

# **Community Viewer (CV) 3.1**

## **Production Operations Manual**



**August 2019**

**Version 1.2**

**Department of Veterans Affairs**

**Office of Information and Technology (OIT)**

## Revision History

Date	Version	Description	Author
08/22/2019	1.2	Received VA PM Approval	AbleVets
08/19/2019	1.2	Submitted for VA PM Approval	AbleVets
08/15/2019	1.1	Implemented client feedback	AbleVets
08/08/2019	1.0	Delivered for review	AbleVets
07/17/2019	0.1	Initial draft of document from the last approved	AbleVets

## Artifact Rationale

The Production Operations Manual (POM) provides the information needed by the Production Operations team to maintain and troubleshoot the product. The POM must be provided prior to release of the product.

## Table of Contents

<b>1. Introduction .....</b>	<b>1</b>
<b>2. Routine Operations.....</b>	<b>1</b>
2.1. Administrative Procedures .....	1
2.1.1. System Startup.....	1
2.1.1.1. System Startup from Emergency Shutdown .....	3
2.1.2. System Shutdown.....	3
2.1.2.1. Emergency System Shutdown .....	4
2.1.3. Backup and Restore .....	4
2.1.3.1. Backup Procedures .....	4
2.1.3.2. Restore Procedures.....	5
2.1.3.3. Backup Testing .....	6
2.1.3.4. Storage and Rotation .....	7
2.2. Security/Identification (ID) Management .....	7
2.2.1. Identity Management .....	8
2.2.2. Access Control.....	8
2.3. User Notifications .....	9
2.3.1. User Notification Points of Contact .....	9
2.4. System Monitoring, Reporting, and Tools .....	10
2.4.1. Dataflow Diagram.....	10
2.4.2. VistA Imaging (VI) Data Retrieval .....	11
2.4.3. PPMS Data Web Service (DWS) Retrieval .....	12
2.4.4. Availability Monitoring .....	12
2.4.4.1. Domain-Level Availability Monitoring .....	14
2.4.5. Performance/Capacity Monitoring .....	15
2.4.6. Critical Metrics .....	15
2.5. Routine Updates, Extracts, and Purges .....	15
2.5.1. Routine Updates.....	15
2.5.2. Quarterly Update of the VistA Site List.....	16
2.5.3. Extracts .....	16
2.5.4. Purges .....	16
2.6. Scheduled Maintenance .....	16
2.7. Capacity Planning.....	16
2.7.1. Initial Capacity Plan .....	17
<b>3. Exception Handling.....</b>	<b>17</b>
3.1. Routine Errors .....	17
3.1.1. Security Errors .....	17
3.1.2. Login Errors.....	17

3.1.3.	Timeouts .....	17
3.1.3.1.	Application Timeout .....	17
3.1.3.2.	Connection Errors .....	18
3.1.4.	Concurrency .....	19
3.2.	Significant Errors .....	19
3.2.1.	Application Error Logs .....	19
3.2.2.	Application Error Codes and Descriptions .....	21
3.2.3.	Infrastructure Errors .....	21
3.2.3.1.	DB .....	21
3.2.3.2.	Web Server .....	25
3.2.3.3.	Application Server .....	25
3.2.3.4.	Network.....	25
3.2.3.5.	Authentication and Authorization (A&A).....	25
3.2.3.6.	Logical and Physical Descriptions .....	26
3.3.	Dependent System(s) .....	26
3.4.	Troubleshooting.....	27
3.5.	System Recovery .....	27
3.5.1.	Restart After Unscheduled System Interruption .....	27
3.5.2.	Restart After DB Restore.....	27
3.5.3.	Backout Procedures .....	27
3.5.4.	Rollback Procedures .....	27
4.	Operations and Maintenance Responsibilities .....	27
5.	Approval Signatures .....	30
A.	Acronyms and Abbreviations .....	31

## Table of Figures

Figure 1: Database Names Tree .....	5
Figure 2: Source/Device/Database Dialog Box .....	5
Figure 3: Restore Plan Dialog Box .....	6
Figure 4: Data Retrieval from VA Systems .....	11
Figure 5: PPMS DWS Retrieval .....	12
Figure 6: System Status Check Sequence .....	13
Figure 7: Connection Status Details.....	14
Figure 8: Patching Process for CV Components.....	16
Figure 9: Session Timeout Notification .....	18
Figure 10: Session Timeout .....	18
Figure 11: Connection Error .....	19
Figure 12: jMeadows Log Output.....	20
Figure 13: CV Architecture and Components.....	22
Figure 14: Audit Log .....	24

## Table of Tables

Table 1: Virtual Machine (VM) Hardware Specifications.....	4
Table 2: Access Control Design .....	9
Table 3: CV Scheduled Downtime Notification List (VA Stakeholders).....	9
Table 4: Response Time Log Location .....	20
Table 5: User Authentication Sequence Overview .....	25
Table 6: CV External Dependent Systems.....	26
Table 7: Responsibility Matrix (Operational Roles and Responsibilities).....	27
Table 8: Acronyms and Abbreviations .....	31

# 1. Introduction

Community Viewer (CV) is a browser-based software application that facilitates the secure exchange of data between Department of Veterans Affairs (VA) systems and authorized non-VA providers, known as Community Care Providers (CCPs) or Provider Profile Management System (PPMS) providers. The exchange of data improves the coordination of care and continuity of care for VA patients receiving treatment outside of the VA network.

CV pulls information from VA health care systems in real time for viewing within a web browser. Through CV, VA Staff (VAS) assign patients to CCPs and Risk Management (RM) users, allowing them access to view consolidated patient data from multiple Veterans Information Systems and Technology Architecture (VistA) systems.

## 2. Routine Operations

Routine operations are performed by System Administrators to ensure the upkeep, configuration, and reliable operation of computer systems. System Administrators also ensure that the uptime, performance, resources, and security of the systems meet the needs of the end users.

### 2.1. Administrative Procedures

#### 2.1.1. System Startup

The start of the CV database (DB) servers is performed by Team AbleVets Operations in the Austin Information Technology Center (AITC).

A detailed list of the servers referenced throughout the system startup procedures can be found in the International Business Machines Corporation (IBM) [Rational Source Control Repository](#).<sup>1</sup>



**NOTE:** The following procedures apply to both the VA Staff and CCP modules of CV.

1. Start the CV DB servers in AITC
  - a. The DB server processes are configured to run as system services and are automatically started with the DB servers
  - b. Validation
    - i. Startup is validated through the successful smoke test of the application; loading the CV Login page and logging in to the application confirms that the DB servers are up and operational
    - ii. The Operations team logs in to each DB server to validate that the Microsoft (MS) Structured Query Language (SQL) Server service has started; if the service has started, it signifies that the DB servers are up and operational
    - iii. The Operations team logs in to each DB server, opens SQL Server Management Studio (SSMS) and connects to the DB; the connection is successful if the DB servers are up and operational

---

<sup>1</sup> **NOTE:** Access to IBM Rational is restricted and must be requested.

2. Start the VistA Data Service (VDS) servers in AITC
  - a. The service processes are configured to run as system services and are automatically started with the VDS servers
  - b. Validation
    - i. Startup is validated through the successful smoke test of the application; loading the CV Login page and logging in to the application confirms that the servers are up and operational
    - ii. If startup is unsuccessful, the Operations team investigates the server log files and determines the correct resolution, possibly server reboots
3. Start the jMeadows servers in AITC
  - a. The service processes are configured to run as system services, which are automatically started with the servers
  - b. Validation
    - i. Startup is validated through the successful smoke test of the application; loading the CV Login page and logging in to the application confirms that the servers are up and operational
    - ii. If startup is unsuccessful, the Operations team investigates the server log files and determines the correct resolution, possibly server reboots
4. Start the CV web application servers (cloud)
  - a. The service processes are configured to run as system services and are automatically started with the application servers
  - b. Validation
    - i. Startup is validated through the successful smoke test of the application; loading the CV Login page and logging in to the application confirms that the servers are up and operational (Detailed information can be found in the *Installation Verification Procedures* section of the *CV 3.1 Deployment, Installation, Backout and Rollback Guide [DIBR]*. Once approved, all project documentation is available on the [Project Joint Legacy Viewer \(JLV\)/CV SharePoint](#) site<sup>2</sup>.)
    - ii. If startup is unsuccessful, the Operations team investigates the server log files and determines the correct resolution, possibly server reboots
5. Infrastructure Operations (IO) personnel start the CV web application servers for CCPs in AITC non-cloud environment
  - a. The service processes are configured to run as system services and are automatically started with the servers
  - b. Validation
    - i. Startup is validated through the successful smoke test of the application; loading the CV Login page and logging in to the application confirms that the DB is up and operational (Detailed information can be found in *Section 4.9* of the *CV 3.1 DIBR*. Once approved, all project documentation is available on the Project JLV/CV SharePoint site. See [4.b.i](#), immediately above, for the repository link.

---

<sup>2</sup> **NOTE:** Access to the Project JLV/CV SharePoint site is restricted and must be requested.

- ii. If startup is unsuccessful, IO investigates the server log files and determines the correct resolution, possibly server reboots
6. Log in with a VA Staff user test account:
    - a. Use a Personal Identity Verification (PIV) card and Personal Identification Number (PIN), when prompted
    - b. Verify that the CV Login page for VA Staff displays as expected and that the system status indicates services are online and connected
    - c. Enter Access/Verify codes
    - d. Verify VA Staff Portal loads



**NOTE:** The CV Operations and Engineering teams run a script to ensure that all systems are operational. In addition, opening the Uniform Resource Locator (URL) for CV ensures that all CV context roots are successfully reached.

7. Log in to the CV web application with a CCP test username and password:
  - a. Verify that the CV Login page for CCPs displays as expected and indicates that the system status indicates that services are online and connected
  - b. Enter username (National Provider Identifier [NPI] or e-mail address) and password
  - c. Verify Provider Portal loads

#### **2.1.1.1. System Startup from Emergency Shutdown**

If there is a power outage or other abrupt termination of the server operating systems, start up the servers as detailed in [System Startup](#) and allow the operating system to check the disks for corruption. Consult with IO to ensure that the DB successfully recovers.

