2.09 - Democracy Suite® Adjudication System Maintenance Manual

Version: 5.17-CO::3

April 17, 2023

DOMINION VOTING

Our customers come first.

Table of Contents

CHAPTER 1: INTRODUCTION

This document is a specification for maintenance of EMS Adjudication ("Adjudication") designed and manufactured by Dominion Voting Systems Corporation.

1.1 Document Use

This document is intended for use with the Democracy Suite® 5.17 platform.

1.2 Relevant Disclaimers

This document may make reference to certain Democracy Suite functionalities that are not part of the current 5.17-CO 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.

1.3 Purpose and Scope

This document describes the Adjudication application maintenance procedures. This document provides all information necessary by all personnel who support pre-election and election preparation, post-election and central counting activities, as applicable.

1.3.1 Network Data Transmission

The Adjudication system expects to transmit data over an internal network for the purposes of enabling multiple machines to adjudicate at the same time. Data transmission is done over a standard TCP/IP network configuration, using the tools and network technologies provided by Windows and the .NET Framework. There are no special considerations in regards to maintenance besides what is normal for such networks.

1.4 Data Handling in the Processor and Memory Units

No data in the processor or memory units is directly manipulated by the Adjudication system; this is performed by the .NET Framework and/or the Windows Operating System.

1.5 Data Output Initiation and Control

The Adjudication application consists of several outputs: adjudicated ballot images, adjudicated ballot records, and audit logs. All data and files are stored on the EMS NAS, EED database, or in the Adjudication database. The Cast Vote Record (CVR) service is the interface into the RTR system.

1.6 Power Conversion/Conditioning

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

1.7 Acquiring Test and Diagnostic Information

Please refer to 2.07 - Democracy Suite® System Test and Verification and Specification.

1.8 Applicable Documents

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

1.9 Document Organization

Every attempt has been made to produce the document structured according to the VVSG 1.0 requirements (VVSG 1.0, Volume 2, Section 2.9).

- Chapter 1 Introduction: Purpose and scope of the document (this section)
- Chapter 2 Maintenance Procedures: An overview of the system for maintenance and references to specific documents that explain the maintenance procedures and policies in greater detail.

1.10 Design Responsibility

Dominion Voting is the design authority.

1.11 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

The Adjudication system uses the Windows Event Log to log informational, warning, and error entries as the system runs. Maintenance should be performed on the Event Logs of all the machines on which the system is installed (clients or servers).

By default, when the initial maximum size of a log is reached, new events overwrite older events as needed. It is in the best interest of the user to ensure that log sizes are appropriate and to archive old entries regularly.

2.1.1.1 Changing Event Log Size Settings

Event logs exist on any Windows machines used for Adjudication. This means that if remote client machines are used for Adjudication, you may need to follow the instructions on the server and on each machine used for adjudication. However, it's usually unnecessary to change the default log settings, especially for client machines. Follow these instructions if you want to ensure that the correct settings are set, or for circumstances where the default settings are deemed insufficient.

DVS Adjudication Log:

This is the main event log used by the Adjudication system to log information as it runs. Adjudication client applications use this log with much less frequency than the services which are in charge of most processing. As a result, the size of this log for machines that only have a client installed is set to a small default (1 MB). However, the default is 100 MB for the machine where the EMS Adjudication Services are installed.

To change the size settings of the DVS Adjudication log:

1. Right click the **Windows** icon on the lower left of the screen, then select **Computer Management**.
2. On the left, expand **Event Viewer** and then **Applications** and **Services Logs.**
3. Right click **DVS Adjudication** and select **Properties**.
4. Set the value of the **Maximum Log Size** in kilobytes (KB). For example, to set this to the Windows default, 20 MB, specify 20480. For a 100 MB, specify 102400.

5. Select an option for **When maximum event log size is reached**. For this log, the recommended option is **Archive the log when full, do not overwrite events.**

NOTE: If you select the option to archive the log, make sure to monitor disk space regularly. Windows archives logs to the following location: %SystemRoot%\system32\winevt\logs

Application Log:

The Application Log is used by Windows and installed applications as a general logging facility. The Adjudication system does a minimal amount of logging to this log. Because of the large number of events that are logged during normal use, this log grows significantly.

To change the size settings of the Application Log:

1. Right click the **Windows** icon on the lower left of the screen, then select **Computer Management**.
2. On the left, expand **Event Viewer** and then **Windows Logs**.
3. Right click **Application** and select **Properties**.
4. Set the value of the **Maximum Log Size** to at least 20480 KB.
5. Select an option for **When maximum event log size is reached**. For this log, the recommended option is **Overwrite events as needed**.

NOTE: If you select the option to archive the log instead, make sure to monitor disk space regularly. Windows archives logs to the following location: %SystemRoot%\system32\winevt\logs

Security Log:

The Security log is used by Windows to log security audit events that have been activated. The Adjudication system does not directly log entries to this log, but it can be used to track user log-ins and usage of the Adjudication application key. Because of the large number of events that will be logged during normal use, this log will grow significantly.

