

MAINTENANCE TECHNICAL SUPPORT CENTER
HEADQUARTERS MAINTENANCE OPERATIONS
UNITED STATES POSTAL SERVICE



Maintenance Management Order

SUBJECT: Resolving PIVMS Server Login-Access Problems

DATE: September 7, 2016

NO: MMO-102-16

TO: All PIVMS Sites

FILE CODE: O
swil:mm16095ad

This Maintenance Management Order (MMO) provides detailed information to resolve server login-access issues on the Powered Industrial Vehicle Management System (PIVMS). This bulletin applies to Acronym PIVMS and Class Code AA.

Accessing the PIVMS server from an ACE workstation requires using a remote desktop connection. The procedure for creating and properly configuring the remote desktop connection on a local ACE machine depends on the version of ACE workstation being used.

This bulletin is informational and contains suggested best practices for maintaining proper operation of vehicles. Work accomplished under this bulletin will be performed under local work order procedures.

Direct any questions or comments concerning this bulletin to the MTSC HelpDesk, online at <https://tickets.mtsc.usps.gov/login.php> or call (800) 366-4123.

A handwritten signature in black ink, appearing to read 'Kevin Couch'.

Kevin Couch
Manager
Maintenance Technical Support Center
HQ Maintenance Operations

Attachment: Resolving PIVMS Server Login-Access Problems

ATTACHMENT**RESOLVING PIVMS SERVER LOGIN ACCESS PROBLEMS****NOTE**

This bulletin contains detailed technical information requiring PIVMS trained personnel familiar with working on the PIVMS Server. Due to the nature of the material, this bulletin is not intended for use by personnel who have not completed the proper training.

1.0. INTRODUCTION

Numerous calls have been received regarding problems with one of the following:

- Accessing the site PIVMS server
- Logging into Vision
- Lacking the desired access levels in Vision <or> are not able to access the desired functions while in Vision

In general, access to the PIVMS server consists of two tiers; (1) Logging onto the PIVMS server desktop and (2) starting and logging into the Vision Graphical User Interface. Each of these will be addressed in turn.

2.0. ACCESSING THE LOCAL SITE PIVMS SERVER

Accessing the PIVMS server from an ACE workstation requires using a remote desktop connection. The procedure for creating and properly configuring the remote desktop connection on a local ACE machine depends on the version of ACE workstation being used.

2.1. LOGGING INTO THE VISION GRAPHICAL USER INTERFACE (GUI)

Logging into Vision requires the local PIVSM administrator create an account for the user in Vision Software User Setup.

Upon logging into Vision, the “menu bar” (Figure 1) is displayed on the left side of the screen. The number of options in the menu is directly related to the User Roles granted to the user in Software User Setup.



Figure 1. Vision Menu Bar

NOTE

Accessing the Software User Setup options described in the following sections requires Site Champion or User DB Admin access privileges.

2.1.1 User Roles and Their Relationship to User Access

When a user is added to Vision, the role they are assigned is dependent on the functions they will be expected to perform while working with the PIVMS system.

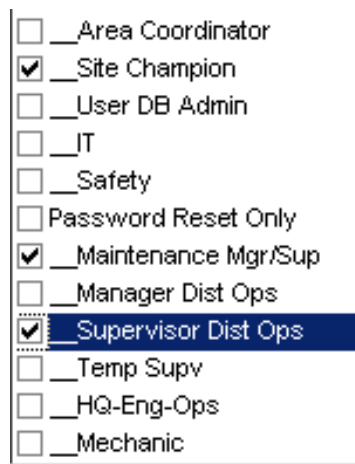
Examples:

- Site Champion Role – Has full access and can perform virtually all functions.

- Maint Mgr/Supv Role – Has almost full access. Can create/manage Reports, Groups, Vehicles, and Operators.
- Mgr Dist Opns Role – Has limited access. Can view System Health Display, create and manage Reports but only view Groups, Vehicles, and Operators in the setup screens.
- Mechanic Role – Has limited access. Can create and manage Reports but only view Groups, Vehicles, and Operators in the setup screens.
- The role selected for the user controls which of the various menu buttons appear in the menu bar.

2.1.1.1 Role Conflicts and Restricted User Access

With the installation of the latest version of Vision the way roles are handled have changed significantly. Figure 2 shows a list of currently available roles. Note the user has more than one role selected from the list. **Having more than one role selected will cause access problems for the user.** This will be further explained in the following section.



