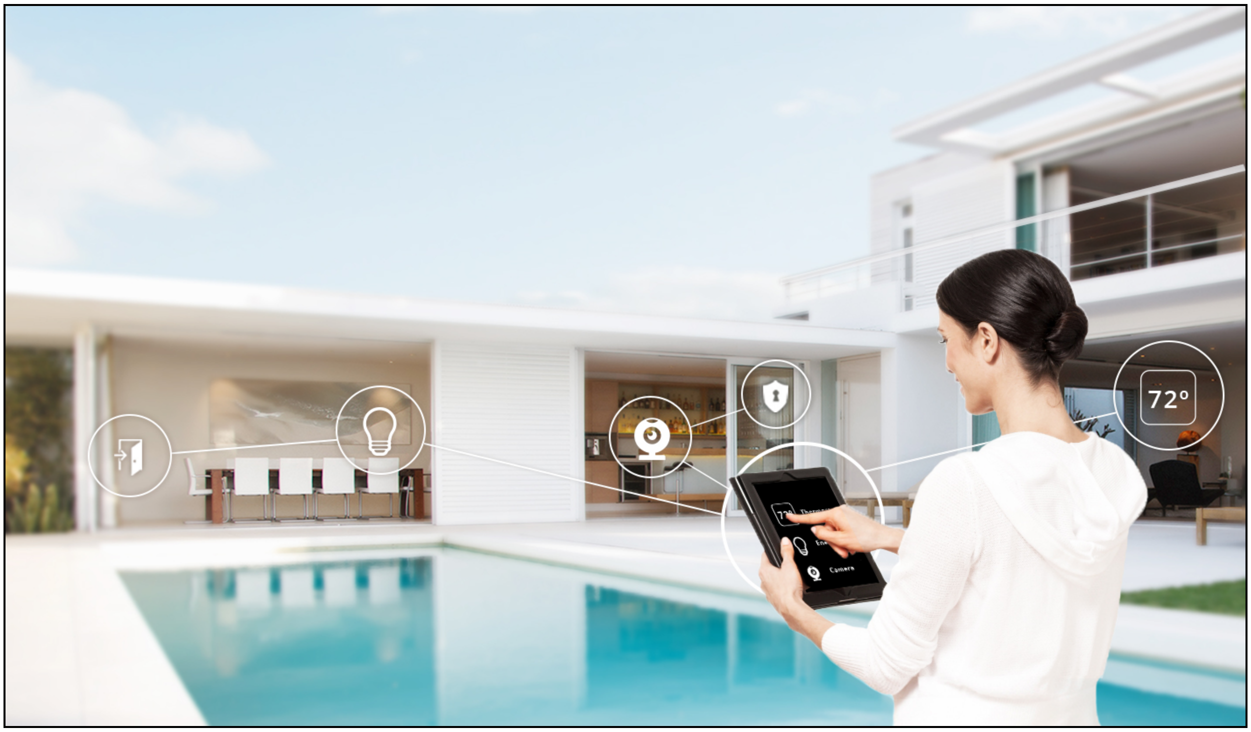
icontrol®
NETWORKS

Converge System Architecture Guide

7.3 Quadra



Document Information

Release version: 7.3 Quadra
Document name: Converge System Architecture Guide
Build date: 7/7/2016

Contents

Revision History

Release	Revisions
7.3 Quadra v2	Removed specific database sizing information from "Application Database" on page 28 and instead provided a link to the *Capacity Planning* spreadsheet on the Customer Support Knowledge Base.
7.3 Quadra v1	Added "Cloud Automation and Control" on page 28 In "Home Domain " on page 13, added reference to the "Overview" section in *Home Security System Installation Guide* for more information about supported ZigBee devices Updated the list of event types sent over cellular in Cellular Levels of Service on page 17
7.2 Padre	Deleted diagram of Cluster Location Service (CLS) system from "Cluster Location Service" on page 27. This diagram has moved to *Cluster Location Service Installation Guide*. Updated "SAN Shared Storage" on page 28 as follows: ❑ Deleted outdated "Hard Drive and Partition Sizes" section ❑ Added link to *Architecture Requirements* document Deleted outdated "Connectivity" section from "Application Database" on page 28 Deleted outdated "Connectivity" section and note from "Backup Alarm Database" on page 29 Updated "Database Replication" on page 29 as follows: ❑ Deleted outdated content ❑ Added reference to *Converge GoldenGate Installation and Setup* document Deleted outdated firmware download procedure from "Bundle Server" on page 30
7.1 Oahu	Removed references to single-cluster server configuration as it is no longer supported as of the Oahu release.
7.0 Nantucket	Added information about the Cluster Location Service. See "Cluster Location Service" on page 27. Corrected inaccuracies in the Logical Architecture diagrams.
6.3 Maui	Removed references to the Relay Server as an *optional* component. Moved Logical Camera-Servers-Relay-Server diagrams to the System Operations Guide, Message Sequence Diagram section, Camera Operations subsection.
6.2 Lanai	System was load and stress-tested for up to 750,000 subscribers on the multiple cluster configuration.

Release	Revisions
6.1 Kodiak	With Telephony Support deprecated, references to the Telephony servers were removed. The description of the Subscriber Portal clarifies that HTTPs is required. See "Subscriber Capacity" on page 23. "Cellular Levels of Service" on page 17 has the following updates and corrections: ❑ "Emails/SMS for rules (no images)" is available on Enhanced level of service only. ❑ The update camera portal command is not available under any cellular level of service.
6.0 Jamaica	Various small edits. SAN Shared Storage section (page 28) moved to it's own separate Heading 2 subsection. The section "Home Domain " on page 13 has had a paragraph added that refers to the Device Descriptor List.

1 Introduction

The purpose of this document is to:

- Describe the system architecture of the Icontrol common application server
- Describe the Converge Security, Monitoring, and Automation (SMA) platform founded on the touchscreen customer premise equipment (CPE)
- Provide a base server architecture needed to support up to 750,000 active, deployed subscribers (multiple-cluster)

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

Note: The multiple-cluster configuration has been Load & Stress tested for up to 750,000 subscribers.

Within the server infrastructure, messaging, and UI, the term *touchscreen* refers to the Converge CPE.

The intended audience for this document includes IT managers and network architects who need to understand the overall architecture within the Operator Domain server environment and how it can be deployed to properly communicate with subscriber homes.

