500 | This is OOB port |

3. Navigate to **Network > Appliance > Configuration > Data Ports** to configure IP mode/VLANs of the data port.

Appliance > Network

Statistics Configuration Tools ACL

Management Port Data Ports Switched Virtual Interface Static Routes

| Name | Switch Port ... | VLAN        | Admin Status | MTU  | Description         |
|------|-----------------|-------------|--------------|------|---------------------|
| eth1 | access          | 1           | Up           | 1500 | This is data port 1 |
| eth2 | trunk           | 299,399,499 | Up           | 1500 | This is data port 2 |

## Chapter 4: UI Navigation

---

cnMaestro c4000 Controller provides several ways to navigate its content. This section includes the following topics:

- [Account Type](#)
- [Home Page](#)
- [Page Structure](#)
- [Page Navigation](#)
- [Access and Backhaul Account](#)
- [Wireless LAN Account](#)
- [Side Menu](#)
- [Section Tabs](#)
- [System Status](#)
- [Logout](#)

### Account Type

cnMaestro c4000 Controller supports three separate account types, based upon the composition of devices installed. The type is set when the UI is first accessed, but it can be changed later through the **Appliance > Settings** page.

### Access and Backhaul Account

The Access and Backhaul Account supports all Fixed Wireless devices as well as Wireless LAN. The device types include ePMP, PMP, PTP, cnMatrix, and cnPilot.

### Industrial Internet Account

Industrial Internet Account provides a single management system to manage fixed wireless, WiFi, and cnReach deployments. The device types include ePMP, PMP, cnReach, PTP, cnMatrix, and cnPilot.

### Wireless LAN Account

The Wireless LAN Account supports the Enterprise Wi-Fi portfolio, which includes cnPilot device types. It provides a simplified UI that only displays Wi-Fi components (hiding fixed wireless features such as Towers).

The Account Type can be changed at any time, with the following restriction: to select the Wireless LAN type, all devices other than cnPilot need to be removed.

## Home Page

The Home Page is the first page displayed when the user logs into cnMaestro c4000 Controller. It provides links to the core functional areas in the UI, as well as Cambium's Support Center, Community, and Documentation. It can be accessed from any page in the UI by selecting the Home tab.

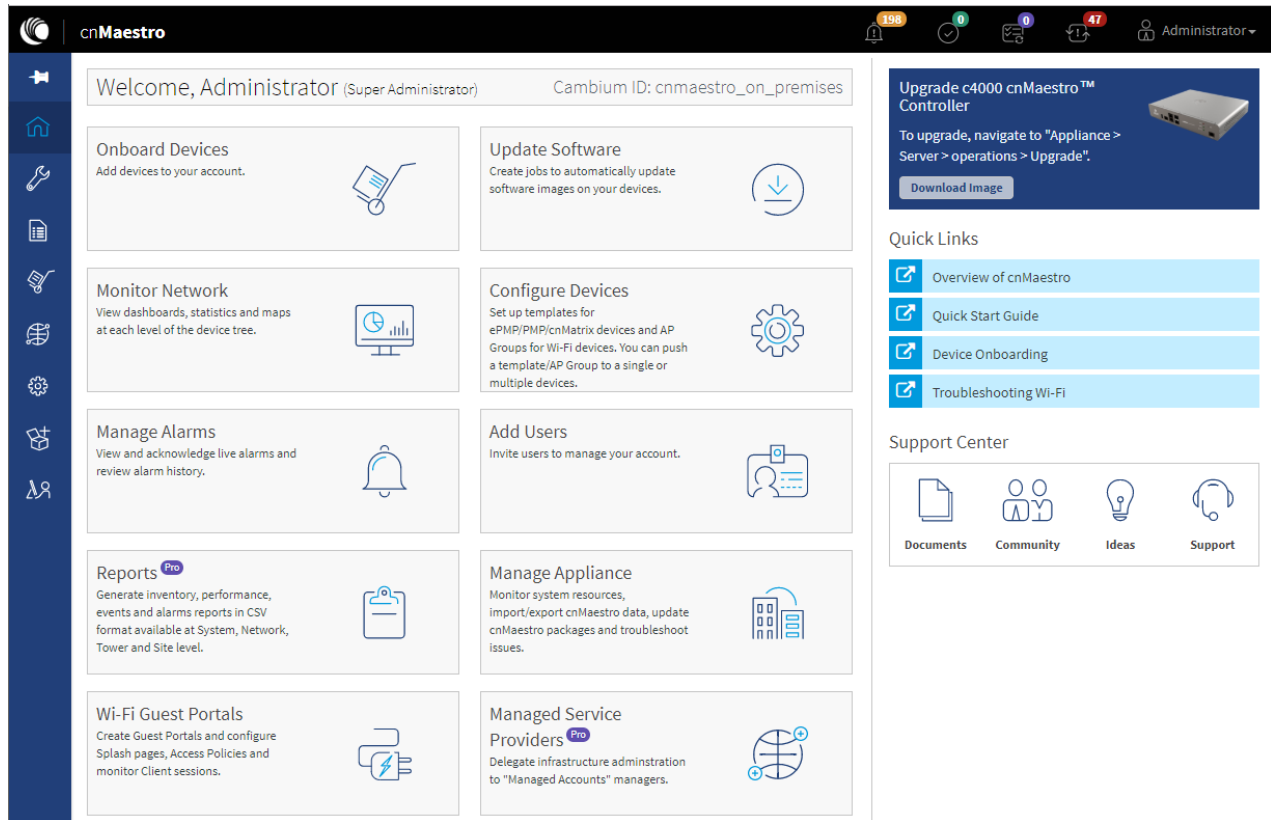


Figure 7 cnMaestro c4000 Controller home page

## Page Structure

Most of the c4000 Controller pages follow a standard structure, which consists of a left-side menu and a content area. In many pages, Tabs provide navigation through the content for a section.

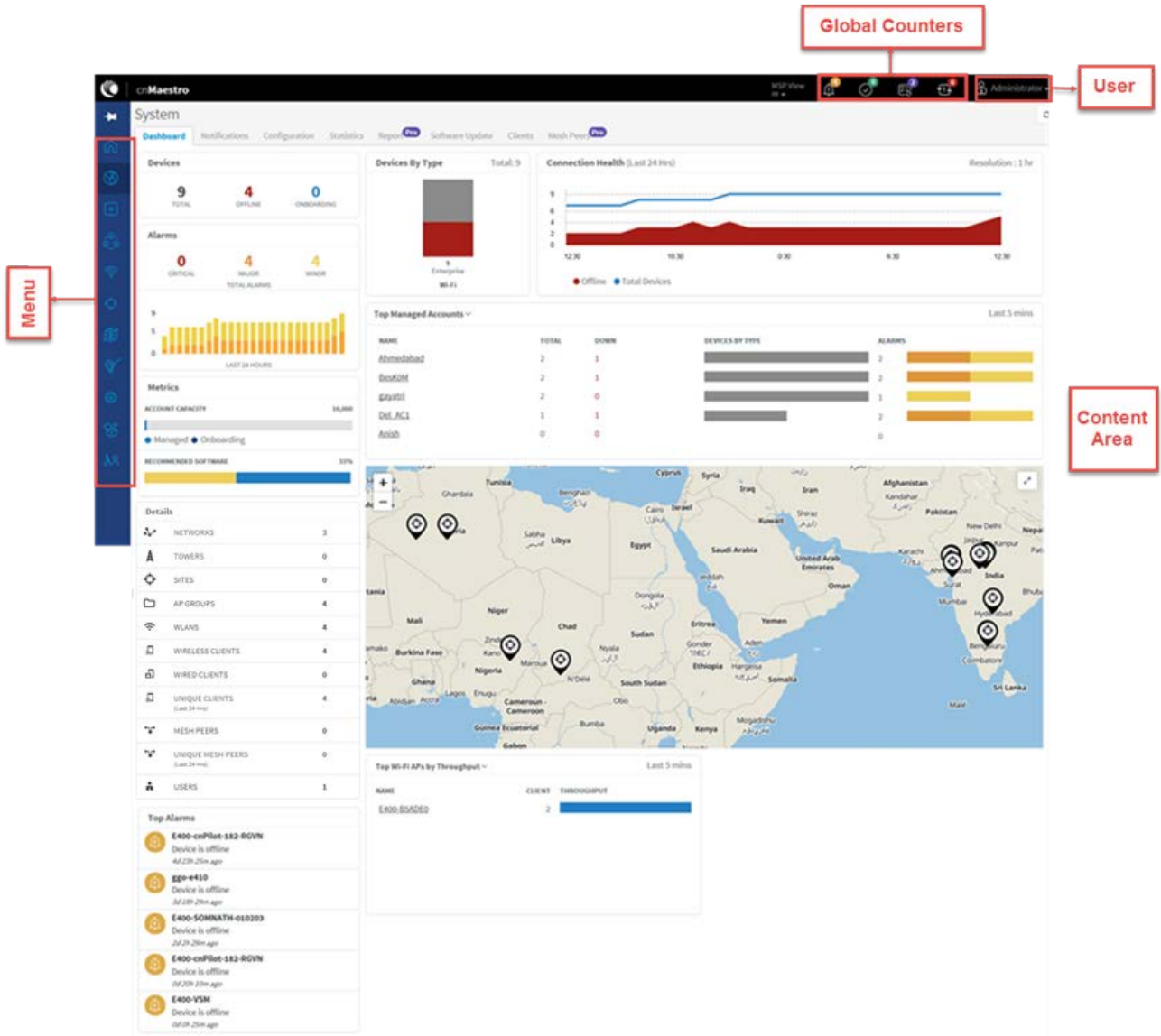


Figure 8 cnMaestro c4000 Controller page structure

## Page Navigation

The cnMaestro c4000 Controller pages include tabs such as Dashboard, Notifications, Software Update, and Tools. The content of a page differs depending upon its context. For example, a Dashboard page will be different at the System/Network/Tower/Site/Device level. The context, or level in the hierarchy, is selected in the Device Tree, which is defined below.

## Menu

The menu provides basic navigation to all the pages in the UI. The menu is different between the Access and Backhaul View and the Fixed Wireless View.

## Header

The page header supports basic counters for alarms, onboarded devices, pending jobs, and out-of-synch devices.

## Access and Backhaul Account

### Overview

The Access and Backhaul View is like the Wireless LAN View, with the exception it leverages a hierarchical tree to display device installations. In this view, customers can group their fixed wireless devices into Networks and display their point-to-multipoint devices in Tower-based sectors. All navigation is performed using the tree.

### Device Tree Navigation

The Device Tree is segmented into two tabs: Network and Wi-Fi AP Groups.

#### Network Tab

The Network Tab displays a hierarchical view of the devices. It consists of System, Networks, Towers, Sites, and Devices (Towers are only visible in the Fixed Wireless view). There is a strict ordering for how nodes can fit in the hierarchy, and as one navigates through and selects nodes, the pages update to display data from the node chosen,

The user can navigate the nodes by single-clicking a row to select it, thereby updating the Content Area to display the data from the node. Selecting an arrow icon will open the node and display the next level of the hierarchy.

**Note**

Opening the node does not automatically select a node in the new hierarchy, instead the desired node needs to be clicked.



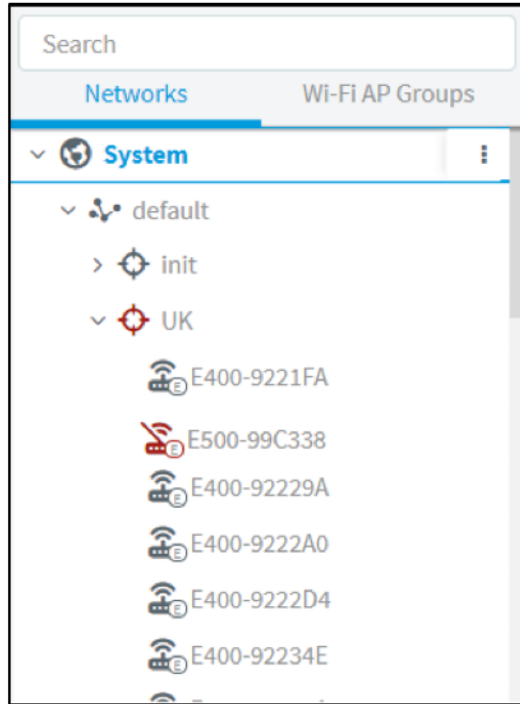









Figure 9 Device Tree navigation

The structured hierarchy has the following nodes:

Table 7 Structured Hierarchy Nodes

| Icon | Name     | Description  |
|------|----------|--|
|      | cnMatrix | cnMatrix devices are located within a Network. Optionally they can also be mapped standalone to a Tower or to a Site.  |
|      | cnReach  | cnReach device which could have zero, one, or two radios, and support one or two roles, including Point-to-Point (PTP), Point-to-Multipoint (AP or EP) (PTMP), or IO Expander.   |
|      | Network  | All devices are placed within Networks. Networks can represent geographical regions or collections of devices with shared responsibility. Accounts can have one network or many networks. Networks allow one to provide structure to accounts with many devices and also provides aggregation buckets for cnMaestro c4000 Controller statistics (essentially the system pre-calculates statistics, so they are displayed quickly.) |
|      | PMP AP   | Point-to-Multipoint Access Points are located in a Network and are optionally mapped to a Tower.   |

| Icon  | Name          | Description   |
|---|---------------|---|
|    | PMP SM        | Point-to-Multipoint Subscriber Modules are located in a Network (if they are standalone, which is only used for bootstrapping) or they are associated with an AP. The SM will inherit the Network and Tower of the AP to which it is associated.  |
|    | PTP Master    | Point-to-Point (PTP) Master device located in a network and optionally mapped to a Tower.   |
|    | PTP Slave     | Point-to-Point (PTP) Slave device located in a network and optionally mapped to a Tower.  |
|    | System        | The System node is at the top-level of the hierarchy, though it does not have an explicit node in the tree. Its pages are displayed when the user logs in for the first time, when one selects the System button in the hierarchical tree (displayed when Networks are shown), or selects the System node in the breadcrumbs. The System-level aggregates data from all devices within the account. |
|    | Site          | Sites are located within networks and hold Wireless Access Points. A site maps to a single area and represents a location on a map that has APs or a building.  |
|   | Tower         | Towers are located within networks and hold Point-to-Point devices or Point-to-Multipoint APs. All the devices on a Tower are mapped to the same Network, and all their children's devices such as Subscriber Modules or Home APs are also mapped to the same network.  |
|  | Wi-Fi/cnPilot | Wi-Fi devices are generally matched to a local SM and inherit its Network. They can also be mapped standalone to a network or to a Site.  |

### Default Network

cnMaestro c4000 Controller has a Default Network into which unmapped devices will be placed. These can remain in the Default Network or moved to a named network. The Default Network cannot be deleted, but it can be renamed.

### Tree Menu








Each node in the device tree has a menu icon (  ) that supports node-specific actions. For example, the System Node lets you add a Network or launch the Software Update page, while individual devices allow you to edit their cnMaestro c4000 Controller settings, reboot, or even delete the device from management (so it can be transferred to another account). The actions supported across the tree include the following:

Table 8 Tree menu

| Icon  | Action      | Node       | Description  |
|---|-------------|------------|--|
|  | Add Network | System     | Add a new Network as a child to the System node.   |
|  | Add Tower   | Network    | Add a new Tower as a child to the Network node.  |
|  | Add Site    | Network    | Add a new Site as a child to the Network node.   |
|  | Edit        | Most Nodes | Edit the cnMaestro c4000 Controller settings, including node name and location. This is available for all nodes except System. |
|  | Reboot      | Devices    | Reboot the device.   |
|  | Refresh     | All        | Refresh the node in the tree. This refreshes the node and its children only, not the entire tree.                              |

## Wi-Fi AP Groups Tab

The AP Groups tab displays the Wi-Fi AP Groups configured in cnMaestro c4000 Controller (and the devices mapped to them). AP Groups allow one to share configuration across many access points. They also aggregated statistics for the devices managed and present them within the AP Groups Dashboard.

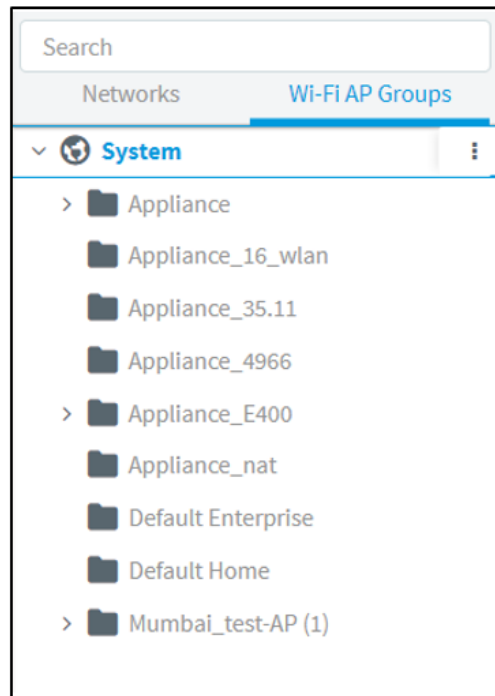


Figure 10 Wi-Fi AP Groups

## Map Navigation

Maps are presented in Dashboard screens as well as a dedicated Map display. Maps often show Tower and Devices located in proximity. Map nodes can also be double-clicked to navigate to the selected Device, Site, or Tower. By selecting a node in the map, the Device Tree is updated to reflect that node.



Figure 11 Map Navigation

## Table Navigation

Some tables display Networks, Towers, or Devices and allow the user to click the node and navigate to the location of the node in the tree.

## Node Search

Administrators can search for nodes within the Device Tree using the Search box. It allows the user to search based upon Device Name and MAC Address. Once the node is found and selected, one can jump to it in the hierarchical tree.

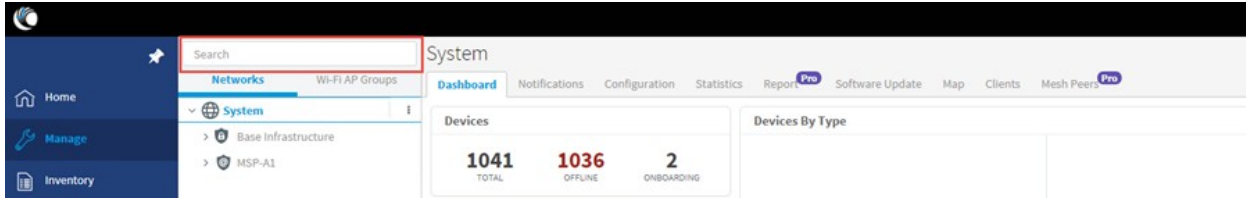


Figure 12 Node search

## Wireless LAN Account

### Overview

The Wireless LAN account differs from Access and Backhaul in that it is largely table-driven. It does not have the Quick Buttons or the Device Tree, instead, it has direct navigation for APs, AP Groups, WLANs, and Sites. Each of these are presented in tabular form and clicking on the row entry will launch the management page.

### System

The System Dashboard and global functionality is presented in the System menu. It aggregates data across the entire installation.

### APs

The AP (Access Point) section provides a searchable table listing all the devices in the system.

 The screenshot shows the 'APs' management page. It features a search bar, a 'Managed Account' dropdown set to 'All', and buttons for 'Delete', 'Export', and 'Claim New AP'. Below is a table with columns: Device, Managed Ac..., Status, Serial Number, IP Address, Type, and AP Group. Three devices are listed: 'Rajesh' (Offline), 'E400-cnPilot-182-RGVN' (Offline), and 'E400-BSADE0' (Online).
 

| Device                | Managed Ac...      | Status                            | Serial Number | IP Address      | Type         | AP Group             |
|-----------------------|--------------------|-----------------------------------|---------------|-----------------|--------------|----------------------|
| Rajesh                | Base Infrastructur | Offline (3d 1h 48m)<br>Onboarded  |               | 10.110.208.1... | cnPilot E500 | N/A                  |
| E400-cnPilot-182-RGVN | BesKOM             | Offline (4d 2h 19m)<br>Onboarded  |               | 10.110.212.1... | cnPilot E400 | N/A                  |
| E400-BSADE0           | BesKOM             | Online (5d 21h 4...)<br>Onboarded |               | 10.110.202.1... | cnPilot E400 | E400-RGVN-SmartWorks |

Figure 13 APs

Selecting a device launches its management page.

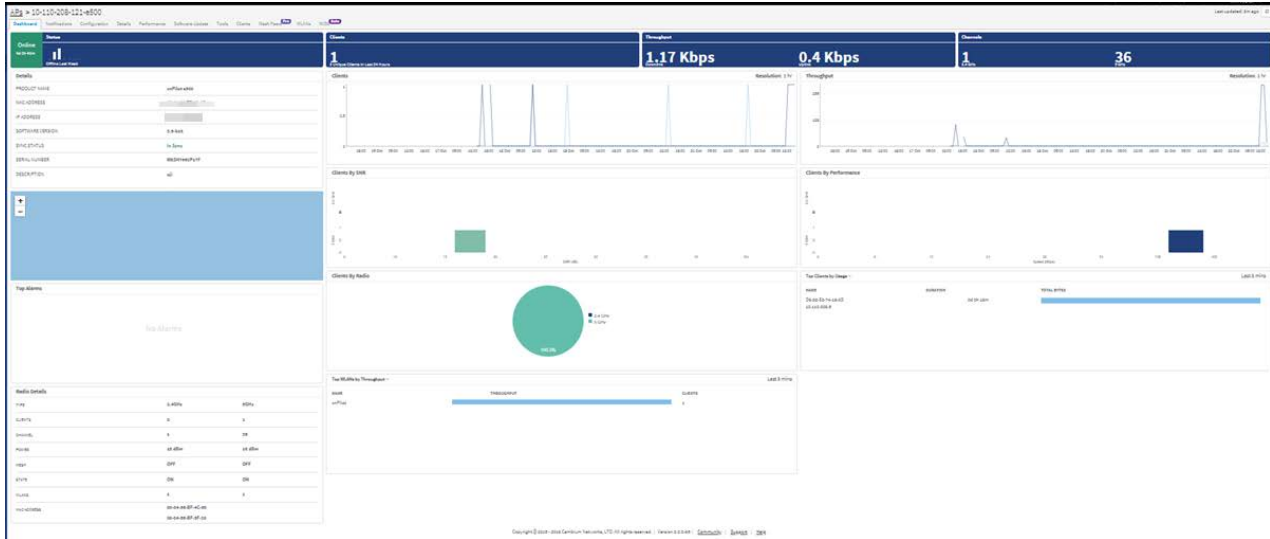


Figure 14 Management page

## AP Groups and WLANs

AP Groups and WLANs manage shared configuration across APs. AP Groups also aggregate data for all the APs that map to them. This includes consolidating statistics and events/alarms and presenting AP Group-centered pages for Dashboard, Notifications, Reports, etc.

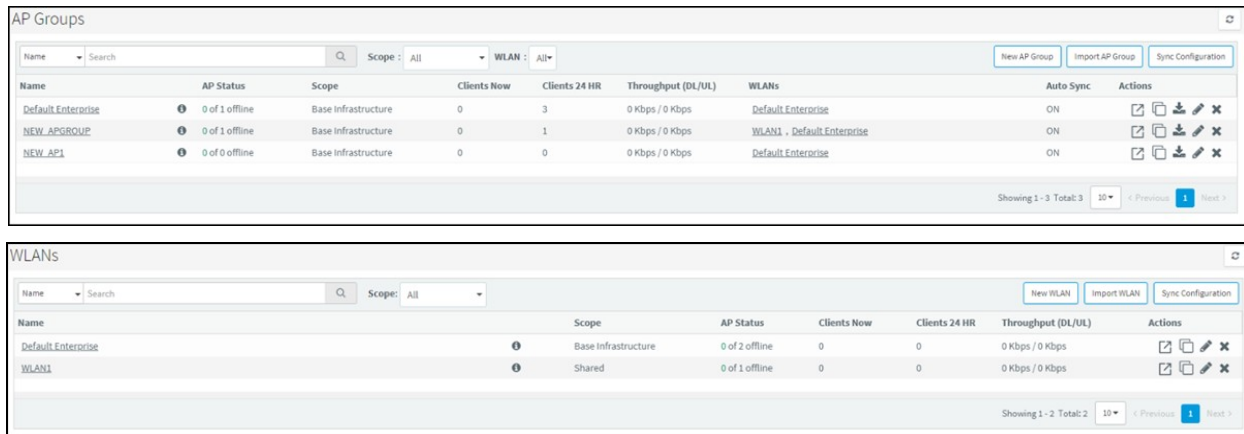


Figure 15 AP Groups

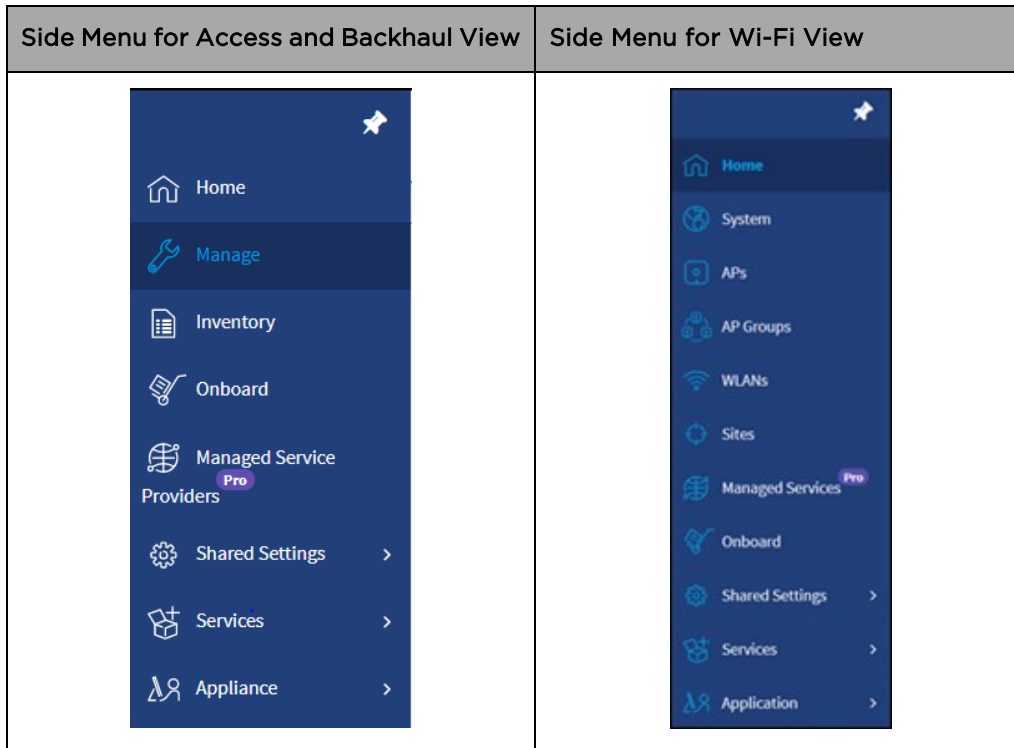
## Sites

Sites are similar to AP Groups in that they aggregate statistics from many APs. The difference is a Site represents APs installed at a single physical location (and mapped to a Floor Plan). Sites also have their own Dashboard and aggregation pages.

## Side Menu

The side-menu provides high-level navigation through the cnMaestro c4000 Controller UI. It can be expanded or collapsed by clicking on the "pin" icon at the top.

The side menu for the Access and Backhaul view is:



## Section Tabs

All management sections are displayed in the context of the managed item, including System, AP, AP Group, and Site. The options vary depending upon the item selected. A breakdown is below:






**Table 9 Section Tabs**

| Page           | Tabs   |
|----------------|--|
| System         | Dashboard > Notifications > Configuration > Statistics > Report > Software Update > Clients                                |
| Site           | Dashboard > Notifications > Configuration > Statistics > Report > Floor Plan > APs > Clients > WIDS                        |
| Wi-Fi AP Group | Dashboard > Notifications > Configuration > Statistics > Reports > APs > Clients   |
| Wi-Fi AP       | Dashboard > Notifications > Configuration > Details > Performance > Software Update > Tools > Clients > Mesh Peers > WLANs |

## System Status

The UI header has several System Status icons that provide a single point to view selected global statistics and operations parameters. Their meanings are highlighted below:

Table 10 System status icon

| Icon  | Name                         | Description   |
|---|------------------------------|---|
|  | Critical Alarms              | The count of critical alarms currently raised in the system (if no critical alarms are raised, then the major alarm count will be displayed)  |
|  | Major Alarms                 | The count of major alarms currently raised in the system.   |
|  | Devices Waiting for Approval | The count of jobs in the queue. It includes both running and pending jobs.  |
|  | Active Software Upgrade Jobs | The number of devices in the onboarding queue that are registered to the account, but which need to be manually accepted prior to completing their onboarding.                                      |
|  | Out-of-Sync Devices          | The number of Wi-Fi devices with unsynchronized configuration (which can occur when automatic synchronization is disabled in the AP Group, or the configuration is changed directly on the device). |

Clicking the icons directs the user to the appropriate UI page for management.

## Logout

The user icon in the upper right corner allows the user to logout of the cnMaestro c4000 Controller.



Figure 16 Logout



# Chapter 5: Device Onboarding

---

## Overview

cnMaestro c4000 Controller is Cambium's hardware management platform. This chapter describes the following topics:

- [Device Onboarding and Provisioning](#)
- [Directing devices to the cnMaestro On-Premises server](#)
- [Claim using Cambium ID](#)

## Device Onboarding and Provisioning

This section includes the following topics:

- [Onboarding to cnMaestro cloud using MSN](#)
- [Onboarding to cnMaestro On-Premises](#)
- [Auto-Provisioning](#)
- [Other options](#)

## Onboarding to cnMaestro Cloud Using MSN

This mode is preferable for cnMaestro cloud. In order to claim through MSN Address, follow the below steps:

1. Login to On-Premises server using default username and password (admin/admin) or the username and password set by the Administrator.
2. Navigate to **Home > Onboard Devices > Claim from cnMaestro**.
3. Select the **Device type** that needs to be onboarded and provide the MSN in the combo box and click the **Claim Devices button**. Multiple MSN Addresses of same device type can be claimed using a ( , ) separator between MSN or by entering them in the new line.

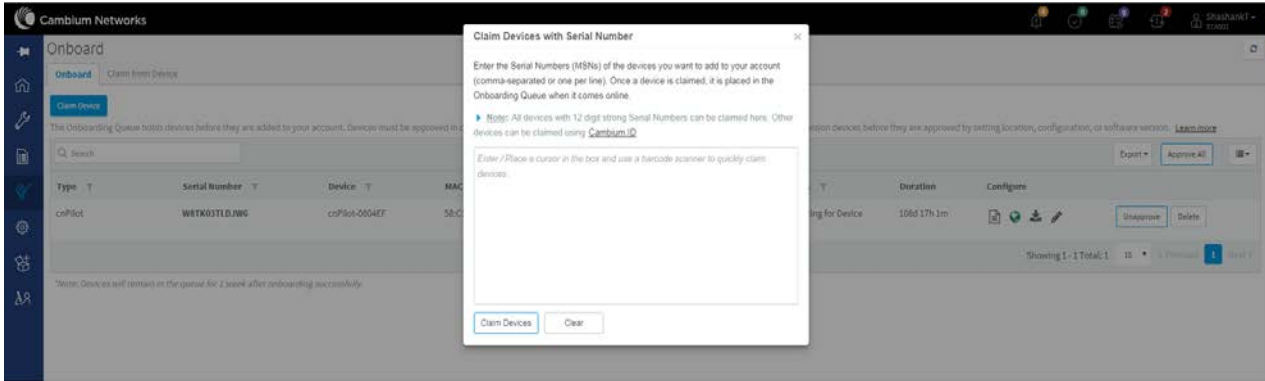


Figure 17 Onboarding to cnMaestro cloud using MSN

## Onboarding to cnMaestro On-Premises

This mode is preferable for cnMaestro On-Premises. In order to claim through MAC Address (ESN), please follow the below steps:

1. Login to On-Premises server using default username and password (admin/admin) or the username and password set by the Administrator at the time of On-Premises server installation.
2. Navigate to **Home > Onboard Devices > Claim from cnMaestro**.
3. Select the **Device type** for which onboarding is to be done and provide the MAC Address in the combo box and click the **Claim Devices** button. Multiple MAC Addresses of same device type can be claimed using a ( , ) separator between MAC Addresses or by entering them in the new line.

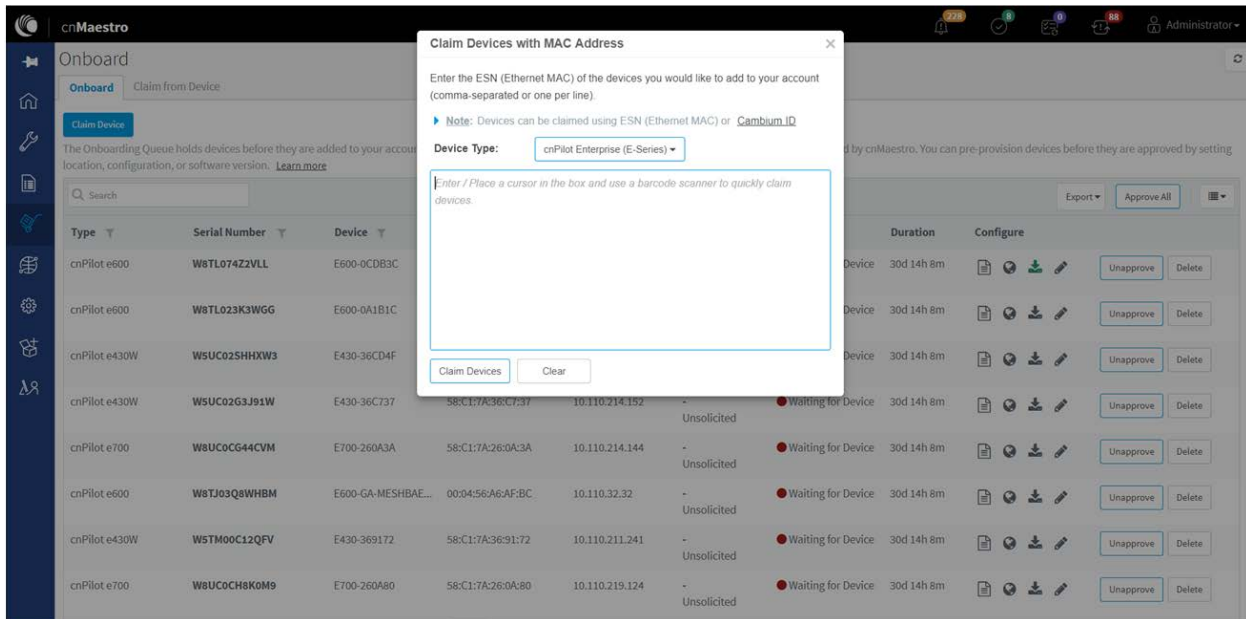


Figure 18 Onboarding to cnMaestro On-Premises

## Pre-Configuration and Approval of Devices (Optional)

To automatically configure and approved devices when they access cnMaestro c4000 Controller, add the device MAC address to the **Onboard > Onboard > Claim Device** button. Adding devices here places them in the Onboarding Queue, where they can be pre-configured and/or pre-approved.

If this step is not configured, the devices would automatically show up in the Onboarding Queue, where they can be approved.

| Type         | Serial Number | Device             | MAC               | IP Address     | Managed Account     | Added By                        | Status             | Duration    | Configure                        |
|--------------|---------------|--------------------|-------------------|----------------|---------------------|---------------------------------|--------------------|-------------|----------------------------------|
| cnPilot e400 | W5H476K2P1ZF  | E300-0F478A        | 00:04:56:0F:47:8A | 10.110.208.121 | Base Infrastructure | -                               | Unsolicted         | 1d 1h 14m   | [Configure] [Unapprove] [Delete] |
| cnPilot      | N/A           | cnPilot-1430F9     | 00:04:56:14:06:F9 | N/A            | Base Infrastructure | Administrator Using MAC Address | Waiting for Device | 22d 0h 51m  | [Configure] [Unapprove] [Delete] |
| cnPilot      | N/A           | cnPilot-CA1820     | 00:45:56:CA:18:20 | N/A            | Base Infrastructure | Administrator Using MAC Address | Waiting for Device | 27d 21h 24m | [Configure] [Unapprove] [Delete] |
| cnPilot      | N/A           | cnPilot-CA1817     | 00:45:56:CA:18:17 | N/A            | Base Infrastructure | Administrator Using MAC Address | Waiting for Device | 27d 21h 24m | [Configure] [Unapprove] [Delete] |
| cnPilot      | N/A           | cnPilot-CA1818     | 00:45:56:CA:18:18 | N/A            | Base Infrastructure | Administrator Using MAC Address | Waiting for Device | 27d 21h 24m | [Configure] [Unapprove] [Delete] |
| cnPilot      | N/A           | cnPilot-CA1819     | 00:45:56:CA:18:19 | N/A            | Base Infrastructure | Administrator Using MAC Address | Waiting for Device | 27d 21h 24m | [Configure] [Unapprove] [Delete] |
| cnPilot      | N/A           | cnPilot-14B0C1     | 00:04:56:14:B0:C1 | N/A            | Base Infrastructure | Administrator Using MAC Address | Waiting for Device | 27d 21h 24m | [Configure] [Unapprove] [Delete] |
| cnPilot      | N/A           | cnPilot-143901     | 00:04:56:14:09:01 | N/A            | Base Infrastructure | Administrator Using MAC Address | Waiting for Device | 27d 21h 24m | [Configure] [Unapprove] [Delete] |
| cnPilot      | N/A           | cnPilot-0FA7A9     | 00:04:56:0F:A7:A9 | N/A            | Base Infrastructure | Administrator Using MAC Address | Waiting for Device | 27d 21h 24m | [Configure] [Unapprove] [Delete] |
| cnPilot e400 | W5H4370QWFW   | E300-8D8236-Rajesh | 00:04:56:8D:82:36 | 10.110.208.147 | Base Infrastructure | -                               | Unsolicted         | 0d 20h 42m  | [Summary] [ONBOARDED]            |

Figure 19 Pre-Configuration and Approval of Devices



**Note**

If the device gets stuck on the Onboarding page, the Force Onboard button will be automatically enabled. Click the Force Onboard button for the device to be onboarded.

| Type         | Serial Number | Device      | MAC | IP Address | Managed Account  | Added By                 | Status                                 | Duration | Configure                   |
|--------------|---------------|-------------|-----|------------|------------------|--------------------------|--|----------|-----------------------------|
| cnPilot e400 |               | E600-A45E28 |     |            | MEP-Account-User | Administrator Unsolicted | Updating<br>Sent the software updat... | 0d 0h 6m | [Configure] [Force Onboard] |

## Device Authentication (Optional)

To require devices to authenticate with cnMaestro c4000 Controller before being added to the Onboarding Queue, enable Cambium ID- based authentication at **Onboard > Claim** from Device. When configured, an Onboarding Key must also be created.

Each user can have their own Onboarding Key. The Onboarding Key needs to be entered the device UI before cnMaestro c4000 Controller will allow it into the Onboarding Queue.

**Note**

When Cambium ID authentication is enabled, the device UI requires both a Cambium ID and an Onboarding Key. For cnMaestro c4000 Controller, the Cambium ID is ignored. This mechanism is optional, and it would only be used to require device authentication before addition to the Onboarding Queue.

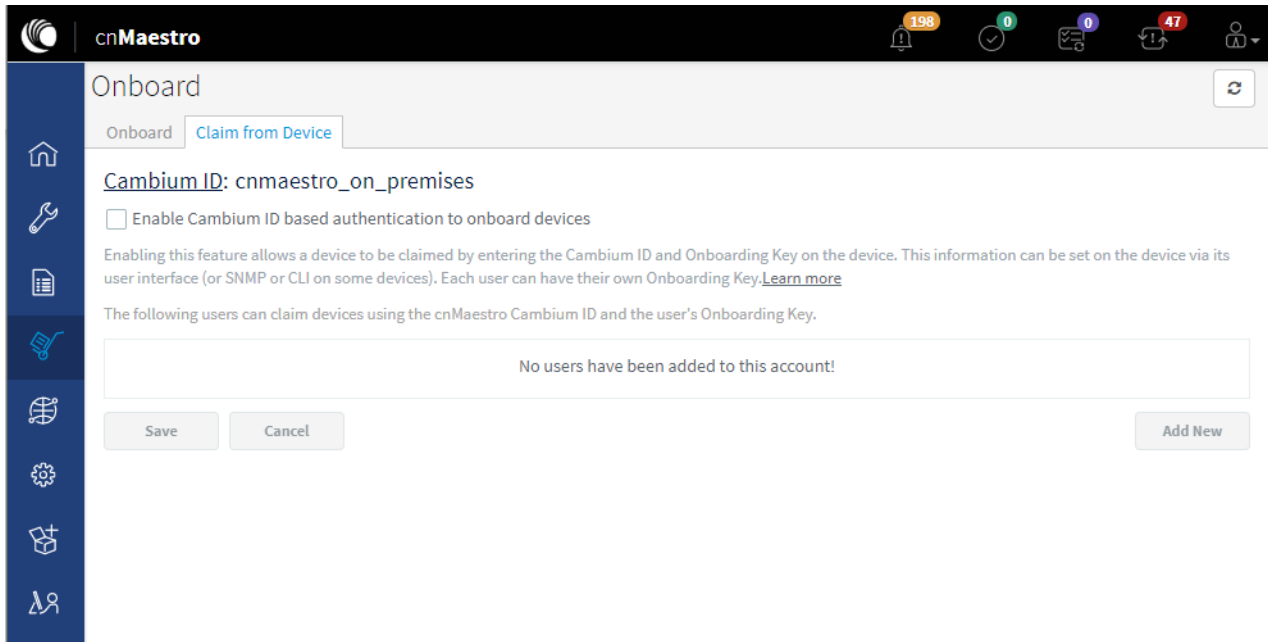


Figure 20 Device Authentication

## Auto-Provisioning

cnMaestro c4000 Controller supports Auto-Provisioning for cnPilot devices. This feature not only enables auto onboarding but also configures the synchronization and positioning of the device in the network architecture. It is triggered only at first instance of device onboarding. It can be configured on cnMaestro as below:

### Configuration

It is enabled at **Shared Settings > Auto-Provisioning**, and it allows one to automatically configure and approve devices based upon IP address. To create rules for cnPilot devices:

1. Navigate to **Shared Settings > Auto-Provisioning** page.
2. To create a new rule, click **Add**. The following window appears:

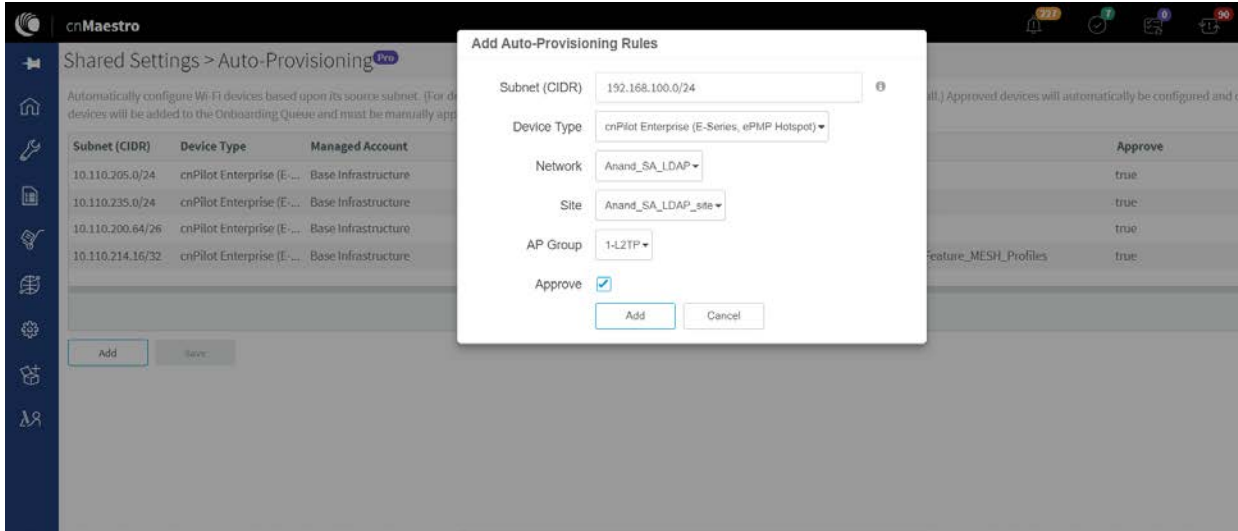


Figure 21 Auto-Provisioning

3. Enter the following details given in **Table 11**:

Table 11 Auto-Provisioning parameter details

| Parameter     | Description  |
|---------------|--|
| Subnet (CIDR) | The subnet with CIDR of the devices to which the rule must be applied. For example, Subnet/CIDR (192.168.100.100/25) maps the devices with the IP addresses ranging from 192.168.100.1 to 192.168.100.126. |
| Device Type   | Select the type of device from the drop-down list.   |
| Network       | Select the network to which the device should be onboarded, once the device contacts the server.   |
| Site          | Select the site under which the device should be onboarded, once the device contacts the server.   |
| AP Group      | Select the AP Group which needs to be applied on the device, once the device contacts the server while onboarding.   |
| Approve       | Enables this option to auto-approve onboarding.  |

4. Click **Add**.



**Note** Auto-Provisioning is supported only for cnMaestro On-Premises and not for cnMaestro cloud.

## Other Options

This section includes the following topics:

- **AP Group**
- **Site dashboard**

The device onboarding screen can also be accessed from other locations in the UI. Below options can be used in both cloud cnMaestro and cnMaestro On-Premises. For cnMaestro On-Premises, ESN/MAC Address is required for onboarding/claiming device in an account whereas for cloud cnMaestro MSN is required to claim/onboard device in an account.

### AP Group

In order to claim multiple devices from the AP Group in the cloud, navigate to the Wi-Fi AP Groups tree view and click the drop-down menu for the selected AP Group.

1. Click the **Claim Devices** option.
2. In the pop-up dialog, select the **Network and Site** under which these devices need to be placed and by default, the devices claimed under this group will have the configuration settings from this AP Group.
3. Specify the MSNs/ESNs (Manufacturing Serial Number) of the devices line-by-line or comma-separated or click **Import .csv** option to **import the MSNs/ESNs** of the devices from a file.
4. Click **Claim Devices** to add to the selected AP Group with the configuration applied.

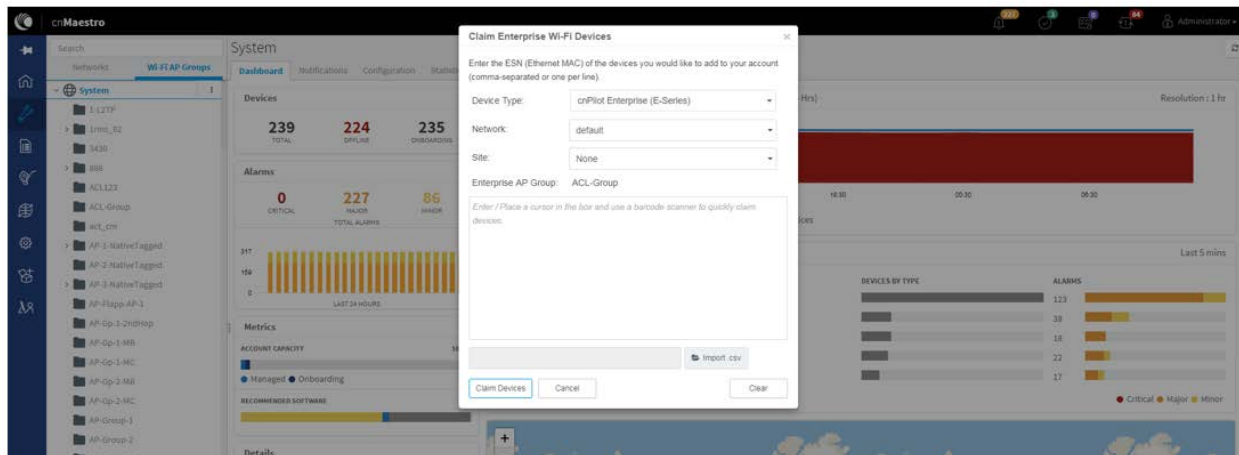


Figure 22 Claiming the device using MAC address (ESN)

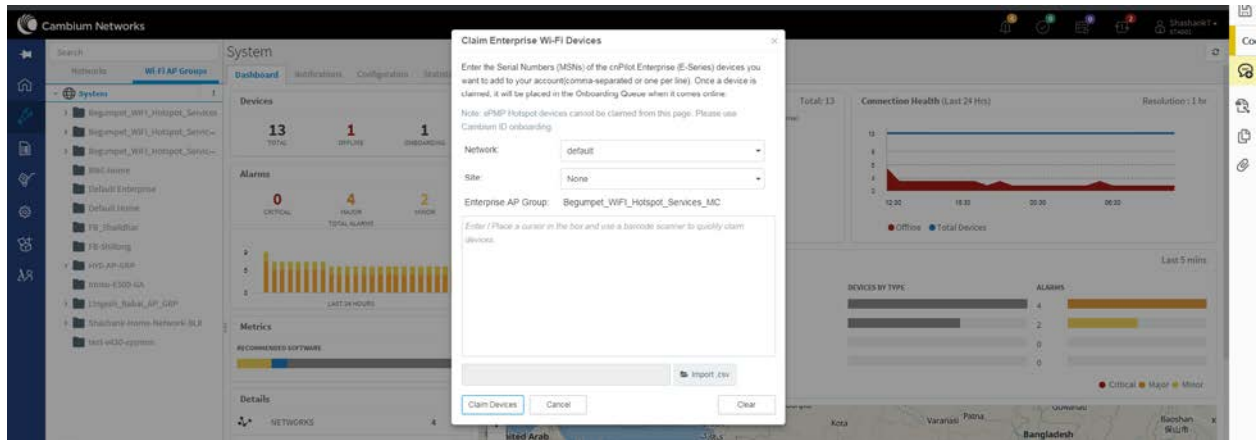


Figure 23 Claiming the device using Serial Number (MSN)

## Site dashboard

In order to claim multiple devices from the Site dashboard in the cloud, navigate to the **Manage** section and select a site under a network and click the drop-down menu for the selected site:

1. Click the **Claim Devices** option.
2. In the pop-up dialog, select the Network and Site under which these devices need to be placed and by default, the devices claimed under this group will have the configuration settings from this AP Group.
3. Specify the MSNs (Manufacturing Serial Number) /ESNs (Equipment Serial Number) of the devices line-by-line or comma-separated or click Import .csv option to import the MSNs/ESNs of the devices from a file.
4. Click **Claim Devices** to add to the selected AP Group with the configuration applied.



**Note** Claim using MAC address is supported by cnMaestro On-Premises only.

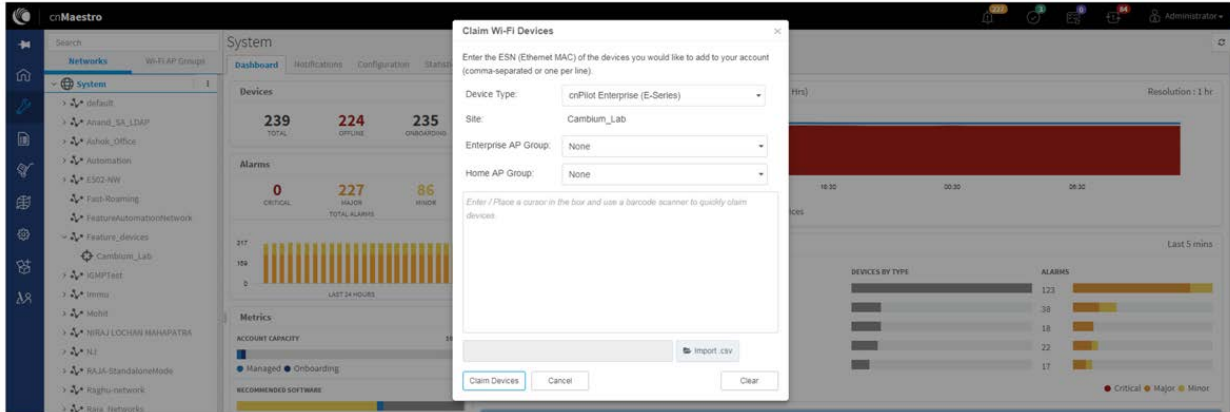


Figure 24 Claim the device using MAC address

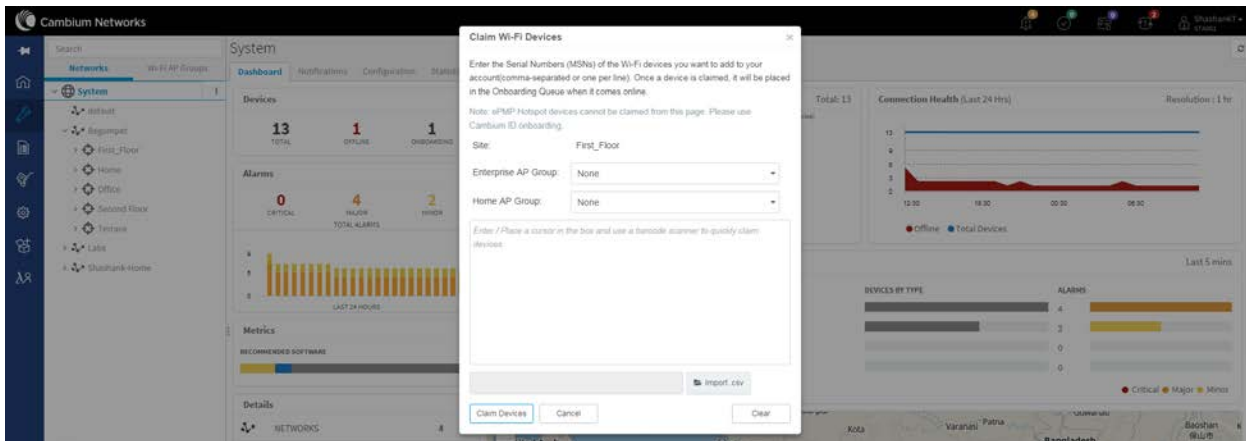


Figure 25 Claim the device using MSN

## Directing Devices to the cnMaestro On-Premises Server Using DHCP

This section includes the following topics:

- [DHCP Option 43](#)
- [DHCP Option 15](#)

### DHCP Option 43

This mode of onboarding is preferred to use when cnMaestro On-Premises is deployed at the customer end. cnPilot reads Option 43 during DHCP transaction and then it connects to respective cnMaestro. This option is given high priority during cnMaestro discovery process. All these devices which have read the Option 43 from DHCP transaction are available in Queue on cnMaestro, which needs to be further approved by end-user.



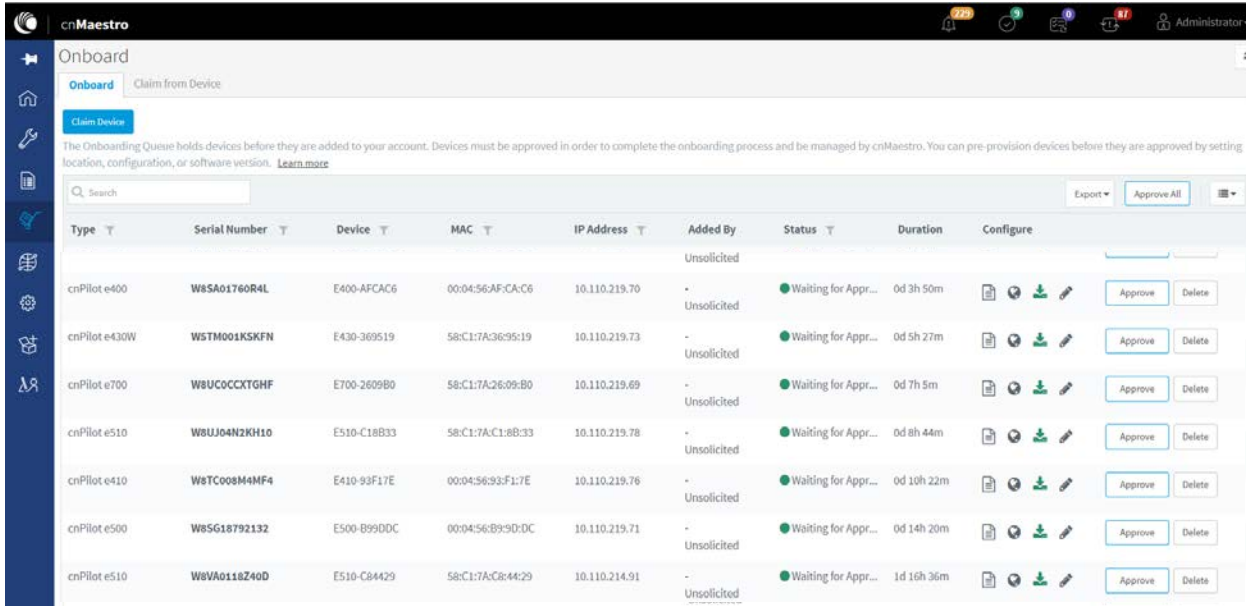


Figure 26 DHCP option 43

## DHCP Option 15

This mode of onboarding is preferred to use when cnMaestro On-Premises is deployed at the customer end. cnPilot reads Option 15 during DHCP transaction and then it connects to respective cnMaestro. All these devices which have read the Option 15 from DHCP transaction are available in Queue on cnMaestro, which needs to be further approved by end-user.

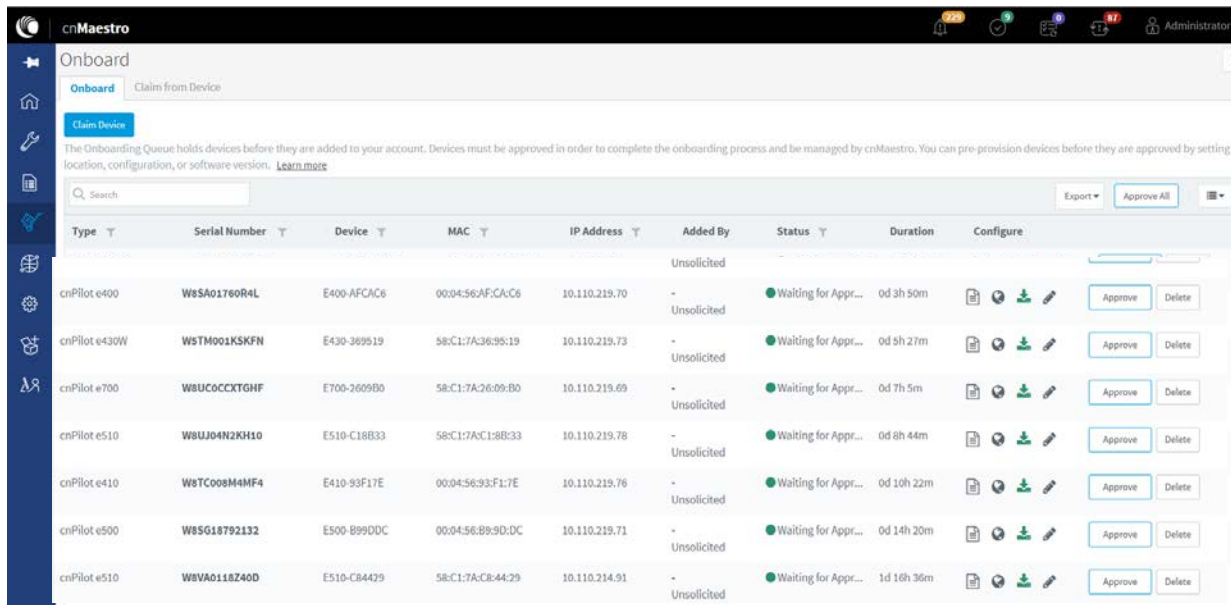


Figure 27 DHCP option 15

## DHCP Server Configuration

More details on various DHCP server configuration for Option 43 is available in Cambium Knowledge Base (KB) section.

## Windows Server Configuration

For Windows server configuration for onboarding devices to cnMaestro On-Premises server, please click the below URL.

<http://community.cambiumnetworks.com/t5/cnMaestro/Device-Onboarding-and-Windows-DHCP-Options-for-cnMaestro-On/m-p/55199>

## Linux Server Configuration

A DHCP Server can be used to configure the IP Address, Gateway, and DNS servers for Cambium devices. If you administer the DHCP Server, you can also configure DHCP Options that will tell the devices how to access the cnMaestro (so the URL doesn't need to be set on each device).

<http://community.cambiumnetworks.com/t5/cnMaestro/Device-Onboarding-and-Linux-DHCP-Options-for-cnMaestro-On/m-p/55187>

## Microtik Server Configuration

For Microtik Routerboard DHCP configuration for onboarding devices to cnMaestro On-Premises server, please click the below link.

<http://community.cambiumnetworks.com/t5/cnMaestro/Microtik-Routerboard-DHCP-configuration-for-Onboarding-devices/m-p/56012>

# Claim using Cambium ID

This section includes the following topics:

- [Claim through static URL without Cambium ID and onboarding key](#)
- [Claim through static URL with Cambium ID and onboarding key](#)

## Claim Through Static URL without Cambium ID and Onboarding Key

In order to claim the devices using the static URL without Cambium ID and onboarding key please follow the below steps:

1. Login to device UI and navigate to **Configure > System > Management > cnMaestro**.
2. Provide a static URL of On-Premises <https://ON-PREMISESIPADDRESSORHOSTNAME> and click **Save**.
3. The device will come to the onboarding queue in the cnMaestro **Home > Onboard Devices > Onboard** page and the user can approve the device.

| Type         | Serial Number | Device                | MAC | IP Address     | Managed Account     | Added By                        | Status    | Duration  | Configure | Actions     |
|--------------|---------------|-----------------------|-----|----------------|---------------------|---------------------------------|-----------|-----------|-----------|-------------|
| cnPilot E500 |               | Rajesh                |     | 10.110.208.167 | Base Infrastructure | Administrator Unsolicited       | Onboarded | 3d 22h 8m | Summary   | ONBOARDED ↗ |
| cnPilot E400 |               | E400-cnPilot-182-RGVN |     | 10.110.212.182 | BesKOM              | Unsolicited                     | Onboarded | 4d 2h 45m | Summary   | ONBOARDED ↗ |
| cnPilot E400 |               | E400-BSADE0           |     | 10.110.202.103 | BesKOM              | Administrator Using MAC Address | Onboarded | 6d 5h 17m | Summary   | ONBOARDED ↗ |

Figure 28 Claim through static URL without Cambium ID and onboarding key

## Claim Through Static URL with Cambium ID and Onboarding Key

In order to claim the devices using the static URL with Cambium ID and onboarding key, please follow the below steps:

1. Login to On-Premises server using default username and password (admin/admin) or the username and password set by the Administrator at the time of installation.
2. Navigate to **Home > Onboard Devices > Claim from Device** page.
3. Select the checkbox for “Enable Cambium ID-based authentication to onboard devices”.
4. Click on **Add new** and select the username from the drop-down list and specify the onboarding key and click **Save**.
5. Login to device UI and navigate to **Configure > System > Management > cnMaestro**.
6. Provide a static URL of On-Premises **https://ON-PREMISESIPADDRESSORHOSTNAME** and Cambium ID (cnMaestro\_On-Premises) and onboarding key for that user and click **Save**.
7. The device will come to the onboarding queue in the cnMaestro **Home > Onboard Devices > Onboard** page and the user can approve the device.

Onboard Devices

Claim from cnMaestro Onboard Claim from Device Unclaim

Claim Devices Using Cambium ID

Cambium ID: cnmaestro\_on\_premises

Enable Cambium ID based authentication to onboard devices

Enabling this feature allows a device to be claimed by entering the Cambium ID and Onboarding Key on the device. This information can be set on the device via its user interface (or SNMP or CLI on some devices). Each administrator can have their own Onboarding Key.

The following users can claim devices using the cnMaestro Cambium ID and the user's Onboarding Key.

User: Admin Onboarding Key: [Redacted] [Delete]

[Add New] [Cancel] [Save]

Figure 29 Claim through static URL with Cambium ID and onboarding key

## Chapter 6: Network Monitoring

The Monitoring tab displays the monitoring pane for cnMaestro c4000 Controller. This section includes the following:

- [Dashboard](#)
- [Notifications](#)
- [Statistics and Details](#)
- [Performance](#)
- [Maps](#)
- [Tools](#)
- [WIDS](#)

### Dashboard

Dashboard pages are customized for each device type and aggregation level (such as System, Network, Tower, and Site). Pages representing devices provide information on location, significant configuration parameters, and performance. A system, Network, Tower, and Site nodes aggregate dashboard data for the devices they contain.

### KPI (Key Performance Indicators)

Each page has a set of KPIs tailored to the node type. These present a current value and often historical trend data over the last 24 hours.

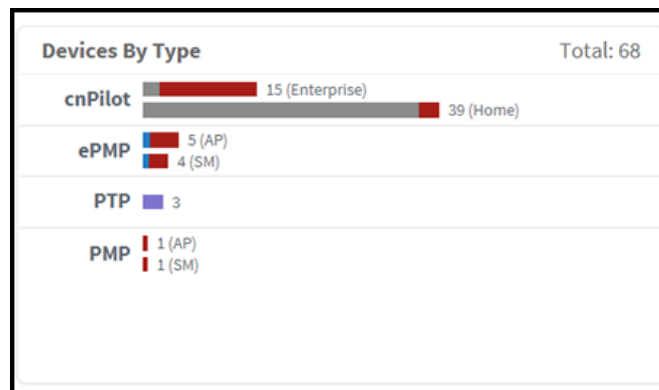


Figure 30 Key performance indicators

### Device Health

Device Health displays the health of the network from the Tower to the Edge.

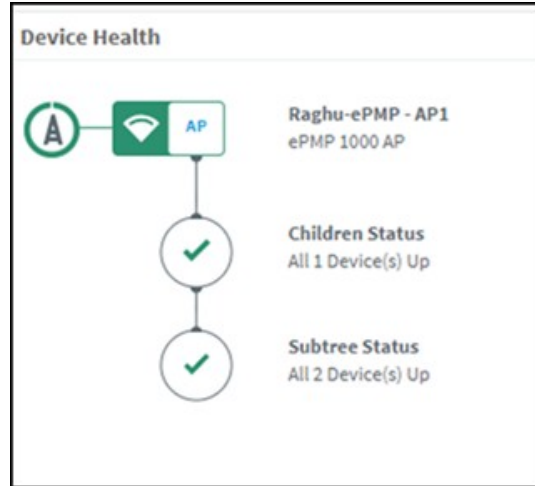


Figure 31 Device Health

## Connection Health

Connection health displays the health of the devices connected to the network.

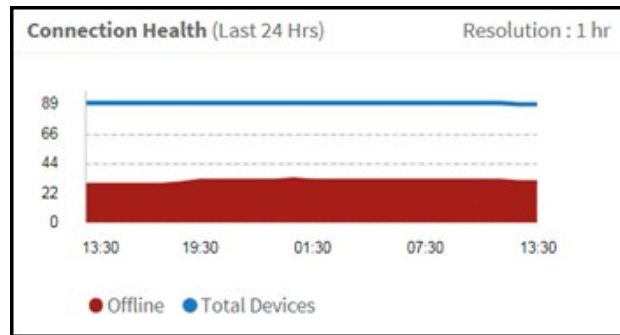


Figure 32 Connection Health

## Charts and Graphs

Contextual charts and graphs provide details on important Dashboard metrics.

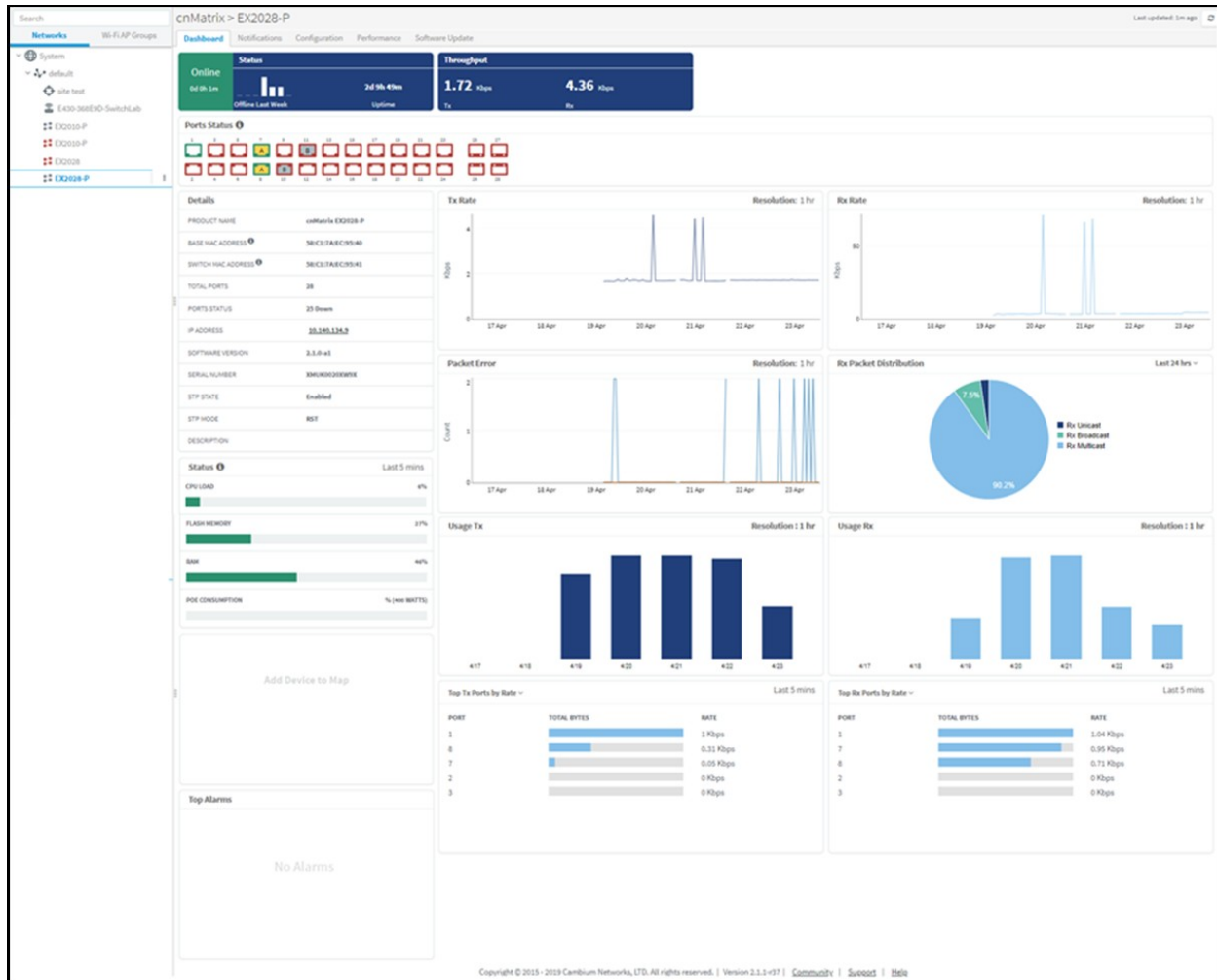


Figure 33 Charts and Graphs

## Notifications

### Overview

Notifications consist of Events and Alarms. They are asynchronous messages that provide real-time system status.

Table 12 Notification parameters

| Type          | Description   |
|---------------|---|
| Alarms        | Alarms have a state and persist if the problematic activity continues; they reflect the current health of the devices in the network. |
| Alarm History | Expired Alarms are added to the Alarm History. The Alarm History displays historical active alarm counts.                             |

| Type   | Description  |
|--------|--|
| Events | Events are stateless, transient messages that occur in response to an input or action, such as if the CPU exceeds a threshold or a device association fails. Events are fire-and-forget; they are stored in an Event Table and provide a history of device activity. |

## Event/Alarm Source

Identity of the source device affected by the event or alarm.

## Aggregation

Notifications are visible at every level of the Device Tree. Higher levels consolidate notifications for all devices at lower levels in the hierarchy. For example, the network level displays the events and alarms for all devices within that network. This aggregation is only available for Networks, Towers, and Sites. When a device is selected, such as an AP, the notifications will only be presented for it, and not its associated SMS (even though they are lower in the tree).

## Storage

Events and Alarms are stored in cnMaestro c4000 Controller for an extended period. They will be removed when the total count of each surpasses 1,000 multiplied by the number of devices in the account. The oldest entries will be cleared first.





## Events

The Event Table stores a history of the most recent events for the selected node.

## Event Severity

Event Severity is mapped to the following levels:

**Table 13 Event Severity**

|   | Severity | Definition  |
|---|----------|---|
|  | Critical | Catastrophic problem that makes the product/feature unusable.                                       |
|  | Major    | Issue that greatly degrades the product/feature, but it is still usable.                            |
|  | Minor    | Limited issue that alters product functionality in a targeted way.                                  |
|  | Notify   | Message used primarily for notification which includes the type of reboot of cnPilot Wi-Fi devices. |

## Event Export

The event data in a table can be exported in a CSV or PDF file format.