A screenshot of a user role selection interface. It features a vertical list of roles, each preceded by a checkbox. The roles are: __Area Coordinator, __Site Champion, __User DB Admin, __IT, __Safety, Password Reset Only, __Maintenance Mgr/Sup, __Manager Dist Ops, __Supervisor Dist Ops, __Temp Supv, __HQ-Eng-Ops, and __Mechanic. The checkboxes for __Site Champion, __Maintenance Mgr/Sup, and __Supervisor Dist Ops are checked. The __Supervisor Dist Ops row is highlighted with a blue background.

<input type="checkbox"/>	__Area Coordinator
<input checked="" type="checkbox"/>	__Site Champion
<input type="checkbox"/>	__User DB Admin
<input type="checkbox"/>	__IT
<input type="checkbox"/>	__Safety
<input type="checkbox"/>	Password Reset Only
<input checked="" type="checkbox"/>	__Maintenance Mgr/Sup
<input type="checkbox"/>	__Manager Dist Ops
<input checked="" type="checkbox"/>	__Supervisor Dist Ops
<input type="checkbox"/>	__Temp Supv
<input type="checkbox"/>	__HQ-Eng-Ops
<input type="checkbox"/>	__Mechanic

Figure 2. User Roles

2.1.1.1.1 Changes How PIVMS User Roles Function

In software versions, prior to version 6.8.1, the PIVMS System Administrator would normally select more than one role for a user to expand the access capabilities of that particular user.

Prior to Version 6.8.1 multiple roles selected for a user were “additive”, meaning that the roles combined, and the user had a combination of access rights taken from all the selected roles as a whole.

Example: If a user was assigned Maintenance and Supervisor roles, the user is granted access to all the functions previously accessible by either the Maintenance User or the Supervisor.

In Version 6.81 and later, the roles are now “subtractive”. This means if a user is assigned to both Maintenance and Supervisor roles, this creates a “role conflict” and any access function accessible by both roles is NOT accessible by the user.

NOTE

For the reasons listed above, it is imperative that the PIVMS system administrator at every PIVMS site review the accounts for every user in Vision Software User Setup and make sure no more than ONE role is selected for a particular user.

Example: If a user was assigned two or more roles that include the ability to Manage Reports, the ability to Manage Reports is lost to this user.

2.1.1.1.2 Obtaining a List of Users and Their Access Roles For The Local System

An Access Control Detail Report listing of all the Software users in the system and their assigned roles is available. This report shows detailed information about each user, the roles assigned to that user, and the database being used. This report can be critical in determining if access role and database are assigned properly to all users. The same information shown by the Access Control report can be obtained by going into Software User Setup and reviewing each listed user one at a time.

NOTE

Due to site access restrictions set up by ID Systems, the report can only be run by someone at Engineering, MTSC, or NCED. To obtain a copy of the report, open a ticket at the MTSC Helpdesk requesting an Access Control Detail report for your PIVMS system.

2.1.1.1.3 Description of the Access Control Detail Report

Figure 3 is an example of an Access Control Detail report. This report highlights a number of very important issues.

1. User is assigned to multiple User Roles and multiple databases (sources). Users must always be assigned to one User Role in the Production database ONLY and must NEVER be assigned to User Control. Assigning users to the User Control database can result in a corrupted database.
2. User is assigned to NON-Underlined roles. Non-Underlined roles are scheduled to be removed and should not be used.
3. Properly assigned user. Assigned to only one role and using the Production database.

PIVMS Reporting
Audit Reports Report: Access Control Detail
11/14/2013 12:00:00 AM to 11/15/2013 12:00:00 AM