This document contains the following information:

- Descriptions of the various functional groupings within the architecture
- Detailed descriptions of specific architectural components for each platform
- Reference production server architecture in multiple-cluster configurations

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

1.1 System Design Goals

The common server platforms are designed to enable large-scale deployments across the operator network infrastructure. It is designed such that the platform:

- Provides an extensible architecture to allow for the deployment of new services/features without impacting the underlying infrastructure
- Uses existing standards, platforms, and open protocols when possible
- Complies with all UL, FCC and PTCRB standards
- Has an optimized service activation flow for the CPE devices

The system design goals also include the following high-level elements:

- System Security
- Scalability

- Fault Tolerance
- Provisioning and Management
- BSS/OSS Integration

1.2 System Security

The following are system security design goals:

- Support confidentiality, authentication, integrity, and access control mechanisms
- Protect the network from various denial-of-service, network-disruption, and theft-of-service attacks
- Protect the Home Domain from denial-of-service attacks, security vulnerabilities, and unauthorized access
- Provide mechanisms for CPE authentication, secure provisioning, secure signaling, secure media, and secure software download

See the "System Security Against Web Application Attacks" section in *System Operations Guide* for more information about system security design.

1.3 Scalability

The common server infrastructure is designed to scale linearly and implement the following design goals:

- Provide an asynchronous architecture
- Provide a stateless architecture
- Use clustering technologies that enable seamlessly adding physical servers to a server cluster to increase capacity
- Provide for physical separation of platform functionality to enable multiple combinations of server clustering and load balancing

1.4 Fault Tolerance

Fault-tolerant means the system can operate in the presence of hardware and system component failures. A single component failure will not cause a system or service interruption because an alternate component will take over automatically and transparently to continue the overall function of the system (no downtime).

High Availability (HA) is a categorization of computer systems where availability is a key metric of applications on these systems. The Icontrol platforms fall into this category. Users expect and demand a high probability that alarms (if applicable) and non-critical security system events are processed when they happen, regardless of whether a system component has failed.

Common server fault tolerance design goals:

- Provide a mechanism on the CPE to ensure that a reboot is not required if a driver or a process fails.
- Provide mechanisms on the touchscreen to protect against unexpected touchscreen app behavior.
- Use server clustering technologies that enable automatic swapping of a failed server's workload to other servers in the cluster with no apparent downtime.
- Provide robust server monitoring hooks that can be used by IT tools to determine server health.

1.5 Provisioning and Management

Common server provisioning and management design goals:

- Provide guided activation/provisioning flows that enable Service Provider representatives to install the system in subscriber homes
- Provide secure firmware updates for CPEs
- Provide back-office management/troubleshooting interfaces for CPEs and paired devices

1.6 BSS/OSS Integration

The BSS/OSS integration design goals are:

- Provide a standards-based integration framework
- Support both synchronous and asynchronous communications
- Provide a pluggable architecture to support multiple integration technologies

2 Understanding the Converge Architecture

The Converge platform enables service providers to deploy the touchscreen and servers to provide their customers with the following services:

Security – Protect lives and property through professional monitoring, notifying first responders (e.g., fire, police, and medical), and providing emergency alerts to authorized individuals like home occupants. For example, fire and smoke sensors alert monitoring agencies who can notify and provide critical information to local emergency personnel.

Monitoring – Monitor the status and activity in the home so that a user can be made aware of any desired state changes. For example, when a motion sensor detects motion, real-time alerts and associated data, such as video or photo clips, can be sent to the user.

Automation – Automate and remotely control lifestyle conveniences such as lighting, heating, cooling, and appliances. For example, a user can remotely use a mobile or web portal to verify and control conditions such as lighting or temperature in the user's home.

2.1 Logical Domain Architecture

The logical architecture consists of a set of domains and functional entities within those domains. This section provides an overview of the logical domains, including a description of the main functional groupings (e.g., Home Domain, Operator Domain) and logical entities (e.g., touchscreen, main server) within those groupings.

The Converge system is divided into the following logical domains:

- **Home Domain**

  The Home Domain is the collection of security and environmental devices (within the subscriber premise) as well as the methods the subscriber uses to monitor and manage the subscriber's system. Devices communicate with the Operator Domain through the touchscreen and security router. The touchscreen is the controlling component, often referred to as a CPE device. The Home Domain system can be managed directly from the touchscreen, web portal, or mobile devices. See "Home Domain " on page 13 for more information.

- **Access Domain**

  The Access Domain consists of the access network elements that allow for communication between the Home Domain (via the touchscreen and security router) and the Operator Domain. The Access domain consists of the broadband and cellular channels. See "Access Domain Communication Channels and Connectivity Protocols" on page 14 for detailed information about the Access Domain channels.

- **Operator Domain**

  The Operator Domain is the logical collection of application servers and other systems in the operator's network that provide end user interfaces, such as the REST API and the Subscriber Portal, and that configure, manage, and control elements within the Home Domain.

  The Common Core application servers support a multiple-cluster configuration and are divided into three WebLogic clusters managed by a single WebLogic Admin server.

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

  In the default configuration, the Operator Domain consists of the following elements:

  - Application Segment
  - Database Segment
  - Relay Server
  - Event Bus
  - Bundle Server
  - BOSS/OSS Systems

  Not all of these elements are required. For example, the system does not require an Event Bus.

