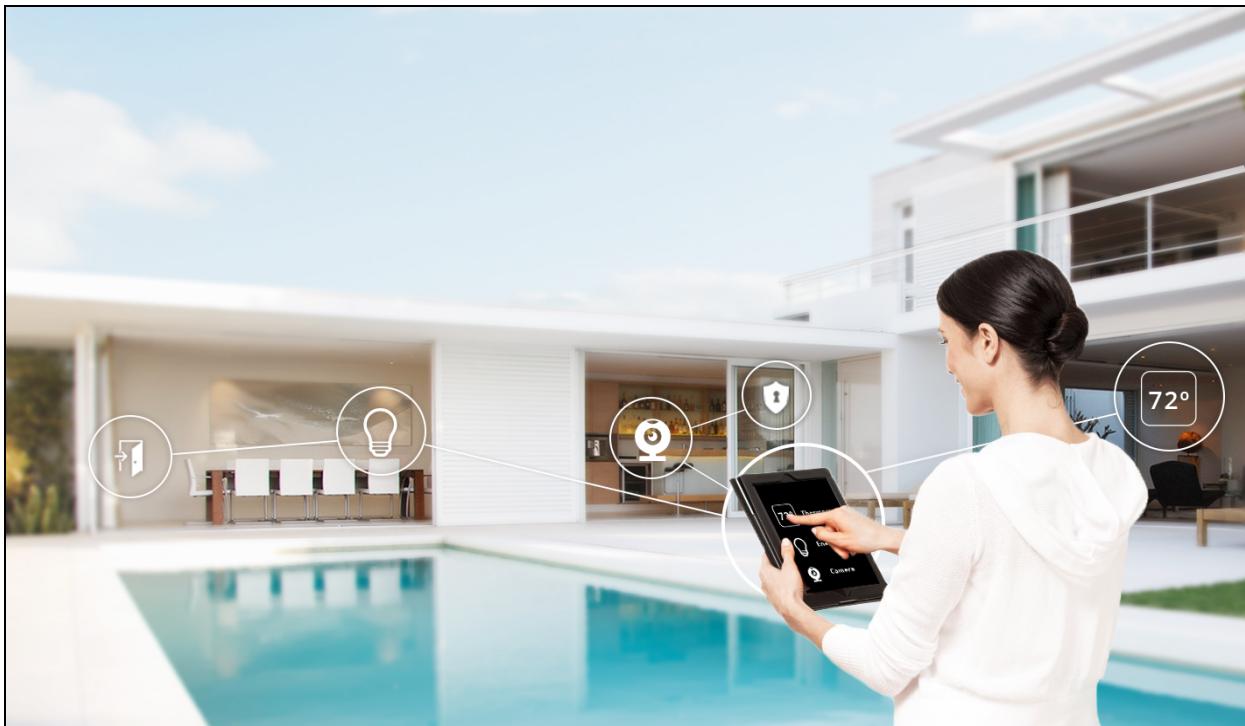




# System Operations Guide

7.3 Quadra



---

Copyright © 2016 Icontrol Networks, Inc. All rights reserved.

No reproduction in whole or in part without prior written approval. Icontrol Networks, Icontrol, and Icontrol logo design are pending trademarks of Icontrol Networks. All other trademarks are the property of their respective owners. Information contained herein is subject to change without notice. The only warranties for Icontrol products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Icontrol Networks shall not be liable for technical or editorial errors or omissions contained herein. All rights reserved.

## **Document Information**

Release version: 7.3 Quadra

Document name: System Operations Guide

Build date: 9/7/2016

# Contents

<b>Contents</b>	<b>3</b>
<b>Revision History</b>	<b>22</b>
<b>1 Introduction</b>	<b>35</b>
<b>2 System Security Against Web Application Attacks</b>	<b>36</b>
2.1 Web Applications Attacks	36
2.2 Cross Site Scripting (XSS)	36
2.3 Injection Flaws	36
2.4 Malicious File Execution	36
2.5 Insecure Direct Object Reference	36
2.6 Cross Site Request Forgery (CSRF)	37
2.7 Information Leakage and Improper Error Handling	37
2.8 Broken Authentication and Session Management	37
2.9 Insecure Cryptographic Storage	37
2.10 Insecure Communications	37
2.11 Failure to Restrict URL Access	37
<b>3 Process Flows</b>	<b>38</b>
3.1 Converge Activation	38
3.2 Touchstone Activation	42
<b>4 CPE Processes</b>	<b>47</b>
4.1 CPE Configuration File Back-up Behavior	47
<b>5 Message Sequence Diagrams</b>	<b>48</b>
5.1 TCP Connection Startup Sequence	49
5.2 UDP Activity	51
5.3 ZigBee Device Events Sequence (Broadband Connection)	53
5.4 Alarm Events Sequence (Broadband Connection)	54
5.5 Remote Arm/Disarm	55
5.5.1 Broadband Connection	55
5.5.2 Cellular-Only Connection	56
5.6 Security Router Provisioning & Reset/RMA Sequences	57
5.6.1 Router Provisioning	57
5.6.2 Router Reset/RMA	57
5.7 Touchscreen Firmware Update Sequence	58
5.7.1 Security Router Firmware Update	60
5.8 Camera Operations	61
5.8.1 Add Camera to Home Domain	61
5.8.2 Access Camera	62
<b>6 Video/Image Capture Details</b>	<b>65</b>
6.1 Legacy Cameras	65
6.2 OpenHome Cameras	65
6.2.1 RRC8026	65
6.2.2 iCamera2	65
6.2.3 OC431	66
6.3 Image/Video Capture Details	66
6.3.1 File Name	66

---

6.3.2 Path .....	66
<b>7 Contact ID Type Codes .....</b>	<b>68</b>
7.1 Icontrol CID Codes .....	68
7.1.1 CID 100 .....	69
7.1.2 CID 110 .....	69
7.1.3 CID 111 .....	70
7.1.4 CID 120 .....	70
7.1.5 CID 121 .....	70
7.1.6 CID 122 .....	71
7.1.7 CID 123 .....	71
7.1.8 CID 130 .....	72
7.1.8.1 alarm.backupServer.boundaryCase.contactId .....	72
7.1.9 CID 131 .....	73
7.1.10 CID 132 .....	73
7.1.11 CID 133 .....	74
7.1.12 CID 134 .....	74
7.1.13 CID 135 .....	75
7.1.14 CID 137 .....	75
7.1.15 CID 139 .....	76
7.1.16 CID 146 .....	76
7.1.17 CID 147 .....	77
7.1.18 CID 150 .....	77
7.1.19 CID 154 .....	78
7.1.20 CID 162 .....	78
7.1.21 CID 301 .....	79
7.1.22 CID 302 .....	79
7.1.23 CID 316 .....	79
7.1.24 CID 342 .....	80
7.1.25 CID 344 .....	80
7.1.26 CID 354 .....	80
7.1.27 CID 374 .....	81
7.1.28 CID 380 .....	81
7.1.29 CID 381 .....	82
7.1.30 CID 383 .....	83
7.1.31 CID 384 .....	83
7.1.32 CID 406 .....	84
7.1.32.1 Source: Touchscreen .....	84
7.1.32.2 Source: Operator Domain .....	84
7.1.33 CID 459 .....	84
7.1.34 CID 602 .....	84
7.1.35 CID 607 .....	85
7.1.36 CID 751 .....	86
7.1.37 CID 752 .....	86
7.2 Zone Function Behaviors .....	86
7.2.1 Entry/Exit Zone Function .....	88
7.2.1.1 Zone Faulted .....	88
7.2.1.2 Comm Failure Trouble .....	90
7.2.1.3 Tamper Trouble .....	90
7.2.2 Perimeter Zone Function .....	90

---

---

7.2.2.1 Zone Faulted .....	90
7.2.2.2 Comm Failure Trouble .....	90
7.2.2.3 Tamper Trouble .....	90
7.2.3 Trouble Day/Alarm Night Zone Function .....	91
7.2.3.1 Zone Faulted .....	91
7.2.3.2 Comm Failure Trouble .....	91
7.2.3.3 Tamper Trouble .....	91
7.2.4 24-Hour Inform Zone Function .....	92
7.2.4.1 Zone Faulted .....	92
7.2.4.2 Comm Failure Trouble .....	92
7.2.4.3 Tamper Trouble .....	92
7.2.5 Silent 24-Hour Zone Function .....	93
7.2.5.1 Zone Faulted .....	93
7.2.5.2 Comm Failure Trouble .....	93
7.2.5.3 Tamper Trouble .....	93
7.2.6 Audible 24-Hour Zone Function .....	94
7.2.6.1 Zone Faulted .....	94
7.2.6.2 Comm Fail .....	94
7.2.6.3 Tamper Trouble .....	94
7.2.7 24-Hour Fire Zone Function .....	95
7.2.7.1 Zone Faulted .....	95
7.2.7.2 Comm Failure Trouble .....	95
7.2.7.3 Tamper Trouble .....	95
7.2.8 Interior Follower Zone Function .....	96
7.2.8.1 Zone Faulted .....	96
7.2.8.2 Comm Failure Trouble .....	96
7.2.8.3 Tamper Trouble .....	96
7.2.9 Interior Follower Arm Night Zone Function .....	97
7.2.9.1 Zone Faulted .....	97
7.2.9.2 Comm Failure Trouble .....	97
7.2.9.3 Tamper Trouble .....	97
7.2.10 Interior With Delay Zone Function .....	98
7.2.10.1 Zone Faulted .....	98
7.2.10.2 Comm Failure Trouble .....	98
7.2.10.3 Tamper Trouble .....	98
7.2.11 Interior Delay Arm Night Zone Function .....	99
7.2.11.1 Zone Faulted .....	99
7.2.11.2 Comm Failure Trouble .....	99
7.2.11.3 Tamper Trouble .....	99
<b>8 Icontrol Connectivity Protocols .....</b>	<b>100</b>
8.1 Broadband Connectivity .....	100
8.1.1 Broadband Heartbeat .....	100
8.1.1.1 Broadband Heartbeat Message Size .....	100
8.1.2 Reporting Interval of Broadband Connectivity .....	101
8.1.3 Broadband Connectivity During Server Cluster Reboots .....	101
8.1.4 Viewer Engaged/Disengaged over Broadband .....	102
8.2 Cellular Connectivity .....	103
8.2.1 Cellular Heartbeat .....	103
8.2.2 Cellular Heartbeat Message Size .....	103

---

---

8.2.3 Reporting Cellular Connectivity .....	104
8.2.3.1 Server Detection .....	104
8.2.3.2 Touchscreen Detection .....	104
8.2.4 Network Address Translation (NAT) for Cellular Traffic .....	105
8.3 Broadband/Cellular Connectivity Problems and Resolutions .....	106
8.4 Loss of Service Protocols .....	108
8.4.1 Back-Up Alarm Server Fail-Over .....	108
8.4.2 Event History During Loss of Service .....	108
8.4.3 System Recovery .....	109
8.4.3.1 Scenario 1: .....	109
8.4.3.2 Scenario 2: .....	109
<b>9 Converge Touchscreen Connectivity .....</b>	<b>110</b>
9.1 Connectivity Test .....	110
9.2 Signal Strength .....	110
9.3 Broadband and Cellular IP Addresses Must Be Different .....	111
9.4 SMCWBR14S-N4 (White Router) Router Reboot Attempt .....	111
<b>10 Understanding Smash &amp; Grab .....</b>	<b>112</b>
10.1 Overview .....	112
10.2 Determining That Smash & Grab Has Occurred .....	112
10.2.1 Touchscreen Settings .....	112
10.2.2 Smash & Grab Tier Properties .....	113
10.2.2.1 alarm.alarm.smashAndGrab.contactId .....	113
10.2.2.2 alarm.smashAndGrab.send .....	113
10.2.2.3 alarm.smashAndGrab.waitTime .....	113
10.2.3 Smash & Grab Detection Custom Settings .....	113
10.2.3.1 alarm.smashAndGrabDisarmEventLookBackInterval .....	113
10.2.3.2 alarm.smashAndGrabAlarmLookBackInterval .....	114
10.3 Confirming a Smash & Grab Event (Cellular Ping) .....	114
10.3.1 Smash & Grab Confirmation Custom Settings .....	115
10.3.1.1 pingCellularUnit.implementation .....	115
10.3.1.2 pingCellularUnit.numerex.accountId .....	115
10.3.1.3 pingCellularUnit.numerex.gateway.url .....	115
10.3.1.4 pingCellularUnit.numerex.gateway.username .....	115
10.3.1.5 pingCellularUnit.numerex.gateway.password .....	116
10.3.1.6 pingCellularUnit.numerex.new.cid .....	116
10.3.1.7 pingCellularUnit.numerex.smsping.timeout.interval .....	116
10.3.1.8 pingCellularUnit.numerex.waiting .....	116
10.3.1.9 pingCellularUnit.att.gateway.url .....	117
10.3.1.10 pingCellularUnit.att.gateway.username .....	117
10.3.1.11 pingCellularUnit.numerex.gateway.password .....	117
10.3.1.12 pingCellularUnit.att.licenseKey .....	117
10.3.1.13 pingCellularUnit.numerex.waiting .....	117
10.4 Smash & Grab Scheduled Tasks .....	118
10.5 Testing Smash & Grab .....	118
<b>11 Alarm Delivery Error Handling .....</b>	<b>120</b>
11.1 Custom Error Handling .....	121
<b>12 Understanding the Icontrol WSDL .....</b>	<b>125</b>
12.1 Methods & API Functions .....	125

---

12.1.1 Create a Subscriber Account .....	126
12.1.2 Update Account Information .....	127
12.1.3 Suspend Service of an Active Account .....	128
12.1.4 Restore Service for a Suspended Account .....	129
12.1.5 Deactivate an Account .....	129
12.1.6 Delete an Unactivated Account .....	130
12.1.7 Get Account Information .....	130
12.1.8 Change Which Tier Is Assigned to an Account .....	131
12.1.9 Change Which Tier Group Is Assigned to an Account .....	131
12.1.10 Add a Package to an Account .....	132
12.1.11 Remove a Package from an Account .....	132
12.1.12 Add a CPE Device to Inventory (Not Implemented) .....	133
12.2 Inputs .....	134
12.2.1 Account .....	135
12.2.2 AccountSourceType .....	136
12.2.3 AccountStatus .....	136
12.2.4 Address .....	137
12.2.5 Camera .....	138
12.2.6 Contact .....	139
12.2.7 Cpe .....	140
12.2.8 CpeInventory .....	141
12.2.9 DeploymentModel .....	143
12.2.10 DoorLock .....	144
12.2.11 EmergencyContact .....	145
12.2.12 EmergencyContactType .....	145
12.2.13 FullAccount .....	146
12.2.14 GenericDevice .....	148
12.2.15 Lighting .....	149
12.2.16 LightingType .....	149
12.2.17 Locale .....	150
12.2.18 Module .....	151
12.2.19 ModuleType .....	151
12.2.20 Peripheral .....	152
12.2.21 PeripheralType .....	153
12.2.22 Phone .....	154
12.2.23 PhoneType .....	154
12.2.24 PortalUser .....	154
12.2.25 Premise .....	155
12.2.26 ProductName .....	156
12.2.27 Property .....	156
12.2.28 Sensor .....	157
12.2.29 SensorSourceType .....	157
12.2.30 SensorType .....	158
12.2.31 Thermostat .....	160
12.2.32 ThermostatType .....	160
12.2.33 Tier .....	161
12.2.34 Time Zone .....	161
12.2.35 WidgetNameVersion .....	162
12.2.36 Zone .....	163

---

12.2.37 ZoneFunctionType .....	163
12.2.38 ZoneType .....	164
<b>13 Apache/WebLogic HealthCheck Service .....</b>	<b>166</b>
<b>14 ICHealthCheck Service .....</b>	<b>167</b>
14.1 Accessing the ICHealthCheck Page and Queries .....	167
14.1.1 Test Messages Service .....	167
14.2 Configuring the ICHealthCheck .....	168
14.3 Query Details .....	169
14.3.1 getServerVersion .....	169
14.3.2 getTotalEthernetLossAccounts .....	169
14.3.3 getTopNTSRebootAccount .....	169
14.3.4 getNumberOfAccountWithPowerLoss .....	170
14.3.5 getListOfAccountWithPowerLoss .....	170
14.3.6 getSQLStats .....	170
14.3.7 getTopSQLByGetsPerExecution .....	170
14.3.8 getConnectedDeviceCount .....	170
14.3.9 getNumberOfDataSyncPerDay .....	171
14.3.10 getNumberOfDBLocks .....	171
14.3.11 findDBLocksDetails .....	171
14.3.12 findSensComTroubleEventsByTimeRange .....	171
14.3.13 getNumberOfAccountOfCellularTCPConnected .....	171
14.3.14 getPremisesWithHighCellConnection .....	172
14.3.15 getAccountCount .....	172
14.3.16 getConnectedPremiseCount .....	173
14.3.17 getRawBroadbandDownCountByZipCodeCityAndState .....	173
14.3.18 getDatabaseMonitorLogDetail .....	173
14.3.19 getDatabaseMonitorLog .....	174
14.3.20 getConnectedNonActivatedCPECount .....	174
14.3.21 getUDPIIncomingMessageQueueSize .....	174
14.3.22 getUDPOutgoingMessageQueueSize .....	174
<b>15 ICStatusCheck Service .....</b>	<b>175</b>
15.1 Usage .....	175
15.2 Types .....	176
15.2.1 Counters .....	176
15.2.2 Stats in Time Buckets .....	176
15.2.2.1 Name .....	177
15.2.2.2 Date Collected (or timestampCollected and dateCollected) .....	177
15.2.3 Stats in Time Buckets & Average Duration .....	178
15.2.4 WebLogic JMX .....	178
<b>16 Healthcheck Configuration .....</b>	<b>179</b>
16.1 Modify each server to use the 5222CompoundCheck on port 5222 .....	181
16.1.1 Create a Compound Healthcheck .....	182
16.2 Configure the TCP port 5222 Service Group .....	183
<b>17 Management Portal Roles and Privileges .....</b>	<b>183</b>
<b>18 CPE Statistics Collection and Reporting .....</b>	<b>184</b>
18.1 Enabling Statistics Collection .....	184
18.2 Available Reports .....	185

---

18.2.1 BatteryStats .....	185
18.2.2 CommStats .....	186
18.2.3 SystemStats .....	187
18.2.4 ZigbeeTroubleStats .....	187
18.3 Customizing the Reports .....	187
<b>19 Log Files .....</b>	<b>188</b>
19.1 Example Log Messages .....	188
19.2 Debugging Information .....	189
<b>20 Exception Codes (UCE) .....</b>	<b>190</b>
20.1 Integration-Specific UCE Codes .....	191
20.2 Threshold Levels .....	192
20.3 Alarm Handling .....	192
20.4 UCE Codes .....	193
20.4.1 UCE-01000 alarm.missingArsCallbackUrl .....	193
20.4.2 UCE-01001 alarm.devMode .....	193
20.4.3 UCE-01002 alarm.noSender .....	194
20.4.4 UCE-01003 eventBus.initializeFailed .....	194
20.4.5 UCE-03000 server.relay.server.init .....	194
20.4.6 UCE-03001 server.no.deviceFirmwareBaseUrl .....	194
20.4.7 UCE-03002 server.relay.server.insight .....	195
20.4.8 UCE-03003 server.no.cameraFirmwareBaseUrl .....	195
20.4.9 UCE-03004 server.no.systemDeploymentCustomerName .....	195
20.4.10 UCE-03005 server.no.cloudIntegrationOauth2RedirectUrl .....	195
20.4.11 UCE-03600 server.cat.partner.oauth.no.associateAccountUrl .....	196
20.4.12 UCE-03601 server.cat.event.integration.not.enabled .....	196
20.4.13 UCE-11000 alarm.agedMessage .....	196
20.4.14 UCE-11002 alarm.expiredMessage .....	197
20.4.15 UCE-11003 alarm.failedMessage .....	197
20.4.16 UCE-13000 server.media.ffmpeg .....	198
20.4.17 UCE-13001 server.relay.session.creation .....	198
20.4.18 UCE-13002 server.relay.session.ssh.creation .....	198
20.4.19 UCE-13003 server.relay.session.ssh.noport .....	199
20.4.20 UCE-13004 server.touchscreen.sensor.commFail.invalidDelay .....	199
20.4.21 UCE-13005 server.securityEventAttachment.ruleId.length .....	199
20.4.22 UCE-13006 server.nfsservice.unavailable .....	199
20.4.23 UCE-13007 server.schedule.task.exception .....	200
20.4.24 UCE-13008 server.timer.task.exception .....	200
20.4.25 UCE-13600 server.cat.partner.rule.template.type.invalid .....	200
20.4.26 UCE-13601 server.cat.partner.rule.template.trigger.invalid .....	200
20.4.27 UCE-13602 server.cat.partner.rule.template.trigger.type.invalid .....	200
20.4.28 UCE-13603 server.cat.partner.rule.template.trigger.excludeActionIds.not.exist .....	200
20.4.29 UCE-13604 server.cat.partner.rule.template.trigger.targetValues.resource.not.exist .....	201
20.4.30 UCE-13605 server.cat.partner.rule.template.trigger.mediaType.not.exist .....	201
20.4.31 UCE-13606 server.cat.partner.rule.template.action.invalid .....	201
20.4.32 UCE-13607 server.cat.partner.rule.template.action.mediaType.not.exist .....	201
20.4.33 UCE-13608 server.cat.partner.rule.template.resource.not.exist .....	201
20.4.34 UCE-13609 server.cat.partner.rule.template.description.resource.not.exist .....	201
20.4.35 UCE-13610 server.cat.partner.rule.template.inputs.not.exist .....	202

---

20.4.36 UCE-13611 server.cat.partner.rule.template.tags.not.exist .....	202
20.4.37 UCE-13612 server.cat.partner.oauth.account.not.found .....	202
20.4.38 UCE-13613 server.cat.partner.oauth.integration.not.allowed .....	202
20.4.39 UCE-13614 server.cat.partner.oauth.provider.invalid .....	202
20.4.40 UCE-13615 server.cat.partner.oauth.accountInformation.invalid .....	203
20.4.41 UCE-13616 server.cat.partner.oauth.account.retrieve.failed .....	203
20.4.42 UCE-13617 server.cat.partner.oauth.virtualDevice.siteId .....	203
20.4.43 UCE-13618 server.cat.partner.oauth.cloudObject.invalid .....	203
20.4.44 UCE-13619 server.cat.partner.oauth.account.already.associated .....	204
20.4.45 UCE-13620 server.cat.partner.oauth.onboarding.general.problem.serve .....	204
20.4.46 UCE-13621 server.cat.partner.delete.account.already.associated .....	204
20.4.47 UCE-13622 server.cat.partner.oauth.account.associated.mismatch .....	204
20.4.48 UCE-13623 server.cat.partner.rule.template.trigger.mediaType.lifecycle.not.allowed .....	204
20.4.49 UCE-13624 server.cat.partner.oauth.cloudObjectType.invalid .....	205
20.4.50 UCE-13900 persistence.objectDoesNotExistWithTime .....	205
20.4.51 UCE-13901 persistence.nonUniqueResult .....	205
20.4.52 UCE-13902 persistence.nullArgument .....	205
20.4.53 UCE-14000 activation.activated .....	206
20.4.54 UCE-14001 activation.wrong.orderNumber .....	206
20.4.55 UCE-14002 activation.wrong.phoneNumber .....	206
20.4.56 UCE-14003 activation.wrong.cpeld .....	206
20.4.57 UCE-14004 activation.notReadyForActivation .....	206
20.4.58 UCE-14005 activation.deviceAlreadyAttached .....	207
20.4.59 UCE-14006 activation.notActivated .....	207
20.4.60 UCE-14007 activation.userAlreadySetUp .....	207
20.4.61 UCE-14008 activation.cpeAlreadyUsed .....	207
20.4.62 UCE-14009 activation.wrong.orderNumberMultiDeployment .....	207
20.4.63 UCE-14010 activation.missingEmailAddress .....	207
20.4.64 UCE-14011 activation.wrong.productType .....	208
20.4.65 UCE-14012 activation.email.failToSend .....	208
20.4.66 UCE-14013 activation.cls.cpeAlreadyUsed .....	208
20.4.67 UCE-14014 activation.system.failed .....	208
20.4.68 UCE-14600 cellular.communication.messageHandlingException .....	208
20.4.69 UCE-14601 cellular.communication.unsupportedMessageVersion .....	209
20.4.70 UCE-14602 cellular.communication.noHandlerFound .....	209
20.4.71 UCE-14603 cellular.communication.udp.receiverException .....	209
20.4.72 UCE-14604 cellular.communication.udp.senderException .....	210
20.4.73 UCE-15000 integration.cs.exception .....	210
20.4.74 UCE-15001 integration.cs.unknown.receiver .....	210
20.4.75 UCE-15100 integration.account.general .....	211
20.4.76 UCE-15101 integration.account.notFound .....	211
20.4.77 UCE-15102 integration.account.alreadyActivated .....	211
20.4.78 UCE-15103 integration.account.alreadyExist .....	212
20.4.79 UCE-15104 integration.account.missingProperty .....	212
20.4.80 UCE-15105 integration.account.wrongCSAccountNumberLength .....	212
20.4.81 UCE-15106 integration.account.csReceiverNotFound .....	212
20.4.82 UCE-15107 integration.account.csAccountUsed .....	213
20.4.83 UCE-15108 integration.account.notExternal .....	213
20.4.84 UCE-15109 integration.account.firstNameHasWrongChar .....	213

---

---

20.4.85 UCE-15110 integration.account.lastNameHasWrongChar .....	213
20.4.86 UCE-15111 integration.account.emergencyContact.firstNameHasWrongChar .....	214
20.4.87 UCE-15112 integration.account.emergencyContact.lastNameHasWrongChar .....	214
20.4.88 UCE-15113 integration.account.notActivated .....	214
20.4.89 UCE-15114 integration.account.deploymentNotFound .....	214
20.4.90 UCE-15115 integration.account.deploymentDoesNotMatch .....	215
20.4.91 UCE-15116 integration.account.missingDeployment .....	215
20.4.92 UCE-15117 integration.account.illegalCountry .....	215
20.4.93 UCE-15118 integration.group.notFound .....	215
20.4.94 UCE-15119 integration.group.multipleTier .....	216
20.4.95 UCE-15120 integration.group.noTier .....	216
20.4.96 UCE-15121 integration.group.notTier .....	216
20.4.97 UCE-15122 integration.account.generalWithMsg .....	216
20.4.98 UCE-15123 integration.product.notFound .....	217
20.4.99 UCE-15124 integration.missingEmail .....	217
20.4.100 UCE-15125 integration.userExists .....	217
20.4.101 UCE-15126 integration.product.update .....	217
20.4.102 UCE-15127 integration.group.cannot.add .....	218
20.4.103 UCE-15128 integration.account.wrong.csMonitorFlag .....	218
20.4.104 UCE-15129 integration.account.invalid.activationCode .....	218
20.4.105 UCE-15130 integration.account.emergencyContact.invalidPhoneNumber .....	218
20.4.106 UCE-15131 integration.account.externalRefrence.invalidCharacter .....	218
20.4.107 UCE-15132 integration.account.invalid.monitoredFlag .....	219
20.4.108 UCE-15133 integration.account.invalid.internalFlag .....	219
20.4.109 UCE-16000 rest.resource.notFound .....	219
20.4.110 UCE-16001 rest.function.notFound .....	219
20.4.111 UCE-16002 rest.function.invalidparamter .....	219
20.4.112 UCE-16003 rest.point.notFound .....	220
20.4.113 UCE-16004 rest.general.problem.serve .....	220
20.4.114 UCE-16005 rest.general.paramterOutOfRange .....	220
20.4.115 UCE-16006 rest.general.accountNotProvisioned .....	220
20.4.116 UCE-16007 rest.general.accountNotActive .....	220
20.4.117 UCE-16008 rest.general.deviceNotConnected .....	221
20.4.118 UCE-16009 rest.general.usernameAlreadyExists .....	221
20.4.119 UCE-16010 rest.general.invalidPassword .....	221
20.4.120 UCE-16011 rest.general.eventHistory.query.dateRangeTooLong .....	221
20.4.121 UCE-16012 rest.general.contactCustomerSupport .....	221
20.4.122 UCE-16013 rest.general.primaryContactOrderNotAllowed .....	222
20.4.123 UCE-16014 rest.general.invalidEmergencyContactOrder .....	222
20.4.124 UCE-16100 rest.keypad.masterCode.wrongNotLocked .....	222
20.4.125 UCE-16101 rest.keypad.masterCode.wrongLocked .....	222
20.4.126 UCE-16102 rest.keypad.masterCode.stillLocked .....	222
20.4.127 UCE-16103 rest.keypad.masterCode.cantDelete .....	223
20.4.128 UCE-16104 rest.keypad.mastercode.invalid .....	223
20.4.129 UCE-16105 rest.keypad.mastercode.notEditable .....	223
20.4.130 UCE-16106 rest.keypad.duresscode.notEditable .....	223
20.4.131 UCE-16107 rest.take.video.max.quota.reached .....	223
20.4.132 UCE-16108 rest.take.image.max.quota.reached .....	224
20.4.133 UCE-16109 rest.schedule.rule.exists .....	224

---

---

20.4.134 UCE-16110 rest.schedule.rule.not.found .....	224
20.4.135 UCE-16111 rest.rule.video.attachment.not.allowed .....	224
20.4.136 UCE-16200 rest.cloudIntegration.notReady .....	224
20.4.137 UCE-16201 rest.cloudIntegration.refresh.token .....	225
20.4.138 UCE-16202 rest.cloudIntegration.general .....	225
20.4.139 UCE-16203 rest.cloudIntegration.event.history.event.conversion.string.failed .....	225
20.4.140 UCE-16204 rest.cloudIntegration.event.history.event.conversion.icEvent.failed .....	225
20.4.141 UCE-16205 rest.cloudIntegration.event.history.parse.failed .....	225
20.4.142 UCE-16206 rest.cloudIntegration.event.history.save.failed .....	225
20.4.143 UCE-16207 rest.cloudIntegration.renew.token.general .....	226
20.4.144 UCE-16208 rest.bundle.invalid.bundleType .....	226
20.4.145 UCE-16209 rest.bundle.invalid.bundleContent.format .....	226
20.4.146 UCE-16210 rest.bundle.invalid.bundle.device.type .....	226
20.4.147 UCE-16211 rest.bundle.invalid.bundle.type.exists .....	227
20.4.148 UCE-16212 rest.bundle.invalid.bundle .....	227
20.4.149 UCE-16300 rest.cloudIntegrationServer.register.callback.failed .....	227
20.4.150 UCE-16301 rest.cloudIntegrationServer.problem.icEvent .....	227
20.4.151 UCE-16302 rest.cloudIntegrationServer.icEvent.invalidData .....	227
20.4.152 UCE-16303 rest.cloudIntegrationServer.icEvent.partner.inactive .....	228
20.4.153 UCE-16304 rest.cloudIntegrationServer.cache.notEnabled .....	228
20.4.154 UCE-21000 alarm.telephony.failedMessage .....	228
20.4.155 UCE-21001 alarm.telephony.timedoutMessage .....	228
20.4.156 UCE-21020 alarm.session.waitingTooLong .....	229
20.4.157 UCE-22100 notification.failToSendEmail .....	229
20.4.158 UCE-22200 notification.failToSendSms .....	229
20.4.159 UCE-22210 notification.failToSendSimpleWireSms .....	230
20.4.160 UCE-22300 notification.failToSend .....	230
20.4.161 UCE-23500 server.cls.update.exception .....	230
20.4.162 UCE-23501 server.cls.site.create.exception .....	230
20.4.163 UCE-23502 server.cls.user.create.exception .....	231
20.4.164 UCE-23503 server.cls.site.update.exception .....	231
20.4.165 UCE-23504 server.cls.user.update.exception .....	231
20.4.166 UCE-23505 server.cls.site.delete.exception .....	231
20.4.167 UCE-23506 server.cls.user.delete.exception .....	231
20.4.168 UCE-24100 broadband.communication.smapException .....	232
20.4.169 UCE-24101 broadband.communication.connectionTotalLost .....	232
20.4.170 UCE-24102 broadband.communication.broadbandLost .....	232
20.4.171 UCE-24103 broadband.communication.broadbandLost .....	232
20.4.172 UCE-24600 cellular.communication.ipNotFound .....	232
20.4.173 UCE-24601 cellular.communication.cannotSendCommand .....	233
20.4.174 UCE-24602 cellular.communication.missingActorType .....	233
20.4.175 UCE-24603 cellular.communication.udp.senderInterrupted .....	233
20.4.176 UCE-25020 integration.address.ioException .....	233
20.4.177 UCE-25021 integration.address.requestOverLimit .....	233
20.4.178 UCE-25022 integration.address.requestDenied .....	234
<b>21 Properties .....</b>	<b>235</b>
21.1 server.properties .....	235
21.1.1 account.hardDelete.enabled .....	235
21.1.2 account.activationCode.length .....	235

---

---

21.1.3 account.activationCode.numberOnly .....	236
21.1.4 account.character.blacklist .....	236
21.1.5 accountIntegration.returnSecretWord .....	236
21.1.6 alarm.ipAlarmSender .....	237
21.1.7 alarm.ipAlarmSender.httpGetAlarmSender.baseUrl .....	237
21.1.8 alarm.maxAgeToLogError .....	237
21.1.9 alarm.maxCheckingPeriodForUnsendAlarm .....	238
21.1.10 alarm.multipleCidEnabled .....	238
21.1.11 alarm.queue.concurrentConsumers .....	238
21.1.12 alarm.requestErrorHandler .....	238
21.1.13 alarm.smashAndGrabDisarmEventLookBackInterval .....	239
21.1.14 alarm.smashAndGrabAlarmLookBackInterval .....	239
21.1.15 alarm.telephonyAlarmSender .....	239
21.1.16 alarm.unprocessedCheckingPeriod.inWaitingStatus .....	239
21.1.17 alarm.testDuration .....	240
21.1.18 alerts.allowZoneActivitySms .....	240
21.1.19 api.serverToServer.deltas.enabled .....	240
21.1.20 ars.callbackUrl .....	240
21.1.21 ars.callbackUrl.backupServer .....	241
21.1.22 ars.asteriskManagerHostname .....	241
21.1.23 ars.asteriskManagerUsername .....	241
21.1.24 ars.asteriskManagerPassword .....	241
21.1.25 ars.asteriskChannelDialPrefix .....	242
21.1.26 asyncServlet.scavangeInterval .....	242
21.1.27 backupServer.ip .....	242
21.1.28 batchUpdateItem.percentageToAbort .....	242
21.1.29 batchUpdateItem.size .....	242
21.1.30 batchUpdateItem.successPercentage .....	243
21.1.31 batchUpdateItem.timeout .....	243
21.1.32 batchUpdateRequest.sleepInterval .....	243
21.1.33 batchUpdateTask.runInterval .....	243
21.1.34 broadbandCommunicationEvent.markFactor .....	244
21.1.35 broadbandDownCellularMsg.max.try .....	244
21.1.36 bundle.import.file.format .....	244
21.1.37 bundle.import.log.directory .....	245
21.1.38 bundle.import.log.directory.windows .....	245
21.1.39 cameraAccessProxyUrl .....	245
21.1.40 camera.firmwareBaseUrl .....	245
21.1.41 cameraVideoRecordUrl .....	245
21.1.42 cat.onboarding.complete.redirectUrl .....	245
21.1.43 cellular.import.file.format .....	246
21.1.44 cellular.import.log.directory .....	246
21.1.45 cellular.import.log.directory.windows .....	246
21.1.46 centralStation.emergencyContact.notify .....	246
21.1.47 centralStation.emergencyContact.verify.min .....	246
21.1.48 centralStation.emergencyContact.verify.max .....	246
21.1.49 centralStation.implementation .....	247
21.1.50 centralStation.integration.enabled .....	248
21.1.51 centralStation.integration.synchronous .....	248

---

21.1.52 centralStation.integration.accountCreation.waitTime .....	248
21.1.53 centralStation.notification.emailAddress.to .....	249
21.1.54 centralStation.numberOfWorkQueue .....	250
21.1.55 centralStation.notification.emailAddress.to .....	250
21.1.56 centralStation.notification.emailAddress.from .....	250
21.1.57 cloudIntegration.accountGroupAutoAdd .....	250
21.1.58 cloudIntegration.accuWeather.temperatureChangeNotificationBlackoutPeriod .....	251
21.1.59 cloudIntegration.auto.commit.enable .....	251
21.1.60 cloudIntegration.auto.offset.reset .....	251
21.1.61 cloudIntegration.consumer.group.name.prefix .....	251
21.1.62 cloudIntegration.consumer.thread.count .....	252
21.1.63 cloudIntegration.consumer.timeout.ms .....	252
21.1.64 cloudIntegration.enabled .....	252
21.1.65 cloudIntegration.history.consumer.thread.count .....	252
21.1.66 cloudIntegration.history.enabled .....	252
21.1.67 cloudIntegration.history.service.appkey .....	252
21.1.68 cloudIntegration.history.service.password .....	253
21.1.69 cloudIntegration.history.service.username .....	253
21.1.70 cloudIntegration.internal.topic .....	253
21.1.71 cloudIntegration.metadata.broker.list .....	253
21.1.72 cloudIntegration.oauth2.redirectUrl .....	254
21.1.73 cloudIntegration.partnerProxy.connectionPool.connectTimeout .....	254
21.1.74 cloudIntegration.partnerProxy.connectionPool.defaultMaxPerRoute .....	254
21.1.75 cloudIntegration.partnerProxy.connectionPool.maxTotal .....	254
21.1.76 cloudIntegration.partnerProxy.connectionPool.requestTimeout .....	254
21.1.77 cloudIntegration.server.name.system.property .....	254
21.1.78 cloudIntegration.topic .....	255
21.1.79 cloudIntegration.zookeeper.connect .....	255
21.1.80 cloudIntegrationHistory.auto.commit.interval.ms .....	255
21.1.81 cloudIntegrationHistory.auto.offset.reset .....	255
21.1.82 cloudIntegrationHistory.zookeeper.connect .....	256
21.1.83 cloudIntegrationHistory.zookeeper.session.timeout.ms .....	256
21.1.84 cloudIntegrationHistory.zookeeper.sync.time.ms .....	256
21.1.85 cls.auth.password .....	256
21.1.86 cls.auth.username .....	256
21.1.87 cls.url .....	257
21.1.88 cls.cluster.hostname .....	257
21.1.89 cls.cluster.number .....	257
21.1.90 cls.domain .....	257
21.1.91 cls.enabled .....	257
21.1.92 cls.username.prefix .....	257
21.1.93 command.default.timeout .....	258
21.1.94 command.firmwareupdate.timeout .....	258
21.1.95 command.multicast.delay .....	258
21.1.96 configUrl .....	258
21.1.97 contextPathForLoginURL .....	259
21.1.98 contextPathForResetPassword .....	259
21.1.99 converge.camera.trouble.enabled .....	260
21.1.100 converge.sendActivationEmail .....	260

---

21.1.101 cpe.diagnostics.<suffix>	260
21.1.102 cpe.import.file.format	260
21.1.103 cpe.import.file.format.insight	261
21.1.104 cpe.import.log.directory	261
21.1.105 cpe.import.log.directory.windows	261
21.1.106 cpe.panicScreenDisabled	262
21.1.107 cpe.telemetry.collection.maxDay	263
21.1.108 database.monitor.average.duration	263
21.1.109 database.monitor.operation.interval	263
21.1.110 database.monitor.renew.duration	263
21.1.111 database.userName	263
21.1.112 deploymentCustomerName	264
21.1.113 deploymentCustomerSupportPhone	264
21.1.114 deploymentCustomerSupportEmail	264
21.1.115 device.diagnostic.directory	264
21.1.116 device.diagnostic.directory.windows	264
21.1.117 device.dump.directory	264
21.1.118 device.dump.directory.windows	264
21.1.119 device.firmwareBaseUrl	265
21.1.120 device.image.directory	265
21.1.121 device.image.directory.windows	265
21.1.122 device.screenshot.directory	265
21.1.123 device.screenshot.directory.windows	265
21.1.124 device.tamper.enabled	265
21.1.125 diagnosticUrl	266
21.1.126 distributed.cache.enabled	266
21.1.127 dumpUrl	266
21.1.128 email.queue.concurrentConsumers	266
21.1.129 eventHistory.query.dateRange.max	266
21.1.130 eventIntegration.enabled	267
21.1.131 firmware.allowDowngrade	267
21.1.132 firmware.download.timeout	267
21.1.133 firmware.misc.directory	267
21.1.134 firmware.misc.directory.windows	267
21.1.135 firmware.suspendedAccountReconnectTime	267
21.1.136 firmware.waitTimeAfterDisarm	268
21.1.137 imageUrl	268
21.1.138 grps.test.enabled	268
21.1.139 gprs.port	268
21.1.140 gprs.client.port	268
21.1.141 gprs.handlerPoolSize	268
21.1.142 gprs.encrypt	269
21.1.143 html.inputtype.text.autocomplete	269
21.1.144 http.client.connection.default.connection.timeout<.module>	269
21.1.145 http.client.connection.default.connection.timeout.clsIntegration	270
21.1.146 http.client.connection.default.so.timeout<.module>	270
21.1.147 http.client.connection.pool.timeout<.module>	271
21.1.148 http.client.connectionPool.defaultMaxPerRoute	272
21.1.149 http.client.connectionPool.defaultMaxTotal	272

---

21.1.150 ihealthcheck.test.emailAddress.from .....	272
21.1.151 insight.cpePairingWaitTime .....	272
21.1.152 insight.sendActivationEmail .....	272
21.1.153 insight.showInvalidDefaultRules .....	273
21.1.154 insight.singleAccessSessionIdleTimeout .....	273
21.1.155 java.naming.provider.url .....	273
21.1.156 java.naming.provider.url.portal.cluster .....	273
21.1.157 jms.receiveTimeout .....	273
21.1.158 jms.timeToLive.accountCentralStationIntegration .....	274
21.1.159 jms.timeToLive.alarmRequest .....	274
21.1.160 jms.timeToLive.cpeCommand .....	274
21.1.161 jms.timeToLive.default .....	274
21.1.162 jms.timeToLive.nonPersistentTopic .....	275
21.1.163 keypad.code.lockTime .....	275
21.1.164 keypad.code.max.retry .....	275
21.1.165 managementPortal.localeList .....	275
21.1.166 managementPortal.login.lockTime .....	275
21.1.167 managementPortal.login.max.retry .....	276
21.1.168 managementPortal.session.timeout.interval .....	276
21.1.169 mdu.enabled .....	276
21.1.170 media.file.cipher.keys .....	276
21.1.171 media.file.encrypt .....	277
21.1.172 motion.events.blackout.period .....	277
21.1.173 mp.password.max.length .....	277
21.1.174 mp.password.min.length .....	277
21.1.175 mp.password.wellknown.words .....	277
21.1.176 multiple.deployment .....	278
21.1.177 oauth2.<suffix> .....	278
21.1.178 password.min.length .....	278
21.1.179 password.max.length .....	278
21.1.180 password.reset.emailAddress.from .....	278
21.1.181 pingCellularUnit.att.gateway.url .....	279
21.1.182 pingCellularUnit.att.gateway.username .....	279
21.1.183 pingCellularUnit.gateway.password .....	279
21.1.184 pingCellularUnit.att.licenseKey .....	279
21.1.185 pingCellularUnit.implementation .....	279
21.1.186 pingCellularUnit.numerex.accountId .....	279
21.1.187 pingCellularUnit.numerex.gateway.password .....	279
21.1.188 pingCellularUnit.numerex.gateway.url .....	279
21.1.189 pingCellularUnit.numerex.gateway.username .....	280
21.1.190 pingCellularUnit.numerex.new.cid .....	280
21.1.191 pingCellularUnit.numerex.prefixes .....	280
21.1.192 pingCellularUnit.numerex.smsspinglevel.timeout.interval .....	280
21.1.193 pingCellularUnit.numerex.waiting .....	280
21.1.194 portalViewer.timeout .....	280
21.1.195 postalcode.validation.country .....	280
21.1.196 postalcode.validation.country.CA.pattern .....	281
21.1.197 postalcode.validation.country.US.pattern .....	281
21.1.198 premise.countryList .....	281

---

---

21.1.199 relay.server.converge.enabled .....	281
21.1.200 relay.server.credential.encrypting.enabled .....	281
21.1.201 relay.server.enabled .....	282
21.1.202 relay.server.password .....	282
21.1.203 relay.server.sp.videotoken.appkey .....	282
21.1.204 relay.server.url .....	283
21.1.205 relay.server.username .....	283
21.1.206 rest.csrf.token.enabled.modules .....	283
21.1.207 restApi.login.lockTime .....	283
21.1.208 restApi.admin.login.enabled .....	284
21.1.209 restApi.login.max.retry .....	284
21.1.210 restBasedPortalURL .....	284
21.1.211 restOperation.installerAccess.duration.minutes .....	285
21.1.212 restsubscriber.session.timeout.interval .....	285
21.1.213 rule.action.arm .....	285
21.1.214 rule.action.disarm .....	285
21.1.215 rule.action.lighting.duration .....	285
21.1.216 rule.action.set.thermostat.to.cool .....	286
21.1.217 rule.action.set.thermostat.to.heat .....	286
21.1.218 rule.action.turn.thermostat.off .....	286
21.1.219 rule.doNotConvertArmDisarmDefaultServerRule .....	286
21.1.220 rule.showxml .....	286
21.1.221 search.character.blacklist .....	287
21.1.222 serverStats.enabled .....	287
21.1.223 server.enableIntegrationLoggingThatWillWritePrivacyDataInLogs .....	287
21.1.224 server.health.check.expected.duration.in.seconds .....	287
21.1.225 serverStats.length .....	287
21.1.226 share.file.root .....	288
21.1.227 share.file.root.windows .....	288
21.1.228 sms.queue.concurrentConsumers .....	288
21.1.229 speedTestUrl .....	288
21.1.230 sso.enabled .....	289
21.1.231 subscriberPortalBackdoorUrl .....	289
21.1.232 subscriberPortal.insuranceCertificate.show .....	289
21.1.233 subscriberPortal.localeList .....	289
21.1.234 subscriberPortal.login.lockTime .....	289
21.1.235 subscriberPortal.login.max.retry .....	290
21.1.236 subscriberPortalRootUrl .....	290
21.1.237 subscriberPortal.session.timeout.interval .....	290
21.1.238 subscriberPortal.temporary.password.expirationTime .....	290
21.1.239 threadDump.enabled .....	291
21.1.240 threadDump.interval .....	291
21.1.241 threadDump.separate.file.enabled .....	291
21.1.242 timezone.default .....	291
21.1.243 validation.pattern.csnum .....	291
21.1.244 validation.pattern.name .....	291
21.1.245 validation.pattern.phone .....	292
21.1.246 validation.pattern.postalcode .....	292
21.1.247 validation.pattern.zone .....	292

---

---

21.1.248 video.convert.command .....	292
21.1.249 video.convert.command.windows .....	292
21.1.250 video.convert.command.concurrent.number .....	292
21.1.251 video.convert.h264 .....	292
21.1.252 video.convert.mjpeg .....	293
21.1.253 white.list.peripheralTrouble.to.centralStation .....	293
21.1.254 white.list.zoneTrouble.to.centralStation .....	294
21.1.255 widget.image.directory .....	294
21.1.256 widget.image.directory.windows .....	294
21.1.257 widget.p5.android.supported .....	295
21.1.258 widgetStoreUrl .....	295
21.1.259 widget.weatherUrl .....	295
21.1.260 xmpp.routeConfig.<suffix> .....	295
21.1.261 xmpp.threaddump.policy .....	296
21.2 custom.properties .....	297
21.2.1 General Properties .....	297
21.2.2 Background Tasks .....	298
21.2.3 Numerex Properties .....	300
21.2.4 COPS Integration .....	301
21.2.5 DICE Integration .....	302
21.2.6 SIMS Integration .....	302
21.2.7 SSO Integration .....	303
21.2.8 OAuth 2 Integration .....	305
21.3 mail.properties .....	305
21.3.1 General Mail Properties .....	305
21.3.2 Quota Properties .....	306
21.3.3 Email Properties .....	307
21.3.4 SMS Properties .....	308
21.3.4.1 Simplewire Properties .....	308
21.3.4.2 Numerex Properties .....	309
21.3.4.3 HTTP Post Requests .....	309
21.4 message.properties .....	310
21.4.1 Email Message Suffix .....	311
21.4.2 Account Notifications .....	312
21.4.2.1 Files from Cameras Over Allowed File Size Limits Notifications .....	312
21.4.2.1.1.Image Files Over Allowed Limits Notifications .....	312
21.4.2.1.2.Video Files Over Allowed Limits Notifications .....	312
21.4.2.3 Activation Confirmations .....	313
21.4.3.1 Single-Sign-On Enabled .....	313
21.4.3.1.1.Activation .....	313
21.4.3.1.2.Reset Account for Activation .....	313
21.4.3.2 Single-Sign-On NOT Enabled .....	314
21.4.3.2.1.Activation .....	314
21.4.3.2.2.Reset Account for Activation .....	314
21.4.4 Touchstone System Event Notifications .....	315
21.4.4.1 Mode Event Notifications .....	315
21.4.5 Security Event Notifications .....	316
21.4.5.1 Alarm Notifications .....	317
21.4.5.1.1.Alarm Initiated Notifications .....	318

---

21.4.5.1.1.1 Monitored Accounts .....	318
21.4.5.1.1.2 Not Monitored Accounts .....	319
21.4.5.1.1.3 Alarm Detail Notifications .....	320
21.4.5.1.2.Exit Error Notifications .....	322
21.4.5.1.2.1 Monitored Accounts .....	322
21.4.5.1.2.2 Not Monitored Accounts .....	323
21.4.5.1.3.Panic Alarm Notifications .....	324
21.4.5.1.3.1 Monitored Accounts .....	324
21.4.5.1.3.2 Not Monitored Accounts .....	324
21.4.5.1.4.Alarm Aborted Notifications .....	325
21.4.5.1.4.1 Monitored Accounts .....	325
21.4.5.1.4.2 Not Monitored Accounts .....	325
21.4.5.1.5.Alarm Canceled Notifications .....	326
21.4.5.1.5.1 Monitored Accounts .....	326
21.4.5.1.5.2 Not Monitored Accounts .....	326
21.4.5.1.6.Alarm Reset Notifications .....	327
21.4.5.1.6.1 Monitored Accounts .....	327
21.4.5.1.6.2 Not Monitored Accounts .....	327
21.4.5.1.7.Smash and Grab Alarm Notifications .....	328
21.4.5.1.7.1 Monitored Accounts .....	328
21.4.5.1.7.2 Not Monitored Accounts .....	328
21.4.5.1.8.Alarm Sent to Central Monitoring Station Notification .....	329
21.4.5.2 Arm/Disarm System Notifications .....	330
21.4.5.3 Keypad Code Change Notifications .....	331
21.4.5.4 Password Reset Notifications .....	331
21.4.5.5 Username Retrieve Notifications .....	331
21.4.6 Device Event Notifications .....	332
21.4.6.1 Camera Image/Video Capture Event Notifications .....	332
21.4.6.2 Door Lock Event Notifications .....	334
21.4.6.3 Lighting Device Event Notifications .....	335
21.4.6.4 Motion Sensor Event Notifications .....	336
21.4.6.5 Thermostat Event Notifications .....	337
21.4.6.6 Zone Event Notifications .....	338
21.4.7 Trouble Event Notifications .....	339
21.4.7.1 CPE Device (System) Trouble Events .....	339
21.4.7.2 Camera Trouble Event Notifications .....	341
21.4.7.3 Connectivity Trouble Event Notifications .....	342
21.4.7.4 Door Lock Device Trouble Event Notifications .....	343
21.4.7.5 Lighting Device Trouble Event Notifications .....	344
21.4.7.6 Peripheral Trouble Event Notifications .....	345
21.4.7.7 Thermostat Trouble Event Notifications .....	347
21.4.7.8 Zone Trouble Event Notifications .....	348
21.5 Tier Properties .....	349
21.6 Account Read Only Properties .....	349
21.7 Database System Properties .....	350
21.7.1 system_property .....	350
21.7.2 xmpp_property .....	351
<b>22 Proactively Monitoring the Oracle Database .....</b>	<b>352</b>
22.1 Oracle Enterprise Manager .....	352

---

22.1.1 Advantages .....	352
22.1.2 Disadvantages .....	352
22.1.3 Recommendation .....	352
22.2 OS Shell Script Running on OS Level .....	353
22.2.1 Advantages .....	353
22.2.2 Disadvantages .....	353
<b>23 Database Management Processes .....</b>	<b>354</b>
23.1 Data Maintenance .....	354
23.1.1 Troubleshooting: Purge Script Takes a Long Time to Finish .....	354
23.1.2 Setting up the Purge Scripts .....	354
23.1.2.1 Prepare to create the cron job: .....	354
23.1.2.2 Install the Cleanup SQL Package: .....	355
23.1.2.3 Set Up a Cron Job to Run the Oracle Cleanup Procedure .....	355
23.1.2.4 Set Up a Cron Job to Delete the Expired Image/Video Files: .....	355
23.2 Standard Replication Cron Jobs .....	356
23.2.1 Manage the Cron Job to Perform Standard Replication .....	356
23.2.1.1 Monitor the Status of the Cron Job to Data Replication .....	356
23.2.1.2 Set Up a Cron Job to Perform Standard Replication .....	356
23.2.1.2.1.Preparation .....	356
23.2.1.2.2.Operations .....	357
23.2.2 Other Standard Replication Process Actions .....	358
23.2.3 Create a Cron Job to Perform Nightly Database Cleanup .....	358
<b>24 Load Balancer Configuration .....</b>	<b>361</b>
24.1 Load Balancer Configuration .....	361
24.1.1 URLs and Port Configurations .....	361
24.1.2 Connection Rate Limit .....	363
24.1.3 Timeout and Persistence .....	366
24.1.3.1 TCP Session Timeout Needs to be Larger than the Largest Broadband Heartbeat Interval .....	366
24.1.3.2 TCP XMPP Persistence Enabled with Persistence Timer Larger than the Largest Broadband Heartbeat Interval .....	368
24.2 Updating the Load Balancer for Multiple-Cluster Configurations .....	369
24.2.1 Update the serverstatus Health Monitor .....	370
24.2.2 Update the Source IP Persistence Template .....	370
24.2.3 Create New Service Groups .....	371
24.2.3.1 CPEAppInterface .....	371
24.2.3.2 CPEBroadbandConnector .....	372
24.2.3.3 CPECellularConnector .....	372
24.2.3.4 MediaAppInterface .....	373
24.2.3.5 PortalAppInterface .....	374
24.2.4 Create an App Switching HTTP Template .....	375
24.2.4.1 URL Switching Section .....	375
24.2.4.2 App Switching Section .....	375
<b>25 Devices Details .....</b>	<b>377</b>
25.1 Default Device Settings .....	377
25.2 Motion-Capable Cameras .....	378
25.2.1 Device Descriptor List Controls .....	379
<b>26 Interface Branding .....</b>	<b>380</b>

---

26.1 Touchscreen .....	380
26.1.1 Boot-Up .....	380
26.1.1.1 Image Requirements .....	381
26.1.2 Main Screen .....	381
26.1.2.1 Background .....	381
26.1.2.2 Header Elements .....	381
26.1.2.3 Footer Elements .....	382
26.1.2.4 General Recommendations .....	382
26.1.3 Custom App Icons .....	382
26.2 Subscriber Portal .....	383
26.2.1 Header Logo .....	383
26.2.2 Content, Fonts, and Background .....	384
26.2.3 Menus .....	384
26.2.4 Buttons .....	385
26.2.5 Layout .....	385
<b>27 Glossary .....</b>	<b>386</b>

## Revision History

Release	Revisions
7.3 Quadra v7	<p>Added the version element to the list of CPE elements in "<a href="#">Cpe</a>" on page 140</p>
7.3 Quadra v6	<p>Added the following server properties for the OAuth 2.0 provider to "<a href="#">oauth2.&lt;suffix&gt;</a>" and "<a href="#">OAuth 2 Integration</a>":</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> oauth2.authorization.server.enabled</li> <li><input type="checkbox"/> oauth2.resource.server.key</li> <li><input type="checkbox"/> oauth2.resource.server.secret</li> <li><input type="checkbox"/> oauth2.authorization.server.url</li> <li><input type="checkbox"/> oauth2.token.cache.ttl.seconds</li> </ul> <p>Added the following custom properties for the OAuth 2.0 provider to <a href="#">OAuth 2 Integration</a>:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> oauth2.convergeIntegrationServiceUserName</li> <li><input type="checkbox"/> oauth2.convergeIntegrationServicePassword</li> </ul> <p>Removed Apache configurations and the following deprecated server properties for the legacy OAuth provider from <a href="#">OAuth 2 Integration</a>:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> oauth2.server.access.token.url</li> <li><input type="checkbox"/> oauth2.server.authorize.code.url</li> <li><input type="checkbox"/> oauth2.webapp-oauth.client.id</li> <li><input type="checkbox"/> oauth2.webapp-oauth.client.secret</li> <li><input type="checkbox"/> oauth2.webapp-oauth.implicit.clientAccessToken.groups</li> </ul> <p>Renamed <code>restsubscriber.session.timeout.internal</code> server property to <code>restsubscriber.session.timeout.interval</code></p>

Release	Revisions
7.3 Quadra v5	<p>Added new CID for Zigbee Jamming Detection feature. See <a href="#">CID 344</a> on page 80.</p> <p>Added the server property <code>subscriberPortalBackdoorUrl</code> to <a href="#">server.properties</a> on page 235.</p> <p>Added the following UCE codes. See "UCE Codes" on page 193</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> UCE-13900</li> <li><input type="checkbox"/> UCE-13901</li> <li><input type="checkbox"/> UCE-13902</li> </ul> <p>Removed the section "Using the Mobile Portal In Range of the Security Router" from <a href="#">Access Camera</a> on page 62</p> <p>Removed Australia/Hobart from <a href="#">Time Zone</a> on page 161.</p>
7.3 Quadra v4	<p>Added the server property <code>contextPathForLoginPage</code> to <a href="#">server.properties</a> on page 235.</p> <p>Added a note addressing the case where the touchscreen is tampered while the <code>device.tamper.enabled</code> property is modified. See <a href="#">device.tamper.enabled</a> on page 265.</p> <p>Added a note clarifying the <code>converge.sendActivationEmail</code> and <code>insight.sendActivationEmail</code> properties are ignored if SSO is enabled. See <a href="#">converge.sendActivationEmail</a> on page 260 and <a href="#">insight.sendActivationEmail</a> on page 272.</p> <p>Added the applicable platforms to the values in the table for <a href="#">AccountStatus</a> on page 136.</p> <p>Added <a href="#">Test Messages Service</a> on page 167</p>

Release	Revisions
7.3 Quadra v3	<p>Added new server properties for the XMPP routing management feature. See "<a href="#">xmpp.routeConfig.&lt;suffix&gt;</a>"</p> <p>Added new server properties for the diagnostics offloading feature. See "<a href="#">cpe.diagnostics.&lt;suffix&gt;</a>"</p> <p>Added the following server properties. See "<a href="#">server.properties</a>" on page 235</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> pingCellularUnit.att.gateway.url</li> <li><input type="checkbox"/> pingCellularUnit.att.gateway.username</li> <li><input type="checkbox"/> pingCellularUnit.att.gateway.password</li> <li><input type="checkbox"/> pingCellularUnit.att.licenseKey</li> <li><input type="checkbox"/> pingCellularUnit.numerex.prefixes</li> </ul> <p>Updated <a href="#">Smash &amp; Grab Confirmation Custom Settings</a> with new server properties used to activate dual AT&amp;T/Numerex cellular ping.</p>
7.3 Quadra v2	<p>Updated zone function behaviors and timing diagrams in <a href="#">Zone Function Behaviors on page 86</a></p> <p>Updated <a href="#">Silent 24-Hour Zone Function on page 93</a> Tamper Trouble behavior</p> <p>Clarified when changes to motion sensitivity take effect on <a href="#">Motion-Capable Cameras on page 378</a></p> <p>Updated <a href="#">UCE-11002 alarm.expiredMessage</a> on page 197</p>

Release	Revisions
7.3 Quadra v1	<p>Added/updated the following server properties. See "server.properties" on page 235</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> bundle.import.file.format</li> <li><input type="checkbox"/> bundle.import.log.directory</li> <li><input type="checkbox"/> bundle.import.log.directory.windows</li> <li><input type="checkbox"/> cloudIntegration.accountGroupAutoAdd</li> <li><input type="checkbox"/> cloudIntegration.accuWeather.temperatureChangeNotificationBlackoutPeriod</li> <li><input type="checkbox"/> cloudIntegration.auto.commit.enable</li> <li><input type="checkbox"/> cloudIntegration.auto.offset.reset</li> <li><input type="checkbox"/> cloudIntegration.consumer.group.name.prefix</li> <li><input type="checkbox"/> cloudIntegration.consumer.thread.count</li> <li><input type="checkbox"/> cloudIntegration.consumer.timeout.ms</li> <li><input type="checkbox"/> cloudIntegration.history.consumer.thread.count</li> <li><input type="checkbox"/> cloudIntegration.history.enabled</li> <li><input type="checkbox"/> cloudIntegration.history.service.appKey</li> <li><input type="checkbox"/> cloudIntegration.history.service.password</li> <li><input type="checkbox"/> cloudIntegration.history.service.username</li> <li><input type="checkbox"/> cloudIntegration.internal.topic</li> <li><input type="checkbox"/> cloudIntegration.metadata.broker.list</li> <li><input type="checkbox"/> cloudIntegration.oauth2.redirecturl</li> <li><input type="checkbox"/> cloudIntegration.partnerProxy.connectionPool.connectTimeout</li> <li><input type="checkbox"/> cloudIntegration.partnerProxy.connectionPool.defaultMaxPerRoute</li> <li><input type="checkbox"/> cloudIntegration.partnerProxy.connectionPool.maxTotal</li> <li><input type="checkbox"/> cloudIntegration.partnerProxy.connectionPool.requestTimeout</li> <li><input type="checkbox"/> cloudIntegration.server.name.system.property</li> <li><input type="checkbox"/> cloudIntegration.topic</li> <li><input type="checkbox"/> cloudIntegration.zookeeper.connect</li> </ul>

Release	Revisions
	<ul style="list-style-type: none"> <li><input type="checkbox"/> cloudIntegrationHistory.auto.commit.interval.ms</li> <li><input type="checkbox"/> cloudIntegrationHistory.auto.offset.reset</li> <li><input type="checkbox"/> cloudIntegrationHistory.zookeeper.connect</li> <li><input type="checkbox"/> cloudIntegrationHistory.zookeeper.session.timeout.ms</li> <li><input type="checkbox"/> cloudIntegrationHistory.zookeeper.sync.time.ms</li> <li><input type="checkbox"/> contextPathForResetPassword</li> <li><input type="checkbox"/> http.client.connection.default.connection.timeout&lt;.module&gt;</li> <li><input type="checkbox"/> http.client.connection.default.connection.timeout.clsIntegration</li> <li><input type="checkbox"/> http.client.connection.default.so.timeout&lt;.module&gt;</li> <li><input type="checkbox"/> http.client.connection.pool.timeout&lt;.module&gt;</li> <li><input type="checkbox"/> http.client.connectionPool.defaultMaxPerRoute</li> <li><input type="checkbox"/> http.client.connectionPool.maxTotal</li> <li><input type="checkbox"/> relay.server.sp.videotoken.appkey</li> <li><input type="checkbox"/> rest.csrf.token.enabled.modules</li> <li><input type="checkbox"/> restBasedPortalURL</li> <li><input type="checkbox"/> validation.pattern.name</li> </ul> <p>Added/updated the following UCE codes. See "UCE Codes" on page 193</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> UCE-01003</li> <li><input type="checkbox"/> UCE-03004</li> <li><input type="checkbox"/> UCE-03005</li> <li><input type="checkbox"/> UCE-03600</li> <li><input type="checkbox"/> UCE-03601</li> <li><input type="checkbox"/> UCE-13005</li> <li><input type="checkbox"/> UCE-13006</li> <li><input type="checkbox"/> UCE-13007</li> <li><input type="checkbox"/> UCE-13008</li> </ul>

Release	Revisions
	<ul style="list-style-type: none"><li><input type="checkbox"/> UCE-13600</li><li><input type="checkbox"/> UCE-13601</li><li><input type="checkbox"/> UCE-13602</li><li><input type="checkbox"/> UCE-13603</li><li><input type="checkbox"/> UCE-13604</li><li><input type="checkbox"/> UCE-13605</li><li><input type="checkbox"/> UCE-13606</li><li><input type="checkbox"/> UCE-13607</li><li><input type="checkbox"/> UCE-13608</li><li><input type="checkbox"/> UCE-13609</li><li><input type="checkbox"/> UCE-13610</li><li><input type="checkbox"/> UCE-13611</li><li><input type="checkbox"/> UCE-13612</li><li><input type="checkbox"/> UCE-13613</li><li><input type="checkbox"/> UCE-13614</li><li><input type="checkbox"/> UCE-13615</li><li><input type="checkbox"/> UCE-13616</li><li><input type="checkbox"/> UCE-13617</li><li><input type="checkbox"/> UCE-13618</li><li><input type="checkbox"/> UCE-13619</li><li><input type="checkbox"/> UCE-13620</li><li><input type="checkbox"/> UCE-13621</li><li><input type="checkbox"/> UCE-13622</li><li><input type="checkbox"/> UCE-13623</li><li><input type="checkbox"/> UCE-13624</li><li><input type="checkbox"/> UCE-16202</li></ul>

Release	Revisions
	<ul style="list-style-type: none"><li><input type="checkbox"/> UCE-16203</li><li><input type="checkbox"/> UCE-16204</li><li><input type="checkbox"/> UCE-16205</li><li><input type="checkbox"/> UCE-16206</li><li><input type="checkbox"/> UCE-16207</li><li><input type="checkbox"/> UCE-16208</li><li><input type="checkbox"/> UCE-16209</li><li><input type="checkbox"/> UCE-16210</li><li><input type="checkbox"/> UCE-16211</li><li><input type="checkbox"/> UCE-16212</li><li><input type="checkbox"/> UCE-16303</li><li><input type="checkbox"/> UCE-16304</li></ul> <p>Replaced "Employee Roles" and "Role Privileges" sections in "<a href="#">Management Portal Roles and Privileges</a> on page 183 with reference to the "Management Portal Roles" section in <i>Management Portal Guide</i></p>

Release	Revisions
7.2 Padre	<p>Added the following caution to "Create a Subscriber Account" on page 126:</p> <p style="color: red;"><b>IMPORTANT: If Cluster Location Service (CLS) is not available, the create account operation will fail.</b></p> <p>Added the following caution to "Update Account Information" on page 127:</p> <p style="color: red;"><b>IMPORTANT: If Cluster Location Service (CLS) is not available, the update account operation will fail.</b></p> <p>Added Australian time zones to <a href="#">Time Zone on page 161</a>.</p> <p>Updated the description for ICHealthCheck queries getUDPIIncomingMessageQueueSize and getUDPOutgoingMessageQueueSize. They are available on the CPE and portal servers only. See page <a href="#">174</a>.</p> <p>Added a new section, <a href="#">Management Portal Roles and Privileges on page 183</a>.</p> <p>Changed the error messages for UCE-14603 and UCE-14604 as follows (see "<a href="#">Exception Codes (UCE) on page 190</a>"). These changes were made to prevent the UDP sender and receiver service from stopping when an exception occurs.</p> <ul style="list-style-type: none"> <li>❑ UCE-14603: Changed from "Error receiving UDP data, receiver stopping service" to "Error receiving UDP data, resuming"</li> <li>❑ UCE-14604: Changed from "Error sending UDP data, sender stopping service" to "Error sending UDP data, resuming"</li> </ul> <p>Updated the Cluster Location Service (CLS) properties as follows (see "<a href="#">server.properties on page 235</a>):</p> <ul style="list-style-type: none"> <li>❑ Added the following caution to the <code>cls.domain</code> property:           <p style="color: red;"><b>IMPORTANT: Do not change the value of this property from its default value unless your Icontrol representative advises otherwise.</b></p> </li> <li>❑ Changed the value type of the <code>cls.cluster.number</code> property from integer to string</li> </ul>

Release	Revisions
7.1 Oahu	<p>Removed references to single-cluster server configuration as it is no longer supported as of the Oahu release.</p> <p>Added a note to the "getConnectedDeviceCount" section in "<a href="#">ICHealthCheck Service</a>" on <a href="#">page 167</a></p> <p>Changed 'status' field in "<a href="#">Account</a>" on <a href="#">page 135</a> and 'postalCode' field in "<a href="#">Address</a>" on <a href="#">page 137</a> as follows:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Required: No</li> <li><input type="checkbox"/> Allowed Occurrences: 0..1</li> </ul> <p>Deleted the following caution from "<a href="#">PortalAppInterface</a>" on <a href="#">page 374</a>:</p> <p style="color: red;"><b>IMPORTANT: Allow outbound traffic from the Portal Cluster on port 9091 for UDP traffic.</b></p> <p>Changed 'group' field in "<a href="#">Account</a>" on <a href="#">page 135</a> and "<a href="#">FullAccount</a>" on <a href="#">page 146</a> as follows:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Required: Yes</li> </ul> <p>Replaced CID 337 with CID 316. See "<a href="#">CID 316</a>" on <a href="#">page 79</a></p> <p>Added CID 751 for panel interface module (PIM) communication failure. See "<a href="#">CID 751</a>" on <a href="#">page 86</a></p> <p>Renamed ICHealthCheck query <code>findTopNETHerLossAccount</code> to <code>getTotalEthernetLossAccounts</code> and also updated the query description. See "<a href="#">ICHealthCheck Service</a>" on <a href="#">page 167</a></p> <p>Renamed ICHealthCheck query <code>findTopNTSRebootAccount</code> to <code>getTopNTSRebootAccount</code> and also updated the query description and parameters. See "<a href="#">ICHealthCheck Service</a>" on <a href="#">page 167</a></p> <p>Added the following server properties. See "<a href="#">server.properties</a>" on <a href="#">page 235</a></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> <code>converge.camera.trouble.enabled</code></li> <li><input type="checkbox"/> <code>ichealthcheck.test.emailAddress.from</code></li> <li><input type="checkbox"/> <code>managementPortal.localeList</code></li> <li><input type="checkbox"/> <code>mdu.enabled</code></li> </ul> <p>Added note that the following WSDL APIs do not support multiple concurrent operations (see "<a href="#">Understanding the Icontrol WSDL</a>" on <a href="#">page 125</a>):</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> <code>deactivateAccount</code></li> <li><input type="checkbox"/> <code>deleteUnactivatedAccount</code></li> </ul>

Release	Revisions
	<p>Added the following section: "Integration-Specific UCE Codes" on page 191</p> <p>Added the following UCE codes. See "UCE Codes" on page 193</p> <ul style="list-style-type: none"><li><input type="checkbox"/> UCE-13004</li><li><input type="checkbox"/> UCE-14013</li><li><input type="checkbox"/> UCE-14014</li><li><input type="checkbox"/> UCE-15131</li><li><input type="checkbox"/> UCE-15132</li><li><input type="checkbox"/> UCE-15133</li><li><input type="checkbox"/> UCE-16013</li><li><input type="checkbox"/> UCE-16014</li><li><input type="checkbox"/> UCE-16107</li><li><input type="checkbox"/> UCE-16108</li><li><input type="checkbox"/> UCE-16111</li><li><input type="checkbox"/> UCE-16200</li><li><input type="checkbox"/> UCE-16201</li><li><input type="checkbox"/> UCE-16202</li><li><input type="checkbox"/> UCE-16300</li><li><input type="checkbox"/> UCE-16301</li><li><input type="checkbox"/> UCE-16302</li><li><input type="checkbox"/> UCE-23500</li><li><input type="checkbox"/> UCE-23501</li><li><input type="checkbox"/> UCE-23502</li><li><input type="checkbox"/> UCE-23503</li><li><input type="checkbox"/> UCE-23504</li><li><input type="checkbox"/> UCE-23505</li><li><input type="checkbox"/> UCE-23506</li></ul>

Release	Revisions
7.0 Nantucket	<p>Added many new server properties. See the <i>Upgrade to Server Version 7.0 Nantucket (Single Cluster or Multiple Cluster)</i> for a complete list.</p> <p>Updated the Converge activation workflow diagram in "Process Flows" on page 38.</p> <p>Added the getUDPIIncomingMessageQueueSize and getUDPOutgoingMessageQueueSize ICHealthCheck queries. See "ICHealthCheck Service" on page 167.</p> <p>Added information about exit errors. See "If this zone is opened and left open at the end of the Exit Delay, the system reports an Exit Error. CID 374 and CID 134 are sent. See the timing diagram below:" on page 88.</p> <p>Added UCE-15130 on page 218</p>
6.3 Maui v2	<p>Updated the Message Sequence Diagrams:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> To remove the Telephony server from "Alarm Events Sequence (Broadband Connection)" on page 54.</li> <li><input type="checkbox"/> To add the Relay Server to the diagrams in "Camera Operations" on page 61. Also added the Logical Architecture Camera-Servers-Relay illustrations.</li> </ul>

Release	Revisions
6.3 Maui	<p>Added new section "Background Tasks" on page 298. [DE12409]</p> <p>Added new server properties:</p> <ul style="list-style-type: none"> <li>"asyncServlet.scavangeInterval" on page 242</li> <li>"cpe.panicScreenDisabled" on page 262</li> </ul> <p>Added a new server property related to Smash &amp; Grab for Numerex users:</p> <ul style="list-style-type: none"> <li>"pingCellularUnit.numerex.smsspingletimeout.interval" on page 116</li> </ul> <p>Also updated the process description for Numerex SMS ping to incorporate this server.property value. See "Confirming a Smash &amp; Grab Event (Cellular Ping)" on page 114.</p> <p>Updated "Devices Details" on page 377:</p> <ul style="list-style-type: none"> <li>❑ Added new section "Device Descriptor List Controls" on page 379</li> <li>❑ Added new section "Default Device Settings" on page 377</li> </ul> <p>Removed deprecated mail.properties values. See "mail.properties" on page 305.</p> <p>Added information about UDP messaging between the touchscreen and the Portal cluster in the following sections:</p> <ul style="list-style-type: none"> <li>❑ "UDP Activity" on page 51</li> <li>❑ "PortalAppInterface" on page 374</li> </ul>
6.2 Lanai	<p>v3 Corrected the description of the server property "cameraVideoRecordUrl" on page 245.</p> <p>For clarity, edited the summary text of the message property "Smash and Grab Alarm Notifications" on page 328.</p>
6.2 Lanai	<p>v2 Additional details added to "Boot-Up" on page 380 in the Interface Branding section.</p>

Release	Revisions
6.2 Lanai	<p>Added a GenericDevices complex data type to the WSDL. See "<a href="#">GenericDevice</a>" on page <a href="#">148</a>.</p> <p>New branding information about the start up screen. See "<a href="#">Touchscreen</a>" on page <a href="#">380</a>.</p> <p>The description of the deactivateAccount WSDL method has been updated to clarify that it only works against <i>activated</i> accounts. See "<a href="#">Deactivate an Account</a>" on page <a href="#">129</a>.</p> <p>Added a new subsection describing background tasks. See "<a href="#">Background Tasks</a>" on page <a href="#">298</a>.</p> <p>Added a section to better describe how images/video are delivered to the storage medium on the servers. This is intended to outline how containers are created on the server, file names the server creates and URLs that server sends to the camera to send image/video stream. This was added to address <i>DE11710: Documentation needed on the specifics on how video/images are delivered to the storage medium</i>. See "<a href="#">Image/Video Capture Details</a>" on page <a href="#">66</a>.</p> <p>Created a new chapter "<a href="#">CPE Processes</a>" on page <a href="#">47</a> to address <i>DE11933: No Documentation Exists for CPE Config Back up Behavior and how it affects RMA</i>.</p> <p>The server property validation.pattern.zone is modified to validation.pattern.zone. "<a href="#">validation.pattern.zone</a>" on page <a href="#">292</a>.</p>

## 1 Introduction

The purpose of this document is to: detail the information and operations used by customer Operations departments to maintain the Icontrol Operations Domain.

