2.09 - Democracy Suite® EMS System Maintenance Manual

Version: 5.13-A::4

December 13, 2022

DOMINION VOTING

Our customers come first.

Table of Contents

CHAPTER 1: INTRODUCTION

NOTE: This document is a specification for maintenance of the Democracy Suite Election Management system designed and manufactured by Dominion Voting Systems Corporation.

1.1 Document Use

This document is intended for use with the Democracy Suite® 5.13-A platform.

1.2 Purpose and Scope

This document describes Democracy Suite Election Management System maintenance procedures. This document provides all information necessary for the Election Management System use by all personnel who support pre-election and election preparation, post-election and central counting activities, as applicable.

1.3 Relevant Disclaimers

This document may make reference to certain Democracy Suite functionalities that are not part of the current 5.13-A campaign and should be disregarded throughout the document.

For a full list of relevant disclaimers, please see the "Relevant Disclaimers" section in the *2.02 - Democracy Suite System Overview* document.

1.4 Network Data Transmission

Please, be aware that, at this point, there is no modem transmission of results data over a network.

1.5 Data Handling in the Processor and Memory Units

Within the EMS, the data is handled by Windows Operating System.

1.6 Data Output Initiation and Control

The EMS consists of several data outputs. They are, here, grouped by the activities (see *2.03 - Democracy Suite® EMS Functional Description*, section the Basic EMS Workflow). After the election project has been defined, the ballot artwork is satisfying, the official ballots are produced.

Furthermore, during the process of the defining and configuring optical

tabulators - (ImageCast® Precinct, ImageCast® Evolution and ImageCast® Central devices), the Device Configuration Files (DCF), MBS (machine/or device behavioral settings) and Voting Information Files (VIF) output data needed for the proper operation of the tabulator devices are created. This phase also includes producing (programming) the Compact Flash memory packs with election files for tabulator devices and programming the security tokens for tabulator access control activities. Next, the set of reports can be created. Among them is the auditing report. This report lists all the actions performed for the current election project. All aforementioned outputs are initiated by the electoral office representative. A Dominion representative assists when jurisdiction representatives and officers need help. In addition, please, refer to TDP *2.10 - Democracy Suite® Personnel Deployment and Training Requirements*.

1.7 Power Conversion/Conditioning

For information on power conversion, please refer your workstation vendor documentation.

1.8 Acquiring Test and Diagnostic Information

Please refer to *2.07 - Democracy Suite® System Test and Verification Specification* in addition to this manual.

1.9 Applicable Documents

VVSG 1.0, Volume II, Version 1.0, Section 2.9 System Maintenance Procedures

1.10 Document Organization

Every attempt has been made to produce the document structured according to the VVSG 1.0 requirements (VVSG 1.0, Volume II, Section 2.9).

- Section 1 - Introduction - purpose and scope of the document (this section)
- Section 2 - System Maintenance Manual - provides an overview of the system for maintenance and references to specific documents that explain the maintenance procedures and policies in greater detail.

1.11 Design Responsibility

Dominion Voting is the design authority.

1.12 Patent Status

Certain system concepts, as well as many implementation and construction details are protected by a series of U.S. and foreign patents pending.

CHAPTER 2: MAINTENANCE PROCEDURES

2.1 Preventative Maintenance

2.1.1 Audit Log Contents

According to industry standards, EMS uses Windows Event Audit logging for tracking the details of each change event of all system software and hardware changes.

By default, when the initial maximum size of a log is reached, new events overwrite older events as needed. As such, it is in the best interest of the user to Archive old items.

2.1.1.1 Increasing the Size of an Audit Log

The Audit logs will reside on a disk that has at least 20GB available space. A separate disk or disk array may be considered for these which must be secure against physical and logical tampering.

Application Log

The Application Log is used by Windows to log application audit events that have been activated. Because of the large number of events that will be logged during normal use, this log will grow significantly.

Dominion Voting requires the following policies be put in place for the Application Log:

- The size of the Application log will be set to a minimum of 2GB.

To set the size:

1. Start, Administrative Tools, Event Viewer.
2. Expand “Windows Logs” in left tree.
3. Right click “Application” and select “Properties”.
4. Increase the value of the “Maximum Log Size” to at least 20480 KB.
5. Choose the “Overwrite events as needed” option.