#### **2.1.2. System Shutdown**

Shutdown procedures are performed during a published maintenance window, when there are few users accessing the system, to avoid impacting transactions in progress. [Table 1](#) lists the AITC servers. A diagram of the CV Production environment can be found in the *CV 3.1 DIBR (Figure 1)*. Once approved, all project documentation is available on the Project JLV/CV SharePoint site. See [System Startup](#) for the link to the repository.

1. Shut down the WebLogic services on the CV web application servers in AITC
2. Shut down the CV web application servers in AITC (cloud)
3. Shut down the CV web application servers in AITC (non-cloud)
4. Shut down the WebLogic services on the jMeadows servers in AITC
5. Shut down the jMeadows servers in AITC
6. Shut down the WebLogic services on the VDS servers in AITC
7. Shut down the VDS servers in AITC
8. Shut down the CV DB servers in AITC



**Table 1: Virtual Machine (VM) Hardware Specifications**

Required Hardware	Model	Configuration	Manufacturer	Server Count
<b>CV Web Application (for VA Staff users)</b>	Red Hat Enterprise Linux Server release 6.9 (Santiago)	2 Central Processing Units (CPUs), 16 Gigabytes (GB) Random Access Memory (RAM)	Virtual	2 Servers
<b>CV Web Application (for CCP users)</b>	Red Hat Enterprise Linux Server release 6.9 (Santiago)	2 CPUs, 16 GB RAM	Virtual	3 Servers
<b>VDS Servers</b>	Red Hat Enterprise Linux Server release 6.9 (Santiago)	2 CPUs, 16 GB RAM	Virtual	3 Servers
<b>jMeadows Quality of Service (QoS) Servers</b>	Red Hat Enterprise Linux Server release 6.9 (Santiago)	2 CPUs, 16 GB RAM	Virtual	4 Servers
<b>CV DB Servers</b>	MS Windows Server 2012 R2 Standard	4 CPUs, 16 GB RAM	Virtual	2 Servers

A detailed list of the servers referenced throughout this POM can be found in IBM Rational Source Control. See [System Startup](#) for the link to the repository.

#### **2.1.2.1. Emergency System Shutdown**

The emergency system shutdown procedure is to shut down all servers (CV web applications in both cloud and non-cloud environments, jMeadows, VDS, and the CV DB) in AITC, in any order.

A detailed list of the servers referenced throughout this POM can be found in IBM Rational Source Control. See [System Startup](#) for the link to the repository.

#### **2.1.3. Backup and Restore**

This section provides a high-level description of the backup and restore strategy, including all components that require backup and the devices or infrastructure that perform the backup and restore procedures.

IO manages the platform and installation of both the operating systems and the baseline installation of the MS SQL Server in the VA Production environment.

##### **2.1.3.1. Backup Procedures**

Backups of the CV DB are configured to run, automatically, at midnight daily. The DB servers are backed up at the IO data center by the AITC Systems Administrators using IO's backup solution. The DB servers also have a MS SQL DB maintenance that automatically backs up each DB to the following location on each server:

A detailed list of the servers referenced throughout this POM can be found in IBM Rational Source Control. See [System Startup](#) for the link to the repository.

- D:\DBBackups

- D:\DBBackups\TransactionLogs

### 2.1.3.2. Restore Procedures

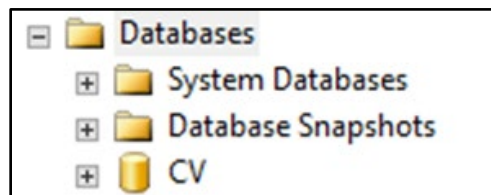
The items necessary for the recovery of the DBs are:

- DB backup (.bak) file for the CV DB
- Encryption keys for the DB

Restore a full DB backup:

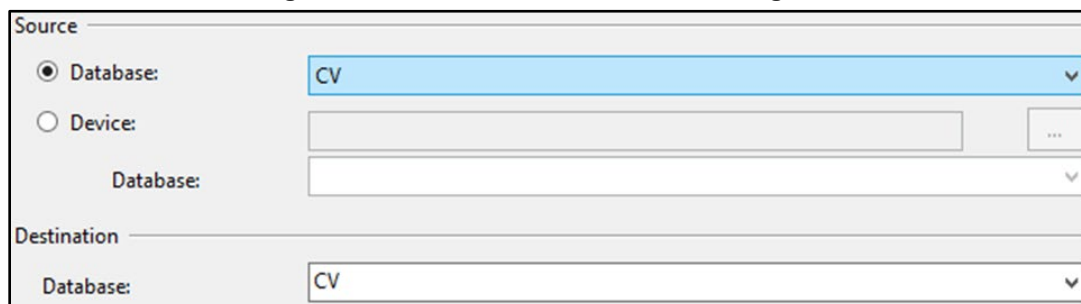
1. Connect to the appropriate instance of the MS SQL Server DB Engine in SSMS
2. Click the server name to expand the server tree
3. Right-click **Databases**

**Figure 1: Database Names Tree**



4. Click **Restore Database**
5. Use the **Source** section on the **General** page to specify the source and location of the backup sets to restore; select the following options:
  - a. Click the **Browse (...)** button to open the **Select Backup Devices** dialog box
  - b. Select **File** in the Backup Media Type box, then click **Add**
  - c. Navigate to the location of the backup file (.bak) of the CV DB, then click **OK**
  - d. After you add the devices you want to the **Backup Media Type** box, click **OK** to return to the **General** page
  - e. Select the name of the DB to be restored (CV) in the **Source Device: DB List** box

**Figure 2: Source/Device/Database Dialog Box**



6. The **Database** box in the **Destination** section automatically populates with the name of the DB to be restored

- a. Select CV from the dropdown
7. Leave the default in the **Restore To** box as the last backup taken, or click **Timeline** to access the **Backup Timeline** dialog box to manually select a point in time to stop the recovery action
8. Select the backups to restore in the **Backup Sets to Restore** grid
  - a. This grid displays the backups available for the specified location
  - b. By default, a recovery plan is suggested; to override the suggested recovery plan, change the selections in the grid

**Figure 3: Restore Plan Dialog Box**

Restore plan						
Backup sets to restore:						
Restore	Name	Component	Type	Server	Database	Position
<input checked="" type="checkbox"/>	CV_backup_2018_12_13_000002_1596274	Database	Full	VAAUSGTDSQL200	CV	1

- c. Backups dependent upon the restoration of an earlier backup are automatically deselected when the earlier backup is deselected



**NOTE:** Default options are not selected if an attribute necessary for restoration is not contained within the default backup.

9. Alternatively, click **Files** in the **Select a Page** pane to access the **Files** dialog box
  - a. Restore the DB to a new location by specifying a new restore destination for each file in the **Restore the database files as** grid

### 2.1.3.3. Backup Testing

A detailed list of the servers referenced throughout this POM can be found in IBM Rational Source Control. See [System Startup](#) for the link to the repository.

1. Servers
  - a. Backups of the VMs are done at the VA data center by AITC Systems Administrators
  - b. Backups are performed daily
  - c. Testing of the backups is performed by IO
  - d. Validation of restorations are confirmed by:
    - i. Validating that all software/configurations are restored from the expected configuration
    - ii. Confirming that the configuration files contain server-specific settings
    - iii. Validating that the application server starts as expected through logs and a smoke test of the application
2. DB
  - a. Backups are performed at midnight daily

- b. Backups are periodically restored, on an ad hoc basis, to the backup DB servers to test the restore procedures and the integrity of the backup files
- c. AITC System Administrators validate that data in the DB contains up-to-date entries for the user profiles and audit logging
- d. Validation of operations is confirmed through a smoke test of the application

#### **2.1.3.4. Storage and Rotation**

IO manages the platform and any storage and rotation scheduling in the CV Production environment. IO ensures the system and storage arrays are operating properly, with daily inspections of CV QoS logs and system notifications.

Team AbleVets is responsible for ensuring that the partition structure in use is sufficient, which, in turn, ensures there is enough storage space.

## **2.2. Security/Identification (ID) Management**

Access to CV is restricted to authorized VistA users within, and authorized providers outside of, the VA. Authorized VistA users are referred to as VA Staff. Authorized providers outside of the VA are referred to as CCPs (or PPMS providers). CV utilizes HTTP Strict Transport Security (HSTS) which is a web security policy mechanism that helps to protect websites against protocol downgrade attacks and cookie hijacking.

Three tables within the CV DB are used for ID management; the PPMS\_Provider table, the C\_Provider table, and the VAS\_UserRole table:

- The PPMS\_Provider table within the CV DB lists CCPs' first names, last names, e-mail address, and their associated NPI numbers
- The C\_Provider table within the CV DB lists CCPs' and RM users' first names, last names, and their associated e-mail addresses
- The VAS\_UserRole table within the CV DB assigns roles to VA Staff users specific to their function (e.g., Tier 1 VA Staff, Tier 2 VA Staff, Risk Management Provider Manager [RMPPM], or Service Desk User [SDU]) and stores their associated PIV information

The CV Login page guides VA Staff users through the login process, including, where necessary, fields to enter specific credentials. The CV Login page fields request the VA Staff user's Access/Verify Codes, Agency, and Site. VA Staff users must have their PIV card in place before entering the CV URL into the address bar of a supported browser.

SDUs must have their PIV card in place before entering the CV URL into the address bar of a supported browser. SDUs log in with their PIV card and PIN but are not required to have or use Access/Verify codes.

CCPs can use either the e-mail address associated with their account or their NPI, and a password to log in. CV queries PPMS during login to see if a provider has an NPI listed within PPMS. If they do, they are considered "active." If there is no NPI listed for a provider, they are not considered active, and will be unable to log in to CV.



**NOTE:** The *username* field of the CV Login page has been made a free text field to accommodate either an e-mail address or NPI entry.

A detailed overview of the login process, from the user's perspective, can be found in the *CV 3.1 VA Staff User Guide* and the *CV 3.1 Community Care Provider (CCP) User Guide*. Once approved, all project documentation is available on the Project JLV/CV SharePoint site. See [System Startup](#) for the link to the repository.

