VMX300
VIDEO MANAGEMENT SYSTEM

Server Configuration Manual

C1553M-B (4/05)

Contents

List of Illustrations

List of Tables

Introduction

The Pelco VMX300(-E) Video Management System uses a Windows®-based interface to control any combination of analog and IP devices in a single integrated video security system. With a mouse, you can click a camera icon on a system map and then drag it to a video display window. Mapping configurations and a visual interface allow you to easily control the following devices:

- Matrix switchers (CM6700, CM6800, CM9740, CM9760, CM9770, CM9780)
- PelcoNet™ MPEG Series transmission systems (NET300 Series, NET350 Series, NET4001A)
- DX8000 and DX9000 Series digital video recorders (DVRs) and NVR300 network video recorders (DX8000 software version level 1.1.00.1121 only)
- Spectra® and Esprit® camera positioning systems
- CM9760-ALM and CM9760-REL input/output devices

VMX300 provides control and monitoring of CCTV equipment in a client-to-server configuration. VMX300-E provides control and monitoring of CCTV equipment in the following configurations: client-to-server; multiple clients-to-server; or server-to-server.

Each VMX300(-E) system must have at least one workstation with server software. Workstations with server software always include client software and, therefore, are called client/server workstations. A VMX300 system can have only one client/server workstation. A VMX300-E system can have multiple client/server workstations.

Each VMX300(-E) system must have at least one workstation with client software. This can be the client/server workstation, described above, or you can add a separate workstation with only client software to the system. Each VMX300(-E) system can have multiple client workstations in addition to the client/server workstation.

The system administrator configures the system using the VMX300(-E) server software, and then launches the VMX300(-E) server into "run" mode. A system operator uses the VMX300(-E) client software to view and control the area under surveillance. The operator can connect to the VMX300(-E) system from the client/server workstation, or from a separate client workstation. With the VMX300-E version, an operator could also connect from another client/server workstation.

DOCUMENTATION RESOURCES

This manual is for system administrators responsible for configuring and maintaining VMX300(-E) servers.

Instructions on configuring the server and operating the system are also provided in the manual titled Software Guide: Basic Configuration and Operation. More comprehensive information on operating the VMX300(-E) system is provided in the VMX300(-E) Client Operation Manual.

For hardware installation instructions, refer to the VMX300(-E) Installation Quick Start Guide and the VMX300(-E) Installation Manual.

Configuring a New System

When configuring a new VMX300(-E) system, it is recommended that you start with a minimal configuration that allows you to test core system functionality, such as viewing video and controlling devices. Once this is working, build on the minimal configuration by adding users and user groups, workspaces, maps, archive servers, automation, and whatever other customization you want.

SET UP THE MINIMAL CONFIGURATION

This section outlines how to configure a single server with a minimal configuration. If your system has more than one server, repeat these steps for each server. Each server must have its own base license.

Perform the following steps in the given order:

1. **Log on and configure network settings**
2. **Start server:** Run the server from the Windows Start menu, or double-click the VMX300(-E) icon on the Windows desktop, if there is one.
3. **Enter base license:** When asked whether you want to enter a base license, click Yes. Follow the instructions in *License Manager*.
4. **Create database:** When prompted to create or restore the server database, click Create.
5. **Log in to configuration mode:** Use the predefined administrator account (user name: **administrator**, password: **2899100**) to log in to configuration mode. Refer to *Starting and Stopping the Server - Launch the Server* for instructions.
6. **Add clients:** Add each computer that will log in to the server. Refer to *Clients, Custom Windows, and Canvases - Clients* for instructions.
7. **Add windows:** For each client, add the custom windows the client will have access to. Refer to *Clients, Custom Windows, and Canvases - Custom Windows* for instructions.
8. **Add canvases:** For each custom window, add the canvases required to view video. Refer to *Clients, Custom Windows, and Canvases - Canvases* for instructions.
9. **Start device drivers:** Start each device driver needed to control a device in your system. Create a database for each driver when prompted. Refer to *Starting and Stopping Device Drivers* for instructions.
10. **Add device drivers:** Add each device driver that you started. Add as many drivers as you can using the Autodiscover feature. If the autodiscover feature missed any drivers, add them using the Add feature. Refer to *Device Drivers* for instructions.
11. **Add devices:** Add each device in the system to the appropriate device driver. Refer to *Devices* for instructions.
12. **Define connections:** Add connections to reflect the analog connections between devices. Refer to *Connections* for instructions.
13. **Backup the database:** Use the Backup utility to create a backup of the server database. Refer to *Database Utilities* for instructions.
14. **Exit configuration and run server:** Select File > Exit and Run. You will be asked whether you want to save the changes you made to the configuration. Click Yes.

TIP: If you are adding a number of similar custom windows to the same or different clients, configure the window once, then copy and paste it as needed. The canvases defined for the window will be copied with the window.

TEST THE MINIMAL CONFIGURATION

Testing the minimal configuration ensures that the devices in your system are connected and configured correctly and custom windows are configured correctly.

To test the minimal configuration:

1. **Start client:** Start the client on any workstation that you added as a client. Select the VMX300(-E) client from the Windows Start menu, or double-click the VMX300(-E) client icon on the desktop, it there is one.
2. **Configure server:** Click the Servers button at the bottom of the Client Login dialog box. Click Discover All to autodiscover servers. Select the server and Set as Home Server. Refer to *Configuring Servers* in the VMX300(-E) Client Operation Manual for more information.
3. **Log in:** Use the predefined user account (user name: user; no password) to log in to the client. Refer to *Logging In When the Client Is Not Already Running* in the VMX300(-E) Client Operation Manual for more information.
4. **Build workspace:** When asked whether you want the system to build a workspace for you, click Yes.
5. **Test devices:** Drag a PTZ camera from the Device List to a custom window with the appropriate type of canvas to make sure you can view video from the camera. Right-click the camera in the Device List, and then select Show Control Dialog to open the camera's Device Control. Test controlling the camera. Repeat this for all the cameras that are configured.

   Test the other devices in the Device List. How you test each device will depend on the type of device. Refer to *Devices* in the VMX300(-E) Client Operation Manual for more information.
6. **Evaluate the CPU workload:** It is recommended that you monitor the CPU workload under a variety of system conditions while testing your system configuration. If your system frequently exceeds 85% CPU usage, you may experience system performance problems. The following factors can contribute to a high CPU workload:
   - The number of custom windows that an operator is using at one time to view digital video streams
   - The quality, bit rate, and type of digital video streams
   - The file size of a map that an operator is viewing
   - The size of device icons and alarm/event icons on maps
   - The size and function of hotlinks on maps
   - Whether a device icon or alarm/event icon is flashing to indicate an alarm state

To monitor the CPU workload, you can use either the VMX300(-E) Session Manager in the client application or the Windows Task Manager.

Using the Windows Task Manager to Evaluate CPU Workload

Open the Windows Task Manager, and then click the Performance tab. The CPU Usage portion of the window displays the current workload level.

You can also click on the Processes tab to see which programs are using which percentage of the CPU.

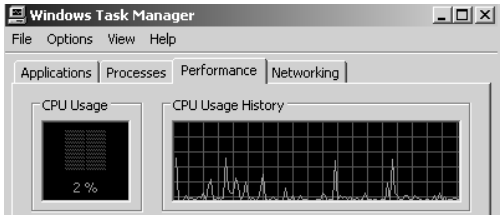


Figure 1. Windows Task Manager

Using the Session Manager to Evaluate CPU Workload

The rectangle at the right end of the Session Manager tool bar in the client application represents the CPU usage of the workstation you are logged in to. As usage increases, the rectangle fills with color from the bottom. Position the pointer over the rectangle to see a dynamic numeric readout of the CPU usage percentage.

Figure 2. Session Manager Tool Bar

Log On and Configure Operating System Settings

⚠ **CAUTION:** Contact your network administrator to assist you in configuring the network features of the VMX300(-E) workstation.

1. Connect the VMX300(-E) workstation power cord to the workstation power input and then to an uninterruptible power supply (UPS).
2. On the front panel of the workstation, press the power button to power on the unit.
3. The VMX300(-E) boots, and then the Microsoft® Windows log on dialog box appears.
4. Log on to the Windows desktop with the following user name and password:

   User Name: AvUser

   Password: 1234
5. Click OK. The Windows XP desktop appears.
6. Configure the operating system settings, as described in the following sections.
7. Repeat steps 1-6 for each VMX300(-E) workstation in your system.

CONFIGURE OPERATING SYSTEM SETTINGS

Before starting the VMX300(-E), you must configure the following operating system settings; instructions for the first three tasks are provided in the subsequent sections. If you are using a DX8000 Series DVR, refer to the DX8000 Installation manual for instructions on disabling the IPSec security services.

- Assign the VMX300(-E) IP address to the workstation.
- Identify the VMX300(-E) workstation on the network.
- If you are not using a DX9000 Series DVR, disable the NetBIOS service in the Windows operating system.
- If you are using a DX8000 Series DVR, disable the IPSec security services in all DX8000 Series DVR units (including any remote DX8000 Client units).

A NOTE ON WINDOWS XPSP2 SETTINGS: The VMX300(-E) workstation is configured with Windows XP and the XP Service Pack 2 (XPSP2). Note, however, that the XPSP2 firewall protection and automatic update features are turned off by default in the VMX300(-E) workstation. To enable these features for your VMX300(-E) system refer to the Windows XP Service Pack 2 instructions available on the Microsoft web site (www.microsoft.com).

ASSIGN AN IP ADDRESS TO THE VMX300(-E) WORKSTATION

⚠ **CAUTION:** Each device driver and device added to the VMX300(-E) system is identified with the VMX300(-E) server IP address. Therefore, it is essential to assign the VMX300(-E) IP address before continuing with the VMX300(-E) configuration.

1. Click Start > Settings > Network Connections. The Network Connections window appears.
2. Right-click Local Area Connection, and then select Properties from the pop-up menu.

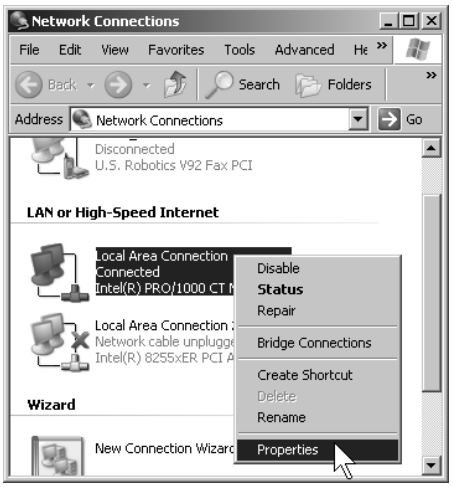


Figure 3. Opening the Local Area Connection Properties Dialog Box

3. In the Local Area Connection Properties dialog box, double-click the Internet Protocol (TCP/IP) listing. The Internet Protocol (TCP/IP) Properties dialog box appears.

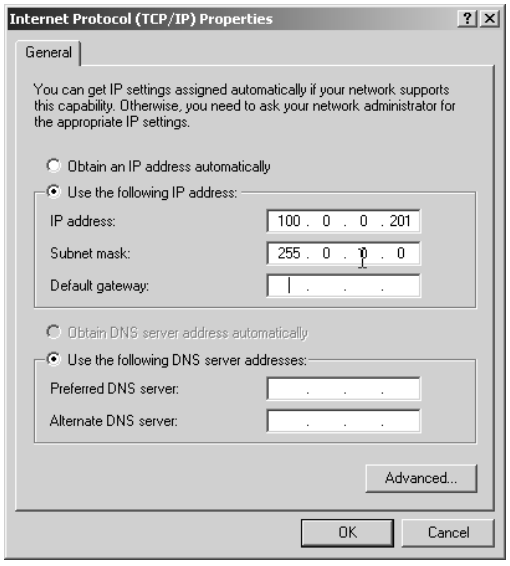


Figure 4. Internet Protocol (TCP/IP) Properties Dialog Box

By default, the properties are set to "Obtain an IP address automatically" and "Obtain DNS server address automatically."

4. Click "Use the following IP address," and then complete the following steps:

   a. Enter the IP address of the VMX300(-E) workstation.

   b. Enter the subnet mask address.

   c. If applicable, enter the default gateway address, and the preferred and alternate DNS server addresses; otherwise, skip this step and proceed to step 5.

NOTE: You must assign a unique IP address to each VMX300(-E) workstation in your system.

5. Click OK to close the Internet Protocol (TCP/IP) Properties dialog box, and then click OK to close the Local Area Connection Properties dialog box.

6. Close the Network Connections window by clicking the X in the upper right-hand corner of the window.

IDENTIFY THE VMX300(-E) WORKSTATION ON THE NETWORK

This procedure includes assigning a unique computer name to the VMX300(-E) workstation and then assigning the VMX300(-E) workstation to a workgroup or a domain. If these steps are not applicable in your system, skip this procedure. Note that if you are using a DX9000 Series DVR in your system, you must assign the VMX300(-E) to the appropriate DX9000 workgroup.

To identify the VMX300(-E) on the network, complete the following steps:

1. On the Windows XP desktop, right-click the My Computer icon, and then click Properties. The System Properties dialog box appears.
2. Click the Computer Name tab, and then click Change. The Computer Name Changes dialog box appears.

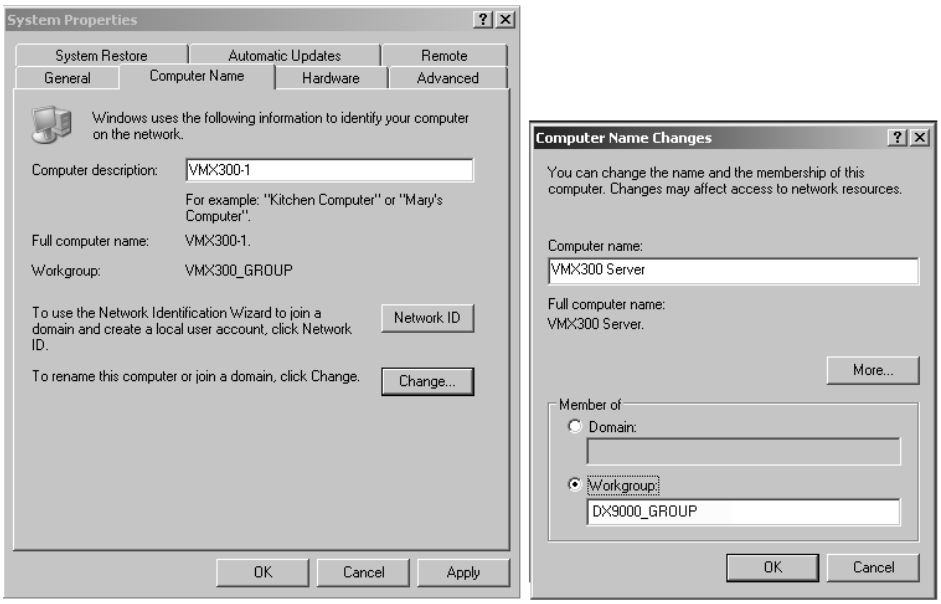


Figure 5. Identify the VMX300(-E) Workstation on the Network

3. In the "Computer name" field type the new name.
4. (Optional) Assign the VMX300(-E) to be a member of a workgroup or a domain:

   To assign the VMX300(-E) to a workgroup enter the workgroup name in the Workgroup field.

   To assign the VMX300(-E) to a domain click Domain, and then enter the domain name. Click OK, and then enter the user name and password in the Domain Username and Password dialog box.
5. Click OK. The Computer Name Changes message appears indicating that the VMX300(-E) has been assigned to the specified workgroup or domain.
6. Click OK. The restart message appears.
7. Click OK, close all windows, and then restart the VMX300(-E) workstation.

DISABLE NETBIOS

A workstation running the NetBIOS service on a network can be vulnerable to attack from outside sources. If you are not using a DX9000 Series DVR, you should complete the following steps to disable the NetBIOS service in the Windows operating system. Note, however, that you should contact your network administrator before changing any NetBIOS settings.

⚠ **CAUTION:** The NetBIOS service is required for the DX9000. Do not complete this procedure if you are using a DX9000 Series DVR or if any other applications in your system require the NetBIOS service. You should follow proper security measures to limit the network's exposure to potential threats when the NetBIOS service is enabled.

To disable NetBIOS, complete the following tasks; instructions are provided in the following sections:

- Disable the NetBIOS setting in the Advanced TCP/IP Settings dialog box.
- Disable the NetBIOS Helper in the Services window.

After completing these tasks, restart the workstation.

Disable NetBIOS in the Advanced TCP/IP Settings Dialog Box

1. Click Start > Settings > Network Connections. The Network Connections window appears.
2. Right-click Local Area Connection, and then select Properties from the pop-up menu.
3. In the Local Area Connection Properties dialog box, double-click the Internet Protocol (TCP/IP) listing. The Internet Protocol (TCP/IP) Properties dialog box appears (refer to Figure 4).
4. Click Advanced. The Advanced TCP/IP Settings dialog box appears.

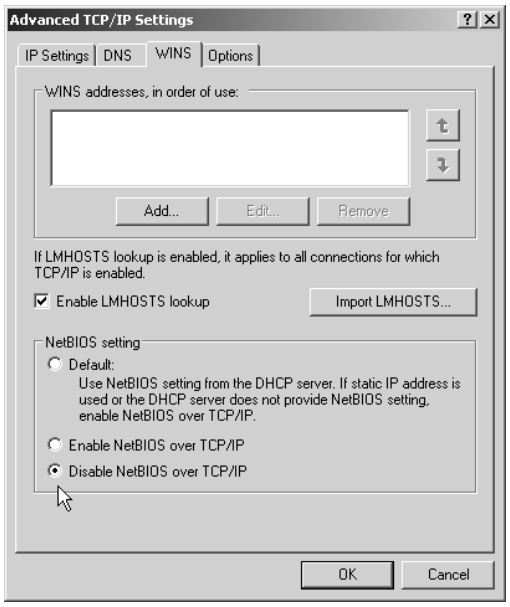


Figure 6. Advanced TCP/IP Settings Dialog Box–WINS Page

5. Click the WINS tab, and then click "Disable NetBIOS over TCP/IP."
6. Click OK.
7. Click No in any messages regarding bindings (you do not need any bindings).
8. Click Yes in any additional messages that appear, and then click OK to close the remaining open dialog boxes.
9. Continue with the steps described in the next section to disable the NetBIOS Helper service.

Disable the NetBIOS Helper Service

1. Click the Windows Start button, and then select Settings > Control Panel > Administrative Tools > Services. The Services window appears.

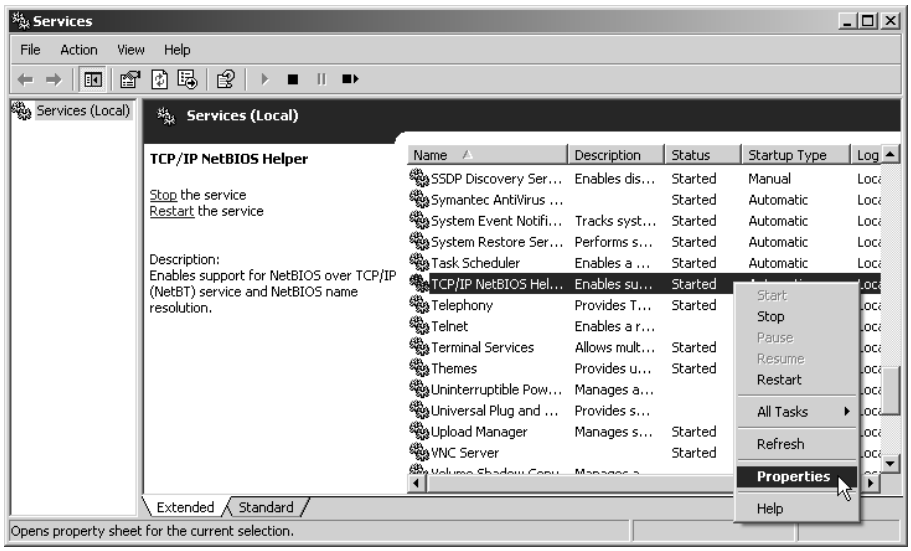


Figure 7. Windows Operating System Services Window

2. Right-click the service named TCP/IP NetBIOS Helper, and then click Properties. The TCP/IP NetBIOS Helper Properties dialog box appears.

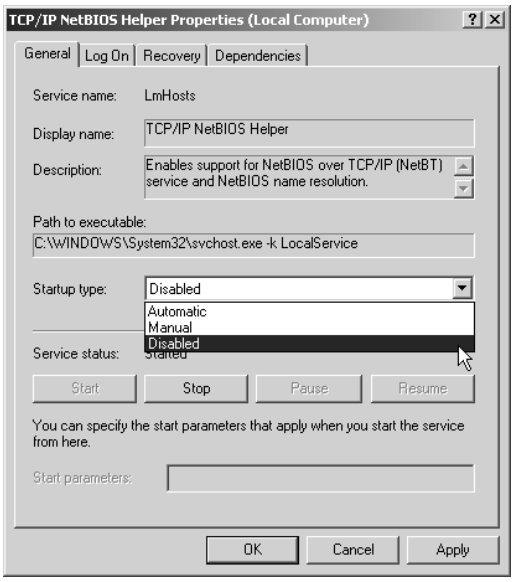


Figure 8. TCP/IP NetBIOS Helper Properties Dialog Box

3. Click the down arrow in the "Startup type" drop-down box, and then click Disabled.

4. Click OK, close all windows, and then restart the VMX300(-E) workstation.

Starting and Stopping the Server

The VMX300(-E) server can be launched in run mode or configuration mode. Configuration mode has a user interface that allows you to configure any type of object, including the following objects:

- Users
- Maps
- Devices
- Scripts
- Alarms and events

To launch the VMX300(-E) server in configuration mode, a user must have permission to configure the software. Refer to *User Groups - Group Permissions* for more information.

Run mode has no user interface. When the VMX300(-E) server is in run mode, the server application is moved to the Windows system tray, where it continues to run in the background. The server must be in run mode for clients to connect to it.

Run mode has a pop-up menu that is opened by right-clicking the VMX300(-E) icon in the Windows system tray. The menu has the options listed in Table A.

Table A. Options for Run Mode

MENU OPTION	SECTION OF MANUAL
Configure	*Configure the Server While It Is Running*
Current Status	*Scripts and Expressions - Variables and Values*
Exit	*Shut Down the Server*

TIP: You can log in and out of configuration mode while the server is running. This allows you to perform administrative tasks without preventing operators from working in the VMX300(-E) client. Refer to *Configure the Server While It Is Running* for instructions.

Save configuration: When you change the server configuration, most changes do not come into effect until after the configuration has been saved. Only changes to device drivers and devices come into effect immediately, with the exception of a device's local settings, which come into effect after the configuration is saved. Refer to *Device Settings - Edit a Device's Local Settings* for information on local settings.

To save the server configuration, select File > Save or exit configuration mode and say Yes when asked whether you want to save the configuration. The server will verify that all scripts and expressions are valid before saving. Operators logged in to the VMX300(-E) client will be momentarily interrupted while the configuration is being saved. After the interruption, operators will see the new configuration.

If one or more scripts or expressions contain errors, the server displays an error message and gives you the opportunity to make corrections. Refer to *Scripts and Expressions - Syntax Error-Checking* for instructions on using the Scripts and Expressions Verification tools to make corrections.

Scripts and expressions are also verified when you launch the server. If there are any errors, you do not have the option to launch the server in run mode. You are automatically presented with the login dialog box for configuration mode.

NOTE: The server will not save changes to the configuration if there are any errors. If you do not correct the errors before exiting, all the changes you made to the configuration will be lost, except for changes to device drivers and devices.

LAUNCH THE SERVER

NOTES:

- If this is the first time you have launched the server, or if your base license has expired, you must enter a base license before proceeding with the configuration. Click Yes when asked whether you want to enter a base license. The License Manager will open. Follow the instructions in *License Manager - Add a License*.
- If the server configuration has more devices or clients than your licensing allows, possibly because an upgrade license has expired, VMX300(-E) will warn you and present you with the login dialog box for configuration mode. If desired, log in to configuration mode and delete devices and clients until you are within the allowable limit, or contact Pelco to obtain additional licenses.

To start the server:

1. Run the VMX300(-E) application from the Windows Start menu, or double-click the VMX300(-E) icon on the Windows desktop if there is one.

   If this is the first time you are launching the server, the Corrupt or Missing Database message appears because VMX300(-E) must create a new database the first time you use it. Click Create.

   If this is not the first time you are launching the server, and the Corrupt or Missing Database message appears, then the server database is corrupted or missing. If this is the case you need to restore a backup or create a new database. Creating a new server database destroys the existing server database if there is one. For information on restoring a backup, refer to *Database Utilities*.

   Once a valid database is in place, the VMX300(-E) start-up screen will open. The start-up screen has a timer that counts down from 15 seconds.

2. **Mode:**

   a. **Run mode:** To launch the server in run mode, click Run, or let the timer count down to zero. The VMX300(-E) icon appears in the Windows system tray, indicating that the server is running.

   b. **Configuration mode:** To launch the server in configuration mode, click Configure before the counter reaches zero. The Server Login dialog box opens.