## Alarms

### Alarm Life Cycle

The basic alarm life cycle has the following states:





**Table 14 Alarm Life Cycle**

| State        | Description   |
|--------------|---|
| Raised       | The creation of the alarm.  |
| Active       | The alarm remains active until the combination of inputs that generated it is cleared.  |
| Acknowledged | Active alarms can be acknowledged, which signifies they are known and being handled. Acknowledgment does not affect the total alarm count - it is a convenience to the administrator.   |
| Inactive     | Inactive alarms remain visible in the active Alarm Table for 10 minutes, before they are moved to Alarm History. An alarm becomes inactive when the inputs that generated are no longer present. An Inactive alarm can be pulled back to the Active/Acknowledged states if a new event reactivates the alarm. |

### Alarm Severity

Alarms have a severity that determines how they are handled.

**Table 15 Alarm Severity**

|   | Severity | Definition   |
|---|----------|--|
|  | Critical | Catastrophic problem that makes the product/feature unusable.                        |
|  | Major    | Significant issue that greatly degrades the product/feature, but it is still usable. |
|  | Minor    | Limited issue that alters product functionality in a targeted way.                   |
|  | Notify   | It is clear and is used for inactive alarms.   |



## Alarm Types

**Table 16 Alarm Types**

| Alarm Type    | Definition  |
|---------------|---|
| Configuration | Tracks issues encountered during a device configuration update.                   |
| Upgrade       | Tracks issues encountered during the device software upgrade.                     |
| DFS State     | Tracks issues related to DFS operational status.                                  |
| GPS State     | Tracks issues related to GPS synchronization.                                     |
| Link State    | Tracks issues related to the status of device interfaces.                         |
| Status        | Tracks when connectivity between cnMaestro c4000 Controller and a device is lost. |

## Alarm Acknowledgment

Active alarms can be acknowledged in the Alarm Table. This is for convenience – acknowledgment makes the alarm less visible in the table, and the administrator can further add a note describing how the alarm is being resolved.

Acknowledging an alarm will not change any of the alarm counts – either at the page or the system level. The only way the alarm count is decreased is when alarms become inactive.

Alarm Acknowledge

Acknowledgement Details:  
- NA:

Please enter notes about this alarm in the text box below and click Submit.

Cancel Acknowledge

**Figure 34 Alarm Acknowledge**

## Alarm History

Expired Alarms are added to the Alarm History. The Alarm History displays historical active alarm counts. Clicking the bar chart filters the table data underneath, allowing one to view which alarms were active at a specific time in the past.

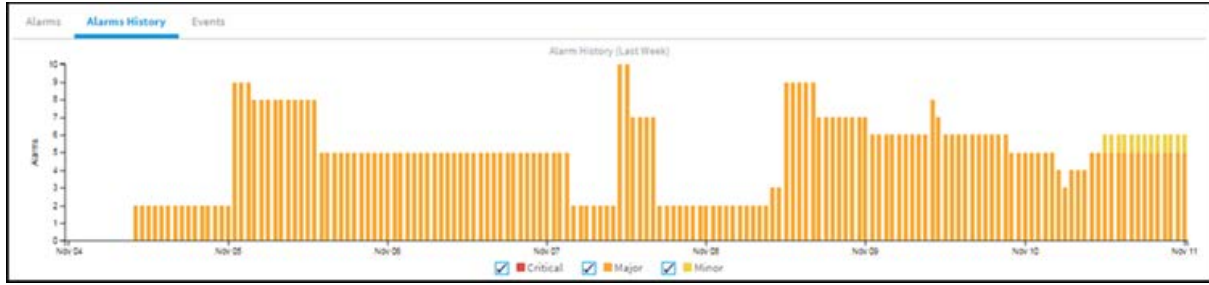


Figure 35 Alarm History

## Statistics and Details

Statistics provide a tabular aggregation of data, including General information on the devices monitored, as well as Wireless, Network, and Traffic metrics. Details pages provide information on a single device, generally in a page format.

The table below highlights the type of information that is generally found in cnMaestro c4000 Controller Statistics and Details sections (separated by Device Type).

Table 17 Device Statistics

| Device                        | Fields   |
|-------------------------------|--|
| cnMatrix                      | <ul style="list-style-type: none"> <li>• Device</li> <li>• Product Name</li> <li>• Serial Number</li> <li>• IP Address</li> <li>• Status</li> <li>• Session Time</li> <li>• Throughput (UL)</li> <li>Throughput (DL)</li> </ul>    |
| cnPilot (Home and Enterprise) | <p><b>General</b></p> <ul style="list-style-type: none"> <li>• Device</li> <li>• Serial Number</li> <li>• Product Name</li> <li>• IP Address</li> <li>• Status</li> <li>• State</li> <li>• Type</li> <li>• Client Count</li> </ul> |

| Device  | Fields   |
|---------|--|
|         | <p><b>Wireless</b></p> <ul style="list-style-type: none"> <li>• Device</li> <li>• IP Address</li> <li>• Status</li> <li>• Type</li> <li>• Channel</li> <li>• Power</li> </ul> <p><b>Traffic</b></p> <ul style="list-style-type: none"> <li>• Device</li> <li>• IP Address</li> <li>• Status</li> <li>• Type</li> <li>• Throughput (UL)</li> <li>• Throughput (DL)</li> </ul>   |
| cnReach | <p><b>Overview</b></p> <ul style="list-style-type: none"> <li>• System</li> <li>• Software Update</li> <li>• Configuration Update</li> <li>• Network</li> <li>• Radio Details</li> </ul> <p><b>Interfaces</b></p> <ul style="list-style-type: none"> <li>• Name</li> <li>• IP Address</li> <li>• Mask</li> <li>• Gateway</li> <li>• DNS</li> <li>• MAC</li> </ul> <p><b>Neighbors</b></p> <ul style="list-style-type: none"> <li>• IP Address</li> <li>• Device ID</li> <li>• Local RSSI</li> <li>• Remote RSSI</li> </ul> |

| Device  | Fields  |
|---------|---|
|         | <ul style="list-style-type: none"> <li>• Local Noise</li> <li>• Remote Noise</li> <li>• Remote Tx Power</li> <li>• MAC</li> </ul> <p><b>Radio 1 (AP) Children</b></p> <ul style="list-style-type: none"> <li>• Device</li> <li>• Managed Account</li> <li>• Address</li> <li>• Status</li> <li>• Radio</li> <li>• Role</li> <li>• Neighbor Count</li> </ul>   |
| ePMP AP | <p><b>General</b></p> <ul style="list-style-type: none"> <li>• Device</li> <li>• IP Address</li> <li>• Status</li> <li>• Registered SM Count</li> <li>• DFS Status</li> <li>• Serial Number</li> <li>• Reregistration Count</li> </ul> <p><b>Wireless</b></p> <ul style="list-style-type: none"> <li>• Device</li> <li>• SSID</li> <li>• Antenna Gain</li> <li>• Frequency</li> <li>• Tx Power</li> <li>• Bandwidth</li> <li>• DL/UL Ratio</li> <li>• Maximum Range</li> </ul> <p><b>Network</b></p> <ul style="list-style-type: none"> <li>• Device</li> <li>• Status</li> </ul> |

| Device  | Fields  |
|---------|---|
|         | <ul style="list-style-type: none"> <li>• LAN Interface</li> <li>• LAN Interface 2</li> </ul> <p><b>Traffic</b></p> <ul style="list-style-type: none"> <li>• Device</li> <li>• Throughput (UL)</li> <li>• Throughput (DL)</li> <li>• Retransmission Rate (DL)</li> </ul>   |
| ePMP SM | <p><b>General</b></p> <ul style="list-style-type: none"> <li>• Device</li> <li>• IP Address</li> <li>• Status</li> <li>• Session Time</li> <li>• Distance</li> <li>• DFS Status</li> <li>• Serial Number</li> </ul> <p><b>Wireless</b></p> <ul style="list-style-type: none"> <li>• Device</li> <li>• Wireless MAC</li> <li>• Status</li> <li>• Antenna Gain</li> <li>• SSID</li> <li>• IP Address</li> <li>• RSSI (DL)</li> <li>• RSSI (UL)</li> <li>• MCS (UL)</li> <li>• MCS (DL)</li> <li>• Quality</li> <li>• Capacity</li> <li>• Tx Power</li> <li>• Connected AP</li> </ul> <p><b>Network</b></p> <ul style="list-style-type: none"> <li>• Device</li> </ul> |

| Device | Fields   |
|--------|--|
|        | <ul style="list-style-type: none"> <li>• Status</li> <li>• LAN Interface</li> <li>• LAN Interface 2</li> <li>• IP Address</li> </ul> <p><b>Traffic</b></p> <ul style="list-style-type: none"> <li>• Device</li> <li>• IP Address</li> <li>• Status</li> <li>• Throughput (UL)</li> <li>• Throughput (DL)</li> <li>• Retransmission Rate (UL)</li> <li>• Retransmission Rate (DL)</li> </ul>  |
| PMP AP | <p><b>General</b></p> <ul style="list-style-type: none"> <li>• Device</li> <li>• IP Address</li> <li>• Status</li> <li>• Registered SM Count</li> <li>• DFS Status</li> <li>• Serial Number</li> <li>• Status</li> <li>• Reregistration Count</li> </ul> <p><b>Wireless</b></p> <ul style="list-style-type: none"> <li>• Device</li> <li>• Color code</li> <li>• Frequency</li> <li>• Tx Power</li> <li>• Bandwidth</li> <li>• Downlink Ratio</li> <li>• Maximum Range</li> <li>• Antenna Gain</li> </ul> <p><b>Network</b></p> <ul style="list-style-type: none"> <li>• Device</li> </ul> |

| Device | Fields  |
|--------|---|
|        | <ul style="list-style-type: none"> <li>• Status</li> <li>• LAN Interface</li> </ul> <p><b>Traffic</b></p> <ul style="list-style-type: none"> <li>• Device</li> <li>• Throughput (UL)</li> <li>• Throughput (DL)</li> <li>• Frame Utilization (UL)</li> <li>• Frame Utilization (DL)</li> </ul>  |
| PMP SM | <p><b>General</b></p> <ul style="list-style-type: none"> <li>• Device</li> <li>• IP Address</li> <li>• Status</li> <li>• Session Time</li> <li>• Distance</li> <li>• DFS Status</li> <li>• Serial Number</li> </ul> <p><b>Wireless</b></p> <ul style="list-style-type: none"> <li>• Device</li> <li>• Color Code</li> <li>• IP Address</li> <li>• Modulation (DL)</li> <li>• Tx Power</li> <li>• Connected AP</li> <li>• RSSI Imbalance</li> <li>• Modulation (UL)</li> <li>• Antenna Gain</li> <li>• Status</li> <li>• RSSI</li> </ul> <p><b>Network</b></p> <ul style="list-style-type: none"> <li>• Device</li> <li>• Status</li> <li>• LAN Interface</li> </ul> |

| Device | Fields  |
|--------|---|
|        | <ul style="list-style-type: none"> <li>• IP Address</li> <li>• WAN IP Address</li> </ul> <p><b>Traffic</b></p> <ul style="list-style-type: none"> <li>• Status</li> <li>• Device</li> <li>• IP Address</li> <li>• Packet Loss</li> <li>• Packet Loss (Overcapacity) (UL)</li> <li>• Packet Loss (Error Drop) (UL)</li> <li>• Packet Loss (Overcapacity) (DL)</li> <li>• Packet Loss (Error Drop) (DL)</li> <li>• Throughput (UL)</li> <li>• Throughput (DL)</li> </ul>  |
| PTP    | <p><b>System</b></p> <ul style="list-style-type: none"> <li>• Name</li> <li>• Device Type</li> <li>• System Uptime</li> <li>• Coordinates</li> <li>• Description</li> <li>• Hardware Version</li> <li>• DA Version</li> </ul> <p><b>Network</b></p> <ul style="list-style-type: none"> <li>• Main PSU Interface</li> <li>• Auxiliary Interface</li> <li>• SFP Interface</li> <li>• IP Address</li> <li>• Subnet Mask</li> <li>• Gateway</li> <li>• DNS Server</li> <li>• Management VLAN ID</li> <li>• Management VLAN Type</li> </ul> <p><b>Wireless</b></p> |



| Device | Fields  |
|--------|---|
|        | <ul style="list-style-type: none"> <li>• Transmit Frequency</li> <li>• Receive Frequency</li> <li>• Channel Bandwidth</li> <li>• Maximum Transmit Power</li> <li>• County Code</li> <li>• Antenna Gain</li> <li>• Symmetry</li> <li>• Errored Seconds</li> <li>• Severely Errored Seconds</li> <li>• Unavailable Seconds</li> </ul> |

## Performance

Performance pages display a synchronized view of time-series data for devices. The data can be filtered using the interval ranges in the upper left (last 4 hours to last week), or by dragging the cursor on the graph to select a specific range. The data presented vary based on device type.

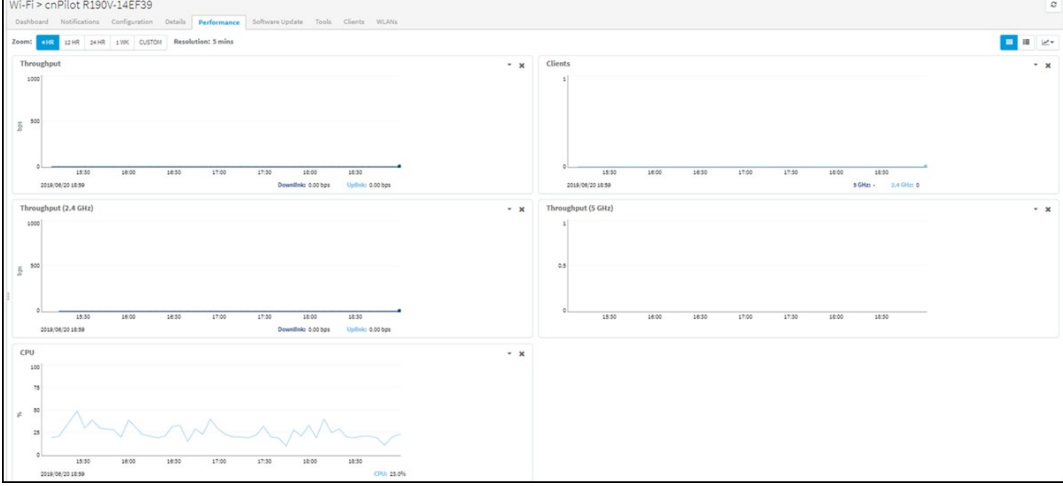
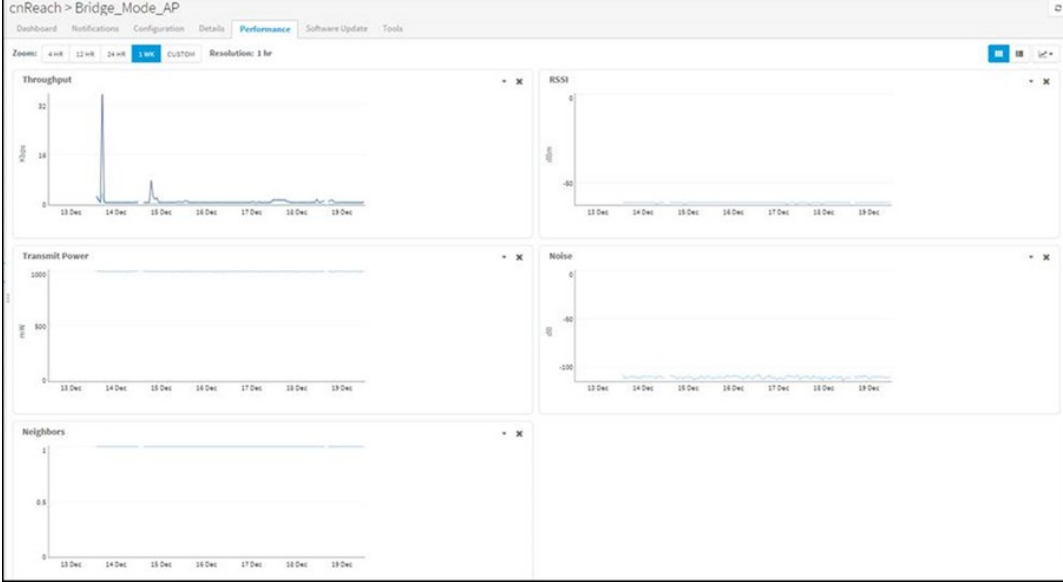
The following images represent the sample performance graphs for cnMatrix, cnPilot Enterprise, cnPilot Home, cnReach, ePMP AP, ePMP SM, PMP AP, PMP SM, PTP.

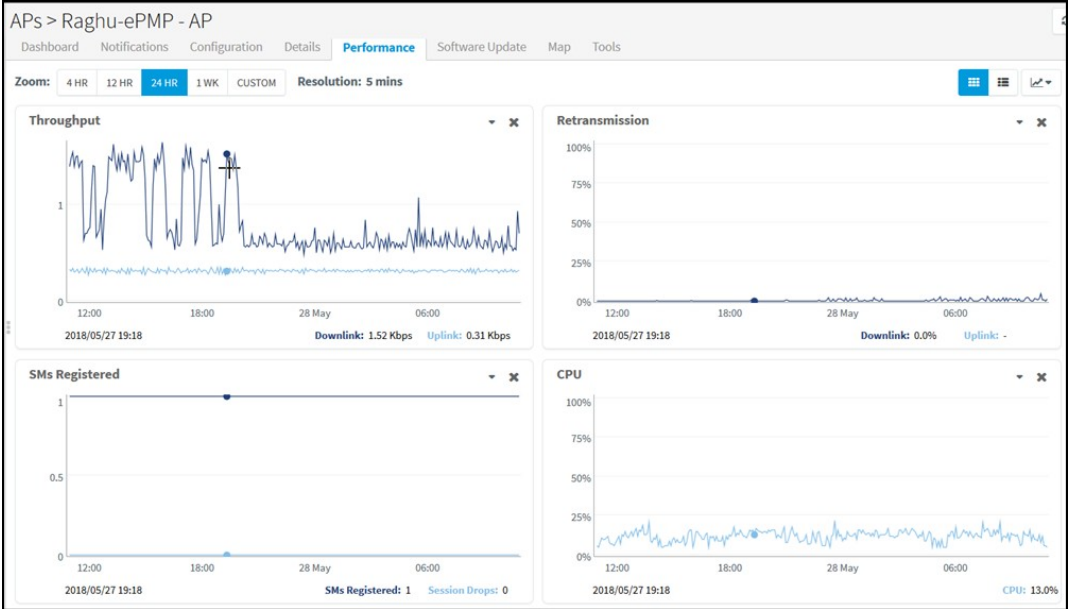
**Table 18 Performance**

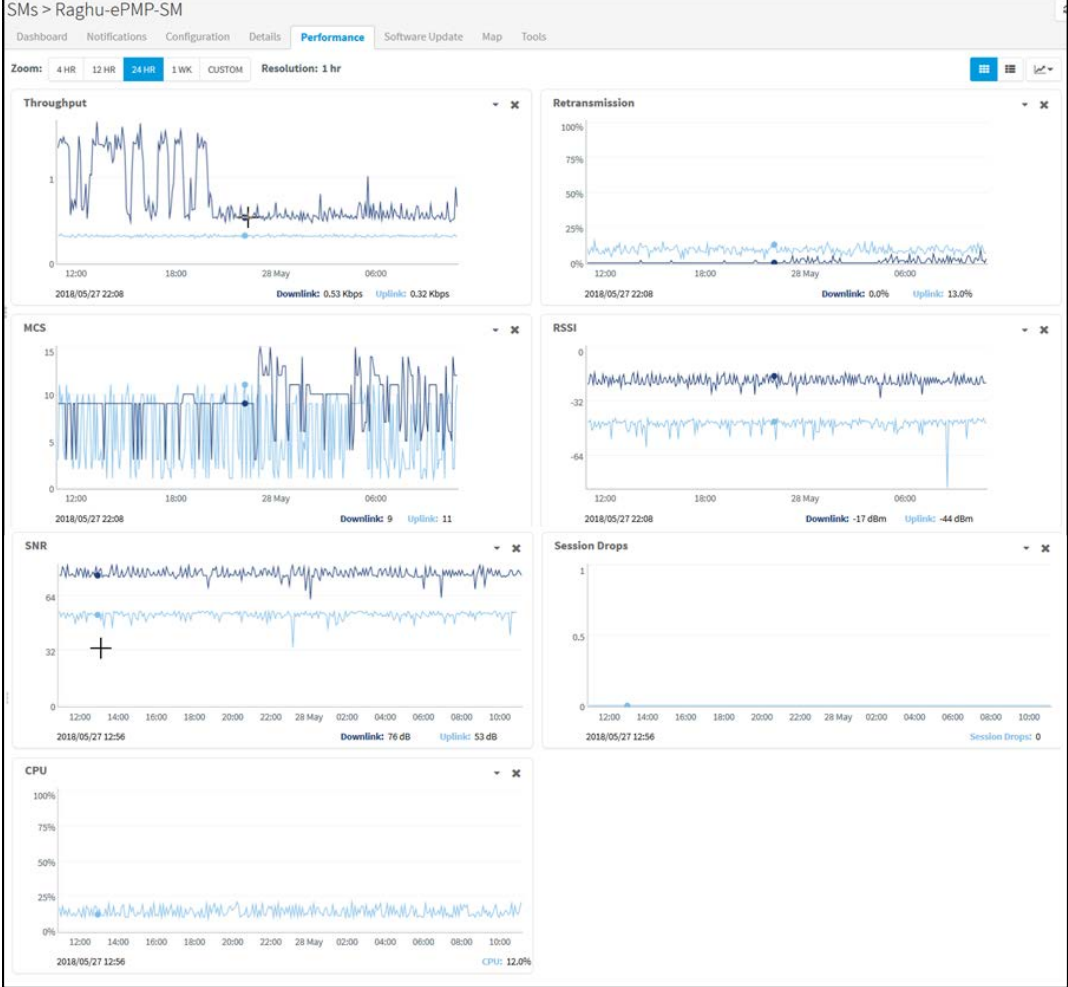
| Device   | Fields  |
|----------|---|
| cnMatrix | Displays the following graphs: <ul style="list-style-type: none"> <li>• Throughput</li> <li>• Tx Packets</li> <li>• Rx Packets</li> <li>• CPU</li> <li>• Packets</li> </ul> |

| Device                       | Fields   |
|------------------------------|--|
|                              |  |
| <p>cnPilot Enterprise AP</p> | <p>Displays the following graphs:</p> <ul style="list-style-type: none"> <li>• Throughput</li> <li>• Clients</li> <li>• Throughput (2.4 GHz)</li> <li>• Throughput (5 GHz)</li> <li>• Noise Floor</li> <li>• Interference</li> <li>• Airtime (2.4 GHz)</li> <li>• Airtime (5 GHz)</li> <li>• Packet Rate</li> <li>• CPU</li> <li>• Available Memory</li> </ul> |

| Device                 | Fields   |
|------------------------|--|
|                        |  |
| <p>cnPilot Home AP</p> | <p>Displays the following graphs:</p> <ul style="list-style-type: none"> <li>• Throughput</li> <li>• Throughput (2.4 GHz)</li> <li>• Clients</li> <li>• Throughput (5 GHz)</li> <li>• CPU</li> </ul> |

| Device         | Fields  |
|----------------|---|
|                |   |
| <p>cnReach</p> | <p>Displays the following graphs:</p> <ul style="list-style-type: none"> <li>• Throughput</li> <li>• RSSI</li> <li>• Transmit Power</li> <li>• Noise</li> <li>• Neighbors</li> </ul>  |
| <p>ePMP AP</p> | <p>Displays the following graphs:</p> <ul style="list-style-type: none"> <li>• Throughput</li> <li>• Retransmission</li> <li>• SMs Registered</li> </ul>  |

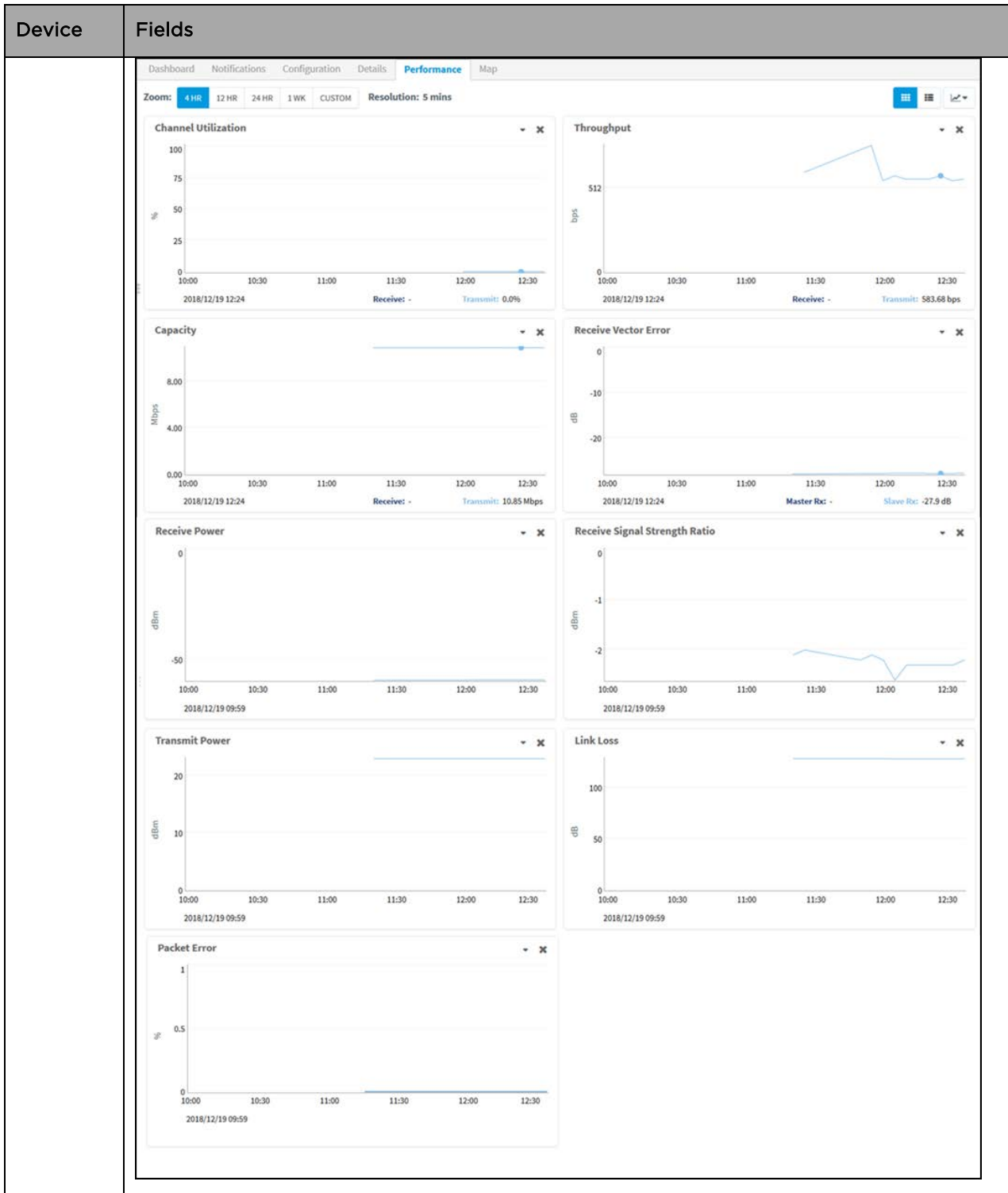
| Device  | Fields  |
|---------|---|
|         | <ul style="list-style-type: none"> <li>• CPU</li> </ul>  <p>The screenshot displays the Performance page for 'Raghu-ePMP - AP'. It features a navigation bar with 'Performance' selected. Below the navigation bar, there are zoom and resolution controls. The main area contains four graphs:         <ul style="list-style-type: none"> <li><b>Throughput:</b> Shows data for Downlink (1.52 Kbps) and Uplink (0.31 Kbps) over a 24-hour period.</li> <li><b>Retransmission:</b> Shows a percentage of retransmissions, currently at 0.0%.</li> <li><b>SMs Registered:</b> Shows the number of sessions registered, currently at 1.</li> <li><b>CPU:</b> Shows CPU usage percentage, currently at 13.0%.</li> </ul> </p> |
| ePMP SM | <p>Displays the following graphs:</p> <ul style="list-style-type: none"> <li>• Throughput</li> <li>• MCS</li> <li>• SNR</li> <li>• CPU</li> <li>• Retransmission</li> <li>• RSSI</li> <li>• Session Drops</li> </ul>  |

| Device | Fields   |
|--------|--|
|        |  <p>Sms &gt; Raghu-ePMP-SM</p> <p>Dashboard Notifications Configuration Details <b>Performance</b> Software Update Map Tools</p> <p>Zoom: 4 HR 12 HR <b>24 HR</b> 1 WK CUSTOM Resolution: 1 hr</p> <p><b>Throughput</b></p> <p>12:00 18:00 28 May 06:00</p> <p>2018/05/27 22:08 Downlink: 0.53 Kbps Uplink: 0.32 Kbps</p> <p><b>Retransmission</b></p> <p>100% 75% 50% 25% 0%</p> <p>12:00 18:00 28 May 06:00</p> <p>2018/05/27 22:08 Downlink: 0.0% Uplink: 13.0%</p> <p><b>MCS</b></p> <p>15 10 5 0</p> <p>12:00 18:00 28 May 06:00</p> <p>2018/05/27 22:08 Downlink: 9 Uplink: 11</p> <p><b>RSSI</b></p> <p>0 -32 -64</p> <p>12:00 18:00 28 May 06:00</p> <p>2018/05/27 22:08 Downlink: -17 dBm Uplink: -44 dBm</p> <p><b>SNR</b></p> <p>64 32 0</p> <p>12:00 14:00 16:00 18:00 20:00 22:00 28 May 02:00 04:00 06:00 08:00 10:00</p> <p>2018/05/27 12:56 Downlink: 76 dB Uplink: 53 dB</p> <p><b>Session Drops</b></p> <p>1 0.5 0</p> <p>12:00 14:00 16:00 18:00 20:00 22:00 28 May 02:00 04:00 06:00 08:00 10:00</p> <p>2018/05/27 12:56 Session Drops: 0</p> <p><b>CPU</b></p> <p>100% 75% 50% 25% 0%</p> <p>12:00 14:00 16:00 18:00 20:00 22:00 28 May 02:00 04:00 06:00 08:00 10:00</p> <p>2018/05/27 12:56 CPU: 12.0%</p> |
| PMP AP | <p>Displays the following graphs:</p> <ul style="list-style-type: none"> <li>• Throughput</li> <li>• Frame Utilization</li> <li>• SMs Registered</li> <li>• CPU</li> </ul>   |

| Device | Fields   |
|--------|--|
|        | <p>APs &gt; PMP-AP-Dev1</p> <p>Dashboard   Notifications   Configuration   Details   <b>Performance</b>   Software Update   Map   Tools</p> <p>Zoom: 1 HR   12 HR   24 HR   1 WK   CUSTOM   Resolution: 5 mins</p> <p><b>Throughput</b></p> <p>Downlink: 8.42 Kbps   Uplink: 16.18 Kbps</p> <p><b>Frame Utilization</b></p> <p>Downlink: 0.0%   Uplink: 0.0%</p> <p><b>SMS Registered</b></p> <p>SMS Registered: 1   Session Drops: 0</p> <p><b>CPU</b></p> <p>CPU: 2.0%</p> |
| PMP SM | <p>Displays the following graphs:</p> <ul style="list-style-type: none"> <li>• Throughput</li> <li>• Modulation</li> <li>• RSSI</li> <li>• RSSI Imbalance</li> <li>• Session Drops</li> <li>• LQI (Link Quality Indicator)</li> <li>• SNR (Vertical)</li> <li>• SNR (Horizontal)</li> <li>• CPU</li> </ul>   |

| Device              | Fields   |
|---------------------|--|
|                     |  |
| <p>PTP and HCMP</p> | <p>Displays the following graphs:</p> <ul style="list-style-type: none"> <li>• Channel Utilization</li> <li>• Throughput</li> <li>• Capacity</li> <li>• Receive Vector Error</li> <li>• Receive Power</li> <li>• Receive Signal Strength Ratio</li> <li>• Transmit Power</li> <li>• Link Loss</li> <li>• Packet Power</li> </ul> |





## Maps

Maps provide visualization for Towers, Sites, and Devices. They display proximity to other devices, connectivity between devices, device health, and selectable status parameters. An example Map is presented below.

Two views are supported in System Maps and Network/Tower dashboard Maps:

1. Street view
2. Satellite view

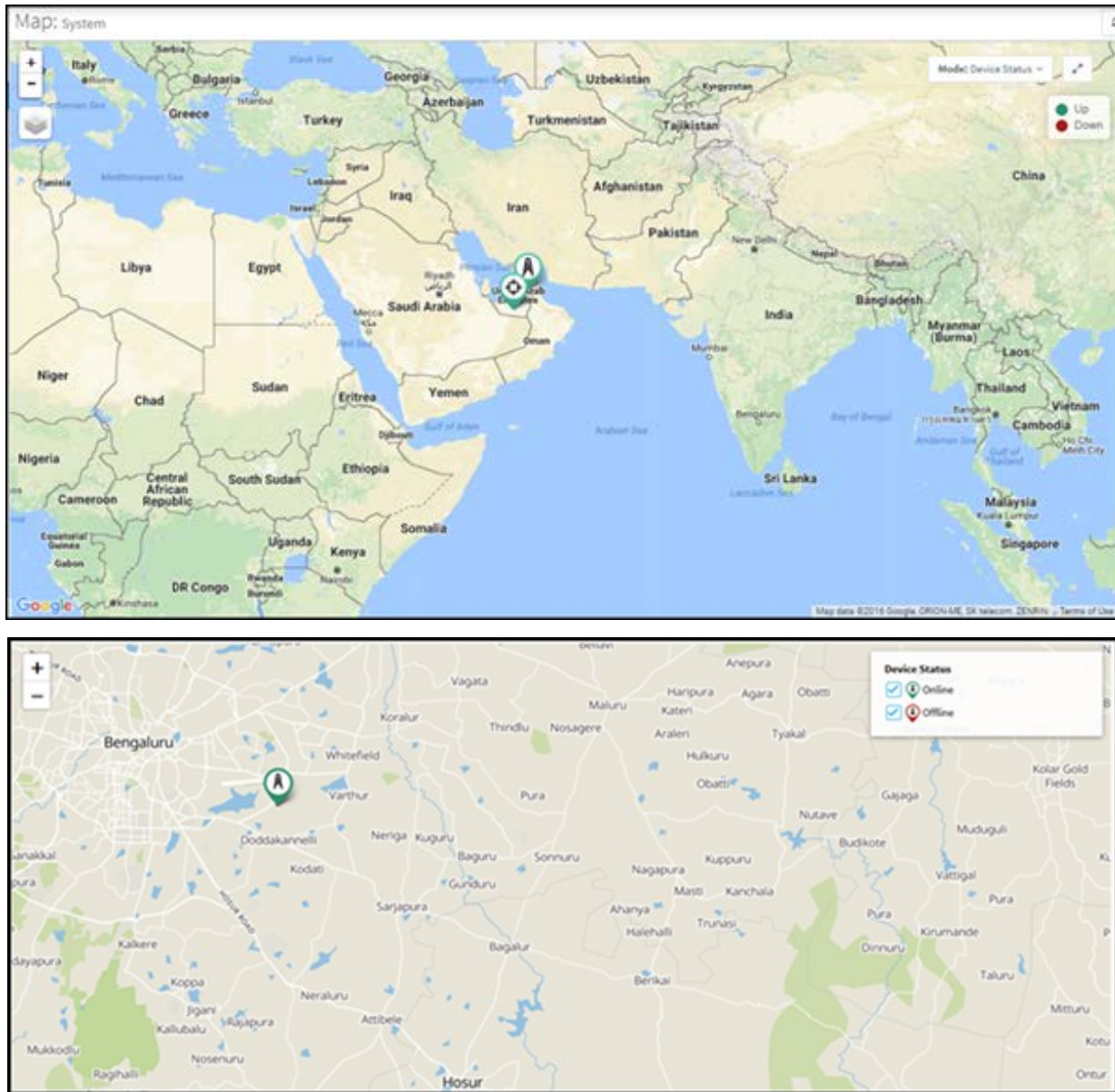
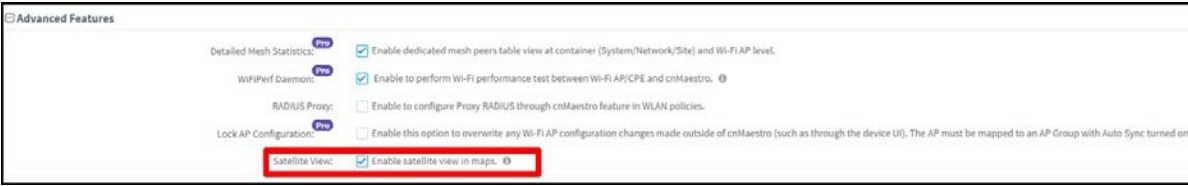


Figure 36 Map Street View

To enable the satellite view:

1. Navigate to **Settings > Advanced Features**.
2. Select the **Satellite View** checkbox to enable satellite view in maps.



The satellite view is supported in limited US and EU regions.

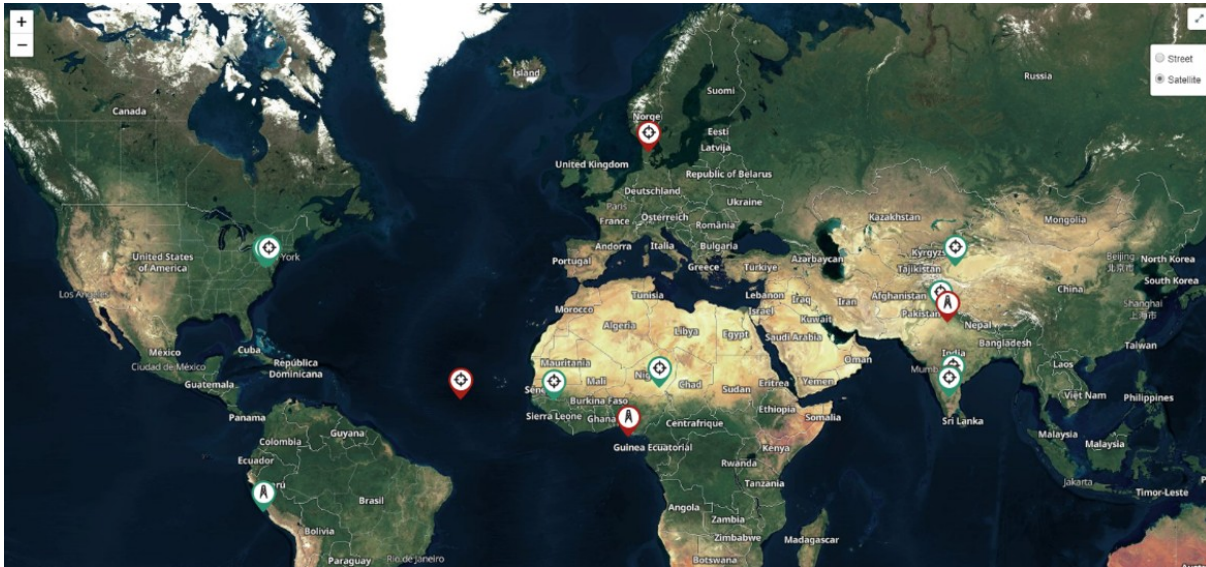


Figure 37 Map Satellite View

## Map Navigation

There are several ways to navigate through the map display.

|                     |   |
|---------------------|---|
| Standard Components | In the upper-left corner are generic map navigation components that allow one to zoom in and out. One can also use the mouse to drag and reposition the view as well as turn on satellite display.                  |
| Hover               | Hovering over a tower or device will pop-up a tooltip that provides basic status information. Hovering over an RF link will display status on the link.   |
| Single Click        | If the user single-clicks on the following items on the Map, auto-select the same item in the tree. <ul style="list-style-type: none"> <li>• Tower</li> <li>• ePMP SM</li> </ul>                                    |
| Double Click        | If the user double-clicks on the following items on the Map, the UI should auto-navigate to the Dashboard of that item <ul style="list-style-type: none"> <li>• Tower</li> <li>• ePMP SM</li> <li>• Site</li> </ul> |

## Mode

The map can be placed in a number of different modes, which define how the device status is presented.

**Table 19 Mode**

| Mode                                  | Details   |
|---------------------------------------|---|
| Device Status                         | Displays whether a device is up (green) or down (red).  |
| Alarm Status                          | Highlights devices based upon alarm count (critical, major, minor).   |
| Reregistration Count                  | Displays the nodes based upon the number of re-registrations in the last 24 hours. The more reregistration's, the larger the node will display. |
| Retransmission Percentage (ePMP only) | Displays the percentage of packets retransmitted between ePMP SM and AP on the wireless link.   |
| Average MCS (ePMP only)               | Displays the uplink or downlink average MCS per device.   |
| Frequency                             | Displays the sector frequency.  |

## Embedded Maps

Maps are embedded into some additional UI views (most notably, the Dashboard). These embedded maps do not provide the full feature set of the Map view.

## Sector Visualization

cnMaestro c4000 Controller is able to present a basic Sector View for ePMP and PMP fixed wireless devices. This requires configuration of Height, Azimuth, Elevation and Beam Width under ePMP/PMP AP configuration. This configured data is used to generate the Sector View: the presentation is not based upon link planning or geographic topology.

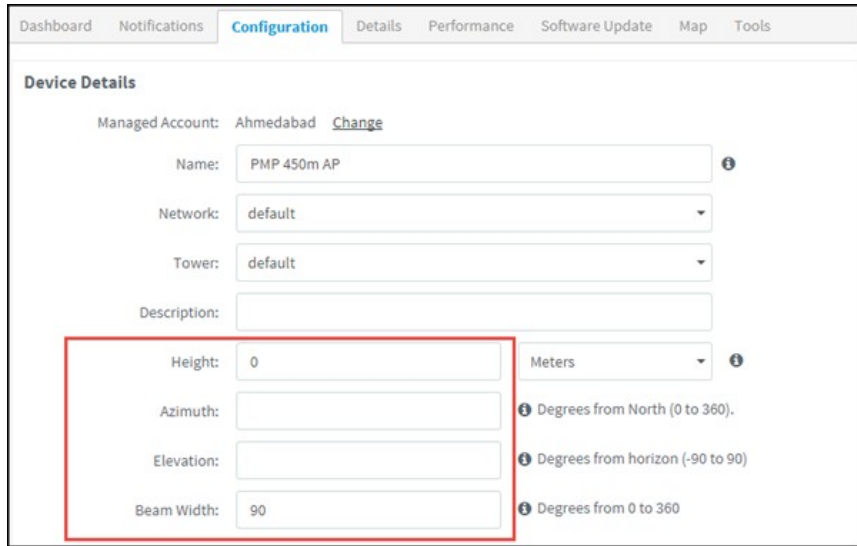


Figure 38 AP Configuration Page

A new option for Sector Visualization is available in Map View. By selecting the **Show Sector** option, the following Map will be displayed:

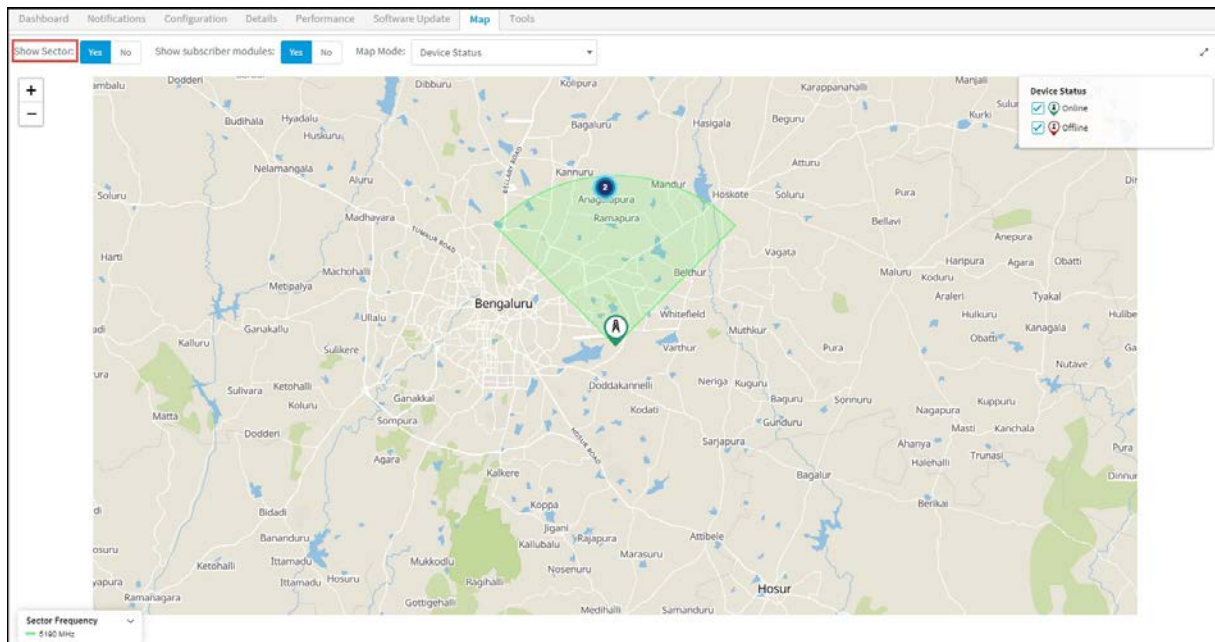


Figure 39 Sector Visualization

In addition to Sector Visualization, a new option is available to show/hide Subscriber Modules. This is present at System, Network, Tower, and AP levels. You can also choose to set the color of SMs based upon frequency or online/offline state.



**Note**

The default settings to show/hide subscriber modules is No.





## Tools

This section provides the following details:

- Tower-to-Edge View
- cnPilot Tools
- cnReach Tools
- PMP Tools
- ePMP Tools
- cnMatrix Tools

## Tower-to-Edge View

This component displays the network from the Point-to-Multipoint AP to the edge WLAN devices.

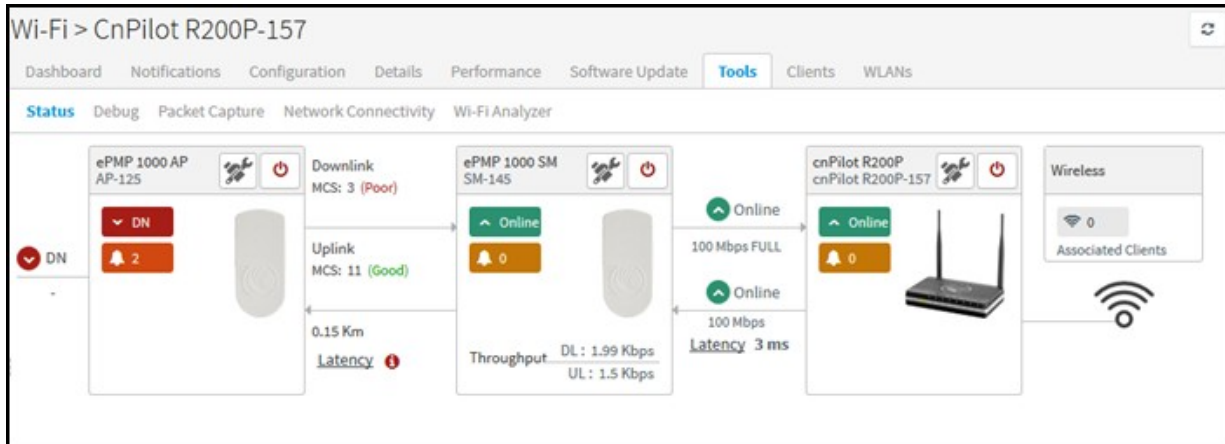




Figure 40 Tower-to-Edge View

## cnPilot Tools

The Tools page for cnPilot devices consolidates a number of operations into a single troubleshooting interface. The operations are listed below.

| Tools                | Description                              |
|----------------------|--|
| Status               | Displays the status of the device.       |
| Network Connectivity | Executes Ping, DNS, or Traceroute tests. |
| Wi-Fi Analyzer       | Displays radio traffic and signals.      |

|                                     |   |
|-------------------------------------|---|
| <p>Debug</p>                        | <ul style="list-style-type: none"> <li>• The Basic Debug mode displays log details.</li> <li>• The Advanced Debug mode is enabled for Super Admin and Admin users only. The user can switch between basic and advanced mode through the Basic or Advanced radio buttons. Non-eligible devices or users will only see basic debug mode. The user can provide the CLI command in the Command textbox. The output will be displayed in the output window.</li> </ul> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;">  <p><b>Note</b><br/>The commands that require user interaction (Eg: service start-shell) will not work in Advance Debug.</p> </div> <p>The Download button will download the output in a text file and the clear button clears the output window.</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;">  <p><b>Note</b><br/>Advanced Debug option is available for cnPilot E-series devices with a minimum software version of 3.11.</p> </div> |
| <p>Packet Capture</p>               | <p>Lists packet capture details.</p>  |
| <p>Wi-Fi Performance (wifiperf)</p> | <p>Wi-Fi performance measures the backhaul speed across devices with respect to cnMaestro c4000 Controller.</p>   |

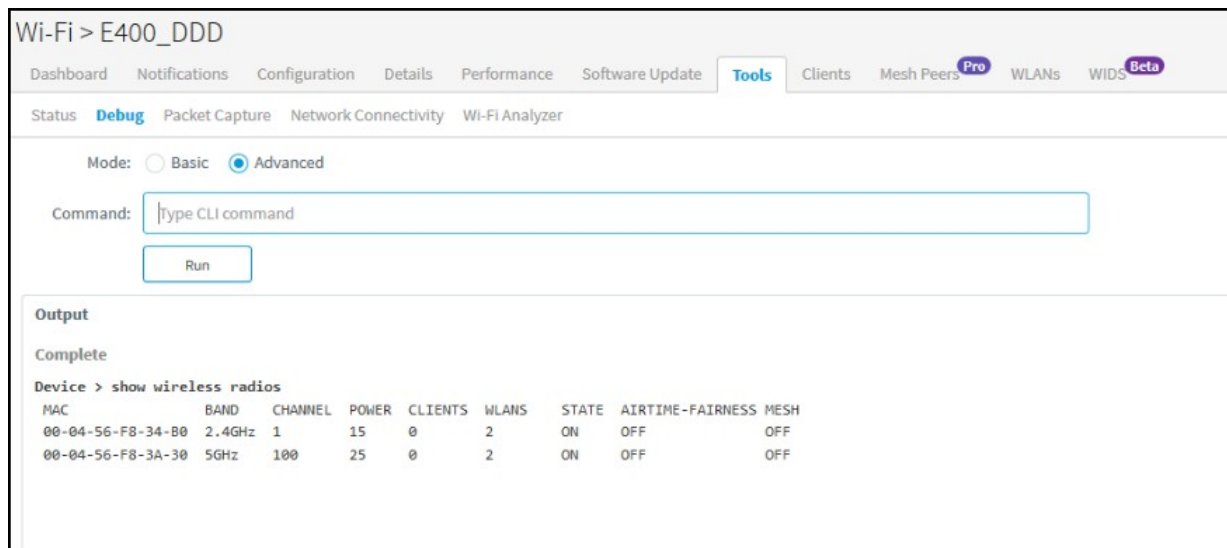


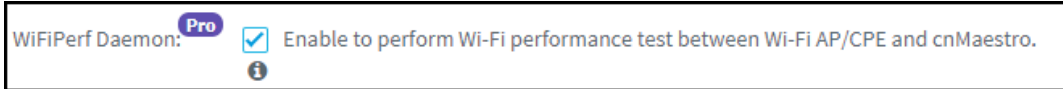
Figure 41 cnPilot Tools

### Wi-Fi Performance Test

Currently, the Wi-Fi Performance Test feature is supported only on cnPilot devices. Wi-Fi Performance Test will be triggered between the AP and Wi-FiPerf Endpoint.

Wi-FiPerf Endpoint can be either the cnMaestro c4000 Controller hardware or a locally installed speed test server.

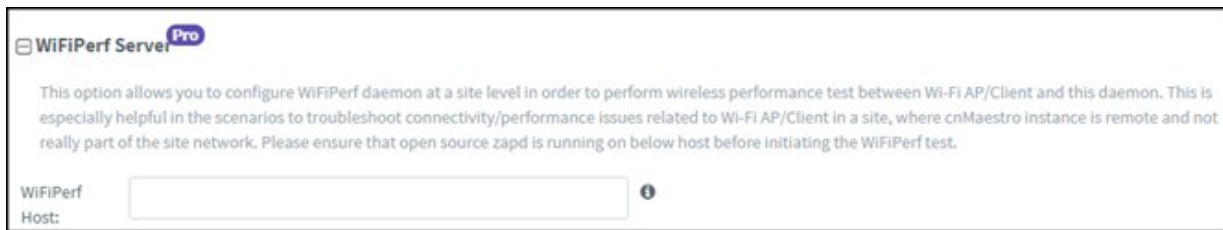
- cnMaestro c4000 Controller Hardware: To enable Wi-Fi Performance Test, navigate to **Appliance > Settings > Advanced Features** page and enable WiFiPerf Daemon option.



- Locally installed Wi-Fi Performance Server: Wifiperf performance interoperates with the open-source zap wireless tool.

(<https://code.google.com/archive/p/zapwireless/>). So install zap on the local host on the site. This is especially helpful in the scenarios to troubleshoot connectivity/performance issues related to Wi-Fi AP/Client in a site.

To configure locally installed Site level speed test server on cnMaestro c4000 Controller, navigate to **Site > Configuration > WiFiPerf Server**. page.



**Note**

The Wifiperf manager running on cnMaestro c4000 Controller establishes a control session with AP (and other endpoint-local hosts) using TCP port number 18301. So, it is mandatory that both the AP and the other endpoint is reachable from cnMaestro c4000 Controller. Make sure that the NAT/firewall does not block the wifiperf traffic from cnMaestro c4000 Controller to any endpoint or AP (also between the endpoints and AP). Ensure that the port number 18301 is not blocked in the network for TCP and UDP.



**Note**

For more details on the Wi-Fi performance (wifiperf) feature, please refer [here](#).



**Performing the Test:**

To run the Wi-Fi performance test, navigate to Tools > Wi-Fi Performance page.

It can be used to measure the following parameters with intervals of 10, 20 and 30 seconds:

**Traffic Types**

- UDP
- TCP

**Traffic Direction**

- Downlink
- Uplink

**WiFiPerf Endpoint**

- cnMaestro c4000 Controller
- WiFi Perf Local Host

**cnReach Tools**

The Tools page for cnReach devices consolidates a number of operations into a single troubleshooting interface. The operations are listed below.

**Table 20 cnReach Tools**

| Tools         | Description  |
|---------------|--|
| Ping          | Network ping to a hostname or IP address.  |
| RF Ping       | RF reachability test between local radios that provides details on signal quality. |
| RF Throughput | RF throughput test between local radios that provides details on throughput.       |

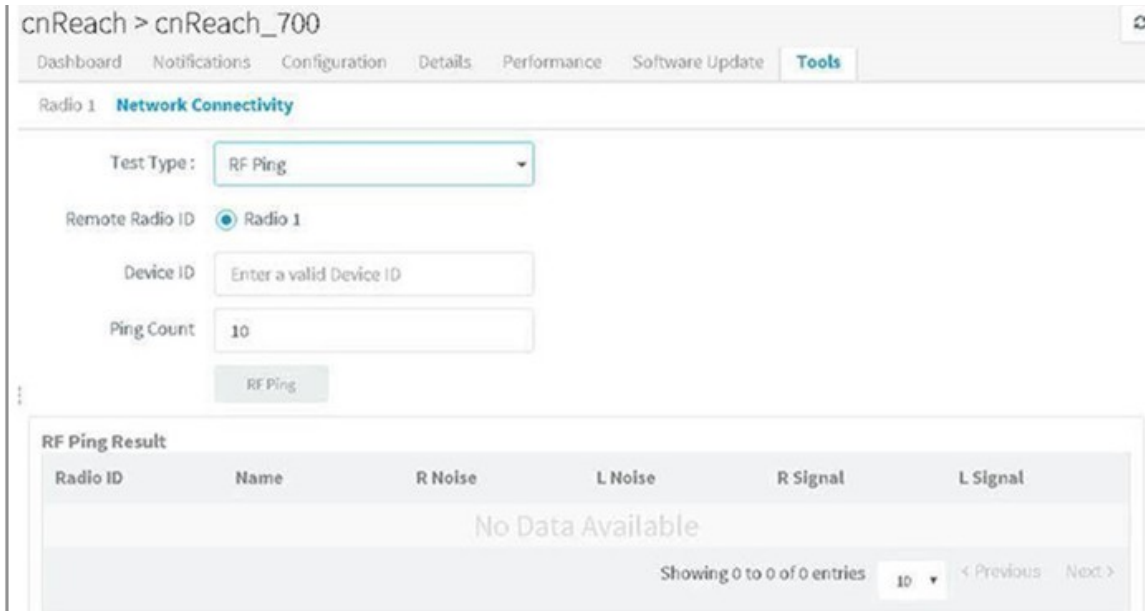


Figure 42 cnReach Tools

## PMP Tools

The Tools page for PMP devices consolidates a number of operations into a single troubleshooting interface. The operations are listed below.

Table 21 PMP Tools

| Tools                | Description  |
|----------------------|--|
| Status               | Displays the status.   |
| Debug                | Displays the log details.  |
| Network Connectivity | Executes Ping, DNS, or Traceroute tests.   |
| Subscriber Modules   | Lists all the SMs connected to the selected AP. This is available for PMP APs only.  |
| Link Test            | <p>The Link Capacity Test measures the throughput and efficiency of the RF link between two PMP modules. Many factors, including packet length, affect throughput. Packets are added to one or more queues in the AP in order to fill the frame. Throughput and efficiency are then calculated during the test</p> <p>The Link Capacity Test tool has the following modes:</p> <ul style="list-style-type: none"> <li>Link Test without Bridging: Tests radio-to-radio communication but do not bridge traffic.</li> </ul> |

| Tools   | Description   |   |   |   |   |
|---|---|---|---|---|---|
|   | <ul style="list-style-type: none"> <li>Link Test with Bridging: Bridges traffic to “simulated” Ethernet ports, providing a status of the bridged link.</li> <li>Link Test with Bridging and MIR: Bridges the traffic during the test and also adheres to any MIR (Maximum Information Rate) settings for the link.</li> <li>Extrapolated Link Test: Estimates the link capacity by sending a few packets and measuring link quality.</li> </ul> <p>Displays the link related test result with respect to Throughput and Interference. Link Tests can be performed on the PMP AP and its SM link. In order to run this operation, select the device and then the Tools tab.</p> <ul style="list-style-type: none"> <li>If a PMP AP is selected, you can choose the SM from the list and start the test.</li> </ul> <div data-bbox="380 667 1414 1104" style="border: 1px solid black; padding: 5px;"> <p>APs &gt; PMP450AP-KR</p> <p>Dashboard Notifications Configuration Details Performance Software Update Map <b>Tools</b></p> <p>Status Debug Network Connectivity Subscriber Modules <b>Link Test</b></p> <p>The Link Capacity Test measures the throughput and efficiency of the RF link between two PMP modules. Many factors, including packet length, affect throughput. <a href="#">Learn more</a></p> <p>Link Test Mode: <input type="text" value="Link Test with Bridging"/> ⓘ</p> <p>Current SM: <input type="text" value="PMP-SM_430"/></p> <p>Packet Length: <input type="text" value="1714"/> Bytes (64 – 1714 Bytes) ⓘ</p> <p>Result:</p> <table border="1" style="width: 100%; text-align: center;"> <tr> <td style="width: 50%; padding: 5px;"> <p><b>Downlink</b></p> <p><b>12.05 Mbps</b></p> <p>76% Efficient</p> <p>Signal to Noise Ratio: 0 dB V, 0 dB H</p> </td> <td style="width: 50%; padding: 5px;"> <p><b>Uplink</b></p> <p><b>4.90 Mbps</b></p> <p>100% Efficient</p> <p>Signal to Noise Ratio: 0 dB V, 0 dB H</p> </td> </tr> </table> </div> <ul style="list-style-type: none"> <li>If a PMP SM is selected, click Start Test to run the Link Test.</li> </ul> <div data-bbox="380 1178 1414 1570" style="border: 1px solid black; padding: 5px;"> <p>SMs &gt; PMP-SM_430</p> <p>Dashboard Notifications Configuration Details Performance Software Update Map <b>Tools</b></p> <p>Status Debug Network Connectivity <b>Link Test</b></p> <p>The Link Capacity Test tab allows to measure the throughput and efficiency of the RF link between two PMP modules. Many factors, including packet length, affect throughput. <a href="#">Learn more</a></p> <p>Link Test Mode: <input type="text" value="Link Test with Bridging"/> ⓘ</p> <p>Packet Length: <input type="text" value="1714"/> ⓘ Bytes (64 – 1714 Bytes) ⓘ</p> <p>Result:</p> <table border="1" style="width: 100%; text-align: center;"> <tr> <td style="width: 50%; padding: 5px;"> <p><b>Downlink</b></p> <p><b>15.21 Mbps</b></p> <p>96% Efficient</p> <p>Signal to Noise Ratio: 0 dB</p> </td> <td style="width: 50%; padding: 5px;"> <p><b>Uplink</b></p> <p><b>4.88 Mbps</b></p> <p>100% Efficient</p> <p>Signal to Noise Ratio: 0 dB</p> </td> </tr> </table> <p style="text-align: center;"><a href="#">Re-Test</a></p> </div> | <p><b>Downlink</b></p> <p><b>12.05 Mbps</b></p> <p>76% Efficient</p> <p>Signal to Noise Ratio: 0 dB V, 0 dB H</p> | <p><b>Uplink</b></p> <p><b>4.90 Mbps</b></p> <p>100% Efficient</p> <p>Signal to Noise Ratio: 0 dB V, 0 dB H</p> | <p><b>Downlink</b></p> <p><b>15.21 Mbps</b></p> <p>96% Efficient</p> <p>Signal to Noise Ratio: 0 dB</p> | <p><b>Uplink</b></p> <p><b>4.88 Mbps</b></p> <p>100% Efficient</p> <p>Signal to Noise Ratio: 0 dB</p> |
| <p><b>Downlink</b></p> <p><b>12.05 Mbps</b></p> <p>76% Efficient</p> <p>Signal to Noise Ratio: 0 dB V, 0 dB H</p> | <p><b>Uplink</b></p> <p><b>4.90 Mbps</b></p> <p>100% Efficient</p> <p>Signal to Noise Ratio: 0 dB V, 0 dB H</p>   |   |   |   |   |
| <p><b>Downlink</b></p> <p><b>15.21 Mbps</b></p> <p>96% Efficient</p> <p>Signal to Noise Ratio: 0 dB</p>           | <p><b>Uplink</b></p> <p><b>4.88 Mbps</b></p> <p>100% Efficient</p> <p>Signal to Noise Ratio: 0 dB</p>   |   |   |   |   |

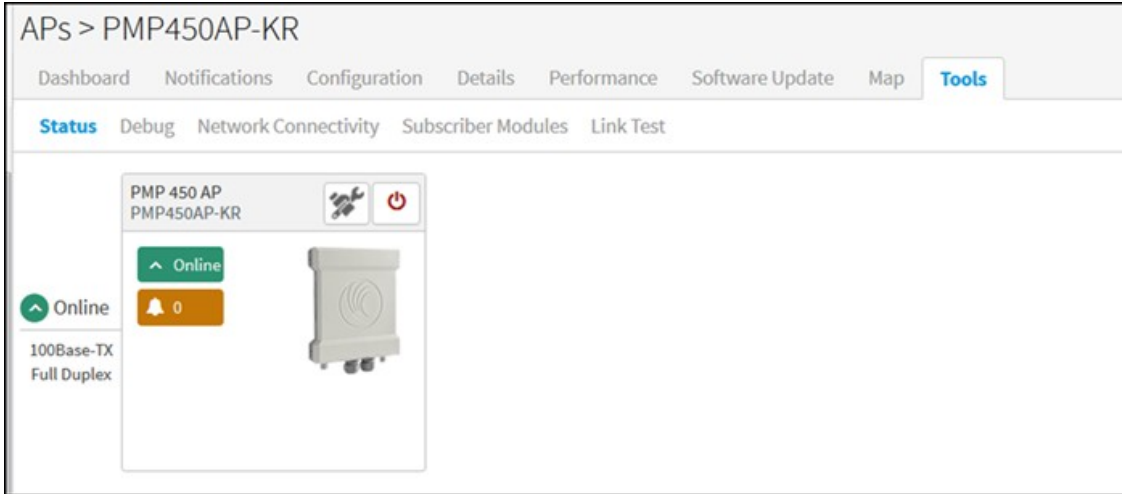


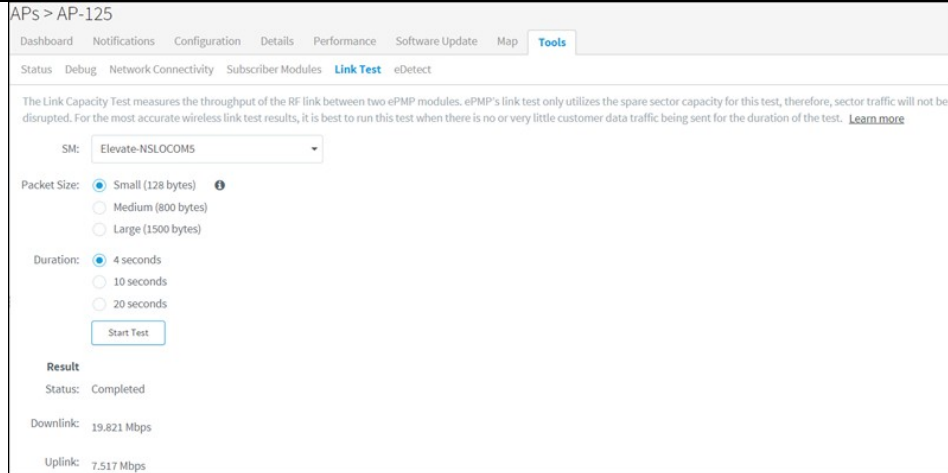
Figure 43 PMP Tools

## ePMP Tools

The Tools page for ePMP devices consolidates a number of operations into a single troubleshooting interface. The operations are listed below.

Table 22 ePMP Tools

| Tools                | Description   |
|----------------------|---|
| Status               | Displays the status.  |
| Debug                | Displays the log details.   |
| Network connectivity | Executes Ping, DNS, or Traceroute tests.  |
| Link Test            | <p>The Link Capacity Test measures the throughput of the RF link between two ePMP modules. ePMP’s link test only utilizes the spare sector capacity for this test, therefore, sector traffic will not be disrupted. For the most accurate wireless link test results, it is best to run this test when there is no or very little customer data traffic being sent for the duration of the test.</p> <p>Displays the link related test result with respect to Throughput. Link Tests can be performed on the ePMP AP and its SM link. In order to run this operation, select the device and then the Tools tab.</p> <ul style="list-style-type: none"> <li>• If an ePMP AP is selected you can choose the SM from the list and start the test.</li> </ul> |

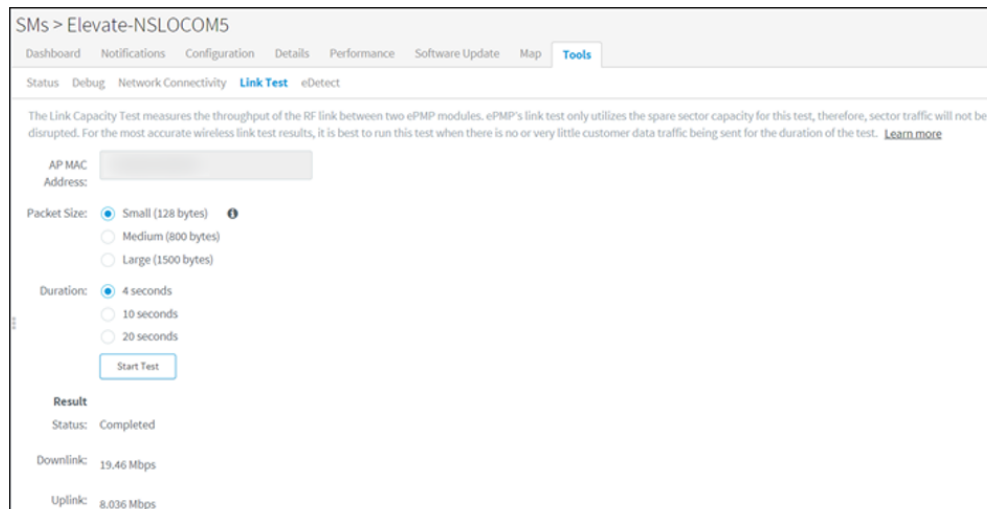


Displays the following fields:

**Packet Size:** Choose the Packet Size to use for the throughput test.

**Duration:** Choose the time duration in seconds to use for the throughput test.

- If an ePMP SM is selected, click Start Test to run the link test.



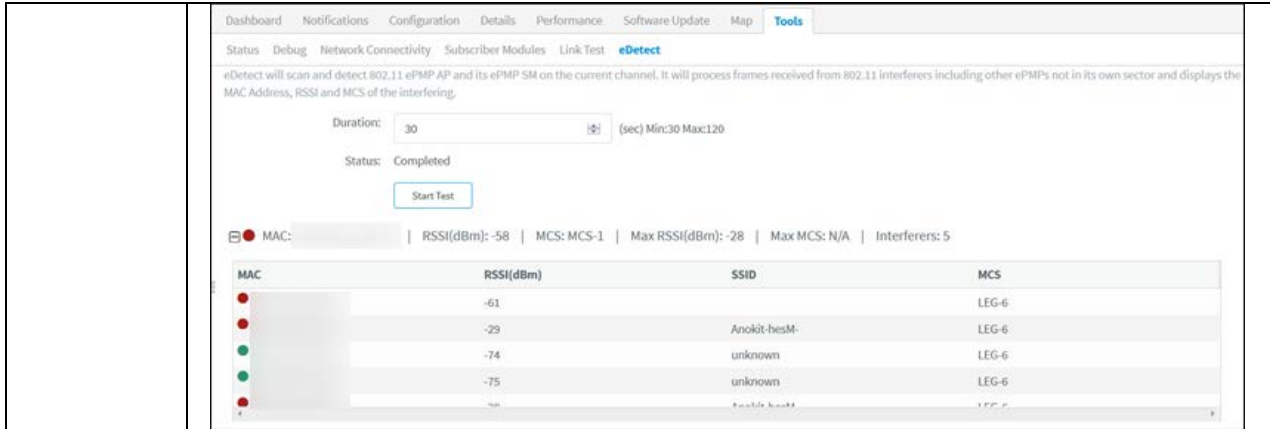
Displays the following fields:

**Packet Size:** Choose the Packet Size to use for the throughput test.

**Duration:** Choose the time duration in seconds to use for the throughput test.

**eDetect**

eDetect is supported on the ePMP AP or SM. It is also launched from the Tools tab. The eDetect tool (not available in ePMP Master/Slave mode) is used to measure the 802.11 interference at the ePMP radio or system when run from the AP or the SM, on the current operating channel. When the tool is run, the ePMP device processes all frames received from devices not connected to the ePMP system and collects the interfering frame's information such as MAC Address, RSSI, and MCS. Configure the duration for which the AP scans for interference.



Configure the duration for which the SM scans for interference.