Last Name	First Name	Login Name	Active	Role Name	Source Name
test	student	Student1	Yes	<u>Manager Dist Ops</u>	NCED Production
test	student	Student1	Yes	<u>NCED Training</u>	NCED Production
test	student	Student1	Yes	<u>Site Champion</u>	NCED Production
test	student	Student1	Yes	<u>Supervisor</u>	NCED User Control
test	student	Student1	Yes	<u>System Settings Admin</u>	NCED User Control
Test	Student	Student10	No	<u>Manager Dist Ops</u>	NCED Production
test	student	Student10	Yes	(AO) Access Ctrl V	NCED User Control
test	student	Student10	Yes	(AO) Access Ctrl V/U/A	NCED User Control
test	student	Student10	Yes	(AO) Manage Floorplan	NCED User Control
test	student	Student12	Yes	<u>IT</u>	NCED Production
test	student	Student12	Yes	<u>Mechanic</u>	NCED Production
test	student	Student12	Yes	<u>Safety</u>	NCED Production
Test	Student	Student13	Yes	<u>Area Coordinator</u>	NCED Production
Test	Student	Student13	Yes	<u>Manager Dist Ops</u>	NCED Production
Test	Student	Student13	Yes	<u>Report Writer Only</u>	NCED Production
test3	student	Student3	Yes	<u>Manager Dist Ops</u>	NCED Production
Test	Student	Student4	No	<u>Manager Dist Ops</u>	NCED Production
test5	student	Student5	Yes	<u>Manager Dist Ops</u>	NCED Production
test	student	Student6	Yes	<u>Manager Dist Ops</u>	NCED Production
Test	Student	Student7	Yes	<u>Manager Dist Ops</u>	NCED Production
Test	Student	Student8	Yes	<u>Manager Dist Ops</u>	NCED Production
Test	Student	Student9	Yes	<u>Manager Dist Ops</u>	NCED Production

Annotations:

- Underline Roles:** Points to underlined role names (e.g., Manager Dist Ops, NCED Training, Site Champion, Supervisor, System Settings Admin, Manager Dist Ops).
- Non-Underline Role:** Points to non-underlined role names (e.g., (AO) Access Ctrl V, (AO) Access Ctrl V/U/A, (AO) Manage Floorplan).
- User Roles (Sources):** Points to Source Name column entries (e.g., NCED Production, NCED User Control).
- Properly Assigned User:** Points to the row for test5, student, Student5, Yes, Manager Dist Ops, NCED Production.

Figure 3. Access Control PIVMS Reporting

2.1.1.1.4 Role Selections in Software User Setup

Figure 4 illustrates the various issues regarding Role Selections.

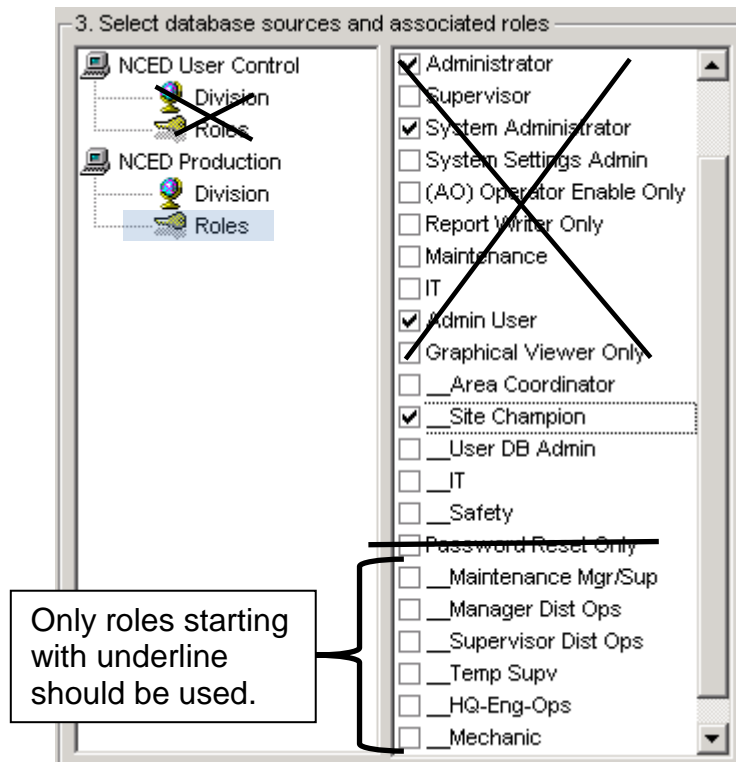


Figure 4. Role Selections

- The User Control database section has a X superimposed, indicating that roles/options for that database should never be used.
- All role selections must be made using the Production database as highlighted.
- Multiple Roles have been selected which will cause access problems. Only ONE role should ever be selected.
- **The roles with a beginning underline (i.e. _Site Champion) are the only roles that should be used.** Roles that do not start with an underline will be removed in a future software release. If a user has a non-underline role assigned, they will lose access when that role is removed from Vision.