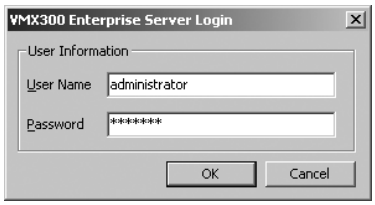


Figure 9. Server Login Dialog Box

   c. Type your user name and password. If this is the first time the server has been launched, use the predefined administrator account (user name: administrator, password: 2899100) supplied with the system.

      User names are not case sensitive. For example, *Administrator* and *ADMINISTRATOR* are equivalent to *administrator*.

      Passwords are case sensitive. For example, *Password* and *PASSWORD* are not equivalent to *password*.

   d. Click OK. The Configuration window opens after several seconds.

      Note that VMX300 synchronizes the device drivers each time you launch the server configuration. You can skip this process by clicking Skip in the Synchronizing Drivers dialog box.

TIP: For security reasons, it is recommended that you change the password for the built-in user administrator account the first time you log in.

CONFIGURE THE SERVER WHILE IT IS RUNNING

You can log in and out of configuration mode while the server is running. This allows you to perform administrative tasks without preventing operators from working in the VMX300(-E) client. When the server is in run mode, perform the following steps:

1. Double-click the VMX300(-E) icon in the Windows system tray, or right-click the icon and select Configure from the pop-up menu. The Server Login dialog box opens.

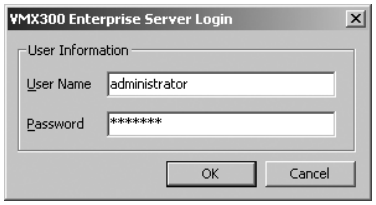


Figure 10. Server Login Dialog Box

2. **User name:** Type your user name. User names are not case sensitive. For example, **Bob** and **BOB** are equivalent to **bob**.
3. **Password:** Type your password. Passwords are case sensitive. For example, **Admin1** and **ADMIN1** are not equivalent to **admin1**.
4. Click OK. After several seconds, the Configuration window opens.
5. Make whatever changes you want to the server configuration.
6. **Save changes:** If you made changes to the server configuration, select File > Save to save your changes. The server verifies your changes. If one or more scripts or expressions contain errors, the server displays an error message and gives you the opportunity to make corrections. Refer to *Scripts and Expressions - Syntax Error-Checking* for instructions on using the Scripts and Expressions Verification tools to make corrections.
7. **Exit configuration mode:** Click File > Close or click the Close button at the right of the Configuration window title bar.

   If you made changes to the configuration that have not been saved, the server asks whether you want to save your changes. Click Yes to save your changes. The server verifies your changes. Make corrections as needed.

   Once there are no errors, the Configuration window closes, momentarily interrupting operators logged in to the client. The server continues to run.

NOTE: You must exit server configuration mode to make changes to the configuration come into effect. The exception to this is changes to device drivers and devices, which come into effect immediately.

LOG OUT OF CONFIGURATION MODE AND LAUNCH RUN MODE

To put the server in run mode from configuration mode:

1. **Save changes:** If you made changes to the server configuration, select File > Save to save your changes. The server verifies your changes. If one or more scripts or expressions contain errors, the server displays an error message and gives you the opportunity to make corrections. Refer to *Scripts and Expressions - Syntax Error-Checking* for instructions on using the Scripts and Expressions Verification tools to make corrections.
2. **Exit configuration mode:** Click File > Exit and Run.

   If you made changes to the configuration that have not been saved, the server asks whether you want to save your changes. Click Yes to save your changes. The server verifies your changes. Make corrections as needed.

   Once there are no errors, the Configuration window closes and the server launches. When the server is running, the VMX300(-E) icon appears in the Windows system tray.

SHUT DOWN THE SERVER

SHUTTING DOWN WHILE IN RUN MODE

1. Right-click the VMX300 icon in the Windows system tray, and then select Exit from the pop-up menu.

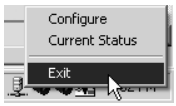


Figure 11. Run Mode Pop-up Menu

2. The shutdown prompt appears.
3. Click Yes. The server shuts down.

SHUTTING DOWN WHILE IN CONFIGURATION MODE ONLY

NOTE: If the server is in both Run mode and Configuration mode, you must shut it down through Run mode. You cannot shut down the server from Configuration mode when the server is running. Closing the configuration when the server is in Run mode leaves the server running.

1. If the server is in Configuration mode only, click File > Exit.

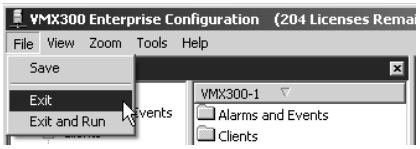


Figure 12. File Menu

2. If the server configuration has not changed, the server shuts down immediately.

   If you made any changes to the configuration, the Save Changes prompt appears. Click Yes to save changes.

   If any scripts or expressions contain errors, the Script and Expression Verification window appears. Use this window to correct the errors (refer to *Syntax Error-Checking* in the *Scripts and Expressions* section for instructions), and then click OK. The Script and Expression Verification window closes and the server shuts down.

License Manager

License Manager provides a convenient means of managing your software licenses. Each server in your system must have a valid base license to run VMX300(-E). If no valid base license is registered, you will not be able to launch the server without first adding a license.

ADD A LICENSE

1. If the server has prompted you to enter a license, click Yes. Otherwise, open the License Manager by clicking Tools > License Manager. Then click Add in the License Manager dialog box. The Add License dialog box opens.

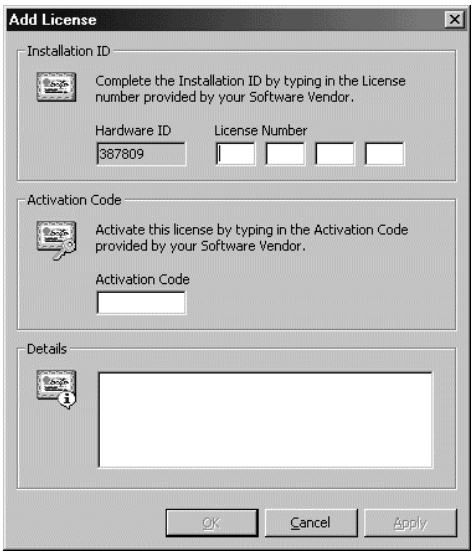


Figure 13. License ID

2. Enter your license ID in the Add License dialog box. The base license ID and any additional license IDs (each ID is a four-part number) are provided on the VMX300(-E) Licenses sheet. The hardware ID is entered by Pelco at the factory.

IMPORTANT: Once you have entered your License ID, you must obtain your activation code (step 3) and then enter it (step 4) within 45 days.

3. Obtain your activation code.

   a. Open your Internet browser and go to the VMX Series Activation page at Pelco.com. http://www.pelco.com/vmxactivation

   b. Enter your hardware ID and license ID, and then complete the remaining fields.

   c. Click Activate. A confirmation screen appears, containing your activation code.

   OR

   Call Pelco Technical Support:
   1-800-289-9100 or
   1-559-292-1981

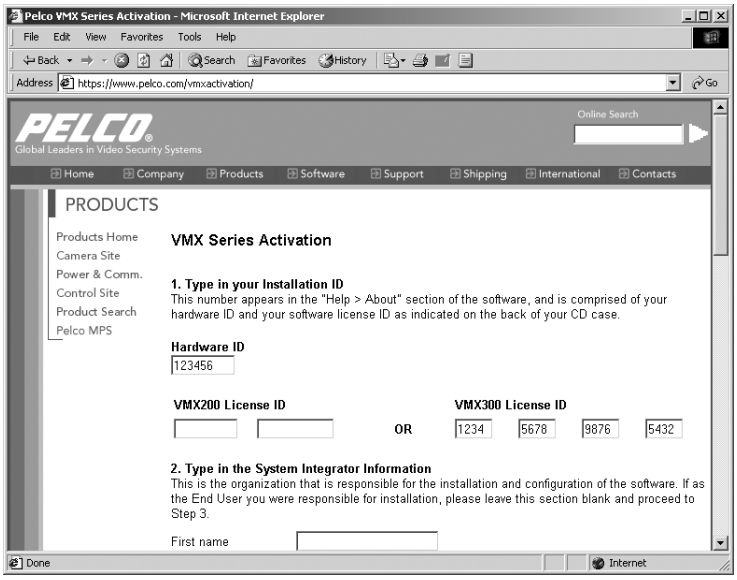


Figure 14. Hardware ID and License ID

4. Enter your activation code in the Add License dialog box.

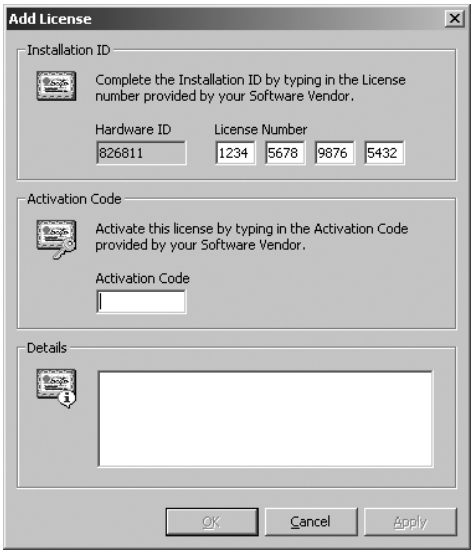


Figure 15. Activation Code

5. Click Apply.

   If you purchased additional license IDs, repeat steps 1-4 for each license ID.

   Note that licenses are applied as follows:

VMX300 Client Application	Five licenses for each additional client (licenses for the first client application are covered by the base license)
VMX300-E Client Application	Ten licenses for each additional client (licenses for the first client application are covered by the base license)
Cameras	One license for each camera

6. Click Close.

NOTE: To refer to the installation ID or activation code at a later time, complete the following steps:

- Select Tools > License Manager from the menu bar. The License Manager dialog box appears.
- Click your license, and then click Properties. The License Properties dialog box appears.

DELETE A LICENSE

If you delete the base license, the server will ask you if you want to enter a new license. If you select No, the server will shut down. If you select Yes, the Add License dialog box will open. Refer to *Add a License* for instructions on entering licensing information.

1. In the Licenses area of License Manager, select the license you want to delete and click Remove. The server prompts for confirmation.
2. If you are sure you want to delete the license, click Yes. The license name disappears from the Licenses list and details for that license are removed from the summary.

TIP: Delete any licenses that have expired, as they serve no purpose. They cannot be reactivated.

Starting and Stopping Device Drivers

START A DEVICE DRIVER

Start each device driver needed to control the devices in your system. You can start the drivers before you start the VMX300(-E) server, or after.

When you start a device driver, you have the choice of running it as an executable or as a service. If you ever have to restart a driver that is run as an executable, you will have to follow the steps outlined here. To restart a driver that is run as a service, restart the computer the driver is installed on, or start the driver through the Windows Control Panel Administrative Tools.

TIP: If you run a device driver as a service, you can set the driver to restart automatically in the event of failure. Once the driver is running as a service, go into Windows Control Panel Administrative Tools, open the driver service, and set the restart options on the Recovery tab.

To start a device driver:

1. Run the device driver application from the Windows Start menu, or double-click the driver icon if there is one on the Windows desktop.

   If this is the first time you are launching the device driver, the Corrupt or Missing Database message appears because VMX300(-E) must create a new database the first time you use it. Click Create.

   If this is not the first time you are launching the device driver, and the Corrupt or Missing Database message appears, then the driver database is corrupted or missing. If this is the case you will need to either restore a backup or create a new database. Creating a new database destroys the existing database if there is one. For information on restoring a backup, refer to *Database Utilities*.

Figure 16. Create or Restore Database Dialog Box

   Once a valid database is in place, the Configure Driver dialog box opens.

Figure 17. Configure Driver Dialog Box

2. If the driver is currently installed to run as a service and you want to run it as an executable, click "Remove the driver as a service," then click OK. Repeat step 1 to re-open the Configure Driver dialog box.
3. **Local network adapter:** Select the IP address of the computer the driver is installed on from the drop-down list.
4. **Listening port:** The listening port is the port the device driver uses to receive commands from the server.

   If you have not yet added the device driver to the server configuration, use the default port number provided, or type in a port number between 2 000 and 10 000 that has not been assigned to another driver. Use this port number as the Listening Port when you add the device driver to the server configuration.

   If the device driver has previously been added to the server configuration, select the driver's listening port from the drop-down list. The listening port is the port that was specified when the driver was added to the server configuration. To find out the listening port, log in to configuration mode. The port is displayed beside the driver in the Object Browser.

5. **Mode:**

    a. **Executable:** To run the device driver as an executable, click "Start the driver as an executable."

    b. **Service:** To run the device driver as a service, click "Install the driver as a service."

DX8000 NOTE: The option to run the DX8000 driver as a service is not available at this time. When starting the DX8000 driver, you must click "Start the driver as an executable."

6. Some device drivers support additional options. For more information on a particular driver's options, refer to *Device Drivers* for that driver.

7. Click OK. The Configure Driver dialog box closes. If you are running the driver as a service, start the driver through the Windows Control Panel Administrative Tools, or restart the computer the driver is installed on. An icon representing the driver appears in the Windows system tray, indicating that the driver is running.

TIP: To check whether a device driver is running, log in to configuration mode, edit the device driver, and click Check Now. While the server is checking, the buttons in the dialog box are unavailable. If the server succeeds in finding a driver, the buttons become available again. If no driver is found, the server displays a warning message. Refer to *Edit a Device Driver's Properties* for more information.

SHUT DOWN A DEVICE DRIVER

1. Right-click the driver icon in the Windows system tray and select Exit from the pop-up menu. You are prompted to confirm.

2. If you are sure you want to shut down the driver, click Yes. The driver shuts down.

NOTE: If the device driver is running as a service, you can also shut it down through the Windows Control Panel Administrative Tools.

Clients, Custom Windows, and Canvases

VMX300(-E) provides tools to define custom windows that are viewable through the client. Custom windows are used for the following functions:

- Viewing live and archived video
- Displaying maps
- Displaying an Internet browser
- Connecting to a remote computer

In order for an operator to be able to connect to a server and use a custom window in the client, you must do the following:

- Add the operator's workstation to the server configuration as described in *Add a New Client*.
- Create a custom window for the new client as described in *Add a New Custom Window*.
- If the operator is going to view video in the window, add one or more canvases to the window as described in *Add a New Canvas (General)*, and, for analog canvases, specify the connections between devices.

Canvases are only required if the window will be used to view video. Canvases define the video display technology available to that client, and can include both analog and digital (IP-based) technologies. Refer to *Canvases* for more information.

Connections map out how video equipment is physically connected. Refer to *Connections* for more information.

TIP: If you are configuring a newly-installed server and find you have many clients to create with a similar configuration, you can do it very quickly as follows: Add one client with the desired windows and canvases. Use Copy and Paste Many to create multiple copies of the client. Each copy of the client will have the identical windows and canvases defined for it. Then edit the copies one at a time to customize them as needed. This technique is particularly useful for clients that will have access to the same custom windows. Refer to *Pop-Up Menus* in the *Appendix* for detailed instructions on using Copy and Paste Many.

CLIENTS

Adding an operator's computer to the server configuration allows that workstation to connect to the server. When you add a client to the server configuration, you can

- Supply a default workspace for the client
- Make custom windows available on the client

Refer to *Workspaces* for information on creating a default workspace. Refer to *Custom Windows* for information on configuring custom windows.

WORKSPACES

Workspaces control the appearance of the VMX300(-E) client. In particular, they control which windows are displayed, and their size, position, and content.

You can create a default workspace that loads automatically on a specified client when an operator logs in to that client. Operators with permission to work with workspaces can override the default by setting preferences to load a workspace of their choosing automatically, or by explicitly opening a workspace once they have logged in. Refer to *User Groups* for information on workspace permissions.

To create a workspace, you must log in to the VMX300(-E) client under a user group that allows you to work with workspaces, and you must be connected to your home server. Refer to *Configuring Servers* in the VMX300(-E) Client Operation Manual for information on selecting a home server.

Once logged in, you can change the appearance of the display either by using standard Windows techniques for resizing and repositioning windows, or by editing the workspace. When the display is adjusted as you want it, save the workspace. Refer to *Workspaces* in the VMX300(-E) Client Operation Manual for information on editing and saving a workspace.

To use the workspace as the default workspace for a client, log in to the server in configuration mode and edit the client as described in *Edit a Client's Properties*

ADD A NEW CLIENT

1. Navigate the Object Browser to [project name] > Clients. Double-click <Add New Client> in the right pane, or right-click Clients in the left pane and select Add New from the pop-up menu. The Add New Client dialog box opens.

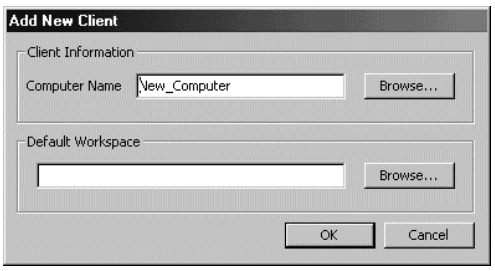


Figure 18. Add New Client Dialog Box

2. **Computer name:** Type in the name of the computer you want to add as a client of the VMX300(-E) server, or click Browse to select from a list of computers visible on the network. The computer name you enter here must be identical to the computer name listed in Windows Control Panel System on the computer you want to add. Use the computer name to refer to the client in scripts and expressions. For a list of client properties that can be scripted, refer to *Scripts and Expressions - Properties of Objects.*

3. **Default workspace:** If you want the server to supply a default workspace to the client you are adding, type in the pathname of the workspace file you want to load, or Browse to select the desired file. VMX300(-E) loads the default workspace for any operator whose user preferences are set to "Use the workspace supplied by the server." Refer to *Workspaces* for information on creating workspaces.

4. Click OK. The Add New Client dialog box closes and the new client is added. The name of the new client appears in the Object Browser.

EDIT A CLIENT'S PROPERTIES

1. Navigate the Object Browser to [project name] > Clients. In either pane, right-click the client whose properties you want to change and select Edit from the pop-up menu. The Edit Client Properties dialog box opens.

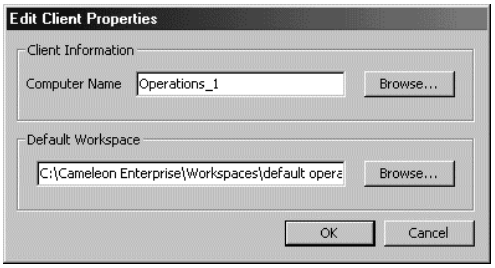


Figure 19. Edit Client Properties Dialog Box

2. Change properties of the client as desired. Refer to *Add a New Client* for information on specific properties.

3. Click OK. The Edit Client Properties dialog box closes.

DELETE A CLIENT

NOTES:

- Deleting a client is irreversible. If you delete a client and then change your mind, you must add it back as described in *Add a New Client*.
- Deleting a client does not affect workspace files.

1. Navigate the Object Browser to [project name] > Clients. In either pane, right-click the client you want to delete and select Delete from the pop-up menu. The Confirm dialog box opens.
2. If you are sure you want to delete the client, click Yes.The selected client is deleted and the Confirm dialog box closes. The deleted client disappears from the Object Browser.

CUSTOM WINDOWS

Custom windows are viewed through the VMX300(-E) client. They are used for the following functions:

- Viewing live and archived video
- Displaying maps
- Displaying an Internet browser
- Connecting to a remote computer

Any window that will be used to view video must have one or more canvases defined for it that reflect the video display technologies available to the client. Refer to *Canvases* for more information.

You can configure custom windows so that more than one client can view a particular window, simply by giving the window the same name and script tag on each client. Any action affecting the window that is executed automatically by a script will affect that window on every client that runs the script. Anything done manually by an operator, such as dragging a camera to a window, will not affect any other operator's window.

For example, suppose you want to alert several different operators when an exit door is opened. First, create a recipient group and make the operators members of the group. Now create an alarm/event category that simultaneously sends notification to each member of that recipient group. Finally, define an alarm belonging to that category with an On Event script that loads live video of the exit area into a particular window that is defined on each operator's client. When the alarm is triggered, the script will automatically load the video in the window of each recipient operator who is logged in at the time.

TIP: You can copy a custom window from one client to another using Copy and Paste. Refer to *Pop-Up Menus* in the *Appendix* for detailed instructions on using Copy and Paste.

HOW MANY CUSTOM WINDOWS TO CONFIGURE

The number of custom windows that you need to configure will vary based on your specific system parameters. In general, configure as many custom windows as you want the operator using this client to view at any one time.

For example, a total of nine custom windows are required for an operator to view the following types of content at one time:

- A map (operators can view maps in custom windows as well as in the viewport)
- A web page
- Three analog video streams
- Four digital video streams

Note, however, that your specific system parameters will limit the number of digital video streams that an operator can view at any one time. Refer to Table B in the *How to Choose the Video Stream Settings for Your Configuration* section for an overview of the maximum number of streams recommended for specific digital settings.

ADD A NEW CUSTOM WINDOW

NOTE: If the same custom window will be viewed by more than one client, it must have the same name and script tag for every client.

To add a new custom window to a particular client:

1. Navigate the Object Browser to [project name] > Clients > [client name] > Windows. Double-click <Add New Window> in the right pane, or right-click Windows in the left pane and select Add New from the pop-up menu. The Add New Window dialog box opens.

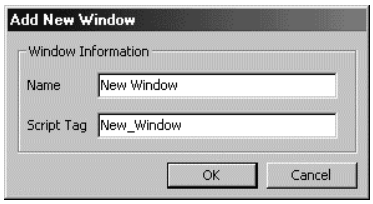


Figure 20. Add New Window Dialog Box

2. **Name:** Type in a descriptive name for the custom window you want to add. A particular client cannot have two windows with the same name. However, different clients can have windows with the same name. Window names are at most 50 characters long and can include any letter, digit or special character, with the exception of single and double quotation marks. Window names are not case sensitive.

   A tag resembling the window name appears in the Script Tag box. If the window name contains special characters, they are omitted from the tag. Spaces are replaced with underscores. Leading digits are removed.

3. **Script tag:** If you do not want to use the script tag provided by the server, type in a tag. Script tags are at most 50 characters long. They can include any letter, digit or the underscore character, but cannot begin with a digit. They cannot contain spaces or special characters. Tags are not case sensitive. Use the script tag to refer to the custom window in scripts. For a list of window properties that can be scripted, refer to *Scripts and Expressions - Properties of Objects*.

4. Click OK. The Add New Window dialog box closes and the new window is added. The name and script tag of the new window appear in the Object Browser. When logged in to the client for which the window is defined, an operator with permission to edit workspaces will see the window listed in the Edit Workspace dialog box.

EDIT A CUSTOM WINDOW

NOTE: If you change the script tag for a custom window, any script that refers to the window will contain an error. To correct the error, update the scripts so they use the window's new script tag. Refer to *Scripts and Expressions* for more information.

To change the properties of an existing custom window:

1. Navigate the Object Browser to [project name] > Clients > [client name] > Windows. In either pane, right-click the window you want to change and select Edit from the pop-up menu. The Edit Window Properties dialog box opens.

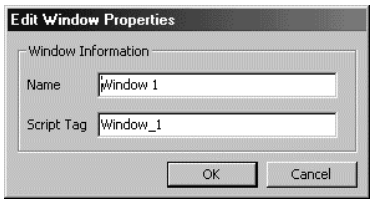


Figure 21. Edit Window Properties Dialog Box

2. Change properties of the window as desired. Refer to *Add a New Custom Window* for information on specific properties.

3. Click OK. The Edit Window Properties dialog box closes.

DELETE A CUSTOM WINDOW

Deleting a custom window is irreversible. If you delete a custom window and then change your mind, you must add a new custom window. Also note that if you delete a custom window, any script that refers to the custom window will contain an error.

1. Navigate the Object Browser to [project name] > Clients > [client name] > Windows. In either pane, right-click the window you want to delete and select Delete from the pop-up menu. The Confirm dialog box opens.
2. If you are sure you want to delete the window, click Yes. The selected window is deleted and the Confirm dialog box closes. The deleted window disappears from the Object Browser.

CANVASES

Any custom window that will be used to display video must have at least one canvas defined for it. Canvases specify the video display technology available to the client the custom window is configured for. This can include both analog and digital (IP) technologies. VMX300(-E) supports two analog video display technologies:

- Quad Video Display
- Video for Windows

To use either of these analog technologies, the client computer must have an appropriate video card installed in it.

If you add more than one canvas to a custom window, VMX300(-E) will have a choice of which video display technology to employ when an operator views video in that window. VMX300(-E) makes its choice based on the order the canvases are listed in the Object Browser. Refer to *Re-Order a Window's Canvases* for more information.

TIP: To provide maximum flexibility for a client, add as many canvases as you can: one for each analog video card in the client, and one for each video encoder configured on the server.

ADD A NEW CANVAS (GENERAL)

To add a new canvas to a custom window:

1. Navigate the Object Browser to [project name] > Clients > [client name] > Windows > [window name] > Canvases. Double-click <Add New Canvas> in the right pane, or right-click Canvases in the left pane and select Add New from the pop-up menu. The Add New Canvas dialog box opens.