This document is applicable to systems that support the Converge platform or the Touchstone platform or both.

**Note:** Single-cluster server configuration is no longer supported as of the Oahu release.

## 2 System Security Against Web Application Attacks

This section lists the most common web application security attacks with an explanation on how the system addresses them.

### 2.1 Web Applications Attacks

This section lists the most common web application security attacks with an explanation on how the system addresses them.

### 2.2 Cross Site Scripting (XSS)

XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.

**Protection:** The system sanitizes all user-supplied data before the data is passed from the high level client application layer to lower layers (service layer, DAO, database). This is done using a design pattern that does not require special attention to each place user data is entered.

### 2.3 Injection Flaws

Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data fools the interpreter into executing unintended commands or changing data.

**Protection:** The system sanitizes all user-supplied data before the data is passed from the high level client application layer to lower layers (service layer, DAO, database). It also uses Hibernate for escaping. The system's custom SQL commands (used for performance) are handled as only as intended.

### 2.4 Malicious File Execution

Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework which accepts filenames or files from users.

**Protection:** The system does not use any user-supplied data in filenames or other server based resources (like images).

### 2.5 Insecure Direct Object Reference

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.

**Protection:** The system does not use IDs that directly map to internal server references.

## 2.6 Cross Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the web application that it attacks.

**Protection:**The system limits the lifetime of authentication cookies.

## 2.7 Information Leakage and Improper Error Handling

Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data, or conduct more serious attacks.

**Protection:**The system does not expose exceptions in the applications. Configuration files and their values are not accessible. This can be a problem with PHP, but the system uses a Java, J2EE-based application.

## 2.8 Broken Authentication and Session Management

Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.

**Protection:**The system stores all passwords with one-way encryption in the database.

## 2.9 Insecure Cryptographic Storage

Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.

**Protection:**The system uses cryptographic functions to protect data and credentials.

## 2.10 Insecure Communications

Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.

**Protection:**The system encrypts network traffic.

## 2.11 Failure to Restrict URL Access

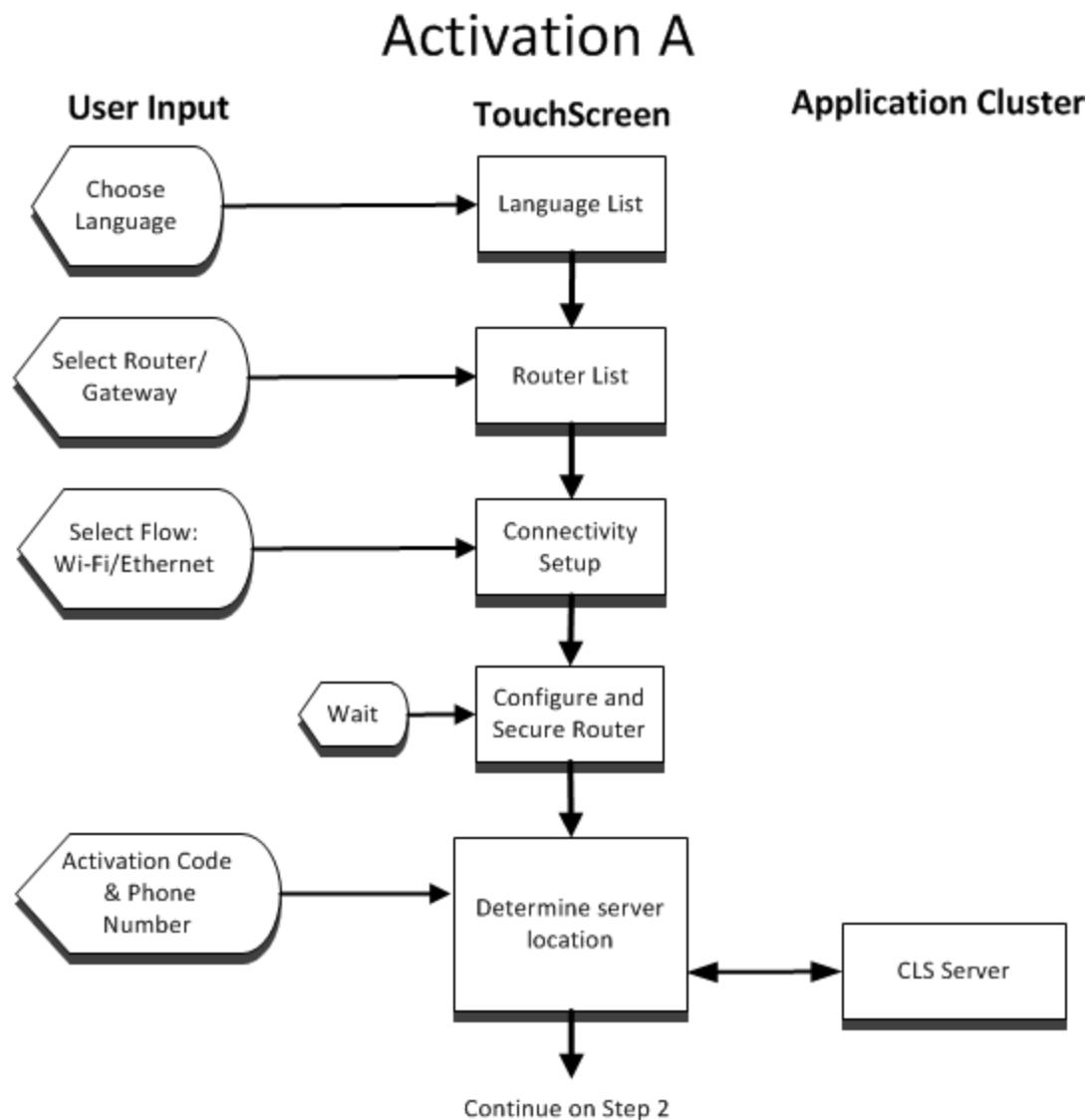
Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.

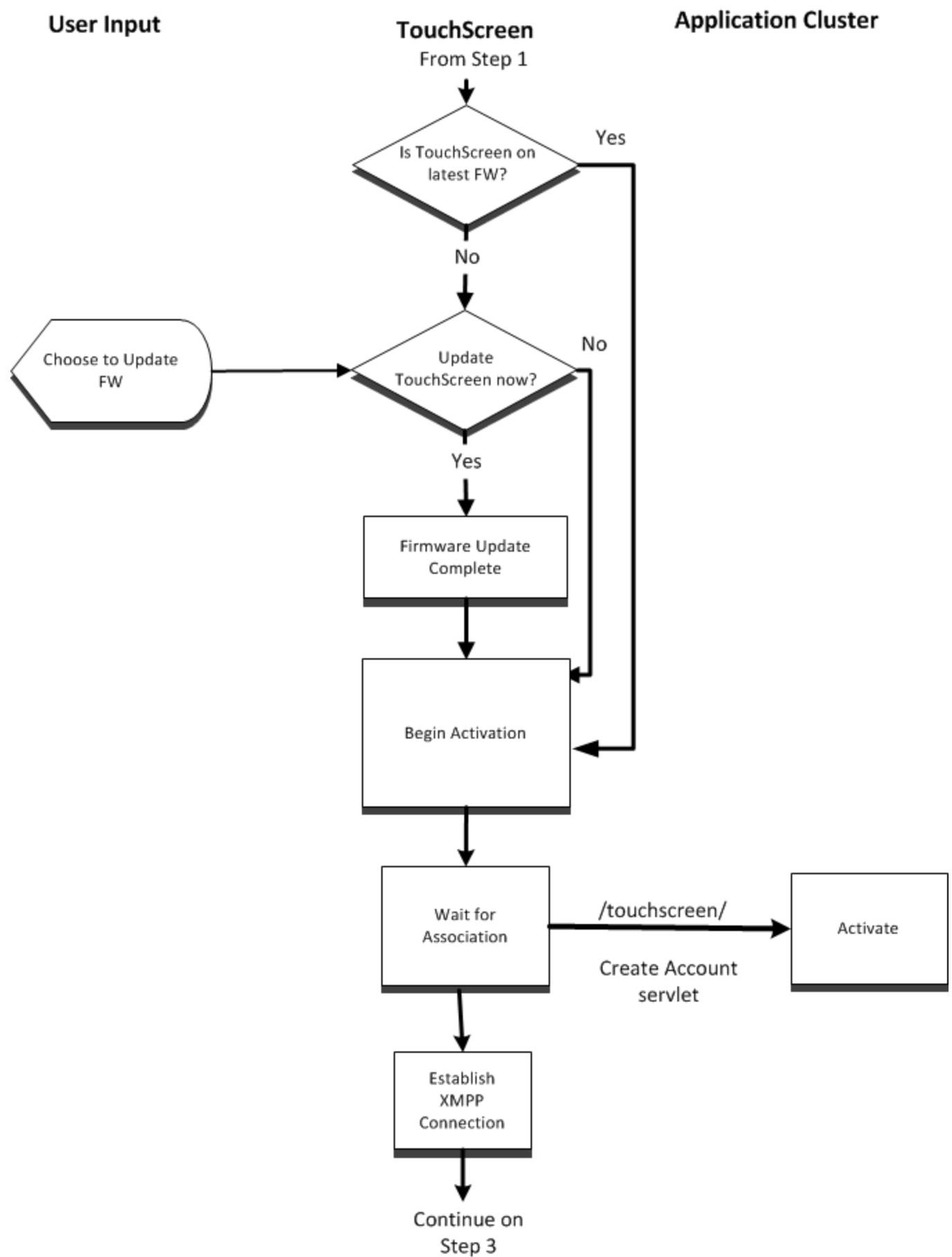
**Protection:**The system prevents direct access to URLs.

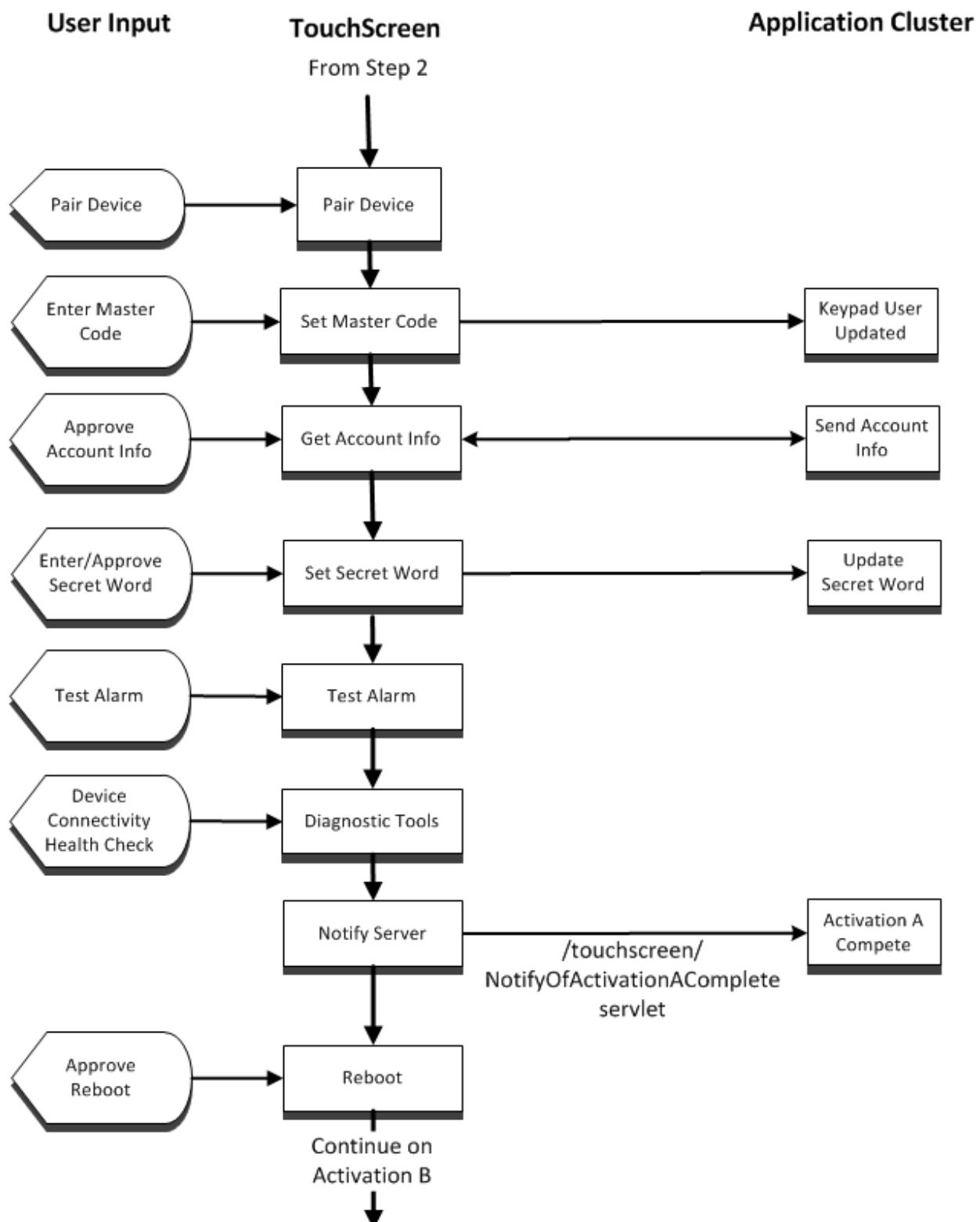
## 3 Process Flows

### 3.1 Converge Activation

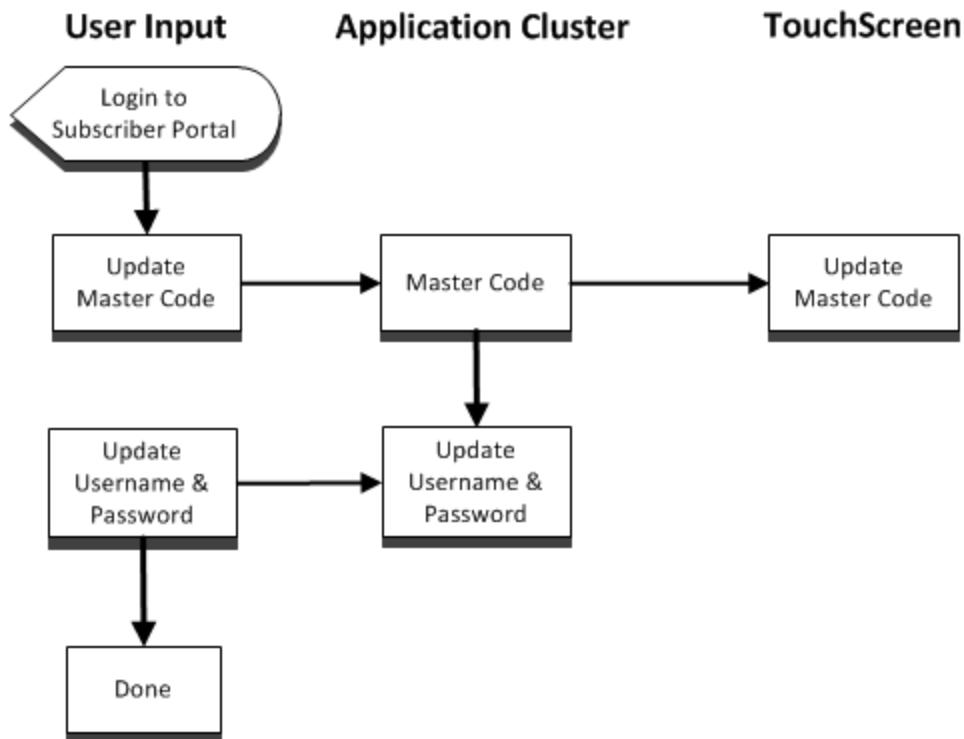
The following diagrams describe the Activation sequence for the CPE.



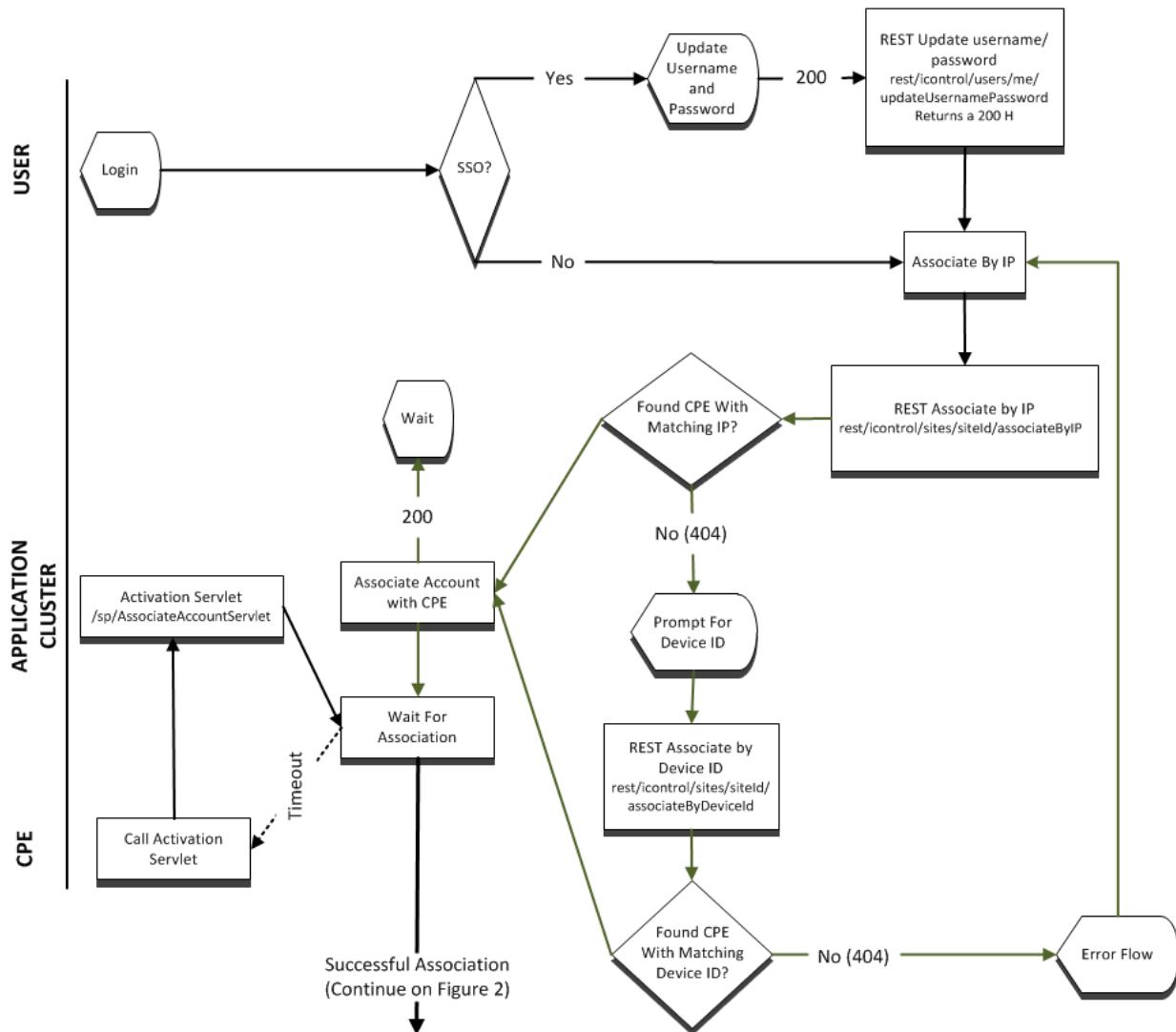


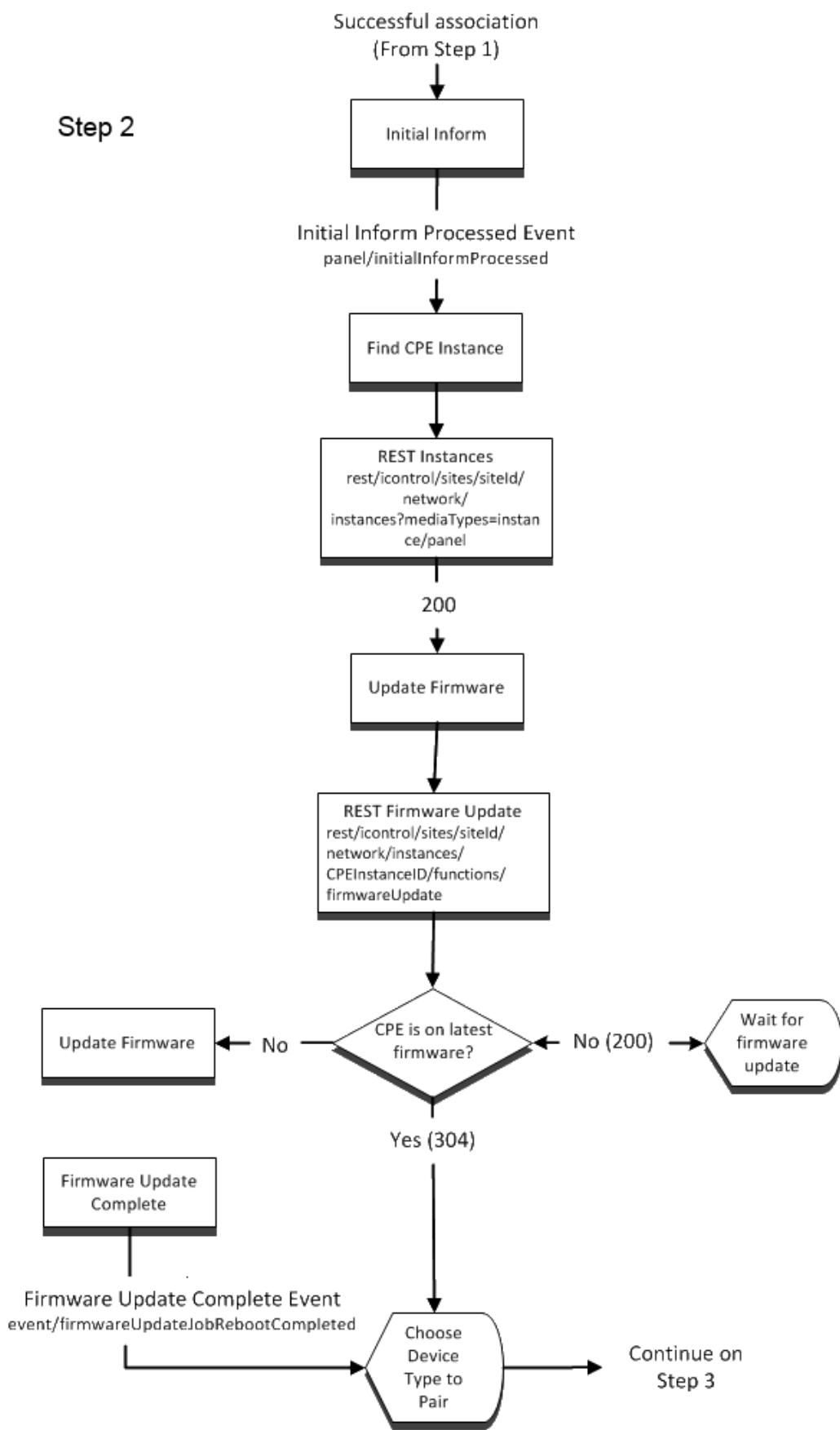


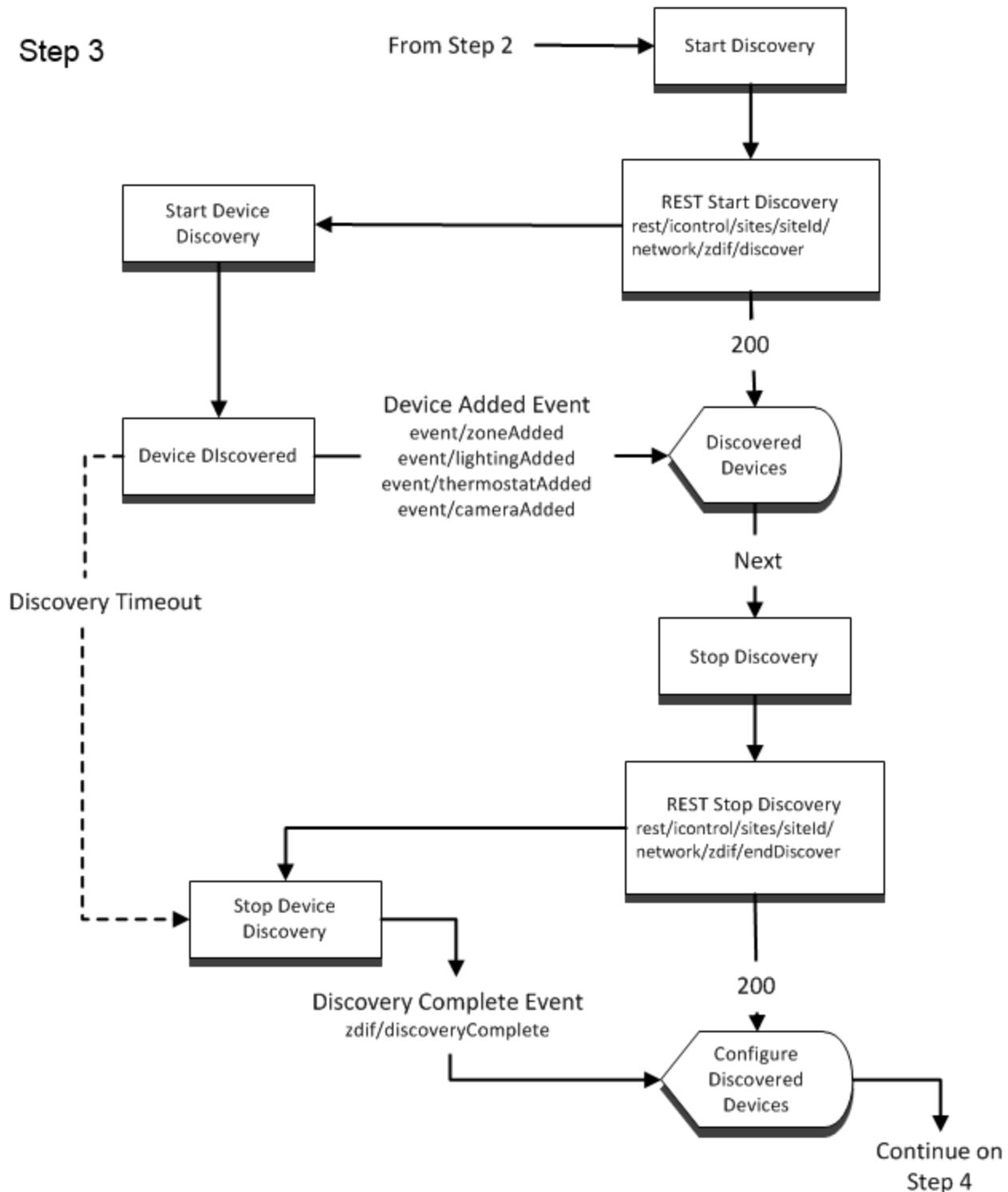
## Activation B

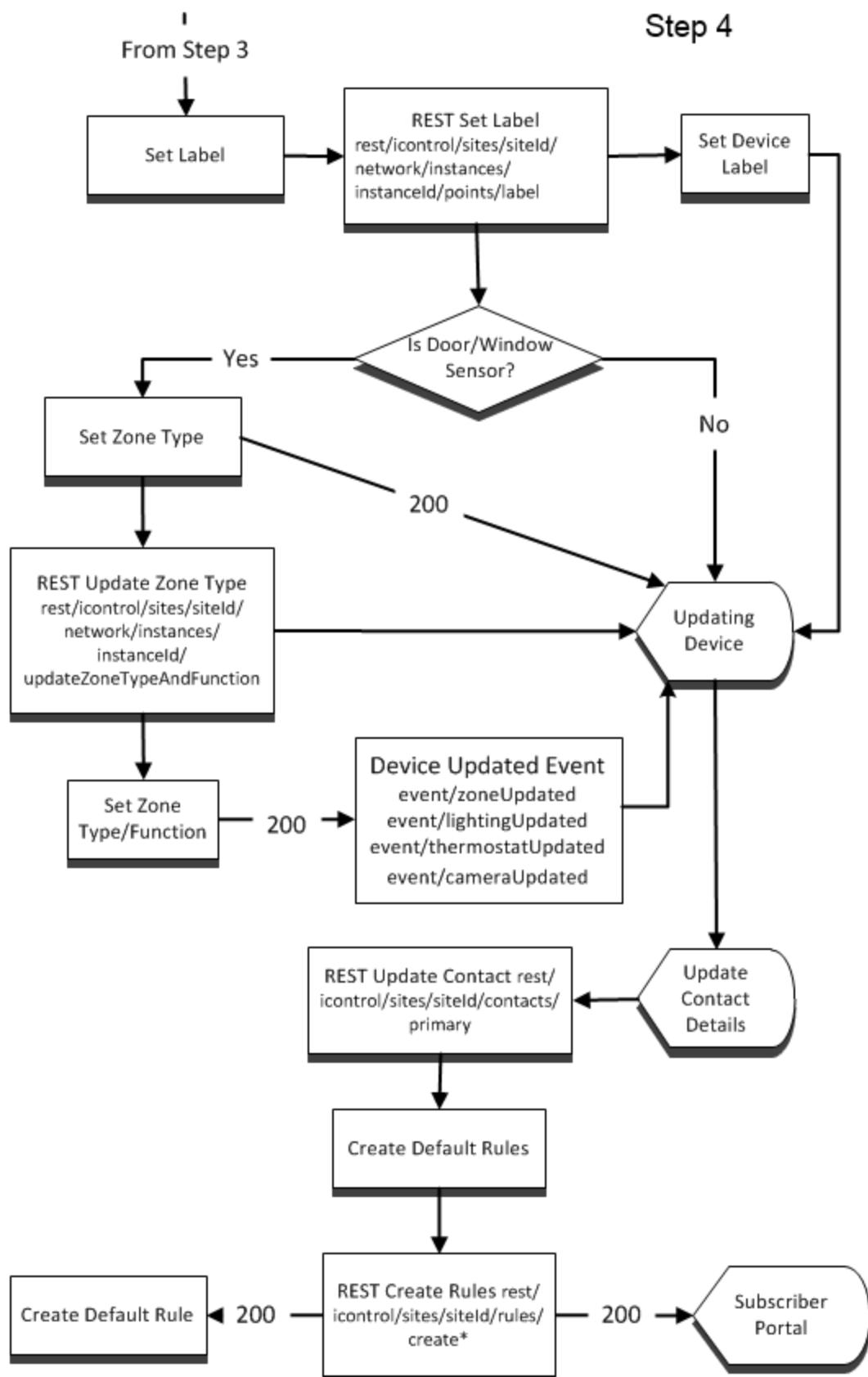


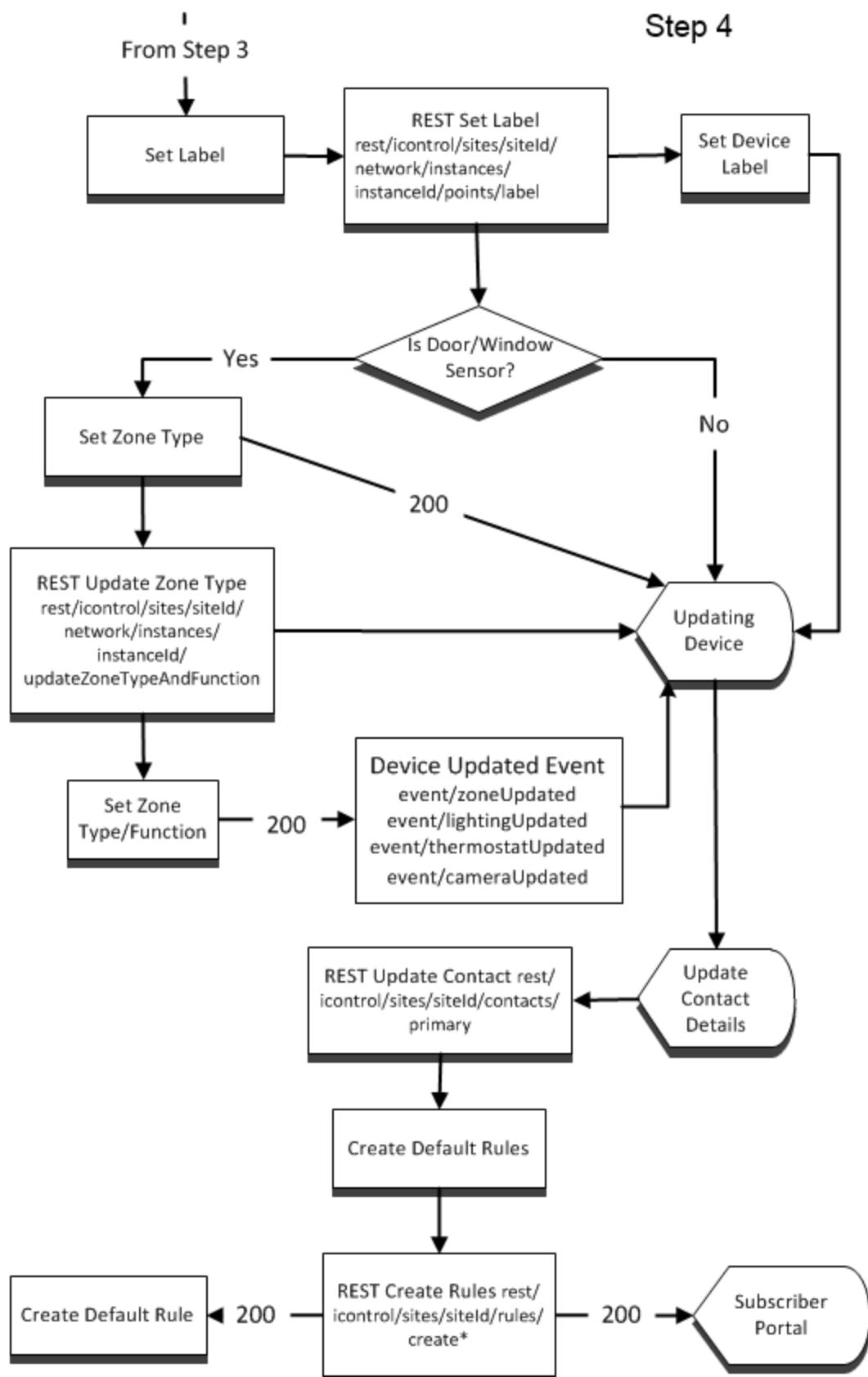
## 3.2 Touchstone Activation











## 4 CPE Processes

### 4.1 CPE Configuration File Back-up Behavior

The configuration files on the CPE define the various device and connectivity configurations in the subscriber systems. These files are stored as an encrypted TAR file on the Application servers and serves as the CPE's back-up. During the RMA process, the last-known configuration of the CPE is extracted from the configuration TAR file and applied to the new CPE.

The configuration file is uploaded to the server immediately after the CPE reboots at the end of activation. An update will not occur until the CPE configuration changes. For example, the configuration file is considered *updated*:

- At RMA
- After a device is added, modified, or deleted
- At CPE upgrade
- After a rule is added, modified, or deleted
- After a CPE reboot
- After the zone order is modified (Converge only)
- When app is added or a hometone is changed

When the configuration file is updated, the CPE starts a timer to upload an encrypted TAR of the configuration files to the server. This timer is a random number between 1-12, and it defines the number of hours before the configuration TAR is uploaded. After the configuration is uploaded to the server, the information is accessible to the CPE when necessary. A configuration back-up is uploaded to the server only after it has been updated. There is not a method to manually trigger a configuration upload.

#### To determine when the last configuration file was last uploaded from a CPE:

1. In the Management Port, access the Account Details Information screen of the subscriber account.
2. In the Status reports, see **CPE → CPE Last Config Backup Time**.

Alternately, review the `cpe_config` table in the database.

## 5 Message Sequence Diagrams

This section provides diagrams that illustrate how the CPEs communicates with the server, cameras, and other elements in the Icontrol system.

- ❑ "TCP Connection Startup Sequence" on page 49
- ❑ "UDP Activity" on page 51
- ❑ "ZigBee Device Events Sequence (Broadband Connection)" on page 53
- ❑ "Alarm Events Sequence (Broadband Connection)" on page 54(Converge only)
- ❑ "Remote Arm/Disarm " on page 55
- ❑ "Security Router Provisioning & Reset/RMA Sequences" on page 57
- ❑ "Touchscreen Firmware Update Sequence" on page 58
- ❑ "Camera Operations" on page 61

## 5.1 TCP Connection Startup Sequence

The CPE and the Application cluster maintain an always-on TCP connection over broadband and, for Converge when necessary, over cellular. If the TCP connection is lost, the CPE device and Operator Domain attempt to re-establish the connection as soon as possible. See the "Access Domain Communication Channels and Connectivity Protocols" section in *Converge System Architecture Guide* or *Touchstone System Architecture Guide* for more information on the broadband protocol stacks and Converge cellular protocol stacks.

If the Converge CPE has only cellular connectivity, it does not maintain a TCP connection. It only establishes a TCP connection if the Operator Domain needs to send a command to the CPE, such as remotely arming/disarming the system. See page 56 for details of the cellular Remote Arm/Disarm messaging sequence.

In the following diagram, messages are transmitted by XMPP.

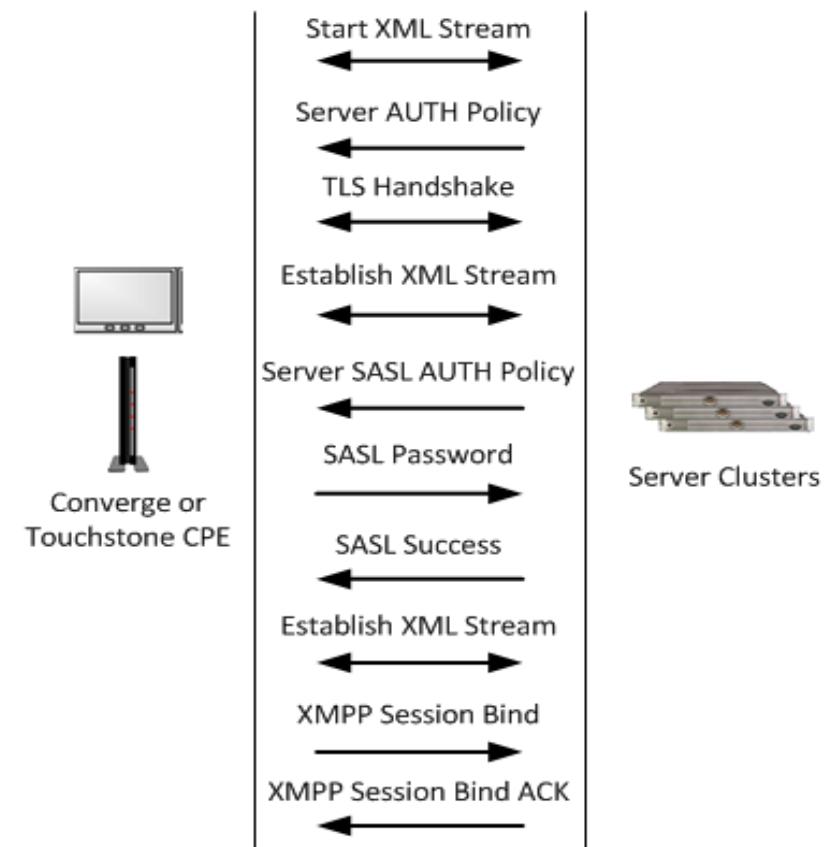


Figure 1: TCP Startup Sequence Diagram

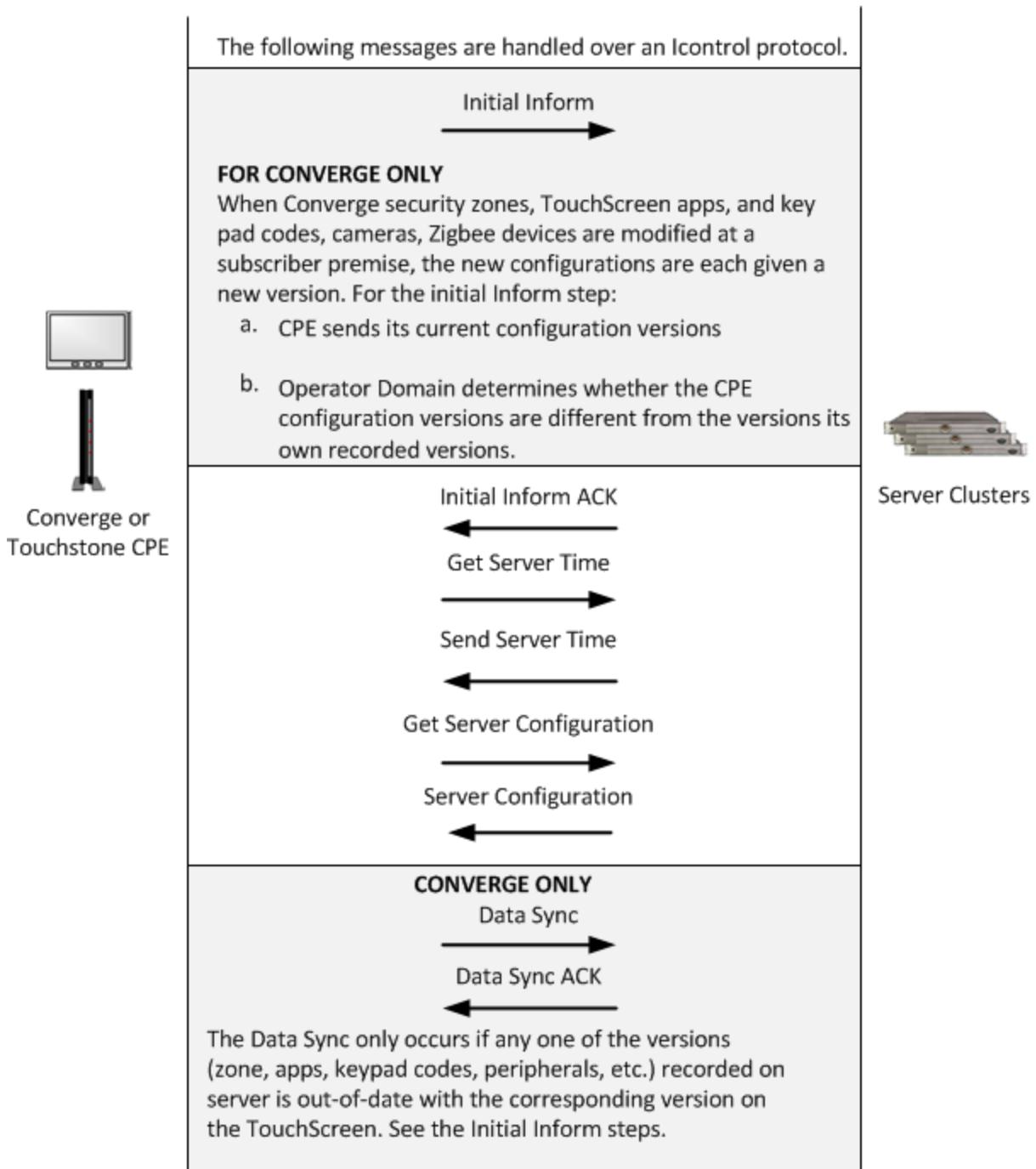


Figure 2: TCP Startup Sequence Diagram (Continued)

## 5.2 UDP Activity

### CONVERGE ONLY

When broadband is unavailable, the system continues to communicate with the touchscreen over cellular UDP. Zone Events continue to be sent from the touchscreen, but no Ack messages are sent. Touchscreen app transmission and firmware update activity is halted until a broadband TCP connection is re-established (see ["TCP Connection Startup Sequence" on page 49](#)).

The touchscreen sends every alarm to the Application cluster over broadband *and* cellular simultaneously.

The Heartbeat message is sent periodically (default 4 hours) to let the Operator Domain know that the touchscreen still has cellular connectivity. If a heartbeat is missed, the system assumes the touchscreen has lost cellular connectivity as well.

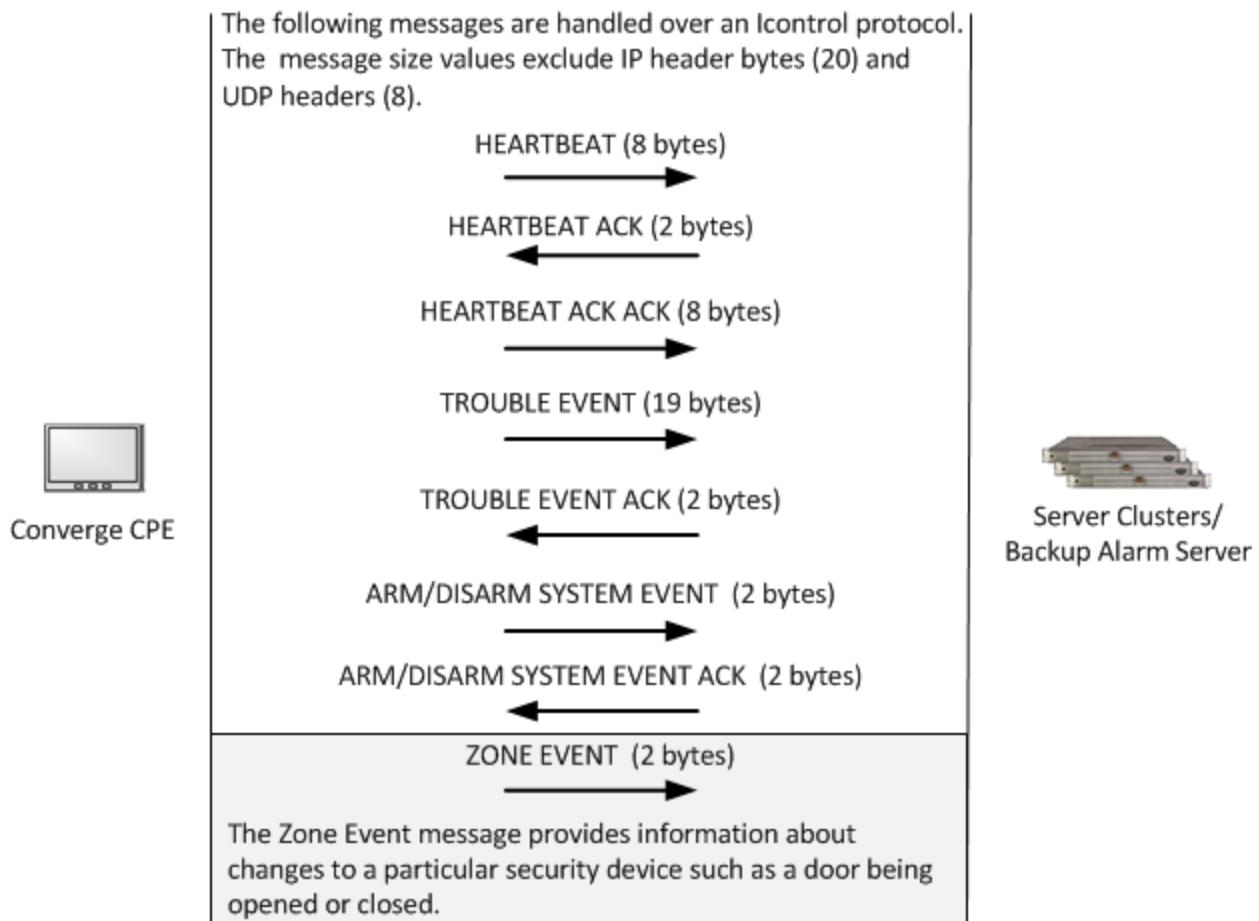
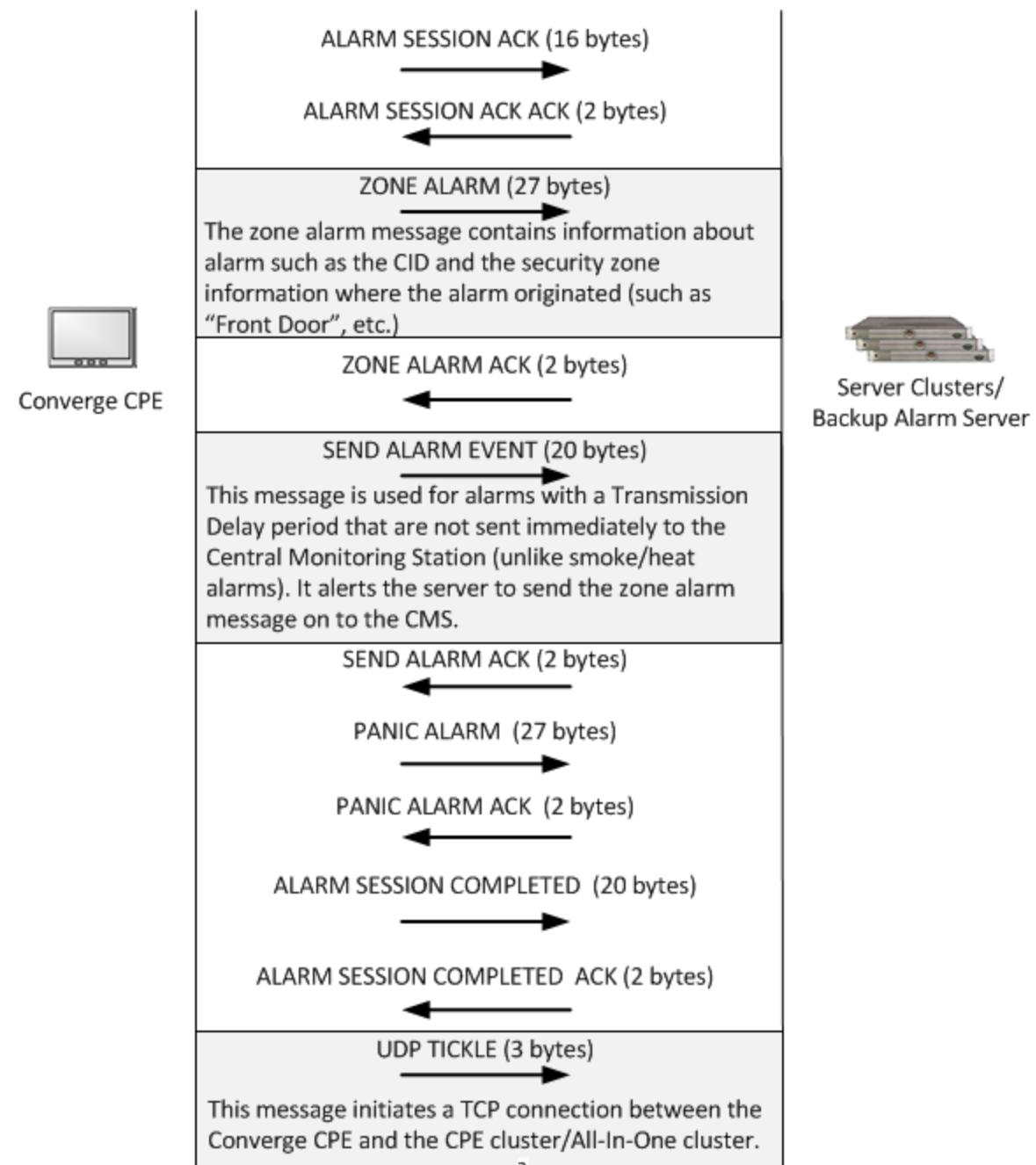


Figure 3: UDP Activity Over Cellular Network Sequence Diagram



UDP Activity Over Cellular Network Sequence Diagram (Continued)

### 5.3 ZigBee Device Events Sequence (Broadband Connection)

ZigBee device events comprise over 95% of Home-to-Operator Domain traffic. When the Operator Domain receives a device event from a CPE device , The following messages are also sent under specific circumstances:

- ❑ JSON message to the Subscriber Portal/Management Portal if someone is currently using those applications to view the account information for the CPE.
- ❑ Email/SMS message to the SMTP/SMSC server if the customer has configured to be sent an alert in the case of the current device event

In the following diagram, message size values exclude TLS overhead.

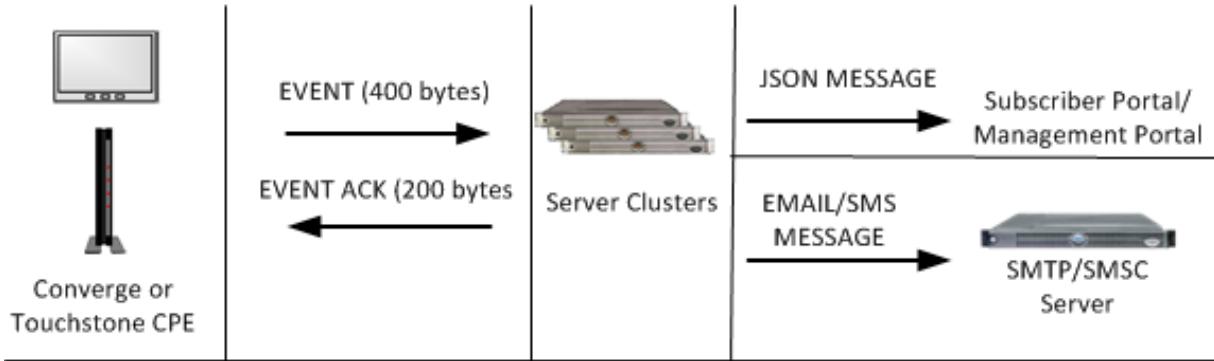


Figure 4: ZigBee Device Events Sequence Diagram

## 5.4 Alarm Events Sequence (Broadband Connection)

### CONVERGE ONLY

A Zone Alarm message contains information about alarm such as the CID and the security zone information where the alarm originated (such as “Front Door”, etc.). The touchscreen sends every alarm to the Application cluster over broadband *and* cellular simultaneously.

The following diagram describes Zone alarms transmitted from touchscreen to Operator Domain over broadband TCP. If broadband is not available, alarms are transmitted over cellular UDP (see [“UDP Activity” on page 51](#)).

#### Notes:

- Zone Alarm and Zone Alarm Ack size values do not include TLS overhead.
- JSON messages to the Subscriber Portal/ Management Portal are only sent if someone is currently using those applications to view the account information for the touchscreen.

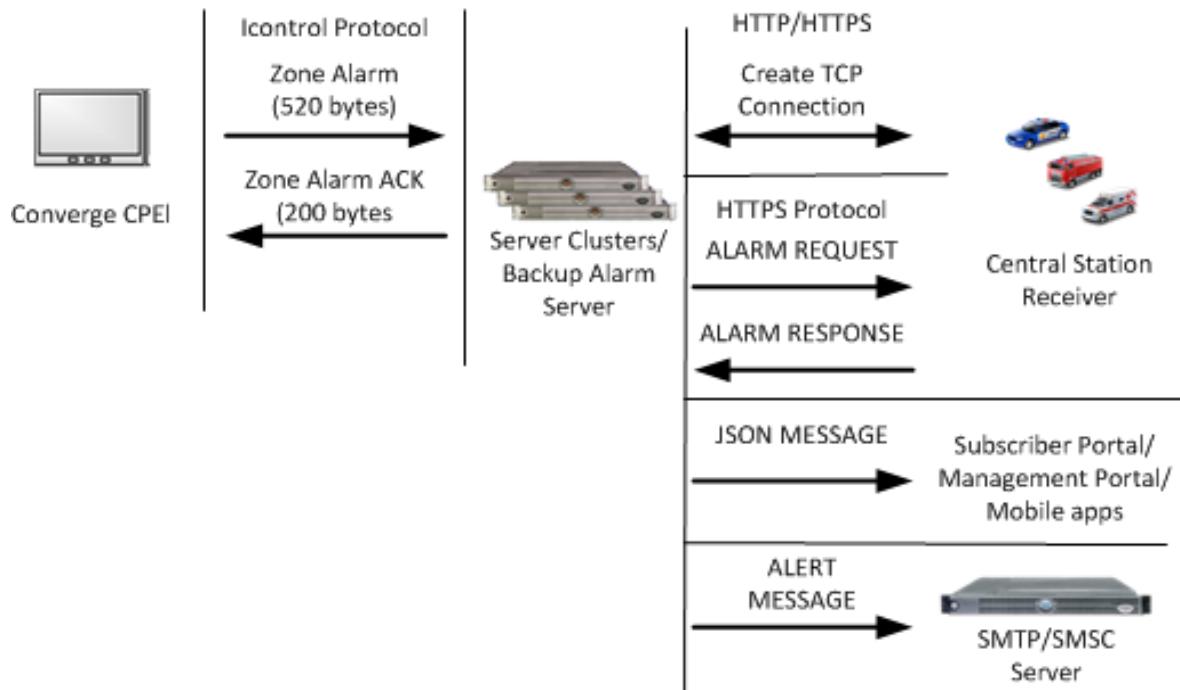


Figure 5: Alarm Events Sequence Diagram

## 5.5 Remote Arm/Disarm

**CONVERGE ONLY**

### 5.5.1 Broadband Connection

Customers can arm their systems remotely using the Subscriber Portal. Remote Arm/Disarm requests are not performed by the Back-up Alarm Server.

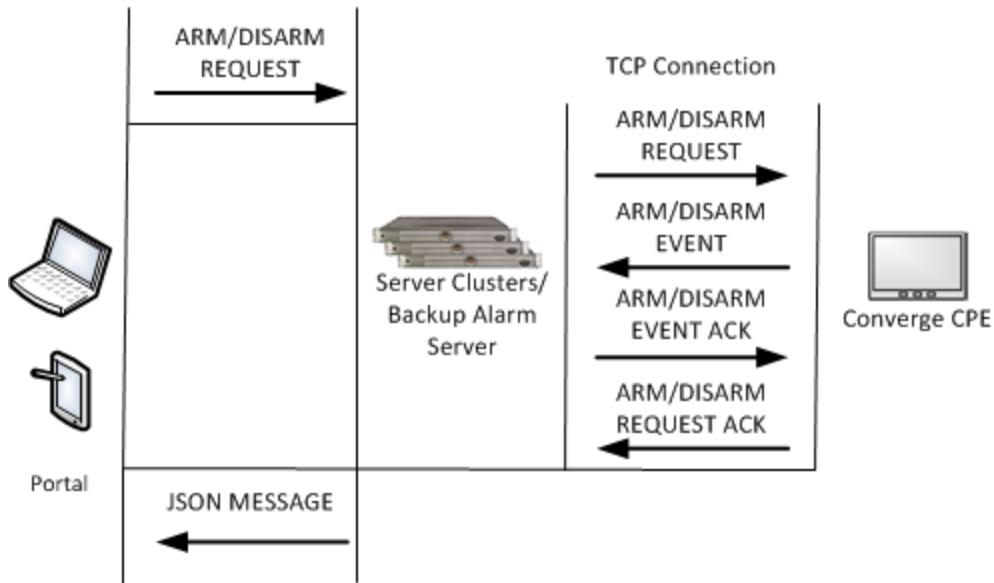
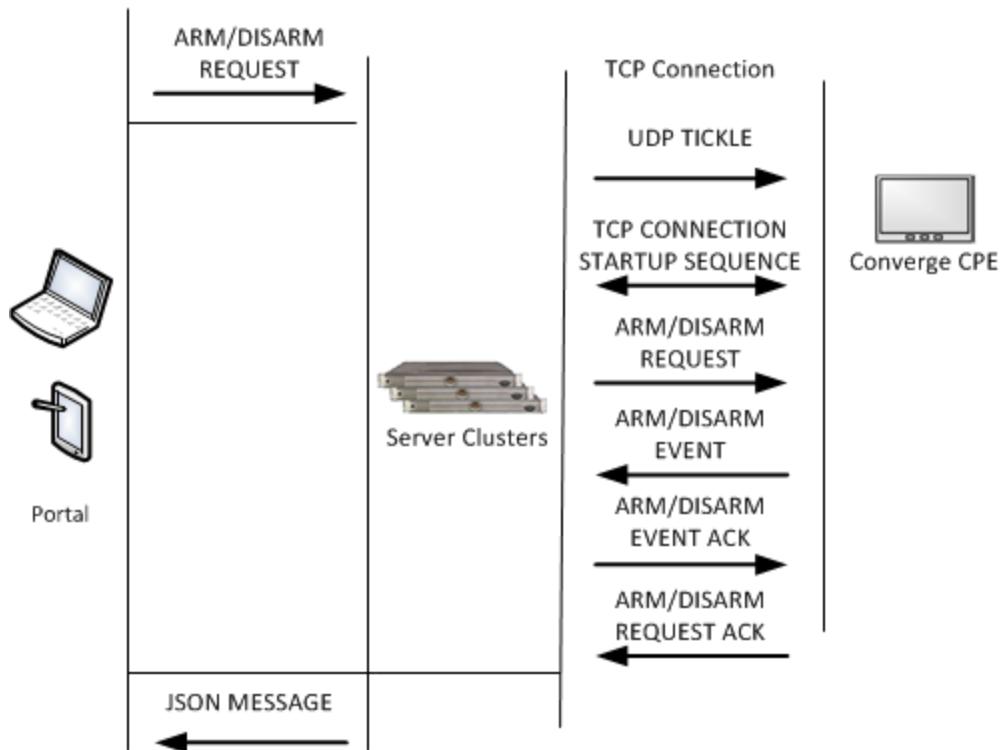


Figure 6: Remote Arm/Disarm (Broadband Connection) Sequence Diagram

### 5.5.2 Cellular-Only Connection

While there is no broadband connectivity to the touchscreen, it continues to communicate with the Application cluster over the cellular network using UDP. When the Application cluster receives a Remote Arm/Disarm request from the Subscriber Portal, it opens a TCP connection over cellular. See "[TCP Connection Startup Sequence](#)" on page 49 for details



**Figure 7: Remote Arm/Disarm (Cellular Connection) Sequence Diagram**

## 5.6 Security Router Provisioning & Reset/RMA Sequences

### CONVERGE ONLY

#### 5.6.1 Router Provisioning

The following defines the sequences involved in provisioning the dedicated router over WiFi during Activation.

**Note:** Reboots might occur after any step during this procedure depending on the device & firmware

1. Technician begins the Activation process and chooses the router brand and to connect to the router over Wi-Fi.
  - a. Touchscreen scans for best channel.
  - b. Touchscreen attaches to the router as open system.
  - c. Touchscreen locates an unpaired router base on out-of-box SSID pattern, filtering out everything else.
2. The Technician selects the proper router, and the touchscreen performs the sequences described in "Touchscreen Firmware Update Sequence" on page 58.

#### 5.6.2 Router Reset/RMA

The following details the sequences involved in resetting or performing a Return Merchandise Authorization (RMA) on the dedicated router during Activation.

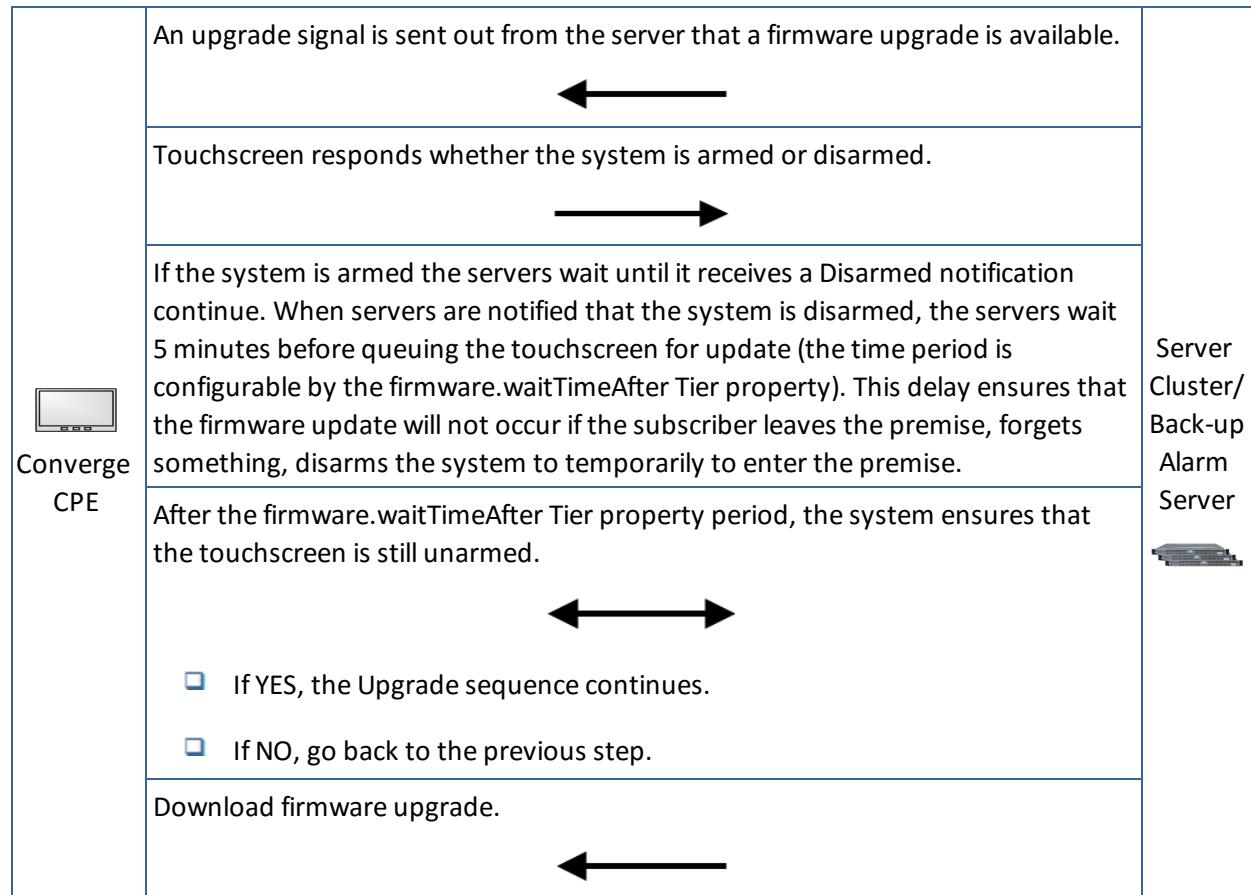
**Note:** Reboots might occur after any step during this procedure depending on the device & firmware

1. From the Technician Settings menu, select **Advanced Settings > Connectivity > Reset Router From Factory**.
  - a. Touchscreen scans for best channel.
  - b. Touchscreen attaches to the router as open system.
  - c. Touchscreen locates an unpaired router base on out-of-box SSID pattern, filtering out everything else.
  - d. If a previously configured router is located (ID'd by matching the MAC), proceed to step 2.If a previously configured router is not located, touchscreen It displays a choice list of found routers as an initial configuration. The Technician selects the proper router.
2. The touchscreen performs the sequences described in "Touchscreen Firmware Update Sequence" on page 58.

## 5.7 Touchscreen Firmware Update Sequence

### CONVERGE ONLY

The typical touchscreen firmware update bundle is about 60 MB in size. Transactions occur using the Icontrol protocols.



**Figure 8: Firmware Update Sequence Diagram**

When 10% of the upgrade file has been downloaded:

1. An alert is displayed on the touchscreen that a system upgrade in progress.
2. Most UI services are shut down to reclaim required memory (for example, the interactive UI, app engines, etc.)

Although the UI is disabled, the security system is still functioning: Zone events are processed, alarms are sent (fire, environmental, etc.).

The new firmware bundle is stored in RAM as it is downloaded, not in the file system. This preserves the integrity of the touchscreen's secondary partition in case the operation aborts. In that case, the touchscreen can merely reboot to restore the device as it was before the firmware download began.

3. Once the firmware is downloaded and the file integrity is checked, the bundle is written to the secondary partition.

**Note:** Normally, the secondary partition only contains apps.

4. After the new image is written, the active partition flag is switched and the touchscreen is rebooted.

There is a short window of time (about 15-20 seconds) when the ZigBee module is rebooting, this time might be a bit longer if a ZigBee code update is included in the firmware update. Even though the ZigBee network is unavailable during this time, the sensors will retry any messages until the ZigBee module and network come back on-line.