Security Log

The Security log is used by Windows to log security audit events that have been activated. Because of the large number of events that will be logged during normal use, this log will grow significantly. Dominion Voting requires the following policies be put in place for the Security Log:

- The size of the Security log will be set to a minimum of 2GB.

To set the size:

1. Start, Administrative Tools, Event Viewer.
2. Expand “Windows Logs” in left tree.
3. Right click “Security” and select “Properties”.
4. Increase the value of the “Maximum Log Size” to at least 20480 KB.
5. Choose “Overwrite events as needed” option.

EMS System Log

The Event Log is used by Windows to log audit events that have been activated. Because of the large number of events that will be logged during normal use, this log will grow significantly.

Dominion Voting requires the following policies be put in place for the Event Log:

- The size of the Event Log will be set to a minimum of 2GB.

To set the size:

1. Start, Administrative Tools, Event Viewer.
2. Expand “Applications and Services Logs” in left tree.
3. Right click “EMS System” and select “Properties”.
4. Increase the value of the “Maximum Log Size” to at least 20480 KB.
5. Choose the “Overwrite events as needed” option.

2.1.1.2 How to Archive a Log

If you want to save your log data, you can archive event logs in any of the following formats:

- Log-file format (.evt)
- Text-file format (.txt)
- Comma-delimited text-file format (.csv)

To archive a log, follow these steps:

1. Click “Start”, “Administrative Tools”, and then click “EventViewer”.
2. Expand the tree and locate the log you want to archive. Right-click on the log and then click “Save All Events As”.
3. Specify a file name and location where you want to save the file. In the “Save As” window, select the desired format to save the file as, and then click “Save”.

The suggested period for archiving is once a week, on Friday after all work has been done.

2.1.1.3 Enabling Audit Log on Specific Folders

You must be careful which objects you audit or you will end up with information overload problems. It's very easy to end up with information overload because if you audit a folder, the audit applies to every object within the folder and within any subfolders. The audit applies to child objects, grandchild objects, and so on. Therefore, when possible, auditing objects at the file level is recommended.

We also recommend that you avoid auditing system files and folders. Doing so can also result in information overload. For example, if you were to audit the Windows folder, you would end up with countless audit log entries because the system is constantly accessing files found in this folder. If you really wanted to audit Windows, a better solution might be to audit the registry files.

To audit a file or folder, open Windows Explorer and navigate to the folder you want to audit. Right-click it and select the Properties command from the resulting menu. You will see the objects Properties sheet. Select the Security tab, and click the Advanced button to display the Access Control Settings Properties sheet for the object. Select the Auditing tab. Click the Continue button, and you will be presented with a list of users and groups which actions were audited. If you want to add some user which actions you want to audit click on Add button and type the users or groups name that you wish and click OK. New window will open as shown in Figure 2-1. As you can see, you can enable success and/or failure audits for many types of access to the file or folder on a user or group basis.