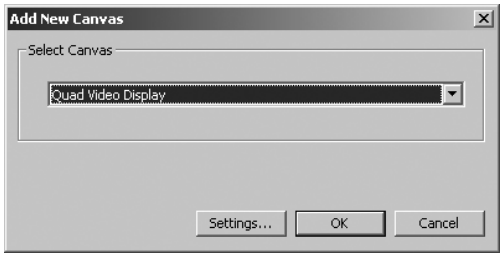


Figure 22. Add New Canvas Dialog Box

2. Select the canvas you want to add from the drop-down list.
3. **Settings:** If the Settings button is available, click Settings to configure the canvas settings. Some canvases do not have settings. If there are no settings, go to step 6.
4. **General tab:** For Video for Windows and Quad Video Display canvases, the settings available on the General tab assign hardware to the canvas, and are hardware dependent. Instructions for configuring Video for Windows and Quad Video Display settings follow.
    a. **Card number:** Use the default card number setting.

b. **Video input number (Quad Video Display cards only):** Select the video input number for the canvas you are configuring from the drop-down list. Click OK to close the dialog box.

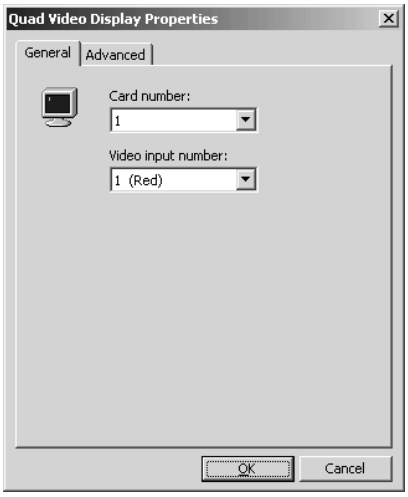


Figure 23. General Setting for Quad Video Display

5. **Advanced tab:** For all types of canvas, the canvas settings Advanced tab allows you to configure the image quality for image capture files, including both automatic FTP image capture and image capture initiated by an operator using the Capture button. You only need to configure the settings on the Advanced tab if the canvas is going to be used to capture images.

   a. **Picture quality:** Use the slider to set the quality of the images you want captured from this canvas. Lower the quality to reduce the file size of captured images.

   b. **Stretch picture:** Select Stretch picture if you want to change the dimensions of captured images. The dimensions are given in pixels. It is recommended that you only reduce the size, not increase it, since increasing the picture dimensions will make the picture look grainy. To prevent distortion, reduce the width and height by the same proportion. Reduce the dimensions to 80 x 60 for thumbnails.

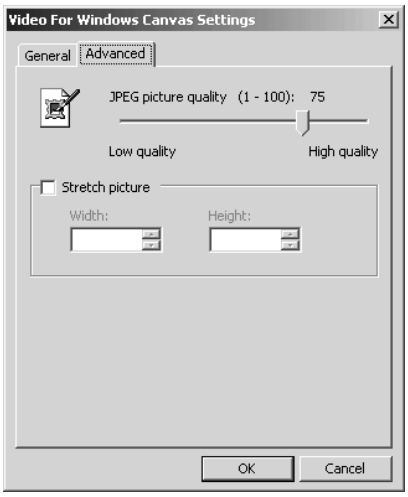


Figure 24. Advanced Settings

6. Click OK. The Add New Canvas dialog box closes and the new canvas is added. The name of the canvas appears in the Object Browser.

ADD A NEW CANVAS (PELCONET)

Any custom window that is used to display video encoded by a PelcoNet encoder or encoder/decoder must have a PelcoNet MPEG Series canvas defined for it. Windows used to display analog video that is decoded by a PelcoNet device do not require a PelcoNet MPEG Series canvas.

1. Navigate the Object Browser tree to [project name] > Clients > [client name] > Windows > [window name] > Canvases for the window that will be used to display video encoded by a PelcoNet encoder or encoder/decoder.
2. Double-click <Add New Canvas>. The Add New Canvas dialog box appears.

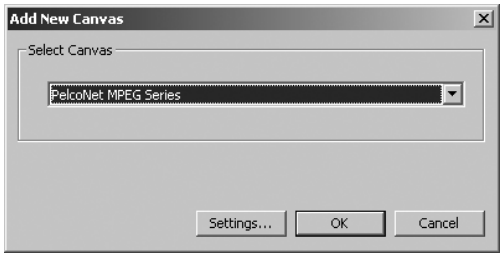


Figure 25. Add a PelcoNet Canvas

3. Select PelcoNet MPEG Series from the drop-down box, and then click Settings. The Canvas Settings dialog box appears.

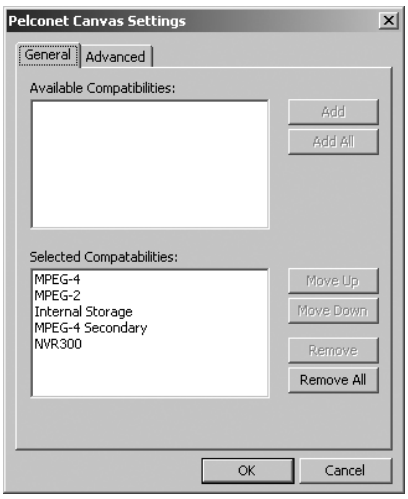


Figure 26. General PelcoNet Canvas Settings

The Selected Compatibilities field lists the types of video signal that the VMX300(-E) video window can display. By default, the window can display all types of video signal. If you move a signal from the Selected Compatibilities field to the Available Compatibilities field, the VMX300(-E) video window will not display those types of signals.

A VMX300(-E) video window can display the following types of signals:

- MPEG-4: PelcoNet encoders and encoder/decoders support this signal type. For information on configuring PelcoNet 4001A encoder/decoders for this signal type, refer to *Devices*. For PelcoNet 3xx encoders, the MPEG-4 signal type corresponds to Stream 1, configured as described in the *Devices* section.
- MPEG-2: PelcoNet 4001A encoder/decoders support this signal type. Refer to *Devices* for information on configuring the encoder for MPEG-2 streaming.
- Internal Storage: This is the video signal from a PelcoNet device's built-in recorder. This signal type applies to any PelcoNet NET350 encoder that has integral recording capability selected. Refer to *Devices* for instructions on configuring integral recording capability.
- MPEG-4 Secondary: PelcoNet 3xx encoders support this signal type. The MPEG-4 Secondary signal type corresponds to Stream 2, configured as described in the *Devices* section.
- NVR300: The video signal from an NVR300. This signal type applies to PelcoNet encoders and encoder/decoders that have been configured to have their streams recorded by an NVR300. Refer to *Devices* for more information.

Change the List of Selected Signal Types

To change the list of selected signal types, you can do any of the following operations:

- Click the signal type, and then click remove; the signal type appears in the Available Compatibilities list.
- To select multiple signal types, press the Ctrl key while clicking signal types.
- To remove all signal types, click Remove All.
- To move a signal type from the Available Compatibilities list to the Selected Compatibilities list, click the signal type, and then click Add; the signal type appears in the Selected Compatibilities list.
- To move all signal types from the Available Compatibilities list to the Selected Compatibilities list, click Add All.

Reorder the List of Selected Signal Types

VMX300(-E) attempts to display signal types in the order they appear in the Selected Compatibilities list. You can sort the list in the order you want VMX300(-E) to try signal types. To move a signal type higher in the list, click the signal type, and then click Move Up. To move a signal type lower in the list, click the signal type, and then click Move Down.

Refer to the *Clients, Custom Windows, and Canvases* section for additional information on adding a canvas.

Configure Image Quality of Captured Images

1.Click the Advanced tab on the PelcoNet Canvas Settings dialog box.

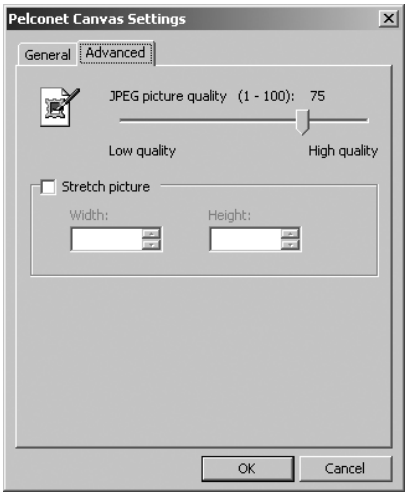


Figure 27. Advanced PelcoNet Canvas Settings

2. Configure the image quality settings as desired.

ADD A NEW CANVAS (DX8000 OR DX9000 DVR)

Any custom window that is used to display video from a DX8000 or DX9000 DVR must have a DVR canvas defined for it.

1. Navigate the Object Browser tree to [project name] > Clients > [client name] > Windows > [window name] > Canvases for the window that will be used to display video from a DVR.
2. Double-click <Add New Canvas>. The Add New Canvas dialog box appears.

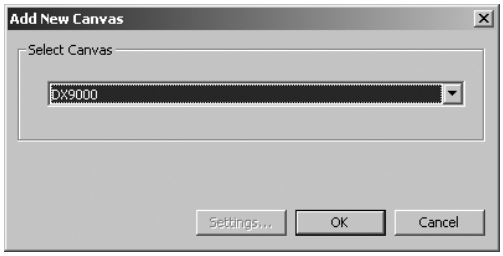


Figure 28. Add a DVR Canvas

3. Select the appropriate DVR (either the DX8000 or the DX9000) from the drop-down box, and then click OK.

EDIT A CANVAS

To edit an existing canvas:

1. Navigate the Object Browser to [project name] > Clients > [client name] > Windows [window name] > Canvases. In the right pane, double-click the canvas you want to edit, or right-click the canvas and select Edit from the pop-up menu. The Edit Canvas Properties dialog box opens.

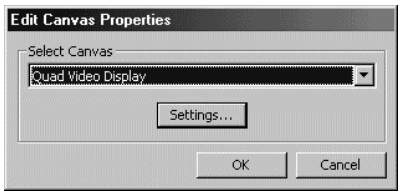


Figure 29. Edit Canvas Properties Dialog Box

2. Change properties of the window as desired. Refer to *Add a New Canvas (General)* for information on specific properties.
3. Click OK. The Edit Canvas Properties dialog box closes.

RE-ORDER A WINDOW'S CANVASES

If you add more than one canvas to a custom window, VMX300(-E) will have a choice of which video display technology to employ when an operator views video in that window. VMX300(-E) makes its choice based on how the canvases are ordered in the Object Browser. The server tries the canvas at the top of the list first, then, if it is not available, the second canvas in the list, and so on.

You can re-order the canvases for a custom window using the Move Up and Move Down options.

To change the order of a window's canvases, navigate the Object Browser to [project name] > Clients [client name] > Windows > [window name] > Canvases. In the right pane, right-click the canvas you want to move and select Move Up or Move Down from the pop-up menu. The canvas moves up or down one position.

DELETE A CANVAS

Deleting a canvas is irreversible. If you delete a canvas and then change your mind, you must add a new canvas.

1. Navigate the Object Browser to [project name] > Clients > [client name] > Windows > [window name] > Canvases. In the right pane, right-click the canvas you want to delete and select Delete from the pop-up menu. The Confirm dialog box opens.
2. If you are sure you want to delete the canvas, click Yes. The selected canvas is deleted and the Confirm dialog box closes. The deleted canvas disappears from the Object Browser. The window is no longer able to display video of the type supported by the deleted canvas.

Device Drivers

VMX300(-E) uses device drivers to control and manage devices. Each device driver controls a particular type of equipment, such as surveillance camera, video recorder, or any other type of device.

There are several steps involved in configuring device drivers on the VMX300(-E) server:

1. Launch the device driver. Refer to *Starting and Stopping Device Drivers - Start a Device Driver*.
2. Add the device driver to the server configuration as described in *Add a New Device Driver*.

ADD A NEW DEVICE DRIVER

NOTES:

- To add a device driver to the VMX300(-E) server, the driver must be running on the network. Once you have added a device driver to the server configuration, you can add devices of that type.
- Changes to device drivers, such as adding a new driver to the server configuration, come into effect immediately. You cannot discard your changes by exiting configuration mode without saving.

To add a new device driver to the VMX300(-E) server:

1. Navigate the Object Browser to [project name] > Device Drivers. Double-click <Add New Driver> in the right pane, or right-click Device Drivers in the left pane and select Add New from the pop-up menu. The Add New Driver dialog box opens.

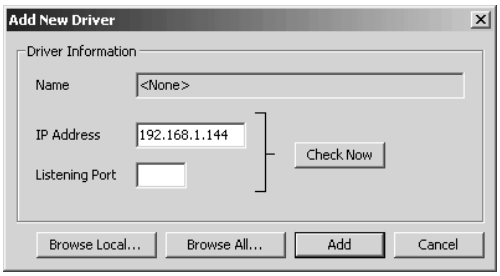


Figure 30. Add New Driver Dialog Box

2. Select the device driver you want to add using one of the following methods:

   a. **Browse local:** To browse the server workstation for running drivers, click Browse Local. The Browse Drivers dialog box opens.

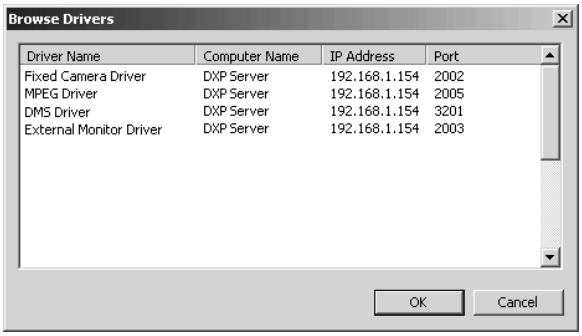


Figure 31. Browse Local Drivers Dialog Box

The Browse Drivers dialog box lists all device drivers running on the server workstation. Select the driver you want to add and click OK to close the Browse Drivers dialog box. The driver name, IP address, and listening port appear in their respective boxes.

b. **Browse all:** To browse the network for running drivers, click Browse All. The Browse Drivers dialog box opens.

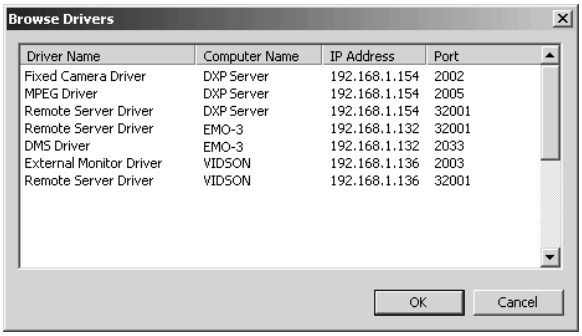


Figure 32. Browse All Drivers Dialog Box

The Browse Drivers dialog box lists all device drivers running at network locations visible to the server you are configuring. Select the driver you want to add and click OK to close the Browse Drivers dialog box. The driver name, IP address, and listening port will appear in their respective boxes.

c. **Add driver manually:** If you know the IP address and port number of the driver you want to add, you can add the driver by typing the address and port directly, without browsing drivers.

(1) **Driver IP address:** By default, the server's IP address is entered in the Driver IP Address box. If the device driver is not installed on the server, type the IP address of the computer the driver is installed on.

(2) **Listening port:** The listening port is the port the device driver uses to receive commands from the server. Type in the listening port for the device driver you want to add. This is the port that was entered in the Configure Driver dialog box when the device driver was launched. To find out the listening port, position the pointer over the driver icon in the Windows system tray of the computer the driver is installed on.

(3) **Check now:** If you want the server to verify that a device driver is running at the specified IP address and port number, click Check Now. While the server is checking, the dialog box's buttons are unavailable. If the server succeeds in finding a driver, the buttons become available again. If no driver is found, the server displays a warning message.

3. Click Add. The Add New Driver dialog box closes and the new driver appears in the Object Browser, with the IP address and port number beside the driver name. If the driver has previously been configured, its devices also appear in the Object Browser. If you are adding a remote server driver, the remote server's alarms and events appear in the Object Browser as read properties of the server, and the remote server's devices appear as sources.

TIP: The easiest way to add a remote server driver is to Browse All and select the desired driver. Refer to *Server Ties* and *Alarms and Events - Access Alarms and Events Defined on Another Server* for information on remote server drivers.

AUTODISCOVER DEVICE DRIVERS

The Autodiscover All Drivers function locates all drivers that are running on the local area network (LAN). To add a driver that is running on a wide area network (WAN), use the Add New Driver option.

NOTE: In order for the VMX300(-E) system to locate a device driver automatically, the driver must be installed at a network location that is visible to the VMX300(-E) server. If you know the IP address and port number of a driver that was not located, use the Add New Driver option.

Note that changes to device drivers, such as autodiscovering drivers, come into effect immediately. You cannot discard your changes by exiting configuration mode without saving.

1. Navigate the Object Browser to [project name] > Device Drivers. In the right pane, double-click <Autodiscover All Drivers>. The server warns you that autodiscovering all device drivers will add to or update the currently configured drivers.

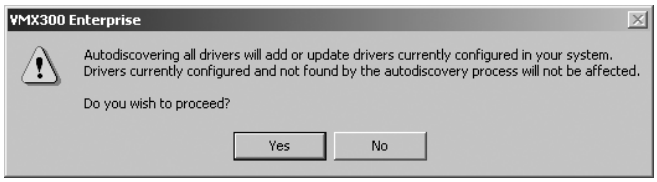


Figure 33. Autodiscover Warning

2. If you are sure you want to proceed, click Yes. The server adds the drivers it finds to the server configuration. The drivers appear in the Object Browser.

EDIT A DEVICE DRIVER'S PROPERTIES

You can change the IP address and port number of a device driver, but not the driver's name.

NOTE: Changes to device drivers, such as autodiscovering drivers, come into effect immediately. You cannot discard your changes by exiting configuration mode without saving.

To change the properties of an existing device driver:

1. Navigate the Object Browser to [project name] > Device Drivers. Right-click the driver you want to edit and select Edit from the pop-up menu. The Edit Driver Properties dialog box opens.

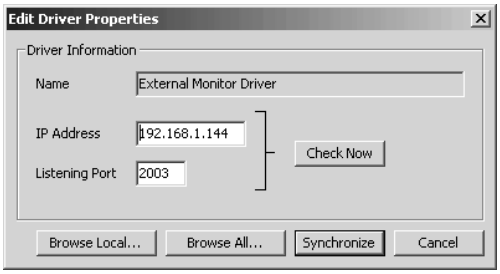


Figure 34. Edit Driver Properties Dialog Box

2. Edit the properties as desired. Refer to *Add a New Device Driver* for more information.
3. Click Synchronize. The Edit Driver Properties dialog box closes.

DELETE A DEVICE DRIVER

NOTES:

- Changes to device drivers, such as deleting a driver from the server configuration, come into effect immediately. You cannot discard your changes by exiting configuration mode without saving.
- Deleting a device driver deletes all the devices of that type and removes their icons from maps. This introduces an error into scripts that refer to one of the deleted devices.
- Deleting a device driver is irreversible. If you delete a device driver and then change your mind, you must add it back as described in *Add a New Device Driver* or *Autodiscover Device Drivers*. Any devices that were configured before you deleted the driver will automatically be added to the server configuration when you add the driver back.

1. Navigate the Object Browser to [project name] > Device Drivers. In either pane, right-click the driver you want to delete and select Delete from the pop-up menu. The Confirm dialog box opens.
2. If you are sure you want to delete the device driver, click Yes. The selected driver is deleted and the Confirm dialog box closes. All the driver's devices are deleted and their icons removed from maps.

CONFIGURE A PELCONET MPEG TIME SERVER

The PelcoNet MPEG driver allows you to configure a time server for the driver to periodically synchronize its clock to. To ensure that synchronization works properly, set the time zone on the PelcoNet device to the time zone where the device is installed. Refer to the appropriate PelcoNet manual for instructions on setting the device's time zone.

NOTE: Be sure that the time zone settings are synchronized appropriately on all devices in the VMX300(-E) configuration.

Time servers are configured when you start the driver.

Configure Time Servers

1. Start the PelcoNet MPEG driver. The Configure Driver dialog box appears.

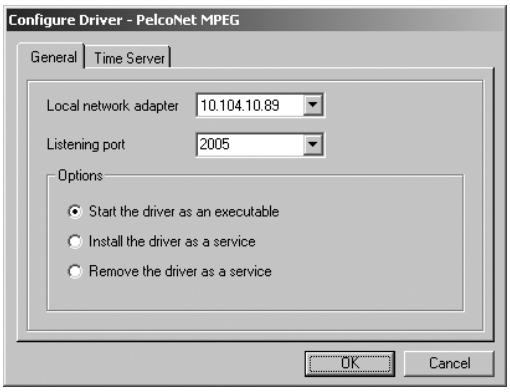


Figure 35. General Tab for PelcoNet Driver

2. If necessary, configure the settings on the General tab, and then click the Time Server tab. The Time Server fields appear.

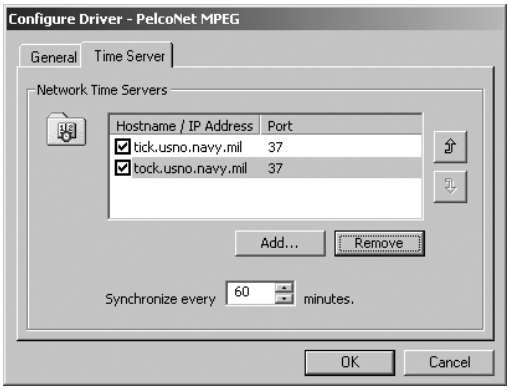


Figure 36. Time Server Tab for PelcoNet Driver

3. Click Add to specify a server to synchronize to. The Add Time Server dialog box appears.

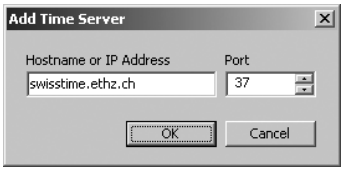


Figure 37. Add Time Server Dialog Box

4. Type the time server's host name or IP address, and the port number the time server opens for synchronization requests.
5. Click OK. The Add Time Server dialog box closes and the time server appears in the Network Time Servers list.

6. Optional: repeat steps 3-5 to add time servers as necessary.
7. Optional: Each time server that you add to the list is checked by default. If you do not want to use a particular time server click it to uncheck the server. If more than one time server is selected, the driver will attempt to synchronize to the first selected server in the list. If that fails, the driver will attempt to synchronize to the next selected server in the list, and so on, until synchronization succeeds or there are no more selected servers.
8. Optional: To move a time server to a higher or lower order in the list, click the time server, and then click the up or down arrow.

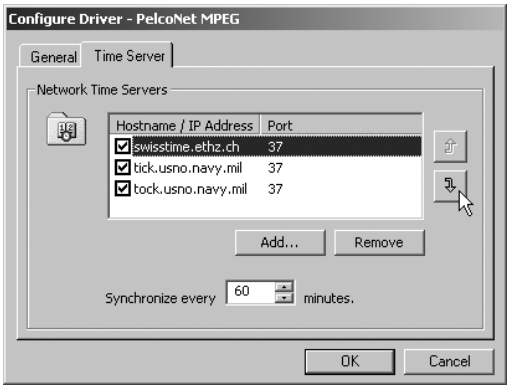


Figure 38. Moving a Time Server

9. Specify how often you want the device driver's clock synchronized with the time server's clock in the Synchronize minutes field.
10. Click OK to close the Configure Driver dialog box.

Remove a Time Server

1. Start the PelcoNet MPEG driver. The Configure Driver dialog box appears.
2. Click the Time Server tab. The Time Server fields appear.
3. Click the server you wish to remove from the list, and then click Remove.
4. Optional: repeat step 3 to remove additional time servers as necessary.
5. Click OK to close the Configure Driver dialog box.

Devices

Changes to devices, such as adding a new device to the server configuration or deleting a device, come into effect immediately. You cannot discard your changes by exiting configuration mode without saving.

Before you can add a device to the server configuration, you must first start the device driver—either on the server workstation or on the network—and then add the driver to the server configuration. Refer to the *Device Drivers* section for instructions.

To add a device, complete the following steps:

1. Navigate the Object Browser tree to [project name] > Device Drivers > [device driver name] > Devices.

   Note that some device drivers, such as the PelcoNet MPEG driver or the ASCII driver, do not list the generic "Devices" label under the driver name. These drivers list either a specific type of device, such as "Switchers" or "Cameras," or they list the device model, such as "PelcoNet 300 Encoders." The specific navigation path is included in the instructions provided for the specific device, in the following pages.

2. In the right pane, two functions are provided for adding devices—Add New Device and Autodiscover All Devices. Use either option.

ADD A NEW DEVICE

You can enter a device manually by completing the following steps:

1. Double-click <Add New Device>. The Add New Device dialog box appears.

TIP: As an alternative, you can use the Copy and Paste Many options to add up to 100 devices at once based on an existing device. Refer to *Pop-Up Menus* in the *Appendix* for instructions. If you are adding cameras with addressing, remember to edit each camera in turn to correct the camera address.

2. Configure the device settings, as described in the instructions provided for the specific device, in the following pages.
3. Click OK to close the Add New Device dialog box.

AUTODISCOVER DEVICES

The Autodiscover All Devices function locates all IP devices of the selected type that are running on the local area network (LAN). To add a device that is running on a wide area network (WAN), use the Add New Device option.

Note that you can only locate IP devices automatically. You cannot automatically locate devices that are connected serially.

1. Navigate the Object Browser tree to [project name] > Device Drivers > [device driver name] > Devices.
2. Double-click <Autodiscover All Devices>.
3. Wait several seconds for the process to complete. When the process is complete, the new devices appear in the Object Browser.