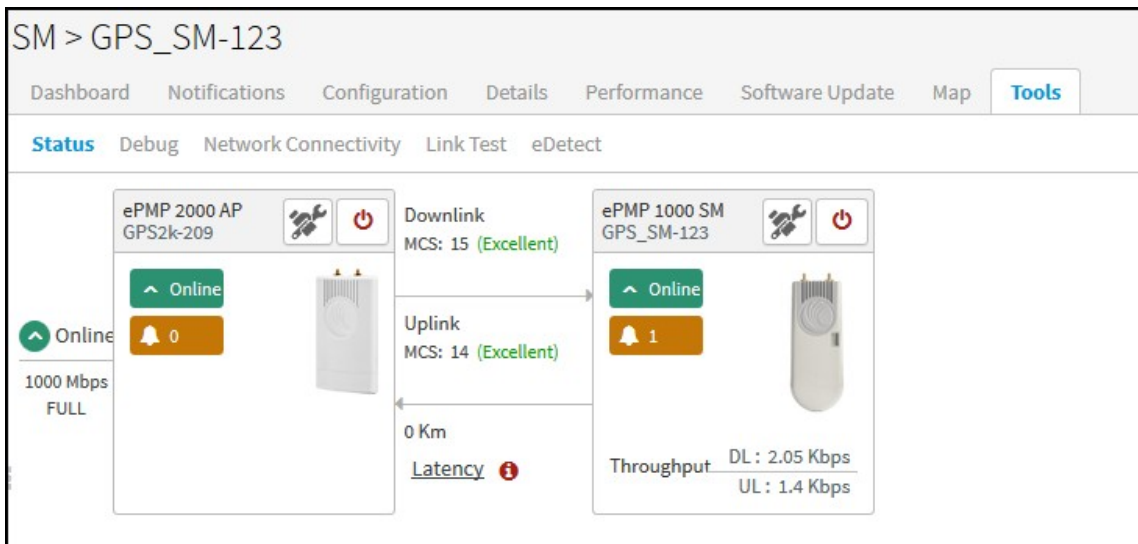
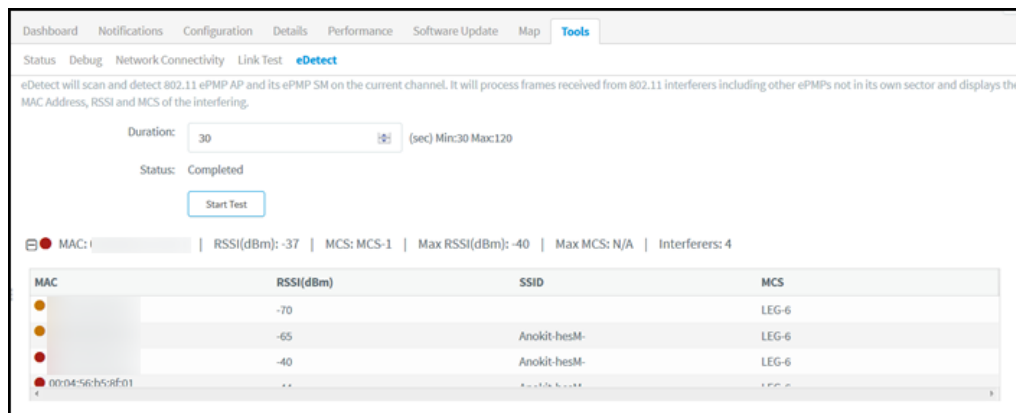


Figure 44 ePMP Tools

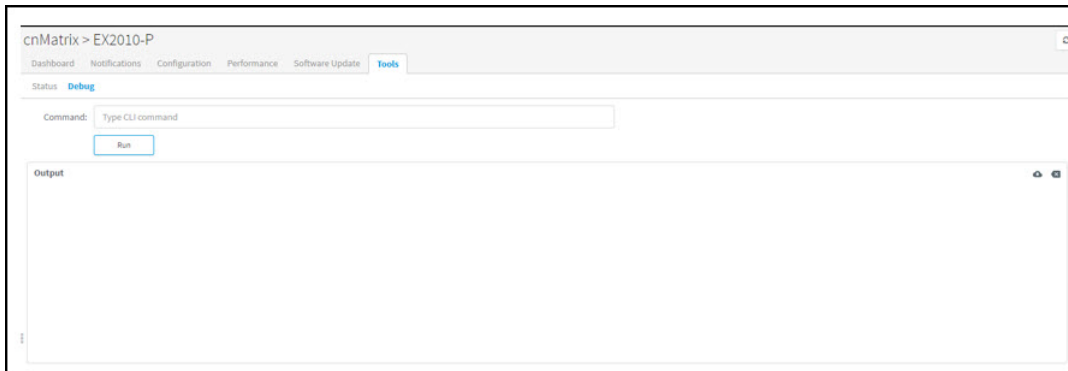
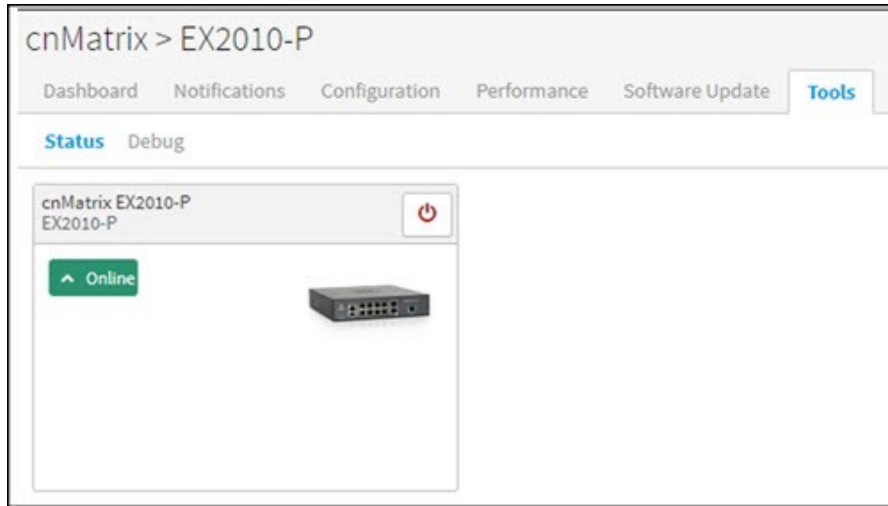
## cnMatrix Tools

In the Status tab, you can view the status of the device either Online or Offline and you can reboot the device.

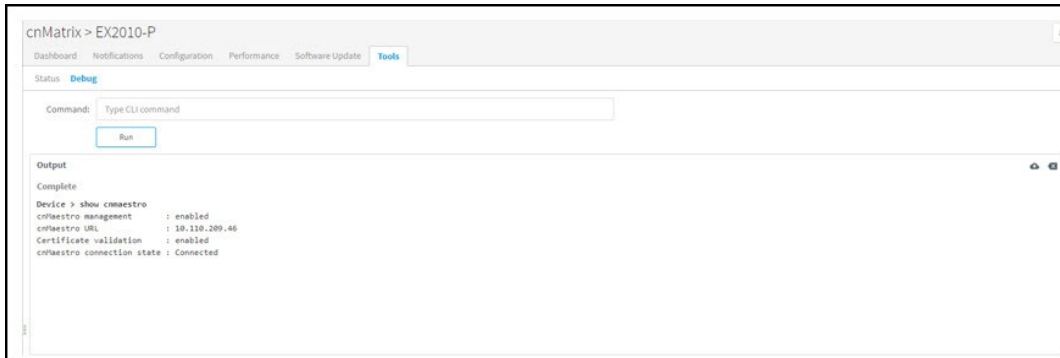




**Note**

Advanced Debug option supports cnMatrix software version 2.0.5-x and above.



In Tools > Debug, when you enter a command type and click Run, the following output is displayed:



- You can download the generated output by clicking the  icon.
- You can clear the generated output by clicking the  icon.

## WIDS

This section provides details on Rogue APs.

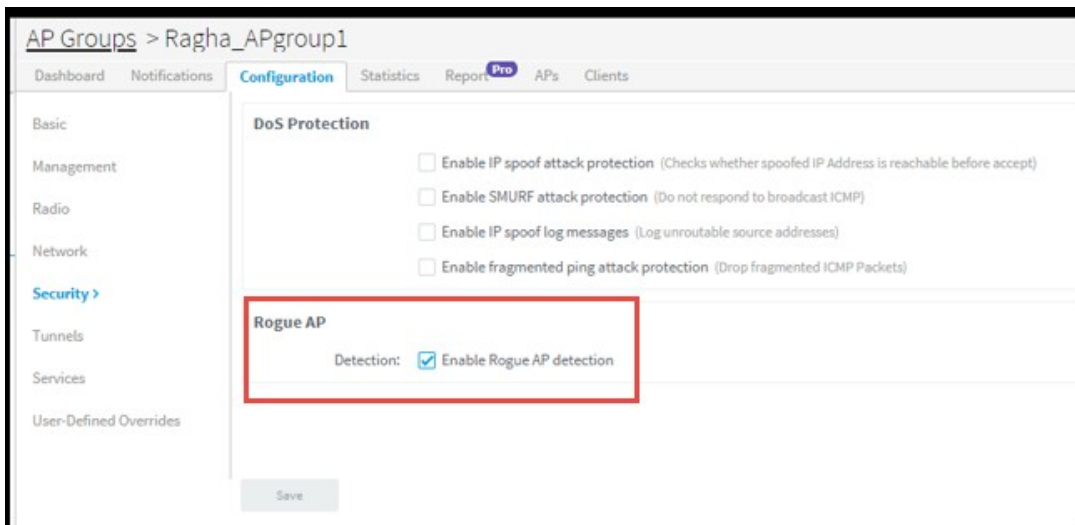
### Detecting Rogue APs

A rogue AP is an unsanctioned AP, which is not onboarded to cnMaestro c4000 Controller. The AP scans the channels, collects the details about the neighbor APs and sends them to cnMaestro c4000 Controller.

#### Configuring Rogue AP

To enable the Rogue AP feature:

1. Navigate to **AP Groups > Configuration > Security** page.
2. Select the Rogue AP Detection checkbox.



To enable OCS (Off Channel Scan):

1. Navigate to **AP Groups > Configuration > Radio** (Available on both radio 2.4Ghz and 5Ghz) page.
2. Select the **Enable OCS** checkbox under the OCS tab.



⊕ Automatic Channel Select

⊕ Enhanced Roaming

⊖ Off-Channel Scan

Enable:  Enable OCS

Dwell-time:  Configure Off-Channel Scan dwelltime in milliseconds (50-120)

Samples:  Configure Off-Channel Scan samples (1-5)

Interval:  Configure Off-Channel Scan scanning interval in seconds (6-300)

Number of Channels:  Configure number of channels scanned per Off-Channel-Scan (1-5)

Deprecated (Version 3.6)

Period:  Configure Off-Channel Scan (channel hold) period in minutes (5-1800)

You can grant valid APs to provide secure access to the network by adding them to the Whitelist by providing their MAC address and SSID.

To add Rogue APs to whitelist:

1. Navigate to **APs > WIDS** page.
2. Click **Add Whitelist** under Site Whitelist tab.
3. Enter MAC and SSID of the device to be whitelisted.
4. Click **Save**.

⊖ Site Whitelist

⚠ These values are shared across all APs at the Site.

Search  Add Whitelist Delete All

| SSID             | MAC               | Manufacturer             |   |
|------------------|-------------------|--------------------------|---|
| kreddum-2.4-156  | 00:04:56:04:27:A0 | Cambium Networks Limited | ✕ |
| cnPilot          | 00:04:56:04:27:B8 | Cambium Networks Limited | ✕ |
| wlan_RaghavTest3 | 00:04:56:93:F9:B3 | Cambium Networks Limited | ✕ |
| CambiumGuest     | 00:04:56:AF:1D:A0 | Cambium Networks Limited | ✕ |
| wlan4            | 58:C1:7A:60:08:32 | Cambium Networks Limited | ✕ |

Showing 1 - 5 Total: 5 10 < Previous Next >

The whitelisted Rogue AP WLAN will be grayed out in the Rogue AP list and it will be removed after 24 hours.

Rogue APs (Last 24 Hours)

Search Whitelist 0 devices

| SSID                        | MAC  | Channel | First Seen            | Last Seen             | Signal (dBm) | Manufacturer             |
|-----------------------------|--|---------|-----------------------|-----------------------|--------------|--------------------------|
| CambiumMobile               | 00:04:56:AF:1D:A1                                      | 6       | Thu Apr 11 2019 15:37 | Wed Apr 24 2019 11:03 | -36          | Cambium Networks Limited |
| CambiumGuest                | 00:04:56:AF:1D:A2<br><small>Added to whitelist</small> | 6       | Tue Apr 23 2019 14:38 | Wed Apr 24 2019 11:03 | -37          | Cambium Networks Limited |
| Cambium                     | 00:04:56:AF:1D:A0                                      | 6       | Thu Apr 11 2019 15:37 | Wed Apr 24 2019 11:03 | -38          | Cambium Networks Limited |
| 1 NAT Test                  | 58:C1:7A:C1:8F:B0                                      | 11      | Wed Apr 17 2019 15:26 | Wed Apr 24 2019 11:03 | -38          | Cambium Networks Limited |
| Auto_pilot_3                | 00:04:56:B1:84:82                                      | 1       | Mon Apr 22 2019 16:06 | Tue Apr 23 2019 11:21 | -39          | Cambium Networks Limited |
| Auto_pilot_1                | 00:04:56:9F:28:30                                      | 6       | Mon Apr 22 2019 16:06 | Tue Apr 23 2019 11:16 | -40          | Cambium Networks Limited |
| Auto_pilot_4                | 00:04:56:B1:84:83                                      | 1       | Mon Apr 22 2019 16:21 | Tue Apr 23 2019 11:21 | -40          | Cambium Networks Limited |
| EPSK-Test2                  | 00:04:56:9B:0B:20                                      | 6       | Thu Apr 11 2019 15:37 | Wed Apr 24 2019 11:03 | -40          | Cambium Networks Limited |
| BugVerification2.4GHz_2_4_1 | 5A:C1:7A:55:55:54                                      | 1       | Tue Apr 23 2019 17:08 | Tue Apr 23 2019 17:58 | -41          |                          |
| BugVerification2.4GHz_2_4_2 | 5A:C1:7A:65:55:54                                      | 1       | Tue Apr 23 2019 17:03 | Tue Apr 23 2019 17:58 | -41          |                          |

Showing 1 - 10 Total: 501 10 < Previous 1 2 3 4 5 ... 51 Next >

To whitelist multiple Rogue APs:

1. Select the **Rogue APs** in the list.
2. Click **Whitelist Devices**.

Rogue APs (Last 24 Hours)

Search Whitelist 2 devices

| SSID   | MAC  | Channel | First Seen            | Last Seen             | Signal (dBm) | Manufacturer             |
|--|--|---------|-----------------------|-----------------------|--------------|--------------------------|
| CambiumMobile                                    | 00:04:56:AF:1D:A1                                      | 6       | Thu Apr 11 2019 15:37 | Wed Apr 24 2019 11:03 | -36          | Cambium Networks Limited |
| CambiumGuest                                     | 00:04:56:AF:1D:A2<br><small>Added to whitelist</small> | 6       | Tue Apr 23 2019 14:38 | Wed Apr 24 2019 11:03 | -37          | Cambium Networks Limited |
| Cambium  | 00:04:56:AF:1D:A0                                      | 6       | Thu Apr 11 2019 15:37 | Wed Apr 24 2019 11:03 | -38          | Cambium Networks Limited |
| <input checked="" type="checkbox"/> 1 NAT Test   | 58:C1:7A:C1:8F:B0                                      | 11      | Wed Apr 17 2019 15:26 | Wed Apr 24 2019 11:03 | -38          | Cambium Networks Limited |
| <input checked="" type="checkbox"/> Auto_pilot_3 | 00:04:56:B1:84:82                                      | 1       | Mon Apr 22 2019 16:06 | Tue Apr 23 2019 11:21 | -39          | Cambium Networks Limited |
| Auto_pilot_1                                     | 00:04:56:9F:28:30                                      | 6       | Mon Apr 22 2019 16:06 | Tue Apr 23 2019 11:16 | -40          | Cambium Networks Limited |
| Auto_pilot_4                                     | 00:04:56:B1:84:83                                      | 1       | Mon Apr 22 2019 16:21 | Tue Apr 23 2019 11:21 | -40          | Cambium Networks Limited |
| EPSK-Test2                                       | 00:04:56:9B:0B:20                                      | 6       | Thu Apr 11 2019 15:37 | Wed Apr 24 2019 11:03 | -40          | Cambium Networks Limited |
| BugVerification2.4GHz_2_4_1                      | 5A:C1:7A:55:55:54                                      | 1       | Tue Apr 23 2019 17:08 | Tue Apr 23 2019 17:58 | -41          |                          |
| BugVerification2.4GHz_2_4_2                      | 5A:C1:7A:65:55:54                                      | 1       | Tue Apr 23 2019 17:03 | Tue Apr 23 2019 17:58 | -41          |                          |

Showing 1 - 10 Total: 501 10 < Previous 1 2 3 4 5 ... 51 Next >

The following popup will be displayed after successfully adding the Rogue APs to the whitelist.

Wi-Fi > E510-C18B5F

**Success**

Whitelist added Successfully. The device(s) will be removed from the Rogue APs list within 5 minutes.

Last Seen: Apr 23 11:04 AM ▶ Apr 24 11:04 AM

Rogue APs (Last 24 Hours)

Search Whitelist 0 devices

| SSID          | MAC  | Channel | First Seen            | Last Seen             | Signal (dBm) | Manufacturer             |
|---------------|--|---------|-----------------------|-----------------------|--------------|--------------------------|
| CambiumMobile | 00:04:56:AF:1D:A1                                      | 6       | Thu Apr 11 2019 15:37 | Wed Apr 24 2019 11:03 | -36          | Cambium Networks Limited |
| CambiumGuest  | 00:04:56:AF:1D:A2<br><small>Added to whitelist</small> | 6       | Tue Apr 23 2019 14:38 | Wed Apr 24 2019 11:03 | -37          | Cambium Networks Limited |
| Cambium       | 00:04:56:AF:1D:A0                                      | 6       | Thu Apr 11 2019 15:37 | Wed Apr 24 2019 11:03 | -38          | Cambium Networks Limited |
| 1 NAT Test    | 58:C1:7A:C1:8F:B0<br><small>Added to whitelist</small> | 11      | Wed Apr 17 2019 15:26 | Wed Apr 24 2019 11:03 | -38          | Cambium Networks Limited |
| Auto_pilot_3  | 00:04:56:B1:84:82<br><small>Added to whitelist</small> | 1       | Mon Apr 22 2019 16:06 | Tue Apr 23 2019 11:21 | -39          | Cambium Networks Limited |
| Auto_pilot_1  | 00:04:56:9F:28:30                                      | 6       | Mon Apr 22 2019 16:06 | Tue Apr 23 2019 11:16 | -40          | Cambium Networks Limited |
| Auto_pilot_4  | 00:04:56:B1:84:83                                      | 1       | Mon Apr 22 2019 16:21 | Tue Apr 23 2019 11:21 | -40          | Cambium Networks Limited |
| EPSK-Test2    | 00:04:56:9B:0B:20                                      | 6       | Thu Apr 11 2019 15:37 | Wed Apr 24 2019 11:03 | -40          | Cambium Networks Limited |

## View List of Rogue APs

You can view the list of Rogue APs at the device level in the Monitor page:

| SSID           | MAC | Channel | First Seen            | Last Seen             | Signal (dBm) | Manufacturer             |
|----------------|-----|---------|-----------------------|-----------------------|--------------|--------------------------|
| CambiumGuest   |     | 1       | Mon Apr 15 2019 07:01 | Tue Apr 16 2019 12:26 | -31          | Cambium Networks Limited |
| Ha test        |     | 11      | Thu Apr 04 2019 17:01 | Tue Apr 16 2019 12:26 | -33          | Cambium Networks Limited |
| Cambium        |     | 1       | Thu Apr 04 2019 17:01 | Tue Apr 16 2019 12:26 | -34          | Cambium Networks Limited |
| ASUS-2.4G      |     | 10      | Thu Apr 11 2019 15:51 | Tue Apr 16 2019 12:26 | -34          | ASUSTek Computer Inc.    |
| CambiumMobile  |     | 1       | Thu Apr 04 2019 17:01 | Tue Apr 16 2019 12:26 | -35          | Cambium Networks Limited |
| e410_dhcp      |     | 9       | Thu Apr 04 2019 17:01 | Tue Apr 16 2019 12:26 | -37          | Cambium Networks Limited |
| Dns acl test   |     | 1       | Fri Apr 12 2019 12:36 | Tue Apr 16 2019 12:26 | -39          | Cambium Networks Limited |
| 200_Test123_12 |     | 2       | Mon Apr 15 2019 16:56 | Tue Apr 16 2019 12:26 | -41          | Cambium Networks Limited |
| Jaggu*WLAN     |     | 11      | Mon Apr 15 2019 17:56 | Tue Apr 16 2019 12:26 | -47          | Cambium Networks Limited |
| WiFiChoupal    |     | 1       | Tue Apr 09 2019 19:16 | Tue Apr 16 2019 12:26 | -49          | Cambium Networks Limited |

The following parameters are displayed:

- **SSID:** SSID of the Rogue AP.
- **MAC:** MAC address of the Rogue AP.
- **Channel:** Channel in which the Rogue AP operates.
- **First Seen:** Time at which the Rogue AP is detected for the first time.
- **Last Seen:** Time at which the Rogue AP is detected last.
- **Signal:** Signal strength of the Rogue AP detected by the device.
- **Manufacturer:** Manufacturer of the Rogue AP (Cambium, Cisco, Aruba, etc) You can view the list of Rogue APs at the Site level in the Monitor page:

You can view the list of Rogue APs at the Site level in the Monitor page:

Sites > site2

Rogue APs (Last 24 Hours)

| SSID                | MAC               | Channel | First Seen            | Last Seen             | Strongest RSSI              | Detecting APs | Manufacturer             |
|---------------------|-------------------|---------|-----------------------|-----------------------|-----------------------------|---------------|--------------------------|
| WiFiChoupal         | 00:04:56:91:5C:F2 | 36      | Thu Apr 11 2019 15:42 | Mon Apr 22 2019 15:31 | 58:C1:7A:C1:8B:5F (-37 dBm) | 1             | Cambium Networks Limited |
|                     | 00:04:56:91:5C:F0 | 36      | Thu Apr 11 2019 15:42 | Mon Apr 22 2019 15:31 | 58:C1:7A:C1:8B:5F (-37 dBm) | 1             | Cambium Networks Limited |
|                     | 00:04:56:91:5C:F1 | 36      | Thu Apr 11 2019 15:42 | Mon Apr 22 2019 15:31 | 58:C1:7A:C1:8B:5F (-38 dBm) | 1             | Cambium Networks Limited |
| E400-220R33HA       | 00:04:56:B0:FF:90 | 157     | Thu Apr 11 2019 15:42 | Mon Apr 22 2019 15:31 | 58:C1:7A:C1:8B:5F (-39 dBm) | 1             | Cambium Networks Limited |
| Auto_pilot_3        | 00:04:56:B1:84:82 | 1       | Mon Apr 22 2019 16:06 | Tue Apr 23 2019 11:21 | 58:C1:7A:C1:8B:5F (-39 dBm) | 1             | Cambium Networks Limited |
| CAMBIUM_2.4GHz_1... | 00:04:56:12:D4:20 | 6       | Mon Apr 15 2019 12:27 | Mon Apr 22 2019 16:16 | 58:C1:7A:C1:8B:5F (-40 dBm) | 1             | Cambium Networks Limited |
| Auto_pilot_1        | 00:04:56:9F:28:30 | 6       | Mon Apr 22 2019 16:06 | Tue Apr 23 2019 11:16 | 58:C1:7A:C1:8B:5F (-40 dBm) | 1             | Cambium Networks Limited |
| Auto_pilot_4        | 00:04:56:B1:84:83 | 1       | Mon Apr 22 2019 16:21 | Tue Apr 23 2019 11:21 | 58:C1:7A:C1:8B:5F (-40 dBm) | 1             | Cambium Networks Limited |
| CAMBIUM_2.4GHz_1... | BC:E6:7C:00:AC:80 | 11      | Mon Apr 22 2019 16:26 | Mon Apr 22 2019 16:31 | 58:C1:7A:C1:8B:5F (-41 dBm) | 1             | Cambium Networks Limited |
| Ha test             | 58:C1:7A:0C:3C:70 | 149     | Thu Apr 11 2019 15:42 | Mon Apr 22 2019 15:31 | 58:C1:7A:C1:8B:5F (-43 dBm) | 1             | Cambium Networks Limited |

Showing 1 - 10 Total: 691

The following parameters are displayed:

- **SSID:** SSID of the Rogue AP.
- **MAC:** MAC address of the Rogue AP.
- **Channel:** Channel in which the Rogue AP operates.
- **First Seen:** Time at which the Rogue AP is detected for the first time.
- **Last Seen:** Time at which the Rogue AP is detected last.
- **Strongest RSSI:** Rogue AP RSSI which is detected strongest RSSI by AP.
- **Detecting AP:** Number of Aps detecting the same Rogue AP.
- **Manufacturer:** Manufacturer of the Rogue AP (Cambium, Cisco, Aruba, etc).

You can search for a specific Rogue AP based on the MAC, SSID, Channel, and the Manufacturer by using the search option.

Wi-Fi > E510-C18B5F

| SSID         | MAC               | Manufacturer             |
|--------------|-------------------|--------------------------|
| Auto_pilot_3 | 00:04:56:81:84:82 | Cambium Networks Limited |
| Auto_pilot_3 | 00:04:56:9F:28:32 | Cambium Networks Limited |
| Auto_pilot_3 | 00:04:56:86:3E:72 | Cambium Networks Limited |

Showing 1 - 3 Total: 3

Site Whitelist

| SSID           | MAC               | Manufacturer             |
|----------------|-------------------|--------------------------|
| 2.4GHz_027CA0  | 00:04:56:02:7C:A0 | Cambium Networks Limited |
| -A-151         | 00:04:56:04:26:D6 | Cambium Networks Limited |
| Cambiumouest   | 00:04:56:AF:1D:A2 | Cambium Networks Limited |
| onPilot-rajesh | 00:04:56:B1:53:80 | Cambium Networks Limited |



**Note**

- OCS (on both 2.4 GHz and 5 GHz) and Rogue AP detection should be enabled for the WIDS option to work at the site and device level in cnMaestro c4000 Controller.
- It will take 5 minutes to detect Rogue AP on AP boot up.

## Chapter 7: cnPilot Dashboards

You should make sure your Cambium devices support the minimum versions in order to access the features described below.



### Note

A number of graphs and metrics are only supported by cnPilot Enterprise devices.

| Family  | Model  | Version   |
|---------|--|---|
| cnPilot | cnPilot E400, cnPilot E410, cnPilot E501S, cnPilot E500, cnPilot e 502S, cnPilot e600, cnPilot e 430W/H, cnPilot e700, cnPilot e425H | 3.2.1-r6 (E400/E500/E501S/e502S)<br>3.5.2-r4 (E410/e430w/e600)<br>3.7-r9 (e700)<br>4.0-r2 (e425H) |
|         | cnPilot R200, cnPilot R201   | 4.4.2-R2  |
|         | cnPilot R190   | 4.4.2-R2  |
|         | cnPilot r195W  | 4.6-Rx  |

## Device dashboard

The Device dashboard page displays details of all the Wi-Fi devices in cnMaestro c4000 Controller. It mainly focuses on the following parameters:

- [Overview](#)
- [Clients](#)
- [Network Info](#)
- [Mesh Peers](#)
- [Neighbors](#)

### Overview

The Overview section displays the radio details, clients, throughput, channels, recent alarms, clients by SNR, clients by performance, clients by Radio, top clients, and top WLANs.

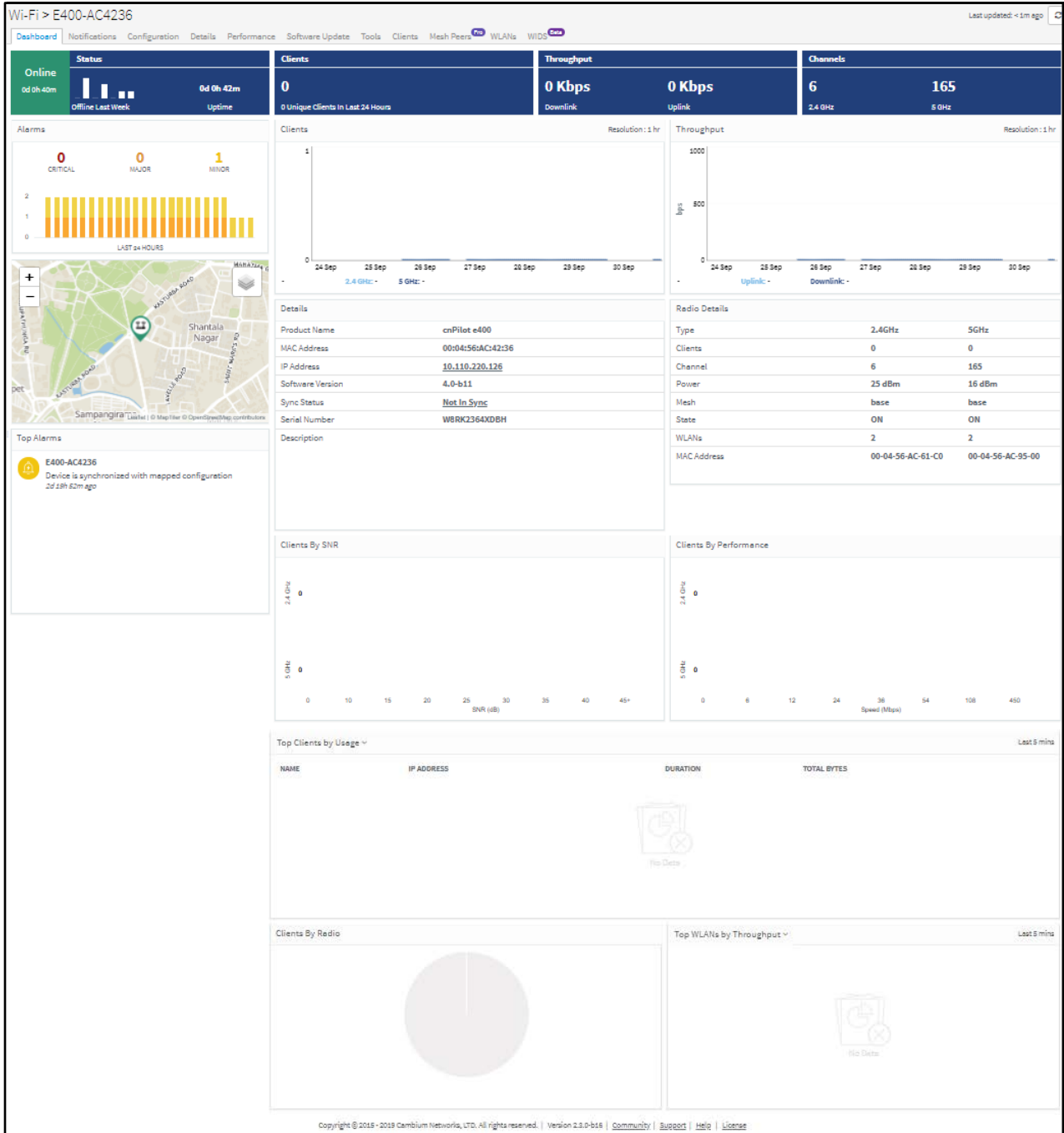


Figure 45 Dashboard > Overview Page

## Clients

The Clients section displays the details of all the wireless and wired clients. Following parameters are displayed for wired clients for R-Series:

- Name
- IP Address
- MAC
- Address Type
- Expires
- Interface
- Status

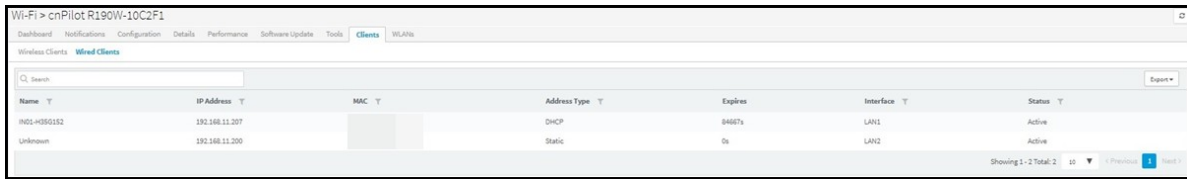


Figure 46 R-Series: Device Dashboard > Wired Clients Page

Following parameters are displayed for wireless clients for R-Series:

- Host Name
- IP Address
- MAC
- Manufacturer
- WLAN
- Band
- RSSI
- Upload
- Download

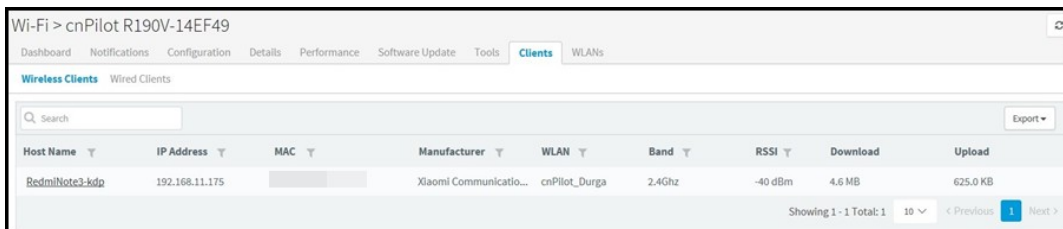


Figure 47 R-Series: Device Dashboard > Wireless Clients Page

Following parameters are displayed for wireless clients for E-Series:



- Host Name
- User
- IP Address
- MAC
- OS
- Manufacturer
- WLAN
- Band
- Mode
- SNR
- RSSI
- VLAN
- Client Type
- Type
- GA Mode
- Authentication
- Session Expiry
- Guest Access Type
- Upload
- Download
- Upload Quota
- Download Quota
- Upload Quota Balance
- Download Quota Balance
- Managed Account
- Actions

| Host Na...   | User | IP Address   | MAC               | OS    | Manufacturer       | WLAN      | Band   | Mode | SNR   | RSSI    | VLAN | Client Type    | Type | GA Mode | Authentication | Session Expiry |
|--------------|------|--------------|-------------------|-------|--------------------|-----------|--------|------|-------|---------|------|----------------|------|---------|----------------|----------------|
| android-c27- |      | 10.110.202.2 | DO:F8:9C:2A:4E:8C | Other | Motorola (Wuhan... | E700_WLAN | 2.4GHz | bgn  | 35 dB | -60 dBm | 1    | Regular Client |      | false   |                | 0d 0h 0m       |

Figure 48 E-Series: Device Dashboard > Wireless Clients Page

Following parameters are displayed for wired clients for E-Series:

- Host Name

- IP Address
- MAC
- OS
- Manufacturer
- VLAN-ID
- Client Type
- Authentication-Type
- Portal Mode
- Auth Status
- Guest Access Type
- Age
- Upload
- Download
- Total Quota
- Total Quota Balance
- Upload Quota
- Download Quota
- Upload Quota Balance
- Download Quota Balance

| Host Name      | IP Address    | MAC               | OS         | Manufacturer       | VLAN-ID | Client Type  | Authentication Type | Portal Mode | Auth Status | Guest Access Type | Age    | Upload | Download |
|----------------|---------------|-------------------|------------|--------------------|---------|--------------|---------------------|-------------|-------------|-------------------|--------|--------|----------|
| cnPilot R190W  | 172.10.99.106 | 00:04:36:11:20:99 | Other      | Cambium Netwo...   | 99      | Guest Client | RADIUS              | External    | True        | XWF               | 1556 s | 30413  | 14743    |
| IN03-FR7TJ2    | 172.10.99.128 | D4:8A:8A:E7:D0:15 | Windows 10 | Hon Hai Preciso... | 99      | Guest Client | RADIUS              | External    | True        | XWF               | 29 s   | 151275 | 82338    |
| android-467b20 | 172.10.99.202 | 64:DB:43:E1:08:BA | Android    | Motorola (Wuhan... | 99      | Guest Client | RADIUS              | External    | True        | XWF               | 2122 s | 59282  | 131277   |

Figure 49 E-Series: Device Dashboard > Wired Clients Page

## Network Info

The Network Info section displays the details of the Network: Following parameters are displayed for R-Series:

- Ethernet Ports
  - Type
  - TX Bytes
  - RX Bytes
  - TX Packets

- RX Packets
- TX Error Bytes
- RX Error Bytes
- FXS Ports
  - Type
  - SIP Account Status
  - Phone Number
  - Hook State

The screenshot shows the 'Network Info' page for a device. It contains two tables: 'Ethernet Ports' and 'FXS Ports'.

| Ethernet Ports |           |           |            |            |                |                |
|----------------|-----------|-----------|------------|------------|----------------|----------------|
| Type           | TX Bytes  | RX Bytes  | TX Packets | RX Packets | TX Error Bytes | RX Error Bytes |
| WAN            | 4969884   | 7838058   | -          | -          | -              | -              |
| LAN 1          | 424461014 | 258843480 | 363490     | 307952     | 0              | 0              |
| LAN 2          | 269201985 | 423097046 | 315389     | 367799     | 0              | 0              |
| LAN 3          | 13911078  | 418605347 | 145313     | 282634     | 0              | 0              |
| LAN 4          | 418021663 | 9928114   | 277924     | 140333     | 0              | 0              |

| FXS Ports |                    |              |            |
|-----------|--------------------|--------------|------------|
| Type      | SIP Account Status | Phone Number | Hook State |
| FXS 1     | Disable            | -            | On         |
| FXS 2     | Disable            | -            | On         |

Figure 50 R-Series: Device Dashboard > Network Info Page

Following parameter details are displayed in E-Series:

- VLAN
- Routes
- Ethernet Ports
- Tunnels
- PPPoE

Dashboard : E400-B67324 Critical Alarms 0 | Major Alarms 0

Overview Clients VLANs **Network Info** Mesh Peers Neighbors

| VLAN           |                |        |          |          |          |          |
|----------------|----------------|--------|----------|----------|----------|----------|
| Interface Name | IP Address     | Source | Tx Bytes | Rx Bytes | Tx Drops | Rx Drops |
| ETH1           | 0.0.0.0        |        | 459034   | 585845   | 0        | 12       |
| VLAN1          | 10.110.211.105 |        | 456756   | 525617   | 0        | 0        |

| Routes       |               |                |       |        |           |  |
|--------------|---------------|----------------|-------|--------|-----------|--|
| Destination  | Mask          | Gateway        | Flags | Metric | Interface |  |
| 0.0.0.0      | 0.0.0.0       | 10.110.211.254 | UG    | 0      | VLAN1     |  |
| 10.110.211.0 | 255.255.255.0 | 0.0.0.0        | U     | 0      | VLAN1     |  |
| 169.254.0.0  | 255.255.0.0   | 0.0.0.0        | U     | 0      | VLAN1     |  |

| Ethernet Ports |        |             |             |            |              |            |
|----------------|--------|-------------|-------------|------------|--------------|------------|
| Type           | Mode   | Access VLAN | Native VLAN | Native Tag | Allowed VLAN | Port Speed |
| ETH1           | access | 1           | 1           | false      |              | 1000M      |
| ETH2           | access | 1           | 1           | false      |              |            |

| Tunnels |        |             |  |
|---------|--------|-------------|--|
| Type    | Status | Remote Host |  |
| I2tp    | Down   | 0.0.0.0     |  |
| I2gre   | Down   | 0.0.0.0     |  |

| PPPoE |      |              |            |
|-------|------|--------------|------------|
| Type  | VLAN | Status       | IP Address |
| PPPOE | NA   | Disconnected | 0.0.0.0    |

Figure 51 E-Series: Device Dashboard > Network Info Page

Following parameter details are displayed in E-Series:

- Port
- Tx Octets
- Rx Octets
- Tx Frames
- Rx Frames
- Rx Frames with Error
- Tx Broadcasts
- Rx Broadcasts
- Rx Frames Undersize
- Rx Frames Oversize

| Ethernet Ports |           |           |           |           |                      |               |               |                     |                    |
|----------------|-----------|-----------|-----------|-----------|----------------------|---------------|---------------|---------------------|--------------------|
| Port           | Tx Octets | Rx Octets | Tx Frames | Rx Frames | Rx Frames With Error | Tx Broadcasts | Rx Broadcasts | Rx Frames Undersize | Rx Frames Oversize |
| Main PSU       | 958727    | 1901406   | 8404      | 10474     | 0                    | 20            | 676           | 0                   | 0                  |
| AUX            | 0         | 0         | 0         | 0         | 0                    | 0             | 0             | 0                   | 0                  |
| SFP            | 0         | 0         | 0         | 0         | 0                    | 0             | 0             | 0                   | 0                  |

Showing 1 - 3 Total: 3    10    < Previous    3    Next >

Figure 52 PTP: Device Dashboard > Network Info Page

## Mesh Peers

The Mesh Peers tab displays information related to Mesh Clients and respective RF parameters such as SNR, RSSI, and Band. This tab helps the user to trigger Wi-Fi Performance between the Mesh Client and Mesh Base.

| Mesh Base | Mesh Client | End Hosts | Host Name | IP Address     | Band   | SNR | RSSI | Actions |
|-----------|-------------|-----------|-----------|----------------|--------|-----|------|---------|
|           |             |           |           | 10.110.211.102 | 2.4GHz | 49  | -53  |         |

Figure 53 Device Dashboard > Mesh Peers Page

You can also perform the Wi-Fi performance test by clicking the icon below the Action field.

## Neighbors

Displays the BSSID, SSID, Channel, RSSI details of neighboring 2.4 GHz and 5 GHz Radios.

| BSSID | SSID                   | Channel | SNR |
|-------|------------------------|---------|-----|
|       | cnPilot123             | 144     | 45  |
|       | Defaultvgffewfejhhfgbd | 144     | 56  |
|       | Savone-Wireless        | 140     | 53  |

Figure 54 Device Dashboard > Neighbors Page

## Site Dashboard

The Site dashboard page provides an overview of site-related parameters and devices as shown below:

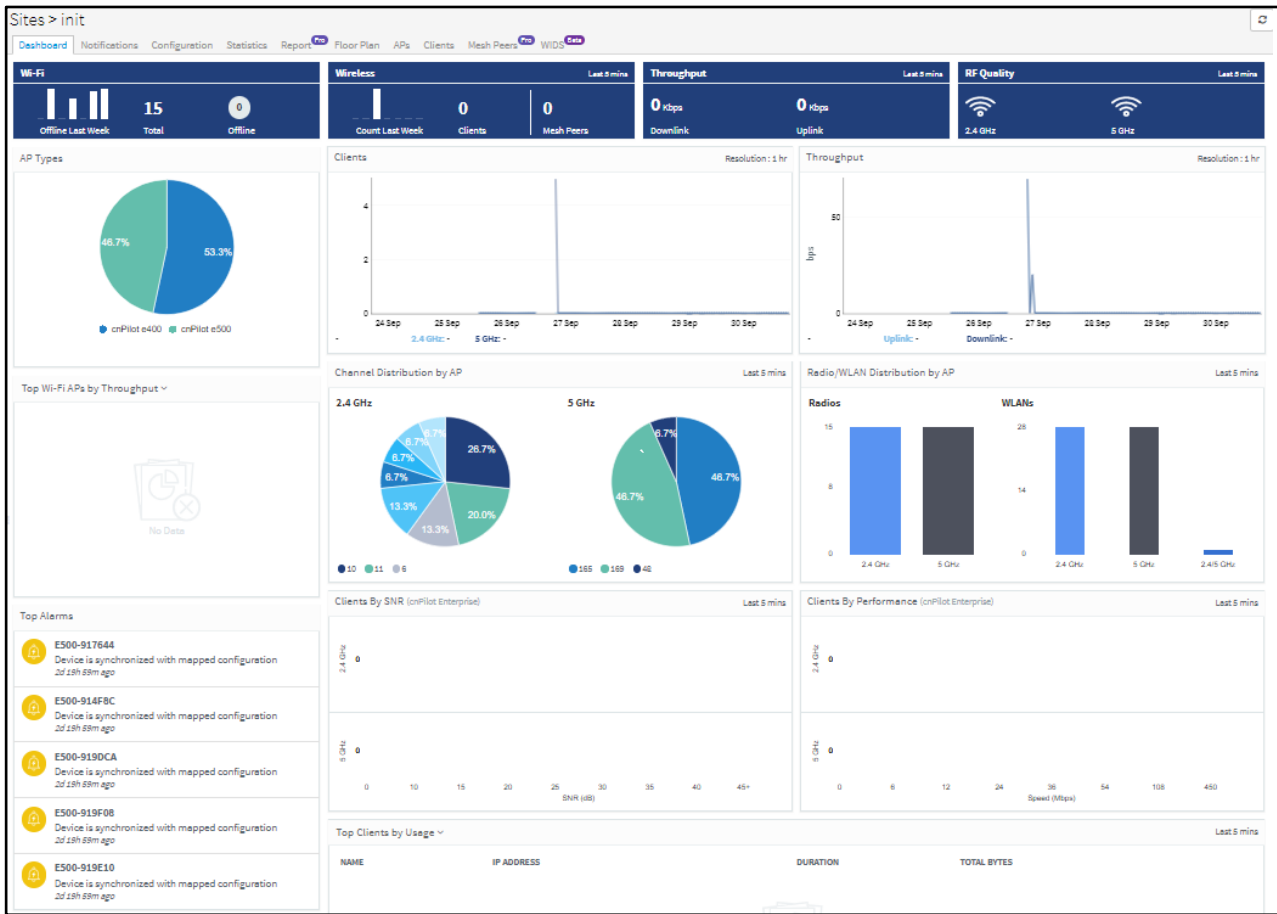


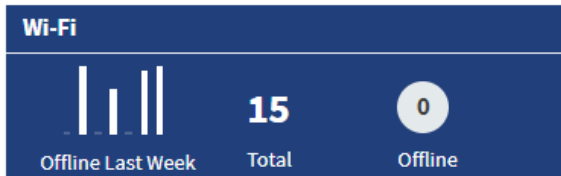
Figure 55 Site Dashboard

The Site Dashboard focuses on the following parameters:

- Wi-Fi Devices Availability (Total and Offline)
- Throughput
- RF Quality
- AP Types
- Top APs
- Channel Distribution by APs
- Radio/WLAN Distribution by APs
- Clients by SNR
- Clients by Performance
- Wireless Clients Graph
- Throughput Graph
- Wi-Fi Access Points
- Wireless Clients
- Floor Plan

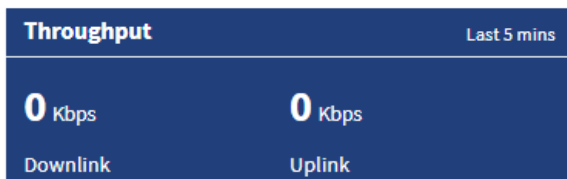
## Wi-Fi Devices Availability (Total and Offline)

Displays the total number of access points in the Site and the devices that are offline.

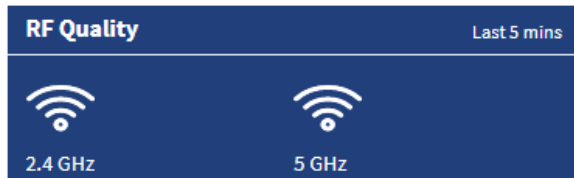


## Throughput

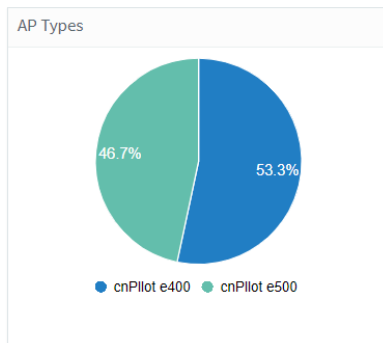
Displays aggregated throughput for all the clients.



## RF Quality



## AP Types

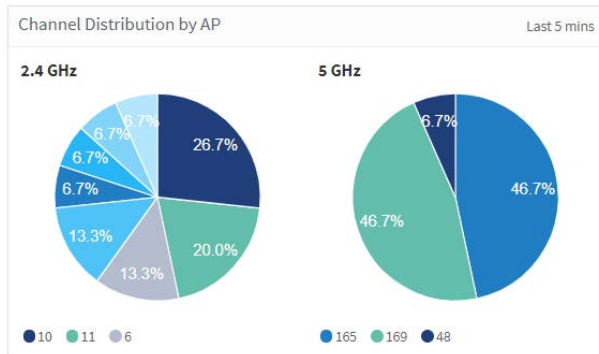


## Top Aps

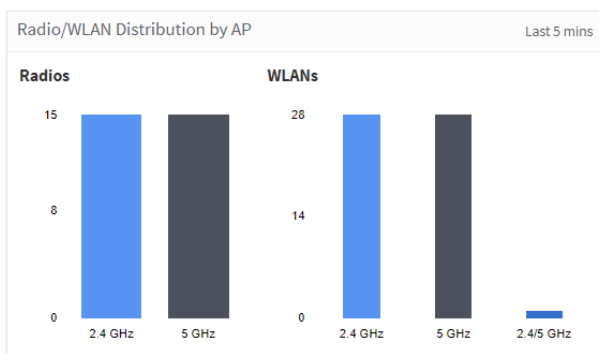
| Top Wi-Fi APs by Throughput ▾     |                                 |
|-----------------------------------|---------------------------------|
| <b>NAME</b><br><u>E500-B83D86</u> | <b>MAC</b><br>00:04:56:B8:3D:86 |
| <b>THROUGHPUT</b><br>13.45 Kbps   | <b>WIRELESS CLIENTS</b><br>0    |
| <b>NAME</b><br><u>E510-C18BA8</u> | <b>MAC</b><br>58:C1:7A:C1:8B:A8 |
| <b>THROUGHPUT</b><br>2.9 Kbps     | <b>WIRELESS CLIENTS</b><br>1    |

## Channel Distribution by APs

Channel distribution displays the usage of channels in 2.4 and 5 GHz. This helps users in planning and implementing WLANs within a high-density environment.

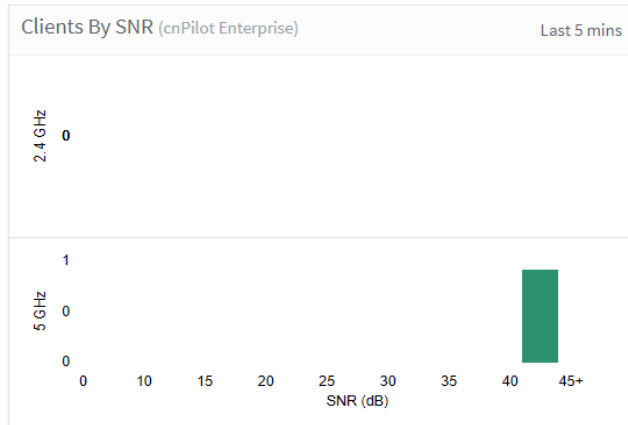


## Radio/WLAN Distribution by Aps

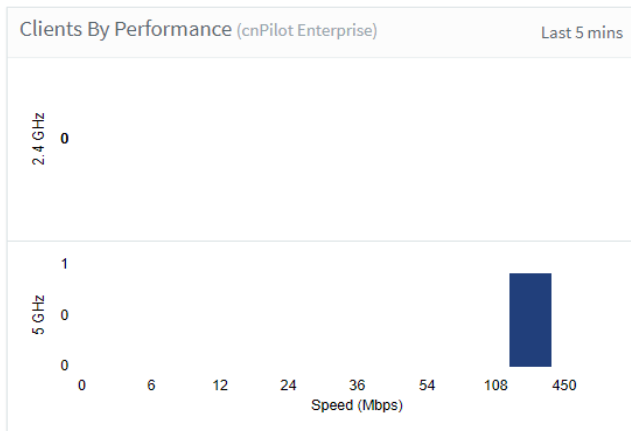




## Clients by SNR

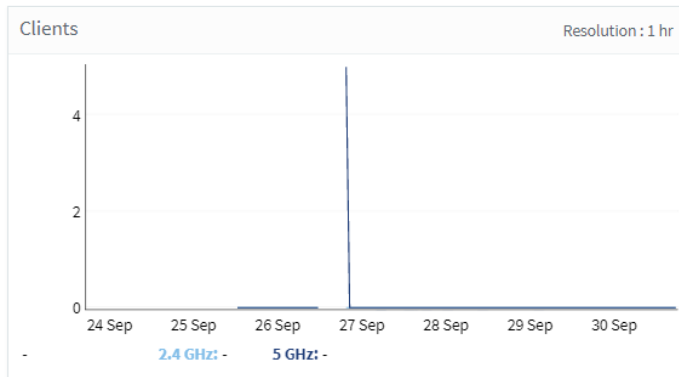


## Clients by Performance



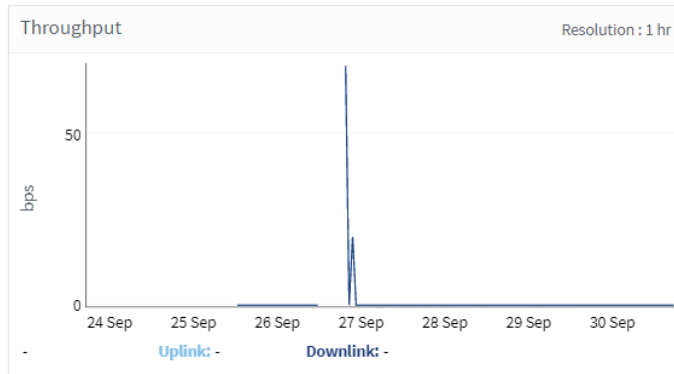
## Wireless Clients Graph

Wireless clients graph displays clients that are connected in 2.4 and 5 GHz for the last week.



## Throughput Graph

Throughput graph displays client traffic for the last week.



## Wi-Fi Access Points

Wi-Fi Access points will focus on parameters like device type, Band, Channel, Tx Power, Connected Clients, and Throughput (uplink and downlink). User has the option to export Wi-Fi access point data to PDF or CSV.

| Name          | Type          | Band           | Channel   | Power            | Clients | Uplink Throughput | Downlink Throughput |
|---------------|---------------|----------------|-----------|------------------|---------|-------------------|---------------------|
| cnPilot ES300 | cnPilot ES300 | 2.4GHz<br>5GHz | 6<br>36   | 10 dBm<br>10 dBm | 0       | -                 | -                   |
| cnPilot E400  | cnPilot E400  | 2.4GHz<br>5GHz | 11<br>149 | 11 dBm<br>13 dBm | 0       | -                 | -                   |
| cnPilot ES300 | cnPilot ES300 | 2.4GHz<br>5GHz | 6<br>147  | 10 dBm<br>10 dBm | 0       | -                 | -                   |

## Wireless Clients

Wireless Clients focus on parameters like Client name, IP Address, Client MAC, Manufacturer, Client WLAN, and Client AP. The table can be exported as PDF or CSV.

| Name | WLAN | Band   | IP Address    | MAC | User | Manufacturer         | SNR   | RSSI    | Download | Upload   | AP                |
|------|------|--------|---------------|-----|------|----------------------|-------|---------|----------|----------|-------------------|
|      |      | 5GHz   | 10.110.208.13 |     |      | Intel Corporation    | 31 dB | -64 dBm | 789.3 KB | 467.7 KB | 208.101.donttouch |
|      |      | 5GHz   | 10.110.208.4  |     |      | Intel Corporation    | 36 dB | -59 dBm | 101.0 MB | 27.9 MB  | 208.101.donttouch |
|      |      | 5GHz   | 10.110.208.18 |     |      | Motorola (Wuhan...   | 39 dB | -66 dBm | 10.3 KB  | 132.8 KB | 208.101.donttouch |
|      |      | 2.4GHz | 10.110.208.12 |     |      | LG Electronics (M... | 26 dB | -72 dBm | 485.0 KB | 130.6 KB | 208.101.donttouch |
|      |      | 5GHz   | 10.110.208.3  |     |      | Apple                | 21 dB | -74 dBm | 3.0 KB   | 3.2 KB   | 208.101.donttouch |

## Floor Plan

Floor Plan is used to locate all APs on the Map (and present device status, connected clients, and Tx power). This is done by uploading the map in Site > Floor Plan > Edit > Upload or floor map can be uploaded when the site is created. Placing the AP's on the floor map is done by clicking the full-screen option and then click edit; then place the AP's on the Map and Save



# Chapter 8: Reports

---

This section provides details on how to schedule and generate different types of data reports in cnMaestro c4000 Controller.

- [Generating Reports](#)
- [Remote Upload](#)
- [Report Jobs](#)

## Generating Reports

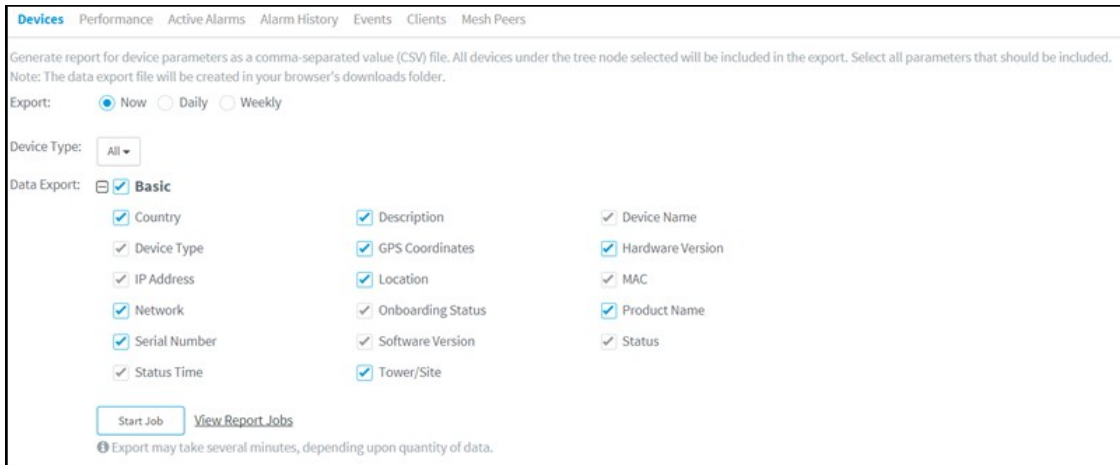
The following reports can be generated for ePMP/PMP and cnPiot devices.

- [Device Report](#)
- [Performance Report](#)
- [Active Alarms Report](#)
- [Alarms History Report](#)
- [Events Report](#)
- [Clients Report](#)
- [Mesh Peers Report](#)

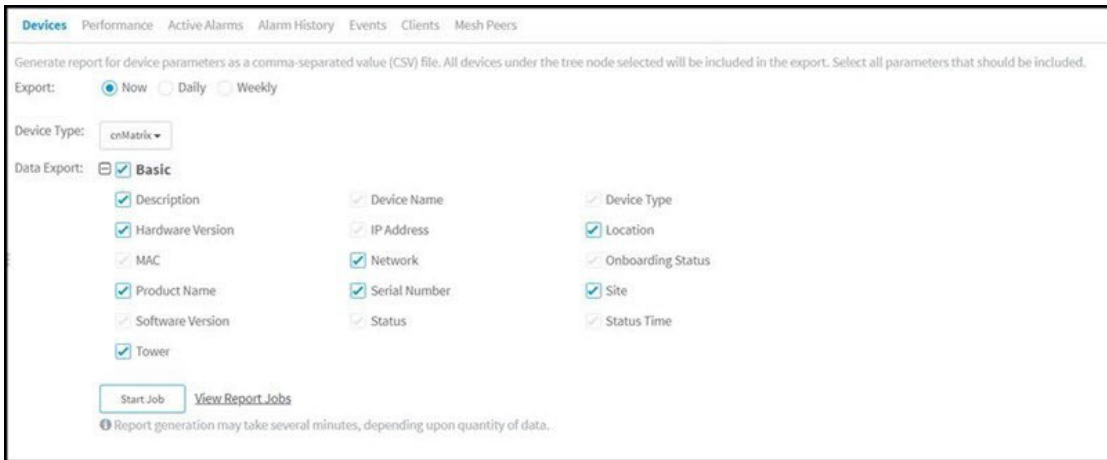
## Device Report

To generate device reports:

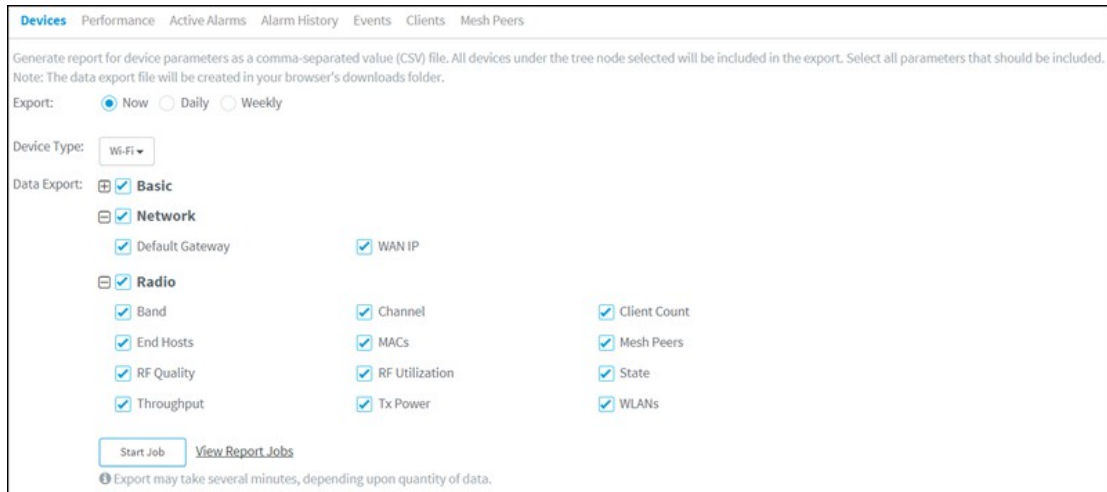
1. Navigate to **Report > Device** tab and select the **Data Export** tab.
2. Select the device type for which the user wants to generate the report or select ALL for generating the report for All device types.
3. Click Start-Job or Schedule based the Selected Export (Now, Daily or Weekly). Based on the device type selection the Data Export parameters will change.
  - a. If ALL is selected as the Device Type, the Basic Data Export parameters will be exported.



b. If cnMatrix is selected as the Device Type, then Basic data will be exported.



c. If cnPilot is selected as the Device Type, then Basic and Network Data will be exported.



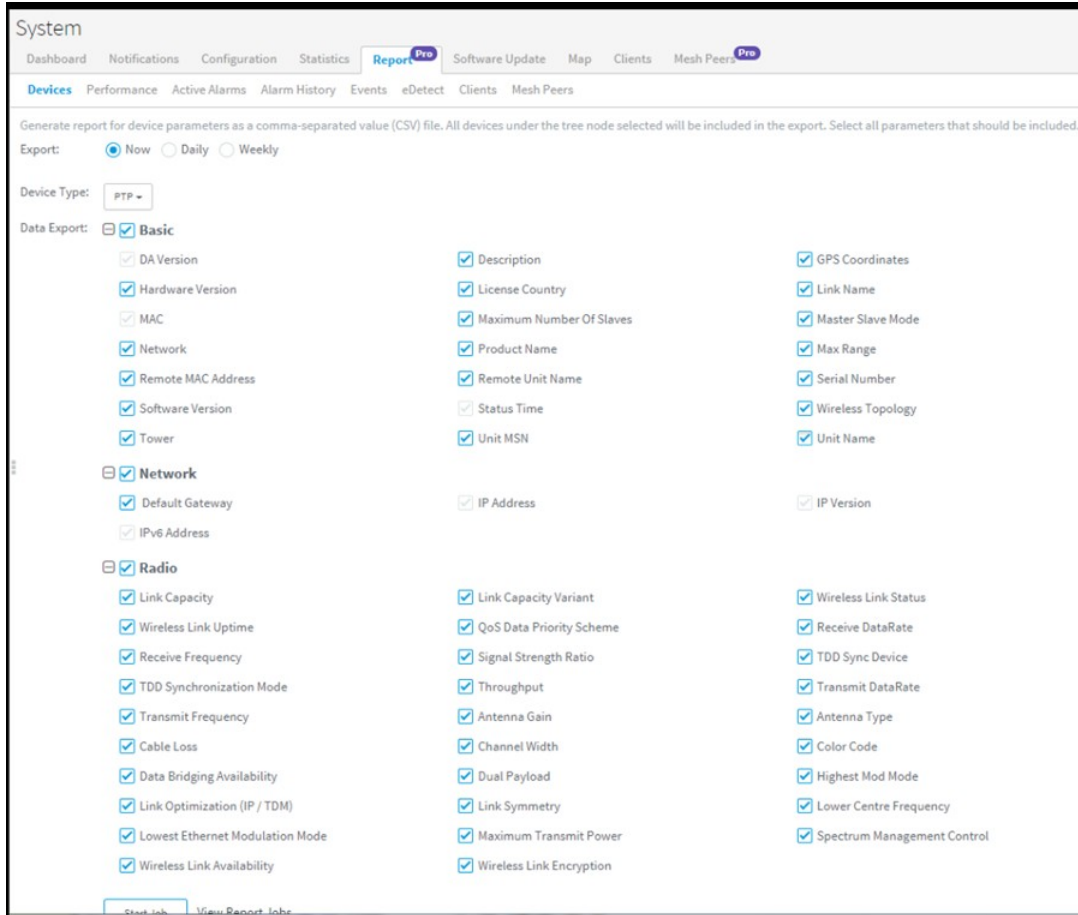
d. If ePMP is selected as the Device Type, then Basic, Network and Radio data will be exported. Users can select to generate the report for either AP or SM or both. Based on the AP or SM selection, the data related to AP or SM will be exported.

The screenshot shows the 'Devices' report generation page. At the top, there are navigation tabs: 'Devices', 'Performance', 'Active Alarms', 'Alarm History', 'Events', 'Clients', and 'Mesh Peers'. Below the tabs, a note states: 'Generate report for device parameters as a comma-separated value (CSV) file. All devices under the tree node selected will be included in the export. Select all parameters that should be included. Note: The data export file will be created in your browser's downloads folder.' The 'Export' section has three radio buttons: 'Now' (selected), 'Daily', and 'Weekly'. The 'Device Type' dropdown is set to 'ePMP'. There are two checked checkboxes: 'AP' and 'SM'. Under 'Data Export', there are three expandable sections: 'Basic', 'Network', and 'Radio', all of which are expanded. The 'Radio' section contains the following checked items: Channel Width, DFS Status, MCS, RF Frequency, RSSI, Radio Mode, Radio TX Power, Retransmission, Retransmission Percentage, SM TX Capacity, SM TX Quality, SNR, Session Drops, and Usage (Packet Count). At the bottom, there are two buttons: 'Start Job' and 'View Report Jobs'. A small information icon is followed by the text: 'Export may take several minutes, depending upon quantity of data.'

- e. If PMP is selected as the Device Type, then Basic, Network and Radio data will be exported. Users can select to generate the report for either AP or SM or both. Based on the AP or SM selection, the data related to AP or SM will be exported.

The screenshot shows the 'Devices' report generation page with the 'Device Type' dropdown set to 'PMP'. The 'AP' and 'SM' checkboxes are still checked. The 'Data Export' sections are the same as in the previous screenshot, but the 'Radio' section contains a different set of checked items: Channel Width, DFS Status, Frame Period, RF Frequency, Radio TX Power, Sync Source, Sync State, and Usage (Packet Count). The 'Start Job' and 'View Report Jobs' buttons are present at the bottom, along with the note: 'Export may take several minutes, depending upon quantity of data.'

- f. If PTP is selected as the Device Type, then Basic, Network and Radio data will be exported.



**Note**

The data will be exported for the devices which are under the System > Network > Tower > Site > AP Group based on the selection made by the user in the LHS Tree.

## Performance Report

To generate performance reports:

1. Navigate to **Report > Performance** tab and select the **Data Export** tab.
2. Select Time Interval based on which the report can be generated for Last Day or Last Week or custom Interval.
3. Select **Interval** to report at either 5 Minutes or 60 Minutes.
4. Select **Device Type**.
5. Click Start-Job or Schedule based the Selected Export (Now, Daily or Weekly).



**Note**

Custom Interval is currently supported only for one week and in future releases, it will be expanded for Monthly data.

## cnMatrix Performance Report

Devices **Performance** Active Alarms Alarm History Events

Generate report for the "device time-based performance data" as a comma-separated value (CSV) file. All devices of selected type under the tree node will be included in the export. Select all parameters that should be included.  
 Note: This feature may generate a large file if many devices are selected.

Period:  Last Day  Last Week  Custom Interval

Resolution:  5 Minutes  60 Minutes  24 Hours

Device Type:

Data Export:  **Basic**

|  |  |  |
|--|--|--|
| <input checked="" type="checkbox"/> CPUs       | <input checked="" type="checkbox"/> Device Name  | <input checked="" type="checkbox"/> Device Type        |
| <input checked="" type="checkbox"/> MAC        | <input checked="" type="checkbox"/> Packet Error | <input checked="" type="checkbox"/> Packets Count (Rx) |
| <input checked="" type="checkbox"/> Throughput | <input checked="" type="checkbox"/> Timestamp    | <input checked="" type="checkbox"/> Packets Count (Tx) |

Report generation may take several minutes, depending upon quantity of data.

Figure 56 cnMatrix performance report

## cnPilot Performance Report

Dashboard Notifications Configuration Statistics **Report** Software Update Map Clients Mesh Peers

Devices **Performance** Active Alarms Alarm History Events Clients Mesh Peers

Generate report for the "device time-based performance data" as a comma-separated value (CSV) file. All devices of selected type under the tree node will be included.  
 Note: This feature may generate a large file if many devices are selected.

Export:  Now  Daily  Weekly

Period:  Last Day  Last Week  Custom Interval

Resolution:  5 Minutes  60 Minutes  24 Hours

Device Type:

Data Export:  **Basic**

|   |  |  |
|---|--|--|
| <input checked="" type="checkbox"/> Airtime (2.4 GHz)     | <input checked="" type="checkbox"/> Airtime (5 GHz)          | <input checked="" type="checkbox"/> Avg No. Of Clients     |
| <input checked="" type="checkbox"/> Avg No. Of Mesh Peers | <input checked="" type="checkbox"/> Avg Receive Rate         | <input checked="" type="checkbox"/> Avg Send Rate          |
| <input checked="" type="checkbox"/> Avg Usage             | <input checked="" type="checkbox"/> Device Mode              | <input checked="" type="checkbox"/> Device Name            |
| <input checked="" type="checkbox"/> Device Type           | <input checked="" type="checkbox"/> Interference (2.4 GHz)   | <input checked="" type="checkbox"/> Interference (5 GHz)   |
| <input checked="" type="checkbox"/> MAC                   | <input checked="" type="checkbox"/> Max Receive Rate         | <input checked="" type="checkbox"/> Max Send Rate          |
| <input checked="" type="checkbox"/> Max Usage             | <input checked="" type="checkbox"/> Min Receive Rate         | <input checked="" type="checkbox"/> Min Send Rate          |
| <input checked="" type="checkbox"/> Min Usage             | <input checked="" type="checkbox"/> Network                  | <input checked="" type="checkbox"/> Noise Floor (2.4 GHz)  |
| <input checked="" type="checkbox"/> Noise Floor (5 GHz)   | <input checked="" type="checkbox"/> Received Bytes (2.4 GHz) | <input checked="" type="checkbox"/> Received Bytes (5 GHz) |
| <input checked="" type="checkbox"/> Sent Bytes (2.4 GHz)  | <input checked="" type="checkbox"/> Sent Bytes (5 GHz)       | <input checked="" type="checkbox"/> Site                   |
| <input checked="" type="checkbox"/> Timestamp             | <input checked="" type="checkbox"/> Total Received Bytes     | <input checked="" type="checkbox"/> Total Sent Bytes       |

[View Report Jobs](#)

Report generation may take several minutes, depending upon quantity of data.

Figure 57 cnPilot performance report



## cnReach Performance Report

System

Dashboard Notifications Configuration Statistics **Report Pro** Software Update Map Clients Mesh Peers Pro

Devices **Performance** Active Alarms Alarm History Events Clients Mesh Peers

Generate report for the "device time-based performance data" as a comma-separated value (CSV) file. All devices of selected type under the tree node will be included in the export.  
 Note: This feature may generate a large file if many devices are selected.

Export:  Now  Daily  Weekly

Period: **Last Day** Last Week Custom Interval

Resolution:  5 Minutes  60 Minutes  24 Hours

Device Type: cnReach

Data Export:  **Basic**

|   |   |  |
|---|---|--|
| <input checked="" type="checkbox"/> Device Name | <input checked="" type="checkbox"/> Device Type | <input checked="" type="checkbox"/> MAC  |
| <input checked="" type="checkbox"/> Neighbors   | <input checked="" type="checkbox"/> Noise       | <input checked="" type="checkbox"/> RSSI |
| <input checked="" type="checkbox"/> Throughput  | <input checked="" type="checkbox"/> Timestamp   |  |

[View Report Jobs](#)

Report generation may take several minutes, depending upon quantity of data.

Figure 58 cnReach Performance Report

## ePMP Performance Report

Devices **Performance** Active Alarms Alarm History Events Clients Mesh Peers

Generate report for the "device time-based performance data" as a comma-separated value (CSV) file. All devices of selected type under the tree node will be included in the export. Select all parameters that should be included.  
 Note: This feature may generate a large file if many devices are selected.

Export:  Now  Daily  Weekly

Period: **Last Day** Last Week Custom Interval

Interval:  5 Minutes  60 Minutes  24 Hours

Device Type: ePMP  AP  SM

Data Export:  **Basic**

|   |  |  |
|---|--|--|
| <input checked="" type="checkbox"/> CPUs              | <input checked="" type="checkbox"/> Device Mode          | <input checked="" type="checkbox"/> Device Name    |
| <input checked="" type="checkbox"/> Device Type       | <input checked="" type="checkbox"/> MAC                  | <input checked="" type="checkbox"/> MCS            |
| <input checked="" type="checkbox"/> Network           | <input checked="" type="checkbox"/> RSSI                 | <input checked="" type="checkbox"/> Retransmission |
| <input checked="" type="checkbox"/> SM Count          | <input checked="" type="checkbox"/> SNR                  | <input checked="" type="checkbox"/> Session Drops  |
| <input checked="" type="checkbox"/> Status Last value | <input checked="" type="checkbox"/> Throughput           | <input checked="" type="checkbox"/> Timestamp      |
| <input checked="" type="checkbox"/> Tower             | <input checked="" type="checkbox"/> Usage (Packet Count) |  |

[View Report Jobs](#)

Export may take several minutes, depending upon quantity of data.