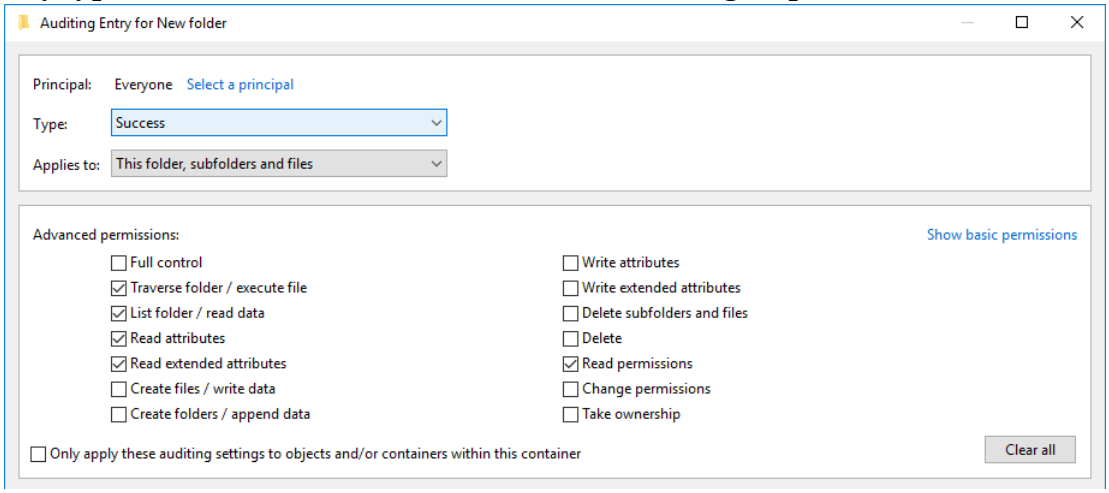

Figure 2-1: Auditing of Different Access Types for Files and Folders.

We recommend only auditing the folders NAS and Databases.

2.1.1.4 Monitoring Audit Log on Specific Folders

To view the audit results, open the Start, then Administrative Tools and then the Event Viewer. When the Event Viewer opens, open Windows Logs in left side tree, then click the Security container to see the security logs. You will notice how many log entries were applied in a matter of a few seconds. This is why it's so important to use discretion when creating an audit policy. If you want to get more information on a particular event, simply double-click it.

2.1.2 Updating Anti-Virus Software

For information regarding the installation and configuration of the anti-virus software, please refer to the Democracy Suite® EMS Standard Installation and Configuration Procedure document. Also, refer to the same document for details on how to download manually download updates for the anti-virus software.

Suggested period for checking updates for anti-virus software is once a week, on Friday after all work has been done.

2.1.3 Defragmenting

Disk defragmentation should be done on regular basis. Suggested period for defragmenting is once a week, on Friday after all work has been done.

To defragment the partition, go to **Start > All Programs > Accessories > System Tools > Disk Defragmenter**. You will see here the list of all partitions you have (see Figure 2-2).

Select the partition you want to defragment and push Defragment disk button. The process may take some time to finish.

