



VOTING SOLUTIONS FOR ALL PEOPLE



Use Procedures

VSAP-UPM-001

Version 1.9

06/19/2020

Document Revision History

Date	Version	Section/Page	Update Description
06/03/2019	1.1	Document	Initial Publication
07/15/2019	1.2	Document	Miscellaneous updates
10/14/2019	1.3	Document	Miscellaneous updates
11/2/2019	1.4	Document	Miscellaneous updates
12/2/2019	1.5	Document	Miscellaneous updates
1/31/2020	1.6	Chapter 5 and chapter 10.4	Updated security procedures
02/03/2020	1.7	Cover page	Finalized certification version; document version number
05/30/2020	1.8	Document	More consistent formatting throughout document; updated graphics and pictures; removed redundant information or added section referral; revised section numbers/headings
06/19/2020	1.9	Document	Updated information about security seals.

1. Contents

1.	Introduction.....	8
1.1.	Ballot Marking Device.....	9
1.2.	Ballot Marking Device Manager.....	10
1.3.	Enterprise Signing Authority.....	11
1.4.	Interactive Sample Ballot.....	12
1.5.	Tally.....	13
1.6.	VSAP Ballot Layout.....	14
1.7.	Terms and Definitions.....	14
2.	System Components: Definitions and Descriptions.....	15
2.1.	Functional Components.....	15
2.1.1.	Ballot Marking Device (BMD) Functional Components.....	17
2.1.2.	Ballot Marking Device Manager (BMG) Functional Components.....	18
2.1.3.	Electronic Signing Authority (ESA) Functional Components.....	20
2.1.4.	Interactive Sample Ballot (ISB) Functional Components.....	21
2.1.5.	Tally Functional Components.....	23
2.1.6.	VSAP Ballot Layout (VBL) Functional Components.....	24
3.	Ballot Definition.....	25
3.1.	Overview Procedures to Operate Voter Ballot Layout.....	25
3.2.	Paper and Printing Specifications.....	25
3.2.1.	Specifications for Thermal Paper (BMD).....	25
3.2.2.	Specifications for Tally.....	29
3.3.	Layout Requirements and Specifications.....	29
4.	System Installation and Configuration.....	30
4.1.	Programming and Configuration of Election Management System.....	30
4.2.	Hardware Requirements and Specifications.....	30
4.2.1.	BMG Hardware Requirements.....	30
4.2.2.	BMD Hardware Requirements.....	31
4.2.3.	ESA Hardware Requirements.....	31
4.2.4.	ISB Hardware Requirements.....	32
4.2.5.	Tally Hardware Requirements.....	33
4.2.6.	VBL Hardware Requirements.....	38
4.3.	Hardware and Network Setup and Configuration.....	41
4.3.1.	BMG Hardware Installation.....	41
4.3.2.	BMD Hardware Installation.....	41
4.3.3.	ESA Hardware Installation.....	41
4.3.4.	ISB Hardware Installation.....	41

4.3.5.	Tally Hardware Installation	41
4.3.6.	VBL Hardware Installation.....	41
4.4.	Software Installation and Configuration	42
4.4.1.	BMG	42
4.4.2.	BMD	42
4.4.3.	ESA Hardware Installation	42
4.4.4.	ISB	42
4.4.5.	Tally	42
4.4.6.	VBL.....	42
4.5.	Software and Firmware Upgrades.....	43
5.	Acceptance Testing.....	44
5.1.	Development Test Specifications.....	44
5.2.	Logic Correctness, Data Quality, and Security	44
5.3.	Test Identification and Design	44
5.4.	Standard and Special Purpose Test Procedures.....	49
5.5.	Test Details.....	50
5.5.1.	Test Specifications	54
6.	Election Setup and Definition.....	56
6.1.	Programming and Configuration of Vote Recording Tabulation Device – Tally	56
6.1.1.	General Prerequisites	56
6.1.2.	Building Distribution Kit	56
6.1.3.	Install minimal CentOS.....	57
6.1.4.	Preparing Tally Nodes	64
6.1.5.	Getting Nodes Ready for the Main Installer	65
6.1.6.	Main Installer	66
6.1.7.	Starting Tally	69
6.1.8.	Viewing Tally	69
6.1.9.	Stopping Tally.....	70
6.1.10.	Other Helpful Commands	70
7.	System Diagnostic Testing Procedures.....	72
8.	System Proofing.....	73
8.1.	Generate VBM L&A Ballot Decks	73
8.1.1.	Generation Process for VBM L&A Ballot Decks:	73
8.2.	Generate BMD L&A Poll Passes	73
8.2.1.	Generation Process BMD L&A poll passes:	74
8.3.	Using L&A on the BMD	74
8.4.	Lab Test Mode	77

8.5.	Remake Mode	78
8.5.1.	Activating the Remake Mode on the BMD	78
9.	Multiple Elections	82
10.	Ballot Tally Programs	83
10.1.	Tally Connection Process	83
11.	Election Observer Panel.....	84
11.1.	Invitation.....	84
11.2.	Group Presentations.....	84
11.3.	Appointment Letters (for introduction to precinct workers)	84
11.4.	Mechanism for Feedback.....	84
12.	Hardware Maintenance and Preparation for Use	86
12.1.	Preventative Maintenance Schedule by System	86
13.	Polling Place Procedures.....	88
13.1.	Voting Center Supplies, Delivery, and Inspection	88
13.2.	Vote Center Set-up	89
13.2.1.	Additional Ports.....	99
13.2.2.	Setup Completion.....	100
13.3.	Cleaning the BMD Scanner and Touchscreen.....	102
13.4.	Scanners.....	103
13.4.1.	Bar Code Reader	103
13.4.2.	Ballot Scanner and Printer Rollers	104
13.5.	Opening the Polls.....	110
13.6.	Polling Procedures	115
13.6.1.	Voting Using the BMD Touchscreen.....	115
13.6.2.	Using a Poll Pass	119
13.6.3.	Emptying the Ballot Box During the Day	122
13.6.4.	Restarting BMD After Interruption.....	124
13.6.5.	Dealing with Fleeing Voters	125
13.7.	Voters with Disabilities and Voters using Audio Features.....	126
13.7.1.	Auxiliary Device and Ports	126
13.7.2.	Handheld Controller	126
13.7.3.	Headphone Ports	127
13.7.4.	Dual-Switch Port	127
13.8.	Provisional Voters	128
13.9.	Closing the Polls and Vote Reporting	129
13.10.	Securing Audit Logs and Backup Records.....	133
13.11.	Troubleshooting and Problem Resolution	134

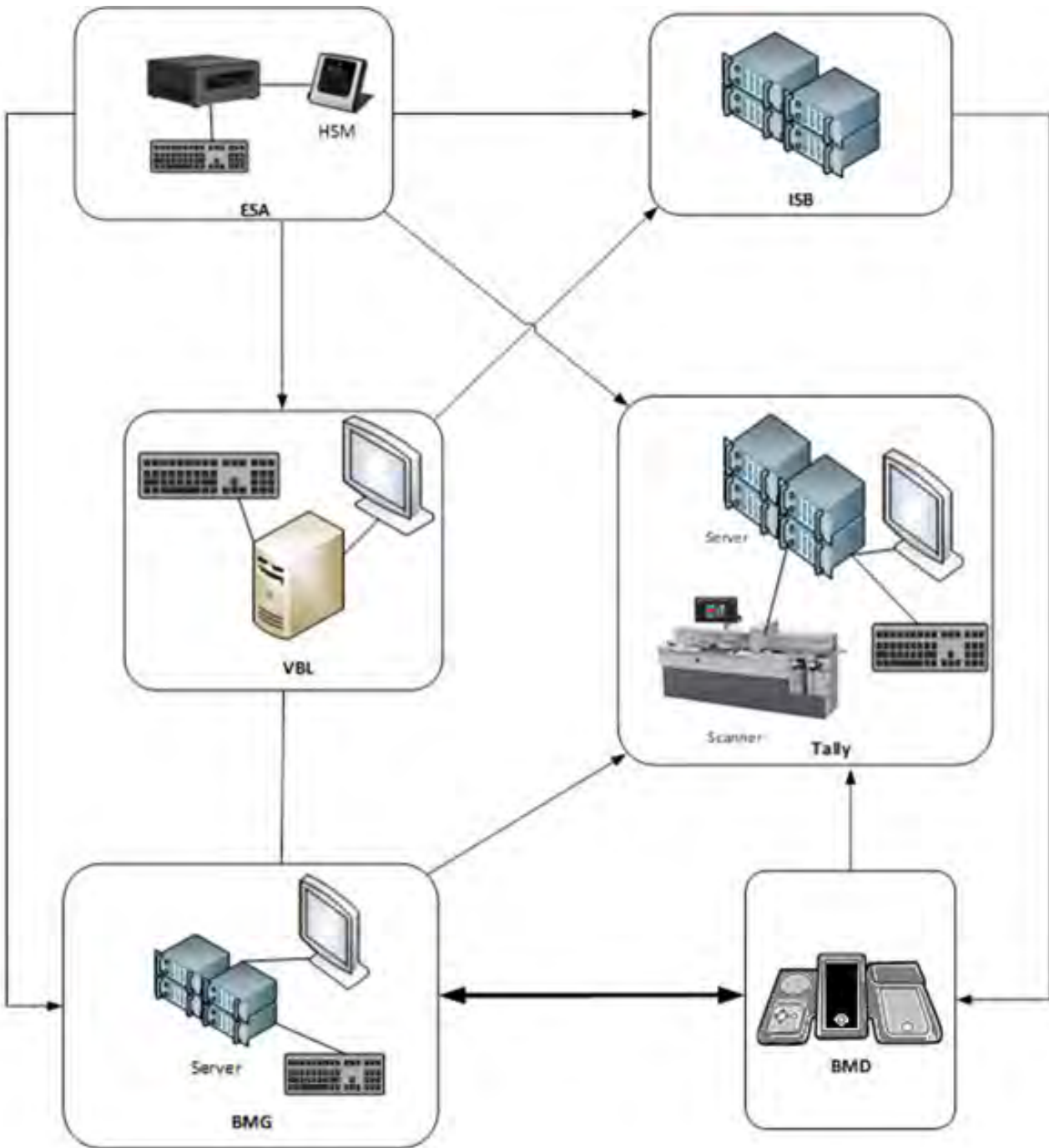
13.11.1.	Problem: Printer has a paper jam	134
13.11.2.	Problem: BMD Cannot Read a Ballot.....	138
13.11.3.	Problem: BMD Touchscreen is Frozen.....	138
13.11.4.	Problem: Headphones are not working	139
14.	Absentee/Mail Ballot Procedures	140
14.1.	System Startup and Pre-Tabulation Report Procedures	140
14.2.	Configuration.....	140
14.3.	Starting Tally	141
14.4.	Tabulation Procedures	142
14.4.1.	Generate Report:	142
14.4.2.	Generate Final Report:	143
14.5.	Post-Tabulation Report and Shutdown Procedures	143
15.	Semi-Official Canvass	144
15.1.	System Start-up and Pre-tabulation Reports.....	144
15.1.1.	Start Tally Services	144
15.1.2.	VSAP Tally Manager	144
15.1.3.	Processing VBM Ballots	145
15.2.	Processing vote reports.....	145
15.3.	Central tabulation	146
15.4.	Precinct Tabulation.....	146
15.5.	Integration with Other Systems and Calvoter Aggregator Application	146
15.5.1.	CalVoter	146
16.	Official Canvass and Post-Election Procedures.....	147
16.1.	Election Observer Panel	147
16.2.	Canvassing Precinct Returns	149
16.3.	Canvassing Absentee Ballots.....	150
16.3.1.	Processing and Counting Vote by Mail Ballots	150
16.3.2.	Processing Vote by Mail Ballots.....	150
16.3.3.	Observation of Vote by Mail Ballot Processing and Counting.....	150
16.3.4.	Challenges	151
16.3.5.	Comparing Signatures	151
16.4.	Canvassing Provisional Ballots	156
16.4.1.	Voting a Provisionally Cast Ballot.....	156
16.4.2.	Handling of Ballot.....	156
16.5.	Canvassing Write-in Votes.....	158
16.5.1.	Counting Write-In Votes.....	158
16.6.	Manual Tally Procedures.....	160

16.6.1.	Manual Tally Using a Voting System	160
16.7.	Handling Ballot Exceptions.....	162
16.8.	Post-Election Logic and Accuracy Testing	163
16.9.	Final Reporting of Official Canvass.....	164
16.9.1.	Sealing of Ballots	164
16.9.2.	Results	164
16.9.3.	Transmission to Secretary of State.....	165
16.9.4.	Announcement of Results	165
16.10.	Backup and Retention of Election Material	167
16.10.1.	BMG.....	167
16.10.2.	BMD Logs.....	168
17.	Manual Recount Procedures	170
18.	Security	171
18.1.	Physical Security of System and Components	171
18.2.	Logical Security of System and Components.....	172
18.2.1.	Essential and Non-Essential Services and Ports	172
18.2.2.	User-Level Security.....	174
18.2.3.	Anti-Virus Protection	174
18.2.4.	Verifying, Checking, and Installing Essential Updates and Changes	175
18.3.	Event Logging Capabilities	175
18.3.1.	BMD.....	175
18.3.2.	BMG.....	175
18.3.3.	ESA	175
18.3.4.	ISB.....	176
18.3.5.	Tally	176
18.3.6.	VBL.....	176
18.4.	Event Logging Design and Implementation.....	176
18.4.1.	BMD.....	176
18.4.2.	BMG.....	176
18.4.3.	ESA	176
18.4.4.	ISB.....	177
18.4.5.	Tally	177
18.4.6.	VBL.....	177
18.5.	Installation Procedures	177
18.5.1.	Acceptance Testing After the Installation.....	177
18.6.	Security Procedures for the BMD Warehouse	178
18.7.	Security Procedures for Vote Center	183

18.7.1.	BMD Vote Center Storage and Security Seal	183
18.7.2.	Ballot QR Codes.....	184
19.	Audit Trails	185
19.1.	Programming and Configuration of Election Management System/Software	185
19.1.1.	Definitions	185
19.2.	BMD Log Files.....	188
20.	Biennial Hardware Certification and Notification.....	189
20.1.	Notification of Equipment	189

1. Introduction

The VSAP voting system allows voters to engage in elections using interactive technology, mobile devices, touchscreen interfaces, QR code readers, and application-based candidate selection. The system is comprised of six core components: Ballot Marking Device (BMD), BMD Manager (BMG), Enterprise Signing Authority (ESA), Interactive Sample Ballot (ISB), Tally, and VSAP Ballot Layout (VBL).



VSAP components

1.1. Ballot Marking Device

The BMD is the primary touchpoint for the voter and hub of the voting system, guiding users with screen prompts and symbols. The BMD features a touchscreen, an audio and tactile controller, and dual-switch input that voters use to generate, verify, and cast a paper ballot. Completed ballots are transferred to the Integrated Ballot Box, which can be detached for unloading. Through the BMD, voters participate in elections.



BMD

1.2. Ballot Marking Device Manager

The BMG manages and maintains the BMDs. It allows operators to manage software, configurations, and data. The BMG provides files necessary for BMDs to present election data such as candidate information, multi-lingual audio, and supporting text. The BMG is the manager and custodian of the voting system.

System Users

User Name	User Role	Status	Actions
John Doe	Advanced User	Locked	[Lock] [Unlock]
Jane Smith	Basic User	Locked	[Lock] [Unlock]
Bob Jones	System Admin	Locked	[Lock] [Unlock]
Charlie Brown	Advanced User	Online	[Unlock]
Diana Prince	Basic User	Online	[Unlock]
Edward Norton	System Admin	Online	[Unlock]
Fred Flounders	Basic User	Offline	[Unlock]
George Jetson	Advanced User	Offline	[Unlock]
Helen Mirren	Basic User	Offline	[Unlock]

Search BMDs by 32,768 Units

Election Status Hardware Issues Location
Software Version Firmware Version MAC Address Serial Number

List All

System Alerts

Time	Issue
12:55 am	Hardware Issue - Screen
11:23 am	OS System - Update Failure
10:12 am	Hardware Issue - Contoller
10:10 am	Hardware Issue - Scanner
09:01 am	Hardware Issue - Printer

View All >

Scheduled Elections

Date	Name
11/06/18	General Elections
02/05/19	Inglewood City (Mayoral)
03/05/19	General Law and Charter Cities
03/05/19	Special Election - Glendora City
03/05/19	Special Election - Hidden Hills

View All >

User Event Log

Time	Event	User Name
12:55 pm	Logged In	John Doe
12:14 pm	Logged Out	Jane Smith
10:25 am	Logged In	Bob Jones
09:01 am	Password Incorrect	Charlie Brown
April 20, 2020		
02:34 am	Logged In	Diana Prince
12:14 pm	Logged Out (Admin)	Edward Norton
April 19, 2020		
08:55 am	Password Incorrect	Fred Flounders

View All >

BMG

1.3. Enterprise Signing Authority

The ESA establishes the security root and chain of trust for the VSAP voting solution. This subsystem comprises the following processes: key management, distribution, and authentication. The ESA uses a cryptographic module to generate a public/private key pair, which authenticates devices and transactions. The ESA is the basis of the authorization, authentication, and data integrity for the voting system.



ESA

1.4. Interactive Sample Ballot

The ISB is a web-based application that allows voters to mark their selections on a sample ballot, either on their desktop or mobile device, prior to formally voting at a vote center. The ISB generates a Quick Response (QR) code called a Poll Pass, which pre-populates selections in the BMD. The ISB also supports Remote Accessible Vote by Mail (RAVBM) and the Overseas Citizens Absentee Voting Act (UOCAVA). The ISB is what voters use when they interact with the system on their computers or mobile devices.

The screenshot shows the 'LA County Pre-Mark Ballot' application interface. At the top left is the LA County logo and the text 'LA County Pre-Mark Ballot'. At the top right are three utility buttons: 'English', 'Settings', and 'Help'. The main content area features a large heading: 'You are about to start pre-marking your sample ballot.' Below this, a sub-heading reads: 'There are three steps to using your pre-marked selections as your official ballot vote for this election.' To the right, a vertical list of three steps is displayed: 1. 'Pre-mark the ballot' (Complete Online) with the instruction 'Pre-mark your ballot selections, using any device.' 2. 'Generate a Poll Pass' (Complete Online) with the instruction 'Your unique Poll Pass will contain your ballot selection information.' 3. 'Cast your vote' (Complete at Voting Center) with the instruction 'Scan your Poll Pass at any LA County Voting Center to mark your ballot.' At the bottom right, a yellow button labeled 'Pre-Mark the ballot' with a right-pointing chevron is visible.

ISB

1.5. Tally

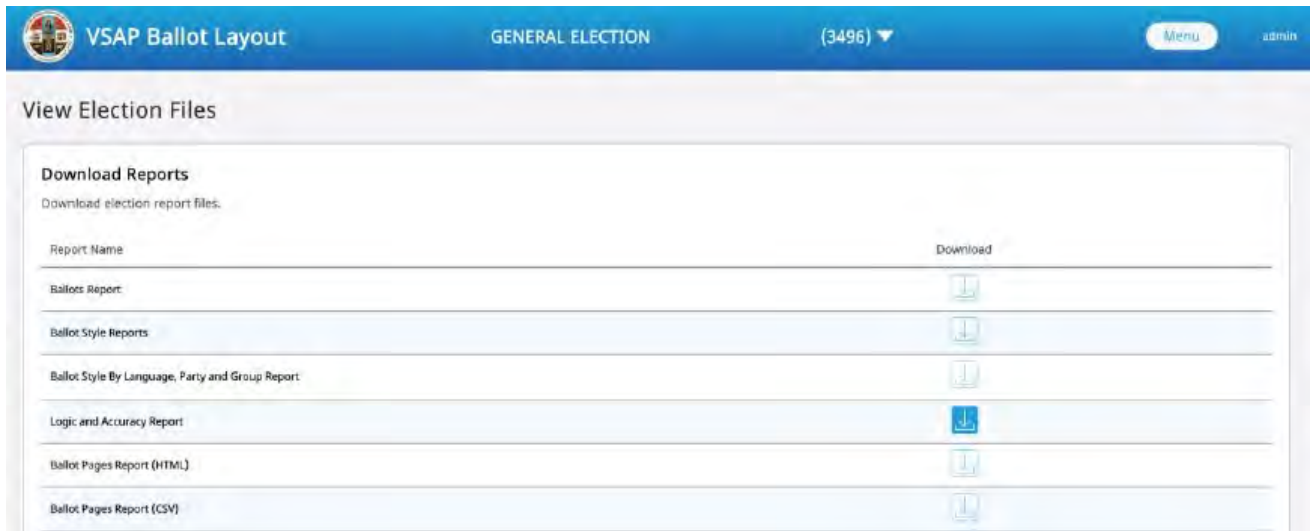
Tally captures and processes ballot images to digitally count voter selections from paper ballots. Tally scans and creates images of ballots, converts the images into Cast Vote Records (CVRs), tabulates them, and allows the election results to be exported. Tally is responsible for counting votes at the end of an election.



Tally

1.6. VSAP Ballot Layout

The VBL enables election managers to configure and generate ballot layouts. The VBL subsystem ingests election information files and generates ballot layout files to be used by other components of the system. The VBL makes setting up elections possible.



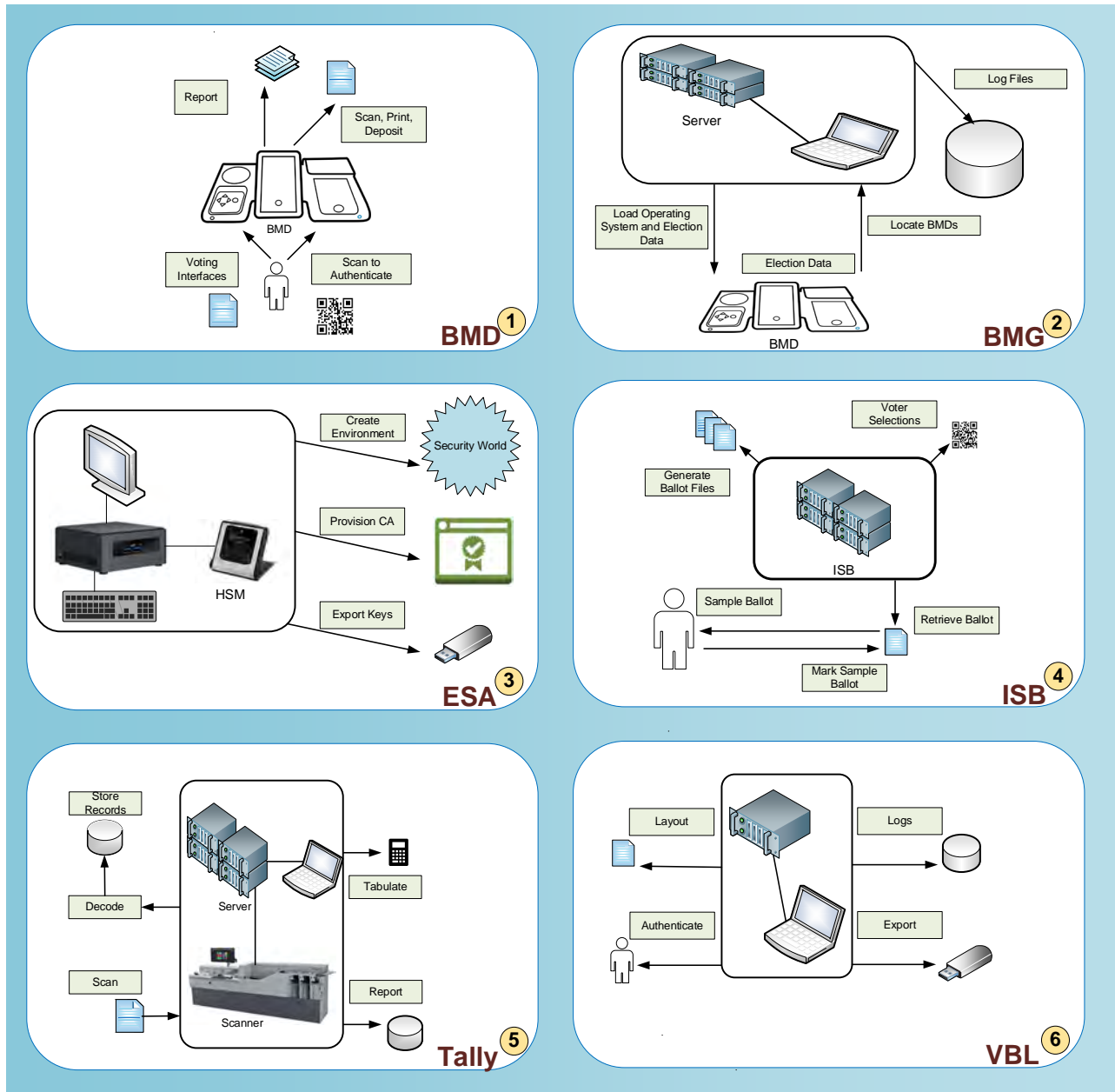
VBL

1.7. Terms and Definitions

Terms and definitions used in this document are described in **VSAP-TDP-011 Acronyms and Definitions**.

2. System Components: Definitions and Descriptions

2.1. Functional Components

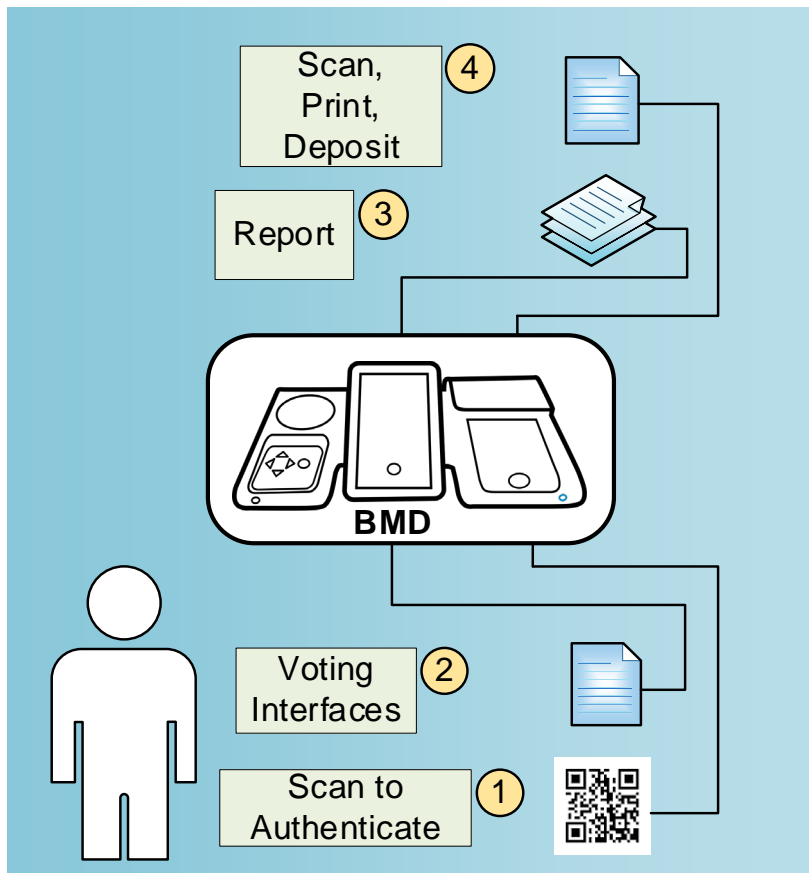


VSAP functional components

Each subsystem of the VSAP system is described at a high level in the following table:

#	Subsystem	Description
1	BMD	The BMD is the primary touchpoint for the voter and the hub of the voting system. It includes a tablet touchscreen interface and several hardware peripherals supporting manual interaction, scanning, and printing capabilities.
2	BMG	The BMG allows operators to manage the software, configurations, and data on the BMDs. Although some diagnostics require manual intervention (e.g., scanner and printer diagnostics, which require paper), the BMG performs automated diagnostics on the BMD without physical access.
3	ESA	The Enterprise Signing Authority (ESA) is a cryptographic module used to ensure each component of the VSAP system is conforming to security standards and to validate the data passed to components are secure and authenticated.
4	ISB	The ISB is a digital version of the sample ballot. It is accessible as a web application that permits prospective voters to review election material and mark their selections on their desktop or mobile device.
5	Tally	The Tally system is responsible for capturing and processing ballot images so that voter selections originating from paper ballots are digitally represented and counted.
6	VBL	The VBL defines the ballot print formats for BMD, VBM, RAVBM and UOCAVA ballots, and generates data files and packages necessary to configure the BMD, BMG, ISB, and Tally.

2.1.1. Ballot Marking Device (BMD) Functional Components



BMD functional components

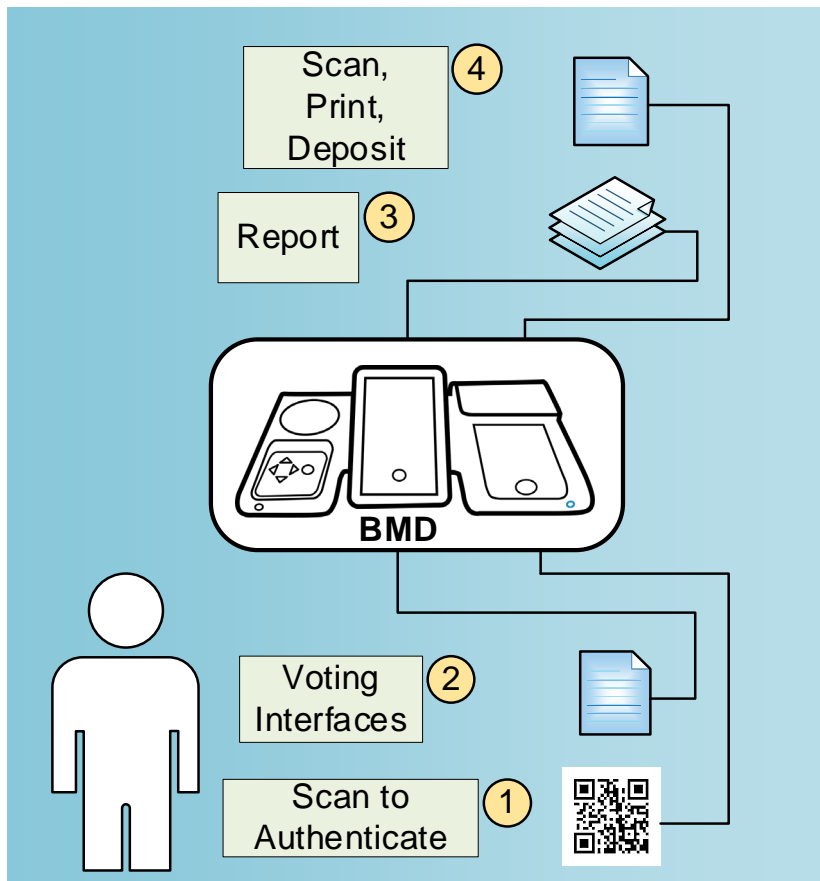
At the warehouse, the BMDs are connected to the BMG network using network cables. The BMDs run diagnostics, receive election and configuration files, and download election log files. At the Vote Center, an election worker scans an authentication QR code and enters a personal identification number (PIN) to activate the BMD and perform the poll opening procedures. During the voting day, voters receive their ballot from the election workers. The BMD scans the ballot's Ballot Page Meta-data (BPM) QR code containing information used by the BMD to determine the appropriate ballot style to display. After making selections, the voter's ballot is printed with election information, voting selections, and a Selection Barcode Encoding (SBE) QR code containing their selections and BMD information. The voter has an opportunity to review and verify the printed ballot before the BMD deposits it in the ballot box. During the voting day, the election worker empties the ballot box as needed. At the end of the voting day, the election worker performs the poll closing procedures.

Following the election, the BMDs are returned to carts or cases and moved back to the warehouse. Once the BMDs are reconnected to the BMG network, the BMD log files are uploaded to the BMG.

Each function of the BMD system is described at a high level in the following table:

#	Function Name	Description
1	User Authentication	Election workers scan a QR code and enter a PIN for system access
2	Voting	Voters interact with the BMD to mark their ballot selections using various interfaces including the touchscreen, controller, and dual-switch input device; to ensure privacy, headphones provide the audio interface
3	Ballot Management	The BMD scans the ballot BPM QR code, prints the voter's selections and SBE QR code, presents the printed ballot for voter approval, and deposits the approved ballot into the ballot box
4	Reports and Logs	The BMD creates Open Poll and Close Poll reports, election logs, and BMD interaction logs

2.1.2. Ballot Marking Device Manager (BMG) Functional Components



BMG functional components

The BMD Manager (BMG) manages and maintains the BMDs and allows operators to manage software, configurations, and data.

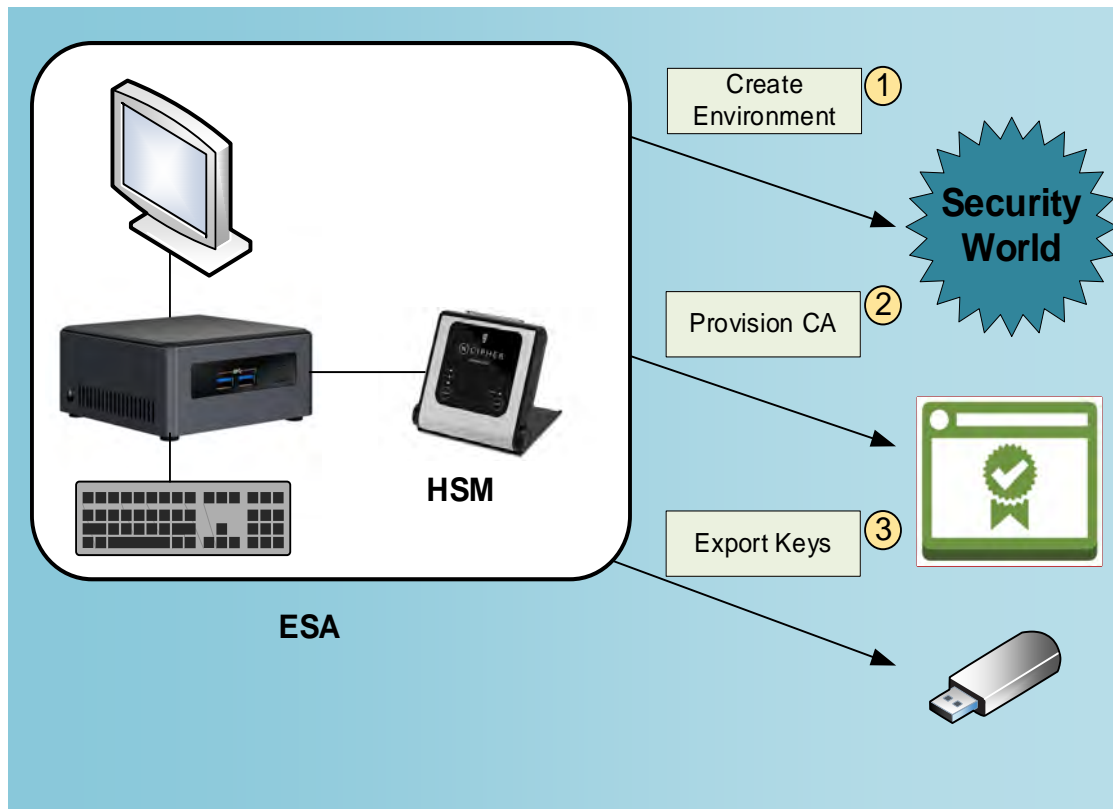
The BMG loads the operating system and the voting application onto the BMDs and conducts system verification. The BMG maintains the location information of the BMDs connected to the BMG network. Processes and interactions are logged. Additionally, the BMG also runs automated diagnostics of the BMDs.