**Note:** Reboots might occur after any sequence during this procedure depending on the device & firmware.

5. After the touchscreen firmware is successfully updated, the security router firmware is updated if necessary.

### 5.7.1 Security Router Firmware Update

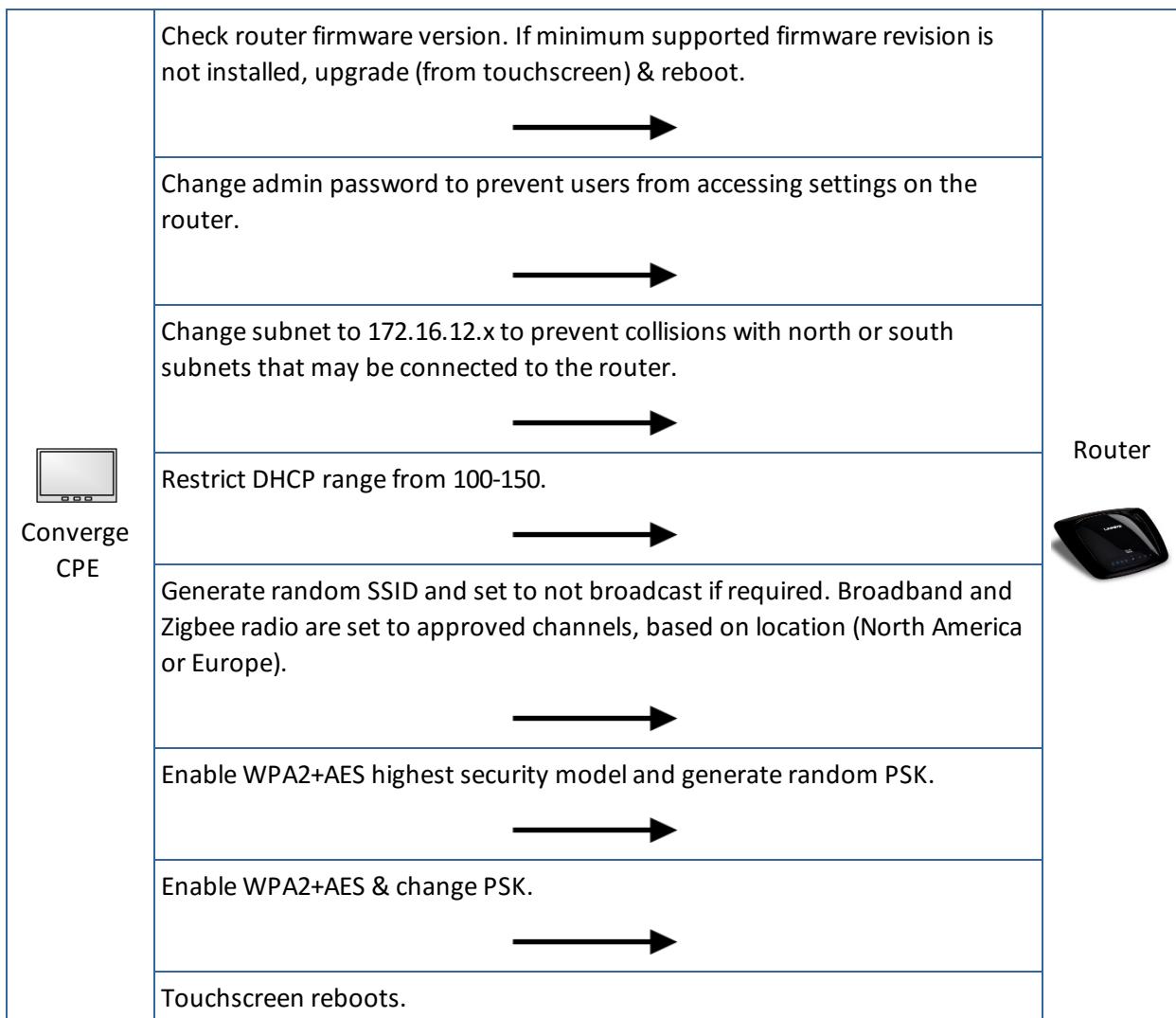


Figure 9: Dedicated Router Reset/RMA Recovery Diagram

## 5.8 Camera Operations

This section provides sequence diagrams for the following operations:

- Add Camera to Home Domain
- "Access Camera" on page 62

### 5.8.1 Add Camera to Home Domain

Adding a camera is performed from the touchscreen for the Converge platform and from the Subscriber Portal web browser for the Touchstone platform. To add a camera to the Home Domain, the camera must be connected to the Converge security router or the Touchstone Hub (LAN port) with an Ethernet cable. See the *Converge Installation Guide* for more information.

The CPE device uses Universal Plug and Play (UPnP) protocol to locate new cameras to add.

For Converge, the CPE's security router must support the following UPnP commands:

- |  |   |
|--|---|
| <input type="checkbox"/> GetPortMappingNumberOfEntries | <input type="checkbox"/> GetExternalIPAddress |
| <input type="checkbox"/> GetPortMappingNumberOfEntries | <input type="checkbox"/> AddPortMapping       |
| <input type="checkbox"/> GetPortMappingNumberOfEntries | <input type="checkbox"/> DeletePortMapping    |

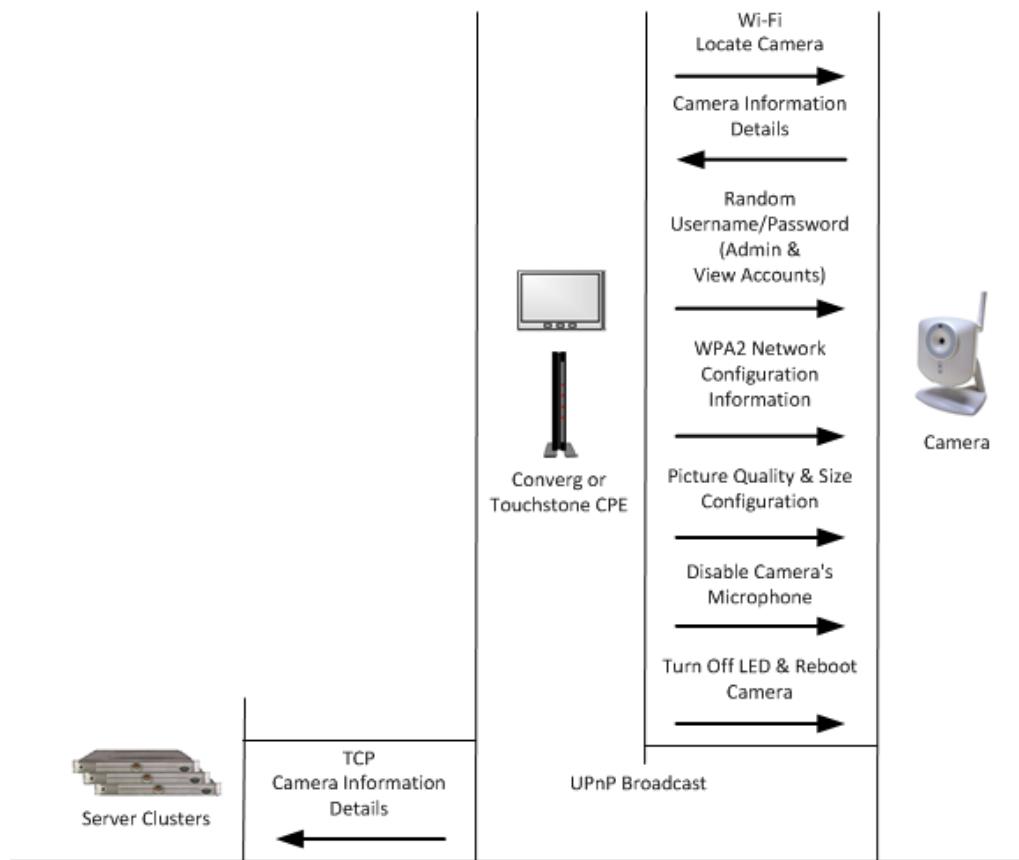


Figure 10: Add Camera to Home Domain Sequence Diagram

### 5.8.2 Access Camera

A camera in the Home Domain can be accessed remotely by the Subscriber Portal or the mobile app.

**Note:** The illustrations in this section do not apply to video and images viewed from the Converge CPE. That device accesses the cameras images directly (through the security router) over HTTP.

The following illustration describes the sequence to access an OpenHome standard camera from the Subscriber Portal or the Mobile Portal.

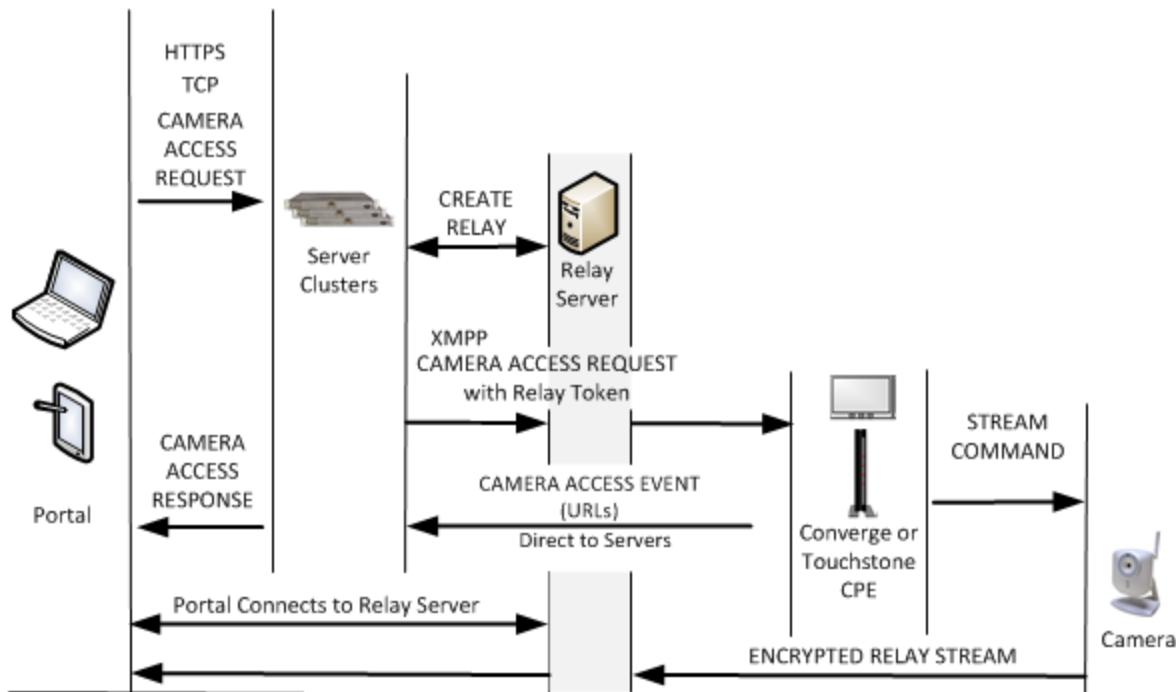


Figure 11: Streaming Video (OpenHome Cameras) Sequence Diagram

Legacy cameras on Converge Systems stream to the Relay Server through the CPE. Legacy cameras include the following:

- RC8021       RC8026
- iCamera       OC431
- OC810

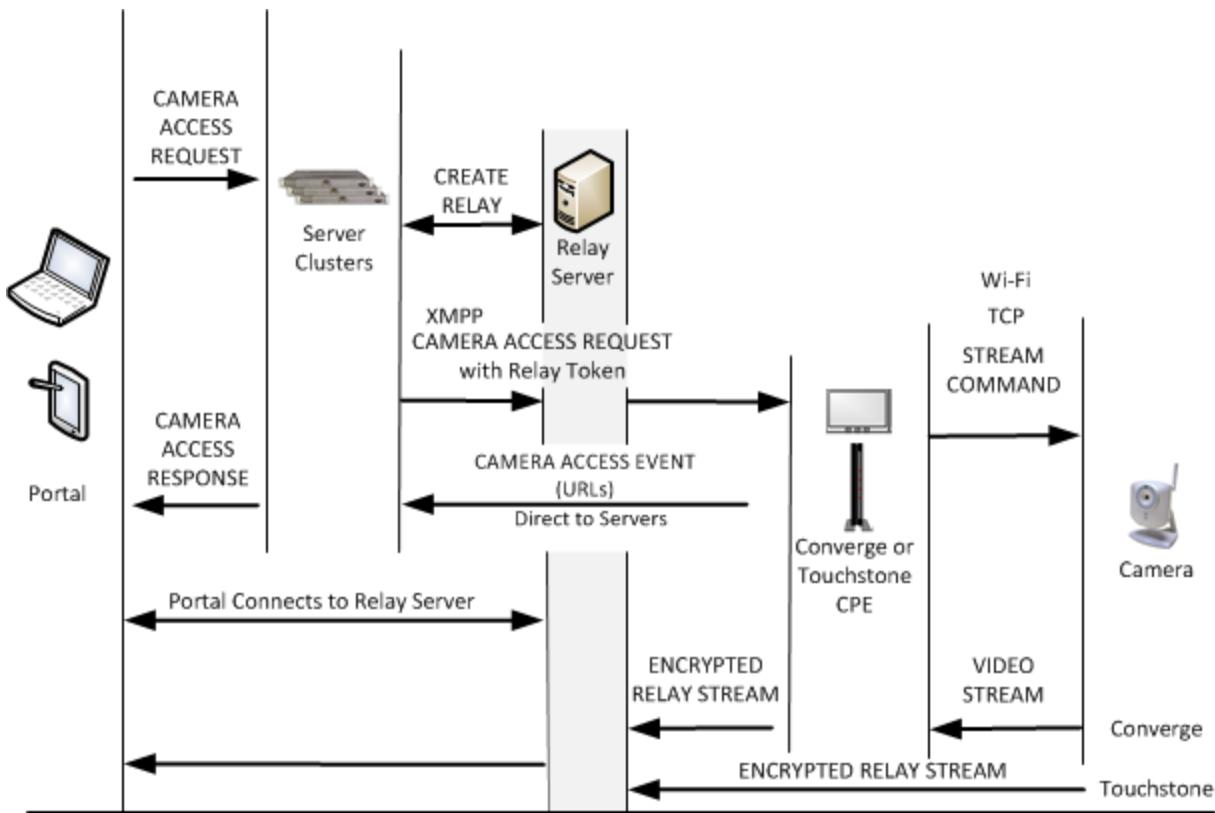


Figure 12: Streaming Video (Legacy Cameras) Sequence Diagram

The following illustration describes the connectivity between the cameras and the other elements in a multiple-cluster configuration. While live video is being viewed through a portal, the camera video feeds directly from the camera to the Relay server to the portal.

**Note:** Single-cluster server configuration is no longer supported as of the Oahu release.

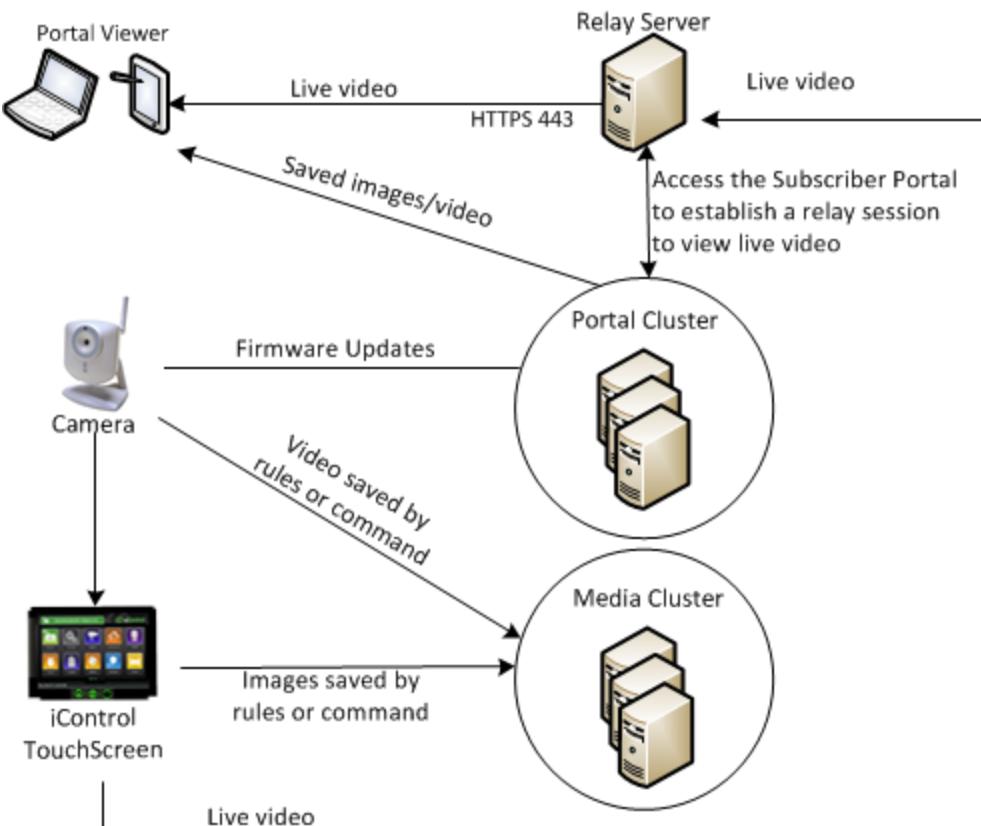


Figure 13: Cameras Logical Architecture: Multiple Clusters

## 6 Video/Image Capture Details

Channel	Converge	Touchstone
0	Upload clips & Mobile/SP	Upload clips & Mobile/SP
1	Touchscreen	Not used
2	MJPEG for Windows mobile, and Blackberry	MJPEG for Windows mobile, and Blackberry

### 6.1 Legacy Cameras

- ❑ **RC8021** Only uses channels 0 and 2. Does not support H.264.
- ❑ **iCamera** Supports 3 channels (all 3 are functional). Supports H.264.
- ❑ **OC810** Supports 3 channels (all 3 are functional). Supports H.264.
- ❑ **RC8026** Supports 3 channels (all 3 are functional). Supports H.264.
- ❑ **OC431** Supports 3 channels (all 3 are functional). Supports H.264.

### 6.2 OpenHome Cameras

#### 6.2.1 RRC8026

Channel	C	R	B	F	Profile
0	H.264	VGA	768 kbps	15 fps	Baseline
1	H.264	VGA	512 kbps	10fps	Baseline
2	MJPEG	VGA		10 fps	

#### 6.2.2 iCamera2

Channel	Codec	Resolution	Bitrate	Frame Rate	Profile
0	H.264	720HD	768 kbps	15 fps	M
1	H.264	720HD	512 kbps	5 fps	M
2	MJPEG	VGA		10 fps	

### 6.2.3 OC431

Channel	Codec	Resolution	Bitrate	Frame Rate	Profile
0	H.264	720HD	768 kbps	15 fps	Main
1	H.264	720HD	512 kbps	5 fps	Main
2	MJPEG	VGA		10 fps	

## 6.3 Image/Video Capture Details

Captured images and video are saved in the shared storage via the Application cluster. Based on the configuration of the subscriber's sensors or Subscriber Portal rules, the Home Domain might capture and upload images and video from the IP cameras. Subscribers can also manually capture images and video. This section describes how the images are stored on the Application Cluster servers.

Captured images are uploaded to the web app /fileUpload with the Camera ID and CPE ID.

Captured video is uploaded from the camera to the web app /cameraProxy/video. Then the servers get the file path and name from the database and saves it to shared storage.

### 6.3.1 File Name

The file name is created as described below:

#### Images:

premise\_id + event\_id + time + 'sec' + sequence\_number.jpg

#### Video:

premise\_id + event\_id + time + one-time code + 'sec' + sequence number .mp4

### 6.3.2 Path

The path where the image and video files are stored is generated based in the Premise ID of the subscriber (a unique ID based on the subscriber's address) and the Event ID (a unique ID based on the event that caused the images/video to be captured). Files are always saved to the following path:

[root] / [some directoryname] / [some directoryname] / [some directoryname] / [event id] / [uploaded file]

The directory names are generated in the following way:

Based on the Premise ID, the system calculates a SHA1 hash code.

For example, if the user's Premise ID is 5613, the hash code might be 77cwes90.

- ❑ The system creates a directory path based on the first three characters of the generated hash code. Each directory name is one character long.
- ❑ The system creates a new directory at the generated path based on the Event ID of the images. The system saves the video/images to the final directory.

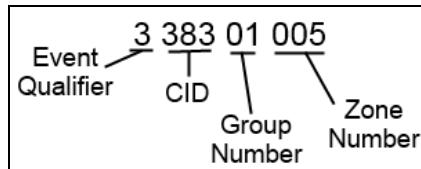
For example, if the hash code is 77cves90, and the Event ID is 55621, then the files are saved to 7/7/c/55621, where:

- 7/7/c is based on the first three characters of the generated hash code
- 55621 is the Event ID of the files

## 7 Contact ID Type Codes

### CONVERGE ONLY

The Contact ID Type (CID) code is also known as the *Event code*. This portion of the message to the central monitoring station describes the type of event that initiated the message. The CID is included in the <centralStationCode> tags of the message.



The Event Qualifier portion is always either **1** (for a new event or an *opening*, which is a Fault) or **3** (for the resolution of an event, or a *closing*, which is a Restore). The Group Number (that is, Partition Number) portion of the alarm message is always either **01** or **02** or **00** for *no information*.

See "[Zone Function Behaviors](#)" on page 86 for detailed information on CIDs generated by the touchscreen based on zone events.

The `white.list.zoneTrouble.to.centralStation` server.property lets you control what sensor troubles generate CIDs. See "[white.list.zoneTrouble.to.centralStation](#)" on page 294 for details.

### 7.1 Icontrol CID Codes

The following CID codes are used by the Icontrol System:

- CID 100 (see page 69)
- CID 110 (see page 69)
- CID 111 (see page 70)
- CID 120 (see page 70)
- CID 121 (see page 70)
- CID 122 (see page 71)
- CID 123 (see page 71)
- CID 130 (see page 72)
- CID 131 (see page 73)
- CID 132 (see page 73)
- CID 133 (see page 74)
- CID 134 (see page 74)
- CID 137 (see page 75)
- CID 139 (see page 76)
- CID 146 (see page 76)
- CID 147 (see page 77)
- CID 150 (see page 77)
- CID 154 (see page 78)
- CID 162 (see page 78)
- CID 301 (see page 79)
- CID 302 (see page 79)
- CID 316 (see page 79)
- CID 342 (see page 80)
- CID 354 (see page 80)
- CID 380 (see page 81)
- CID 381 (see page 82)
- CID 383 (see page 83)
- CID 384 (see page 83)
- CID 406 (see page 84)
- CID 459 (see page 84)
- CID 602 (see page 84)
- CID 607 (see page 85)
- CID 406 (see page 84)
- CID 751 (see page 86)
- CID 752 (see page 86)

- CID 135 (see page 75)
- CID 374 (see page 81)

### 7.1.1 CID 100

#### Categories

Medical  
Panic Alarm  
Fault/Restore

#### Description

This is generated when a user pressing the red Panic hardware button on the front of the touchscreen, and then selecting the Medical icon.

There is no Entry Delay or Transmission Delay period when this CID is generated.

#### Source

Touchscreen

### 7.1.2 CID 110

#### Categories

Fire  
Panic Alarm  
Fault/Restore

#### Description

This is generated when a user pressing the red Panic hardware button on the front of the touchscreen, and then selecting the Fire icon.

There is no Entry Delay or Transmission Delay period when this CID is generated.

#### Source

Touchscreen

### 7.1.3 CID 111

#### Categories

Fire  
Panic Alarm  
Fault/Restore

#### Description

One of the smoke detectors has been activated.

If the Fire Alarm Verification is set on the touchscreen, the contact ID is sent when the customer verifies the fire alarm. Otherwise, the touchscreen sends the CID if the smoke zone is faulted for 60 seconds, or if multiple smoke zones are faulted.

Zone function types that generate this CID:

- 24-Hour Fire (see page [95](#))

#### Source

Touchscreen

### 7.1.4 CID 120

#### Categories

Police  
Panic Alarm  
Audible 24-Hour  
Fault

#### Description

This is caused when a legacy Panic Zone has been faulted.

#### Source

Touchscreen

### 7.1.5 CID 121

#### Categories

Duress Alarm

#### Description

User has previously configured a Duress keypad code, and has entered that code to disarm the system..

#### Source

Touchscreen

### 7.1.6 CID 122

#### Categories

Police  
Panic Alarm  
Silent 24-Hour  
Fault

#### Description

This is caused by a user pressing the red Panic hardware button on the front of the touchscreen, and then selecting the Police icon. Furthermore, the user did **not** press the touchscreen after this (when prompted to "press the touchscreen to sound alarm").

#### Source

Touchscreen

### 7.1.7 CID 123

#### Categories

Police  
Panic Alarm  
Audible 24-Hour  
Fault

#### Description

This is caused by a user pressing the red Panic hardware button on the front of the touchscreen, and then selecting the Police icon. Subsequently, the user **did** press the touchscreen when this when prompted to "press the touchscreen to sound alarm").

#### Source

Touchscreen

## 7.1.8 CID 130

### Categories

Police  
Burglary  
Fault

### Description

This is generated when a zone is faulted when the system is armed.

### Source

Touchscreen

## 7.1.8.1 *alarm.backupServer.boundaryCase.contactId*

### Categories

Backup Server Boundary Case  
Alarm  
Fault

### Description

This CID is generated by the **alarm.backupServer.boundaryCase.contactIdTier** Property.

The default is **130**.

It is very rare that a CID would be generated in this way. In this rare event, a non-panic alarm has been tripped (with a Dialer Delay/Transmission Delay to the central monitoring station), but the Server Cluster crashed or could not be reached during the Transmission Delay period. Consequently, the **sendAlarms** message is sent to the backup server. The backup server does not know what alarm it needs to send, so it sends the CID defined by this Tier Property.

### Source

Operator Domain

### 7.1.9 CID 131

#### Categories

Burglary  
Perimeter Alarm  
Fault/Restore

#### Description

Someone opened a window or non-entry/exit doorway while the system was armed.

Zone function types that generate this CID:

- Perimeter (see page [90](#))
- 24-Hour Inform(see page [92](#))

#### Source

Touchscreen

### 7.1.10 CID 132

#### Categories

Burglary  
Interior Motion  
Fault/Restore

#### Description

A motion detector was faulted while the system was in Arm Away mode, or the device was tampered while armed.

Zone function types that generate this CID:

- Interior Follower (see page [96](#))
- Interior Follower Arm Night (see page [97](#))
- Interior With Delay (see page [98](#))
- Interior Delay Arm Night (see page [99](#))

#### Source

Touchscreen

### 7.1.11 CID 133

#### Categories

Burglary  
Audible 24-Hour  
Fault/Restore

#### Description

A zone that is configured as a *Audible 24-hour* has been faulted (or restored). This is not an alarm.

Zone function types that generate this CID:

Audible 24-Hour (see page [94](#))

#### Source

Touchscreen

### 7.1.12 CID 134

#### Categories

Burglary  
Entry/Exit Alarm  
Fault/Restore

#### Description

An Entry/Exit zone was faulted while the system was armed. The configured Entry Delay period expired before the correct keypad code was entered.

Zone function types that generate this CID:

Entry Exit (see page [88](#)).

#### Source

Touchscreen

### 7.1.13 CID 135

#### Categories

Door/Window

Trouble Day/Alarm Night

#### Description

A sensor assigned the Trouble Day/Alarm Night zone function was faulted while the system was in Arm Night mode.

Zone function types that generate this CID:

Trouble Day/Alarm Night (see page [91](#)).

#### Source

Touchscreen

### 7.1.14 CID 137

#### Categories

Tamper ARMED

Touchscreen or Sensor

Fault/Restore

#### Description

If originating from a touchscreen, then the stand or mount was removed while the system was armed.

By default, the touchscreen does not monitor this activity. See the `server.property device.tamper.enable` on page [265](#).

This can also be caused when a sensor's backplate has been removed when the system is armed.

See CID 316.

Zone function types that generate this CID:

- Entry Exit (see page [88](#))
- Perimeter (see page [90](#))
- Trouble Day/Alarm Night (see page [91](#))
- Silent 24-Hour (see page [93](#))
- Audible 24-Hour (see page [94](#))
- Interior Follower (see page [96](#))
- Interior Follower Arm Night (see page [97](#))
- Interior With Delay (see page [98](#))
- Interior Delay Arm Night (see page [99](#))

#### Source

Touchscreen

### 7.1.15 CID 139

#### Categories

Smash & Grab

Fault

#### Description

The server has adequately determined that the touchscreen screen is not in commission after it receives an entry delay. This could occur if an intruder has entered the house and destroyed the touchscreen. The CID number is configured specified by the **alarm.alarm.smashAndGrab.contactId** Tier Property.

"Understanding Smash & Grab" on page 112 for details.

#### Source

Operator Domain

### 7.1.16 CID 146

#### Categories

Burglary

Silent

Fault/Restore

#### Description

If the sensor is faulted when the system when armed or disarmed, it generates an instant alarm with no audible sound at any keypad or siren or the touchscreen.

Zone function types that generate this CID:

Silent 24-Hour (see page 93).

#### Source

Touchscreen

### 7.1.17 CID 147

#### Categories

Sensor Supervision Failure ARMED

Alarm

Fault

#### Description

The system is *armed* and the touchscreen has lost contact with a sensor.

The **touchscreen.sensor.commFail.alarmDelayTier** Property determines how long to wait before sending the CID.

Zone function types that generate this CID:

- Entry Exit (see page [88](#))
- Perimeter (see page [90](#))
- Trouble Day/Alarm Night (see page [91](#))
- Silent 24-Hour (see page [93](#))
- Audible 24-Hour (see page [94](#))
- 24-Hour Fire (see page [95](#))
- Interior Follower (see page [96](#))
- Interior Follower Arm Night (see page [97](#))
- Interior With Delay (see page [98](#))
- Interior Delay Arm Night (see page [99](#))

#### Source

Touchscreen

### 7.1.18 CID 150

#### Categories

Audible 24-hour

#### Description

Generic environmental device that produces an alarm. This CID is not currently assigned to any zone function type.

#### Source

Touchscreen

### 7.1.19 CID 154

#### Categories

Audible 24-hour

#### Description

Water leakage was detected.

Zone function types that generate this CID:

Audible 24-Hour (see page [94](#))

#### Source

Touchscreen

### 7.1.20 CID 162

#### Categories

Audible 24-hour

#### Description

Carbon Monoxide sensor fault.

Zone function types that generate this CID:

Audible 24-Hour (see page [94](#))

#### Source

Touchscreen

### 7.1.21 CID 301

This CID reports that the touchscreen has lost A/C power or has had that power restored.

#### Categories

A/C Power Loss  
Fault/Restore

#### Description

The touchscreen has lost A/C power. The touchscreen automatically goes into Low Power Mode  
(<centralstationcode>1301xxxx</centralstationcode>)

OR

The touchscreen (that had lost A/C power and was in Low Power Mode) has had A/C Power restored.  
(<centralstationcode>3301xxxx</centralstationcode>)

#### Source

Touchscreen

### 7.1.22 CID 302

#### Categories

Touchscreen Low Battery  
Fault

#### Description

The touchscreen has no A/C power and it detects that the battery is lower than 10% of capacity.

#### Source

Touchscreen

### 7.1.23 CID 316

#### Categories

Tamper DISARMED  
Touchscreen or Sensor Fault/Restore

#### Description

The stand or mount of a touchscreen was removed while the system was disarmed. By default, the touchscreen does not monitor this activity. See the server.property device.tamper.enable on page [265](#).

See "CID 137" on page [75](#).

#### Source

Touchscreen

### 7.1.24 CID 342

#### Categories

Sensor No A/C Power  
Fault

#### Description

A sensor with a battery back-up that uses A/C power has lost A/C power.

#### Source

Touchscreen

#### Associated Zone Trouble Events

senNoPower

### 7.1.25 CID 344

#### Categories

Loss of supervision  
ZigBee zone  
Fault/Restore

#### Description

The touchscreen has detected the possibility of RF jamming on the ZigBee network. For more information, see <https://share-icontrol.atlassian.net/wiki/display/CSKB/ZigBee+Jamming+Detection>.

#### Source

Touchscreen

### 7.1.26 CID 354

#### Categories

Failure to communicate event

#### Description

1. The system determined that a Smash & Grab event has occurred because it received an Entry Delay event from a touchscreen but did not receive an associated Alarm event or Disarm event within the configured window.
2. The system subsequently determined that a Smash & Grab did not occur by other means.

See "Understanding Smash & Grab" on page 112 for more information.

See CID 137.

#### Source

Operator Domain

### 7.1.27 CID 374

#### Categories

Exit Error  
Fault/Restore

#### Description

The system was armed, but the Entry/Exit doorway was never shut.

Specifically, at the end of the Exit Delay, an Entry/Exit zone was not closed. This CID is sent in addition to [CID 134 \(see page 74\)](#).

Zone function types that generate this CID:

Entry Exit (see page [88](#)).

#### Source

Touchscreen

### 7.1.28 CID 380

#### Categories

Sensor trouble  
Zone (generic)  
Fault

#### Description

This contact ID is sent in three cases.

- If the zone goes into swinger-shutdown.
- If the zone's sensor is dirty.
- If the zone's sensor was being upgraded, but the upgrade failed.

#### Source

Touchscreen

#### Associated Zone Trouble Events

- zoneSwingerShutdown
- senDirty
- senBootloadFail

## 7.1.29 CID 381

### Categories

Loss of supervision

ZigBee Zone

Fault

### Description

The touchscreen has lost contact with a sensor. The **touchscreen.sensor.commFail.troubleDelay** tier property determines how long to wait before sending the CID.

Zone function types that generate this CID:

- Entry Exit (see page [88](#))
- Perimeter (see page [90](#))
- Trouble Day/Alarm Night (see page [91](#))
- Silent 24-Hour (see page [93](#))
- Audible 24-Hour (see page [94](#))
- 24-Hour Fire (see page [95](#))
- Interior Follower (see page [96](#))
- Interior Follower Arm Night (see page [97](#))
- Interior With Delay (see page [98](#))
- Interior Delay Arm Night (see page [99](#))

### Source

Touchscreen

### Associated Zone Trouble Events

sensCom

### 7.1.30 CID 383

#### Categories

Sensor tamper

Zone

Fault

#### Description

A sensor was tampered.

Zone function types that generate this CID:

- Entry Exit (see page [88](#))
- Perimeter (see page [90](#))
- Trouble Day/Alarm Night (see page [91](#))
- Silent 24-Hour (see page [93](#))
- Audible 24-Hour (see page [94](#))
- 24-Hour Fire (see page [95](#))
- Interior Follower (see page [96](#))
- Interior Follower Arm Night (see page [97](#))
- Interior With Delay (see page [98](#))
- Interior Delay Arm Night (see page [99](#))

#### Source

Touchscreen

#### Associated Zone Trouble Events

senTamp

### 7.1.31 CID 384

#### Categories

ZigBee low battery

Zone

Fault

#### Description

A sensor is reporting a low battery.

#### Source

Touchscreen

#### Associated Zone Trouble Events

senLowBat

### 7.1.32 CID 406

**IMPORTANT:** It is not possible to tell from the Event information sent to the central monitoring station whether this code originated from the touchscreen or the Operator Domain.

#### Categories

Alarm Abort/Cancel

Fault

#### 7.1.32.1 Source: Touchscreen

An alarm was tripped but the system was disarmed within the Transmission Delay period by the subscriber (aborted).

#### 7.1.32.2 Source: Operator Domain

An alarm was tripped and the Transmission Delay period has expired, but –within five minutes of the start of the alarm session– the system was disarmed by the subscriber (cancelled).

### 7.1.33 CID 459

#### Categories

Recent closing

Fault

#### Description

Sent if an alarm occurs within two (2) minutes after the expiration of the Exit Time. This CID is sent along with the alarm CID.

#### Source

Touchscreen

### 7.1.34 CID 602

#### Categories

Periodic Test Report

Fault

#### Description

A report of the zones that were faulted and restored during the Walkthrough Test.  
Will be preceded and followed by [CID 607](#).

#### Source

Touchscreen

### 7.1.35 CID 607

See also CID 602.

#### Categories

Test Mode

Fault (Test Mode started)/Restore (Test Mode ended)

#### Description

Fault = The Alarm Test during Activation has been started

Restore = The Alarm Test during Activation has ended.

#### Source

Touchscreen

### 7.1.36 CID 751

#### Categories

Loss of supervision  
ZigBee peripheral  
Fault

#### Description

The touchscreen has lost contact with the panel interface module (PIM). The **touchscreen.sensor.commFail.troubleDelay** tier property determines how long to wait before sending the CID.

#### Source

Touchscreen

### 7.1.37 CID 752

#### Categories

Peripheral tamper  
Fault/Restore

#### Description

Sends the "Wireless Keypad tamper" trouble to the server and central monitoring station (CMS).

#### Source

Touchscreen

## 7.2 Zone Function Behaviors

### CONVERGE ONLY

Each security sensor paired with the touchscreen is assigned a zone function at the time of installation. The zone function indicates how the touchscreen should interpret the signals from the sensor when it is armed or disarmed. The system can be armed in the following modes:

- Arm Away
- Arm Stay
- Arm Night

The following is a list of the zone functions supported:

Zone Function	Description	Sensor
Entry/Exit	Used to monitor doorways from which users enter and exit the premises. Depending on how the system is armed, faulting this sensor generates an audible alarm.	Door/Window
Perimeter	Used to monitor windows or doorways that are not used to enter or exit an armed premises. Faulting this sensor generates an audible alarm immediately.	Door/Window Glass Break Detector
24-Hour Inform	Used in areas that need monitoring, but faulting the sensor does not generate an alarm if the system is armed.	Door/Window Glass Break Detector Motion Detector Water Detector
Trouble Day/Alarm Night	Used on doors or windows that need monitoring only when the system is Armed Night. It generates an alarm if the sensor is faulted or tampered when the system is Armed Night.	Door/Window
Silent 24-Hour	Used in areas that need monitoring and generates an alarm if the sensor is faulted, whether the system is armed or disarmed, but there is no sound from the touchscreen, keypad(s), or siren to indicate the alarm has been generated.	Door/Window
Audible 24-Hour	Used in areas that need monitoring and generates an audible alarm if the sensor is faulted, whether the system is armed or disarmed.	Door/Window Carbon Monoxide Detector Water Detector
Interior Follower	Used to monitor large areas inside the premises. Depending on how the system is armed, faulting this sensor generates an audible alarm.	Motion Detector
Interior with Delay	Used to monitor areas near entry and exit points. Depending on how the system is armed, faulting this sensor generates an audible alarm.	Motion Detector
Interior Follower Arm Night	Used to monitor large areas inside the premises. Depending on how the system is armed, faulting this sensor generates an audible alarm.	Motion Detector
Interior Delay Arm Night	Used to monitor large areas inside the premises. Depending on how the system is armed, faulting this sensor generates an audible alarm.	Motion Detector

Zone Function	Description	Sensor
Fire 24-Hour	Used only for smoke detectors and generates an audible alarm when smoke is detected, whether the system is armed or disarmed.	Smoke Detector

## 7.2.1 Entry/Exit Zone Function

At least one door is set as an entry/exit zone when the system is installed. This is usually the door the user most frequently uses to enter and exit the premises. Entry and exit delays are associated with the sensors assigned to entry/exit zones. The delays allow the user to enter or exit the premises without triggering the alarm. These delays can be configured on the touchscreen. See the "Configuring the Entry/Exit Delay Periods" section in *Converge Installation Guide*.

### 7.2.1.1 Zone Faulted

When the system is *disarmed*, there is no alarm when the zone is faulted. No CID is sent.

If this zone is faulted, the system will not arm.

Arming the system initiates the Exit Delay. A person can fault this zone and not cause an alarm during this time. Default is 60 seconds. See the timing diagram below:

Time (min:sec)	0:00	0:50 *	1:00
System State	Disarmed	Exit Delay	Armed
Touchscreen UI	Disarmed	Exit Delay Countdown	Armed
Touchscreen Audible	Exit Delay Chime (1 beep/sec)	Rapid Exit Delay Chime (2 beeps/sec) *	

If this zone is opened, closed, and opened again, the system resets the Exit Delay counter. See the timing diagram below:

Time (min:sec)	0:00	Zone Faulted < 1:00 counter reset to 0:00	0:50 *	1:00
System State	Disarmed	Exit Delay	Restart Exit Delay	Armed
Touchscreen UI	Disarmed	Exit Delay Countdown		Armed
Touchscreen Audible	Exit Delay Chime	Exit Delay Chime	Rapid Exit Delay Chime*	

If this zone is opened and left open at the end of the Exit Delay, the system reports an Exit Error. **CID 374** and **CID 134** are sent. See the timing diagram below:

Time (min:sec)	0:00	0:50 *	1:00	1:20 *	1:30	2:00	6:30
----------------	------	--------	------	--------	------	------	------

<b>System State</b>	disarmed	Exit Delay		Entry Delay		Alarm (Abort Window begins)	Alarm	Armed Away
		Exit Delay Countdown		Entry Delay Disarm Screen		Alarm Disarm Screen		
		Exit Delay Chime	Rapid Entry Delay Chime *	Entry Delay Chime and Audible Alarm	Rapid Entry Delay Chime * and Audible Alarm	Audible Alarm		
							Transmit Alarm & Exit Error	

When the system is *armed* and a person faults this zone, the Entry Delay is initiated. The person must disarm the system during this time to avoid triggering an alarm. Default is 30 seconds. See the timing diagram below:

Time (min:sec)		0:00	0:20 *	<0:30
<b>System State</b>	Armed	Entry Delay (entry/exit/delayed zone faulted)		Disarmed (valid entry code entered)
<b>Touchscreen UI</b>	Armed	Entry Delay Disarm Screen		Disarmed
<b>Touchscreen Audible</b>		Entry Delay Chime (1 beep/sec)	Rapid Entry Delay Chime (2 beeps/sec) *	

\* The Rapid Entry/Exit Delay Chime (2 beeps/sec) always begins 10 seconds before the end of the entry and exit delays.

When the zone is faulted and the system is *armed*:

- Arm Away** Alarms if entry delay expires and **CID 134** is sent.
- Arm Stay** Alarms if entry delay expires and **CID 134** is sent.
- Arm Night** Issues an audible alarm without an Entry Delay and **CID 134** is sent.

### 7.2.1.2 Comm Failure Trouble

When the system is *disarmed*, a trouble is displayed at the touchscreen in the Trouble Header. The system will not arm. **CID 381** is sent.

When the system is *armed*, this trouble results in an alarm. **CID 147** is sent.

### 7.2.1.3 Tamper Trouble

When the system is *disarmed*, a trouble is displayed at the touchscreen in the Trouble Header. The system will not arm. **CID 383** is sent.

When the system is *armed*, this trouble results in an alarm. **CID 137** is sent.

## 7.2.2 Perimeter Zone Function

### 7.2.2.1 Zone Faulted

When the system is *disarmed*, there is no alarm. The system will not arm. No CID is sent.

When the system is *armed*, it issues an audible alarm without an Entry Delay. **CID 131** is sent.

### 7.2.2.2 Comm Failure Trouble

When the system is *disarmed*, a trouble is displayed at the touchscreen in the Trouble Header. The system will not arm. **CID 381** is sent.

When the system is *armed*, the system generates an audible alarm. A trouble is displayed at the touchscreen in the Trouble Header. **CID 147** is sent.

### 7.2.2.3 Tamper Trouble

When the system is *disarmed*, a trouble is displayed at the touchscreen in the Trouble Header. The system will not arm. **CID 383** is sent.

When the system is *armed*, this trouble results in an alarm. **CID 137** is sent.

### 7.2.3 Trouble Day/Alarm Night Zone Function

An entryway that alarms instantly if faulted when armed in Arm Night mode. However, it does not take any action if it is faulted in any other arming mode.

**Note:** Despite the function name, the system does not issue a trouble if the zone is faulted in **Arm Away** or **Arm Stay**.

#### 7.2.3.1 Zone Faulted

When the system is *disarmed*, there is no alarm or other action taken. No CID is sent.

When the system is *armed*, the following occurs:

- ❑ **Arm Away** and **Arm Stay** No alarm or other action taken. No CID sent.  
If faulted during *Entry Delay* (for example, after an Entry/Exit zone was faulted) or during *Exit Delay*, no action is taken.
- ❑ **Arm Night** The system issues an audible alarm without an Entry Delay. **CID 135** sent.  
Same action if faulted during *Entry Delay* or during *Exit Delay*

#### 7.2.3.2 Comm Failure Trouble

When the system is *disarmed*, a trouble is displayed at the touchscreen in the Trouble Header. The system will not arm. **CID 381** is sent.

When the system is *armed*, the following occurs:

- ❑ **Arm Away** and **Arm Stay** A trouble is displayed at the touchscreen in the Trouble Header. No alarm. No CID sent.
- ❑ **Arm Night** Issues an audible alarm without an Entry Delay. A trouble is displayed at the touchscreen in the Trouble Header. **CID 147** sent.

#### 7.2.3.3 Tamper Trouble

When the system is *disarmed*, a trouble is displayed at the touchscreen in the Trouble Header. **CID 383** sent.

When the system is *armed*, the following occurs:

- ❑ **Arm Away** and **Arm Stay** A trouble is displayed at the touchscreen in the Trouble Header. No alarm. No CID sent.
- ❑ **Arm Night** Issues an audible alarm without an Entry Delay . **CID 137** sent.

## 7.2.4 24-Hour Inform Zone Function

### 7.2.4.1 Zone Faulted

When the system is *armed* or *disarmed* or in any other state, no action is taken. No CID sent.

When the system is in *alarm*, **CID 131** is sent.

### 7.2.4.2 Comm Failure Trouble

When the system is *disarmed* or *armed*, a trouble is displayed at the touchscreen in the Trouble Header. Does not prevent arming. No CID is sent.

### 7.2.4.3 Tamper Trouble

When the system is *disarmed* or *armed*, a trouble is displayed at the touchscreen in the Trouble Header. Does not prevent arming. No CID is sent.

## 7.2.5 Silent 24-Hour Zone Function

### 7.2.5.1 Zone Faulted

When the system is *armed* or *disarmed*, the system issues a silent alarm without an Entry Delay. **CID 146** is sent.

The same action is taken if the zone is faulted during *Entry Delay* or during *Exit Delay*.

### 7.2.5.2 Comm Failure Trouble

When the system is *disarmed*, a trouble is displayed at the touchscreen in the Trouble Header. Does not prevent arming. **CID 381** is sent.

When the system is *armed*, silent alarm is issued without an Entry Delay. A trouble is displayed at the touchscreen in the Trouble Header. **CID 147** is sent.

### 7.2.5.3 Tamper Trouble

When the system is *disarmed*, a trouble is displayed at the touchscreen in the Trouble Header. **CID 383** is sent.

When the system is *armed*, a trouble is displayed at the touchscreen in the Trouble Header. **CID 137** is sent.

## 7.2.6 Audible 24-Hour Zone Function

### 7.2.6.1 Zone Faulted

When the system is *armed* or *disarmed*, the system issues an audible alarm without an Entry Delay.

The **CID sent** is dependent on the sensor type:

- Door/Window: CID 133
- Water: CID 154
- Carbon Monoxide: CID 162

The same action is taken if the zone is faulted during an *Entry Delay* or during *Exit Delay*.

### 7.2.6.2 Comm Fail

When the system is *disarmed*, a trouble is displayed at the touchscreen in the Trouble Header. **CID 381** is sent. Does not prevent arming.

When the system is *armed*, the system issues an alarm without an Entry Delay. A trouble is displayed at the touchscreen in the Trouble Header. **CID 147** is sent.

### 7.2.6.3 Tamper Trouble

When the system is *disarmed*, a trouble is displayed at the touchscreen in the Trouble Header. **CID 383** is sent. Does not prevent arming.

When the system is *armed*, a trouble is displayed at the touchscreen in the trouble header. It does not cause the system to issue an alarm. The **CID sent** is dependent on the sensor type:

- Door/Window: CID 137
- Water: CID 144
- Carbon Monoxide: CID 144

## 7.2.7 24-Hour Fire Zone Function

### 7.2.7.1 Zone Faulted

When the system is *disarmed* or *armed*, the system issues an audible alarm without an Entry Exit Delay. **CID 111** sent.

### 7.2.7.2 Comm Failure Trouble

When the system is *disarmed*, a trouble is displayed at the touchscreen in the Trouble Header. Does not prevent arming. **CID 381** is sent.

When the system is *armed*, the system issues an audible alarm without an Entry Exit Delay. A trouble is displayed at the touchscreen in the Trouble Header. **CID 147** is sent.

### 7.2.7.3 Tamper Trouble

When the system is *disarmed*, a trouble is displayed at the touchscreen in the Trouble Header. Does not prevent arming. **CID 383** is sent.

When the system is *armed*, a trouble is displayed at the touchscreen in the Trouble Header. **CID 144** is sent.

## 7.2.8 Interior Follower Zone Function

### 7.2.8.1 Zone Faulted

When the system is *disarmed*, no action is taken. No CID is sent.

When the system is *armed*, the following occurs:

- Arm Away** Issues an audible alarm without an Entry Delay. **CID 132** sent.
- Arm Stay or Arm Night** There is no alarm. No CID is sent.

If faulted during *Entry Delay* (after an Entry/Exit zone was faulted) or during *Exit Delay*, no additional action is taken.

### 7.2.8.2 Comm Failure Trouble

When the system is *disarmed*, a trouble is displayed at the touchscreen in the Trouble Header. The system cannot arm. **CID 381** is sent.

When the system is *armed*, the following occurs:

- Arm Night and Arm Stay** A trouble is displayed at the touchscreen in the Trouble Header. No alarm. No CID sent.
- Arm Away** Issues an audible alarm without an Entry Delay. A trouble is displayed at the touchscreen in the Trouble Header. **CID 147** sent.

### 7.2.8.3 Tamper Trouble

When the system is *disarmed*, a trouble is displayed at the touchscreen in the Trouble Header. **CID 383** sent.

When the system is *armed*, the following occurs:

- Arm Stay or Arm Night** A trouble is displayed at the touchscreen in the Trouble Header. No CID sent.
- Arm Away** Issues an audible alarm without an Entry Delay. **CID 137** sent.

## 7.2.9 Interior Follower Arm Night Zone Function

### 7.2.9.1 Zone Faulted

When the system is *disarmed*, no action is taken. No CID is sent.

When the system is *armed*, the following occurs:

- Arm Night or Arm Away** Issues an audible alarm without an Entry Delay. **CID 132** sent.
- Arm Stay** There is no alarm. No CID is sent.

If faulted during *Entry Delay* (after an Entry/Exit zone was faulted) or during *Exit Delay*, no additional action is taken.

### 7.2.9.2 Comm Failure Trouble

When the system is *disarmed*, a trouble is displayed at the touchscreen in the Trouble Header. The system cannot arm. **CID 381** is sent.

When the system is *armed*, the following occurs:

- Arm Night or Arm Away** Issues an audible alarm without an Entry Delay. A trouble is displayed at the touchscreen in the Trouble Header. **CID 147** sent.
- Arm Stay** A trouble is displayed at the touchscreen in the Trouble Header. No alarm. No CID sent.

### 7.2.9.3 Tamper Trouble

When the system is *disarmed*, a trouble is displayed at the touchscreen in the Trouble Header. **CID 383** sent.

When the system is *armed*, the following occurs:

- Arm Away or Arm Night** Issues an audible alarm without an Entry Delay. **CID 137** sent.
- Arm Stay** A trouble is displayed at the touchscreen in the Trouble Header. No CID sent.

## 7.2.10 Interior With Delay Zone Function

### 7.2.10.1 Zone Faulted

When the system is *disarmed*, no action is taken. No CID is sent.

When the system is *armed*, the following occurs:

- Arm Away** The system initiates an Entry Delay and issues an alarm if the Entry Delay period expires. **CID 132** sent.
- Arm Night or Arm Stay** There is no alarm. No CID is sent.

If faulted during an *Entry Delay* (after an Entry/Exit zone was faulted) or during *Exit Delay*, no additional action is taken.

### 7.2.10.2 Comm Failure Trouble

When the system is *disarmed*, a trouble is displayed at the touchscreen in the Trouble Header. The system cannot arm. **CID 381** is sent.

When the system is *armed*, the following occurs:

- Arm Away** The system initiates an Entry Delay and issues an alarm if the Entry Delay period expires. **CID 147** sent.
- Arm Night or Arm Stay** A trouble is displayed at the touchscreen in the Trouble Header. No alarm. No CID sent.

### 7.2.10.3 Tamper Trouble

When the system is *disarmed*, a trouble is displayed at the touchscreen in the Trouble Header. **CID 383** sent.

When the system is *armed*, the following occurs:

- Arm Away** The system initiates an Entry Delay and issues an alarm if the Entry Delay period expires. **CID 137** sent.
- Arm Night or Arm Stay** A trouble is displayed at the touchscreen in the Trouble Header. No CID sent.

## 7.2.11 Interior Delay Arm Night Zone Function

### 7.2.11.1 Zone Faulted

When the system is *disarmed*, no action is taken. No CID is sent.

When the system is *armed*, the following occurs:

- Arm Night or Arm Away** The system initiates an Entry Delay and issues an alarm if the Entry Delay period expires. **CID 132** sent.
- Arm Stay** There is no alarm. No CID is sent.

If faulted during an *Entry Delay* (after an Entry/Exit zone was faulted) or during *Exit Delay*, no additional action is taken.

### 7.2.11.2 Comm Failure Trouble

When the system is *disarmed*, a trouble is displayed at the touchscreen in the Trouble Header. The system cannot arm. **CID 381** is sent.

When the system is *armed*, the following occurs:

- Arm Night or Arm Away** The system initiates an Entry Delay and issues an alarm if the Entry Delay period expires. **CID 147** sent.
- Arm Stay** A trouble is displayed at the touchscreen in the Trouble Header. No alarm. No CID sent.

### 7.2.11.3 Tamper Trouble

When the system is *disarmed*, a trouble is displayed at the touchscreen in the Trouble Header. **CID 383** sent.

When the system is *armed*, the following occurs:

- Arm Night or Arm Away** The system initiates an Entry Delay and issues an alarm if the Entry Delay period expires. **CID 137** sent.
- Arm Stay** A trouble is displayed at the touchscreen in the Trouble Header. No CID sent.

## 8 Icontrol Connectivity Protocols

This section is intended to explain the CPE device to server connectivity for all platforms.

### 8.1 Broadband Connectivity

Each CPE, Converge or Touchstone, has an always-on TCP connection to the application clusters. This connection made it possible for the CPE to send events from the Home Domain in near real-time to server, and allow server to send commands, such as turning on lights or remote arm/disarm down to CPE.

The connection can be disrupted for many reasons. In cases such as CPE reboot, the server gets notified immediately. If the home router is removed, server will not be notified at TCP level until the underlying socket connection times out.

#### 8.1.1 Broadband Heartbeat

Broadband heartbeat messages are sent periodically from the CPE device to the application clusters over broadband. The purpose of the heartbeat signals is to do the following:

- Keep open the TCP connection between the CPE device and the Application cluster in the Operator domain.
- Keep the Operator domain apprised of each sensor's connectivity to the CPE.

The time interval for heartbeat messages is determined by the customer's Tier of service.

The default broadband heartbeat intervals (`connection.broadbandHeartBeatRate` `Tier` property) for each platform are the following:

**Converge:** The Gold tier is 10 minutes, Silver tier is 20 minutes, Bronze tier is 30 minutes

**Touchstone:** The base tier is 30 minutes

The heartbeat interval values are chosen to help with broadband fluttering which is outside of the CPE device's control and to control server load. These values can be lowered, but it is not recommended as it increases bandwidth in and out of the data center and increase resource usage on the server.

**Note:** For Converge systems, the NAT timeout on your corporate router should exceed the heartbeat intervals. See "[Network Address Translation \(NAT\) for Cellular Traffic](#)" on page 105

The broadband heartbeat is sent as a standard XMPP (SMAP) message. This means that the heartbeat is logged when using the server's Single Device Debugging feature.

#### 8.1.1.1 Broadband Heartbeat Message Size

The payload size for broadband heartbeat/ACK is **120/73** bytes.

The TCP header is **20** bytes.

The total for heartbeat/ACK size is **120 + 73 + 40 = 233** bytes (not including SSL encryption overhead).

### 8.1.2 Reporting Interval of Broadband Connectivity

Many broadband outages are transient in nature. To filter out transient broadband failures, the application servers use the concept of 'marked' broadband connectivity.

Once the Application cluster is notified by a broadband down (either by the underlying TCP connection, or by lack of heartbeat message), it will generate an 'unmarked' broadband down event. If after a time period (controlled by server property `broadbandCommunicationEvent.markFactor`), the broadband is still down, the server will generate a *marked* broadband-down event.

The time for server to wait is determined by the following formula:

`(broadbandCommunicationEvent.markFactor minus 1) times  
(connection.broadbandHeartBeatRate)`

For example, if the value for the `markFactor` property is **2** (default) and the `heartbeat Tier` property value is **10** minutes, then

$$(2 - 1) * (10 \text{ minutes}) = 10 \text{ minutes}$$

This means if the server generates an *unmarked* broadband down event for an account, the server will wait 10 minutes for the account to re-establish the broadband connection before the server generates a *marked* broadband down event.

We recommend that the `markFactor` set to **2** or above. If the `mark markFactor` is **1**, all *unmarked* connectivity events become *marked*.

All connectivity events are stored in the database; however, the Management Portal Account View and the Subscriber Portal only display the *marked* connectivity events. Server only takes action on marked connectivity events in the case of connectivity alerts/rules.

For advanced connectivity troubleshooting, use the Management Portal's Root Cause Analysis page to view the unmarked connectivity events.

**IMPORTANT:** Contact your Icontrol representative if you need to change any of the connectivity related server or tier property values.

### 8.1.3 Broadband Connectivity During Server Cluster Reboots

After the Application server cluster has been rebooted, it takes **40 to 50 minutes** for any changes in CPE connectivity to be updated. If a CPE was connected by broadband **before** the cluster reboot, and the broadband connectivity was lost **during** the reboot, then it could take 40 to 50 minutes after the restart for the connection to be marked down. This is dependent on the broadband heartbeat interval. The unmarked connectivity for broadband down (viewable in the Management Portal's Root Cause Analysis page) is set sooner.

### 8.1.4 Viewer Engaged/Disengaged over Broadband

When a user is interacting with the system via the portals or mobile applications, the CPE is notified via a Viewer Engaged XMPP message. CPE stops using the `connection.broadbandHeartBeatRate` property value and uses the `connection.broadbandQuickHeartBeatRate` property value (default is 1 minute) as long as a viewer is engaged to help ensure a more responsive reporting of broadband connectivity. For this reason, when looking at an account in a Portal or Mobile app, broadband fluttering could be more visible.

The Viewer Engaged/Disengaged message is only sent over broadband. The viewer engaged flag is also in the XMPP initial inform response. This means CPE will have the correct value after reboot.

In addition to quicker heartbeat, CPE also sends more events like thermostat temperature change and lighting event to server in viewer engaged mode.

See the "Access Domain Communication Channels and Connectivity Protocols" section in Converge System Architecture Guide and Touchstone System Architecture Guide for more information the broadband channel.

## 8.2 Cellular Connectivity

### CONVERGE ONLY

Each Converge CPE device has the ability to send messages over cellular. The cellular channel is a backup communication channel in case the primary channel (broadband) is down.

#### 8.2.1 Cellular Heartbeat

Cellular heartbeat messages are UDP messages that are sent periodically from the CPE device to the Application cluster servers over cellular. The purpose of the heartbeat signals is to keep the Operator domain apprised of each CPE device's cellular connectivity.

The time interval for heartbeat messages is determined by the customer's tier of service.

The default cellular heartbeat intervals (`connection.cellularHeartBeatRate.Tier` property) for Converge are 1 hour (gold tier), 4 hours (silver tier), and 24 hours (bronze tier). The values are chosen to reduce the amount of base cellular traffic for each CPE.

For each cellular heartbeat message, server will reply an ACK message over cellular. CPE will reply an ACKACK message once it receives the ACK message from server. The ACKACK message is necessary to make sure the cellular channel is bi-directional.

If an ACK is not received by CPE after a cellular heartbeat is sent, the CPE will try to send another heartbeat message after a period (defined by `Tier` Property `connection.cellularRetryInterval`). The CPE will continue to send heartbeat for a number of times (defined by `tier` property `connection.numOfRetries`) before it reverts to the normal heartbeat rate.

The heartbeat message is logged when using the server's Single Device Debugging feature.

#### 8.2.2 Cellular Heartbeat Message Size

The size of the cellular heartbeat and the ACKACK UDP message is 36 bytes and the size of the heartbeat ACK message is 30 bytes (including IP/UDP header but not including optional TEA encryption).

### 8.2.3 Reporting Cellular Connectivity

The server determines that the cellular connectivity is down by one of the following methods:

- Detecting it
- Receiving a Cellular Down connectivity event from the touchscreen over broadband.

#### 8.2.3.1 Server Detection

The server considers the cellular connection with a touchscreen to be down if the server has not received a cellular heartbeat message from a CPE in the time period defined by:

```
connection.cellularHeartBeatRate+
(connection.cellularRetryInterval* connection.numOfRetries)
```

Cellular connectivity can be lost if the cell tower kicks off the touchscreen's cellular modem.

If server receives a heartbeat message but not an ACKACK (the second acknowledgment), the cellular connection is considered to be one-way. If this happens to a large number of CPEs, check the cellular VPN settings.

If broadband is down as well, depending on cellular level of service, server will try to send a broadband down cellular message to the CPE. The CPE will return an ACK if it receives the message. If the ACK is not received, server will try to send the message for a number of times Defined by server property broadbandDownCellularMsg.max.try at a time interval defined by tier property connection.bbdwncellularRetryRate. If there is no ACK after three tries (default value of broadbandDownCellularMsg.max.try), cellular connection is considered down by server.

#### 8.2.3.2 Touchscreen Detection

For Enhanced cellular level of service, WHEN the following is true for the touchscreen:

- Has broadband connectivity
- Detects that it lost the cellular PPP connectivity (no cellular connectivity)

THEN it sends a Cellular Down connectivity event to the server over broadband. The touchscreen tries to re-establish a PPP IP address every minute for up to 5 minutes, then in 15 minutes, 30 minutes, and 60 minutes.

### 8.2.4 Network Address Translation (NAT) for Cellular Traffic

For service providers that use NAT for cellular traffic, the NAT table in the service provider router is responsible for performing the port mapping between the server and the touchscreen.

The server saves the cellular IP and port of each touchscreen's cellular traffic (virtual IP/port) in the `system_status` table (`cellular_vip` and `cellular_vport`). All server-originated tickles and commands (UDP traffic) going to the touchscreen from the server over cellular use the virtual IP and port.

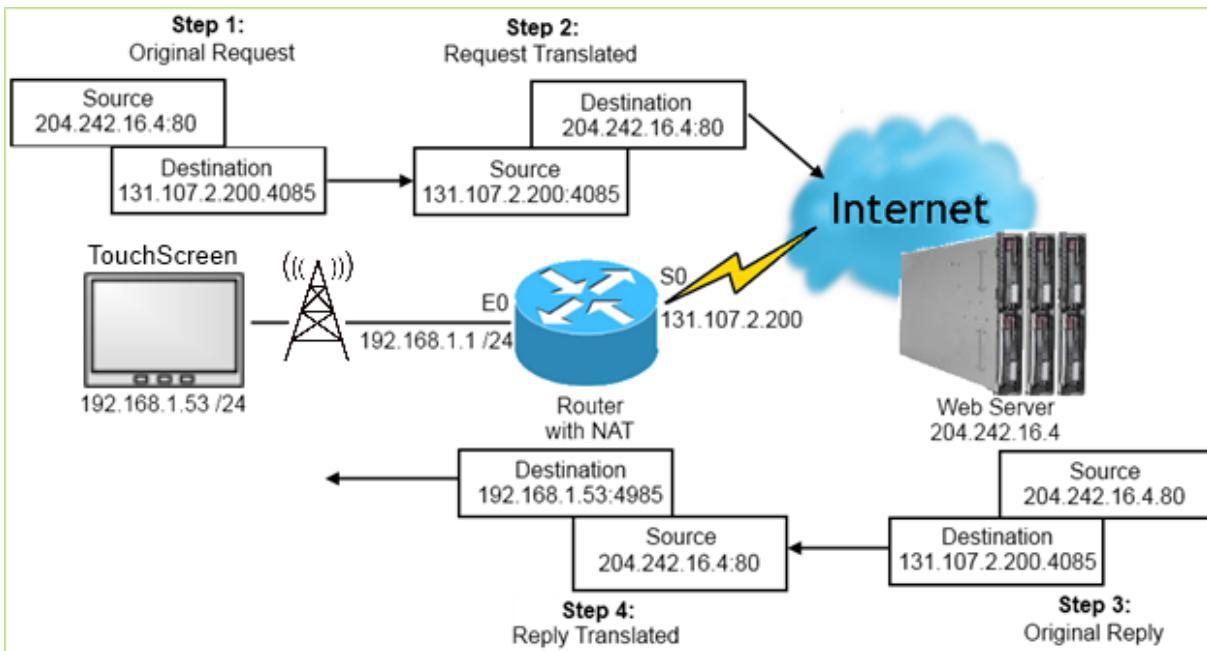


Figure 14: NAT Cellular Communication

For service providers not using NAT, the server responds to port 9091.

For NAT users, the NAT table's connection time-out should be greater than the touchscreen's cellular heartbeat interval (`connection.cellularHeartBeatRate` tier property). This ensures that the server has up-to-date information to communicate to the touchscreen through cellular. If the cellular heartbeat is equal or less than the connection time-out, then cellular communication from the server to the touchscreen can fail.

## 8.3 Broadband/Cellular Connectivity Problems and Resolutions

Connectivity Problem	System Resolution
No alarm; touchscreen detects no cellular signal	<ol style="list-style-type: none"> <li>1. The touchscreen issues an alert over broadband to the Operator domain.</li> <li>2. If configured, the Operator domain sends an email and/or SMS alert to the customer.</li> </ol>
No alarm; Operator domain receives broadband heartbeat but no cellular heartbeat	Operator domain assumes cellular channel is down.
No alarm; touchscreen detects no connectivity with the router	<p><b>Note:</b> The touchscreen can detect whether it has lost connectivity with the router. It cannot know if the router has lost connectivity with the rest of the network or with the Internet.</p> <ol style="list-style-type: none"> <li>1. The touchscreen issues an alert over cellular UDP to the Operator domain that broadband is down.</li> <li>2. If configured, the Operator domain sends an email and/or SMS alert to the customer.</li> </ol>
No alarm; Operator Domain receives no broadband or cellular heartbeat within a configured amount of time	<ol style="list-style-type: none"> <li>1. Operator Domain assumes that the touchscreen has no broadband or cellular connectivity. When the touchscreen realizes it has lost connectivity with the Operator domain, it continuously attempts to reconnect.</li> <li>2. If configured, the Operator domain sends an email and/or SMS alert to the customer.</li> </ol>

Connectivity Problem	System Resolution
No alarm; Operator domain receives a cellular heartbeat but no broadband heartbeat	<p>A connectivity event is logged in the Database.</p> <p>The Operator domain:</p> <ol style="list-style-type: none"> <li>1. Sends a Broadband Down message to the touchscreen over cellular UDP if set by the cellular level of service. See the "Cellular Levels of Service" section in <i>Converge System Architecture Guide</i> for more information.</li> <li>2. If configured, sends an email and/or SMS alert to the customer.</li> </ol> <p>The touchscreen:</p> <ol style="list-style-type: none"> <li>1. Sends a heartbeat over cellular as soon as it realizes broadband is down</li> </ol> <p><b>Note:</b> This could take a little as a few seconds if the security router in the Home Domain, or—if the WAN or Internet service is lost—the time is based on the tier properties, potentially as long as 30.5 minutes (1830 seconds):</p> <pre>connection.broadbandHeartBeatRate + touchscreen.connection.serverResponseTimeout</pre> <ol style="list-style-type: none"> <li>2. Attempts to reconnect to the server over broadband TCP</li> <li>3. Displays a Broadband Connectivity alert (if configured to do so) until it reconnects with the server.</li> </ol>
During an alarm; touchscreen has broadband and/or cellular connectivity but receives no acknowledgment from the Application cluster	Touchscreen attempts to connect to the Back-up Alarm Server using broadband and cellular.
During an alarm; touchscreen has broadband and/or cellular connectivity and cannot connect to the Application cluster or the Back-up Alarm server.	Touchscreen continues attempting to connect to the Application cluster and the Back-up Alarm Server on broadband and cellular until the alarms are sent.
During an Entry Delay Period: Operator domain loses all connectivity with the touchscreen on broadband and cellular	If the server receives an Entry Delay alert, but no further alerts and the server has adequately determined that the touchscreen screen is not in commission, the server IMMEDIATELY sends <code>alarm.alarm.sendMessageAndGrab.contactId</code> to the central monitoring station.

## 8.4 Loss of Service Protocols

This section explains protocols during Operator system failure or when Subscriber CPEs lose total connectivity with the Application cluster(s).

### 8.4.1 Back-Up Alarm Server Fail-Over

#### CONVERGE ONLY

1. The touchscreen sends an alarm over broadband and cellular to the Application Cluster.
2. If an acknowledgment is not received in 30 seconds on either channel, the touchscreen attempts a UDP and then TCP connection over cellular (waiting 30 seconds on each attempt for an acknowledgment). If an acknowledgment is not received, the touchscreen assumes the Application cluster is down and fails-over to the Back-up Alarm server.
3. If the touchscreen fails over on both channels, then cellular and broadband alarms are sent out to the Backup Server, and alarm retries are sent only to the Back-up Alarm server.

**Note:** Cellular messaging to the Back-up Alarm server is limited to UDP only. The touchscreen will not attempt a full TCP connection over GPRS. For more information see the "UDP Activity" section in *System Operations Guide*.

4. The alarms continue to be resent to the Back-up Alarm server until the touchscreen receives ANY acknowledgment message (whether from the Application cluster or the Back-up Alarm server).
5. The system reverts back to the Application Cluster when any of the following occurs:
  - After 30 minutes has elapsed.
  - When the touchscreen receives an *Alarm Cancel* acknowledgment from the Application Cluster.
  - When the touchscreen receives an *Alarm Reset* acknowledgment from the Application Cluster.

### 8.4.2 Event History During Loss of Service

If the Home Domain loses connectivity to the Operator Domain, the previous 24 hours of event history is retained by the CPE. When connectivity to the Operator Domain is reestablished, the CPE device sends the last 24 hours of unsent events to Application Cluster.

### 8.4.3 System Recovery

The following describes Icontrol's recommended resolutions in the event of major server outages in the Server Cluster.

#### 8.4.3.1 Scenario 1:

Total system crash all servers in the Application cluster have gone down.

##### Resolution:

Before restoring the servers, set the load balancers to block all communication with the CPEs until all the servers in the cluster are back online. Otherwise, when the first server is brought online, all the CPE devices will attempt to connect to it at once (overloading that machine). Failing to connect, the CPE devices shift to the next server that is brought online. The result in that case is that none of the servers ever quite becomes fully operational.

#### 8.4.3.2 Scenario 2:

All servers did not go down, but enough did go down that the remaining servers are swamped with CPE requests.

##### Resolution:

Set the load balancers to block all new connections to the remaining servers. Restore connectivity only after enough servers are available to handle the new load per system capacity. For example, (assuming a system capacity of 50,000 subscribers per server) if there are 40,000 potential connections, only unblock new connections after at least two servers are available. This will ensure uninterrupted service even if one the servers goes down again.

# 9 Converge Touchscreen Connectivity

## CONVERGE ONLY

### 9.1 Connectivity Test

The Connectivity Test determines the connectivity over broadband and cellular. The test can be accessed from the touchscreen Settings app by tapping **Advanced Settings -> Connectivity -> Test Connectivity** or as part of the touchscreen installation and activation process.

The broadband connectivity test connects to port 5222 on TCP. It is functionally similar to running the `# telnet <ServerHost> 5222` command.

The cellular connectivity test also connects to port 5222 on TCP and is the functional equivalent of running the `"# telnet <cellularserverHost> 5222` command. This test also ensures the cellular modem can get on the network.

These connectivity tests do not test the application-level protocols. Therefore, they do not correlate to what is shown in the Management Portal for connectivity.

### 9.2 Signal Strength

The touchscreen graphically displays the detected signal strength of the following:

- Wi-Fi connection to the router
- GPRS/EDGE connection to the cellular network



Figure 15: Wi-Fi & Cellular Signal Strength Displays

This test does not determine whether the touchscreen is successfully communicating with the Operator Domain.

The number of bars in the Wi-Fi and Cellular graphics represents ranges of signal strength. The following tables explain how the Wi-Fi and cellular signal strengths are converted into the graphic displayed on the touchscreen.

Decibels	Percent Value	Bars
-80 to -85	20	1
-75 to -80	40	2
-70 to -75	60	3
-60 to -70	80	4
> -60	100	5
All other		0

Decibels	Indicator Value	Bars
-114 to -103	0 – 5	1
-102 to -91	6 - 11	2
-90 to -79	12 - 17	3
-78 to -67	18 - 23	4
-66 to -51	24 - 31	5
All other		0

### 9.3 Broadband and Cellular IP Addresses Must Be Different

Some customer environments have the same IP address for the cellular and broadband connections to the server. This is not allowed. It causes fluttering as the cellular channel adjusts the IP level routing on the touchscreen when connecting to the server over the cellular connection. While the touchscreen is connected by cellular only, it checks periodically to see if the broadband path is available again. If the broadband and cellular IP addresses are the same, it causes the touchscreen to think that broadband is available again, and attempt to establish a broadband connection. This leads to cellular fluttering.