   In order for the VMX300(-E) system to locate a device automatically, the driver must be running at a network location that is visible to the VMX300(-E) server. If you know the IP address and port number of a device that was not located, use the Add New Device option.

4. To change any specific device settings, right-click the device, and then select Edit from the pop-up menu.

DELETE A DEVICE

1. Navigate the Object Browser to [project name] > Device Drivers > [device driver name] > Devices.
2. In either pane, right-click the device you want to delete and then select Delete from the pop-up menu. The Confirm dialog box opens.
3. If you are sure you want to delete the device, click Yes. The selected device is deleted and the Confirm dialog box closes. The deleted device disappears from the Object Browser and its device icons are removed from maps.

   Note that deleting a device that is referred to in a script introduces an error into the script. Refer to *Scripts and Expressions* for more information.

TIP: You can delete multiple devices of a particular type at once. Navigate the Object Browser to display the devices you want to delete in the right pane. To select nonconsecutive devices, hold the Ctrl key down while selecting with the mouse. To select consecutive devices, select the first device, hold the Shift key down, and select the last device. Once you have selected the devices you want to delete, right-click and then select Delete from the pop-up menu.

ADD A FIXED CAMERA DEVICE

The fixed camera driver supports any noncontrollable video source, such as a noncontrollable camera.

Before you can add a device to the server configuration, you must first start the device driver—either on the server workstation or on the network—and then add the driver to the server configuration. Refer to the *Device Drivers* section for instructions.

1. Navigate the Object Browser tree to [project name] > Device Drivers > Fixed Camera > Devices.
2. Double-click <Add New Device>. The Add New Fixed Camera dialog box appears.

   You can also configure settings after you have added the camera to the server configuration. Right-click the camera, and then select Edit from the pop-up menu. The Edit Properties dialog box appears, which contains the same tabs and fields as the Add New Fixed Camera dialog box.
3. Configure the camera settings, as described in the following sections.
4. Click OK to close the Add new Device dialog box.

CONFIGURE THE GENERAL TAB

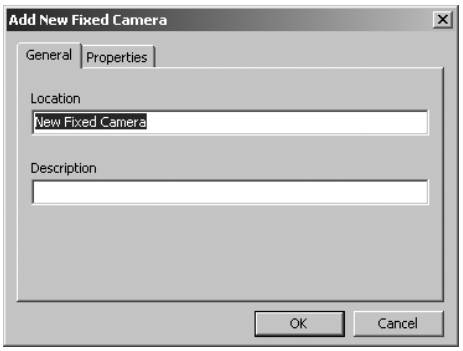


Figure 39. General Tab for Fixed Camera

Use the General tab to enter a location name and an optional description. The location name is used to identify the device. The location name can be a maximum of 50 characters and can include any letter, digit, or special character, with the exception of single and double quotation marks. Location names are not case sensitive.

CONFIGURE THE PROPERTIES TAB

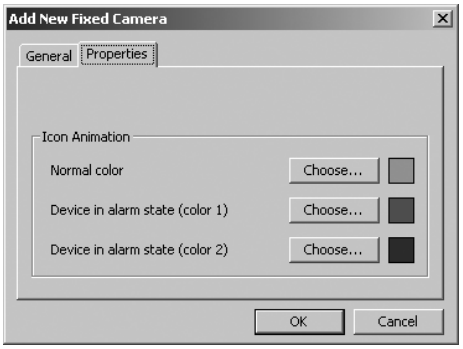


Figure 40. Properties Tab for Fixed Camera

Use the Properties tab to configure the animation settings of fixed camera icons viewed on maps in the VMX300(-E) client. Click Choose next to each condition to select the color settings for that condition. Note that you can configure a different color setting for each camera.

Normal state: When the device's Alarm property equals False, device icons in the client are the color specified here.

Alarm state: When the camera's Alarm write property equals True, the icon flashes alternately between Color 1 and Color 2. Note, however, that flashing icons can increase the CPU workload. To reduce the overall workload, set Color 1 and Color 2 to the same color.

ADD A PELCO PTZ DEVICE

The Pelco PTZ device driver currently supports the following camera models:

- Pelco Spectra II
- Pelco Spectra III
- Pelco Esprit

The Spectra III model operating under D protocol has a feedback feature that communicates camera position to the device driver. VMX300(-E) uses this information to rotate Spectra III device icons placed on maps, so the icon represents the actual direction the camera is pointing. Device icons for Spectra III (P protocol), Spectra II, and Esprit cameras never change direction, regardless of actual camera position.

Before you can add a PTZ camera to the server configuration, you must first start the PTZ device driver—either on the server workstation or on the network—and then add the driver to the server configuration. Refer to *Device Drivers* for instructions.

1. Navigate the Object Browser tree to [project name] > Device Drivers > Pelco PTZ Camera > Devices.
2. Double-click <Add New Device>. The Add New PTZ Camera dialog box appears.

   You can also configure camera settings after you have added the camera to the server configuration. Right-click the camera, and then select Edit from the pop-up menu. The Edit Properties dialog box appears, which contains the same tabs and fields as the Add New PTZ Camera dialog box.
3. Configure the camera settings, as described in the following sections.
4. Click OK to close the Add New Device dialog box.

CONFIGURE THE GENERAL TAB

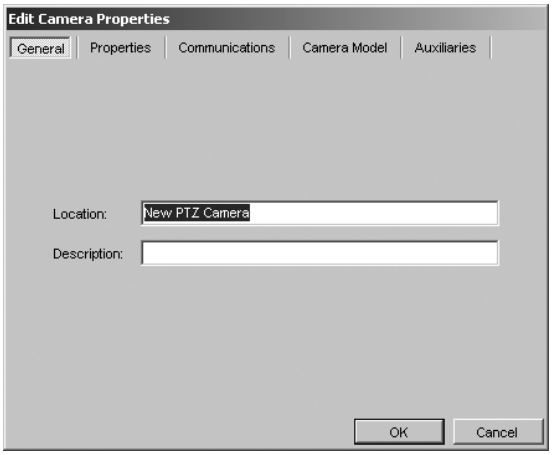


Figure 41. General Tab for PTZ Camera

Use the General tab to enter a location name and an optional description. The location name is used to identify the device. The location name can be a maximum of 50 characters and can include any letter, digit, or special character, with the exception of single and double quotation marks. Location names are not case sensitive.

CONFIGURE THE PROPERTIES TAB

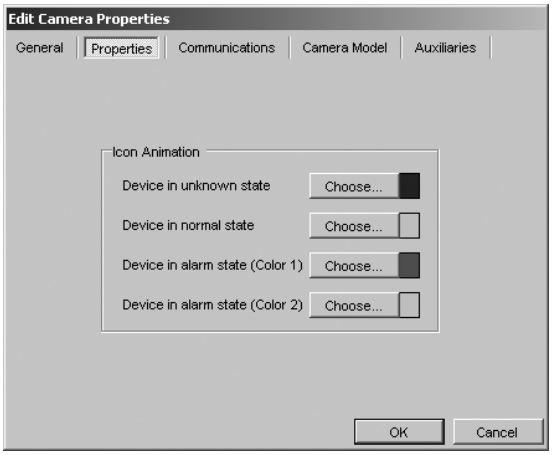


Figure 42. Properties Tab for PTZ Camera

Use the Properties tab to configure the animation settings of camera icons viewed on maps in the VMX300(-E) client. Click Choose next to each condition to select the color settings for that condition. Note that you can configure a different color setting for each camera.

Unknown state: When the camera's CommStatus property equals Offline, device icons in the client are the color specified here.

Normal state: When the camera's CommStatus property equals Online, device icons in the client are the color specified here.

Alarm state: When the camera's Alarm write property equals True, the icon flashes alternately between Color 1 and Color 2. Note, however, that flashing icons can increase the CPU workload. To reduce the overall workload, set Color 1 and Color 2 to the same color.

CONFIGURE THE COMMUNICATIONS TAB

1. **Connection Type:** Specify the type of connection between the device driver and the camera.
   - DIRECT SERIAL: The camera is connected using an RS-232 to RS-422 converter or using an RS-422 PC serial port.
   - INTERNET PROTOCOL: The camera is connected to the serial port on a networked device.
   - MODEM: This feature is reserved for future development.
2. **Settings:** Complete the instructions provided below for the appropriate connection type specified in Step 1. The settings must match the settings specified within the camera. Refer to the appropriate camera installation/operation manual for information on camera settings.

Direct Serial Settings

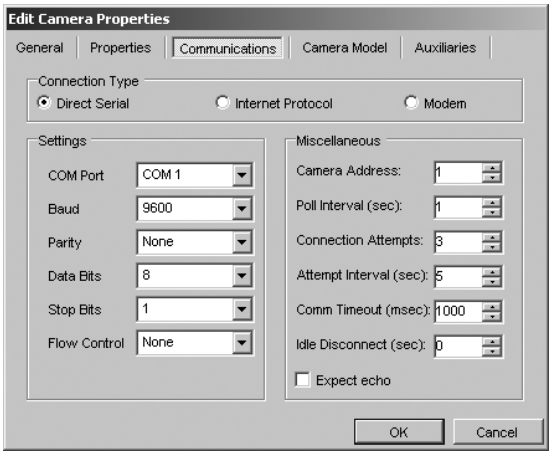


Figure 43. Communications Tab for PTZ Serial Settings

a. Select the COM port that the camera is connected to from the drop-down box.

b. Select the appropriate baud rate and parity settings to match the settings specified in the camera.

c. The remaining settings should specify 8 data bits, 1 stop bit, and no flow control.

d. Refer to Step 3 for instructions on completing the fields in the Miscellaneous section.

Internet Protocol Settings

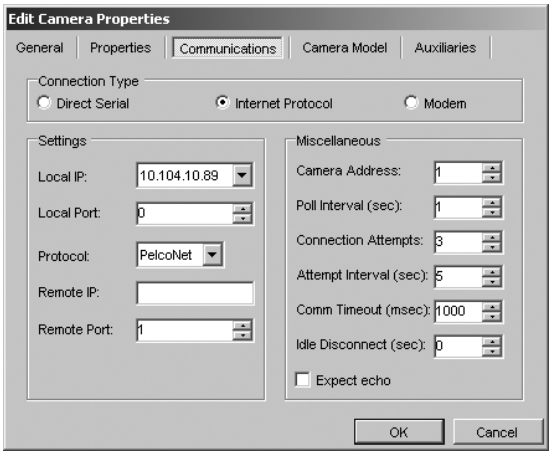


Figure 44. Communications Tab for PTZ Internet Settings

a. Local IP: The local IP is the IP address of the computer that the Pelco PTZ device driver runs on. Select the local IP from the drop-down box.

b. Local Port: The local port is the port the Pelco PTZ device driver uses to transmit commands. If your system is secured behind a firewall, enter one of the ports made available by the firewall. Otherwise, enter 0 to have the driver randomly assign an available port. Tip: To find out what port the driver assigned, switch or control the device in the VMX300(-E) client, and then use the netstat command at the DOS prompt to view assigned ports.

c. Remote IP, Remote Port, Protocol: The remote device is the device the Pelco PTZ camera is physically connected to. If the camera is connected to a PelcoNet device, follow the instructions in step (1). If the camera is connected to some other kind of device, follow the instructions in step (2).

(1) PelcoNet: Select the PelcoNet protocol from the Protocol drop-down box. If the PelcoNet device has a user name and password defined in the device settings, you will be prompted to enter the user name and password before proceeding. Enter the IP address of the PelcoNet device in the Remote IP box. In the Remote Port box, select the port on the PelcoNet device that the camera is connected to. Select 1 if the camera is connected to COM 1 on the PelcoNet device. Select 2 if the camera is connected to COM 2. This port must be exposed in the PelcoNet device properties configuration. For more information on configuring PelcoNet device properties, refer to the *Add a PelcoNet MPEG Device* section.

(2) Other: Select the desired transport protocol from the Protocol drop-down box. The remote IP is the IP address of the VMX300(-E) workstation the remote device's driver runs on. Enter the remote IP in the Remote IP box. In the Remote Port box, enter the port the remote device's driver uses to receive commands.

d. Refer to Step 3 for instructions on completing the fields in the Miscellaneous section.

3. **Miscellaneous:** Configure the following fields in the Miscellaneous section of the Communications tab:

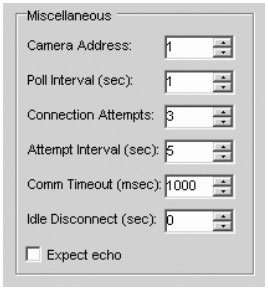


Figure 45. Miscellaneous Section of Communications Tab

Camera Address: Enter the camera address. The address must match the address specified by the camera DIP switch settings.

Poll Interval (sec): Applies to the Spectra III (D Protocol) only. The poll interval specifies how often the device driver attempts to query the camera for feedback on its position. This determines how often the positions of device icons in the client are updated. Feedback queries are suspended when the camera is being controlled. The optimal value of 1 is recommended.

Idle Disconnect (sec): (Optional) Enter the number of seconds of inactivity you want to elapse before VMX300(-E) closes the COM port (direct serial connection) or the local port (IP connection). The port will open again automatically when a new command is sent to the camera. Use the default value of 0 to indicate that the port should never be closed while the driver is running.

Note that the following fields should not be changed:

Connection Attempts: This field is used for troubleshooting and should specify the default value of 3.

Attempt Interval (sec): This field is used for troubleshooting and should specify the default value of 5.

Comm Timeout (msec): This field is used for troubleshooting and should specify the default value of 1000.

Expect echo: This field is reserved for future development.

CONFIGURE THE CAMERA MODEL TAB

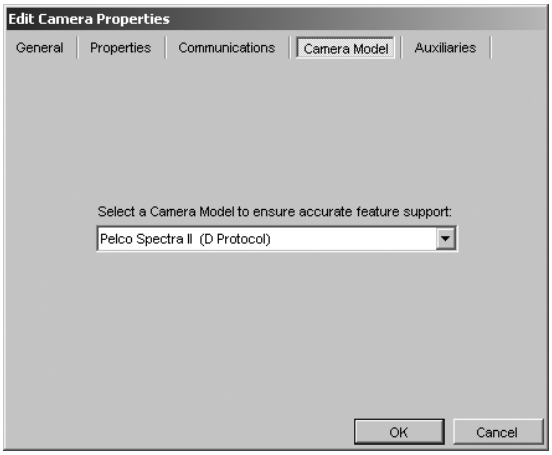


Figure 46. Camera Model Tab

Select the camera model and protocol from the drop-down box. Refer to the appropriate camera installation/operation manual for the recommended protocol.

CONFIGURE THE AUXILIARIES TAB

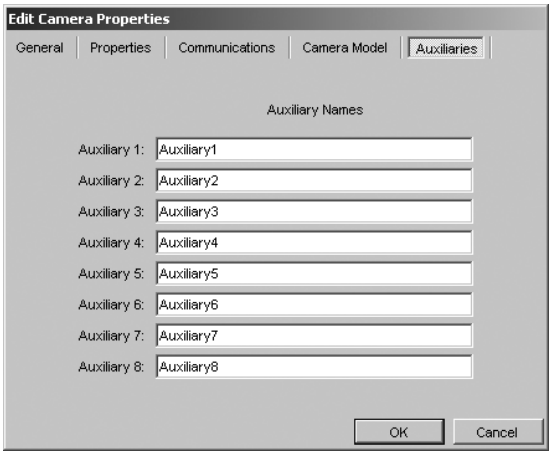


Figure 47. Auxiliaries Tab

The Auxiliaries tab allows you to give the camera's auxiliaries meaningful names. By default, auxiliaries are named Auxiliary***i***, where *i* is the auxiliary's number.

Auxiliary names appear in the VMX300(-E) client, where auxiliaries are controlled, and also appear in scripts, where they are used to refer to the auxiliary. When you rename an auxiliary, the write property for that auxiliary is changed to the name you have specified.

Example: you might rename an auxiliary that controls a camera's wiper to Wiper, then use it in a script as follows: SET Camera1. Wiper = On FOR 3.

To rename an auxiliary, position the cursor in the box for the auxiliary you want to rename and edit the name as desired. No two auxiliary names can be the same for a particular camera, but the same auxiliary name can be used for different cameras. Auxiliary names can be a maximum of 50 characters and can include any letter, digit, or special character, with the exception of single and double quotation marks. Auxiliary names are not case sensitive.

Refer to the appropriate camera installation/operation manual for information on connecting auxiliaries.

NOTE: Changing the name of an auxiliary that is referred to in a script introduces an error into the script. Refer to the *Scripts and Expressions* section for more information.

ADD A PELCONET MPEG DEVICE

The PelcoNet MPEG device driver currently supports the following devices:

- PelcoNet NET300 Series and NET350 Series decoders (denoted “3xx” in this document)
- PelcoNet NET300 Series and NET350 Series encoders (denoted “3xx” in this document)
- PelcoNet NET4001A encoder/decoder
- NVR300 Series network video recorders

The PelcoNet MPEG driver allows you to configure a time server for the driver to periodically synchronize its clock to. Refer to the *Device Drivers* section for information on configuring a time server.

Before you can add a device to the server configuration, you must first start the device driver—either on the server workstation or on the network—and then add the driver to the server configuration. Refer to the *Device Drivers* section for instructions.

1. Navigate the Object Browser tree to [project name] > Device Drivers > PelcoNet MPEG Driver > [PelcoNet device].
2. Double-click <Add New Device>. The Add New PelcoNet dialog box appears.

   To configure PelcoNet settings after you have added the device to the server configuration right-click the device, and then select Edit from the pop-up menu. The Edit Properties dialog box appears, which contains the same tabs and fields as the Add New PelcoNet dialog box.
3. Configure the device settings, as described in the following sections. You must configure the PelcoNet settings in VMX300(-E) to match the PelcoNet device’s internal settings. For example, the Motion read property works only if motion detection is turned on in the device. Refer to the appropriate PelcoNet device installation/operation manual for information on internal device settings.
4. Click OK to close the Add New Device dialog box.
5. Configure the analog connections between the PelcoNet and other devices in the system. Refer to the *Connections* section.

CONFIGURE THE GENERAL TAB

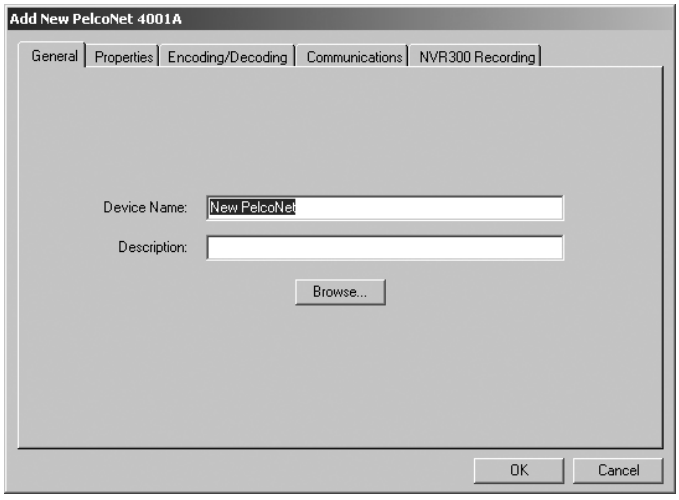


Figure 48. General Tab for PelcoNet Device

1. You can either enter a device name or click Browse to browse for existing PelcoNet devices. The name can be a maximum of 50 characters and can include any letter, digit, or special character, with the exception of single and double quotation marks. Device names are not case sensitive.

   If you click Browse, the Browse Units dialog box appears. Click a device in the list of units, and then click OK. The device name and description are uploaded from the PelcoNet device, along with the unit IP address and multicast settings, overwriting any current settings. The Unit IP Address is set on the Communications tab. Multicast settings are on the Encoding or Encoding/Decoding tab.

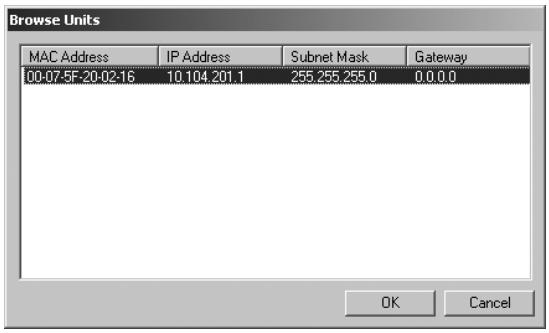


Figure 49. Browse Units Dialog Box

2. Optional: Type a description of the device.

CONFIGURE THE PROPERTIES TAB

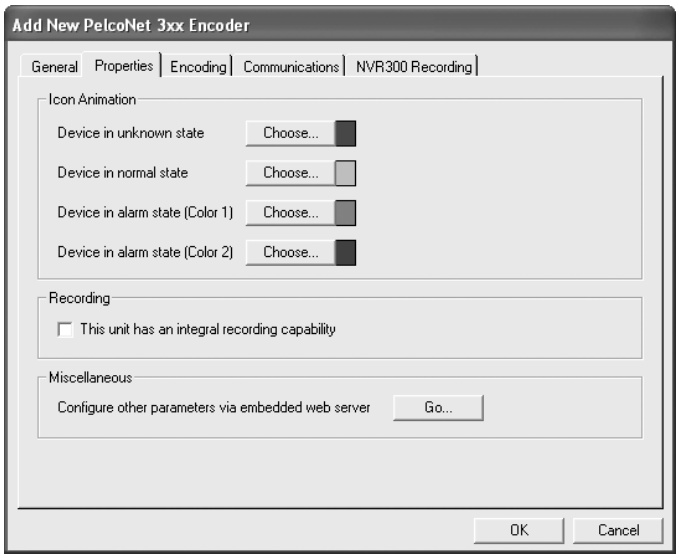


Figure 50. Properties Tab for PelcoNet Device

Icon Animation

Use this portion of the Properties tab to configure the animation settings of PelcoNet device icons viewed on maps in the VMX300(-E) client. Click Choose next to each condition to select the color settings for that condition. Note that you can configure a different color setting for each device.

Unknown state: When the device's Status property equals Commloss or Unknown, device icons in the client are the color specified here.

Normal state: When the device's Status property equals Normal, device icons in the client are the color specified here.

Alarm state: When the device's Status property equals CommonAlarm, the icon flashes alternately between Color 1 and Color 2. Note, however, that flashing icons can increase the CPU workload. To reduce the overall workload, set Color 1 and Color 2 to the same color.

Recording

This portion of the Properties tab applies to PelcoNet NET350 encoders only. If the PelcoNet device has built-in ability to record audio and video, click "This unit has an integral recording capability."

To use the recording feature you must set the PelcoNet device's time zone and clock to ensure that you can locate video archived using the integral recording capability. Note the following parameters:

- **Time zone:** Set the time zone on the PelcoNet device to the time zone where the PelcoNet device is installed.
- **Clock:** Set the clock on the PelcoNet device to the local time where the PelcoNet device is installed, without compensating for Daylight Saving Time (DST). If you set the PelcoNet's clock when DST is in effect (during the summer), set the clock one hour behind DST.

Refer to the appropriate PelcoNet manual for instructions on setting the device's time zone and clock.

RECORDING NOTES:

- To display internally-archived video in a custom window, the window's canvas must be configured to display the Internal Storage signal type. For instructions on configuring the canvas, refer to the *Canvases* section.
- When integral recording capability is selected, the PelcoNet_HDD property becomes available for use in scripts and expressions. Refer to the *Scripts and Expressions* section for more information.

Miscellaneous

Use this portion of the Properties tab to configure the PelcoNet device's internal settings.

1. Click Go. The PelcoNet Device Control window appears.

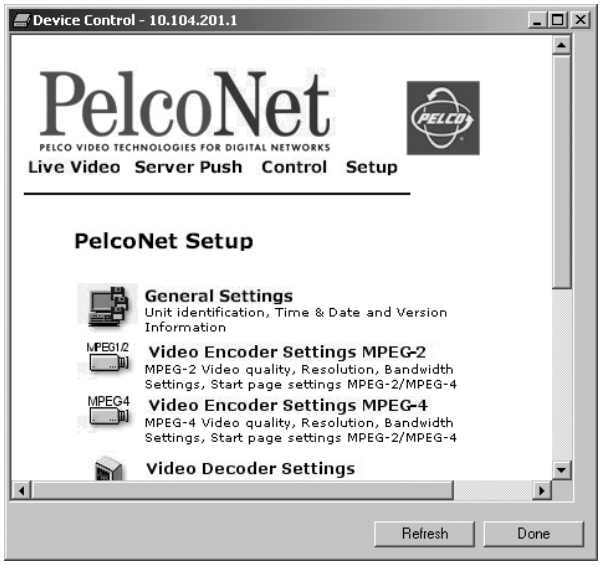


Figure 51. PelcoNet Device Control Window

2. Configure the PelcoNet device's internal settings as necessary. When you have finished, click Done to close the window. Refer to the appropriate PelcoNet manual for information on the device's internal settings.

CONFIGURE THE ENCODING TAB

This tab is available only on encoder units.