Figure 59 ePMP performance report

## PMP Performance Report

Figure 60 PMP performance report

## PTP Performance Report

Figure 61 PTP performance report

## Active Alarms Report

To generate the Active Alarms reports, navigate to Report > Active Alarms and select the Data Export tab. This report will export the data for the Alarms which are currently active at the report generation time.

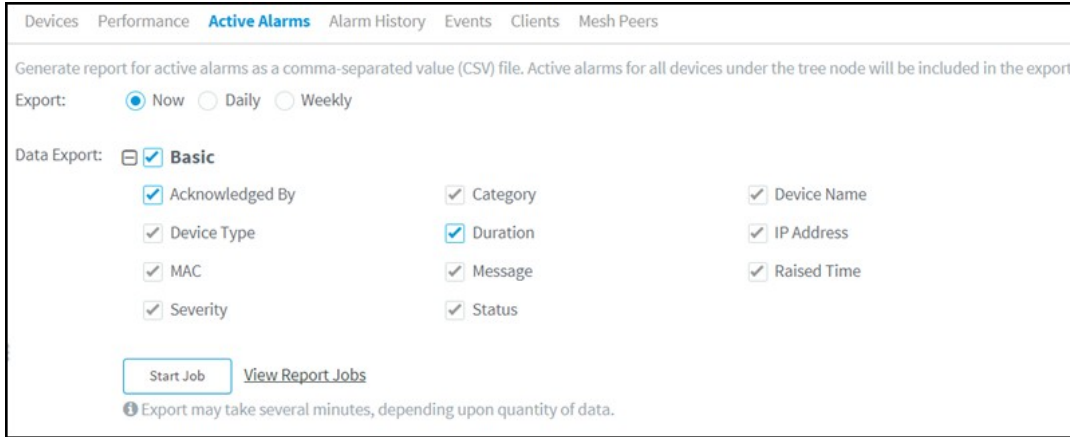


Figure 62 Active alarms report

## Alarms History Report

In order to generate the Active Alarms reports, navigate to Report > Alarm History and select the Data Export tab.

This report will export the data for the Alarms which are currently active at the report generation time and the historical alarms for the specified Time Period and Interval.

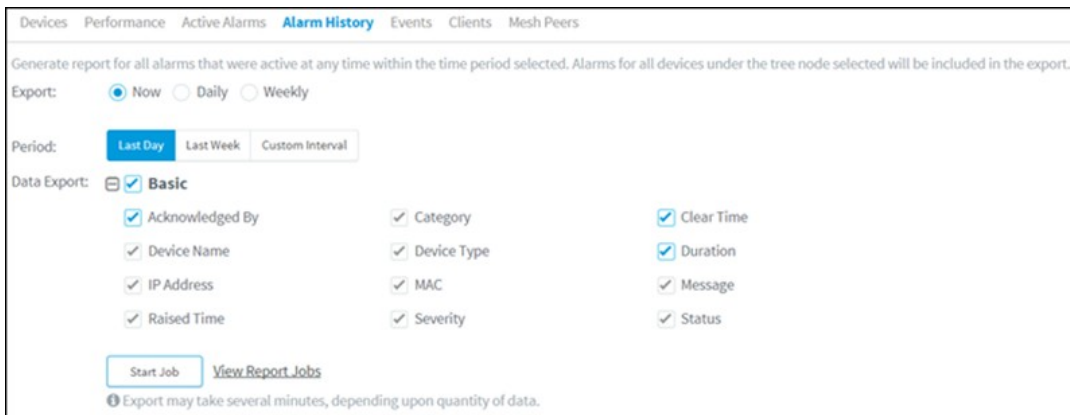


Figure 63 Alarms history report

## Events Report

To generate the Events reports:

1. Navigate to Report > Events tab and select the Data Export tab.
2. Select the Time Interval based on which the report can be generated Last Day or Last Week or Custom Interval and Reporting Interval of either 5 Minutes or 60 Minutes.
3. Click Start-Job or Schedule based the Selected Export (Now, Daily or Weekly).

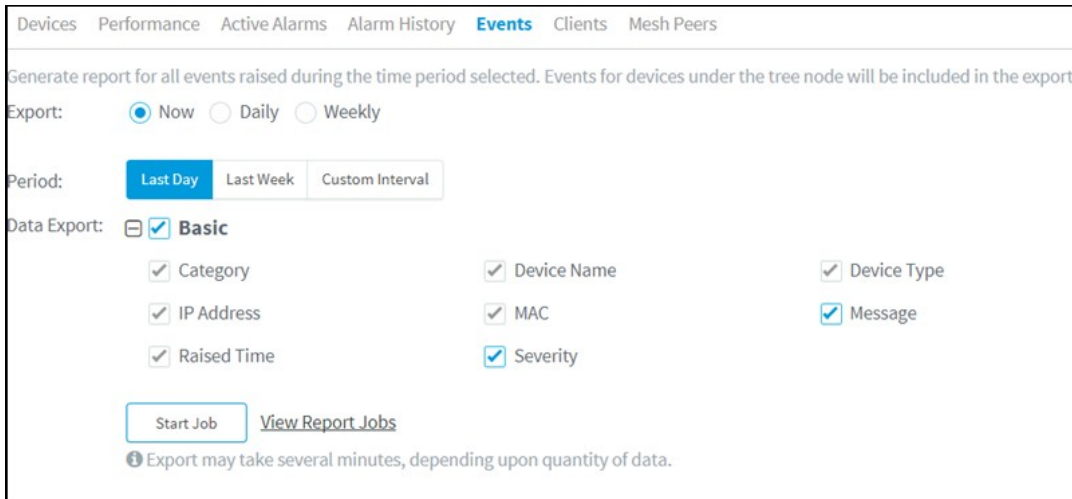


Figure 64 Events report

The events report will export the data for the events for the specified Time Period and Interval.

## Clients Report

To generate the reports for Client data:

1. Navigate to Report > Clients tab and select the Data Export tab.
2. Select Time Interval based on which the report can be generated Now, Daily or Weekly.
3. Click Start-Job or Schedule based the Selected Export (Now, Daily or Weekly).

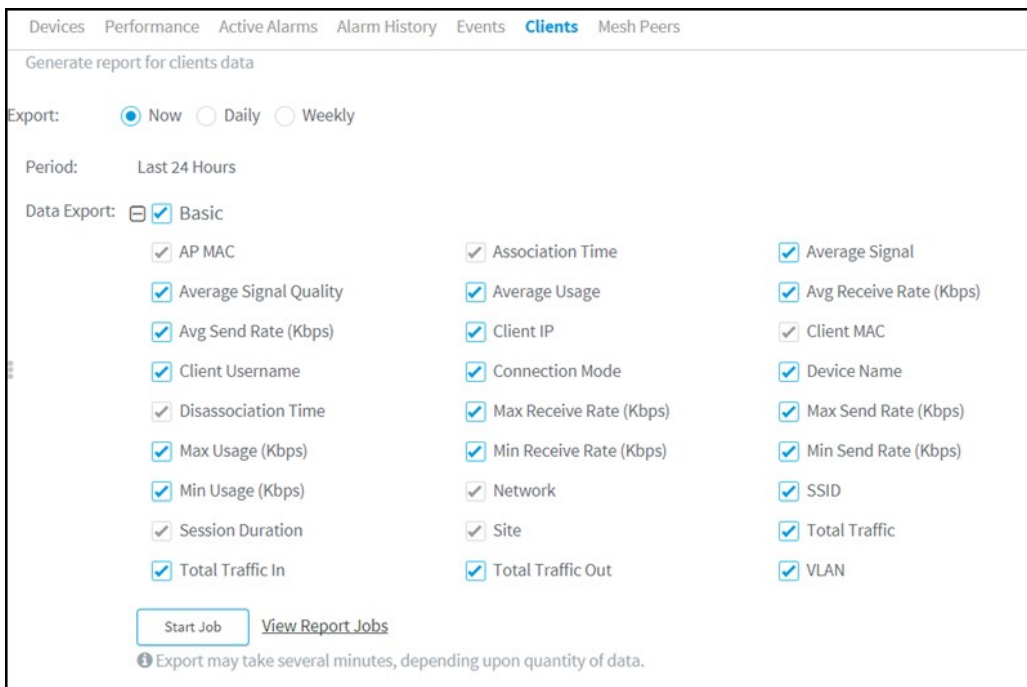


Figure 65 Clients report

The Client report will export the data for the clients for the specified Time Period and Interval.

## Mesh Peers Report

To generate the Mesh Peers report:

1. Navigate to Appliance > Settings page and enable Detailed Mesh Statistics checkbox under Advanced Features. The Mesh Peers tab will appear in the Reports page.
2. Select the Data Export tab under the Mesh Peers tab.
3. Click Start-Job or Schedule based the Selected Export (Now, Daily or Weekly). The Mesh Report for the last 24 hours will be generated.

The screenshot shows the 'Mesh Peers' configuration page. At the top, there are navigation tabs: Devices, Performance, Active Alarms, Alarm History, Events, Clients, and Mesh Peers. Below the tabs, it says 'Generate report for mesh peers data'. The 'Export' section has three radio buttons: 'Now' (selected), 'Daily', and 'Weekly'. The 'Period' is set to 'Last 24 Hours'. Under 'Data Export', there is a 'Basic' checkbox which is checked. Below this, there are 18 individual checkboxes for various data points, all of which are checked: AP MAC, AP Name, Association Time, Avg RSSI, Avg Receive Rate, Avg SNR, Avg Send Rate, Avg Throughput, Band, Base MAC Address, Disassociation Time, Hostname, IP Address, Last Data Rate, MAC Address, Max Data Rate, Min Data Rate, Network, Received Bytes, SSID, Sent Bytes, Session Duration, and Site. At the bottom, there is a 'Start Job' button and a 'View Report Jobs' link. A small information icon and text at the bottom state: 'Export may take several minutes, depending upon quantity of data.'

Figure 66 Mesh peers report



### Note

1. Every Report page has a View Report Jobs link that directs the user to the Report Jobs page under Appliance > Jobs > Reports.
2. To schedule a report Now, click the Start button under the respective Report section. cnMaestro c4000 Controller downloads the report immediately for the current system time.  
  
Daily reports will generate reports on a daily basis depending upon the start and the end time. The weekly report generates a report on seven days intervals depending upon the start and the end time. Click the Schedule button and configure the start and end time to schedule daily or weekly reports under the respective Reports section.
3. Export Now option helps the user to create no export Jobs and these will be stored under the Appliance > Jobs> Report tab in the export page and can be downloaded within seven days from the day of generation. This saves the user's local memory from downloading each and every export report.

## Remote Upload

Reports scheduled, for Now, Daily or Weekly can be downloaded directly through the UI, or from an FTP or SFTP server.

To transfer reports to FTP or SFTP server:

1. Navigate to Appliance > Settings page and select the Optional Features tab.
2. Select the Report Scheduler checkbox to enable scheduling features for data reports.
3. Select the Remote Upload checkbox to upload the generated reports to the configured file server by FTP or SFTP.
4. Enter the remote name or IP address of the host in the Remote host text box.
5. Enter the port number in the Port Number text box.
6. Enter the name of the user in the Username text box.
7. Enter the password in the Password text box.
8. Enter the path of the file to upload the report in the File Path text box.
9. Click Save.

Figure 67 Scheduling reports

## Report Jobs

Displays the list of scheduled reports created by different users.

Application > Jobs

Configuration Update Software Update **Reports** Actions

Displays the list of scheduled reports created by different users. [Learn more](#)

Managed Account: All Accounts Delete

| ID | Type        | Managed Account      | Source  | Schedule | Starts At          | Ends After         | Created by     | Created on         | Status                         | Last Report        |            |
|----|-------------|----------------------|---------|----------|--------------------|--------------------|----------------|--------------------|--------------------------------|--------------------|------------|
| 54 | Performance | Trimp                | default | Now      | Jun 13, 2019 17:38 | Jun 13, 2019 17:38 | Administrator  | Jun 13, 2019 17:38 | Completed                      | Jun 13, 2019 17:38 | 🔍 ⏏️ 🗑️ ✖️ |
| 53 | Performance | Trimp                | default | Now      | Jun 13, 2019 17:37 | Jun 13, 2019 17:37 | Administrator  | Jun 13, 2019 17:37 | Completed                      | Jun 13, 2019 17:37 | 🔍 ⏏️ 🗑️ ✖️ |
| 22 | Events      | Managed-Account-User | default | Daily    | Jun 13, 2019 12:07 | Sep 10, 2019 12:07 | Rgnmoni Login  | Jun 13, 2019 12:02 | Scheduled (Jun 14, 2019 12:07) | Jun 13, 2019 12:07 | 🔍 ⏏️ 🗑️ ✖️ |
| 21 | Performance | Managed-Account-User | default | Daily    | Jun 13, 2019 12:07 | Jun 17, 2019 12:07 | Rgnmoni Login  | Jun 13, 2019 12:01 | Scheduled (Jun 14, 2019 12:07) | Jun 13, 2019 12:07 | 🔍 ⏏️ 🗑️ ✖️ |
| 20 | Performance | Managed-Account-User | default | Daily    | Jun 13, 2019 12:07 | Jun 17, 2019 12:07 | Rgnmoni Login  | Jun 13, 2019 12:01 | Scheduled (Jun 14, 2019 12:07) | Jun 13, 2019 12:07 | 🔍 ⏏️ 🗑️ ✖️ |
| 19 | Performance | Managed-Account-User | default | Daily    | Jun 13, 2019 12:07 | Jun 17, 2019 12:07 | Rgnmoni Login  | Jun 13, 2019 12:01 | Scheduled (Jun 14, 2019 12:07) | Jun 13, 2019 12:07 | 🔍 ⏏️ 🗑️ ✖️ |
| 18 | Performance | Managed-Account-User | default | Now      | Jun 13, 2019 12:01 | Jun 13, 2019 12:01 | Rgnmoni Login  | Jun 13, 2019 12:01 | Completed                      | Jun 13, 2019 12:02 | 🔍 ⏏️ 🗑️ ✖️ |
| 17 | Devices     | Managed-Account-User | default | Now      | Jun 13, 2019 12:01 | Jun 13, 2019 12:01 | Rgnmoni Login  | Jun 13, 2019 12:01 | Completed                      | Jun 13, 2019 12:02 | 🔍 ⏏️ 🗑️ ✖️ |
| 16 | Performance | Managed-Account-User | System  | Daily    | Jun 13, 2019 04:31 | Jun 17, 2019 04:31 | RgnAdmin Login | Jun 12, 2019 16:25 | Scheduled (Jun 15, 2019 04:31) | Jun 14, 2019 04:31 | 🔍 ⏏️ 🗑️ ✖️ |
| 15 | Performance | Managed-Account-User | System  | Daily    | Jun 13, 2019 04:31 | Jun 17, 2019 04:31 | RgnAdmin Login | Jun 12, 2019 16:25 | Scheduled (Jun 15, 2019 04:31) | Jun 14, 2019 04:31 | 🔍 ⏏️ 🗑️ ✖️ |

Showing 1 - 10 Total: 76 10 Previous 1 2 3 4 5 8 Next

Figure 68 Report jobs

A scheduled report Job displays the following action buttons:

- Edit: Visible only for the active Jobs which are not yet run once. With this option, you can reschedule a Job.
- Terminate: Stop active Jobs.
- Show History: Display the detailed status of the generated reports and the file transfer status.
- Delete: Delete active and completed Jobs.
- Instant Download: Users can instantly download the latest report directly once the download is complete without checking the show history.

## Chapter 9: Software Update

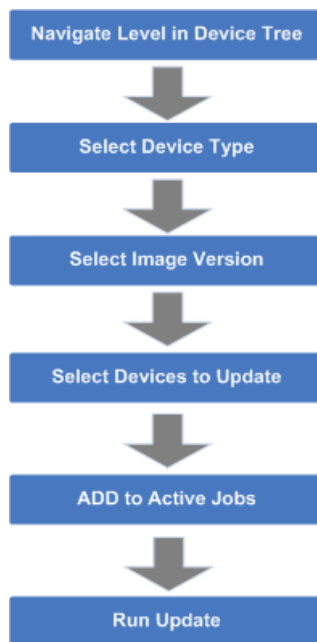
---

The Software Update tab displays the device update details for cnMaestro c4000 Controller. This chapter includes the following:

- [Software Update Overview](#)
- [Software Update Jobs](#)
- [cnReach Bulk Software Upgrade](#)

### Software Update Overview

The Software Update feature allows users to deploy the latest software images to devices. Software updates can be started at any level in the Device Tree, and individual devices can be selected for update. Updates are created as Jobs and placed into the Jobs Queue. When the update is ready to run, it can be started. The basic flow is the following:



**Figure 69 Software Update Overview**

When a job finishes, it is placed in the Completed Jobs table, where it will remain for a week before it is deleted.



## Create Software Update Job

### Device Selection

Navigate the Device Tree to an appropriate level for the devices to be updated. For example, selecting an AP will filter the selectable devices to include itself and its children.

### Device Type

Software Updates are executed on one device-type at a time. The type includes specific hardware (Backhaul and Wi-Fi devices).

### Software Update Dashboard

Once the device type is chosen, the Software Update Dashboard displays the most recent software release version for that device type. It also displays a breakdown of the different software versions currently installed on the devices in the upgrade view.

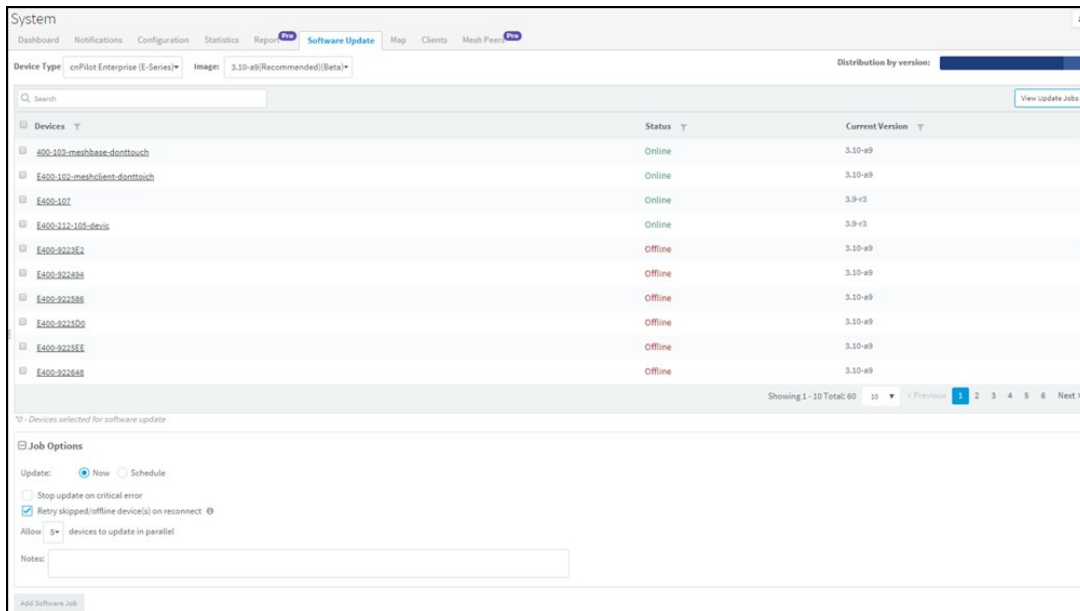


Figure 70 Software Update Dashboard (cnPilot Enterprise AP)

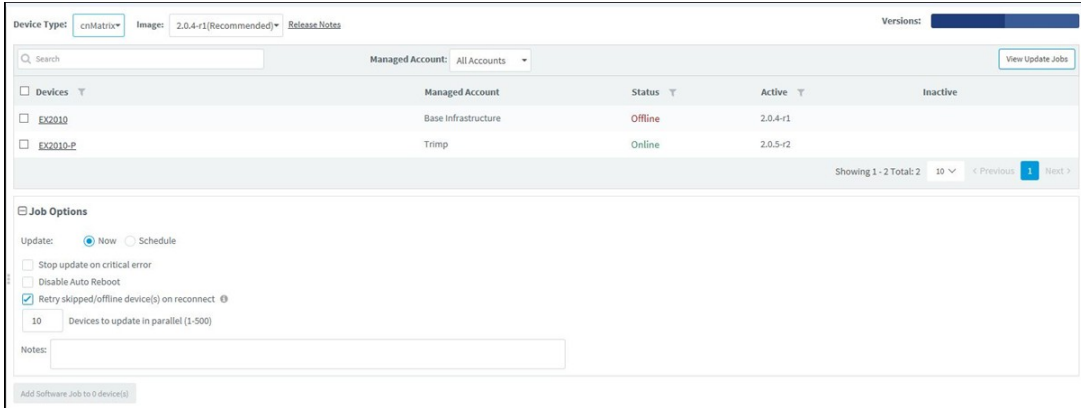


Figure 71 Software Update Dashboard (cnMatrix)

Disable Auto Reboot option disables reboot after applying the new software image. The user has to manually reboot the switch to complete the software update and boot with the new version.

### Scheduling Software Update Job

You can now schedule a software update job on the devices by selecting a Schedule radio button and providing the Start Date and Start Time.

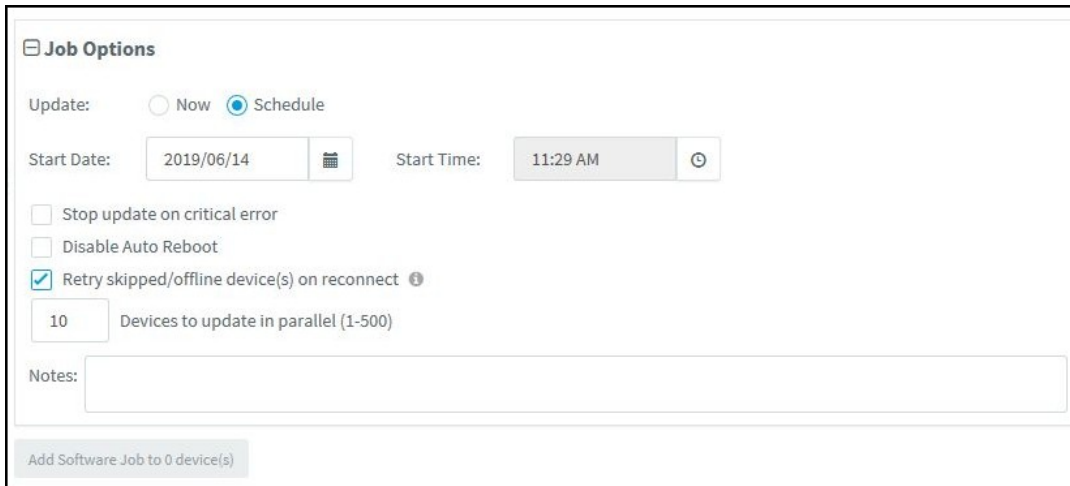
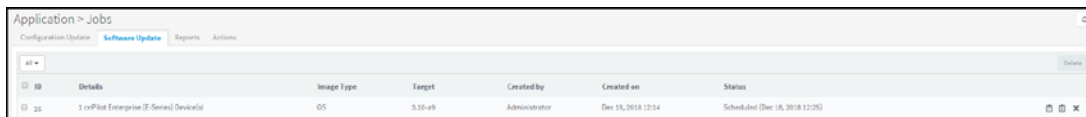


Figure 72 Scheduling Software Update Job

You can view the status of Software Update Job in **Appliance > Jobs > Software Update** page.



You need to download the newly released image from the [Support Site](#). Please refer to [Managing Device Software Images](#) for more details.

### Device Table

Select the devices to upgrade in the Devices Table.

**Note**

You can upgrade a device only when its status is Up. If you try to upgrade a device when it is Down, the selected device is down message is displayed in the UI.

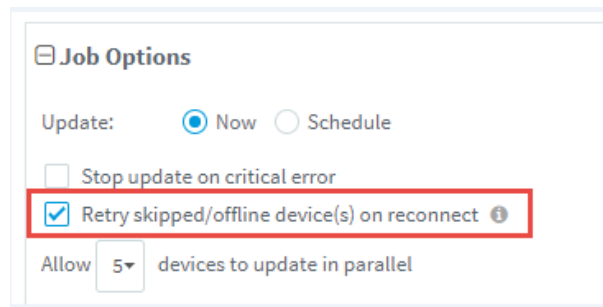
The following parameters are visible (though some are only available for certain device types).

**Table 23 Parameters Displayed in Device Table**

| Parameter       | Description   |
|-----------------|---|
| Devices         | The names of available devices in a system. The list is pre-filtered based upon the node selected in the Device Tree. |
| Selected SMs    | If the AP is selected, the corresponding SMs will also be selected.   |
| Status          | The status of a device in a system. Devices that are not connected and cannot have images pushed to them.             |
| Current Version | The version of the active software image running on the device.   |

## Retry Software Update

The Retry Software Update option is available in every Software Update tab, and it is enabled by default.



**Figure 73 Retry Software Update**

If the software update job was skipped for a device as it was offline, an icon ( ) appears next to the Active Software version of the device. This indicates that the software update for the device will be done with the Target device version in the Job, whenever it reconnects to cnMaestro c4000 Controller.

If the software update job was skipped while upgrading with the same version as the device active version, then the icon will not be displayed, and the device will not update when it reconnects.

**Note**

The device which undergoes Retry Software Update, will not create a new Job.

## Options

### Stop Updates on Critical Error

If one of the updates fails, then don't start any additional updates and instead pause the update job. All existing, concurrent updates will be allowed to proceed until completion. The administrator will be able to continue the update where it left off, if desired.

### Sector Upgrade Order

The recommended update ordering for devices within a sector will be pre-configured according to the recommendations for the device. It can be changed if desired.



#### Note

Device updates will occur sector-by-sector. One sector needs to complete before a second sector is started.

### Parallel Upgrades

Specify how many device upgrades to perform in parallel to complete the upgrade faster. However if the job is configured to halt on an error, all concurrent sessions will still be allowed to complete.

## Upgrade Steps

To upgrade an ePMP (Sectors) device:

1. Navigate to System or Network or Tower or Device level. From the list, select the system or network or tower or device to which the device belongs.
2. Navigate to Manage > Software Update > Select Devices page.
3. Select ePMP (Sectors) from the following Select Device Type drop-down list:
  - a. ePMP (Sectors)
  - b. PMP (Sectors)
  - c. cnPilot R200/R190/R201
  - d. ePMP 1000 Hotspot
  - e. e. cnPilot E400/E410/E500/E501S/E600/E502S/E430W/e700
  - f. cnMatrix
  - g. PTP
4. Select the software image to update from the Select Image Version drop-down list.
5. Select the devices to update by clicking the tick icon.
6. Set desired Job Options.
7. Click the Add Software Job button.

## Software Update Jobs

The Software Update Jobs table lists all currently running, queued, and completed jobs. The jobs can be triggered immediately or can be run later.

(Appliance > Jobs > Software Update tab)

The following table displays the list of parameters displayed in the Software Update Jobs tab:

**Table 24 Parameters displayed in Software Update Jobs tab**

| Parameter  | Description  |
|--|--|
| ID   | Identification number of the active job.   |
| Details  | Count of devices and date and time the upgrade process is initiated.   |
| Target   | Target software version to upgrade.  |
| Created By   | The user who has created this job.   |
| Created On   | Date and time on which the job is created.   |
| Parallel   | Number of device to start in parallel.   |
| Stop on Error  | Stop the job, if any device in the middle finds any error.   |
| Sector Priority  | For ePMP/PMP, the priority of AP/SM to start.  |
| Status   | Status of update.  |
| Action   | Use the <b>Start</b> or <b>Delete</b> button to manage the upgrade process. After the upgrade has started, the <b>Pause</b> button will stop new upgrades from the beginning. If the upgrade process fails or the upgrade has been paused, you can restart the process by clicking the <b>Resume</b> button. |
| By selecting the <b>Show More</b> icon, you can view the following parameters: |  |
| Device   | Device for which the upgrade is initiated.   |
| Status   | Status of the device.  |
| Mode   | The mode if AP or SM.  |
| Original Version   | The current software image version of the device.  |
| Result   | The upgrade status of the device.  |
| Message  | The message that is displayed after the update.  |

The user can filter the Jobs based on the running status. The user can also filter the devices in a particular Job based on the parameters mentioned in the above table.

## Abort Software Job

Abort operation will skip devices that are waiting for an update to begin. Devices already being updated may continue, but cnMaestro c4000 Controller will stop tracking their progress. Aborting a Software Job puts the device into a "complete" state that cannot be manually restarted by the user. The "pending" devices will not begin their updates.

| ID  | Details                                     | Managed Account     | Image Type | Occurrence | Target  | Created by    | Created on         | Completed on       | Status                          |
|-----|---|---------------------|------------|------------|---------|---------------|--------------------|--------------------|---------------------------------|
| 162 | 1 cnPilot Enterprise (E-Series) Device(s)   | Base Infrastructure | Device     | Now        | 3.10-r6 | Administrator | Apr 16, 2019 13:32 | Apr 16, 2019 13:32 | Aborted: [red progress bar]     |
| 161 | 4 cnPilot Home (R-Series) Device(s)         | Base Infrastructure | Device     | Now        | 4.5-R7  | Administrator | Apr 15, 2019 18:02 | Apr 15, 2019 18:06 | Completed: [green progress bar] |
| 160 | 680 cnPilot Enterprise (E-Series) Device(s) | All Accounts        | Device     | Now        | 3.10-r6 | Administrator | Apr 15, 2019 17:58 | Apr 15, 2019 17:58 | Aborted: [yellow progress bar]  |
| 159 | 1 cnPilot Enterprise (E-Series) Device(s)   | Base Infrastructure | Device     | Now        | 3.10-r6 | Administrator | Apr 15, 2019 17:56 | Apr 15, 2019 17:56 | Aborted: [red progress bar]     |
| 158 | 1 cnPilot Enterprise (E-Series) Device(s)   | Base Infrastructure | Device     | Now        | 3.10-r6 | Administrator | Apr 15, 2019 17:31 | Apr 15, 2019 17:31 | Aborted: [red progress bar]     |
| 157 | 1 cnPilot Enterprise (E-Series) Device(s)   | Base Infrastructure | Device     | Now        | 3.10-r6 | Administrator | Apr 15, 2019 17:30 | Apr 15, 2019 17:30 | Aborted: [red progress bar]     |
| 156 | 1 cnPilot Enterprise (E-Series) Device(s)   | Base Infrastructure | Device     | Now        | 3.10-r6 | Administrator | Apr 15, 2019 17:28 | Apr 15, 2019 17:28 | Aborted: [red progress bar]     |
| 154 | 1 cnPilot Enterprise (E-Series) Device(s)   | Base Infrastructure | Device     | Now        | 3.11-b4 | Administrator | Apr 15, 2019 12:14 | Apr 15, 2019 12:14 | Aborted: [red progress bar]     |
| 152 | 3 cnPilot Enterprise (E-Series) Device(s)   | Base Infrastructure | Device     | Now        | 3.11-b4 | Administrator | Apr 15, 2019 12:09 | Apr 15, 2019 12:13 | Completed: [green progress bar] |
| 151 | 3 cnPilot Enterprise (E-Series) Device(s)   | Base Infrastructure | Device     | Now        | 3.10-r6 | Administrator | Apr 15, 2019 12:03 | Apr 15, 2019 12:07 | Completed: [green progress bar] |


Figure 74 Abort Software Job



**Note**

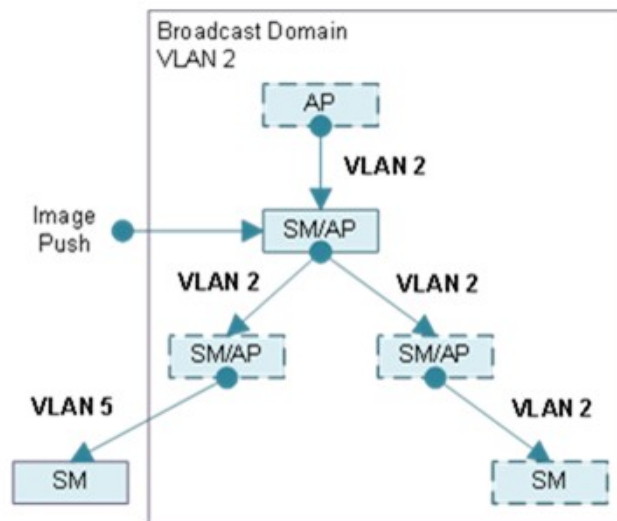
1. Devices that are already completed display as "completed" with a message "update complete" along with the status as Completed.
2. Devices which are ongoing display as "Aborted" with a message "Manually Aborted" with the status as Aborted.
3. Devices that have not yet started display as "skipped" with a message "job was aborted" with the status as Skipped.

## Viewing Running Jobs in Header

Click the  icon in the top right corner of the UI. This directs you to the Jobs page of the Software Update section. For more information, see [Software Update Jobs](#)

## cnReach Bulk Software Upgrade

Distributing software to cnReach devices can take many hours, due to the relatively low RF bandwidth. In order to minimize wireless traffic, cnMaestro c4000 Controller supports the cnReach mechanism by which a single AP coordinates the broadcast distribution of firmware to every cnReach device within its VLAN. In the graphic below, the bulk upgrade operation transfers an image to the middle AP, which then distributes it to all APs with VLAN 2. The APs are not updated in this process; the firmware is just pushed into their storage, where it can be applied later (once the distribution completes). cnReach has a mechanism to handle offline devices during the distribution (which can take upwards of a day), or devices added midway through the transfer. Often this means the process repeats a second time, to handle any updates.



The Bulk Upgrade mechanism is optional, and meant to be used for efficiency. One can still use the standard Software Update mechanism to transfer images to cnReach devices one-at-a-time, though the distribution could be many hours or days.

## Firmware Versions (OS and Radio)

cnReach devices have two versions of software: one for the Motherboard OS, and another for the Radio. Each Radio can have a different version of the firmware. When selecting software to distribute, one should choose either OS or Radio. During the Apply phase, when the image is updated, one or both Radios can be selected.

## Bulk Upgrade Page

The Bulk Upgrade page is accessed by selecting a cnReach AP then Software Update > Bulk Upgrade. The Motherboard (OS) or Radio software is available, and the distribution started and stopped. Once started, the distribution continues until stopped, so be sure to manually stop the process when complete.

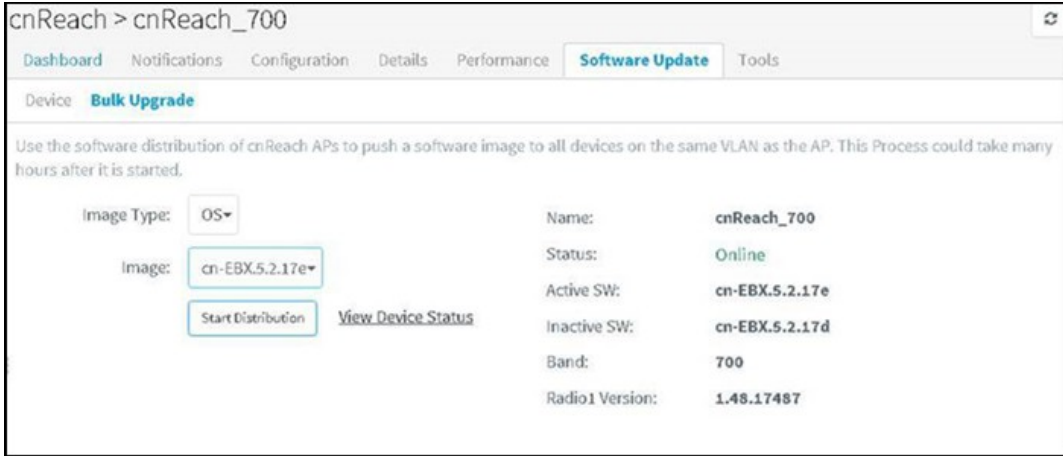


Figure 75 Bulk upgrade package



**Note**

You must start the distribution on a single AP in a cnReach VLAN, and only run it from that AP. Executing Bulk Upgrade on more than one AP in a VLAN will not be prevented by cnReach devices, and it could lead to distribution failures.

## Upgrade Tracking

The following page is displayed when an AP is actively distributing software. One can view other devices in the VLAN (and their current software versions), and the distribution status. Distribution can be stopped at any time, and images can be applied directly to the devices in the list.

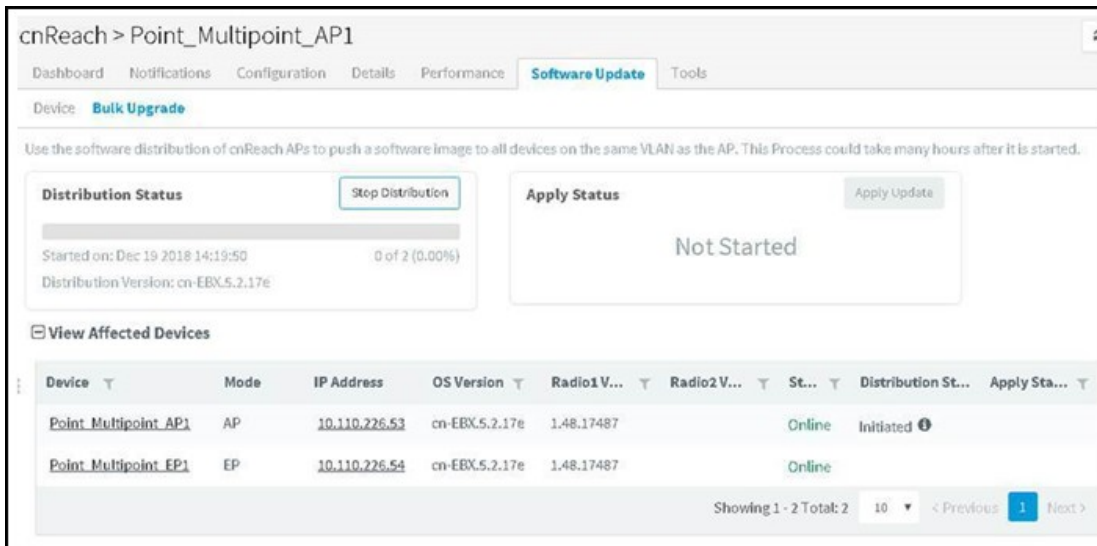


Figure 76 Upgrade tracking



# Chapter 10: Inventory

This chapter provides the following information:

- **Inventory Export**
- **Bulk Move**
- **Bulk Delete**
- **Bulk Reboot**
- **CSV Configuration Import**

Inventory displays a list of devices under the selected node. It presents health and maintenance information that can be toggled through a button bar at the top. It aggregates children devices and provides a tabular view that allows for sorting and filtering. When selected for a single device, it presents a detailed page tailored to that device.

Navigate to the Inventory tab on the left pane.

| Device      | Type         | IP Address     | Health               | Serial Number | Description | Onboarded  | Active S/W V... |
|-------------|--------------|----------------|----------------------|---------------|-------------|------------|-----------------|
| E500-B39748 | cnPilot e500 | 10.110.220.123 | Online<br>0d 12h 52m |               |             | 0d 15h 35m | 4.0-b11         |
| E500-919DCA | cnPilot e500 | 10.110.222.212 | Online<br>0d 16h 42m |               |             | 0d 21h 15m | 3.11.3-b9       |
| E500-917644 | cnPilot e500 | 10.110.220.103 | Online<br>0d 16h 42m |               |             | 0d 21h 15m | 3.11.3-b9       |
| E400-B67566 | cnPilot e400 | 10.110.220.120 | Online<br>0d 16h 42m |               |             | 0d 21h 15m | 3.11.3-b9       |
| E400-AE28DA | cnPilot e400 | 10.110.220.241 | Online<br>0d 16h 42m |               |             | 0d 21h 15m | 3.11.3-b9       |
| E500-919F10 | cnPilot e500 | 10.110.220.53  | Online<br>0d 16h 42m |               |             | 0d 21h 15m | 3.11.3-b9       |
| E500-919DCA | cnPilot e500 | 10.110.220.234 | Online<br>0d 16h 41m |               |             | 0d 21h 15m | 3.11.3-b9       |
| E500-919DCA | cnPilot e400 | 10.110.220.233 | Online<br>0d 16h 41m |               |             | 0d 21h 15m | 3.11.3-b9       |
| E400-AD3C0E | cnPilot e400 | 10.110.220.132 | Online<br>0d 16h 42m |               |             | 0d 21h 15m | 3.11.3-b9       |
| E400-B4587C | cnPilot e400 | 10.110.222.137 | Online<br>0d 16h 42m |               |             | 0d 21h 15m | 3.11.3-b9       |

Figure 77 Inventory - Access and Backhaul View

| Device                | Managed Account     | Status                            | Serial Number | IP Address      | Type         | AP Group             |
|-----------------------|---------------------|-----------------------------------|---------------|-----------------|--------------|----------------------|
| Rajesh                | Base Infrastructure | Offline (3d 1h 48m)<br>Onboarded  |               | 10.110.208.1... | cnPilot E500 | N/A                  |
| E400-cnPilot-182-RGVN | BesKOM              | Offline (4d 2h 19m)<br>Onboarded  |               | 10.110.212.1... | cnPilot E400 | N/A                  |
| E400-BSADEFQ          | BesKOM              | Online (5d 21h 4...)<br>Onboarded |               | 10.110.202.1... | cnPilot E400 | E400-RGVN-SmartWorks |

Figure 78 Inventory - Wi-Fi View

## Inventory Export

The inventory can be exported in either CSV or PDF format. The values exported will match those in the selected table columns. You can customize the health and maintenance views to add or delete columns.

## Bulk Move

The Bulk Move option is available in the inventory page of **System > Tower > Network > Site** in cnMaestro c4000 Controller On-Premises.

This feature helps the users in bulk movement of devices in the following scenarios:

- From one Network/Tower/Site to another according to the device type.
- Between different Tower/Site within the same Network according to the device type.
- Between different Tower/Site across the different Networks according to the device type.

When the devices are moved using the Bulk Move option, all the **Network > Tower > Site** dashboards, graphs, clients, reports, and mesh peers will also get updated accordingly.



### Note

1. ePMP/PMP AP and SMs cannot be moved to any Site.
2. The independent Wi-Fi devices cannot be moved to Towers.
3. If a Wi-Fi device is a child of AP and SM, it is moved automatically to a Tower along with the AP and SM.
4. ePMP/PMP SMs cannot be selected for the bulk move operation. SMs are moved automatically along with the AP.
5. In case of moving multiple devices, cnMaestro c4000 Controller detects the device type and moves the devices to Tower/Site accordingly.

| Device   | Managed Account     | Type          | IP Address     | Health              | Serial Number | Description | Onboarded  | Active S/W Version  |
|--|---------------------|---------------|----------------|---------------------|---------------|-------------|------------|---------------------|
| <input type="checkbox"/> No Site Name<br>0A00:3E:8B:84:25            | Base Infrastructure | PMP 450i SM   | 10.110.208.83  | Online (od 18h ...) | M9TL00TN84ZC  | N/A         | 0d 18h 46m | 15.2 (Build SIT-25) |
| <input checked="" type="checkbox"/> No Site Name<br>0A00:3E:8B:83:51 | Base Infrastructure | PMP 450i AP   | 10.110.208.82  | Online (od 18h ...) | M9TE09942KBW  | N/A         | 0d 18h 46m | 15.1.3              |
| <input type="checkbox"/> No Site Name<br>0A00:3E:8B:95:F3            | Base Infrastructure | PMP 450i AP   | 10.110.208.81  | Online (od 18h ...) | M9TH133C1RCX  | N/A         | 0d 18h 47m | 15.1.3              |
| <input type="checkbox"/> cnPilot R201P<br>0004:960D:43F9             | Base Infrastructure | cnPilot R201P | 10.110.208.124 | Online (48d 19 ...) | WFSH003L7GCM  | N/A         | 5d 19h 57m | 4.3.3-84            |

Figure 79 Bulk Move

To move devices using Bulk Move:

1. Navigate to Inventory page of **System > Network > Tower > Site**.
2. Select one or multiple devices as per the requirement.
3. Click **Move**. A new window appears.
4. Select the **Network**, Tower or Site from the drop-down list to which the devices need to be moved.
5. Click **Save**.



**Note**

1. When the Managed Service Provider (MSP) feature is enabled, the user is allowed to move the devices at Network > Site > Tower levels within the tenant accounts and not across different tenant accounts.
2. The Bulk Move option is not available at the System level, when MSP is enabled.

## Bulk Delete

The Bulk Delete option is available in the inventory page of **System > Tower > Network > Site** in cnMaestro c4000 Controller. This feature helps the users in bulk deletion of devices from **System > Tower > Network > Site**.

| Device   | Managed Account     | Type        | IP Address    | Health              | Serial Number | Description | Onboarded  | Active S/W Version  |
|--|---------------------|-------------|---------------|---------------------|---------------|-------------|------------|---------------------|
| <input type="checkbox"/> No Site Name<br>0A00:3E:8B:84:25            | Base Infrastructure | PMP 450i SM | 10.110.208.83 | Online (od 18h ...) | M9TL00TN84ZC  | N/A         | 0d 18h 46m | 15.2 (Build SIT-25) |
| <input checked="" type="checkbox"/> No Site Name<br>0A00:3E:8B:83:51 | Base Infrastructure | PMP 450i AP | 10.110.208.82 | Online (od 18h ...) | M9TE09942KBW  | N/A         | 0d 18h 46m | 15.1.3              |
| <input type="checkbox"/> No Site Name<br>0A00:3E:8B:95:F3            | Base Infrastructure | PMP 450i AP | 10.110.208.81 | Online (od 18h ...) | M9TH133C1RCX  | N/A         | 0d 18h 47m | 15.1.3              |

Figure 80 Bulk Delete

To delete devices using Bulk Delete:

1. Navigate to Inventory page of **System > Network > Tower > Site**.
2. Select one or multiple devices as per the requirement.
3. Click **Delete**.



**Note**

In the Wi-Fi view, the Bulk Delete option can also delete the devices that are in waiting for the approval state.

## Bulk Reboot

The Bulk Reboot option is available in the inventory page of **Tower > Network > Site** in cnMaestro c4000 Controller. This feature helps the users in bulk reboot of devices.

When the devices are moved using the Bulk Reboot option, all the **Network > Tower > Site** dashboards, graphs, clients, reports, and mesh peers will also get updated accordingly.

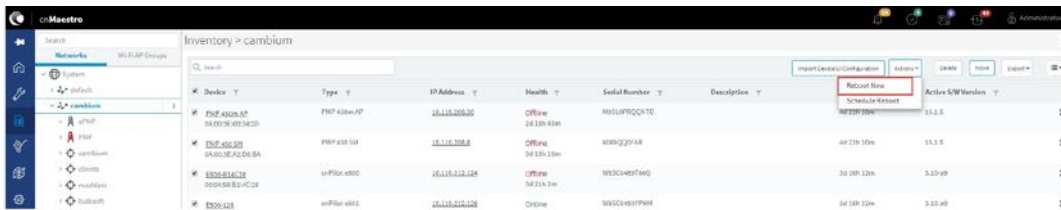


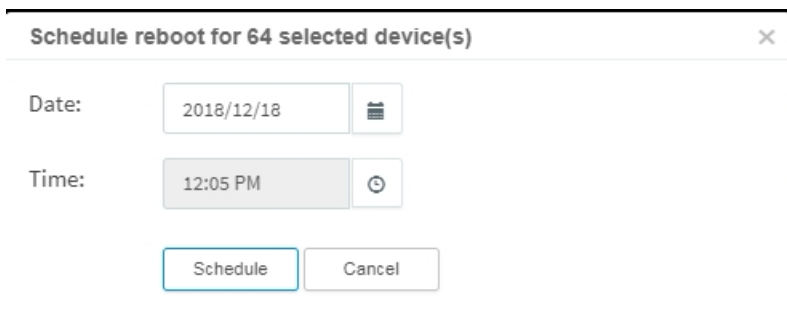
Figure 81 Bulk Reboot

To reboot devices using Bulk Reboot:

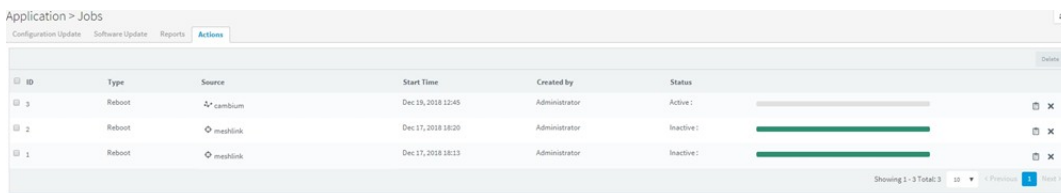
1. Navigate to Inventory page of **Network > Tower > Site**.
2. Select one or multiple devices as per the requirement.
3. Click **Actions** and choose **Reboot Now**.

## Schedule Reboot

You can also schedule the reboot of the device/device(s) by selecting the Schedule Reboot button from Actions drop-down list, and by providing the Date and Time.



After creating a scheduled Reboot Job, you can view the status in the **Appliance > Jobs > Actions** page.



## CSV Configuration Import

Import device(s) configuration is available from inventory page at **System > Network > Managed Account/ePMP or PMP AP device levels**.



### Note

The Import Device configuration is supported only for the Access and Backhaul account and is applicable only on ePMP/PMP AP and SM devices.

The following parameters are supported for ePMP/PMP AP in the CSV file:

- Latitude
- Longitude
- Height
- Azimuth
- Elevation
- Beam Width

The following parameters are supported for ePMP/PMP SM is in the CSV file:

- Latitude
- Longitude

| Device                           | Type         | IP Address     | Health               | Serial Number | Description | Onboarded  | Active S/W V... |
|----------------------------------|--------------|----------------|----------------------|---------------|-------------|------------|-----------------|
| E500-B39748<br>00:04:56:B3:97:48 | cnPilot e500 | 10.110.220.123 | Online<br>0d 13h 19m | W8SE1796WD9K  |             | 0d 16h 2m  | 4.0-b11         |
| E500-919DCA<br>00:04:56:91:9D:CA | cnPilot e500 | 10.110.222.212 | Online<br>0d 17h 8m  | W8SK02264577  |             | 0d 21h 41m | 3.11.3-b9       |
| E500-917644<br>00:04:56:91:76:44 | cnPilot e500 | 10.110.220.103 | Online<br>0d 17h 8m  | W8SK01DL2MLB  |             | 0d 21h 41m | 3.11.3-b9       |
| F400-B67566<br>00:04:56:B6:75:66 | cnPilot e400 | 10.110.220.120 | Online<br>0d 17h 8m  | W8SF092899LS  |             | 0d 21h 41m | 3.11.3-b9       |
| F400-AE28DA<br>00:04:56:AE:28:DA | cnPilot e400 | 10.110.220.241 | Online<br>0d 17h 8m  | W8RK57642P4S  |             | 0d 21h 41m | 3.11.3-b9       |

Figure 82 Import Device Configuration

## Sample Configuration File

| MAC   | LATITUDE                         | LONGITUDE                        | AZIMUTH                       | ELEVATION                        | BEAM WIDTH            | HEIGHT                   | HEIGHT UNIT |
|---|----------------------------------|----------------------------------|-------------------------------|----------------------------------|-----------------------|--------------------------|-------------|
| Supports formats with ':', '-', 'no space', upper and lower case. | Signed degrees format (DDD.ddd). | Signed degrees format (DDD.ddd). | Degrees from North (0 to 360) | Degrees from horizon (-90 to 90) | Degrees from 1 to 360 | Min=0, Max=5 Meters/Feet |             |
| 01:14:56:CA:E6:25   | 16                               | 19                               | 17                            | 17                               | 130                   | 1500                     | Feet        |
| 01-14-56-C4-C3-2e   | -90                              | 119.0123                         | 190                           | 64                               | 120                   | 1000                     | feet        |
| 0a113e84260D  | 79.0123                          | 11                               | 111                           | 74                               | 112                   | 110                      | Meters      |
| 0a:11:3e:b1:2a:78   | -44                              | -12.78                           | 124                           | 67                               | 177                   | 190                      | meters      |

Figure 83 Sample configuration file

## Uploading a Configuration File

To upload a configuration file (CSV) as per the format specified in the sample template:

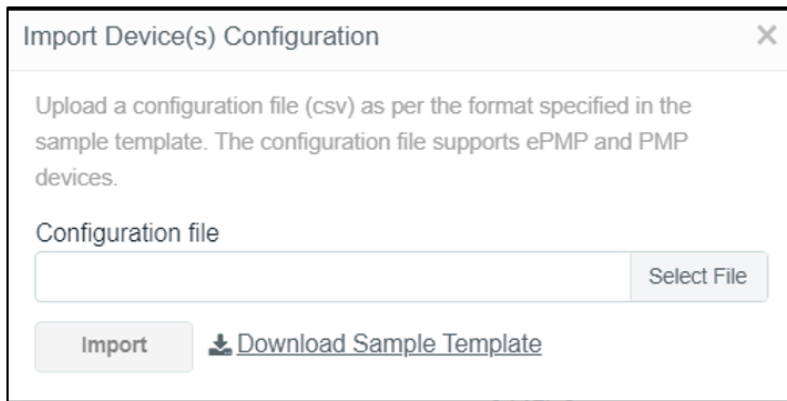
1. Download Sample Template or prepare a sheet in CSV file format with necessary column details.
2. Upload a configuration file (CSV) as per the format specified in the sample template.



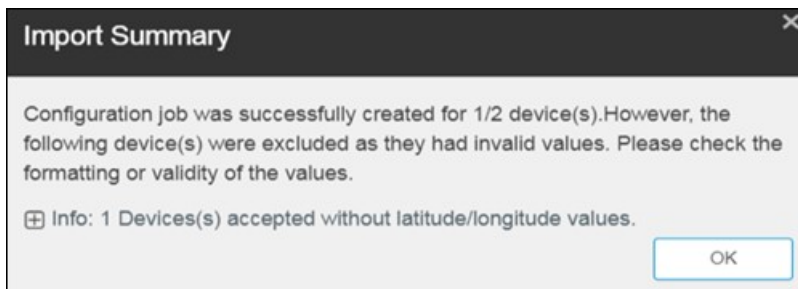
**Note**

You must know the MAC address of the device to push the configuration.

3. Click Import to import the configuration.



4. A configuration job will be created in the tower page.



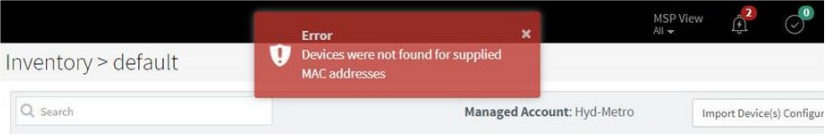
5. You can view the completed status of import device (s) configuration in the Managed Account page.

| ID  | Details                                 | Managed Account     | Target             | Created by     | Created on         | Completed on       | Parallel | Stop on Error | Sector Priority | Status  |
|-----|---|---------------------|--------------------|----------------|--------------------|--------------------|----------|---------------|-----------------|---|
| 205 | 1 cnPilot R195W device(s)               | Base Infrastructure |                    | Administrator  | Jun 14, 2019 10:36 | Jun 14, 2019 10:36 | -        | false         | N/A             | Completed: <span style="width: 100%;"></span> |
| 204 | 1 cnPilot R195W device(s)               | Base Infrastructure |                    | Administrator  | Jun 13, 2019 18:16 | Jun 13, 2019 18:16 | -        | false         | N/A             | Completed: <span style="width: 100%;"></span> |
| 203 | 1 cnPilot R195W device(s)               | Base Infrastructure | 8-195W-APgrp       | Administrator  | Jun 13, 2019 18:12 | Jun 13, 2019 18:12 | -        | false         | N/A             | Completed: <span style="width: 100%;"></span> |
| 4   | 1 cnPilot Enterprise (E-Series) devi... | Managed-Account-Use | MX-Client          | RgvAdmin Lo... | Jun 13, 2019 16:54 | Jun 13, 2019 16:54 | 10       | false         | N/A             | Completed: <span style="width: 100%;"></span> |
| 3   | 1 cnPilot Enterprise (E-Series) devi... | Managed-Account-Use | Default Enterprise | RgvAdmin Lo... | Jun 13, 2019 15:57 | Jun 13, 2019 15:58 | 10       | false         | N/A             | Completed: <span style="width: 100%;"></span> |
| 202 | 1 cnPilot R195W device(s)               | Base Infrastructure | 8-195W-APgrp       | Administrator  | Jun 13, 2019 15:41 | Jun 13, 2019 15:41 | -        | false         | N/A             | Completed: <span style="width: 100%;"></span> |
| 201 | 1 cnPilot R195W device(s)               | Base Infrastructure | 8-195W-APgrp       | Administrator  | Jun 13, 2019 15:21 | Jun 13, 2019 15:22 | -        | false         | N/A             | Completed: <span style="width: 100%;"></span> |
| 200 | 1 device(s)                             | Base Infrastructure |                    | Auto-Sync      | Jun 13, 2019 14:32 | Jun 13, 2019 14:32 | 15       | false         | N/A             | Completed: <span style="width: 100%;"></span> |
| 199 | 1 device(s)                             | Base Infrastructure |                    | Auto-Sync      | Jun 13, 2019 14:29 | Jun 13, 2019 14:29 | 15       | false         | N/A             | Completed: <span style="width: 100%;"></span> |
| 198 | 1 cnPilot R190V device(s)               | Base Infrastructure | Test_Router        | Administrator  | Jun 13, 2019 14:26 | Jun 13, 2019 14:26 | -        | false         | N/A             | Completed: <span style="width: 100%;"></span> |

The following table provides details on different errors that might occur while importing a CSV file:

**Table 25 Error list**

| Error   | Description   |
|---|---|
| <p>Error1:<br/>Error: {Count of Devices} Device(s) with invalid MAC</p>     | <p>This error is displayed if the uploaded CSV file contains invalid MAC Address.</p>   |
| <p>Error2:<br/>{Count of Devices} Device(s) skipped due to invalid data</p> | <p>This error is displayed if the uploaded CSV file contains invalid Data or data not relevant for Latitude, Longitude, Azimuth, Height, and Elevation.</p> |

| Error   | Description  |
|---|--|
| <p>Error3:<br/>Devices were not found for supplied MAC Address</p>              | <p>This error message is displayed if the devices were not found with the supplied MAC address in the CSV file.</p>  <p>The screenshot shows a web interface with a red error dialog box in the center. The dialog box contains the text: "Error" followed by a close button (X) and "Devices were not found for supplied MAC addresses". The background interface includes a breadcrumb "Inventory &gt; default", a search bar, and a button labeled "Import Device(s) Configur".</p> |
| <p>Error4:<br/>Info: 1 Device(s) accepted without latitude/longitude values</p> | <p>This error is displayed when the latitude and longitude values are tried to push on to ePMP AP or PMP AP which are under a Tower.</p>   |



# Chapter 11: Fixed Wireless Configuration

---

This chapter provides the following information:

- [Overview](#)
- [Template](#)
- [Configuration Update](#)
- [Jobs](#)
- [Onboarding Configuration Update](#)

## Overview

Template configuration is supported for ePMP, PMP, and cnReach devices. Templates are textual representations of device settings that contain a full configuration or partial configuration. When a template is applied to a device, the only parameters changed are those in the template.

The graphic below presents the basic template configuration flow:

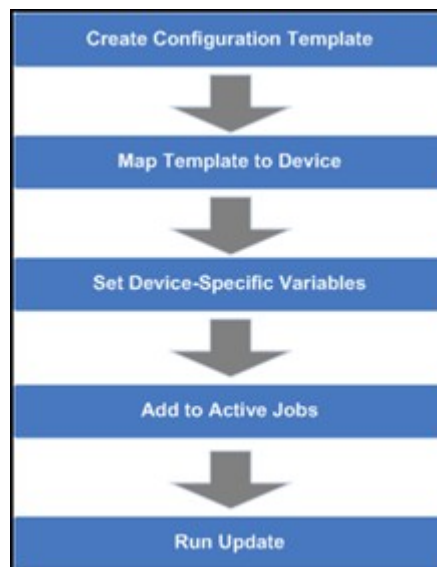


Figure 84 Basic Template Configuration Flow

## Configuration Templates

Templates can be pushed to a device manually through a configuration job. This is accomplished in the configuration management page. Templates can also be applied prior to onboarding, in which they would be provisioned in the Onboarding Queue.

Some sample templates are listed below. The ellipses (...) represent additional content that has been excised from the example to limit the size of the text.

## Sample ePMP Template

The ePMP template uses the exported ePMP configuration format, which is JSON-encoded.

```

"device_props": {
  "acsEnable": "0",
  "acsScanMinDwellTime": "200",
  "acsScanMaxDwellTime": "300",
  "acsControl": "0",
  "bcPriority": "0",
  "cambiumInternetConnectionServerIP": "",
  "centerFrequency": "5670",
  "dataVLANEnable": "0",
  "dataVLANVID": "",
  ...
  "snmpTrapTable": [{
    "snmpTrapEntryIP": "10.120.143.176",
    "snmpTrapEntryPort": "162"
  }],
  ...
}

```

Figure 85 Sample ePMP Template

## Configuration Variables

Administrators can embed variables into templates that will be replaced when the template is applied to a device. This allows one to leverage a shared, generic template, but to tailor it to individual devices when it is pushed.

Template variables are added to a configuration file by replacing an existing parameter with a customer-defined string of the format `${VARIABLE}`. An example configuration line with a single variable replacement is shown below:

```
"networkLanIPAddr": ${IP ADDRESS}
```

The above variable is named `IP_ADDRESS`. When the template is pushed to a device, this variable will be replaced with a value specific to the device. This value needs to be set for the device prior to the template application, else the configuration will not be pushed. Default values can also be specified for variables, as shown below:

```
"networkLanIPAddr": ${IP ADDRESS="10.1.1.254"},
```

The default value is `"10.1.1.254"`. In this case, if the variable is not set for a device, the default value will be used.

## Variable Usage

The graphic below highlights how Templates and Variables are merged to create the final configuration that is pushed to the device.

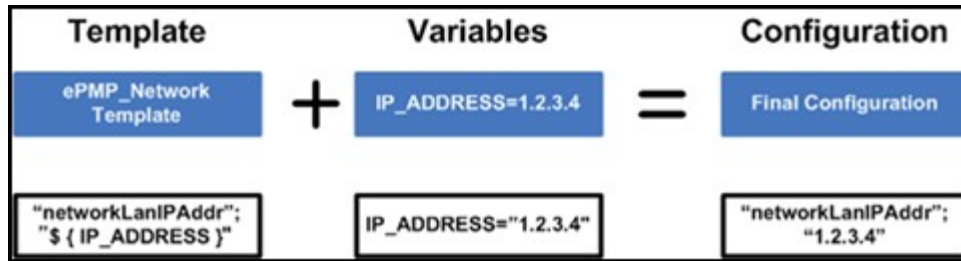


Figure 86 Variable Usage

## Macros

Macros can be used in templates similar to configuration variables except they automatically take values provided by the device itself.

- `%{ESN}` will be replaced with the device's MAC address
- `%{MSN}` will be replaced with the device's Serial Number

## Variable Caching

Variables set for a particular device will be cached, so they can be re-used later. This means the next time you apply a template that leverages a variable with the same name as one used previously, its value will be pre-populated with the previous value. It is therefore beneficial to define a uniform variable naming and usage scheme for variables across different templates.

## Device Type-Specific Configurations

The format and values of a configuration template are unique to the different device types. Templates that work with one type of device will not work with others, and all templates need to be mapped to a specific device type upon creation.

## Device Mode Restrictions

Some devices, such as ePMP, executes in AP and SM modes. The ePMP templates can be configured so they can only be applied to devices that support a selected mode.

## Variable Validation

All variables for a selected template must be mapped to a value in order to create a configuration job. If any variables are not mapped, an error will be generated. Variables that have default settings will not cause an error if they are unset.

## Sample Templates

A number of sample templates are provided for each device type. These are not meant to be applied directly, but rather serve as an example of the configuration data format accepted by the device. Please see the documentation for your devices for full details.

## Template File Creation

The typical process taken for creating your own configuration template text from scratch are below.

1. On a test device configure the parameters you are interested in pushing to devices with values that will be easy to search for. This can be done directly on the device web UI.
2. Export the device configuration. Via cnMaestro c4000 Controller this is done by navigating to Configuration > Templates, selecting the device in the left-hand tree and then clicking the View Device Configuration link. This can also be done via the device web GUI, typically in the Administration or Operations section where there will be an Export button for configuration.
3. View the configuration file in a text editor like Notepad++ and search for the values you entered in step 1. You can also search for the parameter name to try to find the correct lines.
4. Copy and paste the relevant lines into a new file.
5. Optionally Replace values with replacement variable text. This will allow you to set the value per device.
6. Once you have this partial template it can be copied into the template creation text field and saved.

## Template

To create a configuration template:

1. Navigate to Configuration > Templates in the main menu.
2. Click the Add Template button.
3. Choose a Device Type, Name, and Description for the template. For ePMP templates, you should select a Device Mode.
4. Either upload your template into the UI or paste the template text into the text area.
5. After clicking Save, the template will be available in the selection menu on the configuration and onboarding pages, if the device type and mode match the device selected.
6. By selecting the Custom option under Template type filter All Default templates will be hidden.



### Note

When you navigate to the Template page default template type filter will be custom. User needs to select All or Default in order to view other templates.

## Configuration Update

### Device Selection

First navigate to the Configuration Update page, then navigate the Device Tree to the appropriate level for device selection. For example, selecting an AP will enable the selection of the AP and all its SMs.

## Device Type

Configuration jobs are created for a single device type. The type includes the specific hardware (ePMP, PMP) as well as the mode of the device (PMP or PTP mode for ePMP for example).

## Device Table

Select the devices to upgrade in the Devices Table. The following parameters are visible in the table:

**Table 26 Parameters Displayed in the Device Table**

| Parameter     | Description   |
|---------------|---|
| Devices       | The names of available devices in a system. The list is pre-filtered based upon the node selected in the Device Tree. |
| Status        | The status of a particular device in a system. Devices that are “Down” cannot have images pushed to them.             |
| Network/Tower | The network and the tower on which the device is located.   |



### Note

You can save and download the existing device configuration as a template by clicking the View Device Configuration link.

## Options

### Stop all Configuration on a Critical Error

If one of the configuration updates fails, then don't start any additional updates and instead pause the update job. All existing, concurrent updates will be allowed to proceed until completion. The administrator will be able to continue the update where it left off.

### Parallel Upgrades

Define how many configuration updates to perform in parallel.

### Start Job Now

If enabled, attempts to automatically start the configuration job immediately after creation.

### Update Ordering

It allows you to specify update ordering within a sector. Options are SMs first and then AP or AP first and then SMs.

### Abort Configuration

Abort operation will skip devices that are waiting for an update to begin. Devices already that are being updated may continue but cnMaestro c4000 Controller will stop tracking their progress. Aborting a

Configuration Job puts the device into a complete state that cannot be manually restarted by the user. The pending devices will not begin their updates.

| ID   | Details                   | Managed Account     | Target             | Created by    | Created on         | Completed on       | Parallel | Stop on Error | Sector Priority | Status     |
|------|---------------------------|---------------------|--------------------|---------------|--------------------|--------------------|----------|---------------|-----------------|------------|
| 3990 | 1 cnPilot e700 device(s)  | Base Infrastructure | Default Enterprise | Administrator | Apr 16, 2019 19:15 | Apr 16, 2019 19:15 | -        | false         | N/A             | Aborted:   |
| 3989 | 1 cnPilot R200P device(s) | Base Infrastructure | Default Home       | Administrator | Apr 16, 2019 13:33 | Apr 16, 2019 13:33 | -        | false         | N/A             | Completed: |
| 3988 | 1 cnPilot e700 device(s)  | Base Infrastructure | 202_APGROUP        | Administrator | Apr 16, 2019 13:32 | Apr 16, 2019 13:33 | -        | false         | N/A             | Completed: |
| 3987 | 1 cnPilot e400 device(s)  | Base Infrastructure | 45_APGROUP         | Administrator | Apr 16, 2019 12:03 | Apr 16, 2019 12:04 | -        | false         | N/A             | Completed: |
| 3986 | 1 cnPilot e500 device(s)  | Base Infrastructure |                    | Administrator | Apr 15, 2019 16:14 | Apr 15, 2019 16:15 | -        | false         | N/A             | Completed: |
| 3985 | 3 device(s)               | Base Infrastructure |                    | Auto-Sync     | Apr 15, 2019 16:13 | Apr 15, 2019 16:14 | 15       | false         | N/A             | Completed: |
| 3984 | 3 device(s)               | Base Infrastructure |                    | Auto-Sync     | Apr 15, 2019 16:12 | Apr 15, 2019 16:13 | 15       | false         | N/A             | Completed: |
| 3983 | 3 device(s)               | Base Infrastructure |                    | Auto-Sync     | Apr 15, 2019 16:07 | Apr 15, 2019 16:08 | 15       | false         | N/A             | Completed: |
| 3982 | 1 cnPilot e400 device(s)  | Base Infrastructure |                    | Administrator | Apr 15, 2019 16:07 | Apr 15, 2019 16:07 | -        | false         | N/A             | Completed: |
| 3981 | 3 device(s)               | Base Infrastructure |                    | Auto-Sync     | Apr 15, 2019 16:06 | Apr 15, 2019 16:07 | 15       | false         | N/A             | Completed: |

Figure 87 Abort Configuration



**Note**

1. Devices that are already completed display as "completed" with a message "update complete" along with the status as Completed.
2. Devices which are ongoing display as "Aborted" with a message "Manually Aborted" with the status as Aborted.
3. Devices that have not yet started display as "skipped" with a message "job was aborted" with the status as Skipped.

## Configuration Upgrade Steps

To upgrade the configuration of an ePMP (Sectors) device:

1. Navigate to Manage > Configuration > Device Details in the main menu.
2. Navigate to System > Network in the Device Tree. From the list of available networks, select a network in which the device belongs.
3. Select ePMP (Sectors) from the following Device Type drop-down list:
  - a. cnMatrix
  - b. cnPilot Enterprise (E-Series)
  - c. cnPilot Enterprise (ePMP Hotspot)
  - d. cnPilot Home (R-Series)
  - e. cnReach
  - f. ePMP (Sectors)
  - g. PMP (Sectors)
  - h. PTP
4. Select the configuration template to upgrade from the Template drop-down list.
5. Select the device(s) to upgrade by clicking the tick icon.

6. Set any variables that are required for selected devices by clicking the gear icon under the "Configure" column on the right side of the table. The configuration upgrade cannot proceed until all required variables (those without default parameters) are set. If you attempt to create a configuration job without setting required variables, the gear icon will turn red for any devices not meeting this requirement.
7. Click the Apply Configuration button.



**Note**

You can save and download the existing device configuration as a template by clicking the View Device Configuration link.

## Jobs

Appliance > Jobs > Configuration Update tab lists all currently running, queued and completed jobs. The jobs can be triggered immediately or run later.

The following table displays the list of parameters in the Jobs tab:

**Table 27 Parameters displayed in the Configuration Update tab**

| Parameter   | Description  |
|---|--|
| ID  | Identification number of the active job.   |
| Details   | Count of devices and date and time the upgrade process is initiated.   |
| Target  | Target software version to upgrade.  |
| Created By  | The user who has created this job.   |
| Created On  | Date and time on which the job is created.   |
| Parallel  | Number of device to start in parallel.   |
| Stop on Error   | Stop the job, if any device in the middle finds any error.   |
| Sector Priority   | For ePMP/PMP, the priority of AP/SM to start.  |
| Status  | Status of update.  |
| Action  | Use the Start or Delete button to manage the upgrade process. After the upgrade has started, the Pause button will stop new upgrades from the beginning. If the upgrade process fails or the upgrade has been paused, you can restart the process by clicking the Resume button. |
| By selecting the Show More icon, you can view the following parameters: |  |
| Device  | Device for which the upgrade is initiated.   |

| Parameter | Description                             |
|-----------|---|
| Status    | Status of the device.                   |
| Result    | The upgrade status of the device.       |
| Message   | The message displayed after the update. |

## Onboarding Configuration Update

Administrators can apply the configuration to devices during the onboarding process: prior to approving the device in the Onboarding Queue, the configuration template and variables can be specified. These will then be pushed to the device during onboarding. For more details on onboarding, see [Device Onboarding](#).



# Chapter 12: Wireless LAN Configuration

---

Wi-Fi configuration is handled through AP Groups (Fixed Wireless devices, such as ePMP and PMP, use Templates).

This chapter provides the following details:

- [cnPilot Home and Enterprise](#)
- [Association ACL](#)

## cnPilot Home and Enterprise

This section provides the following details:

Configure cnPilot using cnMaestro c4000 Controller

- [Create an AP Group](#)
- [Pre-Defined Overrides](#)
- [User-Defined Overrides \(Advanced\)](#)
- [User-Defined Variables \(Advanced\)](#)

There are two types of cnPilot devices:

1. cnPilot Enterprise is supported by cnPilot e-Series and ePMP 1000 Hotspot devices.
2. cnPilot Home by cnPilot R-Series devices.