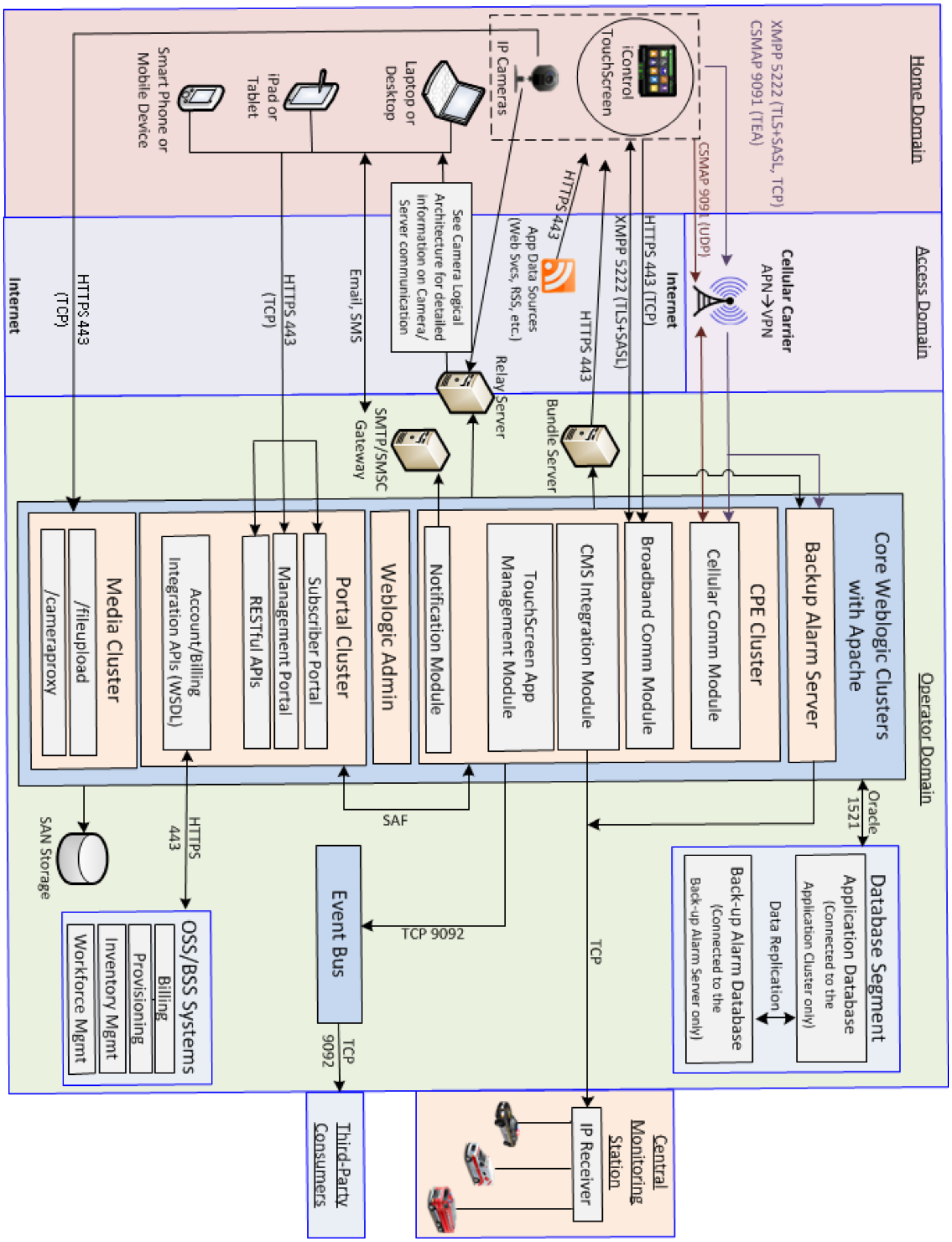
  In addition, Cluster Location Service (CLS) is an optional component that enables multiple server clusters to operate in parallel and increase scalability. When CLS is implemented, CPEs and remote clients do not need to be configured to connect to a single server cluster.

- **Central Monitoring Station (CMS) Domain**

  The CMS Domain processes critical alarms from elements in the Operator Domain related to verification and to alerting emergency personnel.

2.1.1 Multiple-Cluster Logical Architecture

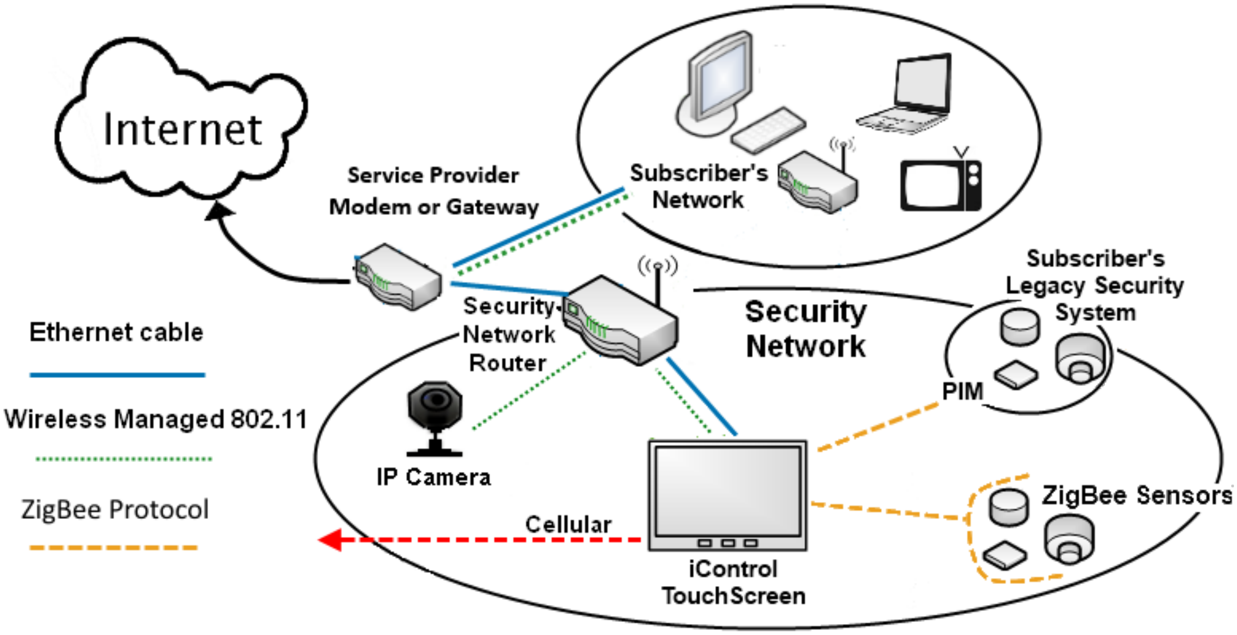
The following figure shows the logical domains and functional entities within each domain.



Logical Architecture for Multiple-Cluster Configuration

2.1.2 Home Domain

The Converge home security network communicates with the service provider modem through a dedicated security router. The touchscreen CPE device maintains constant communication with the Operator Domain through the broadband and cellular channels. In addition to ZigBee sensors, the touchscreen can integrate most legacy wired security systems into its network through a Panel Interface Module (PIM).



Converge Home Security Network

ZigBee devices consist of anything that communicates with the touchscreen CPE over ZigBee protocol, such as door/window sensors, light/appliance modules, thermostats, panel interface modules, keypads, key fobs, siren repeaters, and smoke detectors. For more information about supported ZigBee devices, see the "Overview" section in *Home Security System Installation Guide*.

Subscriber devices that can be added to the Home Domain through the CPE are managed by the Device Descriptor List (DDL). Devices must be included on this list to be integrated with the Icontrol system. These devices can be selectively excluded from integrating with the Icontrol system by the subscriber's tier or package. See *Management Portal Guide* for information about how to manage the Device Descriptor List, tiers, and packages.

See the "Icontrol Connectivity Protocols" and "CPE Statistics Collection and Reporting" sections in *System Operations Guide* for information about CPE connectivity to the router and to the broadband/cellular channels.