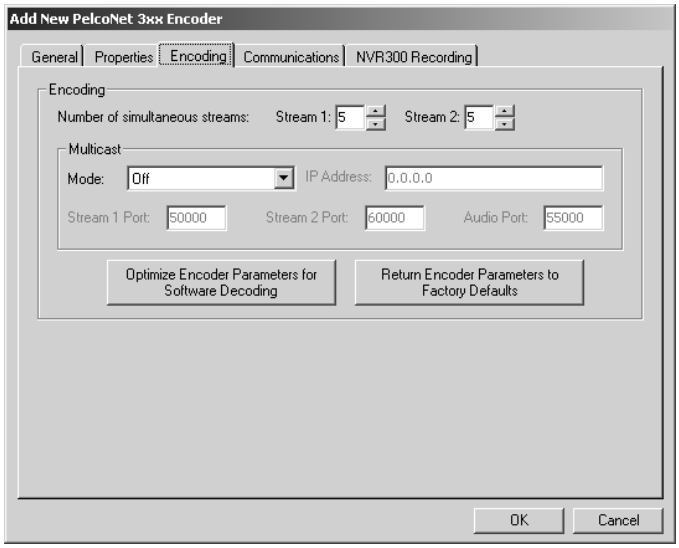


Figure 52. Encoding Tab for PelcoNet Device

PelcoNet 3xx encoders support dual MPEG-4 streams that can be configured to different quality settings. Typically, one stream is configured for viewing video, the other for recording. For information on configuring the streams, refer to the appropriate PelcoNet manual.

Number of Simultaneous Streams

VMX300(-E) can display multiple digital video windows for viewing the area under surveillance. However, the number of digital windows that can be displayed at one time is limited by the size and type of images selected for viewing. Refer to Table B for an overview of the CPU workload and bandwidth amounts used for each type of video stream (the video in a custom window). This table also includes a recommended maximum number of streams for each type.

Stream 1: Enter the maximum number of MPEG-4 primary streams you want the encoder to transmit at one time in the Stream 1 field. The default setting is the maximum number of MPEG-4 streams the encoder is capable of transmitting (without multicasting). To limit bandwidth utilization, reduce the setting below the maximum.To display Stream 1 in a custom window, the window's canvas must be configured to display the MPEG-4 signal type.

Stream 2: Enter the maximum number of MPEG-4 secondary streams you want the encoder to transmit at one time in the Stream 2 field. The default setting is the maximum number of MPEG-4 streams the encoder is capable of transmitting (without multicasting). To limit bandwidth utilization, reduce the setting below the maximum.To display Stream 2 in a custom window, the window's canvas must be configured to display the MPEG-4 Secondary signal type.

NOTE: If a NVR300 Series network video recorder is being used to record video from this encoder, you should subtract a stream from the total number of streams entered on the Encoding tab. For example, if you would normally transmit one primary stream and five secondary streams, and you record the secondary stream, then you should enter 1 in the Stream 1 field and 4 in the Stream 2 field.

For instructions on configuring the a canvas to display MPEG-4 steams, refer to *Add a New Canvas (PelcoNet)*.

Multicast

This feature is available only if your network supports IP multicasting.

To configure multicast settings through VMX300(-E), complete the following steps:

1. Click the Mode field, and then select the type of stream you want the encoder to multicast from the drop-down box.
2. Enter the IP multicast group address.
3. If the encoder is configured to multicast one or more MPEG-4 streams, enter the IP multicast group MPEG-4 port(s) in the Stream Port fields.
4. If the encoder is configured to multicast one or more MPEG-4 streams, enter the IP multicast group audio port.

If the encoder is connected when you configure the settings in VMX300(-E), the settings are updated in the encoder immediately. Otherwise, updating occurs once the encoder is connected.

To configure multicast settings through the encoder, complete the following steps:

1. Configure the encoder's internal multicast settings; refer to the appropriate PelcoNet manual for instructions.
2. In VMX300(-E) click Upload Settings on the Communications tab. Refer to the *Configure the Communications Tab* section.

Encoder Parameters

VMX300(-E) provides the option to quickly configure the internal MPEG-4 settings of the PelcoNet device for either lower frame rate settings, which have been designed to work well with VMX300(-E), or the factory default settings.

NOTE: If the video stream is being recorded by either an NVR or the PelcoNet integral recording feature, these encoder parameter changes will not take effect. Wait until the video stream recording is complete, and then click the appropriate button.

Selecting Lower Frame Rate Settings

1. To select lower frame rate settings, click Optimize Encoder Parameters for Software Decoding. The Software Defaults message appears.

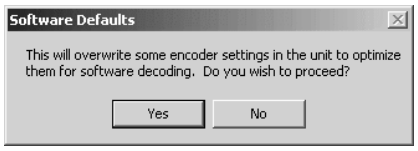


Figure 53. Software Defaults Message

2. Click Yes. The MPEG-4 configuration on the PelcoNet device is changed to the following settings:

   Stream 1: VMX High Quality

   Stream 2: VMX Standard Quality

3. (Optional) To change individual settings, click Go on the Properties tab to display the PelcoNet Device Control window.

Restoring Factory Default Settings

1. To select factory default settings, click Return Encoder Parameters to Factory Defaults. The Factory Defaults message appears.

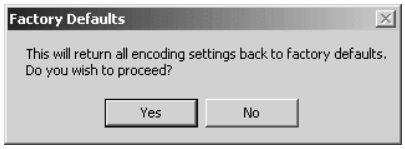


Figure 54. Factory Defaults Message

2. Click Yes. The MPEG-4 configuration on the PelcoNet device is changed to the factory default settings.
3. (Optional) To change individual settings, click Go on the Properties tab to display the PelcoNet Device Control window.

The factory default settings provide higher frame rate settings for connections with high bandwidth, based on parameter preset 1. Refer to the appropriate PelcoNet manual for detailed information.

HOW TO CHOOSE THE VIDEO STREAM SETTINGS FOR YOUR CONFIGURATION

VMX300(-E) can combine analog and digital video streams for viewing on the VMX300(-E) client. The total number of digital streams that can be displayed is limited by the size and type of images selected for viewing. Table B identifies the CPU workload and bandwidth amounts used for each type of video stream.

Table B includes the recommended PelcoNet setting, identified by the gray row. Your selections may vary, depending on system bandwidth limitations or other restrictions.

⚠ **CAUTION:** System performance will be compromised if the number of video streams is exceeded or if the PelcoNet settings exceed the recommendation provided in Table B.

Also note that CPU workload could vary, depending on additional system activity that may be occurring at the same time. For example, using scripts, viewing analog video, or using hyperlinks to change map displays could all affect the CPU workload. It is recommended that you monitor the CPU workload level under a variety of system conditions while testing your system configuration to identify the optimal number of digital video windows allowed for your configuration.

Note that if the VMX300(-E) client is operated from a separate workstation (instead of the same workstation running the VMX300(-E) server), then you may be able to display more digital windows, since the VMX300(-E) client would not be using the VMX300(-E) server's CPU.

A NOTE ABOUT MULTIPLE CLIENTS: If your system requires only one client, the client and server applications can both run on the same workstation. To optimize system performance in a multiple-client system, each client application should run from a dedicated client workstation. Additional servers in the same system (VMX300-E only) should be run from dedicated server workstations as well.

Table B. Digital Video Stream Settings

Settings	Maximum Number of Streams
PelcoNet NET300 Series and NET350 Series Transmission Systems	
VMX High Quality (Stream 1) ["Optimize" setting]	16
VMX Standard Quality (Stream 2) ["Optimize" setting]	16
High Quality (CIF) [Factory default setting]	4
DX9000 Series Digital Video Recorders	
Half Frame Rate	
Live Video	16
Archived Video	16
Full Frame Rate	
Live Video	16
Archived Video	16
PelcoNet NET 4001A Transmission System	
MPEG4	
High Quality (CIF) [Factory default setting]	12
VMX Standard ["Optimize" setting]	16
MPEG2	
5 MBps High Quality [Factory default setting]	5
2 MBps Low Delay ["Optimize" setting]	5
DX8000 Series Digital Video Recorders	
320x240 5 IPS ["Normal" image quality setting]	16
740x480 30 IPS ["Normal" image quality setting]	3 (or 6, if using two DX8000 units)
640x480 10 IPS ["Normal" image quality setting]	16

CONFIGURE THE ENCODING/DECODING TAB (PELCONET 4001A ONLY)

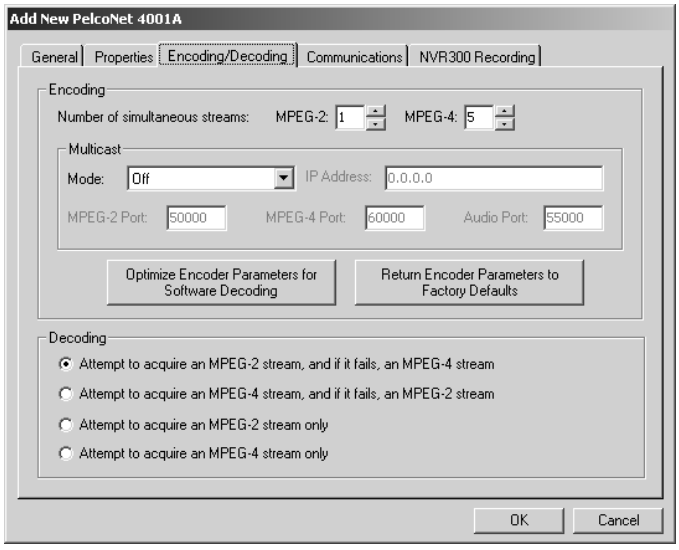


Figure 55. Encoding/Decoding Tab for PelcoNet 4001A

The PelcoNet 4001A supports MPEG-2 and MPEG-4 streaming.

Number of Simultaneous Streams

VMX300(-E) can display multiple digital video windows for viewing the area under surveillance. However, the number of digital windows that can be displayed at one time is limited by the size and type of images selected for viewing. Refer to Table B for an overview of the CPU workload and bandwidth amounts used for each type of vide stream (the video in a custom window). This table also includes a recommended maximum number of streams for each type.

MPEG-2: Enter the maximum number of MPEG-2 streams you want the encoder/decoder to transmit at one time. The default setting is the maximum number of MPEG-2 streams the encoder/decoder is capable of transmitting (without multicasting). In order to display MPEG-2 streams in a custom window, the window's canvas must be configured to display the MPEG-2 signal type.

MPEG-4: Enter the maximum number of MPEG-4 streams you want the encoder/decoder to transmit at one time. The default setting is the maximum number of MPEG-4 streams the encoder/decoder is capable of transmitting (without multicasting). To limit bandwidth usage, reduce this setting below the maximum capacity. In order to display MPEG-4 streams in a custom window, the window's canvas must be configured to display the MPEG-4 signal type.

NOTE: If a NVR300 Series network video recorder is being used to record video from this encoder/decoder, you should subtract a stream from the total number of streams entered on the Encoding/Decoding tab. For example, if you would normally transmit one MPEG-2 stream and five MPEG-4 streams, and you record the MPEG-4 stream, then you should enter 1 in the MPEG-2 field and 5 in the MPEG-4 field.

For instructions on configuring a canvas to display MPEG-2 and MPEG-4 steams, refer to *Add a New Canvas (PelcoNet)*.

Multicast

This feature is available only if your network supports IP multicasting.

To configure multicast settings through VMX300(-E), complete the following steps:

1. Click the Mode field, and then select the type of stream you want the encoder/decoder to multicast from the drop-down box. If your selection includes MPEG-2, the "Number of simultaneous streams" MPEG-2 field is automatically set to 999 If your selection includes MPEG-4, the "Number of simultaneous streams" MPEG-4 field is automatically set to 999. This allows an almost unlimited number of simultaneous recipients of the stream.
2. Enter the IP multicast group address.
3. If the encoder/decoder is configured to multicast MPEG-2 streams, enter the IP multicast group MPEG-2 port in the MPEG-2 Port field. If the encoder/decoder is connected, the MPEG-2 port number is automatically uploaded from the encoder/decoder when you select the mode.

4. If the encoder/decoder is configured to multicast MPEG-4 streams, configure the following settings:
   - Enter the IP multicast group MPEG-4 port in the MPEG-4 Port field.
   - Enter the IP multicast group audio port in the Audio Port field.

   If the encoder/decoder is connected, these port numbers are automatically uploaded from the encoder/decoder when you select the mode.

If the encoder/decoder is connected when you configure the settings in VMX300(-E), the settings are updated in the encoder/decoder immediately. Otherwise, updating occurs once the encoder/decoder is connected.

To configure multicast settings through the encoder/decoder, complete the following steps:

1. Configure the encoder/decoder's internal multicast settings; refer to the appropriate PelcoNet manual for instructions.
2. In VMX300(-E) click Upload Settings on the Communications tab. Refer to the *Configure the Communications Tab* section.

Decoding

Select the stream(s) you want the encoder/decoder to receive. For information on configuring the streams, refer to the appropriate PelcoNet manual. If the MPEG-2 and MPEG-4 streams will be displayed in a custom window, the window's canvas must be configured to display the MPEG-2 and MPEG-4 signal types. For instructions on configuring the canvas, refer to *Canvases*.

Encoder Parameters

VMX300(-E) provides the option to quickly configure the internal MPEG-4 settings of the PelcoNet device for either lower frame rate settings, which have been designed to work well with VMX300(-E), or the factory default settings.

NOTE: If the video stream is being recorded by an NVR, these encoder parameter changes will not take effect. Wait until the video stream recording is complete, and then click the appropriate button.

Selecting Lower Frame Rate Settings

1. To select lower frame rate settings, click Optimize Encoder Parameters for Software Decoding. The Software Defaults message appears.

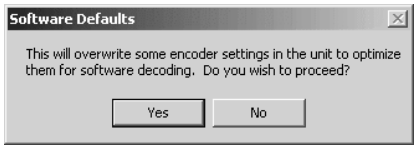


Figure 56. Software Defaults Message

2. Click Yes. The MPEG-4 configuration on the PelcoNet device is changed to the following settings:

   MPEG-2: 2MBPS Low Delay

   MPEG-4: VMX Standard Quality

3. (Optional) To change individual settings, click Go on the Properties tab to display the PelcoNet Device Control window.

Restoring Factory Default Settings

1. To select factory default settings, click Return Encoder Parameters to Factory Defaults. The Factory Defaults message appears.

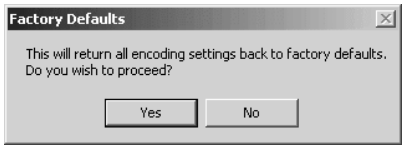


Figure 57. Factory Defaults Message

2. Click Yes. The MPEG-4 configuration on the PelcoNet device is changed to the factory default settings.
3. If necessary, you can change one or more individual settings, in order to customize your system.

The factory default settings provide higher frame rate settings for connections with high bandwidth, based on parameter preset 1. Refer to the appropriate PelcoNet manual for detailed information.

CONFIGURE THE COMMUNICATIONS TAB

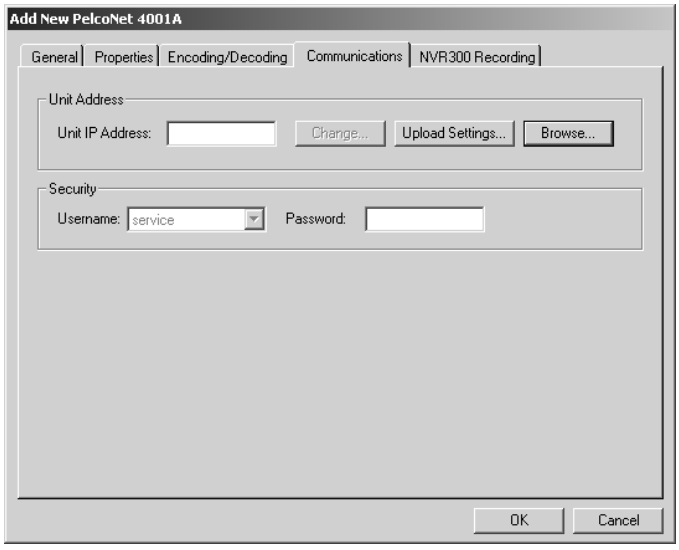


Figure 58. Communications Tab for PelcoNet Device

Unit Address

To add a PelcoNet device, complete the following steps:

1. You can either enter the IP address of the PelcoNet device you are configuring or click Browse. The address in VMX300(-E) is synchronized with the address in the PelcoNet device. Changing the address in VMX300(-E) also changes the address in the device.

   If you click Browse to automatically locate PelcoNet devices that are visible over the network, the Browse Units dialog box appears. Click a device in the list, and then click OK. The IP address of the selected device is uploaded from the PelcoNet device, along with the device name, description, and multicast settings. The uploaded settings will overwrite any existing settings in VMX300(-E).

2. Optional: If the settings in the PelcoNet device have already been configured, click Upload Settings to upload the device name, description, and multicast settings from the device. If the device is not connected when you Upload Settings, the settings are automatically uploaded once the device is connected.

Device name and description are located on the General tab. Multicast settings are on the Encoding tab for encoders, and the Encoding/Decoding tab for encoder/decoders.

To change the address of a PelcoNet device, complete the following steps:

NOTE: The Change feature is becomes available once the IP address in VMX300(-E) has been synchronized with the IP address in the device. Using the Browse option on the Communications tab or on the General tab makes the Change option available.

1. Click Change. The Set New Address dialog box appears.

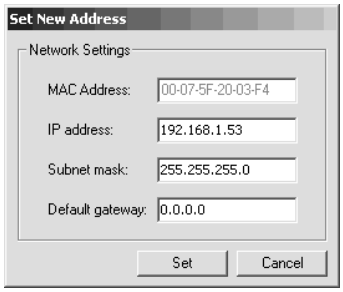


Figure 59. Set New Address Dialog Box

2. Edit the IP address, subnet mask, and gateway as necessary, and then click Set to close the dialog box. The new IP address appear in the Unit IP Address box. The address, mask and gateway settings are downloaded to the PelcoNet device.

Security

The upload features only work on a password-protected device if the password is entered here. You only need to enter the password once in VMX300(-E). Once the password is entered, the upload features can be used freely during the current and future sessions.

Note the following password parameters:

- If a Live or User password is configured in the PelcoNet device-internal settings, enter a password of your choice on the Communications tab.
- If a Service password is configured in the device settings, enter the same password on the Communications tab as is defined in the device-internal settings.

The following upload features are affected by password protection:

- Browse: Located on the General tab and the Communications tab.
- Upload Settings: Located on the Communications tab.
- Autodiscover Devices: Located in the Object Browser in server configuration mode.

NOTE: Since the PelcoNet MPEG driver operates under the Service level of security, the username appears as service by default and cannot be changed.

CONFIGURE THE NVR300 RECORDING TAB

This applies to encoders and encoder/decoders only.

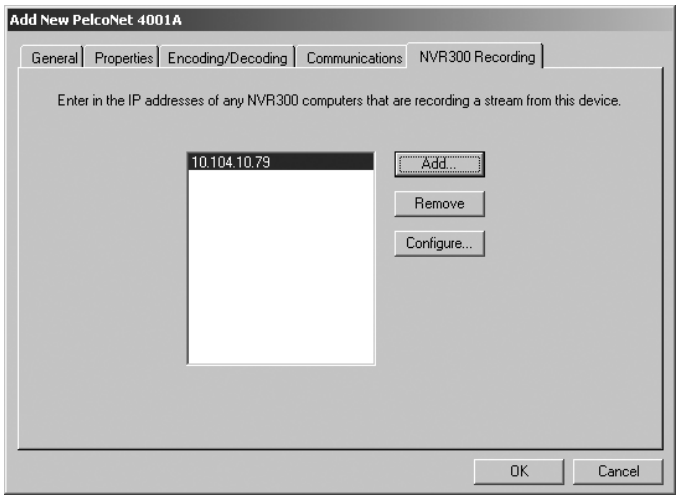


Figure 60. NVR300 Recording Tab

Pelco NVR300 Series network video recorders are used to record streams encoded by the PelcoNet device. When you add an NVR to the VMX300(-E) configuration, the following functionality becomes available:

- A camera connected to the PelcoNet device is enabled as an archive video source. An operator can then view video from the PelcoNet camera that has been archived through the NVR.
- The NVR300_IP signal source property becomes available for that NVR. Refer to *PelcoNet Device Properties Exposed for Scripts and Expressions* for more information.

Note that you must set up and configure the NVR for recording. Refer to the Pelco NVR300 documentation for instructions on working with the NVR300. You can also click the Configure button on the NVR300 recording tab to access the NVR configuration application.

Complete the following steps to add an NVR300 to the list of network video recorders:

1. Click Add. The Add NVR dialog box appears.

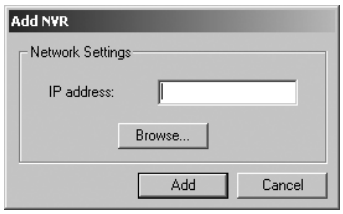


Figure 61. Add NVR Dialog Box

2. You can either enter the IP address of the NVR you want to add or click Browse.

   If you click Browse to automatically locate the NVR300s that are visible over the network the Browse Units dialog box appears. Click the desired NVR, and then click OK.

   Note that the Browse function will not locate NVRs running on the same computer as any VMX300(-E) software (server, client, or device drivers).

3. Click Add. The Add NVR dialog box closes and the selected NVR's IP address is added to the list.

   The NVR300 is now available in the VMX300(-E) client as an archive source. To view archived PelcoNet video from this NVR, you must configure the NVR to record this specific PelcoNet device. Refer to step 6.

4. (Optional) Add another NVR. To add another NVR300 to the list, repeat step 3.

   If you add more than one NVR300 device to this list, and if each NVR has been configured to record video from this specific PelcoNet device, they will simultaneously record the PelcoNet streams from this device, resulting in duplicate recordings. This could create bandwidth issues, depending on your system settings.

5. (Optional) Remove an NVR: Click the NVR, and then click Remove. The selected NVR will disappear from the list and the recorded video from that NVR will no longer be available through the VMX300(-E) client.

   To change the recording status for this PelcoNet device, you must change the NVR configuration. Refer to step 6.

6. (Optional) Access the NVR configuration application: Click Configure to configure the NVR300's internal settings through the embedded web server. Refer to the PelcoNet NVR300 documentation for more information on the NVR's internal settings.

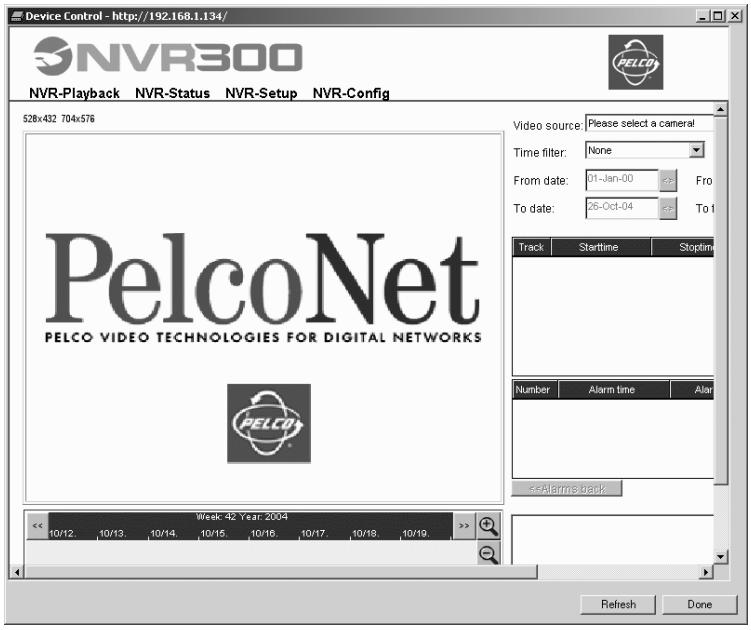


Figure 62. Embedded NVR300 Web Server

NOTE: To ensure that you can play an NVR300 recording through the VMX300(-E), make sure that the date, time, and time zone settings on the VMX300(-E) match those of the NVR300. To configure these settings on the NVR300, go to the Date and Time Properties dialog box, and refer to the NVR300 Network Video Recorder Installation/Operation manual.

ADD AN EXTERNAL MONITOR DEVICE

The external monitor device driver supports any noncontrollable video destination, such as a noncontrollable monitor.

Before you can add a device to the server configuration, you must first start the device driver—either on the server workstation or on the network—and then add the driver to the server configuration. Refer to the *Device Drivers* section for instructions.

1. Navigate the Object Browser tree to [project name] > Device Drivers > External Monitor > Devices.
2. Double-click <Add New Device>. The Add New External Monitor dialog box appears.

   You can also configure settings after you have added the monitor to the server configuration. Right-click the monitor, and then select Edit from the pop-up menu. The Edit Properties dialog box appears, which contains the same tabs and fields as the Add New External Monitor dialog box.
3. Configure the monitor settings, as described in the following sections.
4. Click OK to close the Add New Device dialog box.

CONFIGURE THE GENERAL TAB

Figure 63. General Tab for External Monitor

Use the General tab to enter a location name and an optional description. The location name is used to identify the device. The location name can be a maximum of 50 characters and can include any letter, digit, or special character, with the exception of single and double quotation marks. Location names are not case sensitive.