### 9.4 SMCWBR14S-N4 (White Router) Router Reboot Attempt

When the touchscreen detects that the broadband connection is down, and the first broadband reconnection attempt fails, it attempts to remotely reboot the SMCWBR14S-N4 router. This is to work around an issue where the SMCWBR14S-N4 router sometimes fails to route traffic to the Internet correctly. Currently, this is only done for this particular router only.

# 10 Understanding Smash & Grab

## CONVERGE ONLY

### 10.1 Overview

The scenario of a Smash & Grab event is an intruder has entered the premise and destroyed the touchscreen in order to prevent an alarm. A Smash & Grab alarm is generated by the server when the server determines that the touchscreen is not in commission after it has received an Entry delay.

The system will only monitor for Smash & Grab events if the tier property `alarm.smashAndGrab.send` is set to **true**.

### 10.2 Determining That Smash & Grab Has Occurred

The server detects a Smash & Grab event when it receives an Entry Delay event from a touchscreen but does not receive an associated Alarm event or Disarm event within the configured window.

Mere connectivity loss during the Entry Delay period does not trigger a Smash & Grab as long as the Disarm or Alarm event was received by the server. Finally, it does not matter whether the Touchscreen has connectivity to the server only over the broadband or cellular channel.

When the application server detects a Smash & Grab event, it checks back a number of seconds for relevant Alarm and Disarm events that might have been received from the Touchscreen out-of-order. See [Smash & Grab Detection Custom Settings](#) below.

At default values, the maximum amount of time it can take for the server forward a Smash & Grab to the central monitoring station is **170 seconds**:

Entry Delay period (30 sec.)  
*plus* `checkSmashAndGrabEvent` scheduled task (20 sec.)  
*plus* `alarm.smashAndGrab.waitTime` (120 sec.)

For explanations of these periods, see [Touchscreen Settings](#) and [Smash & Grab Tier Properties](#) below.

#### 10.2.1 Touchscreen Settings

The **Entry Delay period** specifies how long the device will wait after an Entry/Exit zone has tripped before starting the alarm session. Default value is 30 seconds. It is accessed from the Settings menu using the Installer code.

To modify this value from the Settings menu tap **Security -> Entry And Exit Delay**.

## 10.2.2 Smash & Grab Tier Properties

Smash & Grab behavior can be configured by editing certain Tier properties at the Management Portal or by managing Entry Delay time periods from the Touchscreen. Tier properties for Smash & Grab settings are managed in the Management Portal by admin users. See *Management Portal Guide* for information about managing Tier properties.

### 10.2.2.1 `alarm.alarm.smashAndGrab.contactId`

The contact ID sent to the central monitoring station when the system detects a possible Smash & Grab scenario.

Value Type	Value Range	Default Value
string	N/A	113901001

### 10.2.2.2 `alarm.smashAndGrab.send`

Whether the system monitors for Smash & Grab scenarios (true means "yes").

Value Type	Value Range	Default Value
boolean	True/False	true

### 10.2.2.3 `alarm.smashAndGrab.waitTime`

After server has received an Entry Delay event, the amount of time (in seconds) in addition to the Entry Delay time to wait to receive an Alarm event or a Disarm event. After this time expires, the server sends the Smash & Grab contact ID (`alarm.alarm.smashAndGrab.contactId`). The default should not be decreased. This long period acknowledges the potentially longer time that might be required for the server to receive Alarm or Disarm event messages over the cellular channel.

Value Type	Value Range	Default Value
integer	Any positive integer	120

## 10.2.3 Smash & Grab Detection Custom Settings

These server properties manage the Smash & Grab detection behavior. They can be modified by adding them to the `custom.properties` file.

### 10.2.3.1 `alarm.smashAndGrabDisarmEventLookBackInterval`

If the application server suspects that a Smash & Grab event has occurred, this server property specifies how many seconds to look back for Disarm events that arrived from the touchscreen out-of-order (relative to Entry Delay events).

Value Type	Value Range	Default Value
Integer		60

### **10.2.3.2 *alarm.smashAndGrabAlarmLookBackInterval***

If the application server suspects that a Smash & Grab event has occurred, this server property specifies how many seconds to look back for recent alarm events that arrived from the touchscreen out-of-order (relative to Entry Delay events).

Value Type	Value Range	Default Value
Integer		300

## **10.3 Confirming a Smash & Grab Event (Cellular Ping)**

1. After the server determined a Smash & Grab has occurred, it sends an API request to the cellular provider's gateway URL and establishes an HTTP connection. This causes the cellular provider to send an SMS message to the touchscreen's cellular module.
2. The server waits 20 seconds (default) and sends another API request to the cellular provider to report whether they were able to send an SMS to the touchscreen's cellular module.

If the cellular provider can send an SMS ping to the touchscreen's cellular module, the server assumes that the device is still functioning and a Smash & Grab event has not occurred. The server then sends a 354 "Failure to communicate" event Contact ID (CID) to the central monitoring station.

If the cellular provider CANNOT send an SMS to the Touchscreen's cellular module, or the cellular provider's API is unavailable or takes longer than the wait time or fails for any other reason or the cellular provider's API takes longer than the wait time for any other reason, then the server sends the 139 "Smash & Grab" CID to the central monitoring station.

### 10.3.1 Smash & Grab Confirmation Custom Settings

These server properties manage the Smash & Grab confirmation behavior. They can be modified by adding them to the `custom.properties` file.

#### 10.3.1.1 `pingCellularUnit.implementation`

Specifies cellular provider of the Touchscreen's SIM card used for Smash & Grab confirmation.

Value Type	Value Range	Default Value
string	<b>dummyCellularUnitPingManager</b> Smash & Grab confirmation is not employed.  <b>numerexCellularUnitPingManager</b> Smash & Grab confirmation uses the implementation for Numerex as a cellular provider.  <b>numerexAttDuplexCellularUnitPingManager</b> Smash & Grab confirmation uses the implementation for Numerex and AT&T as cellular providers.	dummyCellularUnitPingManager

#### 10.3.1.2 `pingCellularUnit.numerex.accountId`

Specifies cellular provider's gateway account ID used for Smash & Grab confirmation. Only applicable if the `pingCellularUnit.implementation` is set to **numerexCellularUnitPingManager** or **numerexAttDuplexCellularUnitPingManager**.

Value Type	Value Range	Default Value
string	N/A	5033

#### 10.3.1.3 `pingCellularUnit.numerex.gateway.url`

Specifies cellular provider's gateway URL used for Smash & Grab confirmation. Only applicable if the `pingCellularUnit.implementation` is set to **numerexCellularUnitPingManager** or **numerexAttDuplexCellularUnitPingManager**.

Value Type	Value Range	Default Value
string	N/A	<a href="https://webservice.numerexpress.com/CWB/DCWS.asmx">https://webservice.numerexpress.com/CWB/DCWS.asmx</a>

#### 10.3.1.4 `pingCellularUnit.numerex.gateway.username`

Specifies cellular provider's gateway username used for Smash & Grab confirmation. Only applicable if the `pingCellularUnit.implementation` is set to **numerexCellularUnitPingManager** or **numerexAttDuplexCellularUnitPingManager**.

Value Type	Value Range	Default Value
string	N/A	icontrolwebservdev

### **10.3.1.5 pingCellularUnit.numerex.gateway.password**

Specifies cellular provider's gateway password used for Smash & Grab confirmation. Only applicable if the pingCellularUnit.implementation is set to **numerexCellularUnitPingManager** or **numerexAttDuplexCellularUnitPingManager**.

Value Type	Value Range	Default Value
string	N/A	Nw5b6Z8A

### **10.3.1.6 pingCellularUnit.numerex.new.cid**

Specifies the CID sent to the central monitoring station if, after *determining* that a Smash & Grab has occurred, the system fails to *confirm* that it has occurred. Only applicable if the pingCellularUnit.implementation is set to **numerexCellularUnitPingManager** or **numerexAttDuplexCellularUnitPingManager**.

Value Type	Value Range	Default Value
string	N/A	<p>135401001</p> <p>In the default value:</p> <p><b>1</b> means <i>a new event</i></p> <p><b>354</b> is the event code for "Failure to communicate event"</p> <p><b>01</b> is <i>the partition number</i></p> <p><b>001</b> is <i>the zone number</i></p>

### **10.3.1.7 pingCellularUnit.numerex.smsspingle.timeout.interval**

This server property sets the timeout value (in milliseconds) for the HTTP-based connection to Numerex's SMS ping proxy server. The Application servers use this connection to send SMS message pings and to check the status of the pings. If the output traffic to the Numerex gateway is blocked, after the timeout value has expired, the server responds with a *Failure to Send* exception code. Only applicable if the pingCellularUnit.implementation is set to **numerexCellularUnitPingManager**.

Value Type	Value Range	Default Value	Unit
Integer	Greater than zero.	60000 (that is, 60 seconds)	milliseconds

### **10.3.1.8 pingCellularUnit.numerex.waiting**

The maximum waiting time (in seconds) to check the return value of the SMS ping message call. Only applicable if the pingCellularUnit.implementation is set to **numerexCellularUnitPingManager**.

Value Type	Value Range	Default Value	Unit
Integer	20-30	20	seconds

#### **10.3.1.9 pingCellularUnit.att.gateway.url**

Specifies cellular provider's gateway URL used for Smash & Grab confirmation. Only applicable if the pingCellularUnit.implementation is set to **numerexAttDuplexCellularUnitPingManager**.

Value Type	Value Range	Default Value
String	N/A	https://api.jasperwireless.com/ws/service/Sms

#### **10.3.1.10 pingCellularUnit.att.gateway.username**

Specifies cellular provider's gateway username used for Smash & Grab confirmation. Only applicable if the pingCellularUnit.implementation is set to **numerexAttDuplexCellularUnitPingManager**.

Value Type	Value Range	Default Value
string	N/A	none

#### **10.3.1.11 pingCellularUnit.numerex.gateway.password**

Specifies cellular provider's gateway password used for Smash & Grab confirmation. Only applicable if the pingCellularUnit.implementation is set to **numerexAttDuplexCellularUnitPingManager**.

Value Type	Value Range	Default Value
string	N/A	none

#### **10.3.1.12 pingCellularUnit.att.licenseKey**

The license key assigned to access the unit. Only applicable if the pingCellularUnit.implementation is set to **numerexAttDuplexCellularUnitPingManager**.

Value Type	Value Range	Default Value	Unit
Integer	20-30	20	seconds

#### **10.3.1.13 pingCellularUnit.numerex.waiting**

The list of SIM ICCID prefixes (6 digits each) used to identify Numerex SIMs. Prefixes not listed in this property are assumed to be AT&T SIMs. Only applicable if the pingCellularUnit.implementation is set to **numerexAttDuplexCellularUnitPingManager**.

Value Type	Value Range	Default Value
string	n/a	890164

## 10.4 Smash & Grab Scheduled Tasks

The `ENTRY_DELAY_EVENT` is a temporary record of Entry Delay events. When the server receives an Alarm or Disarm event, the corresponding Entry Delay event is removed from the table.

In rare circumstances, the server receives the Entry Delay event after the Disarm event. To prevent false Smash & Grabs, the server checks for such out-of-order events, and does not add the Entry Delay event to the `ENTRY_DELAY_EVENT` table if any are found.

The `checkSmashAndGrabEvent` scheduled task runs on the server checks the `ENTRY_DELAY_EVENT` table to see if any Touchscreen has an expired Entry Delay. This scheduled task runs every 30 seconds.

## 10.5 Testing Smash & Grab

On the CPE servers, set

`fn.service.impl.NumerexAttDuplexCellularUnitPingManagerImpl` logging to debug. Watch for SMS communication by using `tail -f <server>.log | grep SMS`.

### To produce a Smash & Grab alarm:

1. Remove battery from the Touchscreen.
2. Ensure the value for `alarm.smashAndGrab.send` is **true** for the customer's tier.
3. Arm the customer's system.
4. Fault an Entry/Exit security zone (for example, open the front door).

*The Entry Delay countdown timer begins.*

5. Unplug the Touchscreen.
6. Let the Entry Delay period expire.
7. Let the `alarm.smashAndGrab.waitTime` value expire (default is 120 seconds) plus 20 seconds (`checkSmashAndGrabEvent` scheduled event).

**Note:** After the application server detects the Smash & Grab event, it checks back a number of seconds (`alarm.smashAndGrabAlarmLookBackInterval` value) for recent Alarm events that arrived from the touchscreen out-of-order (relative to Entry Delay events). It also checks back a number of seconds (`alarm.smashAndGrabDisarmEventLookBackInterval` value) for recent Disarm events that arrived from the touchscreen out-of-order (relative to Entry Delay events).

8. IF the `pingCellularUnit.implementation` value is set to **dummyCellularUnitPingManager** (default), then the system is NOT USING Smash & Grab confirmation.

The application server sends a Smash & Grab alarm  
(`alarm.alarm.smashAndGrab.contactId` tier property) to the central

monitoring station (default contact ID is 113901001).

IF the value is set to **numerexCellularUnitPingManager**, then the system is USING Smash & Grab confirmation with the Numerex cellular provider.

- a. The application server sends an API request to cellular provider's gateway server URL value (`pingCellularUnit.numerex.gateway.url`) with the customer's account ID (`pingCellularUnit.numerex.accountId`) and appropriate username and password (`pingCellularUnit.numerex.gateway.username` and `pingCellularUnit.numerex.gateway.password`).

This API request has the cellular provider send an SMS message to the touchscreen's cellular module.

- b. The application server waits the number of seconds set for `pingCellularUnit.numerex.waiting` (default: 20).
- c. The application server sends a different API request to cellular provider's gateway server URL value (see step a).

This API request has the cellular provider report whether it was able to send an SMS message to the touchscreen's cellular module.

- d. If the *SMS message send* was successful, the application server sends a Failure To Communicate CID (`pingCellularUnit.numerex.new.cid` custom property) to the central monitoring station (default:13540100).

If the *SMS message send* was NOT successful, the application server sends a Smash & Grab alarm (`alarm.alarm.smashAndGrab.contactId tier` property) to the central monitoring station (default contact ID is 113901001).

## 11 Alarm Delivery Error Handling

Ensuring the successful delivery of alarms to the central monitoring station is a critical part of the Icontrol system. In order to ensure that an alarm has been successfully handled, it is essential that your system is properly monitored for important error messages. See “Exception Codes” on page 89 for detailed descriptions of all relevant error codes potentially returned by the Icontrol system and an explanation of the messages that require close monitoring. However, any exception code in the Alarm subsystem should be closely monitored. For example, the following errors are logged when an alarm failed to reach the central monitoring station:

- ❑ "UCE-11002 alarm.expiredMessage" on page 197
- ❑ "UCE-11003 alarm.failedMessage" on page 197

For UCE-11002, Operations personnel with database access, must search the database for the "session\_cpe\_id" in the `session_cpe_id` field of the `alarm_session` table.

For UCE-11003, you should call the central monitoring station to see if alarm has been delivered, and alert them directly if necessary.

In either case, Operations personnel should triage the server to determine the cause of the error.

## 11.1 Custom Error Handling

You can also implement custom error handling logic to more closely monitor your system's alarm handling. For example, you can develop a listener to send an email alert to Operations personnel when alarms fail to be processed.

The **AlarmRequestErrorHandler** is a Java interface that service providers can implement to provide custom error handling logic for failed alarms.

```
package fn.service;
import fn.service.msg.jaxb.ArsCentralStationRequestMessage;
/**
 * Interface for alarm request error handling
 *
 */
public interface AlarmRequestErrorHandler
{
    /**
     *
     * @param acsr
     * @throws Exception
     */
    public void handle(ArsCentralStationRequestMessage acsr) throws
Exception;
}
```

**To create and install the AlarmRequestErrorHandler Java interface in your system:**

1. Develop the implementation class.
2. Declare the implementation class in the integration application context file (something descriptive such as requestErrorHandler).
3. Package the implementation java class into the integration.jar.
4. Deploy the jar file to each Application server node.
5. Add the following entry to custom.properties file:

```
alarm.requestErrorHandler=[the implementation class name as
defined in the integration application context file]
```

For example,

```
alarm.requestErrorHandler=requestErrorHandler
```

The following is a dummy implementation of the AlarmRequestErrorHandler Java interface:

```
package fn.service.impl;
```

```
import org.apache.commons.logging.Log;
import org.apache.commons.logging.LogFactory;
import com.ucontrol.common.java.exception.CodedExceptionHelper;
import com.ucontrol.common.java.text.MessageCatalog;
import fn.model.AlarmSession;
import fn.model.SecurityEvent;
import fn.service.AlarmRequestErrorHandler;
import fn.service.AlarmSessionManager;
import fn.service.SecurityEventManager;
import fn.service.msg.jaxb.ArsCentralStationRequestMessage;

/**
 * The default implementation of AlarmRequestErrorHandler that logs
 * alarm request failures.
 *
 */
public class AlarmRequestErrorHandler implements
AlarmRequestErrorHandler
{
    private static final MessageCatalog ERROR_MSGS =
MessageCatalog.getCatalogRelativeToClass("resources/ErrorMessages",
AlarmRequestErrorHandler.class);

    private Log log = LogFactory.getLog(getClass());
    private SecurityEventManager securityEventManager;
    private AlarmSessionManager alarmSessionManager;

    public void handle(ArsCentralStationRequestMessage arsMsg) throws
Exception
    {
        boolean logMsg = true;

        if (arsMsg.getArsSecurityAlarmIds().size() > 0) //always true
        {
```

```
SecurityEvent event =
this.securityEventManager.getSecurityEvent(Long.parseLong
(arsMsg.getArsSecurityAlarmIds().get(0)));

if (event != null && event.getAlarmSessionId() != null)
{
    AlarmSession as =
    this.alarmSessionManager.findById
    (event.getAlarmSessionId());

    if (as != null)
    {
        if (as.isErrorLogged())
            logMsg = false;
        else
        {
            as.setStatus
            (AlarmSession.Status.Complete
            d);
            as.setErrorLogged(true);
            this.alarmSessionManager.update
            AlarmSession(as);
        }
    }
}

if (logMsg)
    log.error(CodedExceptionHelper.getCodedMessageForKey(ERROR_MSGS, "alarm.failedMessage",
arsMsg.getArsCids().get(0), arsMsg.getCsAccountId()));

public void setSecurityEventManager(SecurityEventManager securityEventManager)
{
    this.securityEventManager = securityEventManager;
```

```
}

public void setAlarmSessionManager(AlarmSessionManager alarmSessionManager)
{
    this.alarmSessionManager = alarmSessionManager;
}

}
```

## 12 Understanding the Icontrol WSDL

This section describes the following elements of the Icontrol Web Service Definition Language.

- Methods & API Functions
- "Inputs" on page 134

### 12.1 Methods & API Functions

The Icontrol WSDL performs the following functions:

- Create a Subscriber Account on page 126
- Update Account Information on page 127
- Suspend Service of an Active Account on page 128
- Restore Service for a Suspended Account on page 129
- Deactivate an Account on page 129
- Delete an Unactivated Account on page 130
- Get Account Information on page 130
- Change Which Tier Is Assigned to an Account on page 131
- Add a Package to an Account on page 132
- Remove a Package from an Account on page 132
- Add a CPE Device to Inventory (Not Implemented) on page 133

### 12.1.1 Create a Subscriber Account

Account Creation adds a new subscriber account to the Icontrol system. It passes the account information and returns the Account ID (the account id in external system) as a response.

**IMPORTANT:** If Cluster Location Service (CLS) is not available, the create account operation will fail.

The SOAP operation is createAccount.

#### Request

Input Message (type)	Input element name	Input element Type
CreateAccountRequest (utp:AccountRequest)	account	ctp:Account See page 135.

#### Response

Output Message (type)	Output element name	Output Element Type
CreateAccountResponse (utp:BaseAccountResponse)	accountId	string

Figure 16: Management Portal: Account Data Entry Fields is an example of the new account data entry fields in the Management Portal:

★ Fields marked with a green star, required to create a database customer record  
 ▲ Fields marked with an orange triangle, required for activation of the customer

★First Name:	<input type="text"/>
★Last Name:	<input type="text"/>
★Address Street1:	<input type="text"/>
Address Street2:	<input type="text"/>
★Address City:	<input type="text"/>
★Address State:	<input type="text"/> AB
★Address Postal Code:	<input type="text"/>
Cross Street:	<input type="text"/>
Address Validation Key:	<input type="text"/>
Address Validation Flag:	<input type="checkbox"/>
★Address Timezone:	<input type="text"/> Canada/Atlantic
★TouchScreen Locale:	<input type="text"/> en
★Address Phone:	<input type="text"/> (format: 5126370909)
★Email Address:	<input type="text"/> pvttwo
Monitored:	<input checked="" type="checkbox"/>
Permit Required:	<input type="checkbox"/>
Secret Word:	<input type="text"/> .....
Confirm Secret Word:	<input type="text"/>
Primary Language:	<input type="text"/>
Special Instruction:	<input type="text"/>

Figure 16: Management Portal: Account Data Entry Fields

### 12.1.2 Update Account Information

Account Update changes a subscriber account already created in Icontrol system.

**IMPORTANT:** If Cluster Location Service (CLS) is not available, the update account operation will fail.

The SOAP operation is updateAccount.

Request		
Input Message (type)	Input element name	Input element Type
UpdateAccountRequest (utp:AccountRequest)	account	ctp:Account  See page 135.

Response		
Output Message (type)	Output element name	Output Element Type
UpdateAccountResponse (utp:BaseAccountResponse)	accountId	string

Figure 17: Account Data Entry Fields is an example of the Edit Account Information fields in the Management Portal that are displayed for not activated accounts. For activated accounts, the account details are updated on the Account Information screen (Figure 18: Account Information Screen)

The screenshot shows the uControl Management Portal interface. On the left, there is a detailed 'Edit Account Information' form with various fields for account creation and activation. On the right, the main dashboard displays account details (First Name: Demo, Last Name: Fourteen, Address: 78730, etc.) and a 'Change User Address' dialog box is open over the dashboard. The dialog box contains fields for 'Address 1' (5914 West Courtyard Dr.), 'Address 2' (Austin), 'City' (TX), 'State/Province' (TX), 'Postal Code' (78730), 'Deduction', 'External Reference', and 'Address Validation Flag'. A red box highlights the 'Change Address' button in the dialog box. The overall interface is dark-themed with green header bars.

Figure 17: Account Data Entry Fields

Figure 18: Account Information Screen

### 12.1.3 Suspend Service of an Active Account

Only accounts that have completed Activation or Activation A (*for Converge*) can be suspended.

When an account is suspended:

- All broadband and cellular connectivity between the CPE device and system server is disconnected.
- Events and alarms are not forwarded to the system servers.
- Email and SMS notifications are disabled.
- CPE device configuration changes are not sent to the system servers
- Account is not included in global connectivity reports. For example connectivity stats on the Dashboard will not include suspended accounts and queries based on connectivity will not include suspended accounts
- Account is still included in queries for activated accounts
- Account is not included in firmware updates
- Converge touchscreen apps can not be added or updated
- Customer does not have access to the Subscriber Portal

The SOAP operation is suspendAccount.

Request

Input Message (type)	Input Element Name	Input Element Type
SuspendAccountRequest (utp:IdRequest)	id (account id)	string

Response

Output Message (type)	Output element name	Output Element Type
SuspendAccountResponse (utp:BaseAccountResponse)	accountId	string

### 12.1.4 Restore Service for a Suspended Account

Accounts that have been suspended can be restored to normal service.

The SOAP operation is restoreAccount.

#### Request

Input Message (type)	Input element name	Input element Type
RestoreAccountRequest (utp:IdRequest)	id (account id)	string

#### Response

Output Message (type)	Output element name	Output Element Type
RestoreAccountResponse (utp:BaseAccountResponse)	accountId	string

### 12.1.5 Deactivate an Account

This operation is used when subscribers cancel their service. Deactivated accounts are considered deleted from the Icontrol system. They are not visible in the Management Portal or any reports. The information is not removed from the system databases.

This operation only affects activated accounts. If this message is directed to an unactivated account, nothing happens. See "[Delete an Unactivated Account](#)" on page 130.

The SOAP operation is deactivateAccount.

**IMPORTANT:** You can deactivate only one account at a time. This API does not support multiple concurrent operations.

#### Request

Input Message (type)	Input element name	Input element Type
DeactivateAccountRequest (utp:IdRequest)	id (account id)	string

#### Response

Output Message (type)	Output element name	Output Element Type
DeactivateAccountResponse (utp:BaseAccountResponse)	accountId	string

### 12.1.6 Delete an Unactivated Account

This operation is used to delete an account that is not yet activated in the Icontrol system. When an account is deleted, all the account information and history are removed from the system servers.

The SOAP operation is deleteUnactivatedAccount.

**IMPORTANT:** You can delete only one account at a time. This API does not support multiple concurrent operations.

#### Request

Input Message (type)	Input element name	Input element Type
DeleteUnactivatedAccountRequest (utp:DeleteUnactivatedAccountRequest)	id (account id)	string

#### Response

Output Message (type)	Output element name	Output Element Type
DeleteUnactivatedAccountResponse (utp:DeleteUnactivatedAccountResponse)	accountId	string

### 12.1.7 Get Account Information

This operation retrieves information from the database about an existing account.

The SOAP operation is getAccount.

#### Request

Input Message (type)	Input element name	Input element Type
GetAccountRequest (utp:IdRequest)	id (account id)	string

#### Response

Output Message (type)	Output element name	Output Element Type
GetAccountResponse (utp:AccountResponse)	account	ctp: <a href="#">FullAccount</a> See page 146.

### 12.1.8 Change Which Tier Is Assigned to an Account

**This operation is deprecated.** Use `updateAccountTierGroup` instead.

This operation changes the Tier to which an account is assigned.

For example, an account assigned to the `silver` Tier is changed to the `gold` Tier.

The SOAP operation is `updateAccountTier`.

Request

Input Message (type)	Input element name	Input element Type
UpdateAccountTierRequest (utp:UpdateTierRequest)	id (account id) tier	string ctp:Tier See page <a href="#">161</a> .

Response

Output Message (type)	Output element name	Output Element Type
UpdateTierRequest (utp:BaseAccountResponse)	accountId	string

### 12.1.9 Change Which Tier Group Is Assigned to an Account

This operation changes the Tier to which an account is assigned.

The SOAP operation is `updateAccountTierGroup`.

Request

Input Message (type)	Input Element Name	Input Element Type
UpdateAccountTierGroupRequest (utp:UpdateAccountTierGroupRequest)	id (account id) tierGroup	string string

Response

Output Message (type)	Output Element Name	Output Element Type
UpdateAccountTierGroupResponse (utp:UpdateAccountTierGroupResponse)	accountId	string

### 12.1.10 Add a Package to an Account

This operation adds a Package to an account.

The SOAP operation is addAccountGroup.

Request

Input Message (type)	Input element name	Input element Type
AddAccountGroupRequest (utp:AddAccountGroupRequest)	id (account id)	string
	group	string

Response

Output Message (type)	Output element name	Output Element Type
AddAccountGroupResponse (utp:AddAccountGroupResponse)	accountId	string

### 12.1.11 Remove a Package from an Account

This operation removes a Package from an account.

The SOAP operation is removeAccountGroup.

Request

Input Message (type)	Input element name	Input element Type
RemoveAccountGroupRequest (utp:RemoveAccountGroupRequest)	id (account id)	string
	group (package)	string

Response

Output Message (type)	Output element name	Output Element Type
RemoveAccountGroupResponse (utp:RemoveAccountGroupResponse)	accountId	string

### 12.1.12 Add a CPE Device to Inventory (Not Implemented)

This operation adds a CPE device to the inventory.

The SOAP operation is `createCpeInventory`.

Request

Input Message (type)	Input element name	Input element Type
CreateCpeInventoryRequest (utp:CreateCpeInventoryRequest)	cpeInventory	ctp:CpeInventory See page 141.

Response

Output Message (type)	Output element name	Output Element Type
CreateCpeInventoryResponse (utp:CreateCpeInventoryResponse)	cpelid	string

[Figure 19: Add New CPE Information Screen](#) is an example of the screen to add a CPE device to inventory in the Management Portal.

\* TouchScreen ID:  (format: 00185a010201)

Hardware Model:

Hardware Revision:

Serial Number:

IMEI Number:

ICC ID:

SIM Card Phone Number:

SIM Card Account Number:

Cellular Profile:

[Figure 19: Add New CPE Information Screen](#)

## 12.2 Inputs

The following are the available inputs:

- "Account" on page 135
- "AccountSourceType" on page 136
- "AccountStatus" on page 136
- "Address" on page 137
- "Camera" on page 138
- "Contact" on page 139
- "Cpe" on page 140
- "CpeInventory" on page 141
- "DeploymentModel" on page 143
- "DoorLock" on page 144
- "EmergencyContact" on page 145
- "EmergencyContactType" on page 145
- "FullAccount" on page 146
- "GenericDevice" on page 148
- "Lighting" on page 149
- "LightingType" on page 149
- "Locale" on page 150
- "Module" on page 151
- "ModuleType" on page 151
- "Peripheral" on page 152
- "PeripheralType" on page 153
- "Phone" on page 154
- "PhoneType" on page 154
- "PortalUser" on page 154
- "Premise" on page 155
- "Property" on page 156
- "Sensor" on page 157
- "SensorSourceType" on page 157
- "SensorType" on page 158
- "Thermostat" on page 160
- "ThermostatType" on page 160
- "Tier" on page 161
- "Understanding the Icontrol WSDL" on page 125
- "WidgetNameVersion" on page 162
- "Zone" on page 163
- "ZoneFunctionType" on page 163
- "ZoneType" on page 164

**Note:** The server property

`server.enableIntegrationLoggingThatWillWritePrivacyDataLogs` specifies whether to log input and output from the account integration webservice when the debug level is set to DEBUG. See "["server.enableIntegrationLoggingThatWillWritePrivacyDataInLogs" on page 287](#)" for more information on this server property.

## 12.2.1 Account

This complex data type contains the details of an account. This information is sent to the database during the [Create a Subscriber Account](#) operation (see page 126) and the [Update Account Information](#) operation (see page 127). The cardinality of all elements is 1.

Account Complex Data Type Elements

Complex Type Elements	Description	Element Type	Req'd?	Allowed Occurrences
accountID	A unique identification number assigned to the account in the external system	string	Yes	1
status	See the <a href="#">AccountStatus</a> simple data type on page 136.	ctp:AccountStatus	No	0..1
activationCode	Unique code that technician must input this code during activation. If not provided, Icontrol system will generate one automatically.	Long	No	0..1
deploymentName	The name of the Operator Domain instance of the account	string	No	0..1
firstName	First and last name of the account owner	string	Yes	1
lastName		string	Yes	1
phoneNumber	Phone number of the account premise	string	Yes	1
emailAddress	Contact email of the account.	string	No	0..1
<b>Required for Touchstone</b>				
specialInstruction	Additional instructions regarding the account for the installers and customer care	string	No	0..1
primaryLanguage	Primary language of the customer	string	No	0..1
address	See the <a href="#">Address</a> complex type on page 137.	ctp:Address	Yes	1
portalUsername <b>TOUCHSTONE ONLY</b>	The portal user name if known. This value is used to seed a portal user for Touchstone . Ignored if portalUserSSOId is provided.	string	No	0..1
portalUserSSOId <b>TOUCHSTONE ONLY</b>	The web SSO ID of a Touchstone portal user. Required if SSO is enabled.	string	No	0..1
product	The platform this account is going to use. If null, defaults to <i>converge</i> .	ctp:ProductName	No	0..1
tier	<b>Deprecated.</b> Use group instead.	ctp:Tier	N/A	0..1
group	Name of the Group to which this account is assigned. See <i>Management Portal Guide</i> for more information about groups.	string	Yes	0..16
internal	Whether the account is an internal account	boolean	Yes	1

Complex Type Elements	Description	Element Type	Req'd?	Allowed Occurrences
monitored	Whether the account should be monitored by central monitoring	boolean	Yes	1
centralStationAccountNumber	Assigned central monitoring station full account number (if not provided, depending in install, Icontrol system can obtain the number from the central monitoring station )	string	No	0..1
permitRequired	Whether the local emergency services require a permit for dispatching to the address	boolean	No	0..1
secretWord	Secret word for the account	string	No	0..1
timeZone	See the <a href="#">Understanding the Icontrol WSDL simple type on page 125</a> .	ctp:Under-standing the Icontrol WSDL	No	0..1
locale	See the <a href="#">Locale simple data type on page 150</a> .	ctp:Locale	No	0..1
emergencyContact	See the <a href="#">EmergencyContact complex type on page 145</a> .	ctp:EmergencyContact	No	0..n
property	Custom account property. See the <a href="#">Property complex type on page 156</a> .	ctp:Property	No	0..n
creator	Username of the Operations rep that added the account	string	Yes	1

### 12.2.2 AccountSourceType

This simple data type refers to the protocol method of a Sensor complex data type. See the [FullAccount](#) complex data type description on page 146.

AccountSourceType Simple Data Type Values

Values	Description
internal	Account created within Icontrol system
external	Account created via the web service interface

### 12.2.3 AccountStatus

This simple data type refers to the current status of an account. See the [Account](#) complex data type description on page 135, and the [FullAccount](#) complex data type description on page 146.

AccountStatus Simple Data Type Values

Values	Description	Platform(s)
new	Account that has unfinished data fields	Converge

Values	Description	Platform(s)
created	Account has the required fields completed, but has not been marked as Ready for Activation	Converge
readyForActivation	Account has been marked as Ready for Activation	Converge & Touchstone
activationAStarted	CPE device has been activated up to the point that the Activation Code and account Phone Number was entered at the touchscreen (for Converge) or the hub has been associated through use of serial number or MAC address (for Touchstone).	Converge & Touchstone
activationAEnd	CPE device is activated and the Activation email is sent to the subscriber, but the subscriber has not yet accessed the Subscriber Portal.	Converge
activationBStarted	Subscriber has accessed the Subscriber Portal, but has not set the login username and password.	Converge
activationBUsernameSet	The login username and password is set in the Subscriber Portal	Converge
activationBAlertStarted	Subscriber has started setting up rules.	Converge
activationBAlertEnd	User finished setting up rules.	Converge
activated	Account activation is complete	Converge & Touchstone

#### 12.2.4 Address

This complex data type contains the details of the premise location of an account. See the [Account](#) complex data type description on page [135](#), and the [FullAccount](#) complex data type description on page [146](#).

Address Elements

Complex Type Elements	Description	Element Type	Required?	Allowed Occurrences
address1	Street address of the premise location	string	Yes	1
address2	Additional address information of the premise address, such as suite or apartment number	string	No	0..1
city	The city location of the premise address	string	Yes	1
province	The state or province location of the premise address	string	Yes	1

Complex Type Elements	Description	Element Type	Required?	Allowed Occurrences
postalCode	The postal code/zip code of the premise address;  Accepts format nnnn or nnnnn-nnnn.	string	No	0..1
country	Country location of the premise address	string	No	0..1
direction	Information about the premise address to aid in locating it	string	No	0..1
externalReference	Service Provider's reference ID for the address	string	No	0..1
verified	Whether the address location has been verified.	boolean	Yes	1

### 12.2.5 Camera

This complex data type contains the details of a camera at an account premise.

See the [Premise](#) complex data type description on page [155](#).

Camera Elements

Complex Type Elements	Description	Element Type	Required?	Allowed Occurrences
id	Unique identifier assigned to the camera by the CPE device	string	Yes	1
name	Label of the camera assigned by the customer	string	Yes	1
macAddress	MAC address of the current camera	string	Yes	1
manufacturer	Manufacturer of the current camera	string	Yes	1
model	Model of the current camera	string	Yes	1
serialNumber	Serial number of the current camera	string	Yes	1
firmwareversion	Firmware version installed on the camera	string	Yes	1
hardwareVersion	Hardware version installed on the camera	string	Yes	1

## 12.2.6 Contact

This complex data type contains the details of a contact who can be added to an email or SMS alert for an account. See the [FullAccount](#) data type description page [146](#).

Contact Elements

Complex Type Elements	Description	Element Type	Required?	Allowed Occurrences
firstName	First and last name of the current emergency contact	string	Yes	1
		string	Yes	1
primary	Whether the current contact is the person named in the account	boolean	Yes	1
active	Whether the current contact is currently active	boolean	Yes	1
phone	See the <a href="#">Phone</a> complex type on page <a href="#">154</a> .	ctp: Phone	No	0..n
email	Email of the current user	string	No	0..n

## 12.2.7 Cpe

This complex data type contains the details of a CPE device at a subscriber premise. See the [Premise](#) complex data type description on page [155](#).

Cpe Elements

Complex Type Elements	Description	Element Type	Required?	Allowed Occurrences
cpelid	Unique CPE device ID of the device	string	Yes	1
name	Deprecated	string	No	0..1
deploymentModel	See the <a href="#">DeploymentModel</a> simple data type on page <a href="#">143</a> .	ctp: <a href="#">DeploymentModel</a>	Yes	1
serialNumber	Serial number of the device	string	No	0..1
manufacturer	Manufacturer of the CPE device	string	No	0..1
model	Model ID of the CPE device Hardware (such as P5, TCA200, etc.)	string	No	0..1
hardwareRev	Revision code of the CPE device	string	No	0..1
passPhrase <b>CONVERGE ONLY</b>	ID required for making certain sensitive changes to the CPE device	string	No	0..1
cellularProfileName <b>CONVERGE ONLY</b>	This value identifies a particular cellular account and its level of service	string	Yes	1
imeiNumber <b>CONVERGE ONLY</b>	Unique ID of the cellular device that the CPE device uses to connect to the cellular network	long	No	0..1
iccid <b>CONVERGE ONLY</b>	Unique ID for the SIM card used by the CPE device cellular device	string	No	0..1
simCardPhoneNumber <b>CONVERGE ONLY</b>	Phone number assigned to the CPE device's SIM card for two-way voice communication through the touchscreen	string	No	0..1
simCardAccountNumber <b>CONVERGE ONLY</b>	Account number that the cellular service provider associates with the CPE device's SIM card for two-way voice communication through the touchscreen	string	No	0..1
wifiMacAddress <b>CONVERGE ONLY</b>	Unique identifier assigned to the CPE device WiFi network adapter	string	No	0..1
firmwareVersion	Unique ID for the current firmware version installed on the CPE device	string	No	0..1
version	Name of firmware installed on the CPE device	string	No	1
widget <b>CONVERGE ONLY</b>	The list of widgets installed on the CPE device. See the <a href="#">WidgetNameVersion</a> complex type on page <a href="#">162</a> .	ctp: <a href="#">WidgetNameVersion</a>	No	0..n
module	The list of installed modules. See the <a href="#">Module</a> complex type on page <a href="#">151</a> .	ctp: <a href="#">Module</a>	Yes	1..2

### 12.2.8 CpeInventory

This complex data type contains the details of a CPE device inventory entry that is associated with an account. This information is sent to the database by the [Add a CPE Device to Inventory \(Not Implemented\)](#) operation (see page 133).

CpeInventory Complex Data Type Elements

Complex Type Elements	Description	Element Type	Required?	Cardinality
cpelid	Unique CPE device ID of the device	string	Yes	1
deploymentName	Name of the deployment to which the CPE device is assigned	string	Yes	1
serialNumber	Serial number of the CPE device	string	No	1
manufacturer	Manufacturer of the CPE device	string	No	1
model	Model ID of the CPE deviceHardware (such as P5, TCA200, etc.)	string	No	1
hardwareRev	Revision code of the CPE device	string	No	1
imeiNumber <b>CONVERGE ONLY</b>	Unique ID of the cellular device that the CPE device uses to connect to the cellular network	long	No	1
iccid <b>CONVERGE ONLY</b>	Unique ID for the SIM card used by the CPE cellular device	string	No	1
simCardPhoneNumber <b>CONVERGE ONLY</b>	Phone number assigned to the CPE device's SIM card for two-way voice communication through the touchscreen	string	No	1
simCardAccountNumber <b>CONVERGE ONLY</b>	Account number that the cellular service provider associates with the CPE device's SIM card for two-way voice communication through the touchscreen	string	No	1
wifiMacAddress <b>CONVERGE ONLY</b>	WiFi MAC address of the CPE device	string	No	1
firmwareVersion	Firmware version currently installed on the CPE device	string	No	1
passPhrase	ID required for making certain sensitive changes to the CPE device	string	No	1
module1Type	See the <a href="#">ModuleType</a> simple data type on page 151.	ctp: ModuleType	No	1
module1SerialNumber	Unique serial number of the ZigBee module1	string	No	1
module1FirmwareVersion	Firmware version currently installed on the ZigBee module1	string	No	1

Complex Type Elements	Description	Element Type	Required?	Cardinality
module1Manufacturer	ZigBee	string	No	1
module1Model	Model number of the ZigBee module1	string	No	1
module2Type	See the <a href="#">ModuleType</a> complex type on page <a href="#">151</a> .	ctp: <a href="#">ModuleType</a>	No	1
module2SerialNumber	Not currently applicable	string	No	1
module2FirmwareVersion		string	No	1
module2Manufacturer		string	No	1
module2Model		string	No	1

### 12.2.9 DeploymentModel

This simple data type refers to a CPE device's broadband connectivity method. See the [Cpe](#) complex data type description on page [140](#).

DeploymentModel Simple Data Type Values

Values	Description
ethernetMode	CPE device is connected to an undefined router by Ethernet cable
ethernetWithRouterSMC	CPE device is connected to an SMC WBR14S-N4 (white) router by Ethernet cable
ethernetWithRouterLinkSys	CPE device is connected to a Linksys (DOCSIS 2.x 8014-WN) router by Ethernet cable
ethernetWithMSOCPE	CPE device is connected to an MSO gateway device (modem) by Ethernet cable
wifiWithMSOCPE	CPE device is connected to an MSO gateway device (modem) by WiFi
wifiClientPskMode	CPE device is connected by WiFi to a router in PSK client mode
wifiClientPsk2Mode	CPE device is connected by WiFi to a router in PSK2 client mode
wifiClientWepMode	CPE device is connected by WiFi to a router in WEP client mode
wifiClientPskModeSMC	CPE device is connected by WiFi to an SMC WBR14S-N4 (white) router in PSK client mode
wifiClientPsk2ModeSMC	CPE device is connected by WiFi to an SMC WBR14S-N4 (white) router in PSK2 client mode
wifiClientWepModeSMC	CPE device is connected by WiFi to an SMC WBR14S-N4 (white) router in WEP client mode
wifiClientPskModeLinkSys	CPE device is connected by WiFi to Linksys DOCSIS 2.x 8014-WN (black) router in PSK client mode
wifiClientPsk2ModeLinkSys	CPE device is connected by WiFi to Linksys DOCSIS 2.x 8014-WN (black) router in PSK2 client mode
wifiClientWepModeLinkSys	CPE device is connected by WiFi to Linksys DOCSIS 2.x 8014-WN (black) router in WEP client mode
wifiApMode	CPE device is connected by WiFi to a router in API client mode
homeplugWithRouter	CPE device is connected to broadband via homeplug

### 12.2.10 DoorLock

This complex data type refers to a particular door lock paired with the CPE device. See the [Premise](#) complex data type description on page [155](#).

DoorLock Complex Data Type Values

Values	Description				
id	Unique identifier assigned to the door lock by the CPE device	string	No	0..1	
name	Label assigned to the door lock by the customer	string	No	0..1	
manufacturer	Manufacturer of the door lock	string	No	0..1	
serialNumber	Serial number of the	string	No	0..1	
model	Model number of the	string	No	0..1	
firmwareVersion	Firmware version ID	string	No	0..1	
hardwareVersion	Hardware version ID	string	No	0..1	

### 12.2.11 EmergencyContact

#### CONVERGE ONLY

The EmergencyContact complex data type contains the details of the emergency contacts, that is the persons that central monitoring calls when an alarm event occurs at the account premises to verify that an actual emergency event is occurring.. See the [Account](#) complex data type description on page [135](#), and the [FullAccount](#) complex data type description on page [146](#).

EmergencyContact Elements

Complex Type Elements	Description	Element Type	Required?	Allowed Occurrences
firstName	First and last name of the current emergency contact	string	Yes	1
lastName		string	Yes	1
secretWord	Secret word for the account	string	No	0..1
phone	See the <a href="#">Phone</a> complex type on page <a href="#">154</a> .	ctp:Phone	Yes	1
type	See the <a href="#">EmergencyContactType</a> simple data type on page <a href="#">145</a> .	ctp: EmergencyContactType	Yes	1

### 12.2.12 EmergencyContactType

#### CONVERGE ONLY

This simple data type refers to whether an account emergency contact must contacted to verify that an alarm is an authentic emergency or whether they is contacted to notify them that an alarm has occurred. See the [EmergencyContact](#) complex data type description.

The possible string values are:

- Verify
- Notify

### 12.2.13 FullAccount

This complex data type contains the details of an account. This information is returned by the [Get Account Information](#) operation (see page 130).

FullAccount Elements

Complex Type Elements	Description	Element Type	Required?	Allowed Occurrences
accountID	A unique identification number assigned to the account at the time of creation	string	Yes	1
status	See the <a href="#">AccountStatus</a> simple data type on page 136.	ctp:AccountStatus	Yes	1
activationCode	Unique code that is generated at the time an account is created; The Technician must input this code during activation.	long	No	1
deploymentName	The name of the Operator Domain instance used by the account	string	No	0..1
firstName	First and last name of the account owner	string	Yes	1
lastName		string	Yes	1
homePhone	Phone number of the account premise	string	Yes	1
mobilePhone	Mobile phone of the account	string	No	0..1
businessPhone	Business phone of the account	string	No	0..1
emailAddress	Contact email of the account	string	No	0..1
specialInstruction	Additional instructions regarding the account for the installers and customer care	string	No	0..1
primaryLanguage	Primary language of the customer	string	No	0..1
product	The platform this account uses	ctp:ProductName	No	0..1
tier	<b>Deprecated.</b> Use group instead.	ctp:Tier	Yes	1
group	Name of the Group to which this account is assigned. See <i>Management Portal Guide</i> for more information about groups.	strongUnderstanding the Icontrol WSDL	Yes	1..16
internal	Whether the account is an internal account (not a subscriber)	boolean	Yes	1
active	Whether the account is active. This flag is specifically modified during the <a href="#">Deactivate an Account</a> operation on page 129.	boolean	Yes	1

Complex Type Elements	Description	Element Type	Required?	Allowed Occurrences
suspended	Whether the account has been suspended. This flag is specifically modified during the following operations:  <a href="#">Suspend Service of an Active Account</a> (see page 128)  <a href="#">Restore Service for a Suspended Account</a> (see page 129)	boolean	Yes	1
readyForRMA	Whether the account has been marked for RMA	boolean	Yes	1
property	See the <a href="#">Property</a> complex type on page 156.	ctp:Property	No	0..n
user	See the <a href="#">PortalUser</a> complex type on page 154.	ctp:PortalUser	Yes	1..n
contact	See the <a href="#">Contact</a> complex type on page 139.	ctp:Contact	Yes	1..n
emergencyContact	See the <a href="#">EmergencyContact</a> complex type on page 145.	ctp:EmergencyContact	Yes	1..n
premise	See the <a href="#">Premise</a> complex type on page 155.	ctp:Premise	Yes	1
source	See the <a href="#">AccountSourceType</a> complex type on page 136.	ctp:AccountSourceType	Yes	1
creator	Username of the Operations rep that added the account to the system	string	Yes	1

### 12.2.14 GenericDevice

This complex data type refers to a particular generic (uncategorized) device paired with the CPE. See the [Premise](#) complex data type description on page [155](#).

GenericDevice Complex Data Type Values

Complex Type Elements	Description	Element Type	Required?	Allowed Occurrences
id	Unique identifier assigned to the generic device by the CPE	string	No	0..1
name	Label assigned to the generic device by the subscriber	string	No	0..1
uxCategory	UX Category name of the device.	string	No	0..1
manufacturer	Manufacturer of the generic device	string	No	0..1
model	Model number of the generic device	string	No	0..1
firmwareVersion	Firmware version ID of the generic device	string	No	0..1
hardwareVersion	Hardware version ID of the generic device	string	No	0..1

### 12.2.15 Lighting

This complex data type refers to a particular lighting/appliance device or in-wall switch paired with the CPE device. See the [Premise](#) complex data type description on page [155](#).

Lighting Elements

Complex Type Elements	Description	Element Type	Required?	Allowed Occurrences
id	Unique identifier assigned to the lighting module by the CPE device	string	Yes	1
name	Label assigned to the lighting module by the subscriber	string	No	0..1
type	See the <a href="#">LightingType</a> simple data type.	ctp: <a href="#">LightingType</a>	Yes	1
manufacturer	Manufacturer of the lighting module	string	No	0..1
serialNumber	Serial number of the lighting module	string	No	0..1
model	Model number of the lighting module	string	No	0..1
firmwareVersion	Firmware version ID	string	No	0..1
hardwareVersion	Hardware version ID	string	No	0..1

### 12.2.16 LightingType

This simple data type refers to a type of lighting device that can be paired with a CPE device. See the [Lighting](#) complex data type description on page [149](#).

LightingType Simple Data Type Values

Values	Description
onOffLight	A lighting module with only on-off options
dimmableLight	A lighting module with dimmable capability
onOffSwitch	An in-wall light switch with only on-off options
dimmableSwitch	An in-wall light switch with a dimming control

### 12.2.17 Locale

This simple data type refers to the language localization to which the information is being ported. See the [Account](#) complex data type description on page [135](#), and the [Premise](#) complex data type description on page [155](#).

Locale Simple Data Type Values

Values	Description
en	English
en_GB	English (Great Britain)
en_US	English (US)
fr	French
fr_FR	French (France)
fr_CA	French (Canada)
de	German
it	Italian
ja	Japanese
ko	Korean
zh_CN	Chinese (China)
zh_TW	Chinese (Taiwan)

### 12.2.18 Module

This complex data type contains the details of the ZigBee module installed in a CPE device. See the [Cpe](#) complex data type description on page [140](#).

Module Complex Data Type Elements

Complex Type Elements	Description	Element Type	Required?	Allowed Occurrences
slotNumber	Slot where the module is installed in the CPE device; Can be 1 or 2.	int	Yes	1
type	See the <a href="#">ModuleType</a> simple data type.	ctp: <a href="#">ModuleType</a>	Yes	1
serialNumber	Unique serial number of the module	string	No	0..1
firmwareVersion	Firmware version currently installed to the module	string	No	0..1
manufacturer	Manufacturer of the module	string	No	0..1
model	Model of the ZigBee module	string	No	0..1

### 12.2.19 ModuleType

This simple data type refers to the type of module used by the CPE device to communicate with the sensors. See the [Module](#) complex data type description on page [151](#), and the [CpelInventory](#) complex data type description on page [141](#).

ModuleType Simple Data Type Values

Values	Description
bosch	Not used
dect	Digital Enhanced Cordless Telecommunications
zigbee	ZigBee module without an integrated piezzo.  <b>Note:</b> This type is generally not used.
ZIP	ZigBee module with integrated piezzo
zwave	Z-Wave
keybus	Keybus

## 12.2.20 Peripheral

This complex data type contains the details of a key pad or key fob installed at a premise. See the [Premise](#) complex data type description on page [155](#).

Peripheral Elements

Complex Type Elements	Description	Element Type	Req'd?	Allowed Occurrences
id	Unique identifier assigned to the key pad or key fob by the CPE device	string	Yes	1
name	Label assigned to the peripheral by the customer	string	Yes	1
serialNumber	Serial number for the key pad or key fob	string	Yes	1
type	See the <a href="#">PeripheralType</a> simple data type description.	ctp: <a href="#">PeripheralType</a>	Yes	1
model	Model ID of the key pad or key fob	string	No	0..1
manufacturer	Manufacturer of the key pad or key fob	string	No	0..1
firmwareVersion	Firmware version of the key pad or key fob	string	No	0..1
hardwareVersion	Hardware version of the key pad or key fob	string	No	0..1

### 12.2.21 PeripheralType

This simple data type refers to a type of peripheral paired to a CPE device, such as a key fob, key pad, or siren/repeater. See the [Peripheral](#) complex data type description.

PeripheralType Simple Data Type Values

Values	Description
gateway	The system gateway.
router	The system router
keyfob	A mobile RF device that allows simple operations by pressing a button. Key fobs must be within RF range of the CPE device to work.
keypad	A Zigbee device that allow users to perform many of the CPE device functions from other parts of the premise.
siren	A Zigbee device that produces a loud siren when an alarm is tripped.
takeoverKeypad	A Panel Interface Module
wifiRepeater	A device that extends the range of the cameras
router	The system router
zigbeeVSMCT101_1Btn	Visonic 1 Button Remote
zigbeeVSMCT102_2Btn	Visonic 2 Button Remote
zigbeeVSMCT103_3Btn	Visonic 3 Button Remote
zigbeeVSMCT104_4Btn	Visonic 4 Button Remote
zigbeeVSMCT124_4Btn	Visonic Twin Button Remote
zigbeeVSMCT220EmerBtn	Visonic Emergency Button
zigbeeVSMCT241Pendant	Visonic Pendant

## 12.2.22 Phone

The Phone complex data type contains the details of a phone number of a contact (who can receive alerts), for *Converge systems*, or an emergency contact (who is contacted when an alarm is faulted). See the [Contact complex data type description on page 139](#), and the [EmergencyContact complex data type description on page 145](#).

Phone Elements

Complex Type Elements	Description	Element Type	Required?	Allowed Occurrences
number	A phone number (without hyphens)	string	Yes	1
type	See the <a href="#">PhoneType simple data type description</a> .	ctp: PhoneType	Yes	1

## 12.2.23 PhoneType

This simple data type refers to a phone type of a phone number of a contact. See the [Phone complex data type description](#). The possible string values are:

- Mobile
- Home
- Work
- Other

## 12.2.24 PortalUser

The PortalUser complex data type contains the details of a Management Portal or Subscriber Portal user. See the [FullAccount complex data type description on page 146](#).

PortalUser Elements

Complex Type Elements	Description	Element Type	Required?	Allowed Occurrences
username	Login username of the current user	string	Yes	1
password	Login password of the current user	string	Yes	1
email	Contact email address of the current user	string	Yes	1
primary	Whether the current user is the person named in the account	boolean	Yes	1
enabled	Whether the current user's Portal account is active	boolean	Yes	1

### 12.2.25 Premise

The Premise complex data type contains the details of the premise of an account. See the [FullAccount](#) complex data type description on page [146](#).

Premise Elements

Complex Type Elements	Description	Element Type	Required?	Allowed Occurrences
address	See the <a href="#">Address</a> complex data type on page <a href="#">137</a> .	ctp:Address	Yes	1
timeZone	See the <a href="#">Understanding the Icontrol WSDL</a> simple type on page <a href="#">125</a> .	ctp: Understanding the Icontrol WSDL	Yes	1
locale	See the <a href="#">Locale</a> simple data type on page <a href="#">150</a> .	ctp:Locale	Yes	1
centralStationAccountNumber	Assigned central monitoring station and its phone number	string	No	0..1
secretWord	Secret word assigned to the account;	string	Yes	1
permitRequired	Whether the security system requires a permit for the address	boolean	No	0..1
permitNumber	Permit number for the security system	string	No	0..1
expirationDate	Expiration date of the permit for the security system.	date	No	0..1
monitored	Whether the account is monitored by central monitoring	boolean	Yes	1
enabled	Deprecated	boolean	Yes	1
inTestMode	Whether the current account is in Test mode	boolean	Yes	1
camera	See the <a href="#">Camera</a> complex data type on page <a href="#">138</a> .	ctp:Camera	No	0..n
thermostat	See the <a href="#">Thermostat</a> complex data type on page <a href="#">160</a> .	ctp: Thermostat	No	0..n
lighting	See the <a href="#">Lighting</a> complex data type on page <a href="#">149</a> .	ctp:Lighting	No	0..n
doorLock	See the <a href="#">DoorLock</a> complex data type on page <a href="#">144</a> .	ctp:DoorLock	No	0..n
GenericDevice	See the <a href="#">GenericDevice</a> complex data type on page <a href="#">148</a> .	ctp:Gen- ericDevice	No	0..n

Complex Type Elements	Description	Element Type	Required?	Allowed Occurrences
peripheral	See the <a href="#">Peripheral</a> complex data type on page <a href="#">152</a> .	ctp:Peripheral	No	0..n
zone	See the <a href="#">Zone</a> complex data type on page <a href="#">163</a> .	ctp:Zone	Yes	1..n
cpe	See the <a href="#">Cpe</a> complex data type on page <a href="#">140</a> .	ctp:Cpe	Yes	1

## 12.2.26 ProductName

This simple data type lists the supported Icontrol platforms.

ProductName Simple Data Type Values

Values	Description
converge	Converge
insight	Touchstone

## 12.2.27 Property

This complex data type contains a custom key/value pair for an account. See the [Account](#) complex data type description on page [135](#), and the [FullAccount](#) complex data type description on page [146](#).

Property Elements

Complex Type Elements	Description	Element Type	Required?	Allowed Occurrences
key	Name of the property	string	Yes	1
value	Value of the property	string	Yes	1

## 12.2.28 Sensor

### CONVERGE ONLY

The Sensor complex data type contains the details of a sensor associated with a security zone. See the Zone complex data type description on page [163](#).

Sensor Elements

Complex Type Elements	Description	Element Type	Required?	Allowed Occurrences
id	Zone ID (number) assigned to the zone of the current sensor	int	Yes	1
type	See the <a href="#">SensorType</a> simple data type on page <a href="#">158</a> .	ctp: <a href="#">SensorType</a>	Yes	1
sourceType	See the <a href="#">SensorSourceType</a> simple data type description.	ctp: <a href="#">SensorSourceType</a>	No	0..1
serialNumber	Serial number of the sensor device	string	Yes	1
model	Model of the sensor device	string	No	0..1
manufacturer	Manufacturer of the sensor device	string	No	0..1
firmwareVersion	Firmware version of the sensor device	string	No	0..1
hardwareVersion	Hardware version of the sensor device	string	No	0..1

## 12.2.29 SensorSourceType

### CONVERGE ONLY

This simple data type refers to the protocol method of a Sensor. See the [Sensor](#) complex data type description.

SensorSourceType Simple Data Type Values

Values	Description
bosch	Not used
zigbee	ZigBee Sensor
hardwired	Not used
legacyAlarmPanel	A legacy alarm panel connected through an a Panel Interface

### 12.2.30 SensorType

#### CONVERGE ONLY

This simple data type refers to the type of sensor in a zone. See the [Sensor](#) complex data type description on page [157](#).

SensorType Simple Data Type Values

Values	Description	ModuleType
boschCoDetector	Not used	bosch
boschDoor	Not used	bosch
boschDUALMotion	Not used	bosch
boschGas	Not used	bosch
boschGlassBreak	Not used	bosch
boschHeat	Not used	bosch
boschInertia	Not used	bosch
boschLrPir	Not used	bosch
boschMiniDoor	Not used	bosch
boschPirMotion	Not used	bosch
boschRecessedDoor	Not used	bosch
boschSmoke	Not used	bosch
boschWater	Not used	bosch
drycontact	Not used	
gas	Not used	
glassBreak	Not used	
motion	Not used	
smoke	Not used	
water	Not used	
vibration	Not used	
zigbeeBigGEMotion	GE motion detector	zigbee
zigbeeCODetector	Carbon monoxide detector	zigbee
zigbeeDoorWindow	Not used	zigbee
zigbeeGECODetector	GE carbon monoxide detector	zigbee
zigbeeGlassBreak	Not used	zigbee
zigbeeInertia	Not used	zigbee
zigbeeMicroDoorWindow	Micro door/window sensor	zigbee

Values	Description	ModuleType
zigbeeMotion	Not used	zigbee
zigbeeMTLDoorWindow	Door/window sensor	zigbee
zigbeeMTLGECODetector	GE CO detector (MTL module)	zigbee
zigbeeMTLGEMotion	GE AP950W motion detector (MTL module)	zigbee
zigbeeMTLGlassBreak	MTL glass break sensor	zigbee
zigbeeMTLSmoke	MTL smoke detector	zigbee
zigbeeMTLSurenMotion	Suren motion detector (MTL module)	zigbee
zigbeeSmoke	SMC smoke detector	zigbee
zigbeeSMCCOSensor	SMC CO detector	zigbee
zigbeeSMCGlassBreak	SMC glass break detector	zigbee
zigbeeSMCMotion	SMC motion detector	zigbee
zigbeeSMCSmoke	SMC smoke detector	zigbee
zigbeeSMCSmokeNoSiren	SMC silent smoke detector	zigbee
zigbeeSurenRFMotion	Suren RF motion detector	zigbee
zigbeeVSCLIPMotion	Visonic CLIP motion detector	zigbee
zigbeeVSCO	Visonic MCT-442 CO detector	zigbee
zigbeeVSDDiscoveryK9_80Motion	Visonic K9-80MCW motion detector	zigbee
zigbeeVSDDiscoveryPIRMot	Visonic Discovery PIR motion detector	zigbee
zigbeeVSDDiscoveryQuad_80Mot	Visonic Discovery Quad motion detector	zigbee
zigbeeVSDoorWindow	Visonic MCT-320 door/window sensor	zigbee
zigbeeVSDW_1Wired	Visonic MCT-302 DW plus 1 Wired	zigbee
zigbeeVSFlood	Visonic flood detector	zigbee

Values	Description	ModuleType
zigbeeVSK9_85Motion	Visonic NEXT K9-85 motion detector	zigbee
zigbeeVSK940MCWMotion	Visonic K-940MCW motion detector	zigbee
zigbeeVSMCT100Universal	Visonic MCT-100 universal transmitter	zigbee
zigbeeVSMCT441Gas	Visonic MCT-441 gas detector	zigbee
zigbeeVSMCT501GlassBreak	Visonic MCT-501 glass break detector	zigbee
zigbeeVSMCT560Temp	Visonic MCT-560 temperature sensor	zigbee
zigbeeVSNextpK9_85Motion	Visonic Next+ K9-85 motion detector	zigbee
zigbeeVSSmoke	Visonic smoke detector	zigbee
zigbeeVSTower40MCWMot	Visonic Tower-40 motion detector	zigbee
zigbeeWater	Not used	zigbee

### 12.2.31 Thermostat

This complex data type refers to a particular temperature regulating device paired with the CPE device. See the [Premise](#) complex data type description on page [155](#).

Thermostat Elements

Complex Type Elements	Description	Element Type	Required?	Allowed Occurrences
id	Unique identifier assigned to the thermostat device by the CPE device	string	Yes	1
name	Label assigned to the thermostat by the customer	string	No	0..1
type	See the <a href="#">ThermostatType</a> simple data type.	ctp:ThermostatType	Yes	1
manufacturer	Manufacturer of the thermostat device	string	No	0..1
serialNumber	Serial number of the thermostat	string	No	0..1
firmwareVersion	Firmware version ID	string	No	0..1
hardwareVersion	Hardware version ID	string	No	0..1
model	Model id	string	No	0..1

### 12.2.32 ThermostatType

This simple data type refers to the type of temperature regulating. See the [Thermostat](#) complex data type description.

### ThermostatType Simple Data Type Values

Values	Description
thermostat	Device for controlling a central heating and air-conditioning system
radiatorValve	Device for controlling a radiator

### 12.2.33 Tier

**Deprecated.** Complex data types that use this type now use the `groups` value instead.

See the [Account](#) complex data type description on page [135](#), and the [FullAccount](#) complex data type description on page [146](#). This simple data type refers to the Tier-level of an account. This value can be modified by the [Change Which Tier Is Assigned to an Account](#) operation (see page [131](#)). The possible string values are:

- gold
- silver
- bronze
- test

### 12.2.34 Time Zone

This simple data type refers to the time zone of an account's premise.

See the [Account](#) complex data type description on page [135](#), and the [Premise](#) complex data type description on page [155](#).

The possible string values are:

- |                                      |  |  |   |
|--------------------------------------|--|--|---|
| <input type="checkbox"/> US/Eastern  | <input type="checkbox"/> Canada/Newfoundland | <input type="checkbox"/> Europe/London   | <input type="checkbox"/> Australia/Adelaide |
| <input type="checkbox"/> US/Central  | <input type="checkbox"/> Canada/Atlantic     | <input type="checkbox"/> Europe/Zurich   | <input type="checkbox"/> Australia/Darwin   |
| <input type="checkbox"/> US/Mountain | <input type="checkbox"/> Canada/Eastern      | <input type="checkbox"/> Europe/Helsinki | <input type="checkbox"/> Australia/Brisbane |
| <input type="checkbox"/> US/Arizona  | <input type="checkbox"/> Canada/Central      | <input type="checkbox"/> Asia/Shanghai   | <input type="checkbox"/> Australia/Sydney   |
| <input type="checkbox"/> US/Pacific  | <input type="checkbox"/> Canada/Mountain     | <input type="checkbox"/> Asia/Taipei     |   |
| <input type="checkbox"/> US/Alaska   | <input type="checkbox"/> Canada/Saskatchewan | <input type="checkbox"/> Asia/Calcutta   |   |
| <input type="checkbox"/> US/Aleutian | <input type="checkbox"/> Canada/Pacific      | <input type="checkbox"/> Asia/Tokyo      |   |
| <input type="checkbox"/> US/Hawaii   | <input type="checkbox"/> Canada/Yukon        | <input type="checkbox"/> Australia/Perth |   |

### 12.2.35 WidgetNameVersion

#### CONVERGE ONLY

This complex data type contains the details of a touchscreen app currently installed on a touchscreen.

See also the [Cpe](#) complex data type description on page [140](#).

WidgetNameVersion Elements

Complex Type Elements	Description	Element Type	Required?	Allowed Occurrences
name	Name of the touchscreen app	string	Yes	1
version	Installed version of the touchscreen app	string	Yes	1

## 12.2.36 Zone

### CONVERGE ONLY

This complex data type contains the details of a zone at a premise.

See the [Premise](#) complex data type description on page [155](#).

Zone Elements

Complex Type Elements	Description	Element Type	Required?	Allowed Occurrences
id	Number of the security zone	Int	Yes	1
name	Customer-assigned (or default) label of the security zone	String	Yes	1
type	See the <a href="#">ZoneType</a> simple data type on page <a href="#">164</a> .	ctp:ZoneType	Yes	1
functionType	See the <a href="#">ZoneFunctionType</a> simple data type on page <a href="#">163</a> .	ctp:ZoneFunctionType	Yes	1
sensor	See the <a href="#">Sensor</a> complex data type on page <a href="#">157</a> .	ctp:Sensor	Yes	1..n

## 12.2.37 ZoneFunctionType

### CONVERGE ONLY

This simple data type refers to the assigned function of a zone.

See the [Zone](#) complex data type description on page [163](#).

ZoneFunctionType Simple Data Type Values

Values	Description
entryExit	Entry/Exit zone If the system is armed, an alarm is sent if a valid key pad code is not entered.
Perimeter	Perimeter entryway If the system is armed, an alarm is sent immediately.
interiorFollower	Motion detector Monitors the internal living spaces of the premises and triggers an immediate alarm if the system is armed in Away mode. Not armed when the system is in Armed Stay mode.

Values	Description
troubleDayAlarmNight	If the system is armed, a zone fault issues a trouble message if it is faulted during the day and issues an alarm if it is faulted at night. Not used.
silent24Hr	Usually assigned to a zone containing an emergency button. Sends a report to the central station, but provides no keypad display or sound.
audible24Hr	Usually assigned to a zone containing an emergency
fire24Hr	Smoke detector
interiorWithDelay	Motion detector that initiates an Entry Delay if the system is armed.
interiorArmNight	Allows the use of a motion detector in Arm Night mode. The alarm trips immediately if motion is detected. This zone should be assigned to motion detectors that are placed in areas of low traffic, such as attics, basements, and garages.
interiorArmNightDelay	Provides a delay equal to the entry delay when the detector is tripped. This zone can be used in a high-traffic area.
monitor24Hr	A 24-hour inform motion detector The zone report faults to its sensors but will never trip an alarm.
inform24Hr	24-hour inform The zone report faults to its sensors but will never trip an alarm.
armSTAY	Only issues alarm if the system is armed in Arm Stay mode
armAWAY	Only issues alarm if the system is armed in Arm Away mode
disarm	Not used
noAlarmResponse	Not used.
silentBurglary	Not used.

### 12.2.38 ZoneType

#### CONVERGE ONLY

This simple data type identifies the of a zone at a premise.

See the [Zone](#) complex data type description on page [163](#).

Zone Elements

Simple Type Elements	Description
door	Doorway
window	Window opening
motion	Zone is faulted by detected motion
panic	When faulted this zone issues a police panic alarm when it is faulted
medical	When faulted this zone issues a medical panic alarm when it is faulted

Simple Type Elements	Description
environmental	When faulted
glassBreak	Zone is faulted at the sound of glass breaking
carbonMonoxide	Zone is faulted by the presence of carbon monoxide
duress	When faulted this zone issues a Duress alert.
smoke	Zone is faulted by the presence of smoke or heat
water	Zone is faulted by the presence of moisture
vibration	Zone is faulted by vibrations

## 13 Apache/WebLogic HealthCheck Service

This healthcheck service tests the health of your Apache and Weblogic instance.

You must have a login created and managed through the Management Portal with a systemMonitor role to access this tool.

Health Check URL: `https://[host]/ICHealthCheck/serverstatus`

The Health Check tests the following:

- Apache
- Apache's proxying to WebLogic
- Whether WebLogic is responsive
- Whether WebLogic has access to the database. This is performed by retrieving a Tier Property

**Note:** Upon success, this URL returns **OK** (http 200). If an error occurs, the URL returns a value of 500.

## 14 ICHealthCheck Service

The ICHealthCheck summary page provides a set of queries that determine the status of the server, database, accounts and other aspects of the Icontrol common architecture. You must have a login created and managed through the Management Portal with a systemMonitor role to access this tool.

Use the following URL to access the summary page:

```
https://<host>/mp/ICHealthCheckService?  
method=ichealthcheck.getSummaryPage
```

**To bypass the ICHealthCheck summary page and run a query directly:**

Use the following URL template:

```
https://<server>/mp/ICHealthCheck/ICHealthCheckService?method=ichealt  
hcheck.<QueryName>
```

for example:

```
https://<server>/mp/ICHealthCheckService?  
method=ichealthcheck.getLongestRunningSql
```

If the query requires parameters, then use the following URL template:

```
https://<server>/mp/ICHealthCheckService?method=ichealthcheck.<QueryN  
ame>&<Parameter1>=<Value1>&  
<Parameter2>=<Value2>
```

for example:

```
https://<server>/mp/ICHealthCheckService?  
method=ichealthcheck.getTotalEthernetLossAccounts&  
accounts=12&etherlosses=3&minutes=60
```

### 14.1 Accessing the ICHealthCheck Page and Queries

A user must be assigned the systemMonitor role to access the ICHealthCheck pages and run the queries. Refer to “Managing Employee Details” in *Management Portal Guide* for information about assigned roles.

#### 14.1.1 Test Messages Service

You can use the testMessages service to check the health of the email and SMS alert connectivity in your system. You must have a Management Portal account with the systemMonitor role to access the following URL: [https://\[host\]/ICHealthCheck/testMessages](https://[host]/ICHealthCheck/testMessages)

**To test your system's email functionality:**

1. Enter an email address in the **Send Test Email To** field.
2. Click **Send Email**. The system sends the following email message to the specified email address:  
This is a test email from ICHealthCheck webapp.

**To test your system's SMS functionality:**

1. Enter a phone number in the **Send Test SMS To** field.
2. Click **Send SMS**. The system sends the following text message to the specified phone number:  
This is a test SMS from ICHealthCheck webapp.

**Note:** If the service provider uses a short code for SMS messages instead of traditional phone number format, the recipient's phone number must allow short codes in order to receive the text message.

## 14.2 Configuring the ICHealthCheck

The following properties in the server.properties file pertain to the ICHealthCheck processes. See "[server.properties](#)" on page 235 for more information about these properties and overriding the defaults.

- ❑ database.userName
- ❑ serverStats.enabled
- ❑ serverStats.length

## 14.3 Query Details

The following subsections describe the queries available from the ICHealthCheckService.

A query with a Node scope retrieves the information from server memory. These queries use an insignificant level of production have very little affect on performance.

Most queries have a System scope. These retrieve the information from the database, and use more system resources.

### 14.3.1 getServerVersion

This ICHealthCheck query returns the server's build version.

Parameters	Scope	Suggested Frequency
None	Node	Hourly

### 14.3.2 getTotalEthernetLossAccounts

This ICHealthCheck query returns accounts that have broadband outages that exceed the specified number of etherlosses. It requires a full table scan of the security\_event table and creates a heavy load on the database.

Internal accounts are excluded from the search results.