Each WLAN or AP Group, prior to creation, is mapped to one of these device categories and can only be used with supported device types. Two categories are required because the features available in Enterprise and Home are different.

## Configure cnPilot using cnMaestro c4000 Controller

cnPilot devices are configured by creating an AP Group, mapping it to shared WLANs, and then assigning it to a particular device through the Configuration page. Once assigned, the configuration is pushed automatically if Auto-Sync is enabled, or manually if disabled (this requires manual sync).

### Auto Synchronization

AP Groups can automatically synchronize device configuration whenever the AP Group or associated WLANs are updated. This is done by enabling Auto Sync in the AP Group configuration page.

### Manual Synchronization

When a device is mapped to an AP Group without Auto-Sync turned on, the device will be placed in an unsynchronized state until it is manually synchronized. This can be done by navigating to the device Configuration page and clicking the Sync Now button, or by navigating to the Sync Configuration page (Appliance > Sync Configuration).

The process for creating a Wi-Fi device configuration is as follows:

1. Navigate to Shared Settings > WLANs and AP Groups.
2. Create an AP Group.
3. Select an AP Group Type. The choices are cnPilot Home (which represents the R-Series) and cnPilot Enterprise (which maps to the E-Series and ePMP Hotspot). The configuration options depend upon the AP Group Type. (Note the Wireless LAN view supports cnPilot Enterprise devices, so the cnPilot Home Device Type is not available.)
4. Assign WLANs to the AP Group (you may want to update WLAN SSID and security parameters during this step).
5. Map Devices to an AP Group by selecting the AP Group in the Device Configuration screen.

AP Groups support all Wi-Fi devices, including cnPilot R190/200/201, cnPilot E400/E410/E500, and ePMP 1000 Hotspot.

## Creating a WLAN

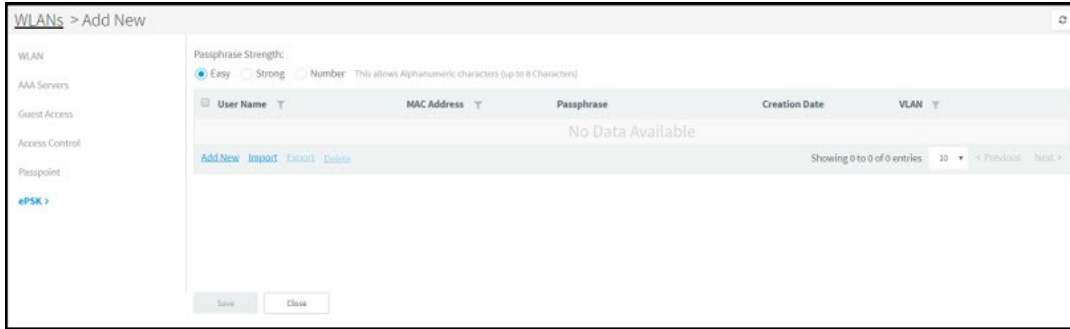
To create a WLAN, navigate to Shared Settings > WLAN and AP Groups (or the WLAN page in the Wireless LAN View) and select New WLAN. As with AP Groups, WLANs are separated into cnPilot Home and cnPilot Enterprise types. cnPilot Enterprise WLANs are able to configure WLAN, RADIUS, Guest Access, Usage Limits, Scheduled Access, and Access parameters. cnPilot Home WLANs can configure SSID, Scheduled Access, and Access parameters.

Steps to create WLAN policy:

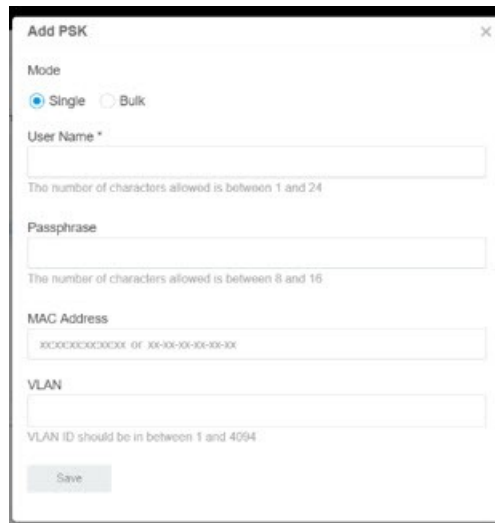
1. From homepage navigate to **Shared Settings > WLANs and AP Groups**.
2. Click Add WLAN, provide basic parameters to WLAN, and ensure WPA2 Pre-Shared keys are enabled in Security drop-down.

The screenshot shows the 'WLANs > Add New' configuration page. On the left is a navigation menu with 'WLAN >' selected. The main content area is split into two sections: 'Basic Information' and 'Basic Settings'.  
**Basic Information:**  
 - Type\*: cnPilot Enterprise (E-Series, ePMP Hotspot)  
 - Name\*: Cambium-WiFi  
 - Description: EPSK Feature  
**Basic Settings:**  
 - SSID\*: Cambium-WiFi (The SSID of this WLAN (up to 32 characters))  
 - Enable:   
 - Mesh: Off (Mesh Base/Client/Recovery mode)  
 - VLAN\*: 1 (Default VLAN assigned to clients on this WLAN (1-4094))  
 - Security: WPA2 Pre-Shared Keys (Set authentication and encryption type)  
 - Passphrase\*: [masked] (WPA2 Pre-shared security passphrase or key)  
 - Radios: 2.4GHz and 5GHz (Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported)  
 - Client Isolation: Disable (When selected, it allows wireless clients connected to the same AP or different APs to communicate with each other in the same VLAN)  
 - cnMaestro Managed Roaming:  Enable centralized management of roaming for wireless clients through cnMaestro

3. Click Save.
4. Navigate to ePSK tab. Select the Passphrase Strength as Easy or Strong or Number.



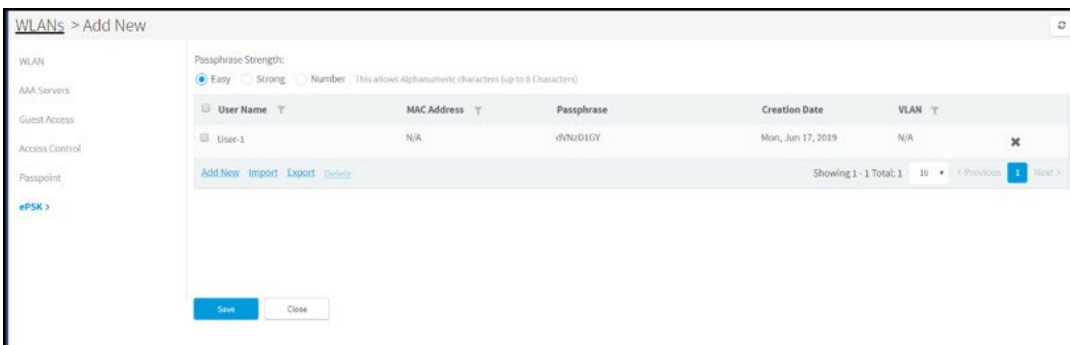
5. Click Add New. The Add PSK window pops-up where you can select the Mode as either Single or Bulk. In Single Mode Username is mandatory and the rest of the entries are optional.



**Note**

The passphrase is optional and it will be automatically generated based on the selected passphrase strength.

6. In Single Mode, we can see a single entry only.



7. In Bulk Mode, Count and Username Prefix are mandatory fields. Enter the Count and Username Prefix.

**Add PSK**

Mode  
 Single  Bulk

Count\*  
  
This allows value between 2 and 1024

User Name Prefix\*  
  
Username and Passphrase will be auto generated i.e prefix.1

VLAN  
  
Use comma "," separated VLANs. You can use "-" to provide a range also.

Save

8. In Bulk Mode, we can see many entries.

WLANs > Add New

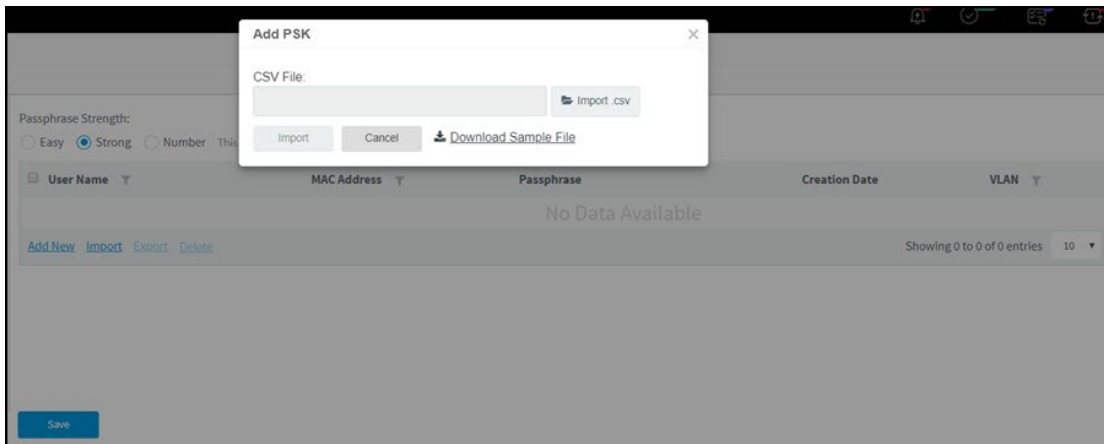
Passphrase Strength:  
 Easy  Strong  Number This allows Alphanumeric and Special Characters (up to 16 Characters)

| User Name | MAC Address | Passphrase        | Creation Date     | VLAN |
|-----------|-------------|-------------------|-------------------|------|
| Room-10   | N/A         | 6wK63P-%&Tka76a   | Mon, Jun 17, 2019 | N/A  |
| Room-9    | N/A         | BEzjDFK*8Q5-m+    | Mon, Jun 17, 2019 | N/A  |
| Room-8    | N/A         | ]Kj@]H-(9wHsde*p  | Mon, Jun 17, 2019 | N/A  |
| Room-7    | N/A         | W4(U-m]1][DZB@Y   | Mon, Jun 17, 2019 | N/A  |
| Room-6    | N/A         | R6aEAFb3yn36-b6   | Mon, Jun 17, 2019 | N/A  |
| Room-5    | N/A         | t+5:QI~sa45;RG    | Mon, Jun 17, 2019 | N/A  |
| Room-4    | N/A         | dZs1>3g@4mw-Z[    | Mon, Jun 17, 2019 | N/A  |
| Room-3    | N/A         | gr[(@_!%+45XZIG-T | Mon, Jun 17, 2019 | N/A  |
| Room-2    | N/A         | &N6K90GzyUw(RQ    | Mon, Jun 17, 2019 | N/A  |
| Room-1    | N/A         | yNFF4j]ggD)MhW#B  | Mon, Jun 17, 2019 | N/A  |

Showing 1 - 10 Total: 10

Import ePSK

1. Click **Import**. A dialogue box appears.
2. Select **import.csv** and import the file.



- When you click **Download Sample File**, you can see the Sample ePSK excel sheet.

|    | A           | B   | C  | D  | E | F | G | H | I |
|----|-------------|---|--|--|---|---|---|---|---|
| 1  | username    | mac   | passphrase   | vlan   |   |   |   |   |   |
| 2  | Unique name | MAC address of the client,if any (optional) | The Passphrase (Pre Shared Key) to be used in the WPA2 handshake | The VLAN to which the client traffic should be mapped (optional) |   |   |   |   |   |
| 3  | Lounge-1    | 11:11:11:11:11:11                           | 6-46]h]6ab;^B{(:   | 9  |   |   |   |   |   |
| 4  | Lounge-2    | 22:22:22:22:22:22                           | 9jdf];q]*38GU53%   | 10   |   |   |   |   |   |
| 5  | Lounge-3    |   | *{;{;nQg=UdeM2ErR  | 1  |   |   |   |   |   |
| 6  | Lounge-4    |   | ]jzam4F1]x]Zgg%  | 2  |   |   |   |   |   |
| 7  |             |   |  |  |   |   |   |   |   |
| 8  |             |   |  |  |   |   |   |   |   |
| 9  |             |   |  |  |   |   |   |   |   |
| 10 |             |   |  |  |   |   |   |   |   |
| 11 |             |   |  |  |   |   |   |   |   |
| 12 |             |   |  |  |   |   |   |   |   |

Export ePSK

- Click **Export**. A dialogue box appears.
- Select **export.csv** and export the file.

The screenshot shows the 'WLANs > Cambium-WiFi' configuration page. On the left, there is a navigation menu with 'ePSK' selected. The main area displays a table of ePSK configurations. The table has columns for 'User Name', 'MAC Address', 'Passphrase', 'Creation Date', and 'VLAN'. There are 10 rows, each representing a different room (Room-1 to Room-10). At the bottom of the table, there are buttons for 'Add New', 'Import', 'Export', and 'Delete'. The 'Export' button is highlighted with a red box.

- When you click **Download Sample File**, you can see the Sample ePSK excel sheet.

|    | A           | B           | C                    | D  | E | F | G | H | I |
|----|-------------|-------------|----------------------|--|---|---|---|---|---|
| 1  | username    | mac         | passphrase           | vlan   |   |   |   |   |   |
| 2  | Unique name | MAC address | The Passphrase       | The VLAN to which the client traffic should be mapped (optional) |   |   |   |   |   |
| 3  | Room-1      |             | WVghr8SmY_a;;Q(e     |  |   |   |   |   |   |
| 4  | Room-2      |             | a{n5&amp;Hepk]~Qt%,  |  |   |   |   |   |   |
| 5  | Room-3      |             | 6q@Qk#WU8JzC.Br)     |  |   |   |   |   |   |
| 6  | Room-4      |             | eX~g!n!s]j]tZw[j     |  |   |   |   |   |   |
| 7  | Room-5      |             | y\$csqds{!YAw5gJ;p   |  |   |   |   |   |   |
| 8  | Room-6      |             | j;Ag]EBKk8kNRS*c     |  |   |   |   |   |   |
| 9  | Room-7      |             | 8H(\$F}u;m9C4_MQ=    |  |   |   |   |   |   |
| 10 | Room-8      |             | _(hgH7;dzb]Ys~9w     |  |   |   |   |   |   |
| 11 | Room-9      |             | 7%[C5bqDMpt^(]2]     |  |   |   |   |   |   |
| 12 | Room-10     |             | 3mq=xY~zg&amp;fn!mN% |  |   |   |   |   |   |

Delete ePSK

To delete ePSK, select the ePSK and click **Delete**.

WLANs > Add New

Passphrase Strength:  Easy  Strong  Number This allows Alphanumeric and Special Characters (up to 16 Characters)

| User Name                                     | MAC Address | Passphrase        | Creation Date     | VLAN |   |
|---|-------------|-------------------|-------------------|------|---|
| <input checked="" type="checkbox"/> Lounge-10 | N/A         | v=64z{7k7CseHv    | Mon, Jun 24, 2019 | N/A  | ✕ |
| <input checked="" type="checkbox"/> Lounge-9  | N/A         | trgB+{j8R4D;c-n   | Mon, Jun 24, 2019 | N/A  | ✕ |
| <input checked="" type="checkbox"/> Lounge-8  | N/A         | ]5T-]WHP]]-@ d    | Mon, Jun 24, 2019 | N/A  | ✕ |
| <input checked="" type="checkbox"/> Lounge-7  | N/A         | U EYhEcn{RkK}Me   | Mon, Jun 24, 2019 | N/A  | ✕ |
| <input checked="" type="checkbox"/> Lounge-6  | N/A         | dz2kQ3;Bffx>Df    | Mon, Jun 24, 2019 | N/A  | ✕ |
| <input checked="" type="checkbox"/> Lounge-5  | N/A         | pgH{C SPGRavg @+3 | Mon, Jun 24, 2019 | N/A  | ✕ |
| <input checked="" type="checkbox"/> Lounge-4  | N/A         | KWFM-g3 ~5 _6DQe  | Mon, Jun 24, 2019 | N/A  | ✕ |
| <input checked="" type="checkbox"/> Lounge-3  | N/A         | 5 Sp_&43cva MM    | Mon, Jun 24, 2019 | N/A  | ✕ |
| <input checked="" type="checkbox"/> Lounge-2  | N/A         | MouKng\$MAntF}M   | Mon, Jun 24, 2019 | N/A  | ✕ |
| <input checked="" type="checkbox"/> Lounge-1  | N/A         | + _C 666m~>Q6_K   | Mon, Jun 24, 2019 | N/A  | ✕ |

Add New Import Export Delete

Showing 1 - 10 Total: 10 10 < Previous 1 10

Save Close



### Note

You can group select or individually select ePSK entry and delete the same.



### Note

ePSK feature is supported on cnPilot from system release 3.11.1.

## Create an AP Group

To create an AP Group,

1. Navigate to **Configuration > WLAN AP Groups page > AP Group tab**.
2. Click the **New AP Group** tab.
3. Enter values for AP Group name, Country name, and WLAN parameters.
4. Click Add WLAN and select WLAN from the list.
5. Click **Save**.

## Map WLANs to AP Groups

WLANs are added to AP Groups in the AP Group configuration. Ensure that the WLANs are ordered correctly if Mesh mode is used.

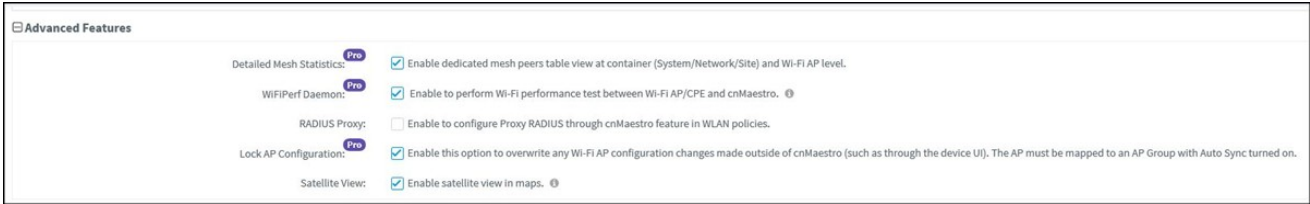


### Note

A maximum of 16 WLAN policies are supported for E430W/E400/E500 and 8 WLAN policies are supported for ePMP 1000 Hotspot.

## Lock AP Configuration

This feature supports automatically restoring the configuration of devices to their mapped AP Group if their configuration is changed outside of cnMaestro. When this feature is enabled in cnMaestro c4000 Controller, the configurations changed from the UI or CLI of the device are reverted back by pushing the existing AP Group configuration. The configuration will get pushed only if the device is in-sync status.



To enable this feature:

1. Navigate to **Appliance > Settings > Advanced Features** page.
2. Enable the **Lock AP Configuration** checkbox.
3. Click **Save**.

When a configuration change is made on the device via its UI or CLI, cnMaestro c4000 Controller detects the change as Device's configuration changed outside of cnMaestro c4000 Controller and the device is marked as Not In Sync. In this scenario, an Auto-Sync job is triggered automatically by cnMaestro c4000 Controller to revert the changes.

The Auto-Sync job can be viewed in **Appliance > Jobs > Configuration Update** page.

| ID   | Details                  | Managed Account     | Target              | Created by    | Created on         | Completed on       | Parallel | Stop on Error | Sector Priority | Status   |
|------|--------------------------|---------------------|---------------------|---------------|--------------------|--------------------|----------|---------------|-----------------|--|
| 3986 | 1 cnPilot e500 device(s) | Base Infrastructure | Base Infrastructure | Administrator | Apr 15, 2019 16:14 | Apr 15, 2019 16:15 | -        | false         | N/A             | Completed: <span style="width: 100%; background-color: green;"></span> |
| 3985 | 3 device(s)              | Base Infrastructure | Base Infrastructure | Auto-Sync     | Apr 15, 2019 16:13 | Apr 15, 2019 16:14 | 15       | false         | N/A             | Completed: <span style="width: 100%; background-color: green;"></span> |
| 3984 | 3 device(s)              | Base Infrastructure | Base Infrastructure | Auto-Sync     | Apr 15, 2019 16:12 | Apr 15, 2019 16:13 | 15       | false         | N/A             | Completed: <span style="width: 100%; background-color: green;"></span> |
| 3983 | 3 device(s)              | Base Infrastructure | Base Infrastructure | Auto-Sync     | Apr 15, 2019 16:07 | Apr 15, 2019 16:08 | 15       | false         | N/A             | Completed: <span style="width: 100%; background-color: green;"></span> |
| 3982 | 1 cnPilot e400 device(s) | Base Infrastructure | Base Infrastructure | Administrator | Apr 15, 2019 16:07 | Apr 15, 2019 16:07 | -        | false         | N/A             | Completed: <span style="width: 100%; background-color: green;"></span> |
| 3981 | 3 device(s)              | Base Infrastructure | Base Infrastructure | Auto-Sync     | Apr 15, 2019 16:06 | Apr 15, 2019 16:07 | 15       | false         | N/A             | Completed: <span style="width: 100%; background-color: green;"></span> |
| 3980 | 3 device(s)              | Base Infrastructure | Base Infrastructure | Auto-Sync     | Apr 15, 2019 16:04 | Apr 15, 2019 16:04 | 15       | false         | N/A             | Completed: <span style="width: 100%; background-color: green;"></span> |
| 3979 | 3 device(s)              | Base Infrastructure | Base Infrastructure | Auto-Sync     | Apr 15, 2019 16:01 | Apr 15, 2019 16:02 | 15       | false         | N/A             | Completed: <span style="width: 100%; background-color: green;"></span> |
| 3978 | 1 device(s)              | Base Infrastructure | Base Infrastructure | Auto-Sync     | Apr 15, 2019 15:56 | Apr 15, 2019 15:56 | 15       | false         | N/A             | Completed: <span style="width: 100%; background-color: green;"></span> |
| 3977 | 1 device(s)              | Base Infrastructure | Base Infrastructure | Auto-Sync     | Apr 15, 2019 15:51 | Apr 15, 2019 15:51 | 15       | false         | N/A             | Completed: <span style="width: 100%; background-color: green;"></span> |

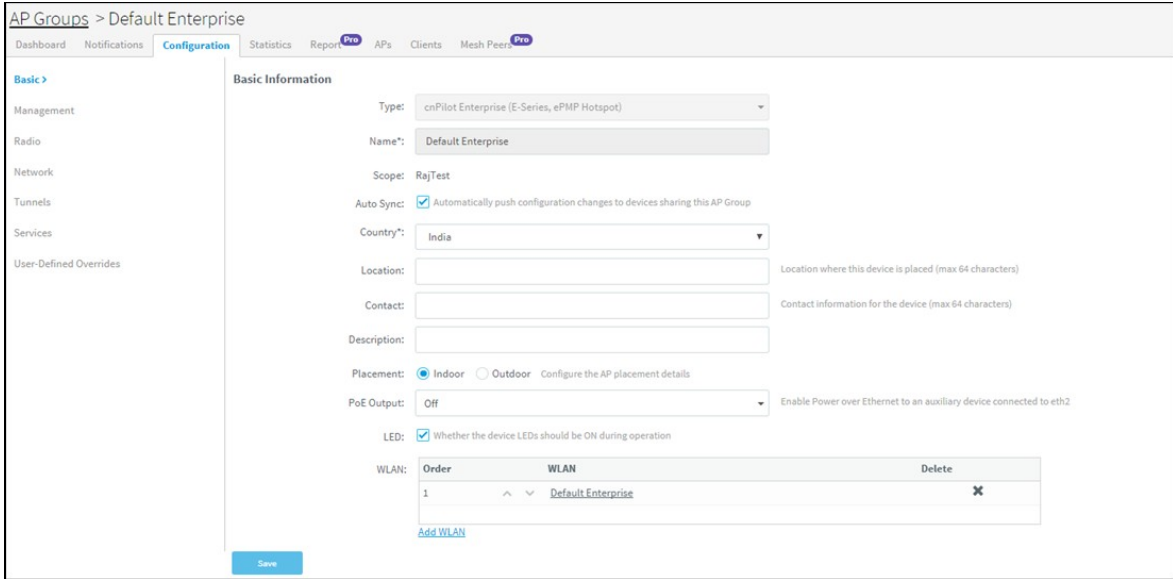
## Retry Configure

When the user tries to apply any AP Group on the device and if the job was skipped for the device as it was offline, the reason for the skip will be displayed as "Device was offline", in the Jobs page. In this case, when the device comes Up and connects to cnMaestro c4000 Controller, then cnMaestro c4000 Controller will create an Auto-sync job for that device and pushes the AP group. (It will not apply the AP group if the "Auto-Sync" was disabled in the AP group).



### Note

The config update (auto-sync) will happen only when the "Auto-Sync" option was enabled in the AP Groups page. If the device was skipped/failed because of any other reason other than the "Device was offline", then the device will not be updated.



## Import/Export of WLAN and AP Group

The WLAN and AP Groups are created for cnPilot Home and Enterprise devices. The configurations created for each WLAN and AP Groups in a server can be exported and imported to different servers. This will help the users reduce the effort of manually creating the WLAN and AP Group each time.

| Name                  | Scope               | Type  | AP Status      | Clients Now | Clients 24 HR | Throughput (DL/UL) | Actions                    |
|-----------------------|---------------------|---|----------------|-------------|---------------|--------------------|----------------------------|
| guestsomnath          | Base Infrastructure | cnPilot Enterprise (E-Series, ePMP Hotspot) | 0 of 0 offline | 0           | 0             | 0 Kbps / 0 Kbps    | [Export] [Import] [Delete] |
| new_wlan_common_clone | AHM-2               | cnPilot Enterprise (E-Series, ePMP Hotspot) | 0 of 0 offline | 0           | 0             | 0 Kbps / 0 Kbps    | [Export] [Import] [Delete] |
| new_wlan_common_clone | Ahmedabad           | cnPilot Enterprise (E-Series, ePMP Hotspot) | 0 of 0 offline | 0           | 0             | 0 Kbps / 0 Kbps    | [Export] [Import] [Delete] |

| Name                | AP Status      | Scope               | Clients Now | Clients 24 HR | Throughput (DL/UL) | WLANs           | Auto Sync | Actions                    |
|---------------------|----------------|---------------------|-------------|---------------|--------------------|-----------------|-----------|----------------------------|
| guestsomnath        | 0 of 0 offline | Base Infrastructure | 0           | 0             | 0 Kbps / 0 Kbps    | guestsomnath    | ON        | [Export] [Import] [Delete] |
| new_APgroup_common1 | 0 of 1 offline | Ahmedabad           | 0           | 0             | 0 Kbps / 0 Kbps    | new_wlan_common | ON        | [Export] [Import] [Delete] |
| new_APgroup_common1 | 0 of 0 offline | AHM-2               | 0           | 0             | 0 Kbps / 0 Kbps    | new_wlan_common | ON        | [Export] [Import] [Delete] |
| new_APgroup_common  | 1 of 1 offline | Shared              | 0           | 0             | 0 Kbps / 0 Kbps    | new_wlan_common | ON        | [Export] [Import] [Delete] |

To export WLAN and AP Group,

1. Navigate to Shared Settings > WLAN and AP Groups page > WLAN or AP Group tab (according to the choice).
2. Click the Export button.



**Note**

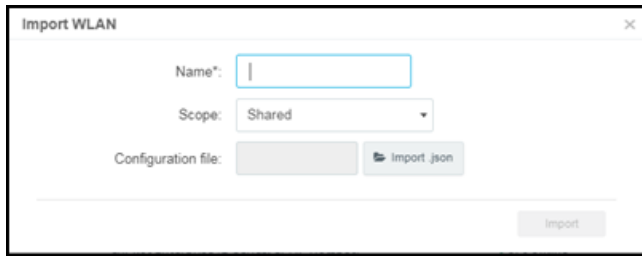
The WLANs and the AP Group should be exported separately as the associated WLANs are not exported while exporting an AP Group.

To import WLAN and AP Group,

1. Navigate to **Configuration > WLAN and AP Groups page > WLAN or AP Group tab** (according to the choice).



2. Click the **Import WLAN** button.



3. Enter the name and select the exported WLAN or AP Group file in Json format.
4. Click **Import**.



**Note**

1. To import an AP Group, ensure that all the associated WLANs in that AP Group are already imported. If the WLAN associated with the AP Group is unavailable, an error message will be displayed during AP Group import.
2. If the name is not provided for WLAN or AP Group while importing, it will take the name of the file that is to be imported, automatically.
3. If the name provided for the AP Group/WLAN while importing matches with the existing list of WLAN or AP Group in the system, an error " The specified policy name already exists" will be displayed.

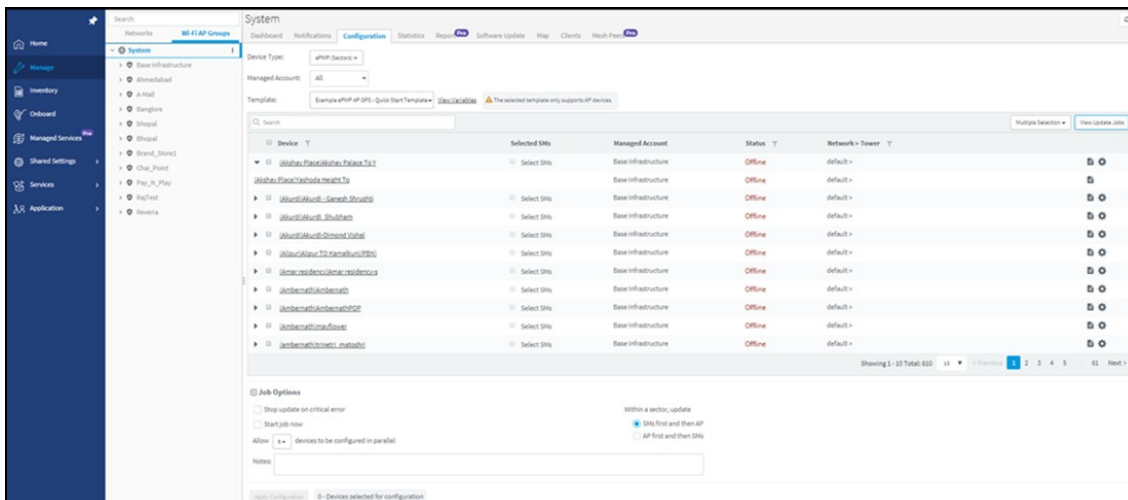


**Note**

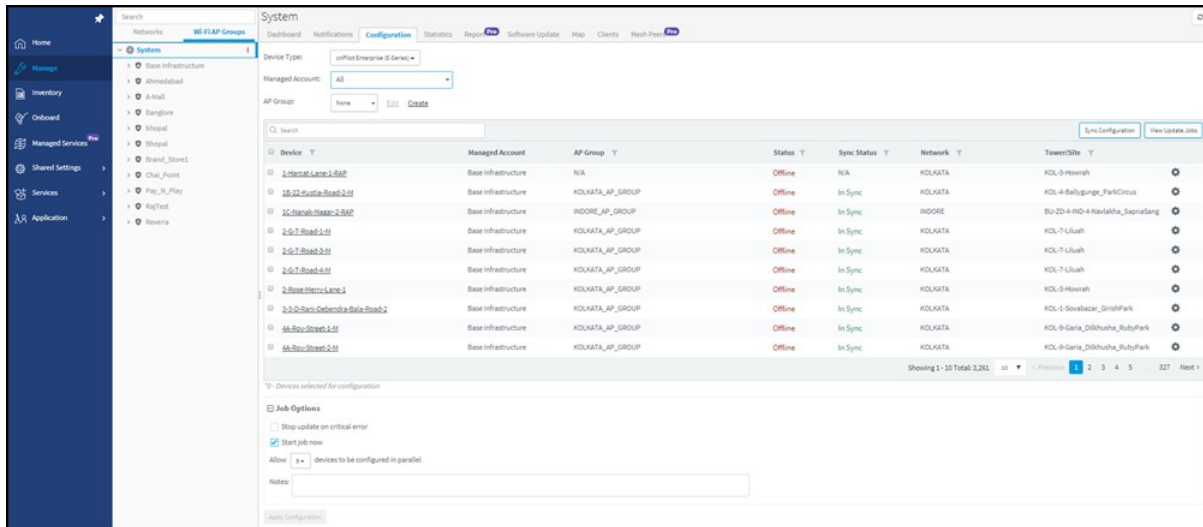
Importing WLAN and AP group type R-series are not allowed in Wi-Fi mode.

## Create a Configuration Job

Configuration job can be created from **Manage > Configuration > Device Details**. Select a device type and a set of devices along with AP groups to which they will be mapped. This can be done in three steps:



1. Select the AP Group that needs to be pushed.
2. Select the list of Wi-Fi Devices.
3. Click **Apply Configuration**.

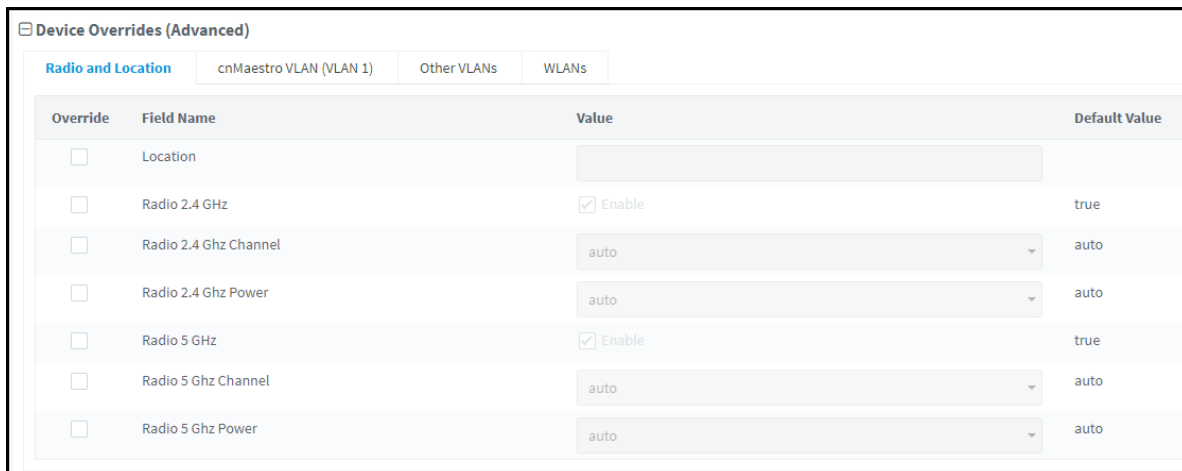


## Pre-Defined Overrides

Some device configuration is generally specific to an individual device, and hence not easily shared through an AP Group. This includes IP Address, Radio Channel Settings, and WLAN details such as SSID, Enabling/Disabling SSID, Enabling/Disabling Radio 2.4 GHz and Radio 5 GHz, and Passphrase. These items can be configured in the Device Configuration page, which can be selected by choosing Manage > Configuration in the menu, and then selecting the device in the tree to update.

You can then choose/change different values from AP Group to be overridden. The icon to the left of a field must be selected first to override that parameter. After specifying override parameters, select Apply Configuration on the bottom right to save your changes to the server and create a job to push the new values to the device. This option is also applicable to the Onboarding process queue.

By default, Enterprise Wi-Fi devices will have "Auto-set from device" enabled. This option reads several network-related configuration fields from the device and uses those as override values to prevent overwriting values that would disconnect the device.



## User-Defined Overrides (Advanced)

User-Defined Overrides can be entered into the end of an AP Group configuration. They will be merged into or appended to the AP Groups before the configuration is applied to the device. This allows setting configuration parameters that are not supported by GUI, and they are considered as the advanced operation that should rarely be used. The format of the commands would be the same as with the device CLI.

For example, if a new version of the software had a feature unsupported in cnMaestro c4000 Controller, it could be pushed to the device using CLI commands through the User-Defined Override mechanism

This can be explained with the following example, in which country-code and hostname are appended to the end of the configuration, and will override any settings in the UI.

```
country-code
IN hostname
Wi-Fi_Device
```

## User-Defined Variables (Advanced)

Override configuration also supports a programmatic concept called user-defined variables (which are also used with Fixed Wireless templates). User-Defined Variables can be embedded into the User-Defined Override text area. They require a value to be set for each device mapped to the AP Group before the configuration can be applied. This is either through a default value or an explicit setting in the device configuration.

The syntax for user-defined variables is shown in the following example: the VariableName maps to an identifier set by each Device. If the value is not set, the optional DefaultValue will be used.

```
Parametername ${VariableName=DefaultValue}
```



### Note

You can also configure the user-defined variables in the Onboarding process queue page. They are mapped individually to each device.

### Other Examples

```
cnPilot Enterprise Hotspot/E-Series
```

```
country-code ${countryname=US} // country name with US as default value hostname
${hostname=ePMP_1000_Hostpot}
```

```
cnPilot Home R-Series
```

```
Parameter name ${variableName=someDefaultValue}
```

### Example

```
CountryCode=${countryName=IE} RTDEV_CountryCode=${5GHz_CountryName=IE}
wan_ipaddr=${wan_ip=10.110.68.10}
```

Macros can be used in Advanced Configuration similar to User-Defined Overrides except they automatically take values provided by the device itself.

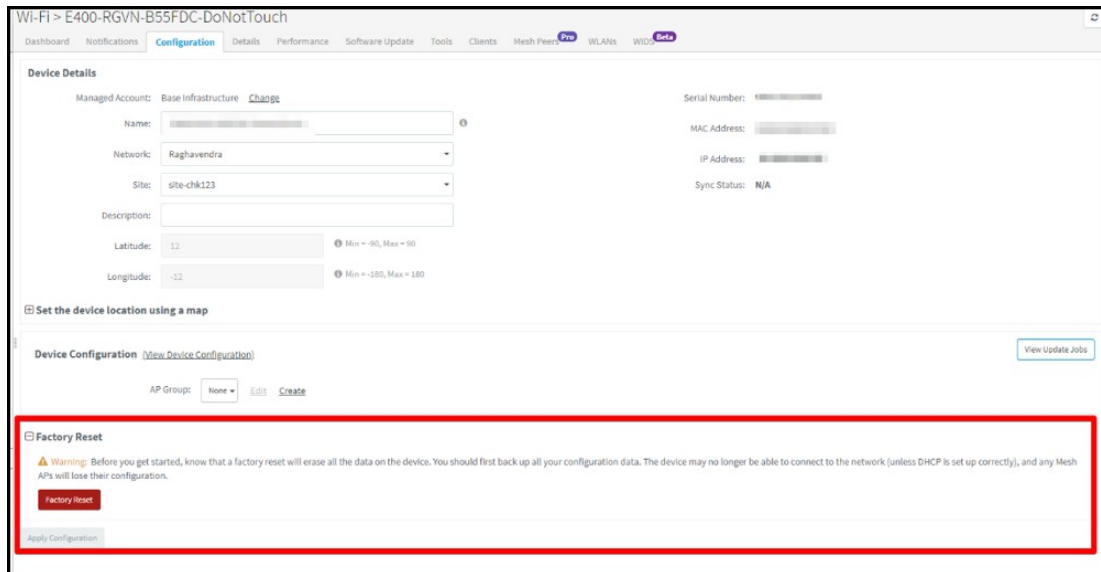
- `%{ESN}` will be replaced with the device's MAC address

- %{MSN} will be replaced with the device's Serial Number

## Factory Reset

A factory reset will erase all the data on the device. The device software version should be greater than 3.10-R6. To factory reset the device from cnMaestro c4000 Controller:

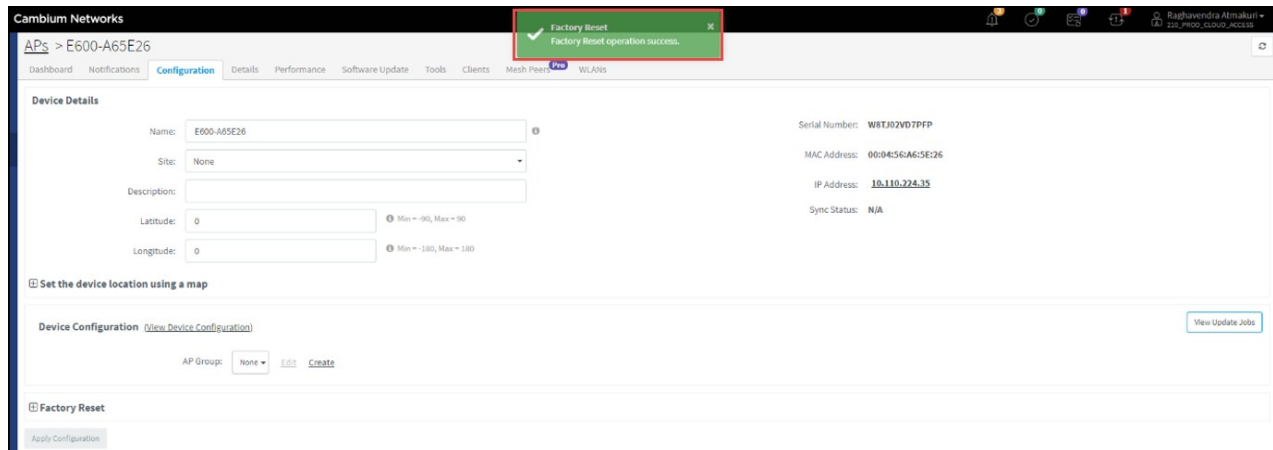
1. Navigate to the Configuration page of the device.
2. Select **Factory Reset**.



3. Click the **Factory Reset** button.



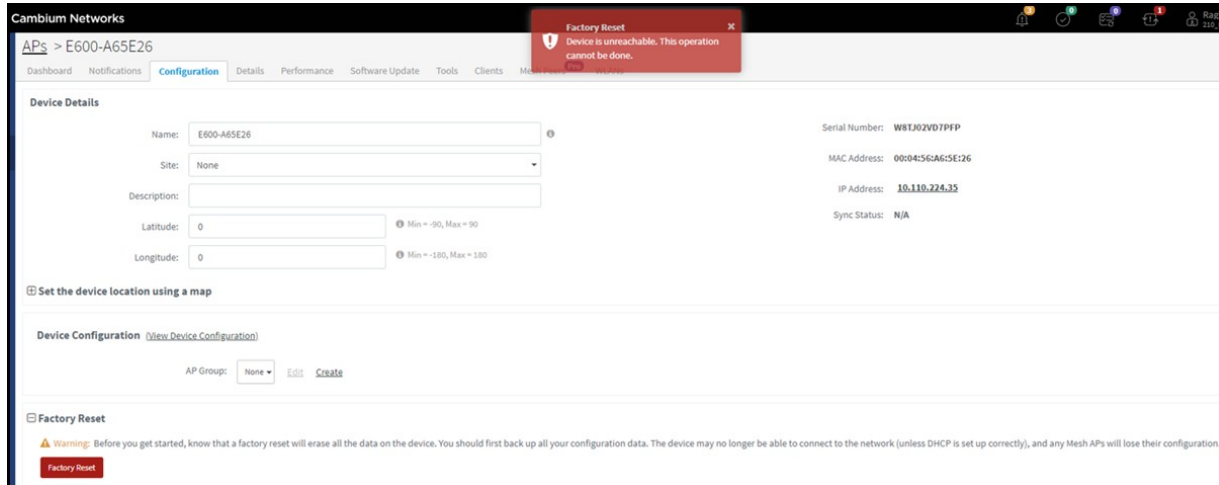
The following window pops-up once you click Yes, Factory reset option.



Once the Factory Reset is successful, the following message is displayed in the Notifications page.

| Managed Account: MSP-Account-User |              |                                  |                  |                   |                         |  |                                   | Export |
|-----------------------------------|--------------|----------------------------------|------------------|-------------------|-------------------------|--|-----------------------------------|--------|
| Severity                          | Device Type  | Device                           | Managed Account  | IPv4/IPv6 Address | Category                | Message  | Raised Time                       |        |
| Major                             | cnPilot e600 | E600-A65E26<br>00:04:56:A6:5E:26 | MSP-Account-User | 10.110.224.35     | STATUS                  | Device is offline<br><a href="#">View Details</a>                          | Wed Apr 17 2019 14:33:08 GMT+0530 |        |
| Notify                            | cnPilot e600 | E600-A65E26<br>00:04:56:A6:5E:26 | MSP-Account-User | 10.110.224.35     | SYSTEM_CONFIG_DEFAULTED | System configuration was reset to default:<br><a href="#">View Details</a> | Wed Apr 17 2019 14:33:07 GMT+0530 |        |

If the user does Factory Reset on an offline device it displays error as shown below:



## Association ACL

This section describes how cnMaestro c4000 Controller replies to AP's request to allow or disallow client associations. This feature allows you to configure MAC association list on the controller.

### Overview

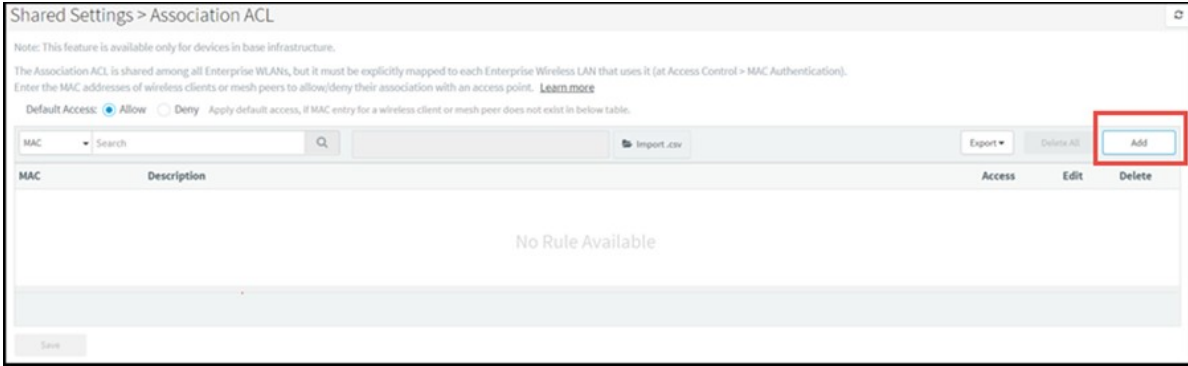
When a client using requests to get connected to an AP,

1. The AP sends MAC authentication request along with the client's MAC and the Customer ID (CID) to the Controller. This is optional and occurs only if MAC ACL is configured for the WLAN on the AP and the policy for the MAC ACL is cnMaestro c4000 Controller.
2. Controller checks and responses with an action to allow or deny the request.
3. AP allows or denies the client's request based on the Controller's response.

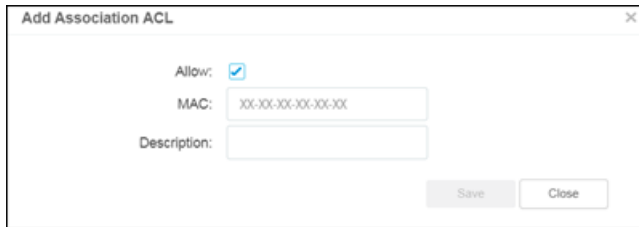
### Configuring Association ACL

To configure the Access Control List (ACL) in cnMaestro c4000 Controller:

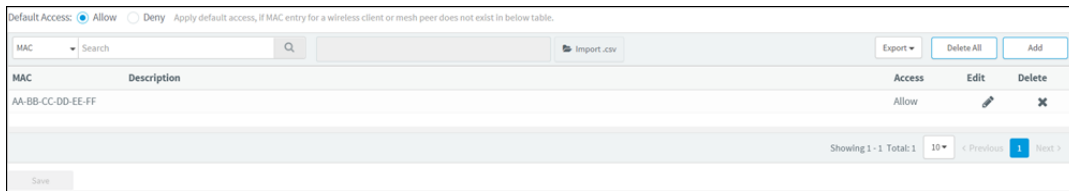
1. Navigate to Shared Settings > Association ACL page.
2. Click Add to add a MAC under Association ACL.



3. Enter the required MAC, select or deselect the Allow checkbox, and click Save.

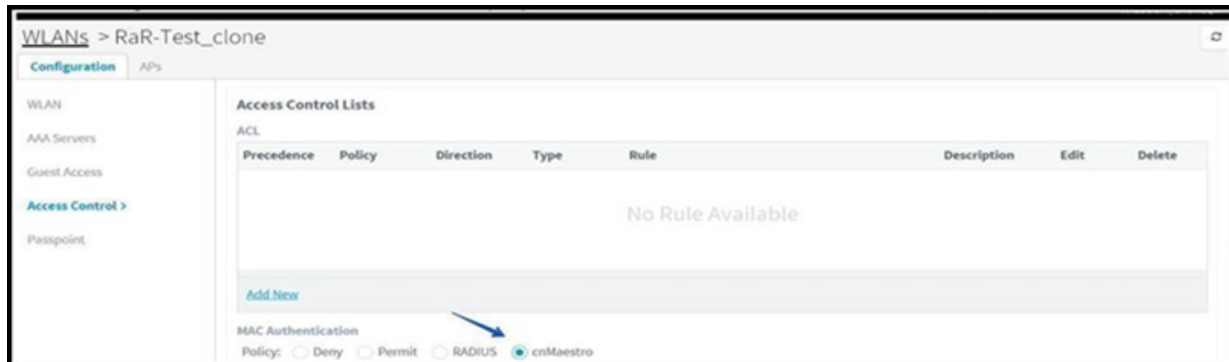


4. Once the MAC is successfully configured, a pop-up Association ACL default action is saved successfully is displayed and lists the configured MAC in Shared Settings > Association ACL page.



5. To configure MAC authentication as cnMaestro c4000 Controller:

The Association ACL is shared among all Enterprise WLANs, but it must be explicitly mapped to each Enterprise Wireless LAN that uses it (at Access Control > MAC Authentication).



**Note**

- If MAC is not configured under the policy (to allow/deny), the default action will be applied.
- To edit/delete Association ACL, click on the respective icons.
- You can import Association ACL, by clicking the Import.csv button and export using the Export button.

# Chapter 13: Services

This chapter provides the following information:

- [API Client](#)
- [cnPilot GRE Tunnels](#)
- [cnPilot Guest Access](#)

## API Client

### Overview

cnMaestro c4000 Controller supports a RESTful API as part of its cnMaestro c4000 Controller deployment. This API allows customers to read data and perform operations programmatically using their own client applications. The API is supported over HTTPS, and messages are exchanged in JSON format. Modern programming languages have rich support for RESTful interfaces.



#### Note

cnMaestro c4000 Controller currently provides monitoring data over the API (such as inventory, statistics, events, and alarms).

### API Clients

API Clients are external applications able to access the RESTful API over HTTPS using OAuth 2.0 Authentication. Full details on how to enable API Support, configure API Clients, and access monitoring data is provided in the cnMaestro c4000 Controller RESTful API Specification, which can be downloaded from the Support Center website.

cnMaestro supports a RESTful API as part of its On-Premises deployment. This API allows customers to read data and perform operations programmatically using their own client applications. The API is supported over HTTPS, and messages are exchanged in JSON format. [Learn more](#)

| Application Name  | Application Description | Client Id | Actions |
|-------------------|-------------------------|-----------|---------|
| No Data Available |                         |           |         |

Showing 0 to 0 of 0 entries 10 < Previous Next >

Figure 88 API Clients



**Note**

You can download the latest API specification from <https://support.cambiumnetworks.com/files/cnmaestro/>

## cnPilot GRE Tunnels

This section provides the following information:

- [Overview](#)
- [Configuring L2GRE/EoGRE Tunnel Concentrator](#)
- [Access Control List \(ACL\) Configuration](#)

### Overview

While deploying access points, the ability to tunnel wireless traffic from the APs to a tunnel concentrator (L2GRE/EoGRE) often plays a key role. By using the tunnel feature, the following can be avoided:

- Reconfiguration of switches and routers (for VLANs)
- Networking issues that arise when the clients IP range is not routable

The cnMaestro c4000 Controller accepts tunneled traffic from the APs. With end to end tunnel solutions from Cambium Networks, it is easy to get up the network fast and in a reliable way. By default, Cambium L2GRE is enabled on cnMaestro c4000 controller. Only cnPilot devices will be able to establish tunnel.

### Configuring L2GRE/EoGRE Tunnel Concentrator

To configure L2GRE/EoGRE tunnel concentrator, navigate to **Services > Data Tunnel** page of the UI.

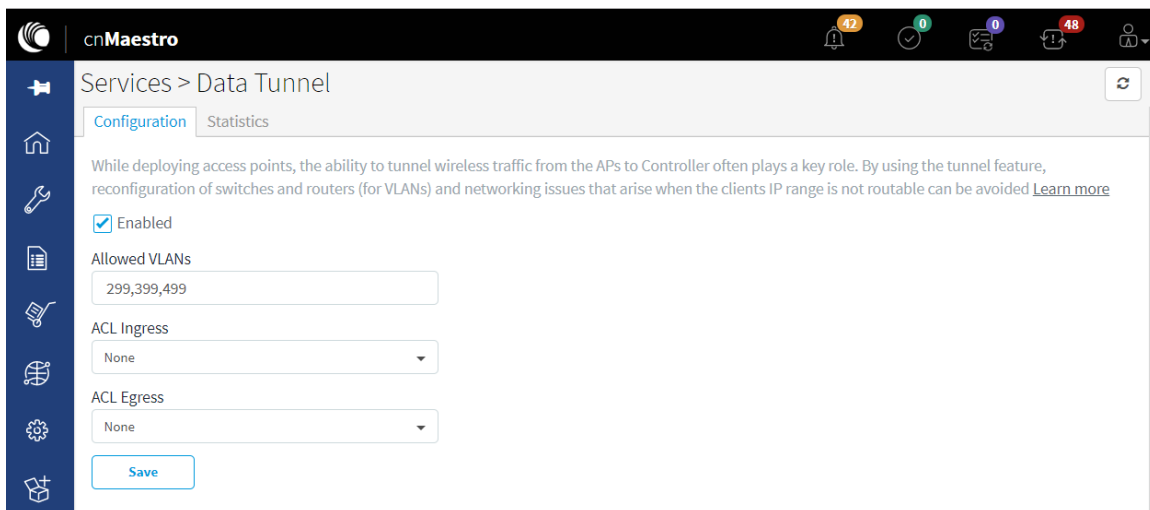


Figure 89 Configuring L2GRE/EoGRE Tunnel Concentrator

**Note**

Ensure that Promiscuous mode is enabled on the virtual interface that is mapped to the Auxiliary/bridge port of GRE.

Table 28 Parameters displayed in configuring data tunnel page

| Parameter     | Description   |
|---------------|---|
| Allowed VLANs | Represents a list of VLANs allowed through the tunnel. This list is used for allowed VLANs on aux/bridge port and also serves as a filtering list for inter AP packet forwarding. |
| ACL Ingress   | Provision to apply the ACL policies based on required ingress traffic.  |
| ACL Egress    | Provision to apply the ACL policies based on required egress traffic.   |

## Logs and Statistics

- **Collecting Logs:** Logs are useful for debugging purposes. All related tunnel specific logs can be found in `/var/log/aurora/tunnel.log`
- **Statistics:** Tunnel statistics are available under the **Services > Data Tunnel > Statistics** page.

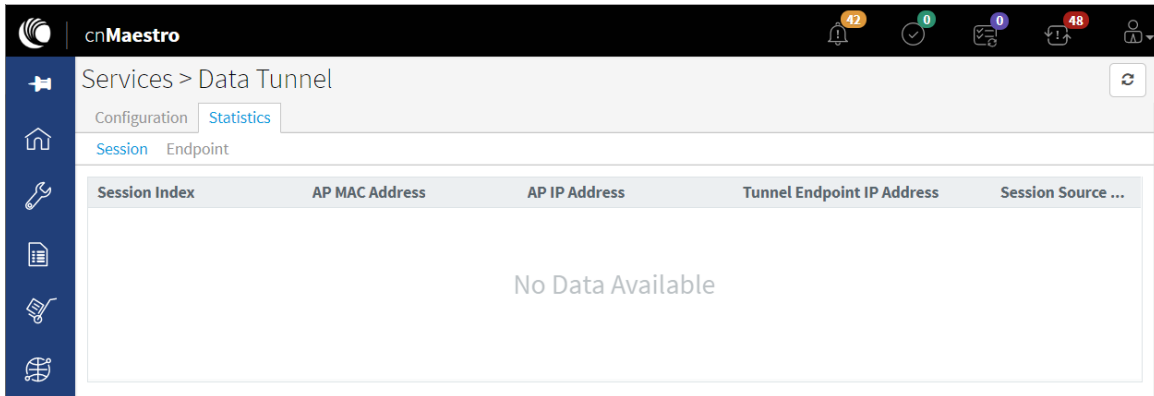


Figure 90 Logs and Statistics

## Access Control List (ACL) Configuration

ACL provides a mechanism to filter out the unwanted traffic passing through the tunnel as well as traffic going between the APs. ACL provides many options to deny or permit the traffic. Traffic can be denied/permitted based on the MAC layer, IP layer, and Protocol layer along with the direction of flow. ACL is configured with the help of rules, each of them comes with precedence. In these rules, IN direction refers to traffic coming from APs to the concentrator and OUT direction refers to the reverse.

ACL comes up with default rules that prevent unnecessary broadcast and multicast to go out towards APs. With these rules, the inter AP communication is blocked.













| ACLs <span style="float: right;">Add ACL</span> |        |           |       |                       |   |
|---|--------|-----------|-------|-----------------------|---|
| Precedence                                      | Policy | Direction | Type  | Rule                  | Action  |
| 1   | permit | in        | proto | udp any 68 any 67     |   |
| 2   | permit | out       | proto | udp any 67 any 68     |   |
| 3   | deny   | out       | proto | udp any 68 any 67     |   |
| 4   | deny   | out       | mac   | any ff:ff:ff:ff:ff:ff |   |
| 9   | deny   | out       | mac   | any multicast         |   |
| 10  | permit | any       | mac   | any any               |   |

Figure 91 ACL Configuration

Here are the screenshots for the different ACL rule categories: MAC Layer ACL

**Add ACL** ✕

Precedence:

Policy:

Direction:

Type:

Source MAC:

Destination Mac:

Figure 92 MAC Layer ACL

IP Layer ACL

**Add ACL** ✕

Precedence:

Policy:

Direction:

Type:

Source IP / Mask:

Destination IP / Mask:

Figure 93 IP Layer ACL

## Transport Layer ACL

Figure 94 Transport Layer ACL

## cnPilot Guest Access

This section describes how to configure Guest Access using cnMaestro c4000 Controller. This feature allows the clients to connect through Free Tier, Buying Vouchers or Paid Access types.

The Guest Access feature creates a separate network for guests by providing internet access to guest wireless devices (mobiles, laptops, etc).



### Note

The Guest Access feature is supported on Enterprise devices, including cnPilot E400/E500 and ePMP 1000 Hotspot.

## Configuration

- Create the Guest Access Portal in cnMaestro c4000 Controller
- Map the device to cnMaestro c4000 Controller

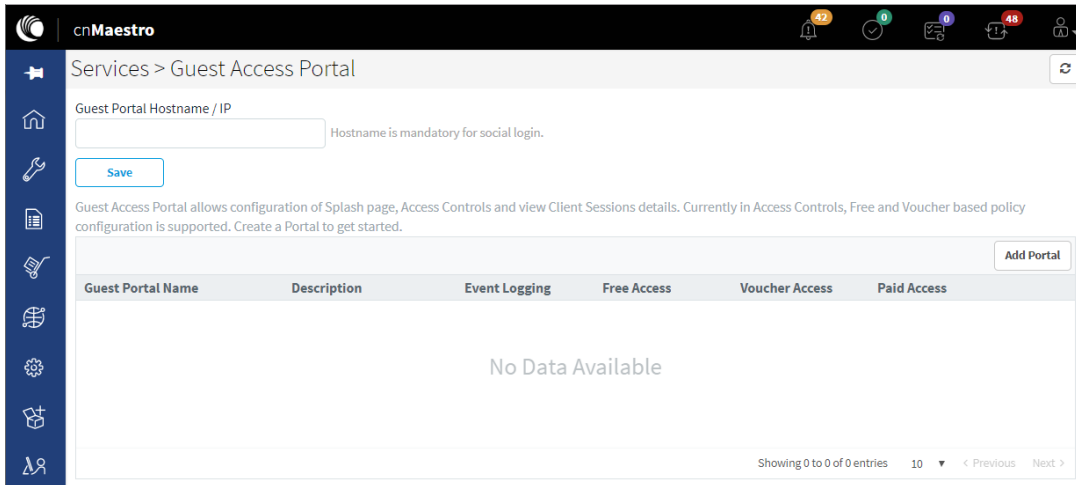
### Create the Guest Access Portal in cnMaestro c4000 Controller

1. Basic details
2. Access Portal
3. Splash page
4. Sessions

## Procedure for creating Guest Access

### Prerequisites

1. Navigate to **Services > Guest Access Portal**.

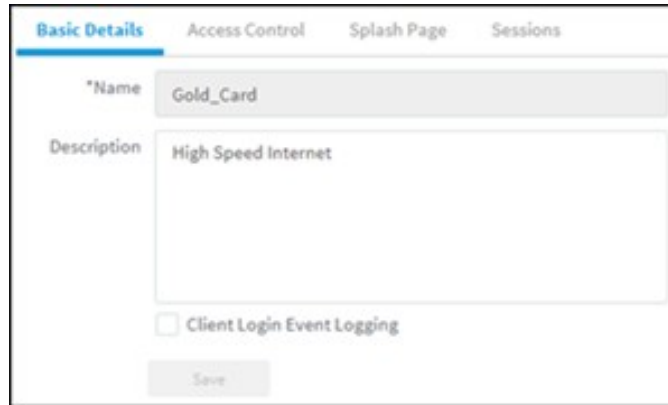


2. Click **Add Portal**. A maximum of four portals can be created per account.
3. Configure the name and a brief description for the portal.

The screenshot shows the 'Add Guest Portal' dialog box. It has a title bar with a close button (X). The form contains a 'Name\*' input field, a 'Description' text area, and a checkbox labeled 'Client Login Event Logging'. At the bottom, there are 'Save' and 'Cancel' buttons.

### Basic Details

The Basic Details page contains the Name and Description which are configured at the time of adding a new portal.



The screenshot shows a web interface with four tabs: 'Basic Details', 'Access Control', 'Splash Page', and 'Sessions'. The 'Basic Details' tab is active. It contains a form with the following fields:

- \*Name: Gold\_Card
- Description: High Speed Internet
- Client Login Event Logging
- Save button

**Note**

A name once created for the Portal cannot be changed.

### Access Portal

The Access Portal tab has three different access types:

- Free
- Paid
- Vouchers

The parameters under each access method can only be configured once the corresponding access method is enabled.

## Free Access Type Configuration

The screenshot shows the configuration page for the Free Access Type. The breadcrumb is "Guest Access Portal > Redundancy". The page has tabs for "Basic", "Access", "Splash", and "Sessions", with "Access" selected. Below the tabs are sub-tabs for "Free", "Paid", and "Vouchers", with "Free" selected. The main configuration area includes:

- Enable Free Access
- Enable Logout functionality for the guest client
- Bypass Captive Portal Detection
- Client Session** (expanded):
  - Renewal Frequency: 20 (Min(s)) Valid range is 1-2628000 minutes
  - Session Duration: 20 (Min(s)) Valid range is 1-2628000 minutes
- Client Rate Limit** (collapsed)
- Client Quota Limit** (collapsed)
- Social Login** (collapsed)
- SMS Authentication** (collapsed)
- Add Whitelist** (collapsed)

A "Save" button is located at the bottom left of the configuration area.

**Figure 95 Free access type configuration**

Free access type contains session validity, renewable frequency, client rate limits, and social login configurable parameters.

You can select authentication using Google, Facebook, Twitter and Office 365, or all. You will need to enter the App ID of your social login App. If you enable Facebook login you will also need to enter your Facebook App secret.

**Table 29 Free Access Type Parameters**

| Parameter           | Description   |
|---------------------|---|
| Session Duration    | The duration for which the client is provided access.   |
| Renewable Frequency | Once the session duration for the client expires, the client needs to wait for the period specified by renewal frequency before logging in again.   |
| Client Rate Limit   | It contains options for configuring downlink and uplink parameters in kbps to limit the data transfer rate to or from the client. If a client rate-limit parameter is blank, no limits are applied.   |
| Client Quota Limit  | <p>The data quota limit feature has been added for RADIUS-based as well as for controller-based guest portals. For controller-based, it is either directional or total data quota limit. Once the client logs in as a guest, the data quota limit is enforced and the values are sent to the access point to which the client is connected. The access point keeps track of the data limits. Access point also sends client statistics to the controller every thirty minutes. In the case of multiple devices allowed for a given policy then the data quota limits enforcement has some limitations and works with the latency of thirty minutes during which the cumulative data quota limits of the devices can be exceeded beyond the configured data quota limits.</p> <p>The similar behavior is supported through RADIUS attributes for RADIUS-based onboard guest access clients.</p> <p>RADIUS_VENDOR_ID_CAMBIUM 9 (17713)</p> <p>RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_UP (151)</p> <p>RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_DOWN (152)</p> <p>RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_UP_GIGWORDS (153)</p> <p>RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_DOWN_GIGWORDS (154)</p> <p>RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_TOTAL (155)</p> <p>RADIUS_VENDOR_ATTR_CAMBIUM_WIFI_QUOTA_TOTAL_GIGWORDS (156)</p> <p>The gigwords attributes are used for supporting data quota limits above 4GB when required.</p> |
| Social Login        | <p>Consists of the following options:</p> <ul style="list-style-type: none"> <li>• Domain URL: The redirected URL in the client when trying to access the Internet.</li> <li>• Google: Consists of ID and Secret options to configure, which admin can create from <a href="https://console.developers.google.com/iam-admin/projects">https://console.developers.google.com/iam-admin/projects</a></li> <li>• Facebook: Consists of ID and Secret options to configure, which admin can create from <a href="https://developers.facebook.com/apps/">https://developers.facebook.com/apps/</a></li> <li>• Twitter: Consists of consumer key, consumer secret key, and callback URL.</li> <li>• Office 365: Consists of Id and Replyback URL.</li> </ul>  |



| Parameter          | Description  |
|--------------------|--|
| SMS Authentication | SMS OTP supports Twilio, SMS Country, and SMS Gupshup SMS gateway providers. Anyone of the gateway providers can be used to support the SMS OTP to be delivered to the cell phone of the end-user. Once OTP is received the client can enter the OTP to get Internet access. |

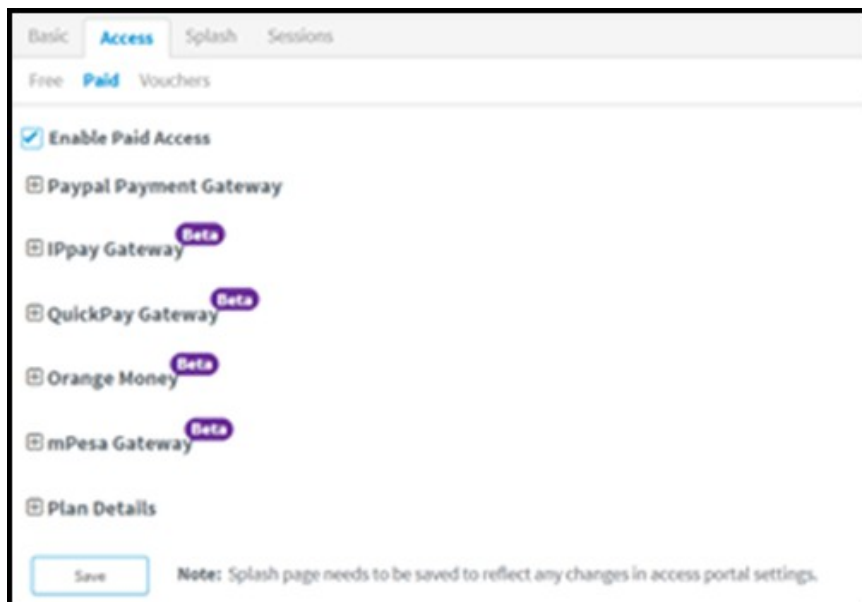


**Note**

- Renewal frequency should be greater than session expiration.
- The client will get social login options only when enabled in the Access Control page in Portal.
- If Social login is enabled, it is mandatory in a free access method for the client to log in through Google/Facebook/Twitter/Office 365.

**Paid Access Type Configuration**

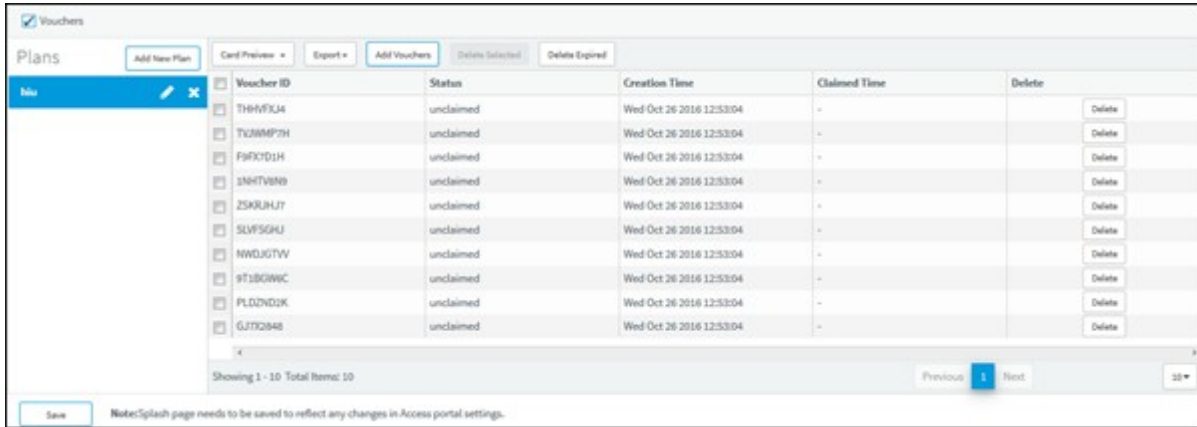
Paypal has been added as a payment gateway support where end users can purchase Internet connection using either the credit card or their existing paypal accounts. For purchasing the Internet plans, the clients are directed to paypal portal where they purchase the plan and then they are automatically redirected to the guest access portal where the purchased Voucher is displayed. The user should ensure to save this Voucher information if he plans to use it on multiple devices.



**Voucher Access Type Configuration Important Points to Remember**

- Vouchers can only be generated after enabling Vouchers and creating at least one Voucher plan.
- A maximum of 50,000 Vouchers per portal can be created on cnMaestro c4000 Controller.

- A maximum of 1,000 Vouchers per portal can be created on the cloud-hosted version. (cloud.cambiumnetworks.com).
- The total number of generated Vouchers = Vouchers Unclaimed + Vouchers Claimed + Vouchers Expired.
- The admin can export all/valid/current page Voucher codes as PDF/CSV documents.



The voucher contains options to add new plans and Vouchers. Based on user requirements, the plans can be created with different validity and rate limits.

1. Create a plan
  - a. Navigate to Services > Access Control Portal page and select Access Control tab.
  - b. Enable Vouchers
  - c. Click Add New Plan button. The window with general and design parameters for the plan is displayed.

**Table 30 Voucher Access Type Parameters**

| Parameter | Description  |
|-----------|--|
| General   | <ul style="list-style-type: none"> <li>• Name: The name of the plan.</li> <li>• Session Duration: The duration for which the client is allowed network access.</li> <li>• Voucher Expiry: The expiry time for the generated Vouchers. Once this time lapses, the Vouchers cannot be used.</li> <li>• Client Rate Limit: The uplink and the downlink values in kbps to limit the data transfer rate to or from the client. If a client rate-limit parameter is blank, no limits are applied.</li> </ul> |
| Design    | <ul style="list-style-type: none"> <li>• Color: There are options to modify colors for the title, message, code, and background.</li> <li>• Background Image: You can browse and select a background image for this page.</li> </ul>   |

With all the above parameters, administrators can create their own design for the card with text, color, and message to be displayed on the card.

2. Adding Vouchers

Once a plan is configured, Vouchers can be generated for it. Each Voucher is a unique, randomized alphanumeric code.

- a. Select a plan.

- b. Add Vouchers.

Once the plan is created and the Vouchers are generated, the following page is displayed:

| Voucher ID | Status    | Creation Time            | Claimed Time | Delete |
|------------|-----------|--------------------------|--------------|--------|
| 8962227e   | unclaimed | Tue Oct 20 2018 13:44:51 | -            | Delete |
| 4385966d   | unclaimed | Tue Oct 20 2018 13:44:51 | -            | Delete |
| 4f22a99e   | unclaimed | Tue Oct 20 2018 13:44:51 | -            | Delete |
| 956c4202   | unclaimed | Tue Oct 20 2018 13:44:51 | -            | Delete |
| 82791647   | unclaimed | Tue Oct 20 2018 13:44:51 | -            | Delete |

## c. Sample Voucher Code.

**Note**

The modified values in the Access Portal page is reflected on the splash page only when the splash page is saved after making the changes.

**Splash Page**

The Splash page refers to the page to which a wireless client is redirected when it connects to the guest portal. Administrators can create their own splash page by modifying the default logo, background, and text to be displayed on the splash page with different colors and fonts.