Pre-election, the BMG uploads election data into its repository. The election data can then be loaded onto the BMDs that will be provisioned for an election. Post-election, the BMG downloads the public key files and the log files from the BMDs.

Each function of the BMG system is described at a high level in the following table:

#	Function Name	Description
1	Configure BMDs	Initially, the BMG loads the operating system and BMD applications onto the BMDs. The BMG loads election data and configuration data onto the BMDs prior to an election
2	Inventory and Location	The BMG identifies the warehouse locations of the BMDs when they are attached to the BMG network
3	Event Logging	The BMG logs processes and interactions
4	Retrieve Election Data	Following an election, the BMG retrieves election logs, interaction logs, and the security keys from the BMDs

2.1.3. Electronic Signing Authority (ESA) Functional Components



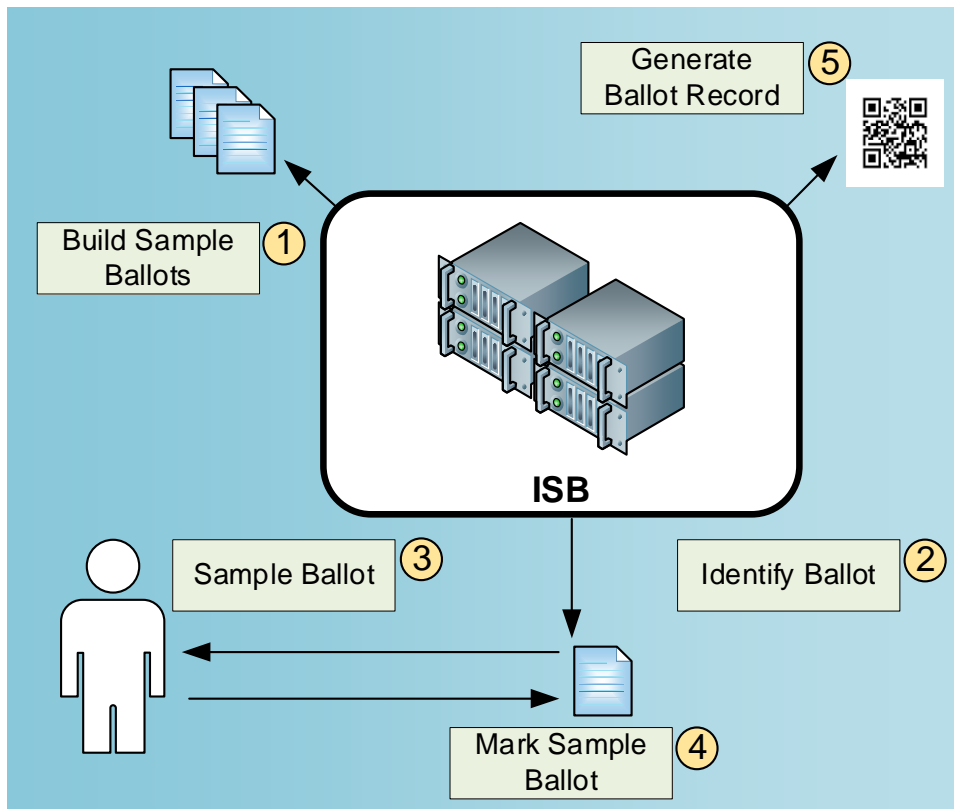
ESA functional components

The Enterprise Signing Authority (ESA) subsystem is a cryptographic module used to ensure each component of the VSAP system is conforming to security standards and to help ensure that the data being passed to components are secure and authenticated. The ESA creates a “security world” in the Hardware Security Module (HSM). The ESA sets up sets of operator cards to manage security keys. The ESA provision Certificate Authorities to establish the security root and chain of trust using a cryptographic module to generate a public/private key pair. Once this process is completed, the ESA generates public/private export key pairs for each component (VBL, ISB, BMG, Tally and the Trusted Environment), encrypts each key with its private key, and exports the keys for use in their target servers.

Each function of the ESA system is described at a high level in the following table:

#	Function Name	Description
1	Create Secure Environment	The ESA creates a security world and operator cards
2	Provision Certificate Authorities	The ESA creates a single root CA key and intermediate CA keys
3	Generate and Export Keys	The ESA creates server keys that are exported to target servers in an encrypted state

2.1.4. Interactive Sample Ballot (ISB) Functional Components



ISB functional components

The Interactive Sample Ballot (ISB) is a software application that allows voters to review and mark their sample ballots, either on their desktop or mobile device, prior to voting at a vote center. The preprocessor takes the input files and generates data packages optimized for the ISB client application. A map assembles the data about precincts, ballot styles, and parties to associate the voter with the appropriate precinct and identify ballot style. The Voter Selection Manager tracks voter selections and enforces legal and business rules.

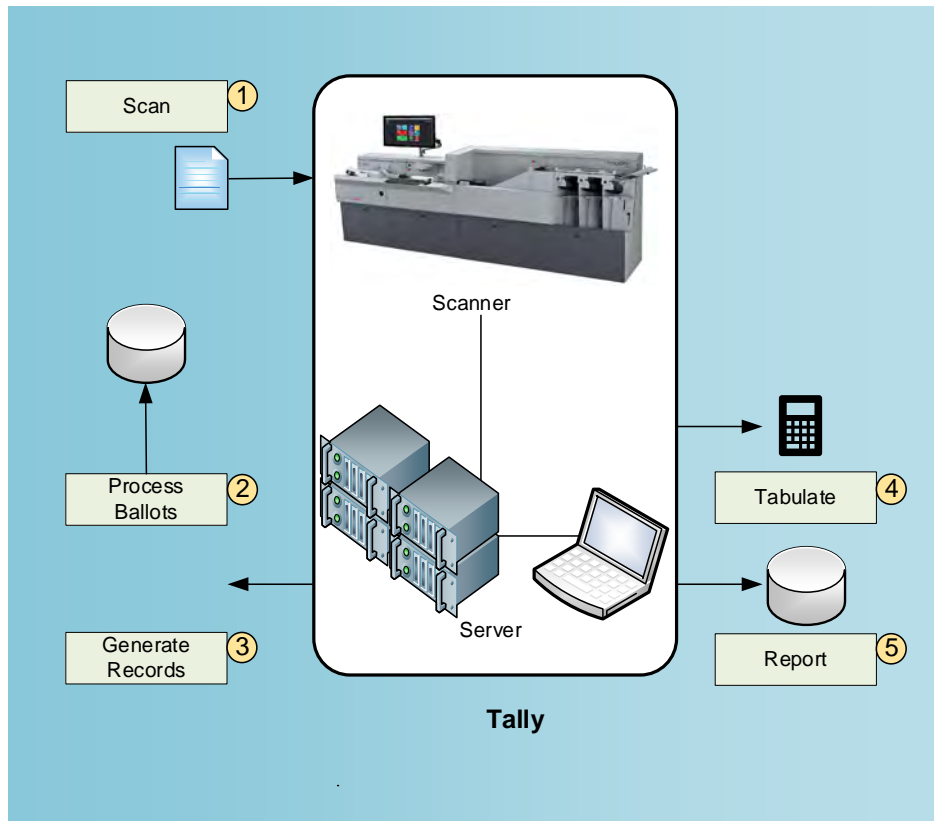
To set up the ISB session, the voter enters either their voter information (last name, date of birth, house number), or address only lookup, allowing the client application to identify the correct precinct and display the appropriate ballot. The voter marks their selections on the sample ballot on their mobile device or personal computer, then reviews their selections. The ISB generates a Poll Pass, which is a QR code representing the selected information. Voter selections can be saved locally on their mobile device for use at the Vote Center to populate their selections onto the BMD via the Poll Pass.

The ISB also enables Remote Accessible Vote by Mail (RAVBM) and Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA).

Each function of the ISB system is described at a high level in the following table:

#	Function Name	Description
1	Build Sample Ballots	Generate data packages for the ISB client application, map precincts to ballot styles, publish ballot files
2	Identify Ballot	The ISB identifies and retrieves the appropriate ballot based on voter information and location
3	Present Sample Ballot	The ISB displays the sample ballot to the voter
4	Mark Sample Ballot	The voter marks their selections on the sample ballot
5	Generate Poll Pass	The ISB generates a QR code with the information about the election, ballot style, and precinct, as well as codes corresponding to the voter selections

2.1.5. Tally Functional Components



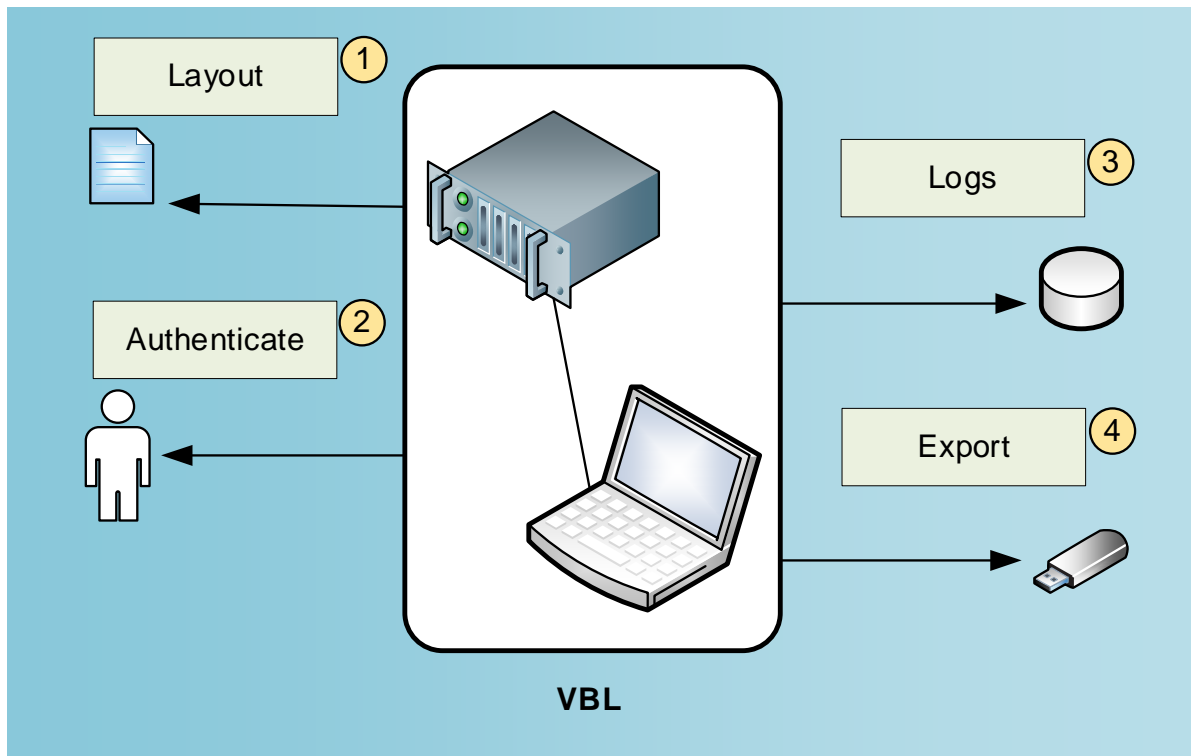
Tally functional components

The Tally system is responsible for capturing and processing ballot images so that voter selections from paper ballots (including BMD, VBM, RAVBM and UOCAVA ballots) may be digitally counted. There are, from the perspective of the software system architecture, four main Tally processes: (1) Ballots are scanned and images captured; (2) ballot images are converted into Cast Vote Records (CVRs); (3) CVRs are tabulated; and (4) Tabulated results are exported for reporting and auditing.

Each function of the Tally system is described at a high level in the following table:

#	Function Name	Description
1	Scan	The scanning process captures a digital image of each paper ballot
2	Process Ballots	Tally processes the ballots to decode voter intent
3	Generate Ballot Record	The processed ballot data is saved as a tabulation-ready record in the database
5	Tabulate	Records in Tally database are refined and counted to determine election results
6	Report Data	The raw vote data produced by the tabulator is copied to an external database used by an external reporting system

2.1.6. VSAP Ballot Layout (VBL) Functional Components



VBL functional components

The VSAP Ballot Layout is an application that enables election managers to configure and generate ballot layouts.

The VBL application supports the logical layout and production of VBM Ballots and election files. These output files provide the rest of VSAP with a definition of the election and ballot layout information. The Auth Service is a standalone authentication service used to manage users, roles, and permissions. The log viewer provides a primary location that consolidates records of critical issues, errors, warnings and other information.

Each function of the VBL system is described at a high level in the following table:

#	Function Name	Description
1	Generate Ballot Layout	The VBL application produces the ballots and election configuration files (aka configuration files)
2	Logs	Events executed by VBL are captured and available for review
3	Export Ballot Layout	The Ballot Layout is exported to receiving subsystems

3. Ballot Definition

3.1. Overview Procedures to Operate Voter Ballot Layout

See the VSAP Ballot Layout User Guide for instructions on how to configure and generate ballot layouts.

3.2. Paper and Printing Specifications

3.2.1. Specifications for Thermal Paper (BMD)


This section provides specific information about thermal paper. Use the specifications below for thermal Paper Grades, Substance GSM and Caliper MM.

<p>SEE TABLE FOR PAPER SPECIFICATION LONG GRAIN ORIENTATION</p> <p>Cambr Consu</p>	<p>OFFICIAL BALLOT General Election</p> <p>2020 Nov. 3</p> <p>County of Los Angeles</p> <p>TYPICAL BALLOT PRE-PRINT CONTENT</p>
<p>SEE TABLE FOR PAPER SPECIFICATION LONG GRAIN ORIENTATION</p> <p>Cambr Consu</p>	<p>OFFICIAL BALLOT General Election</p> <p>2020</p> <p>1.50" — SECURITY WAVE COLOR: OFFICIAL ELECTION TINT (30-40% OPACITY)</p> <p>CALIFORNIA BEAR COLOR: OFFICIAL ELECTION TINT (-10% OPACITY)</p>

1.13" 0.82"

OFFICIAL BALLOT - "OFFICIAL BALLOT": Noto Sans ExtraBold - 24 PT - UPPERCASE
General Election - ELECTION TITLE: Noto Sans Bold - 18 PT

2020
 Nov. 3



County of Los Angeles

TYPICAL STATIC BALLOT HEADER CONTENT
 (Non-Primary, Single-Line Election Title)

OFFICIAL BALLOT
General Election

2020 - ELECTION YEAR: Noto Sans ExtraBold - 48 PT
 Nov. 3 - ELECTION DATE: Noto Sans Bold - 18 PT




County of Los Angeles - COUNTY SEAL: 0.85" diam.
 County of Los Angeles - COUNTY: Noto Sans Black - 10 PT

TYPICAL STATIC BALLOT MARGIN CONTENT

OFFICIAL BALLOT
General Election

2020 0.63" 0.86" 1.62" 2.31"
 Nov. 3



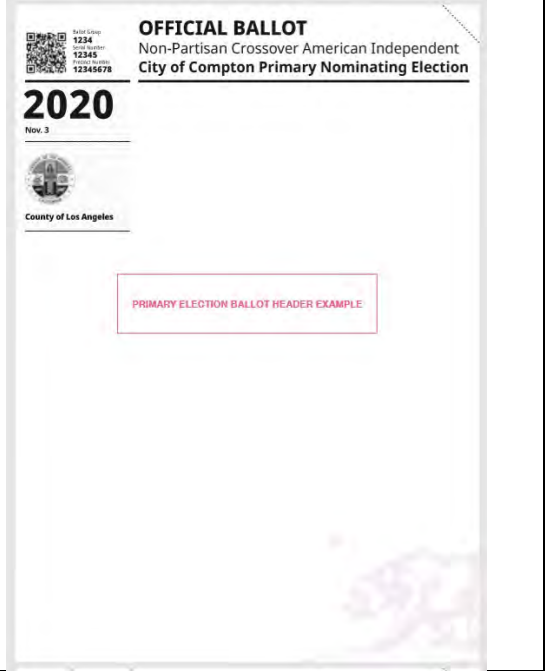
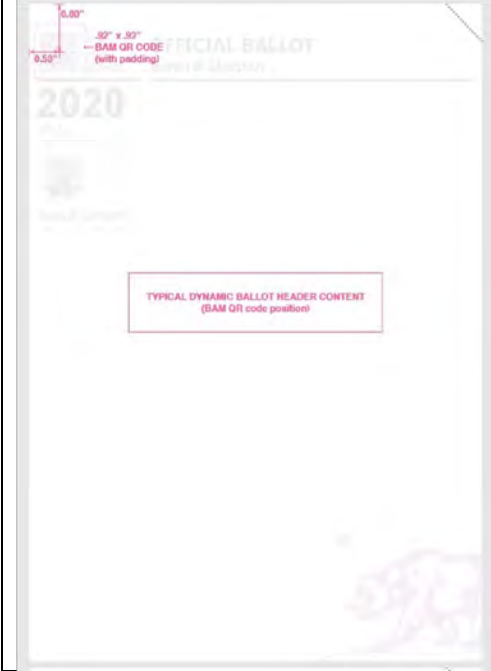
County of Los Angeles

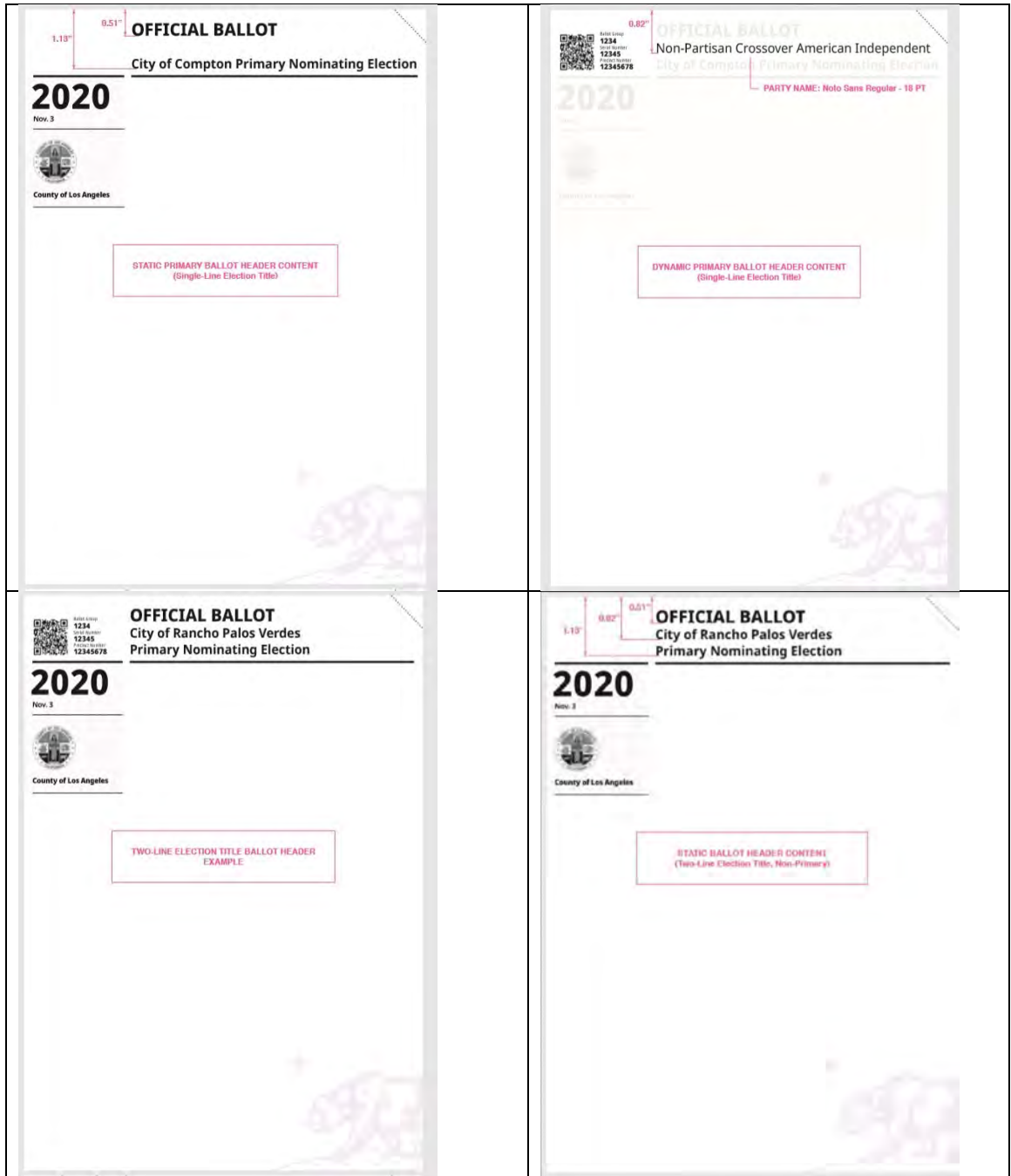
TYPICAL STATIC BALLOT MARGIN CONTENT

SAMPLE



SAMPLE







3.2.2. Specifications for Tally

Before beginning the system setup for Tally, there are two basic setups required: Single Node and Two Node.

3.2.2.1. Single Node

The first required setup is Single Node deployment. The Single Node has two machines, one with a file system and the other is a machine comprised with Tally Node of services, Cassandra database and Kafka. Kafka is used for building real-time data pipelines and streaming applications.

3.2.2.2. Two Node

The second setup requirement is a Two Node deployment, which has three machines:

1. File System - two machines comprising the Tally Node
2. Services
3. Cassandra database (and Kafka)

3.3. Layout Requirements and Specifications

See Section 15 of the VBL User Guide for ballot layout specifications.

4. System Installation and Configuration

4.1. Programming and Configuration of Election Management System

See VBL User Guide.

4.2. Hardware Requirements and Specifications

This section details the hardware components of each subsystem of the VSAP solution.

4.2.1. BMG Hardware Requirements

The following components are used to set up the BMG and server cluster:

BMG Item Name	Manufacturer/ Vendor	Model Number	Software/ Firmware Version	Hardware Version/ Revision	Range, Capacity or Value	Notes
Server Hardware						
NTP Time Server	Meinberg	LANtime M200/GPS				NTP Time Server in compact slimline housing (1x RJ45) GPS Receiver, incl. GPSANT and 20 meters RG58 antenna coax cable and 19" rack mount adapter plate
File Server	NetApp	FAS8200				50 TB data storage
Backup System	Commvault	CN-CV-E-13120-31				12TB raw capacity hyper converged infrastructure

BMG Item Name	Manufacturer/ Vendor	Model Number	Software/ Firmware Version	Hardware Version/ Revision	Range, Capacity or Value	Notes
Server	Hewlett Packard Enterprise	DL380 GEN10 4114				DL380 GEN10 4114 1P 16G 24SFF SVR SB
Workstation Hardware						
Laptop	Dell	Latitude 5400	1.4.2		<ul style="list-style-type: none"> • Intel Core i7 • 8GB Memory • 256GB Solid State Drive 	Trusted Build workstation, client workstation

4.2.2. BMD Hardware Requirements

BMD Item Name	Manufacturer/ Vendor	Model Number	Software/ Firmware Version	Hardware Version/ Revision	Range, Capacity or Value	Notes
System Hardware						
BMD	Smartmatic	BMD-100				Reference: BMD-Parts-List.pdf

4.2.3. ESA Hardware Requirements

ESA Item Name	Manufacturer / Vendor	Model Number	Software/ Firmware Version	Hardware Version/ Revision	Range, Capacity or Value	Notes
Server Hardware						

ESA Item Name	Manufacturer / Vendor	Model Number	Software/ Firmware Version	Hardware Version/ Revision	Range, Capacity or Value	Notes
Server	Intel	NUC7i7DNHE				Small form factor server
HSM	nShield	Edge F2				Hardware Security Module (HSM)
IronKey S1000 USB 3.0 Flash Drive	Kingston	IKS1000B			64GB	Protective metallic form factor

4.2.4. ISB Hardware Requirements

ISB Item Name	Manufacturer/ Vendor	Model Number	Software/ Firmware Version	Hardware Version/ Revision	Range, Capacity or Value	Notes
System Hardware						
Laptop	Dell	Latitude 5400	1.4.2		<ul style="list-style-type: none"> • Intel Core i7 • 8GB Memory • 256GB Solid State Drive 	Client workstation

4.2.5. Tally Hardware Requirements

Tally Item Name	Manufacturer/ Vendor	Model Number	Software/ Firmware Version	Hardware Version/ Revision	Range, Capacity or Value	Notes
Server Hardware						
HPE ProLiant DL360 Gen10 Server	Hewlett Packard	867959-B21			<ul style="list-style-type: none"> • 2x Xeon 4110 (8-core, 16-thread, 2.1 – 3.0 GHz) • 8x 16GB module • SmartArray with 2GB cache • 2x 240GB Read-Intensive SSD for boot • 5x 480GB Read-Intensive SSD RAID5 for DATA • 2port 10g BASE-T FlexLO M 	Reference : HPE ProLiant DL360 Gen10 Server Quick Specs.pdf

Tally Item Name	Manufacturer/ Vendor	Model Number	Software/ Firmware Version	Hardware Version/ Revision	Range, Capacity or Value	Notes
HPE ProLiant DL360 Gen10 Server	Hewlett Packard	867959-B21			<ul style="list-style-type: none"> • 1x Xeon 4110 (8-core, 16-thread, 2.1 – 3.0 GHz) • 4x 16GB module • SmartArray with 2GB cache • 2x 240GB Read-Intensive SSD for boot • 3x 480GB Read-Intensive SSD RAID5 for DATA • 2port 10g BASE-T FlexLOM 	Reference : HPE ProLiant DL360 Gen10 Server Quick Specs.pdf
Hybrid Storage	NETAPP	FAS2750 A-EXP-181			24X1.8TB	Reference : NETAPP FAS270 Hybrid Storage Datasheet.pdf
Workstation Hardware						

Tally Item Name	Manufacturer/ Vendor	Model Number	Software/ Firmware Version	Hardware Version/ Revision	Range, Capacity or Value	Notes
G7 Laptop	Dell	I7588-7385BL K-PUS			<ul style="list-style-type: none"> • Intel Core i7 • 8GB Memory • NVIDIA GeForce GTX 1060 • 256GB Solid State Drive 	Tally workstation laptop
Scanner Hardware						

Tally Item Name	Manufacturer/ Vendor	Model Number	Software/ Firmware Version	Hardware Version/ Revision	Range, Capacity or Value	Notes
HPE ProLiant DL360 Gen10 Server	Hewlett Packard	867959-B21			<ul style="list-style-type: none"> • 1x Xeon 3106 (8-core, 8-thread 1.7 GHz) • 1x 16GB module • SmartArray controller with 2GB cache • 2x 480GB Read-Intensive SSD for boot and MSSQL DB and logs • 4x 1.2 TB 10K SFF SAS drives • 2port 10g BASE-T FlexLOM 	<p>IBML Scanning image file server</p> <p>Reference : HPE ProLiant DL360 Gen10 Server Quick Specs.pdf</p>

Tally Item Name	Manufacturer/ Vendor	Model Number	Software/ Firmware Version	Hardware Version/ Revision	Range, Capacity or Value	Notes
HPE ProLiant DL360 Gen10 Server	Hewlett Packard	867959-B21			<ul style="list-style-type: none"> • 1x Xeon 3106 (8-core, 8-thread 1.7 GHz) • 1x 16GB module • SmartArray controller with 2GB cache • 2x 480GB Read-Intensive SSD for boot and MSSQL DB and logs • 2port 10g BASE-T FlexLOM 	ibml SQ:/Controller server Reference : HPE ProLiant DL360 Gen10 Server Quick Specs.pdf
Document Scanner	Imaging Business Machines, LLC. (IBML)	ImageTrac 6400			<ul style="list-style-type: none"> • 429 ppm 	Reference : ImageTrac Series 6400 features.pdf
Network Hardware						

Tally Item Name	Manufacturer/ Vendor	Model Number	Software/ Firmware Version	Hardware Version/ Revision	Range, Capacity or Value	Notes
Switch	CISCO	N9K-C93180L C-EX			<ul style="list-style-type: none"> • 40-Gb and 50-Gb access connectivity • 40-Gb and 100-Gb uplinks 	Reference Cisco Nexus 9300-EX Series Switches Datasheet. pdf
Fabric Extender	CISCO	N2K-C2348T Q-E				Reference Cisco Nexus 2300 Platform Fabric Extender Datasheet. pdf

4.2.6. VBL Hardware Requirements

VBL Item Name	Manufacturer/ Vendor	Model Number	Software/ Firmware Version	Hardware Version/ Revision	Range, Capacity or Value	Notes
Server Hardware						

VBL Item Name	Manufacturer/ Vendor	Model Number	Software/ Firmware Version	Hardware Version/ Revision	Range, Capacity or Value	Notes
HPE ProLiant DL360 Gen10 Server	Hewlett Packard	867959-B21			<ul style="list-style-type: none"> • 2x Xeon 4110 (8-core, 16-thread, 2.1 – 3.0 GHz) • 4x 16GB module • SmartArray with 2GB cache • 2x 480GB Read-Intensive SSD for boot • 6x 1.92TB Read-Intensive SSD • 2port 10g BASE-T FlexLO M 	Reference HPE ProLiant DL360 Gen10 Server Quick Specs.pdf
Hybrid Storage	NETAPP	FAS2750 A-EXP-181			24X1.8TB	Reference NETAPP FAS270 Hybrid Storage Datasheet.pdf

Workstation Hardware

VBL Item Name	Manufacturer/ Vendor	Model Number	Software/ Firmware Version	Hardware Version/ Revision	Range, Capacity or Value	Notes
G7 Laptop	Dell	I7588-7385BLK-PUS			<ul style="list-style-type: none"> • Intel Core i7 • 8GB Memory • NVIDIA GeForce GTX 1060 256GB Solid State Drive	VBL workstation laptop
Network Hardware						
Switch	CISCO	N9K-C93180L C-EX			<ul style="list-style-type: none"> • 40-Gb and 50-Gb access connectivity • 40-Gb and 100-Gb uplinks 	Reference Cisco Nexus 9300-EX Series Switches Datasheet.pdf
Fabric Extender	CISCO	N2K-C2348T Q-E				Reference Cisco Nexus 2300 Platform Fabric Extender Datasheet.pdf

4.3. Hardware and Network Setup and Configuration

This details the configuration and setup of each component of the VSAP voting system. See the sections below to learn how to set up each component.

4.3.1. BMG Hardware Installation

See VSAP-USG-033 BMG Deployment Guide.

4.3.2. BMD Hardware Installation

The BMD is delivered as a turnkey appliance, with no hardware installation requirements.

4.3.3. ESA Hardware Installation

The ESA consists of an Intel NUC server, the nShield Hardware Security Module (HSM), and a keyboard, mouse, and monitor.

To install the hardware, plug the peripherals and the HSM into the NUC in the appropriate ports. It is an air-gapped system, with no need or ability to connect to a network.

4.3.4. ISB Hardware Installation

ISB is a completely virtualized system running on the AWS cloud service, without any hardware installation requirements.

4.3.5. Tally Hardware Installation

See Tally Build/Installation User Guide.

4.3.6. VBL Hardware Installation

See VBL Build/Installation User Guide.

4.4. Software Installation and Configuration

The setup guides listed below include step-by-step procedures for installing and configuring software on each VSAP component.

Note: Each VSAP system must be reformatted and installed from the certified software after every election.

4.4.1. BMG

See VSAP-USG-033 BMG Deployment Guide.

4.4.2. BMD

See VSAP-USG-003 BMG User Guide for initial file uploads to BMDs.

4.4.3. ESA Hardware Installation

See VSAP-USG-044 ESA Server Build Guide.

4.4.4. ISB

See VSAP-USB-054 ISB Installation Guide.

4.4.5. Tally

See Tally Build/Installation User Guide.

4.4.6. VBL

See VBL Build/Installation User Guide.

4.5. Software and Firmware Upgrades

Upgrades and updates to software and firmware will use the same process as the initial installation. See Section 18.5 Installation Procedures for further details regarding security aspects of upgrades.

Note: Each VSAP system must be reformatted and installed from the certified software after every election.

5. Acceptance Testing

VSAP components must be tested for acceptance through the successful running of the tests specified in the System Test Specification documents. For each component, those documents which detail the tests required to successfully authenticate their acceptance and readiness for use are referenced here.

5.1. Development Test Specifications

See attachments:

- BMD Test Plan.pdf
- BMG Test Plan.pdf
- ISB Test Plan.pdf
- VBL and Tally Test Plan.pdf

5.2. Logic Correctness, Data Quality, and Security

See attachments:

- BMD Test Plan.pdf
- BMD Test Cases.pdf
- BMG Test Plan.pdf
- BMG Test Cases.pdf
- ISB Test Plan.pdf
- ISB Test Cases.pdf
- VBL and Tally Test Plan.pdf
- Tally Test Cases.pdf
- VBL Test Cases.pdf

5.3. Test Identification and Design

See attachments:

- BMD Test Cases.pdf
- BMG Test Cases.pdf
- ISB Test Cases.pdf
- Tally Test Cases.pdf
- VBL Test Cases.pdf

Test	Structure	Sequence or Progression	Conditions
Unit Testing	Unit testing isolates the smallest testable parts of a build. Testing is performed on each module or block of code.	Tests written prior to code. All unit tests are run against the build. All tests need to pass before quality assurance testing.	Metrics are collected and reported at the end of every sprint. At the project level, the metrics are used to identify areas of improvement and address them.
Functional Testing	Functional testing checks all documented functions/requirements of the application/product. Functional testing is conducted by feeding inputs and validating expected outputs against observed outputs from the application.	Unit tests for code low-level modules (can overlap with engineering unit testing). Integration testing with other products. End-to-end functional testing for the overall solution, including input from stakeholders. User experience testing by community stakeholders. A selection of people from different parts of the community will document all issues found and will convert the issues to "defects." Testing will be conducted at the end of Engineering Verification Testing (EVT), Development Verification Testing (DVT), and Production Verification Testing (PVT).	Metrics are collected and reported at the end of every sprint. At the project level, the metrics are used to identify areas of improvement and address them. Some of the metrics gathered are code coverage for unit tests, velocity, burndown, test progress per sprint, and functional breakdown of defects.