3 Access Domain Communication Channels and Connectivity Protocols

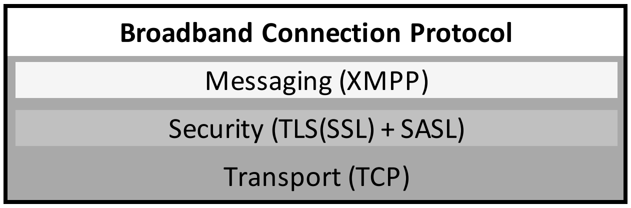
The Access Domain contains the channels used for communication between the Home Domain and the Operator Domain. The following channels are used:

- Broadband
- Cellular

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

3.1 Broadband Channel

The broadband channel is the primary communication channel between the Home Domain and the Operator Domain. The broadband communication module handles non-alarm and alarm events, broadband heartbeat, and command traffic over the broadband channel between the Home Domain and the Operator Domain.



Broadband Connection Protocol

Messaging (XMPP)

Security (TLS(SSL) + SASL)

Transport (TCP)

Broadband Protocol Stack

For multiple-cluster configurations, the broadband module is located in the CPE cluster.

There is an always-on persistent TCP socket connection maintained between each touchscreen CPE device and the Operator Domain. *Extensible Messaging and Presence Protocol* (XMPP) is an XML-based protocol on top of the CPE connection used for the communication. The communication is encrypted using *Transport Layer Security* (TLS) 1.0/*Secure Sockets Layer* (SSL) 3.1, and *Simple Authentication and Security Layer* (SASL) is used for authentication. The default TCP port is 5222. The port is configurable during deployment.

The always-on socket connection enables near real-time communication between each CPE device and the Operator Domain. For example, if a subscriber trips a sensor while viewing the Subscriber Portal, the sensor fault is reflected immediately in the Subscriber Portal user interface. In this scenario, the CPE device sends the sensor fault event to the server over this persistent TCP connection. This also enables commands from the server to the CPE device to execute immediately. For example, if a user changes the system mode or arming state using the Subscriber Portal, the change happens immediately on the CPE device and is reflected in the Subscriber Portal and the touchscreen CPE device.

See the "Icontrol Connectivity Protocols" section in *System Operations Guide* for information about broadband heartbeats.

3.2 Cellular Channel

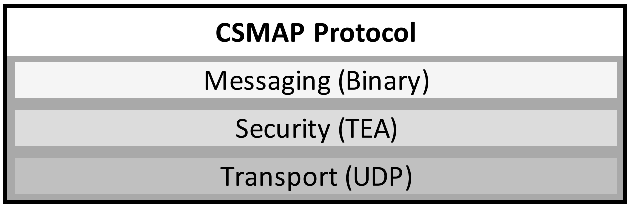
The cellular channel is the emergency backup communication channel within the Home Domain. This means that whenever the broadband channel goes down, the touchscreen communicates certain zone events, system arm/disarm events, and alarms to the Operator Domain over the cellular channel. In addition, the application cluster uses cellular to communicate remote commands (such as remotely arming/disarming the Home Domain).

The events reported by the touchscreen and the commands that can be remotely performed on the subscriber's system are limited when broadband is down. The communication and functionality when broadband is down are determined by the cellular level of service (see "Cellular Levels of Service" on page 17).

Heartbeats are used to monitor the connectivity status of the touchscreen to the cellular channel. The frequency of heartbeat transmissions is configurable by tier. See the "Icontrol Connectivity Protocols" section in *System Operations Guide* for information about cellular heartbeats.

IMPORTANT: Cellular-only connectivity is an emergency backup channel designed to ensure that your security system will continue to communicate alarms and perform other vital actions during an unforeseen loss of broadband. Home Domains with cellular-only connectivity lose most remote-control functionality and only broadcast major system events such as alarms.

Although UDP is less reliable than TCP, the touchscreen ensures the successful delivery of important messages such as alarms and arm/disarm events by requiring an acknowledgment from the cellular communication module. If it does not receive an expected acknowledgment for important UDP events, the touchscreen continues transmitting the event until it does receive the acknowledgment. Since cellular usage is expensive, the touchscreen does not require an acknowledgment for non-critical zone events such as the opening and closing of a door. Such messages make up more than 95% of the traffic between the touchscreen and the application cluster.



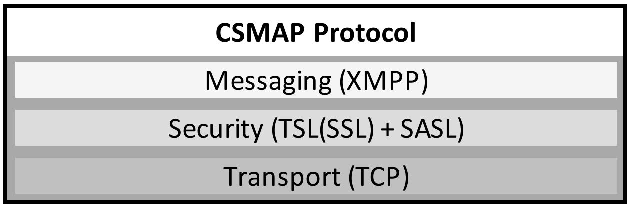
Cellular UDP Protocol Stack

Messages are sent over UDP using a compressed binary messaging protocol in order to minimize cellular costs. Optionally, these messages are secured using the Tiny Encryption Algorithm (TEA).

Communication from the touchscreen to the Operator Domain occurs over a private, secure network. Communication is established over two segments:

- Cellular service provider's network from the touchscreen to a General Packet Radio Service (GPRS) access point or to an Enhanced Data Rates for GSM Evolution (EDGE) access point
- An Internet Protocol Security (IPSEC) tunnel or a Virtual Private Network (VPN) between the access point and the data center that hosts the Icontrol application servers

While broadband is down, a TCP socket connection can be established between the touchscreen and the application cluster to send remote commands to the touchscreen, such as arming/disarming the system using the Subscriber Portal or the Mobile App. Once the command messages have been exchanged, the TCP connection is shut down. XMPP is the messaging protocol used for these communications. All TCP communication is secured using TLS 1.0 (SSL 3.1) and SASL authentication.



CSMAP Protocol

Messaging (XMPP)

Security (TSL(SSL) + SASL)

Transport (TCP)

Cellular TCP Protocol Stack

For more information, see the "Broadband/Cellular Connectivity Problems and Resolutions" section in *System Operations Guide*. For details about UDP activity, see the "UDP Activity" section in *System Operations Guide*.

3.2.1 Cellular Levels of Service

The amount of data that is transmitted over cellular between the touchscreen and the server when broadband is down varies depending on the customer's cellular level of service. The system provides the following levels of support for cellular:

Basic - Only important events and commands are transmitted over cellular.

Basic Plus - An intermediate level of service.

Enhanced - This level provides the fullest set of features that are supported over cellular. With this level of support, if the subscriber does not have an unlimited voice/SMS cellular plan, an alarm or other event might not be sent if the subscriber has already exceeded the usage limit.

The `cellular.levelOfService` tier property defines which level of support customers receive. The default value for all tiers is enhanced. See *Management Portal Guide* for more information about this property.

The following table lists the event types that are supported over cellular for each level of service.