### **2.2.1. Identity Management**

Any VA user with VistA credentials can access either the Community Care PPMS Provider Management widget or the Risk Management Provider Management widget on the CV VA Staff portal page, depending on their role.

CCP user accounts are created by VA Staff or the Community Provider Technical Service Desk. Detailed instructions for creating CCP user accounts are found in the *CV 3.1 VA Staff User Guide*. Once approved, all project documentation is available on the Project JLV/CV SharePoint site. See [System Startup](#) for the link to the repository.

### **2.2.2. Access Control**

CV access control for CCPs consists of the validation of user credentials, retrieved from the Login page, against the CV DB. When the user's credentials are found in the PPMS\_Provider table of the CV DB, the user is granted access to CV. CCPs may encounter a login error message if they attempt to access CV when their status is not set to *active* in PPMS: *There is an issue preventing your access to Community Viewer. Please contact your VA Contractor or VA Medical Center for assistance.*

VA Staff control CCP access to patient records by making assignments for a specified date range. A CCP can access only the records of the patient with whom they have an assigned consultation for the time period set by VA Staff.

SDUs must be added to the VAS\_UserRole table as authorized users. Once authorized, they use their PIV card and PIN to gain access to the application.

VA Staff use their PIV card, PIN, and VistA credentials to access either the Community Care PPMS Provider Management widget or the Risk Management Provider Management widget on the VA Staff portal page, depending on their role.

[Table 2](#) summarizes the CV system components and the settings utilized for access control.

**Table 2: Access Control Design**

Component	Description
<b>DB</b>	The PPMS_Provider table within the DB contains NPI values used as usernames for CCPs. The C_Provider table within the DB contains e-mail addresses used as usernames for CCPs and RM users. System design specifications and diagrams can be found in the <a href="#">CV Design, Engineering, and Architecture (DE&amp;A) Compliance Requirements collection</a> in the Rational Tool Suite <sup>3</sup> .
<b>DB script</b>	A DB script is used to deliver changes or updates to the pertinent tables within the CV DB.
<b>Configuration settings</b>	A configuration setting within the appconfig-production.properties file that enables access control. <ul style="list-style-type: none"> <li><i>Enable VA Access Control, On/Off:</i> This setting enables access control for VA Staff.</li> </ul>
<b>VAS_UserRole table</b>	The VAS_UserRole table is the authorized user table for SDUs. Once added to the table, SDUs can gain access to CV.

## 2.3. User Notifications

Notifications are sent via e-mail to VA Stakeholders when there are scheduled or unscheduled changes in system state, including but not limited to: planned us, system upgrades, maintenance work, and any unexpected system outages. The Veterans Health Administration (VHA) CV team is responsible for crafting and approving outage notification messages before they are posted to the Announcements section of the CV Login page and banners within the application.

Notifications for planned outages are initiated 24 hours in advance of anticipated system downtime, and notification of an unscheduled outage occurs if an error does not clear within 15 minutes. The notification process for unscheduled outages is as follows:

3. The CV Support team monitors and evaluates all system issues
4. The QoS service alerts are e-mailed to the CV Support team and a defined list of contacts when a service disruption occurs
5. The CV Support team notifies Tier 2 Support of the Enterprise Service Desk (ESD) about any outage, and reports the same to VA users via e-mail, with an ESD ticket number, and the date and time of the outage

### 2.3.1. User Notification Points of Contact

[Table 3](#) details the current notification list for alerting VA stakeholders of scheduled CV downtime. This list is maintained by Team AbleVets.

**Table 3: CV Scheduled Downtime Notification List (VA Stakeholders)**

Name	Organization	Email Address
Reed, Colleen	VA-Government	colleen.reed@va.gov
Freeny, Vincent	VA-Government	vincent.freeny@va.gov

<sup>3</sup> **NOTE:** Access to IBM Rational is restricted and must be requested.

Name	Organization	Email Address
Renee, Jolie	VA-Government	joile.renee@va.gov
Crumpler, Judy	AbleVets	judith.crumpler@va.gov
Guebert, Chad	AbleVets	chad.guebert@va.gov
Lukens, Rich	AbleVets	richard.lukens@va.gov
Carvalho, Robert	AbleVets	robert.carvalho@va.gov
Goo, Brad	HRG	brad.goo@va.gov
Cardenas, Michael	HRG	michael.cardenas5@va.gov
Suenaga, Gregory	HRG	gregory.suenaga@va.gov
Ruble, Ronald (JR)	VA-Government	ronald.ruble@va.gov
Beloro, Bill	VA-Government	bill.beloro@va.gov
Roberts, Jerilyn	VA-Government	jerilyn.roberts1@va.gov
Boie, Michelle	VA-Government	michelle.boie@va.gov
Haas, Christine	VA-Government	christine.haas@va.gov
Jernigan, Jeannie	VA-Government	jeannie.jernigan@va.gov
Tirupati, Kiran	Systems Made Simple (SMS)	kiran.tirupati@va.gov
Punyala, Dinesh	SMS	dinesh.punyala@va.gov
Obiahu, Juliet	Government CIO	juliet.obiahu@va.gov
Peterkin, Brittany	Government CIO	brittany.peterkin@va.gov
Tran, Le-An	Government CIO	le-an.tran@va.gov
Xu, James	Government CIO	james.xu@va.gov

## 2.4. System Monitoring, Reporting, and Tools

CV traces and audits actions that a user executes within the application. CV audits are provided through audit trails and audit logs that offer a backend view of system use, in addition to storing user views of patient data. Audit trails and logs record key activities (date and time of the event, patient identifiers, user identifiers, type of action, and access location) to show system threads of access and the views of patient records. Refer to [Application Error Logs](#) for more information about audit and server logs.

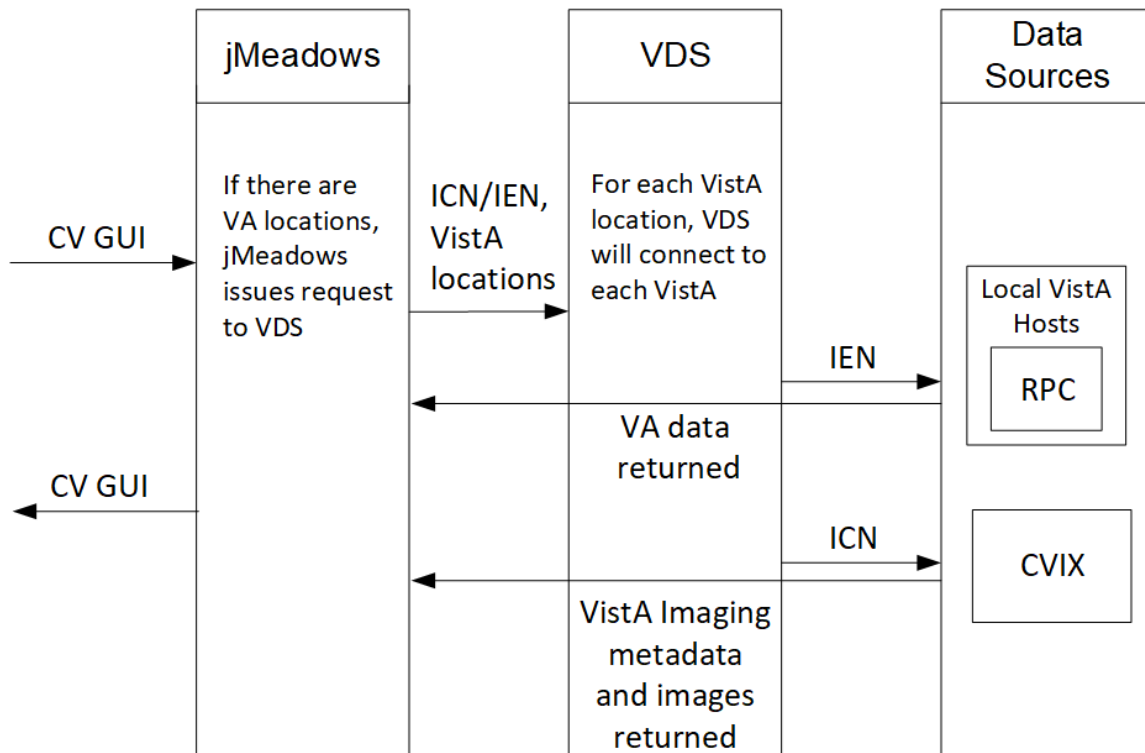
The CV QoS service monitors the availability of data sources. Refer to [Availability Monitoring](#) for more information.

### 2.4.1. Dataflow Diagram

The data retrieval sequence, depicted in [Figure 4](#), occurs after a patient is selected:

1. jMeadows issues a request to VDS with the VA Integration Control Number (ICN)/Internal Entry Number (IEN) and VistA location for each VA location in the patient record; the ICN and VistA location information is received from the Master Veteran Index (MVI)
2. VDS connects to each VistA and returns the clinical data to jMeadows for each VistA location, detailed in [VistA Imaging \(VI\) Data Retrieval](#)
3. jMeadows aggregates the data and returns the data to the CV application

**Figure 4: Data Retrieval from VA Systems**



### 2.4.2. VistA Imaging (VI) Data Retrieval

CV utilizes the Central VistA Imaging Exchange (CVIX) Viewer Service Application Programming Interface (API) to retrieve and display nondiagnostic quality Joint Photographic Experts Group (JPEG) images and Portable Document Formats (PDFs). Images and/or PDFs are displayed in the Radiology Exams, Encounters, and Progress Notes widgets. Some progress notes that have images associated with them appear in the Pain Management widget.

The retrieval and display sequence involve three requests to CVIX.