Parameters	Scope	Suggested Frequency
accounts	System	Every two hours
etherlosses		
minutes		

### 14.3.3 getTopNTSRebootAccount

This ICHealthCheck query performs a full table scan of the cpe\_event table to find the accounts that exceed the specified number of CPE device reboots.

Internal accounts are excluded from the search results.

The value of parameter product can be Converge or Insight (defaults to Converge).

Parameters	Scope	Suggested Frequency
accounts	Systemget	Once every two hours
numberOfReboots		
type		
minutes		
product		

#### 14.3.4 getNumberOfAccountWithPowerLoss

This ICHealthCheck query retrieves the number of accounts with a power loss.

Internal accounts are excluded from the search results.

Parameters	Scope	Suggested Frequency
None	System	Hourly

#### 14.3.5 getListOfAccountWithPowerLoss

This ICHealthCheck query retrieves a list of accounts with a power loss.

Internal accounts are excluded from the search results.

Parameters	Scope	Suggested Frequency
count	System	Hourly

#### 14.3.6 getSQLStats

This ICHealthCheck query returns the following information:

- TopActiveSQLs  
Up to the top five active SQL queries for the ucontrol database user (if any found)
- LockedSessionSQLs  
All SQL sessions that are currently locked for the ucontrol database user (if any found).
- LongRunningSQLs  
Details of the longest currently running SQL queries for the ucontrol database user (if any found).

Parameters	Scope	Suggested Frequency
None	System	Hourly

#### 14.3.7 getTopSQLByGetsPerExecution

This ICHealthCheck query gets the list of top SQL queries based on GETS\_PER\_EXECUTION

Parameters	Scope	Suggested Frequency
size	System	Hourly

#### 14.3.8 getConnectedDeviceCount

This ICHealthCheck query retrieves the number of CPEs connected over TCP connections, either broadband or cellular. Internal accounts are excluded from the search results.

**Note:** Only run this query from a CPE node. Running this query from a portal node returns no data.

Parameters	Scope	Suggested Frequency
None	Node	Hourly

### 14.3.9 getNumberOfDataSyncPerDay

This ICHealthCheck query retrieves the number of data syncs per day.

Internal accounts are excluded from the search results.

Parameters	Scope	Suggested Frequency
None	System	Daily

### 14.3.10 getNumberOfDBLocks

This ICHealthCheck query retrieves the number of database locks.

Parameters	Scope	Suggested Frequency
totalMinutes	System	Hourly

### 14.3.11 findDBLocksDetails

This ICHealthCheck query retrieves the details of all database locks.

Parameters	Scope	Suggested Frequency
totalMinutes	System	Hourly

### 14.3.12 findSensComTroubleEventsByTimeRange

This ICHealthCheck query retrieves sensor communication trouble events within a given time range.

Parameters	Scope	Suggested Frequency
startDate	System	Hourly
endDate		
product		

### 14.3.13 getNumberOfAccountOfCellularTCPConnected

**CONVERGE ONLY**

This ICHealthCheck query retrieves the number of accounts with Cellular TCP connected.

Parameters	Scope	Suggested Frequency
None	System	Hourly

### 14.3.14 getPremisesWithHighCellConnection

#### **CONVERGE ONLY**

This ICHealthCheck query gets a list of premise IDs, the number of cellular TCP connections in the past given number of days with a minimum number of cellular TCP connections. The result is limited to by maxResults. If cellular service level is basic, this value should always be 0.

Parameters	Scope	Suggested Frequency
days	System	Daily
minCellTcpConnections		
maxResults		

### 14.3.15 getAccountCount

This ICHealthCheck query gets the account count using the specified criteria.

Parameters	Scope	Suggested Frequency
firstName	System	As needed
lastName		
primaryUserName		
postalCode		
activationCode		
accountStatus		
primaryPhoneNumber		
employeeExtReference		
csInSync		
deployment		

### 14.3.16 getConnectedPremiseCount

This ICHealthCheck query searches premises count based on connectivity and other factors.

**Note:** This query was previously named `getPremiseCountByFailureTypezipCodeCityAndState`.

Parameters	Scope	Suggested Frequency
broadbandOnline	System	Every four hours
cellularOnline		
anyChannelOnline		
zipCode		
city		
state		
deployment		

### 14.3.17 getRawBroadbandDownCountByZipCodeCityAndState

This ICHealthCheck query returns the raw Broadband Down count based on zip code, city, state and deployment parameters.

Parameters	Scope	Suggested Frequency
zipCode	System	Every four hours
city		
state		
deployment		

### 14.3.18 getDatabaseMonitorLogDetail

This ICHealthCheck query retrieves the database monitor log entries over a specified time span for one of the db\_monitor tables.

Parameters	Scope	Suggested Frequency
tableName	Node	Every 15 minutes
startDate		
endDate		
maximumLogs		

### 14.3.19 getDatabaseMonitorLog

This ICHealthCheck query returns the most recent database monitor logs and includes the average number of selects, inserts, and deletes over a 15 minute period.

Parameters	Scope	Suggested Frequency
maximumLogs	Node	Every 15 minutes

### 14.3.20 getConnectedNonActivatedCPECount

#### TOUCHSTONE ONLY

This ICHealthCheck query returns the number of currently connected non-activated Touchstone accounts.

Parameters	Scope	Suggested Frequency
None	Node	Hourly

### 14.3.21 getUDPIIncomingMessageQueueSize

This ICHealthCheck query retrieves the size of the UDP incoming message queue for CPE and portal servers.

Parameters	Scope	Suggested Frequency
None	System	Hourly

### 14.3.22 getUDPOutgoingMessageQueueSize

This ICHealthCheck query retrieves the size of the UDP outgoing message queue for CPE and portal servers.

Parameters	Scope	Suggested Frequency
None	System	Hourly

## 15 ICStatusCheck Service

The ICStatusCheck tool provides a set of queries that determine the status of the server, database, accounts and other aspects of the Icontrol common architecture. This is a logging framework to help monitor and diagnose the performance of the server. The stats can be monitored using a servlet, and are exposed via XML. Use the parameter ?html=true to expose stats by HTML as shown below.

Name	Value	Date Collected
com.icontrol.server.stats.alarmDelivery/14400/0	5	Wed Mar 13 15:00:00 CDT 2013
com.icontrol.server.stats.alarmDelivery/14400/0/avedur	46	Wed Mar 13 15:00:00 CDT 2013
com.icontrol.server.stats.alarmDelivery/14400/1	0	Wed Mar 13 11:00:00 CDT 2013
com.icontrol.server.stats.alarmDelivery/14400/2	0	Wed Mar 13 07:00:00 CDT 2013
com.icontrol.server.stats.alarmDelivery/14400/3	0	Wed Mar 13 03:00:00 CDT 2013
com.icontrol.server.stats.alarmDelivery/14400/4	0	Tue Mar 12 23:00:00 CDT 2013
com.icontrol.server.stats.alarmDelivery/14400/5	0	Tue Mar 12 19:00:00 CDT 2013
com.icontrol.server.stats.alarmDelivery/3600/0	2	Wed Mar 13 15:00:00 CDT 2013
com.icontrol.server.stats.alarmDelivery/3600/0/avedur	29	Wed Mar 13 15:00:00 CDT 2013
com.icontrol.server.stats.alarmDelivery/3600/1	1	Wed Mar 13 14:00:00 CDT 2013
com.icontrol.server.stats.alarmDelivery/3600/1/avedur	13	Wed Mar 13 14:00:00 CDT 2013

Stats are stored in memory and use a very small amount of memory to retrieve. However, this means:

- All stat data is lost when the server is restarted
- Stats are only applicable to a particular node – hitting the load balancer to get a stat will not get the result you expect.

### 15.1 Usage

You must have System Monitor privileges to access ICStatusCheck.

Use the following URL to return an XML page of all stats in the system

XML return:

`https://<host>/ICHealthCheck/ICStatusCheck`

HTML return:

`https://<host>/ICHealthCheck/ICStatusCheck`

To run a specific status check, use the following URL:

XML return:

`https://<server>/ICHealthCheck/ICStatusCheck?statname=<StatName>`

HTML return:

`https://<server>/ICHealthCheck/ICStatusCheck?statname=<StatName>?html=true`

## 15.2 Types

The status checks can be categorized as:

- Counters
- Stats in Time Buckets (page [176](#))
- Stats in Time Buckets and Average Duration (page [178](#))
- WebLogic JMX (page [178](#))

### 15.2.1 Counters

Name	Value	Date Collected
com.icontrol.server.stats.accountActivation/count	26	Wed Mar 13 14:28:31 CDT 2013

This status check type displays the present count of some value, such as the number of subscriber portal sessions or the number of account activations. The name is in the form: <statname>/count.

### 15.2.2 Stats in Time Buckets

Name	Name	Value	Date Collected
com.icontrol.server.stats.managementPortalLogouts/14400/0		6	Wed Mar 13 15:00:00 CDT 2013
com.icontrol.server.stats.managementPortalLogouts/14400/1		0	Wed Mar 13 11:00:00 CDT 2013
com.icontrol.server.stats.managementPortalLogouts/14400/2		0	Wed Mar 13 07:00:00 CDT 2013
com.icontrol.server.stats.managementPortalLogouts/14400/3		0	Wed Mar 13 03:00:00 CDT 2013
com.icontrol.server.stats.managementPortalLogouts/14400/4		0	Tue Mar 12 23:00:00 CDT 2013
com.icontrol.server.stats.managementPortalLogouts/14400/5		0	Tue Mar 12 19:00:00 CDT 2013

This status check type returns historical data about counts over time. The name is in the form: <statname>/<buckets of duration in seconds>/<bucket increment>.

### 15.2.2.1 Name

Each stat is displayed in *buckets* of time of the following various sizes:

com.icontrol.server.stats.managementPortalSessions/14400/0
com.icontrol.server.stats.managementPortalSessions/14400/1
com.icontrol.server.stats.managementPortalSessions/14400/2
com.icontrol.server.stats.managementPortalSessions/14400/3
com.icontrol.server.stats.managementPortalSessions/14400/4
com.icontrol.server.stats.managementPortalSessions/14400/5
com.icontrol.server.stats.managementPortalSessions/3600/0
com.icontrol.server.stats.managementPortalSessions/3600/1
com.icontrol.server.stats.managementPortalSessions/60/0
com.icontrol.server.stats.managementPortalSessions/60/1
com.icontrol.server.stats.managementPortalSessions/60/2
com.icontrol.server.stats.managementPortalSessions/60/3
com.icontrol.server.stats.managementPortalSessions/60/4
com.icontrol.server.stats.managementPortalSessions/600/0
com.icontrol.server.stats.managementPortalSessions/600/1
com.icontrol.server.stats.managementPortalSessions/600/2

- 14400 4 hours in seconds,  
6 bucket increments covering 24 hours
- 3600 1 hour in seconds,  
2 bucket increments covering two  
hours
- 600 (10 minutes in seconds),  
3 bucket increments covering 30  
minutes
- 60 (1 minute in seconds),  
5 bucket increments covering 5  
minutes

In the example to the left, /14400/0 refers to the current 4 hour time period. /14400/1 refers to the just previous 4 hour time period, and so on. So, if the server has been running for 8 hours and 1 minute, there are three 14400 buckets that contain data. The 0 14400 bucket only has 1 minute of data.

On the other hand, if the server has only been running for 360 seconds there is only one 14400 bucket that potentially contains any data at all (bucket 0). The same is true for the 3600, 600, and 60 buckets.

As each bucket is "filled", the 0 bucket data becomes 1 bucket data, and 1 bucket data becomes 2 bucket data, and so on. The last bucket (increment 5 for 14400 and increment 1 for 3600) drops off. If the data for 3600 drops off, you have to examine the data from 14400 to get that information.

### 15.2.2.2 Date Collected (or timestampCollected and dateCollected)

This date refers to the date/time of the end of each bucket increment. So, in the case of the 0 buckets, it is always a time later than the current time.

### 15.2.3 Stats in Time Buckets & Average Duration

Name
com.icontrol.server.stats.xmpp.homeAutomation.lightingStatus/14400/0/avedur
com.icontrol.server.stats.xmpp.homeAutomation.lightingStatus/14400/1
com.icontrol.server.stats.xmpp.homeAutomation.lightingStatus/14400/1/avedur
com.icontrol.server.stats.xmpp.homeAutomation.lightingStatus/14400/2

This status check type returns the average of all the values for each instance *in milliseconds* and *per bucket*. The name is in the form: <statname>/<window duration in seconds>/<window number>/avedur.

For example:

com.icontrol.server.stats.xmpp.broadbandHeartbeat/60/0	3
com.icontrol.server.stats.xmpp.broadbandHeartbeat/60/0/avedur	15

This means that less than 1 minute ago the server had 3 broadband heartbeats averaging 15 ms.

### 15.2.4 WebLogic JMX

This status check type returns a simple value from WebLogic JMX stats regularly.

## 16 Healthcheck Configuration

Interval time  (that is, how often to send a probe to the server)	5 (seconds)
Timeout value  (that is, time to receive a reply from the server acknowledging a probe)	5 (seconds)
Number of times before marking a server down	2
Number of times before marking a server back up	2
What to do if a server is marked down	Tear down connections
Number of connections per second	25500

The screenshot shows the A10 Networks AX2500 / AX5000 configuration interface. The top navigation bar includes the A10 Networks logo, model information (AX2500 / AX5000), HA status (Not Configured), Save, Logout(admin), and Help buttons.

The main menu on the left has sections for Monitor Mode and Config Mode, with Get Started selected. Under Service, the Health Monitor option is highlighted. Other service options include SLB, Template, ManagementPortal, ping, ServerStatus, SubscriberPortal, TCP-Port-5038-Check, TCP-Port-5222-Check, and UDP-Port-9091-Check.

The central pane displays the Health Monitor configuration. It shows a table of nine configured health checks:

Name	Type	Retry	Consec Pass Req'd	Interval(Seconds)	Timeout(Seconds)
5222CompoundCheck	Compound	2	1	12	12
Compound-Check	Compound	2	1	5	5
ManagementPortal	HTTPS	2	1	5	5
ping	ICMP	2	1	5	5
ServerStatus	HTTPS	2	1	5	5
SubscriberPortal	HTTPS	2	1	5	5
TCP-Port-5038-Check	TCP	2	1	5	5
TCP-Port-5222-Check	TCP	2	1	5	5
UDP-Port-9091-Check	UDP	2	1	5	5

At the bottom of the configuration pane, there are buttons for Select, Unselect, Add, and Delete.

**A10 Networks** AX2500 / AX2500 HA: Not-Configured Save Logout(admin) Help

Monitor Mode Config Mode

Get Started >

Service >

- » SLB
- » Template
- » **Health Monitor**
- » PBSLB
- » Firewall
- » GSLB
- » aFlex
- » IP Source NAT
- » SSL Management

Network >

System >

HA >

Health Monitor >> **Health Monitor** >> ServerStatus

**Health Monitor**

Name: *	ServerStatus
Retry:	2
Consec Pass Req'd:	1
Interval:	5 Seconds
Timeout:	5 Seconds
Strictly Retry:	<input type="checkbox"/>
Disable After Down:	<input type="checkbox"/>

**Method**

Override IPv4:	
Override IPv6:	
Override Port:	
Method:	<input checked="" type="radio"/> Internal <input type="radio"/> External
Type:	HTTPS
Port:	443
Host:	
URL:	GET /managementPortal/se
User:	
Password:	
Expect:	OK
Maintenance Code:	<input checked="" type="radio"/> Text <input type="radio"/> Code

**OK** **Cancel**

**A10 Networks** AX2500 / AX2500 HA: Not-Configured Save Logout(admin) Help

Monitor Mode Config Mode

Get Started >

Service >

- » SLB
- » Template
- » **Health Monitor**
- » PBSLB
- » Firewall
- » GSLB
- » aFlex
- » IP Source NAT
- » SSL Management

Network >

System >

HA >

Health Monitor >> **Health Monitor** >> TCP-Port-5222-Check

**Health Monitor**

Name: *	TCP-Port-5222-Check
Retry:	2
Consec Pass Req'd:	1
Interval:	5 Seconds
Timeout:	5 Seconds
Strictly Retry:	<input type="checkbox"/>
Disable After Down:	<input type="checkbox"/>

**Method**

Override IPv4:	
Override IPv6:	
Override Port:	
Method:	<input checked="" type="radio"/> Internal <input type="radio"/> External
Type:	TCP
Port: *	5222
HalfOpen:	<input checked="" type="radio"/> False <input type="radio"/> True

**OK** **Cancel**

## 16.1 Modify each server to use the 5222CompoundCheck on port 5222

The screenshot shows the A10 Networks AX2500 / AX2500 configuration interface. The top navigation bar includes 'Save', 'Logout(admin)', and 'Help'. The main menu on the left has sections for 'Monitor Mode', 'Config Mode', 'Get Started', 'Service' (selected), 'Network', 'System', and 'HA'. Under 'Service', 'SLB' is selected, showing options like SLB, Template, Health Monitor, PBSLB, Firewall, GSLB, aFlex, IP Source NAT, and SSL Management.

The 'Server' tab is active in the top navigation bar. The 'General' configuration for 'App1' is displayed, including fields for Name (App1), IP Address/Host (10.0.6.83), Weight (1), Health Monitor (Compound-Check), Status (Enabled), Connection Limit (8000000), and Server Template (default). A 'Description' field is also present.

The 'Port' configuration table is shown below. It lists ports 443, 5222, 9091, and 8080. For port 5222, the 'Protocol' is TCP, 'CL' is 8000000, 'CR' is 1, 'W' is 1, 'No SSL' is checked, 'SPT' is default, 'HM' is Compound-Check, and 'SD' is Enabled. The row for port 5222 is circled in red.

	Port	Protocol	CL	CR	W	No SSL	SPT	HM	SD
<input type="checkbox"/>	443	TCP	8000000	1	1	<input checked="" type="checkbox"/>	default	Compound-Check	<input checked="" type="checkbox"/>
<input type="checkbox"/>	5222	TCP	8000000	1	1	<input checked="" type="checkbox"/>	default	5222CompoundCheck	<input checked="" type="checkbox"/>
<input type="checkbox"/>	9091	UDP	8000000	1	1	<input checked="" type="checkbox"/>	default	UDP-Port-9091-Check	<input checked="" type="checkbox"/>
<input type="checkbox"/>	8080	TCP	8000000	1	1	<input checked="" type="checkbox"/>	default		<input checked="" type="checkbox"/>

Buttons at the bottom include 'OK' and 'Cancel'.

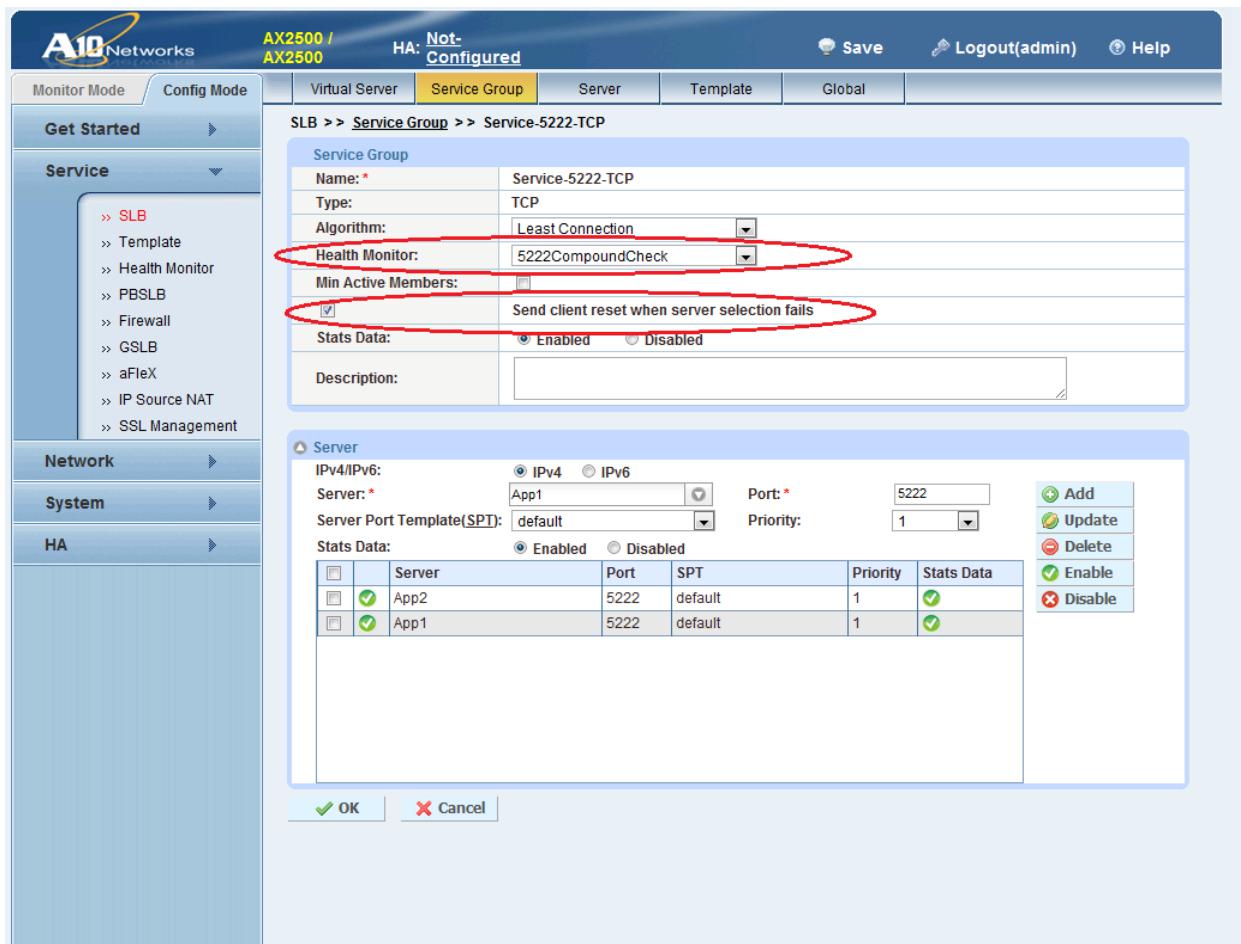
### 16.1.1 Create a Compound Healthcheck

Create a compound health check that checks not only that port 5222 is available, but also that Weblogic managementPortal is returning **OK** on its health check (<https://<host>/ICHealthCheck/serverstatus>).

Name:	5222CompoundCheck	
Retry:	2	
Consec Pass Req'd:	1	
Interval:	5	Seconds
Timeout:	5	Seconds
Strictly Retry:	<input type="checkbox"/>	
Disable After Down:	<input type="checkbox"/>	
<b>Method</b>		
Override IPv4:		
Override IPv6:		
Override Port:		
Method:	<input checked="" type="radio"/> Internal <input type="radio"/> External	
Type:	Compound	
Boolean Expression: <sup>*</sup>		
( Reverse Polish Notation, e.g. sub ping sub <my_hm> and )		
<input checked="" type="radio"/> ping <input type="radio"/> or sub ServerStatus sub TCP-Port-5222-Check and <span style="float: right;"> <input type="button" value="Add"/> <input type="button" value="Clear"/> </span>		
<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

## 16.2 Configure the TCP port 5222 Service Group

Configure the TCP port 5222 Service Group to use the 5222CompoundCheck and to send client reset when server selection fails.



## 17 Management Portal Roles and Privileges

Each Management Portal user is assigned a role that grants certain privileges in the Management Portal. For more information about roles and privileges, see the "Management Portal Roles" section in *Management Portal Guide*.

# 18 CPE Statistics Collection and Reporting

## CONVERGE ONLY

The Icontrol system has the ability to collect information from CPE devices that can be used to proactively identify issues and aid in trouble analysis. The system provides reports that collect data samples at regular intervals, then uploads the data to the server. The server then inserts the data into the system database for subsequent analysis and viewing.

### 18.1 Enabling Statistics Collection

For the server to know about the reports supported in the CPE devices, the firmware image must be loaded into the Management Portal. The server reads the report specification file, which is inside the firmware image , then creates the appropriate tables in the database. If you do not perform this step, the server will simply ignore all report data uploaded to it.

By default, touchscreen statistics are not collected. To enable this feature on a single CPE device, the `logging.debug advanced` property must be set to true from the Management Portal. (Click **Advanced > Advanced Properties** to set this property.) This feature cannot be enabled globally.

Each report has common configuration options with defaults defined as follows:

Option	Description
<code>status</code>	One of the following:  on - Statistics are always collected  off - Statistics are not collected  debug - Statistics are collected only when the <code>logging.debug advanced</code> property is set to true for the CPE devices. This is the default value.
<code>sampleFrequency</code>	The time, in milliseconds, between each sample. The smaller the number, the more data is collected. This has an impact on the device's resources (CPU, Flash) as well as the amount of data uploaded to the server.
<code>uploadFrequency</code>	The time, in milliseconds, between report generations and uploads to the server. Smaller numbers will result in smaller datasets uploaded to the server, but overall server impact would be higher due to more frequent uploads. Care must be taken to not set this too low and also to consider the overall server impact when large numbers of devices have reports enabled.  The time span is calculated from the last reboot of the CPE devices.
<code>historicalDataWindow</code>	The age, in milliseconds, of data to keep in the device's sample database. Larger numbers will retain more data for analysis in diagnostic file uploads, but will consume more flash space on the device.

## 18.2 Available Reports

The following reports are each configured to run only if the device is in debug logging mode :

- BatteryStats
- CommStats
- SystemStats
- ZigbeeTroubleStats

### 18.2.1 BatteryStats

The BatteryStats report collects basic details on the state of the main system battery at each sample interval. The data collected in each sample contains:

- Timestamp (in UTC milliseconds)
- State ("Charging", "Full", etc.)
- Voltage (in microvolts)
- Temperature (in Celsius)

**Note:** State changes in-between samples will not be noticed (for example, a brief "Charging" state).

This report's default configuration is:

```
status = debug
sampleFrequency = 3600000
uploadFrequency = 86400000
historicalDataWindow = 86400000
```

## 18.2.2 CommStats

The CommStats report collects details related to connectivity (broadband, cellular, and WiFi). The data collected in each sample contains:

- ❑ Timestamp (in UTC milliseconds)
- ❑ Average server response time to a broadband heartbeat request
- ❑ Number of times Wi-Fi was lost
- ❑ Number of times cellular was lost
- ❑ Wi-Fi signal strength (in dBm)
- ❑ Cellular signal strength (in dBm)
- ❑ Number of bytes transmitted over cellular
- ❑ Number of bytes received over cellular
- ❑ Number of InitialInforms sent over broadband
- ❑ Number of InitialInform responses received over broadband
- ❑ Number of InitialInforms sent over cellular
- ❑ Number of InitialInform responses received over cellular
- ❑ Note that these counters will reset after a device reboot.

This report's default configuration is:

```
status = debug
sampleFrequency = 3600000
uploadFrequency = 86400000
historicalDataWindow = 86400000
```

### 18.2.3 SystemStats

The SystemStats report collects various system related details about the device. The data collected in each sample contains:

- ❑ Timestamp (in UTC milliseconds)
- ❑ Available memory (in bytes).
- ❑ System partition usage (percentage full)
- ❑ Data partition usage (percentage full)
- ❑ Cache partition usage (percentage full)
- ❑ Opt partition usage (percentage full)

This report's default configuration is:

```
status = debug
sampleFrequency = 43200000
uploadFrequency = 86400000
historicalDataWindow = 2592000000
```

### 18.2.4 ZigbeeTroubleStats

The ZigbeeTroubleStats report collects various counters about Zigbee troubles. The data collected in each sample contains:

- ❑ Timestamp (in UTC milliseconds)
- ❑ Number of devices that reported a low battery trouble
- ❑ Number of devices that reported being tampered
- ❑ Number of devices identified as being in communication failure

This report's default configuration is:

```
status = debug
sampleFrequency = 3600000
uploadFrequency = 86400000
historicalDataWindow = 86400000
```

The counters will reset after a reboot.

## 18.3 Customizing the Reports

Customizing a report requires SSH access to the CPE device. Contact your Icontrol representative for more information.

## 19 Log Files

The operator should monitor the Application cluster server logs for any occurrence of the pattern “UCE-XXXXX” which identify errors (error, warning, or fatal).

The server log file is stored at the following location:

```
/ [BEA_INSTALL_DIR]/user_
projects/domains/ucontrol/servers/AdminServer/logs/
```

Each log message is presented in the following format:

```
##<date time zone> <log level> <subsystem> <servername>
<wl name> <thread> <><owner>> <weblogic internal marker> <timestamp>
<weblogic message id> <message threshold -message text>
```

The following table explains the meaning of each element in the Log message format.

Log Message Elements

Element	Description
<date time zone>	The date/time of the log file based on the Application Cluster or Back-up Alarm server that registered it. This tag provides the following information about log: The date, time (in 12 hour format), AM or PM, and the time zone (such as EST for Eastern Standard Time or CST for Central Standard Time).  For example:  Dec 7, 2009 10:57:06 AM CST
<log level>	Error level of the log. For example: Warning, Error, Critical, Alert, Emergency, Debug
<subsystem>	Subsystem reporting the log;  For example, <i>socket</i> , <i>security</i> , or <i>ucontrol</i> (ear)
<servername>	OS machine name of the reporting server
<wl name>	WebLogic machine name of the reporting server
<thread>	Log thread
<owner>	Owner of the current log thread
<weblogic internal marker>	Not applicable
<timestamp>	Timestamp of the current log message in milliseconds since January 1, 1970.
<weblogic message id>	A unique ID assigned to each message by the WebLogic application.
<message threshold – message text>	A category for the event and a message generally describing the event.

### 19.1 Example Log Messages

See "Exception Codes (UCE)" on page 190 for a complete catalog of exception code messages.

Error Message 11000

**Note:** Support for telephony servers has been deprecated.

---

```
<Jun 24, 2010 11:21:07 AM EDT> <Error> <ucontrol> <BEA-000000>
<fn.service.impl.AlarmTelephonyRequestManagerImpl - UCE-11000 - The
alarm message with CID 0025181137000007 for account 18-01-0025 failed
to reach central for 3 minutes. Will keep trying for 56 minutes. >
```

#### Error Message 14008

```
<Jun 29, 2010 3:48:38 PM EDT> <Warning> <ucontrol> <BEA-000000>
<fn.service.impl.AccountManagerImpl - UCE-14008 - The touch screen
0026f300021c is already used by exr170989.>
```

#### Error Message 14601

```
<Jul 7, 2010 3:22:19 PM EDT> <Error> <ucontrol> <BEA-000000>
<fn.service.impl.GprsMessageManagerImpl - UCE-14601 - Unsupported
gprs message version 0>
```

#### Error Message 21001

**Note:** Support for telephony servers has been deprecated.

```
<Jun 24, 2010 11:26:42 AM EDT> <Warning> <ucontrol> <BEA-000000>
<fn.service.impl.AlarmTelephonyRequestManagerImpl - UCE-21001 - A
timeout has occurred for telephony request 288761. Returning to queue
for reprocessing.>
```

#### Error Message 22222

```
<Jul 6, 2010 8:57:28 PM EDT> <Warning> <ucontrol> <BEA-000000>
<fn.service.impl.RogersSmsSender - UCE-22222 - Failed to send Rogers
sms message to 15063335555>
```

#### Error Message 24100

```
<Jul 7, 2010 12:04:32 PM EDT> <Warning> <ucontrol> <BEA-000000>
<fn.xmpp.v2.IQSMAPHandler - UCE-24100 - Server exception while
processing SMAP message '/cpe/dataSync' from '242@xmpp/00185a0280c4'>
```

## 19.2 Debugging Information

To filter out all single device debugging logs from a given account/premise that includes CSMAP information, run a command similar to the following. In this example, the CpeID is 0026f30003d2.

```
awk -v key="SingleDeviceDebugger.*CpeId:.*03d2" '$0~/####/ && $0
!~key{f=0} $0~key{ f=1 } f{print} ' AdminServer.log
```

If there are multiple CpeIDs that end with the same string, use the premise ID as a differentiator, as shown below:

```
awk -v key="SingleDeviceDebugger.*(premise.586.*CpeId:.*03d2) |
(CpeId:.*0026f30003d2)" '$0~/####/ && $0 !~key{f=0} $0~key{ f=1 } f
{print} ' AdminServer.log
```

## 20 Exception Codes (UCE)

The tables in this section describe the log thresholds and coded messages that are issued when an exception happens. The `ErrorMessages.properties` file describes system exceptions that currently have been coded. All Fatal and Error messages are coded. Most warning messages have been coded.

It is only necessary to monitor the exception codes that meet *both* of the following criteria:

- From 01000- 19999
- The code is underlined (00000) in the section, "[UCE Codes](#)" on page 193

When an event occurs it is recorded in the WebLogic server log, using the pattern *UCE-XXXXX*. where *XXXXX* is the exception code number. The threshold-level of an exception code is designated by the first digit [0, 1, 2] in the exception code number. For example:

- 0** designates a fatal exception such as UCE-**0**1000 and UCE-**0**1001.
- 1** designates an error exception such as UCE-**1**4000
- 2** designates a warning exception such as UCE-**2**1001.

See "[Threshold Levels](#)" on page 192 for more information.

The Management Portal and Subscriber Portal have their own exception codes, but they follow the same numbering format.

In some cases, the applicable group is identified to resolve an exception:

- Operations** IT support, Management Information support
- Level 3 Support** Representatives responsible for interfacing with customers, central monitoring stations, and installers

## 20.1 Integration-Specific UCE Codes

Icontrol can provide custom UCE codes and error messages for your deployment that are specific to your integration and are not documented in this guide. Be sure to monitor for these integration-specific codes in your system. For example, the following alarm codes are critical and require an immediate response:

- ❑ 12000: Alarm is rejected by the central station
- ❑ 12001: Failed to send the alarm message to the central station; will re-try soon
- ❑ 12002: Failed to send the alarm message to the central station; will not re-send it
- ❑ 12003: Failed to update the status of the event after sending the alarm
- ❑ 12004: Error sending failed alarm delivery notice

For more information about UCE codes specific to your environment, see the Icontrol Customer Support Knowledge Base.

## 20.2 Threshold Levels

Exception Code Threshold Levels

Threshold Level	Threshold Level Designation	Description
Debug	Not coded	A debug message. Should be output only when the server is configured in a debug mode. May contain detailed information about operations or the state of the server.
Error	1	A user level error has occurred. The system is able to handle the error with no interruption and limited degradation in service.
Fatal	0	A system or service level error has occurred from which the system was able to recover perhaps with a momentary loss or permanent degradation of service <i>or</i> A notification of a successful recovery from a failure.  Immediate attention is probably required.
Info	Not coded	An informational message. Used for the logging of normal operations for later examination.
Trace	Not coded	A trace message. Trace messages are generated when Diagnostic Tracing is enabled for server and application classes. These messages indicate the flow of a request through the system.
Warning	2	A warning message. A suspicious operation or configuration, which does not affect the normal operation of the server.

## 20.3 Alarm Handling

Ensuring the successful delivery of alarms to the central monitoring station is a critical part of the Icontrol system. In order to ensure that an alarm has been successfully handled, it is essential that your system is properly monitored for important error messages. See ["UCE Codes" on page 193](#) for detailed descriptions of all relevant error codes potentially returned by the Icontrol system and recommended resolutions. However, any exception code in the *Alarm* subsystem should be closely monitored. For example, the following errors are logged when an alarm failed to reach the central monitoring station:

- ❑ ["UCE-11002 alarm.expiredMessage" on page 197](#)
- ❑ ["UCE-11003 alarm.failedMessage" on page 197](#)

For UCE-11002, Operations personnel with database access, must search the database for the error message's "session cpe id" in the `session_cpe_id` field of the `alarm_session` table.

For UCE-11003, call the central monitoring station to see if alarm has been delivered, and alert them directly if necessary.

In either case, Operations personnel should triage the server to determine the cause of the error.

## 20.4 UCE Codes

### 20.4.1 UCE–01000 alarm.missingArsCallbackUrl

#### DEPRECATED

**Note:** Support for telephony servers has been deprecated.

#### CONVERGE ONLY

**Message:** arsCallbackUrl is not set. The telephony server will not be able to acknowledge the calls to the central.

**Usage:** This exception only happens during WebLogic startup. It is only used for systems that employ a Telephony server for central monitoring service integration.

**Action:** Ensure custom.properties are properly configured for arsCallbackUrl .

**Responsible Group:** Operations

**Subsystem:** Alarm

**Level:** Fatal

### 20.4.2 UCE–01001 alarm.devMode

#### CONVERGE ONLY

**Note:** Support for telephony servers has been deprecated.

**Message:** Not actually calling the central as server is in dev mode. TelephonyRequestId {0}.

{0} = Telephony Request ID of the current alarm

**Usage:** This should never happen in Production mode.

**Action:** If this happens in Production mode, contact a iControl Networks representative.

**Responsible Group:** Operations

**Subsystem:** Alarm

**Level:** Fatal

### **20.4.3 UCE–01002 alarm.noSender**

**CONVERGE ONLY**

**Message:** No alarm sender specified. Cannot send any alarm to central.

**Usage:** This should never happen in Production mode.

**Action:** Ensure `custom.properties` are properly configured for `alarm.ipAlarmSender`.

*Responsible Group:* Operations

**Subsystem:** Alarm

**Level:** Fatal

### **20.4.4 UCE–01003 eventBus.initializeFailed**

**Message:** Failed to initialize Kafka event consumer.

**Usage:** This error occurs if a Kafka or Zookeeper cluster is offline when the CPE server starts.

**Subsystem:** Event Bus

**Level:** Fatal

### **20.4.5 UCE–03000 server.relay.server.init**

**Message:** Relay server initialization failed.

**Usage:** The relay server could not be contacted.

**Subsystem:** Server

**Level:** Fatal

### **20.4.6 UCE–03001 server.no.deviceFirmwareBaseUrl**

**Message:** Server property 'device.firmwareBaseUrl' not defined.

**Usage:** Server property `device.firmwareBaseUrl` not defined.

**Action:** Ensure `custom.properties` are properly configured for `device.firmwareBaseUrl`.

*Responsible Group:* Operations

**Subsystem:** Server

**Level:** Fatal

#### **20.4.7 UCE–03002 server.relay.server.insight**

##### **TOUCHSTONE ONLY**

**Message:** Relay server must be enabled for Touchstone deployment.

**Usage:** The server property `relay.server.enabled=false` and an Touchstone account has attempted to perform an action which requires relay (such as, viewing a camera or SSHing into the CPE device).

**Action:** Ensure `custom.properties` are properly configured for `relay.server.enabled=`.

**Responsible Group:** Operations

**Subsystem:** Server

**Level:** Fatal

#### **20.4.8 UCE–03003 server.no.cameraFirmwareBaseUrl**

**Message:** Server property 'camera.firmwareBaseUrl' not defined.

**Usage:** The system does not check whether the URL actually has downloadable or working firmware.

**Action:** Ensure `custom.properties` are properly configured for `camera.firmwareBaseUrl=`.

**Responsible Group:** Operations

**Subsystem:** Server

**Level:** Fatal

#### **20.4.9 UCE–03004 server.no.systemDeploymentCustomerName**

**Message:** Server property 'system\_deployment\_customer\_name' not defined.

**Subsystem:** Server

**Level:** Fatal

#### **20.4.10 UCE–03005 server.no.cloudIntegrationOauth2RedirectUrl**

**Message:** Server property 'cloudIntegration.oauth2.redirectUrl' not defined.

**Subsystem:** Server

**Level:** Fatal

#### **20.4.11 UCE–03600 server.cat.partner.oauth.no.associateAccountUrl**

**Message:** 'associate\_account\_url' not defined for partner {0}

{0} = <partner name>

**Usage:** The ASSOCIATE\_ACCOUNT\_URL database column in the CLOUD\_OBJECT\_DEF table is not defined for the specified partner.

**Subsystem:** Server

**Level:** Fatal

#### **20.4.12 UCE–03601 server.cat.event.integration.not.enabled**

**Message:** Server property 'eventIntegration.enabled' must be set to true if 'cloudIntegration.enabled' is true.

**Subsystem:** Server

**Level:** Fatal

#### **20.4.13 UCE–11000 alarm.agedMessage**

**CONVERGE ONLY**

**Note:** Support for telephony servers has been deprecated.

**Message:** The alarm message with CID {0} for account {1} failed to reach central for {2} minutes. Will keep trying for {3} minutes

{0} = CID of the current alarm

{1} = ID for the account issuing the alarm

{2} = Number of minutes since the alarm was sent to the central monitoring station

{3} = Number of the minutes that the Telephony servers will continue to send the alarm to the central monitoring station

**Usage:** This message is issued when an alarm is taking too long being sent or has failed to be sent to the central monitoring station.

**IMPORTANT:** This error code should be carefully monitored because it relates to sending alarms in a timely manner.

**Action:** Escalate alarm manually (Level 3 Support) and then triage for the cause (Operations).

**Responsible Group:** Operations and Level 3 Support

**Subsystem:** Alarm

**Level:** Error

## **20.4.14 UCE-11002 alarm.expiredMessage**

### **CONVERGE ONLY**

**Message:** The alarm session with the session cpe id {0} (CID: {1} for account {2}) failed to reach central in {3} minutes. Please contact CMS directly.

{0} = An internal alarm session ID generated by the CPE

{1} = Alarm contact ID/event code

{2} = Central station account number

{3} = Number of minutes since the alarm was received

**Note:** This event occurs only if there is a server failure in the main server cluster, and the server happens to be processing the alarm message.

**Usage:** Very rare exception. An alarm session has been found in the database that did not go to the central monitoring station and did not generate a UCE-11003 error message.

*Action:*

1. Having database access, search the database for the message's "session cpe id" in the `session_cpe_id` field of the `alarm_session` table.
2. Triage server to determine the cause of the error.

**Responsible Group:** Operations

**Subsystem:** Alarm

**Level:** Error

## **20.4.15 UCE-11003 alarm.failedMessage**

### **CONVERGE ONLY**

**Message:** The alarm message with CID {0} for account {1} failed to reach central. Please contact CMS directly.

{0} = CPE ID of the current alarm session

{1} = ID for the account issuing the alarm

**Usage:** Very rare exception. An alarm session failed to be sent to the central monitoring station and was logged by the default alarm error logger.

*Action:*

- Level 3 Support:** Call the central monitoring station to see if the alarm has been delivered (from previous UCE – 11000 error).  
If not, contact the central monitoring station to provide them with the account number and the

CID in order to generate alarm manually.

**Operations:** Triage server to determine the cause of the error.

**Subsystem:** Alarm

**Level:** Error

#### **20.4.16 UCE–13000 server.media.ffmpeg**

**Message:** The execution of ffmpeg.exe command for {0} file has been more than 10 seconds.

**Usage:**

**Action:** Immediately kill the `ffmpeg` process and monitor for more `ffmpeg` processes. If this exception continues, triage the issue further.

**Responsible Group:** Operations

**Subsystem:** Server

**Level:** Error

#### **20.4.17 UCE–13001 server.relay.session.creation**

**Message:** Failed to create a relay session for camera\_cpe\_id {0}

{0} = Unique id of a camera for an account.

**Usage:** Probably, a user has attempted to hack the camera video URL by changing the camera ID in the browser URL.

**Subsystem:** Server

**Level:** Error

#### **20.4.18 UCE–13002 server.relay.session.ssh.creation**

**Message:** Failed to create a relay session for SSH request of premise id {0}.

{0} = <account Premise ID>/<CPE ID>

**Usage:** Upon an attempt to establish an SSH connection to a CPE device from the Management Portal, either:

- The CPE is one of the following:
  - Off
  - Disconnected from the Converge security router
  - Does not currently have broadband service
- The relay server is down.

**Subsystem:** Server

**Level:** Error

#### **20.4.19 UCE–13003 server.relay.session.ssh.noport**

**Message:** Failed to create a relay session for SSH request of premise id {0}, run out of port.

{0} = <account Premise ID>/<CPE ID>

**Usage:** An attempt to establish an SSH connection to a CPE device from the Management Portal was unsuccessful because there are too many current SSH connections.

**Subsystem:** Server

**Level:** Error

#### **20.4.20 UCE–13004 server.touchscreen.sensor.commFail.invalidDelay**

**Message:** Tier property touchscreen.sensor.commFail.alarmDelay should not be less than touchscreen.sensor.commFail.troubleDelay.

**Subsystem:** Server

**Level:** Error

#### **20.4.21 UCE–13005 server.securityEventAttachment.ruleId.length**

**Message:** Length of RuleIDs for Security Event Attachment {0} exceeds the limit.

{0} = <attachment ID>

**Usage:** This UCE code is logged when the length of the RULE\_IDS database column in the SECURITY\_EVENT\_ATTACHMENT table exceeds the limit of 4000 bytes.

**Subsystem:** Server

**Level:** Error

#### **20.4.22 UCE–13006 server.nfsservice.unavailable**

**Message:** NFS service is not available.

**Usage:** This error occurs if the Network File System (NFS) cannot be accessed when trying to retrieve a file from the image/video shared storage server (i.e., media server). Also, the timer task checks availability of the NFS every five seconds, and this error occurs if the NFS is not available.

**Subsystem:** Server

**Level:** Error

#### 20.4.23 UCE–13007 server.schedule.task.exception

**Message:** Exception while running Schedule Task {0}.

{0} = <name of schedule task>

**Subsystem:** Server

**Level:** Error

#### 20.4.24 UCE–13008 server.timer.task.exception

**Message:** Exception while running Timer Task.

**Subsystem:** Server

**Level:** Error

#### 20.4.25 UCE–13600 server.cat.partner.rule.template.type.invalid

**Message:** Invalid template type

**Note:** This error is logged only in DEBUG mode.

**Subsystem:** Server

**Level:** Error

#### 20.4.26 UCE–13601 server.cat.partner.rule.template.trigger.invalid

**Message:** Invalid trigger template

**Note:** This error is logged only in DEBUG mode.

**Subsystem:** Server

**Level:** Error

#### 20.4.27 UCE–13602 server.cat.partner.rule.template.trigger.type.invalid

**Message:** Invalid trigger template type

**Note:** This error is logged only in DEBUG mode.

**Subsystem:** Server

**Level:** Error

#### 20.4.28 UCE–13603 server.cat.partner.rule.template.trigger.excludeActionIds.not.exist

**Message:** One or more action IDs in excludeActionIds does not exist

**Note:** This error is logged only in DEBUG mode.

**Subsystem:** Server

**Level:** Error

**20.4.29 UCE–13604 server.cat.partner.rule.template.trigger.targetValues.resource.not.exist**

**Message:** Resource for target value description does not exist

**Note:** This error is logged only in DEBUG mode.

**Subsystem:** Server

**Level:** Error

**20.4.30 UCE–13605 server.cat.partner.rule.template.trigger.mediaType.not.exist**

**Message:** Media type must be one of supported media types

**Note:** This error is logged only in DEBUG mode.

**Subsystem:** Server

**Level:** Error

**20.4.31 UCE–13606 server.cat.partner.rule.template.action.invalid**

**Message:** Invalid action template

**Note:** This error is logged only in DEBUG mode.

**Subsystem:** Server

**Level:** Error

**20.4.32 UCE–13607 server.cat.partner.rule.template.action.mediaType.not.exist**

**Message:** Media type must be one of the supported function media types

**Note:** This error is logged only in DEBUG mode.

**Subsystem:** Server

**Level:** Error

**20.4.33 UCE–13608 server.cat.partner.rule.template.resource.not.exist**

**Message:** No resource defined for partner

**Note:** This error is logged only in DEBUG mode.

**Subsystem:** Server

**Level:** Error

**20.4.34 UCE–13609 server.cat.partner.rule.template.description.resource.not.exist**

**Message:** Resource for template description does not exist

**Note:** This error is logged only in DEBUG mode.

**Subsystem:** Server

**Level:** Error

**20.4.35 UCE–13610 server.cat.partner.rule.template.inputs.not.exist****Message:** No input defined**Note:** This error is logged only in DEBUG mode.**Subsystem:** Server**Level:** Error**20.4.36 UCE–13611 server.cat.partner.rule.template.tags.not.exist****Message:** No tags defined**Note:** This error is logged only in DEBUG mode.**Subsystem:** Server**Level:** Error**20.4.37 UCE–13612 server.cat.partner.oauth.account.not.found****Message:** No account associated with token {0} for {1}

{0} = &lt;token name&gt;

{1} = &lt;partner name&gt;

**Subsystem:** Server**Level:** Error**20.4.38 UCE–13613 server.cat.partner.oauth.integration.not.allowed****Message:** Integration {0} not allowed for premise id {1}

{0} = &lt;partner name&gt;

{1} = &lt;premise ID&gt;

**Subsystem:** Server**Level:** Error**20.4.39 UCE–13614 server.cat.partner.oauth.provider.invalid****Message:** No cloudObjectDefinition found for {0}

{0} = &lt;partner name&gt;

**Subsystem:** Server**Level:** Error

**20.4.40 UCE–13615 server.cat.partner.oauth.accountInformation.invalid**

**Message:** Invalid partner account information for partner {0}

{0} = <partner name>

**Subsystem:** Server

**Level:** Error

**20.4.41 UCE–13616 server.cat.partner.oauth.account.retrieve.failed**

**Message:** Unable to fetch partner account information for partner {0} partner server returned {1}

{0} = <partner name>

{1} = <HTTP status code>

**Subsystem:** Server

**Level:** Error

**20.4.42 UCE–13617 server.cat.partner.oauth.virtualDevice.siteId**

**Message:** No site information in partner account information for partner {0}

{0} = <partner name>

**Usage:** The virtualDevice.siteId field is not available in the associateAccount call that is used to acquire user account information when onboarding a partner account.

**Subsystem:** Server

**Level:** Error

**20.4.43 UCE–13618 server.cat.partner.oauth.cloudObject.invalid**

**Message:** No cloud object information for partner {0} and partner account {1}

{0} = <partner name>

{1} = <user account ID>

**Usage:** The virtualDevice.instanceIds field is not available in the associateAccount call that is used to acquire user account information when onboarding a partner account.

**Subsystem:** Server

**Level:** Error

**20.4.44 UCE–13619 server.cat.partner.oauth.account.already.associated**

**Message:** Account {0} for partner {1} is already associated with other premise

{0} = <user account ID>

{1} = <partner name>

**Usage:** This error occurs when a user tries to associate a single account with multiple premises.

**Subsystem:** Server

**Level:** Error

**20.4.45 UCE–13620 server.cat.partner.oauth.onboarding.general.problem.serve**

**Message:** General problem while associating partner {0} for premise {1}

{0} = <partner name>

{1} = <premise ID>

**Subsystem:** Server

**Level:** Error

**20.4.46 UCE–13621 server.cat.partner.delete.account.already.associated**

**Message:** Partner {0} has associated accounts.

{0} = <partner name>

**Subsystem:** Server

**Level:** Error

**20.4.47 UCE–13622 server.cat.partner.oauth.account.associated.mismatch**

**Message:** New partner account is not the same as existing paired partner account with premise {0} for partner {1}

{0} = <premise ID>

{1} = <partner name>

**Usage:** When an existing user account ID tries to re-onboard a partner account, this error occurs if the new account ID does not match the existing account ID.

**Subsystem:** Server

**Level:** Error

**20.4.48 UCE–13623 server.cat.partner.rule.template.trigger.mediaType.lifecycle.not.allowed**

**Message:** Life cycle event is not allowed in trigger template

**Note:** This error is logged only in DEBUG mode.

**Subsystem:** Server

**Level:** Error

#### **20.4.49 UCE–13624 server.cat.partner.oauth.cloudObjectType.invalid**

**Message:** Invalid cloud object type {0} for partner {1} and partner account {2}

{0} = <cloud object type>

{1} = <partner name>

{2} = <user account ID>

**Subsystem:** Server

**Level:** Error

#### **20.4.50 UCE–13900 persistence.objectDoesNotExistWithTime**

**Message:** Object of type "{0}" with id "{1}" does not exist

{0} = <object type>

{1} = <object ID>

**Usage:** A synchronization issue may exist between the database and the CPE. Contact Icontrol customer support for assistance.

**Subsystem:** Server

**Level:** Error

#### **20.4.51 UCE–13901 persistence.nonUniqueResult**

**Message:** Query for object of type "{0}" returned more than one result

{0} = <object type>

**Usage:** A synchronization issue may exist between the database and the CPE. Contact Icontrol customer support for assistance.

**Subsystem:** Server

**Level:** Error

#### **20.4.52 UCE–13902 persistence.nullArgument**

**Message:** Cannot find object of type "{0}" with null id

{0} = <object type>

**Usage:** A synchronization issue may exist between the database and the CPE. Contact Icontrol customer support for assistance.

**Subsystem:** Server

**Level:** Error

#### **20.4.53 UCE-14000 activation.activated**

**Message:** Failed to create a relay session for SSH request of premise id {0}, run out of port.

{0} = <account Premise ID>/<CPE ID>

**Subsystem:** Activation

**Level:** Error

#### **20.4.54 UCE-14001 activation.wrong.orderNumber**

**Message:** The activation code entered was not found for deployment {0}. (You entered: {1})

{0} = Deployment for which a CPE attempted to be activated

{1} = Activation code entered for the CPE

**Subsystem:** Activation

**Level:** Error

#### **20.4.55 UCE-14002 activation.wrong.phoneNumber**

**Message:** The phone number entered may be incorrect or does not match with the activation code. (You entered: {0})

{0} = Phone number entered for during Activation process

**Subsystem:** Activation

**Level:** Error

#### **20.4.56 UCE-14003 activation.wrong.cpeId**

**Message:** The activation was not properly provisioned. The touch screen Ethernet MAC address might not have been entered or imported into the server.

**Subsystem:** Activation

**Level:** Error

#### **20.4.57 UCE-14004 activation.notReadyForActivation**

**Message:** The account is not ready for activation. Please check the account in the Management Portal on the server.

**Subsystem:** Activation

**Level:** Error

#### **20.4.58 UCE–14005 activation.deviceAlreadyAttached**

**Message:** A device is already associated with the account. Please reset the account in the Management Portal and try again.

**Subsystem:** Activation

**Level:** Error

#### **20.4.59 UCE–14006 activation.notActivated**

**Message:** The account is not activated. Cannot send activation complete email.

**Subsystem:** Activation

**Level:** Error

#### **20.4.60 UCE–14007 activation.userAlreadySetUp**

**Message:** No need to send activation complete email as user is already set up.

**Subsystem:** Activation

**Level:** Error

#### **20.4.61 UCE–14008 activation.cpeAlreadyUsed**

**Message:** The touch screen is already used by {0}.

{0} = Account ID

**Subsystem:** Activation

**Level:** Error

#### **20.4.62 UCE–14009 activation.wrong.orderNumberMultiDeployment**

**Message:** The activation code entered was not found for deployment {0} (You entered: {1}).

{0} = Deployment for which a CPE attempted to be activated

{1} = Activation code entered for the CPE

**Subsystem:** Activation

**Level:** Error

#### **20.4.63 UCE–14010 activation.missingEmailAddress**

**Message:** Email address is required to finish activation for account {0}.

{0} = Account ID

**Subsystem:** Activation

**Level:** Error

**20.4.64 UCE–14011 activation.wrong.productType**

**Message:** The account is not set up to use the product given.

**Subsystem:** Activation

**Level:** Error

**20.4.65 UCE–14012 activation.email.failToSend**

**Message:** Cannot send activation email to {0} for account {1}.

{0} = Account email

{1} = Account ID

**Subsystem:** Activation

**Level:** Error

**20.4.66 UCE–14013 activation.cls.cpeAlreadyUsed**

**Message:** The touchscreen is already used by another account in Cluster Location Service.

**Subsystem:** Activation

**Level:** Error

**20.4.67 UCE–14014 activation.system.failed**

**Message:** Cluster Location Service error, could not activate the device.

**Subsystem:** Activation

**Level:** Error

**20.4.68 UCE–14600 cellular.communication.messageHandlingException**

**CONVERGE ONLY**

**Message:** Unsupported gprs message version {0}

{0} = Premise ID

**Usage:**

*Action:* Triage the account (using a diag file if possible) and contact iControl Networks support.

*Responsible Group:* Operations

**Subsystem:** Cellular

**Level:** Error

**20.4.69 UCE–14601 cellular.communication.unsupportedMessageVersion****CONVERGE ONLY**

**Message:** Unsupported gprs message version {0}

**Usage:**

*Action:* Triage the account (using a diag file if possible) and contact iControl Networks support.

*Responsible Group:* Operations

**Subsystem:** Cellular

**Level:** Error

**20.4.70 UCE–14602 cellular.communication.noHandlerFound****CONVERGE ONLY**

**Message:** No handler found for message type {0}

{0} = Cellular

**Usage:**

*Action:* Triage the account (using a diag file if possible) and contact iControl Networks support.

*Responsible Group:* Operations

**Subsystem:** Cellular

**Level:** Error

**20.4.71 UCE–14603 cellular.communication udp.receiverException****CONVERGE ONLY**

**Message:** Error receiving UDP data, resuming

**Usage:**

*Action:* Triage the account (using a diag file if possible) and contact iControl Networks support.

*Responsible Group:* Operations

**Subsystem:** Cellular

**Level:** Error

## **20.4.72 UCE–14604 cellular.communication.udp.senderException**

### **CONVERGE ONLY**

**Message:** Error sending UDP data, resuming

**Usage:**

*Action:* Triage the account (using a diag file if possible) and contact Icontrol Networks support.

*Responsible Group:* Operations

**Subsystem:** Cellular

**Level:** Error

## **20.4.73 UCE–15000 integration.cs.exception**

### **CONVERGE ONLY**

**Message:** Received a unknown receiver id {0} from central station after creating a new account.

{0} = Account ID

**Usage:**

*Action:* Triage the exception.

*Responsible Group:* Operations

**Subsystem:** Integration

**Level:** Error

## **20.4.74 UCE–15001 integration.cs.unknown.receiver**

### **CONVERGE ONLY**

**Message:** Received a unknown receiver id {0} from central station after creating a new account

{0} = Account ID

**Usage:**

*Action:* Triage the exception.

*Responsible Group:* Operations

**Subsystem:** Integration

**Level:** Error

## 20.4.75 UCE–15100 integration.account.general

### CONVERGE ONLY

**Message:** There is a general server exception that prevents the completion of the call.

**Usage:**

*Action:* Triage the exception.

**Note:** This exception is not logged in server logs. These are codes returned to the caller.

*Responsible Group:* Operations

**Subsystem:** Integration

**Level:** Error

## 20.4.76 UCE–15101 integration.account.notFound

### CONVERGE ONLY

**Message:** Account {0} not found.

{0} = Account ID

**Usage:**

*Action:* Triage the exception. Ensure the Account ID is in iControl system.

**Note:** This exception is not recorded in server logs. These are codes returned to the caller.

*Responsible Group:* Operations

**Subsystem:** Integration

**Level:** Error

## 20.4.77 UCE–15102 integration.account.alreadyActivated

### CONVERGE ONLY

**Message:** Account {0} already activated.

{0} = Account ID

**Usage:**

*Action:* Triage the exception.

**Note:** This exception is not recorded in server logs. These are codes returned to the caller.

*Responsible Group:* Operations

**Subsystem:** Integration

**Level:** Error

## 20.4.78 UCE–15103 integration.account.alreadyExist

### CONVERGE ONLY

**Message:** Account {0} already exists.

{0} = Account ID

**Usage:** This exception is not recorded in server logs. These are codes returned to the caller.

**Subsystem:** Integration

**Level:** Error

## 20.4.79 UCE–15104 integration.account.missingProperty

### CONVERGE ONLY

**Message:** Missing required account field {0}.

{0} = The required account field that is missing

**Usage:** This exception is not recorded in server logs. These are codes returned to the caller.

**Subsystem:** Integration

**Level:** Error

## 20.4.80 UCE–15105 integration.account.wrongCSAccountNumberLength

### CONVERGE ONLY

**Message:** Central Station account number should be greater than four digits.

**Usage:** This exception is not recorded in server logs. These are codes returned to the caller.

**Subsystem:** Integration

**Level:** Error

## 20.4.81 UCE–15106 integration.account.csReceiverNotFound

### CONVERGE ONLY

**Message:** Central station receiver not found for central station account {0}.

{0} = Central Station Account Number

**Usage:** This exception is not recorded in server logs. These are codes returned to the caller.

**Subsystem:** Integration

**Level:** Error

### **20.4.82 UCE–15107 integration.account.csAccountUsed**

#### **CONVERGE ONLY**

**Message:** Central station account {0} is already used.

{0} = Central Station Account Number

**Usage:** This exception is not recorded in server logs. These are codes returned to the caller.

**Subsystem:** Integration

**Level:** Error

### **20.4.83 UCE–15108 integration.account.notExternal**

#### **CONVERGE ONLY**

**Message:** Account {0} is not externally created.

{0} = Account ID

**Usage:** This exception is not recorded in server logs. These are codes returned to the caller.

**Subsystem:** Integration

**Level:** Error

### **20.4.84 UCE–15109 integration.account.firstNameHasWrongChar**

#### **CONVERGE ONLY**

**Message:** First name has the black list's characters.

**Usage:** This exception is not recorded in server logs. These are codes returned to the caller.

**Subsystem:** Integration

**Level:** Error

### **20.4.85 UCE–15110 integration.account.lastNameHasWrongChar**

#### **CONVERGE ONLY**

**Message:** Last name has the black list's characters.

**Usage:** This exception is not recorded in server logs. These are codes returned to the caller.

**Subsystem:** Integration

**Level:** Error

**20.4.86 UCE–15111 integration.account.emergencyContact.firstNameHasWrongChar****CONVERGE ONLY**

**Message:** First name of emergency contact has the black list's characters.

**Usage:** This exception is not recorded in server logs. These are codes returned to the caller.

**Subsystem:** Integration

**Level:** Error

**20.4.87 UCE–15112 integration.account.emergencyContact.lastNameHasWrongChar****CONVERGE ONLY**

**Message:** Last name of emergency contact has the black list's characters.

**Usage:** This exception is not recorded in server logs. These are codes returned to the caller.

**Subsystem:** Integration

**Level:** Error

**20.4.88 UCE–15113 integration.account.notActivated****CONVERGE ONLY**

**Message:** Account {0} is not activated.

{0} = Account ID

**Usage:** This exception is not recorded in server logs. These are codes returned to the caller.

**Subsystem:** Integration

**Level:** Error

**20.4.89 UCE–15114 integration.account.deploymentNotFound****CONVERGE ONLY**

**Message:** Deployment {0} does not exist.

{0} = Deployment name

**Usage:** This exception is not recorded in server logs. These are codes returned to the caller.

**Subsystem:** Integration

**Level:** Error

## **20.4.90 UCE–15115 integration.account.deploymentDoesNotMatch**

### **CONVERGE ONLY**

**Message:** Account deployment {0} does not match the deployment of the central station receiver.

{0} = Deployment name

**Usage:** This exception is not recorded in server logs. These are codes returned to the caller.

**Subsystem:** Integration

**Level:** Error

## **20.4.91 UCE–15116 integration.account.missingDeployment**

### **CONVERGE ONLY**

**Message:** Account needs to have deployment {0} in order to use the central station receiver.

{0} = Deployment name

**Usage:** This exception is not recorded in server logs. These are codes returned to the caller.

**Subsystem:** Integration

**Level:** Error

## **20.4.92 UCE–15117 integration.account.illegalCountry**

### **CONVERGE ONLY**

**Message:** Country must be one of the countries defined in premise.countryList in custom.properties.

**Usage:** This exception is not recorded in server logs. These are codes returned to the caller.

**Subsystem:** Integration

**Level:** Error

## **20.4.93 UCE–15118 integration.group.notFound**

### **CONVERGE ONLY**

**Message:** Account group {0} not found.

{0} = Tier or package name

**Usage:** This exception is not recorded in server logs. These are codes returned to the caller.

**Subsystem:** Integration

**Level:** Error

**20.4.94 UCE–15119 integration.group.multipleTier****CONVERGE ONLY****Message:** Multiple tier group specified for Account {0}.

{0} = Account ID

**Subsystem:** Integration**Level:** Error**20.4.95 UCE–15120 integration.group.noTier****CONVERGE ONLY****Message:** No tier group specified for Account {0}.

{0} = Account ID

**Subsystem:** Integration**Level:** Error**20.4.96 UCE–15121 integration.group.notTier****CONVERGE ONLY****Message:** Group {0} is not a Tier group.

{0} = Tier or package name

**Subsystem:** Integration**Level:** Error**20.4.97 UCE–15122 integration.account.generalWithMsg****CONVERGE ONLY****Message:** Server exception: {0}.

{0} = Text of the error

**Subsystem:** Integration**Level:** Error

**20.4.98 UCE–15123 integration.product.notFound****CONVERGE ONLY****Message:** Product {0} not found.{0} = Platform name, such as *converge* or *touchstone***Usage:** Only messages from Converge are sent to central stations.**Subsystem:** Integration**Level:** Error**20.4.99 UCE–15124 integration.missingEmail****CONVERGE ONLY****Message:** Missing required email address for account {0}.

{0} = Account ID

**Subsystem:** Integration**Level:** Error**20.4.100 UCE–15125 integration.userExists****CONVERGE ONLY****Message:** User {0} already exists.

{0} = Account username

**Subsystem:** Integration**Level:** Error**20.4.101 UCE–15126 integration.product.update****CONVERGE ONLY****Message:** Product cannot be updated for account {0}.

{0} = Account ID

**Subsystem:** Integration**Level:** Error

**20.4.102 UCE–15127 integration.group.cannot.add****CONVERGE ONLY****Message:** P5 QNX account cannot be added to the group {0}.

{0} = Tier or package name

**Usage:** An attempt was made to add an account to a package that uses an SMC P5 QNX touchscreen.**Subsystem:** Integration**Level:** Error**20.4.103 UCE–15128 integration.account.wrong.csMonitorFlag****CONVERGE ONLY****Message:** Cannot create or update a non-monitorable account with monitor flag is true.**Usage:** An attempt was made to add or modify an account that cannot be monitored with the monitor variable set to true.**Subsystem:** Integration**Level:** Error**20.4.104 UCE–15129 integration.account.invalid.activationCode****CONVERGE ONLY****Message:** Invalid activation code {0}. System supports numeric activation code only.

{0} = Activation code

**Subsystem:** Integration**Level:** Error**20.4.105 UCE–15130 integration.account.emergencyContact.invalidPhoneNumber****Message:** Invalid emergency contact phone number format.**Subsystem:** Integration**Level:** Error**20.4.106 UCE–15131 integration.account.externalReference.invalidCharacter****Message:** Special characters are not allowed in accountId.**Usage:** This error occurs if invalid or special characters are used in the value of accountId when attempting to create an account using the Icontrol WSDL.**Subsystem:** Integration**Level:** Error

#### **20.4.107 UCE–15132 integration.account.invalid.monitoredFlag**

**Message:** Missing required monitor flag for account.

**Usage:** This error occurs if the monitored flag is not provided when updating an account using the Icontrol WSDL.

**Subsystem:** Integration

**Level:** Error

#### **20.4.108 UCE–15133 integration.account.invalid.internalFlag**

**Message:** Missing required internal flag for account.

**Usage:** This error occurs if the internal flag is not provided when updating an account using the Icontrol WSDL.

**Subsystem:** Integration

**Level:** Error

#### **20.4.109 UCE–16000 rest.resource.notFound**

**Message:** Resource identified by {0} not found

{0} = Resource ID

**Usage:** A call was made against a resource that does not exist. A *resource* can be anything: a zone, a device, etc. This is a generic error where the resource ID will be provided

**Subsystem:** General REST API

**Level:** Error

#### **20.4.110 UCE–16001 rest.function.notFound**

**Message:** Function with name "{0}" not found

{0} = The invalid function name

**Usage:** A call was made against a function that does not exist.

**Subsystem:** General REST API

**Level:** Error

#### **20.4.111 UCE–16002 rest.function.invalidparamter**

**Message:** Required parameters are missing or parameters supplied are not valid

**Usage:** A call is missing a necessary parameter.

**Subsystem:** General REST API

**Level:** Error

#### **20.4.112 UCE–16003 rest.point.notFound**

**Message:** Point with name "{0}" not found

{0} = Point name

**Usage:** A call was made against a point that does not exist.

**Subsystem:** General REST API

**Level:** Error

#### **20.4.113 UCE–16004 rest.general.problem.serve**

**Message:** There was a general problem while serving your request

**Usage:** This is a general catch-all message for an undefined error.

**Subsystem:** General REST API

**Level:** Error

#### **20.4.114 UCE–16005 rest.general.paramterOutOfRange**

**Message:** Supplied parameter out of range

**Usage:** A call attempted to configure an element with a not permitted value.

**Subsystem:** General REST API

**Level:** Error

#### **20.4.115 UCE–16006 rest.general.accountNotProvisioned**

**Message:** The account is not provisioned for the operation

**Usage:** A call made a request against a subscriber account that does not have sufficient privileges to perform the operation.

**Subsystem:** General REST API

**Level:** Error

#### **20.4.116 UCE–16007 rest.general.accountNotActive**

**Message:** The account is no longer active

**Usage:** A call made an unallowed request against a suspended or deactivated subscriber account.

**Subsystem:** General REST API

**Level:** Error

#### **20.4.117 UCE–16008 rest.general.deviceNotConnected**

**Message:** The device is off-line

**Usage:** A call made an unallowed request against a CPE that is out-of-communication with the server clusters.

**Subsystem:** General REST API

**Level:** Error

#### **20.4.118 UCE–16009 rest.general.usernameAlreadyExists**

**Message:** The username "{0}" already exists in the system

{0} =username

**Usage:** A call attempted to create a new username or change an existing one to a username already in the database.

**Subsystem:** General REST API

**Level:** Error

#### **20.4.119 UCE–16010 rest.general.invalidPassword**

**Message:** Enter your old password correctly

**Usage:** When trying to change the password of her account, a user did not use the correct current password of the account.

**Subsystem:** General REST API

**Level:** Error

#### **20.4.120 UCE–16011 rest.general.eventHistory.query.dateRangeTooLong**

**Message:** Date range is too long

**Usage:** When trying to find event history for days more than maximum number of days allowed to query history events (See server.property "["eventHistory.query.dateRange.max"](#) on page 266).

**Subsystem:** General REST API

**Level:** Error

#### **20.4.121 UCE–16012 rest.general.contactCustomerSupport**

**Message:** Please contact customer support

**Usage:** An action has encountered a roadblock that require that the subscriber receive assistance from a company representative.

**Subsystem:** General REST API

**Level:** Error

**20.4.122 UCE–16013 rest.general.primaryContactOrderNotAllowed**

**Message:** Primary contact cannot be changed.

**Subsystem:** General REST API

**Level:** Error

**20.4.123 UCE–16014 rest.general.invalidEmergencyContactOrder**

**Message:** Emergency contact order is not valid.

**Subsystem:** General REST API

**Level:** Error

**20.4.124 UCE–16100 rest.keypad.masterCode.wrongNotLocked**

**Message:** Enter your 4-digit master code correctly

**Usage:** A subscriber entered a wrong keypad code.

**Subsystem:** Subscriber REST API

**Level:** Error

**20.4.125 UCE–16101 rest.keypad.masterCode.wrongLocked**

**Message:** To protect your account, access to keypad code will be locked for {0} minutes

{0} = Number of minutes (rounded up) until the account is unlocked (based on the server property `keypad.code.lockTime`).

**Usage:** A subscriber entered the wrong keypad code the maximum number of times (server property `keypad.code.max.retry`), and the account is now locked for a period of time.

**Subsystem:** Subscriber REST API

**Level:** Error

**20.4.126 UCE–16102 rest.keypad.masterCode.stillLocked**

**Message:** For your protection, access to keypad code will be unlocked in {0} minutes

{0} = Number of minutes (rounded up) from this time until the account is unlocked .

**Usage:** A subscriber has attempted to enter a keypad code on a locked account. The system returns the number of minutes left until the account is no longer locked (based on the server property `keypad.code.lockTime`).

**Subsystem:** Subscriber REST API

**Level:** Error

**20.4.127 UCE–16103 rest.keypad.masterCode.cantDelete**

**Message:** Master Code cannot be deleted

**Usage:** A user has attempted to delete the Master code from the Subscriber Portal.

**Subsystem:** Subscriber REST API

**Level:** Error

**20.4.128 UCE–16104 rest.keypad.mastercode.invalid**

**Message:** Please enter a valid value for Master Code

**Usage:** A user has attempted to change the Master code from the Subscriber Portal using invalid characters.

**Subsystem:** Subscriber REST API

**Level:** Error

**20.4.129 UCE–16105 rest.keypad.mastercode.notEditable**

**Message:** Only access code is editable for Master Code

**Usage:** A user has attempted to update a label or level of the Master key pad code.

**Subsystem:** Subscriber REST API

**Level:** Error

**20.4.130 UCE–16106 rest.keypad.duresscode.notEditable**

**Message:** Only access code is editable for Duress Code

**Usage:** A user has attempted to update label or level of Duress Code.

**Subsystem:** Subscriber REST API

**Level:** Error

**20.4.131 UCE–16107 rest.take.video.max.quota.reached**

**Message:** Your service package only allows for {0} saved video(s). If you would like this increased, please contact support for information on upgrading your account.