CONFIGURE THE PROPERTIES TAB

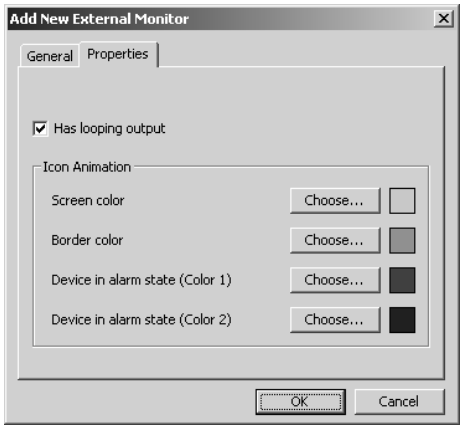


Figure 64. Properties Tab for External Monitor

Looping output on an external monitor device allows the device to function as a source device. Refer to *Devices - Switching a Device* in the VMX300(-E) Client Manual for information on source and destination devices. To enable looping output complete the following steps:

1. Click Looping Output.
2. Add an analog video connection to the server configuration for this device. Refer to the *Connections* section for information on analog video connections.

Use the icon animation portion of the Properties tab to configure the animation settings of external monitor icons viewed on maps in the VMX300(-E) client. Click Choose next to each condition to select the color settings for that condition. Note that you can configure a different color setting for each monitor.

Screen color: When the device's Alarm property equals False, device icons in the client display a monitor screen in the color specified here. Each external monitor device can use a different screen color for its icons.

Border color: When the device's Alarm property equals False, device icons in the client display a border in the color specified here. Each external monitor device can use a different border color for its icons.

Alarm state: When the monitor's Alarm property equals True, the icon flashes alternately between Color 1 and Color 2. Note, however, that flashing icons can increase the CPU workload. To reduce the overall workload, set Color 1 and Color 2 to the same color.

ADD A DX8000 DVR

The DX8000 device driver controls Pelco DX8000 Series digital video recorders (DVRs). In this document, the term "DX8000 DVR" is used to refer to any DVR in the DX8000 series that is supported by the DX8000 driver. Note that the VMX300(-E) supports DX8000 software version level 1.1.00.1121 only.

A DX8000 DVR is a specialized PC that runs the Windows operating system. If your system has more than one DX8000 DVR, each one must be configured.

PREPARING TO CONFIGURE THE DX8000 DVR

DX8000 recorders are password-protected. To access a DX8000 recorder, each client workstation and the DX8000 driver must have an account defined in the Power User group on the recorder. For information on setting up Power User accounts, refer to the DX8000 documentation.

Add Accounts to the Power User Group for Client Workstations

For each client workstation that will retrieve video from the recorder, add a Power User account with the following settings:

- **USER NAME:** The user name must be the computer name of the client workstation. The user name is at least 4 characters in length, and is case sensitive. If the computer name is less than 4 characters in length, change the computer name to a name that is 4 or more characters long, or you will not be able to use the computer to access video from a DX8000 recorder.
- **PASSWORD:** Each client workstation account and the device driver account must all use the same password. The password must be 6 - 11 characters in length. The password is case sensitive.

Add an Account to the Power User Group for the Device Driver

Add a Power User account for the DX8000 driver:

- **USER NAME:** Define a user name of your choosing. The user name is at least 4 characters in length, and is case sensitive. Do not use the name of any computer visible over the network, as computer names are reserved for client accounts. Enter the user name on the Communications tab when you configure the DX8000 recorder, as described in the *Configure the Communications Tab* section.
- **PASSWORD:** The password for the device driver account must be the same as the password for the client workstations accounts. The password must be 6 - 11 characters in length. The password is case sensitive. Enter the password on the Communications tab when you configure the DX8000 driver as described in the *Configure the Communications Tab* section.

ADD A DX8000 DVR TO THE SERVER CONFIGURATION

Before you can add a device to the server configuration, you must first start the device driver—either on the server workstation or on the network—and then add the driver to the server configuration. Refer to the *Device Drivers* section for instructions.

NOTE: When starting the DX8000 driver, click "Start the driver as an executable." The option to run the DX8000 driver as a service is reserved for future use.

1. Navigate the Object Browser tree to [project name] > Device Drivers > Pelco DX8000 Driver > Recorders.
2. Double-click <Add New Device>. The Add New DX8000 dialog box appears.

   You can also configure DX8000 settings after you have added the DVR to the server configuration. Right-click the DX8000 recorder, and then select Edit from the pop-up menu. The Edit Properties dialog box appears, which contains the same tabs and fields as the Add New DX8000 dialog box.
3. Configure the DX8000 settings, as described in the following sections. Note that you must configure the settings in VMX300(-E) to match the DVR settings configured through the software provided with the DVR. Refer to the appropriate DVR installation/operation manual for information on internal DVR settings.
4. Click OK to close the Add New Device dialog box.
5. (Optional) If you want to control cameras through the recorder, add each camera to the server configuration. Refer to the *Add a DX8000 Camera* section.
6. Configure the analog connections between the recorder, cameras, and output devices. Refer to the *DVR Connections* section.

CONFIGURE THE GENERAL TAB

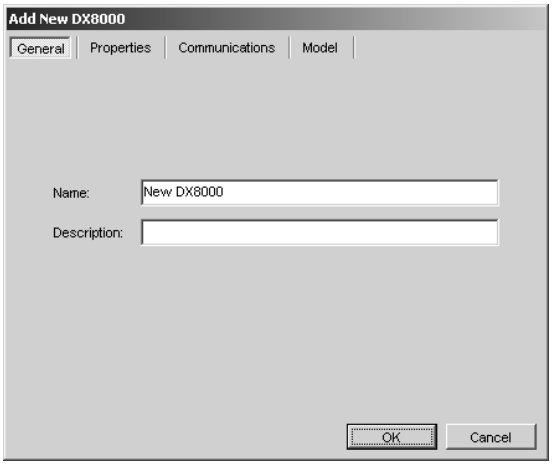


Figure 65. General Tab for DX8000 DVR

Use the General tab to name and describe the DVR. The device name can be a maximum of 50 characters. You cannot use single or double quotation marks in a name, but you can use any other letter, digit, or special character. Device names are not case sensitive. The optional description appears in the Object Browser beside the device name.

CONFIGURE THE PROPERTIES TAB

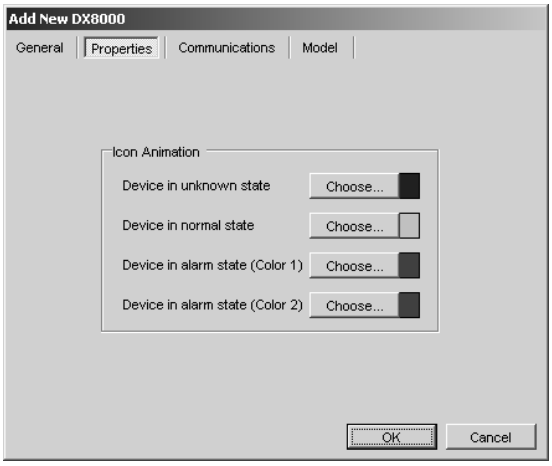


Figure 66. Properties Tab for DX8000 DVR

Use the Properties tab to configure the animation settings of DX8000 icons viewed on maps in the VMX300(-E) client. Click Choose next to each condition to select the color settings for that condition. Note that you can configure a different color setting for each recorder.

Unknown state: When the recorder's CommStatus property equals Offline, device icons in the client are the color specified here.

Normal state: When the recorder's CommStatus property equals Online, device icons in the client are the color specified here.

Alarm state: When the recorder's Alarm write property equals True, the icon changes to the color specified here. If you change either Color 1 or Color 2, then the icon flashes alternately between the two colors when the recorder is in the alarm state. Note, however, that flashing icons can increase the CPU workload.

CONFIGURE THE COMMUNICATIONS TAB

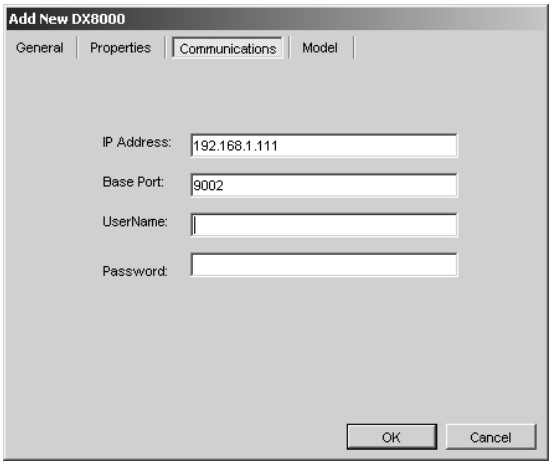


Figure 67. Communications Tab for DX8000 DVR

1. IP Address: Type the recorder's IP address.
2. Base Port: Type the recorder's listening port.
3. UserName: Type the user name that the device driver will use to access the recorder. This must be the same as the user name defined for the device driver's Power User account, described in the *Add an Account to the Power User Group for the Device Driver* section.
4. Password: Type the password that the device driver will use to access the recorder. This must be the same as the password defined for the the device driver's Power User account, described in the *Add an Account to the Power User Group for the Device Driver* section.

CONFIGURE THE MODEL TAB

Figure 68. Model Tab for DX8000 DVR

1. Select the recorder model from the drop-down box.
2. (Optional) Click “Looping Inputs” to make the recorder’s looping inputs appear as sources for connections.

ADD A DX8000 CAMERA

If you will be controlling cameras through the DVR, add each camera to the VMX300(-E) server configuration and configure the camera settings within VMX300(-E), as described in this section.

Before you can add a DX8000 camera to the server configuration, you must first start the DX8000 device driver—either on the server workstation or on the network—and then add the driver to the server configuration. Refer to the *Device Drivers* section for instructions.

1. Navigate the Object Browser tree to [project name] > Device Drivers > DX8000 Driver > Cameras.
2. Double-click <Add New Device>. The Add New Camera dialog box appears.

   You can also configure DX8000 camera settings after you have added the cameras to the server configuration. Right-click the DX8000 camera, and then select Edit from the pop-up menu. The Edit Properties dialog box appears, which contains the same tabs and fields as the Add New Camera dialog box.
3. Configure the camera settings, as described in the following sections.
4. Click OK to close the Add New Device dialog box.
5. Configure the analog connections between the DVR, cameras, and output devices. Refer to the *DVR Connections* section.

CONFIGURE THE GENERAL TAB

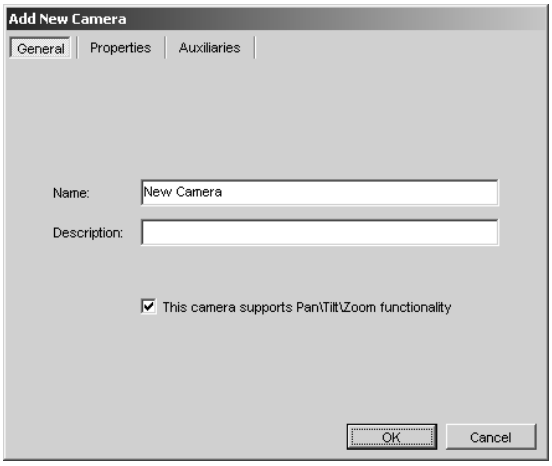


Figure 69. General Tab for DX8000 Camera

1. Use the General tab to name and describe the camera. The device name can be a maximum of 50 characters. You cannot use single or double quotation marks in a name, but you can use any other letter, digit, or special character. Device names are not case sensitive. The optional description appears in the Object Browser beside the device name.
2. If the camera can be panned, tilted, zoomed, focused or the iris adjusted, click “This camera supports Pan/Tilt/Zoom functionality.” If the camera is fixed, leave this box unchecked.

CONFIGURE THE PROPERTIES TAB

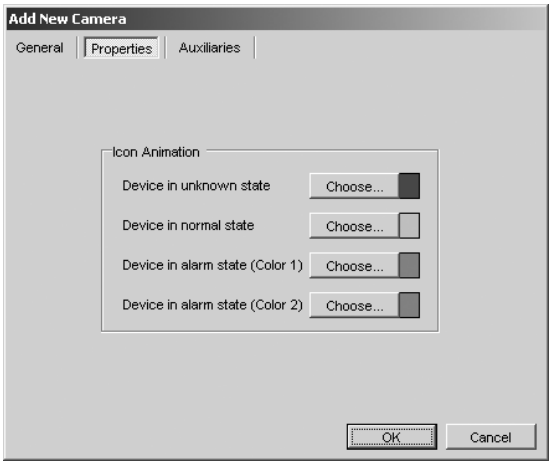


Figure 70. Properties Tab for DX8000 Camera

Use the Properties tab to configure the animation settings of the DX8000 camera icon viewed on maps in the VMX300(-E) client. Click Choose next to each condition to select the color settings for that condition. Note that you can configure a different color setting for each camera.

Unknown state: When the camera is not communicating normally with the recorder, the icon is the color specified here.

Normal state: When the camera is communicating normally with the recorder, the icon is the color specified here.

Alarm state: When the camera's Alarm write property equals True, the icon changes to the color specified here. If you change either Color 1 or Color 2, then the icon flashes alternately between the two colors when the camera is in the alarm state. Note, however, that flashing icons can increase the CPU workload.

CONFIGURE THE AUXILIARIES TAB

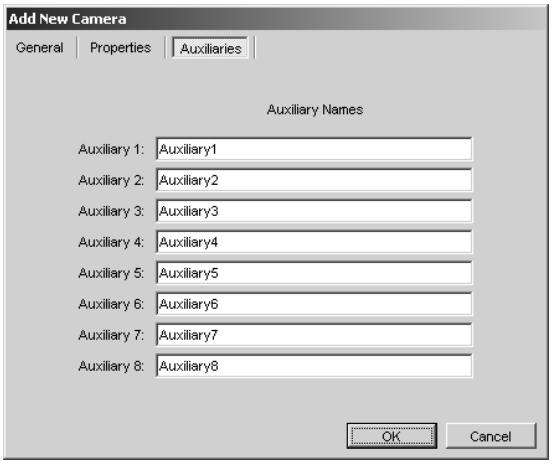


Figure 71. Auxiliaries Tab for DX8000 Camera

Auxiliary names appear in the VMX300(-E) client, where auxiliaries are controlled, and also appear in scripts, where they are used to refer to the auxiliary. When you rename an auxiliary, the write property for that auxiliary is changed to the name you have specified.

> **Example:** You might rename an auxiliary that controls a camera's wiper to "Wiper," and then use it in a script as follows:
> SET Camera1.Wiper = On FOR 3.

To rename an auxiliary, click the box next to the auxiliary you want to rename, and then type the new name. No two auxiliary names can be the same for a particular camera, but the same auxiliary name can be used for different cameras. Auxiliary names can include any letter, digit, or special character, with the exception of single and double quotation marks. Auxiliary names are not case sensitive.

Note that the VMX300(-E) supports up to eight auxiliaries. The actual number of auxiliaries available to you depends on the number of auxiliaries the camera supports. If the camera has fewer than eight auxiliaries, for example six auxiliaries, then only the first six auxiliaries on the Auxiliaries tab will work. If the camera supports more than eight auxiliaries, then you can only access the first eight auxiliaries through the Auxiliaries tab.

Refer to the appropriate camera installation/operation manual for information on connecting auxiliaries.

NOTE: Changing the name of an auxiliary that is referred to in a script introduces an error into the script. Refer to the *Scripts and Expressions* section for more information.

ADD A DX9000 DVR

The DX9000 device driver controls Pelco DX9000 Series digital video recorders (DVRs). In this document, the term "DX9000 DVR" is used to refer to any DVR in the DX9000 series that is supported by the DX9000 driver.

A DX9000 DVR is a specialized PC that runs the Windows operating system. If your system has more than one DX9000 DVR, each one must be configured.

PREPARING TO CONFIGURE THE DX9000 DVR

Before you can configure the DX9000 DVR in VMX300(-E), you must complete the following tasks:

- Add users to the Windows group called Avusers on the DX9000 computer.
- Configure each computer/user pair that will access or manage the DX9000 DVR.

Adding Users to the Avusers Group

Before you can configure the computers that will be used to access or manage the DX9000 DVR, you must add the users who will be accessing the DVR to the Windows group called Avusers on the DX9000 computer. You must add each administrator who will launch or configure the DX9000 driver, and each operator who will view video from the DX9000 DVR. The Avusers group is predefined on the DX9000 computer.

To add a user to the Avusers group complete the following steps:

1. Log in to the DX9000 DVR.
2. Right-click the My Computer icon on the Windows desktop, and then select Manage from the pop-up menu. The Computer Management window appears.

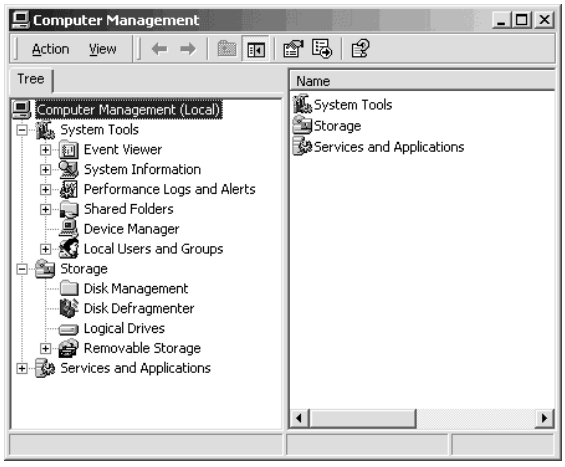


Figure 72. Computer Management Window

3. Navigate to Local Users and Groups > Users.

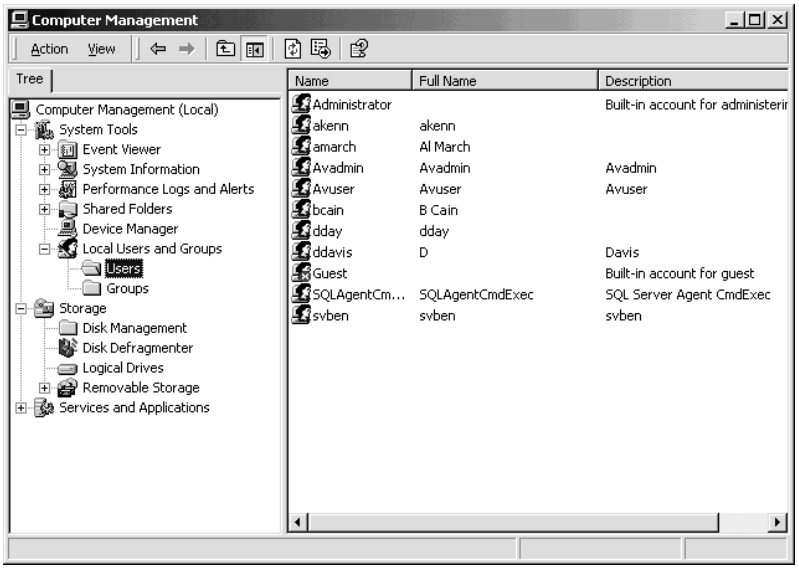


Figure 73. Users Folder

4. Click Action > New User. The New User dialog box appears.

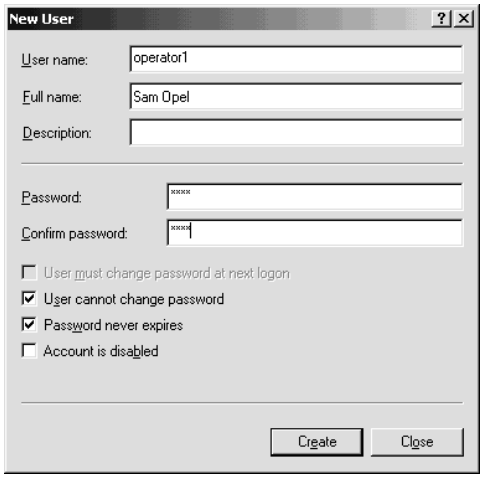


Figure 74. New User Dialog Box

5. Click the "User must change password at next logon" field to clear the checkmark.
6. Click the "User cannot change password" and "Password never expires" fields to select these options.
7. In the User name box, type the Windows user name of the user you want add.
8. Optional: Type the user's full name and a description, if desired.
9. In the Password and Confirm password fields, type the Windows password of the user you want to add.
10. Click Create, and then click Close. The New User dialog box closes.
11. In the Computer Management window, navigate to Local Users and Groups > Groups, and then click the Avusers group in the right pane.

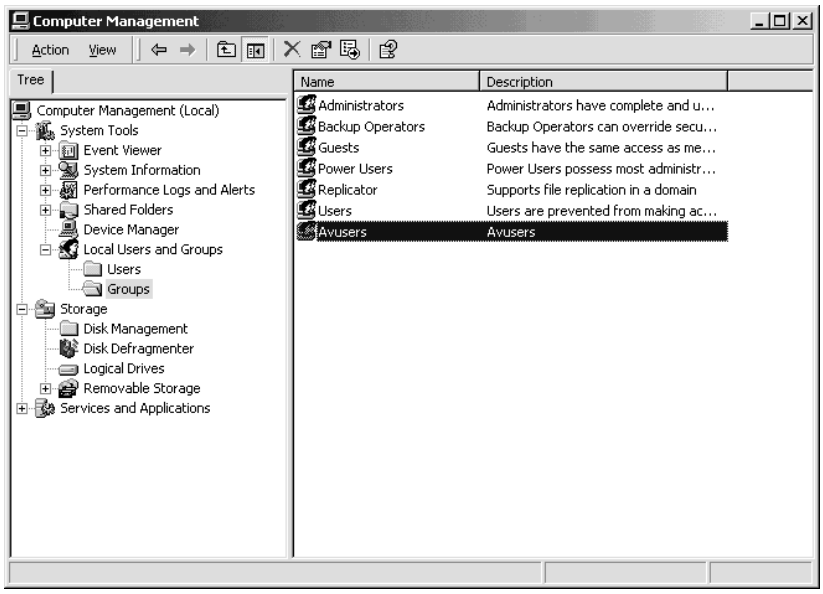


Figure 75. Groups Folder

12. Click Action > Add to Group. The Avusers Properties dialog box appears.

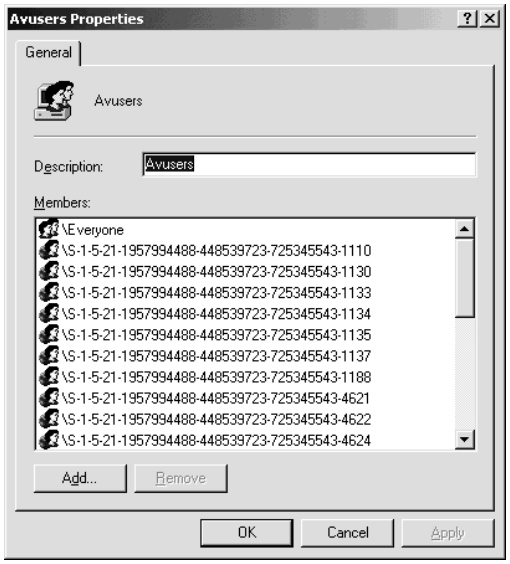


Figure 76. Avusers Properties Dialog Box

13. Click Add. The Select Users or Groups dialog box appears.

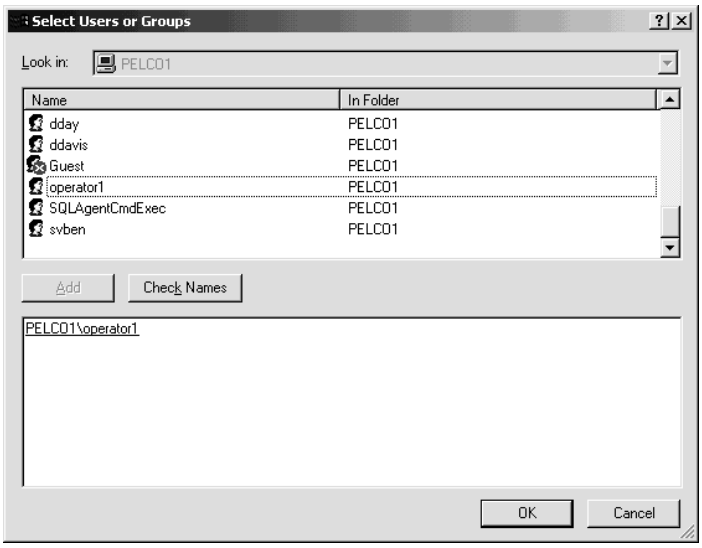


Figure 77. Select Users or Groups Dialog Box

14. Click the user you just added from the list, and then click Add.
15. Click OK. The Select Users or Groups dialog box closes and the new user appears in the Avusers group.

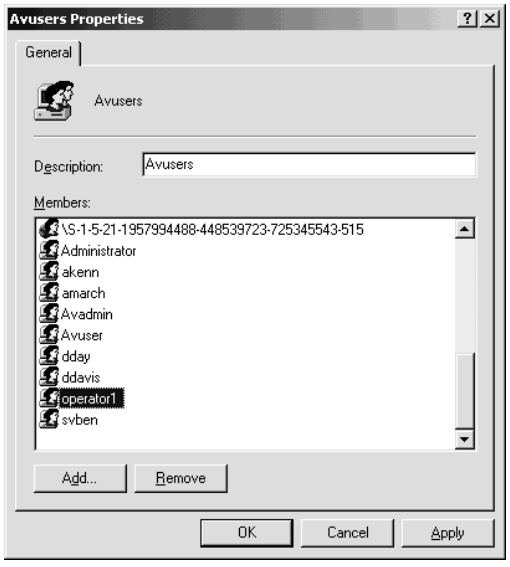


Figure 78. New User Added to Avusers Group

⚠ **WARNING:** Do not proceed with configuring the user's computer if the user does not appear in the Avusers group.

16. Click OK. The Avusers Properties dialog box closes.
17. Click the X in the upper right corner of the Computer Management window to close it.