Message Type	Basic	Basic Plus	Enhanced
Alarm events	Yes	Yes	Yes
Trouble events	Yes	Yes	Yes
Entry delay events	Yes	Yes	Yes
Heartbeat events	Yes	Yes	Yes
Arm/disarm events	Yes	Yes	Yes
Keycode Create/Update/Delete	Yes	Yes	Yes
Emails/SMS for rules (no images)	No	Yes	Yes
Zone events	No	No	Yes
Touchscreen App install/update	No	No	No
Video	No	No	No
Broadband down event	No	No	Yes

IMPORTANT: Event history that is not reported when broadband is down is not retained.

3.2.1.1 All Portal Commands Over Cellular

Various commands that originate from the Management Portal, the Subscriber Portal, or a mobile device are sent to the touchscreen over cellular. The following table lists which commands each level of service supports.

Command	Basic	Basic Plus	Enhanced
Create, update, or delete keypad code	Yes	Yes	Yes
Arm	No	Yes	Yes
Disarm	No	Yes	Yes
Enable or disable rule	No	Yes	Yes
Create rule	No	No	Yes
Update rule	No	No	Yes
Delete rule	No	Yes	Yes
Bypass zone	No	Yes	Yes
Update zone	No	Yes	Yes
Access camera	No	No	No
Camera on-demand video	No	No	No
Change lighting settings	No	No	No
Change thermostat settings	No	No	No
Change door lock settings	No	No	No
Change cloud object settings	No	No	No
Delete touchscreen app(s)	No	No	Yes
Reorder touchscreen app(s)	No	No	No

3.2.1.2 Management Portal Commands During Cellular-only Connectivity

The following Management Portal commands are always disabled over cellular-only connectivity:

- Start SSH tunnel
- Stop SSH tunnel
- Initiate VNC (SMC P5 only)
- Upgrade touchscreen firmware
- Get Diagnostic File
- Device Health Check Request
- CPE Screen Capture
- Viewer engaged
- Reboot Router
- Adjust Wi-Fi Channel

4 Understanding the Common Server Architecture

The common server architecture manages the subscriber's system. It is capable of simultaneously managing subscriber systems using Converge or Touchstone platforms. The platforms do not necessarily use all of the same elements of the common server.

The common server architecture hardware and software details described in this document are for reference purposes only. This information is meant to be a starting point from which the final production-quality architecture may be derived. The architecture is subject to change based on input from various groups involved in this process.

The common server architecture consists of the following elements:

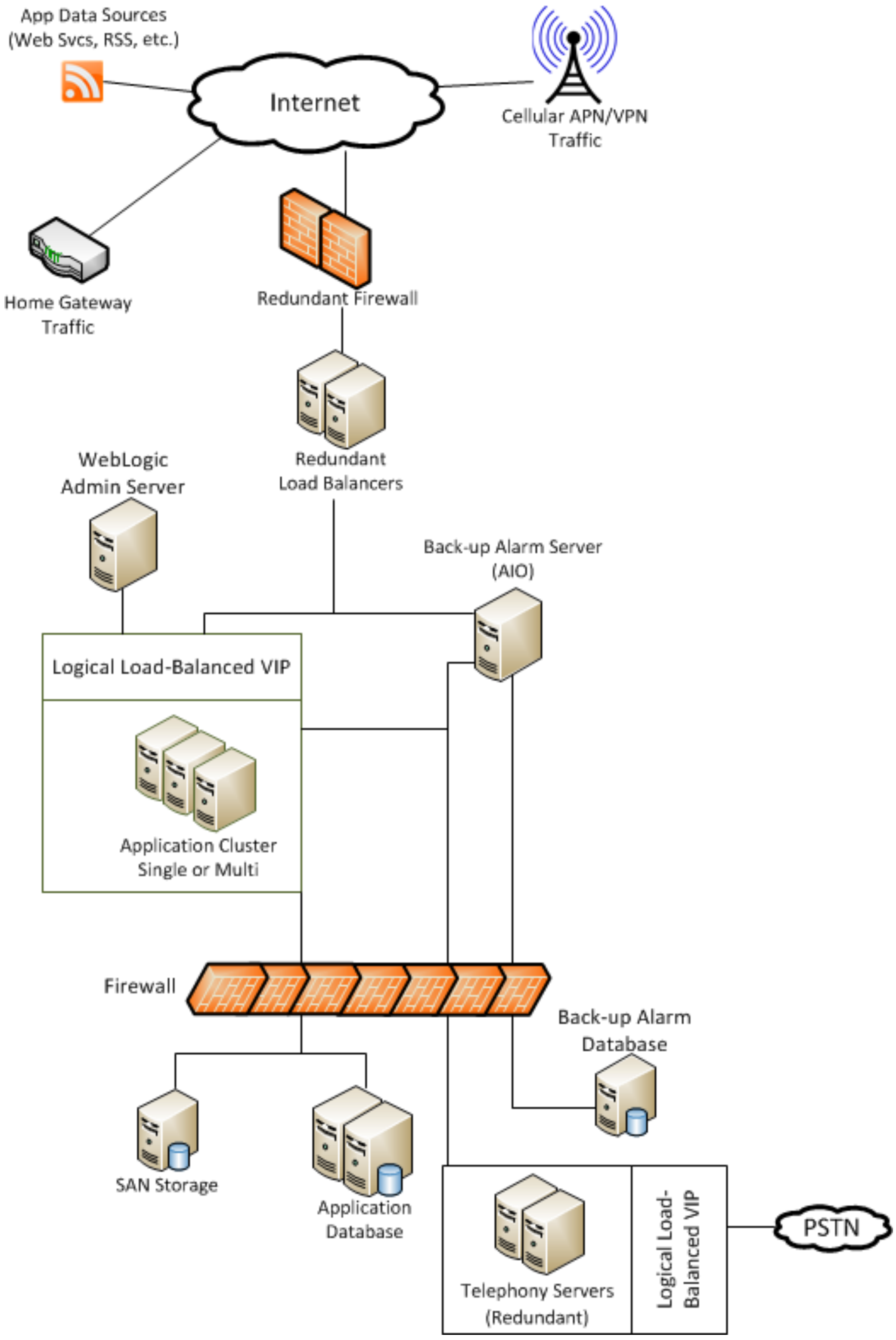
- Server Cluster(s)
- Database Segment
- Relay Server
- Event Bus
- Bundle Server
- BOSS/OSS Systems

4.1 Server Architecture

The following figure shows the server architecture of the Operator Domain. The server cluster(s) described in this figure use a multiple-cluster configuration.

Note: Support for telephony servers has been deprecated.