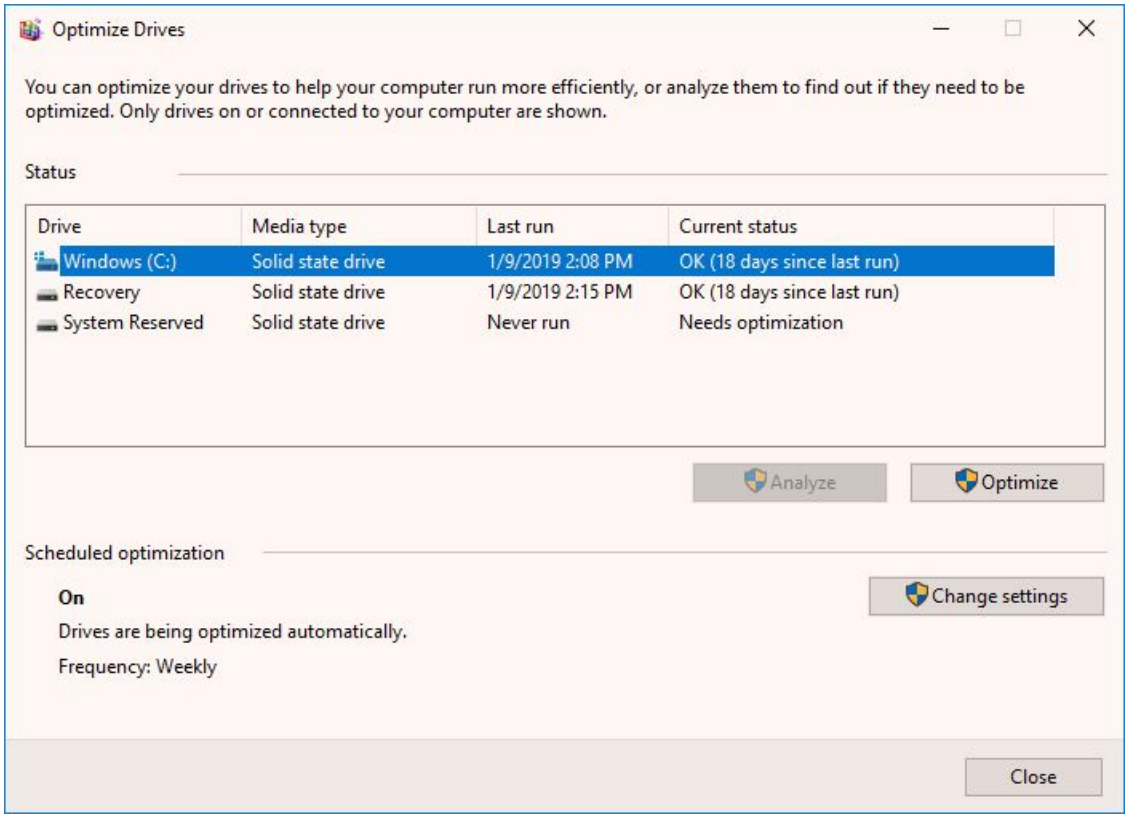

Figure 2-2: Disk Defragmentation.

2.1.4 Personnel Requirements

All preventive maintenance procedures must be performed by an EMS Administrator or by Dominion support personnel. At minimum, each jurisdiction must have at least one EMS Administrator who is experienced in server and database installation, configuration and administration as well Democracy Suite EMS.

2.2 Direct Server Maintenance

Follow the procedures and guidance provided in the various Manufacturers manuals that arrived with your server and client computer hardware. In addition, here are some common Administrator tasks that are recommended. Your jurisdiction may also have IT hardware and software maintenance programs.

NOTE: The system you were provided was certified to a certain configuration. Do not take steps to invalidate that Certification by installing unauthorized software and hardware. Contact your Dominion Voting Systems customer service staff before installing or removing anything on the voting system.

Activities include the following:

1. Review Audit logs
    a. Check application log for warning and error messages for service startup errors, application or database errors and unauthorized application installs
    b. Check security log for warning and error messages for invalid logons, unauthorized user creating, opening or deleting files
    c. Check system log for warning and error messages for hardware and network failures
    d. Check EMS logs for warnings and error messages
    e. Report suspicious activity to the proper authorities for your jurisdiction.
2. Perform/verify daily backup
    a. Run and/or verify that a successful backup of system and data files has completed.
3. Track/monitor system performance and activity
    a. Use Task Manager to check for CPU and memory usage
    b. Use Resources Monitor in Task Manager to monitor all system resources
    c. If hardware vendor provided some kind of software as hardware monitor, use it to check if hardware is operating normally.
4. Physically check and clean the server and client computers
    a. Ensure that cooling fans are operational
    b. Remove dust and other buildup from computer chassis
    c. Pay attention to new and odd noises emanating from a computer
    d. Ensure network and power connections are fully seated

NOTE: Please refer to *Democracy Suite® EMS Election Event Designer User Guide*, section Exporting Project Data.

2.3 Corrective Maintenance Procedures

The corrective maintenance procedure are handled as described in the *Problem and Incident Management* and *Change Control Procedures* sections of the TDP document *2.11 - Democracy Suite® Configuration Management Plan*.

2.4 Troubleshooting and Recovering From an Abnormal State

If any issues are encountered while configuring the EMS Application Server (EMS APPS) using DCM, please try the following troubleshooting procedure:

1. Open SQL Configuration Server
2. Open SQL Server Service
3. Change user to 'Local System' and click 'Apply'
4. Restart SQL Server Service
5. Start SQL Server Agent service if it is available
6. Open Computer Management
7. Navigate to 'Local Users and Groups'
8. Delete the following user accounts:
    - emssqluser
    - emsdbuser
    - emsdbadmin
9. Reboot the computer
10. Run DCM again
11. If the problem persists, please refer to Section 2.7.

If the EMS system becomes unresponsive during any interaction with the operator, please follow the steps below to recover from that state:

- Make sure that all servers you are using are switched on and working, and that all network equipment (if any) is switched on and working.
- Make sure that all client computers you are using are switched on and working.
- For any problems encountered during installation, make sure you followed the installation and configuration manual for both the server and the client computers.
- Try to log in to the server you are using with the default administrator account. Open Task Manager (press Ctrl+Alt+Delete and click on the Start Task Manager button). Under the Process tab, make sure that no process that begins with the name DVS occupies 0% of CPU usage. If so, select that process and click on the End Process button at the bottom. Repeat the process, if necessary.
- Try to log in to each client computer you are using with the default administrator account.