1. A Station 200 service account is created for CV to communicate with the VI services
  - a. When the user logs in to CV, a Broker Security Enhancement (BSE) token is retrieved for the service account to enable communication with the CVIX Viewer Study Query service
  - b. The service account credentials and site information are used for the basic authentication when communicating with the VI Study and VI Image services
2. When the user clicks the camera icon, CV first makes a Study Query request to CVIX
3. jMeadowsCCP constructs the contextID needed by the CVIX API
  - a. The accepted file types are identified in the VDS code
    - i. **Example:** contentType=image/JPEG 2000 (j2k),image/jpeg,application/pdf
  - b. The J2K file types are converted to JPEG format using GraphicsMagick
4. CV then makes a request to retrieve the study details
5. When the two requests to CVIX are complete, CV displays the list of study groups and images in a dialog



6. When the user clicks a study's image link, CV initiates a third request to CVIX for the image data
7. The image data is returned, and CV displays the image in a new browser tab
  - a. The image quality is set in the CV CCP configuration file
    - i. **Example:** `grails.vixImageQuality=90`



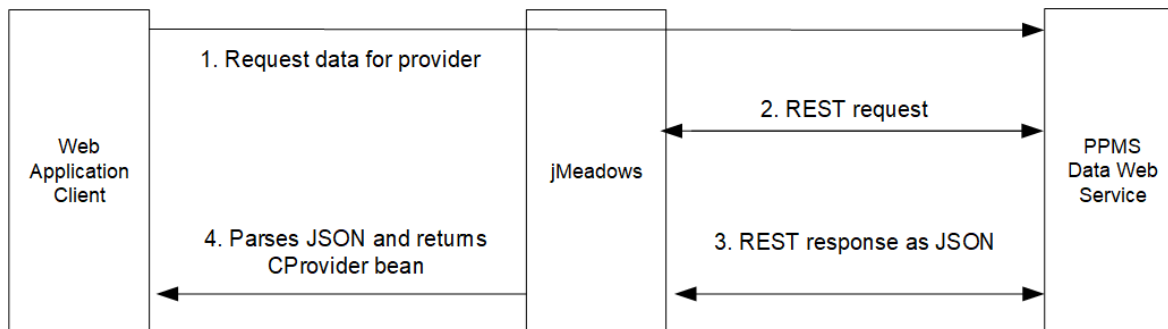
**NOTE:** If the image is not in JPEG or PDF format the error message, *"The current image is not a supported file type and cannot be displayed."* appears.

### 2.4.3. PPMS Data Web Service (DWS) Retrieval

The PPMS data retrieval sequence is depicted in [Figure 5](#).

1. CV requests data for a provider from the jMeadows SOAP service
2. The jMeadows SOAP service layer makes the corresponding REST request and sends the security token to PPMS
3. PPMS returns a REST response as JSON to jMeadows
4. jMeadowsVAS parses the JSON and returns a CProvider bean
5. The CProvider bean is communicated back to the Graphical User Interface (GUI), which returns the response to the Manage PPMS Providers screen

**Figure 5: PPMS DWS Retrieval**



For detailed information, see the *PPMS Data Service Interface Control Document (ICD)*. The ICD can be found in Rational Source Control<sup>4</sup>. See [System Startup](#) for the link to the repository.

### 2.4.4. Availability Monitoring

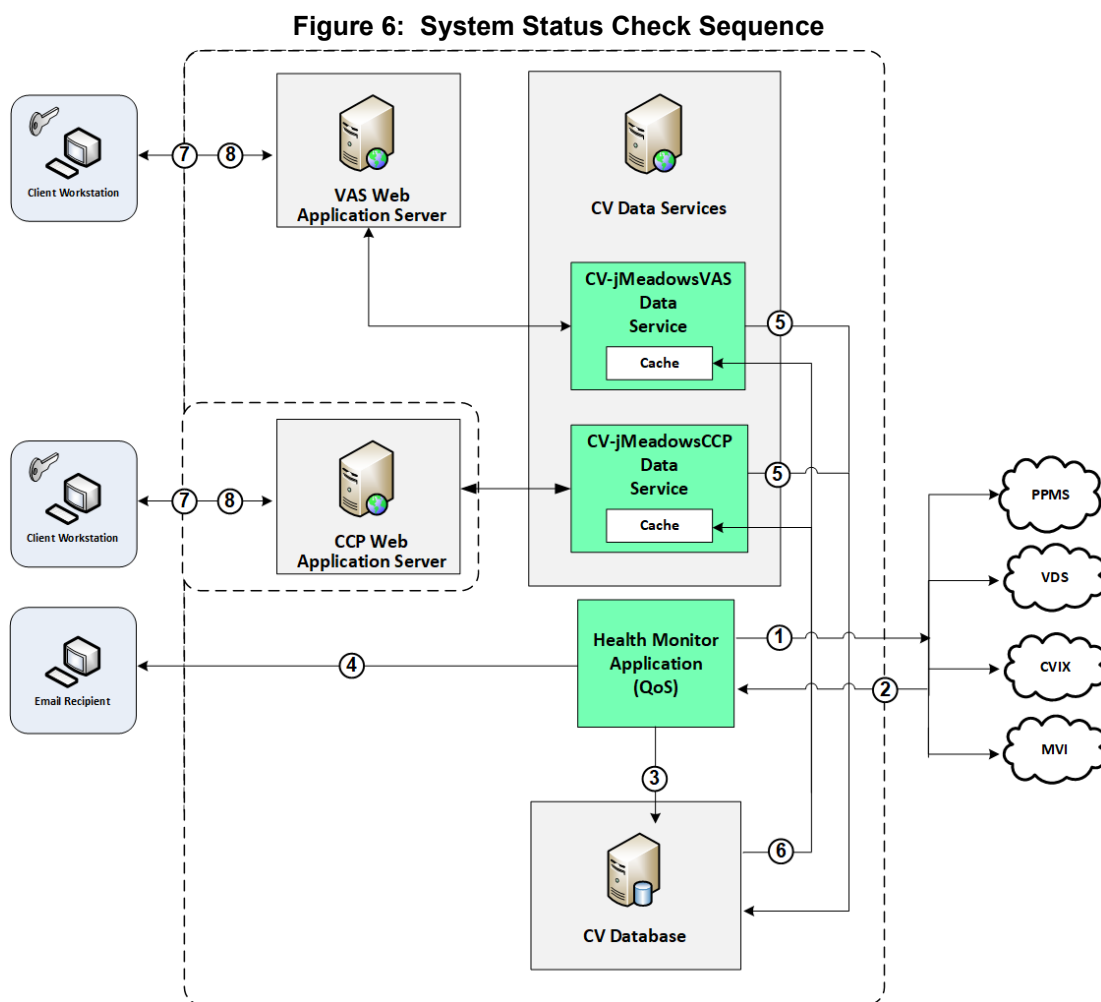
The QoS monitors the health of the CV application and checks for the availability or disruption of dependent services within the systems in VA environments. The CV QoS Service monitors:

- MVI
- VDS:
  - CVIX

<sup>4</sup> **NOTE:** Access to IBM Rational is restricted and must be requested.

- VistA Hosts
- jMeadows Data Service
- PPMS

System status is displayed on the Login page and in the application when there is a degradation. System status events are logged to the CV DB, and users are notified of system status via the Login page.





System status checks ([Figure 6](#)) are performed as follows:

1. The Health Monitor pings the monitored services every 5 minutes
2. The Health Monitor receives a system status from each monitored service
3. System status events are written to the QOS\_LOGS table, within the CV DB
4. The Health Monitor sends an automated e-mail notification every 6 hours, unless a status change is detected
  - a. Detection of a status change immediately triggers an e-mail notification, and the 6-hour timer is reset

- b. The next e-mail is generated after 6 hours, if no further system status changes are detected
5. The CV-jMeadowsVAS and CV-jMeadowsCCP Data Services ping the CV DB every 2 minutes for status checks
6. The CV-jMeadowsVAS and CV-jMeadowsCCP Data Services store the data returned from the CV DB in their internal caches, the CV-jMeadowsVAS or CV-jMeadowsCCP Data Services cache, respectively
7. When a user accesses the CV Login page, the CV application requests and receives system status data from either the CV-jMeadowsVAS or CV-jMeadowsCCP Data Service cache
8. Every 5 minutes of an active user session, CCP or VAS application server requests system status data from either the CV-jMeadowsCCP or CV-jMeadowsVAS Data Service cache
  - a. Current system status is retrieved from either cache and sent to the CCP or VA Staff GUI

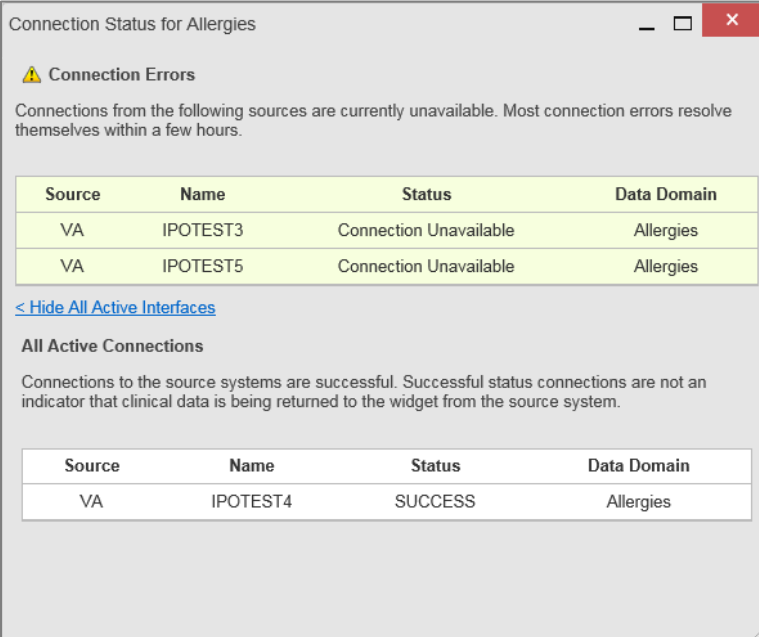
#### 2.4.4.1. Domain-Level Availability Monitoring

CV displays interface status icons on the toolbars of multiple Patient Portal widgets to communicate the status of the data source for the widget's clinical domain. There are two conditions:


- The information icon  indicates that all sources are available
- The warning icon  indicates one or more data sources are unavailable

Both icons are used to provide status for data sources. Clicking the status icon opens interface status details in a separate window, as shown in [Figure 7](#).

**Figure 7: Connection Status Details**



Connection Status for Allergies

 **Connection Errors**

Connections from the following sources are currently unavailable. Most connection errors resolve themselves within a few hours.