{0} = Daily limit of video upload

**Subsystem:** Subscriber REST API

**Level:** Error

#### **20.4.132 UCE–16108 rest.take.image.max.quota.reached**

**Message:** Your service package only allows for {0} saved image(s). If you would like this increased, please contact support for information on upgrading your account.

{0} = Daily limit of image upload

**Subsystem:** Subscriber REST API

**Level:** Error

#### **20.4.133 UCE–16109 rest.schedule.rule.exists**

**Message:** Schedule rule already exists for resource identified by {0}

{0} = Thermostat ID

**Usage:** A user tries add thermostat schedule rule for thermostat with an associated schedule rule.

**Subsystem:** Subscriber REST API

**Level:** Error

#### **20.4.134 UCE–16110 rest.schedule.rule.not.found**

**Message:** Schedule rule does not exist.

**Usage:** A user tries to get, update or delete a thermostat schedule rule for thermostat that is not paired to the system.

**Subsystem:** Subscriber REST API

**Level:** Error

#### **20.4.135 UCE–16111 rest.rule.video.attachment.not.allowed**

**Message:** Video attachment is not allowed.

**Usage:** When a user creates or updates a rule using the REST API, this error occurs if the rule has the:

- Send email with attached video action, and the value of tier property `mail.allowVideoAttachment` is false.
- Send SMS with attached video action, and the value of tier property `sms.mms.allowVideoAttachment` is false.

**Subsystem:** Rules REST API

**Level:** Error

#### **20.4.136 UCE–16200 rest.cloudIntegration.notReady**

**Message:** Cloud account is not ready for API access.

**Subsystem:** Cloud Integration REST API

**Level:** Error

**20.4.137 UCE–16201 rest.cloudIntegration.refresh.token**

**Message:** Cannot get a new authentication token by using the refresh token.

**Subsystem:** Cloud Integration REST API

**Level:** Error

**20.4.138 UCE–16202 rest.cloudIntegration.general**

**Message:** There was a general problem while serving request for premise {0} partner {1} path {2} {3}

{0} = <premise ID>

{1} = <partner name>

{2} = <method>

{3} = <URL>

**Subsystem:** Cloud Integration REST API

**Level:** Error

**20.4.139 UCE–16203 rest.cloudIntegration.event.history.event.conversion.string.failed**

**Message:** Failed to convert from IcEvent to String.

**Subsystem:** Cloud Integration REST API

**Level:** Error

**20.4.140 UCE–16204 rest.cloudIntegration.event.history.event.conversion.icEvent.failed**

**Message:** Failed to convert from String to IcEvent.

**Subsystem:** Cloud Integration REST API

**Level:** Error

**20.4.141 UCE–16205 rest.cloudIntegration.event.history.parse.failed**

**Message:** Unable to parse String event to JSON.

**Subsystem:** Cloud Integration REST API

**Level:** Error

**20.4.142 UCE–16206 rest.cloudIntegration.event.history.save.failed**

**Message:** History event could not be saved.

**Subsystem:** Cloud Integration REST API

**Level:** Error

#### **20.4.143 UCE–16207 rest.cloudIntegration.renew.token.general**

**Message:** Failed to renew token for premise {0} partner {1} due to {2}

{0} = <premise ID>

{1} = <partner name>

{2} = <case-specific error message>

**Subsystem:** Cloud Integration REST API

**Level:** Error

#### **20.4.144 UCE–16208 rest.bundle.invalid.bundletype**

**Message:** Bundle Type ID does not exist. Please enter a valid Bundle Type

**Usage:** This error occurs when creating a bundle and the value of the `bundleTypeID` parameter does not exist.

**Subsystem:** Operational REST API

**Level:** Error

#### **20.4.145 UCE–16209 rest.bundle.invalid.bundlecontent.format**

**Message:** Invalid Bundle Content format. Please enter a valid Bundle Content in JSON format

**Usage:** This error occurs when creating a bundle type and the request body (bundle content) JSON uses an incorrect format.

Example bundle content:

```
{"bundleContent": [{"count":5,"deviceType":"Water Sensors"}, {"count":6,"deviceType":"Door Window Sensors"}]}
```

**Subsystem:** Operational REST API

**Level:** Error

#### **20.4.146 UCE–16210 rest.bundle.invalid.bundle.device.type**

**Message:** Invalid Bundle Device Type. Please enter a valid Bundle Device Type

**Usage:** This error occurs when creating a bundle type and the value of any `deviceType` attribute in the request body (bundle content) does not exist.

Example of `deviceType` attributes in bundle content:

```
{"bundleContent": [{"count":5,"deviceType":"Water Sensors"}, {"count":6,"deviceType":"Door Window Sensors"}]}
```

**Subsystem:** Operational REST API

**Level:** Error

**20.4.147 UCE–16211 rest.bundle.invalid.bundle.type.exists**

**Message:** Bundle Type already exists. Please enter a new Bundle Type

**Usage:** This error occurs when creating a bundle type and the specified bundleTypeId already exists.

**Subsystem:** Operational REST API

**Level:** Error

**20.4.148 UCE–16212 rest.bundle.invalid.bundle**

**Message:** Bundle ID does not exist. Please enter a valid Bundle ID

**Usage:** This error occurs when retrieving a bundle and the specified bundleId does not exist.

**Subsystem:** Subscriber REST API

**Level:** Error

**20.4.149 UCE–16300 rest.cloudIntegrationServer.register.callback.failed**

**Message:** Unable to update {0}

{0} = EventCallbackUrl or HealthCheckCallbackUrl according to operation

**Subsystem:** Cloud Integration Service

**Level:** Error

**20.4.150 UCE–16301 rest.cloudIntegrationServer.problem.icEvent**

**Message:** There was a problem while processing IcEvent: {0}

{0} = Error message

**Subsystem:** Cloud Integration Service

**Level:** Error

**20.4.151 UCE–16302 rest.cloudIntegrationServer.icEvent.invalidData**

**Message:** {0} is not valid

{0} = instanceId or metadata or mediaType or integrationname or accountId, according to operation

**Subsystem:** Cloud Integration Service

**Level:** Error

**20.4.152 UCE–16303 rest.cloudIntegrationServer.icEvent.partner.inactive****Message:** {0} is not active

{0} = &lt;partner name&gt;

**Usage:** This error occurs when trying to interact with an existing partner that is no longer active in the system.**Subsystem:** Cloud Integration Service**Level:** Error**20.4.153 UCE–16304 rest.cloudIntegrationServer.cache.notEnabled****Message:** CIS {0} cache is not configured properly, it will cause performance issues. Calling the REST service directly.

{0} = &lt;cache name&gt;

**Usage:** This error occurs when the specified Cloud Integration Service cache is not properly configured (e.g., a non-integer value is specified for time). For more information, see the "Server Properties" section in *Cloud Integration Service Installation Guide*.**Subsystem:** Cloud Integration Service**Level:** Error**20.4.154 UCE–21000 alarm.telephony.failedMessage****DEPRECATED****Note:** Support for telephony servers has been deprecated.**CONVERGE ONLY****Message:** Telephony request {0} did not complete successfully. Returning to queue for reprocessing..

{0} = Telephony Request ID of the current alarm

**Usage:** An alarm request failed to reach telephony server and is returning to the alarm queue for reprocessing.**Subsystem:** Alarm**Level:** Warning**20.4.155 UCE–21001 alarm.telephony.timedoutMessage****DEPRECATED****Note:** Support for telephony servers has been deprecated.

**CONVERGE ONLY**

**Message:** A timeout has occurred for telephony request {0}. Returning to queue for reprocessing.

{0} = Telephony Request ID of the current alarm

**Subsystem:** Alarm

**Level:** Warning

**20.4.156 UCE–21020 alarm.session.waitingTooLong****CONVERGE ONLY**

**Message:** Sending alarm session {0} to central station since it is in waiting state for {1} seconds.

{0} = Session ID of the current alarm

{1} = Number of seconds

**Subsystem:** Alarm

**Level:** Warning

**20.4.157 UCE–22100 notification.failToSendEmail**

**Message:** Failed to send email to {0}.

{0} = Email address for configured alert

**Usage:** This error message is issued when an email alert was not successfully sent upon an alert event.

**Subsystem:** Notification

**Level:** Warning

**20.4.158 UCE–22200 notification.failToSendSms**

**Message:** Failed to send SMS message to {0}.

{0} = SMS phone number for configured alert

**Usage:** This error message is issued when an SMS alert was not successfully sent upon an alert event.

**Subsystem:** Notification

**Level:** Warning

#### **20.4.159 UCE–22210 notification.failToSendSimpleWireSms**

**Message:** Failed to send SimpleWire SMSs message to {0}\n Error Code: {1} Error Description: {2} Error Resolution: {3}

{0} = Phone number for configured alert

{1} = SimpleWire error code

{2} = Simple Wire error message text

{3} = SimpleWire error resolution text

**Usage:** This error message is issued when an SMS alert sent via SimpleWire was not successfully sent upon an alert event.

**Subsystem:** Notification

**Level:** Warning

#### **20.4.160 UCE–22300 notification.failToSend**

**Message:** Failed to send message to {0}.

{0} = Phone number for configured alert

**Usage:** This error message is issued when an email or SMS alert due to a rule was not successfully sent.

**Subsystem:** Notification

**Level:** Warning

#### **20.4.161 UCE–23500 server.cls.update.exception**

**Message:** There was an exception while updating device details in CLS for premise id {0}

{0} = Premise ID of CLS account

**Subsystem:** Cluster Location Service

**Level:** Warning

#### **20.4.162 UCE–23501 server.cls.site.create.exception**

**Message:** There was an exception while creating site entry with id {0} in CLS

{0} = Premise ID of CLS account

**Subsystem:** Cluster Location Service

**Level:** Warning

#### **20.4.163 UCE–23502 server.cls.user.create.exception**

**Message:** There was an exception while creating user entry in CLS for username {0}

{0} = Username of CLS account that you are creating

**Subsystem:** Cluster Location Service

**Level:** Warning

#### **20.4.164 UCE–23503 server.cls.site.update.exception**

**Message:** There was an exception while updating site entry with id {0} in CLS

{0} = Premise ID of CLS account

**Subsystem:** Cluster Location Service

**Level:** Warning

#### **20.4.165 UCE–23504 server.cls.user.update.exception**

**Message:** There was an exception while updating user entry with username {0} in CLS

{0} = Username of CLS account

**Subsystem:** Cluster Location Service

**Level:** Warning

#### **20.4.166 UCE–23505 server.cls.site.delete.exception**

**Message:** There was an exception while deleting site entry with id {0} from CLS

{0} = Premise ID of CLS account

**Subsystem:** Cluster Location Service

**Level:** Warning

#### **20.4.167 UCE–23506 server.cls.user.delete.exception**

**Message:** There was an exception while deleting user entry with username {0} from CLS

{0} = Username of CLS account that you are deleting

**Subsystem:** Cluster Location Service

**Level:** Warning

#### **20.4.168 UCE–24100 broadband.communication.smapException**

**Message:** Server exception while processing SMAP message "{0}" from "{1}"

{0} = Request URL. (for example, /datasyncor /event /zone)

{1} = <account Premise ID>/<CPE ID>

**Subsystem:** Broadband

**Level:** Warning

#### **20.4.169 UCE–24101 broadband.communication.connectionTotalLost**

**Message:** Device not connected to server

**Subsystem:** Broadband

**Level:** Warning

#### **20.4.170 UCE–24102 broadband.communication.broadbandLost**

**Message:** Device not connected to server via broadband

**Subsystem:** Broadband

**Level:** Warning

#### **20.4.171 UCE–24103 broadband.communication.broadbandLost**

##### **TOUCHSTONE ONLY**

**Message:** Mode "{0}" not found for premise "{1}"

{0} = Touchstone mode name

{1} = <account Premise ID>/<CPE ID>

**Subsystem:** Broadband

**Level:** Warning

#### **20.4.172 UCE–24600 cellular.communication.ipNotFound**

##### **CONVERGE ONLY**

**Message:** Cellular IP "{0}" not found in database.

{0} = Cellular IP for SMS service

**Subsystem:** Cellular

**Level:** Warning

### **20.4.173 UCE–24601 cellular.communication.cannotSendCommand**

#### **CONVERGE ONLY**

**Message:** Cannot send the command via cellular channel based on the user's cellular level of service.

**Subsystem:** Cellular

**Level:** Warning

### **20.4.174 UCE–24602 cellular.communication.missingActorType**

#### **CONVERGE ONLY**

**Message:** Missing the actor type in thread local when calling createCpeCommand() method.

**Subsystem:** Cellular

**Level:** Warning

### **20.4.175 UCE–24603 cellular.communication.udp.senderInterrupted**

#### **CONVERGE ONLY**

**Message:** UDP Sender interrupted, resuming.

**Subsystem:** Cellular

**Level:** Warning

### **20.4.176 UCE–25020 integration.address.ioException**

#### **CONVERGE ONLY**

**Message:** IO Exception trying to get geolocation for address {0}.

**Subsystem:** Integration

**Level:** Warning

### **20.4.177 UCE–25021 integration.address.requestOverLimit**

#### **CONVERGE ONLY**

**Message:** Geolocation request over daily limit. Need to purchase premier license.

**Usage:** Generated by the Google Maps API. This occurs if your system has configured 2500 or more accounts in a 24-hour period.

**Subsystem:** Integration

**Level:** Warning

## **20.4.178 UCE–25022 integration.address.requestDenied**

**CONVERGE ONLY**

**Message:** Geolocation request denied.

**Subsystem:** Integration

**Level:** Warning

## 21 Properties

The properties *files* are located on each server in the Application cluster and on the Back-up Alarm server. They define the way the system handles various activities. The properties files can be edited with any text editor. Do not attempt to edit them without clearly understanding the implications of your changes.

The Tier Properties are modified from the Management Portal.

The properties defined in the XMPP\_PROPERTY and SYSTEM\_PROPERTY tables are modified by SQL commands.

- [server.properties on page 235](#)
- [custom.properties on page 297](#)
- [mail.properties on page 305](#)
- [message.properties on page 310](#)
- [Tier Properties on page 349](#)
- [Account Read Only Properties on page 349](#)

### 21.1 server.properties

The `server.properties` file located on all the nodes in the Server cluster and on the Converge Back-up Alarm Server. It provides settings that control various activities of each server. This file must be the same for all the servers in the Server cluster. Use the `custom.properties` file to override the values of the `server.properties` file.

The following subsections define the details of each available property.

#### 21.1.1 account.hardDelete.enabled

This property determines what happens when **Delete Account** is clicked on the Account Information page. See the "Deleting an Account" section in *Management Portal Guide*.

Value Type	Value Range	Default Value
boolean	<b>true</b> = delete account information from database <b>false</b> = deactivate account	true

#### 21.1.2 account.activationCode.length

This `server.property` determines the length of auto-generated activation codes. It must be between 6-10. The default value is 6.

Value Type	Value Range	Default Value	Cluster
number	6 -minimum length 10 - maximum length	6	Portal

### 21.1.3 account.activationCode.numberOnly

#### CONVERGE ONLY

This server.property determines whether the Activation Code will only use numbers or will include alphanumeric characters.

Value Type	Value Range	Default Value
boolean	<b>true</b> = Activation codes only generate with numbers. <b>false</b> = Activation codes generate with alphanumeric characters.	true

### 21.1.4 account.character.blacklist

This property lists characters to be excluded from first name and last name fields in both the Management Portal and the web service. Non-ASCII characters are entered in escaped Unicode format.

For example:

```
account.character.blacklist=\u00C5\u00F8\u00EF\u00AB\u00A1\u00BF
```

**Note:** Do not use spaces or punctuation between characters.

This property is not defined in the server.properties file.

Value Type	Value Range	Default Value

### 21.1.5 accountIntegration.returnSecretWord

#### CONVERGE ONLY

This server.property determines whether, upon a getAccount() SOAP request, the information in the response will include the account's secret word. See "[Get Account Information](#)" on page 130 .

Value Type	Value Range	Default Value
boolean	<b>true</b> = The secret word is included in the information with the other account information in the getAccount() return. <b>false</b> = The secret word is NOT included in a getAccount() return.	true

## 21.1.6 alarm.ipAlarmSender

### CONVERGE ONLY

This server.property specifies the name of the implementation class to send IP alarms to the central monitoring station. The value can be:

- copsIpAlarmSender  
Used with the C.O.P.S. Monitoring.
- httpGetAlarmSender  
Used for IP alarm testing without an official IP receiver. If used, you must configure the [alarm.ipAlarmSender.httpGetAlarmSender.baseUrl](#) property (page 237).
- simsAlarmSender  
Used with the SIMS Monitoring.
- dummyAlarmSender  
Used when no IP Alarm Server is specified.

Value Type	Value Range	Default Value
string	N/A	dummyAlarmSender

## 21.1.7 alarm.ipAlarmSender.httpGetAlarmSender.baseUrl

### CONVERGE ONLY

This server property specifies the base URL used for IP alarm testing without an official IP receiver. To use this property set the value of [alarm.ipAlarmSender](#) to [httpGetAlarmSender](#).

Value Type	Value Range	Default Value
string	N/A	http://www.wqwerwerucontrol.com

## 21.1.8 alarm.maxAgeTo.LogError

### CONVERGE ONLY

This server property specifies the maximum time (in seconds) for an alarm to stay in alarm request queue before server starts to log alarm send error.

Value Type	Value Range	Default Value
number		180

### 21.1.9 alarm.maxCheckingPeriodForUnsendAlarm

#### CONVERGE ONLY

This server property specifies the maximum time period (in seconds) to check a failed alarm session.

Value Type	Value Range	Default Value
number	1200 - 3600	1800

### 21.1.10 alarm.multipleCidEnabled

#### CONVERGE ONLY

This server property specifies whether server is allowed to send multiple contact ids to the central monitoring station in a single message.

Value Type	Value Range	Default Value
boolean	<b>true</b> = send multiple CIDs as a single message <b>false</b> = send multiple CIDs as separately	true

### 21.1.11 alarm.queue.concurrentConsumers

#### CONVERGE ONLY

**Note:** Support for telephony servers has been deprecated.

This server property specifies the number of concurrent consumers created by the system to process the alarms in the alarm request queue in a server. This value is the number of phone lines in the telephony server, if the telephony server is the backup alarm sender.

Value Type	Value Range	Default Value
number	1 - 8	4

### 21.1.12 alarm.requestErrorHandler

#### CONVERGE ONLY

This server property specifies the handler class for alarm request failures.

Value Type	Value Range	Default Value
string	N/A	alarmRequestErrorHandler

### 21.1.13 alarm.smashAndGrabDisarmEventLookBackInterval

#### CONVERGE ONLY

This server property is used for Smash & Grab detection. See "Understanding Smash & Grab" on page 112.

### 21.1.14 alarm.smashAndGrabAlarmLookBackInterval

#### CONVERGE ONLY

This server property is used for Smash & Grab detection. See "Understanding Smash & Grab" on page 112.

### 21.1.15 alarm.telephonyAlarmSender

#### DEPRECATED

**Note:** Support for telephony servers has been deprecated.

#### CONVERGE ONLY

This server property specifies the name of the implementation class to send alarms to the central monitoring station over POTS. The value can be:

- dummyAlarmSender  
Used when no Telephony Alarm Server is specified.
- defaultTelephonyAlarmSender

Value Type	Value Range	Default Value
string	N/A	defaultTelephonyAlarmSender

See [alarm.ipAlarmSender](#) on page 235.

If both the IP and the Telephony Servers are specified, the Telephony server is the fallback. See also the following subsections to configure the defaultTelephonyAlarmSender.

### 21.1.16 alarm.unprocessedCheckingPeriod.inWaitingStatus

#### CONVERGE ONLY

This server property specifies the time in seconds that the server waits *after the start of an alarm session* for a Send or Cancel message from the CPE. After this period, if the server has not received a Send or Cancel message, it forwards the alarm to the central monitoring station anyway. The checkWaitingAlarmSession background task uses this server property. See "Background Tasks" on page 298 for details.

Value Type	Value Range	Default Value
positive number	Not zero or lower	45

**Note:** Since the subscriber can set the Transmission Delay from 15 to 45 seconds, this value must not be set to less than 45 seconds.

### 21.1.17 alarm.testDuration

#### CONVERGE ONLY

This server property specifies the length (in seconds) of an alarm test.

Value Type	Value Range	Default Value
positive number		1800 (30 minutes)

### 21.1.18 alerts.allowZoneActivitySms

This server property specifies whether to permit SMS notifications for Touchstone events and for Converge non-alarm related zone activity.

Value Type	Value Range	Default Value
boolean	true	false
	false	

### 21.1.19 api.serverToServer.deltas.enabled

This server property determines whether the Server-To-Server API delivers real time events as a deltas resource via async servlet. For more than larger numbers of users, set this property to **false** and use the real-time Event Bus to deliver events. For more information about the Deltas Resource and the Event Bus, see:

- ❑ [Converge System Architecture Guide](#)
- ❑ [Touchstone System Architecture Guide](#)
- ❑ <https://share-icontrol.atlassian.net/wiki/display/APID/7.3+Quadra+Core+-+Event+Bus+Documentation>
- ❑ <https://share-icontrol.atlassian.net/wiki/display/APID/7.3+Quadra+Core+-+API+Documentation>

**Note:** Support for telephony servers has been deprecated.

Value Type	Value Range	Default Value
boolean	<b>true</b> = The Deltas Resource is enabled. <b>false</b> = The Deltas Resource is disabled.	<a href="http://[serverip]:8080/managementPortal/arsTelephonyRequestCallback">http://[serverip]:8080/managementPortal/arsTelephonyRequestCallback</a>

### 21.1.20 ars.callbackUrl

#### CONVERGE ONLY

**Note:** Support for telephony servers has been deprecated.

This server property specifies the URL for the Telephony server to call back to the Application servers.  
 Note: For cluster deployment, the server IP can be a virtual IP.

Value Type	Value Range	Default Value
string	URL	http://[serverip]:8080/managementPortal/arsTelephonyRequestCallback

### 21.1.21 ars.callbackUrl.backupServer

**CONVERGE ONLY**

**Note:** Support for telephony servers has been deprecated.

This server property specifies the URL for the Telephony server to call back to the backup server.

Value Type	Value Range	Default Value
string	URL	http://[backupserverip]:8080/managementPortal/arsTelephonyRequestCallback

### 21.1.22 ars.asteriskManagerHostname

**CONVERGE ONLY**

This server property specifies the Asterisk manager host name.

Value Type	Value Range	Default Value
string	DEV-MODE=disabled	DEV-MODE

### 21.1.23 ars.asteriskManagerUsername

**CONVERGE ONLY**

This server property specifies the Asterisk manager username.

Value Type	Value Range	Default Value
string		ars

### 21.1.24 ars.asteriskManagerPassword

**CONVERGE ONLY**

This server property specifies the Asterisk manager password.

Value Type	Value Range	Default Value
string		Asterisk manager password.

## 21.1.25 ars.asteriskChannelDialPrefix

### CONVERGE ONLY

This server property specifies the Asterisk Channel Dial Prefix.

Value Type	Value Range	Default Value
string	g3 (test) g1 (production)	ucontrol

## 21.1.26 asyncServlet.scavangeInterval

### CONVERGE ONLY

This server property sets the interval period (in seconds) for REST API Deltas requests: the interval period at which async requests are checked for timeouts. For more information about the Deltas, see:

<https://share-icontrol.atlassian.net/wiki/display/APID/7.3+Quadra+Core+-+REST+API+User+Guides>

Value Type	Value Range	Default Value	Unit
integer	Greater than zero.	10	seconds

## 21.1.27 backupServer.ip

### CONVERGE ONLY

This server property specifies the Back-up Alarm Server Ethernet IP. If this property is defined, Backup GPRS Server IP and Backup GPRS APN are required fields when creating a new cellular profile in the Management Portal. If this property is not defined, these fields are not required when creating a new cellular profile in the Management Portal.

For more information, see the "Managing Cellular Profiles (Converge Only)" section in *Management Portal Guide*.

Value Type	Value Range	Default Value
string	IP address	ip

## 21.1.28 batchUpdateItem.percentageToAbort

This server property specifies the percentage below which to abort a firmware update batch update.

Value Type	Value Range	Default Value
positive number	1-100	5

## 21.1.29 batchUpdateItem.size

This server property specifies the size of the sub-batches within a firmware update batch job.

Value Type	Value Range	Default Value
positive number	1 - 1000	400

### 21.1.30 batchUpdateItem.successPercentage

This server property specifies the percentage above which a firmware update sub-batch is considered a success.

Value Type	Value Range	Default Value
positive number	1-100	80

### 21.1.31 batchUpdateItem.timeout

This server property specifies the number of seconds until a firmware update sub-batch must have completed a configured percentage of devices (batchUpdateItem.percentageToAbort) or else the system will stop the sub-batch and go on to the next one.

Value Type	Value Range	Default Value
Value Type	Value Range	Default Value
positive number	1200 - 2700	1800

### 21.1.32 batchUpdateRequest.sleepInterval

This server property specifies the number of milliseconds the server should pause between issuing firmware update requests. This value is used to prevent queue flooding.

Value Type	Value Range	Default Value
positive number	500 - 3000	500 (that is, one half second)

### 21.1.33 batchUpdateTask.runInterval

This server property specifies the number of milliseconds until the system checks each firmware update batch progress. This value is used to prevent queue flooding.

Value Type	Value Range	Default Value
positive number		250000 (that is, 4.5 minutes)

### 21.1.34 broadbandCommunicationEvent.markFactor

This server property is used in conjunction with the connection.broadbandQuickHeartBeatRate tier property to manage how connectivity losses are displayed in the Management Portal.

The relevant formula is:

(broadbandCommunicationEvent.markFactor minus 1) times (connection.broadbandHeartBeatRate)  
plus 2 minutes

For example, if the value for this property is 2 and the heartbeat tier property value is 10 minutes,

{ (2 minus 1) times (10 minutes) } plus 2 minutes

then IF the system misses a broadband heartbeat from an account, the Management Portal will wait 12 minutes (10 minutes plus 2 minutes) for the account to re-establish the connection before it displays that broadband is down on the Account Information screen.

However, if the value for this property is 1,

{ (1 minus 1) times (10 minutes) } plus 2 minutes

then the Management Portal will only wait 2 minutes for the account to re-establish a broadband connection before it displays the down status on the Account Information screen.

Value Type	Value Range	Default Value
positive number		2

### 21.1.35 broadbandDownCellularMsg.max.try

#### CONVERGE ONLY

This server property specifies the number of times to send the broadband down message over cellular channel if no ack message is received.

Value Type	Value Range	Default Value
positive number		2

### 21.1.36 bundle.import.file.format

This server property specifies the file format of the imported bundles data file. This text file, which contains a list of bundles, is imported into the Management Portal. The bundleId is the only supported field, so you must use the default value.

For more information, see the "Import Multiple Bundles" section in *Management Portal Guide*.

Value Type	Value Range	Default Value
string		bundleId

#### Example File Format

```
Bundle ID
CPE Bundle ID 1
CPE Bundle ID 2
CPE Bundle ID 3
```

CPE Bundle ID 4

### 21.1.37 bundle.import.log.directory

#### 21.1.38 bundle.import.log.directory.windows

This server property specifies the absolute root directory to save the log file for importing a bundle.

Operating System	Value Type	Value Range	Default Value
Linux	string	Directory path	\${share.file.root}/bundleImport
Windows			\${share.file.root.windows}\bundleImport

### 21.1.39 cameraAccessProxyUrl

This server property specifies the relative URL to the camera access proxy server.

Value Type	Value Range	Default Value
string	URL	/cameraProxy/proxy

### 21.1.40 camera.firmwareBaseUrl

This server property specifies the absolute base URL for camera device firmwares.

Value Type	Value Range	Default Value
string	URL	dummy

**IMPORTANT:** The device descriptor list relies on the configured value of this property to function.

See *Management Portal Guide* for information about the Device Descriptor List and the `blacklist.xml`, as well as related concepts such as Tiers, Packages, and Tier Properties.

### 21.1.41 cameraVideoRecordUrl

This server property specifies the relative URL to the video clip HTTP post server.

Value Type	Value Range	Default Value
string	URL	/cameraProxy/video

### 21.1.42 cat.onboarding.complete.redirectUrl

This server property specifies the redirect URL for Card UI Subscriber Portal users after a cloud object is associated with the user's account.

The default value must be changed in environments where the Card UI Subscriber Portal has been implemented.

Value Type	Value Range	Default Value	Clusters
string	Full or relative URL	/cui/onboardingcompleted.html	Portal

## 21.1.43 cellular.import.file.format

### CONVERGE ONLY

This server property specifies the field format of comma-delimited file for batch importing SIM cards to inventory.

See *Management Portal Guide* for information about how to use this setting.

Value Type	Value Range	Default Value
string (comma delimited)	N/A	iccid,phoneNumber,accountNumber

## 21.1.44 cellular.import.log.directory

## 21.1.45 cellular.import.log.directory.windows

### CONVERGE ONLY

This server property specifies the absolute root directory to save the log file for operations related to importing cellular touchscreen data.

Operating System	Value Type	Value Range	Default Value
Linux	string	Directory path	\${share.file.root}/cellularImport
Windows			\${share.file.root.windows}\cellularImport

## 21.1.46 centralStation.emergencyContact.notify

### CONVERGE ONLY

This server property specifies the maximum number permitted for a monitored account of emergency contacts that are NOTIFIED by the central monitoring station when an alarm is tripped at a premise. See also [centralStation.emergencyContact.verify.min](#).

Value Type	Value Range	Default Value
integer	> 1	2

## 21.1.47 centralStation.emergencyContact.verify.min

## 21.1.48 centralStation.emergencyContact.verify.max

### CONVERGE ONLY

These server properties specify the minimum/maximum number of emergency contacts—who are contacted to verify that an alarm event is genuine—that are permitted for a monitored account.

Due to central station limitation, these values must be the same.

Value Type	Value Range	Default Value
integer	> 1	2

### 21.1.49 centralStation.implementation

#### CONVERGE ONLY

This server property specifies the name of the implementation class for communicating with the central monitoring station about account changes.

Value Type	Value Range	Default Value
enum	<ul style="list-style-type: none"> <li><input type="checkbox"/> diceCentralstationMessageSender for synchronous integration to communicate with the DICE central monitoring station.</li> <li><input type="checkbox"/> simsCentralstationMessageSender for synchronous integration to communicate with the SIMS central monitoring station. The value for <a href="#">alarm.ipAlarmSender</a> must be set to <a href="#">simAlarmSender</a>. See page <a href="#">237</a> for other required settings.</li> <li><input type="checkbox"/> copsCentralstationMessageSender for synchronous integration to communicate with the COPS central monitoring station. The value for <a href="#">alarm.ipAlarmSender</a> must be set to <a href="#">copsIpAlarmSender</a>. See page <a href="#">301</a> for other required settings.</li> <li><input type="checkbox"/> emailCentralstationMessageSender for ASYNCHRONOUS integration to communicate with the central monitoring station using email</li> </ul>	emailCentralStationMessageSender

See also the other integration-related server.properties:

- [centralStation.emergencyContact.notify](#)
- [centralStation.emergencyContact.verify.min](#)
- [centralStation.integration.enabled](#)
- [centralStation.integration.synchronous](#)
- [centralStation.integration.accountCreation.waitTime](#)
- [centralStation.notification emailAddress.to](#)
- [centralStation.notification emailAddress.from](#)

## 21.1.50 centralStation.integration.enabled

### CONVERGE ONLY

This server property specifies whether the system communicates account changes to central station.

Value Type	Value Range	Default Value
boolean	<input type="checkbox"/> true (system uses central station account integration) <input type="checkbox"/> false (system DOES NOT use central station account integration)	false

When this value is set to true and [centralStation.integration.synchronous](#) is set to true, Management Portal users can search for accounts with an "integration failure" flag. See the "Searching for a Customer Account" section in *Management Portal Guide* for more information.

## 21.1.51 centralStation.integration.synchronous

### CONVERGE ONLY

This server property specifies whether the system communicates account changes to the central monitoring station synchronously or asynchronously (via email).

Value Type	Value Range	Default Value
boolean	<input type="checkbox"/> true (synchronous integration) <input type="checkbox"/> false (asynchronous integration)	false

This property is used with the [centralStation.integration.enabled](#) property to search for accounts in the Management Portal for accounts with an "integration failure" flag.

## 21.1.52 centralStation.integration.accountCreation.waitTime

### CONVERGE ONLY

This server property specifies the number of seconds to wait for an acknowledgment from the central monitoring station that a new account data was successfully received.

For synchronous integration only ([centralStation.integration.synchronous=true](#)).

Value Type	Value Range	Default Value
positive number		30

### 21.1.53 centralStation.notification emailAddress.to

#### CONVERGE ONLY

This server property specifies the email address of the central monitoring station.

For asynchronous integration only ([centralStation.integration.synchronous=false](#)).

Value Type	Value Range	Default Value
string	N/A	DEV-MODE

## 21.1.54 centralStation.numberOfQueue

### CONVERGE ONLY

The number of the JMS queues used for notification of account changes.

**Note:** This helps limit the timeouts for an account observed by a Management Portal user when attempting to save account edits.

Value Type	Value Range	Default Value
string	N/A	3

## 21.1.55 centralStation.notification emailAddress.to

### CONVERGE ONLY

This server property specifies the email address of the central monitoring station.

For asynchronous integration only ([centralStation.integration.synchronous=false](#)).

Value Type	Value Range	Default Value
string	N/A	DEV-MODE

## 21.1.56 centralStation.notification emailAddress.from

### CONVERGE ONLY

This server property specifies the email address to which the central monitoring station sends responses.

For asynchronous integration only ([centralStation.integration.synchronous=false](#)).

Value Type	Value Range	Default Value
string	N/A	DEV-MODE

## 21.1.57 cloudIntegration.accountGroupAutoAdd

This server property specifies whether to add accounts to a specific cloud integration account group automatically at the time of onboarding.

Value Type	Value Range	Default Value	Clusters
boolean	<input type="checkbox"/> <b>true</b> (system adds accounts to a cloud integration account group automatically) <input type="checkbox"/> <b>false</b> (system DOES NOT add accounts to a cloud integration account group automatically; instead, the account group must be associated with the account manually)	false	Portal

### 21.1.58 cloudIntegration.accuWeather.temperatureChangeNotificationBlackoutPeriod

This server property specifies the AccuWeather temperature change notification blackout period (in hours). This property only applies when using the temperature trigger to send email or text message notifications to a user. During the blackout period, the user will not receive any temperature notifications via email or text message.

Value Type	Value Range	Default Value
integer		6

### 21.1.59 cloudIntegration.auto.commit.enable

This server property specifies whether to write the latest consumed offset to ZooKeeper for the Cloud Automation and Control CPE event consumer.

Value Type	Value Range	Default Value	Clusters
boolean		false	CPE

### 21.1.60 cloudIntegration.auto.offset.reset

This server property specifies the offset value when there is no initial offset in ZooKeeper or if an offset is out of range for the Cloud Automation and Control CPE event consumer.

Possible values are:

- smallest: automatically resets the offset to the smallest offset
- largest: automatically resets the offset to the largest offset

Value Type	Value Range	Default Value	Clusters
string		largest	CPE

### 21.1.61 cloudIntegration.consumer.group.name.prefix

This server property specifies the prefix of the Cloud Automation and Control CPE event consumer group name.

Group name format: cloudIntegration-<WebLogic server name>

Example: cloudIntegration-managedServer1

The suffix of the consumer group name is the WebLogic server name, which is defined by the value of `cloudIntegration.server.name.system.property`

**IMPORTANT:** Do not change the value of this property from its default value unless your Icontrol representative advises otherwise.

Value Type	Value Range	Default Value	Clusters
string		cloudIntegration-	CPE

### 21.1.62 cloudIntegration.consumer.thread.count

This server property specifies the number of consumer threads per topic for the Cloud Automation and Control CPE event consumer.

Value Type	Value Range	Default Value	Clusters
integer		2	CPE

### 21.1.63 cloudIntegration.consumer.timeout.ms

This server property specifies the Kafka consumer timeout (in milliseconds) for the Cloud Automation and Control CPE event consumer.

Value Type	Value Range	Default Value	Clusters
integer		1000	CPE

### 21.1.64 cloudIntegration.enabled

This server property specifies whether cloud integration is enabled. The default value is false.

Value Type	Value Range	Default Value	Clusters
boolean	<input type="checkbox"/> <b>true</b> (Cloud integrations are enabled) <input type="checkbox"/> <b>false</b> (Cloud integrations are disabled)	false	CPE

### 21.1.65 cloudIntegration.history.consumer.thread.count

This server property specifies the number of consumer threads per topic.

Value Type	Value Range	Default Value
integer		2

### 21.1.66 cloudIntegration.history.enabled

This server property specifies whether events are enabled for the cloud integration history service.

Value Type	Value Range	Default Value
boolean	<input type="checkbox"/> <b>true</b> (Events are enabled) <input type="checkbox"/> <b>false</b> (Events are disabled)	false

### 21.1.67 cloudIntegration.history.service.appkey

This server property specifies the encrypted AppKey that the Icontrol Server uses to access the cloud integration history service API.

**IMPORTANT:** Do not change the value of this property from its default value unless your Icontrol representative advises otherwise.

Value Type	Value Range	Default Value
string		3DES_!MiKDkp3o+aQHCLzxC22z/Y/zg92AxuX

### 21.1.68 cloudIntegration.history.service.password

This server property specifies the encrypted password that the Icontrol Server uses to access the cloud integration history service API.

**IMPORTANT:** Do not change the value of this property from its default value unless your Icontrol representative advises otherwise.

Value Type	Value Range	Default Value
string		3DES_qI7TtOXZMiDVfU1PJbPeUw==

### 21.1.69 cloudIntegration.history.service.username

This server property specifies the username that the Icontrol Server uses to access the cloud integration history service API.

**IMPORTANT:** Do not change the value of this property from its default value unless your Icontrol representative advises otherwise.

Value Type	Value Range	Default Value
string		historyservice

### 21.1.70 cloudIntegration.internal.topic

This server property specifies the Kafka topic name for internal outgoing cloud events. This property is required if cloud integration is enabled.

**IMPORTANT:** Do not change the value of this property from its default value unless your Icontrol representative advises otherwise.

Value Type	Value Range	Default Value	Clusters
string	N/A	cloudIntegrationInternal	CPE, Portal

### 21.1.71 cloudIntegration.metadata.broker.list

This server property specifies a list of Kafka hosts and their ports that act as brokers for a cloud integration. This property is required if cloud integrations are enabled.

**Note:** This property is disabled by default and can be enabled only in the `custom.properties` file.

Value Type	Value Range	Default Value	Clusters
string	N/A	host1:port1,host2:port2	CPE

### 21.1.72 cloudIntegration.oauth2.redirectUrl

This server property specifies the root URL to send in the OAuth 'redirect\_uri'. This property is used only if CLOUD\_OBJECT\_DEF.USE\_REDIRECT\_URL in the Icontrol database is set to true for a partner.

Value Type	Value Range	Default Value
string	URL	

Example: https://servername/oauth

### 21.1.73 cloudIntegration.partnerProxy.connectionPool.connectTimeout

This server property specifies how long (in milliseconds) to wait before disconnecting a partner server from the Icontrol Server due to inactivity.

Value Type	Value Range	Default Value
integer		1800000

### 21.1.74 cloudIntegration.partnerProxy.connectionPool.defaultMaxPerRoute

This server property specifies the maximum number of connections allowed per host. This is used to manage HTTP client connection pooling to the Icontrol Server.

Value Type	Value Range	Default Value
integer		10

### 21.1.75 cloudIntegration.partnerProxy.connectionPool.maxTotal

This server property specifies the maximum number of connections available to the Icontrol Server.

Value Type	Value Range	Default Value
integer		100

### 21.1.76 cloudIntegration.partnerProxy.connectionPool.requestTimeout

This server property specifies the timeout (in milliseconds) used to get a connection from the Icontrol Server's connection pool.

Value Type	Value Range	Default Value
integer		10000

### 21.1.77 cloudIntegration.server.name.system.property

This server property specifies the suffix of the Cloud Automation and Control CPE event consumer group name. The suffix of the group name is the WebLogic server name, which is derived from the value of the system property name (weblogic.Name).

Group name format: cloudIntegration-<WebLogic server name>

Example: cloudIntegration-managedServer1

The prefix of the consumer group name is defined by the value of `cloudIntegration.consumer.group.name.prefix`

**IMPORTANT:** Do not change the value of this property from its default value unless your Icontrol representative advises otherwise.

Value Type	Value Range	Default Value	Clusters
string		weblogic.Name	CPE

### 21.1.78 cloudIntegration.topic

This server property specifies the Kafka topic name for incoming cloud events. This property is required if cloud integration is enabled.

**IMPORTANT:** Do not change the value of this property from its default value unless your Icontrol representative advises otherwise.

Value Type	Value Range	Default Value	Clusters
string	N/A	cloudIntegration	CPE, Portal

### 21.1.79 cloudIntegration.zookeeper.connect

This server property specifies the ZooKeeper connection string in the form `hostname:port,hostname:port` where hostname and port are the host and port for a node in your ZooKeeper cluster for the Cloud Automation and Control CPE event consumer.

**Note:** This property must be added to the `custom.properties` file for CPE servers.

To allow connection through other ZooKeeper nodes when the host is down, you can specify a comma-separated list of multiple hosts as follows: `hostname1:port1,hostname2:port2,hostname3:port3`

Value Type	Value Range	Default Value	Clusters
String		127.0.0.1:2181	CPE

### 21.1.80 cloudIntegrationHistory.auto.commit.interval.ms

This server property specifies the frequency (in milliseconds) that consumer offsets are committed to ZooKeeper.

Value Type	Value Range	Default Value
integer		1000

### 21.1.81 cloudIntegrationHistory.auto.offset.reset

This server property specifies the offset value when there is no initial offset in ZooKeeper or if an offset is out of range.

Possible values are:

- smallest: automatically resets the offset to the smallest offset
- largest: automatically resets the offset to the largest offset

Value Type	Value Range	Default Value
string		smallest

### 21.1.82 cloudIntegrationHistory.zookeeper.connect

This server property specifies the ZooKeeper connection string in the form hostname:port,hostname:port where hostname and port are the host and port for a node in your ZooKeeper cluster.

**Note:** This property is disabled by default and can be enabled only in the `custom.properties` file.

To allow connection through other ZooKeeper nodes when the host is down, you can specify a comma-separated list of multiple hosts as follows: hostname1:port1,hostname2:port2,hostname3:port3

Value Type	Value Range	Default Value
String		

### 21.1.83 cloudIntegrationHistory.zookeeper.session.timeout.ms

This server property specifies the ZooKeeper timeout (in milliseconds). If the consumer fails to send a heartbeat to ZooKeeper for this period of time, it is considered dead and a rebalance will occur.

Value Type	Value Range	Default Value
integer		6000

### 21.1.84 cloudIntegrationHistory.zookeeper.sync.time.ms

This server property specifies the amount of time (in milliseconds) that a ZooKeeper follower can lag behind a ZooKeeper leader.

Value Type	Value Range	Default Value
integer		2000

### 21.1.85 cls.auth.password

This server property specifies the password for the authorized LDAP user.

Value Type	Value Range	Default Value	Clusters
string			CPE, Portal

### 21.1.86 cls.auth.username

This server property specifies the user ID for the authorized LDAP user.

Value Type	Value Range	Default Value	Clusters
string			CPE, Portal

### 21.1.87 cls.url

This server property specifies the URL to the Cluster Location Service. This must be in the following format: `http://<IP>:<Port>/cls-admin`

Value Type	Value Range	Default Value	Clusters
string			CPE, Portal

### 21.1.88 cls.cluster.hostname

This server property specifies the hostname or IP address of the current cluster.

**Note:** This value must be set, even if CLS is not enabled.

Value Type	Value Range	Default Value	Clusters
string			CPE, Portal

### 21.1.89 cls.cluster.number

This server property indicates the cluster number for the current cluster.

Value Type	Value Range	Default Value	Clusters
string		1	CPE, Portal

### 21.1.90 cls.domain

This server property specifies the CLS domain name. If CLS is enabled, this value must be the same as the domain column in the `user_entry` table in the CLS database.

**IMPORTANT:** Do not change the value of this property from its default value unless your Icontrol representative advises otherwise.

Value Type	Value Range	Default Value	Clusters
string		icontrol	CPE, Portal

### 21.1.91 cls.enabled

This server property specifies whether Cluster Location Service (CLS) is enabled.

Value Type	Value Range	Default Value	Clusters
Boolean	<b>true</b> = CLS is enabled. <b>false</b> = CLS is disabled.	false	CPE, Portal

### 21.1.92 cls.username.prefix

This server property specifies a prefix for system-generated temporary user names in the current cluster. The naming convention is `cx_` where `x` is the cluster number (`x=1` for the first cluster, `2` for the second cluster, and so on).

Make sure that no username with the selected prefix exists before specifying a value.

Value Type	Value Range	Default Value	Clusters
string		c1_	CPE, Portal

### 21.1.93 command.default.timeout

#### CONVERGE ONLY

This server property specifies the time (in seconds) the server waits before considering a command timed out.

**Note:** A command that is in the status *created*, *queued*, *sent* status is marked *timedout* only during initial inform. If a touchscreen is not connected via broadband, the command status does not go to change until it comes on line.

Value Type	Value Range	Default Value
positive number		300

### 21.1.94 command.firmwareupdate.timeout

#### CONVERGE ONLY

This server property specifies the firmware update command timeout in seconds.

Value Type	Value Range	Default Value
positive number		3600 (that is, 1 hour)

### 21.1.95 command.multicast.delay

#### CONVERGE ONLY

This server property specifies the how frequently (in milliseconds) to send multicast commands, that is a single command sent to multiple touchscreens—for example, a new touchscreen app download.

Value Type	Value Range	Default Value
positive number	500 - 10,000	5000 (that is, 5 seconds)

### 21.1.96 configUrl

#### CONVERGE ONLY

This server property specifies the relative URL to upload the touchscreen configuration files.

Value Type	Value Range	Default Value
string	URL	/fileUpload/cpeConfig

### 21.1.97 contextPathForLoginURL

This server property specifies the suffix of the URL used for logging into the Subscriber Portal and the Subscriber Portal Backdoor.

Value Type	Value Range	Default Value
string		/login.jsp

### 21.1.98 contextPathForResetPassword

This server property specifies the suffix of the URL that is included in the email that is sent to a subscriber when the subscriber clicks the "Forgot your Password?" link on the login page of a REST-based portal (e.g., Card UI Mobile App and Web App) to reset the subscriber's password.

**Note:** This property is used for REST-based portals only. The "classic" Subscriber Portal uses the subscriberPortalRootUrl property.

Value Type	Value Range	Default Value
string		/#view=missingcredentials?cto=

The generated URL uses the following format, and the prefix of the one-time code is the product name (converge or insight).

`https://<host>/cui/#view=missingcredentials?cto=<product>_<one-time-code>`

#### Example URLs for Reset Password

Converge: `https://beta.icontrol.com/cui/view=missingcredentials?cto=converge_1035014319889`

Touchstone: `https://beta.icontrol.com/cui/view=missingcredentials?cto=insight_1035014319889`

#### Example Email for Reset Password

A subscriber receives the following email when the value of the contextPathForResetPassword property is `/#view=missingcredentials?cto=`:

From: <system@beta.icontrol.com>  
 Date: Oct 8, 2015 1:01 PM  
 Subject: Your Account Password  
 To: <bob@company.com>  
 Cc:

To reset your password we'll need some more account validation.

Click the following link to reset your password:

`https://beta.icontrol.com/cui/view=missingcredentials?cto=converge_1035014319889`

Please call customer service if you still cannot access your account.

## 21.1.99 converge.camera.trouble.enabled

### CONVERGE ONLY

This server property enables/disables camera communication trouble events on the Converge server. Camera troubles are displayed on the Subscriber Portal and Management Portal. When the value of this property is true, camera troubles are stored in the database for Converge accounts. If you change the value to false, existing camera troubles will remain in the database unless you manually clear them.

**Note:** This does not affect Touchstone camera trouble reporting, as camera communication trouble events are already enabled on Touchstone.

Value Type	Value Range	Default Value
boolean	<b>true</b> = enable camera trouble events <b>false</b> = disable camera trouble events	true

## 21.1.100 converge.sendActivationEmail

### CONVERGE ONLY

This server property specifies whether to send an activation email to the subscriber.

**Note:** Not applicable if the service provider has SSO enabled. When SSO is enabled, an activation email is not sent to the subscriber.

Value Type	Value Range	Default Value
boolean	<b>true</b> = send an email <b>false</b> = do not send an email	true

For Touchstone systems, see "insight.sendActivationEmail" on page 272.

## 21.1.101 cpe.diagnostics.<suffix>

The following server properties are used for the diagnostics offloading feature. For more information, see: <https://share-icontrol.atlassian.net/wiki/display/CSKB/7.3+Quadra+-+Diagnostics+Offloading>

- cpe.diagnostics.AuthorizationHeader
- cpe.diagnostics.URL

## 21.1.102 cpe.import.file.format

### CONVERGE ONLY

This server property specifies the field format of comma-delimited file for batch importing Converge touchscreen devices to inventory.

See *Management Portal Guide* for information about how to use this setting.

Value Type	Value Range	Default Value
string	comma-delimited string	itemNumber, poNumber, model, serialNumber, macAddress, zigbeeSN, iccid, imeiNumber, shipDate

## 21.1.103 cpe.import.file.format.insight

### TOUCHSTONE ONLY

This server property specifies the field format of comma-delimited file for batch importing Touchstone devices to inventory.

See *Management Portal Guide* for information about how to use this setting.

Value Type	Value Range	Default Value
string	comma-delimited string	itemNumber, poNumber, model, serialNumber, macAddress, shipDate

## 21.1.104 cpe.import.log.directory

## 21.1.105 cpe.import.log.directory.windows

### CONVERGE ONLY

These server properties specify the absolute root directory to save the log file for touchscreen inventory file import.

Operating System	Value Type	Value Range	Default Value
Linux	string	Directory path	\${share.file.root}/cpelimport
Windows			\${share.file.root.windows}\cpelimport

### 21.1.106 cpe.panicScreenDisabled

#### CONVERGE ONLY

This server property specifies whether the Emergency screen is accessed when the Panic button is pressed.

Value Type	Value Range	Default Value
boolean	<p><b>true</b> = Emergency Screen is disabled. The user is presented with instructions for what to do in the case of an emergency. The default text is “In case of an emergency please dial 911.” Contact your Icontrol representative for assistance in editing the default text for your brand.</p> <p><b>false</b> = The Emergency Screen is enabled. The user is presented with the standard Emergency screen functionality.</p>	true

For Touchstone systems, see ["insight.sendActivationEmail"](#) on page 272.

### **21.1.107 cpe.telemetry.collection.maxDay**

This server property specifies the maximum time (in days) allowed for CPE telemetry collection and upload..

Value Type	Value Range	Default Value
Integer		900

### **21.1.108 database.monitor.average.duration**

This server property specifies how often, in seconds, to re-calculate the average transaction time. The average transaction time is the total of each transaction time spent divided by the number of transactions.

Value Type	Value Range	Default Value
Integer		900

### **21.1.109 database.monitor.operation.interval**

This server property specifies how often, in milliseconds, a background task reads/writes and queries the database sample tables

Value Type	Value Range	Default Value
integer		60000

### **21.1.110 database.monitor.renew.duration**

This server property specifies how long to keep database monitoring results, in hours.

Value Type	Value Range	Default Value
Integer		1140 (47.5 days)

### **21.1.111 database.userName**

This server property specifies the user name used to connect to the iControl database.

Value Type	Value Range	Default Value
string		UCONTROL

### 21.1.112 deploymentCustomerName

This server property specifies the deployment name for the current installation.

**Note:** These properties are only applicable for installations that DO NOT use multiple deployments.  
See the multiple.deployment property.

Value Type	Value Range	Default Value
string		uControl

### 21.1.113 deploymentCustomerSupportPhone

This server property specifies the phone number for Customer Care.

**Note:** These properties are only applicable for installations that DO NOT use multiple deployments.  
See the multiple.deployment property.

Value Type	Value Range	Default Value
string		1-866-608-8324

### 21.1.114 deploymentCustomerSupportEmail

This server property specifies the email address for Customer Care

**Note:** These properties are only applicable for installations that DO NOT use multiple deployments.  
See the multiple.deployment property.

Value Type	Value Range	Default Value
string	Properly formatted email address	support@ucontrol.com

### 21.1.115 device.diagnostic.directory

#### 21.1.116 device.diagnostic.directory.windows

This server property specifies the absolute directory to save the diagnostic file from a CPE.

Operating System	Value Type	Value Range	Default Value
Linux	string	Directory path	\${share.file.root}/diagnostic
Windows			\${share.file.root.windows}\diagnostic

### 21.1.117 device.dump.directory

#### 21.1.118 device.dump.directory.windows

This server property specifies the absolute directory to save the dump file from a CPE.

Operating System	Value Type	Value Range	Default Value
Linux	string	Directory path	\${share.file.root}/dump
Windows			\${share.file.root.windows}\dump

### 21.1.119 device.firmwareBaseUrl

This server property defines the absolute base URL for CPE firmware versions.

Value Type	Value Range	Default Value
string	URL	dummy

**IMPORTANT:** The device descriptor list relies on the configured value of this property to function.

See *Management Portal Guide* for information about the Device Descriptor List and the `blacklist.xml`, as well as related concepts such as Tiers, Packages, and Tier Properties.

### 21.1.120 device.image.directory

#### 21.1.121 device.image.directory.windows

This server property specifies the absolute root directory to save the image file for a CPE.

Operating System	Value Type	Value Range	Default Value
Linux	string	Directory path	<code> \${share.file.root}/image</code>
Windows			<code> \${share.file.root.windows}\`</code>

### 21.1.122 device.screenshot.directory

#### 21.1.123 device.screenshot.directory.windows

This server property specifies the absolute root directory to save the screenshot file from a CPE.

Operating System	Value Type	Value Range	Default Value
Linux	string	Directory path	<code> \${share.file.root}/screenshot</code>
Windows			<code> \${share.file.root.windows}\`screenshot</code>

### 21.1.124 device.tamper.enabled

#### CONVERGE ONLY

This server property specifies whether the touchscreen should send trouble events when it is being tampered with, including when the touchscreen is removed from its stand or wall mount. This server property and the CPE property `device.tamper.enabled` must both be set to "true" for the tamper trouble and tamper trouble cleared events to be sent to the server. For more information on CPE properties, see the "Advanced Group Reports" section in *Management Portal Guide*.

Value Type	Value Range	Default Value
boolean	<b>true</b> = yes <b>false</b> = no	false

**Note:** If the touchscreen is in a tampered state when the CPE or server device.tamper.enabled property is set to "false", the tamper trouble cleared event will not be sent when the touchscreen becomes no longer tampered. If the server property is modified, the touchscreen must be rebooted to clear the trouble from the touchscreen and user interfaces. If the CPE property is modified, the trouble will clear from the touchscreen, but it will not clear from the user interfaces until the touchscreen is rebooted.

### 21.1.125 diagnosticUrl

This server property specifies the relative URL to upload diagnostic data.

Value Type	Value Range	Default Value
string	URL	/fileUpload/diagnosticFile

### 21.1.126 distributed.cache.enabled

This server property specifies whether distributed cache is enabled for the system.

Value Type	Value Range	Default Value
boolean	<b>true</b> = distributed cache enabled for this system <b>false</b> = distributed cache is NOT enabled for this system	true

### 21.1.127 dumpUrl

This server property specifies the relative URL to upload dump files.

Value Type	Value Range	Default Value
string	URL	/fileUpload/diagnosticFile

### 21.1.128 email.queue.concurrentConsumers

This server property specifies the number of concurrent consumers for the email queue.

Value Type	Value Range	Default Value
integer	Greater than zero	4

### 21.1.129 eventHistory.query.dateRange.max

The maximum number of days that history event can be queried by a subscriber.

Value Type	Value Range	Default Value
positive number	Any whole number greater than zero.	2

### 21.1.130 eventIntegration.enabled

The Operator Domain includes the Event Bus.

Value Type	Value Range	Default Value
boolean	<b>true</b> = Event Bus is employed in the current configuration  <b>false</b> = Event Bus is not employed	false

### 21.1.131 firmware.allowDowngrade

This server property specifies whether devices will be offered to install earlier than current firmware versions.

Value Type	Value Range	Default Value
boolean	<b>true</b> = allow  <b>false</b> = do not allow	false

### 21.1.132 firmware.download.timeout

This server property specifies the timeout, in milliseconds, to download the content of the firmware.

Value Type	Value Range	Default Value
Integer		600000

### 21.1.133 firmware.misc.directory

#### 21.1.134 firmware.misc.directory.windows

These server properties specify the absolute root directory to save the files associated with firmware.

Operating System	Value Type	Value Range	Default Value
Linux	string	Directory path	\${share.file.root}/firmware
Windows			\${share.file.root.windows}\firmware

### 21.1.135 firmware.suspendedAccountReconnectTime

#### CONVERGE ONLY

This server property specifies the time (in hours) from the time of suspension for a suspended account to reconnect to server to check account status (-1 means never).

Value Type	Value Range	Default Value
Integer;	-1 and greater	12
-1 and greater		

### 21.1.136 firmware.waitTimeAfterDisarm

#### **CONVERGE ONLY**

This server property specifies the number of seconds the system will wait after a subscriber system has been disarmed to queue the touchscreen for firmware update.

Value Type	Value Range	Default Value
integer		300 (that is 5 minutes)

### 21.1.137 imageUrl

This server property specifies the relative URL to upload images.

Value Type	Value Range	Default Value
string	URL	/fileUpload/image

### 21.1.138 grps.test.enabled

#### **CONVERGE ONLY**

deprecated

### 21.1.139 gprs.port

#### **CONVERGE ONLY**

This server property specifies the cellular (GPRS) port.

Value Type	Value Range	Default Value
integer	1025 to 10000	9091

### 21.1.140 gprs.client.port

#### **CONVERGE ONLY**

This server property specifies the touchscreen cellular (GPRS) port.

Value Type	Value Range	Default Value
integer	1025 to 10000	9091

### 21.1.141 gprs.handlerPoolSize

#### **CONVERGE ONLY**

This server property specifies the size of the UDP packet handler thread pool.

Value Type	Value Range	Default Value
integer	Greater than 1	2

## 21.1.142 gprs.encrypt

### CONVERGE ONLY

This server property specifies whether UDP messages are encrypted.

Value Type	Value Range	Default Value
boolean	<b>true</b> = UDP messages are encrypted  <b>false</b> = UDP messages are not encrypted	false

## 21.1.143 html.inputtype.text.autocomplete

This server property specifies whether to allow auto-complete for text fields in the Subscriber Portal and the Management Portal.

Value Type	Value Range	Default Value
boolean	<b>true</b> = allow  <b>false</b> = do not allow	false

## 21.1.144 http.client.connection.default.connection.timeout<.module>

This server property specifies the timeout (in milliseconds) until a connection is established. This property is defined for both the CPE server and the Portal server.

Value Type	Value Range	Default Value
integer		60000

In the `custom.properties` file, you can replace `<.module>` with one of the modules listed in the following table. Prior to Quadra, this timeout value was hard-coded. The following table compares the pre-Quadra hard-coded value with this property's default value for each module. The base property value overrides the hard-coded value. If the base property value cannot be determined, the timeout is set to the hard-coded value.

**IMPORTANT:** Pre-Quadra values are different from the property default value. If you are upgrading to Quadra, additional tuning may be required.

Module	Hard-Coded Value (Before Quadra)	Property Default Value
restSamlAuth	20000	60000
rogersAuth	10000	60000
sunriseSunsetTime	4000	60000

In the `custom.properties` file, you can have multiple occurrences of this property using a different module/value for each occurrence.

Examples:

- http.client.connection.default.connection.timeout.restSamlAuth=60000
- http.client.connection.default.connection.timeout.sunriseSunsetTime=50000

If a timeout value is specified for a module in the `custom.properties` file, this value overrides the base property value. If no timeout is specified for a module in the `custom.properties` file, the timeout is set to the base property value.

### 21.1.145 http.client.connection.default.connection.timeout.clsIntegration

This server property specifies the timeout (in milliseconds) until a connection is established for Cluster Location Service (CLS) integration. This property is defined for both the CPE server and the Portal server.

Value Type	Value Range	Default Value
integer		1800000

Prior to Quadra, this timeout value was hard-coded. The following table compares the pre-Quadra value with this property's default value. The base property value overrides the hard-coded value. If the base property value cannot be determined, the timeout is set to the hard-coded value.

Hard-Coded Value (Before Quadra)	Property Default Value
1800000	1800000

If a timeout value is specified for this property in the `custom.properties` file, this value overrides the base property value. If no timeout is specified in the `custom.properties` file, the timeout is set to the base property value.

### 21.1.146 http.client.connection.default.so.timeout<.module>

This server property defines the socket timeout (SO\_TIMEOUT) (in milliseconds). This property is defined for both the CPE server and the Portal server.

Value Type	Value Range	Default Value
integer		10000

In the `custom.properties` file, you can replace `<.module>` with one of the modules listed in the following table. Prior to Quadra, this timeout value was hard-coded. The following table compares the pre-Quadra hard-coded value with this property's default value for each module. The base property value overrides the hard-coded value. If the base property value cannot be determined, the timeout is set to the hard-coded value.

**IMPORTANT:** Pre-Quadra values are different from the property default value. If you are upgrading to Quadra, additional tuning may be required.

Module	Hard-Coded Value (Before Quadra)	Property Default Value
clsIntegration	10000	10000
restSamlAuth	20000	10000
rogersAuth	5000	10000

Module	Hard-Coded Value (Before Quadra)	Property Default Value
sunriseSunsetTime	4000	10000

In the `custom.properties` file, you can have multiple occurrences of this property using a different module/value for each occurrence.

Examples:

- `http.client.connection.default.so.timeout.clsIntegration=15000`
- `http.client.connection.default.so.timeout.sunriseSunsetTime=5000`

If a timeout value is specified for a module in the `custom.properties` file, this value overrides the base property value. If no timeout is specified for a module in the `custom.properties` file, the timeout is set to the base property value.

#### 21.1.147 `http.client.connection.pool.timeout<.module>`

This server property specifies the timeout (in milliseconds) used when requesting a connection from the connection manager. This property is defined for both the CPE server and the Portal server.

Value Type	Value Range	Default Value
integer		10000

In the `custom.properties` file, you can replace `<.module>` with one of the modules listed in the following table. Prior to Quadra, this timeout value was hard-coded. The following table compares the pre-Quadra hard-coded value with this property's default value for each module. The base property value overrides the hard-coded value. If the base property value cannot be determined, the timeout is set to the hard-coded value.

Module	Hard-Coded Value (Before Quadra)	Property Default Value
clsIntegration	10000	10000
restSamlAuth	N/A	10000
rogersAuth	N/A	10000
sunriseSunsetTime	N/A	10000

In the `custom.properties` file, you can have multiple occurrences of this property using a different module/value for each occurrence.

Examples:

- `http.client.connection.pool.timeout.clsIntegration=15000`
- `http.client.connection.pool.timeout.sunriseSunsetTime=10000`

If a timeout value is specified for a module in the `custom.properties` file, this value overrides the base property value. If no timeout is specified for a module in the `custom.properties` file, the timeout is set to the base property value.

### 21.1.148 http.client.connectionPool.defaultMaxPerRoute

This server property specifies the maximum number of connections allowed per host. This is used to manage HTTP client connection pooling to the Cluster Location Service (CLS) Server.

Value Type	Value Range	Default Value
integer		20

### 21.1.149 http.client.connectionPool.defaultMaxTotal

This server property specifies the maximum number of connections available to the Cluster Location Service (CLS) Server.

Value Type	Value Range	Default Value
integer		50

### 21.1.150 ihealthcheck.test.emailAddress.from

This server property specifies the From email address used to ensure that ICHealthCheck can send a test email. The body of the test email message includes the following: "This is a test email from ICHealthCheck webapp."

Value Type	Value Range	Default Value
string	Email address	emailtest@icontrol.com

### 21.1.151 insight.cpePairingWaitTime

#### TOUCHSTONE ONLY

This server property specifies the number of seconds for the Touchstone CPE to wait for pairing

Value Type	Value Range	Default Value
integer		45

### 21.1.152 insight.sendActivationEmail

#### TOUCHSTONE ONLY

This server property specifies whether to send an activation email to the consumer.

**Note:** Not applicable if the service provider has SSO enabled. When SSO is enabled, an activation email is not sent to the subscriber.

Value Type	Value Range	Default Value
boolean	<b>true</b> = send an email <b>false</b> = do not send an email	true

For Converge systems, see "[converge.sendActivationEmail](#)" on page 260.

### 21.1.153 insight.showInvalidDefaultRules

#### TOUCHSTONE ONLY

This server property specifies whether to show invalid default rules for Touchstone.

Value Type	Value Range	Default Value
boolean	true = show invalid rules false = hide invalid rules	false

### 21.1.154 insight.singleAccessSessionIdleTimeout

#### TOUCHSTONE ONLY

This server property specifies how long (in seconds) to timeout an idle Touchstone REST client that is accessing a single-user resource (activation or settings).

Value Type	Value Range	Default Value
integer		60

### 21.1.155 java.naming.provider.url

This server property specifies the URL of the Java Naming and Directory Interface (JNDI).

Value Type	Value Range	Default Value
string	URL	false

### 21.1.156 java.naming.provider.url.portal.cluster

#### MULTIPLE CLUSTER CONFIGURATIONS ONLY

Portal cluster address for the Media cluster servers to access the JMS topic.

Value Type	Value Range	Default Value
string	URL	t3://portal-server1:8080,portal-server2:8080

### 21.1.157 jms.receiveTimeout

This server property specifies the milliseconds for the Java Message Service (JMS) to receive a message.

Value Type	Value Range	Default Value
integer	Greater than 10000	30000 (that is, 30 seconds)

### 21.1.158 jms.timeToLive.accountCentralStationIntegration

This server property specifies the milliseconds for the Java Message Service to mark the JMS message of the account integration to be expired in the JMS queue.

Value Type	Value Range	Default Value
integer	Greater than 300000	600000 (that is, 10 minutes)

### 21.1.159 jms.timeToLive.alarmRequest

#### CONVERGE ONLY

This server property specifies the milliseconds for the Java Message Service to mark the JMS message of an alarm request to be expired in the JMS queue.

Value Type	Value Range	Default Value
integer	Greater than 300000	600000 (that is, 10 minutes)

### 21.1.160 jms.timeToLive.cpeCommand

This server property specifies the milliseconds before JMS server marks a message expired and removed it from JMS server. Removed JMS messages are not received by the message handler and are not processed.

Value Type	Value Range	Default Value
number	Greater than zero	60000 (that is, 1 minute)

**Note:** Setting this value too high can lead to unnecessary usage of system resources (such as system memory).

### 21.1.161 jms.timeToLive.default

This server property specifies the milliseconds for the Java Message Service to mark the JMS message of any type not specified by another jms.timeToLive server property to be expired in the JMS queue.

Value Type	Value Range	Default Value
integer	Greater than 300000	120000 (that is, 2 minutes)

### 21.1.162 jms.timeToLive.nonPersistentTopic

This server property specifies the milliseconds for the Java Message Service to mark the JMS message of a Touchstone request or a Converge non-alarm request to be expired in the JMS queue.

Value Type	Value Range	Default Value
integer	Greater than 300000	30000 (that is, 30 seconds)

### 21.1.163 keypad.code.lockTime

#### CONVERGE ONLY

When the customer fails to enter a valid keypad code in the Subscriber Portal the maximum configured number of times ([keypad.code.max.retry](#)), this server property specifies how long (in seconds) the user is prevented from attempting to enter the key pad code again.

Value Type	Value Range	Default Value
integer	Greater than 600	1800 (that is, 30 minutes)

### 21.1.164 keypad.code.max.retry

#### CONVERGE ONLY

This server property specifies the maximum number of failed attempts to enter a keypad code in the Subscriber Portal before the system temporarily locks the user out.

Value Type	Value Range	Default Value
integer	Greater than 2	3

### 21.1.165 managementPortal.localeList

This server property specifies a comma-separated list of supported Management Portal locales other than English. There is no need to specify en (English).

Example: ja\_JP,de\_DE

Value Type	Value Range	Default Value
String		

### 21.1.166 managementPortal.login.lockTime

When the customer fails to successfully log into the Management Portal Login page the maximum configured number of times ([managementPortal.login.max.retry](#)), this server property specifies how long (in seconds) the user is prevented from attempting to log in again.

Value Type	Value Range	Default Value
integer	Greater than 600	1800 (that is, 30 minutes)

### 21.1.167 managementPortal.login.max.retry

This server property specifies the maximum number of failed attempts to enter a valid username and password at the Management Portal before the system temporarily locks the user out.

Value Type	Value Range	Default Value
integer	Less than 11	10

### 21.1.168 managementPortal.session.timeout.interval

This server property specifies the number of seconds a session on the Management Portal must be inactive before it times out.

Value Type	Value Range	Default Value
integer	Less than 3600	1800 (that is, 30 minutes)

### 21.1.169 mdu.enabled

This server property enables/disables the multiple-dwelling unit (MDU) feature. This feature enables the MDU administrator, such as the manager of an apartment block, to manage accounts using the MDUPartner-Insight tier package.

For more information, see "Multi-Dwelling Unit Package for Touchstone" in *Management Portal Guide*.

Value Type	Value Range	Default Value
boolean	<b>true</b> = MDU feature is enabled  <b>false</b> = MDU feature is disabled	false

### 21.1.170 media.file.cipher.keys

This server property specifies the keys are used to encrypt and decrypt the media files, such as image/thumbnaill or video clip files.

See the customCipherSeeds custom.property value on page [297](#).

Value Type	Value Range	Default Value
string	A 16-character string. Multiple keys are separated by commas. Newest key is appended at the end of the key string	icontrolCipher12

### 21.1.171 media.file.encrypt

This server property specifies whether media files are encrypted when on the server.

See the customCipherSeeds custom.property value on page [297](#).

Value Type	Value Range	Default Value
boolean	<b>true</b> = Keys are used  <b>false</b> = Keys are not used	true

### 21.1.172 motion.events.blackout.period

This server property specifies the time in seconds that a motion-capable camera will wait after reporting a motion event before reporting another motion event.

Value Type	Value Range	Default Value
number	Non-negative numbers	180 (3 minutes)

**IMPORTANT:** Contact your iControl representative before changing the default value (in `custom.properties`). Setting this value to a too small threshold can cause DDoS issues with your server clusters(s).

**Note:** This property only defines behavior for motion-capable cameras. It does not apply to other motion sensor devices.

### 21.1.173 mp.password.max.length

This server property specifies the maximum password length for a Management Portal account.

Value Type	Value Range	Default Value
Integer		16

### 21.1.174 mp.password.min.length

This server property specifies the minimum password length for a Management Portal account.

Value Type	Value Range	Default Value
Integer		6

### 21.1.175 mp.password.wellknown.words

This server property specifies a comma-separated list of strings that cannot be used as passwords.

Value Type	Value Range	Default Value
String		iControl1,uControl1

### 21.1.176 multiple.deployment

This server property specifies whether the system uses multiple deployments.

Value Type	Value Range	Default Value
boolean	<b>true</b> = Use multiple deployments <b>false</b> = Do not use multiple deployments	false

### 21.1.177 oauth2.<suffix>

Icontrol's OAuth 2.0 provider enables a third-party device to authenticate against the Icontrol system using an OAuth token for access to a specific account. The OAuth provider uses the following server properties, some of which must be added to the `custom.properties` file on the Icontrol portal server:

- `oauth2.authorization.server.enabled`
- `oauth2.resource.server.key`
- `oauth2.resource.server.secret`
- `oauth2.authorization.server.url`
- `oauth2.token.cache.ttl.seconds`

For more information, see: "[OAuth 2 Integration](#)" on page 305

### 21.1.178 password.min.length

This server property specifies the minimum length of passwords created for the Subscriber Portal.

Value Type	Value Range	Default Value
integer	4	4

### 21.1.179 password.max.length

This server property specifies the maximum length of passwords created for the Subscriber Portal.