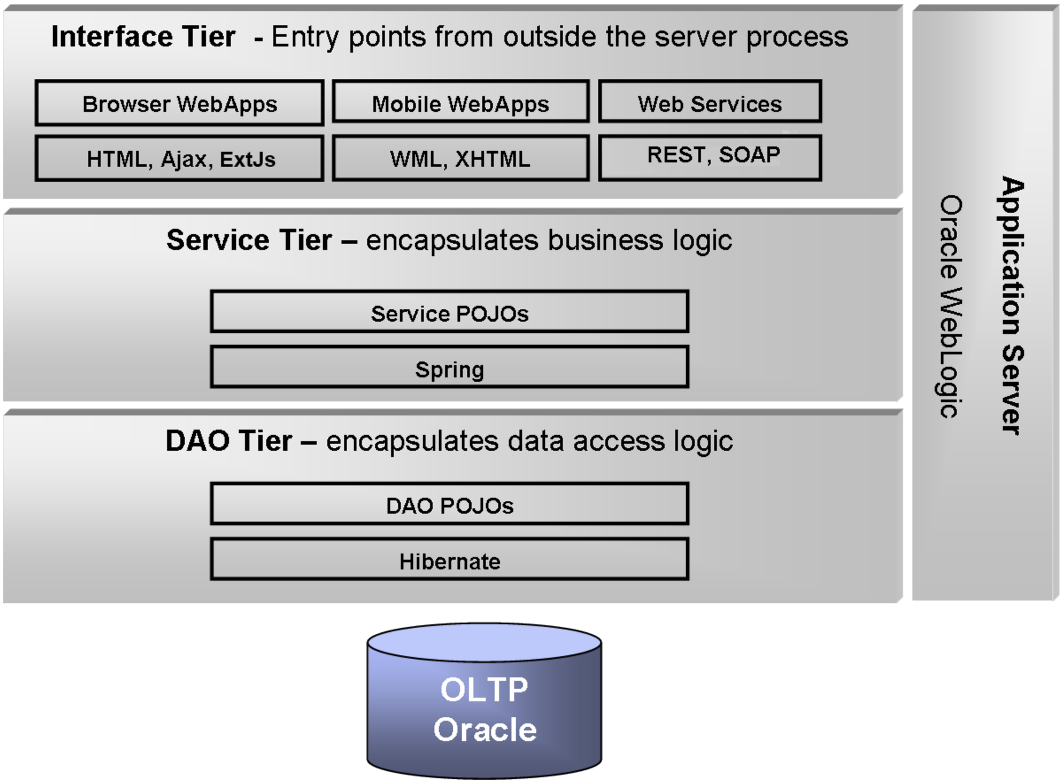
Note: Single-cluster server configuration is no longer supported as of the Oahu release.



Server Architecture - Converge

4.2 SOA Architecture

The Common Server Architecture is a standard tiered Java 2 Enterprise Edition (J2EE) Service Oriented Architecture (SOA). The server cluster(s) servers run within a WebLogic Application Server and implement the Interface, Service, and DAO tiers.



Tiered J2EE SOA Architecture

4.3 Application Segment

The Application Segment of the Operator Domain includes the following elements:

- Server cluster(s)
- Backup Alarm Server

The following sections in *System Operations Guide* are also relevant to understanding this segment of the Operator Domain:

- "Loss of Service Protocols"
- "Image/Video Capture Paths and Algorithms"

4.3.1 Server Cluster(s)

The server clusters are redundant, load-balanced, WebLogic server clusters that receive and handle all calls and alerts from the touchscreens. The cluster also hosts the Subscriber Portal and Management Portal to manage end-user-specific account settings. Finally, the server clusters require a separate, properly configured WebLogic Admin Server.

The server cluster handles all non-alarm and alarm events at the Home Domains, heartbeats, and command traffic between servers and the Home Domains. In addition, it manages end-user email and SMS notification as well as integrations with the OSS/BSS systems.

Note: If the server cluster loses communication with a Converge CPE device for any reason, the CPE device fails over to the Backup Alarm Server for reporting alarm events. See "Backup Alarm Server" on page 27 for more information.

The server clusters are secured within a DMZ, a sub-network inserted as a "neutral zone" between the operator’s private network and the outside public network (Internet, cellular, etc.). This provides an added layer of security for both the Icontrol network and the service provider’s private network.

IMPORTANT: The firewall settings should prevent access to the Management Portal from outside the company’s private network.

4.3.1.1 Configuration Options

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

4.3.1.1.1.Multiple Cluster

This configuration for the server cluster is being Load and Stress tested with the intent to support up to 750,000 active, deployed subscribers. It consists of the following three clusters managed by a single WebLogic Admin Server. Each cluster must include at least two (2) server nodes for redundancy.

- ❑ **CPE Cluster**: This cluster is primarily tasked with communicating with the Home Domain over broadband and cellular. It forwards security messaging to the Central Monitoring Station. It manages apps on the Converge touchscreen. It also processes SMTP/SMSC messages. The CPE cluster communicates with the Portal cluster through WebLogic Store-and-Forward (SAF).
- ❑ **Portal Cluster**: This cluster contains the user portals (Subscriber Portal and Management Portal) that interface with subscribers and customer representatives. It also contains the Integration module and Service Layer. The Portal cluster communicates with the CPE cluster through WebLogic Store-and-Forward (SAF).
- ❑ **Media Cluster**: This cluster manages operations related to saving images and video captured at the Home Domain. It also processes camera proxy operations.

4.3.1.1.2.Subscriber Capacity

As a rule of thumb, the multiple-cluster CPE cluster supports about 50,000 subscribers per server. In practice, this means that a system supporting 50,000 to 100,000 subscribers requires a minimum of three servers per cluster. This is necessary in order to allow the system to function without potential overload when one of the servers needs to be taken down for maintenance or upgrades.

For the Portal cluster and the Media cluster in the multiple-cluster environment, each server is currently estimated to support 5,000 concurrent user logins.

4.3.1.2 WebLogic Admin Server

The WebLogic Admin Server serves as the central control entity for the configuration and monitoring of the server clusters. It maintains the cluster configuration and pushes applications and configuration changes to managed servers within the domain.

One WebLogic Admin Server manages the server clusters.

As the size of the server clusters increases, the size of the admin server needs to grow as well (per WebLogic best practices) since large clusters can get bottle-necked at the admin server.

Server administrators can use the WebLogic Admin Console to interact with the admin server and manage the cluster.

4.3.1.3 Hard Drive and Partition Sizes

The required software installed on the server clusters servers and the WebLogic Admin Server consumes less than 1 GB; however, the log files can require a lot of additional space. A minimum of 30 GB combined hard drive space is required for the server clusters and 20 GB of space for the WebLogic Admin Server.