<p>System Testing</p>	<p>System integration tests are performed on all components. The test cases will incorporate test scenarios that confirm continuity and accuracy across modules and accommodate testing of files produced by or for external systems.</p>	<p>The tests follow the general assumptions for functional tests. The testers validate the input and output of each test and make sure they align with the requirements/stories. The tests cover software, hardware, and any files consumed. Non-functional tests like performance, compliance, accessibility, security, and design validation are also performed at this level. All issues are reported in Jira as defects. Performance tests in this context include scenarios like average response time on the Get and Post APIs. Security tests at this level will be, for example, secure communication between the different modules. Smoke tests are a predefined set of tests that touch critical features of the system. When a new build is delivered to the test team, smoke testing can quickly give feedback to the testers on the status of the build.</p>	<p>Metrics are collected on an ongoing basis and reported at the end of every sprint. They include defect and sprint summary reports with test/pass numbers. At the project level, the metrics are used to identify areas of improvement; they are also discussed during the sprint retrospective meeting with action items for the following sprint. Metrics gathered at the project level are code coverage for unit tests, velocity and burndown charts, and defects found by severity. Additional metrics can be considered if they help the team with continuous improvement.</p>
------------------------------	---	---	--

<p>Integration Testing</p>	<p>Integration test activities are performed on all the components and results from those tests are reported. The test cases incorporate test scenarios that confirm continuity and accuracy across modules and accommodate testing of files produced by or for external systems.</p>	<p>Verify the functional aspects of the integrated system including hardware, software, and consumables. Verify the compliance of non-functional requirements such as performance targets and security for this level. Report defects found in the integration tests. Identify solution design problems.</p>	<p>Metrics are collected and reported at the end of every sprint. At the project level, the metrics are used to identify areas of improvement and address them. Some of the metrics gathered are code coverage for unit tests, velocity, burndown, test progress per sprint, and functional breakdown of defects.</p>
<p>Hardware/Software Integration Testing</p>	<p>The QA team will verify functional and non-functional requirements of the system using hardware, so that any deviation from the expected behavior is identified to serve as information for possible hardware or software adjustments.</p>	<p>Tests are defined by the QA team and reviewed to ensure they meet VSAP requirements. These reviews are at the end of every sprint or on a schedule established before testing begins.</p>	<p>Defect Summary Report: The defects found in a sprint along with their priority and impact.</p> <p>Sprint Summary Report: Rollup of testing progress for the week, such as the daily report.</p> <p>Daily and weekly Project Level Reports: Determined by the project manager; they may include overall velocity, burndown charts, hot spots, potential problem areas, and/or trending information.</p>

<p>User acceptance Testing</p>	<p>User acceptance tests are performed by the appropriate team using the test suites, test cases, and checklists as well as the information about the required data and environment. Acceptance testing validates that business functions are operating in a manner suited to real-world circumstances and usage. It also gives a chance for stakeholders to review the product before starting production.</p>	<p>Tests are defined by the QA team and reviewed to ensure they meet VSAP requirements. These reviews are at the end of every sprint or on a schedule established before testing begins.</p>	<p>Defect Summary Report: The defects found in a sprint along with their priority and impact.</p> <p>Sprint Summary Report: Rollup of testing progress for the week, like the daily report.</p> <p>Daily and Weekly Project Level Reports: Determined by the project manager; they may include overall velocity, burndown charts, hot spots, potential problem areas, and/or trending information.</p>
---------------------------------------	---	--	---

<p>Pre-certification Testing</p>	<p>This testing is integral to the overall successful development of the VSAP solution. The pre-certification testing encompasses both in- and out-of-scope VSAP components.</p>	<p>The first step of pre-certification testing is to ensure all requirements are accounted for in the development process. Certification specialists will be present at scrum meetings to ensure the CVSS requirements are being considered prior to coding. They participate in code reviews to ensure proper coding conventions are adhered to.</p> <p>During the EVT and DVT stages, State-Approved Testing Agency (S-ATA) resources are integrated into the QA teams. As builds are completed, they are verified by the compliance team, and copies of the build are provided to the S-ATA for review.</p>	<p>As builds are completed, they are verified by the compliance team, and copies of the build are provided to the S-ATA for review.</p>
<p>Non-functional Testing</p>	<p>Non-functional testing is performed to check non-functional requirements of the application/product. This testing is conducted by validating expected outputs against observed outputs from the application.</p>	<p>Performance testing Usability testing</p>	<p>As builds are completed, they are verified by the compliance team, and copies of the build are provided to the S-ATA for review.</p>

5.4. Standard and Special Purpose Test Procedures

Attachments

- BMD Test Cases.pdf
- BMG Test Cases.pdf
- ESA Test Cases.pdf
- ISB Test Cases.pdf
- Tally Test Cases.pdf
- VBL Test Cases.pdf

5.5. Test Details

Test	Test Data (Source, Real or Simulated, Controls)	Expected Results	Evaluation Criteria
Unit Testing	Source: Software specific Type: Simulated Controls: User defined	<ul style="list-style-type: none"> • Verify the functional aspects of the integrated system including hardware, software, and consumables • Verify the compliance of non-functional requirements such as performance targets and security for this level • Report defects • Identify solution design problems 	<ul style="list-style-type: none"> • Planning phase is completed • System design, technical design, and other relevant documents are properly reviewed, analyzed, and approved • Business and functional requirements are defined and approved • Testable codes or units are available • Test environment is available
Functional Testing	Source: Software specific Type: Real Controls: User defined	<ul style="list-style-type: none"> • Verify the functional aspects of the integrated system including hardware, software, and consumables • Verify the compliance of non-functional requirements such as performance targets and security for this level • Report defects • Identify solution design problems 	<ul style="list-style-type: none"> • Unit testing phase is complete • Priority bugs found during unit testing have been fixed and closed • Integration plan and test environment to carry out integration testing are ready • Unit testing for each module is complete

<p>System Testing</p>	<p>Source: Software specific</p> <p>Type: Real</p> <p>Controls: User defined</p>	<ul style="list-style-type: none"> • Verify the functional aspects of the integrated system including hardware, software, and consumables • Verify the compliance of non-functional requirements such as performance targets and security for this level • Report defects • Identify solution design problems 	<ul style="list-style-type: none"> • Integration testing completed successfully • Priority bugs found during previous testing activities are fixed and closed • The system testing environment is available • Test cases are available to execute
<p>Integration Testing</p>	<p>Source: Software specific</p> <p>Type: Real</p> <p>Controls: User defined</p>	<ul style="list-style-type: none"> • Verify the functional aspects of the integrated system including hardware, software, and consumables • Verify the compliance of non-functional requirements such as performance targets and security for this level • Report defects • Identify solution design problems 	<ul style="list-style-type: none"> • Stress, performance, and load tests have executed satisfactorily • Priority bugs are fixed and closed
<p>Hardware/Software Integration Testing</p>	<p>Source: Software specific</p> <p>Type: Real</p> <p>Controls: User defined</p>	<ul style="list-style-type: none"> • Verify the functional aspects of the integrated system including hardware, software, and consumables • Verify the compliance of non-functional requirements such as performance targets and security for this level • Report defects • Identify solution design problems 	<ul style="list-style-type: none"> • Stress, performance, and load tests have executed satisfactorily • Priority bugs are fixed and closed

<p>User acceptance testing</p>	<p>Source: Software specific</p> <p>Type: Real</p> <p>Controls: User defined</p>	<ul style="list-style-type: none"> • Verify the functional aspects of the integrated system including hardware, software, and consumables • Verify the compliance of non-functional requirements such as performance targets and security for this level • Report defects • Identify solution design problems 	<ul style="list-style-type: none"> • The user acceptance tests have executed successfully • Management has approved user acceptance testing completion • Business requirements are fulfilled • No critical defects are remaining • Acceptance testing signed off
<p>Pre-certification testing</p>	<p>Source: Software specific</p> <p>Type: Real</p> <p>Controls: User defined</p>	<ul style="list-style-type: none"> • Verify the functional aspects of the integrated system including hardware, software, and consumables • Verify the compliance of non-functional requirements such as performance targets and security for this level • Report defects • Identify solution design problems 	<ul style="list-style-type: none"> • Hardware and software received. • TDP documentation completed • User and installation guides completed • User defined procedures followed

Non-functional testing	Source: Software specific Type: Real Controls: User defined	<ul style="list-style-type: none"> • Verify the functional aspects of the integrated system including hardware, software, and consumables • Verify the compliance of non-functional requirements such as performance targets and security for this level • Report defects • Identify solution design problems 	User defined
------------------------	--	---	--------------

Please see VSAP-CMP-001 Configuration Management Plan for further details about tests.

5.5.1. Test Specifications

5.5.1.1. Specifications

Procedures for the verification and validation of overall software performance have been based on CVSS requirements and are included in the test cases. These tests provide procedures for assessing and demonstrating the suitability of the software for election use.

5.5.1.2. Control and Data Input/Output

As multiple features/functions are combined to simulate an election, testing is performed on those sets of features and functions with a set of steps and procedures. The data entry process is defined by the "Steps" section listed for each test case.

5.5.1.3. Acceptance Criteria

The features/functions under test are known before the start of the election and are integrated into the design of the test. When the test is performed, these features/functions are examined and must meet the expected results described in each test case.

5.5.1.4. Processing Accuracy

Every feature and function tested must meet acceptance criteria as described in each test case.

5.5.1.5. Data Quality Assessment and Maintenance

Data quality and accuracy is measured by determining the expected results of the simulation before any voting is performed. Test results are inspected to ensure they match the expected outcome for the specific input. The data is always within the boundaries of the election system, so any maintenance is inherent in the assessment of data quality.

5.5.1.6. Ballot Interpretation Logic

Ballot interpretation logic is defined before the start of the test. The results of the voting and the response of the system to the voting variations are then known beforehand and listed in the "Expected Results" section of test cases.

5.5.1.7. Exception Handling

Exception handling is verified using the test cases that check for correct handling of exceptions. These test cases represent Error or Exception Handling test scenarios, or the exception handling addressed in individual test cases if the possible exceptions are within scope.

5.5.1.8. Security

Security is an overall functionality tested independently of voting variations. The security aspects are tested within individual test cases.

5.5.1.9. Production of Audit Trails and Statistical Data

Statistical data in the form of election results may be used for determining accuracy and data quality. In each election test, all election test results are produced and examined. Audit trail production is an overall functionality that can be tested independently of voting variations. The election results or statistical data tests steps are addressed in an individual test if the tabulation of results are within scope.

5.5.1.10. Procedures for Assessing Suitability for Election Use

Suitability for election use is controlled by the CVSS. All equipment, hardware, and software are assessed and only items that meet the requirements are employed in the VSAP system. This

determination is developed via the design and architecture documentation for each sub-system where requirements are outlined and component selection is controlled, and the requirements are analyzed by the corresponding conformity matrices. Please see attachments:

Attachments

- BMD Software Architecture Document.pdf
- BMD Software Design Document.pdf
- BMD Test Cases.pdf
- BMD Test Plan.pdf
- BMG Software Architecture Document.pdf
- BMG Software Design Document.pdf
- BMG Test Cases.pdf
- BMG Test Plan.pdf
- Designing and Using the BMD.pdf
- ESA Security Architecture.pdf
- ISB Software Architecture Document.pdf
- ISB Software Design Document.pdf
- ISB Test Cases.pdf
- ISB Test Plan.pdf
- Tally and VBL Software Design and Specification.pdf
- Tally and VBL Software Functional Specification.pdf
- Tally Test Cases.pdf
- VBL and Tally Test Plan.pdf
- VBL Test Cases.pdf

6. Election Setup and Definition

6.1. Programming and Configuration of Vote Recording Tabulation Device – Tally

This section provides instructions for a production deployment of Tally. Color conventions to keep in mind with Terminal Code:

- White/Gray - The command to run in the terminal. Run one line at a time
- Turquoise - The output of the command where applicable to display
- Red - String/Text these values are variable depending on your own server equipment
- Green - Comments

6.1.1. General Prerequisites

To complete the offline deployment, the following items are necessary:

- Collection of machines to install Tally
- Install media for CentOS 7.6.1810
- Access to the following VSAP repositories: installer, tally-core, auth-service, and logviewerservice
- Golang 1.12.4 for Linux AMD64 (from <https://golang.org/dl/>)
- Access to VSAP Azure container registry
- Build system: a system from which it is possible to clone Git repos to and build the Docker images
- Deployment system: a second system on the air-gapped network in which the pre-built distribution package can be run to build the cluster

Two users are needed to complete the installation of Tally:

- “user” will reference the user created during CentOS configuration
- “ssh-user” will reference the user that has been granted ssh access to all nodes in the cluster This readme is made up of the following sections:
 - Building Distribution Kit
 - Preparing Tally Nodes
 - Getting Nodes Ready for the Main Installer
 - Main Installer
 - Starting Tally
 - Viewing Tally
 - Stopping Tally
 - Other Helpful Commands

6.1.2. Building Distribution Kit

The following is required before moving the repositories to the Tally machines:

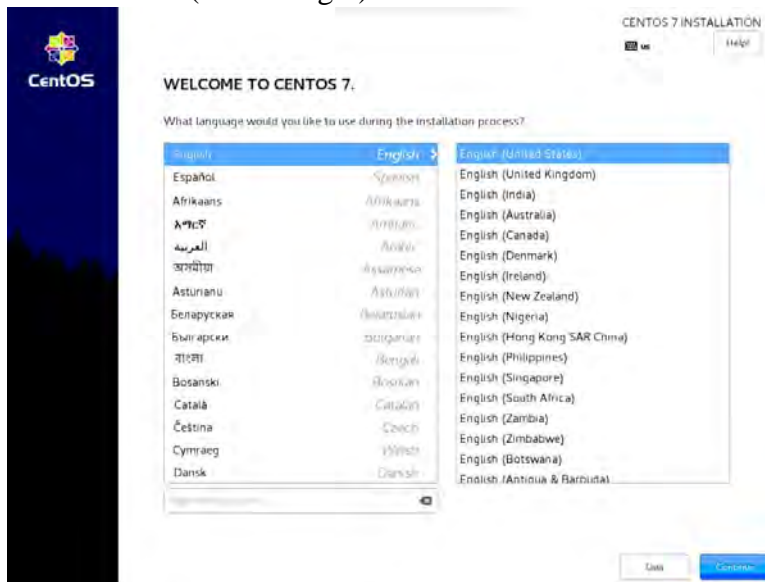
- Install minimal CentOS 7.6.1810 to the Tally machines
- Clone Tally Repositories
- Build Docker Images
- Download Golang
- Move Go to VSAP Directory and Create Bundle

6.1.3. Install minimal CentOS

All machines must be running CentOS 7.6.1810 with the minimal installer option and the "file and storage server" selection.

A USB flash drive or CD will contain the minimal CentOS 7.6.1810 ready for install. To do so follow these steps:

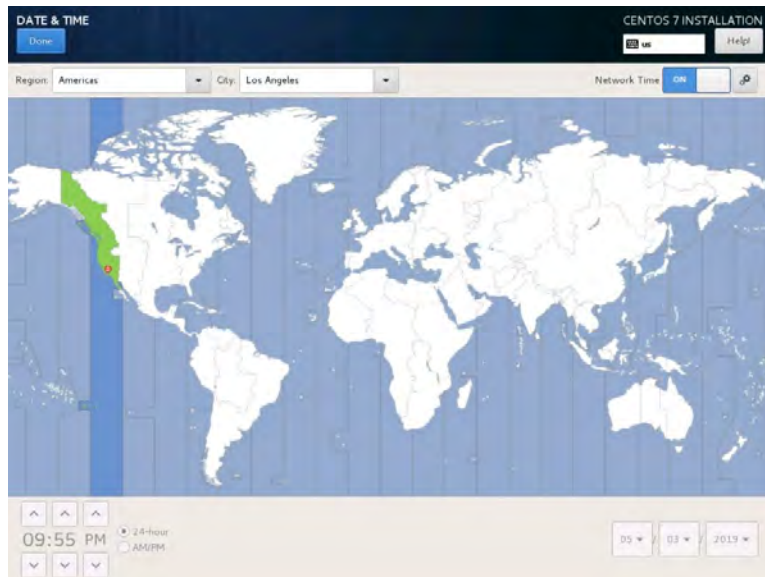
1. Plug in the USB flash drive or CD
2. Look up instructions to get to the Quick Boot menu for the specific machine
3. Select EFI Boot drive for the flash drive
4. Select "Install CentOS 7"
5. Select English > English (United States)
 - a. Click "Continue" (bottom right)



6. Select "Date & Time"

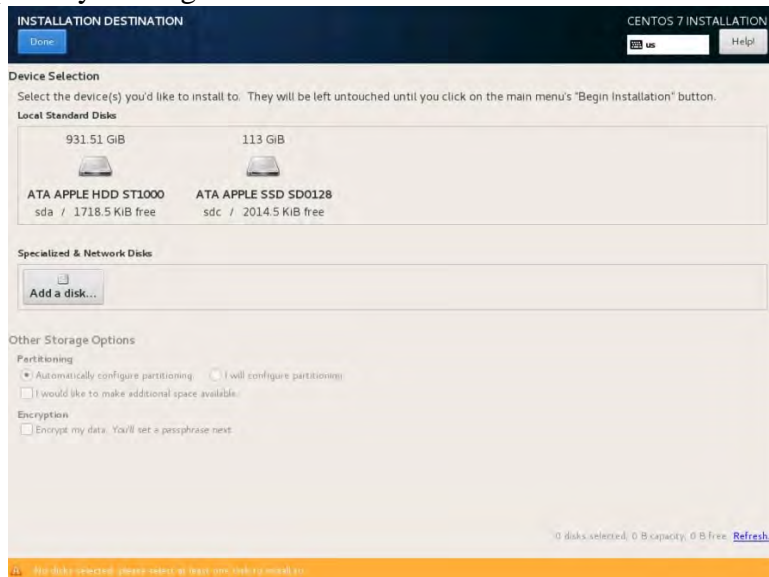


7. Select Los Angeles on the map



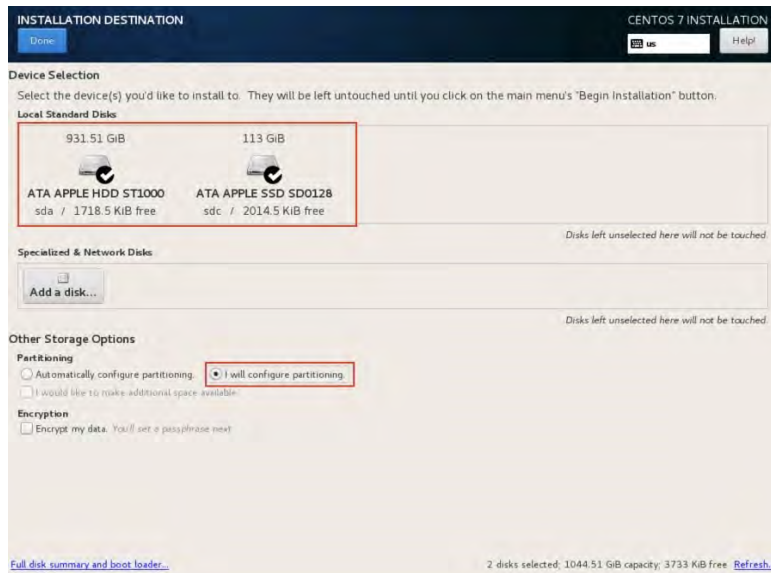
8. Click "Done" (top left)

9. From the primary menu go to "Installation Destination"



10. Select all disks in "Local Standard Disks"

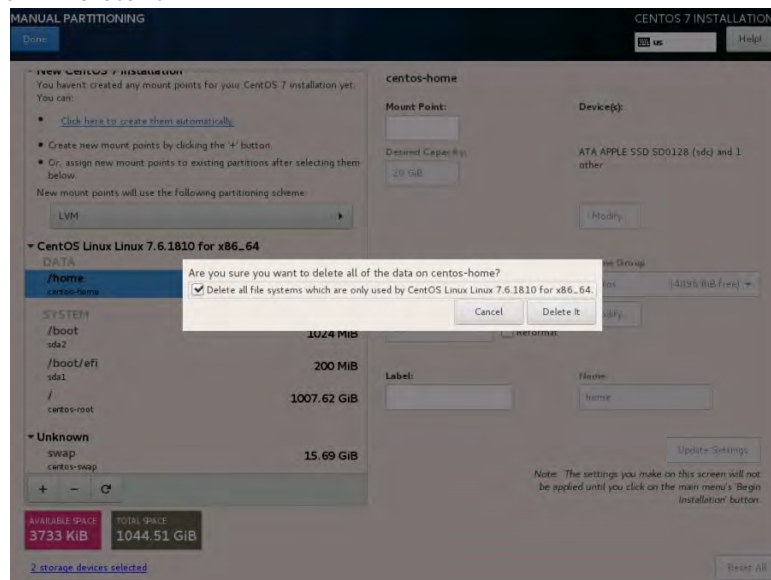
11. Check "I will configure partitioning" in "Other Storage Options"



12. Click "Done" (top left)

13. (Skip if fresh install on new machine) Delete any existing groups of partitions (e.g. CentOS Linux 7.6.1810 for x86_64 OR Unknown)

- a. Open each dropdown
- b. Select the minus button (near the bottom left)
- c. Check "Delete all file systems..."
- d. Click "Delete it"

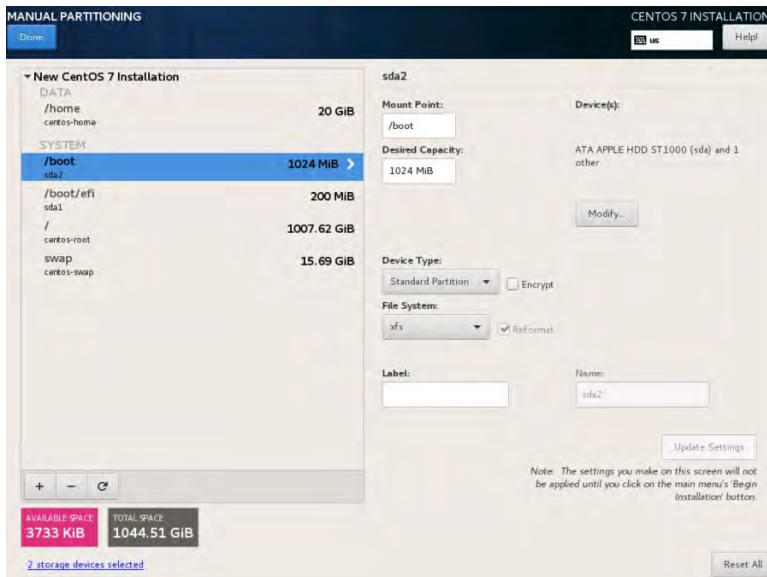


14. Repeat (if necessary)

15. Select option 'Click here to create them automatically'

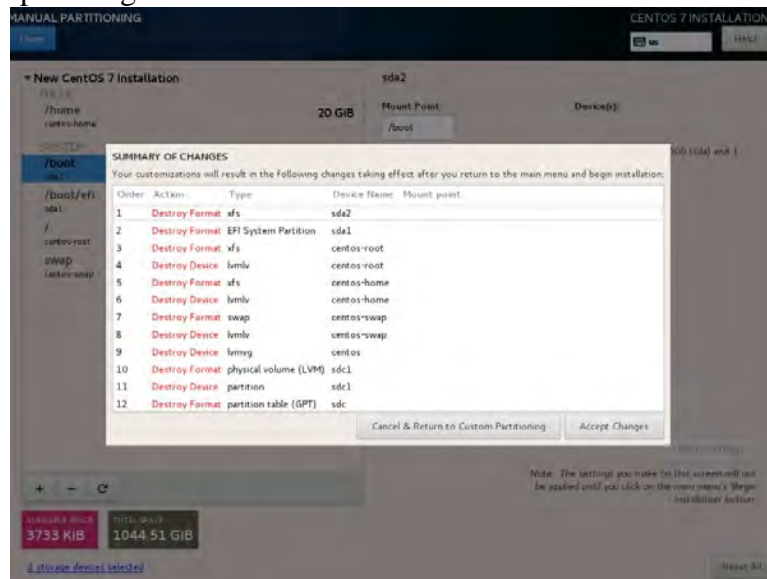
16. Set /home capacity to be about 3% of total storage

17. Delete any storage entered in /(centos-root). This will allocate all remaining available space to /



18. Click "Done" (top left)

19. Click "Accept Changes"

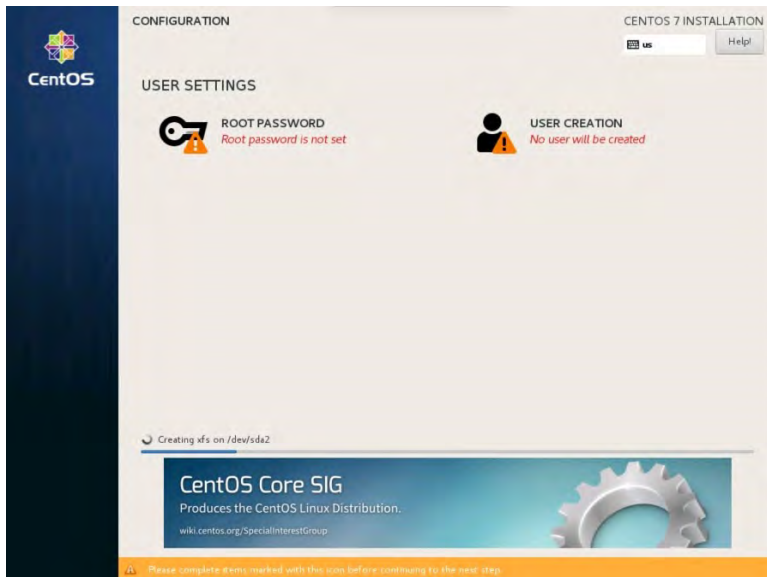


20. Select "Network & Host Name"

- a. Set Host name (e.g. lac-df-master1) (bottom left)
- b. Click "Apply"
- c. Plug in the network cable to the system
- d. Choose the network interface on the left-hand list. If there are multiple network interfaces in the system, choose the one that is not listed as "unplugged"
- e. Toggle on Ethernet (top right)
- f. Click on [Configure...] to configure static IP address
- g. Click "Apply"
- h. Click "Done" (top left)

21. Check that "Software Selection" is set to "Minimal Install"

22. Click "Begin Installation" (bottom right)

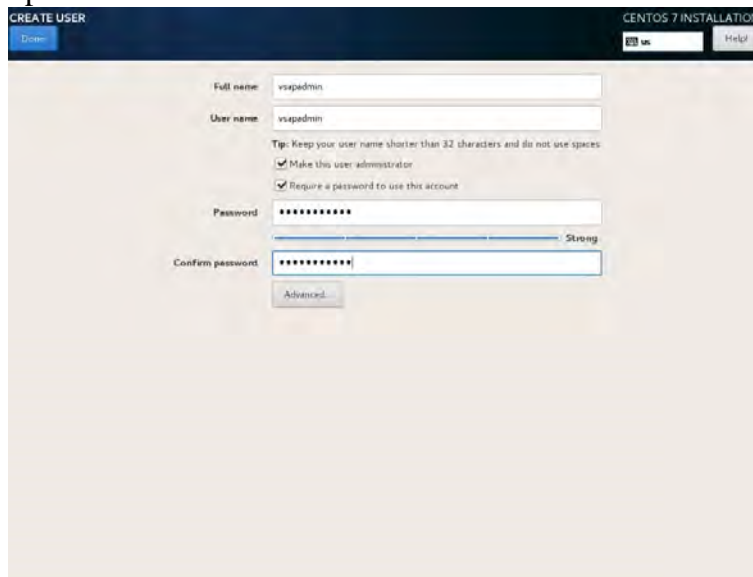


23. Select "Root Password"

- a. Set root password and confirm it
- b. Click "Done" (top left)

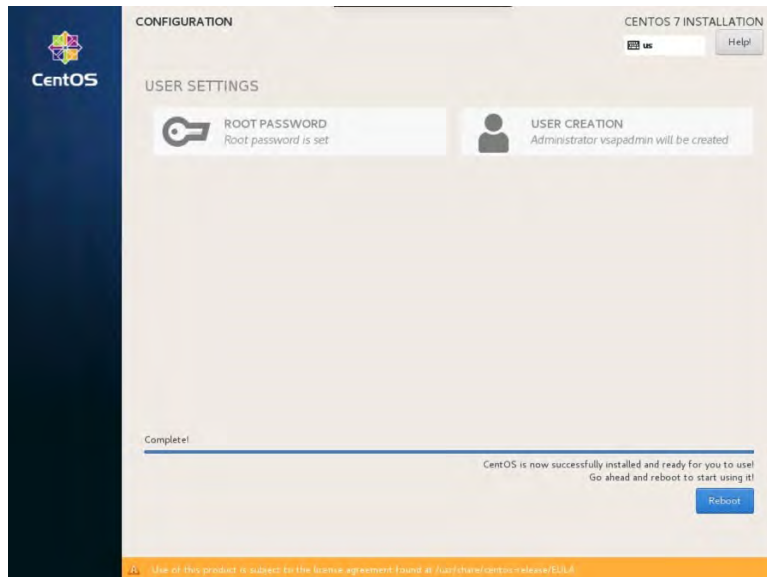
24. Select "User Creation"

- a. Enter Full Name
- b. Enter username
- c. Check both 'Make this user admin' and 'Require a password to use this account'
- d. Set a password and confirm it



25. Click "Done" (top left)

26. Once installation is complete (this may take a few minutes), click the "Reboot" button (bottom right)



6.1.3.1. Clone Tally Repos

Once Go has been downloaded, you will need to clone the Tally repos. Once the Tally repos have been cloned both Go and the repos will be moved over to the deployment system. To clone the Tally repos run the following commands from the build system:

```
mkdir -p /tmp/go/src/bitbucket.org/
export GOPATH=/tmp/gocd /tmp/go/src/bitbucket.org/
mkdir vsap
cd $_
# clone the tally repositories
git clone git@bitbucket.org:vsap/installer.git
git clone git@bitbucket.org:vsap/tally-core.git
#currently takes ~ 50 min
git clone git@bitbucket.org:vsap/auth-service.git
git clone git@bitbucket.org:vsap/logviewer-service.git
# Download resources from Git LFS
cd tally-core
gitlfs pull
cd ../installer
git lfs pull
```

6.1.3.2. Build Docker Images

Once the repos have successfully been cloned, the next step is to provide to build the images on the build system.

Prior to initiating the build, the user must have installed and logged in to Microsoft's Azure service.

```
# login to azure. This command only needs to be run once per system build.
```

```
az login
```

```
# login to the vsap acr. This needs to be run every time we build images.
```

Note: This cannot be done through BlueCoat: lac users must use a system with a BlueCoat bypass.

```
az acr login --name vsapacr
```

```
# begin building the images
```

```
go run
```

```
/tmp/go/src/bitbucket.org/vsap/installer/cmd/tally/build_deployment/main.go -d
```

```
# enter project directory values for each prompt
```

```
Enter the tally-core project directory
```

```
Enter a value: ../tally-core
```

```
Enter the auth-service project directory
```

```
Enter a value: ../auth-service
```

```
Enter the auth-service project directory
```

```
Enter a value: ../logviewer-service
```

After entering the directories, the docker images will be built. This will take upwards of 30 minutes to complete.

6.1.3.3. Download Golang

The deployment system requires that Golang 1.12.4 for Linux AMD64 be installed prior to running the installer script.

Start from the build system. Download the Go Linux package from <https://golang.org/dl/>. If not readily available, check the Archived versions which are towards the bottom of the page.

6.1.3.4. Move Go to VSAP Directory and Create Bundle

Once the images have been built, move the downloaded Go package to the VSAP directory, so they can be bundled together.

Run the following commands from the build system:

```
# copy Go to the directory the repos were cloned into.
```

```
cd ~/directory Go was downloaded into
```

```
cp go1.12.4.linux-amd64.tar.gz /tmp/go/src/bitbucket.org/vsap
```

```
cd /tmp/go/src/bitbucket.org/
```

```
# tar the vsap bundle
```

```
tar -czf vsap.tar.gz --exclude .git vsap
```


6.1.4. Preparing Tally Nodes

Once the Distribution Kit has been built, the remaining Tally nodes need to be setup. To setup the Tally nodes the following steps need to be taken:

- Install minimal CentOS (these are the same instructions used in the first section)
- SSH User Generation

6.1.4.1. SSH User Generation

All machines should be set up with a user with an SSH authorized key, owned by the user doing the install on the deployment system. This will allow password-less login to the node systems during the install process.

To create a new ssh user with an authorized key, first create a new ssh key from the deployment system on the user that will be running the installer. Run the following commands and *leave all response fields empty*.

```
# generate ssh key from the deployment system
ssh-keygen -C "add comment to identify key"
# copy the ssh public key to the other nodes
scp ~/.ssh/id_rsa.pub user@node-ipaddress:/tmp/masteruser.pub
# repeat for each Tally machine
# replace this string in the next command with the username you are
trying to create (e.g. tallyadmin2)
NEW_USER="newusername"
# the user in the following command is the user created during the
CentOS setup
SSH_KEY="/user/.ssh/id_rsa.pub"
# add a new user
sudo useradd -m ${NEW_USER} -G wheel
# set ssh configurations
sudo mkdir -m 0700 /home/${NEW_USER}/.ssh
# ssh is being set to the contents
sudo sh -c "cat ${SSH_KEY} >>
/home/${NEW_USER}/.ssh/authorized_keys"
sudo chown -R ${NEW_USER}:${NEW_USER} /home/${NEW_USER}/.ssh
sudo chmod 600 /home/${NEW_USER}/.ssh/authorized_keys
# allow passwordless ssh
sudo sed -i '/NOPASSWD:\sALL/c%wheel ALL=(ALL) NOPASSWD: ALL'
/etc/sudoers
```

Once this has been done for the deployment system, it will need to be done for each Tally machine running the following commands:

```
# ssh to a Tally machine from the deployment system
```

```

ssh user@node-ip-address

# replace this string with the username you are trying to create (e.g.
tallyadmin2)

NEW_USER="new-username" # replace this string with the ssh public key
copied from the previous step

SSH_KEY="/tmp/masteruser.pub" # add a new user

sudo useradd -m

${NEW_USER} -G wheel # set ssh configurations

sudo mkdir -m 0700 /home/${NEW_USER}/.ssh

# ssh is being set to the contents

sudo sh -c "cat ${SSH_KEY} >>
/home/${NEW_USER}/.ssh/authorized_keys"

sudo chown -R ${NEW_USER}:${NEW_USER} /home/${NEW_USER}/.ssh sudo
chmod 600 /home/${NEW_USER}/.ssh/authorized_keys

# allow passwordless ssh

sudo sed -i '/NOPASSWD:\sALL/c%wheel ALL=(ALL) NOPASSWD: ALL'
/etc/sudoers

# repeat for each Tally machine

```

6.1.5. Getting Nodes Ready for the Main Installer

Once the images have been built, everything necessary to run the installer will be ready to move to the deployment system. The following sections describe getting the images on the deployment system and installing Go.