Value Type	Value Range	Default Value
integer	20	20

### 21.1.180 password.reset.emailAddress.from

This server property specifies the From email address of the password reset system email..

Value Type	Value Range	Default Value
string	Email address	system@ucontrol.com

## 21.1.181 pingCellularUnit.att.gateway.url

### **CONVERGE ONLY**

This server property is used for Smash & Grab confirmation.  
See "Understanding Smash & Grab" on page 112.

## 21.1.182 pingCellularUnit.att.gateway.username

### **CONVERGE ONLY**

This server property is used for Smash & Grab confirmation.  
See "Understanding Smash & Grab" on page 112.

## 21.1.183 pingCellularUnit.gateway.password

### **CONVERGE ONLY**

This server property is used for Smash & Grab confirmation.  
See "Understanding Smash & Grab" on page 112.

## 21.1.184 pingCellularUnit.att.licenseKey

### **CONVERGE ONLY**

This server property is used for Smash & Grab confirmation.  
See "Understanding Smash & Grab" on page 112.

## 21.1.185 pingCellularUnit.implementation

### **CONVERGE ONLY**

This server property is used for Smash & Grab confirmation.  
See "Understanding Smash & Grab" on page 112.

## 21.1.186 pingCellularUnit.numerex.accountId

### **CONVERGE ONLY**

This server property is used for Smash & Grab confirmation.  
See "Understanding Smash & Grab" on page 112.

## 21.1.187 pingCellularUnit.numerex.gateway.password

### **CONVERGE ONLY**

This server property is used for Smash & Grab confirmation.  
See "Understanding Smash & Grab" on page 112.

## 21.1.188 pingCellularUnit.numerex.gateway.url

### **CONVERGE ONLY**

This server property is used for Smash & Grab confirmation.  
See "Understanding Smash & Grab" on page 112.

**21.1.189 pingCellularUnit.numerex.gateway.username****CONVERGE ONLY**

This server property is used for Smash & Grab confirmation.

See "Understanding Smash & Grab" on page 112.

**21.1.190 pingCellularUnit.numerex.new.cid****CONVERGE ONLY**

This server property is used for Smash & Grab confirmation.

See "Understanding Smash & Grab" on page 112.

**21.1.191 pingCellularUnit.numerex.prefixes****CONVERGE ONLY**

This server property is used for Smash & Grab confirmation.

See "Understanding Smash & Grab" on page 112.

**21.1.192 pingCellularUnit.numerex.smmspинг.timeout.interval****CONVERGE ONLY**

This server property is used for Smash & Grab confirmation.

See "Understanding Smash & Grab" on page 112.

**21.1.193 pingCellularUnit.numerex.waiting****CONVERGE ONLY**

This server property is used for Smash & Grab confirmation.

See "Understanding Smash & Grab" on page 112.

**21.1.194 portalViewer.timeout**

This server property specifies the time (in seconds) for the server to reset the portal viewer count.

Value Type	Value Range	Default Value
integer	1 to 7200	7200 (2 hours)

**21.1.195 postalcode.validation.country**

This server property specifies the two-letter country code that corresponds to the postal code to be validated.

Value Type	Value Range	Default Value
string	US = United States CA= Canada	US

### 21.1.196 postalcode.validation.country.CA.pattern

### 21.1.197 postalcode.validation.country.US.pattern

These server properties specify the regular expression to use to validate postal codes.

Value Type	Value Range	Default Value
string	n/a	US: ^([0-9]{5})(?:[-\\s]*([0-9]{4}))?\\\$ CA: ^([A-Z][0-9][A-Z])\\s*([0-9][A-Z][0-9])\\\$

### 21.1.198 premise.countryList

The server property specifies a comma separated list of countries where a customer premise can be located.

For example, [premise.countryList=en,en\_GB,en\_US,fr,fr\_FR,fr\_CA,de,it,ja,ko,zh\_CN,zh\_TW].

Value Type	Value Range	Default Value
string	en = English (Caribbean) en_GB = English (United Kingdom) en_US = English (United States) fr = French (Standard) fr_FR = French (France) fr_CA = French (Canada) de = German (Standard) it = Italian ja = Japanese zh_CN = Chinese (Chinese) zh-TW = Chinese (Taiwan)	US

### 21.1.199 relay.server.converge.enabled

#### CONVERGE ONLY

This server property specifies whether Converge touchscreen systems use the relay server. If the value is true, then relay.server.enabled value must be true as well .

Value Type	Value Range	Default Value
boolean	true = yes false = no	true

### 21.1.200 relay.server.credential.encrypting.enabled

This server property specifies whether the relay server username and password should be encrypted in the custom.properties file. The default value is false. If you set this value to true, see the *Relay Server Installation Guide* for details on specifying encrypted values.

Value Type	Value Range	Default Value	Clusters
boolean	<b>true</b> = Encrypting enabled <b>false</b> = Encrypting disabled	false	Portal

### 21.1.201 relay.server.enabled

This server property specifies whether the relay server is enabled. For Converge systems, if this value is false, `relay.server.converge.enabled` is treated as false as well.

Value Type	Value Range	Default Value
boolean	<b>true</b> = yes <b>false</b> = no	false

### 21.1.202 relay.server.password

This server property specifies the password for the relay server.

Value Type	Value Range	Default Value
string	n/a	none

### 21.1.203 relay.server.sp.videotoken.appkey

This server property specifies the app key required to enable the Relay Server video token in the legacy Subscriber Portal. This property applies only to the legacy Subscriber Portal when using Relay Server version 8 or later; it does not affect the Card UI Web App.

On the Portal nodes, the value of this property must be a valid app key to enable the Relay Server video token feature in the legacy Subscriber Portal if the Relay Server is enabled. The value of this property must be the same as the header app key used in the subscriber REST API. If the value is empty or invalid, the Relay Server video token feature will not be enabled in the legacy Subscriber Portal.

**IMPORTANT:** If you are using the legacy Subscriber Portal with Relay Server version 8 or later, you must add this property to the `custom.properties` file and specify a valid app key.

Value Type	Value Range	Default Value	Clusters
string			Portal

#### Example

`relay.server.sp.videotoken.appkey=myKey`

## 21.1.204 relay.server.url

This server property specifies the URL to the relay server, which is used to create new relay sessions. For example, `https://somrelay.icontrol.com/relay/`

Value Type	Value Range	Default Value
string		<code>https://relay-host/relay/</code>
This value must be changed if the relay server is enabled.		

## 21.1.205 relay.server.username

This server property specifies the user name for the relay server.

Value Type	Value Range	Default Value
string	n/a	none

## 21.1.206 rest.csrf.token.enabled.modules

This server property defines webapp modules for which a CSRF token is required for client access.

**Note:** This property is disabled by default and can be enabled only in the `custom.properties` file.

When this property is enabled, the X-expires HTTP header is required to generate a CSRF token. To create a token, the client needs to pass the X-expires header with a value in milliseconds (maximum 10 minutes or 60,000 milliseconds). The server returns a response that contains the X-token HTTP header with the token value. Subsequent requests use the X-token header to pass in the token value, and the token expiration timer resets to the defined X-expires value with each request.

Value Type	Value Range	Default Value
String		

The value of this property is a comma-separated list of webapp modules. This is primarily used with the REST webapp modules, but can also be used for the Subscriber Portal webapp module for Touchstone-related REST API calls.

Available modules: `rest`, `restOperation`, `restServer`, `restIntegration`, `subscriberPortal`

Example comma-separated property value: `rest,restOperation`

For more information, see the "X-expires and X-token: Token Expiration for REST Modules" section in *REST API Getting Started Guide*.

## 21.1.207 restApi.login.lockTime

This server property specifies how long to lock the login for the RESTful API, in seconds.

Value Type	Value Range	Default Value
integer	true = yes false = no	1800

### 21.1.208 restApi.admin.login.enabled

This server property specifies whether to enable admin user login of the RESTful API.

Value Type	Value Range	Default Value
boolean	true = yes  false = no	false

### 21.1.209 restApi.login.max.retry

This server property specifies the maximum number of retries for RESTful API login.

Value Type	Value Range	Default Value
integer		5

### 21.1.210 restBasedPortalURL

This server property specifies the URL that is included in the email that is sent to a subscriber when the subscriber clicks the "Forgot your Username/Password?" links on the login page of a REST-based portal (e.g., Card UI Mobile App and Web App) to retrieve the subscriber's username or to reset the subscriber's password.

**Note:** This property is used for REST-based portals only. The "classic" Subscriber Portal uses the subscriberPortalRootUrl property.

Value Type	Value Range	Default Value
string	URL	https://localhost/cui

#### Example URL for Card UI Web App

<https://beta.icontrol.com/cui>

#### Example Email for Retrieve Username

A subscriber receives the following email when the value of the restBasedPortalURL property is <https://beta.icontrol.com/cui>:

From: <system@beta.icontrol.com>  
 Date: Oct 8, 2015 12:58 PM  
 Subject: Your Username Retrieval  
 To: <bob@company.com>  
 Cc:

The username for your account is: bob.  
 You may log in to the website here:  
<https://beta.icontrol.com/cui>  
 Please call customer service if you still cannot access your account.

### 21.1.211 restOperation.installerAccess.duration.minutes

This server property specifies the duration, in minutes, that an installer is allowed to access installer level APIs for a premise after a user has granted access.

A value of -1 means the check will be disabled and installer users will always be allowed access.

The default is 60 minutes.

Clusters			
Value Type	Value Range	Default Value	
integer		60 (minutes)	Portal

### 21.1.212 restsubscriber.session.timeout.interval

This server property specifies the HTTP session timeout, in seconds, for the REST subscriber service.

Value Type	Value Range	Default Value
integer		1800

### 21.1.213 rule.action.arm

This server property specifies whether to allow customers to create a rule that contains an action to arm the system.

Value Type	Value Range	Default Value
boolean	<b>true</b> = yes <b>false</b> = no	false

### 21.1.214 rule.action.disarm

This server property specifies the whether to allow customers to create a rule that contains an action to disarm the system.

Value Type	Value Range	Default Value
boolean	<b>true</b> = yes <b>false</b> = no	false

### 21.1.215 rule.action.lighting.duration

This server property specifies whether to allow subscribers to create a rule that contains an action that specifies a lighting duration.

Value Type	Value Range	Default Value
boolean	<b>true</b> = yes <b>false</b> = no	false

### 21.1.216 rule.action.set.thermostat.to.cool

This server property specifies whether to allow customers to create a rule that contains an action to set the thermostat to cool.

Value Type	Value Range	Default Value
boolean	<b>true</b> = yes <b>false</b> = no	false

### 21.1.217 rule.action.set.thermostat.to.heat

This server property specifies whether to allow customers to create a rule that contains an action to set the thermostat to heat.

Value Type	Value Range	Default Value
boolean	<b>true</b> = yes <b>false</b> = no	false

### 21.1.218 rule.action.turn.thermostat.off

This server property specifies whether to allow the customers to create a rule that contains an action to turn the thermostat off.

Value Type	Value Range	Default Value
boolean	<b>true</b> = yes <b>false</b> = no	false

### 21.1.219 rule.doNotConvertArmDisarmDefaultServerRule

This server property specifies whether to put a constraint for converting arm/disarm default server rule to clients

Value Type	Value Range	Default Value
boolean	<b>true</b> = yes <b>false</b> = no	false

### 21.1.220 rule.showxml

This server property specifies whether to allow customers to add their own rules in the Subscriber Portal.

Value Type	Value Range	Default Value
boolean	<b>true</b> = yes <b>false</b> = no	false

### 21.1.221 search.character.blacklist

This server property specifies a list of characters that cannot be used in database searches.

Value Type	Value Range	Default Value
String		,;"

### 21.1.222 serverStats.enabled

This server property specifies whether to enable the ICHealthCheck feature.

Value Type	Value Range	Default Value
boolean	<b>true</b> = yes	true
	<b>false</b> = no	

### 21.1.223 server.enableIntegrationLoggingThatWillWritePrivacyDataInLogs

This server property specifies whether to log input and output from the account integration webservice when the debug level is set to DEBUG.

Value Type	Value Range	Default Value
boolean	true = yes	false
	false = no	

### 21.1.224 server.health.check.expected.duration.in.seconds

This server property specifies the seconds to execute an ICHealthCheck before the request times out.

Value Type	Value Range	Default Value
boolean	Greater than zero	3

### 21.1.225 serverStats.length

This server property specifies the number of hours to retain server stats.

Value Type	Value Range	Default Value
number	2 - 24	6

## 21.1.226 share.file.root

Linux version

## 21.1.227 share.file.root.windows

Windows version

Root directory used by the following properties:

- cellular.import.log.directory  
*CONVERGE ONLY*
- cpe.import.log.directory  
*CONVERGE ONLY*
- device.dump.directory
- device.diagnostic.directory
- device.screenshot.directory
- device.image.directory
- firmware.misc.directory
- video.convert.command
- widget.image.directory  
*CONVERGE ONLY*

**Note:** If you change the default values in custom.properties, you must copy the directories and files associated with the properties listed above to that location. Otherwise, users will not be able to show previously captured files, images, or other related information.

Operating System	Value Type	Value Range	Default Value
Linux	string	path	/tmp
Windows			C:\\\\tmp

## 21.1.228 sms.queue.concurrentConsumers

This server property specifies the number of concurrent consumers for the SMS queue.

Value Type	Value Range	Default Value
integer	Greater than zero	4

## 21.1.229 speedTestUrl

This server property specifies the relative URL to upload a file to test the Home Domain broadband speed (used for camera configuration).

Value Type	Value Range	Default Value
string	Path	/fileUpload/speedTest

### 21.1.230 sso.enabled

This server property specifies the whether single sign on is enabled for the Subscriber Portal.

Value Type	Value Range	Default Value
boolean	<b>true</b> = yes <b>false</b> = no	false

### 21.1.231 subscriberPortalBackdoorUrl

The Subscriber Portal Backdoor accessed via the Management Portal is still based off of the legacy Subscriber Portal. This server property specifies the URL to the legacy Subscriber Portal.

Value Type	Value Range	Default Value
String	URL	https://localhost/subscriberPortal/login.jsp

### 21.1.232 subscriberPortal.insuranceCertificate.show

This server property specifies the whether to show the insurance certificate is viewable from the Subscriber Portal.

Value Type	Value Range	Default Value
boolean	<b>true</b> = yes <b>false</b> = no	false

### 21.1.233 subscriberPortal.localeList

This server property specifies a comma separated list of supported Subscriber Portal Locales, other than English. There is no need to specify en (English).

Value Type	Value Range	Default Value
String		de_DE,fr_FR,it_IT

### 21.1.234 subscriberPortal.login.lockTime

When the customer fails to successfully log into the Subscriber Portal Login page the maximum configured number of times (subscriberPortal.login.max.retry), this server property specifies how long (in seconds) the user is prevented from attempting to log in again.

Value Type	Value Range	Default Value
integer		1800 (30 minutes)

### 21.1.235 subscriberPortal.login.max.retry

This server property specifies the maximum number of failed attempts to enter a valid username and password at the Subscriber Portal before the system temporarily locks the user out.

Value Type	Value Range	Default Value
integer		5

### 21.1.236 subscriberPortalRootUrl

This server property specifies the Subscriber Portal root URL.

**Note:** This value should map to the following directive in your Apache configuration:

```
ProxyPassReverseCookiePath /subscriberPortal/
[subscriberPortalRootUrl]
```

For example,

IF you added the following directive to the apache configurations:

```
ProxyPassReverseCookiePath /subscriberPortal/securehome
```

THEN the configuration in the custom.properties file should be the following:

```
subscriberPortalRootUrl=
```

```
https://255.255.255.255/securehome
```

where 255.255.255.255 is the IP address of the Subscriber Portal server.

This would cause the Subscriber Portal URL to be:

```
https:// 255.255.255.255/securehome
```

Value Type	Value Range	Default Value
string	URL	https://localhost/subscriberPortal

### 21.1.237 subscriberPortal.session.timeout.interval

This server property specifies the number of seconds a session on the Subscriber Portal before it times out.

Value Type	Value Range	Default Value
integer		1800 (30 minutes)

### 21.1.238 subscriberPortal.temporary.password.expirationTime

This server property specifies the number of hours until the Subscriber Portal temporary password (assigned when an Account is ready for activation) expires.

Value Type	Value Range	Default Value
integer		336 (two weeks)

### 21.1.239 threadDump.enabled

This server property specifies whether the system will perform regular thread dumps to the logs. See the dumpThreadsTimerTask background task described in "Background Tasks" on page 298

Value Type	Value Range	Default Value
integer	true = The dumpThreadsTimeTask background task is enabled false = The dumpThreadsTimeTask background task is not enabled	true

### 21.1.240 threadDump.interval

If the server property `threadDump.enabled` is set to true, this server property specifies how often the `dumpThreadsTimeTask` background task is performed (in milliseconds).

Value Type	Value Range	Default Value
positive number	Note zero or negative (that is, every 10 minutes)	600000

### 21.1.241 threadDump.separate.file.enabled

If the server property `threadDump.enabled` is set to true, this server property specifies whether to store thread dumps in separate file rather than the system log file.

Value Type	Value Range	Default Value
integer	true = Thread dumps are saved to their own log file rather than the system log file false = Thread dumps are saved to the system log file	false

### 21.1.242 timezone.default

This server property specifies the default time zone for subscribers.

Value Type	Value Range	Default Value
string	From <code>timezone.properties</code> in the <code>ucontrol.ear</code>	US/Eastern

### 21.1.243 validation.pattern.csnum

This server property specifies a string that is used to validate the format of Central Station numbers.

Value Type	Value Range	Default Value
String		<code>^[0-9]{4}\\$</code>

### 21.1.244 validation.pattern.name

This server property specifies a string that is used to validate the format of names.

Value Type	Value Range	Default Value
String		<code>=^[\w\W\s"]+\\$</code>

This property accepts the pattern in JavaScript format. In the case of multiple patterns — e.g. `/^([ \u4E00-\u9FAF| \u3040-\u3096| \u30A1-\u30FA| \uFF66-\uFF9D| \u31F0-\u31FF]+| [a-zA-Z\\\s' '-]+){1}$/` — the {1} ensures that either the English or Japanese characters are considered valid and not a combination of both.

### 21.1.245 validation.pattern.phone

This server property specifies a string that is used to validate the format of phone numbers.

Value Type	Value Range	Default Value
String		<code>^[0-9]{10,11}\$</code>

### 21.1.246 validation.pattern.postalcode

This server property specifies a string that is used to validate the format of postal codes.

Value Type	Value Range	Default Value
String		<code>^([0-9]{5})(?:[-\\s]*([0-9]{4}))?\$/</code>

### 21.1.247 validation.pattern.zone

This server property specifies a string that is used to validate the format of zones.

Value Type	Value Range	Default Value
String		<code>^[a-zA-Z0-9.,\\\\\\s]+\$</code>

### 21.1.248 video.convert.command

#### 21.1.249 video.convert.command.windows

These server properties specify the path to the command used to convert a MPEG4 video clip file to a .flv file.

Operating System	Value Type	Value Range	Default Value
Linux	string	Path	<code>/opt/bin/ffmpeg</code>
Windows			<code> \${share.file.root.windows}\\ffmpeg\\bin\\ffmpeg.exe</code>

### 21.1.250 video.convert.command.concurrent.number

This server property specifies the maximum number of concurrent video convert commands that can be executed.

Value Type	Value Range	Default Value
integer		30

### 21.1.251 video.convert.h264

This server property specifies the ffmpeg command options to convert h264 encoded streams.

Value Type	Value Range	Default Value	Clusters
string		-y -i {0} -vcodec copy -acodec copy {1}	Portal

### 21.1.252 video.convert.mjpeg

This server property specifies the ffmpeg command options to convert mjpeg streams.

Value Type	Value Range	Default Value	Clusters
string		-i {0} -vcodec libx264 -vpre normal -vpre main -level 31 -b 768000 -r 15 {1}	Portal

### 21.1.253 white.list.peripheralTrouble.to.centralStation

This server property specifies a white list of peripheral troubles that will always be sent to the Central Station

Other peripheral troubles and their respective restore events can be added to this list, such as senTamp (sensor tamper) and senTampRes. In this case, the property would be set to

sensCom, sensComRes, senTamp, senTampRes

Value Type	Value Range	Default Value	Clusters
string		sensCom,sensComRes	CPE

### 21.1.254 white.list.zoneTrouble.to.centralStation

This server property specifies a white list of zone troubles that will always be sent to the Central Station. By default, the senCom trouble is always sent to the Central Station. You can add other zone troubles to the white list by separating each entry with a comma. For example:

```
sensCom, senTamp, senLowBat
```

Value Type	Value Range	Default Value
String	N/A	sensCom

The following table associates sensor troubles with their CIDs.

Trouble	Enumeration	CID
Sensor Comm Fail when system is armed	sensCom	147 (see page <a href="#">77</a> )
A sensor that uses an A/C power back-up has lost A/C power.	senNoPower	342 (see page <a href="#">80</a> )
Sensor Comm Fail when system is unarmed	sensCom	381 (see page <a href="#">82</a> )
A sensor was being upgraded, but the upgrade failed	senBootloadFail	380 (see page <a href="#">81</a> )
A sensor is dirty	senDirty	380 (see page <a href="#">81</a> )
A zone has gone into swinger-shutdown	zoneSwingerShutdown	380 (see page <a href="#">81</a> )
A sensor is being tampered	senTamp	383 (see page <a href="#">83</a> )
A sensor is reporting a low battery.	senLowBat	384 (see page <a href="#">83</a> )

See "Zone Function Behaviors" on page [86](#) for details on the CIDs generated by zones in various scenarios.

### 21.1.255 widget.image.directory

### 21.1.256 widget.image.directory.windows

#### CONVERGE ONLY

These server properties specify the absolute root directory to save the touchscreen app images.

Operating System	Value Type	Value Range	Default Value
Linux	string	Path	<code> \${share.file.root}/widget</code>
Windows			<code> \${share.file.root.windows}\widget</code>

## 21.1.257 widget.p5.android.supported

### CONVERGE ONLY

This server property specifies a comma-delimited list of the apps that can be installed in SMC P5 touchscreen using the Android firmware build. The maximum number of apps for this property is six (6).

Value Type	Value Range	Default Value
string	Path	com.icontrol.apps.clock,com.icontrol.apps.news.reuters, com.icontrol.apps.sports.reuters,com.icontrol.apps.calc, com.icontrol.apps.photos,com.icontrol.apps.weather

## 21.1.258 widgetStoreUrl

### CONVERGE ONLY

This server property specifies the relative URL to upload and access touchscreen app files.

Value Type	Value Range	Default Value
string	URL	/widgetstore/getWidgets

## 21.1.259 widget.weatherUrl

### CONVERGE ONLY

This server property specifies the URL of the Weather touchscreen app.

Value Type	Value Range	Default Value
string	URL	/widgetstore/getWidgets

## 21.1.260 xmpp.routeConfig.<suffix>

The following server properties are used for the XMPP routing management feature. For more information, see: <https://share-icontrol.atlassian.net/wiki/display/CSKB/7.3+Quadra+-+XMPP+Routing+Management>

- ❑ xmpp.routeConfig.count
- ❑ xmpp.routeConfig.<config-number>.name
- ❑ xmpp.routeConfig.<config-number>.type
- ❑ xmpp.routeConfig.<config-number>.config.<config-property>
- ❑ xmpp.routeConfig.<config-number>.autoReply
- ❑ xmpp.routeConfig.<config-number>.dropMessages
- ❑ xmpp.routeConfig.<config-number>.editable
- ❑ xmpp.routeConfig.<config-number>.filter.type

- ❑ xmpp.routeConfig.<config-number>.filter.config.<config-property>
- ❑ xmpp.routeConfig.<config-number>.config.maxThreads
- ❑ xmpp.routeConfig.<config-number>.config.queueCapacity

### 21.1.261 xmpp.threaddump.policy

This server property specifies the XMPP thread dump policy for the system. [US7972]

In the format [1], [2], [3], [4], where:

[1] is the upper limit of the XMPP queue size to dump the application threads to log file.

For example, 5000 means that if there are more than 5000 XMPP messages queued up and waiting to be processed, the server will save thread dump information to log file.

[2] is the lower limit of the XMPP queue size to stop dumping the application threads to log file.

[3] is the time period (in milliseconds) for the server to check the XMPP queue size and dump the application threads to log file.

Range: 10000 to 30000 (10 to 30 seconds)

[4] Is the maximum number times that an application thread dump is saved in log file.

Range: 1 to 20

Value Type	Value Range	Default Value
Four comma-separated positive numbers	See above.	5000,500,10000,10

## 21.2 custom.properties

The `custom.properties` file overrides the default values defined in the `server.properties` file. It can also be used to set customer-specific properties that are not defined in the `server.properties` file.

### 21.2.1 General Properties

customCipherSeeds	<p>The key seed(s) used to encrypt/re-encrypt any sensitive data in the Server cluster or Converge Back-up Alarm server that is new or accessed.</p> <p>Each seed is a 20-character alphanumeric string. The first two digits of the seeds are unique and cannot be 78.</p> <p>If this property has not been added to the <code>custom.properties</code> file, the system uses the hard-coded key in the application code to do encryption/decryption.</p> <p>When this property has been added to the <code>custom.properties</code> file, the system uses the key value to encrypt/re-encrypt any of the sensitive data that is new or accessed. Any existing encrypted data that is not accessed (read) is not encrypted.</p> <p>Insert new keys before any keys that have already been configured, separated by a space. For example:</p> <p>Original entry:</p> <pre>customCipherSeeds=thisisanexampleseed1</pre> <p>Updated entry:</p> <pre>customCipherSeeds= thisisanexampleseed2&lt;space&gt;thisisanexampleseed1</pre> <p><b>IMPORTANT:</b> Do not update or delete old keys once they have been in use.</p> <p>The server(s) must be rebooted when a new key has been added.</p>
device.firmwareBaseUrl	The absolute base URL for device firmware.
enforce.firmware.ssl	<p>Whether CPE firmware added to the Management Portal must be downloaded from a trusted SSL site (default=true).</p> <p>When set to <b>false</b>, firmware can be downloaded from anywhere (HTTPS or HTTP) but a warning is given.</p> <p><b>IMPORTANT:</b> When the value is set to <b>false</b>, it bypasses the validation of certificate while uploading a firmware. It allows user to upload firmware from non-trusted source. This may compromise the security.</p>

## 21.2.2 Background Tasks

The `runBackgroundTask` custom property is set to `true` by default. For multiple cluster server configurations, set this property to `runBackgroundTask=false` on the servers in the following clusters:

- Portal
- Media

When `runBackgroundTask` is not configured or is set to true, the following background tasks are run on the server.

checkBroadbandConnection	Time task to check the broadband heartbeat of a subscriber's CPE. If the configured number of heatbeats are missing, the broadband connection is marked <i>down</i> . See " <a href="#">Broadband Connectivity</a> " on page 100.
checkCellularConnection	Time task to check the cellular heartbeat of a subscriber's CPE. If the configured number of heatbeats are missing, the cellular connection is marked <i>down</i> . See " <a href="#">Cellular Connectivity</a> " on page 103.
checkOrphanedAlarmSession	Timer task to check the database for alarm sessions of "unknown" type; that is, the server received an alarm session Send All event but no related events.
checkProcessingAlarmSession	<p>Timer task to check the database the rare event in which an alarm session has been processed but has not been sent to central station because of JMS server is down. The alarm session marked <i>expired</i> and is processed manually.</p> <p>In normal cases, alarm delivery error will be handled by the alarm error queue. So the code here is no-op.</p> <p>Note TS reset the alarm after 4 minutes, so we need to check 'completed' alarm session too.</p>
checkWaitingAlarmSession	<p>Check the database for any alarm session for which the Transmission Delay period has expired but no message has arrived from the touchscreen telling the servers either to cancel the alarm or to send the alarm to the Central Monitoring Stations. For any alarm session found, this task sends the alarm to the CMS.</p> <p>This task uses the value of the <code>alarm.unprocessedCheckingPeriod.inWaitingStatus</code> server property to determine the age of alarm sessions it is looking for. See "<a href="#">alarm.unprocessedCheckingPeriod.inWaitingStatus</a>" on page 239.</p>
markBBCommunicationEvent	Check the broadband heartbeat and mark the status of broadband connection based on the <code>checkBroadbandConnection</code> task.

processBatchFirmwareUpdate	A scheduled task the system uses to find/execute schedule firmware update batch jobs.
resendBBDownMessage	If the time since last broadband message is more than an configured time, resend the <i>Broadband Down</i> message via the Cellular channel.
resetWatchCount	Set the <code>watch_count</code> to <b>0</b> if it has not been changed after a certain period time configured in the <code>system.property</code> file.

Set the `threadDump.enabled` server property to *true* to enable the `dumpThreadsTimerTask` background task. This background task dumps the application server's thread-infor-to-log file. See "["threadDump.enabled" on page 291](#)".

The following background tasks run on the CPE cluster servers and the Portal cluster servers, but are not toggled on and off by a custom property:

- ❑ **checkSmashAndGrabEvent:** Detects the SMG event
- ❑ **monitorDatabaseTimerTask:** Sends read/writing/delete operations of a monitor table to the database to monitor the database connection between the application to database

### 21.2.3 Numerex Properties

**Note:** The following values must be configured in `custom.properties` if your system is integrated with Numerex cellular.

- ❑ `sms.numerex.username=`
- ❑ `sms.numerex.password=`
- ❑ `sms.numerex.gatewayId=`

## 21.2.4 COPS Integration

**Note:** Configure COPS properties if the value for centralstation.implementation is copsCentralstationMessageSender. Default values for COPS properties are not included in the server.properties file, but you can add them to the custom.properties file.

COPS Integration Custom Properties

custom.property	Value
centralStation.cops.url	URL for the COPS the central monitoring station API - "COPALINK"
centralStation.cops.dealerNumber	Dealer ID used to authenticate into the COPS API
centralStation.cops.dealerPasscode	Dealer passcode used to authenticate into the COPS API
centralStation.cops.panelType	Touchscreen type originating alarms and other events (must be UCONTROL)
centralStation.cops.templateNumber	COPS template to use to determine response workflow for the accounts
centralStation.cops.billingAccountNumber	Billing account number COPS will use to bill for monitoring services; <b>Note:</b> Must be 13 to 16 characters long
centralStation.cops.activationDateFormat	Date format used in the API for setting/updating the date monitoring first began for the customer; Use the date format appropriate for the java.text.SimpleDateFormat object
centralStation.cops.permitExpirationDateFormat	Date format used in the API for setting/updating the date used for the expiration of a security permit; Use format appropriate for the java.text.SimpleDateFormat object
centralStation.cops.hoursOnTest	How long (in hours) the system stays in Test mode before automatically returning to Monitored mode (from 0 – 72). Used in combination with centralStation.cops.minutesOnTest.
centralStation.cops.minutesOnTest	How long (in minutes) minus the centralStation.cops.hoursOnTest value the system stays in Test mode before automatically returning to Monitored mode (from 0 – 72) Values are: 0, 15, 30, 45
centralStation.cops.disconnectonDelete	Whether to completely close an account at COPS when it is deleted using the Management Portal

### 21.2.5 DICE Integration

**Note:** Configure DICE properties if the value for centralStation.implementation is diceCentralStationMessageSender.

DICE Integration Custom Properties

custom.property	Value
centralStation.dice.url	URL for the DICE the central monitoring station API
centralStation.dice.pgm	Must be CM5262SI
centralStation.dice.panelType	Touchscreen type originating alarms and other events (must be UCONTROL)
centralStation.dice.dealerNumber	Dealer ID used to authenticate into the DICE API
centralStation.dice.idIdentifierName	Not used
centralStation.dice.socketTimeout	Time in milliseconds the Application server will wait for a response from the IP Alarm server before disconnecting the socket and returning an exception to the Application server. (default is 10000 or ten seconds)

### 21.2.6 SIMS Integration

SIMS Integration Custom Properties

custom.property	Value
centralStation.sims.baseUrl	Domain name of the central monitoring station
centralStation.sims.panelType	Touchscreen type originating alarms and other events (must be UCONTROL)
centralStation.sims.alarmSenderId	URL to where the alarms are sent over IP by the Application servers
centralStation.sims.socketTimeout	Time in milliseconds the Application server will wait for a response from the IP Alarm server before disconnecting the socket and returning an exception to the Application server. (default is 10000 or ten seconds)
centralStation.sims.connectionTimeout	Time in milliseconds that the Application server will try to connect to the IP alarm server before it stops trying (default is 5000 or five seconds)

### 21.2.7 SSO Integration

SSO Integration Custom Properties

custom.property	Value
sso.mobileClient.certificate.fileName	The certificate used to verify the authentication assertion from an iPhone application client
sso.private.symmetric.key.file.name	The private symmetrical key file name, such as rsaprivkey.der, that decrypts the token. This file must be copied to the UCONTROL_CONFIG directory before starting the WebLogic server.
sso.public.symmetric.key.file.name	The public symmetrical key file name, such as rsapubkey.der, that decrypts the token matched with the private key. This file must be copied to the UCONTROL_CONFIG directory before starting the WebLogic server.
sso.symmetric.mobileClient.authenticationLocation	The URL that receives the username and password from an iPhone application and returns the authentication token.

## SSO Integration (continued)

Configuration Setting	Value
sso.symmetric.token.timezone	<p>The time zone of the server that generates the authentication token. If no value is specified, the JVM time zone of the iControl server is used.</p> <p>The following values can be specified.</p> <ul style="list-style-type: none"><li><input type="checkbox"/> US/Eastern</li><li><input type="checkbox"/> US/Central</li><li><input type="checkbox"/> US/Mountain</li><li><input type="checkbox"/> US/Arizona</li><li><input type="checkbox"/> US/Pacific</li><li><input type="checkbox"/> US/Alaska</li><li><input type="checkbox"/> US/Aleutian</li><li><input type="checkbox"/> US/Hawaii</li><li><input type="checkbox"/> Canada/Newfoundland</li><li><input type="checkbox"/> Canada/Atlantic</li><li><input type="checkbox"/> Canada/Eastern</li><li><input type="checkbox"/> Canada/Central</li><li><input type="checkbox"/> Canada/Mountain</li><li><input type="checkbox"/> Canada/Saskatchewan</li><li><input type="checkbox"/> Canada/Pacific</li><li><input type="checkbox"/> Canada/Yukon</li></ul>

## 21.2.8 OAuth 2 Integration

Icontrol's OAuth 2.0 provider enables a third-party device to authenticate against the Icontrol system using an OAuth token for access to a specific account. The OAuth provider uses the following server properties, some of which must be added to the `custom.properties` file on the Icontrol portal server:

- `oauth2.authorization.server.enabled`
- `oauth2.resource.server.key`
- `oauth2.resource.server.secret`
- `oauth2.authorization.server.url`
- `oauth2.token.cache.ttl.seconds`

The following properties also must be added to the `custom.properties` file on the Icontrol portal server:

- `oauth2.convergeIntegrationServiceUserName`
- `oauth2.convergeIntegrationServicePassword`

For more information, see the OAuth Provider Management feature guide on the Icontrol Customer Support Knowledge Base: <https://share-icontrol.atlassian.net/wiki/display/CSKB/7.3+Quadra+-+OAuth+Provider+Management>

## 21.3 mail.properties

The `mail.properties` file manages the configuration properties for sending e-mail and SMS messages. This text-based file is located on all the servers in the All-In-One/CPE cluster but not the Converge Back-up Alarm Server. Use the `custom.properties` file to override the values for properties in this file.

**Note:** Single-cluster server configuration is no longer supported as of the Oahu release.

### 21.3.1 General Mail Properties

Simplewire SMS Properties

Configuration Setting	Description	
<code>messaging.enabled</code>	<code>true</code>	Allow the system to send e-mail and SMS messages.
	<code>false</code>	The system will NOT send e-mail and SMS messages.

### 21.3.2 Quota Properties

Quota Properties

Configuration Setting	Description	
messaging.sendDailyFileUploadQuotaExceededEmail	true	Sends an email when the daily file upload quota (image or video) is exceeded.
	false	Does NOT send an email when the daily file upload quota (image or video) is exceeded.
messaging.sendDailySMSQuotaExceededEmail	true	Sends an email when the daily quota for SMS messages is exceeded.
	false	Does not send an email when the daily quota for SMS messages is exceeded.
messaging.fileQuotaExceededEmail.repeatInterval	After a notification has been sent to the subscriber that his image or video files are over-limit, how long the system waits to resend the notification.	

### 21.3.3 Email Properties

General SMS Properties

Configuration Setting	Description
mail.default.from	The default <i>from</i> email address for email notifications
mail.nonemergency.events.from	The <i>from</i> email address for nonemergency events
sms.sourceAddr	SMS address displayed as the sender of the SMS texts
mail.emergency.events.from	Text at the start of all SMS messages
mail.system.events.from	The <i>from</i> email address for system events
mail.armdisarm.events.from	The <i>from</i> email address for arm/disarm events
mail.host	Host name of the email server
mail.port	Port number of the email server
mail.username	Username to log in to the e-mail server
mail.password	Password to log in to the e-mail server

### 21.3.4 SMS Properties

In addition to the SMS-related properties listed in this section, there are also Tier Properties that manage SMS behavior, such as `sms.mms.allowVideoAttachment` and `sms.mms.maxImageAttachments`. See *Management Portal Guide* for more information about these properties.

General SMS Properties

Configuration Setting	Description
<code>sms.message.maxLength</code>	The maximum number of characters to allow in an SMS message. The default is 157. The maximum is 160. If a message contains more than 160 characters, it will be truncated to 160.
<code>sms.service.beanName</code>	SMS implementation to be used in the current build.  For example, for the Simplewise implementation the value is <code>simpleWireSmsSender</code> or <code>numerexSmsSender</code> .

#### 21.3.4.1 Simplewire Properties

Simplewire SMS Properties

Configuration Setting	Description	
<code>sms.subscriberID</code>	Username for the SMS account	
<code>sms.subscriberPassword</code>	Password for the SMS account	
<code>sms.sourceAddr</code>	SMS address displayed as the sender of the SMS texts	
<code>sms.messagePrefix</code>	Text at the start of all SMS messages	
<code>sms.countryCode</code>	A number representing the country code for an HTTP Post request. At this time, only <b>1</b> is valid.	
<code>sms.remoteHost</code>	IP address of the SMS server	
<code>sms.service.beanName</code>	<code>simpleWireSmsSender</code> See General SMS Properties for details.	

#### 21.3.4.2 Numerex Properties

The following values must be configured in `custom.properties` if your system is integrated with Numerex cellular.

Numerex SMS Properties

Configuration Setting	Description
<code>sms.numerex.gatewayId</code>	SMS implementation will be used in the current build.  For example, for the Simplewise implementation the value is <code>simpleWireSmsSender</code> or <code>numerexSmsSender</code> .
<code>sms.numerex.password</code>	IP address of the SMS server
<code>sms.numerex.username</code>	The maximum number of characters to allow in an SMS message. The default is 157. The maximum is 160. If a message contains more than 160 characters, it will be truncated to 160.
<code>sms.service.beanName</code>	<code>numerexSmsSender</code> See General SMS Properties for details.

#### 21.3.4.3 HTTP Post Requests

HTTP Post Request Properties

Configuration Setting	Description
<code>sms.httpPost.username</code>	User name required for an HTTP Post request
<code>sms.httpPost.password</code>	Password required for an HTTP Post request
<code>sms.httpPost.baseUrl</code>	Base URL of the HTTP server
<code>sms.httpPost.shortCode</code>	Short code for an HTTP Post request
<code>sms.httpPost.countryCode</code>	A number representing the country code for an HTTP Post request. At this time, only <b>1</b> is valid.
<code>sms.httpPost.connectionTimeout</code>	Time in seconds for the connection timeout of an HTTP Post request
<code>sms.httpPost.socketTimeout</code>	Time in seconds for the socket timeout of an HTTP Post request

## 21.4 message.properties

The `message.properties` file defines the text of email and SMS notifications that are sent to various users when specific events occur. For example, when a door is opened in a home, the subscriber might receive an email and/or SMS notification informing him that it has occurred.

The following subsections detail the following types of messages:

- ❑ [Account Notifications on page 312](#)
- ❑ [Activation Confirmations on page 313](#)
- ❑ [Files from Cameras Over Allowed File Size Limits Notifications on page 312](#)
- ❑ [Touchstone System Event Notifications on page 315](#)
- ❑ [Security Event Notifications on page 316](#)
- ❑ [Device Event Notifications on page 332](#)
- ❑ [Trouble Event Notifications on page 339](#)

For each tag in the `message.properties` file, the text of email and SMS messages are configurable by modifying them in the `message.properties` file using a text editor such as Notepad or Microsoft Word.

*For example*, suppose a Converge subscriber has configured to receive email notifications whenever someone initiates a panic alarm either from the touchscreen or a key fob device. The subscriber might receive an email with the following text:

You have a burglary alarm in progress at 1234 Abigail Ave. The security monitoring representative is being notified.

Below is a summary of events related to this alarm.

All time in CDT time zone.

04/08/2010 04:58 PM System Armed Stay by Master (1,026 hours and 50 minutes ago)

05/21/2010 11:49 AM Alarm start

This is a monitoring message from your home security service.

This email might have been constructed from the text of the following `message.properties` tags (in order).

- ❑ `Alarm.panic.monitored.emailMsg`
- ❑ `Alarm.eventSummary.prefix`
- ❑ `Alarm.eventSummary.lastArm`
- ❑ `Alarm.eventSummary.alarmStart`
- ❑ `Event.emailMsgSuffix`

The following is the Alarm.panic.monitored.emailMsg line in the message.properties file:

```
Alarm.panic.monitored.emailMsg=You have a {0} alarm in
progress at {1}. The security monitoring representative \nis
being notified.
```

All the text to the right of the = is that portion of the text in the email message. The numbers in brackets ({0}, {1}, etc.) are variables that are filled in by the service modules based on the context of the message. A {0} might not mean the same thing in other tags or other conditions that prompted the notification. In this case, the variables mean the following:

{0} = Panic alarm type, such as burglary, medical, or fire

{1} = Premise address

\n represents a carriage return, as if you pressed the Enter key.

The text value of tags can be modified freely. There is no system limit on the number of characters that you can assign to a tag, but the 160-character limit for SMS messages still applies. The variable meanings cannot be modified, nor can additional variables be added because this information is hard-coded by the application.

#### 21.4.1 Email Message Suffix

The Email Message Suffix is a line of introductory text in email notifications to subscribers. The following tags define the text of the email suffix for all platforms.

Property	Platform	Variables
Event.emailMsgSuffix	Converge	N/A
insight.Event.emailMsgSuffix	Touchstone	{0} = Service Provider name for the Touchstone platform; See the homeAutomationSystem value.

## 21.4.2 Account Notifications

### 21.4.2.1 Files from Cameras Over Allowed File Size Limits Notifications

These notifications are sent to a subscriber when the files stored from his camera are over the allowed limits.

#### 21.4.2.1.1 Image Files Over Allowed Limits Notifications

Tag	Description	Variables
fileOverQuota.image.subject	Subject text of email notifications sent to subscribers when their uploaded image files have exceeded their limitations	N/A
fileOverQuota.image.body	Body text of email notifications sent to subscribers when their uploaded image files have exceeded their limitations	{0} = Maximum stored image size for the account

#### 21.4.2.1.2 Video Files Over Allowed Limits Notifications

Tag	Description	Variables
fileOverQuota.video.subject	Subject text of email notifications sent to subscribers when their uploaded video files have exceeded their limitations	N/A
fileOverQuota.video.body	Body text of email notifications sent to subscribers when their uploaded video files have exceeded their limitations	{0} = Maximum stored image size for the account

### 21.4.3 Activation Confirmations

Activation Confirmations are sent during the Activation process for the subscriber account.

Converge Activation Confirmations

Tag	Description	Variables
ActivationA.complete.subject	Subject text of email notifications sent to subscribers after they have activated their touchscreens (Activation A)	N/A
ActivationA.complete.emailMsg	Body text of email notifications sent to subscribers after they have activated their touchscreens (Activation A)	{0} = URL of Subscriber Portal login {1} = Subscriber's temporary username {2} = Subscriber's temporary password
ActivationB.complete.subject	Subject text of email notifications sent to subscribers after they have activated their Subscriber Portal account (Activation B)	N/A
ActivationB.complete.emailMsg	Body text of email notifications sent to subscribers after they have activated their Subscriber Portal account (Activation B)	N/A

#### 21.4.3.1 Single-Sign-On Enabled

**TOUCHSTONE ONLY**

##### 21.4.3.1.1 Activation

Activation - Single-Sign-On Enabled

Tag	Description	Variables
insightSSO.activation.subject	Subject text of email notifications sent to subscribers when their account is ready for activation (SSO)	{0} = Service Provider term for the Touchstone platform
insightSSO.activation.emailMsg	Body text of email notifications sent to subscribers when their account is ready for activation (SSO)	{0} = {3} = Service Provider name for the Touchstone platform

##### 21.4.3.1.2 Reset Account for Activation

Tag	Description	Variables
insightSSO.resetActivation.subject	Subject text of email notifications sent to subscribers when their account is has been reset activation	{0} = Service Provider term for the Touchstone platform

Tag	Description	Variables
insightSSO.resetActivation.emailMsg	Body text of email notifications sent to subscribers when their account is has been reset activation	{0} = Service Provider term for the Touchstone platform

#### 21.4.3.2 Single-Sign-On NOT Enabled

##### TOUCHSTONE ONLY

###### 21.4.3.2.1 Activation

Tag	Description	Variables
insight.activation.subject	Subject text of email notifications sent to subscribers when their account is ready for activation	{0} = Service Provider term for the Touchstone platform
insight.activation.emailMsg	Body text of email notifications sent to subscribers when their account is ready for activation	{0} = URL of Subscriber Portal login {1} = Subscriber's temporary username {2} = Subscriber's temporary password {3} = Service Provider name for the Touchstone platform

###### 21.4.3.2.2 Reset Account for Activation

Tag	Description	Variables
insight.resetActivation.subject	Subject text of email notifications sent to subscribers when their account is has been reset activation	{0} = Service Provider term for the Touchstone platform
insight.resetActivation.emailMsg	Body text of email notifications sent to subscribers when their account is has been reset activation	{0} = URL of Subscriber Portal login {1} = Service Provider name for the Touchstone platform

## 21.4.4 Touchstone System Event Notifications

### TOUCHSTONE ONLY

This section details notifications to Touchstone subscribers related to normal changes in their system. Currently only changes to subscribers' modes are detailed.

For information on notifications sent to subscribers regarding troubles related to their Hub and paired sensors/zones, see "["Trouble Event Notifications" on page 339](#)".

#### 21.4.4.1 Mode Event Notifications

These notifications might be issued when an Touchstone subscriber's mode setting of their system has been changed manually or as the result of a rule. The "Updated mode" variable uses the `SceneUpdateEvent` type listed in the message.properties file.

Tag	Description	Variables
<code>insight.SceneUpdateEvent.subject</code>	Subject text of email notifications sent to Touchstone subscribers when the mode setting of their system has been changed.	{0} = Updated mode {1} = Date/time of the update {2} = Service Provider name for the Touchstone platform
<code>insight.SceneUpdateEvent.emailMsg</code>	Body text of email notifications sent to Touchstone subscribers when the mode setting of their system has been changed.	{0} = First name on account {1} = Premise address {2} = Updated mode {3} = Date/time of the update {4} = Service Provider name for the Touchstone platform
<code>insight.SceneUpdateEvent.smsMsg</code>	Text of SMS notifications sent to Touchstone subscribers when the mode setting of their system has been changed.	{0} = First name on account {1} = Premise address {2} = Updated mode {3} = Date/time of the update {4} = Service Provider name for the Touchstone platform

## 21.4.5 Security Event Notifications

### CONVERGE ONLY

This section details notifications sent to subscribers and the central monitoring station related to normal changes and alarms in their security system.

- ❑ [Alarm Notifications](#)
- ❑ [Arm/Disarm System Notifications on page 330](#)
- ❑ [message.properties on page 310](#)
- ❑ [Keypad Code Change Notifications on page 331](#)
- ❑ [Password Reset Notifications on page 331](#)
- ❑ [Username Retrieve Notifications on page 331](#)

For information on notifications sent to subscribers regarding troubles related to the touchscreen and paired sensors/zones, see "[Trouble Event Notifications](#)" on page 339 and "[Zone Event Notifications](#)" on page 338.

#### **21.4.5.1 Alarm Notifications**

##### **CONVERGE ONLY**

The alarm notifications are divided into the following categories:

- [Alarm Initiated Notifications](#)
- [Alarm Initiated Notifications on page 318](#)
- [Panic Alarm Notifications on page 324](#)
- [Alarm Aborted Notifications on page 325](#)
- [Alarm Canceled Notifications on page 326](#)
- [Alarm Reset Notifications on page 327](#)
- [Smash and Grab Alarm Notifications](#)
- [Alarm Sent to Central Monitoring Station Notification on page 329](#)

### 21.4.5.1.1.Alarm Initiated Notifications

#### CONVERGE ONLY

The following tags describe the text of notifications that are sent when an alarm occurs, whether or not the alarm is ultimately aborted, canceled or sent to the central monitoring station.

##### 21.4.5.1.1.1 Monitored Accounts

For accounts with central station monitoring Enabled:

Tag	Description	Variables
Alarm.start.monitored.emailMsg	Body text of email notifications sent to subscribers when an alarm is tripped	{0} = Zone name {1} = Date/time the alarm occurred {2} = Number of seconds to abort the alarm
Alarm.start.monitored.emailMsg.1	Additional body text of email notifications sent to subscribers AFTER THE TRANSMISSION DELAY PERIOD HAS EXPIRED when an alarm is tripped	{0} = Zone name {1} = Date/time the alarm occurred
Alarm.start.monitored.smsMsg	Body text of SMS notifications sent to subscribers when an alarm is tripped (not during Entry Delay or Exit Delay)	{0} = Zone name {1} = Date/time the alarm occurred {2} = Number of seconds to abort the alarm
Alarm.start.monitored.smsMsg.1	Body text of SMS notifications sent to subscribers AFTER THE TRANSMISSION DELAY PERIOD HAS EXPIRED when an alarm is tripped (not during Entry Delay or Exit Delay)	{0} = Zone name {1} = Date/time the alarm occurred
Alarm.start.monitored.subject	Subject text of email notifications sent to subscribers when an alarm is tripped	{0} = Date/time the alarm occurred

#### 21.4.5.1.1.2 Not Monitored Accounts

For accounts with central station monitoring Not Enabled:

Tag	Description	Variables
Alarm.start.notmonitored.subject	Subject text of email notifications sent to subscribers when an alarm is tripped	{0} = Date/time the alarm occurred
Alarm.start.notmonitored.emailMsg	Body text of email notifications sent to subscribers when an alarm is tripped	{0} = Zone name {1} = Date/time the alarm occurred
Alarm.start.notmonitored.smsMsg	Body text of SMS notifications sent to subscribers when an alarm is tripped	{0} = Zone name {1} = Date/time the alarm occurred

#### 21.4.5.1.1.3 Alarm Detail Notifications

##### CONVERGE ONLY

The following tags are used to construct the Summary portion of alarm notification emails that describes the alarm in detail. The order and usage of these tags is determined by the service module depending on the reason for the notification. These tags are used whether or not the subscriber account is being monitored or unmonitored accounts.

Alarm Detail Notifications

Tag	Description	Variables
Alarm.eventSummary.prefix	Introduction to the section of an email	{0} = Time zone of security premises
Alarm.eventSummary.alarmCanceled	Details on a canceled alarm	{0} = Date/time the event occurred
Alarm.eventSummary.alarmReset	Details on a reset alarm	{0} = Date/time the event occurred
Alarm.eventSummary.alarmStart	Details on a tripped alarm whether or not it was aborted or canceled	{0} = Date/time the alarm was tripped
Alarm.eventSummary.centralNotified	Details on an alarm that was forwarded to the central monitoring station	{0} = Date/time the event occurred
Alarm.eventSummary.commLost	Details on a communication problem between the touchscreen and the system servers	{0} = Date/time the event occurred
Alarm.eventSummary.eventEntry	Details on an open/close event from an Entry/Exit security zone when the system was armed (resulting in an Entry Delay)	{0} = Date/time the event occurred  {1} = Open or Close  {2} = Name of the security zone
Alarm.eventSummary.openFrontDoor	Date/time an Entry/Exit security zone was opened when the system was disarmed	{0} = Date/time of the zone event
Alarm.eventSummary.lastArm	Details of the system arm status at the time of an alarm	{0} = Time the system was last armed or disarmed  {1} = Arming type (Away, Stay, or Night)  {2} = Keypad code of the user who performed this action  {3} = Number of hours since the system was last armed  {4} = Number of minutes (minus the number of hours) that the system was last armed

## Alarm Detail Notifications (continued)

Tag	Description	Variables
Alarm.eventSummary.lastArm.1	Alternate Details of the system arm status at the time of an alarm	{0} = Date/time the system was last armed {1} = Arming type (Away, Stay, or Night) {2} = Number of hours since the system was last armed {3} = Number of minutes (minus the number of hours) that the system was last armed
Alarm.eventSummary.unknownKeypadCode	Not used	N/A

### 21.4.5.1.2.Exit Error Notifications

#### CONVERGE ONLY

The following tags describe the text of notifications that are sent when an Exit Error occurs, An Exit Error occurs when the system is armed, but an Entry/Exit door is left open at the end of the Exit Delay time period.

##### 21.4.5.1.2.1 Monitored Accounts

For accounts with central station monitoring Enabled:

Tag	Description	Variables
Alarm.start.monitored.exitError.emailMsg	<p>Body text of email notifications sent to subscribers when an Exit Error occurs.</p> <p><b>Note:</b> The notifications that use this tag use the Alarm.start.monitored.subject value for their subject text.</p>	{0} = Zone name {1} = Date/time the alarm occurred {2} = Number of seconds to abort the alarm
Alarm.start.monitored.exitError.emailMsg.1	<p>Body text of email notifications sent to subscribers AFTER THE TRANSMISSION DELAY PERIOD HAS EXPIRED when an Exit Error occurs.</p> <p><b>Note:</b> The notifications that use this tag use the Alarm.start.monitored.subject value for their subject text.</p>	{0} = Zone name {1} = Date/time the alarm occurred
Alarm.start.monitored.exitError.smsMsg	Text of SMS notifications sent to subscribers when an Exit Error occurs	{0} = Zone name {1} = Date/time the alarm occurred {2} = Number of seconds to abort the alarm

#### 21.4.5.1.2.2 Not Monitored Accounts

For accounts with central station monitoring Not Enabled:

Tag	Description	Variables
Alarm.start.notmonitored.exitError.emailMsg	<p>Body text of email notifications sent to subscribers when an Exit Error occurs.</p> <p><b>Note:</b> The notifications that use this tag use the Alarm.start.notmonitored.subject value for their subject text.</p>	{0} = Zone name {1} = Date/time the alarm occurred
Alarm.start.notmonitored.exitError.smsMsg	<p>Text of SMS notifications sent to subscribers when an Exit Error occurs.</p> <p><b>Note:</b> The notifications that use this tag use the Alarm.start.notmonitored.subject value for their subject text.</p>	{0} = Zone name {1} = Date/time the alarm occurred
Alarm.start.monitored.exitError.smsMsg.1	<p>Text of SMS notifications sent to subscribers AFTER THE TRANSMISSION DELAY PERIOD HAS EXPIRED when an Exit Error occurs</p>	{0} = Zone name {1} = Date/time the alarm occurred

### 21.4.5.1.3.Panic Alarm Notifications

#### CONVERGE ONLY

Panic alarms are started manually either from the touchscreen or a key fob.

##### 21.4.5.1.3.1 Monitored Accounts

For accounts with central station monitoring Enabled:

Tag	Description	Variables
Alarm.panic.monitored.subject	Subject text of email notifications sent to subscribers when an alarm is tripped	{0} = Fire, Police, or Medical panic alarm {1} = Date/time the alarm was manually tripped
Alarm.panic.monitored.emailMsg	Body text of email notifications sent to subscribers when an alarm is tripped	{0} = Fire, Police, or Medical panic alarm {1} = Premises address
Alarm.panic.monitored.smsMsg	Body text of SMS notifications sent to subscribers when an alarm is tripped	{0} = Fire, Police, or Medical panic alarm {1} = Premises address

##### 21.4.5.1.3.2 Not Monitored Accounts

For accounts with central station monitoring Not Enabled:

Tag	Description	Variables
Alarm.panic.notmonitored.subject	Subject text of email notifications sent to subscribers when a panic alarm is tripped	{0} = Fire, Police, or Medical panic alarm {1} = Date/time the alarm was manually tripped
Alarm.panic.notmonitored.emailMsg	Body text of email notifications sent to subscribers when a panic alarm is tripped	{0} = Fire, Police, or Medical panic alarm {1} = Premises address
Alarm.panic.notmonitored.smsMsg	Body text of SMS notifications sent to subscribers when a panic alarm is tripped	N/A

#### **21.4.5.1.4. Alarm Aborted Notifications**

Aborting an alarm occurs when a subscriber enters a valid keypad code after an alarm has been faulted and within the Abort window (default: 30 seconds).

##### **21.4.5.1.4.1 Monitored Accounts**

For accounts with central station monitoring Enabled:

Tag	Description
Alarm.abort.monitored.subject	Subject text of email notifications sent to subscribers when an alarm has been aborted with a valid keypad code
Alarm.abort.monitored.emailMsg	Body text of email notifications sent to subscribers when an alarm has been aborted with a valid keypad code
Alarm.abort.monitored.smsMsg	Text of SMS notifications sent to subscribers when an alarm has been aborted with a valid keypad code

##### **21.4.5.1.4.2 Not Monitored Accounts**

For accounts with central station monitoring Not Enabled:

Tag	Description
Alarm.abort.notmonitored.subject	Subject text of email notifications sent to subscribers when an alarm has been aborted with a valid keypad code
Alarm.abort.notmonitored.emailMsg	Body text of email notifications sent to subscribers when an alarm has been aborted with a valid keypad code
Alarm.abort.notmonitored.smsMsg	Text of SMS notifications sent to subscribers when an alarm has been aborted with a valid keypad code

### 21.4.5.1.5. Alarm Canceled Notifications

#### CONVERGE ONLY

Cancelling an alarm occurs when a subscriber enters a valid keypad code after an alarm has been faulted and the Abort window has elapsed. By default, the Cancel window is 4 minutes.

##### 21.4.5.1.5.1 Monitored Accounts

For accounts with central station monitoring Enabled:

Tag	Description
Alarm.cancel.monitored.subject	Subject text of email notifications sent to subscribers when an alarm has been canceled with a valid keypad code
Alarm.cancel.monitored.emailMsg	Body text of email notifications sent to subscribers when an alarm has been canceled with a valid keypad code
Alarm.cancel.monitored.emailMsg.1	
Alarm.cancel.monitored.smsMsg	Body text of SMS notifications sent to subscribers when an alarm has been canceled with a valid keypad code

##### 21.4.5.1.5.2 Not Monitored Accounts

For accounts with central station monitoring Not Enabled:

Tag	Description
Alarm.cancel.notmonitored.subject	Subject text of notifications sent to subscribers when an alarm has been canceled with a valid keypad code
Alarm.cancel.notmonitored.emailMsg	Body text of email notifications sent to subscribers when an alarm has been canceled with a valid keypad code
Alarm.cancel.notmonitored.smsMsg	Text of SMS notifications sent to subscribers when an alarm has been canceled with a valid keypad code

#### 21.4.5.1.6. Alarm Reset Notifications

##### CONVERGE ONLY

The system is reset when one of the following occurs:

- An alarm is aborted or canceled
- The system has been in Alarm state for 4 minutes (default). After that time period, the system silences the sirens and returns to Arm state so it can monitor any new alarms.

##### 21.4.5.1.6.1 Monitored Accounts

For accounts with central station monitoring Enabled:

Tag	Description	Variables
Alarm.reset.monitored.subject	Subject text of email notifications sent to subscribers when has been reset after an alarm	N/A
Alarm.reset.monitored.emailMsg	Body text of email notifications sent to subscribers when the Home system is reset	{0} = Fire, Police, or Medical panic alarm {1} = Premises address

##### 21.4.5.1.6.2 Not Monitored Accounts

For accounts with central station monitoring Not Enabled:

Tag	Description	Variables
Alarm.reset.notmonitored.subject	Subject text of email notifications sent to subscribers when has been reset after an alarm	N/A
Alarm.reset.notmonitored.emailMsg	Body text of email notifications sent to subscribers when an alarm is tripped	{0} = Fire, Police, or Medical panic alarm {1} = Premises address

### 21.4.5.1.7.Smash and Grab Alarm Notifications

#### CONVERGE ONLY

A Smash & Grab alarm is generated by the server when the server has adequately determined that the touchscreen screen is not in commission after it receives an entry delay.

##### 21.4.5.1.7.1 Monitored Accounts

For accounts with central station monitoring Enabled:

Tag	Description	Variables
Alarm.smash.monitored.subject	Subject of email notifications sent to subscribers when a Smash & Grab scenario has been detected;	{0} = Date/time the alarm occurred
Alarm.smash.monitored.emailMsg	Body text of email notifications sent to subscribers when a Smash & Grab scenario has been detected;	{0} = Date/time the alarm occurred
Alarm.smash.monitored.smsMsg	Text of SMS notifications sent to subscribers when a Smash & Grab scenario has been detected;	{0} = Date/time the alarm occurred

##### 21.4.5.1.7.2 Not Monitored Accounts

For accounts with central station monitoring Not Enabled:

Tag	Description	Variables
Alarm.smash.notmonitored.subject	Subject of email notifications sent to subscribers when a Smash & Grab scenario has been detected;	{0} = Date/time the alarm occurred
Alarm.smash.notmonitored.emailMsg	Body text of email notifications sent to subscribers when a Smash & Grab scenario has been detected;	{0} = Date/time the alarm occurred
Alarm.smash.notmonitored.smsMsg	Text of SMS notifications sent to subscribers when a Smash & Grab scenario has been detected;	{0} = Date/time the alarm occurred

#### 21.4.5.1.8.Alarm Sent to Central Monitoring Station Notification

##### CONVERGE ONLY

For accounts with central station monitoring Enabled:

Tag	Description
Alarm.sent.monitored.subject	Subject text of email notifications sent to subscribers after an alarm was successfully sent to the central monitoring station
Alarm.sent.monitored.emailMsg	Text of email notifications sent to subscribers after an alarm was successfully sent to the central monitoring station
Alarm.sent.monitored.smsMsg	Text of SMS notifications sent to subscribers after an alarm was successfully sent to the central monitoring station

### **21.4.5.2 Arm/Disarm System Notifications**

#### **CONVERGE ONLY**

Arm/Disarm notifications might be issued when a Converge system is either armed or disarmed using any method or if an instant arming attempt failed.

**Converge Arm/Disarm System Notifications**

Tag	Description	Variables
ArmDisarmEvent.subject	Subject text of email notifications sent to subscribers when the system is armed or disarmed	{0} = Arm or Disarm {1} = Date/time of the event
ArmDisarmEvent.emailMsg	Body text of email notifications sent to subscribers when the system is armed or disarmed	{0} = First name on account {1} = Premise address {2} = Arm or Disarm {3} = Date/time of the event
ArmDisarmEvent.smsMsg	Text of SMS notifications sent to subscribers when the system is armed or disarmed	{0} = First name on account {1} = Premise address {2} = Arm or Disarm {3} = Date/time of the event

#### **21.4.5.3 Keypad Code Change Notifications**

##### **CONVERGE ONLY**

Notifications for keypad code changes might be sent whenever a system keypad has been modified.

Tag	Description
keypadCode.changed.subject	Subject text of email notifications sent to subscribers when a keypad code was changed.
keypadCode.changed.emailMsg	Body text of email notifications sent to subscribers when a keypad code was changed.
keypadCode.changed.smsMsg	Text of SMS notifications sent to subscribers when a keypad code was changed.

#### **21.4.5.4 Password Reset Notifications**

Notifications for password changes might be sent whenever a Subscriber Portal password has been reset.

Tag	Description
password.reset.subject	Subject text of email notifications sent to subscribers to reset their password
password.reset.body	Body text of email notifications sent to subscribers to reset their passwords

#### **21.4.5.5 Username Retrieve Notifications**

Notifications for username retrieval are sent when a subscriber has forgotten their username and requested a reminder.

Tag	Description
username.retrieve.subject	Subject text of email notifications sent to subscribers to reset their username
username.retrieve.body	Body text of email notifications sent to subscribers to reset their username

## 21.4.6 Device Event Notifications

This section details notifications sent to subscribers regarding normal event reported by their devices. The following types of notifications are covered:

- Camera Image/Video Capture Event Notifications
- Door Lock Event Notifications on page 334
- Lighting Device Event Notifications on page 335
- Motion Sensor Event Notifications on page 336
- Thermostat Event Notifications on page 337
- Zone Event Notifications on page 338

For information regarding troubles reported by subscriber devices, see "Trouble Event Notifications" on page 339.

### 21.4.6.1 Camera Image/Video Capture Event Notifications

These notifications might be issued when a camera takes a picture or video as the result of a rule.

Converge Camera Image/Video Capture Event Notifications

Tag	Description	Variables
OnDemandImageEvent.subject	Subject text of email notifications sent to subscribers when a lighting device is turned on or off	{0} = Date/time of the event
OnDemandImageEvent.emailMsg	Body text of email notifications sent to subscribers when a lighting device is turned on or off	{0} = First name on account {1} = Premise address {2} = Date/time of the event {3} = Name of rule that initiated the action
OnDemandImageEvent.smsMsg	Text of SMS notifications sent to subscribers when a lighting device is turned on or off	{0} = First name on account {1} = Premise address {2} = Date/time of the event {3} = Name of rule that initiated the action

Touchstone Camera Image/Video Capture Event Notifications

Tag	Description	Variables
insight.OnDemandImageEvent.subject	Subject text of email notifications sent to subscribers when a lighting device is turned on or off	{0} = Date/time of the event {1} = Service Provider name for the Touchstone platform

Tag	Description	Variables
insight.OnDemandImageEvent.emailMsg	Body text of email notifications sent to subscribers when a lighting device is turned on or off	{0} = First name on account {1} = Premise address {2} = Date/time of the event {3} = Name of rule that initiated the action {4} = Service Provider name for the Touchstone platform
insight.OnDemandImageEvent.smsMsg	Text of SMS notifications sent to subscribers when a lighting device is turned on or off	{0} = First name on account {1} = Premise address {2} = Date/time of the event {3} = Name of rule that initiated the action {4} = Service Provider name for the Touchstone platform

#### 21.4.6.2 Door Lock Event Notifications

Notifications for door lock device events might be sent when a door lock is unlocked or locked. The "Type of event" variable uses the `DoorLockEvent.on` and `DoorLockEvent.off` values.

##### Converge Door Lock Event Notifications

Tag	Description	Variables
<code>DoorLockEvent.subject</code>	Subject text of email notifications sent to subscribers when a door lock device is locked or unlocked	{0} = Type of event {1} = Date/time of the event
<code>DoorLockEvent.emailMsg</code>	Body text of email notifications sent to subscribers when a door lock device is locked or unlocked	{0} = First name on account {1} = Premise address {2} = Type of event {3} = Label of the device {4} = Date/time of the event
<code>DoorLockEvent.smsMsg</code>	Text of SMS notifications sent to subscribers when a door lock device is locked or unlocked	{0} = First name on account {1} = Premise address {2} = Type of event {3} = Label of the device {4} = Date/time of the event

##### Touchstone Door Lock Event Notifications

Tag	Description	Variables
<code>insight.DoorLockEvent.subject</code>	Subject text of email notifications sent to subscribers when a door lock device is locked or unlocked	{0} = Type of event {1} = Date/time of the event {2} = Service Provider name for the Touchstone platform
<code>insight.DoorLockEvent.emailMsg</code>	Body text of email notifications sent to subscribers when a door lock device is locked or unlocked	{0} = First name on account {1} = Premise address {2} = Type of event {3} = Label of the device {4} = Date/time of the event {5} = Service Provider name for the Touchstone platform
<code>insight.DoorLockEvent.smsMsg</code>	Text of SMS notifications sent to subscribers when a door lock device is locked or unlocked	{0} = First name on account {1} = Premise address {2} = Type of event {3} = Label of the device {4} = Date/time of the event {5} = Service Provider name for the Touchstone platform

### 21.4.6.3 Lighting Device Event Notifications

These notifications might be issued when a lighting device is turned on or off.

#### Converge Lighting Device Event Notifications

Tag	Description	Variables
LightingEvent.subject	Subject text of email notifications sent to subscribers when a lighting device is turned on or off	{0} = Event name {1} = Date/time of the event
LightingEvent.emailMsg	Body text of email notifications sent to subscribers when a lighting device is turned on or off	{0} = First name on account {1} = Premise address {2} = Device event, such as on or off {3} = Device label {4} = Date/time of the event
LightingEvent.smsMsg	Text of SMS notifications sent to subscribers when a lighting device is turned on or off	{0} = First name on account {1} = Premise address {2} = Device event, such as on or off {3} = Device label {4} = Date/time of the event

#### Touchstone Lighting Device Event Notifications

Tag	Description	Variables
insight.LightingEvent.subject	Subject text of email notifications sent to subscribers when a lighting device is turned on or off	{0} = Event name {1} = Date/time of the event {2} = Service Provider name for the Touchstone platform
insight.LightingEvent.emailMsg	Body text of email notifications sent to subscribers when a lighting device is turned on or off	{0} = First name on account {1} = Premise address {2} = Device event, such as on or off {3} = Device label {4} = Date/time of the event {5} = Service Provider name for the Touchstone platform
insight.LightingEvent.smsMsg	Text of SMS notifications sent to subscribers when a lighting device is turned on or off	{0} = First name on account {1} = Premise address {2} = Device event, such as on or off {3} = Device label {4} = Date/time of the event {5} = Service Provider name for the Touchstone platform

#### 21.4.6.4 Motion Sensor Event Notifications

Notifications for motion sensor events might be sent when a motion detector is faulted or cleared. The "Type of event" variable uses the "motion" and "still" Zone.types. For Converge systems, it is not necessary for an event to result in an alarm for the notification to be sent.

##### Converge Motion Sensor Event Notifications

Tag	Description	Variables
ZoneMotionEvent.subject	Subject text of email notifications sent to subscribers when a motion detector event occurs	{0} =Label for the sensor/zone {1} = Type of event {2} = Date/time of the event
ZoneMotionEvent.emailMsg	Body text of email notifications sent to subscribers when a motion detector event occurs	{0} = First name on account {1} = Premise address {2} = Label for the sensor/zone {3} = Type of event {4} = Date/time of the event
ZoneMotionEvent.smsMsg	Text of SMS notifications sent to subscribers when a motion detector event occurs	{0} = First name on account {1} = Premise address {2} = Label for the sensor/zone {3} = Type of event {4} = Date/time of the event

##### Touchstone Motion Sensor Event Notifications

Tag	Description	Variables
insight.ZoneMotionEvent.subject	Subject text of email notifications sent to subscribers when a motion detector event occurs	{0} =Label for the sensor/zone {1} = Type of event {2} = Date/time of the event
insight.ZoneMotionEvent.emailMsg	Body text of email notifications sent to subscribers when a motion detector event occurs	{0} = First name on account {1} = Premise address {2} = Label for the sensor/zone {3} = Type of event {4} = Date/time of the event
insight.ZoneMotionEvent.smsMsg	Text of SMS notifications sent to subscribers when a motion detector event occurs	{0} = First name on account {1} = Premise address {2} = Label for the sensor/zone {3} = Type of event {4} = Date/time of the event

#### 21.4.6.5 Thermostat Event Notifications

These notifications might be issued when a thermostat mode changes (on, off, auto, cool, heat, etc.). The "Type of event" variable uses the ThermostatEvent.systemMode values.