4.3.1.4 Connectivity

Connected Elements	Communicating Module	Protocol	Port
Touchscreen App Data Sources	Touchscreen App Management	HTTPS	443
Email and SMS Alerts to PCs and Mobile Devices	SMTP and SMSC Gateway	SMTP and SMSC	Email and SMS message alerts are received through SMTP and SMSC gateway equipment. **Note:** The number of daily allowed SMS messages per customer is tier-based and can be managed using the sms.dailyLimit property. See *Management Portal Guide* for more information about tier properties.
Database Segment	Not applicable	TCP	1521
CPEs	Broadband	TCP	5222

Connected Elements	Communicating Module	Protocol	Port
CPEs, PCs, and Mobile	Broadband	TCP	443 (HTTPS)
CPEs	Cellular	UDP	9091
		TCP	5222
Note: PCs and mobile devices continue to communicate with the server clusters over broadband when the CPEs are communicating over cellular only.			

4.3.1.4.1.Out-Servers Whitelist

The server clusters must have access to the following domains via port 80 (HTTP) or 443 (HTTPS):

- api.flickr.com
- *.accu-weather.com

4.3.1.5 Staging Server

In addition to the production server system, a secondary, smaller-scale staging server set (also referred to as a test server set) is used to test patches, upgrades, content modifications, configuration changes, or any other type of system change to ensure that it will not adversely affect the production environment.

As a general rule, the staging environment is usually installed in the production data center environment that mimics the production servers as closely as possible. It is also generally accepted that the staging system be unconcerned with issues of scale, but more focused on getting as close as possible to the types of system interactions that happen in the production server set. However, in some cases a service provider may have internal policy that dictates that production and staging server sets are replicas of each other in almost every way. While this is certainly possible, it is generally not a good use of costly hardware or administrative overhead in most cases, as a scaled-down instance of the staging environment can closely approximate upgrade-related behaviors in the vast majority of cases. The Icontrol deployment approach is intended to work closely with the service provider's IT department to create an architecture for the staging system that balances IT requirements with testing capabilities and cost to implement and maintain the staging environment. Depending on policies and IT infrastructure requirements, it is generally safe to budget about 40% - 50% of the cost of the production system hardware into the projected costs of the staging environment. Again, tradeoffs can be made that would take this as low as 25% of the production environment costs or as high as 100% of the production environment costs.

4.3.1.6 Modules

The Core Server software includes the following elements to handle its operational and monitoring functions. Some elements are not used by all platforms:

- ❑ Portals
- ❑ REST API
- ❑ Notification Module
- ❑ Integration API (WSDL)
- ❑ Touchscreen App Management Module
- ❑ CMS Communication Module

4.3.1.6.1.REST API

The Icontrol REST API provides access to Icontrol-powered devices within the end user's home. For more information, see: https://share-icontrol.atlassian.net/wiki/display/APID/7.3+Quadra+Core+-+API+Documentation.

4.3.1.6.2.Notification Module

The Notification Module manages whether and how users should be notified of different events generated within the Home Domain. It is configured using the Subscriber Portal to specify whether and who to notify on particular events and how to notify them (phone call, email, or SMS text message). When alarm and non-alarm events are received in the Operator Domain, they are asynchronously passed to the Notification Module for processing.

4.3.1.6.3.Integration API (WSDL)

The Integration Module provides the infrastructure and interfaces necessary to integrate the BOSS/OSS systems (e.g., billing, provisioning, inventory, tech support, etc.) with the rest of the elements of the Operator Domain.

The Integration Module has a web services interface for upstream integration that BOSS/OSS systems can access in order to perform operations like creating and updating accounts and to query information stored in the Database Segment.

The Integration Module also has an event-driven framework for downstream integration. System-specific plug-ins can be developed for the Integration Module framework to inform external systems of events within the Icontrol system. See *System Operations Guide* for more information about the WSDL.

4.3.1.6.4.Touchscreen App Management Module

The Touchscreen App Management Module is responsible for importing, configuring, and managing touchscreen apps in the system, including upgrades.

4.3.1.6.5.CMS Communication Module

This module is used for communications with the central monitoring station. After the Operator Domain receives an Alarm event and the Notification Module processes it, this component forwards them to the central monitoring station via a TCP connection.

4.3.1.7 Portals

The portals are the integrated tools that enable subscribers and service provider representatives to monitor and manage systems and accounts. The portals are part of the server cluster software architecture, and they report what the Operator Domain knows about a subscriber premise. They can issue certain commands to the touchscreen CPE devices through the secure always-on broadband connection between the CPE devices and the Operator Domain.

4.3.1.7.1.Management Portal

The Management Portal is a web application that enables service providers to monitor and manage subscriber accounts.

4.3.1.7.2.Subscriber Portal

The Subscriber Portal is an interface that enables subscribers to access their home systems remotely via a web browser or a mobile app.

This interface does not provide access to some device configuration options available to Converge subscribers on their touchscreen CPE device; however, it provides several options that cannot be performed from the touchscreen, such as alert management, contact management, and account management.

The subscriber's user experience varies based on whether the subscriber's system is on the Converge or Touchstone platform, whether the system is accessed via a web browser or mobile app, and, potentially, depending on their service tier and packages. Refer to *Management Portal Guide* for information about tiers and packages.

The Subscriber Portal is built using standard web application technologies like HTML, Ajax, and YUI. Standard web application security technologies are used to secure the Subscriber Portal as it is accessible over HTTPS (required) on port 443. The Acegi Security Framework is used in conjunction with forms-based authentication for both authentication and authorization of end users when they log in.

The application servers also provide a Camera Proxy Service. This module is used only as a backup service when direct camera access through the Subscriber Portal fails. This is useful when the customer has high ports blocked due to a corporate firewall or when the viewing client is behind a router that does not allow re-routed packets. The Relay Server handles live video and images.

4.3.2 Backup Alarm Server

If the server cluster cannot be reached, the touchscreen sends alarm events to the Backup Alarm Server. This guarantees that the alarm path is uninterrupted if the server cluster goes down. It can be co-located in case the physical location of the server cluster goes down. This is a lower-cost alternative to replicating the entire Operator Domain.

It takes less than 120 seconds for a touchscreen to fail over to the Backup Alarm Server. If there are any pending acknowledgments for alarm messages that were sent during that time, they are immediately sent when the Backup Alarm Server takes over. See the "Back-Up Alarm Server Fail-Over" section in *System Operations Guide* for more information.

Note: No non-alarm events are logged to the Backup Alarm Server.

The Backup Alarm Server is secure in the DMZ along with the server cluster. It has its own database with the same schema as the primary application database. See "Backup Alarm Database" on page 29 for more information.