6.1.5.1. Move VSAP Directory to Deployment System

Next, create the project structure on the deployment system and then create a \$GOPATH at /go

```

# create the project structure

sudo mkdir -p /go/src/bitbucket.org/

# untar the VSAP bundle

sudo tar -C /go/src/bitbucket.org/ -xzf /tmp/vsap.tar.gz

# grant permissions for Go path

sudo chmod -R 0777 /go

# unbundle the Go tar

sudo tar -C /usr/local -xzf
/go/src/bitbucket.org/vsap/go1.12.4.linuxamd64.tar.gz

echo 'export PATH=$PATH:/usr/local/go/bin' >> ~/.bashrc

# creating the `GOPATH`

echo 'export GOPATH=/go' >> ~/.bashrc

```

Apply the configurations and test the Go install:

```
source ~/.bashrc # test the go installation
```

```
go version
go version go1.12.4 linux/amd64
```

6.1.5.2. Move VSAP Directory to Other Nodes

The previous step copied the VSAP directory to the primary master node. Next the VSAP bundle needs to be copied to all remaining provider and compute nodes. Additional master nodes do not require the VSAP directory.

```
# copy the vsap directory into every other Tally machine
scp /tmp/vsap.tar.gz user@compute-node-ip-address:/tmp
scp /tmp/vsap.tar.gz user@provider-node-ip-address:/tmp
# once the VSAP directory has been copied to every machine, run the
next command
# ssh to a node
ssh user@node-ip-address
# unbundle the VSAP directory
sudo tar -C /mnt -xzf /tmp/vsap.tar.gz
# go back to the deployment system
exit
# repeat for every node
```

Once the project resources are in the right place, we can begin the Kubernetes installer script.

6.1.6. Main Installer

This section covers the main installation process for Tally. It can be executed either as a step-by-step walkthrough or by command flags. For new users, the step-by-step mode is recommended.

```
# go into the installer directory on the deployment system
cd /go/src/bitbucket.org/vsap/installer
# to run the installer, ssh-user is a user that has been granted ssh
access to all nodes in the cluster. To run the command in step-by-step
mode, omit flags.
go run cmd/tally/installer/main.go ssh-user flags
```

6.1.6.1. Configuration

When the main installer starts, it will require the user to specify the nodes that will be included in the cluster, as well as their type.

The first node to be setup will be the deployment system. The deployment system configuration cannot be changed once in the current version of the installer, so double check the entered values before submitting the information. Also, the first node is where HA proxy is deployed and will be the entry point for Tally through the web browser.

```
# enter the deployment system hostname
Enter the hostname configured for this master system
Enter a value: deployment-systemhostname
Enter the ip address configured for this master system
```

Enter a value: deploymentsystem-ip-address

Below is an example configuration once the first master system has been setup:

Node Type	Hostname	IP
MASTER	lac-df-master1	10.0.5.151

Next you will have the option to: 1) Enter a new node, 2) Remove an existing node, 3) Finished. If the only node that has been setup is the deployment node, you will not be able to remove an existing node. Entering a new node will lead to a multi-node cluster and finishing the setup will lead to a single-node cluster.

On a multi-node cluster, it is mandatory to set at least one:

- Master node
- Compute node
- Provider node
- File node

If a dedicated file node does not exist, you can assign the same hostname and IP address as a compute node. This is true for other types of nodes, but a minimum of three nodes is recommended for a multi-node cluster.

What type of node is this?

master (m), compute (c), provider (p), file (f)

Enter a value:

Below is an example of a valid multi-node cluster setup, which appears once you finish the setup:

Node Type	Hostname	IP
MASTER*	lac-df-master1	10.0.5.151
COMPUTE	lac-df-computel	10.0.5.161
PROVIDER	lac-df-provider1	10.0.5.171
FILE	lac-df-computel	10.0.5.161

* = This node (the first master node)

The output above will be paired with the following prompt:

The above are the nodes that you have configured, is this correct?
(y/n)

Enter a value:

Entering 'y' will end the configuration and proceed to the next step in the installer. Entering 'n' will allow you to make changes to the configuration. As a reminder, the only node that cannot be modified is the first master system.

The last step in node configuration is to name the configuration:

```
What is the name of this cluster?
```

```
Enter a value:
```

Keep track of the name you use for the cluster. If the installation is interrupted past this prompt, you will need to input the name to continue with the installation of Tally. Otherwise, you will need to redo the node configuration.

This command will take some time to complete. If this process is interrupted (e.g. machine goes to sleep) it will be set to a bad state, and you will need to reset the machines and start over.

6.1.6.2. Initializing Kubernetes Cluster

After the node configuration is complete, the next step will be to initialize the cluster. The next prompt will be to restart the machines in the cluster:

```
Compiling node resources requires that you restart the machines in the cluster, are you sure you want to proceed? (y/n)
```

```
Enter a value:
```

Entering 'y' will continue with the installation. Entering 'n' will exit out of the installation. This step will take some time.

After the machines are rebooted, you will need to rerun the installer command from the deployment system to continue the installation process from where you left off.

```
# ssh to the deployment system
ssh user@deployment-system-ip-address
# go into the installer directory
cd /go/src/bitbucket.org/vsap/installer
# rerun the installer command
go run cmd/tally/installer/main.go
ssh-user flags
# continue the installation from where it left off
```

```
It looks like you're starting from a node where pre-restart has already been run. Would you like to continue from a saved cluster? (y/n)
```

```
Enter a value:
```

Entering 'y' will then prompt for the name of the configuration cluster set at the end of node configuration. If the name matches a saved configuration, the cluster node configuration will appear to allow for you to review before continuing. Entering 'n' will restart the node configuration.

6.1.6.3. Creating Docker Registry

The next step in the installation process will be to create a username and password for the Docker registry. Keep track of the username and password you enter, since it will be required later in the installation.

Configuring private docker registry specifications...

Username for the Docker registry

Enter a value: Enter the password to create for the docker registry

Confirm docker registry password

You will need to enter the password for the docker registry twice.

6.1.7. Starting Tally

Once the cluster and its various nodes have been set up and Docker images have been built, the Tally system can be started by running the `create_all` command.

To do this, run the following based on whether the installation is for single or multi node deployment:

```
# run for a single-node deployment:
```

```
go run cmd/tally/create_all/main.go deployment-systemhostname -k
```

```
# run for a multi-node deployment:
```

```
go run cmd/tally/create_all/main.go deployment-system-hostname file-  
node-hostname -m -k
```

The `[deployment-system-hostname]` can be referenced in the example configuration output. This will compile template files for the tally system into `.yaml` files to create Kubernetes pods. This process includes 2 flags: `--multinode` and `--kube-create`.

`-m --multinode` indicates that the cluster being used is multinode. Setting this flag indicates that you must also pass the `[file host]`, which is the hostname of the file node.

`-k --kube-create` indicates that the process should also create kubernetes pods based on the compiled `.yaml` files, which will start the Tally system.

Regardless of deployment type, the system may take several minutes to start. To check the status of the pods as they spin up, run `kubectl get pods -n tally`.

When the system is ready, the `tallymanager-deployment` pod will have a status of "Running." On first run, the system may take longer to spin up; if `tallymanager` is unable to reach `cassandra` and/or `kafka`, delete the `tallymanager-deployment` pod and it should automatically restart.

6.1.8. Viewing Tally

On any machines meant to access tally, the accepted hostnames must be mapped to the IPs of the cluster nodes.

To do this, modify `/etc/hosts` (or `C:\Windows\System32\Drivers\etc\hosts` on Windows) to include the hostnames and IP addresses of the deployment system from which Tally was installed. It should be in this format:

```
10.166.135.84 rrcc58607
```

Once the hostname has been mapped, go to a new browser window and navigate to:

<https://deployment-system-hostname:30069/logout> (example: <https://rrcc58607:30069/logout>)

6.1.9. Stopping Tally

There are known issues with the functionality to Stop Tally. This section should be avoided for now. To stop the tally system and delete running services, run the following command:

```
go run cmd/tally/delete/main.go
```

from this installer project root. This will delete all resources generated by files found in the configuration dist directory.

Note: Running this program will clear the MySQL state database.

To check that all resources have been deleted, run the following command:

```
kubectl get all -n tally
```

6.1.10. Other Helpful Commands

6.1.10.1. Set Desired Hostnames

Before beginning installation, ensure that all nodes are set to their desired hostnames and IP addresses.

6.1.10.2. Checking Hostnames

To verify the hostnames of the Tally machines, you can run the following command from each Tally machine:

```
hostname
```

6.1.10.3. Changing Hostnames

If the hostname needs to be changed, it should be reset from each Tally machine with the command:

```
sudo hostnamectl set-hostname desired-hostname
```

6.1.10.4. Configuring IP addresses

Configure the IP address for each Tally machine. Start with the deployment system:

```
sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Once the file has opened, modify the contents to configure the system for your network. Below is an example configuration used on a simple air gapped network:

```
TYPE=Ethernet
BOOTPROTO=none
DEFROUTE=yes
NAME=eth0UUID=0e1b359c-ab0e-4f66abea-095a74c7074a
DEVICE=eth0
ONBOOT=yes
IPADDR=192.168.1.100
GATEWAY=192.168.1.100
NETMASK=255.255.255.0
ZONE=public
```

Below are more detailed instructions for configuring the IP address:

1. Login with the user setup during CentOS installation
2. `run sudo vi /etc/sysconfig/network-scripts/ifcfg-`
 - a. Press <tab> to get the remainder of the name
 - b. Add that back to the command and run it
3. Enter password configured during CentOS installation
4. Using the arrow keys navigate down to `BOOTPROTO=dhcp`
 - a. Replace **dhcp** with **none** (`BOOTPROTO=none`)
 - b. Navigate to `ONBOOT`
 - c. Replace **no** with **yes** (`ONBOOT=yes`)
5. Press <Enter> (to get a new line)
6. Enter `IPADDR=[ip-address]` (e.g. 10.0.5.151)
7. Press <Esc>
8. Type: `:wq`
9. `run sudo systemctl restart network`
10. If prompted, enter password configured during CentOS installation
11. Run `ipaddr` (to check whether IP address was properly set)
12. Repeat for each Tally machine

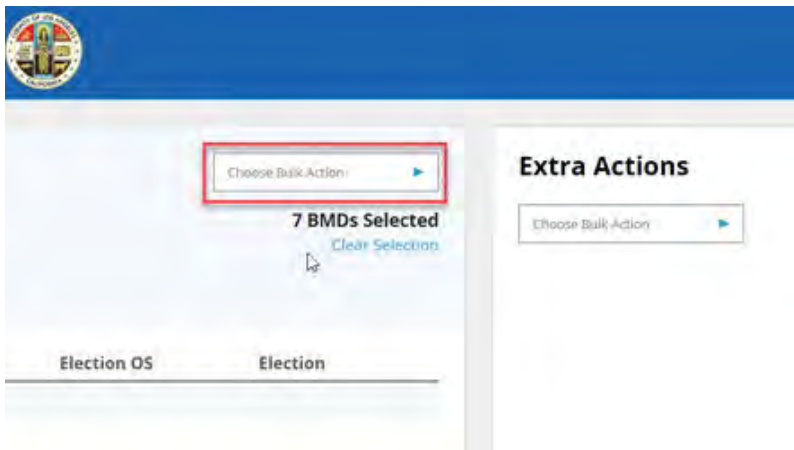
7. System Diagnostic Testing Procedures

Diagnostics can be run on any individual BMD, a filtered group of BMDs, or all BMDs simultaneously using the BMG; the following steps give examples of these features.

1. From the BMG main page, in the "Search BMDs by" menu, click List All, or choose specific search filters to isolate a group of BMDs, or a single BMD



- A list of BMDs, filtered by your search criteria appears
2. Check the boxes next to any BMD or check the box at the top of the list to select all BMDs
 3. Using the first "Choose Bulk Action" dropdown, select **Run Diagnostics**



4. Click **Submit**
5. You'll be brought to a new page where you'll see a status list of the command you've just run. You'll see either the "SUCCESS", or "FAILURE" test results in the "Status" column, along with details in the "Description" column

8. System Proofing

The components of VSAP need to be system proofed to ensure that they are working properly and securely. Each component has its own method of system proofing. See below to learn how.

8.1. Generate VBM L&A Ballot Decks

This process includes generating a Logic and Accuracy deck based on set configurations. It creates archives of generated L&A decks to be retrieved and used for the appropriate testing scenarios on other systems.

8.1.1. Generation Process for VBM L&A Ballot Decks:

1. Navigate to the VBM L&A page from the menu drawer
2. The page displays the current configuration set for Logic and Accuracy. Make sure that this is your desired configuration
3. If not, navigate back to Configure Logic and Accuracy
4. Click the Generate button
5. A message on the Dashboard in Active Processes displays the progress of the generation
6. When generation has completed return to Generate Logic and Accuracy. The configured deck is a new row in the table
7. To access the deck, click the icon in the Create PDF Archive column. This creates a zipped folder on the main VBL server that can be accessed manually following the path defined under Archive Location
8. To convert the deck from PDF to JPEG format, click the icon in the Convert to JPEG column
9. Once the conversion completes, click Create JPEG Archive to create a zipped folder on the main VBL server

Note: The Undervote deck is created during VBM Generation.

8.2. Generate BMD L&A Poll Passes

To execute Logic and Accuracy on the BMDs, VBL produces poll passes following configurable vote patterns. These are produced as sets of PDFs with 4 poll passes per PDF.

Once the L&A poll passes have been scanned and printed, these selection ballots will then have to be scanned into the Tally system to get tabulated. Tally can then print out the list summary of the test results and compare it to the list summary generated by the VBL system to ensure that the results from the BMD match those of the predetermined totals.

8.2.1. Generation Process BMD L&A poll passes:


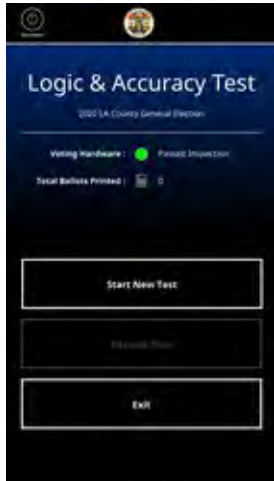


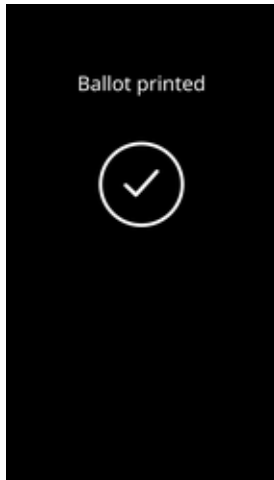


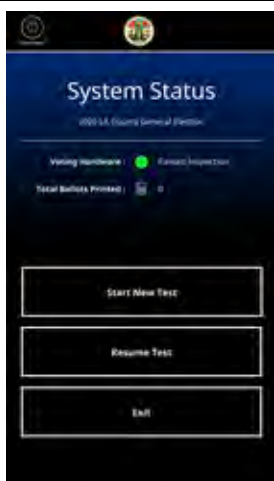
1. Navigate to the BMD L&A page from the menu drawer
2. The page displays the current configuration set for Logic and Accuracy. Make sure that this is your desired configuration
3. If not, navigate back to Configure Logic and Accuracy
4. Click the Generate button
5. A message on the Dashboard in Active Processes displays the progress of the generation
6. When generation has completed return to BMD L&A. The configured deck is a new row in the table

To access the deck, click the icon in the Archive column. This creates a zipped folder on the main VBL server that can be accessed manually following the path defined under Archive Location.

8.3. Using L&A on the BMD

Prior to an election, Logic and Accuracy testing must be done on a BMD to ensure the ballot layouts are correct. In order to perform this procedure, you need to switch a BMD to L&A mode. Follow the steps below to perform Logic and Accuracy testing using a BMD.

A BMD can't be put into L&A mode if the BMD is in Vote mode. Further, Logic and Accuracy testing can only be done by an election worker whose credentials activate L&A mode. Scanning these credentials automatically puts the BMD into L&A mode, given that the BMD is not in Vote mode.

<p>1. Scan and enter Credentials, then tap Return To Start.</p>	<p>2. Tap Start New Test.</p>	<p>3. Insert a blank paper ballot.</p>
		
<p>4. Scan L&A poll pass.</p>	<p>The ballot prints and drops into the ballot box, then returns to the insert a blank paper ballot page.</p>	
		
<p>5. Tap Exit Test to return to the L&A test page.</p>	<p>6. Tap New Test to start a new test or tap Exit to exit L&A mode.</p>	
		



L&A results

8.4. Lab Test Mode

Lab Tests are used by the Certification Lab to perform the environmental test on the BMD. This mode can be accessed at any BMD and the status can be not open, opened or closed. Only Lab Test Operators have access to this mode. The credentials for the Lab Test are generated in the BMG.

To simulate the Voting Process:

1. Scan and park
2. Print image
3. Eject and hold; repeat

The paper handler test has a counter of how many cycles have been done. During the paper handler diagnostic, all LEDs *must* turn white and the QR scanner must come on. The time between the cycles must be 10-seconds.

Prior to an election, Logic and Accuracy testing must be completed on a BMD to ensure the ballot layouts are correct. In order to perform this procedure, you need to switch a BMD to Logic and Accuracy mode.

8.5. Remake Mode

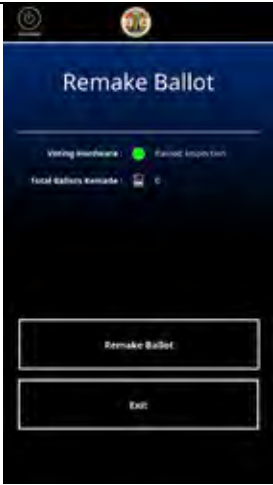

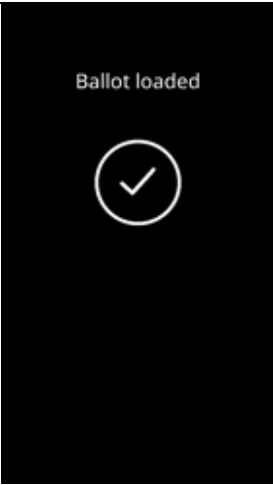
The Remake Mode is used to remake a ballot that has incurred damage and cannot be tabulated by Tally; only Remake operators have access to this mode. The BMG generates credentials for Remake operators. Remake operators can go through the full voting process in order to reprint voter ballots. The Remake Mode can be activated on any BMD from the voting application.


8.5.1. Activating the Remake Mode on the BMD

To activate the Remake Mode on the BMD, an operator with the appropriate authorization will scan their two-factor authentication credentials using the bar code scanner to scan their QR Code, and inputting their PIN using the touchscreen. Authorizations are established within the BMG. The activation is initialized in either the open or closed poll status. After the operator has entered their proper credentials, the operator will be prompted to insert a blank ballot in the BMD and then must scan the SBE from the unusable ballot. The voter selections will be reviewed.

Note: This information is always in English.

After reviewing the information, a new ballot with a unique ID and sequence number will be generated and then printed. The unique ID is located on the upper right-hand corner of the ballot. All Remake ballots are composed by BMD ID + Sequence.

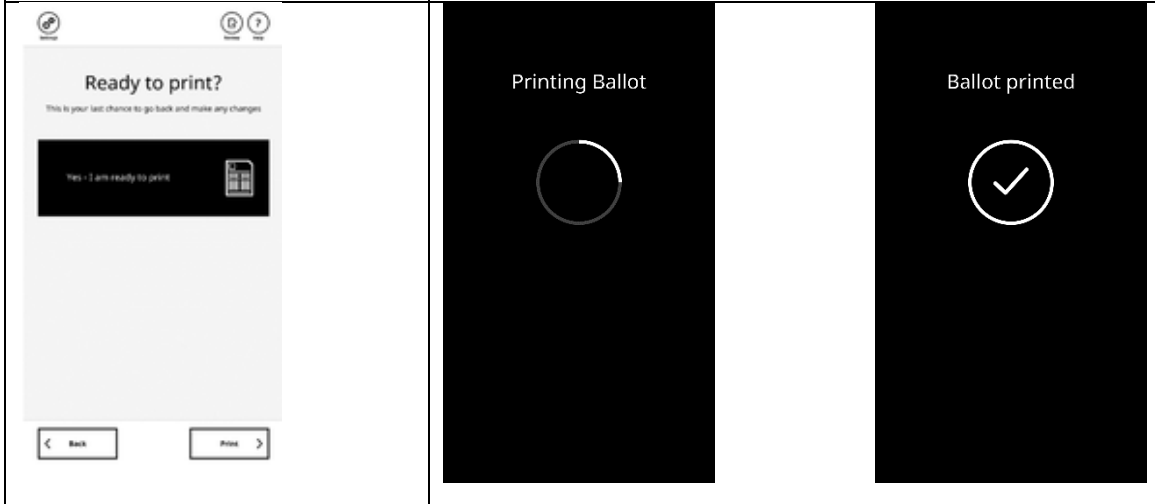
1. Select Remake Ballot	2. Insert Blank Ballot	3. Ballot Loaded
		
4. The precinct can be entered by scanning the BPM of the damaged ballot (the BMP includes Precinct, Provisionality, and Party), or	5. Precinct validation will be displayed, select Next to continue	6. Select Yes or No for Provisional voting, then select Next

<p>by manually inputting the data, and selecting Next.</p> <p>Note: When using the BPM</p>	<p>Note: When using the BPM this screen will not be displayed</p>	<p>Note: When using the BPM this screen will not be displayed</p>
		
<p>7. Select your party, then select Next.</p> <p>Note: When using the BPM this screen will not be displayed</p>	<p>8. Precinct loaded will display briefly</p>	<p>9. The ballot can be remade by scanning the SBE QR code of the damaged ballot, which will include all contest selections, or by manually entering the contests</p>
		
<p>10. **Series of contest**</p>	<p>11. Let's review</p>	<p>12. Review your selections</p>



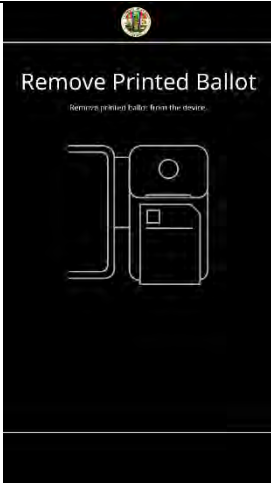
13. Select Yes - Ready to Print, then select Print

14. Printing Ballot & Ballot printed will display briefly



15. Please remove the ballot

16. The remake ballot will be printed with a unique code in upper right-hand corner (highlighted in Yellow)



9. Multiple Elections

All BMDs are designed to accept multiple elections. When a BMD is loaded with multiple elections, a welcome screen displays the name of all elections configured on the BMD. In this configuration, all activation counters will be stored by the election.

10. Ballot Tally Programs

The Tally Scanners need to be connected to the Tally system and a directory needs to be specified in order to receive scanned ballots. Follow the directions below to connect a Tally Scanner to the Tally system.

10.1. Tally Connection Process

1. Once an election is configured, specify which directory will be used to receive the scanned ballot images. From the Home page, select System Management > Scanners from the menu



2. From the Scanner Folders page, click Add Scanner

The screenshot shows the 'Add Scanner' form. It has a blue header with the text 'Add Scanner'. The form contains the following fields:

- Scanner Name:** A text input field with the placeholder text 'Scanner Name'.
- Scanner Path:** A text input field with the placeholder text 'Scanner Path'.
- Election:** A dropdown menu with the selected option 'GENERAL ELECTION, November 06, 2018 • County of Los Angeles (3861)'.

At the bottom right of the form are two buttons: 'Cancel' and 'Save'.

3. Set the scanner name and path to the directory on the file system and select the election to be associated with the scanner
4. Click OK
 - Multiple scanners can be configured either for a single election or for multiple concurrent elections

11. Election Observer Panel

The purpose of the Election Observer Panel is to:

- Provide an avenue for public observation of and input into the election process
- Assist in ensuring the integrity of the election process
- Encourage participation and build voter confidence in the election process

11.1. Invitation

Between E-60 and E-30, prepare a media release and letters of invitation (see samples attached) to parties likely to participate, such as the following:

- County Grand Jury
- Political Party Central Committee Members
- Language Advocacy Groups
- Community Based Organizations
- Media
- Other groups or individuals expressing an interest in observing election day activities may also be included in the observer panel, as deemed appropriate

11.2. Group Presentations

After letters of invitation have been sent out, offer to attend group meetings to provide an opportunity for the groups to ask questions about the process. Groups should be contacted to arrange time on their agendas for staff presentations. This is optional at the request of the group, but staff should make every effort to contact the groups and offer this service.

11.3. Appointment Letters (for introduction to precinct workers)

After the groups have provided the names of interested panelists, prepare letters of introduction (see sample attached) for the panelists to use when visiting polling places on Election Day. Materials to be prepared for each panelist will include a listing of all polling places within the county for that specific election as well as the central counting site location and hours of operation.

11.4. Mechanism for Feedback

Observers attend training at government facilities, where they can ask questions about the process.

General Rules for Observers

- Observe the proceedings at the polls, including the opening and closing procedures
- Obtain information from the precinct index that is posted near the entrance
- Make notes and watch all procedures
- View all activities at the central counting site on election day
- View the canvass of the vote activities following the election
- View absentee and provisional ballot processing
- Ask questions of staff or voters at the polls

- Ask questions of supervisors at the central counting site

Observer Responsibilities

- Check in at each site, whether polling place or central counting site
- Wear an identification badge
- Maintain a professional manner while observing the election processes
- Ensure they do not interfere with the elections process

Observer Prohibitions

- Interfere in any way with the conduct of the election
- Touch any voting materials or equipment or sit at the official worktables
- Converse with voters (within 100 feet of the entrance to a polling place) regarding the casting of a vote, or speak to a voter regarding his or her qualifications to vote
- Display any election material or wear campaign badges, buttons or apparel
- Wear the uniform of a peace officer, a private guard, or security personnel
- Use cellular phones, pagers, or two-way radios inside the polling place and/or within 100 feet of the entrance to the polling place
- Talk to central counting site workers while they are processing ballots
- Use the telephones, computers or other polling place facilities at polling places or the central counting site
- Touch election personnel
- Eat or drink in the polls or the central counting site
- Assist in operations at any polling place

12. Hardware Maintenance and Preparation for Use

The purpose of this document is to provide the end-user with a maintenance schedule to minimize system component downtime and failure.

12.1. Preventative Maintenance Schedule by System

The routine inspection of system components reduces the risk of major system failures. By implementing a preventative maintenance regimen, minor issues can be detected and addressed before failure occurs and renders the system unusable. The following table lists maintenance items that are usage and calendar based. Perform the maintenance items in the interval or time specified for each system component.

System Component	Action Name	Schedule/Timing	Action/Comments
BMG	Archive/back-up, clear logs	Post-election	Per BMG User Guide
	Clean/dust the computing equipment and networking equipment; check any tamper evident seals	Every six months	Do not use canned air or similar, or liquids, on the equipment. Follow County incident response procedure regarding tampered seals
	Run diagnostics	Every six months and 30 days before pre-LAT, whichever is more frequent	See BMG User Guide
BMD	Complementary Metal Oxide Semiconductor (CMOS) battery change	Every three years or upon battery depleted indication	See BMD User Guide
	Clean for any spills, dust, other contaminants - before every election	Every election cycle, either as part of pre-LAT or upon equipment return	Clean the BMD touchscreen using a lint free alcohol wipe before and after every election. Spot clean the screen using a lint free cloth every time the ballot box is emptied as well
	Printer	Every time the ballot box is emptied, or every 200 ballots cast whichever comes first	Open the lid, visually inspect for debris, loose printer parts, clean using compressed air and then a lint free, dust attracting cloth to remove any dust; clean the Contact Image Sensor (CIS, internal scanner) with lint free alcohol wipes

	Privacy Flaps	Before every election	Clean for any spills, dust, other contaminants; inspect for visible damage
	Bar code reader	Before every election	Clean using a lint free, dust attracting cloth to remove any dust; check for scratches/damage to the lens
	Ballot box	Before every election	Clean any spills, dust, other contaminants; inspect for visible damage
	Legs	Every election cycle, either as part of pre-LAT or upon equipment return	Inspect for visible damage; repair/replace if needed
ISB	Archive/back-up, clear logs	Post-election	Per ISB Preprocessor User Guide
	Run diagnostics	Every six months and 30 days before pre-LAT; whichever lends the greater frequency	Per ISB Preprocessor User Guide
	Check AWS Agreements to ensure proper account settings, S3 bucket availability as well as correct expected capacity, and verify configuration of CloudFront (CDN)	Every six months and 30 days before pre-LAT	Per County AWS Agreement

13. Polling Place Procedures

13.1. Voting Center Supplies, Delivery, and Inspection

This section lists the supplies required to setup the voting location with an emphasis on setting up the Ballot Marking Device (BMD).

- Cart containing five BMDs or a case with a single BMD
- BMD peripherals (including stand, privacy shield, headphones, and ballot box)
- Cleaning cloths to wipe the BMD Touchscreen
- Paper ballots shall be in the quantity and manner required by the California Elections Code
- General purpose supplies as provided in the California Elections Code
- Sample ballot booklets of each ballot style if required by the California Elections Code
- Seals and any other supplies and forms
- Tables and chairs
- Power surge protectors
- Power extension cords
- UPS (uninterruptible power supply) if required per jurisdiction procedure

After the carts and containers have arrived, and before the vote center location opens, Election workers will perform the following actions:

1. Perform a visual inspection of all carts and containers. Inspect and record that all seals are intact on the outside of all carts and containers as per LA County procedure
2. Perform a visual inspection of all BMDs. Inspect and record all seals are intact on all BMDs as per LA County procedure
3. Setup the BMDs per procedure described in Section 5.2

13.2. Vote Center Set-up

The Ballot Marking Device (BMD) is used by voters to mark and cast a ballot. BMDs will arrive at the Vote Center in carts, with each cart containing five BMDs.

The BMD is comprised of the following components:

Integrated Ballot Box
Cross-support bar
Headphones
Leg stand
Power cord
Power module
Power module bracket
Privacy shield
BMD top module
Handheld controller
BMD cabinet

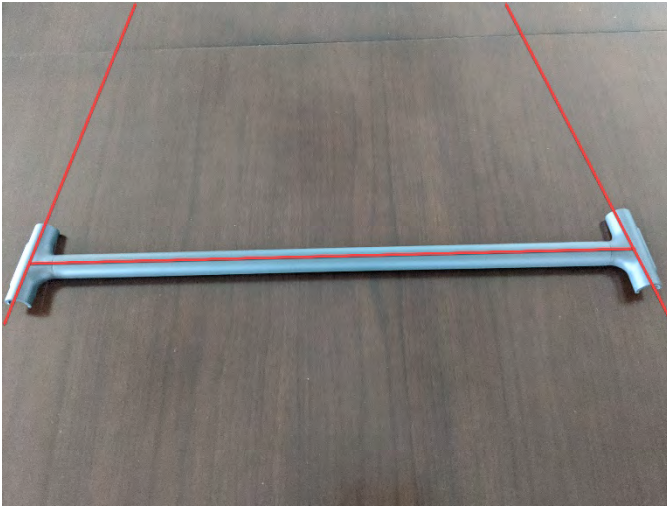
The BMD has a headphone jack and auxiliary port for voter's use. There are two headphones jacks located on the BMD: the first is located on the left-side front of the BMD; the other is located in the back left-side of the BMD, next to the power button. The auxiliary port is located on the lower-right side of the BMD.

The BMD Technician will assemble the BMD using the following instructions:

1. Remove the folded leg stand from the peripherals container.
2. Open the legs by lifting up from the center. Each leg has a spring-loaded feature that allows it to lock securely into place.



3. Remove the cross-support bar from the container.



Note: The cross-support bar should taper inward like the letter A.

4. Line up the grooves on each end of the cross-support bar with the attachment point on the back legs of the stand. Then, use the palm of your hand to gently snap both ends into place, one at a time. There will be a slight clicking sound that indicates that the cross-support bar is securely in place.



5. The stand is ready to have the power cord attached.



6. Remove the power module bracket from the container.

7. Snap the hooks of the Power Module Bracket onto the Leg Stand.



8. Remove the power module and the power cord from the cart.



9. Connect the power cord to the base of the power module.



10. Place the power module inside the power bracket, placing the larger power cord in the larger square opening and the smaller cord in the smaller round opening.



Note: It is necessary to install the power module prior to adding the BMD top module. Do not connect the other end of the power cord into the wall yet.

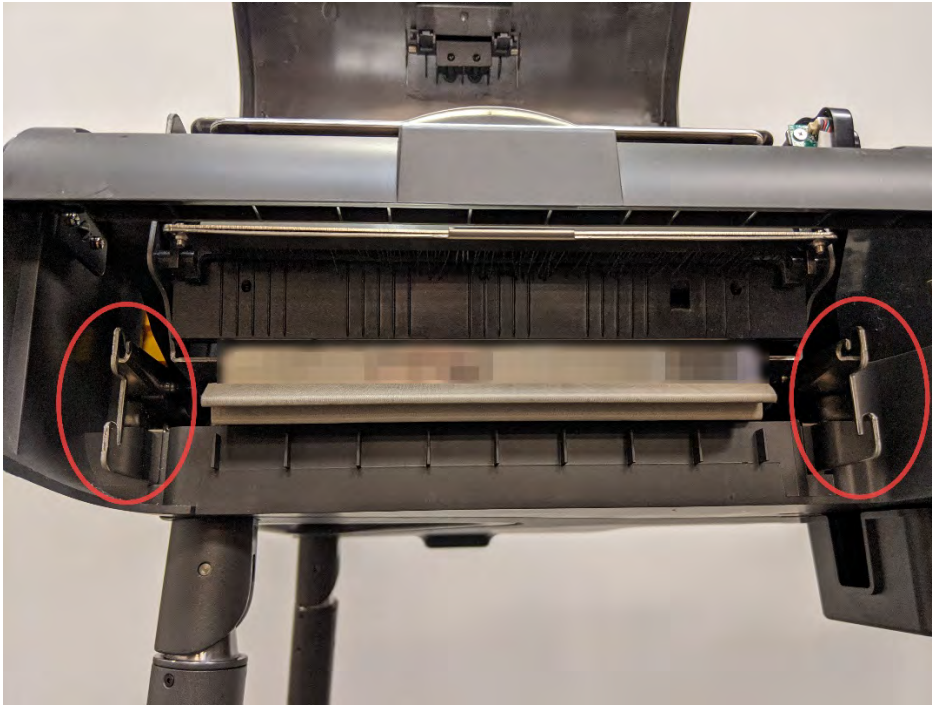
11. Attach the BMD top module to the leg stand by aligning the grooves underneath the BMD top module.



Note: This is a 2-person job.

12. To attach the Integrated Ballot Box, first open the plastic printer cover.

13. Remove the Integrated Ballot Box from the peripheral's container.
14. Line up the openings on the back of the Integrated Ballot Box with the hooks on the BMD top module, ensuring that the openings are lined up and securely fit together.



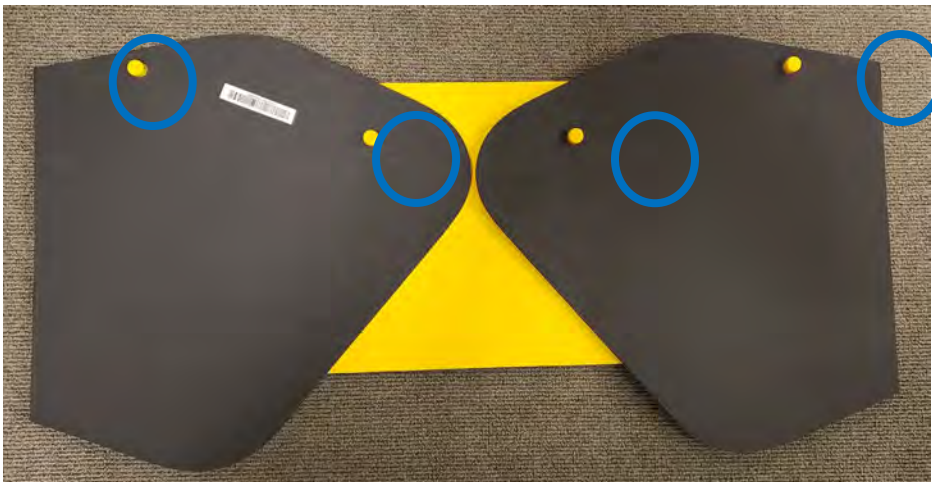
15. Slide the Integrated Ballot Box onto both hooks on the lower end of the BMD top module, then tilt the Integrated Ballot Box slightly upward to snap it into place.



16. Attach and tightly cinch the Zip Tie to secure the IBB. Place the tamper-evident seal over the seam of the IBB and record the seal and Zip Tie in the Chain of Custody per LA County procedure.



17. Remove the privacy shield from the BMD container.

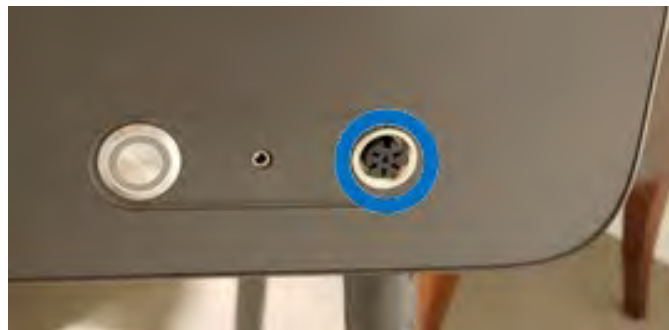


18. Unfold the privacy shield flaps and attach it to the slotted holes on the sides of the BMD top module, one side at a time.

Note: This is a 2-person job



19. Gently insert the six-pronged end of the power cord into the six-pronged socket found on the back of the BMD top module.



20. Plug the power cord into the wall outlet.

21. Remove the headphones from the BMD container. Place them on the left-hand side of the BMD top module.



22. Plug the headphone cord into the rear audio port of the BMD.



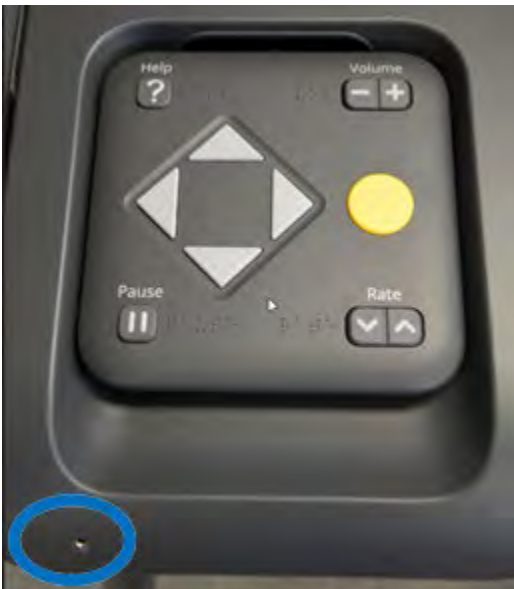
This ends the BMD set up procedure.

13.2.1. Additional Ports

Sip and Puff/Dual-Switch Device: There is an additional port in the lower right-hand corner of the BMD top module that serves as a place to connect personal assistive devices. (Example: Sip and Puff unit or a dual-switch.)



Additional Headphones Port: There is an additional Headphones Auxiliary Port on the front of the BMD top module to plug in another set of headphones for another person to assist a voter who's already using the other port.

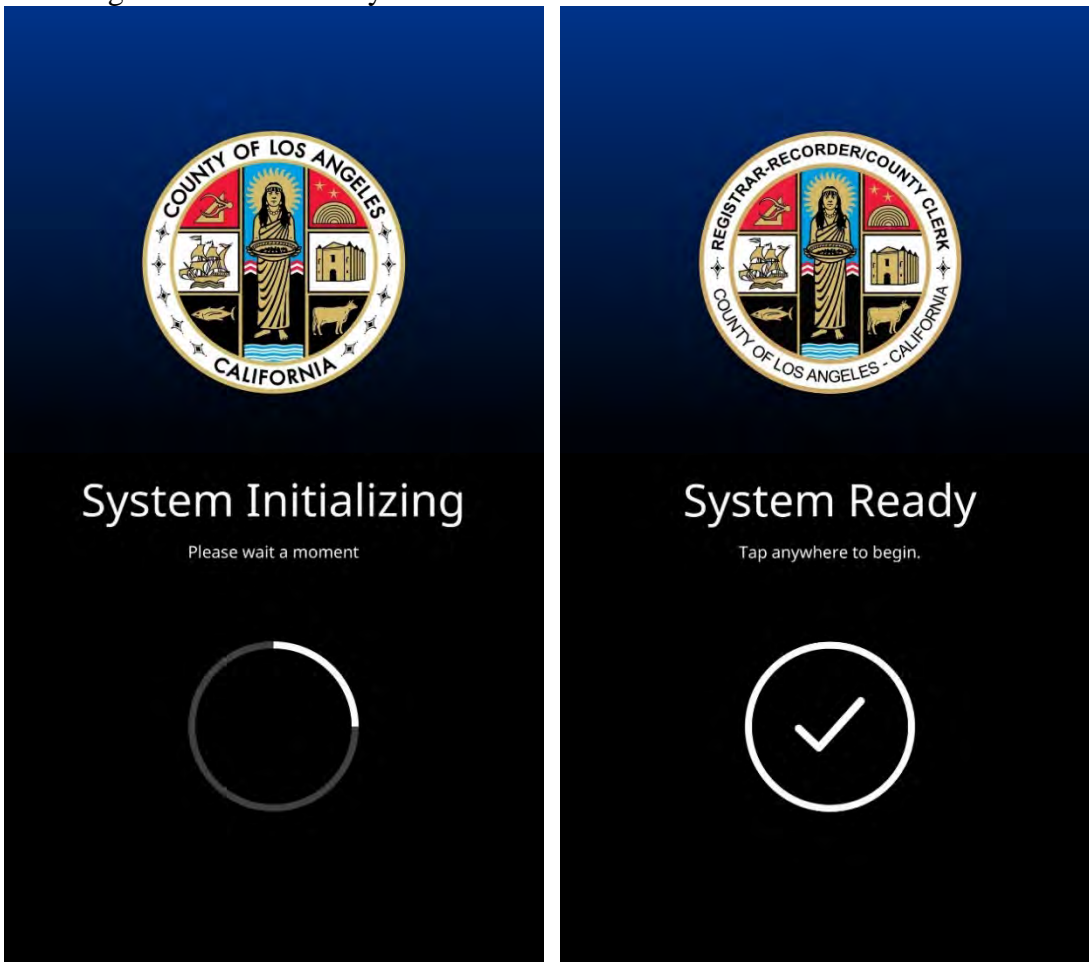


13.2.2. Setup Completion

Press the Power Button to turn on the BMD.



An auto-diagnostics test of the system will occur.



In the event the system fails, an error message (#4422) will display on the screen. Shut down the BMD and reboot. If the system fails again after rebooting, the Election Worker will shut down the BMD and report the issue to the Election Worker Lead.



13.3. Cleaning the BMD Scanner and Touchscreen

To maintain and clean the Touchscreen, use lint free alcohol wipes.



Avoid other chemical agents (except for alcohol) to clean the Touchscreen. Do not spray other cleaning agents directly onto the Touchscreen, as the liquids may seep into the screen or contaminate the front bezel.

Wipe the Touchscreen using gentle wiping motions.

Note: Do not wipe or press the Touchscreen with excessive force.

13.4. Scanners

There are two scanners on the BMD; the Poll Pass/Security Pass scanner underneath the right front corner, and the Ballot scanner located within the Paper Handler.

13.4.1. Bar Code Reader

1. To clean the Poll Pass/Security Pass scanner, first locate the glass scanner lens underneath the front right-side of the BMD.



2. The election worker uses compressed air to remove external dust, followed by polishing the glass surface with a clean dry cloth.
3. If further cleaning is necessary, use a soft cloth dampened with isopropyl alcohol to wipe the scanner glass. Do not spray liquid directly on the scanner surface. Do not use any other cleaning solvents.

13.4.2. Ballot Scanner and Printer Rollers

To clean the Ballot Scanner and Printer Rollers, it is necessary to break the Zip Tie, open the Integrated Ballot Box, and open the Paper Handler to get access to the scanner.

1. Press the Power Button to turn off the BMD.