- If Free is selected in Access Portal, the client only sees free access related parameters.
- If the Voucher is selected in Access Portal, the client only sees Voucher related parameters with a text box to enter the Voucher code.
- If both Free and Voucher are enabled, then the client sees both Free and Voucher related parameters.

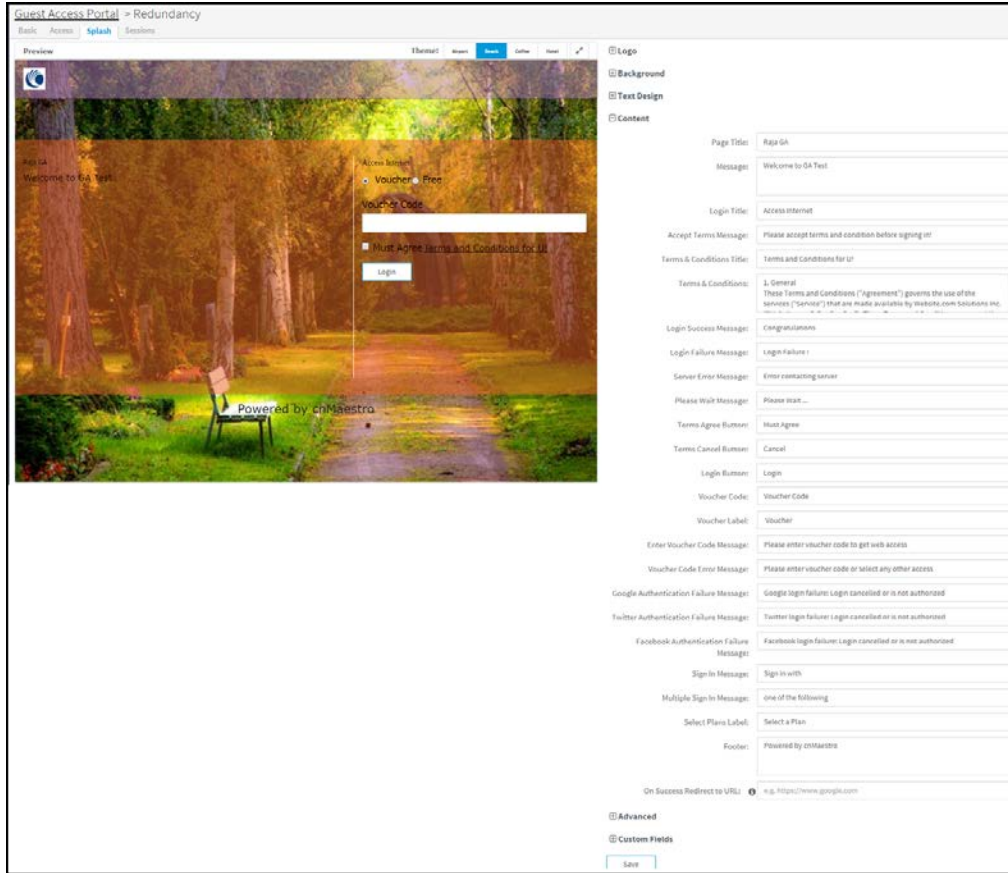


Table 31 Splash Page Parameters

| Parameter            | Description   |
|----------------------|---|
| Logo                 | Browse and select the logo the needs to appear on the splash page.  |
| Background           | Browse and select the image that needs to appear as the background.                                       |
| Opacity              | The transparency of background image.   |
| Repeat Background    | Enable the checkbox if you want the background image to be repeated.                                      |
| Background Placement | Choose the option from the drop-down list for placing the background image on the splash page.            |
| Color                | Choose the appropriate colors for the background, logo in the background, content area, and for the text. |
| Page Title           | Text to appear as the title of the page. You can choose the font style and size for the title.            |
| Message              | Text to appear as the welcome text. You can choose the font style and size for the welcome text.          |

| Parameter                  | Description   |
|----------------------------|---|
| Login Title                | Text to appear for login.   |
| Login Success Message      | Message to appear after a successful login.   |
| Accept Terms Message       | Text to appear as the accept terms message.   |
| Terms and Conditions Title | Text to appear as the title for the terms and the conditions.   |
| Terms and Conditions       | Text to appear as the terms and conditions.   |
| Server Error Message       | Text to appear if there is an error while contacting the server.  |
| Please wait                | Text to appear in the waiting screen.   |
| Terms Agree Button         | Text to appear in the terms agree button.   |
| Terms Cancel Button        | Text to appear in the terms cancel button.  |
| Login Button               | Enter the text that should appear on the button to submit.  |
| Voucher                    | Enter the text to appear in Voucher Code, Voucher Label, Enter Voucher Code Message, and Voucher Code Error Message.  |
| Failure Messages           | Enter the text to appear in Google Authentication Failure Message, Twitter Authentication Failure Message, and Facebook Authentication Failure Message.                               |
| Footer                     | Enter the text to appear as the footer of the page. You can choose the font style and size for the footer.  |
| Sign In                    | Enter the text to appear in Sign In and Multiple Sign In messages.  |
| Select Plans Label         | Enter the text to appear on the label to select the plan.   |
| Advanced                   | Expand the Advanced option. Browse and select the advanced fields.  |
| Custom Fields              | Expand the Custom Field option. The user can customize the fields in the Splash page by choosing the Custom Field option in the Guest Access Portal page and clicking Add New button. |

## Sessions

Sessions tab contains Client MAC address, Access Point MAC address, Access Type as Free (Google or Facebook) or Voucher, WLAN-SSID of the client connected AP, Remaining time and Disconnect option.

The administrator can check how many clients are connected, Access Type (Free/Voucher) of the client and can disconnect the clients.

| Client / Peer MAC | Access Point      | Access Type | WLAN         | Remaining Time | Disconnect |
|-------------------|-------------------|-------------|--------------|----------------|------------|
|                   | 00:04:56:01:48:F0 | Free        | GA_cnMaestro | 14m 38s        | Disconnect |
|                   | 00:04:56:01:48:F0 | Free        | GA_cnMaestro | 7m 15s         | Disconnect |
|                   | 00:04:56:01:48:F0 | Free        | GA_cnMaestro | 7m 46s         | Disconnect |

Client Login Events table will create events of client login sessions. It will maintain this login event for 7 days. This table has Client MAC address, Portal Name, SSID, Access point MAC, Voucher code (if client connected with Voucher), Access type (Google/Facebook/Voucher).

Admin can export the client login events as PDF / CSV.

**Table 32 Sessions Parameters**

| Parameter      | Description  |
|----------------|--|
| Client MAC     | MAC address of the client.   |
| Access Point   | MAC address of the Access Point.   |
| Access Type    | Access type as Free or Voucher.  |
| WLAN           | SSID of the network.   |
| Remaining Time | The time left for the client to access the internet. It depends upon the session duration configured in the Access Portal. |
| Disconnect     | Displays if the client is disconnected from the network.   |



**Note**

For Free Access method, the client MAC address is displayed even after the free session duration expires. It will delete the MAC address of the client after the Renewable Frequency completes,

## SMS Authentication

The following table describes the parameters described in configuring SMS authentication parameters:

| Parameter    | Description  | SMS Gateway Provider |             |             |        |                  |
|--------------|--|----------------------|-------------|-------------|--------|------------------|
|              |  | Fast SMS             | SMS Country | SMS Gupshup | Twilio | Victory Link SMS |
| Enable       | It indicates to enable the SMS Authentication feature.   | ✓                    | ✓           | ✓           | ✓      | ✓                |
| Username     | Indicates the username of the vendor.  | ✓                    | ✓           | ✓           | X      | ✓                |
| Sender ID    | It is the name or number which flashes on the recipients mobile phone when they receive SMS. This is Optional not mandatory. | ✓                    | ✓           | ✓           | X      | ✓                |
| API Key      | It's a token which is provided by vendors.   | ✓                    | X           | X           | X      | X                |
| Account Type | It shows type of accounts such as International, OTP, Promotional and Transaction.   | ✓                    | X           | X           | X      | X                |
| OTP Template | The template with which SMS has to be sent.  | ✓                    | ✓           | ✓           | ✓      | ✓                |
| Password     | It indicates the password.   | X                    | ✓           | ✓           | X      | ✓                |
| Country Code | It enables to select country code based on deployments.  | X                    | ✓           | ✓           | X      | X                |
| Auth Token   | It acts as a password.   | X                    | X           | X           | ✓      | X                |
| Account SID  | It acts as a username.   | X                    | X           | X           | ✓      | X                |
| From         | It enables to select the country code.   | X                    | X           | X           | ✓      | X                |
| Language     | It indicates the Language.   | X                    | X           | X           | X      | ✓                |

To configure SMS Authentication on cnMaestro c4000 Controller:

1. Enable the **SMS Authentication** feature.
2. In the SMS Gateway provider, select your required gateway from the dropdown list.
3. Enter the **Username**.
4. Enter the Sender ID. This field is optional. This will allow the user to send SMS through the ID which he chooses.
5. Enter the **API Key**.



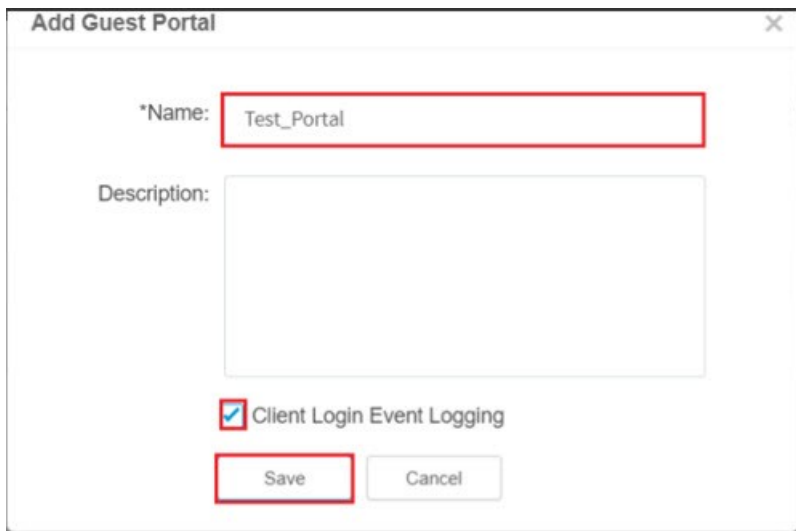
6. Select your **Account Type** from the dropdown list.
7. Enter the OTP Template. The OTP template should include “%code%. %code% will be replaced by the OTP code in the SMS.

## Guest Access using Social Login

### Configuration

To achieve cnMaestro c4000 Controller Guest Access using Social Logins like Google, Twitter, Facebook, Office-365: Create Guest Access profile on cnMaestro c4000 Controller:

1. Login to cnMaestro c4000 Controller and navigate to **Services Guest Access Portal > Add Portal**.
2. Enter Portal Name, Description, enable logging for client login events.
3. Click **Save**.



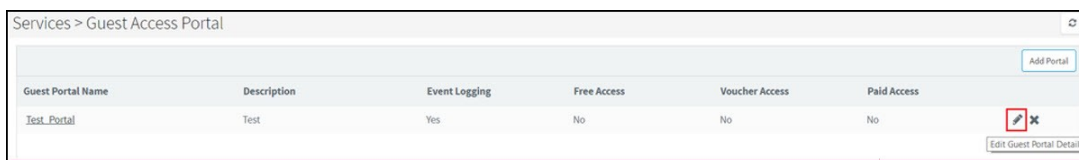
**Add Guest Portal**

\*Name:

Description:

Client Login Event Logging

4. Click **Edit Guest Portal Details**.



Services > Guest Access Portal

| Guest Portal Name           | Description | Event Logging | Free Access | Voucher Access | Paid Access |
|-----------------------------|-------------|---------------|-------------|----------------|-------------|
| <a href="#">Test_Portal</a> | Test        | Yes           | No          | No             | No          |

5. Navigate to **Access** tab and expand **Social Login**.

Guest Access Portal > Test\_Portal

Basic **Access** Splash Sessions

Free **Paid** Vouchers

**Enable**

Client Session

Renewal Frequency:  Min(s) ▼

Session Duration:  Min(s) ▼

Client Rate Limit

Client Quota Limit

**Social Login**

SMS Authentication

Enable Logout functionality for the guest client

Bypass Captive Portal Detection

Add Whitelist

6. Select Google, Twitter, Facebook, Office 365 based on your requirement.

Social Login

Guest Portal Hostname / IP: hacontroller.hacont.com ⓘ

Note: Captive portal bypass will be enabled if social login with Facebook or Google is enabled. This is required as the Captive-portal Network Assistant (Guest portal signon popup on mobile devices) is not compatible with the social login API provided by these services.

Google  
Id:

Twitter  
Consumer API Key:   
Secret Key:

Callback URL: https://hacontroller.hacont.com/cn-ctrl/guest/cnmaestro/Redundancy/twitter/Callback

Facebook  
Id:   
Secret:  Show

Office 365  
Reply URL: https://hacontroller.hacont.com/assets/views/office ⓘ  
Id:

## API Key Generation

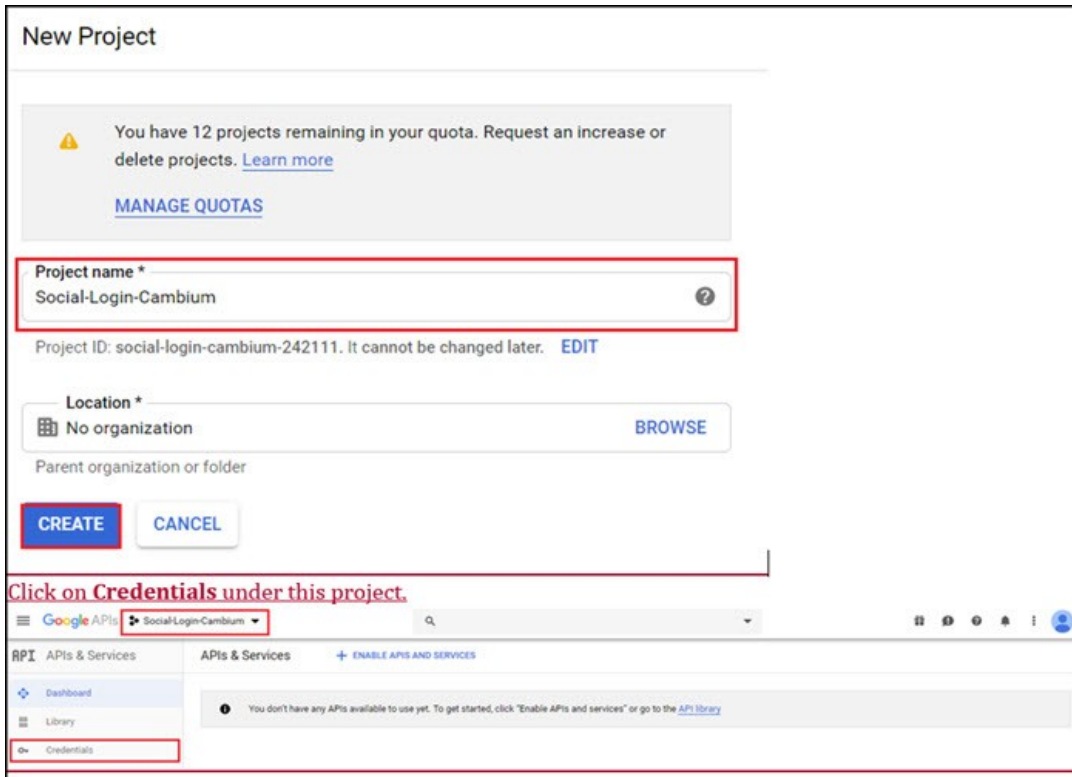
Creating APIs to integrate cnMaestro c4000 Controller with Google, Twitter, Facebook and Office 365.

### Google

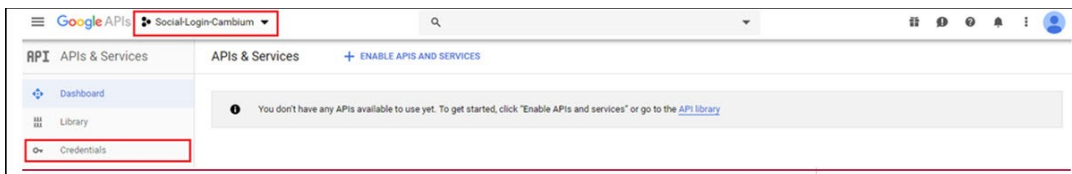
1. Login to Google Account and navigate to <https://console.developers.google.com>.
2. Click **Select a Project** and create a New Project.



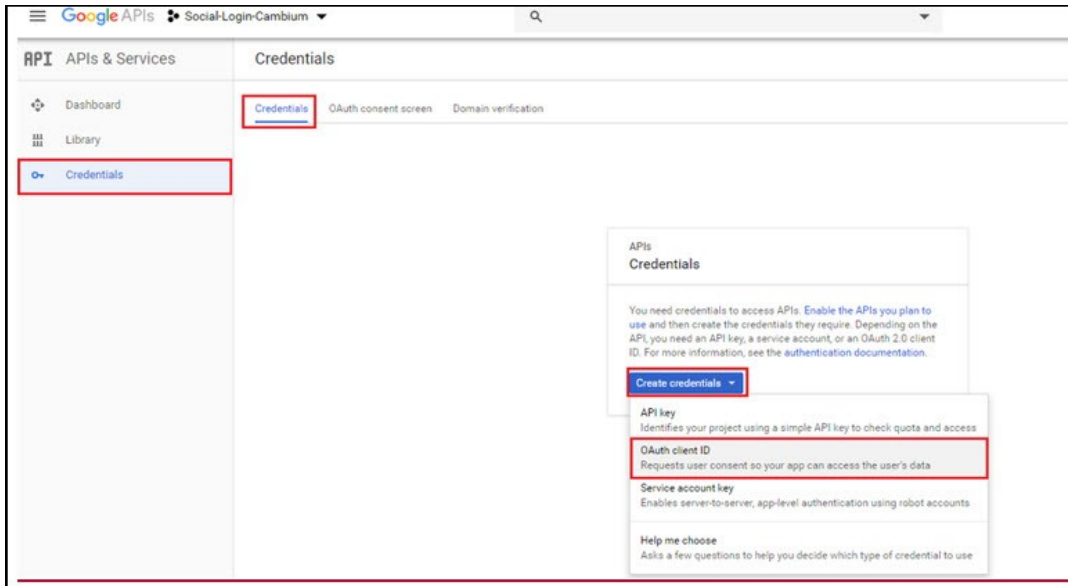
3. Give a name to the Project and click **CREATE**.



4. Click **Credentials** under this project.



5. Under the Credentials tab create **OAuth Client ID**.



6. Configure **Consent Screen**.



7. Assign a name to the application, map to an email ID, add cambiumnetworks.com to the authorized domain and click **Save**.

Google APIs Social-Login-Cambium

RPI APIs & Services

Dashboard  
Library  
Credentials

Credentials OAuth consent screen Domain verification

Before your users authenticate, this consent screen will allow them to choose whether they want to grant access to their private data, as well as give them a link to your terms of service and privacy policy. This page configures the consent screen for all applications in this project.

**Verification status**  
Not published

**Application name** ⓘ  
The name of the app asking for consent  
Social-Login

**Application logo** ⓘ  
An image on the consent screen that will help users recognize your app  
Local file for upload

**Support email** ⓘ  
Shown on the consent screen for user support  
a@gmail.com

**Scopes for Google APIs**  
Scopes allow your application to access your user's private data. [Learn more](#)  
If you add a sensitive scope, such as scopes that give you full access to Gmail or Drive, Google will verify your consent screen before it's published.

email  
profile  
openid

**Authorized domains** ⓘ  
To protect you and your users, Google only allows applications that authenticate using OAuth to use Authorized Domains. Your applications' links must be hosted on Authorized Domains. [Learn more](#)  
cambiumnetworks.com  
example.com  
Type in the domain and press Enter to add it.

**Application Homepage link**  
Shown on the consent screen. Must be hosted on an Authorized Domain.  
https:// or http://

**Application Privacy Policy link**  
Shown on the consent screen. Must be hosted on an Authorized Domain.  
https:// or http://

**About the consent screen**  
The consent screen tells your users who is requesting access to their data and what kind of data you're asking to access.

**OAuth verification**  
To protect you and your users, your consent screen and application may need to be verified by Google. Verification is required if your app is marked as **Public** and at least one of the following is true:

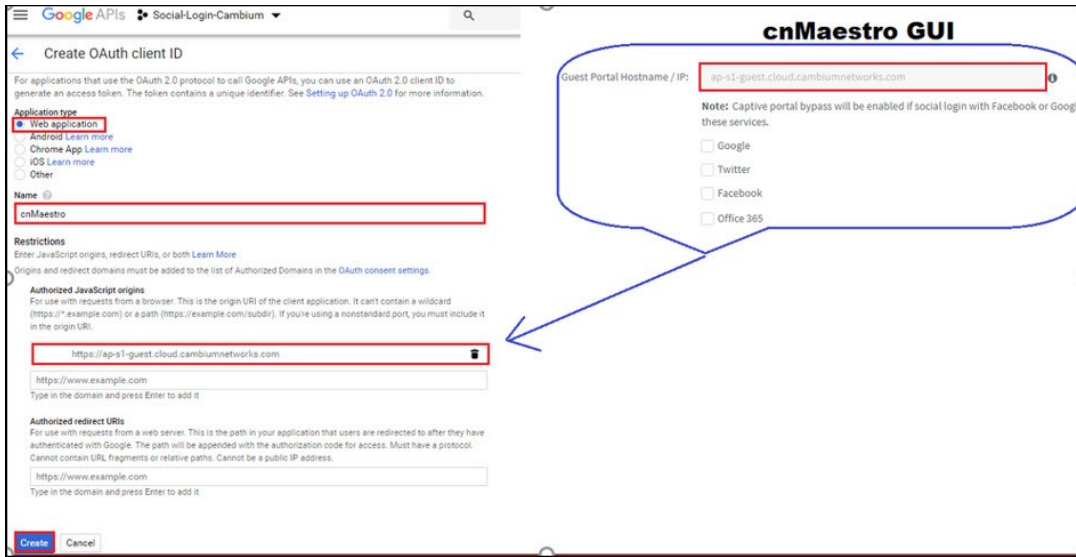
- Your app uses a sensitive and/or restricted scope
- Your app displays an icon on its OAuth consent screen
- Your app has a large number of authorized domains
- You have made changes to a previously-verified OAuth consent screen

The verification process may take up to several weeks, and you will receive email updates as it progresses. [Learn more](#) about verification.

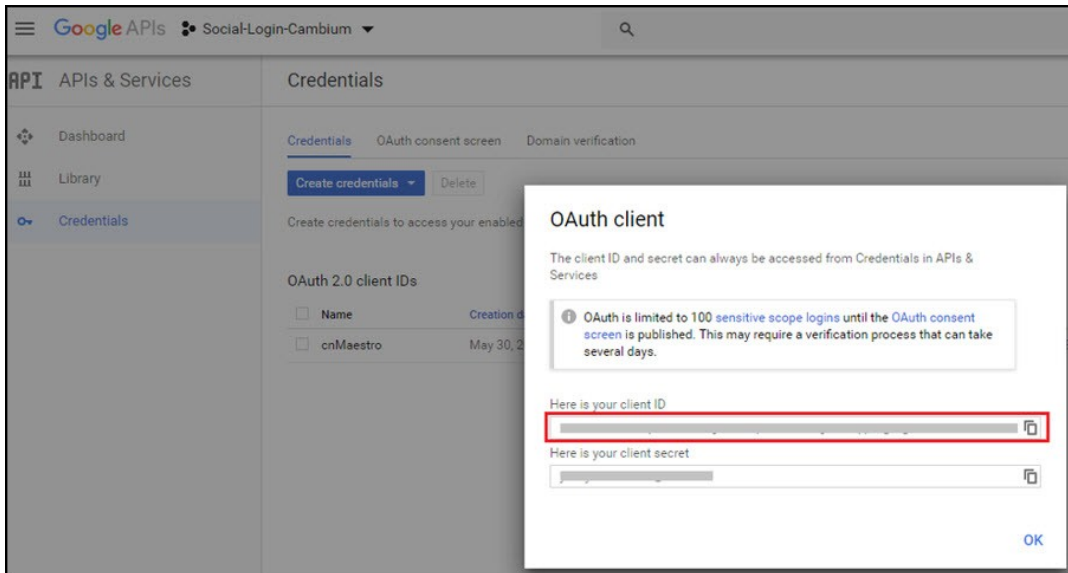
Before your consent screen and application are verified by Google, you can still test your application with limitations. [Learn more](#) about how your app will behave before it's verified.

Let us know what you think about our OAuth experience.

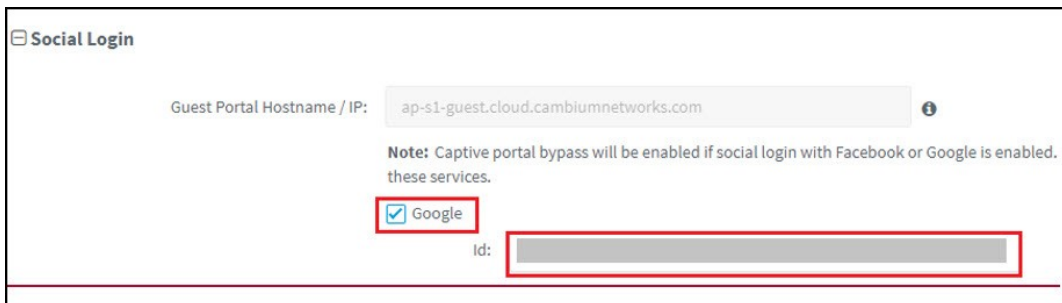
- Once clicked Save for the above page it redirects to the creation of OAuth Client ID.
- Select Application Type as Web Application, give a Name, add Guest Portal Hostname url/IP which you will get from cnMaestro c4000 Controller UI and click Create.



10. Clicking **Create** on the above page it redirects to the screen showing **Client ID** and **Client Secret**.



11. Copy the Client ID and paste it to the cnMaestro c4000 Controller enabling Google under Social Logins and click Save.



Twitter

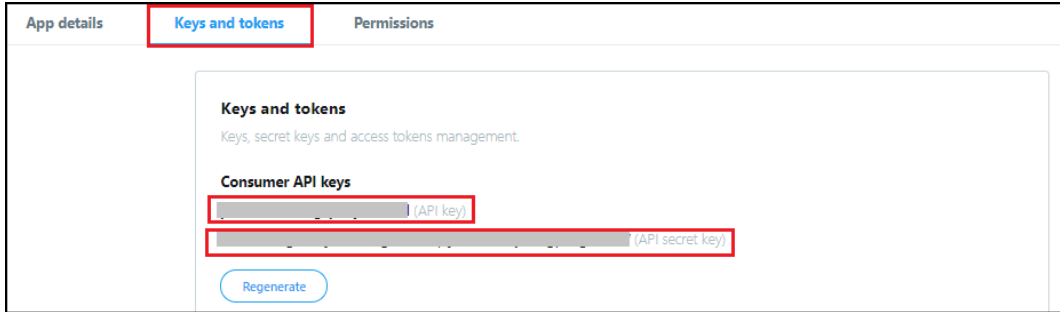
1. Log in to Twitter Account and access <https://developer.twitter.com/en/apps> and click **Create an app**.

The screenshot displays the 'App details' configuration page in the cnMaestro GUI. The page is divided into several sections:

- App details:** Contains an 'App icon Upload' field, an 'App name (required)' field with the value 'TestTwitter', and an 'Application description (required)' text area with the value 'Test\_Twitter'.
- Website URL (required):** A text field containing 'https://www.cambiumnetworks.com'.
- Allow this application to be used to sign in with Twitter:** A checkbox labeled 'Enable Sign in with Twitter' is checked.
- Callback URLs (required):** A text area containing 'https://ap-s1-guest.cloud.cambiumnetworks.com/cn-ctrl/guest/'. A blue arrow points from this field to the 'Keys and tokens' tab on the right.
- Terms of Service URL:** A text field containing 'https://ap-s1i-s1-5pkodub8un.cloud.cambiumnetworks.com'.
- Privacy policy URL:** A text field containing 'https://ap-s1i-s1-5pkodub8un.cloud.cambiumnetworks.com'.
- Organization name:** A text field containing 'Cambium'.
- Organization website URL:** A text field containing 'http://www.cambiumnetworks.com'.
- Tell us how this app will be used (required):** A text area containing 'Provide WiFi access to guest client by using twitter as authentication media. This is purely for WiFi testing purpose.'

On the right side, the 'Keys and tokens' tab is active, showing a 'Twitter' checkbox and input fields for 'Consumer API Key' and 'Consumer API Secret Key'. A 'Callback URL' field is also present with the value 'https://ap-s1-guest.cloud.cambiumnetworks.com/cn-ctrl/guest/756a2'. At the bottom, there are 'Cancel' and 'Save' buttons.

2. Click Keys and tokens and copy Consumer API Key and Consumer API Secret Key.

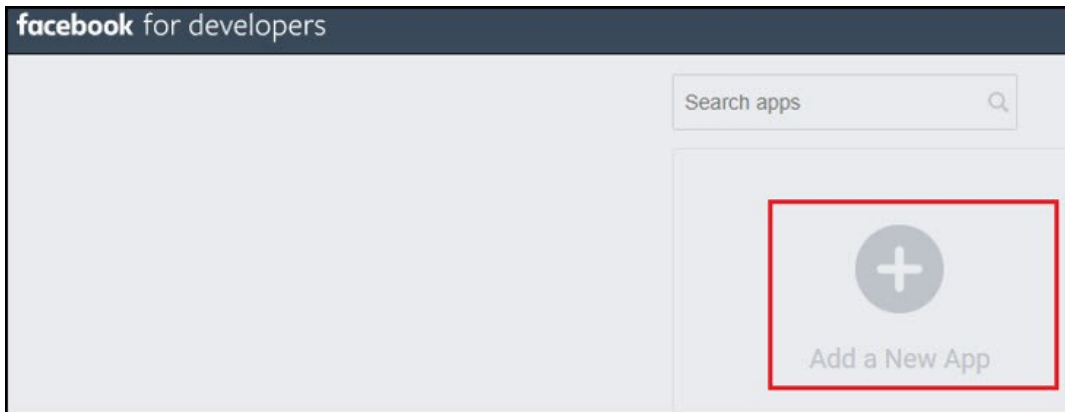


3. Paste them to cnMaestro c4000 Controller GUI for Twitter social login.

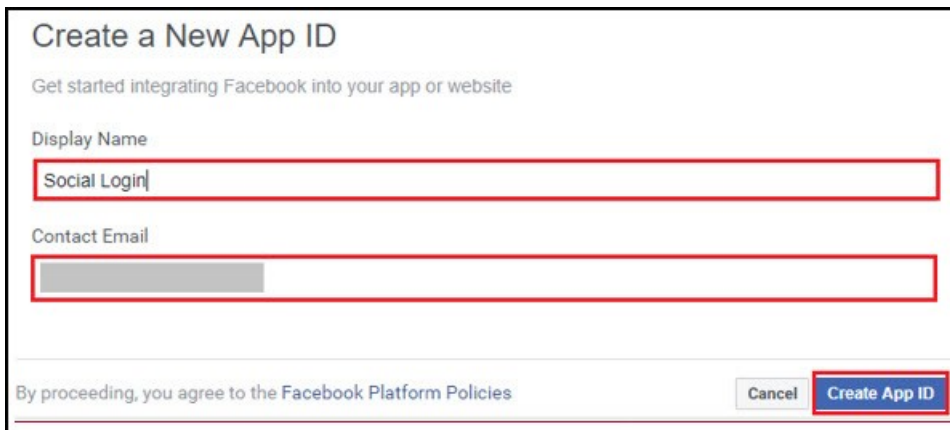


Facebook

1. Login to Facebook Account and access <https://developers.facebook.com/apps/> and click Add a New app.

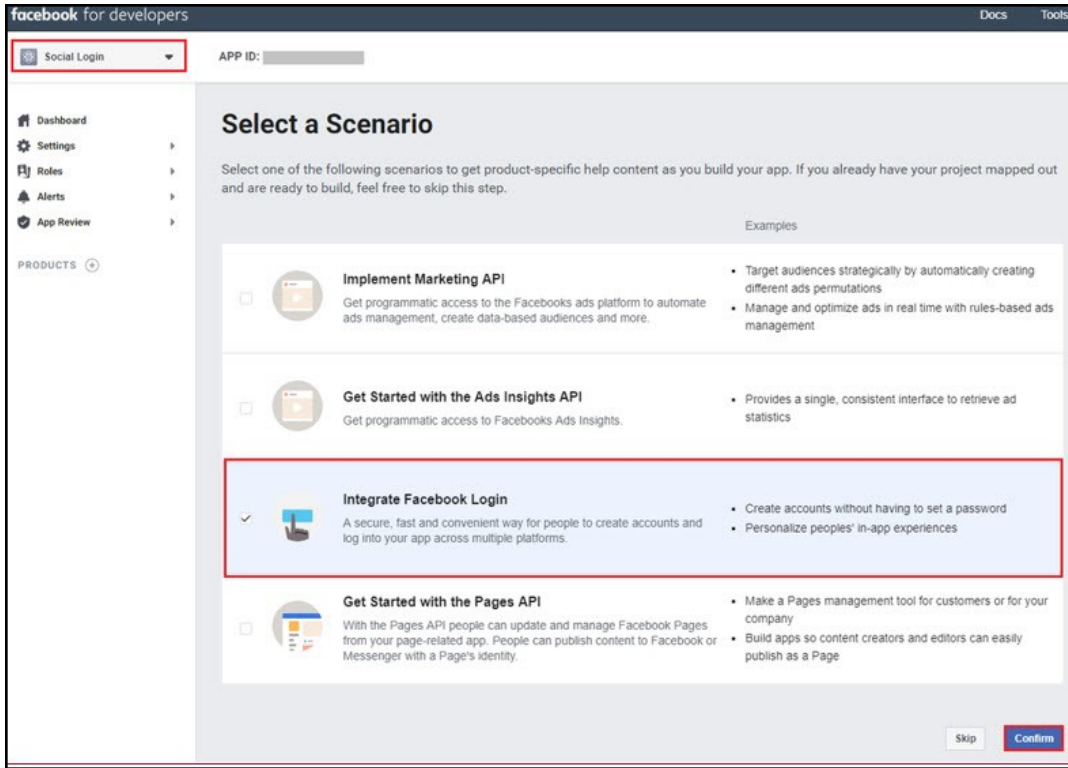


2. Enter App Display Name, Contact Email and click on Create App ID.

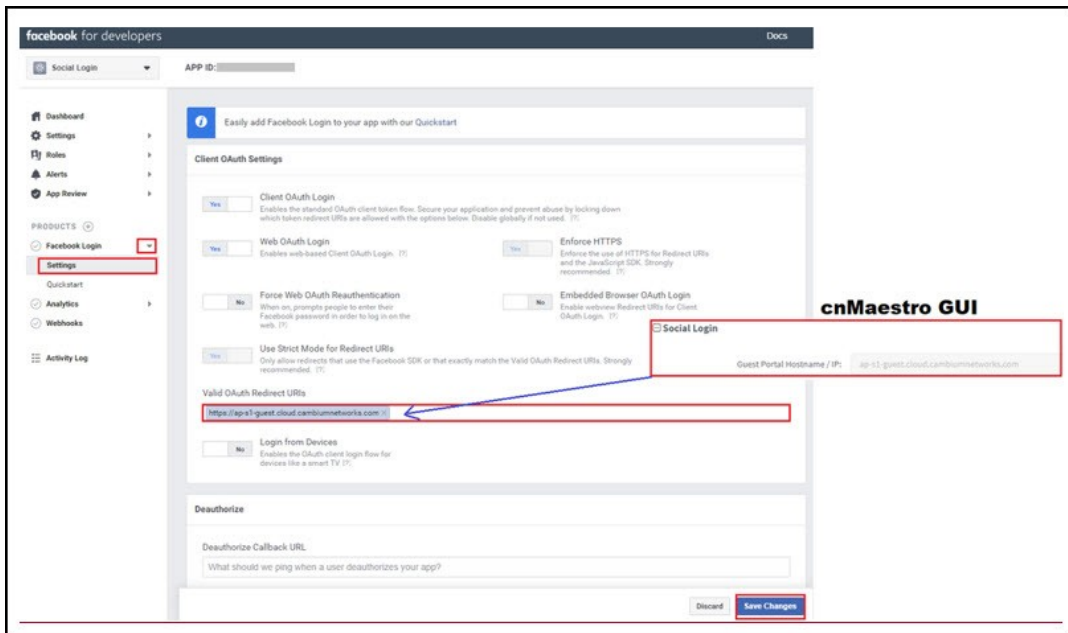


3. Select a Scenario as Integrate Facebook Login and click **Confirm**.





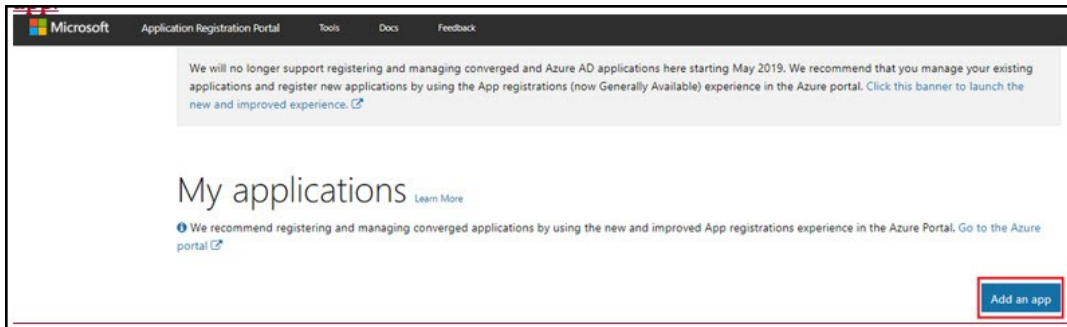
- Navigate to Settings tab under Facebook Login and add Guest Portal Hostname from cnMaestro c4000 Controller to Valid OAuth Redirect URLs section and click Save Changes.

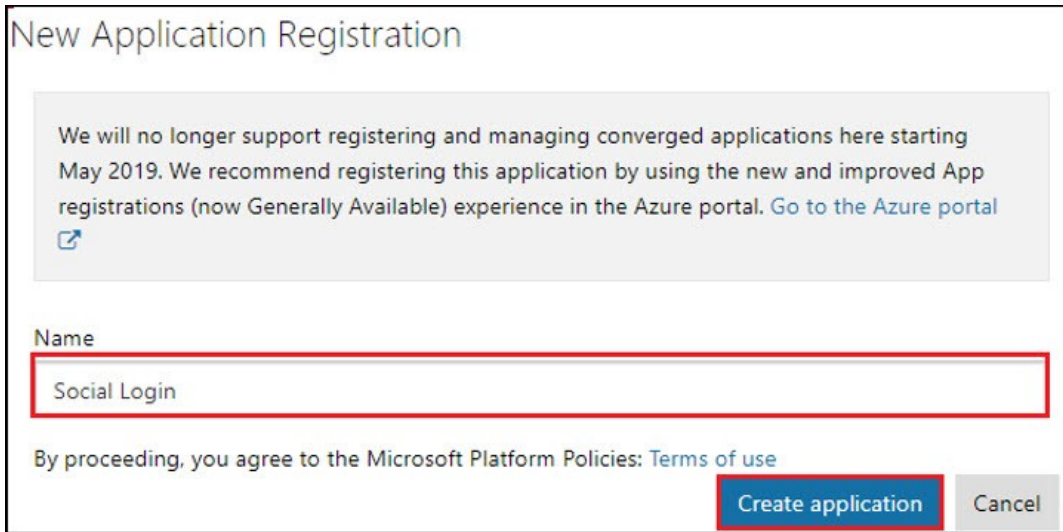


- Navigate to Settings > Basic and copy App ID and App Secret.

Office 365

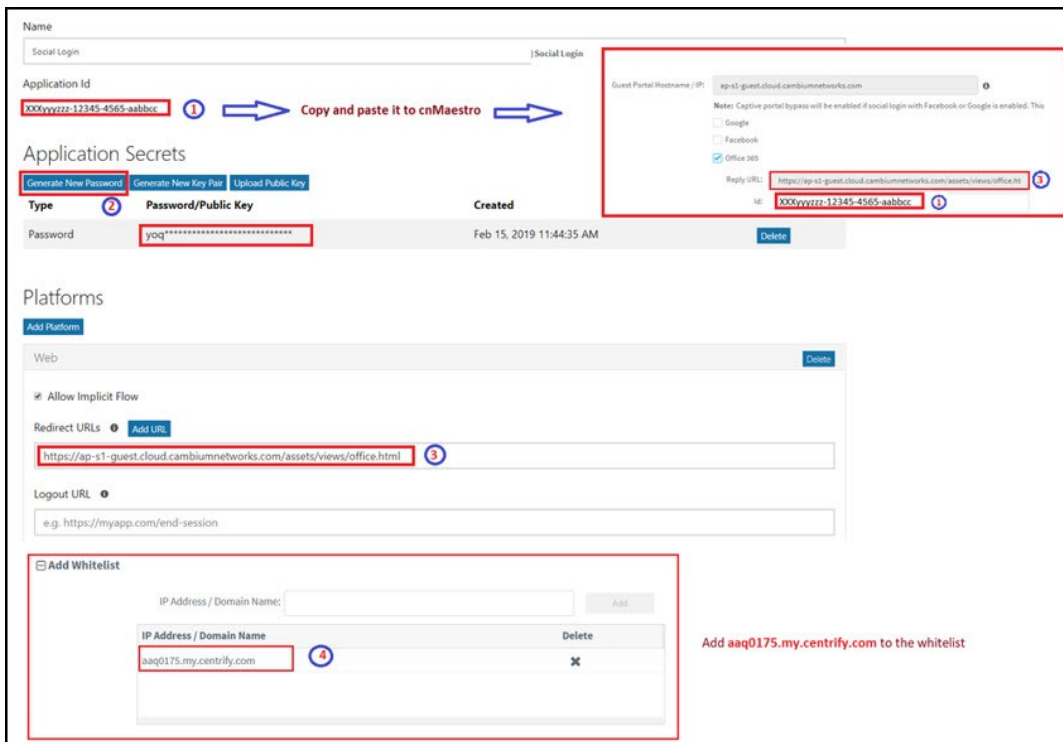
1. Login to Office 365 Account and access <https://apps.dev.microsoft.com/> and click Add an app.





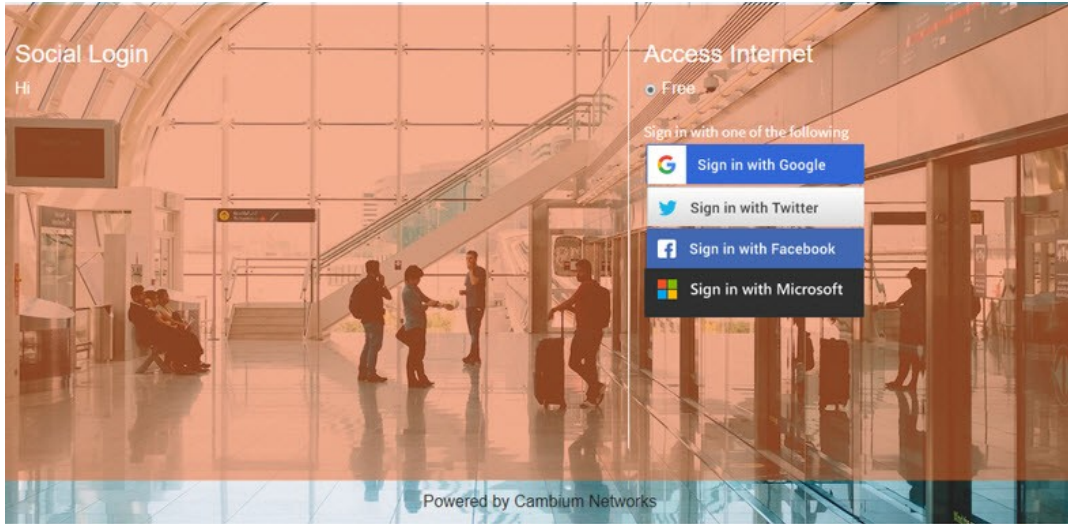
Add your App name and click Create application, it redirects to the App page.

1. Copy Application ID and paste it to cnMaestro c4000 Controller Guest Access page under Office 365.
2. Click **Generate New Password**.
3. Copy Reply URL from cnMaestro c4000 Controller and paste it under Redirect URLs.
4. Add my.centify.com to the Whitelist on the cnMaestro c4000 Controller.



## Sample Template

Sample of the client login page is displayed below:



### Mapping the device to Guest Access Portal in cnMaestro c4000 Controller

The administrator needs to configure the name of the Guest Access Portal in the device which redirects the device to cnMaestro c4000 Controller for client connectivity.



**Note**

The client will get the fully configured splash page for login only if the Access Point is into the server.

#### Configuration at Device Side

1. Login to the device.
2. Navigate to **Configuration > WLAN > Guest Access** page.

**Enable**

**Portal Mode**  Internal Access Point  External Hotspot  cnMaestro

**Guest Portal Name**   
Guest Portal Name which is hosted on cnMaestro

**Redirect**  HTTP-only Enable redirection for HTTP packets only

**Redirect User Page**   
Configure IP address for redirecting user to guest portal splash page

**Proxy Redirection Port**  Port number(1 to 65535)

**Inactivity Timeout**  Inactivity time in seconds (60 to 2592000)

**MAC Authentication Fallback**  Use guest-access only as fallback for clients failing MAC-authentication

**Extend Interface**  Configure the interface which is extended for guest access

3. Select the checkbox to enable **Guest Access**.
4. Choose the **Portal Mode** radio button as cnMaestro.

- In the Guest Portal Name dropbox, select the name of the portal that was created in cnMaestro and enter the respective parameters.

### Configuration at cnMaestro c4000 Controller Side

The administrator can push the configuration from cnMaestro c4000 Controller through policy or advanced configuration.

### Advanced Configurations (optional)

Template settings entered below will be merged into or appended to the profile created. This allows making configuration setting not supported or prevented by previous screens.

**Settings entered below are not validated or error checked, and may overwrite settings made in previous screen. You are solely responsible for ensuring that the resulting profile is valid and safe to use.**

```
!
wireless wlan 1
guest-access
guest-access portal-mode cnMaestro GAP1
!
```

# Chapter 14: Appliance

---

This chapter contains administrative, management and data configuration parameters specific to cnMaestro c4000 Controller.

This chapter provides the following information:

- [User Management](#)
- [Jobs](#)
- [Server](#)
- [Network](#)
- [Synchronize \(Sync\) Configuration](#)

## User Management

This section provides the following details:

- [Authentication](#)
- [Local Users](#)
- [Authentication Servers](#)
- [Session Management](#)

## Authentication

cnMaestro c4000 Controller supports a Primary mode of authentication and an optional Secondary mode. If the Primary mode is Local Users (users specified in cnMaestro c4000 Controller in the Users tab), no Secondary mode is available. If the Primary mode is an Authentication server, then the Secondary mode will be set to Users (and cannot be changed).

## Local Users

cnMaestro c4000 Controller allows you to add local users using the **Appliance > Users** page. Ten users are currently allowed in the system.

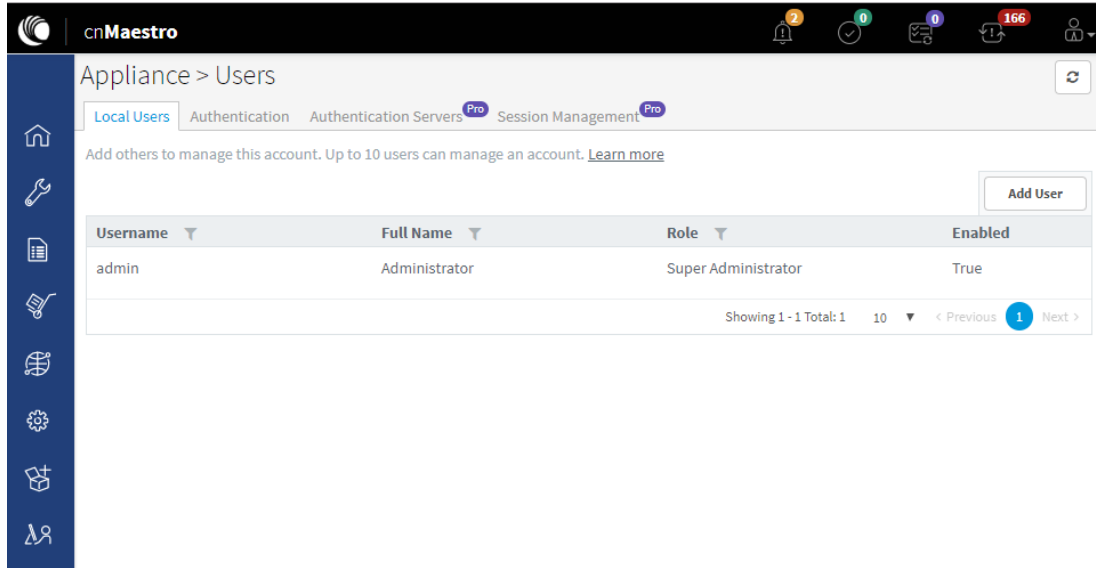


Figure 96 Adding Users

### Role-Based Access

Each user is assigned a Role that defines their authorization. On successful authentication, every request from this user is processed considering their Role.

cnMaestro c4000 Controller supports the following User Roles:

- **Super Administrator:** Super Administrators can perform all operations.
- **Administrator:** Administrators can modify cnMaestro c4000 Controller application functionality, but they are not able to edit User, API, or Server configuration.
- **Operator:** Operators can configure device-specific parameters and view all configuration.
- **Monitor:** Monitors have only view access.



**Note**

cnMaestro c4000 Controller allows the user to limit the number of concurrent sessions for each Role and display current active user sessions.

### Role-Mappings

The table below defines how Roles are authorized to access specific features.

Table 33 Role-Mappings


| Feature                 | Description  |
|-------------------------|--|
| Authentication Services | Create and configure Authentication servers. <ul style="list-style-type: none"> <li>• Super Administrator - All</li> <li>• Administrator - None</li> </ul> |

| Feature   | Description   |
|---|---|
|   | <ul style="list-style-type: none"> <li>• Operator - None</li> <li>• Monitor - None</li> </ul>   |
| API Management  | API Client. administration. <ul style="list-style-type: none"> <li>• Super Administrator - All</li> <li>• Administrator - None</li> <li>• Operator - None</li> <li>• Monitor - None</li> </ul>  |
| Application Operations                                  | Application-level operations such as to create, update and delete operations for Networks, Towers/Sites. Bulk device configuration. <ul style="list-style-type: none"> <li>• Super Administrator - All</li> <li>• Administrator - All</li> <li>• Operator - None</li> <li>• Monitor - None</li> </ul> |
| Application Settings                                    | Change global application configuration and onboarding key. <ul style="list-style-type: none"> <li>• Super Administrator - All</li> <li>• Administrator - All</li> <li>• Operator - None</li> <li>• Monitor - None</li> </ul>   |
| Configuration/Software Update and Scheduled Report Jobs | Manage configuration/software update and scheduled report related jobs <ul style="list-style-type: none"> <li>• Super Administrator - All</li> <li>• Administrator - All</li> <li>• Operator - All</li> <li>• Monitor - None</li> </ul>   |
| Data Tunnel   | Data tunnel configuration. <ul style="list-style-type: none"> <li>• Super Administrator - All</li> <li>• Administrator - All</li> <li>• Operator - View</li> <li>• Monitor - View (Statistics tab only)</li> </ul>  |



| Feature              | Description  |
|----------------------|--|
| Device Operations    | <p>Device operations such as reboot device, link test, connectivity test, tech support file download, and Wi-Fi performance test.</p> <ul style="list-style-type: none"> <li>• Super Administrator - All</li> <li>• Administrator - All</li> <li>• Operator - All</li> <li>• Monitor - None (Except Wi-Fi Performance test which is supported in cnMaestro c4000 Controller only)</li> </ul> |
| Device Overrides     | <p>Per-device configuration, including updating AP Group and applying the configuration.</p> <ul style="list-style-type: none"> <li>• Super Administrator - All</li> <li>• Administrator - All</li> <li>• Operator - All</li> <li>• Monitor - None</li> </ul>  |
| Global Configuration | <p>The ability to create and apply configuration for global features such as Templates, WLANs, AP Groups, auto-provisioning, and bulk sync configuration.</p> <ul style="list-style-type: none"> <li>• Super Administrator - All</li> <li>• Administrator - All</li> <li>• Operator -View</li> <li>• Monitor - None</li> </ul>   |
| Guest Portal         | <p>Guest Portal configuration.</p> <ul style="list-style-type: none"> <li>• Super Administrator - All</li> <li>• Administrator - All</li> <li>• Operator -View</li> <li>• Monitor - View (Sessions only)</li> </ul>  |
| Monitoring           | <p>Display of monitoring data at all levels, VM Monitoring</p> <ul style="list-style-type: none"> <li>• Super Administrator - All</li> <li>• Administrator - All</li> <li>• Operator - All</li> <li>• Monitor - View</li> </ul>  |
| Notifications        | <p>Alarms and Events management.</p> <ul style="list-style-type: none"> <li>• Super Administrator - All</li> </ul>   |

| Feature            | Description   |
|--------------------|---|
|                    | <ul style="list-style-type: none"> <li>• Administrator - All</li> <li>• Operator - All</li> <li>• Monitor - View</li> </ul>   |
| Onboarding         | <p>Device approval, modifying individual device configuration and performing the software updates.</p> <ul style="list-style-type: none"> <li>• Super Administrator - All</li> <li>• Administrator - All</li> <li>• Operator - All</li> <li>• Monitor - None</li> </ul> |
| Reporting          | <p>Report generation.</p> <ul style="list-style-type: none"> <li>• Super Administrator - All</li> <li>• Administrator - All</li> <li>• Operator - All</li> <li>• Monitor - All</li> </ul>   |
| Session Management | <p>Capability to view and logout other user's sessions.</p> <ul style="list-style-type: none"> <li>• Super Administrator - All</li> <li>• Administrator - All</li> <li>• Operator - None</li> <li>• Monitor - None</li> </ul>   |
| Software Images    | <p>Upload and delete device software images.</p> <ul style="list-style-type: none"> <li>• Super Administrator - All</li> <li>• Administrator - All</li> <li>• Operator - None</li> <li>• Monitor - None</li> </ul>  |
| Software Upgrade   | <p>Upgrade the device with the latest software.</p> <ul style="list-style-type: none"> <li>• Super Administrator - All</li> <li>• Administrator - All</li> <li>• Operator - All</li> <li>• Monitor - None</li> </ul>  |
| SNMP Configuration | <p>SNMPv2c configuration parameters.</p> <ul style="list-style-type: none"> <li>• Super Administrator - All</li> <li>• Administrator - All</li> </ul>   |

| Feature                        | Description  |
|--------------------------------|--|
|                                | <ul style="list-style-type: none"> <li>• Operator -View</li> <li>• Monitor - None</li> </ul>   |
| System Operations              | <p>System operations such as Reboot VM, change the log level, system upgrade, system monitoring, uploading SSL certificate, import/export server data and server tech dump, and upload/delete device software images.</p> <ul style="list-style-type: none"> <li>• Super Administrator - All</li> <li>• Administrator - All</li> <li>• Operator - None</li> <li>• Monitor - None</li> </ul>  |
| User Management                | <p>User management operations such as manage users and roles.</p> <ul style="list-style-type: none"> <li>• Super Administrator - All</li> <li>• Administrator - View</li> <li>• Operator - None</li> <li>• Monitor - None</li> </ul>   |
| Managed Service Provider (MSP) | <p>MSP operations such as modification of branded service managed account and user invitations.</p> <ul style="list-style-type: none"> <li>• Super Administrator - All</li> <li>• Administrator - View</li> <li>• Operator - None</li> <li>• Monitor - None</li> </ul> <div style="display: flex; align-items: center; margin-top: 10px;">  <div style="background-color: #e1f5fe; padding: 5px; border: 1px solid #ccc;"> <p><b>Note</b><br/>Operator/Monitor users are not permitted to move devices across managed accounts.</p> </div> </div> |

## Creating Users and Configuring User Roles

To add a user:

1. Navigate to **Appliance > Users** page.
2. Click the **Add User** button. The following window is displayed:

3. Enter the username in the **Username** text box.
4. Enter a full name for the user in the **Full Name** text box.
5. Provide a password for this user in the **Password** text box.
6. Confirm the password by entering the same password in the **Confirm Password** text box.

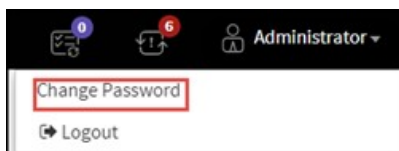
To configure User Roles:

7. Select any one of the roles for the user from the **Role** drop-down list:
  - Super Administrator
  - Administrator
  - Operator
  - Monitor
8. Choose the State as **Enabled** or **Disabled**.
9. Click the **Add User** button to save this user.

To edit or delete a user, click the Edit icon or the Delete icon against the user in the Appliance > Users page.

## Changing Password

Change Password option is available only for local users.



**Figure 97 Changing Password**

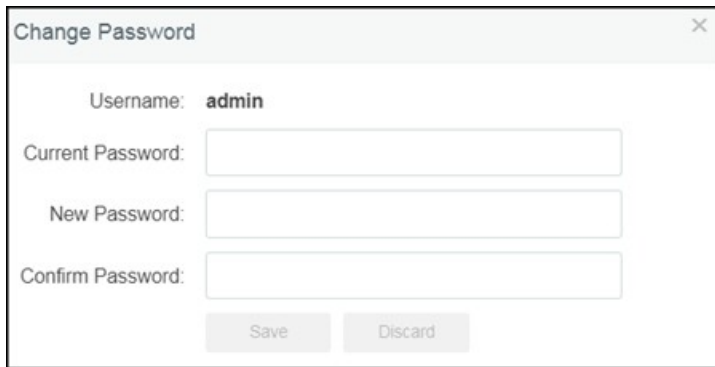
Ensure the primary Authentication must be local users in order to use the Change Password option. After changing the password, the current session will get logged out.

Also, ensure that there are no parallel sessions with the same users before going for the Change Password option. To change password:

1. Click the drop-down icon next to the username in the top right corner of the UI.
2. Enter the following details:

The Current Password in the Current Password text box.

- a. A new password for this user in the **New Password** text box.
- b. Confirm the password by entering the same password in the **Confirm Password** text box.
- c. Click **Save**.



The screenshot shows a 'Change Password' dialog box. The 'Username' field is populated with 'admin'. There are three empty text input fields for 'Current Password', 'New Password', and 'Confirm Password'. At the bottom of the dialog are two buttons: 'Save' and 'Discard'.

## Authentication Servers

cnMaestro c4000 Controller supports authentication and authorization with TACACS+, RADIUS, LDAP, and Active Directory servers, and is a pro feature.

### Authentication Server

Authentication Servers can be configured by cnMaestro c4000 Controller Super Administrators. The following operations are available:

- List All Authentication Servers
- Create New Authentication Server Configuration
- Secondary Server Authentication
- Edit an Existing Authentication Server Configuration
- Delete an Existing Authentication Server Configuration
- Verify the Role of the User
- Show User Groups for Active Directory

#### List All Authentication Servers

To view all the Authentication servers which are configured in cnMaestro c4000 Controller:

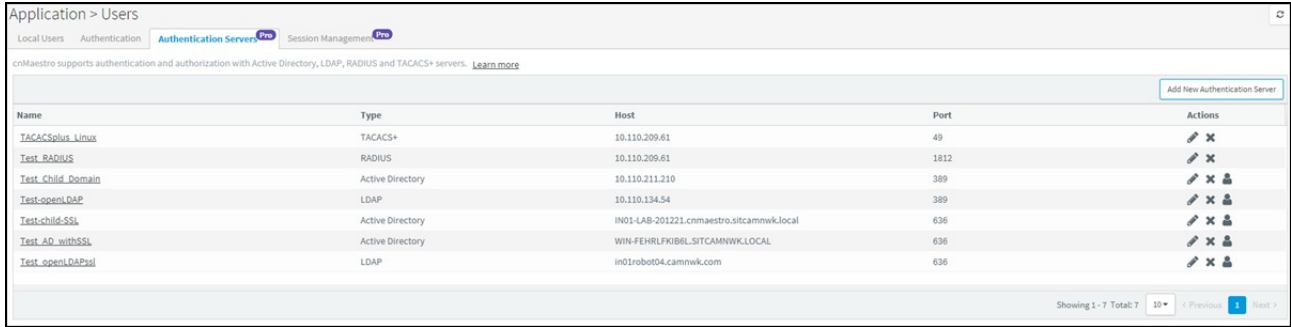
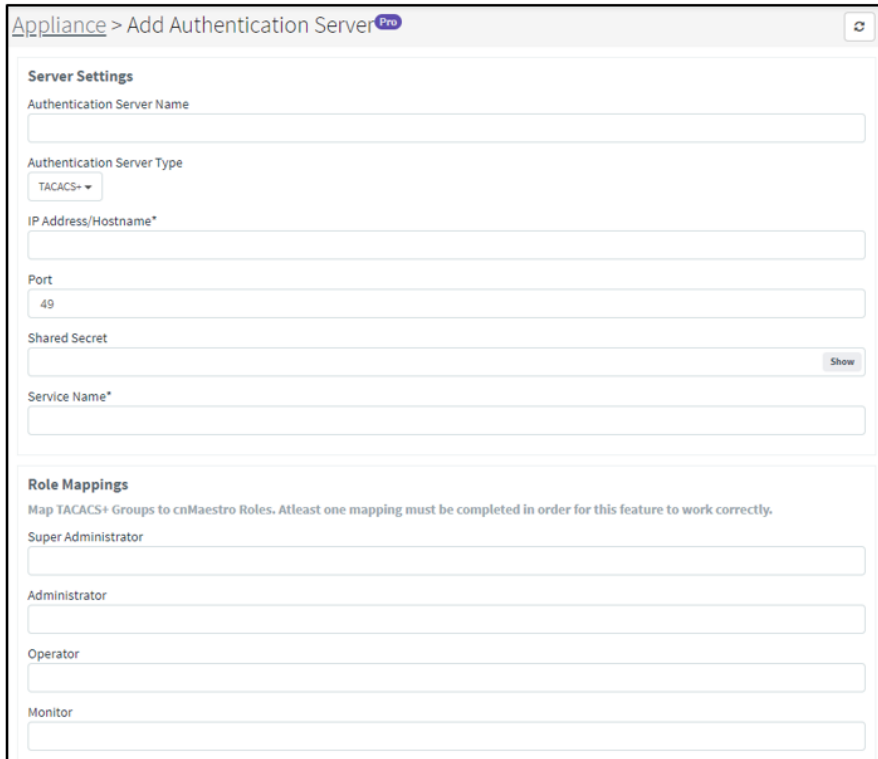


Figure 98 List of Authentication Servers

### Create New Authentication Server Configuration

1. Navigate to **Appliance > Users > Authentication Servers** page.
2. Click **Add New Authentication Server**.



### TACACS+

The fields that are present when TACACS+ server is selected are listed below:

Table 34 TACACS+ Parameters

| Parameter              | Description |
|------------------------|-------------|
| <b>Server Settings</b> |             |

| Parameter                  | Description  |
|----------------------------|--|
| Authentication Server Name | Global name of the server  |
| IP Address/Host name       | Enter the FQDN (Fully Qualified Domain Name) of the server or the IP address of the server.  |
| Port                       | TCP port of the server. (Default value is 49)  |
| Shared Secret              | Shared secret key for communicating with the server.   |
| Service Name               | Name defined in the service configuration table configured by TACACS+ server administrator. This is used to configure service and corresponding user groups.   |
| Role Mappings              | <p>TACACS+ user groups should be mapped to one or more cnMaestro c4000 Controller Roles. Refer Role-Based Access section to view the supported Roles on cnMaestro c4000 Controller.</p> <p>Enter the role strings that are configured in the TACACS+ server. At least one mapping must be completed in order for this feature to work correctly.</p> |

**Note**

TACACS+ server administrator should setup the service name and corresponding user group as per the configuration.

**RADIUS**

The fields present when RADIUS is selected are listed below:

The screenshot shows the 'Add Authentication Server' configuration page. The 'Authentication Server Type' dropdown menu is highlighted with a red dashed box and is set to 'RADIUS'. Other fields include 'Authentication Server Name', 'IP Address/Hostname', 'Port' (1812), and 'Shared Secret'. Below these is a 'Role Mappings' section with input fields for 'Super Administrator', 'Administrator', 'Operator', and 'Monitor'.

Table 35 RADIUS Parameters

| Parameter                  | Description  |
|----------------------------|--|
| <b>Server Settings</b>     |  |
| Authentication Server Name | Global name of the server.   |
| IP Address/Hostname        | Enter the FQDN (Fully Qualified Domain Name) of the server or the IP address of the server.  |
| Port                       | UDP port of the server. (Default is 1812).   |
| Shared Secret              | Shared secret key for communicating with the server.   |
| Role Mappings              | <p>Radius user groups should be mapped to one or more cnMaestro c4000 Controller Roles. Refer the Role-Based Access section to view cnMaestro c4000 Controller supported Roles.</p> <p>Enter the role strings that are configured in the Active Directory server. Atleast one mapping must be completed in order for this feature to work correctly.</p> |





**Note**

The RADIUS administrator should setup the user group as per configuration. The RADIUS administrator can choose a user group and the same should be configured on cnMaestro c4000 Controller Authentication server configuration.

**Active Directory**

The fields present when Active Directory is selected are listed below:

Figure 99 Appliance > Add Authentication Server Type > Active Directory

Table 36 Active Directory Parameters

| Parameter                  | Description   |
|----------------------------|---|
| <b>Server Settings</b>     |   |
| Authentication Server Name | Global name of the server.  |
| IP Address                 | IP address of the server.   |
| Port                       | TCP port of the server. (default 389). When SSL/TLS option is enabled, the port will automatically change to 636.   |
| SSL/TLS                    | Select this checkbox if Active Directory connection should be secured over SSL/ TLS as LDAPS. Browse and select the Root certificate of the Active Directory server in .PEM format. |

| Parameter     | Description  |
|---------------|--|
| BASE DN       | Distinguished name for Active Directory.   |
| Role Mappings | <p>Active Directory user groups should be mapped to one or more cnMaestro c4000 Controller Roles. Refer the Role-Based Access section to view cnMaestro c4000 Controller supported Roles.</p> <p>Enter the role strings that are configured in the Active Directory server. Atleast one mapping must be completed in order for this feature to work correctly.</p> |



**Note**

The Active Directory administrator should setup the user group as per configuration. The Active Directory administrator can choose a user group and the same should be configured on cnMaestro c4000 Controller Authentication server configuration.

Examples: CN=super-admin CN=admin CN=network CN=operator



**Note**

If Role is not configured in the TACACS+/RADIUS server or group is not configured in Active Directory, you cannot login to cnMaestro c4000 Controller.



**Note**

A user with valid credentials will not be able to login if:

1. cnMaestro c4000 Controller role to Authentication server's user group mapping is missing in the Authentication Server configuration
2. user group of the user is not configured in the Authentication server and is a required field for cnMaestro c4000 Controller login.

**LDAP**

The fields present when LDAP is selected are listed below:

The screenshot shows a web interface for configuring an authentication server. The breadcrumb is 'Appliance > Add Authentication Server'. The 'Server Settings' section includes:
 

- Authentication Server Name: [text input]
- Authentication Server Type: [LDAP] (highlighted with a red dashed box)
- IP Address/Hostname\*: [text input]
- Port: [636]
- Suffix\*: [text input, example: dc=EXAMPLE,dc=COM]
- Base DN\*: [text input, example: dc=EXAMPLE,dc=COM]
- LDAP Password\*: [password input, Show button]
- SSL/TLS Security: [checked checkbox]
- Certificate: [text input, Select File button]


 The 'Role Mappings' section includes:
 

- Super Administrator: [text input]
- Administrator: [text input]
- Operator: [text input]
- Monitor: [text input]

Figure 100 Appliance > Add Authentication Server Type > LDAP

Table 37 LDAP Parameters

| Parameter                  | Description   |
|----------------------------|---|
| <b>Server Settings</b>     |   |
| Authentication Server Name | Global name of the server.  |
| IP Address/Hostname        | Provide IP address for LDAP and hostname of the server if SSL/TLS is enabled. |
| Port                       | TCP port of the server. (Default for LDAP is 389 and for LDAPs is 636).       |
| Suffix                     | Suffix is the DNS name. For eg: dc= xyz, dc=com.                              |

| Parameter        | Description   |
|------------------|---|
| Base DN          | Base DN is generally the Admin DN used to log in to LDAP server. For eg: cn=admin,dc=xyz,dc=com.  |
| LDAP Password    | LDAP Password is the admin password used by Admin DN to log in.   |
| SSL/TSL Security | <p>Select this checkbox LDAP connection should be secured over SSL/TLS as LDAPS. Browse and select the Root certificate of the Active Directory server PEM format.</p> <div style="display: flex; align-items: center;">  <div style="background-color: #e1f5fe; padding: 10px; border: 1px solid #ccc;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>If you enable SSL/TSL Security checkbox, the default port will appear as 636 in the Port text box.</li> <li>If you disable SSL/TSL Security checkbox, the default port will appear as 389 in the Port text box.</li> </ul> </div> </div> |
| Certificate      | Browse and update with root certificate in. PEM format.   |
| Role Mappings    | <p>Radius user groups should be mapped to one or more cnMaestro c4000 Controller Roles. Refer the Role-Based Access section to view cnMaestro c4000 Controller supported Roles.</p> <p>Enter the role strings that are configured in the Active Directory server. Atleast one mapping must be completed in order for this feature to work correctly.</p>  |

## Secondary Server Authentication

In addition to the primary server authentication, cnMaestro c4000 Controller now supports configuration for secondary external server for authentication. Secondary authentication and primary authentication servers should be different.



### Note

The same authentication will not be shown on the server. For example, If we select primary as Test-TAC-IP, then we cannot select the same in secondary authentication.

Tertiary authentication will always default to the local users. Local users will be logged in only when primary and secondary are not reachable or when the services are not being run on the authentication server. If the primary server is not reachable then fallback happens to the secondary authentication server. If the secondary authentication server is not reachable then fallback happens to tertiary authentication. If the primary authentication server is running properly then users belonging to a primary authentication server can only be logged in. If the secondary authentication server is running properly then users belonging to a secondary authentication server can only be logged in.

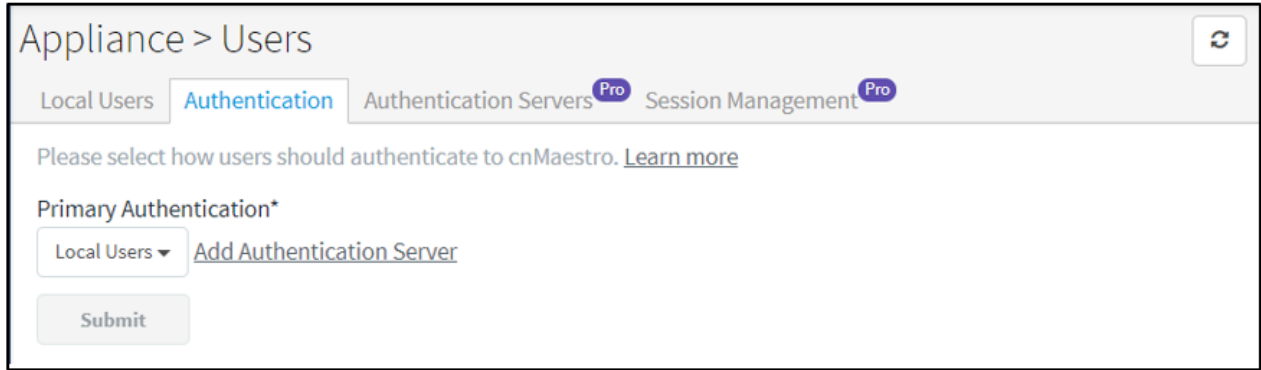
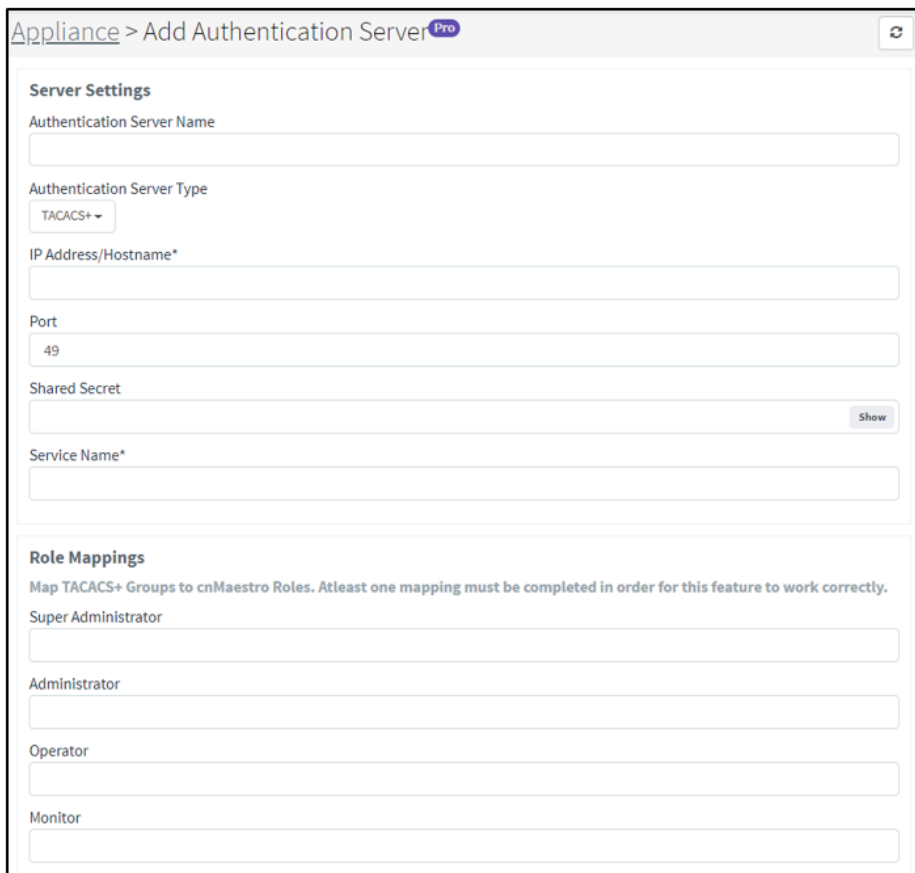


Figure 101 Secondary Server Authentication

### Edit an Existing Authentication Server Configuration

To edit an existing Authentication Server configuration:

1. Navigate to List all **Authentication Servers** page.
2. Click the name of the server or the **Edit** button.



Refer to Create New Authentication Server Configuration section for an explanation of fields on the Edit page.