Source	Name	Status	Data Domain
VA	IPOTEST3	Connection Unavailable	Allergies
VA	IPOTEST5	Connection Unavailable	Allergies

[< Hide All Active Interfaces](#)

**All Active Connections**

Connections to the source systems are successful. Successful status connections are not an indicator that clinical data is being returned to the widget from the source system.

Source	Name	Status	Data Domain
VA	IPOTEST4	SUCCESS	Allergies

### **2.4.5. Performance/Capacity Monitoring**

Query times for each web service call in to jMeadows and VDS are recorded to a file in the /u01/CV\_HOME/logs/ directory on the server, where the services are installed. Performance monitoring data is collected by the AITC Monitoring group using the Computer Associates (CA) Application Performance Management (APM) suite.

Refer to [Application Error Logs](#) for more information on audit and server logs.

### **2.4.6. Critical Metrics**

The CV Development team adds metric requirement reporting to the product backlog as metrics are defined. Current metrics considered critical are user metrics, core system metrics, user transactions, error logging, QoS metrics (service stability/availability), and other industry-standard system/performance metrics. The metric data is reported in the weekly Operations report and the weekly/monthly usage report.

Examples of the critical metrics listed above, and captured in the Operations and Usage reports, include:

- User Access: CV traces and audits the actions a user executes within the application
- Audit data is provided via audit trails and audit logs that offer a backend view of system use and store user views of patient data
- Interface with jMeadows: jMeadows retains user actions within CV
- Specific events (user transactions) are audited or captured in log files, including but not limited to user ID, date and time of the event, type of event, success or failure of the event, successful login, and the identity of the information system component where the event occurred

Each time an attempt is made to interface with jMeadows, whether it is a service communication or a user searching for a patient, the activity is logged and stored in the CV data store. The purpose of retention is for traceability; specifically, to show which calls/actions were made, where, by whom, and when they terminated. Each CV query for data is audited and has the user ID linked to it.

## **2.5. Routine Updates, Extracts, and Purges**

CV system updates, and other routine actions on systems within the AITC cloud environment, are handled by the CV Support team, as needed.

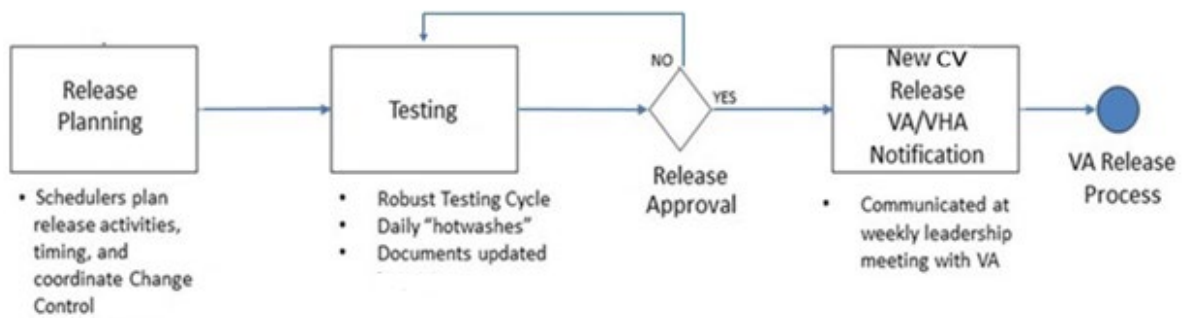
Updates to the CV web application servers within the AITC (non-cloud) environment are performed by AITC personnel.

A detailed list of the servers referenced throughout this POM can be found in IBM Rational Source Control. See [System Startup](#) for the link to the repository.

### **2.5.1. Routine Updates**

Patches and other routine updates follow the CV patching process, shown in [Figure 8](#).

**Figure 8: Patching Process for CV Components**



### **2.5.2. Quarterly Update of the VistA Site List**

The CV Support Team monitors the VistA site list for any changes and updates the DB quarterly.

### **2.5.3. Extracts**

Extracts of the CV audit logs and server logs are available by request only, on an as-needed. The VA Project Manager must approve requests for extracts. Approvals are dependent on the type of request and the organization of the requester. Once a request is approved, an authorized System Administrator extracts the requested data and sends it to the requestor, via an encrypted method. Refer to [Application Error Logs](#) for more information on audit and server logs.

### **2.5.4. Purges**

Neither data, nor audit log entries from the CV DB, nor other system components, are purged.

## **2.6. Scheduled Maintenance**

The Release Manager actively monitors all relevant systems maintenance schedules and follows the scheduled downtime notification process for CV application code-driven patch releases.

A representative from the CV Support team notifies the VA stakeholders and the ESD when the CV system is restored to service.

## **2.7. Capacity Planning**

The CV Support team monitors the performance of CV, the associated servers, user onboarding, and user behavior on a weekly basis. Server resources and CV application data are collected by the AITC Monitoring group, using the CA APM suite.

CA APM monitors and stores data and sends alerts to notify the members of the CV Operations team e-mail distribution group when any metric exceeds its upper or lower boundary. The e-mail distribution group is maintained by the CV Support team.

### **2.7.1. Initial Capacity Plan**

Server processing capacity forecasts and workload modeling is conducted in an ad hoc manner. These forecasts are used to project server capacity based on Production data, CV requirements, and CV application changes planned for future releases.

## **3. Exception Handling**

Like most systems, CV may generate a small set of errors that are considered routine, in the sense that they have minimal impact on users and do not compromise the operational state of the system. Most errors are transient in nature and are resolved by the user trying to execute an operation again. The following subsections describe these errors, their causes, and what, if any, response an operator should take.

### **3.1. Routine Errors**

While the occasional occurrence of errors may be routine, encountering many individual errors over a short period of time is an indication of a more serious problem. In that case, the error must be treated as a significant error. Refer to [Significant Errors](#) for more information.

#### **3.1.1. Security Errors**

A VA Staff user may encounter the login error message, *“Not a valid ACCESS/VERIFY CODE pair,”* if they mistype their VistA Access or Verify code.

CCPs may encounter a login error message if they attempt to access CV when their status is not set to *active* in PPMS: *“There is an issue preventing your access to Community Viewer. Please contact your VA Contractor or VA Medical Center for assistance.”* CCPs may also encounter the error message, *“Username and/or Password is incorrect,”* if they enter an invalid username/password combination.

#### **3.1.2. Login Errors**

A VA Staff user’s login credentials will be locked after five incorrect login attempts by the VistA service to which CV connects. If this occurs, the user contacts the ESD and opens a service request ticket. The user’s local VistA Administrator can unlock their account.

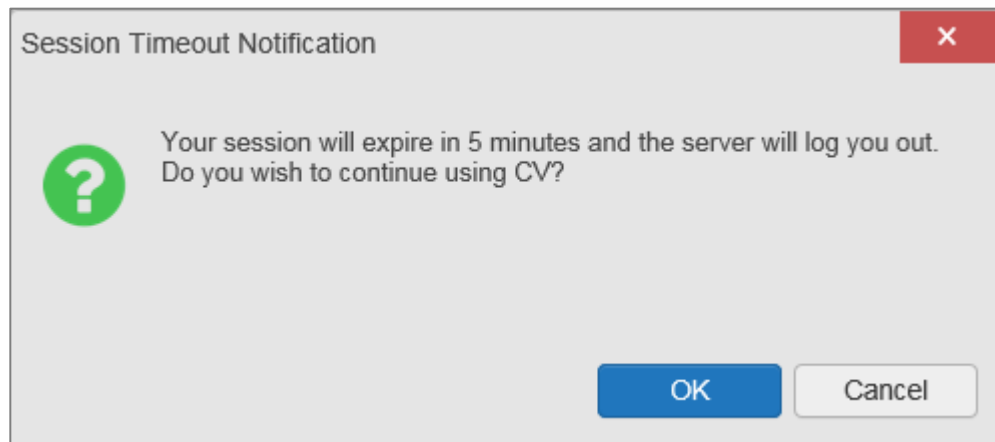
#### **3.1.3. Timeouts**

Each section below describes a possible timeout error.

##### **3.1.3.1. Application Timeout**

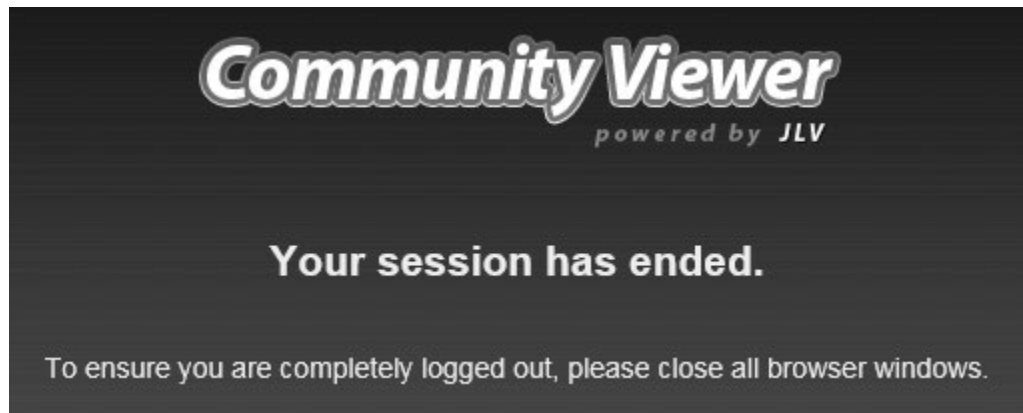
CV has a timeout feature that is set to 30 minutes of inactivity. If users leave the CV application idle for 25 minutes, they receive the Session Timeout Notification ([Figure 9](#)). If the user would like to extend the session, they can click the OK button to continue using CV.

**Figure 9: Session Timeout Notification**



If the user does not interact with the Session Timeout Notification message within the 30-minute time limit, the CV session times out ([Figure 10](#)). The user must then close the browser, reopen the browser, and log back in to CV.

**Figure 10: Session Timeout**
















### **3.1.3.2. Connection Errors**


If users encounter a web browser timeout error or the browser displays, *“This page can’t be displayed,”* when accessing the correct URL, it indicates that CV application services are either not running or there is a network outage.