Configuring Computers and Users

Once you have added the users who will be accessing the DVR to the Avusers group, you must configure the computers from which users will access or manage the DVR, including the VMX300(-E) server, the computer the DX9000 driver is installed on, and every VMX300(-E) client.

You must configure each computer for each user who will access the DVR from that computer. For example, suppose two operators, bsmith and rdarcy, will access a DX9000 DVR from the same computer. You will need to complete the following process to configure the computer for each user:

- Log in as bsmith using bsmith's regular Windows user name and password.
- Configure.
- Log out bsmith.
- Log in as rdarcy using rdarcy's regular Windows user name and password.
- Configure.
- Log out rdarcy.

Similarly, if a particular user will access the DVR from more than one computer, you will have to configure the user on each computer. For example, suppose user mcole will access the DVR from two different computers. You will need to complete the following process to configure the computer for each user:

- Log mcole in to one of the computers.
- Configure.
- Log out mcole.
- Log mcole in to the other computer.
- Configure.
- Log out mcole.

To configure a computer to allow a user to access or manage a DX9000 DVR, complete the following steps:

1. Have the user who will be accessing the DVR log in to Windows using his regular Windows user name and password.
2. Navigate to c:\Program Files\DX 9000 API\Tools.
3. Run AVClientConfig.exe. The DX9000 Client Configuration Utility login dialog box appears.

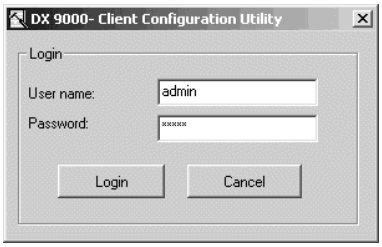


Figure 79. DX9000 Login Dialog Box

4. Enter the user name (admin) and password (admin), and then click Login. The DX9000 Client Configuration Utility dialog box appears.

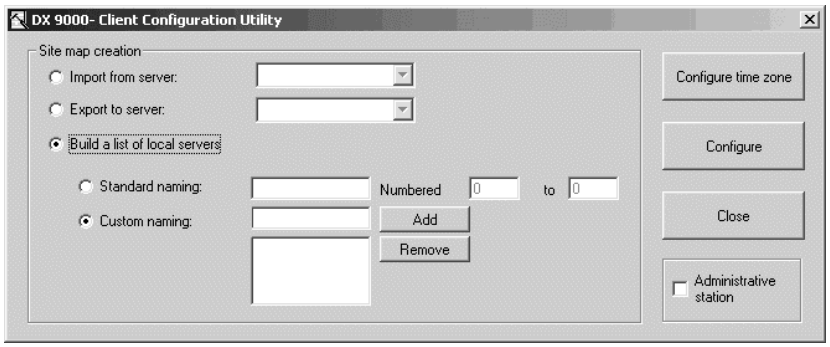


Figure 80. Building Server List

5. Click Build a list of local servers, and then click Custom naming.

6. Type the name of the DX9000 DVR in the Custom naming field. If you do not know the name of the DVR, you can find it out by right-clicking the My Computer icon on the Windows desktop and selecting Properties from the pop-up menu. Click the Network Identification tab. The DVR name is the first part of the full computer name. For example, if the full computer name is pelco1.admin1.corwayfacility, then the DX9000 DVR name is pelco1.

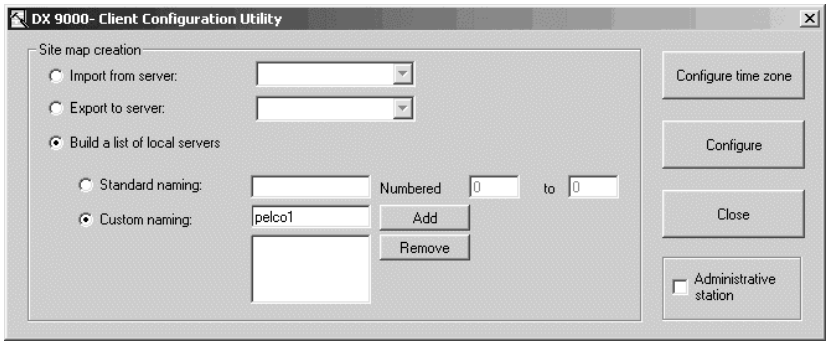


Figure 81. Entering DX9000 Name

7. Click Add. The name of the DX9000 DVR will move to the box below the Custom naming field.

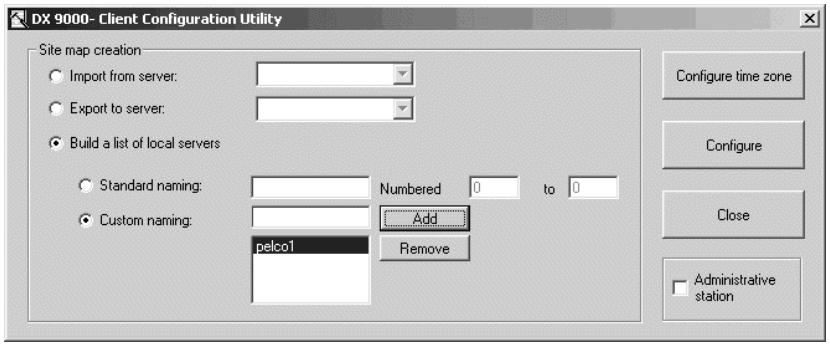


Figure 82. Adding DX9000 Name

8. Click Configure. You will be asked whether you want to change the settings.

9. Click Yes. If the configuration was successful, the name of the DVR will appear in the "Success on" field. A message saying the operation was completed will appear. Click OK to acknowledge the message. If the DVR name appears in the "Failure on" field, refer to the *What if Adding the DVR Failed?* section.

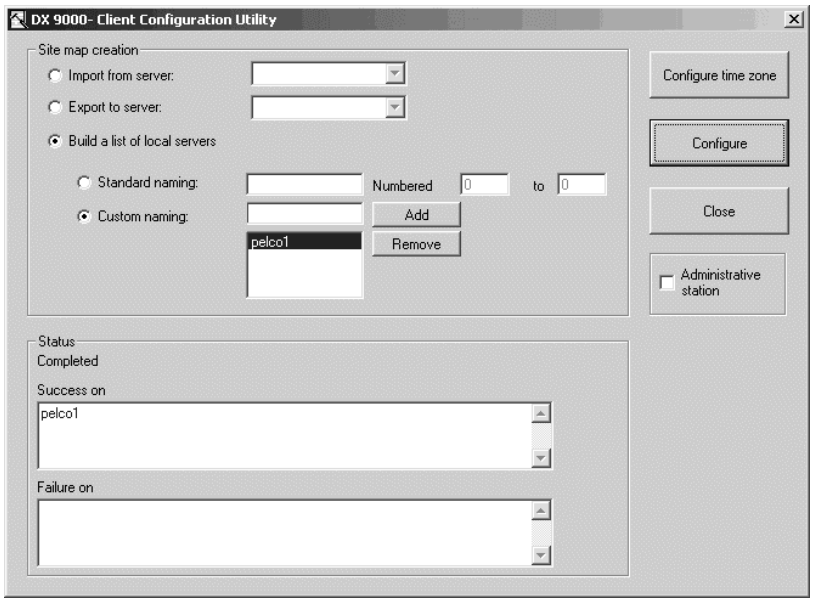


Figure 83. Success or Failure Indication

10. Repeat steps 6 - 8 for each DX9000 DVR you want to be accessible to this user from this computer. If you are configuring the VMX300(-E) server computer, make sure you add each DX9000 in the system. In a multipleserver system, add each DVR to exactly one server. Never add a DVR to more than one server.

11. Click Close. The DX9000 Client Configuration Utility dialog box closes.

What if Adding the DVR Failed?

If the DX9000 Client Configuration Utility fails to add the DVR, the name of the DVR will appear in the "Failure on" field.

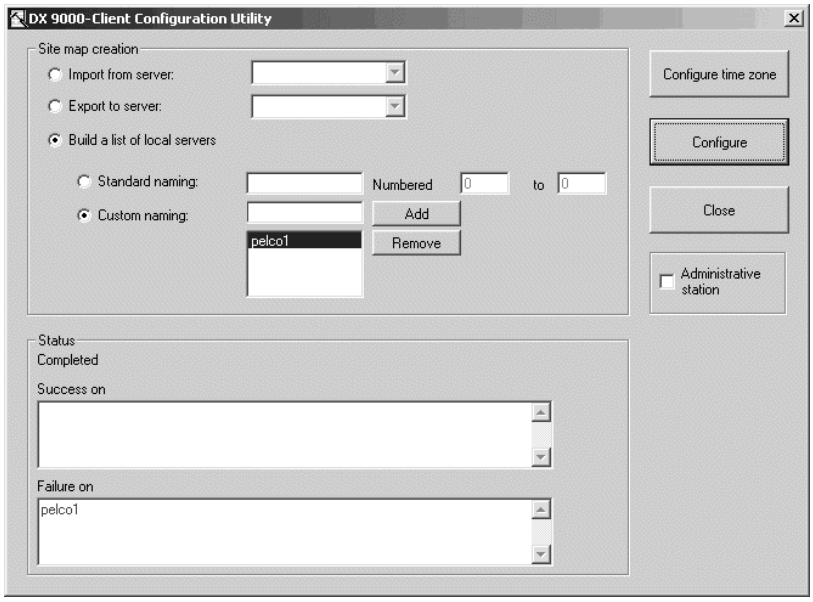


Figure 84. DX9000 Configuration Failure

The most common cause of failure is that the user is not in the Avusers group. If you have already successfully added the user to the Avusers group, make sure you are logged in as the correct user. Log out and log back in, if necessary, then repeat the steps in *Configuring Computers and Users*.

If the user has not yet been added to the Avusers group, follow the instructions in *Adding Users to the Avusers Group*, and then repeat the steps in *Configuring Computers and Users*.

ADD A DX9000 DVR TO THE SERVER CONFIGURATION

Before you can add a device to the server configuration, you must first start the device driver—either on the server workstation or on the network—and then add the driver to the server configuration. Refer to the *Device Drivers* section for instructions.

1. Navigate the Object Browser tree to [project name] > Device Drivers > DX9000 Driver > Devices.
2. Double-click <Add New Device>. The Add New DX9000 dialog box appears.

   You can also configure DX9000 settings after you have added the DVR to the server configuration. Right-click the DX9000, and then select Edit from the pop-up menu. The Edit Properties dialog box appears, with the same tabs and fields as the Add New DX9000 dialog box.
3. Configure the DX9000 settings, as described in the following sections. Note that you must configure the settings in VMX300(-E) to match the DVR settings configured through the software provided with the DVR. Refer to the appropriate DVR installation/operation manual for information on internal DVR settings.
4. Click OK to close the Add New Device dialog box.

CONFIGURE THE GENERAL TAB

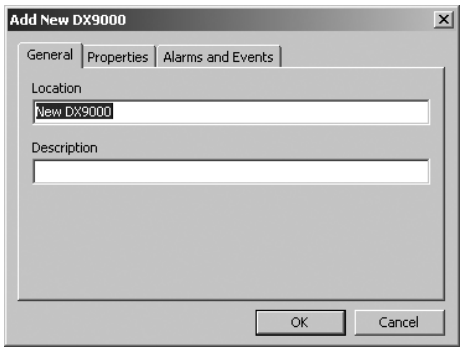


Figure 85. General Tab for DX9000 DVR

Use the General tab to enter a location name and an optional description. The location name is used to identify the DVR. The location name can be a maximum of 50 characters and can include any letter, digit, or special character, with the exception of single and double quotation marks. Location names are not case sensitive.

CONFIGURE THE PROPERTIES TAB

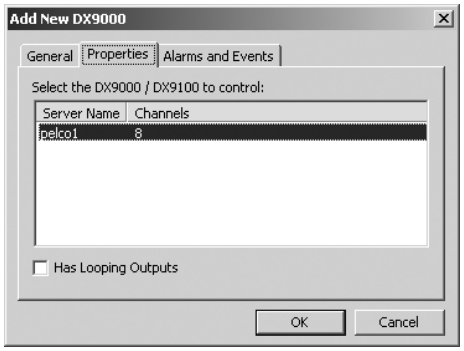


Figure 86. Properties Tab for DX9000 DVR

1. The Properties tab lists all the DX9000 DVRs that were successfully configured from the VMX300(-E) server.

NOTE: If your user name and password have not been configured as described in the *Preparing to Configure the DX9000 DVR* section, no DVRs will appear on the Properties tab.

2. To enable looping outputs on a DVR that supports it, click Looping Outputs. Looping outputs allow the DVR to function as a source device when defining connections. Refer to the *DVR Connections* section for more information.

CONFIGURE THE ALARMS AND EVENTS TAB

This feature is reserved for future development.

DVR TROUBLESHOOTING: IF YOU CHANGE THE VMX300(-E) OPERATING SYSTEM PASSWORD

If you change the VMX300(-E) operating system password (user name: AvUser; password: 1234), system operators must complete the following steps to connect to the DVR server.

1. Click the Windows Start button, and then select Run.
2. Type **\\<serverHostName>\media$** where <serverHostName> is the name of the server; for example, if Pelco1 is the name of the server, type **\\Pelco1\media$.**

   The Connect to <serverHostName> window appears.
3. Type the following user name and password:

   User name: Avuser

   Password: 1234
4. Click Remember my Password.
5. Click OK. The server connection is allowed, and the DVR folder appears.
6. If you have more than one server (for example, Pelco1, Pelco2, and Pelco3), complete steps 1-5 for each server.

ADD A PELCO ASCII SWITCHER

The Pelco ASCII device driver controls cameras routed through a Pelco matrix switcher using the Pelco ASCII protocol.

Each instance of the Pelco ASCII device driver can support a single switcher and multiple cameras. If you have more than one switcher to configure, add the device driver to the server configuration once for each switcher. Refer to the *Device Drivers* section for information on adding device drivers.

The Pelco ASCII device driver supports the following Pelco switchers:

- CM6700 Series
- CM6800 Series
- CM9700 Series

Before you can add a device to the server configuration, you must first start the device driver—either on the server workstation or on the network—and then add the driver to the server configuration. Refer to the *Device Drivers* section for instructions.

1. Navigate the Object Browser tree to [project name] > Device Drivers > Pelco ASCII Driver > Switchers.
2. Double-click <Add New Device>. The Add New Switcher dialog box appears.

   You can also configure switcher settings after you have added the switcher to the server configuration. Right-click the switcher, and then select Edit from the pop-up menu. The Edit Properties dialog box appears, which contains the same tabs and fields as the Add New Switcher dialog box.
3. Configure the switcher settings, as described in the following sections. Note that you must configure the switcher settings in VMX300(-E) to match the switcher settings configured through the management system provided with the switcher. Refer to the appropriate switcher installation/operation manual for information on switcher settings.
4. Click OK to close the Add New Device dialog box.
5. Add ASCII cameras to the server configuration. Refer to the *Add an ASCII Camera* section.
6. Configure the analog connections between the switcher, cameras, and output devices. Refer to the *ASCII Connections* section.

CONFIGURE THE GENERAL TAB

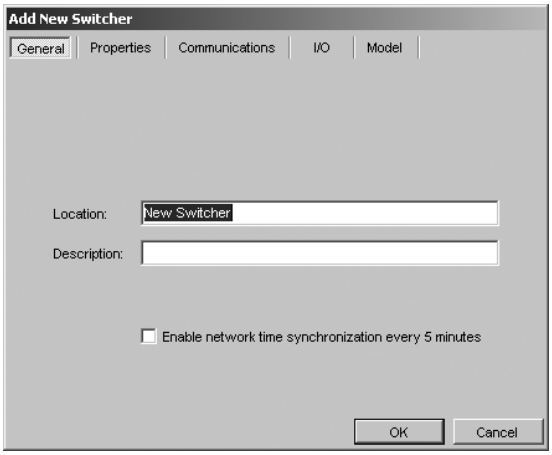


Figure 87. General Tab for an ASCII Switcher

1. Enter a location name and an optional description.

   The location name is used to identify the device. The location name can be a maximum of 50 characters and can include any letter, digit, or special character, with the exception of single and double quotation marks. Location names are not case sensitive.

2. Optional: To synchronize the switcher's internal clock to the clock in the workstation the Pelco ASCII device driver is installed on, click the "Enable network time synchronization every 5 minutes" box.

CONFIGURE THE PROPERTIES TAB

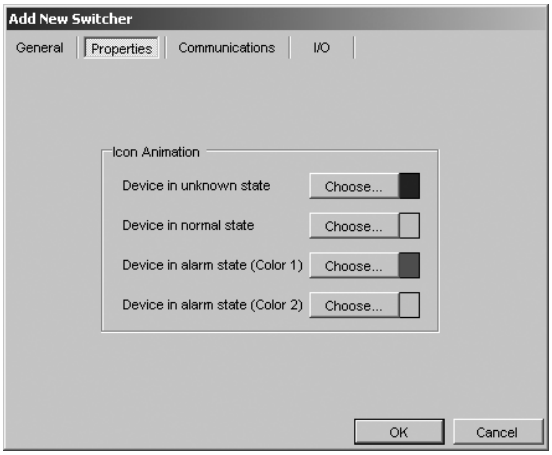


Figure 88. Properties Tab for an ASCII Switcher

Use the Properties tab to configure the animation settings of ASCII switcher icons viewed on maps in the VMX300(-E) client. Click Choose next to each condition to select the color settings for that condition. Note that you can configure a different color setting for each switcher.

Unknown state: When the switcher's CommStatus property equals Offline, device icons in the client are the color specified here.

Normal state: When the switcher's CommStatus property equals Online, device icons in the client are the color specified here.

Alarm state: When the switcher's Alarm write property equals True, the icon flashes alternately between Color 1 and Color 2. Note, however, that flashing icons can increase the CPU workload. To reduce the overall workload, set Color 1 and Color 2 to the same color.

CONFIGURE THE COMMUNICATIONS TAB

1. **Connection Type:** Specify the type of connection between the device driver and the switcher.
   - DIRECT SERIAL: The switcher or data translator is connected directly to the VMX300(-E) workstation using an RS-232 null modem cable.
   - INTERNET PROTOCOL: The switcher or data translator is connected to the serial port on a networked device, such as a PelcoNet device.
   - MODEM: This feature is reserved for future development.
2. **Settings:** Complete the instructions provided below for the appropriate connection type specified in Step 1. The settings must match the settings specified within the switcher. Refer to the appropriate switcher installation/operation manual for information on switcher settings.

Direct Serial Settings

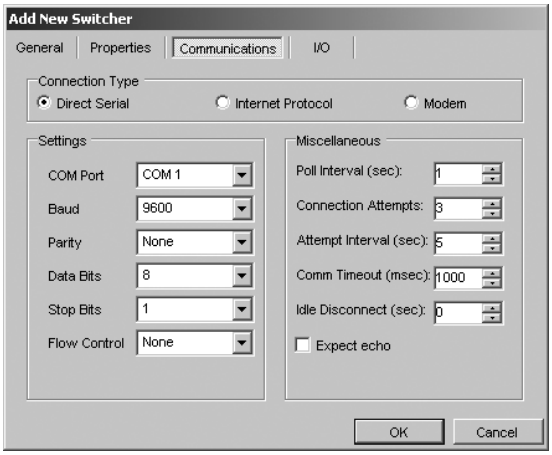


Figure 89. Communications Tab for Switcher Serial Settings

a. Select the COM port that the switcher or data translator is connected to from the drop-down box.

b. Select the appropriate baud rate and parity settings to match the settings specified in the switcher.

c. The remaining settings should specify 8 data bits, 1 stop bit, and no flow control.

d. Refer to Step 3 for instructions on completing the fields in the Miscellaneous section.

Internet Protocol Settings

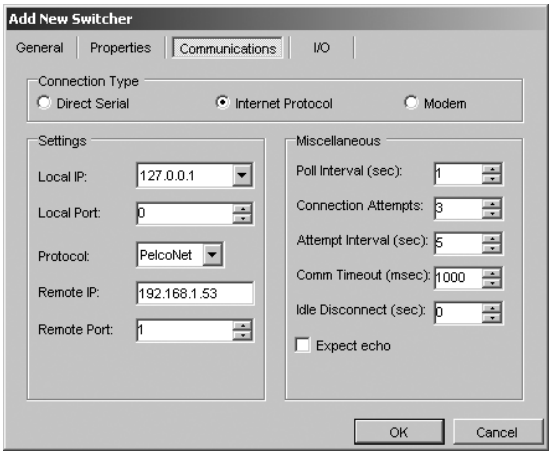


Figure 90. Communications Tab for Switcher Internet Settings

a. Local IP: The local IP is the IP address of the computer that the Pelco ASCII device driver runs on. Select the local IP from the drop-down box.

b. Local Port: The local port is the port the Pelco ASCII driver uses to transmit commands. If your system is secured behind a firewall, enter one of the ports made available by the firewall. Otherwise, enter 0 to have the driver randomly assign an available port. Tip: To find out what port the driver assigned, switch or control the device in the VMX300(-E) client, and then use the netstat command at the DOS prompt to view assigned ports.

c. Remote IP, Remote Port, Protocol: The remote device is the device the Pelco ASCII switcher is physically connected to. If the switcher is connected to a PelcoNet device, follow the instructions in step (1). If the switcher is connected to some other kind of device, follow the instructions in step (2).

   (1) PelcoNet: Select the PelcoNet protocol from the Protocol drop-down box. If the PelcoNet device has a user name and password defined in the device settings, you will be prompted to enter the user name and password before proceeding. Enter the IP address of the PelcoNet device in the Remote IP box. In the Remote Port box, select the port on the PelcoNet device that the switcher is connected to. Select 1 if the switcher is connected to COM 1 on the PelcoNet device. Select 2 if the switcher is connected to COM 2. This port must be exposed in the PelcoNet device properties configuration. For more information on configuring PelcoNet device properties, refer to the section on *Add a PelcoNet MPEG Device*.

   (2) Other: Select the desired transport protocol from the Protocol drop-down box. The remote IP is the IP address of the VMX300(-E) workstation the remote device's driver runs on. Enter the remote IP in the Remote IP box. In the Remote Port box, enter the port the remote device's driver uses to receive commands.

d. Refer to Step 3 for instructions on completing the fields in the Miscellaneous section.

3. **Miscellaneous:** (Optional) Configure the following optional field in the Miscellaneous section of the Communications tab:

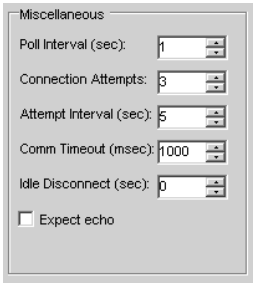


Figure 91. Miscellaneous Section of ASCII Switcher Communications Tab

Idle Disconnect (sec): Enter the number of seconds of inactivity you want to elapse before VMX300(-E) closes the COM port (direct serial connection) or the local port (IP connection). The port will open again automatically when a new connection is established with the switcher. Use the default value of 0 to indicate that the port should never be closed while the driver is running.

Note that the following fields should not be changed:

Poll Interval (sec): This field is reserved for future development.

Connection Attempts: This field is used for troubleshooting and should specify the default value of 3.

Attempt Interval (sec): This field is used for troubleshooting and should specify the default value of 5.

Comm Timeout (msec): This field is used for troubleshooting and should specify the default value of 1000.

Expect echo: This field is reserved for future development.

CONFIGURE THE I/O TAB

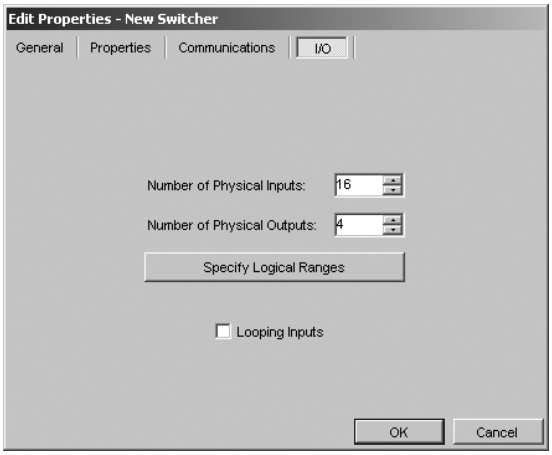


Figure 92. I/O Tab for ASCII Switcher

Use the I/O tab to specify how many physical inputs and outputs are available for switching cameras and to specify logical number ranges.

1. Enter the number of physical inputs available for switching cameras. To prevent VMX300(-E) from using some of the switcher's physical inputs, exclude them from the count of available inputs. For example, if the switcher has a total of 16 physical inputs, 14 of which you want available for switching cameras, enter 14 in this field.

2. Enter the number of physical outputs available for switching cameras. If some of the switcher's outputs are partitioned for dedicated use by another type of device, such as a joystick, exclude them from the count of available outputs. For example, if the switcher has eight physical outputs in total, two of which are going to be used by other devices, enter 6 in this field.

3. Optional: To specify the logical numbering scheme, click Specify Logical Ranges. The Edit Logical Ranges dialog box appears.