2. Remove the security seal on the Integrated Ballot Box. Follow LA County procedure for removing Zip Ties.



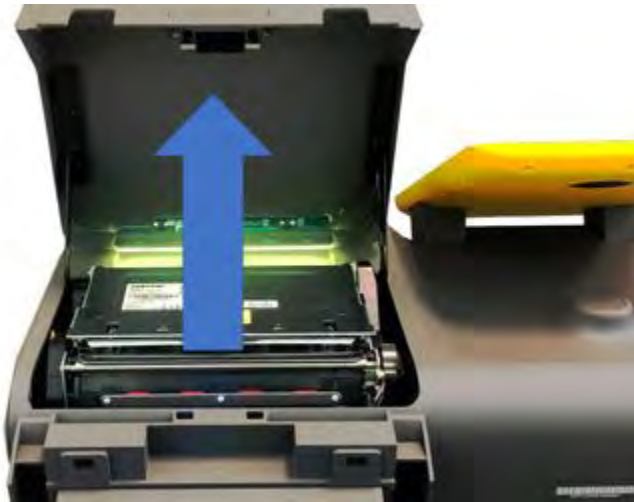
3. Push the button on the upper-left side of the Integrated Ballot Box and pull the back of the Integrated Ballot Box.



4. Press the button at the center of the plastic printer cover and pull the cover upward.



5. Pull the metal printer cover upward.



6. Use compressed air to remove external dust.

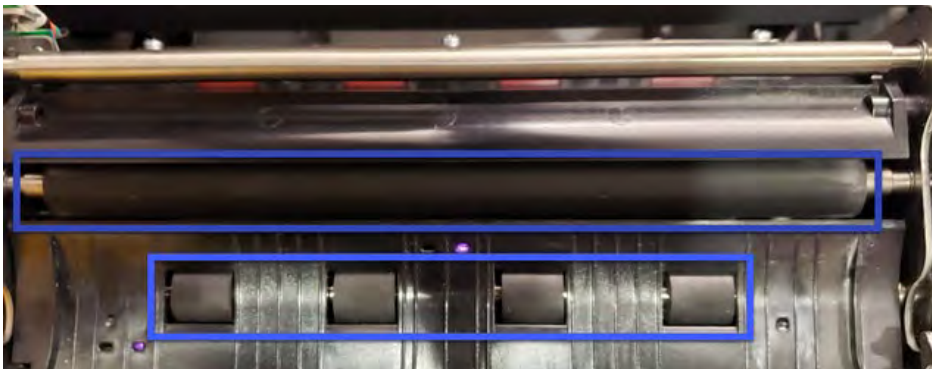


7. Using lint free alcohol wipes, clean the surfaces of the:

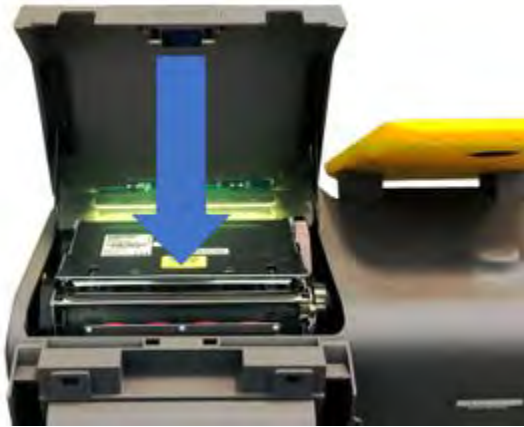
- Ballot Scanner Lens (see picture below); and
- Each Printer Roller (see picture below)

Manually rotate the rollers to ensure that the entire surface of each roller gets cleaned.

Note: Use gentle wiping motions to remove dust. Do not spray liquid directly on the scanner surface; do not use any other cleaning solvents.



8. Close the metal printer cover.



9. Close the plastic top cover.



10. Close the Integrated Ballot Box.



11. Attach the Zip Tie per LA County procedure




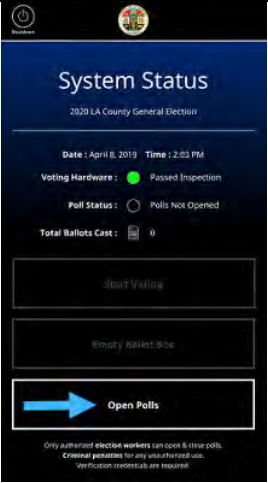

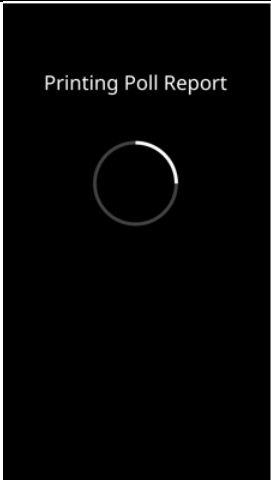
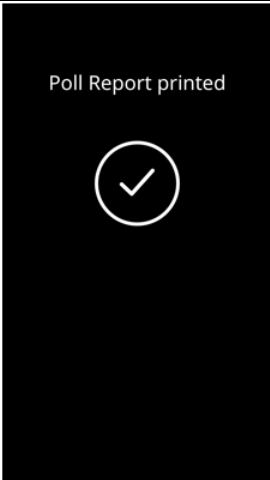
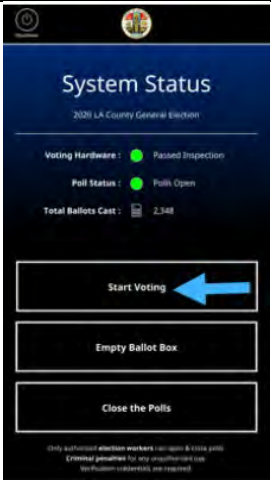
12. Press the Power Button to turn the BMD back on.

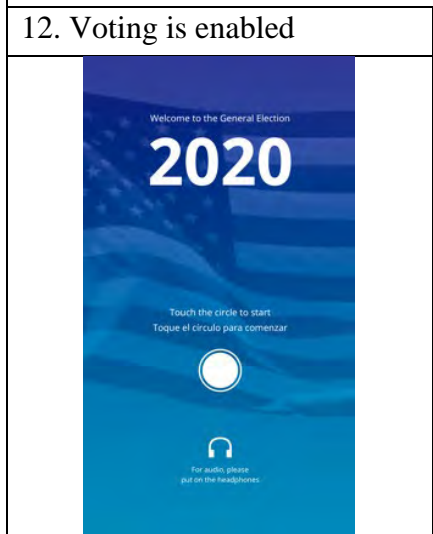


13.5. Opening the Polls

This procedure describes how two Election Workers can "open the poll" to enable voting on each BMD. Opening the polls requires proper Credentials which incorporate a 2-factor security process. These Credentials consist of a six-digit PIN and a QR coded Security Pass that is generated by the BMG and issued to Election Workers. These Credentials are secured and passed out per LA County procedure.

<p>1. Following LA County procedures, check the Zip Tie and the tamper-evident seal placed over the seam of the IBB; verify they have not been tampered with</p>	<p>2. Press the Power Button</p>	<p>3. The system initializes</p>
 		
<p>4. Tap anywhere to begin</p>	<p>5. Scan the Security Pass with the bar code scanner, located under the BMD on the lower right side</p>	
	 	

<p>6. Enter Credentials 7. Tap System Status</p>	<p>8. Tap Open Polls (After the first day of an election, this button will read Re-open Polls)</p>	<p>9. Insert blank thermal paper</p>
		
<p>10. The Open Poll Report is printed. Two Election Workers should verify the report per LA County procedure</p> <p>See samples of Open Poll Reports below</p>		<p>11. Tap Start Voting</p>
		



The following information is found in the Open Poll Report:

Date - The date of the **Open Poll Report**.

Time - The time the **Open Poll Report** is printed.

BMD ID - Each **BMD** has its own unique ID number

HW Test Results - Indicates whether or not the hardware passed the inspection for the **BMD** to properly function.

Election Title - The title for the election, i.e. - Presidential Primary Election

Election Jurisdiction - The jurisdiction of the election

Software version - The **BMD** software version.

OS Version - The **BMD** Operating System version.

Totals:

Cumulative*

- Total Ballots Printed
- Total Ballots Cast
- Total Emptied Ballot Box
- Total ReOpened

*When Polls are Re-Opened, **Cumulative Totals** must be reconciled against the previous day's **Closing Poll Report**.

These totals should match those on the **Close Poll Report** with one exception - the **Total ReOpened** should equal **one plus** the previous day's total.

Daily*

- Total Daily Ballots Printed
- Total Daily Ballots Cast

*Daily totals should equal zero - unless polls are opened **more than once** on the same day.

Sample Open Poll Report for the first day of an election:

OPEN POLL REPORT:

Date: 07/25/2019 **Time:** 2:26 52 PM

BMD ID: 0000008	Election Title: PRESIDENTIAL PRIMARY ELECTION
HW Test Results: Passed Inspection	Election Jurisdiction: Los Angeles

Software version: 0.12.0 **OS version:** 1

TOTALS:

Total Ballots Printed:	0
Total Ballots Cast:	0
Total Emptied Ballot Box:	0
Total Reopened:	0
Total Daily Ballots Printed:	0
Total Daily Ballot Cast:	0

Vote Center Lead Signature

Election Worker Signature

Sample Open Poll Report when polls are re-opened:

OPEN POLL REPORT:

Date: 07/27/2019	Time: 4:32:07 PM
-------------------------	-------------------------

BMD ID: 0000009	Election Title: PRESIDENTIAL PRIMARY ELECTION
HW Test Results: Passed inspection	Election Jurisdiction: Los Angeles



Software version: 0.12.0	OS version: 1
---------------------------------	----------------------

TOTALS:

Total Ballots Printed: 10	Cumulative Totals
Total Ballots Cast: 9	
Total Emptied Ballot Box: 12	
Total Reopened: 11	





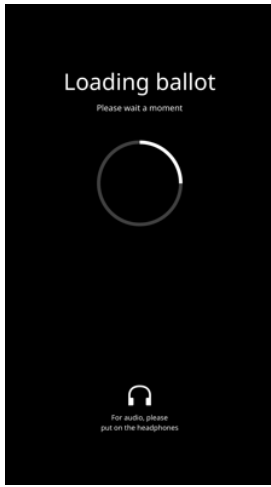
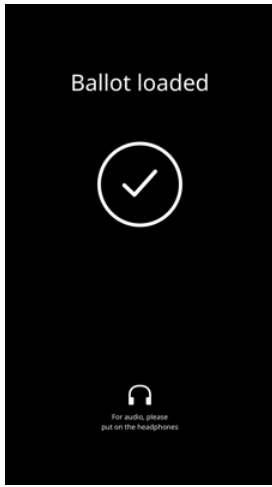
Total Daily Ballots Printed: 0	Daily Totals
Total Daily Ballot Cast: 0	

Two signatures are required for the Open Poll Report

 Vote Center Lead Signature	 Election Worker Signature
---	--

13.6. Polling Procedures

13.6.1. Voting Using the BMD Touchscreen

<p>1. The Election Worker provides the voter with an official paper ballot and directs them to the BMD</p> <p>The BMD displays a blue screen with the year and type of election (general or primary)</p> <p>2. Touch the circle to start</p>	<p>3. Choose language of preference</p> <p>4. Tap Next</p>	<p>5. A message instructs the voter to Insert your ballot</p>
		
<p>6. The voter inserts their ballot into the tray on the right-hand-side of the BMD</p>	<p>7. Loading ballot is displayed</p>	<p>8. Ballot loaded is displayed</p>
		

9. The **Let's get started** screen displays two options:

- a. **I want to start voting** – Brings the voter to the **Make your selections** screen
- b. **I have a Poll Pass to scan** – Asks the voter to Scan your Poll Pass



10. The **Make your selections** screen displays the following message:

There are x contests on today's ballot. When you reach the end, you will be able to review your selections

11. Tap **Next** to begin voting



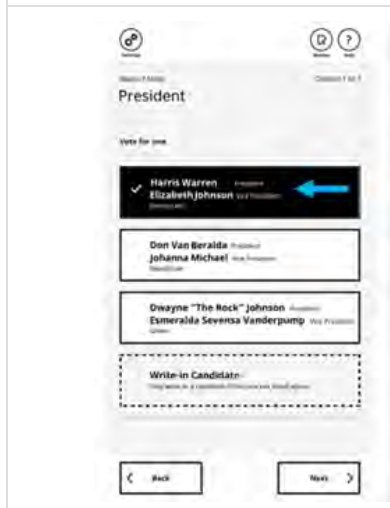
12. To make a selection, tap the **Candidate Name** or Yes/No for a **Proposition** or **Measure**.

13. Tap **Next** to move to the next contest



14. Marked selections will be highlighted with a check mark

To deselect, tap the marked selection - which will remove the highlighting and check mark






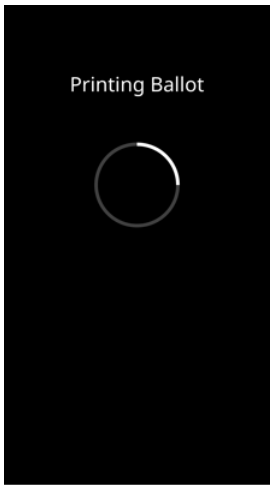
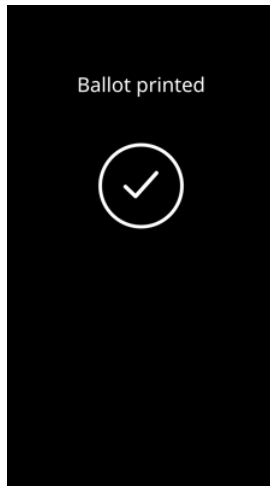
15. To move past a contest without marking a selection, tap **Skip**



16. After all selections are made, the **Let's Review** screen is displayed to notify the voter they can review their selections

17. Tap **Next**



<p>18. The Review your selections screen opens displaying the voter's selections; voters can tap the Change button to make a new selection</p> <p>19. Tap Next when finished</p>	<p>20. The Ready to print? screen displays the following message:</p> <p>This is the voter's last chance to go back and make any changes</p>	<p>21. Tap Yes - I am ready to print</p> <p>22. Tap Print</p>
		
<p>21. Printing Ballot is displayed</p>	<p>22. Ballot printed is displayed</p>	<p>Once the ballot is printed, the Ready to cast? screen appears and the voter can do the following:</p> <ul style="list-style-type: none"> • Cast your ballot now – See the steps below • Read back my printed ballot – Re-scans the ballot and reads back the voter's selections through the headphones • Make a change on the printed ballot – the voter must contact an Election worker; the Election worker will spoil the ballot and provide the voter with a new ballot per LA County procedure
		

<p>23. The Ready to cast? screen displays the following message: Verify your printed ballot before casting</p>	<p>24. Tap Cast your ballot now</p> <p>25. Tap Next</p>	<p>26. Reinsert the ballot into the BMD</p>
<p>27. The Casting ballot screen displays the following message: Please wait, your ballot is being placed into the ballot box</p>	<p>28. Ballot has been cast is displayed</p>	<p>29. The Thanks for voting! screen displays the following message: Take your printed ballot to an Election worker for assistance</p>

13.6.2. Using a Poll Pass

A voter can go online and access their sample ballot and digitally mark it using a computer or mobile device, such as a smart phone or tablet, prior to going to a Vote Center. Voter selections are captured in a QR code called a Poll Pass that can either be printed onto paper or downloaded to their mobile device. A sample of the Poll Pass is shown below. When the voter arrives at the Vote Center, they must check in using the normal check-in process.

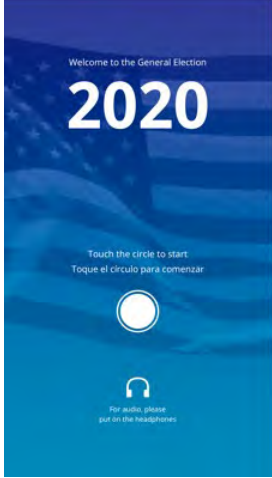

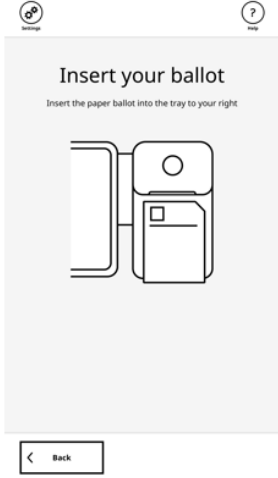
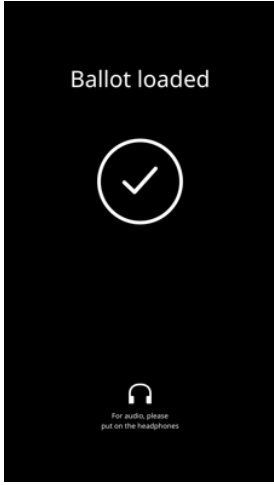
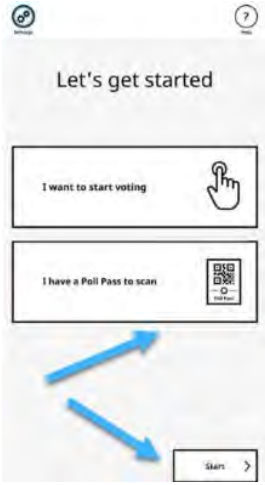
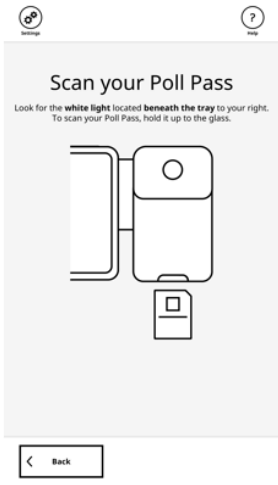


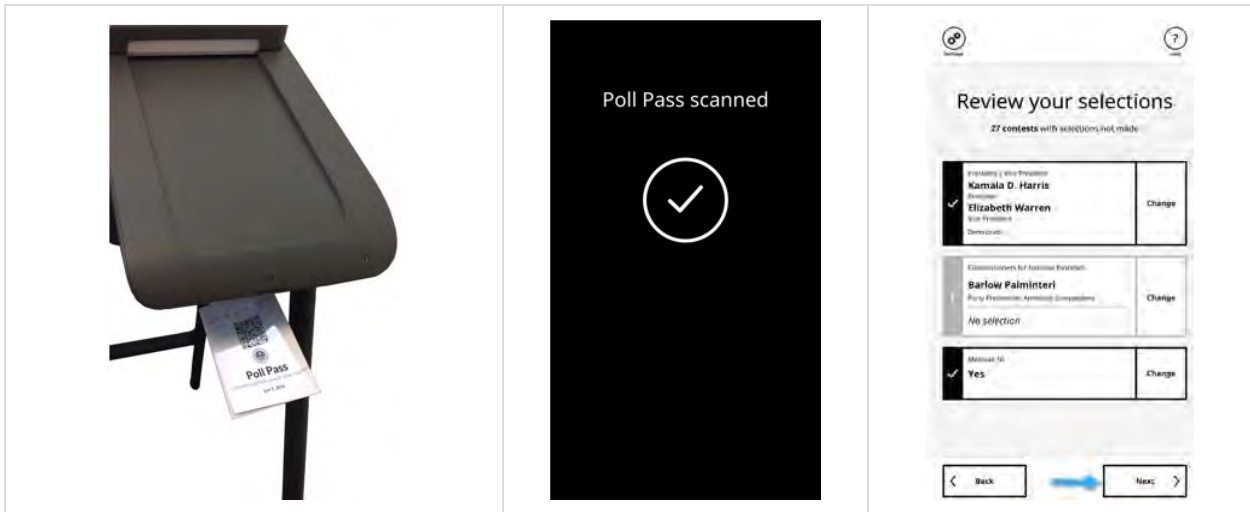
Printed Poll Pass



Mobile Device Poll Pass

After the voter has checked in and received a blank ballot, they will scan their Poll Pass at a BMD to transfer their selections to the BMD for validation before printing on a paper ballot.

<p>1. Touch the circle to start the voting process</p>	<p>2. Tap a language</p>	<p>3. Insert ballot</p>
		
<p>4. After loading the blank ballot in the BMD, Ballot loaded is displayed</p>	<p>5. Tap I have a Poll Pass to scan and then click Start</p>	<p>6. Scan your Poll Pass screen will appear</p>
		
<p>7. Place your mobile Poll Pass or printed copy of a Poll Pass directly beneath the scanner located below the BMD paper deck</p>	<p>8. Message: Poll Pass scanned</p>	<p>9. Review and change selections as desired. Then tap Next</p>



To view additional steps to finish casting a ballot, go to Section 5.4.1 Voting Using the **BMD Touchscreen**.

8. Remove ballots from **Integrated Ballot Box**

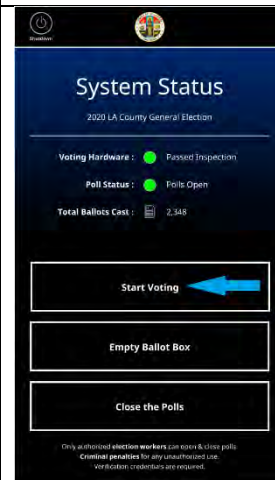
9. Close **Integrated Ballot Box** and listen for a clicking sound, which indicates the **Integrated Ballot Box** is properly closed



Place a new **tamper-evident seal** on the seam of the **IBB** and **Zip Tie** per LA County procedure and log it into the Chain of Custody. Be sure to tightly cinch the **Zip Tie** to ensure the **IBB** is secured

Tap **Confirm all ballots were removed**

10. Tap **Start Voting** from the menu

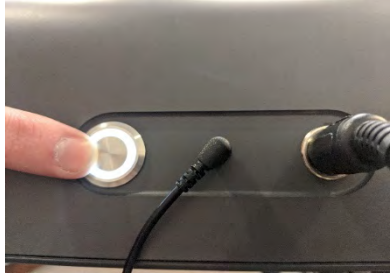
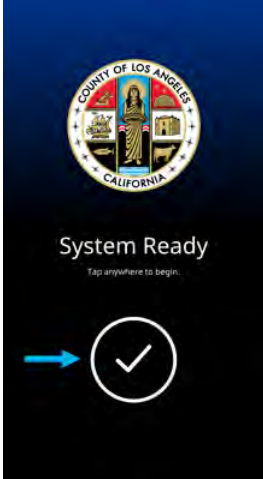

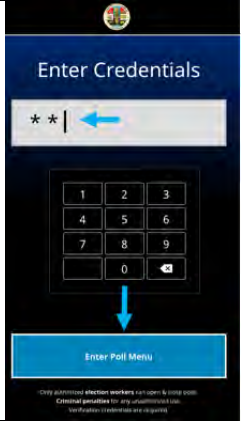
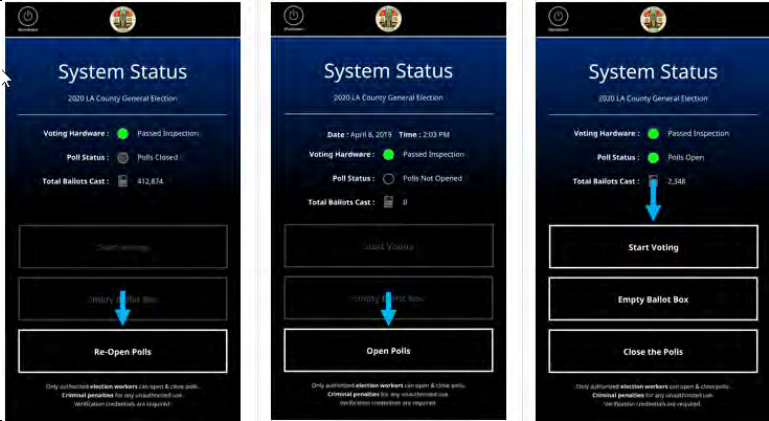


13.6.4. Restarting BMD After Interruption

When a BMD is restarted, it keeps the last status prior to the interruption. If the BMD is interrupted during the day, for example, by a power failure, one of the following status messages is displayed on the BMD screen:

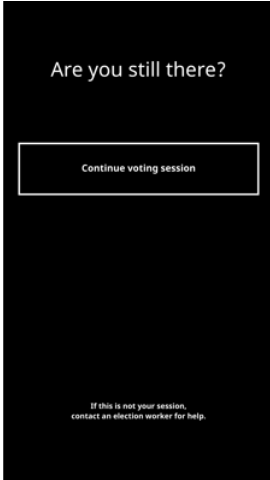
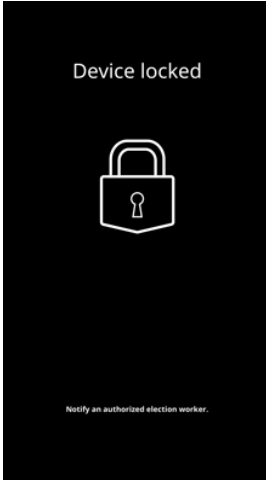

- Re-Open Polls
- Open Polls
- Start Voting

If a ballot was left in the BMD when an interruption occurred, the ballot is ejected from the BMD when the power is restored. The ballot is handled according to LA County procedures. To restart a BMD after an interruption, follow this procedure.

<p>1. Press the Power Button</p>	<p>2. After the system initializes, tap the check mark on the System Ready screen. The Enter Credentials screen displays</p>	<p>3. Scan Security Pass</p>
		
<p>4. Enter Credentials, and then tap Enter Poll Menu</p>	<p>5. One of the three screens below will be shown. Tap either Re-Open Polls, Open Polls, or Start Voting</p>	
		

13.6.5. Dealing with Fleeing Voters

This procedure details what an Election Worker should do when a voter has left before casting their ballot.

<p>1. If during a voting session, the voter stops interacting with the BMD for an administrator-specified period of time, the system will display the screen below.</p> <p>Note: If the voter has not fled, the voter can select Continue voting session</p>	<p>2. After a period of time (set by the BMG administrator), the BMD will lockout. The LED will flash yellow indicating the BMD has been timed-out. At the bottom of the screen, the system will say: Notify an authorized election worker</p>	<p>3. The Election Worker will enter their Credentials and select Enter Poll Menu</p>
 <p>The screenshot shows a black background with the text "Are you still there?" at the top. Below it is a white rectangular button labeled "Continue voting session". At the bottom, there is a small line of text: "If this is not your session, contact an election worker for help."</p>	 <p>The screenshot shows a black background with the text "Device locked" at the top. In the center is a white padlock icon. At the bottom, there is a small line of text: "Notify an authorized election worker."</p>	 <p>The screenshot shows a black background with the text "Enter Credentials" at the top. Below it is a white input field containing six red asterisks. Underneath is a numeric keypad with buttons for digits 1-9, 0, and a backspace icon. At the bottom, there is a small line of text: "Only authorized people (workers) can use it. This poll..."</p>
<p>4. The system automatically ejects the ballot and returns to the Welcome Screen.</p> <p>Follow LA County procedures to cast the ballot</p>		

13.7. Voters with Disabilities and Voters using Audio Features

This section describes procedures for voters utilizing the audio feedback, handheld controller, and customized screen settings.

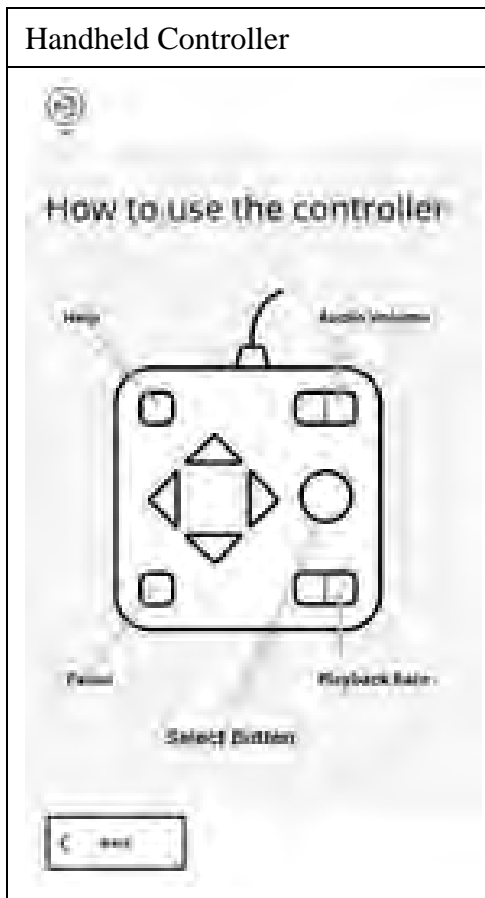
13.7.1. Auxiliary Device and Ports

The BMD has two auxiliary ports, and one connected device which enables voters to mark and cast their ballots:

- Handheld Controller
- Headphones Jack
- Dual-Switch Port

13.7.2. Handheld Controller

The Handheld Controller allows the voter to use the BMD without having to touch the screen to navigate and mark their selections on the ballot. Braille is provided for voters with a visual impairment. The Handheld Controller has several components available for the voter, such as Help, Audio Volume, Pause, and Playback Rate. There are also four directional arrow buttons used to navigate, and a round button used to mark selections.



See table below for controller functionality:

Component/Location	Use/Functionality	Braille
Help	Press this button to access the help menu	Yes
Audio Volume	Press the audio button to increase or decrease the volume	Yes
Pause	Press the pause button to pause the voting process	Yes
Select Button	Press to select Candidate/Measure	No
Rate	Press the rate buttons to increase or decrease the rate of speed for listening to the ballot	Yes
Arrow Up	Press the arrow up to listen to the contest name above current candidate, Proposition/Measure	No
Arrow Down	Press the arrow down to listen to the contest name below the current candidate, Proposition/Measure	No
Arrow Right	Press the arrow to the right to make a selection to the right	No
Arrow Left	Press the arrow to the left to make a selection to the left	No

13.7.3. Headphone Ports

Headphones are located on the top left corner of the BMD and are plugged into the Headphones Jack located on the rear left-hand side, which automatically and continuously plays the audio voting instructions. There is an additional audio port provided at the left front of the BMD where a voter may plug in their own headphones. Both audio ports always remain active in case the voter desires a helper to listen to the voting session at the same time. The two audio ports are always at the same volume level and playback speed—changing the volume level or playback speed always affects both audio ports. The voter can plug in or unplug Headphones from either of the headphone jacks at any time, with no resulting message displayed by the BMD application. The audio can only be played in the language displayed on the screen.

13.7.4. Dual-Switch Port

The right-front port is for connecting any Dual-Switch compatible device, such as a Sip and Puff assistive technology controller. The BMD application detects when a device is plugged into the port and shows a Dual-Switch specific configuration page that also informs the voter that if they are trying to plug in Headphones, they should use the headphones jack. The audio will always be available when using the system regardless of what voting method is being used, i.e.:



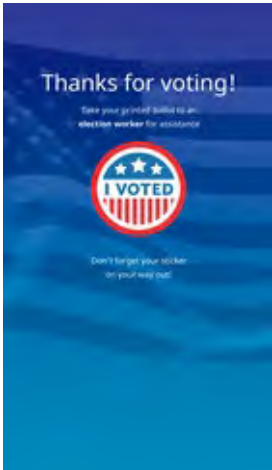
Touchscreen, Audio, or Poll Pass. The language displayed on the Touchscreen will be the same language used when using the audio voting feature.

13.8. Provisional Voters

This section details the procedure for assisting provisional voters. These voters receive a ballot containing a QR code indicating the vote is provisional. The voter's experience is the same with one exception - the voter cannot cast their ballot into the Integrated Ballot Box. Instead, they place their ballot in an envelope and return it to an Election Worker who will place the envelope in the Integrated Ballot Box per LA County procedure.

Note: The same procedure is used across precincts.

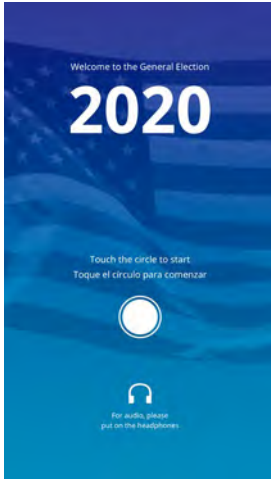
After marking their selections using the BMD, the voter will follow the steps below:

<p>1. Tap Complete voting session on the Ready to cast? screen</p> <p>2. Tap Next</p>	<p>3. Remove the provisional ballot and return it to an Election Worker</p>	<p>4. The screen displays Thanks for voting!</p>
		

13.9. Closing the Polls and Vote Reporting

Follow the steps below when Closing the Polls at the end of each election day. Closing the Polls requires an Election Worker to insert thermal printer paper to print a Close Poll Report (see example below). The Integrated Ballot Box is also emptied when Closing the Polls. After closing the polls, a Close the Polls report is printed. The Close the Polls report will include cumulative and daily totals for the BMD. Election Workers must use this report to reconcile with the Open Polls report the following morning. This procedure must be used at each BMD.

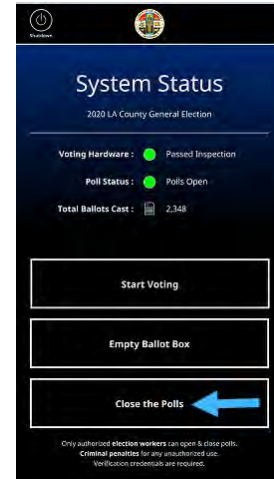
1. Scan a **Security Pass** with the bar code scanner, located under the **BMD** on the lower-right side



2. Enter Credentials
3. Tap Enter Poll Menu



4. Tap Close the Polls



5. Remove the ballots from the **Integrated Ballot Box**



6. Remove the **tamper-evident seal** from seam of the **IBB** and the **Zip Tie** on the **Integrated Ballot Box** per LA County procedure; record removal by logging the serial number into the Chain of Custody



7. Push the button on the upper-left side of the **Integrated Ballot Box** and pull the back of the **Integrated Ballot Box** outward



8. Remove all ballots from the **Integrated Ballot Box**

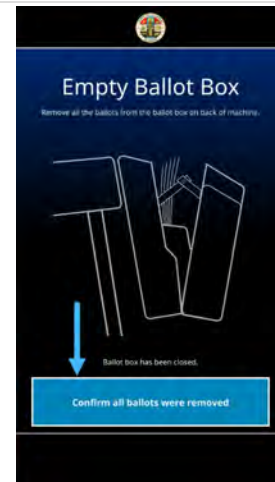


9. Close the **Integrated Ballot Box** and listen for a clicking sound, which indicates the **Integrated Ballot Box** is properly closed.

10. Place a new **tamper-evident seal** on the seam of the **IBB** and **Zip Tie** per LA County procedure and log it into the Chain of Custody



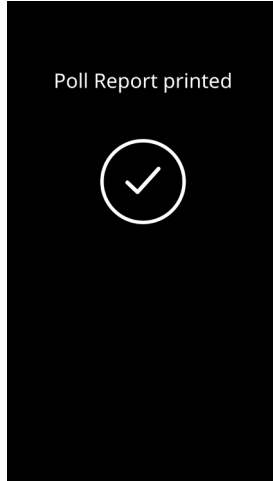
11. Tap **Confirm all ballots were removed**



12. Insert a blank sheet of thermal paper



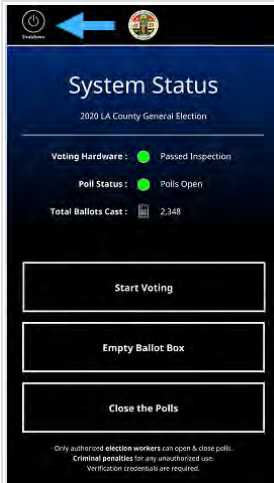
13. The **Close Poll Report** is printed



Note: This **Close Poll Report** must be signed by two **Election Workers** and reconciled per LA County procedure



14. Tap the **Shutdown** icon located in the upper-left side



15. Tap **Shut Down** to power down the **BMD**



Sample Close Poll Report

Note: This **Close Poll Report** must be signed by two **Election workers** and reconciled per LA County procedure.

CLOSE POLL REPORT:			
Date:	08/15/2019	Time:	2:49:39 PM
BMD ID:	0000014	Election Title:	PRESIDENTIAL PRIMARY ELECTION
HW Test Results: Passed Inspection		Election Jurisdiction:	Los Angeles
Software version: 0.12.0		OS version:	1
TOTALS:			
Total Ballots Printed:	14		
Total Ballots Cast:	14		
Total Emptied Ballot Box:	0		
Total Reopened:	0		
Total Daily Ballots Printed:	0		
Total Daily Ballot Cast:	0		
_____ Vote Center Lead Signature		_____ Election Worker Signature	

13.10. Securing Audit Logs and Backup Records

See Section 19. Audit Trails.




13.11. Troubleshooting and Problem Resolution

This procedure details how an Election worker can troubleshoot the following issues:

- Printer has a paper jam
- BMD cannot read a Ballot
- BMD Touchscreen is frozen
- Headphones are not working

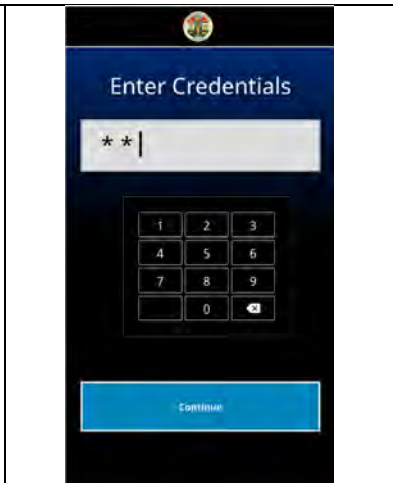
13.11.1. Problem: Printer has a paper jam

If a paper jam occurs in the scanner/printer, the BMD will display an error screen notifying the voter there is a Printer Paper Jam. Call an Election worker for assistance. The screen will display instructions to the Election worker on how to manually remove the jammed ballot.

1. When there is a paper jam, the BMD screen will display Printer Paper Jam	2. Scan Security Pass	3. Enter Credentials and Press Continue
		

<p>4. The following screen will appear, Resolve Paper Jam</p>	<p>5. Remove the tamper-evident seal from seam of the IBB and the Zip Tie on the Integrated Ballot Box per LA County procedure; record removal by logging the serial number into the Chain of Custody</p>	<p>6. Push the button on the upper-left side of the Integrated Ballot Box and pull the back of the Integrated Ballot Box outward</p>
		
<p>7. Press the button at the center of the plastic top cover and pull it outward</p>	<p>8. Open the metal printer cover upward</p>	<p>9. Pull the entire metal printer tray upward</p>
		

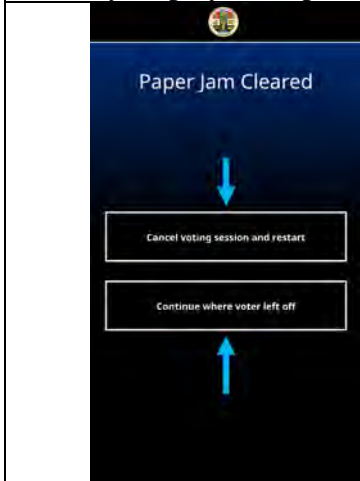
<p>10. Remove the jammed paper from the printer</p>	<p>11. Close the metal printer tray</p>	<p>12. Close the Plastic Top Cover</p>
		
<p>13. Close the Integrated Ballot Box</p>	<p>14. Place a new tamper-evident seal on the seam of the IBB and Zip Tie per LA County procedure and log it into the Chain of Custody. Be sure to tightly cinch the Zip Tie to ensure the IBB is secured</p>	<p>15. Tap Next on the Resolve Paper Jam screen</p>
		
<p>16. The Touchscreen will prompt the Election Worker to scan their Security Pass</p>		<p>17. Enter Credentials</p> <p>18. Tap Continue</p>



19. If the Ballot jammed as the voter was printing the Ballot, tap **Continue where voter left off**. Selecting this option will prompt the **BMD** to reprint the voter's ballot. If the Ballot jammed when entering the **BMD**, tap **Cancel voting session and restart**.

Note: The screen below will only display this option

20. Escort the voter to the Check-in Clerk where a replacement ballot will be printed and given to the voter. Follow LA County procedure to spoil the damaged Ballot. Load the new blank ballot into the **BMD**. If the paper jammed while the ballot was printing, the **BMD** will reprint the ballot at this stage



13.11.2. Problem: BMD Cannot Read a Ballot

1. Unlock BMD with security credentials and retrieve Ballot
2. Check if the ballot is damaged
 - a. If the ballot is damaged, spoil the ballot and issue a new ballot
3. If the ballot is undamaged insert the ballot again
4. If the error message happens again, move voter to a second BMD
 - a. If the ballot cannot be read on the second BMD, spoil the ballot and issue a new ballot
 - b. If the ballot can be read on the second BMD:
 - i. Clean the Scanner on the first BMD
5. If the first BMD cannot read another ballot, remove it from service

13.11.3. Problem: BMD Touchscreen is Frozen

1. Turn the BMD off and then back on again
2. If the Touchscreen remains frozen, remove the BMD from service

13.11.4. Problem: Headphones are not working

<p>1. If the headphones are not working, ensure they are plugged into an audio port</p>	<p>2. If the headphones still do not work, plug them into the other audio port</p>	<p>3. If the headphones still do not work, try a new pair of headphones</p>
		
<p>4. If the new headphones do not work, try them on another BMD. If the headphones function properly in the new BMD, the voter will move to the new BMD and continue voting from there</p>	<p>5. The Election Worker will power down the original BMD. Follow the steps in section 3.3.5 Restarting the BMD after an Interruption</p>	<p>6. If the headphones continue to malfunction with the original BMD, the Election Worker removes the BMD from service</p>
		

14. Absentee/Mail Ballot Procedures

14.1. System Startup and Pre-Tabulation Report Procedures

This section covers the main installation process for Tally. It can be executed either as a step-by-step walk through or by command flags. For new users, the step-by-step mode is recommended.