- Open the EMS EED client application. Ensure that the entered EMS database and network settings, as well as the application user accounts, are correct. Check to see if the election event properties have been entered correctly. Create and then ensure the System and Audio Log reports are correct.
- Open the EMS RTR client application. Ensure that the entered EMS database and network settings are correct. Ensure the transfer point parameters are correct. Reboot the server and try again reboot the defected client computer(s) and try again.
- If the problem persists, please refer to section 2.7.

2.5 Parts and Materials

Parts and materials for system maintenance include:

- Microfiber cloths for removing dust
- Small amount of 70% (or greater) isopropyl alcohol for cleaning stubborn marks that cannot be removed with a cloth
- Storage media (CD or DVD ROM) for performing system updates

2.6 Maintenance Facilities and Support

Depending on configuration, please refer to TDP *2.02 - Democracy Suite® System Overview* or section 2.2 Direct Server Maintenance for details.

Please be aware that Dominion Voting Systems recommends that one unit of each hardware device or component be kept on hand as a spare for repair purposes during periods of system operation.

2.7 Operations Support

2.7.1 Requesting Support

When requesting support from Dominion Voting Systems, customers can use the following methods. The options listed below appear in order of efficiency.

1. Enter your issue directly into Dominion Voting's support database via http://online.dominionvoting. com/customerportal/
2. Email the issue directly to Dominion Voting's support team. In the email message, the following details are mandatory:
   - Name
   - Contact telephone with extension
   - Location

- Detailed description of the problem

The support technician will record the issue in Dominion Voting's Customer Portal database and either resolve it on the spot or assign it to an appropriate resource for action. Once Dominion Voting's support team creates the ticket in the Customer Portal system, an email message will automatically be sent to the customers' primary contact email address notifying them that the ticket has been created.

2.7.2 Prioritizing Support (Impact Levels)

All support request/issues are dealt with according to their priority, which is determined depending on their impact levels.

2.7.3 Impact Level 1

Impact Level 1 is the highest priority support situation and is assigned when one or more of the following conditions occur:

- Multiple users (two or more) are directly affected.
- The IT resource cannot function as designed and installed.
- Problem has a critical impact on the customer's tasks.
- A temporary workaround, alternative, or circumvention is not available.

The first Dominion Voting response must occur within one hour of the service interruption. The Dominion Voting support team will establish definitive contact with the customer's primary contact and maintain contact throughout the interruption. The maximum time for resolution is targeted at four elapsed hours (work will continue after regular working hours or on weekends), or as specified in the customer contract covering the requested service.

2.7.4 Impact Level 2

Impact Level 2 describes a medium priority support situation and is assigned when some or all of the following conditions occur:

- Limited (two or less) users are directly affected.
- IT resource is available with degraded performance and/or is difficult to use.
- A temporary workaround, alternative, or circumvention is available.
- The loss may restrict function and have some operational impact; however the situation is not critical.

Dominion Voting will respond within 1 working day. The maximum time targeted for resolution is 40 working hours from the time of Dominion Voting's initial response. Dominion Voting will escalate the problem to the next level and group manager if the targets for response and resolution are not met.

2.7.5 Impact Level 3

Impact level 3 describes a low priority support situation, and is assigned when some or all of the following conditions occur:

- The problem resolution specifies that a system component or software upgrade is necessary, or a design change is required.
- The customer has requested additional information pertaining to a problem or a feature of the system or service.

Dominion Voting will first respond within 2 working days. There is no target time for a resolution, but a reminder email will be issued to the assignee once the ticket has been assigned, as well as every time the status of the ticket changes as it is acted upon.

REVISION HISTORY

Rev.	Date	Summary
4	12-13-2022	Deleted section 1.12 Document Status
3	12-07-2022	Revised section 2.2 Direct Server Maintenance to correct cross-reference
2	11-02-2022	• Revised section 2.2 Direct Server Maintenance to correct cross-reference • Revised section 2.4 Troubleshooting and Recovering From an Abnormal State to delete reference to SQL Server 2008
1	04-20-2022	Branched for 5.13-A.

LIST OF FIGURES

VVSG TRACE LIST

VVSG Criteria Pg.

End of Document

DOMINION VOTING

Our customers come first.