Either the CV Support team or the active site’s System Administrators may attempt to remote desktop in to each CV application server to ensure the WebLogic services are running. If they are running, System Administrators contact IO to verify that the Local Traffic Manager (LTM) is operating correctly.

CV may also report timeouts to external systems within widgets by displaying a message that one or more data sources could not be connected ([Figure 11](#)).

Figure 11: Connection Error

Allergies (5)       			
	Date Recorded	Allergen	Site
+	Jun 09, 2015	<a href="#">CAFFEINE</a>	 IPO4
+	Feb 16, 2016	<a href="#">CHOCOLATE</a>	 IPO4
+	Oct 26, 2004	<a href="#">ERYTHROMYCIN</a>	 IPO4
+	Jan 26, 2006	<a href="#">NIACIN</a>	 IPO4
+	Jun 09, 2015	<a href="#">PEANUTS</a>	 IPO4
Displaying 1-5 of 5 <a href="#">More &gt;&gt;</a>			

 **NOTE:** Connection errors that persist for more than 5 minutes must be investigated by Tier 3 support.

### 3.1.4. Concurrency

Concurrency is monitored and handled by IO. They optimize the load balancing of the application using an F5 appliance to handle concurrent user sessions.

## 3.2. Significant Errors

Significant errors are defined as errors or conditions that affect the system stability, availability, performance, or otherwise make the system unavailable to its user base. The following subsections contain information to aid administrators, operators, and other support personnel in the resolution of significant errors, conditions, or other issues.

### 3.2.1. Application Error Logs

jMeadows retains user actions in an audit log and stores it in the CV data store. Specific events regarding user transactions are also audited (captured in log files), including but not limited to user ID, date and time of the event, type of event, success or failure of the event, successful and failed login attempts, and the identity of the information system component in which the event occurred.

Each time an attempt is made to interface with jMeadows, whether it is a service communication or a user searching for a patient, the activity is logged and stored in the CV data store. The purpose of retention is for traceability; specifically, to show what calls/actions were made, where, by whom, and when they terminated. Each query for data is audited and has both the user and patient ID linked to it. Only one audit log is produced, and it is included in the overall VM backup.



Query times for each web service call in to jMeadows and VDS are recorded to a file in the /u01/CV\_HOME/logs/ directory on the server, where the services are installed. A log file output for jMeadows Data Service provided in [Figure 12](#). [Table 4](#) lists the response time log locations.

**Table 4: Response Time Log Location**

Data Service	Log File Name
jMeadows Data Service	jmeadows-sql.txt
VDS	vds-sql.txt

**Figure 12: jMeadows Log Output**

```

jmeadows-sql20170206 - Notepad
File Edit Format View Help
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002304.355-0500',
jmeadows.getIehrUserProfile', '1, 1, '
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002304.391-0500',
jmeadows.getAuthUser', '1, 1, '
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002305.485-0500',
jmeadows.getSites', '14, 12, '
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002305.626-0500',
jmeadows.getLoginInfo', '104, 2, '
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002533.132-0500',
jmeadows.getIehrUserProfile', '407, 1, '
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002533.513-0500',
jmeadows.getAuthUser', '2, 1, '
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002615.560-0500',
jmeadows.getIehrUserProfile', '0, 1, '
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002615.607-0500',
jmeadows.getAuthUser', '0, 1, '
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002615.648-0500',
jmeadows.getSites', '0, 12, '
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002615.795-0500',
jmeadows.getLoginInfo', '101, 2, '
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002714.603-0500',
jmeadows.getAuthUser', '1, 1, '
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002714.754-0500',
jmeadows.getLoginInfo', '109, 2, '
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002800.953-0500',
jmeadows.setIehrUserProfile', '2, 0, '
GO
INSERT INTO audit_log (log_date_time, call_type, error_msg, resp_time, doc_count, resp_cached, queryinfo, systemid) VALUES ('20170206002801.087-0500',

```

The QoS service deployed with the CV web application monitors the availability of services that connect to CV data sources and other outside systems. Connection errors within the CV environment are written to the QOS\_LOGS table within the CV DB and displayed in the CV web application.

Service interruptions detected by the QoS service are reported to the CV Support team via e-mail. An automated e-mail notification is sent every 6 hours, unless a status change is detected. Detection of a status change immediately triggers an e-mail notification, and the 6-hour timer is reset. The next e-mail is generated after 6 hours if no further system status changes are detected. The QoS service does not send service interruption notices to external systems or services. Each backend server has its own functional and service-specific application store, for example: /u01/apps/oracle/mwhome/user\_projects/domains/<DOMAIN\_NAME>/servers/<MGD\_SERVE R\_NAME>/logs. Application information and errors are logged to those stores. Error logs are kept indefinitely.

The CV Support team utilizes system notifications generated from the QoS service to diagnose service interruptions and troubleshoot potential issues.

Standard SQL server, WebLogic, Java, Hypertext Markup Language (HTML), and PPMS error codes, generated by the system and recorded in application logs, are used to identify, triage, and resolve complex issues that may arise during system operation.

### **3.2.2. Application Error Codes and Descriptions**

The CV Support team utilizes system notifications generated from the QoS service to diagnose service interruptions and troubleshoot potential issues.

Standard SQL Server, WebLogic, Java, and Hypertext Markup Language (HTML) error codes - generated by the system and recorded in the application logs - are used to identify, triage, and resolve complex issues that may arise during system operation.

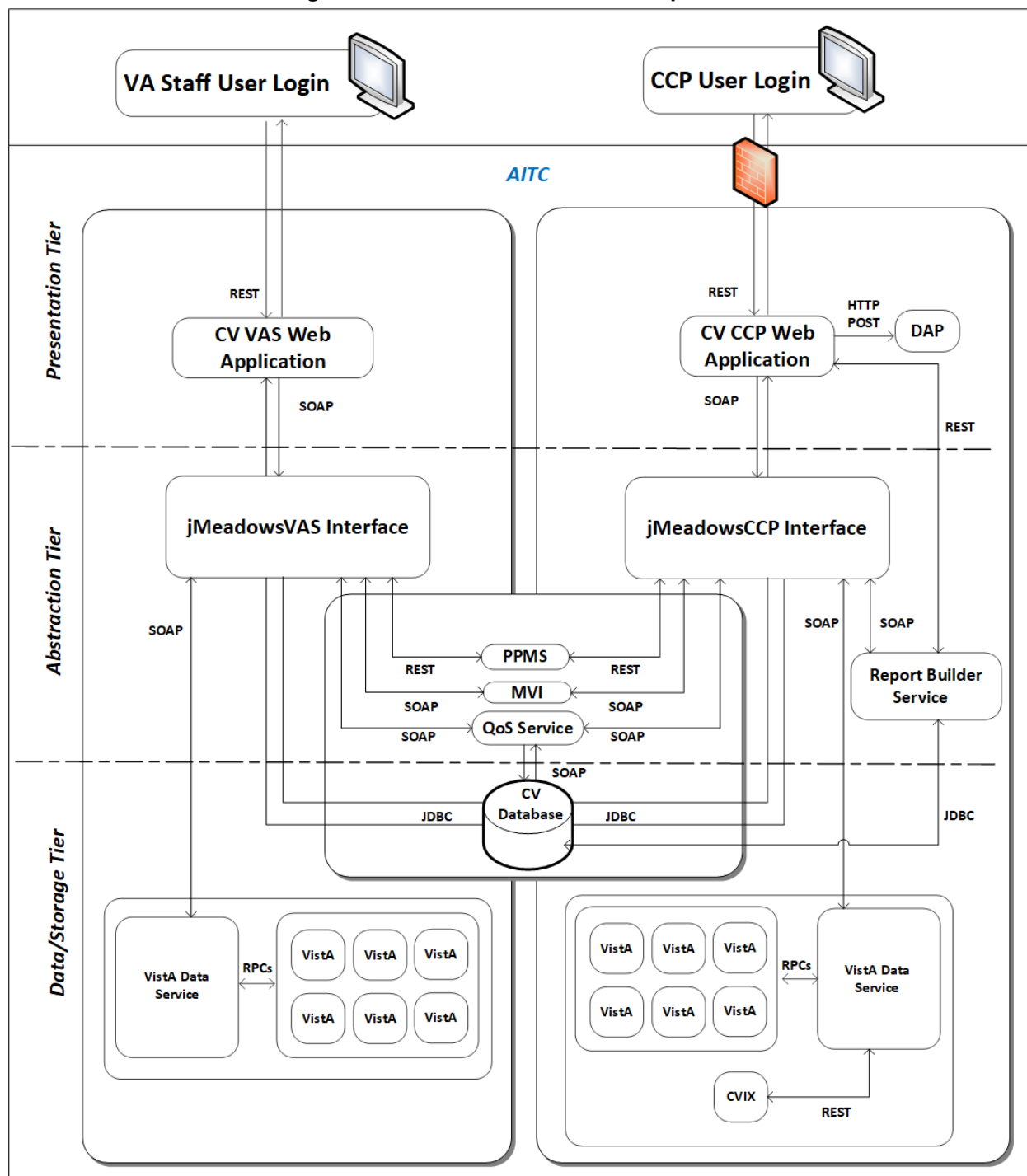
### **3.2.3. Infrastructure Errors**

#### **3.2.3.1. DB**

The CV DB is a relational DB used to store user profile information and audit data. It also stores terminology mappings (both local terminology and national standards). The DB does NOT store, neither long term nor temporarily, patient or provider electronic health records (EHRs) from source systems.

The CV DB sits on a dedicated server within a deployed CV environment, alongside the server hosting the CV application and VDS ([Figure 13](#)). Only the CV application and components of the CV system connect to, and utilize, the CV DB.

Figure 13: CV Architecture and Components



For detailed information about errors and events for the SQL Server DB Engine, please see the website [MS Developer Network Database Engine Events and Errors](https://msdn.microsoft.com/en-us/library/ms365212(v=sql.110).aspx).<sup>5</sup>

<sup>5</sup> [https://msdn.microsoft.com/en-us/library/ms365212\(v=sql.110\).aspx](https://msdn.microsoft.com/en-us/library/ms365212(v=sql.110).aspx)

The CV DB has a table to audit user actions within the application within the AUDIT DB table. This table collects system usage data and provides the CV Support team the ability to create reports and extract pertinent information from the DB, as needed. A sample of the Audit log can be seen in [Figure 14](#).