##### Converge Thermostat Event Notifications

Tag	Description	Variables
ThermostatEvent.subject	Subject text of email notifications sent to subscribers when a thermostat mode changes (on, off, auto, cool, heat, etc.)	{0} = Date/time of the event
ThermostatEvent.emailMsg	Body text of email notifications sent to subscribers when a thermostat mode changes (on, off, auto, cool, heat, etc.)	{0} = First name on account {1} = Premise address {2} = Date/time of the event {3} = Current thermostat mode {4} = Current room temperature
ThermostatEvent.smsMsg	Text of SMS notifications sent to subscribers when a thermostat mode changes (on, off, auto, cool, heat, etc.)	{0} = First name on account {1} = Premise address {2} = Date/time of the event

##### Touchstone Thermostat Event Notifications

Tag	Description	Variables
insight.ThermostatEvent.subject	Subject text of email notifications sent to subscribers when a thermostat mode changes (on, off, auto, cool, heat, etc.)	{0} = Date/time of the event {1} = Service Provider name for the Touchstone platform
insight.ThermostatEvent.emailMsg	Body text of email notifications sent to subscribers when a thermostat mode changes (on, off, auto, cool, heat, etc.)	{0} = First name on account {1} = Premise address {2} = Date/time of the event {3} = Current thermostat mode {4} = Current room temperature {5} = Service Provider name for the Touchstone platform
insight.ThermostatEvent.smsMsg	Text of SMS notifications sent to subscribers when a thermostat mode changes (on, off, auto, cool, heat, etc.)	{0} = First name on account {1} = Premise address {2} = Date/time of the event {3} = Current room temperature {4} = Service Provider name for the Touchstone platform

#### 21.4.6.6 Zone Event Notifications

Notifications of events from sensors might be sent when a sensor faulted. For example, a door is opened or carbon monoxide is detected or an open door is closed or a CO sensor detection is cleared. The "Type of event" variable uses the following `ZoneEvent.fault` and `ZoneEvent.restore` values.

For Converge systems, it is not necessary for an event to result in an alarm for the notification to be sent. The following properties are used for most security zone types.

See "[Motion Sensor Event Notifications](#)" on page 336 for information on motion sensor events.

#### Converge Zone Event Notifications

Tag	Description	Variables
<code>ZoneEvent.subject</code>	Subject text of email notifications sent to subscribers when a Zone event occurs	{0} = Zone name {1} = Date/time of the event
<code>ZoneEvent.emailMsg</code>	Body text of email notifications sent to subscribers when a Zone event occurs	{0} = First name on account {1} = Premise address {2} = Zone name {3} = Date/time of the event
<code>ZoneEvent.smsMsg</code>	Text of SMS notifications sent to subscribers when a Zone event occurs	{0} = First name on account {1} = Premise address {2} = Zone name {3} = Date/time of the event

#### Touchstone Zone Event Notifications

Tag	Description	Variables
<code>insight.ZoneEvent.subject</code>	Subject text of email notifications sent to subscribers when a Zone event occurs	{0} = Zone name {1} = Type of event {2} = Date/time of the event
<code>insight.ZoneEvent.emailMsg</code>	Body text of email notifications sent to subscribers when a Zone event occurs	{0} = First name on account {1} = Premise address {2} = Zone name {3} = Type of event {4} = Date/time of the event
<code>insight.ZoneEvent.smsMsg</code>	Text of SMS notifications sent to subscribers when a Zone event occurs	{0} = First name on account {1} = Premise address {2} = Zone name {3} = Type of event {4} = Date/time of the event

## 21.4.7 Trouble Event Notifications

Trouble Event notifications are supported for the following system elements:

- ❑ [CPE Device \(System\) Trouble Events](#)
- ❑ [Camera Trouble Event Notifications on page 341](#)
- ❑ [Connectivity Trouble Event Notifications on page 342](#)
- ❑ [Door Lock Device Trouble Event Notifications on page 343](#)
- ❑ [Lighting Device Trouble Event Notifications on page 344](#)
- ❑ [Peripheral Trouble Event Notifications on page 345](#)
- ❑ [Thermostat Trouble Event Notifications on page 347](#)
- ❑ [Zone Trouble Event Notifications on page 348](#)

### 21.4.7.1 CPE Device (System) Trouble Events

Notifications for System Trouble events might be sent when a problem is reported for the CPE such as loss of power. The "Type of trouble" variable uses the `SystemTroubleEvent` types listed in the `message.properties` file.

Converge CPE Device (System) Trouble Events

Tag	Description	Variables
<code>SystemTroubleEvent.subject</code>	Subject text of email notifications sent to subscribers when a trouble event is reported from the touchscreen.	{0} = Type of trouble {1} = Date/time of the event
<code>SystemTroubleEvent.emailMsg</code>	Body text of email notifications sent to subscribers when a trouble event is reported from the touchscreen.	{0} = First name on account {1} = Premise address {2} = Type of trouble {3} = Date/time of the event
<code>SystemTroubleEvent.smsMsg</code>	Text of SMS notifications sent to subscribers when a trouble event is reported from the touchscreen.	{0} = First name on account {1} = Premise address {2} = Type of trouble {3} = Date/time of the event

### Touchstone CPE Device (System) Trouble Events

Tag	Description	Variables
insight.SystemTroubleEvent.subject	Subject text of email notifications sent to subscribers when a trouble event is reported from the Hub.	{0} = Type of trouble {1} = Date/time of the event {2} = Service Provider name for the Touchstone platform
insight.SystemTroubleEvent.emailMsg	Body text of email notifications sent to subscribers when a trouble event is reported from the Hub.	{0} = First name on account {1} = Premise address {2} = Type of trouble {3} = Date/time of the event {4} = Service Provider name for the Touchstone platform
insight.SystemTroubleEvent.smsMsg	Text of SMS notifications sent to subscribers when a trouble event is reported from the Hub.	{0} = First name on account {1} = Premise address {2} = Type of trouble {3} = Date/time of the event {4} = Service Provider name for the Touchstone platform

#### 21.4.7.2 Camera Trouble Event Notifications

Notifications for Camera Trouble events might be sent when a problem is reported for a camera such as a loss of communication. The "Type of trouble" variable uses the CameraTroubleEvent types listed in the message.properties file.

##### Converge Camera Trouble Event Notifications

Tag	Description	Variables
CameraTroubleEvent.subject	Subject text of email notifications sent to subscribers when a trouble event is reported from a camera	{0} = Type of trouble {1} = Date/time of the event
CameraTroubleEvent.emailMsg	Body text of email notifications sent to subscribers when a trouble event is reported from a camera.	{0} = First name on account {1} = Premise address {2} = Type of trouble {3} = Label for the camera {4} = Date/time of the event
CameraTroubleEvent.smsMsg	Text of SMS notifications sent to subscribers when a trouble event is reported from a camera.	{0} = First name on account {1} = Premise address {2} = Type of trouble {3} = Date/time of the event

##### Touchstone Camera Trouble Event Notifications

Tag	Description	Variables
insight.CameraTroubleEvent.subject	Subject text of email notifications sent to subscribers when a trouble event is reported from a camera	{0} = Type of trouble {1} = Date/time of the event {2} = Service Provider name for the Touchstone platform
insight.CameraTroubleEvent.emailMsg	Body text of email notifications sent to subscribers when a trouble event is reported from a camera.	{0} = First name on account {1} = Premise address {2} = Type of trouble {3} = Label for the camera {4} = Date/time of the event {5} = Service Provider name for the Touchstone platform
insight.CameraTroubleEvent.smsMsg	Text of SMS notifications sent to subscribers when a trouble event is reported from a camera.	{0} = First name on account {1} = Premise address {2} = Type of trouble {3} = Date/time of the event {4} = Service Provider name for the Touchstone platform

### 21.4.7.3 Connectivity Trouble Event Notifications

Notifications for Connectivity Trouble events might be sent whenever the CPE loses contact with the Server cluster(s) over either broadband or the cellular network (Converge). The notifications might also be sent when the connectivity is restored. The "Connectivity event" variable uses the CommunicationEvent types listed in the message.properties file.

#### Converge Connectivity Trouble Event Notifications

Tag	Description	Variables
CommunicationEvent.subject	Subject text of email notifications sent to subscribers when the CPE device loses broadband or cellular connectivity with the system servers	{0} = Connectivity event {1} = Date/time of the event
CommunicationEvent.emailMsg	Body text of email notifications sent to subscribers when the CPE device loses or regains connectivity with the system servers	{0} = First name on account {1} = Premise address {2} = Connectivity event {3} = Date/time of the event
CommunicationEvent.smsMsg	Text of SMS notifications sent to subscribers when the CPE device loses broadband or cellular connectivity with the system servers	{0} = First name on account {1} = Premise address {2} = Connectivity event {3} = Date/time of the event

#### Touchstone Connectivity Trouble Event Notifications

Tag	Description	Variables
insight.CommunicationEvent.subject	Subject text of email notifications sent to subscribers when the CPE device loses broadband connectivity with the system servers	{0} = Connectivity event {1} = Date/time of the event {2} = Service Provider name for the Touchstone platform
insight.CommunicationEvent.emailMsg	Body text of email notifications sent to subscribers when the CPE device loses or regains connectivity with the system servers	{0} = First name on account {1} = Premise address {2} = Connectivity event {3} = Date/time of the event {4} = Service Provider name for the Touchstone platform
insight.CommunicationEvent.smsMsg	Text of SMS notifications sent to subscribers when the CPE device loses broadband connectivity with the system servers	{0} = First name on account {1} = Premise address {2} = Connectivity event {3} = Date/time of the event {4} = Service Provider name for the Touchstone platform

#### 21.4.7.4 Door Lock Device Trouble Event Notifications

Notifications for Door Lock Device Trouble events might be sent when a problem is reported for a ZigBee door lock device such as low battery or communication. The "Type of trouble" variable uses the DoorLockTroubleEvent types listed in the message.properties file.

##### Converge Door Lock Device Trouble Event Notifications

Tag	Description	Variables
DoorLockTroubleEvent.subject	Subject text of email notifications sent to subscribers when a trouble event is reported from a door lock device.	{0} = Type of trouble {1} = Date/time of the event
DoorLockTroubleEvent.emailMsg	Body text of email notifications sent to subscribers when a trouble event is reported from a door lock device.	{0} = First name on account {1} = Premise address {2} = Type of trouble {3} = Label for the door lock device {4} = Date/time of the event
DoorLockTroubleEvent.smsMsg	Text of SMS notifications sent to subscribers when a trouble event is reported from a door lock device.	{0} = First name on account {1} = Premise address {2} = Type of trouble {3} = Date/time of the event

##### Touchstone Door Lock Device Trouble Event Notifications

Tag	Description	Variables
insight.DoorLockTroubleEvent.subject	Subject text of email notifications sent to subscribers when a trouble event is reported from a door lock device.	{0} = Type of trouble {1} = Date/time of the event {2} = Service Provider name for the Touchstone platform
insight.DoorLockTroubleEvent.emailMsg	Body text of email notifications sent to subscribers when a trouble event is reported from a door lock device.	{0} = First name on account {1} = Premise address {2} = Type of trouble {3} = Label for the door lock device {4} = Date/time of the event {5} = Service Provider name for the Touchstone platform
insight.DoorLockTroubleEvent.smsMsg	Text of SMS notifications sent to subscribers when a trouble event is reported from a door lock device.	{0} = First name on account {1} = Premise address {2} = Type of trouble {3} = Date/time of the event {4} = Service Provider name for the Touchstone platform

#### **21.4.7.5 Lighting Device Trouble Event Notifications**

Notifications for Lighting Device Trouble events might be sent when a lighting device such as loss of power or communication. The "Type of trouble" variable uses the `LightingTroubleEvent` types listed in the `message.properties` file.

##### Converge Lighting Device Trouble Event Notifications

Tag	Description	Variables
<code>LightingTroubleEvent.subject</code>	Subject text of email notifications sent to subscribers when a trouble event is reported from a lighting device.	{0} = Type of trouble {1} = Date/time of the event
<code>LightingTroubleEvent.emailMsg</code>	Body text of email notifications sent to subscribers when a trouble event is reported from a lighting device.	{0} = First name on account {1} = Premise address {2} = Type of trouble {3} = Label for the lighting device {4} = Date/time of the event
<code>LightingTroubleEvent.smsMsg</code>	Text of SMS notifications sent to subscribers when a trouble event is reported from a lighting device.	{0} = First name on account {1} = Premise address {2} = Type of trouble {3} = Date/time of the event

##### Touchstone Lighting Device Trouble Event Notifications

Tag	Description	Variables
<code>insight.LightingTroubleEvent.subject</code>	Subject text of email notifications sent to subscribers when a trouble event is reported from a lighting device.	{0} = Type of trouble {1} = Date/time of the event {2} = Service Provider name for the Touchstone platform
<code>insight.LightingTroubleEvent.emailMsg</code>	Body text of email notifications sent to subscribers when a trouble event is reported from a lighting device.	{0} = First name on account {1} = Premise address {2} = Type of trouble {3} = Label for the lighting device {4} = Date/time of the event {5} = Service Provider name for the Touchstone platform
<code>insight.LightingTroubleEvent.smsMsg</code>	Text of SMS notifications sent to subscribers when a trouble event is reported from a lighting device.	{0} = First name on account {1} = Premise address {2} = Type of trouble {3} = Date/time of the event {4} = Service Provider name for the Touchstone platform

#### 21.4.7.6 Peripheral Trouble Event Notifications

Notifications for Peripheral Trouble events might be sent when a problem is reported for a light module, appliance module, or, for Converge systems, a key fob, siren, or DSC key pad or other sensor/device that cannot be a security zone (`PeripheralTroubleEvent.peripheralType`). Types of troubles might include a low battery or an open cover. The "Type of trouble" variable uses the `PeripheralTroubleEvent` types listed in the `message.properties` file.

#### Converge Peripheral Trouble Event Notifications

Tag	Description	Variables
<code>PeripheralTroubleEvent.subject</code>	Subject text of email notifications sent to subscribers when a trouble event is reported from a peripheral	{0} = Type of trouble {1} = Date/time of the event
<code>PeripheralTroubleEvent.emailMsg</code>	Body text of email notifications sent to subscribers when a trouble event (such as Low Battery or Tamper) is reported from a peripheral	{0} = First name on account {1} = Premise address {2} = Type of trouble {3} = Peripheral type {4} = Serial number of the peripheral {5} = Date/time of the event
<code>PeripheralTroubleEvent.smsMsg</code>	Text of SMS notifications sent to subscribers when a trouble event (such as Low Battery or Tamper) is reported from a peripheral	{0} = First name on account {1} = Premise address {2} = Peripheral type {3} = Date/time of the event

#### Touchstone Peripheral Trouble Event Notifications

Tag	Description	Variables
<code>insight.PeripheralTroubleEvent.subject</code>	Subject text of email notifications sent to subscribers when a trouble event is reported from a peripheral	{0} = Type of trouble {1} = Date/time of the event {2} = Service Provider name for the Touchstone platform
<code>insight.PeripheralTroubleEvent.emailMsg</code>	Body text of email notifications sent to subscribers when a trouble event (such as Low Battery or Tamper) is reported from a peripheral	{0} = First name on account {1} = Premise address {2} = Type of trouble {3} = Peripheral type {4} = Serial number of the peripheral {5} = Date/time of the event {6} = Service Provider name for the Touchstone platform

Tag	Description	Variables
insight.PeripheralTroubleEvent.smsMsg	Text of SMS notifications sent to subscribers when a trouble event (such as Low Battery or Tamper) is reported from a peripheral	{0} = First name on account {1} = Premise address {2} = Peripheral type {3} = Date/time of the event {4} = Service Provider name for the Touchstone platform

#### 21.4.7.7 Thermostat Trouble Event Notifications

Notifications for Thermostat Trouble events might be sent when a problem is reported for a thermostat such as loss of power or communication. The "Type of trouble" variable uses the ThermostatTroubleEvent types listed in the message.properties file.

##### Converge Thermostat Trouble Event Notifications

Tag	Description	Variables
ThermostatTroubleEvent.subject	Subject text of email notifications sent to subscribers when a trouble event is reported from a thermostat.	{0} = Type of trouble event {1} = Date/time of the event
ThermostatTroubleEvent.emailMsg	Body text of email notifications sent to subscribers when a trouble event is reported for a thermostat.	{0} = First name on account {1} = Premise address {2} = Label for the thermostat {3} = Type of trouble event {4} = Date/time of the event
ThermostatTroubleEvent.smsMsg	Text of SMS notifications sent to subscribers when a trouble event is reported for a thermostat.	{0} = First name on account {1} = Premise address {2} = Type of trouble event {3} = Date/time of the event

##### Touchstone Thermostat Trouble Event Notifications

Tag	Description	Variables
insight.ThermostatTroubleEvent.subject	Subject text of email notifications sent to subscribers when a trouble event is reported from a thermostat.	{0} = Type of trouble event {1} = Date/time of the event {2} = Service Provider name for the Touchstone platform
insight.ThermostatTroubleEvent.emailMsg	Body text of email notifications sent to subscribers when a trouble event is reported for a thermostat.	{0} = First name on account {1} = Premise address {2} = Label for the thermostat {3} = Type of trouble event {4} = Date/time of the event {5} = Service Provider name for the Touchstone platform
insight.ThermostatTroubleEvent.smsMsg	Text of SMS notifications sent to subscribers when a trouble event is reported for a thermostat.	{0} = First name on account {1} = Premise address {2} = Type of trouble event {3} = Date/time of the event {4} = Service Provider name for the Touchstone platform

#### 21.4.7.8 Zone Trouble Event Notifications

Notifications for Zone Trouble events might be sent when a problem is reported for a sensor, such as a loss of power or communication, or an open cover. The "Type of trouble" variable uses the ZoneTroubleEvent types listed in the message.properties file.

##### Converge Zone Trouble Event Notifications

Tag	Description	Variables
ZoneTroubleEvent.subject	Subject text of email notifications sent to subscribers when a trouble event is reported from a security sensor:	{0} = Label for security zone {1} = Type of trouble {2} = Date/time of the event
ZoneTroubleEvent.emailMsg	Body text of email notifications sent to subscribers when a trouble event (such as Low Battery or Tamper) is reported from a security sensor	{0} = First name on account {1} = Premise address {2} = Label for security zone {3} = Type of trouble {4} = Date/time of the event
ZoneTroubleEvent.smsMsg	Text of SMS notifications sent to subscribers when a trouble event (such as Low Battery or Tamper) is reported from a security sensor	{0} = First name on account {1} = Premise address {2} = Type of trouble {3} = Date/time of the event

##### Touchstone Zone Trouble Event Notifications

Tag	Description	Variables
insight.ZoneTroubleEvent.subject	Subject text of email notifications sent to subscribers when a trouble event is reported from a sensor:	{0} = Label for the sensor {1} = Type of trouble {2} = Date/time of the event
insight.ZoneTroubleEvent.emailMsg	Body text of email notifications sent to subscribers when a trouble event (such as Low Battery or Tamper) is reported from a sensor	{0} = First name on account {1} = Premise address {2} = Label for the sensor {3} = Type of trouble {4} = Date/time of the event
insight.ZoneTroubleEvent.smsMsg	Text of SMS notifications sent to subscribers when a trouble event (such as Low Battery or Tamper) is reported from a sensor	{0} = First name on account {1} = Premise address {2} = Type of trouble {3} = Date/time of the event {4} = Service Provider name for the Touchstone platform

## 21.5 Tier Properties

While the other properties described in this book, define the behavior of the system for all users, the Tier properties define the behavior and the allowed limits for customers based on their *Tier* or assigned *Packages*.

For example, the `sms.dailyLimit` property defines the maximum number of SMS messages allowed to a single customer account to keep them notified about their system activity (as defined by a Rule). All customers who are assigned to the Gold tier might be allowed 10 SMS messages. All customers assigned to the Bronze tier might only be allowed two.

If no value is assigned a user's Tier or if the service provider does not use tiers, the Global Tier value is used.

If the service provider uses Tiers, every subscriber is assigned one, and only one Tier. Each Tier has a Tier Property value. Each subscriber can be assigned multiple Packages. Each Package only uses some Tier Properties, but typically not all. If the subscriber is assigned a Package with a Tier Property value that is different from that of his Tier, then the Package's Tier Property value overrides the Tier's Tier Property value.

Tier Properties are modified from the Management Portal. See *Management Portal Guide* for information about how to manage Tiers and Packages.

## 21.6 Account Read Only Properties

The `accountreadonly.properties` file determines which account attributes can be changed from the Management Portal when the account was created by an *external source*. When a property is set to true, the attribute cannot be edited.

Table 7: `accountreadonly.properties` File Details

Converge `accountreadonly.properties` File Details

Property	Management Portal Field
<code>firstName</code>	First Name
<code>lastName</code>	Last Name
<code>phoneNumber</code>	Phone Number
<code>emailAddress</code>	Email Address
<code>groups.0.name</code>	Packages assigned to the account
<code>externalReference</code>	Not applicable
<code>emergencyContacts.0</code>	Emergency Contacts  The first emergency contact cannot be edited, deleted, or modified in the Management Portal or Subscriber Portal.
<code>premises.0.timeZone</code>	Manage Account -> Update Time Zone
<code>premises.0.address.address1</code>	Premise Address

### Touchstone accountreadonly.properties File Details

Property	Management Portal Field
insight.firstName	First Name
insight.lastName	Last Name
insight.phoneNumber	Phone Number
insight.emailAddress	Email Address
insight.groups.0.name	Packages assigned to the account
insight.externalReference	Not applicable
insight.emergencyContacts.0	Emergency Contacts  The first emergency contact cannot be edited, deleted, or modified in the Management Portal or Subscriber Portal.
insight.premises.0.timeZone	Manage Account -> Update Time Zone
insight.premises.0.address.address1	Premise Address

## 21.7 Database System Properties

There are several system properties that are defined in the lcontrol database. These properties can be edited directly.

### 21.7.1 system\_property

The key column defines the property name, and the value column contains the value of the property.

key	value	Description
customPatchLevel	0	
dbPatchLevel	N/A	Highest most recent patch number.
dbVersion	1	
event.timeToLive	30	Specifies how many days of events (sensor events, home automation events, cpe commands, cpe events, camera access events, audit log, etc.).  Values can be 15-60.
event.precreateDays	3	Specifies how many days of sub-partitions need to be pre-created when the background database script is trying to split the old partition of the security_event table.  Values can be 1-5.
lastCleanupTime	0	
server.property.version	0	

## 21.7.2 xmpp\_property

The name column defines the property name, and the prop\_value column contains the value of the property.

<b>name</b>	<b>prop_value</b>	<b>Description</b>
tiscali.pool.size	30	Thread pool size to process the incoming packets for XMPP connections
xmpp.client.cert.policy	disabled	
xmpp.client.compression.policy	disabled	
xmpp.client.idle	-1	
xmpp.client.processing.threads	32	Number of Executor that will be used by processors to process incoming stanzas for normal TCP/IP connections
xmpp.client.tls.policy	required	Number of Executor that will be used by processors to process incoming stanzas for SSL connections
xmpp.client_ssl.processing.threads	32	
xmpp.domain	xmpp	
xmpp.socket.ssl.keypass	uc0ntr0l	The password used to open the keystore for SSL
xmpp.socket.ssl.keystore	server/lib/keystore	The keystore file name and path for SSL of XMPP connections
xmpp.socket.ssl.trustpass	changeit	The password for the trust store
xmpp.socket.ssl.truststore	server/lib/cacerts	The trust store file name and path for the SSL of XMPP connections

## 22 Proactively Monitoring the Oracle Database

Once the Oracle database in a production environment, continuous health monitoring is required to reduce or eliminate unexpected downtime. Use the tools described in this section to efficiently monitor the health of the Oracle database.

### 22.1 Oracle Enterprise Manager

This is a set of systems management tools provided by Oracle Corporation to manage the Oracle environment. It can be set up to monitor the Oracle database 24 x 7 and send out alerts of varying levels by email, pager, cell phone, etc. as needed. The following basic contents can be monitored by the Enterprise Manager:

- ❑ Database or listener is down
- ❑ Tablespace usage
- ❑ Critical ORA-error stack, such as critical ORA-0600 and ORA-07445 that could cause instance down.
- ❑ Broken DBMS job if any - Check if a job should be running. If yes, then un-break. If no, then remove it from job queue
- ❑ Invalid objects - Either recompile or remove invalid objects as needed
- ❑ Checking replication process status if such process running.
- ❑ Database server space usage
- ❑ Database server is down.
- ❑ Any important processes in application site.

#### 22.1.1 Advantages

- ❑ Easy to setup and monitor with all graphic output.
- ❑ Comes with enterprise edition without license required

#### 22.1.2 Disadvantages

- ❑ Might require additional license fee if the database is standard edition at early version, like 9i.10g. Verify before using.
- ❑ Needs to maintain an additional database. However, it is a small database and the setup shouldn't be complex.
- ❑ If the Enterprise Manager database is down, there is no monitoring.

#### 22.1.3 Recommendation

The Oracle Enterprise Manager is preferred to monitor the Oracle databases as customer, which is much easier to setup and monitor daily.

## 22.2 OS Shell Script Running on OS Level

Shell scripts including query script can be run as cron jobs on the Operating System level to monitor the database's health. Alerts of varying levels can be sent by email, pager, cell phone, etc.

### 22.2.1 Advantages

- Monitoring is more solid without interruption by other tools.
- More flexible

### 22.2.2 Disadvantages

- More workload to write the script
- Requires potentially more skilled IT personal to set it up

# 23 Database Management Processes

## 23.1 Data Maintenance

The Database segment runs purge scripts to delete the following after a determined amount of time:

- Event data from the Main database
- Video and image files captured at subscribers' premises

The system property `event.timeToLive` in the `system_property` table controls how long event data is kept before they are purged. The default value is **30** days. The system property `event.precreateDays` specifies how many days of sub-partitions need to be pre-created. The default is **3**.

The scripts are employed in a cron job that runs nightly. This operation only needs to be performed once. Server upgrades will not overwrite this process.

### 23.1.1 Troubleshooting: Purge Script Takes a Long Time to Finish

The purge script could take several hours to run or even a full day.

Indexes are retained when the old records are deleted since the system continues to support the current transactions. This requirement causes the purge script to run more slowly than it otherwise would.

**The following circumstances could slow down the process even longer:**

1. The purge script cannot run unless the `security_event` table has been migrated to a partitioned table. The `security_event` is partitioned by `premise_fk` first, then sub-partitioned by date.
2. The purge script is run during the day or at any time when the server is especially busy.
3. The script has not been run for long time, so there is a large back-log of records to process.

### 23.1.2 Setting up the Purge Scripts

#### 23.1.2.1 Prepare to create the cron job:

1. Create a new directory in the file system where the main Oracle database user can access. Grant write permission to Oracle (Unix user) user and read permission to other users.

For example:

```
$ mkdir /u01/converge/data_cleanup
$ chmod 755 /u01/converge/data_cleanup
```

2. Login to Oracle as `sysdba` and create a Directory object called `CLEANUP_DIR` that points to the new directory.

Grant *read/write* permission of the object to the Oracle user who is going to run the cleanup script, such as:

```
SQL> create directory CLEANUP_DIR as '/tmp/cleanup';
```

---

```
SQL> grant read/write on directory CLEANUP_DIR to ucontrol;
```

**Note:** ucontrol is the user name to run the cleanup script.

#### 23.1.2.2 Install the Cleanup SQL Package:

3. Login to Oracle as sysdba and create a Directory object called CLEANUP\_DIR that points to the new directory.

Grant read/write permission of the object to the Oracle user who is going to run the cleanup script, such as:

```
SQL> create directory CLEANUP_DIR as '/u01/converge/data_
cleanup';
```

```
SQL> grant read/write on directory CLEANUP_DIR to ucontrol;
```

#### 23.1.2.3 Set Up a Cron Job to Run the Oracle Cleanup Procedure

**Note:** All following steps need to be run under an Oracle user, such as oracle11 Linux user.

By default this cron job is started every day at 1 am.

It starts the following script to archive data:

```
SQL>exec ucontrol_cleanup.start_cleanup;
```

4. If this is the first time to load the cron job, check the parameters of the shell command in cleanup\_db.cron, including:

- When the job will start
- Database user name/password, etc.
- ORACLE\_HOME, ORACLE\_SID  
(to ensure it is the directory where the SQL script is located)

5. Run crontab -l to check if the cleanup\_db.sh job has been running.

6. Run crontab cleanup\_db.cron to load the job.

**Note:** After the cron job has run, there are two files generated in /CLEANUP\_DIR. In the following formats:

- diagnostic-file-to-delete-yyyy-mm-dd.txt
- event-file-to-delete- yyyy-mm-dd.txt

...where yyyy is the year the file was created, mm is the month, and dd is the date.

#### 23.1.2.4 Set Up a Cron Job to Delete the Expired Image/Video Files:

**Note:** Run these steps as a WebLogic user.

The delete\_file.sh shell script does the following:

- a. Looks for files under /CLEANUP\_DIR for the same day,
- b. Deletes any file based on the file name or path in the files created from step 6.

By default the cron job is started every day at 5 am (four hours after the database cleanup procedure started).

7. Run `crontab -l` to check if `delete_file.sh` job has been running.

8. Run `crontab delete_file.cron` to load the job.

This section describes how to set up the cron jobs used to keep the system running efficiently.

## 23.2 Standard Replication Cron Jobs

This section describes how to set up the cron jobs used if your system uses standard replication.

### 23.2.1 Manage the Cron Job to Perform Standard Replication

#### 23.2.1.1 Monitor the Status of the Cron Job to Data Replication

To monitor the status of the current replication process:

```
./monitor-replication-job.sh
```

This command generates a report about the status of current replication process. If you see STOPPED in the report, it means the replication process is stopped. In this case, ask for your DBA's help to identify the real reason of the issue.

After the issue has been resolved. You can run `./start-replication-job.sh` to restart the process.

#### 23.2.1.2 Set Up a Cron Job to Perform Standard Replication

**Note:** This operation is only performed if a) this operation has not been performed before and b) if your system does not use an alternate streaming method (such as Oracle Streaming or Golden Gate).

**IMPORTANT:** All the steps in this section are run as a user that has direct database access, such as the oracle11 Linux user.

##### 23.2.1.2.1.Preparation

1. On both the Main and Backup databases, edit the `tnsnames.ora` file to identify the TNS name of both database.
2. Note the IP address of the Main and Backup databases and/or the SID and/or SERVER name)
3. Note the global database name of the Main and Backup databases (`SELECT * FROM GLOBAL_NAME;`).
4. Note the password of the system user of the Main and Backup databases.

### 23.2.1.2.2.Operations

**Note:** Execute the following steps from a console environment initialised to connect to standby database server.

1. Create a new Back-up database server:

```
./create-standby-db.sh <params>
```

**Note:** Use this script to recreate the Backup database from scratch. If there is any issue during this process:

- a. Resolve the issue.
- b. Run the drop-standby-db.sh script .
- c. Delete all replication related database objects in the Application nodes and Backup server, and re-run the script in step 1.

2. Set up the cron job to run the synchronizing procedure from Backup database to Main database.

- a. Move the following files in the `replication-script-oracle-SE` to a new file directory as needed by the environment:
  - `sync_standby_to_main.cron`
  - `sync_standby_to_main.sh`
  - `sync_standby_to_main.sql`
  - `refresh-system-status.sql`
- b. Edit `sync_standby_to_main.cron`, and ensure it the proper database link name to access the primary database. *For Converge systems*, ensure it contains the correct username and password for the Back-up Alarm database.
- c. Edit `sync_standby_to_main.sh` file. *For Converge systems*, ensure the proper environment variables are set for accessing the Back-up Alarm database:
  - `ORACLE_BASE`, `ORACLE_HOME`, and `ORACLE_SID` must be set correctly according to the local database environment
  - `SYNC_SCRIPT_DIR` must be set to the directory where the `sync_standby_to_main` files were placed (step a)
- d. Run `crontab -l` to determine whether the `sync_standby_to_main.sh` job is already scheduled in the cron job.  
If not, run `crontab sync_standby_to_main.cron` to load the job.
- e. Open the `sync_standby_to_main.sh` file, and ensure the `ORACLE_HOME`, `ORACLE_SID` is the directory of where the SQL scripts are located.
- f. By default the cron job is started every **15** minutes, which calls `sync_standby_to_`

`main.sh` to start the database transactions to synchronize data that is not replicated via Oracle replication.

### 23.2.2 Other Standard Replication Process Actions

**To stop the replication process:**

```
./stop-replication-job.sh
```

**To manually refresh replicated objects in backup alarm database**

**CONVERGE ONLY**

The Backup database is already set up to periodically refresh at 10 minute intervals. Use this script to manually force a refresh at any time, and fix the broken state of the internal Database Refresh job.

**Recommended:** Invoke this script at one hour intervals in an OS cron job set up as a back-up to the internal Database Refresh job.

```
./refresh-standby-db.sh <params>
```

**To synchronize replicated data in the Backup database**

**CONVERGE ONLY**

Use this script to delete and recreate only the replicated objects in the Backup Alarm server. This script is generally expected to be run after any manual updates to the Main Database (for example, patches, recovery after failure, etc.).

Use this operation when major changes are made to the Main database during upgrades, use this operation to recreate the entire Backup database.

```
./drop-standby-db.sh <params>
./stop-replication-job.sh
./create-standby-db.sh <params>
```

**To delete all replication related database objects in Main and (Converge) Backup databases:**

```
./drop-standby-db.sh <params>
```

### 23.2.3 Create a Cron Job to Perform Nightly Database Cleanup

**Note:** Only performed if this operation has not been performed before.

**Prepare to create the cron job:**

1. Create a new directory in the file system where the main Oracle database user can access. Grant the write permission to Oracle (unix user) user and read permission to other users.

For example, `mkdir /home/oracle/archived`

2. Login to Oracle as `sysdba` and create a Directory object called '`CLEANUP_DIR`' point to the

directory created in step above and grant the read/write permission of the object to the Oracle user who is going to run the cleanup script, such as:

```
SQL> create directory CLEANUP_DIR as '/tmp/cleanup';  
SQL> grant read/write on directory CLEANUP_DIR to ucontrol;  
(ucontrol is the user name to run the cleanup script)
```

#### Install the Cleanup SQL Package:

3. Log in Oracle database as user who has the application tables, install the package:

```
SQL>@ucontrol_cleanup.sql;
```

#### Set Up a Cron Job to Run the Oracle Cleanup Procedure:

**Note:** All following steps need to be run under an Oracle user, such as oracle11 Linux user.

4. If this is the first time to load the cron job, check the parameters of the shell command in cleanup\_db.cron, including:

- When the job will start
- Oracle user name/password, etc.
- File path to access the expired image/video filename created by the SQL procedure
- Root file path of the image/video file is saved
- ORACLE\_HOME, ORACLE\_SID (to ensure it is the directory where the SQL script is located)

5. Run crontab -l to check if the cleanup\_db.sh job has been running.

---

6. Run `crontab cleanup_db.cron` to load the job.

**Note:** By default the cron job is started every day at 1 am, it starts the script to archive data:

```
SQL>exec ucontrol_cleanup.start_cleanup;
```

**Note:** After the cron job has run, there are two files generated in `/CLEANUP_DIR`. In the following formats:

- `diagnostic-file-to-delete-xxxx-yy-dd.txt`
- `event-file-to-delete- xxxx-yy-dd.txt`

...where `xxxx` is the year the file was created, `yy` is the month, and `dd` is the date.

### Set Up a Cron Job to Delete the Expired Image/Video Files

The `delete_file.sh` shell script does the following:

- a. Looks for files under `/CLEANUP_DIR` for the same day,
- b. Deletes any file based on the file name or path in the files created from step 6.

**Note:** All following steps need to be run under a WebLogic user.

7. Run `crontab -l` to check if `cleanup_db.sh` job has been running.

8. Run `crontab delete_file.cron` to load the job.

**Note:** By default the cron job is started every day at 5 am which is four hours after the database cleanup procedure started.

The system property of `event.timeToLive` in the `system_property` table, controls how long event data is kept in the Main database. The default value is 30 days.

# 24 Load Balancer Configuration

This covers the following information:

- "Load Balancer Configuration"
- "Updating the Load Balancer for Multiple-Cluster Configurations" on page 369

## 24.1 Load Balancer Configuration

This section covers the following information:

- "URLs and Port Configurations"
- "Connection Rate Limit" on page 363
- "Timeout and Persistence" on page 366

### 24.1.1 URLs and Port Configurations

The load balancers must correctly identify the source IP address by placing it in the "x-forwarded-for" HTTP header. The following tables display the necessary configurations for the load balancers in the Operator Domain.

**Note:** Support for telephony servers has been deprecated.

Loadbalancer Status URLs and Ports

Element		URL
Health Check		<a href="https://[serverip]/ICHealthCheck/serverstatus">https://[serverip]/ICHealthCheck/serverstatus</a>
Application cluster (each node)	Subscriber Portal	<a href="https://[serverip]/subscriberPortal">https://[serverip]/subscriberPortal</a>
	Management Portal	<a href="https://[serverip]/managementPortal">https://[serverip]/managementPortal</a>
	Server status	<a href="https://[serverip]/managementPortal/serverstatus">https://[serverip]/managementPortal/serverstatus</a>
Telephony servers (each)		Check port 5038 (asterisk management port)

Loadbalancers Connections and Ports

Destination	Source	External Port	Internal Port	LB-Scheduling Method	LB Session Persistence	LB Persistence Timeout	URL
App Server VIP	Internet	TCP 443		Least Connections	https sticky	8 hours	
App Server VIP	Internet	TCP 5222		Least Connections	yes		XMPP, Dependent on the largest broadband heartbeat interval
App Server VIP	Internet	UDP 9091		Round Robin	no		Cellular traffic <b>(Converge only)</b>

Destination	Source	External Port	Internal Port	LB-Scheduling Method	LB Session Persistence	LB Persistence Timeout	URL
App Server VIP	Telephony/ Cell Server Provider Server X		TCP 8080	Round Robin	no		Callback from Telephony/ Cell Server Provider to-app VIP <b>(Converge only)</b>
App Server VIP	Cell IP Range		TCP 5222	Least Connections	yes		Telephony/ Cell Server Provider VPN <b>(Converge only)</b>
App Server VIP	Cell IP Range		UDP 9091	Round Robin	no		Telephony/ Cell Server Provider VPN <b>(Converge only)</b>
Telephony/ Cell Service Provider VIP	App Server X		TCP 5038	Round Robin	no		<b>(Converge only)</b>
Telephony/ Cell Servic Provider VIP	Backup Server		TCP 8080	Round Robin	no		Callback from Telephony/ Cell Server Provider to back-up server <b>(Converge only)</b>
Backup Server	Internet	TCP 5222					<b>(Converge only)</b>
Backup Server	Internet	UDP 9091					<b>(Converge only)</b>
Backup Server	Cell IP Range		TCP 5222	Least Connections			Cell Server Provider VPN <b>(Converge only)</b>
Backup Server	Cell IP Range		UDP 9091	Round Robin			Cell Server Provider VPN <b>(Converge only)</b>
Cell IP Address Home Domain: UDP 9091	App Server X						Cell Server Provider VPN <b>(Converge only)</b> This is server to touchscreen communication

## 24.1.2 Connection Rate Limit

The Connection Rate Limit should be set to 34.

### Adding connection rate limiting to a load balancer:

1. Go to Config Mode -> Service -> SLB -> Template -> Server Port.

Name	Health Monitor	Connection Limit	Connection Rate Limit
5222-connLimit	TCP-Port-5222-Check	34	
default	(default)		

2. Click **Add** to add server port template.
3. Fill in the following settings and click **OK**.

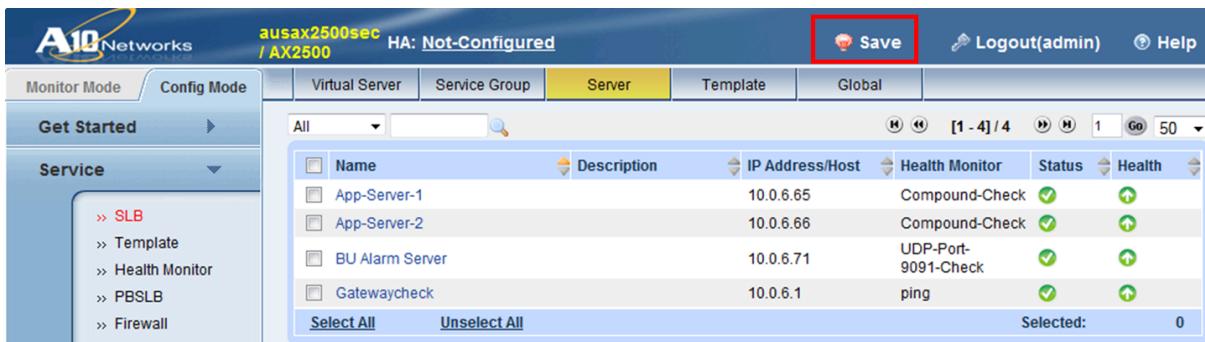
4. Go to **Config Mode** -> **Service** -> **SLB** -> **Server** and double-click **App-Server-1**.

Name	Description	IP Address/Host	Health Monitor	Status	Health
App-Server-1		10.0.6.65	Compound-Check	<span style="color: green;">✓</span>	<span style="color: green;">↑</span>
App-Server-2		10.0.6.66	Compound-Check	<span style="color: green;">✓</span>	<span style="color: green;">↑</span>
BU Alarm Server		10.0.6.71	UDP-Port-9091-Check	<span style="color: green;">✓</span>	<span style="color: green;">↑</span>
Gatewaycheck		10.0.6.1	ping	<span style="color: green;">✓</span>	<span style="color: green;">↑</span>

The details are displayed.

5. Select the check box next to port 5222.
6. Set the Server Port Template to the template you added.
7. Click **Update**.
8. Click **OK**.
9. Repeat steps 4 through 8 for the other Application servers in the cluster.

10. Click **Save** to have your configurations take effect.



The screenshot shows the A10 Networks Management Interface. The top navigation bar includes the A10 Networks logo, the device name "ausax2500sec / AX2500", and status indicators for HA (Not Configured). The main menu has "Monitor Mode" and "Config Mode" tabs, with "Config Mode" selected. Under "Service", the "SLB" option is highlighted. The main content area displays a table of servers with columns: Name, Description, IP Address/Host, Health Monitor, Status, and Health. The table contains four entries: App-Server-1, App-Server-2, BU Alarm Server, and Gatewaycheck. All entries show green checkmarks in the Status and Health columns. The "Save" button in the top right corner is highlighted with a red box.

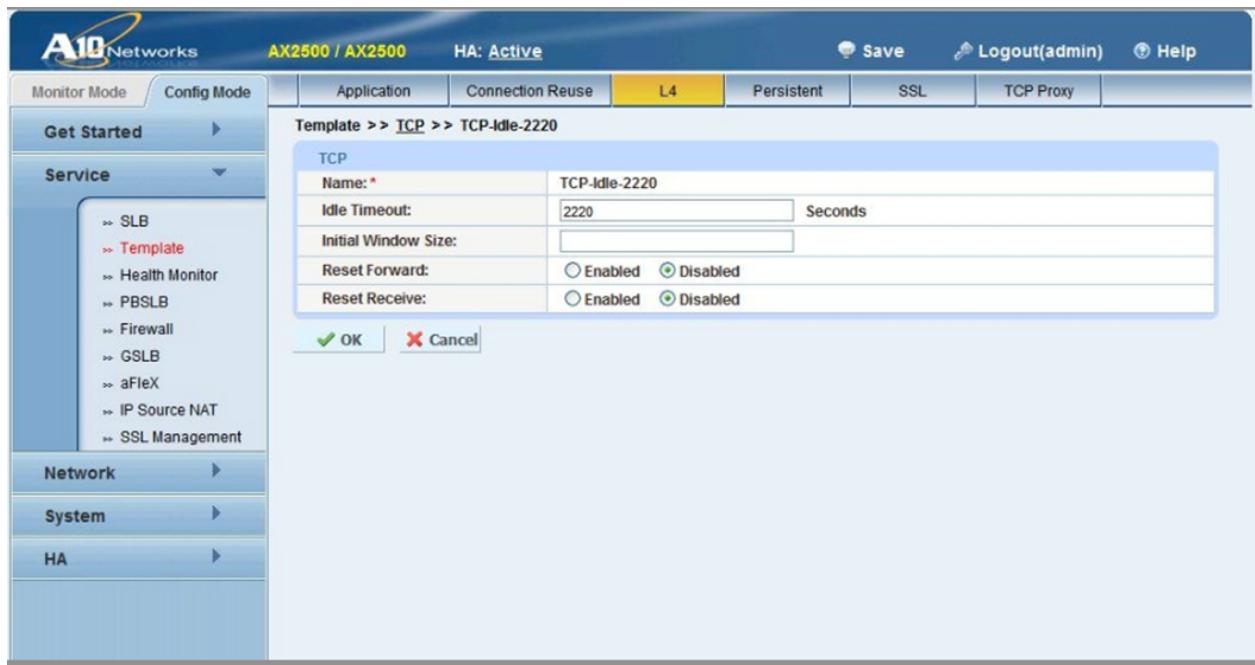
Name	Description	IP Address/Host	Health Monitor	Status	Health
App-Server-1		10.0.6.65	Compound-Check	Green	Green
App-Server-2		10.0.6.66	Compound-Check	Green	Green
BU Alarm Server		10.0.6.71	UDP-Port-9091-Check	Green	Green
Gatewaycheck		10.0.6.1	ping	Green	Green

### 24.1.3 Timeout and Persistence

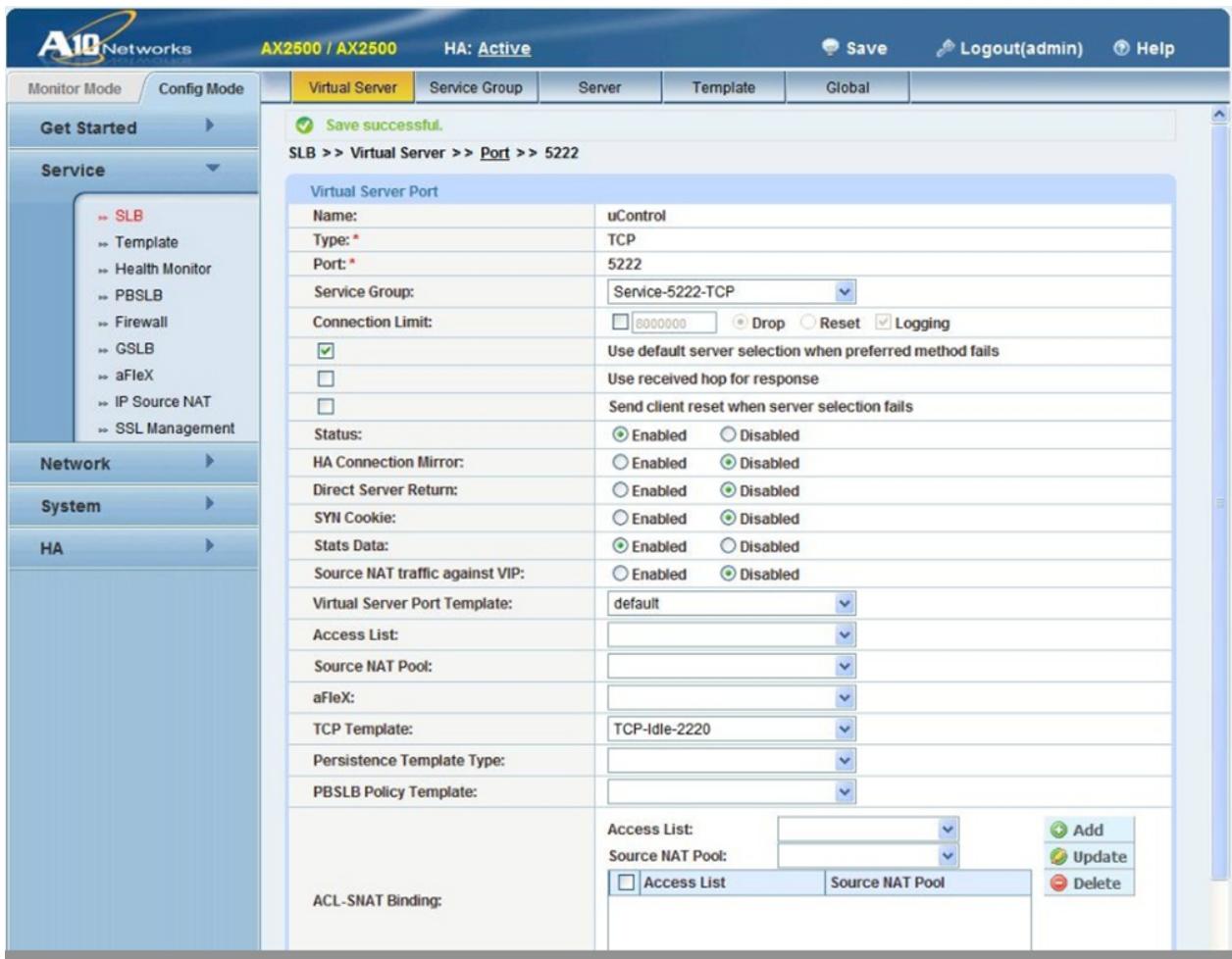
See "Icontrol Connectivity Protocols" on page 100 explanations of the concepts related to these settings.

#### 24.1.3.1 TCP Session Timeout Needs to be Larger than the Largest Broadband Heartbeat Interval

The largest broadband heartbeat interval is 1800 seconds (that is, 30 minutes), we recommend a setting of 2220 for the TCP Session Timeout. In the following image, the Template for a TCP Session Timeout is being created and set to 2220.



In the following image, the Session Timeout template is selected in the Virtual Server Port 5222.



Set the TCP Template selection to the 2220 Session Timeout. In the examples above, the name of the template is `TCP-Idle_2220`.

Once you have made these changes the configuration needs to be saved in order to push that setting to the load balancer config file for use by the virtual server.

### 24.1.3.2 TCP XMPP Persistence Enabled with Persistence Timer Larger than the Largest Broadband Heartbeat Interval

The screenshot shows the A10 Networks AX2500 / AX5000 configuration interface. The top navigation bar includes the A10 Networks logo, the model name "AX2500 / AX5000", the status "HA: Active", and links for "Save", "Logout(admin)", and "Help". The left sidebar has tabs for "Monitor Mode" and "Config Mode", with "Config Mode" selected. Under "Service", the "Template" option is chosen, showing sub-options like SLB, Template, Health Monitor, PBSLB, Firewall, GSLB, aFlex, IP Source NAT, and SSL Management. The main content area displays the "Source IP Persistence" configuration for a template named "5222-persistence". The configuration fields are as follows:

Source IP Persistence	
Name: *	5222-persistence
Match Type:	Port
Timeout:	37 Minutes
Don't Honor Conn Rules:	<input type="checkbox"/>
Netmask:	255.255.255.255

At the bottom of the configuration panel are two buttons: "OK" (with a green checkmark icon) and "Cancel" (with a red X icon).

## 24.2 Updating the Load Balancer for Multiple-Cluster Configurations

This section describes the new load balancer configurations required to modify a single, all-in-one deployment to a multiple-cluster deployment.

**Note:** Single-cluster server configuration is no longer supported as of the Oahu release.

**Note:** Before updating the load balancer, make a backup of the current configuration.

This procedure was tested using SoftAX / AX software version: 2.7.0-P2 (build: 53)

The setup assumes the following server distribution:

Server Distribution	
Type	IP
cpe_node1-x	<cpenode IP>
portal_node1-x	<portal_node IP>
media_node1-x	<media_node IP>

For simplicity, each node is listed as a single logical node. However, your environment may have more than one of each type of node listed.

The general steps for updating the load balancer are as follows:

1. [Update the serverstatus Health Monitor](#) (see page 370).
2. [Update the Source IP Persistence Template](#) (see page 370).
3. Create new service groups (see page 371).
4. Create an HTTP template for app switching (see page 375).
5. Update the virtual server port settings.
6. Restart each managed server.

### 24.2.1 Update the serverstatus Health Monitor

**Path:** Config Mode > Service > Health Monitor > Health Monitor > serverstatus

Make the following changes to the serverstatus health monitor.

serverstatus Health Monitor

Parameter	Value
URL	GET /ICHealthCheck/serverstatus
User	Valid Management Portal user name
Password	Password for specified user

### 24.2.2 Update the Source IP Persistence Template

**Path:** Config Mode > Service > Template > Persistent > Source IP Persistence > SourceIPPersistenceTemplate

Make the following change to the SourceIPPersistenceTemplate.

serverstatus Health Monitor

Parameter	Value
Match Type	Service Group

### 24.2.3 Create New Service Groups

**Path:** Config Mode > Service > SLB > Service Group

The existing service groups that send traffic to all-in-one nodes can be left as-is to simplify the rollback procedure. Do not delete the existing service groups until the configuration is finalized and tested.

**Note:** Single-cluster server configuration is no longer supported as of the Oahu release.

The following service groups are required for multiple-cluster configurations:

- ❑ CPEAppInterface
- ❑ CPEBroadbandConnector (see page 372)
- ❑ CPECellularConnector (see page 372)
- ❑ PortalAppInterface (see page 374)
- ❑ MediaAppInterface (see page 373)

**Note:** When modifying a single all-in-one cluster to a multiple-cluster, the service groups that send traffic to the nodes the existing service groups can be left as-is to simplify the rollback procedure.

**IMPORTANT:** Do not delete the existing service groups until the configuration is finalized and tested.

**Note:** Single-cluster server configuration is no longer supported as of the Oahu release.

#### 24.2.3.1 CPEAppInterface

**Note:** Be sure to create a separate entry for all CPE nodes.

Tab	Service Group Parameter	Value
Service Group	Type: TCP	TCP
	Algorithm	Service Least Connection
	Health Monitor	serverstatus
	Min Active Members	false
	Send client reset when server selection fails	false
	Send log information on backup server events	false
	Stats Data	Enabled
	Extended Stats	Disabled
Server	IPv4/IPv6	IPv4
	Server	cpe_node<x>
	Port	80
	Server Port Template (SPT)	default
	Priority	1

### 24.2.3.2 CPEBroadbandConnector

**Note:** Be sure to create a separate entry for all CPE nodes.

Tab	Service Group Parameter	Value
Service Group	Type: TCP	TCP
	Algorithm	Least Connection
	Health Monitor	TCPport5222open
	Min Active Members	false
	Send client reset when server selection fails	true
	Send log information on backup server events	false
	Stats Data	Enabled
	Extended Stats	Disabled
Server	IPv4/IPv6	IPv4
	Server	cpe_node<x>
	Port	5222
	Server Port Template (SPT)	default
	Priority	1

### 24.2.3.3 CPECellularConnector

**Note:** Be sure to create a separate entry for all CPE nodes.

Tab	Parameter	Value
Service Group	Type: TCP	UDP
	Algorithm	Round Robin
	Health Monitor	<empty>
	Min Active Members	false
	Send log information on backup server events	false
	Stats Data	Enabled
	Extended Stats	Disabled
Server	IPv4/IPv6	IPv4
	Server	cpe_node<x>
	Port	9091
	Server Port Template (SPT)	default
	Priority	1

#### 24.2.3.4 MediaAppInterface

**Note:** Be sure to create a separate entry for all media nodes.

Tab	Service Group Parameter	Value
Service Group	Type: TCP	TCP
	Algorithm	Service Least Connection
	Health Monitor	serverstatus
	Min Active Members	false
	Send client reset when server selection fails	false
	Send log information on backup server events	false
	Stats Data	Enabled
	Extended Stats	Disabled
Server	IPv4/IPv6	IPv4
	Server	media_node<x>
	Port	80
	Server Port Template (SPT)	default
	Priority	1

### 24.2.3.5 PortalAppInterface

**Note:** Create a separate entry for all portal nodes.

Tab	Service Group Parameter	Value
Service Group	Type: TCP	TCP
	Algorithm	Service Least Connection
	Health Monitor	serverstatus
	Min Active Members	false
	Send client reset when server selection fails	false
	Send log information on backup server events	false
	Stats Data	Enabled
	Extended Stats	Disabled
Server	IPv4/IPv6	IPv4
	Server	portal_node<x>
	Port	80
	Server Port Template (SPT)	default
	Priority	1

## 24.2.4 Create an App Switching HTTP Template

**Path:** Config Mode > Service > Template > Application > HTTP

**Note:** The Failed Server Selection parameter does not exist in AX 2.6.9 software.

### 24.2.4.1 URL Switching Section

This section selects a service group based on the URL string requested by the client. The selection overrides the service group configured on the virtual port.

The *URL* parameter specifies the URL string to match on. If the URL-string does not match, the service group configured on the virtual port is used.

The *Service group* parameter specifies which Service group to use when there is a match.

The *Match Type* is performed using the following match filters:

- Starts With** Matches only if the URL starts with the value in the URL field.  
If you use this option with URL switching, use a slash in front of the URL string.  
For example: /urlexample
- Contains** Matches if the value in the URL field appears anywhere within the URL.
- Ends With** Matches only if the URL ends with the value in the URL field.
- Equals** Matches only if the URL equals the value in the URL field.

The match options are always applied in the order listed above, regardless of the order in which they appear in the configuration. The service group for the first match is used.

If a URL matches on more than one match filter of the same type, the most specific match is used.

Each URL matching pattern can be up to 64 bytes long.

**Note:** If you plan to also use source IP persistence or cookie persistence, you must enable the service-group option in the source IP persistence or cookie persistence template.

### 24.2.4.2 App Switching Section

AppInterface\_url\_switching Configuration

Section	Parameter	Value
HTTP	Failover URL	
	String Transaction Switching	Disabled
	Client IP Header Insert	unchecked
	Retry HTTP Request	unchecked
	Log Retry	unchecked
	Terminate HTTP 1.1 client when request has Connection: close	unchecked
	Failed Server Selection:	504 Gateway Timeout

Section	Parameter	.	Value
App Switching	By		URL
	URL Switching		
	URL	Match Type	Service Group
	/touchScreen	Starts With	CPEAppInterface
	/ICHealthCheck	Starts With	PortalAppInterface
	/integration	Starts With	PortalAppInterface
	/mp	Starts With	PortalAppInterface
	/managementPortal	Starts With	PortalAppInterface
	/sp	Starts With	PortalAppInterface
	/subscriberPortal	Starts With	PortalAppInterface
	/rest/	Starts With	PortalAppInterface
	/restServer/	Starts With	PortalAppInterface
	/oauth	Starts With	PortalAppInterface
	/widgetStore	Starts With	MediaAppInterface
	/fileUpload	Starts With	MediaAppInterface
	//fileUpload	Starts With	MediaAppInterface
	/cameraProxy	Starts With	MediaAppInterface

## 25 Devices Details

This section includes general but important information about devices that can be paired to the Icontrol platforms.

### 25.1 Default Device Settings

Sensor Types	Zone Function Options	
Door/Window	Entry/Exit	[Default]
	Perimeter	
	24-Hour Inform	
	Trouble Day/Alarm Night	
	Silent 24-Hour	
	Audible	
Glassbreak	Perimeter	[Default]
	24-Hour Inform	
Motion	Interior Follower	[Default]
	Interior with Delay	
	Interior Delay Arm Night	
	Interior Follower Arm Night	
	24-Hour Inform	
Water	Audible 24-Hour	[Default]
	24-Hour Inform	
Carbon Monoxide (CO2)	Audible 24-Hour	[Default]
Smoke	24-Hour Fire	[Default]

## 25.2 Motion-Capable Cameras

Certified motion-capable cameras are now supported on both the Converge and Touchstone platforms. A subscriber can create rules to capture video/images or any other action that would otherwise require a separate motion sensor.

A camera detects motion events based on its *High*, *Medium*, or *Low* motion sensitivity setting. These are intentionally non-technical designations that are intended to be easily comprehensible to the subscribers. The default setting is *Low*. If they set their cameras to a higher setting and find that they are detecting irrelevant motion, they can lower it.

The camera will not report another motion event for the period configured in the `motion.events.blackout.period` server property (default is 3 minutes). If another motion event is reported immediately after the blackout period, a new blackout period will begin. Changes made to motion sensitivity take effect immediately if the camera is not within the blackout period. If the setting was changed during the blackout period, the change will take effect once the blackout period expires. See "["motion.events.blackout.period" on page 277](#)" for more information.

Motion-capable cameras use a special icons to represent motion/still events in the History and other instances in the user interface.

	Camera Motion	The camera has detected a motion event.
	Still	It has been 3 minutes (default) since the camera has detected a motion event. It is now able to detect another motion event.

When a camera determines that a motion event has occurred (based on its Low, Medium, or High setting), it simultaneously broadcasts the event to the following system entities:

- Rules** To determine if the event has triggered a rule
- History** To display the camera-motion event in the touchscreen History tab (Converge only)
- Comm Mgr** To report the event server cluster where it is logged in History and in RCA
- Cameras App** To display a camera motion notification is displayed on the camera image.

### Converge Only

The following limitations for motion-capable cameras are applicable to Converge systems:

- A motion-capable camera is a non-security device. An alarm can never be initiate by this type of device. It operates under the same restrictions as a motion sensor that is set to *24-Hour Inform* zone functionality. See "["Zone Function Behaviors" on page 86](#)" for details on 24-Hour Inform.
- A rule can arm or disarm the system based on a motion or still event/non-event from a motion-capable camera.

### 25.2.1 Device Descriptor List Controls

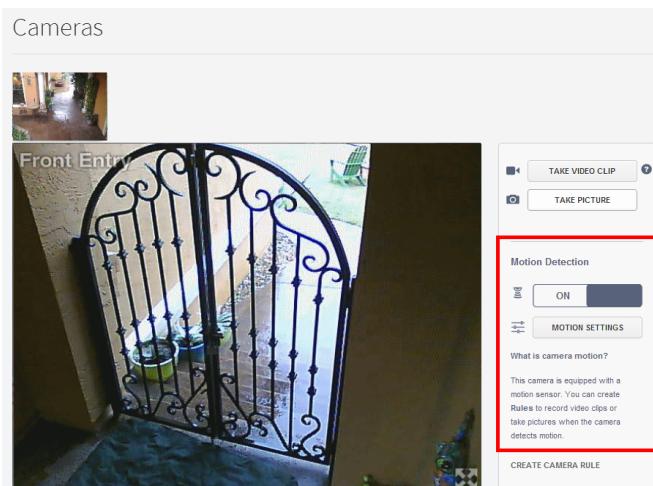
The *High*, *Medium*, or *Low* motion sensitivity settings are determined by an algorithm that uses the `<sensitivityLevel>` values and the `<detectionThreshold>` values in the camera model's section of the Device Descriptor List (DDL). Each manufacturer might use these values differently.

Motion-capability can be toggled off and on from the DDL. The DDL element `<motion><enabled>` determines whether motion-detection is enabled for each camera model.

```
<motion>
  <enabled>false</enabled>
</motion>
```

This value is *true* by default unless it is modified for customer brands. When a motion-capable camera is set to *false* the camera is treated as a non-motion-capable camera in the touchscreen and Subscriber Portal.

- ❑ In the Touchscreen Settings app, the Motion Sensitivity option is not available when configuring the camera.
- ❑ In the Subscriber Portal, the Motion Detection/Settings panel is not available for the camera.



See your Icontrol representative for assistance in editing your Device Descriptor Lists to modify the motion capability of your cameras.

## 26 Interface Branding

This section provides the details for branding the interfaces in the iControl system. Currently the following interfaces are covered:

- Touchscreen
- Subscriber Portal
- Interface Branding

### 26.1 Touchscreen

#### CONVERGE ONLY

The touchscreen allows for several branding opportunities, in terms of logos, icons and apps.

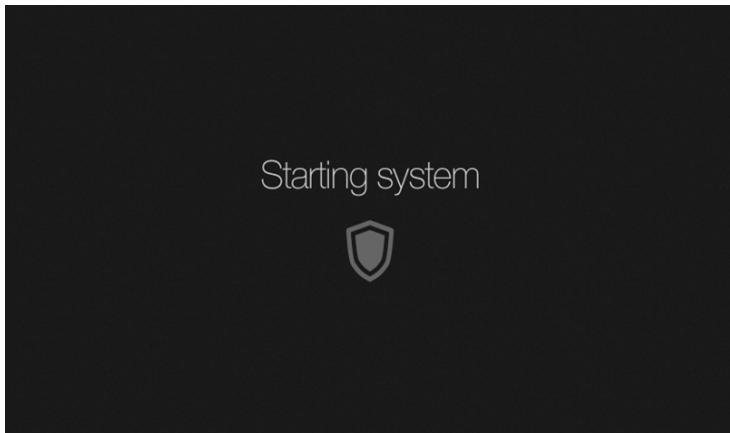
- Background
- Custom App Icons
- Custom Apps (not covered here, but customers own the whole app experience)

The touchscreen display is 800x480. The header and footer graphics are both right-justified. The header and footer appear at the same time on the home screen, but the header can be obscured by notification messages that appear if something is out of the ordinary. The upper left is reserved for system status, and the lower left has the date and time.

After you construct your logo or icon, send it to iControl Networks to be incorporated into your touchscreen build.

#### 26.1.1 Boot-Up

When the touchscreen boots up, it displays the following initial screen. This is the same across all customer builds and is not configurable.



Next, by default, the touchscreen displays the icontrol logo on a black field. This screen is configurable.



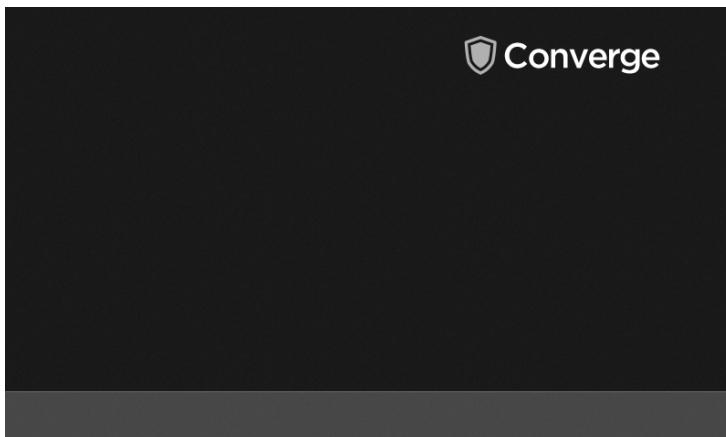
#### **26.1.1.1 Image Requirements**

Attribute	Description	
Dimensions	800px wide x 100px tall	
Size	10 KB max	
Format	PNG, non-transparent, compressed, 8-bit	
Color	Background	Black, #000000
	Glyph	White, #FFFFFF

#### **26.1.2 Main Screen**

##### **26.1.2.1 Background**

The Main screen background is a single, non-transparent, PNG image: size 800x480.



##### **26.1.2.2 Header Elements**

Elements in the header include the Security and Trouble headers.

Maximumsize: 300 px wide by 60 px tall.

Recommended size: 200 px wide by 50 px tall.

Placement: Top margin ~15px, right margin ~10 px.

### 26.1.2.3 Footer Elements

Elements in the footer might include a time and date stamp.

Maximumsize: 300 px wide by 47 px tall.

Recommended size: 200 px wide by 30 px tall.

Placement: Top margin ~410 px, right margin ~10 px.

### 26.1.2.4 General Recommendations

If possible, use insert your brand either in the header or footer. Not both.

Logos require bright colors, so they pop on the darker background. If necessary, white-fill your logo.

Transparent background is essential.

### 26.1.3 Custom App Icons



Use the iControl Networks Photoshop template to create an icon.

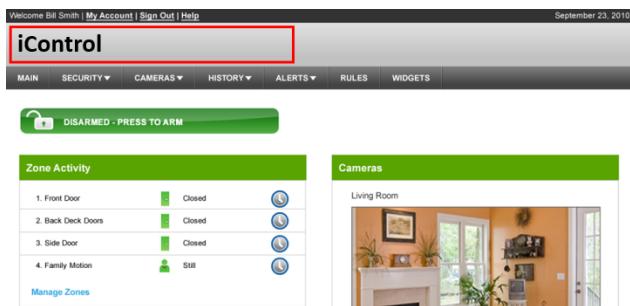
Attribute	Description		
Size	100x100px		
Format	PNG or SVG		
Transparencym	Background	50%	<b>Note:</b> The transparency allows the icons to be produced with rounded corners.
	Glyph	90%	

## 26.2 Subscriber Portal

The Subscriber Portal allows for the most branding opportunities, in terms of logos, fonts and color. However, they vary in the amount of effort required.

Attribute	Description
Header Logo	Light
Content	
Fonts	
Background	
Menus	Medium
Buttons	
Layout	Heavy

### 26.2.1 Header Logo



The header logo must be 32-bit with a transparent background.

Attribute	Description
Size	Up to 880 x 93
Resolution	72 DPI
Format	PNG

## 26.2.2 Content, Fonts, and Background

The screenshot shows the iControl interface. At the top, there's a navigation bar with links: Welcome Bill Smith | My Account | Sign Out | Help, and the date September 23, 2010. Below the navigation is a main header "iControl". The interface is divided into sections: "Zone Activity" (listing Front Door, Back Deck Doors, Side Door, and Family Motion status), "Cameras" (showing a thumbnail of a living room), and a "DISARMED - PRESS TO ARM" button. A dashed orange box highlights the "Zone Activity" section.

Most UI elements are managed with a CSS file.

Attribute	Description
Content header color	#313131
Font	Xfinity Sans, Light 35px
Background	White or #FFFFFF

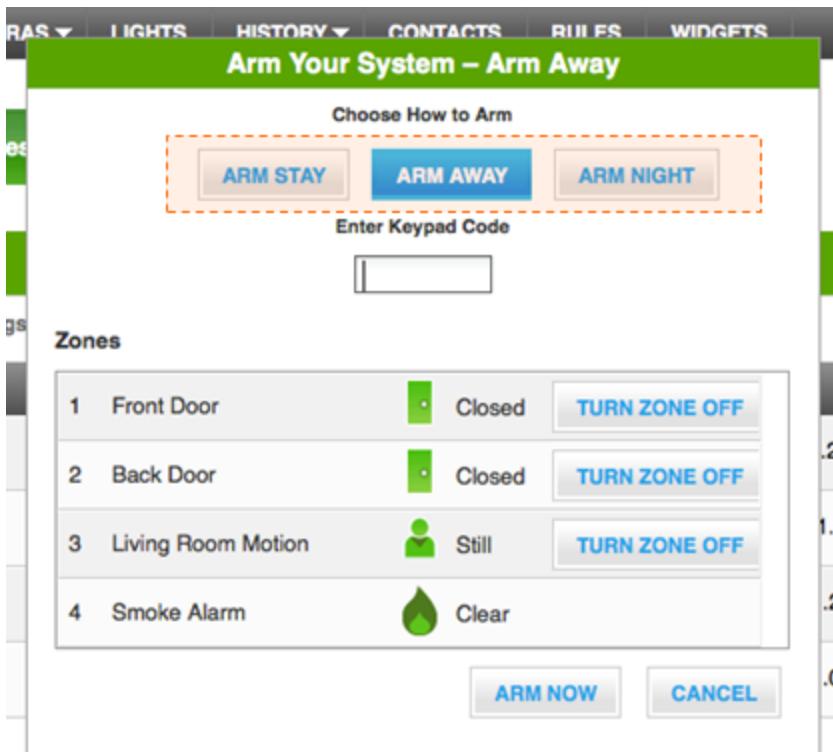
## 26.2.3 Menus

The screenshot shows the iControl interface with a menu toolbar highlighted by a dashed orange box. A blue arrow points to the left edge of the menu toolbar. The menu items include MAIN, SECURITY, CAMERAS, HISTORY, ALERTS, RULES, and WIDGETS.

Menus are managed using a CSS, and override ExtJS. Other image and font changes might be required other than those described below

Attribute	Description
#menutoolbar	.x-toolbar, .x-menu

## 26.2.4 Buttons



Buttons are managed with a CSS file and override ExtJS

To modify them, clone and modify the button tile at `/images/button/button.gif`. Other font color changes might be required.

## 26.2.5 Layout

Layout changes are possible; however, moving UI elements around affects the base UI that all customers rely on. Generally, this requires a custom code set or agreement by the Product Steering Committee.

## 27 Glossary

Term	Definition
Alarm Cancel Period	The after the Alarm Transmission Delay period has completed, the user has about 5 minutes to enter their key code to cancel the alarm. Even though the central station received the relevant CID and other information and might have started to call the Emergency Contact list, they will receive notification that the alarm was canceled. The Cancel window ends when the alarm resets.
Panic Alarm	An alarm caused by pressing a Panic button on a key pad or key fob or by initiating a Police, Medical, or Fire emergency alarm from the touchscreen.
System Trouble Event	A reported trouble from the touchscreen as opposed to a device.
Transmission Delay	<p>If a valid keypad code is not entered by the end of the Entry Delay period, an alarm sounds. From the time an alarm sounds (or starts silently), for most reasons, the user has 30 seconds (default) to enter a valid keypad code to disarm the system and prevent an alarm being sent to the central monitoring station. This is called the Alarm Transmission delay or the Abort Window.</p> <p>The Alarm Transmission Delay is a required period that prevents a report to the central station if an alarm was triggered innocently. The Transmission Delay period is configurable from the touchscreen.</p> <p>Certain types of zone functions issue alarms without a Transmission Delay period.</p>
Zone Alarm	An alarm caused by an action or inaction of a device .
Zone Event	A non-alarm event reported from a security device such as a door opening or closing or motion detector detecting motion or clearing.