To change the size settings of the Security Log:

1. Right click the **Windows** icon on the lower left of the screen, then select **Computer Management**.
2. On the left, expand **Event Viewer** and then **Windows Logs.**
3. Right click **Security** and select **Properties**.
4. Set the value of the **Maximum Log Size** to at least 20480 KB.
5. Select an option for **When maximum event log size is reached**. For this log, the recommended option is **Overwrite events as needed**.

NOTE: If you select the option to archive the log instead, make sure to monitor disk space regularly. Windows archives logs to the following location:
%SystemRoot%\system32\winevt\logs

2.1.1.2 How to Archive a Log

If you want to manually archive or save log data, you can do so by following these steps:

1. Right click the **Windows** icon on the lower left of the screen, select **Computer Management** and expand **Event Viewer.**
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. In the **Save As** window, specify a file name and location for the log file.
4. In the **Save as type** field, select a desired log format (the default is recommended), 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 Properties sheets 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.

We are recommending only auditing the folders NAS and Databases.

2.1.1.4 Monitoring Audit Log on Specific Folders

To view the audit results, right click the Windows icon on the lower left of the screen, select **Computer Management** and expand **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 its 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 Purging Message Queues

The Adjudication system uses the Message Queuing facility provided by Windows to transmit messages between components. Sometimes, especially after ending adjudication for an election or when reinstalling the system, messages end up in the "Dead-Letter Queue". This is a special place for messages that can- not be delivered. Because storing these messages uses system resources, check for and purge these dead messages regularly.

Follow the instructions below to purge dead messages. Since Message Queuing is used on both client and server machines, follow these instructions for all machines used for adjudication. Dominion Voting Systems recommends purging dead messages prior to every election.

NOTE: This procedure purges dead messages for any application that uses Message Queuing, not just the Adjudication system. If you know of other applications that use Message Queuing on the machine, you might want to review their documentation to ensure that purging dead messages will not cause problems.

1. Right click the **Windows** icon on the lower left of the screen, select **Computer Management**.
2. On the left panel, expand **Services and Applications**, **Message Queuing, System Queues**, and select **Transactional dead-letter messages.**
3. To ensure that the view is updated, right-click **Transactional dead-letter messages**, and click **Refresh**.
4. The center panel shows any dead messages currently in the system. If you do not see any messages, then there is nothing to purge. Close the window and stop following these instructions. Otherwise, continue to the next step.
5. To inspect individual messages before removing them, double-click them to see more details. When there are many messages, enable columns to avoid opening each message. To do this:

- Right-click **Transactional dead-letter messages**, select **View**, and select **Add/Remove Columns.**

- In the dialog that appears, select columns from the left and click **Add.** Suggested columns are **"Time Arrived"** and **"Recipient Queue"**, which display the time a message was placed in the queue and the original queue the message was destined for.
- Click **OK** to apply changes and display the selected columns.

6. When you are ready to remove messages, right-click **Transactional dead-letter messages**, then **All Tasks**, and **Purge.**
7. A confirmation message appears; select **Yes** to purge all dead messages.

2.1.3 Updating Security Key

The Adjudication system uses a security key created by the system itself to secure communications be- tween the Adjudication client application and EMS Adjudication Services. It is of paramount importance that this key be kept in a secure location. We recommend that this security key be updated any time a new election is started or in any case where the key may have been compromised. A new key can be created by selecting **Create and install** a new key in the Election Wizard when starting a new adjudication project.

2.1.4 Updating Windows Server 2019 and Windows 10 with the Latest Service Packs

Please refer to *Democracy Suite® EMS Standard System Installation and Configuration Procedure, Democracy Suite® EMS Express Installation and Configuration Procedure* and *Democracy Suite® EMS Client Workstation Installation and Configuration Procedure* documents.

2.1.5 Updating Anti Virus Software

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

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

2.1.6 Defragmenting

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

To optimize drives:

1. Right click the **Windows** icon on the lower left of the screen, select **Search**. Enter **"Defragment"** in the search box, and then select **Defragment** and **Optimize Drives**, , see Figure 2-1.
2. In the center pane, select the drive you want to optimize.
3. To determine if the drive needs to be optimized, press **Analyze**. You might be asked for an administrator password or to confirm your choice.
4. After Windows is finished analyzing the drive, check the **Current** status column to see whether you need to optimize the drive. If the drive is more than 10 percent fragmented, you should optimize the drive now.
5. Press **Optimize** if the drive needs optimization. You might be asked for an administrator password or to confirm your choice.

NOTE: Optimizing a drive might take anywhere from several minutes to a few hours to finish, depending on the size and type of drive, and the degree of optimization needed. You can still use the computer during the optimization process.