Figure 14: Audit Log

	auditID	entryDate	startDate	endDate	systemID	userID	userNPI	userName	patID	category	info	queryType	cardID	ipAddress	email	tester	eventID	siteAgency	siteMoniker	complexTransaction
1	362797	2017-07-18 22:46:00	NULL	NULL	200	10000000270	NULL	USER.PANORAMA	0000000003	RadiologyVixViewer		JLV	654321	NULL	dood@mcluvlin.com	NULL	6899798.8451-1	VA	AINA	NULL
2	362798	2017-07-18 22:46:00	NULL	NULL	200	10000000270	NULL	USER.PANORAMA	0000000003	RadiologyVixViewer		JLV	654321	NULL	dood@mcluvlin.com	NULL	6849870.8462-1	VA	AINA	NULL
3	362795	2017-07-18 22:45:00	NULL	NULL	200	10000000270	NULL	USER.PANORAMA	0000000003	login		JLV	654321	0.0.0.0:0.0:0.1	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
4	362786	2017-07-18 22:45:00	NULL	NULL	200	10000000270	NULL	USER.PANORAMA	0000000003	SelectPatientMVI	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	0000000003	NULL	NULL	NULL
5	362787	2017-07-18 22:45:00	NULL	NULL	200	10000000270	NULL	USER.PANORAMA	0000000003	selectPatientForVASensitive	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
6	362788	2017-07-18 22:45:00	NULL	NULL	200	10000000270	NULL	USER.PANORAMA	0000000003	PatDemographics	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
7	362789	2017-07-18 22:45:00	NULL	NULL	200	10000000270	NULL	USER.PANORAMA	0000000003	PatImmunizations	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
8	362790	2017-07-18 22:45:00	2016-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER.PANORAMA	0000000003	PatVitals	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
9	362791	2017-07-18 22:45:00	2017-03-20 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER.PANORAMA	0000000003	PatLabResults	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
10	362792	2017-07-18 22:45:00	2016-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER.PANORAMA	0000000003	PatVitals	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
11	362793	2017-07-18 22:45:00	2016-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER.PANORAMA	0000000003	PatVitals	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
12	362794	2017-07-18 22:45:00	2017-03-20 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER.PANORAMA	0000000003	PatLabResults	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
13	362795	2017-07-18 22:45:00	2000-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER.PANORAMA	0000000003	PatRads	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
14	362796	2017-07-18 22:45:00	NULL	NULL	200	10000000270	NULL	USER.PANORAMA	0000000003	RadiologyVixViewer		JLV	654321	NULL	dood@mcluvlin.com	NULL	6849796.8287-1	VA	AINA	NULL
15	362783	2017-07-18 22:44:00	NULL	NULL	NULL	NULL	NULL	NULL	NULL	getAuthUser		JLV	6254...	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
16	362784	2017-07-18 22:44:00	NULL	NULL	NULL	NULL	NULL	NULL	NULL	getAuthUser		JLV	6254...	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
17	362773	2017-07-18 22:09:00	NULL	NULL	200	10000000270	NULL	USER.PANORAMA	0000000003	SelectPatientMVI	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	0000000003	NULL	NULL	NULL
18	362774	2017-07-18 22:09:00	NULL	NULL	200	10000000270	NULL	USER.PANORAMA	0000000003	selectPatientForVASensitive	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
19	362775	2017-07-18 22:09:00	NULL	NULL	200	10000000270	NULL	USER.PANORAMA	0000000003	PatDemographics	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
20	362776	2017-07-18 22:09:00	NULL	NULL	200	10000000270	NULL	USER.PANORAMA	0000000003	PatImmunizations	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
21	362777	2017-07-18 22:09:00	2016-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER.PANORAMA	0000000003	PatVitals	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
22	362778	2017-07-18 22:09:00	2016-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER.PANORAMA	0000000003	PatVitals	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
23	362779	2017-07-18 22:09:00	2016-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER.PANORAMA	0000000003	PatVitals	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
24	362780	2017-07-18 22:09:00	2017-03-20 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER.PANORAMA	0000000003	PatLabResults	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
25	362781	2017-07-18 22:09:00	2017-03-20 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER.PANORAMA	0000000003	PatLabResults	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
26	362782	2017-07-18 22:09:00	2000-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER.PANORAMA	0000000003	PatRads	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
27	362771	2017-07-18 22:08:00	NULL	NULL	NULL	NULL	NULL	NULL	NULL	authNoDbVerification		JLV	6254...	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
28	362772	2017-07-18 22:08:00	NULL	NULL	200	10000000270	NULL	USER.PANORAMA	0000000003	login		JLV	654321	0.0.0.0:0.0:0.1	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
29	362769	2017-07-18 22:02:00	NULL	NULL	200	10000000270	NULL	USER.PANORAMA	0000000003	RadiologyVixViewer		JLV	654321	NULL	dood@mcluvlin.com	NULL	6849796.8287-1	VA	AINA	NULL
30	362770	2017-07-18 22:02:00	2000-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER.PANORAMA	0000000003	PatRads	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
31	362768	2017-07-18 21:52:00	2000-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER.PANORAMA	0000000003	PatRads	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
32	362757	2017-07-18 21:51:00	NULL	NULL	NULL	NULL	NULL	NULL	NULL	authNoDbVerification		JLV	6254...	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
33	362758	2017-07-18 21:51:00	NULL	NULL	200	10000000270	NULL	USER.PANORAMA	0000000003	login		JLV	654321	0.0.0.0:0.0:0.1	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
34	362759	2017-07-18 21:51:00	NULL	NULL	200	10000000270	NULL	USER.PANORAMA	0000000003	SelectPatientMVI	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	0000000003	NULL	NULL	NULL
35	362760	2017-07-18 21:51:00	NULL	NULL	200	10000000270	NULL	USER.PANORAMA	0000000003	selectPatientForVASensitive	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
36	362761	2017-07-18 21:51:00	NULL	NULL	200	10000000270	NULL	USER.PANORAMA	0000000003	PatDemographics	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
37	362762	2017-07-18 21:51:00	2017-03-20 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER.PANORAMA	0000000003	PatLabResults	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
38	362763	2017-07-18 21:51:00	2017-03-20 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER.PANORAMA	0000000003	PatLabResults	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
39	362764	2017-07-18 21:51:00	2016-07-18 00:00:00	2017-07-18 00:00:00	200	10000000270	NULL	USER.PANORAMA	0000000003	PatVitals	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL
40	362765	2017-07-18 21:51:00	NULL	NULL	200	10000000270	NULL	USER.PANORAMA	0000000003	PatImmunizations	NULL	NULL	654321	NULL	dood@mcluvlin.com	NULL	NULL	NULL	NULL	NULL

### 3.2.3.2. Web Server

CV uses Oracle WebLogic as its web server in the VA environment. CV does not implement any custom WebLogic error handling or reporting. Please refer to the [Oracle WebLogic Server Error Messages Reference](#)<sup>6</sup> for more information.

### 3.2.3.3. Application Server

CV uses Oracle WebLogic as its application server in the VA environment. CV does not implement any custom WebLogic error handling or reporting. Please refer to the [Oracle WebLogic Server Error Messages Reference](#)<sup>6</sup> for more information.

### 3.2.3.4. Network

CV utilizes the network infrastructure provided at AITC. Any network errors that arise are corrected by the team associated with the location of the error.

### 3.2.3.5. Authentication and Authorization (A&A)

User access control and authentication takes place before CV interfaces with jMeadows. The user is authenticated to their user profile, granting them access to the presentation layer. jMeadows retrieves user profile information from the CV DB, based on their credentials.

VA Staff users must provide their VistA Access and Verify codes to log in. If credentials are not found the message, “*Not a valid Access Code/Verify Code pair.*” displays.

If CCP credentials are not found or are inactive in the CV DB, the message, “*There is an issue preventing your access to Community Viewer. Please contact your VA Contractor or your VA Medical Center for assistance.*” displays. In either case, the login process stops for the user, and no further options appear.

Other A&A error messages are:

- Smart Card Required: The user has not inserted their PIV card into the card reader
- ActivClient: The user’s PIV PIN was entered incorrectly
- Missing Code: The user has not entered their Access/Verify code(s)
- Invalid Access Code: The user has entered an incorrect Access/Verify code

[Table 5](#) provides an overview of the authentication sequence for each user.

**Table 5: User Authentication Sequence Overview**

User	Authentication Sequence Overview
VA Staff	<ul style="list-style-type: none"><li>• VA Staff users must provide their PIV and PIN to log in, as well as their VistA Access and Verify codes</li></ul>

<sup>6</sup> [https://docs.oracle.com/cd/E24329\\_01/doc.1211/e26117.pdf](https://docs.oracle.com/cd/E24329_01/doc.1211/e26117.pdf)

User	Authentication Sequence Overview
CCP	<ul style="list-style-type: none"> <li>CCPs are required to use their NPI or the e-mail address associated with their account in the username field, and a password to log in</li> <li>CV validates their e-mail address against the C_Provider table</li> <li>-OR-</li> <li>CV validates their NPI against the PPMS_Provider table</li> <li>jMeadows retrieves information from PPMS, determines if the CCP exists in PPMS, and verifies the CCP has a status of “active” in PPMS</li> </ul>
RM User (Provider)	<ul style="list-style-type: none"> <li>RM users are required to use their e-mail address (username) and a password to log in</li> <li>CV validates their credentials against the C_Provider table</li> </ul>
SDU	<ul style="list-style-type: none"> <li>SDUs must be added to the VAS_UserRole table as authorized users</li> <li>Once authorized, SDUs must provide their PIV and PIN to log in</li> </ul>
RM VA Staff	<ul style="list-style-type: none"> <li>RMPMs must be added to the VAS_UserRole table as authorized users</li> <li>RMPM users must provide their PIV and PIN to log in, as well as their VistA Access and Verify codes</li> <li>UserRole field of VAS_UserRole set to “RMP” provides RM VA Staff access to the RMP Management Widget</li> </ul>

A detailed overview of the login process from the user’s perspective is provided in the *CV 3.1 VA Staff User Guide* and the *CV 3.1 CCP User Guide*. Once approved, all project documentation is available on the Project JLV/CV SharePoint site. See [System Startup](#) for the link to the repository.