The IP address of the Backup Alarm Server is configured in the `custom.properties` file using the `backupServer.ip` property (see the "server.properties" section in *System Operations Guide*).

See the "Alarm Events Sequence (Broadband Connection)" section in *System Operations Guide* for information about the sequence of alarms over broadband. See the "UDP Activity" section in *System Operations Guide* for information about the sequence over cellular.

4.3.2.1 Connectivity

Source	Communicating Module	Protocol	Port
Touchscreens Only	Broadband	TCP	5222
Touchscreens Only	Cellular	TCP/XMPP	5222
		UDP	9091
Backup Alarm Database	Not applicable	TCP	1521

4.3.2.2 Hard Drive and Partition Sizes

The entire required software installed on the Backup Alarm Server consumes less than 1 GB; however, the log files can require a lot of additional space. A minimum of 30 GB combined hard drive space is required for this server.

4.3.3 Cluster Location Service

Cluster Location Service (CLS) is an optional component of the Icontrol server platform that enables multiple server clusters to operate in parallel and increase scalability. When CLS is implemented, CPEs and remote clients do not need to be configured to connect to a single server cluster. Instead, CLS enables CPEs and remote clients to locate user accounts on various clusters. For more information, see *Cluster Location Service Installation Guide*.

4.3.4 Cloud Automation and Control

Cloud Automation and Control is an optional feature that simplifies the integration of cloud-based devices and services by defining specific ways to interact with the Icontrol platform. This feature enables the creation of automations that interact with a cloud service or device, and the ability to control or monitor a cloud service or device. These subscriber-facing features are only available in the new Mobile App and the new browser-based Web App, which are based on the Card UI framework. Starting with the 7.1 Oahu release, the Web App will replace the “classic” Icontrol Subscriber Portal. Service providers implementing this feature must install the Web App and/or Mobile App for subscribers to access the cloud device(s); the devices are not displayed on the touchscreen.

Icontrol's Cloud Integration Service (CIS) must be installed and configured to enable Cloud Automation and Control. Icontrol has provided a method for third-parties with cloud services or devices to partner with Icontrol and seamlessly become part of the ecosystem. The method is a Cloud Integration Adapter that resides at the partner server and communicates with the service provider's Cloud Integration Server. Once the Cloud Integration Adapter is configured with the Cloud Integration Server, it appears as a device to the subscriber. For more information, see *Cloud Integration Service Installation Guide*.

4.4 SAN Shared Storage

The SAN shared storage is used to archive file-based data used by the Operator Domain, such as images, video, and diagnostic management files. For more information, see the "NAS Sizing" appendix here: https://share-icontrol.atlassian.net/wiki/display/CSKB/7.3+Quadra+Core+-+Architecture+Requirements

4.5 Database Segment

The Database Segment includes the following elements:

- Application Database servers
- Backup Alarm Database

The operator’s database administrator configures and maintains the Database Segment.

4.5.1 Application Database

The Application Database servers store table and data information used by the Operator Domain to perform its operations and manage its accounts.

4.5.1.1 Database Storage

By default, the Application Database servers include the following tablespaces:

- **Default tablespace**: Stores account-related data
- **Event tablespace**: Stores event-related data
- **Event index tablespace**: Specifically used for indexes on the event data tables

For optimal performance, be sure to follow the Oracle Optimal Flexible Architecture guidelines in order to reduce I/O contention within the database server.

The storage space used by the database server varies based on deployment. Refer to the *Capacity Planning* spreadsheet for a detailed estimate (see https://share-icontrol.atlassian.net/wiki/display/CSKB/7.3+Quadra+Core+-+Product+Documentation).

When planning your database implementation, be sure to minimize I/O contention among these tablespaces.

4.5.2 Backup Alarm Database

The Backup Alarm Database stores table and data information for the Backup Alarm Server. See "Backup Alarm Server" on page 27 for information about the Backup Alarm Server. The DBA is responsible for setting up and configuring the elements of the Database Segment.

4.5.2.1 Hard Drive and Partition Sizes

The Back-up Alarm Database server uses approximately 30 GB of disk space. Contact your Icontrol representative for implementation details.

4.5.3 Database Replication

Oracle GoldenGate replication is used to replicate data between the Converge Application Database and the Converge Backup Alarm Database. For more information, see *Converge GoldenGate Installation and Setup*.

4.5.4 Database Monitoring

The system contains several tables that are used to track the status of the database. The ICHealthCheck tool provides queries that you can use to monitor the number of select, insert, and delete operations performed over the last fifteen minutes, or over a specified timespan. For more information, see the "ICHealthCheck Service" section in *System Operations Guide*.

4.6 Relay Server

The Relay (or "Meet-in-the-Middle" server) is responsible for management, allocation, and digital delivery of on-demand video streaming content. This content originates from within the Home Domain cameras and is delivered to Internet streaming clients (browsers, tablets, mobile phones, etc.). For example, when a subscriber views video on the Subscriber Portal using a web browser or a mobile device, the video does not pass through the application servers. Instead, it streams directly from the cameras through the security router to the Relay Server. Although the portals themselves originate from the application servers, the video viewed in the portals does not. It comes from the Relay Server.

Home systems using SMC P5 QNX touchscreens do NOT use the Relay Server.

For more information, see *Relay Server Installation Guide* and *Relay Server Upgrade Guide*.

4.7 Event Bus

The Icontrol Event Bus enables you to access real-time events coming from subscribers' CPEs. The Event Bus, which consists of Kafka and Zookeeper application servers, enables rapid delivery of events to a repository so that third-party applications can consume, analyze, and act upon event messages. The messages can be consumed at any pace and can be replayed if needed. For more information, see: https://share-icontrol.atlassian.net/wiki/display/APID/7.3+Quadra+Core+-+Event+Bus+Documentation

4.8 Bundle Server

The Bundle Server is a web server used to host CPE app bundles and firmware images. Packages for these are maintained in the database only as meta data with a reference to a publicly accessible URL that contains the actual encrypted app/firmware bundles and files. The web server can be hosted locally (behind the firewall with the server cluster(s)) or remotely.

For demos and labs, the Bundle Server can be located on one of the application nodes (as long as the URL is publicly addressable). This is not suitable for production due to the high bandwidth requirements of the Bundle Server, such as when many CPEs download the firmware package during a batch firmware update. This could affect the performance of the server cluster. For more information, see: https://share-icontrol.atlassian.net/wiki/display/CSKB/7.3+Quadra+Core+-+Architecture+Requirements

4.9 BOSS/OSS Systems

The Business/Operations Support System (BOSS/OSS) consists of operator-maintained inventory, provisioning, etc. systems that use Icontrol data for their designated operations.