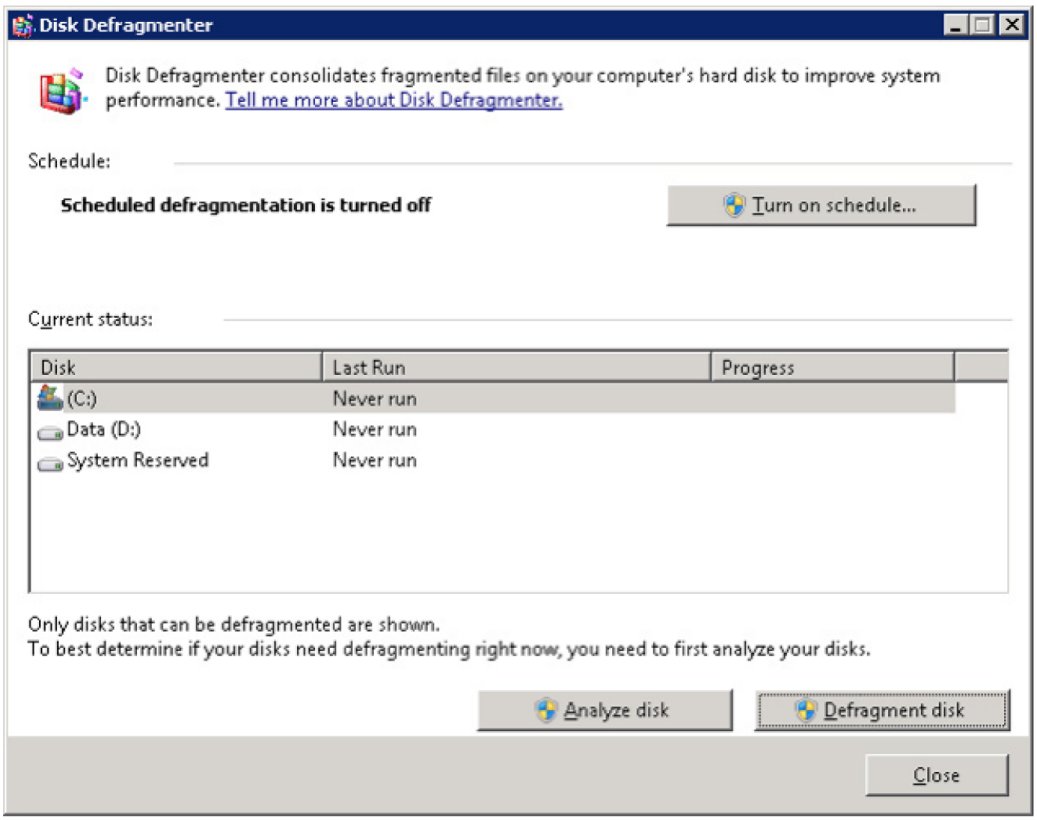

Figure 2-1: Optimize Drives

2.1.7 Personnel Requirements

All preventative 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**
   - Check application log for warning and error messages for service startup errors, application or database errors and unauthorized application installs
   - Check security log for warning and error messages for invalid logons, unauthorized user creating, opening or deleting files
   - Check system log for warning and error messages for hardware and network failures
   - Check EMS logs for warnings and error messages
   - Report suspicious activity to the proper authorities for your jurisdiction
2. **Perform/verify daily backup**
   - Run and/or verify that a successful backup of system and data files has completed. Please refer to *Democracy Suite® EMS Election Event Design User Guide*, Exporting Project Data.
3. Track/monitor system performance and activity
   - Use Task Manager to check for CPU and memory usage
   - Use Resources Monitor in Task Manager to monitor all system resources
   - 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**
   - Ensure that cooling fans are operational
   - Remove dust and other buildup from computer chassis
   - Pay attention to new and odd noises emanating from a computer
   - Ensure network and power connections are fully seated

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 *2.11 - Democracy Suite® Configuration Management Plan*.

2.4 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

2.5 Maintenance Facilities and Support

Depending on configuration, EMS has recommended number for hardware components. Please refer to *2.02 - Democracy Suite® System Overview* and *2.09 - Democracy Suite® EMS System Maintenance Manual*, section *Direct Server Maintenance* for details.

Please be aware that there is no recommended number and locations of spare devices or components to be kept on hand for repair purposes during periods of system operation.

2.6 Operations Support

2.6.1 Requesting Support

When requesting support from Dominion Voting Systems, customers can use the option listed below.

1. 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 Jira which is Dominion Voting System's database project based tracking system 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 an email message will automatically be sent to the customers' primary contact email address notifying them that the ticket has been created.

2.6.2 Prioritizing Support (Impact Levels)

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

2.6.2.1 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.

2.6.2.2 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.

2.6.2.3 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
3	04-17-2023	• Revised using 5.17-CO doc revisions
2	04-05-2023	• Revised with grammar and content corrections
1	02-13-2023	• Branched for 5.17-CO

LIST OF FIGURES

VVSG TRACE LIST

VVSG Criteria Pg.

End of Document

End of Document

DOMINION VOTING

Our customers come first.