### 3.2.3.6. Logical and Physical Descriptions

System design specifications and diagrams can be found in the DE&A Compliance Requirements collection for CV in the IBM Rational Tool Suite. See [Table 2](#) for the link to the collection.

## 3.3. Dependent System(s)

[Table 6](#) lists the external VA systems upon which CV depends, and the errors related to each dependent system.

**Table 6: CV External Dependent Systems**

Other VA System	Related Error(s)
Site VistA instances	If a VistA site is unavailable, CV displays the <i>Connection Unavailable</i> row in the widgets as shown in <a href="#">Connection Errors</a> .
MVI	If MVI is unavailable, CV may display patient search errors or the “ <i>Patient records unavailable</i> ” error message.
PPMS	If PPMS is unavailable, CV displays the “ <i>Failed to retrieve a PPMS response.</i> ” error message.
CVIX	If CVIX is unavailable, CV displays the “ <i>VistA Imaging service is unavailable: Images may not display.</i> ” error message.



### 3.4. Troubleshooting

Tier 1 troubleshooting for VA users is handled through the ESD. The Community Provider Technical Service Desk provides end user support and troubleshooting for CCPs. They can be reached via e-mail ([Community\\_Provider\\_Technical\\_Service\\_Desk@va.gov](mailto:Community_Provider_Technical_Service_Desk@va.gov)).

Tier 2 issues are handled by Health Product Support (HPS).

Tier 3 support and troubleshooting is handled directly by the CV Support team.

### 3.5. System Recovery

The following subsections define the processes and procedures necessary to restore the system to a fully operational state after a service interruption. Each of the subsections starts at a specific system state and ends with a fully operational system.

#### 3.5.1. Restart After Unscheduled System Interruption

The simplest way to bring the system back to normal operation after the crash of a component is to restart the affected server(s). See [System Startup from Emergency Shutdown](#) for guidance.

#### 3.5.2. Restart After DB Restore

Refer to [System Startup](#) for system startup procedures.

#### 3.5.3. Backout Procedures

Backout procedures vary depending on the specific release. Please see the *CV DIBR* specific to the version to be backed out for more information. Once approved, all project documentation is available on the Project JLV/CV SharePoint site. See [System Startup](#) for the link to the repository.

#### 3.5.4. Rollback Procedures

Rollback procedures are dependent on each specific release. Please see the *CV DIBR* specific to the version to be rolled back for more information. Once approved, all project documentation is available on the Project JLV/CV SharePoint site. See [System Startup](#) for the link to the repository.

## 4. Operations and Maintenance Responsibilities

[Table 7](#) represents the operational roles and responsibilities for CV.

**Table 7: Responsibility Matrix (Operational Roles and Responsibilities)**

Name/Organization	Role/Responsibility	Phone Number	E-mail Address
Veterans Health Administration (VHA) Community Support	Tier 1 support for CCPs	N/A	<a href="mailto:vha.communitysupport@va.gov">vha.communitysupport@va.gov</a>
Ronald "JR" Ruble	Business Owner	304-626-5614	<a href="mailto:ronald.ruble@va.gov">ronald.ruble@va.gov</a>



Name/Organization	Role/Responsibility	Phone Number	E-mail Address
<b>VA CV Project Office</b>	<b>Office of Information Technology (OIT) and VHA Stakeholders</b>	<b>N/A</b>	<b>N/A</b>
Colleen Reed	Program Manager (PM)	703-402-8604	colleen.reed@va.gov
Vincent Freeny	CV PM	720-870-5815	vincent.freeny@va.gov
<b>VA Authentication Federation Infrastructure (VAAFI) Data Power</b>	<b>Technical Issues/Support Contacts</b>	<b>N/A</b>	<b>N/A</b>
Basavaraj "Raj" Devershetty	VAAFI Lead	813-842-3432	basavaraj.devershetty@va.gov
Courtney Rive	Deputy PM Single Sign on Internal (SSOi)	757-772-0701	courtney.rive@va.gov
Mayank Acharya	VAAFI	818-804-9928	mayank.acharya@va.gov
<b>IO</b>	<b>Technical Issues/Support Contacts</b>	<b>N/A</b>	<b>N/A</b>
Nellie Garcia	Analyst	512-663-2614	nellie.garcia2@va.gov
Robert Coyle	Analyst	512-638-1266	robert.coyle2@va.gov
Dinesh Punyala	WebLogic / Java Admin	512-638-9296	dinesh.punyala@va.gov
Larry Stanton	Windows Admin	512-696-3050	larry.stanton@va.gov
Eric Erboe	Linux Admin	512-569-9363	eric.erboe@va.gov
<b>MVI (VA)</b>	<b>Technical Issues/Support Contacts</b>	<b>N/A</b>	<b>In VA ServiceNow assigned under: VA—Development—DEV-Person Service VHAISWIAMHELPDESK@va.gov MVITECHLEAD@va.gov</b>
Jason Boire	MVI/VAAFI Lead Developer/Architect	O:503-747-6883 C:240-381-6087	jason.boire@va.gov
Danny Reed	MVI Point of Contact (POC)	205-943-2415	danny.reed@va.gov
Cory Chin	MVI POC	407-593-1963	cory.chin@va.gov
Vicky Steadman	MVI POC	205-943-2381	vicky.steadman@va.gov
Jeff Kemple	SSOi POC	913-707-9037	jeffrey.kemple@va.gov
<b>PPMS</b>	<b>Technical Issues/Support Contact</b>	<b>N/A</b>	<b>N/A</b>
Rashida Franklin	PPMS POC	240-271-5911	rashida.fleming@va.gov

Name/Organization	Role/Responsibility	Phone Number	E-mail Address
<b>VA Network Security Operations Center (NSOC)</b>	<b>Technical Issues/Support Contacts</b>	<b>855-673-4357 Option 6, then 4 304-260-6685</b>	<b>In VA ServiceNow assigned under: VA NSOC Business Partner Extranet (BPE) Operations -OR- Network Support Center (NSC) BPE Operations VANSOCBPEOperations@va.gov</b>
Craig Wasson	Triple-I/VA-NSOC	304-262-5226	craig.wasson@va.gov

## 5. Approval Signatures

Signed: \_\_\_\_\_  
Vince Freeny, Project Manager/Receiving Organization Date

Signed: \_\_\_\_\_  
Rodney J. Laster, Product Owner Date

## A. Acronyms and Abbreviations

[Table 8](#) lists the acronyms and abbreviations used throughout this document and their descriptions.

**Table 8: Acronyms and Abbreviations**

Acronym	Definition
<b>A&amp;A</b>	Authentication and Authorization
<b>AITC</b>	Austin Information Technology Center
<b>API</b>	Application Programming Interface
<b>APM</b>	Application Performance Management
<b>BPE</b>	Business Partner Extranet
<b>BSE</b>	Broker Security Enhancement
<b>CA</b>	Computer Associates
<b>CCP</b>	Community Care Provider
<b>CPU</b>	Central Processing Unit
<b>CV</b>	Community Viewer
<b>CVIX</b>	Central VistA Imaging Exchange
<b>DB</b>	Database
<b>DE&amp;A</b>	Design, Engineering, and Architecture
<b>DIBR</b>	Deployment, Installation, Backout, and Rollback
<b>DWS</b>	Data Web Service
<b>EHR</b>	Electronic Health Record
<b>ESD</b>	Enterprise Service Desk
<b>GB</b>	Gigabyte
<b>GUI</b>	Graphical User Interface
<b>HPS</b>	Health Product Support
<b>HSTS</b>	HTTP Strict Transport Security
<b>HTML</b>	Hypertext Markup Language
<b>HTTP</b>	HyperText Transfer Protocol
<b>IBM</b>	International Business Machines Corporation
<b>ICD</b>	Interface Control Document
<b>ICN</b>	Integration Control Number
<b>ID</b>	Identification
<b>IEN</b>	Internal Entry Number
<b>IO</b>	Infrastructure Operations
<b>JLV</b>	Joint Legacy Viewer
<b>JDBC</b>	Java Database Connectivity
<b>JPEG</b>	Joint Photographic Experts Group
<b>JSON</b>	JavaScript Object Notation
<b>LTM</b>	Local Traffic Manager

<b>Acronym</b>	<b>Definition</b>
<b>MS</b>	Microsoft
<b>MVI</b>	Master Veteran Index
<b>NPI</b>	National Provider Identifier
<b>NSC</b>	Network Support Center
<b>NSOC</b>	Network Security Operations Center
<b>OIT</b>	Office of Information and Technology
<b>PDF</b>	Portable Document Format
<b>PIN</b>	Personal Identification Number
<b>PIV</b>	Personal Identity Verification
<b>PM</b>	Program/Project Manager
<b>POC</b>	Point of Contact
<b>POM</b>	Production Operations Manual
<b>PPMS</b>	Provider Profile Management System
<b>QoS</b>	Quality of Service
<b>RAM</b>	Random Access Memory
<b>REST</b>	Representational State Transfer
<b>RM</b>	Risk Management
<b>RMPM</b>	Risk Management Provider Manager
<b>SOAP</b>	Simple Object Access Protocol
<b>SDU</b>	Service Desk User
<b>SQL</b>	Structured Query Language
<b>SMS</b>	Systems Made Simple
<b>SSMS</b>	SQL Server Management Studio
<b>SSOi</b>	Single Sign on Internal
<b>URL</b>	Uniform Resource Locator
<b>VA</b>	Department of Veterans Affairs
<b>VAAFI</b>	VA Authentication Federation Infrastructure
<b>VAS</b>	VA Staff
<b>VDS</b>	VistA Data Service
<b>VHA</b>	Veterans Health Administration
<b>VI</b>	VistA Imaging
<b>VistA</b>	Veterans Information Systems and Technology Architecture
<b>VM</b>	Virtual Machine