## Delete an Existing Authentication Server Configuration


To delete an existing Authentication Server configuration:

1. Navigate to List all Authentication Servers page.
2. Click the **delete** button.

The primary authentication order will change as Local Authentication if this server is setup as Primary Authentication under Manage Authentication Server Authentication section.

## Verify the Role of the User


To know and verify the role of the Active Directory user:

1. Navigate to List all Authentication Servers page.
2. Click the test icon () next to any of the Active Directory type. The following window appears:



3. Provide the following details:
  - a. Active Directory User ID
  - b. Active Directory Password
  - c. Account to Verify
4. Click the Test button.

To know and verify the role of the LDAP user:

1. Navigate to List all Authentication Servers page.
2. Click the test icon () next to any of the LDAP types. The following window appears:



3. Provide the name of the account to verify in the Account to Verify text box.
4. Click the Test button.

## Show User Groups for Active Directory

cnMaestro c4000 Controller administrator can view user groups for Active Directory server type configuration by providing valid user credentials to login to Active Directory. The user details can then be viewed as shown below:



The screenshot shows a dialog box titled "Test Accounts (AD\_SSL\_Test)". It has three text input fields with the following labels: "Active Directory User ID\*", "Active Directory password\*", and "Account to Verify\*". At the bottom of the dialog, there are two buttons: "Test" and "Cancel".

1. Enter the user ID for Active Directory in the Active Directory User ID text box. The User ID should be a valid string (Eg: user@example.com).
2. Enter the password for Active Directory in the Active Directory Password text box.
3. Enter the account name to verify in the Account to Verify text box.

For searching the group of the user, the user's ID should follow the user@example.com format.

## Session Management

View and optionally log out current cnMaestro c4000 Controller administrator sessions. The users with Super Administrator Role can logout all other user's sessions and the users with Administrator Roles can log out Operator and Monitor accounts.

### Sessions

Displays detailed information on the user sessions.

The screenshot shows the cnMaestro web interface. The top navigation bar includes 'Appliance > Users' and 'Session Management'. Below the navigation, there is a search bar and a table of active sessions. The table has columns for Username, Role, Client IP, Start Time, Duration, and Logou (Logout). The sessions listed are all for 'Administrator' users with the role 'Super Administrator'.

| Username      | Role                | Client IP      | Start Time                      | Duration   | Logou    |
|---------------|---------------------|----------------|---------------------------------|------------|----------|
| Administrator | Super Administrator | 10.110.35.112  | Tue Sep 17 2019 17:58:41 GM...  | 7d 21h 5m  | [Logout] |
| Administrator | Super Administrator | 10.110.35.112  | Tue Sep 17 2019 17:58:42 GM...  | 7d 21h 5m  | [Logout] |
| Administrator | Super Administrator | 10.110.205.236 | Tue Sep 17 2019 18:59:19 GM...  | 7d 20h 4m  | [Logout] |
| Administrator | Super Administrator | 10.110.35.135  | Thu Sep 19 2019 16:34:40 GM...  | 5d 22h 29m | [Logout] |
| Administrator | Super Administrator | 10.110.35.163  | Fri Sep 20 2019 11:06:07 GMT... | 5d 3h 58m  | [Logout] |
| Administrator | Super Administrator | 10.110.35.112  | Fri Sep 20 2019 15:10:40 GMT... | 4d 23h 53m | [Logout] |

Figure 102 Session Management &gt; Sessions

## Jobs

This section covers the following Job operations that are performed in cnMaestro.

- [Configuration Update](#)
- [Software Update Jobs](#)
- [Reports](#)
- [Actions](#)

## Configuration Update

After applying the configuration, the Configuration Job-status is viewed by navigating to **Appliance > Jobs** (for Wireless LAN devices). When the configuration is pushed from the Sync Configuration page, a Configuration job will be created in the background.



Appliance > Jobs

Configuration Update | Software Update | Reports | Actions

| ID   | Details                          | Target            | Created by    | Created on         | Completed on       | Parallel | Stop on Error | Sector Priority | Status   |
|------|----------------------------------|-------------------|---------------|--------------------|--------------------|----------|---------------|-----------------|--|
| 2... | 52 cnPilot Enterprise (E-Seri... | Appliance         | Administrator | Sep 26, 2019 15:46 | Sep 26, 2019 15:47 | 10       | false         | N/A             | Completed: <span style="width: 100%; background-color: green;"></span> |
| 2... | 16 device(s)                     |                   | Auto-Sync     | Sep 26, 2019 15:18 | Sep 26, 2019 15:19 | 15       | false         | N/A             | Completed: <span style="width: 100%; background-color: green;"></span> |
| 2... | 178 device(s)                    |                   | Auto-Sync     | Sep 26, 2019 15:14 | Sep 26, 2019 15:18 | 15       | false         | N/A             | Completed: <span style="width: 100%; background-color: green;"></span> |
| 2... | 177 device(s)                    |                   | Auto-Sync     | Sep 26, 2019 15:04 | Sep 26, 2019 15:08 | 15       | false         | N/A             | Completed: <span style="width: 100%; background-color: green;"></span> |
| 2... | 13 cnPilot Enterprise (E-Seri... | Mumbai_test-AP... | Administrator | Sep 26, 2019 14:23 | Sep 26, 2019 14:28 | 10       | false         | N/A             | Completed: <span style="width: 100%; background-color: green;"></span> |
| 2... | 61 device(s)                     |                   | Auto-Sync     | Sep 26, 2019 14:22 | Sep 26, 2019 14:28 | 15       | false         | N/A             | Completed: <span style="width: 100%; background-color: green;"></span> |
| 2... | 1 device(s)                      |                   | Auto-Sync     | Sep 26, 2019 14:21 | Sep 26, 2019 14:21 | 15       | false         | N/A             | Completed: <span style="width: 100%; background-color: green;"></span> |
| 2... | 1 cnPilot e400 device(s)         | Appliance_E400    | Administrator | Sep 26, 2019 14:20 | Sep 26, 2019 14:20 | -        | false         | N/A             | Completed: <span style="width: 100%; background-color: green;"></span> |
| 2... | 1 cnPilot e400 device(s)         | Appliance_E400    | Administrator | Sep 26, 2019 14:11 | Sep 26, 2019 14:11 | -        | false         | N/A             | Completed: <span style="width: 100%; background-color: green;"></span> |
| 2... | 1 device(s)                      |                   | Auto-Sync     | Sep 26, 2019 14:05 | Sep 26, 2019 14:05 | 15       | false         | N/A             | Completed: <span style="width: 100%; background-color: green;"></span> |

Showing 1 - 10 Total: 2,921 10 | Previous 1 2 3 4 5 ... 293 Next >

Figure 103 Appliance > Jobs > Configuration update



**Note**

Configuration jobs will skip devices that are offline. With manual synchronization, they need to be synchronized by the administrator.

For more information on Wi-Fi AP configuration, refer the following URLs:

Unique per-Device values in Profiles Using User-Defined Overrides

AP Groups and Overrides for Wi-Fi Devices.

Migrating from Templates to Profiles.

## Software Update Jobs

The software update of devices in cnMaestro is either Manual or Auto. **Appliance > Jobs > Software Update** displays the current job that is triggered either manually or automatically. This tab provides more details of job status, which will be helpful for debugging on failure.

Appliance > Jobs

Configuration Update | **Software Update** | Reports | Actions

Manual Auto

| ID | Details                                  | Image Type | Occurrence | Target    | Created by    | Created on         | Completed on       | Status     |  |
|----|--|------------|------------|-----------|---------------|--------------------|--------------------|------------|--|
| 40 | 18 cnPilot Enterprise (E-Series) Devi... | Device     | Now        | 4.0-b11   | Administrator | Sep 26, 2019 14:06 | Sep 26, 2019 14:09 | Aborted:   |  |
| 39 | 166 cnPilot Enterprise (E-Series) Dev... | Device     | Now        | 4.0-b11   | Administrator | Sep 25, 2019 20:04 | Sep 25, 2019 20:48 | Completed: |  |
| 38 | 10 cnPilot Enterprise (E-Series) Devi... | Device     | Now        | 3.11.3-b9 | Administrator | Sep 25, 2019 12:44 | Sep 25, 2019 12:51 | Completed: |  |
| 37 | 15 cnPilot Enterprise (E-Series) Devi... | Device     | Now        | 3.11.3-b9 | Administrator | Sep 25, 2019 12:25 | Sep 25, 2019 12:37 | Completed: |  |
| 36 | 106 cnPilot Enterprise (E-Series) Dev... | Device     | Now        | 4.0-b11   | Administrator | Sep 24, 2019 20:34 | Sep 24, 2019 21:08 | Completed: |  |
| 35 | 10 cnPilot Enterprise (E-Series) Devi... | Device     | Now        | 3.9.2-r11 | Administrator | Sep 24, 2019 20:34 | Sep 24, 2019 20:40 | Completed: |  |
| 34 | 1 cnPilot Enterprise (E-Series) Devi...  | Device     | Now        | 4.0-b11   | Administrator | Sep 24, 2019 20:09 | Sep 24, 2019 20:09 | Completed: |  |
| 33 | 179 cnPilot Enterprise (E-Series) Dev... | Device     | Now        | 4.0-b11   | Administrator | Sep 24, 2019 20:03 | Sep 24, 2019 20:09 | Completed: |  |
| 32 | 127 cnPilot Enterprise (E-Series) Dev... | Device     | Now        | 3.11.2-r2 | Administrator | Sep 24, 2019 19:42 | Sep 24, 2019 20:00 | Completed: |  |
| 31 | 142 cnPilot Enterprise (E-Series) Dev... | Device     | Now        | 4.0-b11   | Administrator | Sep 24, 2019 19:35 | Sep 24, 2019 19:41 | Completed: |  |

Showing 1 - 10 Total: 40 10 | Previous 1 2 3 4 Next >

Figure 104 Appliance > Jobs > Software update

## Reports

**Appliance > Jobs > Reports** displays all the reports generated and are available to download for users. More details on Reports can be found in [Chapter 8: Reports](#).

Appliance > Jobs

Configuration Update | Software Update | **Reports** | Actions

Displays the list of scheduled reports created by different users. [Learn more](#)

| ID | Type        | Source  | Schedule | Starts At          | Ends After         | Created by    | Created on         | Status                            | Last Report      |  |
|----|-------------|---------|----------|--------------------|--------------------|---------------|--------------------|-----------------------------------|------------------|--|
| 16 | Devices     | System  | Now      | Sep 26, 2019 14:42 | Sep 26, 2019 14:42 | Administrator | Sep 26, 2019 14:42 | Completed                         | Sep 26, 2019 ... |  |
| 15 | Devices     | System  | Now      | Sep 26, 2019 14:42 | Sep 26, 2019 14:42 | Administrator | Sep 26, 2019 14:42 | Completed                         | Sep 26, 2019 ... |  |
| 14 | Devices     | System  | Now      | Sep 26, 2019 14:08 | Sep 26, 2019 14:08 | Administrator | Sep 26, 2019 14:08 | Completed                         | Sep 26, 2019 ... |  |
| 13 | Devices     | System  | Now      | Sep 24, 2019 20:14 | Sep 24, 2019 20:14 | Administrator | Sep 24, 2019 20:14 | Completed                         | Sep 24, 2019 ... |  |
| 12 | Devices     | System  | Daily    | Sep 13, 2019 02:15 | Sep 13, 2019 02:15 | Administrator | Sep 12, 2019 14:10 | Completed                         | Sep 13, 2019 ... |  |
| 11 | Performance | System  | Now      | Aug 20, 2019 13:10 | Aug 20, 2019 13:10 | Administrator | Aug 20, 2019 13:10 | Completed                         | Aug 20, 2019 ... |  |
| 10 | Devices     | System  | Daily    | Aug 21, 2019 02:15 | Jan 01, 2039 02:15 | Administrator | Aug 20, 2019 13:10 | Scheduled (Sep 27, 2019 02:15:00) | Sep 26, 2019 ... |  |
| 9  | Devices     | System  | Now      | Aug 20, 2019 13:09 | Aug 20, 2019 13:09 | Administrator | Aug 20, 2019 13:09 | Completed                         | Aug 20, 2019 ... |  |
| 8  | Devices     | System  | Now      | Aug 05, 2019 19:49 | Aug 05, 2019 19:49 | Administrator | Aug 05, 2019 19:48 | Completed                         | Aug 05, 2019 ... |  |
| 7  | Clients     | default | Now      | Jul 24, 2019 13:32 | Jul 24, 2019 13:32 | Administrator | Jul 24, 2019 13:32 | Completed                         | Aug 05, 2019 ... |  |

Showing 1 - 10 Total: 16 10 | Previous 1 2 Next >

Figure 105 Appliance > Jobs > Reports

## Actions

**Appliance > Jobs > Actions** display all the actions performed by the administrator. Below is the sample figure for the bulk reboot action executed by the user.

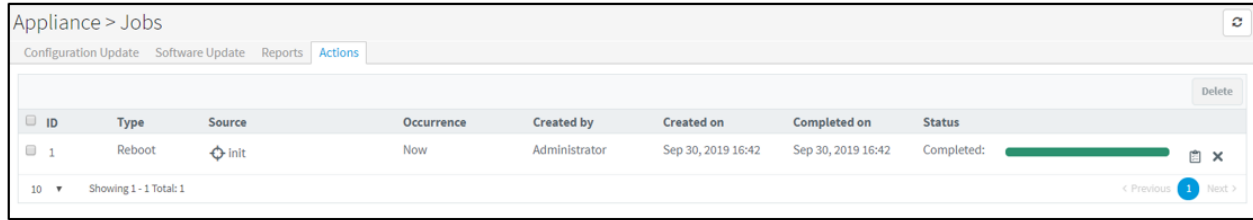


Figure 106 Appliance > Jobs > Actions

## Server

This section describes the following details:

- [Dashboard](#)
- [Monitoring](#)
- [Settings](#)
- [Operations](#)
- [Diagnostics](#)
- [SSL Certificates](#)
- [Software Images](#)

## Dashboard

The below table lists the configured parameters w.r.t to cnMaestro c4000 Controller. The following are the description of the parameters that are viewable in the dashboard.

Table 38 Appliance > Server > Dashboard parameters

| Parameters  | Description  |
|---|--|
| <b>Appliance &gt; Server &gt; Dashboard &gt; Device details</b> |  |
| MAC   | Displays the management interface MAC address                |
| HOST NAME   | Displays the configured hostname.                            |
| SERIAL NO   | Displays the serial number of the cnMaestro c4000 Controller |
| MODEL NO  | Displays the model number of the cnMaestro c4000 Controller  |
| ACTIVE SOFTWARE   | Displays the current operating software.                     |
| UPTIME  | Displays the duration of the time system is powered on.      |

| Parameters   | Description   |
|--|---|
| CURRENT CPU USAGE  | Provides information w.r.t to current CPU usage of cnMaestro c4000 Controller.        |
| CURRENT MEMORY USAGE   | Provides information w.r.t to the current memory usage of cnMaestro c4000 Controller. |
| <b>Appliance &gt; Server &gt; Dashboard &gt; Port Status</b> |   |
| NAME   | Displays the Ethernet interface name.   |
| STATUS   | Displays the current operating status of the Ethernet interface.                      |
| AUTO NEGOTIATION   | Displays the current negotiation of the Ethernet interface.                           |
| <b>Appliance &gt; Server &gt; Dashboard &gt; Data Store</b>  |   |
| It is a repository that stores logs from the appliance.      |   |
| <b>Appliance &gt; Server &gt; Dashboard &gt; Used Store</b>  |   |
| It is a list of user files on the device.                    |   |

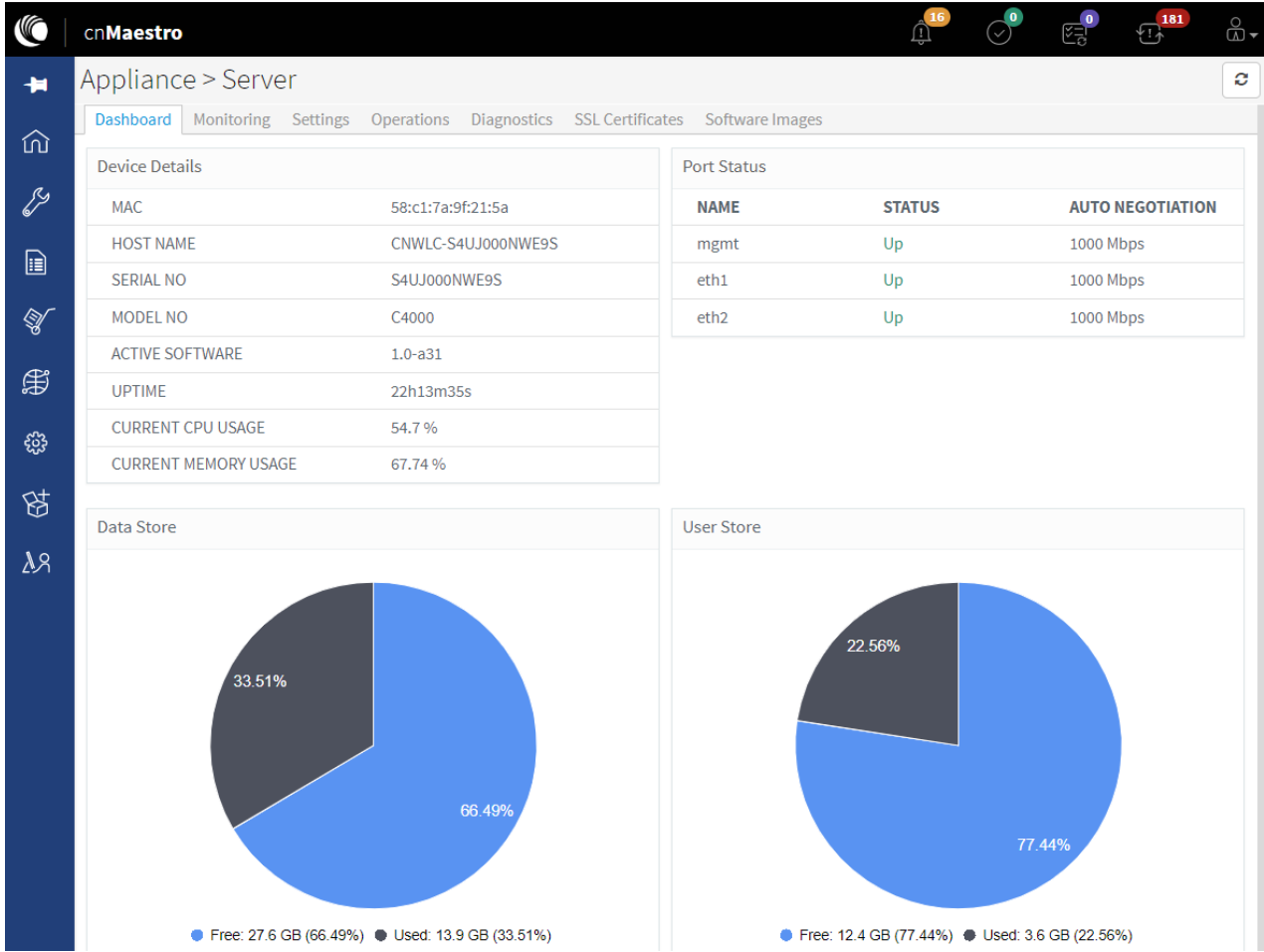


Figure 107 Appliance > Server > Dashboard

## Monitoring

The below table lists the current information of the hardware capabilities of the cnMaestro c4000 Controller. The following are the description of the parameters that are viewable in Monitoring. The hardware resource of cnMaestro c4000 Controller is distributed across cnMaestro and rest of the system.

Table 39 Configure: Appliance > Server > Monitoring parameters

| Parameters   | Description   |
|--|---|
| <b>Appliance &gt; Server &gt; Monitoring &gt; Appliance / cnMaestro VM</b> |   |
| CPU Utilization  | Provides the current CPU utilization of the system.   |
| CPU Load   | Provides information of CPU over or underutilization in a system. It provides additional information such as the number of processes executed by the CPU. |

| Parameters   | Description   |
|--------------|---|
| CPU Jumps    | It provides information on the usage of shared and independent resources redefined in the system. |
| Memory Usage | Provides information on current memory usage of the system.                                       |

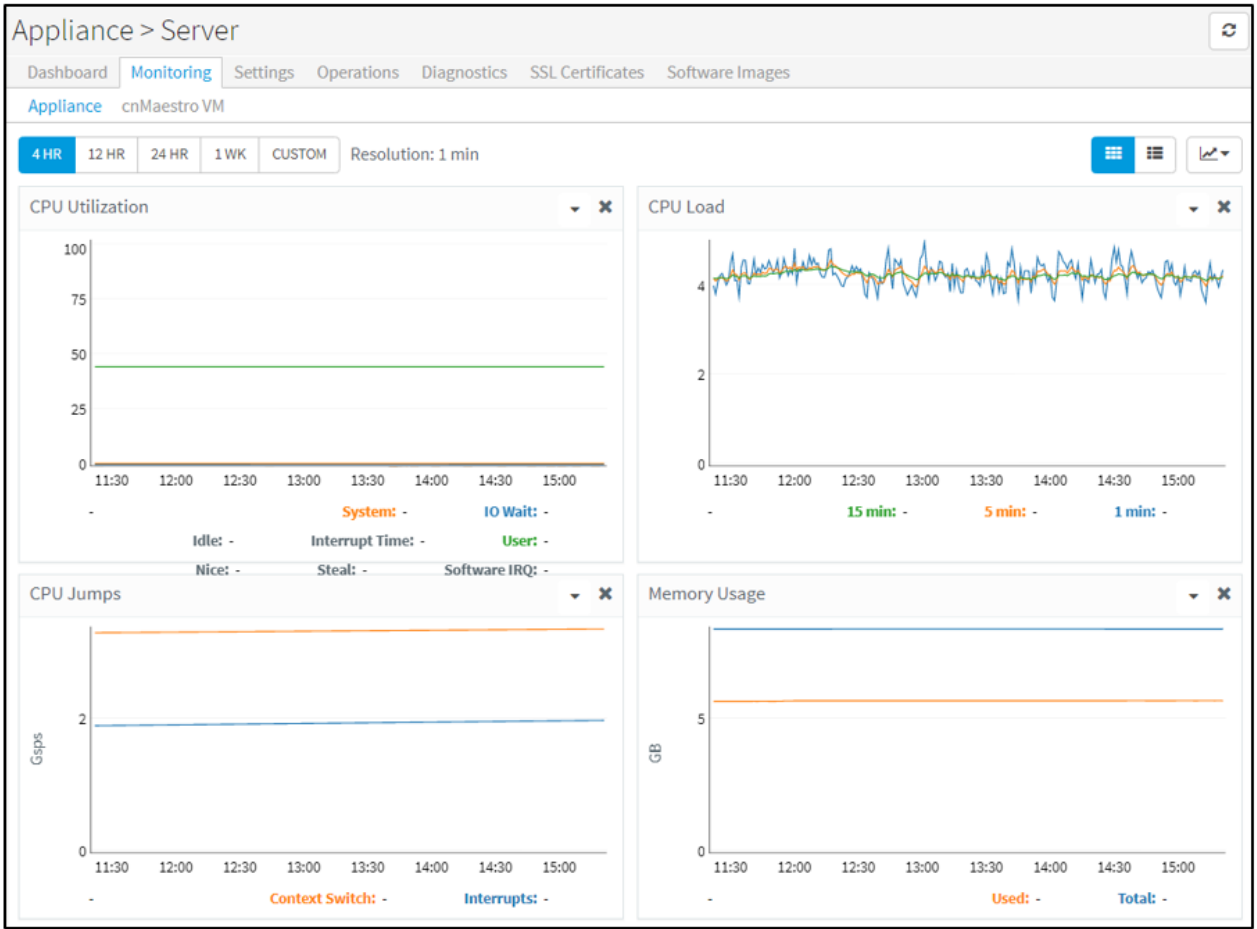


Figure 108 Appliance > Server > Monitoring

## Settings

The below table lists the system level configurable parameters. The user has a provision to configure system details in this section.

Table 40 Appliance > Server > Settings parameters

| Parameters | Description | Range | Default |
|------------|-------------|-------|---------|
|------------|-------------|-------|---------|

| <b>Appliance &gt; Server &gt; Settings &gt; Basic</b>                  |   |   |                              |
|--|---|---|------------------------------|
| System Name  | Provision to configure the name of the system.  | - | cnMaestro                    |
| Country  | Displays the configured country during installation and also provides the user to change the country. | - | -                            |
| <b>Appliance &gt; Server &gt; Settings &gt; System Configuration</b>   |   |   |                              |
| Host Name  | Provision to configure the hostname of the system   |   | CNWLC-<br><serial<br>number> |
| Primary DNS  | Provision to configure primary DNS server IP/hostname.  | - | -                            |
| Secondary DNS  | Provision to configure secondary DNS server IP/hostname.  | - | -                            |
| NTP Server Interface   | Provision to configure the interface through which the system synchronizes time with the NTP server.  |   | Management                   |
| NTP Server1  | Provision to configure primary NTP server IP/hostname.  |   |                              |
| NTP Server2  | Provision to configure secondary NTP server IP/hostname.  |   |                              |
| Description  | User-configurable text.   |   |                              |
| Management SSH   | Provision to enable/disable SSH on management interface.  |   | Enabled                      |
| CLI Password   | Provision to configure the SSH password through the management interface.                             |   | admin                        |
| <b>Appliance &gt; Server &gt; Settings &gt; Configure Email Server</b> |   |   |                              |
| Enable SMTP Server   | Provision to enable/disable SMTP server configuration.  |   | disabled                     |
| Port   | Configure the port as per the SMTP server requirements.   |   | -                            |
| Host   | Configure the SMTP server IP/hostname.  |   |                              |
| Username   | Configure username as per SMTP server requirements.   |   | -                            |
| Password   | Configure the password as per SMTP server requirements.   |   | -                            |

|   |  |  |     |
|---|--|--|-----|
| Sender Email  | Provision to configure sender email address.   |  |     |
| Encryption  | <p>Following encryptions are supported</p> <ul style="list-style-type: none"> <li>• None</li> <li>• TLS</li> <li>• STARTTLS</li> </ul> |  | TLS |
| Ignore server certificate validation                                  | Provision to enable/disable server certificate validation.   |  |     |
| CACertificate   | Provision to upload CA certificate.  |  |     |
| Send Test Mail  | Provision to validate the configured email server.   |  |     |
| <b>Appliance &gt; Server &gt; Settings &gt; Login Security Banner</b> |  |  |     |
| Enable Security Banner during Login                                   | Provision to enable/disable security banner during login.  |  |     |
| Enable User must accept security banner before login                  | Provision to enable/disable acceptance in security banner before login.  |  |     |
| Security Banner Notice  | Provision to configure user text such as disclaimers.  |  |     |



Appliance > Server ↻

Dashboard Monitoring **Settings** Operations Diagnostics SSL Certificates Software Images

---

**Basic**

System Name  
 ⓘ

Country

---

**System Configuration**

Host Name

Primary DNS

Secondary DNS

NTP Server Interface  
 Management  Data

NTP Server1

NTP Server2

Description

Management SSH

CLI Password

---

**Configure Email Server**

Configure SMTP server to manage cnMaestro users pertaining to MSP and to send email notifications.

Enable SMTP Server

Port\*

Host\*

Username

Password  
 Show

Sender Email\*

Encryption  
 None  TLS  STARTTLS

Ignore server certificate validation

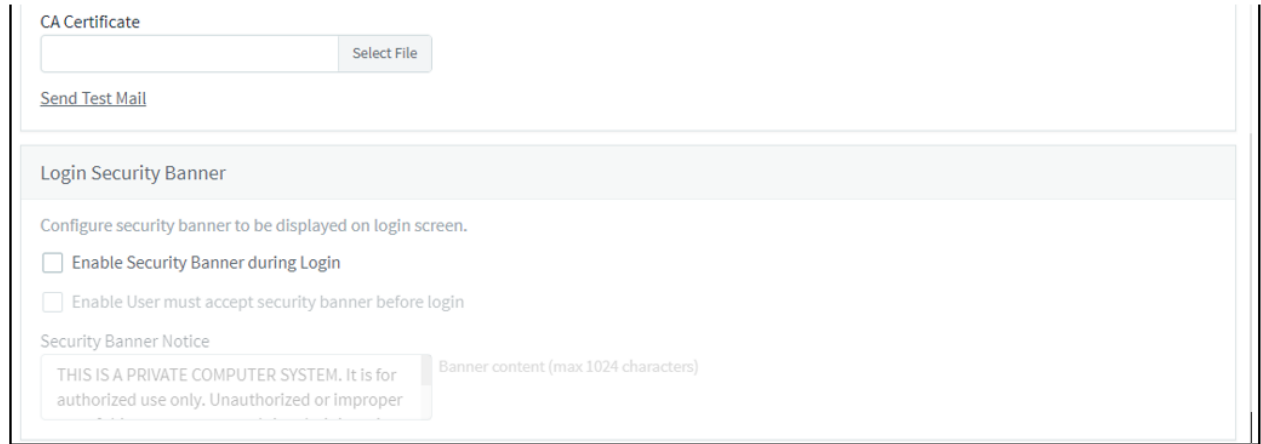


Figure 109 Appliance > Server > Settings

## Operations

This section provides the following details:

- [Reboot](#)
- [Backup and restore](#)
- [Upgrade](#)

### Reboot



**Note**

Rebooting the cnMaestro c4000 Controller will take all devices offline.

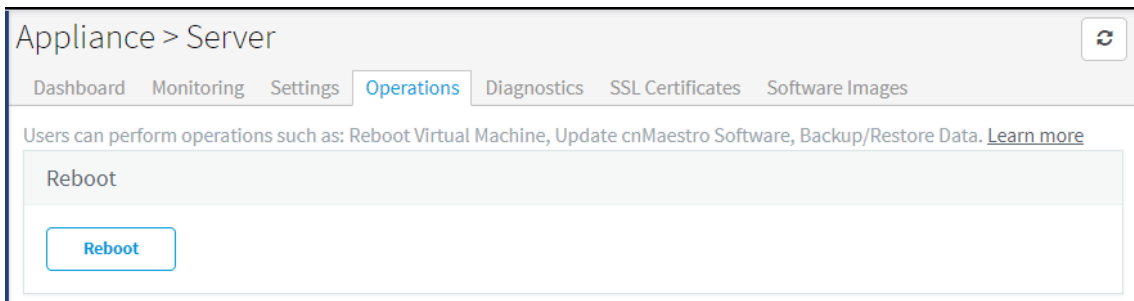


Figure 110 Alliance > Server > Operations > Reboot

## Backup and restore

Cambium recommends customers periodically backup their system as a precautionary measure. This is done through Appliance > Server > Operations > Backup and Restore. Backups can be done manually in real-time or scheduled to execute daily or weekly. cnMaestro c4000 Controller can also automatically transfer backup files off-box using FTP or SFTP (this support is configured under Appliance > Settings > Optional Features > Scheduled Jobs).

A System Backup stores the entire state of cnMaestro c4000 Controller as a file. This file can be downloaded to the local hard drive through the UI and imported into a new cnMaestro c4000 Controller hardware to recreate the application state. Only one System Backup is available at any time, and a later entry will overwrite an earlier one.

### Generate Backup

The user can create a system backup through a system backup job at Appliance > Server > Operations > Backup and Restore page. The created backup file can be downloaded to the user's local machine for archiving.

To generate the system backup Job:

1. Navigate to **Appliance > Server > Operations > Backup and Restore** page.

**Backup and Restore**

Backup or restore configuration and monitoring data from cnMaestro. A System Backup stores the entire state of a cnMaestro On-Premises server as a file. This file can be used to transfer data between two On-Premises instances. This file can be downloaded to the local hard drive through the UI and restored into a new cnMaestro instance to re-create the application state. The File Transfer configuration is defined at Appliance > Settings > Optional Features > Scheduled Jobs, and it is shared with Reports. [Learn more](#)

**Backup**

| Schedule   | Date and Time         | Status                            | Last Backup                           | File Transfer | Download |
|--|-----------------------|-----------------------------------|---------------------------------------|---------------|----------|
| <input type="button" value="Generate Backup"/>   | Now                   | N/A                               | Completed<br>(Sep 24, 2019 8:41 PM)📁  | Completed     | 📄        |
| <input checked="" type="checkbox"/> Daily Backup | 12:50 AM ⌚            | Scheduled<br>(Sep 26, 2019 00:50) | Completed<br>(Sep 25, 2019 12:51 AM)📁 | Completed     | 📄        |
| <input type="checkbox"/> Weekly Backup           | 03:42 PM<br>Wednesday |                                   | N/A                                   | N/A           | 📄        |

**Restore**

2. Select any one of the following:

- **Daily Backup:** You can set time exceeding the current system time. The backup files will be generated every data at the scheduled time.
- **Weekly Backup:** The backup files will be generated for a specified day and time on a weekly basis.

You can download the last backup file using the download icon in the table. The file transfer configuration is defined at Appliance > Settings > Optional Features > Scheduled Jobs and it is shared with Reports. If FTP is enabled, then a copy of each backup file will be stored in the configured FTP/SFTP server. The FTP column table displays the status of the upload to the FTP/SFTP server.

3. Click the **Generate Backup** button.



#### Note

Only the latest backup is retained in the disk and available to download. The old backup is deleted once the new backup is generated.

To view the system backup job:

Click View System Backup Jobs link in **Appliance > Operations > Backup and Restore** page.

## Restore

The user can now restore the downloaded system backup file to the new cnMaestro c4000 Controller hardware to recreate the application state under **Appliance > Server > Operations > Restore**.

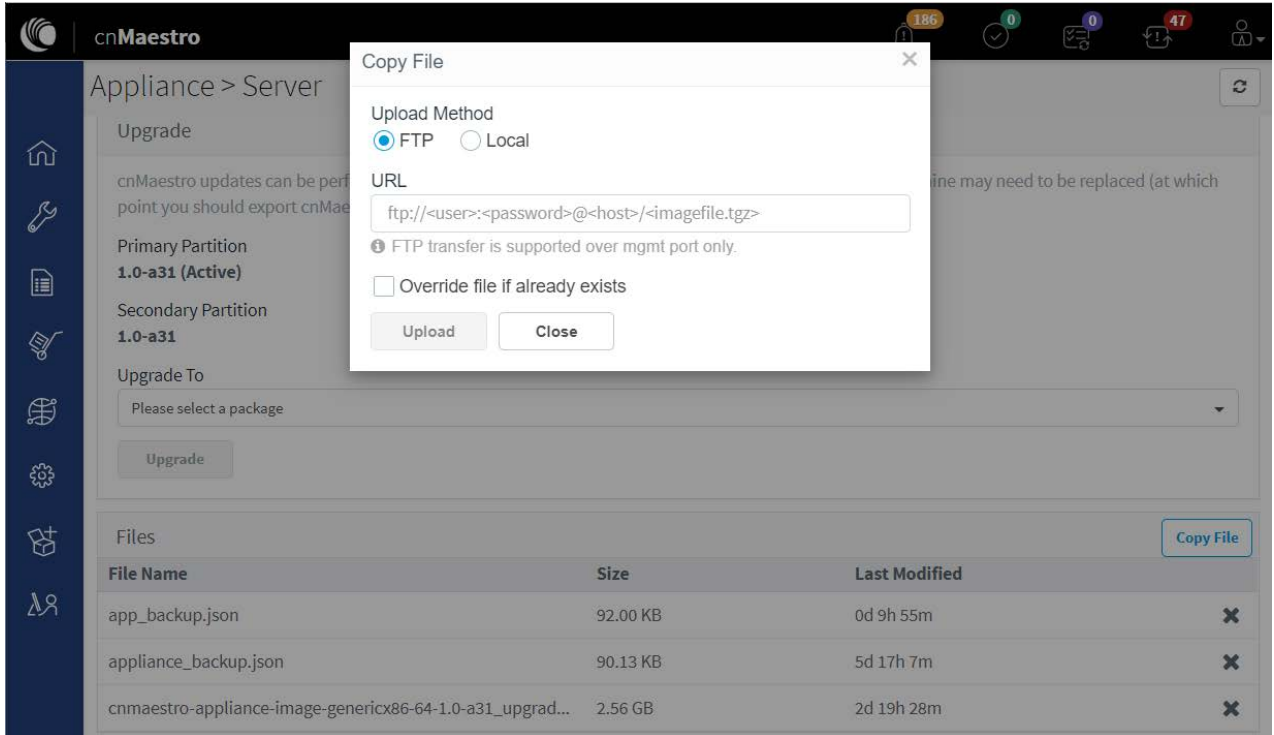
Figure 111 Appliance > Server > Operations > Restore

To restore backup files, select the file from Restore from Backup option and click Restore.

## Upgrade

### Uploading new TAR file

1. Click on the **copy file** button available under **Appliance > Server > Operations > Files**.
2. Select upload method as per the requirements:
  - a. If FTP is selected, download the image using syntax <ftp://<user>:<password>@<host>/<imagefile.tgz>>
  - b. If local selected, provide the path of the image and click on **Upload**.
3. If the same version file is persisting on the cnMaestro c4000 Controller, there is a provision to override the existing file.



### Initiating upgrade

Select the package uploaded on to cnMaestro c4000 Controller as described in Uploading new TAR file procedure and click on Upgrade available in **Appliance > Server > Operations > Upgrade**.

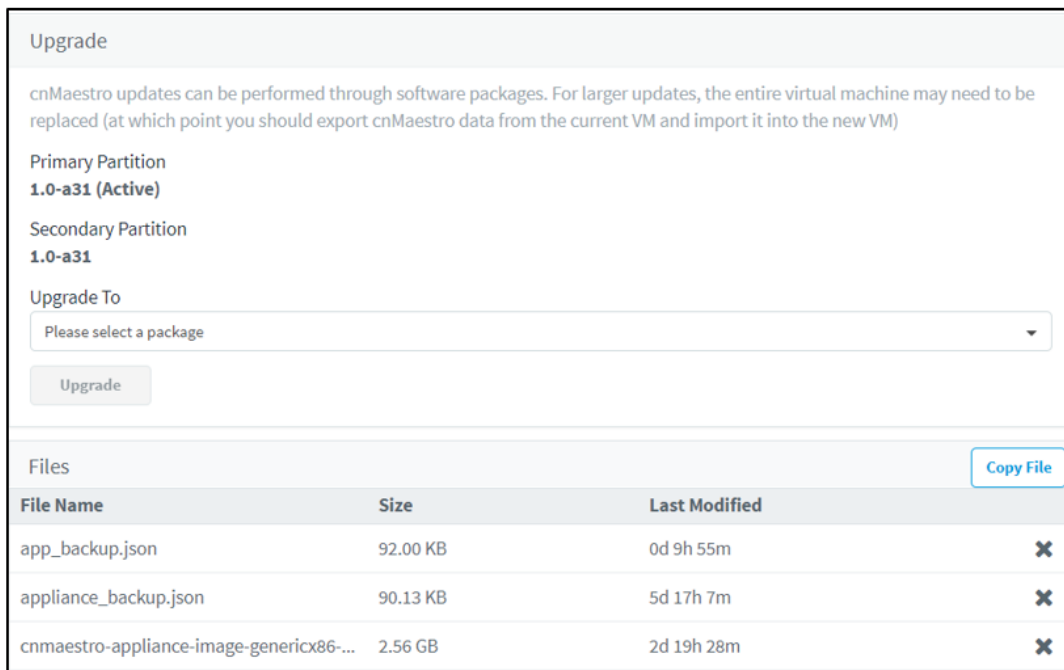


Figure 112 Initiating upgrade

## Diagnostics

This section provides the following details:

- [General](#)
- [Services](#)

### General

#### Technical Support Dump

The technical support dump gathers important runtime information on the cnMaestro c4000 Controller hardware. It is accessed at **Appliance > Server > Diagnostics** and can be used by Cambium Support to aid in resolving issues.


| Technical Support Dump   |        |                                    |   |
|--|--------|------------------------------------|---|
| The technical support dumps gathers important runtime and configuration information from your cnMaestro On-Premises installation. It can be sent to Cambium Support to aid in resolving issues. <a href="#">Learn more</a> |        |                                    |   |
|  | Status | Last Techdump                      | Download  |
| <a href="#">Generate</a>   | N/A    | Completed (Sep 24, 2019 8:42 PM) ⓘ |  |

Figure 113 Technical Support Dump

#### Logging Severity

Change the severity level of the messages logged by the cnMaestro c4000 Controller system. These messages are not accessible directly but can be downloaded as part of the Technical Support Dump. The Log Level Severity can be changed at runtime and it does not require a reboot of the server to take effect.

| Logging Severity   |                       |
|--|-----------------------|
| Change the logging severity level of cnMaestro applications to diagnose issues on the running system. The logging severity should be set to the default (Warning) and it should only be changed under guidance of the technical support team. <a href="#">Learn more</a> |                       |
| Log Level  |                       |
| Warning <span style="float: right;">▼</span>   |                       |
| <a href="#">Save</a>   | <a href="#">Reset</a> |

Figure 114 Logging Level

### Services

Real-time display of the status of critical cnMaestro c4000 Controller services.

| Name             | Type         | Status      | Uptime     | CPU   | Memory          |
|------------------|--------------|-------------|------------|-------|-----------------|
| cnmaestro-health | cnMaestro VM | Running     | 0d 19h 44m | 0.4%  | 0.9% [35.96MB]  |
| cnmaestro-snmp   | cnMaestro VM | Not Running | N/A        | -     | -               |
| mongod           | cnMaestro VM | Running     | 0d 19h 45m | 0.4%  | 8.6% [349.52MB] |
| nginx            | cnMaestro VM | Running     | 0d 19h 45m | 0.0%  | 0.0% [0.55MB]   |
| postgresql       | cnMaestro VM | Running     | 0d 19h 45m | 0.0%  | 0.7% [26.34MB]  |
| rabbitmq-server  | cnMaestro VM | Running     | 0d 19h 45m | 0.3%  | 1.1% [43.47MB]  |
| redis-server     | cnMaestro VM | Running     | 0d 19h 45m | 0.1%  | 0.2% [6.70MB]   |
| snmpd            | cnMaestro VM | Not Running | N/A        | -     | -               |
| wifiperfd        | cnMaestro VM | Running     | 0d 19h 43m | 0.1%  | 0.0% [0.65MB]   |
| cnwlcgmt-server  | Appliance    | Sleep       | 0d 19h 45m | -     | 0.37[30.56 GB]  |
| vpp_main         | Appliance    | Sleep       | 0d 19h 45m | 37.5% | 0.72[59.78 GB]  |

Figure 115 Services

## SSL Certificates

cnMaestro c4000 Controller generates a self-signed certificate when it boots the first time. Because the root CA is not present in standard browsers, cnMaestro c4000 Controller users (administrators or Captive Portal customers) receive an SSL error message as shown below:

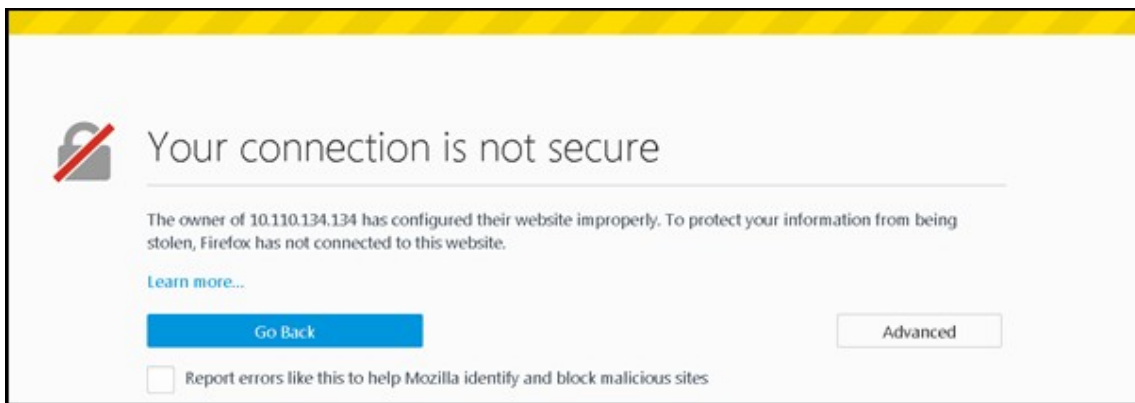


Figure 116 SSL Error Message

## Certificate Management

To fix the browser error, cnMaestro c4000 Controller needs to host a certificate from a trusted certificate authority and map the FQDN (fully qualified domain name) used to access cnMaestro

c4000 Controller. This requires the administrator to export a CSR (Certificate Signing Request) and import the signed Certificate back into cnMaestro c4000 Controller.

The following options are available to manage the certificates:

- View
- Generate a Certificate Signing Request (CSR)
- Import
- Backup
- Reset

### View

To view the certificate details, click the **View** tab.

Appliance > Server

Dashboard Monitoring Settings Operations Diagnostics **SSL Certificates** Software Images

[View](#) [Generate CSR](#) [Import](#) [Backup](#) [Reset](#)

Organization (O) Cambium Networks Ltd.  
 Serial Number 11262909535226380770 (0x9c4de48c808741e2)  
 Issued By Cambium Networks Ltd.  
 Begins On Thu Sep 19 2019 14:41:13 GMT+0530  
 Expires On Sat Sep 18 2021 14:41:13 GMT+0530  
 SHA-256 Fingerprint A3:37:5A:77:EF:3D:DF:35:6C:17:18:F4:A3:29:D5:21:0D:A7:EA:01:96:A6:D0:02:4C:55:48:CF:F8:FE:D1:A6

### Generate a Certificate Signing Request (CSR)

A certificate-signing request leverages the current Private Key and exports a CSR that can be forwarded to any Certificate Authority.

To generate a CSR:

1. Navigate to Appliance > Server > SSL Certificates page.
2. Select the **Generate CSR** tab.



Appliance > Server ↻

Dashboard Monitoring Settings Operations Diagnostics **SSL Certificates** Software Images

View [Generate CSR](#) Import Backup Reset

Generate a Certificate Signing Request (CSR) from the Private Key installed in cnMaestro. The CSR is used by a Certificate Authority to create a Signed Certificate mapped to a FQDN (fully qualified domain name). This allows browsers to trust the Guest Access Portal without a warning.

**Country (C)**

**Common Name (CN)**

FQDN (fully qualified domain name) here.

**Organization (O)**

**Organization Unit (OU)**

**City/Locality (L)**

**State/Province (ST)**

**Subject Alternative Name (SAN)**

3. Specify the parameters as in the below table:

**Table 41 Configuring CSR Parameters**

| Parameter                      | Description   |
|--------------------------------|---|
| Country (C)                    | Select the name of the country from the drop-down list  |
| Common Name                    | Enter the FQDN name of the cnMaestro c4000 Controller server. This is either the Domain Name or the IP Address. |
| Organization (O)               | Enter the name of the organization.   |
| Organization Unit (OU)         | Enter the name of the organization unit.  |
| City/Locality (L)              | Enter the name of the city.   |
| State/Province (ST)            | Enter the name of the state.  |
| Subject Alternative Name (SAN) | Enter DNS or IP Address.  |

4. Click the **Generate CSR** button.

Upon Generate, the user is prompted to save a cnMaestro c4000 Controller .csr file to their hard drive. The CSR can then be sent to a Certificate Authority and signed.

### Import

Once the CSR has been transferred to the Certificate Authority to create a certificate, it can be imported back into cnMaestro c4000 Controller. cnMaestro c4000 Controller will validate the certificate maps correctly to the stored Private Key, and disallow the import if incorrect. Alternatively, the user can append the Private Key to the Certificate file in PEM format and upload both if certificate and key is generated outside cnMaestro c4000 Controller. Users can also provide a password optionally if the key is generated with the password. This will replace both the Certificate and Key on cnMaestro c4000 Controller.

To import a certificate:

1. Click the Import tab.

Appliance > Server

Dashboard Monitoring Settings Operations Diagnostics **SSL Certificates** Software Images

View Generate CSR **Import** Backup Reset

Import a Signed Certificate generated from a CSR or a Signed Certificate along with its Key (optionally encrypted). For either choice, **please make sure all files (including Signed Certificate, Intermediate Certificates, and optional Key) are concatenated into a single PEM encoded file before uploading.** For certificate chaining bundle, the server certificate must appear before the chained certificates in the concatenated file.

Import Signed Certificate from CSR  Import Signed Certificate and New Key

Certificate and Key File

Select File

Import

2. Select any one of the below options:
  - a. Import signed Certificate from CSR

- b. Import signed Certificate and new Key
3. Browse and upload the Certificate and Key file.
4. Click Import.

**Note**

The Certificate and any optional intermediate certificates should be appended and stored in a single PEM- encoded file prior to submission. The signed Certificate should be positioned at the top of the file, followed by any intermediate certificates.

**Note**

When importing a Certificate and Key, a single PEM-encoded file should be submitted with entries in the following order: Certificate, intermediate certificates, and Key. If the Key is encrypted, a password should be provided in the text box on the UI page at the time of import.

## Backup

cnMaestro c4000 Controller generates a 4096-bit Private Key when it boots up. This section lets the customer export this Key and current Certificate for backup. These will be exported as a single file, and the Key can optionally be encrypted with a password. To back up the certificate and the key:

1. Click the **Backup** tab.

The screenshot shows the 'Appliance > Server' page with the 'SSL Certificates' tab selected. The 'Backup' sub-tab is active, displaying a form for backing up the current Certificate and Key. The form includes a text box for 'Key Password (optional)' and a 'Backup' button. The breadcrumb navigation shows 'Dashboard', 'Monitoring', 'Settings', 'Operations', 'Diagnostics', 'SSL Certificates', and 'Software Images'. The sub-navigation includes 'View', 'Generate CSR', 'Import', 'Backup', and 'Reset'.

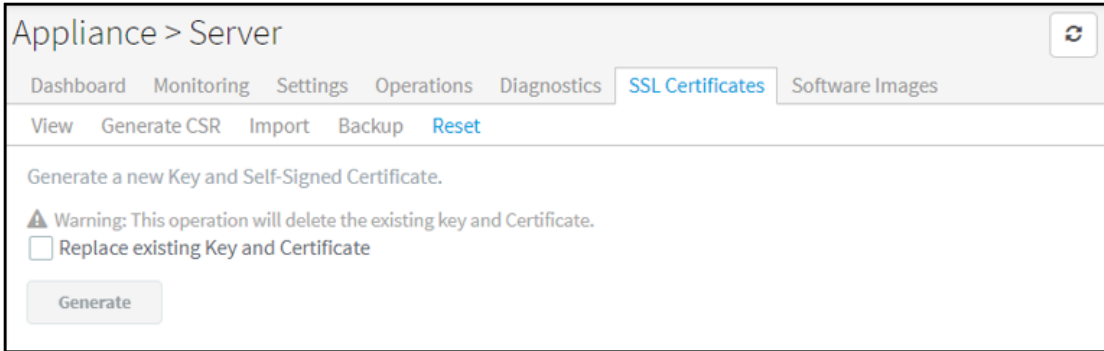
2. Enter the password for the key in the **Key Password** text box.
3. Click **Backup**.

## Reset

It replaces the current Private Key and Certificate and recreates them from scratch. The Certificate is self-signed, and it can be replaced using the Certificate import mechanism detailed above.

To generate a new private key:

1. Click the **Reset** tab.



2. Select the **Replace the existing Key and Certificate** checkbox.
3. Click **Generate**.

## Software Images

This section provides the following details:

- [Overview](#)
- [Automatically Update Device Software](#)

### Overview

cnMaestro c4000 Controller allows one to add new device software images as they are released by the device teams. Adding new device software is a manual process: one needs to first download the images from the Cambium Support Center and then upload them into cnMaestro c4000 Controller. The steps are presented below:

1. Navigate to <https://support.cambiumnetworks.com/files/> and download the device image to your laptop.
2. In the cnMaestro c4000 Controller UI, navigate to **Appliance > Server > Software Images** tab.
3. Select the image file and then click the **Import Software** button.
4. Once the file is successfully uploaded to the server, it will appear in the grid.

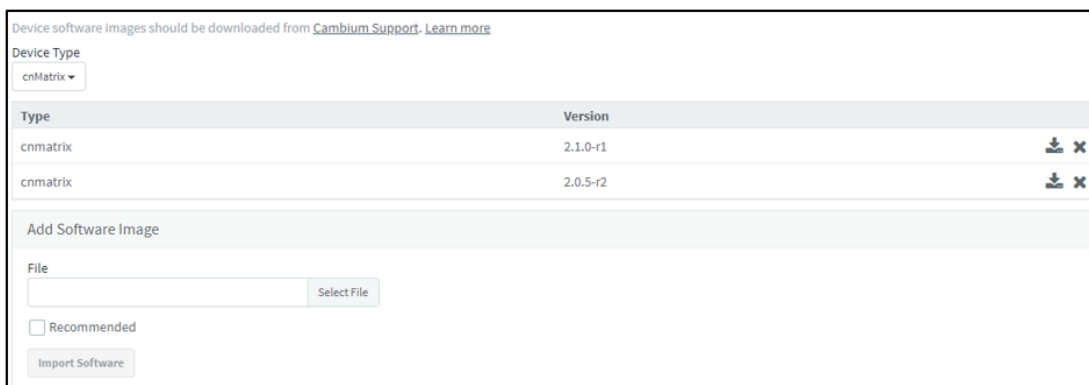


Figure 117 Managing Device Software Images

**Note**

cnMaestro c4000 Controller uses the name of the uploaded file to determine the version and device type. Please don't change the name during the upload or download process.

By default, the minimum required software versions will be available by default in the Server.

- cnMatrix: 2.0.4-r1
- cnPilot E400/E500/E502S/E501S: 3.2.1-r6
- cnPilot E410/E600/E430w: 3.5.2-r4
- cnPilot e700: 3.7-r9
- ePMP 1000 Hotspot: 3.2.1-r6
- ePMP 2000: 3.0
- ePMP 1000, ePMP Force 180/200: 3.1
- ePMP Force 190: 3.5
- ePMP Force 300: 4.1
- ePMP PTP 550: 4.1
- cnPilot R200P/R201P: 4.4.2-R2
- cnPilot R190: 4.4.2-R2
- PMP: 15.0.1
- ePMP Elevate: 3.2

## Automatically Update Device Software

The software version on the devices can be automatically updated to the preferred version when the device first contacts cnMaestro c4000 Controller.

To enable automatically update device software feature,

1. Navigate to Appliance > Server > Software Image > Automatically Update Device Software Section page.
2. Select the option to automatically enable updating the device software feature.
3. Choose the software version depending on the device type.
4. Click Save.

The device will get automatically upgraded based on the software selected while Onboarding.

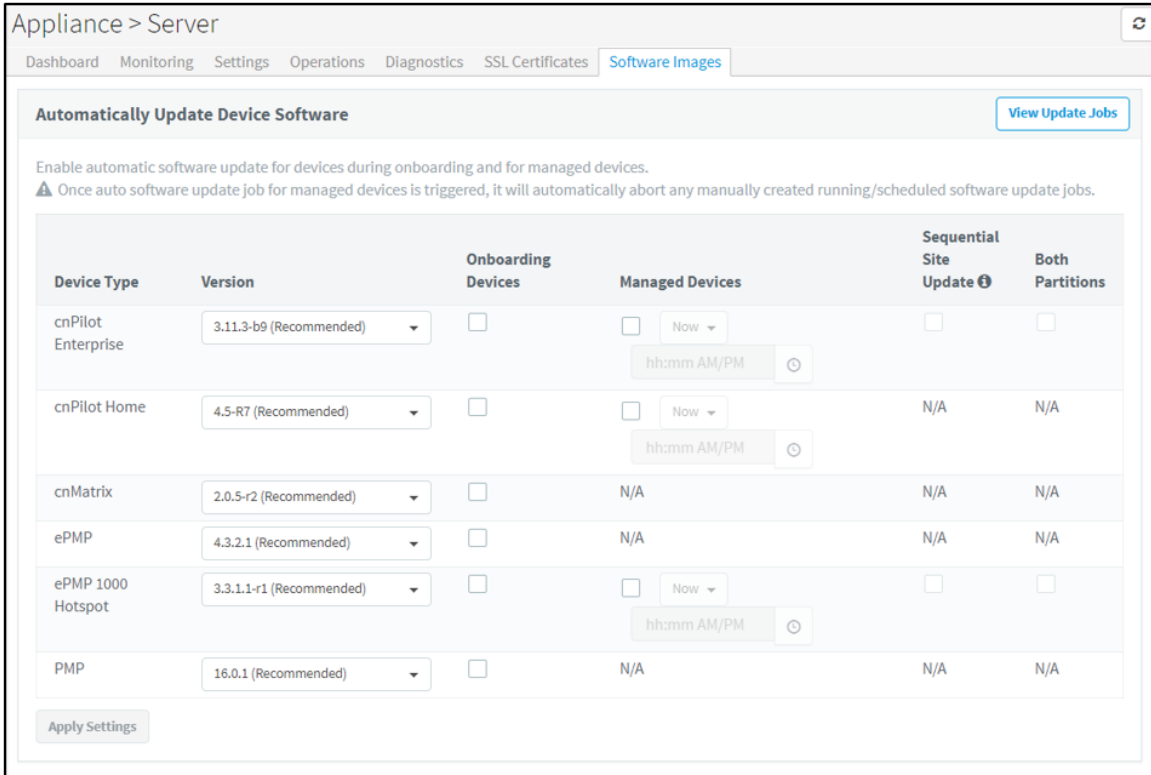


Figure 118 Automatically Update Device Software

## Network

This section describes the following details:

- [Statistics](#)
- [Configuration](#)
- [Tools](#)
- [Access Control List \(ACL\)](#)

### Statistics

It provides statistical data related to all interfaces and routes. Interfaces include all Ethernet and SVI interfaces. To monitor Statistics, go to **Appliance > Network > Statistics**. Below is the screenshot of the Statistic page

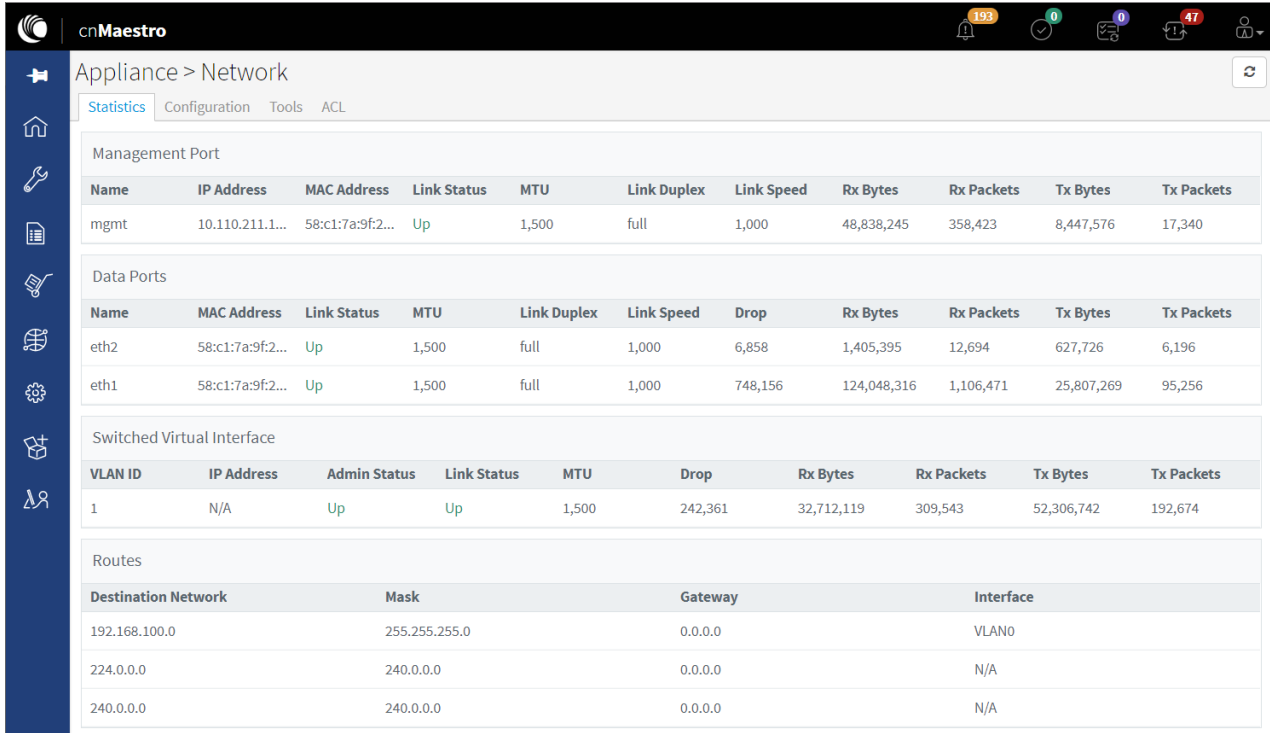


Figure 119 Appliance > Network > Statistics

## Configuration

The following are the description of the parameters that are viewable in the Configuration section.

Table 42 Appliance > Network > Configuration parameters

| Parameters  | Description  | Range | Default          |
|---|--|-------|------------------|
| <b>Appliance &gt; Network &gt; Configuration &gt; Management Port</b> |  |       |                  |
| Name  | Configure interface name.  |       | mgmt             |
| IP Address mode   | Configure mode of IP address.                                    |       | DHCP             |
| Admin Status  | Provides information w.r.t interface state.                      |       | -                |
| MTU   | Provision to configure MTU of the interface.                     |       | 1500             |
| Description   | User friendly text to the interface.                             |       | This is OOB port |
| IP  | Provision to configure IP if static IP address mode is selected. |       |                  |

|  |   |  |        |
|--|---|--|--------|
| Gateway  | Provision to configure gateway if static IP address mode is selected.   |  |        |
| Primary DNS  | Provision to configure static primary DNS.  |  |        |
| Secondary DNS  | Provision to configure static secondary DNS.  |  |        |
| <b>Appliance &gt; Network &gt; Configuration &gt; Data Ports</b>                 |   |  |        |
| Name   | Configure interface name.   |  |        |
| Switch Port Mode   | Provision to configure the mode of the interface: <ul style="list-style-type: none"> <li>• Access</li> <li>• Trunk</li> </ul> |  | Access |
| VLAN   | Provision to configure the VLAN traffic allowed on the interface.   |  | 1      |
| Admin Status   | Provides information w.r.t interface state.   |  |        |
| MTU  | Provision to configure MTU of the interface.  |  | 1500   |
| Description  | User-friendly text to the interface.  |  | -      |
| ACL Ingress  | Provision to apply the ACL policies based on required ingress traffic.  |  |        |
| ACL Egress   | Provision to apply the ACL policies based on required egress traffic.   |  |        |
| <b>Appliance &gt; Network &gt; Configuration &gt; Switched Virtual Interface</b> |   |  |        |
| Device Management VLAN   | Provision to select the management VLAN on which devices are terminated either using HTTP(S) or GRE.                          |  | VLAN 1 |
| SVIs   | Provision to add VLAN interfaces  |  |        |
| VLAN ID  | Provision to configure the VLAN traffic allowed on the interface.   |  |        |
| IP Address   | Configure mode of IP address.   |  |        |
| Admin Status   | Provides information w.r.t interface state.   |  |        |
| Description  | User-friendly text to the interface.  |  |        |



|   |   |  |  |
|---|---|--|--|
| ACL Ingress   | Provision to apply the ACL policies based on required ingress traffic.        |  |  |
| ACL Egress  | Provision to apply the ACL policies based on required egress traffic.         |  |  |
| Add New   | Provision to add new SVI interfaces.  |  |  |
| <b>Appliance &gt; Network &gt; Configuration &gt; Static Routes</b> |   |  |  |
| Destination Network   | User can configure either a unique IP addresses or subnet.                    |  |  |
| Gateway   | Provision to configure the gateway for the above-defined destination network. |  |  |
| Description   | User-friendly text to the interface.  |  |  |

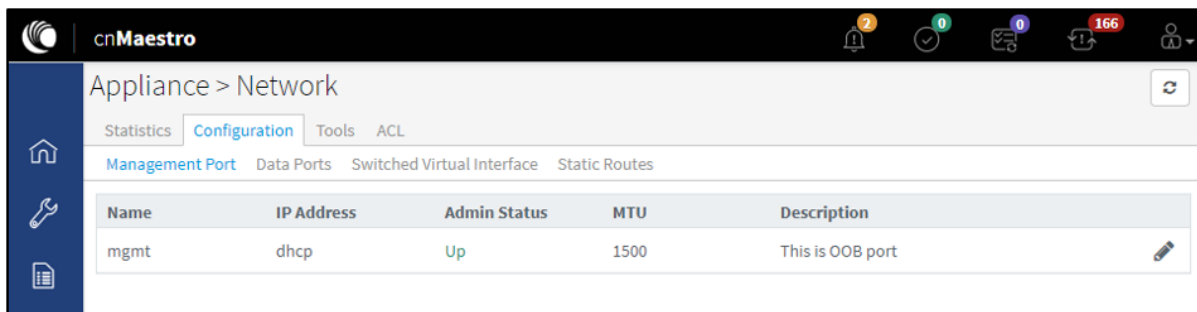


Figure 120 Appliance > Network > Configuration > Management Port

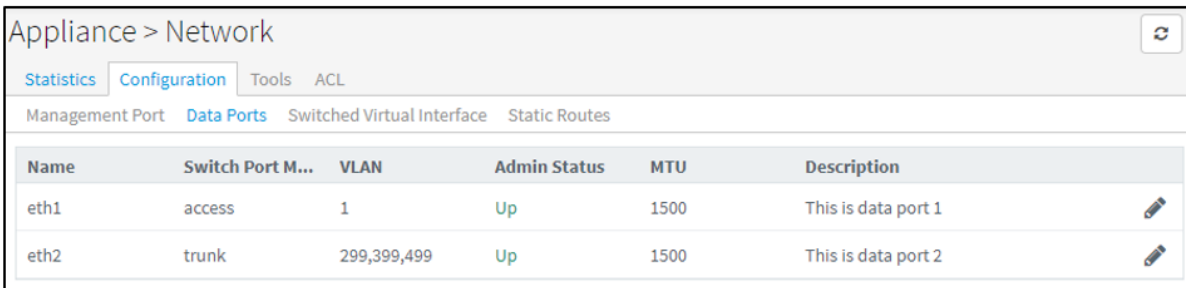


Figure 121 Appliance > Network > Configuration > Data Port

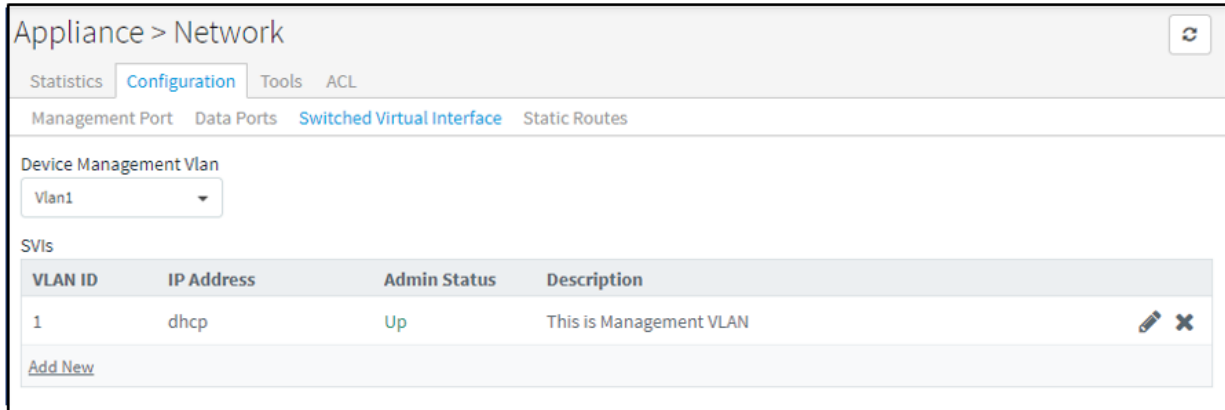


Figure 122 Appliance > Network > Configuration > Switched Virtual Interfaces

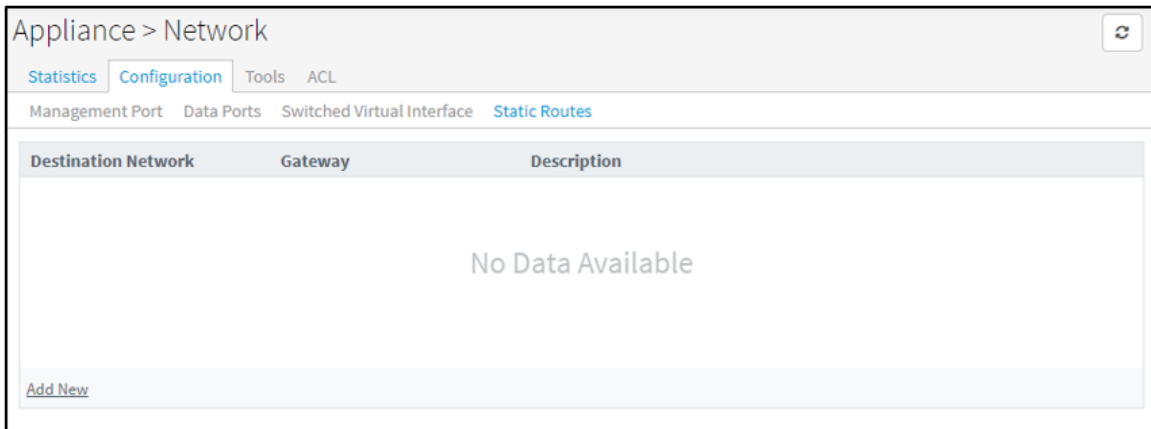


Figure 123 Appliance > Network > Configuration > Static Routes

## Management Interface Configuration

### Management Port in Access Mode - DHCP

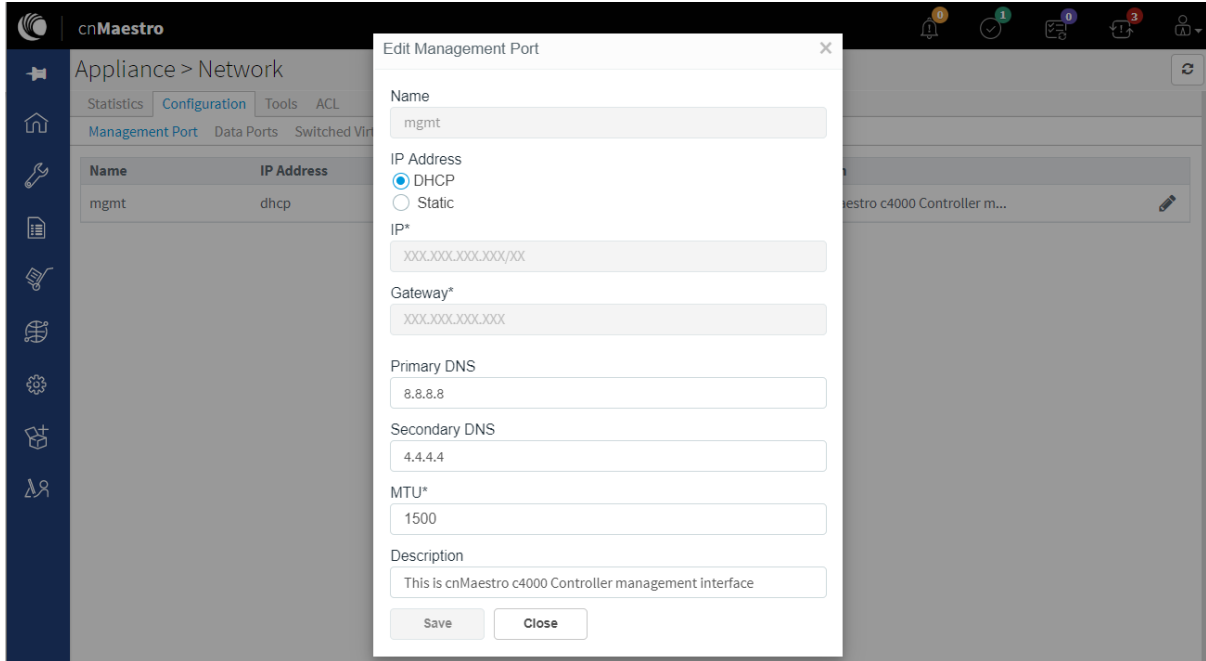


Figure 124 Management port in Access mode - DHCP

### Management Port in Access Mode – Static

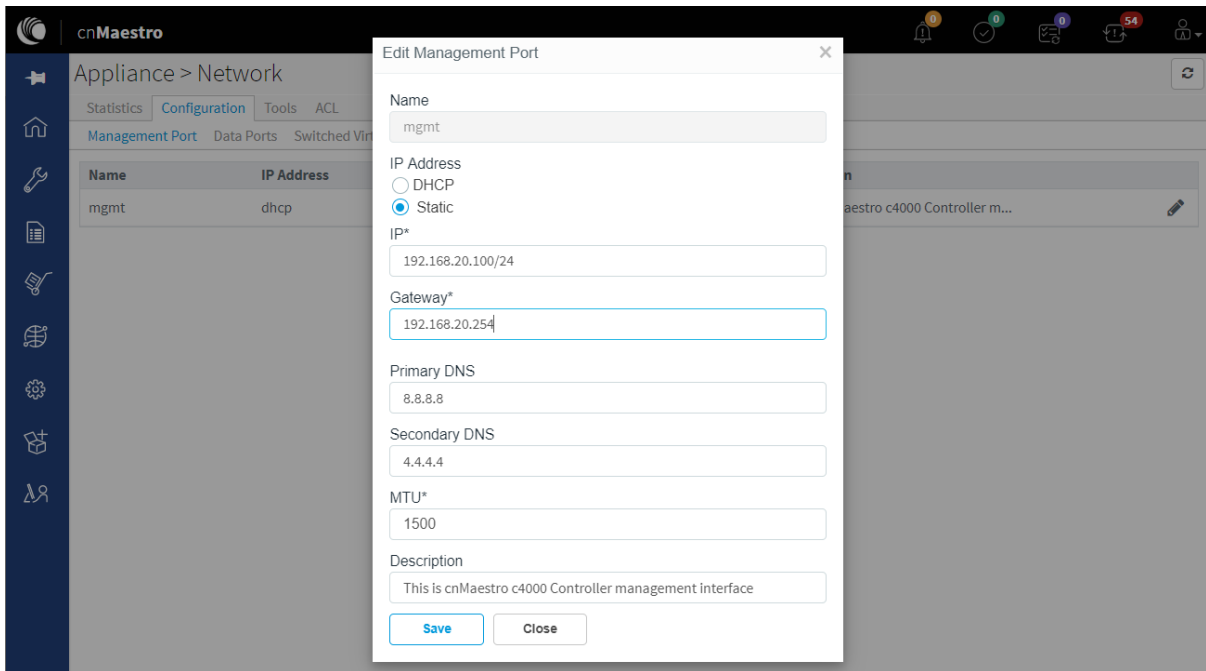


Figure 125 Management port in Access mode - Static

### Data Interface Configuration

### Data Port in Access Mode

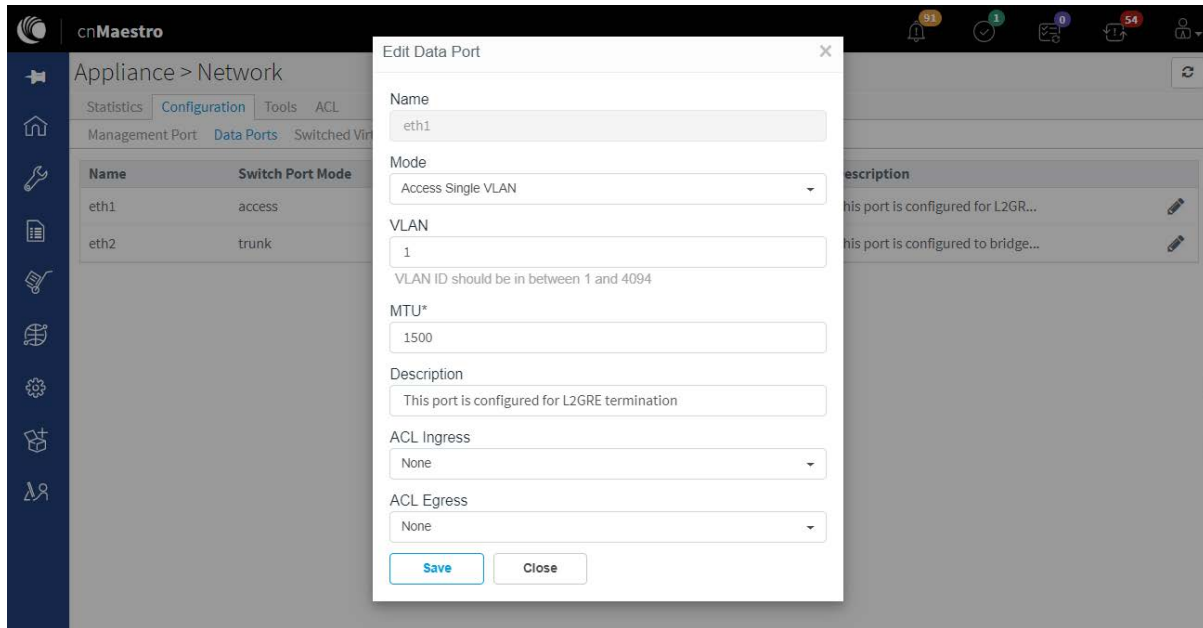


Figure 126 Data port in Access mode

### Data Port in Trunk Mode

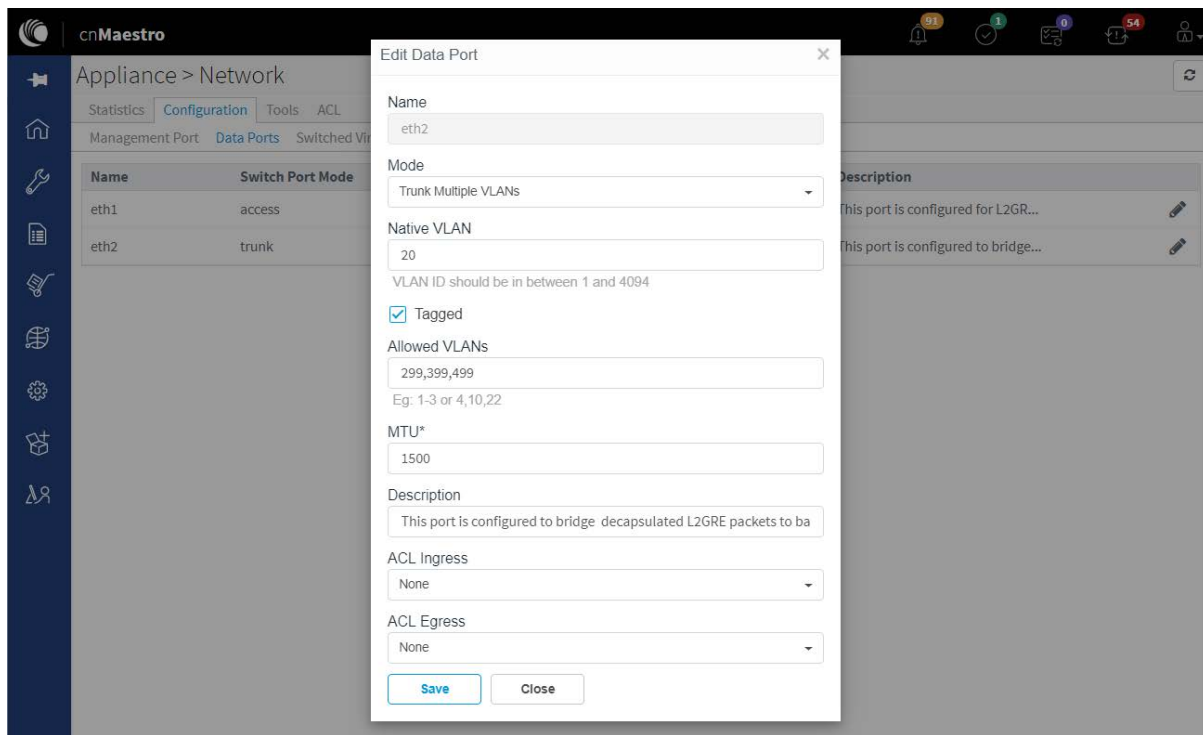


Figure 127 Data port in Trunk mode

## Data Port solution for L2GRE deployment

cnMaestro c4000 Controller has two ethernet hardware and is pre-configured as a Data port. When it is deployed as an L2GRE concentrator, the following are the solutions for deployment:

### Single Port solution for Cambium GRE

For single port solutions for Cambium GRE refer section **Data Port in Trunk Mode** for segregating client traffic.