```
# run command to preserve the output
script /tmp/`date "+%Y%m%d-%H%M"`-installer.script

# go into the scripts directory on the deployment system
cd /tmp/tally_deployment/scripts
# to run the installer, /ssh-user is a user that has been granted ssh access to all
nodes in the cluster.
./installer ssh-user flags
```

14.2. Configuration

When the main installer starts, it will require the user to specify the nodes that will be included in the cluster, as well as their type.

The first node to be setup will be the deployment system. The deployment system configuration cannot be changed once in the current version of the installer, so double check the inputted values before submitting the information. Also, the first node is where HA proxy is deployed and will be the entry point for Tally through the web browser.

```
# enter the deployment system hostname
Enter the hostname configured for this master system
Enter a value: deployment-system-hostname

Enter the ip address configured for this master system
Enter a value: deployment-system-ip-address
```

Below is an example configuration once the first master system has been setup:

```
-----
| Node Type | Hostname | IP |
|-----|-----|-----|
| MASTER | lac-df-master1 | 10.0.5.151 |
|-----|-----|-----|
```

Next you will have the option to: 1) Enter a new node, 2) remove an existing node, 3) Finished. If the only node that has been setup is the deployment node, you will not be able to remove an existing node. Entering a new node will lead to a multi-node cluster and finishing the setup will lead to a single-node cluster.

On a multi-node cluster, it is mandatory to set at least one:

- Master node
- Compute node
- Provider node

If a file node is not added to the configuration, then the file sharing steps will be skipped altogether.

Below is an example of a valid multi-node cluster setup, which appears once you finish the setup:

```
-----  
| Node Type | Hostname | IP |  
-----  
| MASTER* | lac-df-master1 | 10.0.5.151 |  
| COMPUTE | lac-df-compute1 | 10.0.5.161 |  
| PROVIDER | lac-df-provider1 | 10.0.5.171 |  
| FILE | lac-df-compute1 | 10.0.5.161 |  
-----  
* = This node (the build system)
```

The output above will be paired with the following prompt:

```
The above are the nodes that you have configured, is this correct? (y/n)
```

```
Enter a value:
```

Entering 'y' will end the configuration and proceed to the next step in the installer. Entering 'n' will allow you to make changes to the configuration. As a reminder, the only node that cannot be modified is the first master system.

The last step in node configuration is to name the configuration:

```
What is the name of this cluster?  
Enter a value: cluster-name
```

Keep track of the name you use for the cluster. If the installation is interrupted past this prompt, you will need to input the name to continue with the installation of Tally. Otherwise, you will need to redo the node configuration.

14.3. Starting Tally

Once the cluster and its various nodes have been set up and the Docker registry has been loaded onto the cluster, the Tally system can be started by running the `create_all` script.

To do this, run the following:

```
cd /tmp/tally_deployment/scripts  
./create_all -k  
What is the name of the configured cluster to use?  
Enter a value:
```

After this process is complete, check kubernetes system pods and the cluster nodes to check the cluster's status:

```
# check the pods running the kubernetes system
kubect1 get pods -n kube-system
# check the pods updating in realtime
kubect1 get pods -n tally -w
# check the status posted by each node
kubect1 get nodes
```

The [deployment-system-hostname] can be referenced in the example configuration output. This will compile template files for the tally system into .yaml files to create kubernetes pods.

This process includes 3 flags: --node-color , --kube-create, and --development.

-k --kube-create indicates that the process should also create k8s pods based on the compiled .yaml files, which will start the Tally system.

Regardless of deployment type, the system may take several minutes to start.

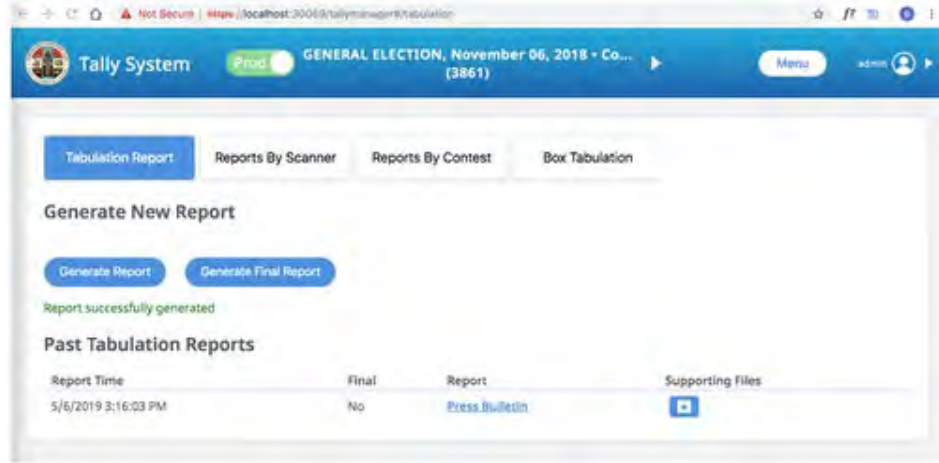
```
# check the status of the pods
kubect1 get pods -n tally
```

To determine when the system is ready for viewing, check the tallymanager-deployment pod's log to determine if tallymanager is completely spun up yet:

```
kubect1 logs [tallymanager-deployment-pod-name] -n tally
```

14.4. Tabulation Procedures

After all the ballots have gone through Receive, Recognize, and Refine, the user can view reports. From the Home page header, navigate via the main menu drop-down to Reports > Tabulation. A tabulator's first tabulation event must not happen before 8 p.m. local time on the night of the election. This is fully managed through the election process.



14.4.1. Generate Report:

- 1. From the heading drop-down, select the election that needs reports run
- 2. Set the test/production toggle to match the type of ballots processed
- 3. Refresh the page

4. Select the type of report needed -- Tabulation (overall), by scanner, by contest, or box tabulation
5. For Tabulation Report, click the “Generate Reports” button, and after a short time a new Press Bulletin link will be generated along with supporting downloadable files. Click on the Press Bulletin link and review the Semi-Final Election results that display in a new browser tab

14.4.2. Generate Final Report:

1. Select the type of report needed and click on the “Generate Final Reports” button. After a short time, a new Press Bulletin link will be generated with a “Yes” in the Final column
2. Click on the Press Bulletin link and review the Final Election results that display in a new browser tab

14.5. Post-Tabulation Report and Shutdown Procedures

To stop the tally system and delete running services, run

```
# go into the installer directory on the deployment system
cd /tmp/tally_deployment/scripts/
# delete the tally resources
./delete
```

This will delete all resources generated by files found in the configuration dist directory.

To check that all resources have been deleted, run the following command:

```
kubectl get all -n tally
```


15. Semi-Official Canvass

Officials will comply with the Use Procedures approved by the Secretary of State for the VSAP Voting System.

15.1. System Start-up and Pre-tabulation Reports

Once the Tally System Environment is set up and the election is configured you can start the system for tabulation.

15.1.1. Start Tally Services

The first step is to start the Tally System services. To start the services you provide a start script. There are several command line options that will need to be provided for different setups.

The following are the individual commands that can be run to start the services:

```
sudo python scripts/run.py # single node Tally machine deployment
sudo python scripts/run.py -t services # services machine deployment
sudo python scripts/run.py -t providers # providers machine deployment
```

The `-t/--type` argument accepts two valid options, “services” and “providers”. If the type parameter is not passed, the run script will assume it is being executed on the single Tally machine deployment. The scripts are run from the `/opt/tally` directory.

If this is the first time starting the environment, or if the database has been cleared, provide the `-seed` argument (or `--seed-db` argument) to empty and recreate the base schema for tally in the database. This will erase all existing database data. For single node deployment, the script should be run on the Tally System machine. For the two node deployment, the script should be run on providers machine.

Single node Tally System machine:

```
sudo python scripts/run.py -seed
```

Two node providers machine:

```
sudo python scripts/run.py -seed -t providers
```

If the `-d/--detached` argument is passed, the Tally System will start detached from terminal, running as a background process:

```
sudo python scripts/run.py -d
```

15.1.2. VSAP Tally Manager

The Tally Manager is the Tally System user interface. It is designed to work on the Google Chrome browser. Other browsers are not supported.

1. Open the Chrome Browser

2. Enter address "192.168.7.80"
3. Log in

15.1.3. Processing VBM Ballots

All staff processing VBM ballots are required to check in with a Tally System supervisor and sign a log in sheet with date, time and scan station. When work is completed or assignments change, staff are to sign out with date, time and scan station.

VBM ballot processing roles per scanner:

- One staff operating the scanner. Role includes loading, removing and starting the scanner
- One supervisor is responsible for managing and monitoring a scanner
- Input runners are used for moving boxes of unprocessed ballots to scanners and assist preparing ballots for scanner operator including unboxing and jogging ballots
- Output runners used to box processed ballots and move them to staging area for ballot storage
- One snag Operator for every two scanners. Manages ballots not able to be processed by the scanner and reports them to ballot remakes
- Ballot storage operators scan processed ballot boxes with a storage location

Instructions on operating the ballot scanners are available in the System Operation Manual.

15.2. Processing vote reports

Once all the ballots have gone through Receive, Recognize, and Refine and have returned to IDLE status, the user can view reports.

From the Home page header, click on a menu tab labeled **Tabulate/Reports** . This displays a page with two subsections: **Generate New Reports** and **Past Tabulation Reports**.



1. Click the **Generate Reports** button, and after a short time a new Tabulation ID link will be generated.
2. Click on the Tabulation ID link and review the Semi-Final Election results that display in a new browser tab.
3. Navigate back to the **Tabulate/Reports** tab and click on the **Generate Final Reports** button, and after a short time, a new Tabulation ID link will be generated.
4. Click on the Tabulation ID link and review the Final Election results that display in a new browser tab.

Once both the Semi-Final Election Results and Final Election Results pages have been reviewed, you may close the browser tabs. Navigating back to the Reports browser tab, you may reload the page and see that new entries under Past Tabulation Reports now display. These were the reports that you previously generated.

15.3. Central tabulation

Tabulation can begin once the Tally System is configured, services have started, and the Tally Manager is logged on.

15.4. Precinct Tabulation

Not applicable as ballots are tabulated centrally.

15.5. Integration with Other Systems and Calvoter Aggregator Application

The Aggregator Application integrates election results between the MTS system with the Tally System. The Aggregator Application is a command line driven application. Below are the basic commands to aggregate totals.

For help on available commands and syntax type:

```
./aggregate -help
```

The mts_summary.dat (MTS results file) and vsap.json (Tally System results file) that need to be aggregated are put into the “inputs” folder. These files are copied using removable digital media.

Type the following to start aggregating the totals:

```
./aggregate
```

The following result files are put into the output and archive folder:

- Mts_summary.dat - New aggregated results in MTS result file format
- Press.html - Semi-Official Results Press Bulletin
- Lna.html - Logic and Accuracy Results Report. Contains a matrix of counter and value
- Vsap.json - New aggregated results in Tally System results file format

To create a version of Final Official Press Bulletin enter the following command:

```
./aggregate -final=true
```

15.5.1. CalVoter

Officials' MTS and ECBMS complies with election night vote reporting using electronic files. These reports are put in the Secretary of State CalVoter II system sftp. The CalVoter II system retrieve the report, transfer the data to the database, and process the information into the elections reporting system.

16. Official Canvass and Post-Election Procedures

16.1. Election Observer Panel

The purpose of Election Observers is to:

- Provide an avenue for public observation of and input into the election process
- Assist in ensuring the integrity of the election process
- Encourage participation and build voter confidence in the election process

Invitation

Between E-60 and E-30, prepare a media release and letters of invitation (see samples attached) to parties likely to participate, such as the following:

- County Grand Jury
- Political Party Central Committee Members
- Language Advocacy Groups
- Community Based Organizations
- Media

Other groups or individuals expressing an interest in observing election day activities may also be included in the observer panel, as deemed appropriate.

Group Presentations

After letters of invitation have been sent out, offer to attend group meetings to provide an opportunity for the groups to ask questions about the process. Groups should be contacted to arrange time on their agendas for staff presentations. This is optional at the request of the group, but staff should make every effort to contact the groups and offer this service.

Appointment Letters (for introduction to precinct workers)

After the groups have provided the names of interested panelists, prepare letters of introduction (see sample attached) for the panelists to use when visiting polling places on Election Day. Materials to be prepared for each panelist will include a listing of all polling places within the county for that specific election as well as the central counting site location and hours of operation.

Mechanism for Feedback

Observers attend training at government facilities, where they can ask questions about the process.

General Rules for Observers

Observers may:

- Observe the proceedings at the polls, including the opening and closing procedures
- Obtain information from the precinct index that is posted near the entrance
- Make notes and watch all procedures
- View all activities at the central counting site on election day

- View the canvass of the vote activities following the election
- View absentee and provisional ballot processing
- Ask questions of staff or voters at the polls
- Ask questions of supervisors at the central counting site

Observers are responsible for:

- Checking in at each site, whether polling place or central counting site
- Wearing an identification badge
- Maintaining a professional manner while observing the election processes
- Ensuring they do not interfere with the elections process

Observers may not:

- Interfere in any way with the conduct of the election
- Touch any voting materials or equipment or sit at the official worktables
- Converse with voters (within 100 feet of the entrance to a polling place) regarding the casting of a vote, or speak to a voter regarding his or her qualifications to vote
- Display any election material or wear campaign badges, buttons or apparel
- Wear the uniform of a peace officer, a private guard, or security personnel
- Use cellular phones, pagers, or two-way radios inside the polling place and/or within 100 feet of the entrance to the polling place
- Talk to central counting site workers while they are processing ballots
- Use the telephones, computers or other polling place facilities at polling places or the central counting site
- Touch election personnel
- Eat or drink in the polls or the central counting site
- Assist in operations at any polling place

16.2. Canvassing Precinct Returns

Time for Conducting Canvass

The canvass shall commence no later than the Thursday following the election, shall be open to the public, and, for state or statewide elections, shall result in a report of results to the Secretary of State. The canvass shall be continued daily, Saturdays, Sundays, and holidays excepted, for not less than six hours each day until completed.

Tasks of the Official Canvass

The official canvass shall include, but not be limited to, the following tasks:

- An inspection of all materials and supplies returned by poll workers
- A reconciliation of the number of signatures on the roster with the number of ballots recorded on the ballot statement
- In the event of a discrepancy in the reconciliation, the number of ballots received from each polling place shall be reconciled with the number of ballots cast, as indicated on the ballot statement
- A reconciliation of the number of ballots counted, spoiled, canceled, or invalidated due to identifying marks, overvotes, or as otherwise provided by statute, with the number of votes recorded, including vote by mail and provisional ballots, by the vote counting system
- Processing and counting any valid vote by mail and provisional ballots not included in the semifinal official canvass
- Counting any valid write-in votes
- Reproducing any damaged ballots, if necessary
- Reporting final results to the governing board and the Secretary of State, as required

Examination of Materials Returned from Precincts

In jurisdictions using a central counting place, the elections official may appoint not less than three deputies to open the envelopes or containers with the materials returned from the precincts. If, after examination, any of the materials are incomplete, ambiguous, not properly authenticated, or otherwise defective, the precinct officers may be summoned before the elections official and examined under oath to describe polling place procedures and to correct the errors or omissions.

16.3. Canvassing Absentee Ballots

16.3.1. Processing and Counting Vote by Mail Ballots

Vote by mail ballots and mail ballot precinct ballots returned to the elections office and to the polls on or before election day that are not included in the semifinal official canvass phase of the election, including any ballots returned to another jurisdiction in the state and forwarded to the elections official who issued the ballot, shall be processed and counted during the official canvass as described below.

16.3.2. Processing Vote by Mail Ballots

(a) Any jurisdiction in which vote by mail ballots are cast may begin to process vote by mail ballot return envelopes beginning 29 days before the election. Processing vote by mail ballot return envelopes may include verifying the voter's signature on the vote by mail ballot return envelope and updating voter history records.

(b) Any jurisdiction having the necessary computer capability may start to process vote by mail ballots on the 10th business day before the election. Processing vote by mail ballots includes opening vote by mail ballot return envelopes, removing ballots, duplicating any damaged ballots, and preparing the ballots to be machine read, or machine reading them, including processing write-in votes so that they can be tallied by the machine, but under no circumstances may a vote count be accessed or released until 8 p.m. on the day of the election. All other jurisdictions shall start to process vote by mail ballots at 5 p.m. on the day before the election.

(c) Results of any vote by mail ballot tabulation or count shall not be released before the close of the polls on the day of the election.

16.3.3. Observation of Vote by Mail Ballot Processing and Counting

(a) The processing of vote by mail ballot return envelopes, and the processing and counting of vote by mail ballots, shall be open to the public, both prior to and after the election.

(b) A member of the county grand jury, and at least one member each of the Republican county central committee, the Democratic county central committee, and of any other party with a candidate on the ballot, and any other interested organization, shall be permitted to observe and challenge the manner in which the vote by mail ballots are handled, from the processing of vote by mail ballot return envelopes through the counting and disposition of the ballots.

(c) The elections official shall notify vote by mail voter observers and the public at least 48 hours in advance of the dates, times, and places where vote by mail ballots will be processed and counted.

(d) Vote by mail voter observers shall be allowed sufficiently close access to enable them to observe the vote by mail ballot return envelopes and the signatures thereon and challenge whether those individuals handling vote by mail ballots are following established procedures, including all of the following:

(1) Verifying signatures and addresses on the vote by mail ballot return envelopes by comparing them to voter registration information.

(2) Duplicating accurately damaged or defective ballots.

(3) Securing vote by mail ballots to prevent tampering with them before they are counted on election day.

(e) A vote by mail voter observer shall not interfere with the orderly processing of vote by mail ballot return envelopes or the processing and counting of vote by mail ballots, including the touching or handling of the ballots.

16.3.4. Challenges

Prior to processing and opening the identification envelopes of vote by mail voters, the elections official shall make available a list of vote by mail voters for public inspection, from which challenges may be presented. Challenges may be made for the same reasons as those made against a voter voting at a polling place. In addition, a challenge may be entered on the grounds that the ballot was not received within the time provided by this code or that a person is imprisoned for a conviction of a felony. All challenges shall be made prior to the opening of the identification envelope of the challenged vote by mail voter.

Except as otherwise provided, the processing of vote by mail ballot return envelopes, the processing and counting of vote by mail ballots, and the disposition of challenges of vote by mail ballots shall be according to the laws now in force pertaining to the election for which they are cast. Because the voter is not present, the challenger shall have the burden of establishing extraordinary proof of the validity of the challenge at the time the challenge is made.

If a challenge is overruled, the board shall open the identification envelope without defacing the affidavit printed on it or mutilating the enclosed ballot and, without viewing the ballot, remove it and destroy the numbered slip, if any remains, and store the ballots in a secure location.

If a challenge is allowed, the board shall endorse on the face of the identification envelope the cause of the challenge and its action thereon.

16.3.5. Comparing Signatures

(a) (1) Upon receiving a vote by mail ballot, the elections official shall compare the signature on the identification envelope with either of the following to determine if the signatures compare:

(A) The signature appearing on the voter's affidavit of registration or any previous affidavit of registration of the voter.

(B) The signature appearing on a form issued by an elections official that contains the voter's signature and that is part of the voter's registration record.

(2) In comparing signatures pursuant to this section, the elections official may use facsimiles of voters' signatures, provided that the method of preparing and displaying the facsimiles complies with the law.

(3) In comparing signatures pursuant to this section, an elections official may use signature verification technology. If signature verification technology determines that the signatures do not compare, the elections official shall visually examine the signatures and verify that the signatures do not compare.

(4) The variation of a signature caused by the substitution of initials for the first or middle name, or both, is not grounds for the elections official to determine that the signatures do not compare.

(b) If upon conducting the comparison of signatures pursuant to subdivision (a) the elections official determines that the signatures compare, he or she shall deposit the ballot, still in the identification envelope, in a ballot container in his or her office.

(c) If upon conducting the comparison of signatures pursuant to subdivision (a) the elections official determines that the signatures do not compare, the identification envelope shall not be opened and the ballot shall not be counted. The elections official shall write the cause of the rejection on the face of the identification envelope only after completing the procedures described in subdivision (d).

(d) (1) A minimum of eight days prior to the certification of the election, the elections official shall provide notice to all voters identified pursuant to subdivision (c) of the opportunity to verify their signatures no later than 5 p.m. two days prior to the certification of the election.

(2) The notice and instructions shall be in substantially the following form:

“READ THESE INSTRUCTIONS CAREFULLY. FAILURE TO FOLLOW THESE INSTRUCTIONS MAY CAUSE YOUR VOTE BY MAIL BALLOT NOT TO COUNT.
1. We have determined that the signature you provided on your vote by mail ballot does not match the signature(s) on file in your voter record. In order to ensure that your vote by mail ballot will be counted, the signature verification statement must be completed and returned as soon as possible.
2. The signature verification statement must be received by the elections official of the county where you are registered to vote no later than 5 p.m. two days prior to certification of the election.
3. You must sign your name where specified on the signature verification statement (Voter’s Signature).
4. Place the signature verification statement into a mailing envelope addressed to your local elections official. Mail, deliver, or have the completed statement delivered to the elections official. Be sure there is sufficient postage if mailed and that the address of the elections official is correct.
5. If you do not wish to send the signature verification statement by mail or have it delivered, you may submit your completed statement by email or facsimile transmission to your local elections official using the information provided.”

(3) The elections official shall not reject a vote by mail ballot identified pursuant to subdivision (c) if each of the following conditions is satisfied:

(A) The voter delivers, in person, by mail, by fax, or by email, a signature verification statement signed by the voter and the elections official receives the statement no later than 5 p.m. two days prior to the certification of the election, or the voter, before the close of the polls on election day, completes and submits a signature verification statement to a polling place within the county or a ballot dropoff box.

(B) Upon receipt of the signature verification statement, the elections official shall compare the signature on the statement with the signature on file in the voter's record.

(i) If upon conducting the comparison of signatures the elections official determines that the signatures compare, he or she shall deposit the ballot, still in the identification envelope, in a ballot container in his or her office.

(ii) If upon conducting the comparison of the signatures the elections official determines that the signatures do not compare, the identification envelope shall not be opened and the ballot shall not be counted. The elections official shall write the cause of the rejection on the face of the identification envelope.

(4) The signature verification statement shall be in substantially the following form and may be included on the same page as the notice and instructions specified in paragraph (2):

"SIGNATURE VERIFICATION STATEMENT
I, am a registered voter of _____ County,
State of California. I declare under penalty of perjury that I requested and returned a vote by mail ballot. I am a resident of the precinct in which I have voted, and I am the person whose name appears on the vote by mail ballot envelope. I understand that if I commit or attempt any fraud in connection with voting, or if I aid or abet fraud or attempt to aid or abet fraud in connection with voting, I may be convicted of a felony punishable by imprisonment for 16 months or two or three years. I understand that my failure to sign this statement means that my vote by mail ballot will be invalidated.
Voter's Signature
Address"

(5) An elections official shall include the vote by mail ballot signature verification statement and instructions provided in this subdivision on his or her Internet Web site, and shall provide the election official's mailing address, email address, and facsimile transmission number on the Internet Web page containing the statement and instructions.

(6) If the elections official determines that the signatures compare, the official shall use the signature in the signature verification statement, even if returned untimely, to update the voter's signature for future elections.

(e) (1) (A) Notwithstanding any other law, if an elections official determines that a voter has failed to sign the identification envelope, the elections official shall not reject the vote by mail ballot if the voter does any of the following:

(i) Signs the identification envelope at the office of the elections official during regular business hours before 5 p.m. on the eighth day after the election.

(ii) Before 5 p.m. on the eighth day after the election, completes and submits an unsigned ballot statement in substantially the following form:

“UNSIGNED BALLOT STATEMENT
I, am a registered voter of _____ County,
State of California. I declare under penalty of perjury that I requested and returned a vote by mail ballot and that I have not and will not vote more than one ballot in this election. I am a resident of the precinct in which I have voted, and I am the person whose name appears on the vote by mail ballot envelope. I understand that if I commit or attempt any fraud in connection with voting, or if I aid or abet fraud or attempt to aid or abet fraud in connection with voting, I may be convicted of a felony punishable by imprisonment for 16 months or two or three years. I understand that my failure to sign this statement means that my vote by mail ballot will be invalidated.
Voter’s Signature
Address”

(iii) Before the close of the polls on election day, completes and submits an unsigned ballot statement, in the form described in clause (ii), to a polling place within the county or a ballot dropoff box.

(B) If timely submitted, the elections official shall accept any completed unsigned ballot statement. Upon receipt of the unsigned ballot statement, the elections official shall compare the voter’s signature on the statement in the manner provided by this section.

(i) If the elections official determines that the signatures compare, he or she shall attach the unsigned ballot statement to the identification envelope and deposit the ballot, still in the identification envelope, in a ballot container in his or her office.

(ii) If the elections official determines that the signatures do not compare, the identification envelope shall not be opened and the ballot shall not be counted.

(C) An elections official may use methods other than those described in subparagraph (A) to obtain a voter’s signature on an unsigned identification envelope.

(2) Instructions shall accompany the unsigned ballot statement in substantially the following form:

“READ THESE INSTRUCTIONS CAREFULLY BEFORE COMPLETING THE STATEMENT. FAILURE TO FOLLOW THESE INSTRUCTIONS MAY CAUSE YOUR BALLOT NOT TO COUNT.
1. In order to ensure that your vote by mail ballot will be counted, your statement should be completed and returned as soon as possible so that it can reach the elections official of the county in which your precinct is located no later than 5 p.m. on the eighth day after the election.
2. You must sign your name on the line above (Voter’s Signature).

3. Place the statement into a mailing envelope addressed to your local elections official. Mail, deliver, or have delivered the completed statement to the elections official. Be sure there is sufficient postage if mailed and that the address of the elections official is correct.

4. If you do not wish to send the statement by mail or have it delivered, you may submit your completed statement by facsimile or email transmission to your local elections official, or submit your completed statement to a polling place within the county or a ballot drop-off box before the close of the polls on election day.”

(3) An elections official shall include the unsigned ballot statement and instructions described in this subdivision on his or her Internet Web site, and shall provide the elections official’s mailing address, email address, and facsimile transmission number on the Internet Web page containing the statement and instructions.

(f) A ballot shall not be removed from its identification envelope until the time for processing ballots. A ballot shall not be rejected for cause after the identification envelope has been opened.

16.4. Canvassing Provisional Ballots

16.4.1. Voting a Provisionally Cast Ballot

(a) At all elections, a voter claiming to be properly registered, but whose qualification or entitlement to vote cannot be immediately established upon examination of the roster for the precinct or upon examination of the records on file with the county elections official, shall be entitled to vote a provisional ballot as follows:

- (1) An elections official shall advise the voter of the voter's right to cast a provisional ballot.
- (2) The voter shall be provided a provisional ballot, written instructions regarding the process and procedures for casting the ballot, and a written affirmation regarding the voter's registration and eligibility to vote. The written instructions shall include the information set forth in subdivisions (c) and (d).
- (3) The voter shall be required to execute, in the presence of an elections official, the written affirmation stating that the voter is eligible to vote and registered in the county where the voter desires to vote.

16.4.2. Handling of Ballot

(b) Once voted, the voter's ballot shall be sealed in a provisional ballot envelope, and the ballot in its envelope shall be deposited in the ballot box. All provisional ballots voted shall remain sealed in their envelopes for return to the elections official in accordance with the elections official's instructions. The provisional ballot envelopes specified in this subdivision shall be of a color different than the color of, but printed substantially similar to, the envelopes used for vote by mail ballots, and shall be completed in the same manner as vote by mail envelopes.

(c) (1) During the official canvass, the elections official shall examine the records with respect to all provisional ballots cast. Using the procedures that apply to the comparison of signatures on vote by mail ballots, the elections official shall compare the signature on each provisional ballot envelope with the signature on the voter's affidavit of registration or other signature in the voter's registration record. If the signatures do not compare or the provisional ballot envelope is not signed, the ballot shall be rejected. A variation of the signature caused by the substitution of initials for the first or middle name, or both, shall not invalidate the ballot.

(2) (A) Provisional ballots shall not be included in any semiofficial or official canvass, except under one or more of the following conditions:

(i) The elections official establishes prior to the completion of the official canvass, from the records in his or her office, the claimant's right to vote.

(ii) The provisional ballot has been cast and included in the canvass.

(iii) Upon the order of a superior court in the county of the voter's residence.

(B) A voter may seek the court order specified in this paragraph regarding his or her own ballot at any time prior to completion of the official canvass. Any judicial action or appeal shall have priority over all other civil matters. A fee shall not be charged to the claimant by the clerk of the court for services rendered in an action under this section.

(3) The provisional ballot of a voter who is otherwise entitled to vote shall not be rejected because the voter did not cast his or her ballot in the precinct to which he or she was assigned by the elections official.

(A) If the ballot cast by the voter contains the same candidates and measures on which the voter would have been entitled to vote in his or her assigned precinct, the elections official shall count the votes for the entire ballot.

(B) If the ballot cast by the voter contains candidates or measures on which the voter would not have been entitled to vote in his or her assigned precinct, the elections official shall count only the votes for the candidates and measures on which the voter was entitled to vote in his or her assigned precinct.

16.5. Canvassing Write-in Votes

16.5.1. Counting Write-In Votes

Any name written upon a ballot for a qualified write-in candidate, including a reasonable facsimile of the spelling of a name, shall be counted for the office, if it is written in the blank space provided and voted as specified below:

- (a) For voting systems in which write-in spaces appear directly below the list of candidates for that office and provide a voting space, no write-in vote shall be counted unless the voting space next to the write-in space is marked or slotted as directed in the voting instructions, except as provided in subdivision (f).
- (b) For voting systems in which write-in spaces appear separately from the list of candidates for that office and do not provide a voting space, the name of the write-in candidate, if otherwise qualified, shall be counted if it is written in the manner described in the voting instructions.
- (c) The use of pressure-sensitive stickers, glued stamps, or any other device not provided for in the voting procedures for the voting systems approved by the Secretary of State to indicate the name of the write-in candidate are not valid, and a name indicated by these methods shall not be counted.
- (d) Neither a vote cast for a candidate whose name appears on the ballot nor a vote cast for a write-in candidate shall be counted if the voter has indicated, by a combination of marking and writing, a choice of more names than there are candidates to be nominated or elected to the office.
- (e) All valid write-in votes shall be tabulated and certified to the elections official on forms provided for this purpose, and the write-in votes shall be added to the results of the count of the ballots at the counting place and be included in the official returns for the precinct.
- (f) (1) In an election that uses a voting system described in subdivision (a), after tallying all eligible votes but prior to completion of the official canvass and the issuance of the certified statement of the results pursuant to this chapter, the elections official, upon the request of a qualified write-in candidate for an office being voted on in that election for an examination of undervotes that is received within five days of completion of the semiofficial canvass, may hand tally the remaining undervotes if any of the following is applicable:
 - (A) In the case of a primary election or a special election, the sum of the total number of votes cast for the write-in candidate and the total number of undervotes cast for the office but not examined pursuant to a hand tally is equal to or greater than the total number of votes cast for the candidate receiving the second highest number of votes for that office.
 - (B) In the case of a general election or a special runoff election, the sum of the total number of votes cast for the write-in candidate and the total number of undervotes cast for the office but not examined pursuant to a hand tally is equal to or greater than the total number of votes cast for the candidate receiving the highest number of votes for that office.
 - (C) In the case of an office for which a voter may vote for more than one candidate, the sum of the total number of votes cast for the write-in candidate and the total number of undervotes cast for the office but not examined pursuant to a hand tally is equal to or greater than the total

number of votes cast for the candidate receiving the least number of votes that would be sufficient in order to be elected.

(2) The elections official may stop a hand tally conducted pursuant to this subdivision when the official determines that the applicable condition in any of subparagraphs (A) to (C), inclusive, of paragraph (1) is no longer applicable, or when all of the undervotes for the office have been examined.

(3) In conducting a hand tally pursuant to this subdivision, the elections official shall count a vote for the office if the intent of the voter can be determined, regardless of whether the voter has complied with the voting instructions. The elections official shall include the results of a hand tally conducted pursuant to this subdivision in the official canvass of the election.

(4) For purposes of this subdivision, “undervote” means a ballot on which a voter failed to cast any vote for a specific office or failed to cast the maximum number of votes permitted, as detected by an electronic, mechanical, or other vote-tabulating device.

16.6. Manual Tally Procedures

16.6.1. Manual Tally Using a Voting System

(a) During the official canvass of every election in which a voting system is used, the official conducting the election shall conduct a public manual tally of the ballots tabulated by those devices, including vote by mail ballots, using either of the following methods:

(1) (A) A public manual tally of the ballots canvassed in the semifinal official canvass, including vote by mail ballots but not including provisional ballots, cast in 1 percent of the precincts chosen at random by the elections official. If 1 percent of the precincts is less than one whole precinct, the tally shall be conducted in one precinct chosen at random by the elections official.

(B) (i) In addition to the 1 percent manual tally, the elections official shall, for each race not included in the initial group of precincts, count one additional precinct. The manual tally shall apply only to the race not previously counted.

(ii) The elections official may, at his or her discretion, select additional precincts for the manual tally, which may include vote by mail and provisional ballots.

(2) A two-part public manual tally, which includes both of the following:

(A) A public manual tally of the ballots canvassed in the semifinal official canvass, not including vote by mail or provisional ballots, cast in 1 percent of the precincts chosen at random by the elections official and conducted pursuant to paragraph (1).

(B) (i) A public manual tally of not less than 1 percent of the vote by mail ballots canvassed in the semifinal official canvass. Batches of vote by mail ballots shall be chosen at random by the elections official.

(ii) For purposes of this section, a “batch” means a set of ballots tabulated by the voting system devices, for which the voting system can produce a report of the votes cast.

(iii) (I) In addition to the 1 percent manual tally of the vote by mail ballots, the elections official shall, for each race not included in the initial 1 percent manual tally of vote by mail ballots, count one additional batch of vote by mail ballots. The manual tally shall apply only to the race not previously counted.

(II) The elections official may, at his or her discretion, select additional batches for the manual tally, which may include vote by mail and provisional ballots.

(b) If vote by mail ballots are cast on a direct recording electronic voting system at the office of an elections official or at a satellite location of the office of an elections official pursuant to Section 3018, the official conducting the election shall either include those ballots in the manual tally conducted pursuant to paragraph (1) or (2) of subdivision (a), or conduct a public manual tally of those ballots cast on no fewer than 1 percent of all the direct recording electronic voting machines used in that election chosen at random by the elections official.

(c) The elections official shall use either a random number generator or other method specified in regulations that shall be adopted by the Secretary of State to randomly choose the initial

precincts, batches of vote by mail ballots, or direct recording electronic voting machines subject to the public manual tally.

(d) The elections official shall not randomly choose the initial precincts or select an additional precinct for the manual tally until after the close of the polls on election day.

(e) The manual tally shall be a public process, with the official conducting the election providing at least a five-day public notice of the time and place of the manual tally and of the time and place of the selection of the precincts, batches, or direct recording electronic voting machines subject to the public manual tally before conducting the selection and tally.

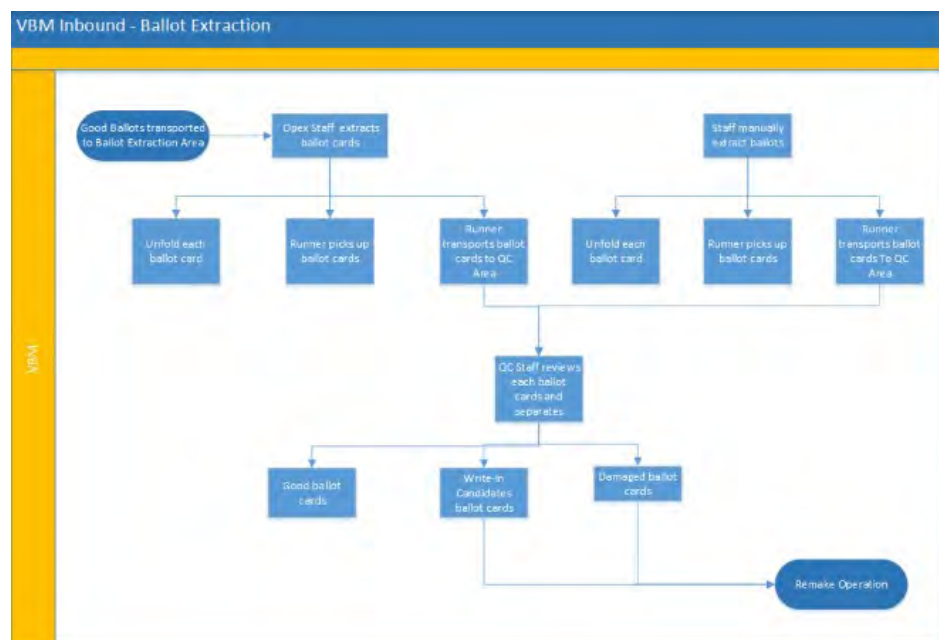
(f) The official conducting the election shall include a report on the results of the 1 percent manual tally in the certification of the official canvass of the vote. This report shall identify any discrepancies between the machine count and the manual tally and a description of how each of these discrepancies was resolved. In resolving a discrepancy involving a vote recorded by means of a punch card voting system or by electronic or electro-mechanical vote tabulating devices, the voter verified paper audit trail shall govern if there is a discrepancy between it and the electronic record.

16.7. Handling Ballot Exceptions

VBM ballot extraction begins e-14. During this process QC Staff reviews each ballot and separates good ballots with ones that need further review.

QC tasks include:

- Remove any portion of the ballot stub, such as an incompletely detached perforation, that remains attached to a ballot card
- Jog cards for static electricity removal
- Inspect the ballots for tears, folds, or damage
- Damaged ballots are to be placed in the ballot remake box
- Inspect the ballots for any identifying marks, such as a person's name, as instructed
- Ballots with identifying marks are placed in the ballot remake box
- Inspect the marks on all ballots as instructed
- When all ballots have been inspected align them so the printed black corner is in the upper right corner



Tally System vote mark detector is an operation that determines if the vote mark is selected or not. Vote mark detector depends on the Tally Layout Definition File (TLDF) to inform how it will be run. The TLDF also lists out the vote marks that need to be processed by ballot style id. When calculating whether a vote mark should be considered as selected or not, the number of pixels counted is compared against this total number of pixels. The target zone of is 113 x 113 pixels with a total of 12,769 pixels, each pixel accounts for about 0.0078% of the total target area. The current configuration for the percentage threshold is 8.1%-100% of the target area. This amounts to at least 1,034px of the 12,769px. If there are more than that many pixels, then the vote mark is counted as a selection.

16.8. Post-Election Logic and Accuracy Testing

After an election, Logic and Accuracy testing must be done on to ensure the ballot layouts are correct. See Section 8.3 Using L&A on the BMD for details regarding testing.

16.9. Final Reporting of Official Canvass

16.9.1. Sealing of Ballots

After ballots are counted and sealed, the elections official may not open any ballots nor permit any ballots to be opened except as permitted by law or in the event of a recount.

16.9.2. Results

Upon completion of the count, the elections official shall add to the results as so determined, the results of the write-in votes and any paper ballots used as certified by the precinct board, and thereupon shall declare the vote, and forthwith post one copy at the counting place for public inspection.

(a) The elections official shall prepare a certified statement of the results of the election and submit it to the governing body within 30 days of the election or, in the case of school district, community college district, county board of education, or special district elections conducted on the first Tuesday after the first Monday in November of odd-numbered years, no later than the last Monday before the last Friday of that month.

(b) The elections official shall post the certified statement of the results of the election on his or her Internet Web site in a downloadable spreadsheet format that may include, but is not limited to, a comma-separated values file or a tab-separated values file and that is compatible with a spreadsheet software application that is widely used at the time of the posting. The certified statement of the election results shall be posted and maintained on the elections official's Internet Web site for a period of at least 10 years following the election. This subdivision shall apply only to an elections official who uses a computer system that has the capability of producing the election results in a downloadable spreadsheet format without requiring modification of the computer system.

When ballots are counted, the result of the vote shall be shown by precinct.

(a) The statement of the result shall show all of the following:

(1) The total number of ballots cast.

(2) The number of votes cast at each precinct for each candidate and for and against each measure.

(3) The total number of votes cast for each candidate and for and against each measure.

(b) The statement of the result shall also show the number of votes cast in each city, Assembly district, congressional district, senatorial district, State Board of Equalization district, and supervisorial district located in whole or in part in the county, for each candidate for the offices of presidential elector and all statewide offices, depending on the offices to be filled, and on each statewide ballot proposition.

16.9.3. Transmission to Secretary of State

The elections official shall send to the Secretary of State within 31 days of the election in an electronic format in the manner requested one complete copy of all results as to all of the following:

- (a) All candidates voted for statewide office.
- (b) All candidates voted for the following offices:
 - (1) Member of the Assembly.
 - (2) Member of the Senate.
 - (3) Member of the United States House of Representatives.
 - (4) Member of the State Board of Equalization.
 - (5) Justice of the Court of Appeal.
 - (6) Judge of the superior court.
- (c) All persons voted for at the presidential primary. The results for all persons voted for at the presidential primary for delegates to national conventions shall be canvassed and shall be sent within 28 days after the election.
- (d) The vote given for persons for electors of President and Vice President of the United States. The results for presidential electors shall be endorsed "Presidential Election Returns" and shall be canvassed and sent within 28 days after the election.
- (e) All statewide measures.
- (f) The total number of ballots cast.

The elections official shall deliver a duplicate of the certified statement of the result of votes cast to the chairperson of the county central committee of each party.

16.9.4. Announcement of Results

The governing body shall declare elected or nominated to each office voted on at each election under its jurisdiction the person having the highest number of votes for that office, or who was elected or nominated under the exceptions noted in law. The governing board shall also declare the results of each election under its jurisdiction as to each measure voted on at the election.

The elections official shall make out and deliver to each person elected or nominated, as declared by the governing body, except those elected to a central committee, a certificate of election or nomination, signed and authenticated by the elections official.

- (a) Whenever a candidate whose name appears upon the ballot at any election for an office other than a voter-nominated office dies after the 68th day before the election, the votes cast for the deceased candidate shall be counted in determining the results of the election for the office for

which the decedent was a candidate. If the deceased candidate receives a majority of the votes cast for the office, he or she shall be considered elected and the office to which he or she was elected shall be vacant at the beginning of the term for which he or she was elected. The vacancy thus created shall be filled in the same manner as if the candidate had died subsequent to taking office for that term.

(b) Whenever a candidate whose name appears on the ballot at any election for a voter-nominated office dies, the votes cast for the deceased candidate shall be counted in determining the results of the election for the office for which the decedent was a candidate. If the deceased candidate receives a majority of the votes cast for the office at the general election, he or she shall be considered elected and the office to which he or she was elected shall be vacant at the beginning of the term for which he or she was elected. The vacancy thus created shall be filled in the same manner as if the candidate had died subsequent to taking office for that term.

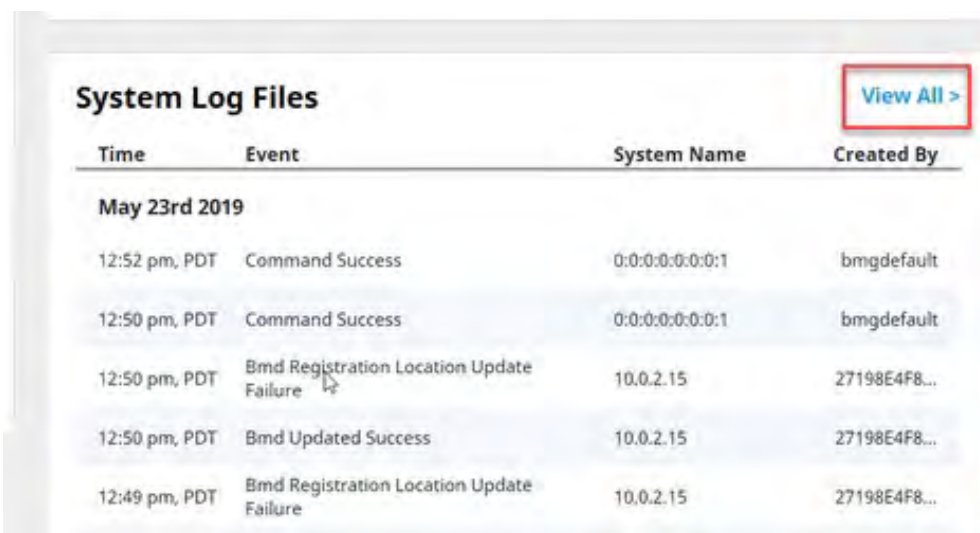
16.10. Backup and Retention of Election Material

After an election, there are some logs and files that must be downloaded and saved. See below to learn how.

16.10.1.BMG

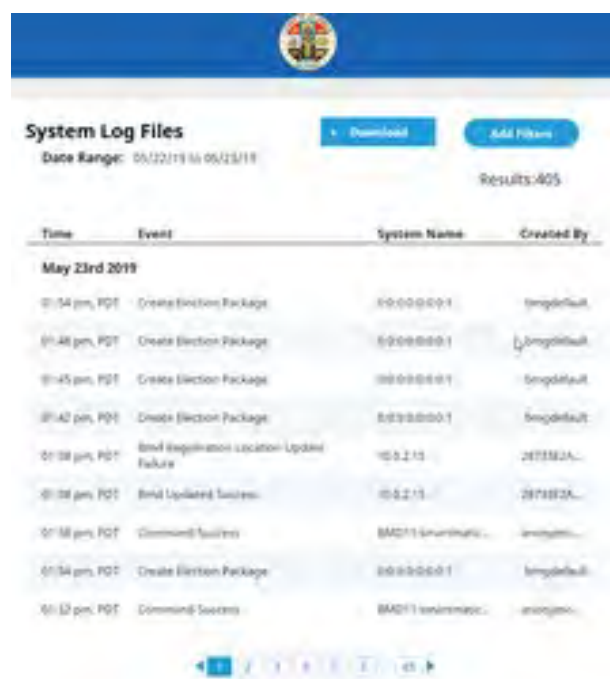
You can download a system log of events that took place in BMG. An *Event* is defined as any sort of system action that occurred on BMG. This includes any and all actions that were run on BMG, from user log-ins, diagnostic checks, BMD uploads and downloads, or any other actions taken on the BMG system. You can view and download these logs, filtered by certain criteria, by following the instructions below.

1. From the BMG home page, in the "System Log Files" menu, click View All



Time	Event	System Name	Created By
May 23rd 2019			
12:52 pm, PDT	Command Success	0:0:0:0:0:0:1	bmgdefault
12:50 pm, PDT	Command Success	0:0:0:0:0:0:1	bmgdefault
12:50 pm, PDT	Bmd Registration Location Update Failure	10.0.2.15	27198E4F8...
12:50 pm, PDT	Bmd Updated Success	10.0.2.15	27198E4F8...
12:49 pm, PDT	Bmd Registration Location Update Failure	10.0.2.15	27198E4F8...

2. A list of all system events appears with a description of the event, the time it occurred, and who performed the event



Time	Event	System Name	Created By
May 23rd 2019			
01:54 pm, PDT	Create Election Package	0:0:0:0:0:0:1	bmgdefault
01:48 pm, PDT	Create Election Package	0:0:0:0:0:0:1	bmgdefault
01:45 pm, PDT	Create Election Package	0:0:0:0:0:0:1	bmgdefault
01:42 pm, PDT	Create Election Package	0:0:0:0:0:0:1	bmgdefault
01:38 pm, PDT	Bmd Registration Location Update Failure	10.0.2.15	27198E4F8...
01:38 pm, PDT	Bmd Updated Success	10.0.2.15	27198E4F8...
01:38 pm, PDT	Command Success	BMD11-Sunshine...	anongem...
01:34 pm, PDT	Create Election Package	0:0:0:0:0:0:1	bmgdefault
01:32 pm, PDT	Command Success	BMD11-Sunshine...	anongem...

3. Click Download and choose a log file format, or click Add Filters. If no filter specification is selected, the system downloads a log of every single action by default
4. Click the dropdown button below to learn more about the different filters you can use

16.10.1.1.Filter Types

Filter by Date

You can specify a specific date range for the logs you'd like to see.

Filter By Created By

You can see a log of actions performed by a specific user.

Filter By System Name

Each type of action is given a specific system name by the BMG system. If you know the system name for the type of action you're looking for, you can enter it here.

Filter By Events

There is a filter by the type of action taken.

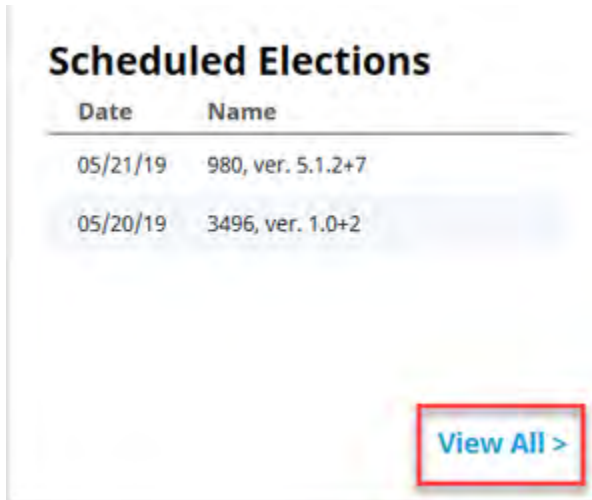
Depending on computer settings, there may be an option to download the file or open without downloading it.

If the file doesn't automatically open and can't be found in the Downloads folder, try searching for the file name *BMG Event Log*.

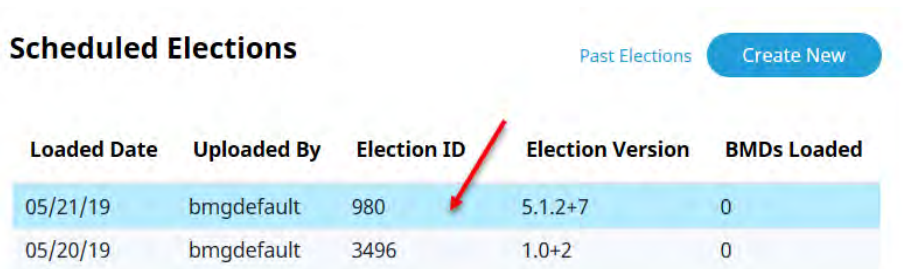
16.10.2.BMD Logs

After an election is over and the BMD devices have returned, it's time to download the election logs and keys from the devices. The election logs don't record any personal voter data, or any of their ballot selections during the voting process. The logs are simply a collection of the different BMD settings that were made by users, such as volume level, screen brightness, language settings, etc. Reviewing these logs allows developers to enhance the voting experience during the next election by gaining a sense for which BMD functionality settings might need to be updated to be more in line with the settings selections of the average user. The following steps describe how to collect logs using the BMG.

1. From the BMG main page, in the "Scheduled Elections" section, click View All



2. A page opens with a list of all upcoming elections that have already been scheduled
3. Click on the election ID and version whose logs or keys you'd like to download



4. Click Show Previous to view a list of elections that have already passed
5. Click either Aggregate Keys, or Aggregate Logs
6. If logs or keys are available for download, a new page opens with the option to download the files
7. Click Download
8. Depending on your computer settings, you will be asked to either download the file, or open it without downloading it
9. Transfer the files to a USB and give it to a Tally representative for processing

17. Manual Recount Procedures

Manual Recount Requests should be made in accordance with the California Elections Code and California Code of Regulations Chapter 8.1, including the jurisdictions Recount Procedures that are on file with the Secretary of State.

To validate the accuracy of the vote count, a public manual recount of at least one percent of the total ballots cast, chosen at random, shall be conducted within fifteen days if requested.

All the original ballots will be reviewed for each contest. Votes will be recorded on tally sheets.

The process for Manual Recounts is as follows:

1. Tally board is prepared with ballots from a batch and tally sheets
2. For each contest the selection from every ballot is read aloud
3. Any voter may request a recount pursuant to the Election Code sections 15620, 15621 or 15623
4. The other party records each vote on the tally sheet with one pencil stroke per vote.
Includes any under or voter voted contests
5. The total of all pencil strokes for each candidate is counted and written into the proper box on the tally sheet

18. Security

18.1. Physical Security of System and Components

The System Security describes the voting system security. The system features access control mechanisms, equipment and data security, software installation and security policies, air gap policies, event logging details, physical security structures, specifications, standards, and regulations designed to protect the voting process from malicious attacks, data breaches, and accidental security incidents.

Network - The network domain that hosts election definition and ballot layout functions is physically separate from system and does not have inter-connectivity of traffic between domains. Data is transferred through a manual process under human control. The system is hosted on a separate network domain that is not physically connected to any other County LAN and no physical interconnections exist between the system and any other network or end-point device that connects to the Internet.

Protective Barrier - The placement and design of the room where the system and components are housed must allow for a secure environment that aims to deter or delay any attempt to disrupt operations while providing a means for interested parties to observe.

Rack-mounted Equipment - Hardware components such as scanners, servers and network devices must be housed in locked enclosures that contain racks for servers, network switches, power distribution units, and other components or peripherals. Serialized tamper-evident seals are used on removable panels. Removal and replacement of seals must be witnessed by at least two election staff members and documented using a log with signatures by both parties.

Access Control - Entry and Exit doors must be protected by an electronic key card access system. Entry and exit must be automatically logged with identity, date, time, and door number recorded for each instance. The key card system must be operated and maintained by a designated team and access shall only be granted when authorized by designated managers. Policies and procedures for access control to the tabulation room must be defined and implemented.

System	Method	Description	Specifications
BMD	Trusted Platform Module (TPM)	The trusted platform module prevents unsigned software from signing onto the system	The TPM, a secure crypto-processor, integrates cryptographic keys into the BMD
BMG	Network Access Control	HP Aruba ClearPass: MAC address control, prevents non-authorized computers from accessing network	Tracks the machine MAC addresses of all computer network cards present on the network and removes any unauthorized network card MAC address from a network
ESA	Two-factor authentication with smart card	Radio Frequency Identification (RFID) limits access to the HSM	The smart card RFID is issued to an authorized individual, which serves as a part of two-factor authentication.

ISB	Network Access Control	HP Aruba ClearPass: MAC address control, prevents non-authorized computers from accessing network	Tracks the machine MAC addresses of all computer network cards present on the network and removes any unauthorized network card MAC address from a network
Tally	Network Access Control	HP Aruba ClearPass: MAC address control, prevents non-authorized computers from accessing network	Tracks the machine MAC addresses of all computer network cards present on the network and removes any unauthorized network card MAC address from a network
VBL	Network Access Control	HP Aruba ClearPass: MAC address control, prevents non-auth computers from accessing network	Tracks the machine MAC addresses of all computer network cards present on the network and removes any unauthorized network card MAC address from a network

18.2. Logical Security of System and Components

18.2.1. Essential and Non-Essential Services and Ports

Unused USB data ports are covered with serialized tamper evident seals on the VSAP servers and related components. The serialized tamper evident seals are manually logged with an operator signature, seal number, location, date and time.

Component	Ports and Access Points
BMD	USB port, Ethernet port, 3 x 3.5 mm ports
BMG	<p>USB port, Ethernet port, 3.5 mm audio, HDMI, SD card reader, and VGA</p> <p>HPE ProLiant DL830 Gen10: Display Port 1, 8 LFF chassis standard Flexible LOM Network Ports, 4 x 1 Gb ports, HPE iLO Remote Management Network Port, 1 Gb Dedicated Front iLO Service Port, Micro SD Slot 1 Micro SD, USB 3.0: 1 front, 2 rear, 2 internal (secure) HP 8320 JL479A: 48p 10G SFP/SFP+ and 6p 40G QSFP+ Switch HP8320 JL579A: 32p 40G QSFP+ HP3810M JL075A: 16 SFP+ fixed 1000/10000 SFP+ ports; Duplex: 100BASE-TX: half or full; 1000BASE-T: full only; Ports 1 – 16 support MACSec HP2930F JL253A: 24 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/ 100BASE-TX: half or full; 1000BASE-T: full only; 4 SFP+ 1/10GbE ports; PHY-less HP2530-8G JL9777A: 8 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Media Type: Auto-MDIX; Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only; 2 dual-personality ports; each port can be used as either an RJ-45 10/100/1000 port (IEEE 802.3 Type 10Base-T; IEEE 802.3u Type 100Base-Tx; IEEE 802.3ab 1000Base-T Gigabit Ethernet) or as a SFP slot (for use with SFP transceivers) ports</p>

ESA	Intel NUC7i7DNHE: USB, SATA, Ethernet nShield Edge F2 HSM: SD card reader and USB
ISB	USB port, Ethernet port, 3.5 mm audio, HDMI, SD card reader, and VGA
Tally	Compute servers: USB, Ethernet, Video/display, PS2, Audio Scanner machines and scanner support machines: Ethernet, Video/display, PS2, Audio Storage Appliance: Ethernet, Audio Workstations: USB, Ethernet, Video/display, PS2, Audio Switches: Various network
VBL	Compute server: USB, Ethernet, Video/display, PS2, Audio Workstations: USB, Ethernet, Video/display, PS2, Audio Switches: Various network

18.2.2. User-Level Security

The system has numerous access controls to deter unauthorized users from accessing the system. There are three role types in the system. The first role is the Linux administrator. The Linux administrator can configure the system, setup new users, set up configuration files, configure the system, and view logs. Second is the application admin. The application administrator can manage running services in the system, tabulate elections, view errors, and conduct all necessary election night operations. Finally, is the view-only user who can look at the Manager interface, but cannot physically affect the system.

The system is only accessible to individuals who have a username and password. Usernames and passwords are managed via process by the system administrator. User passwords are never stored in clear text or reversible formats. There is a system tool for generating password entries. All user passwords are stored with password encoder software. These files are protected via file permissions.

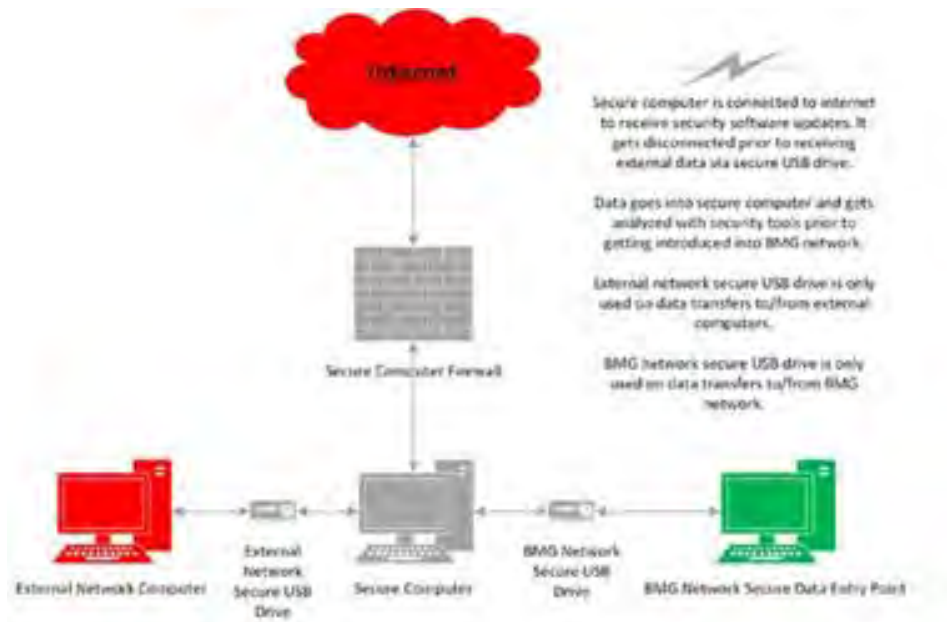
18.2.3. Anti-Virus Protection

SYSTEM SECURITY (*Air-Gapped Environment*)

- **Carbon Black Protect Software (CB Protect):** This software once installed, takes away elevated privileges on any operating system. All software on a computer system with CB protect installed is subject to permission from it to execute. This software functionality reduces the chances of malicious software to run on a computer. In addition, the whitelisting function in Carbon Black is leveraged to restrict USB portable media use in all VSAP Microsoft window products. It is strongly advised to have Smartmatic assist in the install of this product in the air-gap environments and for CVSS testing. Any mis-configuration can interfere with the proper operation of software on a computer system.
- **HP Aruba ClearPass:** tracks the machine (MAC) addresses of all computer network cards present on a computer network. The software, in addition to monitoring MAC addresses, can remove any network card MAC address from a network that is not authorized to be on that network. This software function disrupts any attacker from placing implants or connecting workstations to any air-gap network without authorization.

It is recommended that Smartmatic personnel assist in the installation of this software to any air-gapped network. This software improperly configured can also like CB Protect disrupt proper operation of the computer network.

- **Snare System Information and Event Management (SIEM):** The Snare SIEM tracks all computer system and network activities and records them for a retention period of up to several years provided there is adequate storage. SIEM will be the method by which all network activity will be tracked for review in the event of an attack or issue. Once a SIEM record is created it is locked in the system and cannot be tampered with or changed. Smartmatic recommends that Smartmatic personnel assist or take the lead in the installation of this software inside the air gaps.



18.2.4. Verifying, Checking, and Installing Essential Updates and Changes

Changes are primarily for installing critical updates to operating system, anti-virus protection or other third-party elements related to security and error correction.

18.3. Event Logging Capabilities

18.3.1. BMD

A usage data collection log file records executed events on the device; audit logs will record every event triggered in the BMD as one of the following types: info, error, warn, fatal, and debug. Logging is performed in the voting app. The BMD Interaction Data (BID) is a fixed-sized usage log that counts ballots cast. The BMD Election Log (BEL) is an audit log that creates separate records for each user interaction.

The BMD allows multiple BELs for multiple elections. All logs are written to the data partition. The BMD employs the SIEM to capture system events.

18.3.2. BMG

The BMG contains a file-based audit logging system. Timestamps will be generated in the format ISO8601 including time zone (e.g. 2017-09-26T01:57:58+00:00). Event logs are stored and reported through ElasticSearch. The BMG employs the SIEM to capture system events.

18.3.3. ESA

The ESA uses a file-based logging system. The ESA program and scripts write system logs to a text file located on a central Unix directory. Log files can be read using standard Unix text processing commands such as less and cat. Since the ESA is intended to be used only occasionally and for limited numbers of tasks, log files are not expected to grow significantly, eliminating any need for rotating files.

18.3.4. ISB

The ISB logs specific events to a log file, including:

- System ID
- Unique event ID and/or type
- Timestamp
- Success or failure of event, if applicable
- User ID trigger the event, if applicable
- Resources requested, if applicable

The ISB will use AWS S3 for storage of the statically hosted log files. It will employ encryption and will have AWS CloudTrail logs enabled.

18.3.5. Tally

Tally employs the SIEM to capture system events.

18.3.6. VBL

The VBL employs the SIEM to capture system events.

18.4. Event Logging Design and Implementation

18.4.1. BMD

To facilitate security and traceability of the BMD, logging capabilities are designed to capture information about each unique event, including: sequence number, unique event ID, transaction results, user and event types, average voting session time, and event occurrences.

SSD has four partitions, one of which stores logs (Data partition). Diagnostic (pre-setup) has logs, then logs are captured while users are voting; then they're unpacked or read back at the warehouse when connected to BMG.

18.4.2. BMG

Elastic Search: for daily logs are aggregated into CSV files for export for any period longer than 24 hours

Design = Database (SQL) maybe built into Elastic Search.

The system information and event management (SIEM) software provides an audit trail through continuous logging of network activity. The system uses Snare as its SIEM, in conjunction with the network traffic monitor LANGuardian, providing up to one year of highly detailed log data for the network. This data is suitable to provide actionable intelligence and critical insight both for security monitoring and incident response forensics. These products are also capable of reporting a summary overview.

18.4.3. ESA

Testing output, event logs, and error logs are all stored in a local log file.

18.4.4. ISB

AWS access logs stored in the S3 bucket.

18.4.5. Tally

Each Tally service logs events to the file system and makes them available through the Log Viewer page, which is accessible on the Tally environment. The logs are preserved for auditing and are included in an archive of the election. The archive of the logs includes all election specific logs and general logs that have been generated at the moment the archive is requested. Logs are created and use signed log-chaining to ensure the validity of the audit log and to help discover any logs which have been maliciously added. Rotation of logs is set for each service and is used to preserve disk space as logs grow over time. Log viewer is not a generic tool that can pull in logs from any system. Due to that, third party tools such as Kafka and Cassandra log via their native logging patterns. Those logs are not readily accessible through the Tally UI.

18.4.6. VBL

Each VBL service logs events to logs on the file system. The logs will be preserved for auditing. Logs are created and use signed log-chaining to ensure the validity of the audit log and to help discover any logs which have been maliciously added. Logging also includes rotation of files in order to preserve disk space as logs grow over time.

18.5. Installation Procedures

The system is hosted on a separate network domain that is not physically connected to any other County LAN and has no physical interconnections existing between the system and any other network or end-point device that connects to the Internet. The application runs on a standalone COTS PC and is physically separated from the system. Data between the two systems is transferred through a manual process under human control and performed by trusted staff. Installation of updates is performed through a set of manual procedures overseen by trusted election managers. Installation activities are documented with at least two staff members performing updates. Documentation includes, date-time of update, person who performed activity, person who witnessed the activity, and certification that update installed was previously approved.

18.5.1. Acceptance Testing After the Installation

Before each election, version control testing will be conducted to make sure that each component of the electronic voting system is using a certified version of the vendor's software and firmware.

The California Secretary of State's Office requires parallel testing of voting devices on Election Day. The parallel testing procedure includes the random selection of voting devices the morning of the election from various precincts within the county. Once selected, the voting devices are thoroughly tested for accuracy and reliability by designated California Secretary of State election personnel. The accuracy testing runs the entire duration of the election. Election result reports are then generated from each devices unit once the election concludes so the accuracy of the system can be validated.

18.6. Security Procedures for the BMD Warehouse

Physical security standards for all persons working or entering the BMD Warehouse. These policies comply with NIST 800-171 Physical Protection, Media, and Personal Security Policies.

Authorization is required to enter the BMD Warehouse. The following are the only authorized personnel:

- Select, jurisdictionally appropriate, personnel
- Approved contractors
- Building maintenance personnel

The following personnel are authorized, but may be subject to the jurisdiction's escort and monitor policy:

- Vendors (including delivery personnel)
- Visitors

Valid ID badges are required to enter the BMD warehouse and must be worn and visible when one is inside the building. Visitors will be expected to have temporary badges distributed from the visitor management system. Any person without a badge showing authorization is considered an adversary and will be escorted to the security desk immediately.

Employees will report a badge that's been lost, stolen, or compromised in any way, to the security office.

Refer to jurisdictional procedure guides for further information on existing guidelines governing identification of personnel entering Information Technology areas.

Cameras will monitor all areas of security concern:

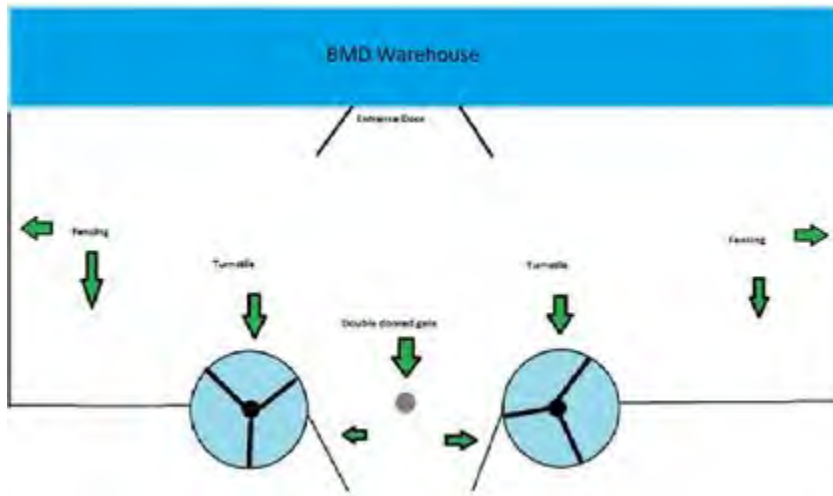
- Truck and delivery yard
- Employee parking
- Visitor center entrances
- Employee entrances
- Warehouse for BMDs
- BMD repair facility
- Kitting area

The facility will create protected yards for employee parking, and facilities for trucks and large equipment.

- Gates and fences will protect the warehouse loading bays from being penetrated by unauthorized persons
- Gates will be monitored by site security personnel

Employee physical access will account for tailgating, which is when an unauthorized person gains access by trailing behind authorized personnel.

- A turnstile connected to the building's access control system shall control access and limit tailgating to the employee entrance to the facility
- Outside of the entryways assigned to the employee entrance, there will be an outer defended area with turnstiles connected to an access control system, allowing only one employee to enter at a time, thus preventing tailgating
- There can also be a gated entrance between turnstiles to comply with current Americans with Disabilities Act standards for those employees who cannot pass between turnstiles
- The employee entrance area will also be monitored by cameras. In addition to monitoring, these cameras will remind employees to be vigilant regarding security while inside the facility



A magnetic card access system will control overall access to the facility. All entrances to the BMD warehouse will be connected to the access control system.

- Fenced off areas will be established inside the warehouse for kitting and the maintenance of the BMDs
- In addition to the magnetic card system, kitting areas will be fenced off and secured with combination locks and the combinations to those locks known only to those authorized to enter the kitting or service areas
- The BMD repair, and inspection area will be isolated from facility personnel by a fence and combination lock and will be accessible only to maintenance staff

In addition, entrances to critical areas will be protected by biometric scanning.

Video will be accessible from inside as well as from outside the facility. Cameras integrated with a cloud-based enterprise mobility management system (EMM) can be accessed from outside the facility via the internet. The EMM will have two-factor authentication for accessing the cameras. Proper authentication will allow for secure access by jurisdictionally appropriate security personnel and the local sheriff's office, as well as from inside the facility.

A burglar alarm will be configured to detect any unauthorized entrance to the facility. The final design of the security system will be determined based on the characteristics of the facility selected for the BMD warehouse.

Kitting and BMD service areas will additionally be protected by combination locks to provide the additional security necessary to keep these elements of the BMD warehouse facility safe.

Critical areas such as the BMG server or switching rooms are to be protected by a biometric iris reader. The biometric iris reader is a retinal scanning device that unlocks doors to those areas. Biometric systems protect against duplication and/or theft of any magnetic cards used by the access control system. A higher level of security for entry is obtained using a “Man Trap”. A “Man Trap” uses two doors with an entry door connected to a small passageway to an exit door on the opposite wall utilizing a combination lock or a lock that is unique to the space. One door of a “Man Trap” cannot be unlocked and opened until the opposite door has been closed and locked. “Man Traps” are used in physical security to separate non-secure areas from secure areas and to prevent unauthorized access.

All USB media are to be serialized and tracked to individual users via a checkout sheet maintained by the IT Security Staff. Any USB media not in use will be inside a safe within the critical protected areas. Placing the safe inside a room, such as the BMD server room, which is only accessible via biometric scanning, provides extra security.

The “Man Trap” will use the building's magnetic card system to control the external door to the server\switching room. A biometric reader will screen the entrance to the interior door entrance. "Man Traps" will be constructed in locations where jurisdictionally prudent.

Because magnetic cards can be stolen or duplicated, biometric devices will control special access to any server/switching room.

- The system will connect to an electric striker to open doors to these areas of the facility when activated.
- The biometric iris reader device requires that a database of authorized users reside on a Windows desktop computer. It is the responsibility of the IT security staff to maintain that database and upkeep the list authorized users to the rooms.

The server\switching rooms shall have restrictions on phones and employee-owned personal electronics inside those areas. The individual devices restriction policy shall be enforced by BMD warehouse staff via written policy. No employee-owned smartphone or personal electronic device will be allowed inside critical air-gapped server rooms or server areas connected to the electronic poll books. All employee-owned electronic devices shall be kept in lockers placed outside of the server rooms. Failure to follow the policy should result in disciplinary action from the BMD warehouse management staff.

- A set of lockers will be positioned next to any critical air-gapped network server\switching room to allow employees to store their devices before entering the area.
- Employee-owned electronic devices can be compromised by improper security, or by the term of service agreements for applications on the phone.
- Terms of service or improper activity may cause cameras, microphones, and the GPS data in the device to be turned on and used for surveillance of restricted sites, without the knowledge or permission of the owner.

Adherence to the following procedures is required:

- All BMD Warehouse employees are expected to keep a clean workstation area
- Any documents related to the voting operations will be in a locked drawer or other secure areas when not in use

- Workstations screens are to be locked when employees are away from their computers by Windows group policy of no longer than five minutes
- Any removable storage devices must be locked in a protected area
- Any documents to be discarded must be shredded

Employees are not allowed to use personal devices to audio- or video-record any activity within the BMD Warehouse. Management must be notified to find a solution if an employee requires audio or video recordings. As stated earlier, it is possible via a term of service for photographs taken on a smartphone to be shared without the user's knowledge.

Only jurisdictionally appropriate or Smartmatic issued computers are allowed to connect to the VSAP network facilities at any time.

All computers must be registered to the network access solution protecting the VSAP network. Any computer not known to the network access software will be restricted, and alerts will be sent to IT security staff immediately.

Personal storage and media devices are not allowed to be connected to computers. Security software will only allow connections by USB to devices designated by an appropriate local, state, or federal jurisdiction personnel. Restricted storage and media devices include:

- USB drives
- Flash drives
- Mobile phones
- Any other devices capable of recording

A vendor who brings these devices into the BMD warehouse must present them to IT security for malware scanning by the designated AI antivirus software. Any necessary or required data will be copied to a USB storage device issued by an appropriate local, state, or federal jurisdiction and provided to the vendor for the work required and returned at the completion of the work to the security desk. This provided storage device must be returned to IT security once the vendor has completed their task. The vendor then will retrieve their personal device. Any vendor who violates these rules will be subject to immediate removal from the BMD warehouse.

In some cases, IT security may authorize, issue, clear, and track media devices that connected to BMD warehouse computers and servers. Any USB device or media shall be purchased by the appropriate local, state, or federal jurisdiction and security tested by IT security personnel prior to use in the network. Devices will then be assigned random serial numbers to verify they are safe to use.

Only serialized USB storage media managed and tracked by BMD warehouse security staff will be connected to VSAP equipment.

All computers not requiring a USB media connection, as determined by BMD warehouse security staff, will have their USB ports disabled by an endpoint security software or physically.

Any device used to connect to VSAP equipment without a serial number must be turned in to IT security for examination.

Security Product	Area of Responsibility	Web Link	Need to be Installed ?	Amount Needed ?
Turnstile	Employee Entrances	https://www.haywardturnstiles.com/product/ht431-secureturn/	Yes	To be determined until site chosen
Biometrics	Critical Server Room and Switching	https://www.eyelock.com/index.php/access-control/nano-nxt	Yes	To be determined until site chosen
Cameras	Server Room, Kitting Areas, Warehouse, Yards, and Offices	https://meraki.cisco.com/products/security-cameras	Yes	To be determined until site chosen
Fencing	Truck Yard (Outside), Kitting (Inside), BMD Repair Area	None	Yes	To be determined until site chosen
Combination Locks	Kitting Area, BMD Repair	https://us.allegion.com/en/home/products/categories/electronic-locks/schiage-ad-400-401.html	Yes	To be determined until site chosen
Access Control System	Entire Facility all Entrances and connecting doors from visitor entrance to warehouse	https://www.security.honeywell.com/product-repository/netaxs-123	Yes	To be determined until site chosen
Safe	Server Room, Holds USB media and media for Certificate of Authority	https://gardall.com/view-product/dual-security-safe-within-a-safe	No	County needs to put out to bid for price
Envoy	Visitor Logging and badging	https://envoy.com/	No	To be determined until site chosen
Burglar Alarm	All ingress and egress to the facility	To be determined	Yes	To be determined until site chosen

Security Product Recommendations

Every quarter, the security staff will perform random tests to assess physical security and compliance with access procedures. It is strongly recommended that a "red team" of security evaluators test the facility after each election to determine security compliance.

18.7. Security Procedures for Vote Center

18.7.1. BMD Vote Center Storage and Security Seal

BMD devices will be delivered to the Vote Centers prior to Election Day. During transit, carts and storage containers are sealed with evidence tape and/or tamper evident seals. Access points (such as the USB and network port) to the BMD are outfitted with tamper-evident seals with either or both tamper evident residue or visual appearance change to the seal itself to reveal modification or removal and to help prevent access or theft (see pictures below). In addition, a tamper-evident seal is also placed over the seam of the IBB (see picture below of tamper-evident seal). Removing, creasing, scratching or laminating the factory applied film exposes prominent "OPEN VOID" messages. Seals use Secure ID technology that has a distinctive finish which serves as an anti-counterfeiting and authentication feature. In addition, the BMD ballot boxes are also outfitted with tamper evident zip-tie security seals utilizing signaling evident technology to reveal modification and/or removal.



Tamper-evident seals placed over the USB and Ethernet ports - examples (color may vary)



Tamper-evident seal placed over the seam of the Integrated Ballot Box



Zip Tie used to secure the Integrated Ballot Box (color may vary)

In addition, BMDs will be kept in a secure location at each Vote Center. During overnight storage, BMDs should be stored in rooms that are sealed with evidence tape at access points and/or in rooms that can be locked with a key.

Zip-tie seals and tamper evident-seals are logged via established "chain-of-custody" procedures; this includes replacing and logging any need to break seal(s) for reason of entering a storage area, room, ballot box, or any other secured locale. An election inspector / overseer will verify that the correct seals are intact on the BMD containers, carts, and devices prior to set up, and use in the election.

18.7.2. Ballot QR Codes

The Ballot Page Metadata (BPM) QR code in the upper left-hand corner of the ballot contains information about current election status and indicates the ballot's originating BMD. BMDs assigned to the election pass their security keys to Tally; BMDs that are not officially part of the election will produce an error.

Additional security measures:

- An audit of each precinct's electronic tally of the number of votes cast will be conducted against the number of signatures in the precinct's ePollbook
- Vote center officials will be required to certify in writing that the proper locks and seals were found intact on the BMD devices, carts, and containers before the polls open. Exceptions and discrepancies will be reported to the Help Desk immediately upon discovery
- A physical inventory of all BMD devices will be conducted before and after each election to ensure custody of all devices is maintained and/or accounted for; there are functions within the BMG that can be used to aid in this inventory (for more information see the BMG User Guide)

19. Audit Trails

Election audit trails are vital to validating the accuracy of election results. All system components create an audit log anytime the system is accessed, or data is changed. Audit logs can be opened and printed to hard copy if needed.

19.1. Programming and Configuration of Election Management System/Software

This defines the processes for conducting the internal quality audits of the Smartmatic quality management system. This procedure applies to all areas of the quality management system, as identified on the Smartmatic process map located in the Manual. Some of these processes, however, such as manufacturing, are managed through the supplier of these processes and this internal audit program will audit the management of these suppliers, specifically related to the manufacturing requirements.

19.1.1. Definitions

QMS Representative - The person with responsibility and authority for day-to-day oversight of the performance of the QMS. This person is appointed by top management at Smartmatic and serves as the owner of the internal audit process.

QMS Review - Described in ISO 9001 as "management review", the QMS Review is the process that reviews the health of the QMS at periodic intervals to ensure the QMS maintains its suitability, adequacy, and effectiveness.

Conformance - Meeting a requirement.

Non-conformance - Not meeting a requirement.

Opportunities for Improvement - A conforming process that might be considered for improvement, due to inefficiencies, chance for increased effectiveness, poor performance trending, use of obsolete technology or processes, cost savings, etc.

Findings - What was found during an audit, may be positive (conformance), negative (non-conformance), or an opportunity for improvement (OFI).

Internal Audit Program - The Smartmatic audit program is designed to determine the extent of conformance in Smartmatic processes and to identify relevant opportunities for improvement. The objective of this internal audit program is to determine if the QMS is meeting the intended results of managements objectives (operational, financial, etc.) as well as continued improvement of the QMS processes.

The audit program is designed to meet the changing needs of Smartmatic and to allow auditors to conduct audits of value on QMS requirements and management objectives. Smartmatic management views this audit program as a dynamic means to assist in meeting the organizations purpose and strategy in the global marketplace.

Internal Audit Schedule - An audit schedule is created annually by the Smartmatic QMS Representative. The schedule is reviewed, possibly revised and approved in Smartmatic QMS Review, and is attached to the QMS review minutes for future use.

The internal audit schedule lists the activities, areas, requirements, processes, or locations to be audited on an annual basis. The audits may be scheduled monthly, every other month, or quarterly. In some cases, the audits may be conducted twice a calendar year with many auditors participating.

The activities, areas, requirements, processes or locations listed on the audit schedule ensure that all core processes are audited in some fashion every year and all parts of the QMS are audited at least every 3 years. Smartmatic management may provide additional input or guidance into certain areas of Smartmatic that need to be added to the audit schedule.

The audit schedule can also be modified during the year based on process issues, customer complaints, non-conformance, management direction, new processes added at Smartmatic, process improvements, or if the QMS scope has changed.

Auditors are assigned to each audit on the audit schedule and are assigned to audit in pairs if resources allow. Auditor pairs will select the "lead auditor" within that pair that will handle any logistics, decisions, etc. related to each audit assignment.

Auditors and Competency - Only personnel that have been trained may perform audits of the Smartmatic QMS. Auditors are selected by management and/or the QMS Representative to be QMS auditors. Auditors are required to participate in auditing each year to maintain their status as an auditor. Auditors are requested to gain additional auditing competence through additional training, seminars, webinars, reading, participating in on-line discussions and groups, etc.

Auditors are expected to demonstrate the "auditor behaviors" identified in ISO 19011 (current version) when conducting audit activities, including maintaining objectivity and impartiality throughout the audit process.

Auditor training is selected and approved by the QMS Representative and/or Smartmatic management. Smartmatic has no requirement for certified or accredited ISO 9001 training classes for requirements or for auditing. Training must be provided by credentialed professionals with extensive knowledge, understanding, and experience in ISO-based management systems and in quality auditing. Trainers should also possess business knowledge to promote value in the QMS and its processes, specifically the internal audit process. Employees that join Smartmatic with previous ISO auditing experience may be added to the auditor roster at the discretion of the QMS Representative.

Planning for the Audit - Planning for scheduled audits begins before the audit scheduled dates. The QMS Representative determines the feasibility of the audit during the time frame and if feasible, notifies the auditors to begin preparations. If the QMS Representative determines it is not feasible, then an alternative time frame is selected. The QMS Representative will make available to the auditors any necessary documents needed to begin the preparation, such as previous audit results for that area/process, any significant changes to that area/process, any recent complaints or non-conformance from last audits, etc. The QMS Representative will then define the audit area/process, the scope of the audit and possibly audit objectives. The auditors will then begin planning for the audit, beginning with determining the exact dates and times for the audit interview. Once this is completed, the auditors begin the preparation.

Preparation for the Audit - The auditors will review process/area, the scope, and the objectives for the audit and begin creating a checklist (or use an internal checklist). This checklist is based on the information received from the QMS Representative or gathered by the auditors.

The auditors will create questions to ask during the audit, based on the checklist of the audit-specific checklist. These questions will focus on what is most important in the process/area being audited and should be asked of different people in different levels of activity in the process/area.

The auditor should have general understanding of the ISO 9001 and 10007 requirements and should consider bringing a copy along on the audits.

The audit checklist should serve as a guide during the audit to help the auditors stay focused, stay in scope, and stay on time. Additionally, the checklist is a good place to take the auditor's notes.

Conducting the Audit - The auditors should conduct the audit at the place where the process is performed. The auditors should use the checklist to lead the audit, knowing that the audit may change based upon findings.

The auditor can use the checklist or other means to keep good notes of the findings (conformance, non-conformance, or opportunities for improvement).

The auditor should use the most appropriate questioning techniques to get information related to the process being audited. These can include: open-ended questions, closed-ended questions, clarifying questions and leading questions. The auditor is looking for conformance and when a possible non-conformance is identified in the audit process, the auditors should use clarifying questions to ensure that we record the actual response.

Audit evidence is collected via interviews with persons working in the process, observations of persons, and reviewing records or evidence of the process being conducted.

The auditor should keep the persons being audited aware of how the audit is progressing and should share any concerns, non-conformance, opportunities, etc. with them.

Once the questions have been answered, the audit trails have been taken and the auditor is satisfied that the audit objectives have been achieved, the auditor should recap the findings, answer any questions, and thank the participants for their assistance. Additionally, the auditor ensures that the notes taken are sufficient to create an accurate, truthful, and complete audit report.

Reporting the Audit Results - The results of the audits are compiled into a single audit report. This report includes a summary of the findings, which includes conformance (including best practices, noteworthy efforts, etc.), non-conformance (which include the requirement not being met and the list of evidence that verifies the requirement was not met), and opportunities for improvement. This report is submitted to the QMS Representative for review and issue. The QMS representative will ensure that any necessary corrective actions are issued to the appropriate process owners. This report is maintained as a record. Evidence collected during the audit that is used for corrective actions may be retained at the discretion of the QMS representative.

Audit Follow-up - If required or requested, a follow-up audit may be performed for certain reasons: corrective action review, to complete the original audit, to conduct a deeper dive into certain parts of a process for better understanding or management request. Any findings that need recording will be added into a separate audit report or appended to a previous audit report. These findings will be included in the Smartmatic QMS Review.

19.2. BMD Log Files

The BMD logs significant system events during elections and anonymous usage data. This information is useful for auditing purposes and for ongoing user experience analysis. These logs are retrieved using the BMG.

Per federal law, County personnel must ensure retention for a 22 month minimum period of all election artifacts. This includes electronic records collected by the VSAP system such as: VBL, BMG, and Tally event logs and the aggregated BMD event logs.

Log File	Type	What it Tracks
BID - BMD Election Interaction Data	Audit	Information about the interactions between the voter and the system, such as: <ul style="list-style-type: none">• Font size• Language• Voting system time Only aggregate interaction data is recorded, not individual voter choices
BEL - BMD Election Logs	Usage	Each event triggered during the voting experience at the BMD, such as: <ul style="list-style-type: none">• Shutdown• Empty ballot box• Cancel voting session

20. Biennial Hardware Certification and Notification

California Elections Code requires jurisdictions to inspect voting systems and certify their accuracy once every two years. All ballot marking devices, tabulators, scanners, elections management software, and supplementary equipment must be certified by California's Secretary of State prior to their use in any election taking place in California. In addition, all specialized tally equipment must be certified for use in elections by the Secretary of State prior to use in any election.

20.1. Notification of Equipment

For each statewide election, the responsible county Election Official prepares a list, including quantities, of all equipment to be used to tabulate votes during the semi-official and official canvass. Seven days before each statewide election, the Election Official shall certify to the Secretary of State the results of the logic tests, as well as the accurate functioning of all ballot tally equipment. This certification shall also affirm the use of the same equipment for the Pre-Election Logic and Accuracy test, and for semi-official and official vote canvasses.

In the event of a change to the ballot tally program after certification, an amended certificate shall be submitted no later than the day before the election. In the event any equipment is repaired, altered or replaced following the certification specified in this section, and prior to completion of the official canvass of the vote, an amended certification of Logic and Accuracy testing and a revised list of equipment used must be submitted to the Secretary of State no later than official canvass submission.