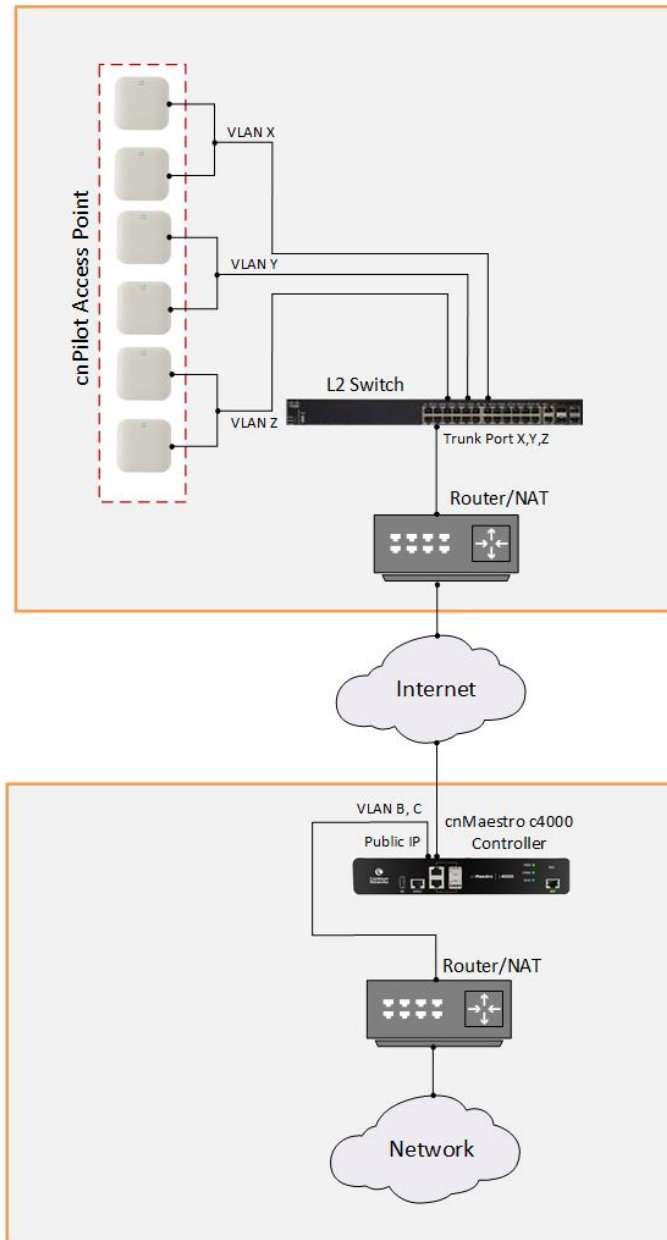


Figure 128 Single-port solution for Cambium GRE

## Two Port solution for Cambium GRE

For two-port solutions for Cambium GRE refer sections [Data Port in Access Mode](#) and [Data Port in Trunk Mode](#) for segregating client traffic.

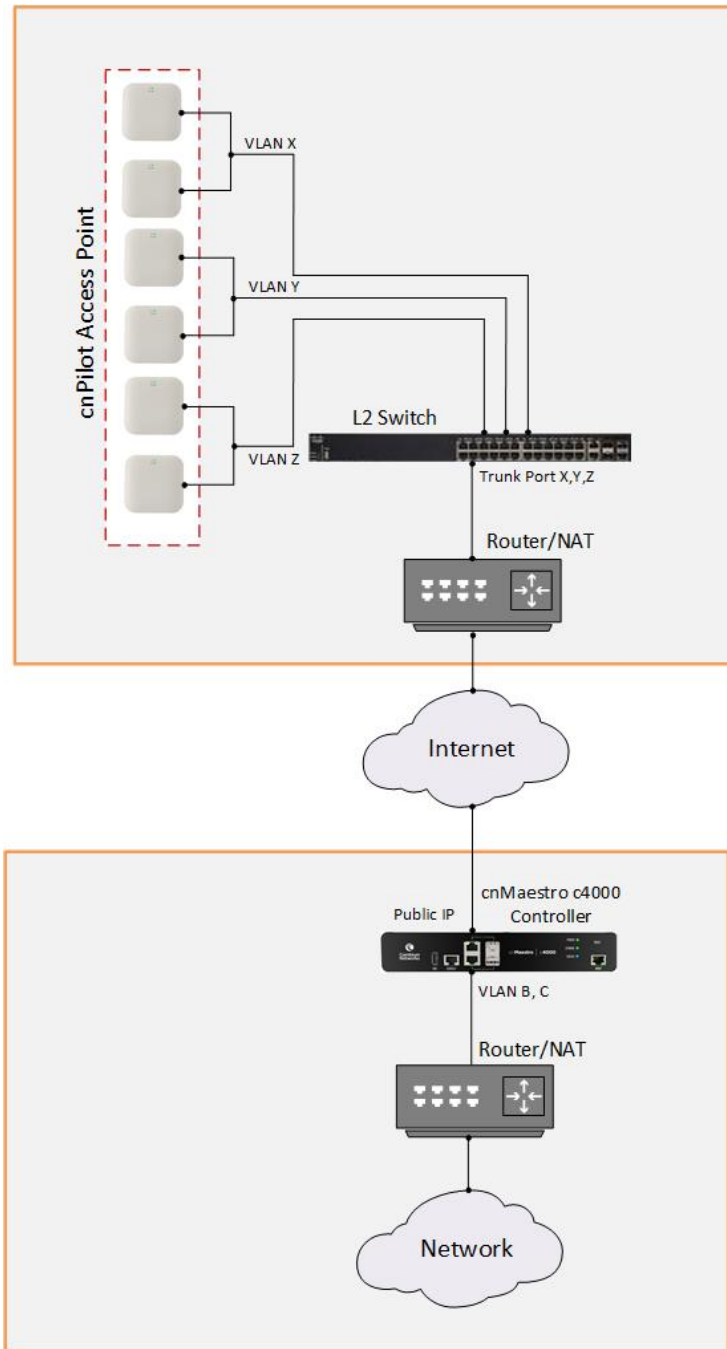


Figure 129 Two-port solution for Cambium GRE

## Tools

**Table 43 Configure: Appliance > Network > Tools parameters**

| Parameters   | Description   | Range                    | Default    |
|--|---|--------------------------|------------|
| <b>Appliance &gt; Network &gt; Tools &gt; Ping</b>           |   |                          |            |
| Host<br>_____  | Configure either IP or hostname to check the reachability.  | -                        | -          |
| Port<br>_____  | Users can configure the source interface through which the reachability of the interface is validated. Possible options are: <ul style="list-style-type: none"> <li>• Management</li> <li>• Data</li> </ul> | -                        | Management |
| Packet Count<br>_____  | The number of packets to be validated to check the reachability of the destined host.   | 3-10 or 0 for continuous | 3          |
| Size<br>_____  | Provision to configure Ping packet size.  | 1-65507                  | 100        |
| Result   | It provides the Ping results.   | -                        | -          |
| <b>Appliance &gt; Network &gt; Tools &gt; Traceroute</b>     |   |                          |            |
| Host<br>_____  | Configure either IP or hostname to check the reachability.  | -                        | -          |
| Port<br>_____  | Users can configure the source interface through which the reachability of the interface is validated. Possible options are: <ul style="list-style-type: none"> <li>• Management</li> <li>• Data</li> </ul> | -                        | Management |
| Result   | Provides the Traceroute results.  | -                        | -          |
| <b>Appliance &gt; Network &gt; Tools &gt; Packet Capture</b> |   |                          |            |
| Interface<br>_____   | Provision to select the interface on which capture has to be triggered  | -                        | -          |
| Count<br>_____   | The number of packets to be captured.   | 10-2000                  | 10         |
| Result (VPP)   | Packet capture display  | -                        | -          |

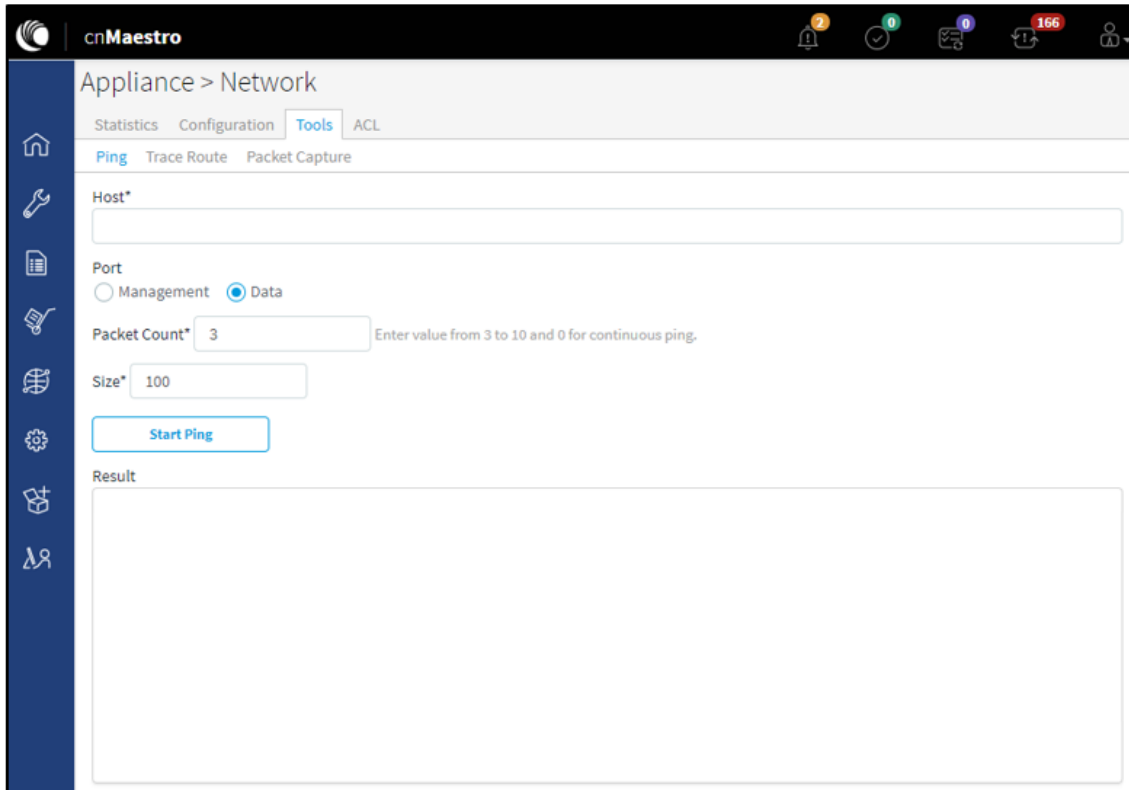


Figure 130 Appliance > Network > Tools



## Examples

### Ping Hostname

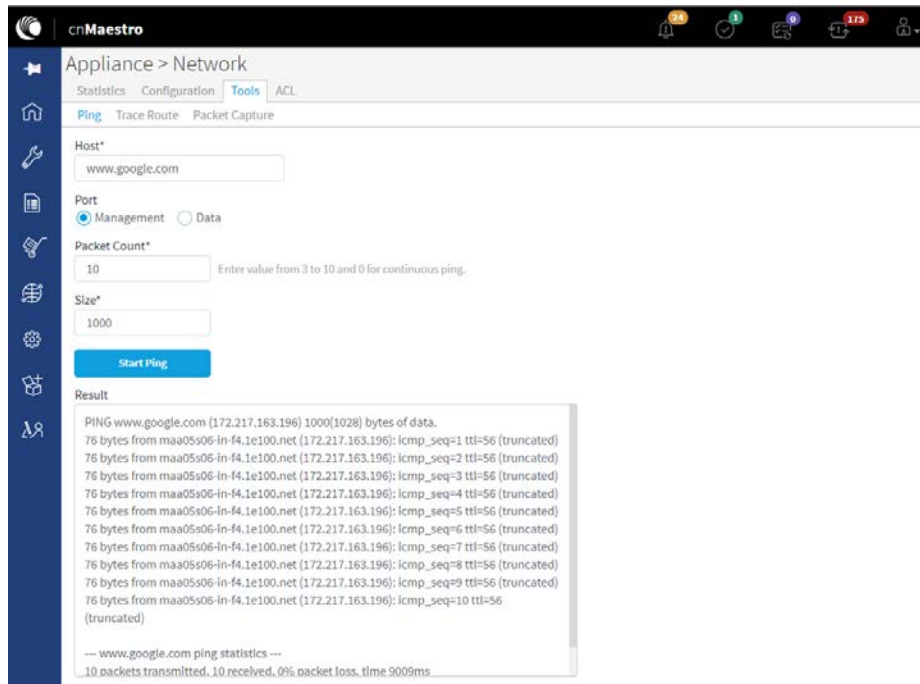


Figure 131 Appliance > Network > Tools > Ping Hostname

### Ping IP

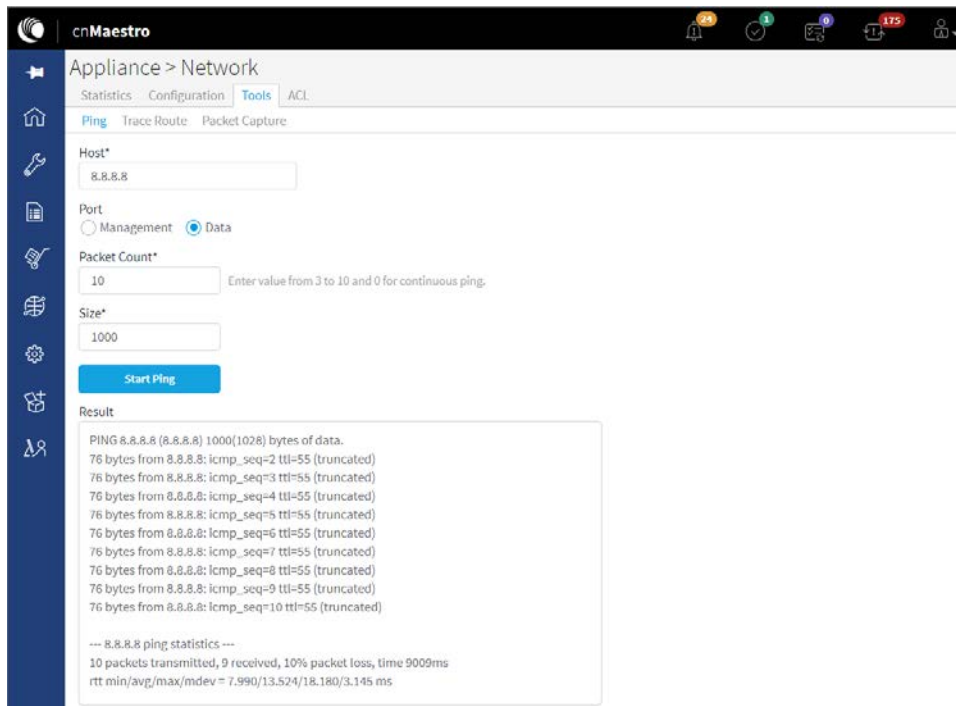


Figure 132 Appliance > Network > Tools > Ping IP

### Traceroute Hostname

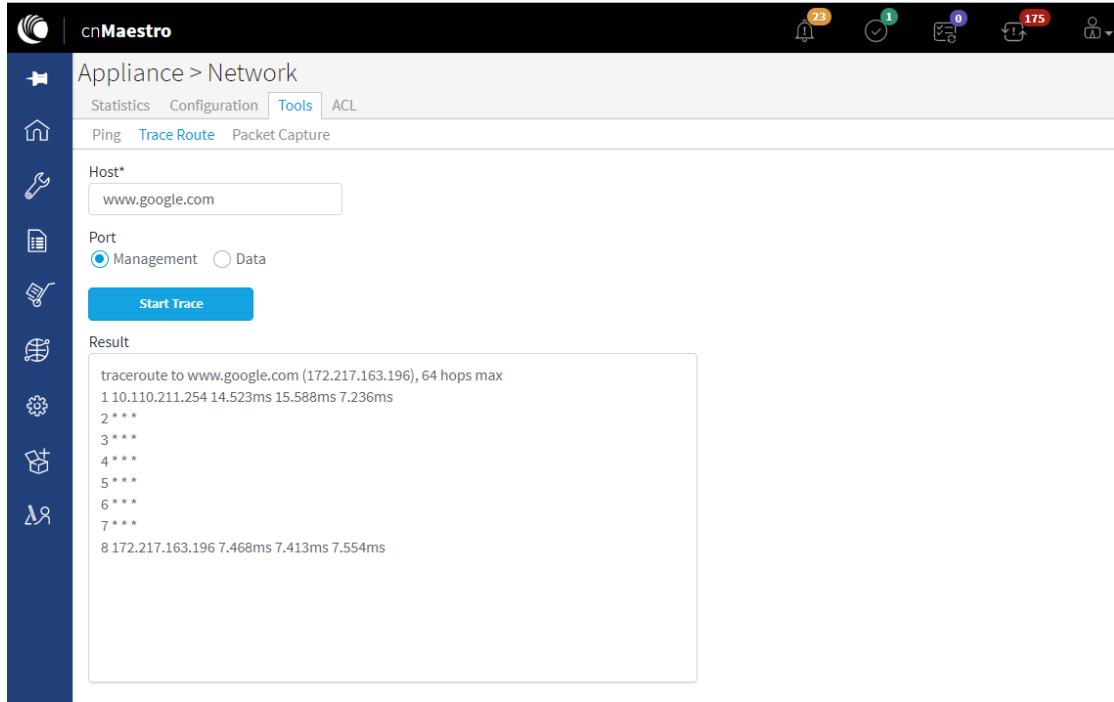


Figure 133 Appliance > Network > Tools > Trace Route Hostname

### Traceroute IP

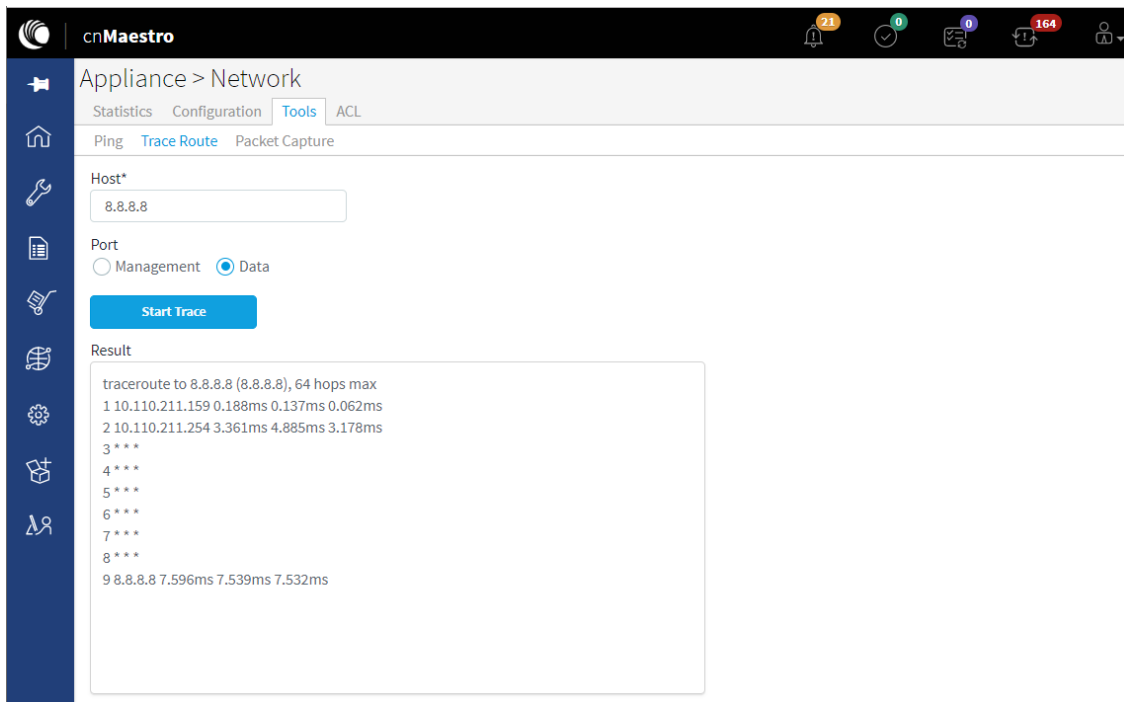


Figure 134 Appliance > Network > Tools > Trace Route IP

## Packet Capture Interface

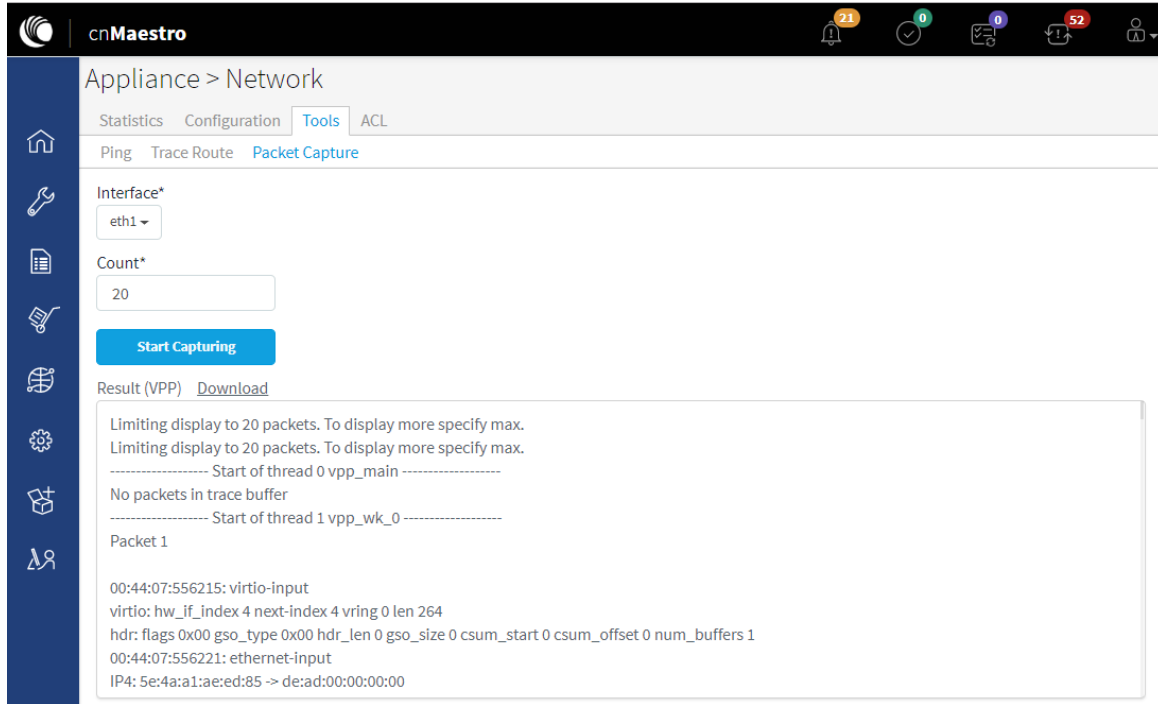


Figure 135 Appliance > Network > Tools > Packet capture

## Access Control List (ACL)

ACLs on the cnMaestro c4000 Controller are configurable based on the deployment requirement. ACLs can be configured at multiple levels based on the requirements. [Figure 136](#) represents the configuration of ACL policies.

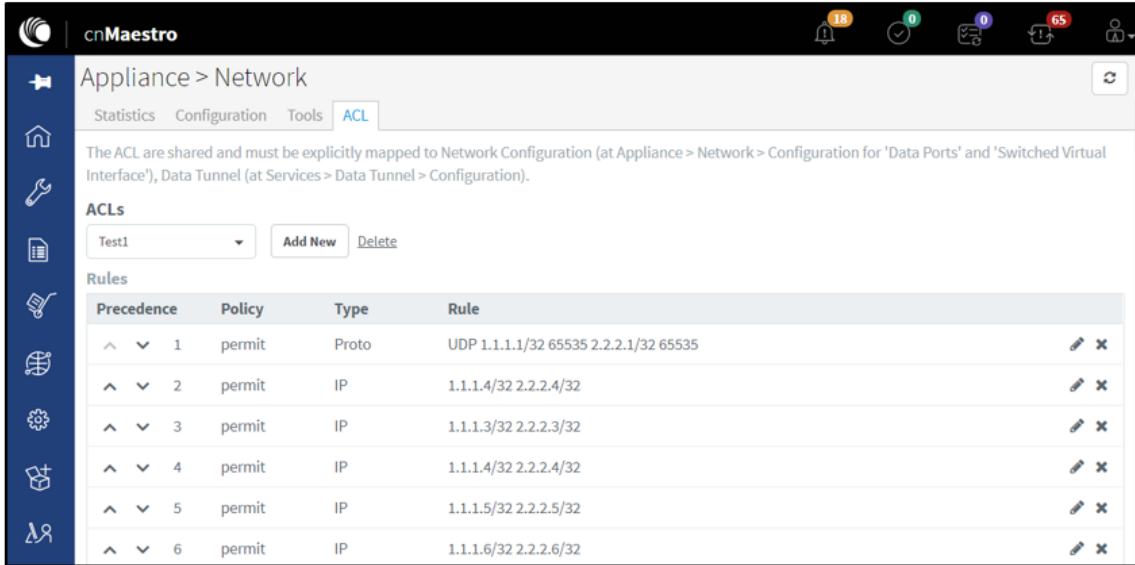


Figure 136 ACL policy configuration

- Figure 137 represents ACLs for inter GRE tunnel traffic.

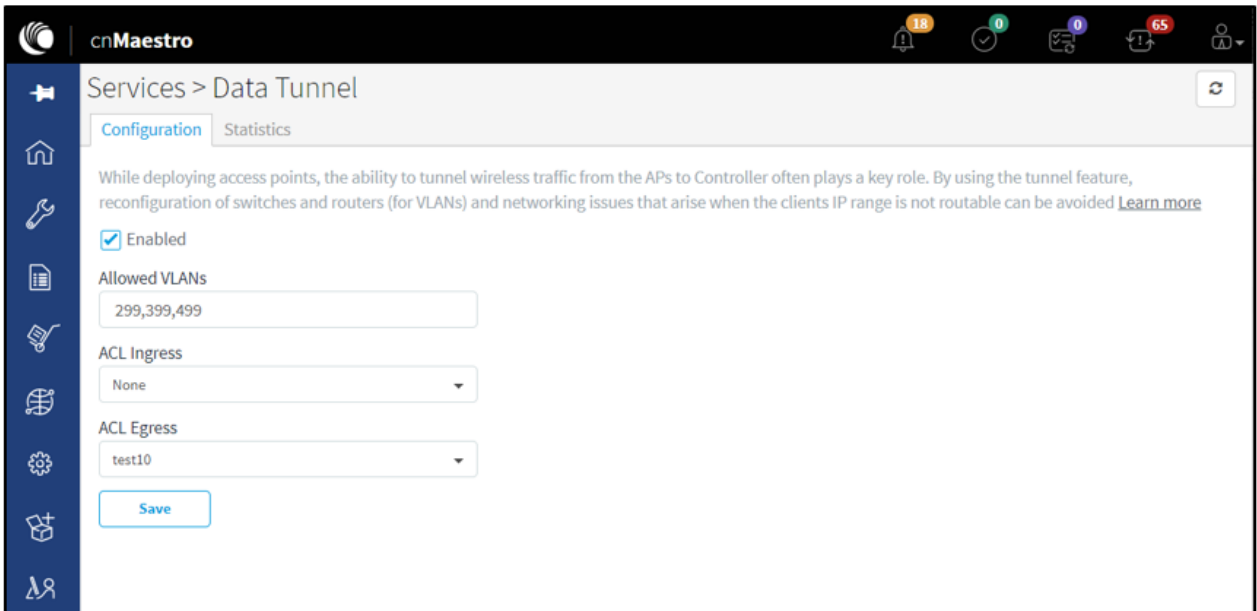


Figure 137 GRE inter tunnel ACL configuration

- To filter traffic either at network interfaces.
  - **Figure 138** represents ACL policies that are applied to Ethernet.

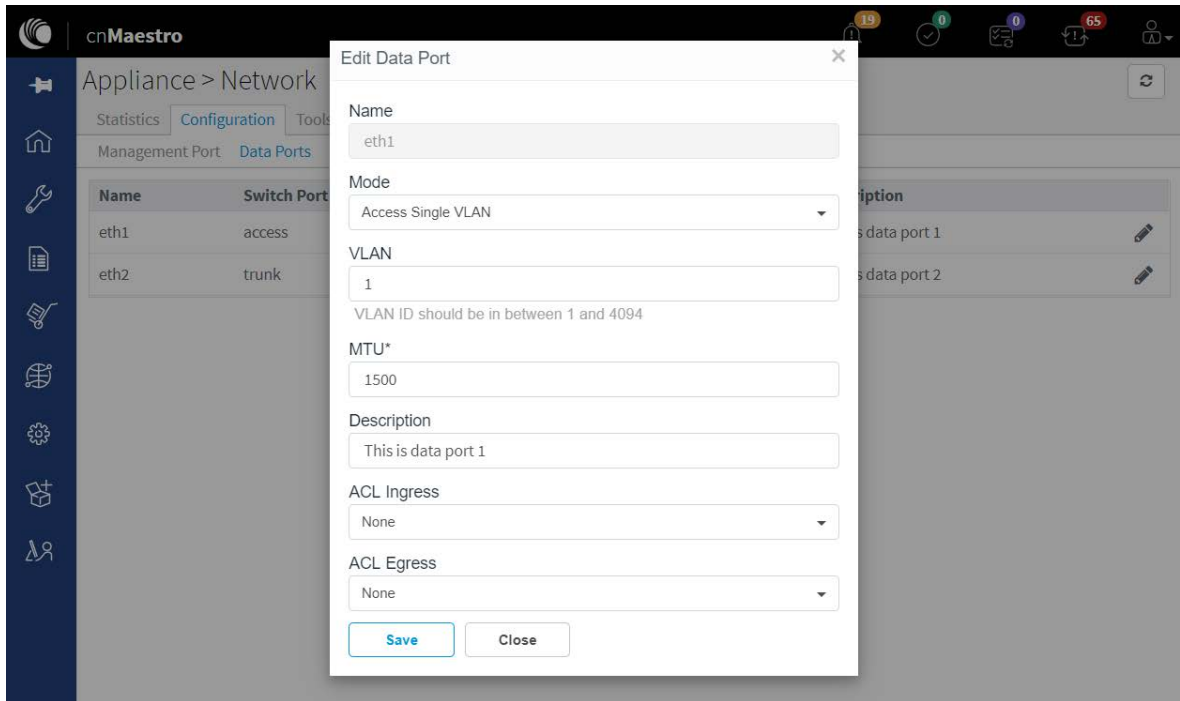


Figure 138 Ethernet ACL policies

- o Figure 139 represents ACL policies that are applied on SVIs.

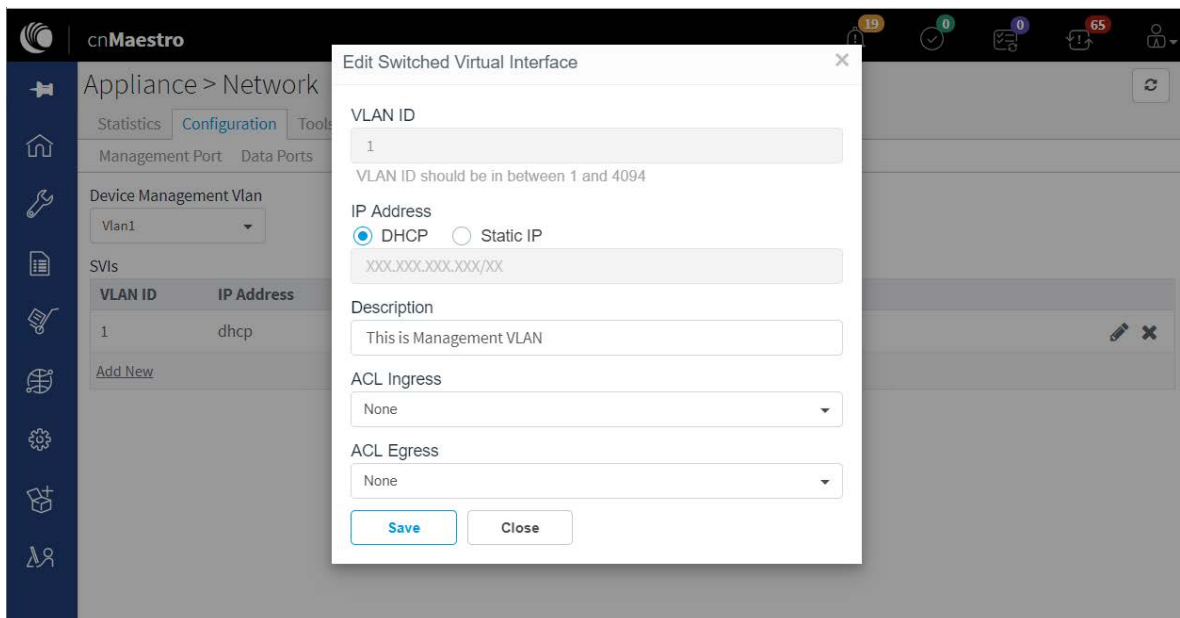


Figure 139 SVI ACL policies

## Synchronize (Sync) Configuration

AP Groups can be configured to synchronize automatically or manually when they are updated. The setting is found in the AP Group configuration.

1. cnPilot Enterprise AP Groups by default synchronize automatically (so any change of AP Group or WLAN, followed by a Save, will immediately push configuration to the devices without manual intervention).
2. cnPilot Home AP Groups by default synchronize manually. Updates to them (or the WLANs to which they map) need manual synchronization to push configuration to the devices.

## Manual Synchronization

Manual configuration synchronization allows the user to synchronize any devices with a single action rather than updating each device separately. The page is located at Appliance > Sync Configuration.

Sync Configuration only displays devices currently out-of-sync with a mapped AP Group. Sync Configuration has the following fields:

- Device (Hostname)
- Device Type
- Status (Up/Down)
- Network (Network in which device is present)
- Site (Site under which device is present)
- AP Group (AP Group to which device is mapped)
- Sync Status (Sync status will tell whether the job is completed or failed)

Steps to do Sync Configuration:

1. Click the Sync Configuration button in the top right of the **Configuration > WLAN and AP Groups** or **Manage > Configuration > Device Details** or **Jobs** tab.
2. Select devices you wish to synchronize.

The screenshot displays the 'Application > Sync Configuration' page. At the top, there's a search bar and filters for 'Managed Account' (set to 'All') and 'Device Type' (set to 'All'). Below this is a table with the following columns: Device, Type, Status, Managed Account, Network, Site, AP Group, and Sync Status. The table lists several devices, all of which are 'Offline'. The 'Sync Status' column indicates various reasons for being out of sync, such as 'Failed to push configuration to device' or 'Device's Overrides were changed'. At the bottom of the table, it shows 'Showing 1 - 10 Total: 54'. Below the table, there are 'Job Options' including a checkbox for 'Stop update on critical error' and a field for 'Allow' devices to be configured in parallel. A 'Sync Now' button is located at the bottom right of the interface.

3. Click the Sync Now button on the bottom right of the screen.



### Note

Sync configuration can only be used if an AP Group is already mapped to the device.

## Chapter 15: RADIUS Proxy

### Overview

cnMaestro c4000 Controller can act as a proxy server to authenticate RADIUS requests for cnPilot Wi-Fi devices. In this scenario, cnMaestro c4000 Controller will act as NAS (Network Access Server) for the RADIUS server.

In the below scenario, the access point sends RADIUS packets to cnMaestro c4000 Controller, and cnMaestro c4000 Controller sends them to the RADIUS server. cnMaestro c4000 Controller can act as a proxy for either authentication or accounting messages.

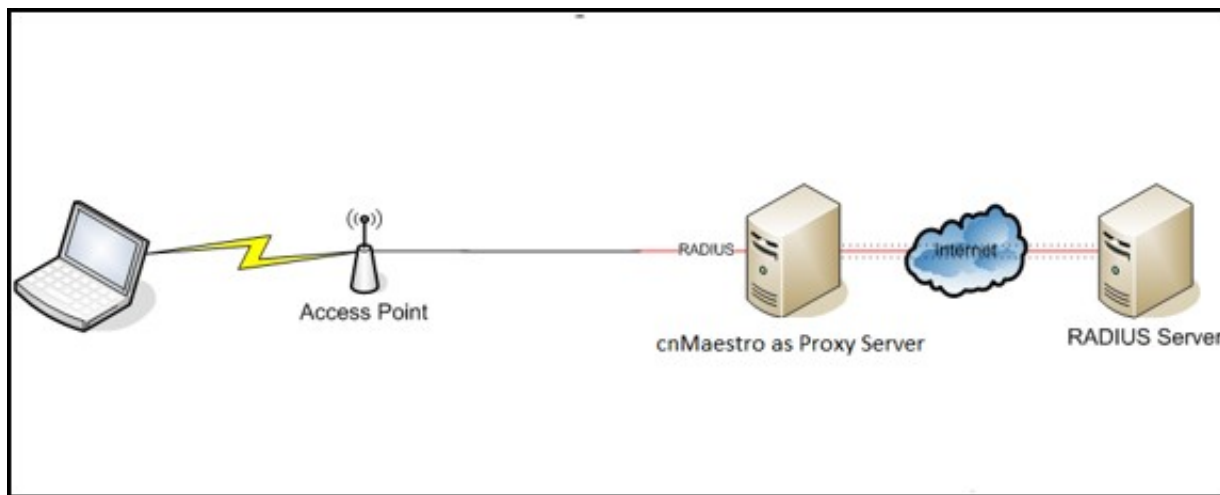


Figure 140 RADIUS Proxy on cnMaestro c4000 Controller

### Minimum cnMaestro c4000 Controller Version Requirements

- Minimum cnMaestro c4000 Controller release version required: 1.0-r7
- Minimum cnPilot AP release required: 3.11



#### Note

This feature is not available on the Cloud version of cnMaestro c4000 Controller.

### RADIUS Proxy Configuration

Follow the below procedure to configure RADIUS proxy on cnMaestro c4000 Controller:

1. Navigate to Shared Settings > WLANs and AP Groups page.
2. Select Enterprise WLAN to edit, and then select AAA Servers
3. Under AAA servers, select Proxy RADIUS through the cnMaestro c4000 Controller checkbox.

4. Configure Authentication Server details.
5. Configure Accounting Server details.
6. Configure NAS-Identifier. For this, include the NAS-Identifier attribute to use in RADIUS Request packets and Default to system name.
7. Push the configuration from cnMaestro c4000 Controller to AP.

**WLANs > Appliance**

[Configuration](#) APs

---

WLAN

**AAA Servers >**

Guest Access

Access Control

Passpoint

ePSK

**⚠ Warning:** AAA Servers are configured separately for each WLAN.

Proxy RADIUS through cnMaestro

**Authentication Server**

| 1. Host              | Secret                                   | Port*                             | Realm                |
|----------------------|--|-----------------------------------|----------------------|
| <input type="text"/> | <input type="text"/> <small>Show</small> | <input type="text" value="1812"/> | <input type="text"/> |
| 2. Host              | Secret                                   | Port*                             | Realm                |
| <input type="text"/> | <input type="text"/> <small>Show</small> | <input type="text" value="1812"/> | <input type="text"/> |
| 3. Host              | Secret                                   | Port*                             | Realm                |
| <input type="text"/> | <input type="text"/> <small>Show</small> | <input type="text" value="1812"/> | <input type="text"/> |

Timeout  Timeout in seconds for each request attempt (1-30)

Attempts  Number of attempts before giving up (1-3)

**⊕ Accounting Server**

**⊕ Advanced Settings**

Figure 141 RADIUS Proxy Configuration



## Appendix: Windows DHCP

---

This section details how to configure a Microsoft Windows-based DHCP server to send DHCP Options to Cambium devices such as ePMP, ePMP 1000 Hotspot, and cnPilot R190/r200P/201P/E400/E410/E500. It consists of the following four tasks:

- [Configuring Option 60](#)
- [Configuring Option 43](#)
- [Configuring Option 15](#)
- [Configuring Vendor Class Identifiers](#)

DHCP servers are a popular way to configure clients with basic networking information such as an IP address, default gateway, network mask, and DNS server. Most DHCP servers have the ability to also send a variety of optional information, including the Vendor-Specific Option Code Option 43. When a Cambium device requests Option 43 Vendor-Specific information, the DHCP server responds with values configured by the DHCP administrator.

### Configuring Option 60

This section describes how to configure the Vendor Class Identifier Code (option 60) on a Microsoft Windows-based DHCP server. As mentioned in the overview section, option 60 identifies and associates a DHCP client with a particular vendor. Since option 60 is not a predefined option on a Windows DHCP server, you must add it to the options list.

### Windows DHCP Server Configuration

1. On the DHCP server, open the DHCP server administration tool by clicking **Start > Administrative Tools > DHCP**.
2. Find your server and right-click on the scope to be configured under the server name. Select **Set Predefined Options**.
3. In the Predefined Options and Values dialog box, click **Add**.
4. In the **Option Type dialog** box, enter the following information and click **OK** to save.

| Field       | Information                             |
|-------------|---|
| Name        | Cambium Option 60                       |
| Data Type   | String (select the Array checkbox also) |
| Code        | 60                                      |
| Description | Cambium AP vendor class identifier      |

5. In the Predefined Options and Values dialog box, make sure 060 **Cambium Option 60** is selected from the Option Name drop-down list.

6. In the Value field, enter the following information: String: Cambium, Cambium-WiFi-AP, Cambium-cnPilot r200P, Cambium-cnPilot R201P.
7. Click **OK** to save this information.
8. Under the server, select the scope you want to configure and expand it. Select **Scope Options**, then select **Configure Options**.
9. In the **Scope Options** dialog box, scroll down and select 060 Cambium Option 60. Confirm the value is set as mentioned in point 7 above and click **OK**.



**Note**

The Data type should be a string. If only one device type is to be onboarded to the cnMaestro c4000 Controller server, then there is no need to select the Array option. If multiple device types need to be onboarded, then please select the Array option, so the value can contain multiple option 60 entries.

## Configuring Option 43

Option 43 returns the cnMaestro c4000 Controller URL to the Cambium Devices.

## Windows DHCP Server Configuration

1. On the DHCP server, open the server administration tool by clicking **Start > Administration Tools > DHCP**.
2. Find your server and right-click on the scope to be configured under the server name. Select **Set Predefined options**.
3. In the Predefined Options and Values dialog box, click **Add**.
4. In the Option Type dialog box, enter the following information

| Field       | Information          |
|-------------|----------------------|
| Name        | Cambium Option 43    |
| Data Type   | String               |
| Code        | 43                   |
| Description | Cambium AP Option 43 |

5. Click **OK** to save this information.
6. In the Predefined Options and Values dialog box, make sure 043 Cambium Option 43 is selected from the **Option Name** drop-down list.
7. In the Value field, enter the following information: String: https://<NOC Server Hostname/IP>
8. Click **OK** to save this information.

**Note**

If Option 43 is already in predefined options with the data type as Binary, then it cannot be changed to string. If this is the case, while defining the policies, specify the values in the ASCII column in the Actions tab of the policy after selecting Option 43. This will be detailed in the Policies section later in the document.

## Configuring Option 15

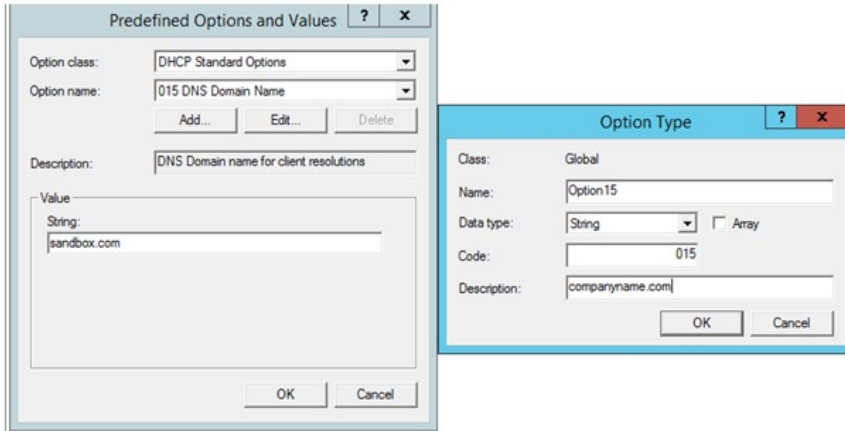
Option 15 returns the domain name to the Cambium Devices.

### Windows DHCP Server Configuration

1. On the DHCP server, open the server administration tool by clicking **Start > Administration Tools > DHCP**.
2. Find your server and right-click on the scope to be configured under the server name. Click on **Set Predefined Options**.
3. In the Predefined Options and Values dialog box, click **Add**.
4. In the Option Type dialog box, enter the following information:

| Field       | Information          |
|-------------|----------------------|
| Name        | Cambium Option 15    |
| Data Type   | String               |
| Code        | 15                   |
| Description | Cambium AP Option 15 |

5. Click **OK** to save this information.
6. In the Predefined Options and Values dialog box, make sure 015 Cambium Option 15 is selected from the **Option Name** drop-down list.
7. In the Value field, enter the following information: String: <companyname.com>
8. Click **OK** to save this information.

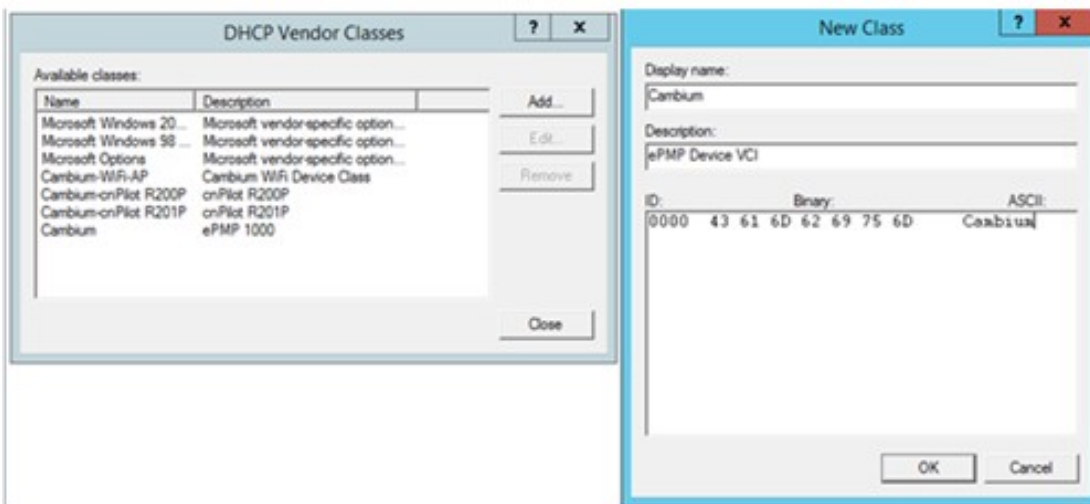


**Note**

In the DNS Server, the user needs to map the cnMaestro c4000 Controller hostname to the IP Address of the cnMaestro c4000 Controller On-Premises server.

## Configuring Vendor Class Identifiers

1. On the DHCP server, open the server administration tool by clicking **Start > Administration Tools > DHCP**.
2. Find your server and right-click on the scope to be configured under the server name. Click on the **Define Vendor Classes** and click the **Add** button in the dialog box that appears.
3. Provide the Display Name, Description and then click on the **ASCII** column and enter the value as **Cambium** as shown in the below figure, and then click **OK**.



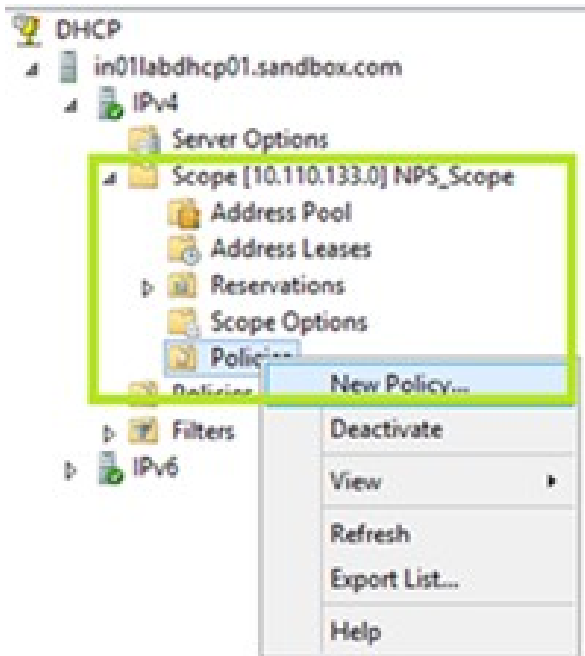
The above example is for an ePMP device. In order to create the VCI for other device types, please follow the same steps, and in the ASCII column provide the following values:

| Product            | VCI (DHCP Option 60)  |
|--------------------|-----------------------|
| cnPilot R200P      | Cambium-cnPilot r200P |
| cnPilot R201P      | Cambium-cnPilot R201P |
| cnPilot R190       | Cambium-cnPilot R190  |
| cnPilot Enterprise | Cambium-WiFi-AP       |
| ePMP               | Cambium               |
| ePMP 1000 hotspot  | Cambium-WiFi-AP       |

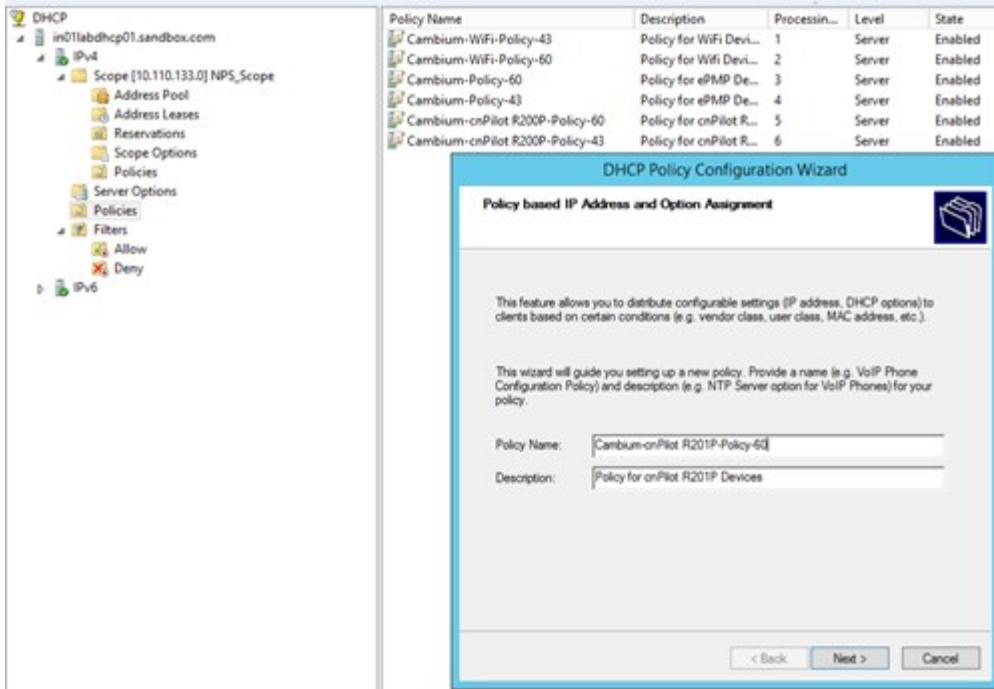
## Configuring the Policies at the SCOPE Level

Once Options 43, 60, 15, and Vendor Classes are created, one needs to create policies at the scope level. This allows the DHCP server to send the Option 43 and 60 to the Cambium Devices -- based on their VCI for that device. The policy will make sure these options are only sent if the VCI matches that provided by the device.

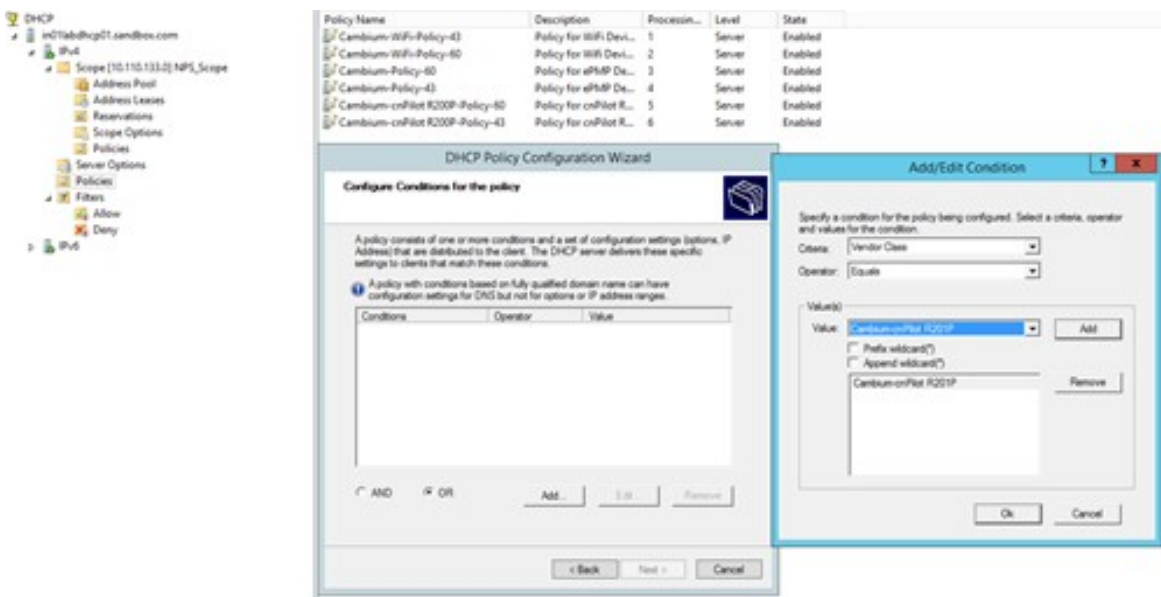
1. Select the scope in which you want to create the policy, and then right-click on the **Policies** option. Select New Policy.



2. In the popup, enter the Policy Name and Description and click **the Next** button.



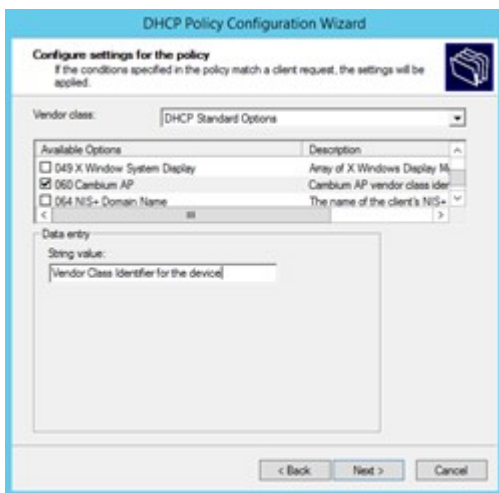
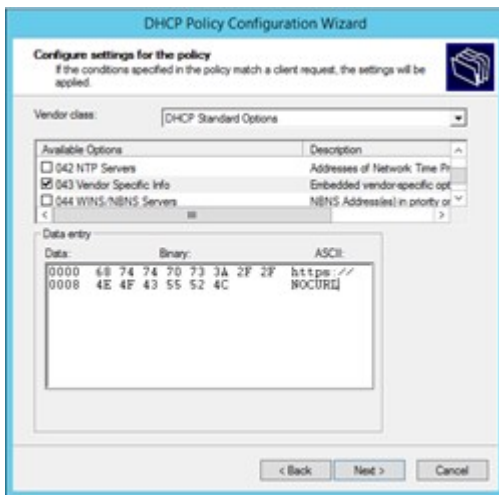
3. The Policy consists of Matching conditions based on Vendor Class, user class, MAC Address, Client Identifiers, FQDN and Relay Agent Information. For Cambium Devices we need Vendor Class-based match conditions only.
  - a. In the dialog, click on the **Add** button and in the popup select the Criteria as Vendor Class, the Operator as Equals, and the Value as the VCI created for the Cambium Device type.
  - b. For example, for cnPilot R201P device, the Vendor Class selection is “Cambium-cnPilot R201P”.
  - c. Click **Add** and then **OK** in the popup. Click **Next** in the Policy Configuration Wizard.



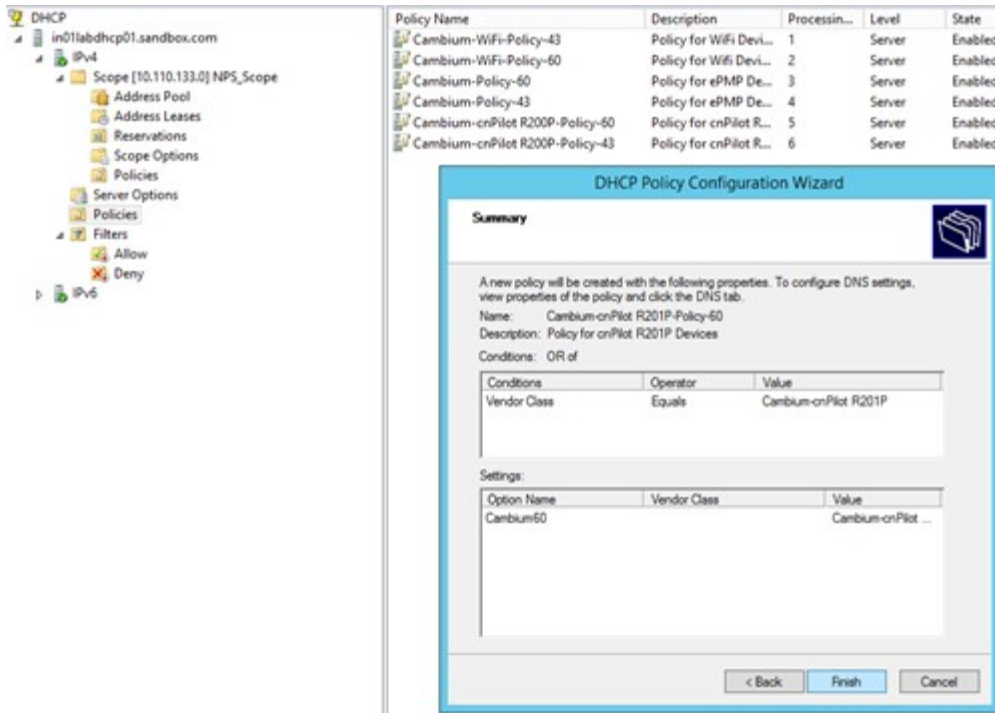
4. In the policy configuration settings wizard, select the **option No** and click **Next**.



Then select the vendor class as DHCP standard options and Select the options 43 and 60 from the available options and specify the values that need to be sent to the device. Click Next once the options are selected and values are specified.



5. Click **Finish** on the final settings page. The policy is displayed in the RHS pane.



The above Policy is a generic one. For all the device types, the policies should be created in a similar way --, with the match conditions and action as follows:

Also, Policies can be created at the Scope level or Server level. If the separate scope is defined for Cambium devices, it is better to define scope level policies; otherwise, the policies can be defined at the Server level in a similar way.

| Device Type       | Match Condition                                  | Actions  |
|-------------------|--|--|
| ePMP              | Vendor Class for ePMP                            | Cambium option 43 and 60 selected and values specified |
| ePMP 1000 Hotspot | Vendor Class for Hotspot                         | Cambium option 43 and 60 selected and values specified |
| cnPilot E-Series  | Vendor Class for E400/E410/E500/E501S/E502S/E600 | Cambium option 43 and 60 selected and values specified |
| cnPilot Home      | Vendor Class for cnPilot R190/R200/R201          | Cambium option 43 and 60 selected and values specified |



## Appendix: Network Port Requirements

### Network Port Requirements for Inbound

The following table provides information about network port requirements for inbound:

**Table 44 Inbound Port Details**

| SLNo. | Port Number | Port Type | Purpose  |
|-------|-------------|-----------|--|
| 1     | 443         | TCP       | HTTPs Web Access and device communication        |
| 2     | 18301       | TCP/UDP   | Wi-Fi Performance Test                           |
| 3     | 161         | UDP       | SNMP Communication                               |
| 4     | 22          | TCP       | Data Replication (High Availability)             |
| 5     | 8300        | TCP       | Distribution Synchronization (High Availability) |
| 6     | 8301        | TCP/UDP   | Distribution Synchronization (High Availability) |
| 7     | 3799        | UDP       | RADIUS CoA for RADIUS Proxy feature              |

### Network Port Requirements for Outbound

The following table provides information about network port requirements for outbound:

**Table 45 Outbound Port Details**

| SLNo. | Port Number | Port Type | Purpose  |
|-------|-------------|-----------|--|
| 1     | 18301       | TCP/UDP   | Wi-Fi Performance Test                             |
| 2     | 162         | UDP       | SNMP Trap Receiver                                 |
| 3     | 465 and 587 | TCP       | SMTP Server communication                          |
| 4     | 20 and 21   | TCP       | FTP and SFTP communication                         |
| 5     | 49          | TCP/UDP   | TACAC Server communication                         |
| 6     | 1812        | UDP       | Free Radius Server Authentication communication    |
| 7     | 1813        | UDP       | RADIUS Server Accounting communication             |
| 8     | 389 and 636 | TCP/UDP   | LDAP or Active Directory (AD) server communication |

# Cambium Networks

---

Cambium Networks provides professional grade fixed wireless broadband and microwave solutions for customers around the world. Our solutions are deployed in thousands of networks in over 153 countries, with our innovative technologies providing reliable, secure, cost-effective connectivity that is easy to deploy and proven to deliver outstanding metrics.

Our flexible Point-to-Multipoint (PMP) solutions operate in the licensed, unlicensed and federal frequency bands, providing reliable, secure, cost-effective access networks. With more than three million modules deployed in networks around the world, our PMP access network solutions prove themselves day-in and day-out in residential access, leased line replacement, video surveillance and smart grid infrastructure applications.

Our award-winning Point to Point (PTP) radio solutions operates in licensed, unlicensed and defined user frequency bands including specific FIPS 140-2 solutions for the U.S. Federal market. Ruggedized for 99.999% availability, our PTP solutions have an impeccable track record for delivering reliable high-speed backhaul connectivity even in the most challenging non-line-of sight RF environments.

Cambium Networks' solutions are proven respected leaders in the wireless broadband industry. We design, deploy and deliver innovative data, voice, and video connectivity solutions that enable and ensure the communications of life, empowering personal, commercial and community growth virtually everywhere in the world.

## Feedback

We appreciate feedback from the users of our documents. This includes feedback on the structure, content, accuracy, or completeness of our documents. To provide feedback, visit our support website.

## Contacting Cambium Networks

|                       |  |
|-----------------------|--|
| Support website       | <a href="https://www.cambiumnetworks.com/support/">https://www.cambiumnetworks.com/support/</a>                  |
| Main website          | <a href="https://www.cambiumnetworks.com/">https://www.cambiumnetworks.com/</a>                                  |
| Solutions enquiries   | <a href="https://www.cambiumnetworks.com/solutions/">https://www.cambiumnetworks.com/solutions/</a>              |
| Support enquiries     | <a href="https://support.cambiumnetworks.com/">https://support.cambiumnetworks.com/</a>                          |
| Repair enquires       | <a href="https://support.cambiumnetworks.com/">https://support.cambiumnetworks.com/</a>                          |
| Telephone number list | <a href="https://www.cambiumnetworks.com/contact-us/">https://www.cambiumnetworks.com/contact-us/</a>            |
| Address               | Cambium Networks Limited,<br>Unit B2, Linhay Business Park, Eastern Road<br>Ashburton, United Kingdom, TQ13 7UP. |