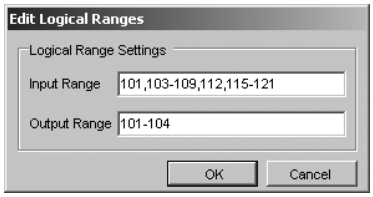


Figure 93. Edit Logical Ranges Dialog Box

   By default, VMX300(-E) assigns sequential identifiers to the available inputs and outputs. Inputs are named Input1, Input2, ... Inputi, where *i* is the total number of physical inputs available for switching cameras. Outputs are named Output1, Output2, ... Outputi, where *i* is the total number of physical outputs available for switching cameras. Looping inputs are named LoopingInput1, LoopingInput2, ... LoopingInputi, where *i* is the total number of physical inputs available for switching cameras.

   a. Enter the numbers you want to use to identify inputs in the Input Range box.

   b. Enter the numbers you want to use to identify outputs in the Output Range box. You can list numbers and/or specify ranges.

   Example, 101,103-109,112,115-121 is a valid input range for a switcher with 16 available inputs. In this case, physical Input1 will be named Input101 in VMX300(-E), physical Input2 will be named Input103, physical Input3 will be named Input 104, and so on. If looping input is enabled for the switcher, the LoopingInputs will be named LoopingInput101, LoopingInput103, LoopingInput104, and so on.

NOTE: If you assigned logical numbers to the inputs and/or outputs when you configured the switcher through the management system provided with the switcher, you must assign the same logical numbers in VMX300(-E). For information on accessing the management system functions, refer to the appropriate switcher installation/operation manual.

4. To enable looping inputs on a switcher that supports it, click Looping Inputs. Looping inputs on a switcher allow the switcher to function as a source device when defining connections. Refer to the *ASCII Connections* section for more information.

CONFIGURE THE MODEL TAB

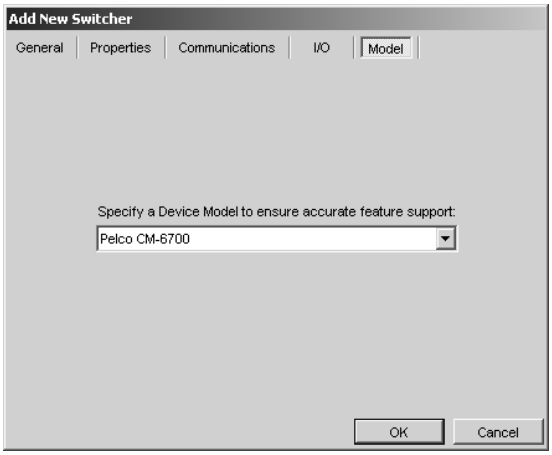


Figure 94. Model Tab for ASCII Switcher

Select the switcher model from the drop-down box.

ADD AN ASCII CAMERA

The Pelco ASCII device driver controls cameras routed through a Pelco matrix switcher using the Pelco ASCII protocol.

The Pelco ASCII device driver supports the following cameras:

- Any fixed camera
- Pelco Spectra II
- Pelco Spectra III
- Pelco Esprit

Before you can add an ASCII camera to the server configuration, you must first start the ASCII device driver—either on the server workstation or on the network—and then add the driver to the server configuration. Refer to the *Device Drivers* section for instructions.

1. Navigate the Object Browser tree to [project name] > Device Drivers > Pelco ASCII Driver > Cameras.
2. Double-click <Add New Device>. The Add New Camera dialog box appears.

   You can also configure camera settings after you have added the camera to the server configuration. Right-click the camera, and then select Edit from the pop-up menu. The Edit Properties dialog box appears, which contains the same tabs and fields as the Add New Camera dialog box.
3. Configure the camera settings, as described in the following sections.
4. Click OK to close the Add New Device dialog box.
5. Configure the analog connections between the switcher, cameras, and output devices. Refer to the *ASCII Connections* section.

CONFIGURE THE GENERAL TAB

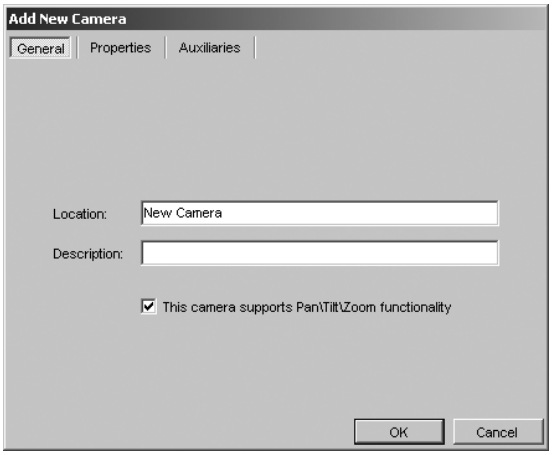


Figure 95. General Tab for ASCII Camera

1. Enter a location name and an optional description.

   The location name is used to identify the device. The location name can be a maximum of 50 characters and can include any letter, digit, or special character, with the exception of single and double quotation marks. Location names are not case sensitive.

2. If the camera can be panned, tilted, zoomed, focused or the iris adjusted, click "This camera supports Pan/Tilt/Zoom functionality." If the camera is fixed, leave this box unchecked.

CONFIGURE THE PROPERTIES TAB

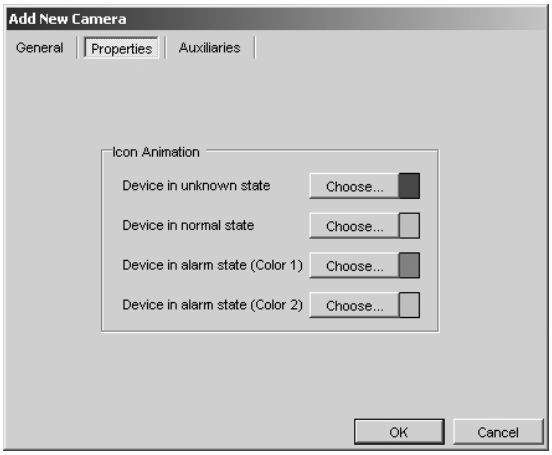


Figure 96. Properties Tab for ASCII Camera

Use the Properties tab to configure the animation settings of camera icons viewed on maps in the VMX300(-E) client. Click Choose next to each condition to select the color settings for that condition. Note that you can configure a different color setting for each camera.

Unknown state: When the camera's CommStatus property equals Offline, device icons in the client are the color specified here.

Normal state: When the camera's CommStatus property equals Online, device icons in the client are the color specified here.

Alarm state: When the camera's Alarm write property equals True, the icon flashes alternately between Color 1 and Color 2. Note, however, that flashing icons can increase the CPU workload. To reduce the overall workload, set Color 1 and Color 2 to the same color.

CONFIGURE THE AUXILIARIES TAB

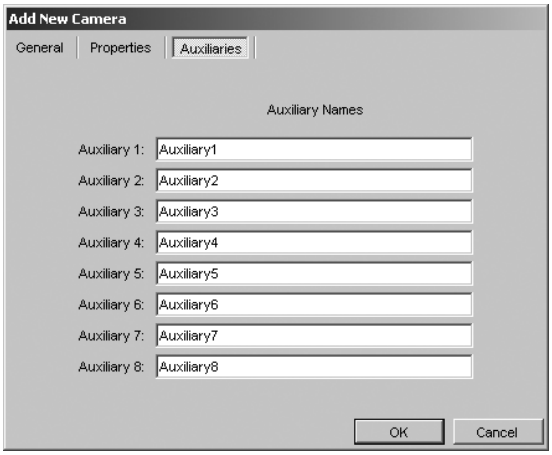


Figure 97. Auxiliaries Tab for ASCII Camera

Auxiliary names appear in the VMX300(-E) client, where auxiliaries are controlled, and also appear in scripts, where they are used to refer to the auxiliary. When you rename an auxiliary, the write property for that auxiliary is changed to the name you have specified.

> **Example:** You might rename an auxiliary that controls a camera's wiper to Wiper, then use it in a script as follows:
> SET Camera1.Wiper = On FOR 3.

To rename an auxiliary, click the box next to the auxiliary you want to rename, and then type the new name. No two auxiliary names can be the same for a particular camera, but the same auxiliary name can be used for different cameras. Auxiliary names can include any letter, digit, or special character, with the exception of single and double quotation marks. Auxiliary names are not case sensitive.

Refer to the appropriate camera installation/operation manual for information on connecting auxiliaries.

NOTE: Changing the name of an auxiliary that is referred to in a script introduces an error into the script. Refer to the *Scripts and Expressions* section for more information.

ADD A KBD300A KEYBOARD

The Pelco KBD300 Driver supports the Pelco KBD300A keyboard in CM6800 ASCII mode, which requires keyboard firmware version 5.00 or higher.

ADD USER ACCOUNTS

You must add appropriate keyboard user accounts to the VMX300(-E) server configuration for each operator and administrator who will need to log in to the KBD300A keyboard. Operators and administrators must use the user name and password configured for them on the VMX300(-E) server when they log in to the KBD300A keyboard.

Keyboard user names and passwords are comprised entirely of digits. For example, 1234 is a valid user name or password. The maximum length of a user name or password is 50 digits. Passwords are optional.

ADD A KBD300A KEYBOARD TO THE SERVER CONFIGURATION

Before you can add a device to the server configuration, you must first start the device driver—either on the server workstation or on the network—and then add the driver to the server configuration. Refer to the *Device Drivers* section for instructions.

1. Navigate the Object Browser tree to [project name] > Device Drivers > Pelco KBD300 > Devices.
2. Double-click <Add New Device>. The Add New Pelco KBD300 dialog box appears.

   You can also configure settings after you have added the keyboard to the server configuration. Right-click the keyboard, and then select Edit from the pop-up menu. The Edit Properties dialog box appears, which contains the same tabs and fields as the Add New Pelco KBD300 dialog box.
3. Configure the keyboard settings, as described in the following sections.
4. Click OK to close the Add New Device dialog box.

CONFIGURE THE GENERAL TAB

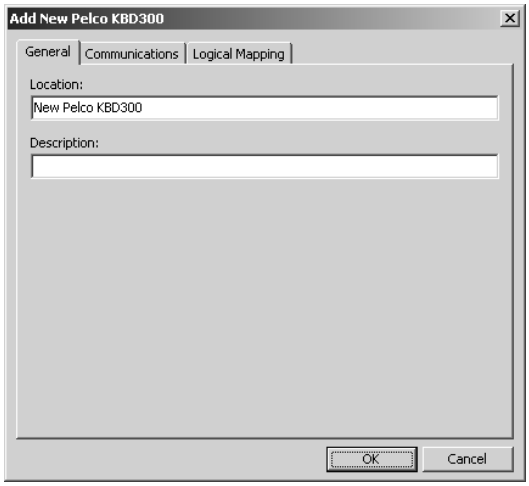


Figure 98. General Tab for KBD300

Use the General tab to enter a location name and an optional description. The location name is used to identify the device. The location name can be a maximum of 50 characters and can include any letter, digit, or special character, with the exception of single and double quotation marks. Location names are not case sensitive.

CONFIGURE THE COMMUNICATIONS TAB

1. **Connection Type:** Specify the type of connection between the keyboard and the switcher.
   - DIRECT SERIAL: The keyboard is connected directly to the VMX300(-E) workstation using a PV140 converter.
   - INTERNET PROTOCOL: The keyboard is connected to the serial port on a networked device, such as a PelcoNet device.
   - MODEM: This feature is reserved for future development.
2. **Settings:** Complete the instructions provided below for the appropriate connection type specified in Step 1.

Direct Serial Settings

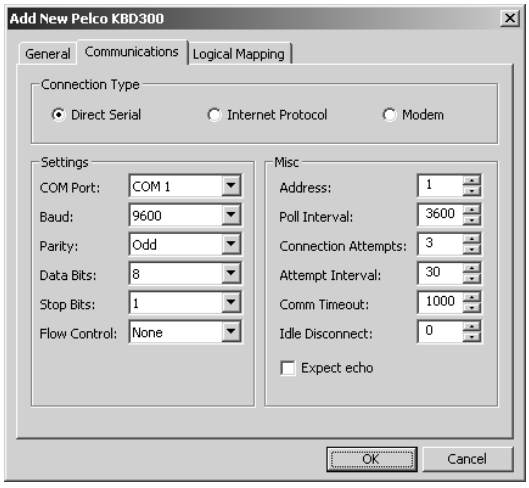


Figure 99. Communications Tab for KBD300 Serial Settings

a. Select the COM port that the keyboard is connected to from the drop-down box.

b. The remaining settings should specify 9600 baud, odd parity, 8 data bits, 1 stop bit, and no flow control.

c. Refer to Step 3 for instructions on completing the fields in the Miscellaneous section.

Internet Protocol Settings

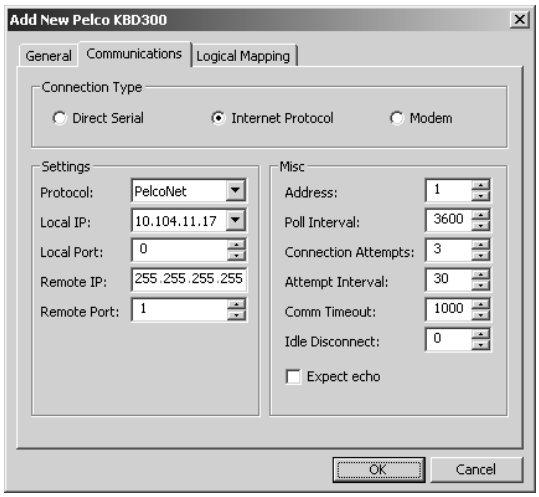


Figure 100. Communications Tab for KBD300 Internet Settings

a. Protocol: If the keyboard is connected to a PelcoNet device, follow the instructions in step (1). If the keyboard is connected to some other kind of device, follow the instructions in step (2).

(1) Select the PelcoNet protocol from the Protocol drop-down list. If the PelcoNet device has a user name and password defined in the internal device settings, you will be prompted to enter the user name and password before proceeding.

Then complete the following fields as described below:

Local IP: The local IP is the IP address of the computer that the Pelco KBD300 device driver runs on. Select the local IP from the drop-down box.

Local Port: The local port is the port the Pelco KBD300 device driver uses to transmit commands. If your system is secured behind a firewall, enter one of the ports made available by the firewall. Otherwise, enter 0 to have the driver randomly assign an available port. Tip: To find out what port the driver assigned, switch or control the device in the VMX300(-E) client, and then use the netstat command at the DOS prompt to view assigned ports.

Remote IP: Enter the IP address of the PelcoNet device in the Remote IP box.

Remote Port: In the Remote Port box, select the port on the PelcoNet device that the keyboard is connected to. Select 1 if the keyboard is connected to COM 1 on the PelcoNet device. Select 2 if the keyboard is connected to COM 2.

(2) Other: Select the desired transport protocol from the Protocol drop-down box.

Then complete the following fields as described below:

Local IP: The local IP is the IP address of the VMX300(-E) workstation that the Pelco KBD300 driver runs on. Select the local IP from the drop-down list.

Local Port: The local port is the port the Pelco KBD300 driver uses to transmit commands. If your system is secured behind a firewall, enter one of the ports made available by the firewall. Otherwise, enter 0 to have the driver randomly assign an available port. Tip: To find out what port was randomly assigned in a particular instance, switch or control the device in the VMX300(-E) client, then use the netstat command at the DOS prompt to view assigned ports.

Remote IP: The remote device is the device the keyboard is physically connected to. The remote IP is the IP address of the VMX300(-E) workstation the remote device's driver runs on. Enter the remote IP in the Remote IP box.

Remote Port: In the Remote Port box, enter the port the remote device's driver uses to receive commands.

b. Refer to Step 3 for instructions on completing the fields in the Miscellaneous section.

3. **Misc:** Configure the following fields in the Misc section of the Communications tab:

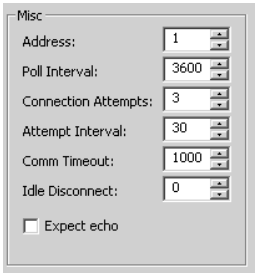


Figure 101. Misc Section of KBD300 Communications Tab

Address: Enter the keyboard address. The address must match the address specified by the keyboard DIP switch settings.

Idle Disconnect (sec): (Optional) Enter the number of seconds of inactivity you want to elapse before VMX300(-E) closes the COM port (direct serial connection) or the local port (IP connection). The port will open again automatically when a new connection is established with the relay unit. Use the default value of 0 to indicate that the port should never be closed while the driver is running.

Note that the following fields should not be changed:

Poll Interval (sec): This field is reserved for future development.

Connection Attempts: This field is used for troubleshooting and should specify the default value of 3.

Attempt Interval (sec): This field is used for troubleshooting and should specify the default value of 30.

Comm Timeout (msec): This field is used for troubleshooting and should specify the default value of 1000.

Expect echo: This field is reserved for future development.

USING THE KBD300A LOGICAL MAPPING FEATURE

When operating a KBD300A keyboard, a user must use camera numbers and monitor numbers to control these cameras and monitors. Since the VMX300(-E) system is based on device names, you must use the "Enable the device number" field in the Edit Local Settings dialog box to assign a number for each device. However, no two device numbers in the VMX300(-E) system can be the same (for example, you cannot use device number 1 for both a monitor and a camera).

To provide system operators with a simple numbering scheme, such as one that would allow the operator to observe "Camera 1" on "Monitor 1", use the KBD300A logical mapping feature.

The KBD300A logical mapping feature allows an operator to control devices using numbers mapped to a specific keyboard. For example, if an operator could switch "Camera 1" to "Monitor 1," "Camera 2" to "Monitor 2," and so on.

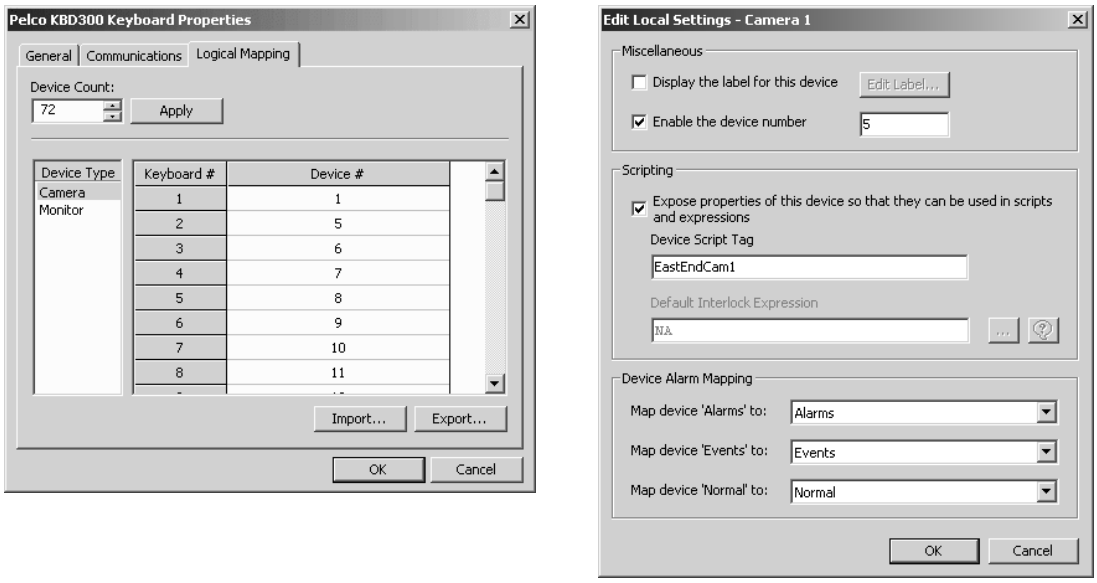


Figure 102. Sample Logical Mapping

To use the KBD300A logical mapping feature you must complete the following tasks:

- Enable a unique device number for each VMX300(-E) device that you want to map to the keyboard. This task is done in the Edit Local Settings dialog box for the specific device. Instructions are provided in the *Enable Camera and Monitor Device Numbers* section.
- Map the device numbers to a keyboard number for the specific keyboard. This task is completed on the Logical Mapping tab of the Add New Pelco KBD300 dialog box (or you can configure these settings after you have added the keyboard to the server configuration, in the Edit Properties dialog box). Instructions are provided in the *Configure the Logical Mapping Tab* section.

ENABLE CAMERA AND MONITOR DEVICE NUMBERS

1. Right-click the camera or monitor in the Object Browser, and then select Local Settings from the pop-up menu. The Edit Local Settings dialog box opens.

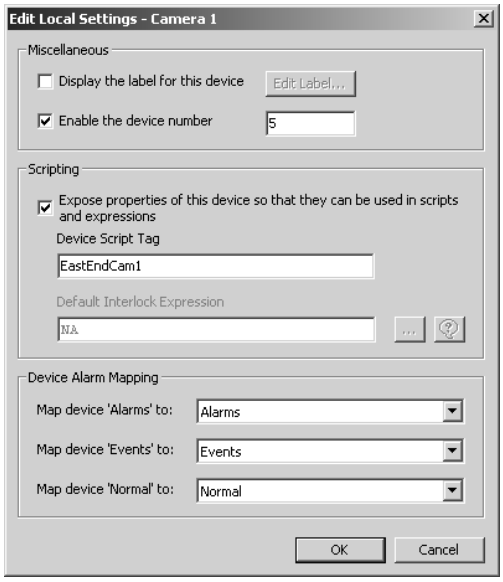


Figure 103. Edit Local Settings Dialog Box

2. Click “Enable the device number,” and then type the desired device number.

   Each device must have a unique device number in its local settings, no matter what type of device it is. For example, you cannot have a monitor with device number 20 and a camera with device number 20. However, these two devices can be mapped to the same keyboard number, so the operator enters the same number on the keyboard for the two devices. Refer to the *Configure the Logical Mapping Tab* section for more information.

3. Click OK. The Edit Local Settings dialog box closes.

CONFIGURE THE LOGICAL MAPPING TAB

The Logical Mapping tab is used to map the device numbers configured in VMX300(-E) to the numbers that an operator enters on the keyboard to control cameras and monitors.

Example:
If you map Device # 5 to Keyboard # 2, as shown in the following figure, then an operator at that keyboard can call up “Camera 2” without having to remember the camera name or device number.

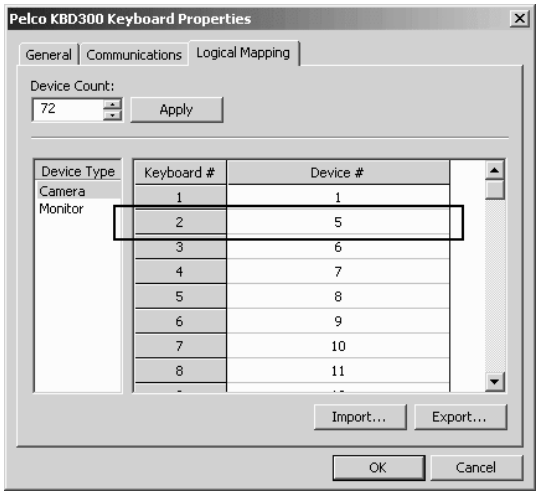


Figure 104. Logical Mapping Tab for KBD300

Refer to the *Enable Camera and Monitor Device Numbers* section for instructions on assigning device numbers to cameras and monitors in VMX300(-E).

To configure the logical number mappings for a keyboard complete the following steps:

1. Click the appropriate device type (either Camera or Monitor) in the Device Type box.

2. Enter the number of devices that you want to be able to control through this keyboard In the Device Count field, and then click Apply.

   The number of rows in the logical mapping table for the device is set to the number that you enter in the Device Count field. For example, if you specify 72 cameras, then there will be 72 rows under the Keyboard # and Device # columns.

3. Map each keyboard logical number to the desired device number by typing the appropriate device number in the Device # column. For example, type 6 to map keyboard logical number to the camera that is assigned device number 6.

   VMX300(-E) provides a shortcut for entering consecutively numbered devices. Refer to the *Mapping Shortcut* section for instructions.

View Logical Mapping Settings

To view the current logical mapping scheme for either cameras or monitors, click the appropriate device type in the Device Type box. The logical mapping for the selected device type appears in the grid containing the Keyboard # and Device # columns.

Export Logical Mapping Settings

If you want to assign the same logical mappings to more than one keyboard, you can save the logical mapping settings to a file by completing the following steps:

1. Configure the logical mappings as described in the previous section.
2. Click Export. The Save As dialog box appears.
3. Browse to the desired folder and type a file name for the logical mappings.
4. Click Save. The Save As dialog box closes and the logical mappings are saved.
5. Click OK. The Keyboard Properties dialog box closes.
6. Refer to the following section for instructions on copying the settings to another keyboard.

Import Logical Mapping Settings

Once you have saved a file of logical mapping settings, you can copy the settings to another keyboard by completing the following steps:

TIP: If you want to use similar but not identical logical mapping settings in another keyboard, import the settings, and then edit them.

1. Add and configure another keyboard, following the instructions provided in the previous sections.
2. Click the Logical Mapping Tab, and then click Import. The Open dialog box appears.
3. Navigate to the folder containing the logical mappings file, and then click the file to select it.
4. Click Open. The Open dialog box closes, and the logical mapping settings for cameras and monitors are imported into the keyboard properties.
5. Repeat steps 1-4 for additional keyboards.

Mapping Shortcut

VMX300(-E) provides a shortcut for entering consecutively numbered devices. For example, map device numbers 50-55 to keyboard numbers 20-25 as follows:

1. Enter the first device number, in this example, 50.
2. Using the mouse, position the pointer over the square to the right of Device # 50. The pointer changes into cross hairs.

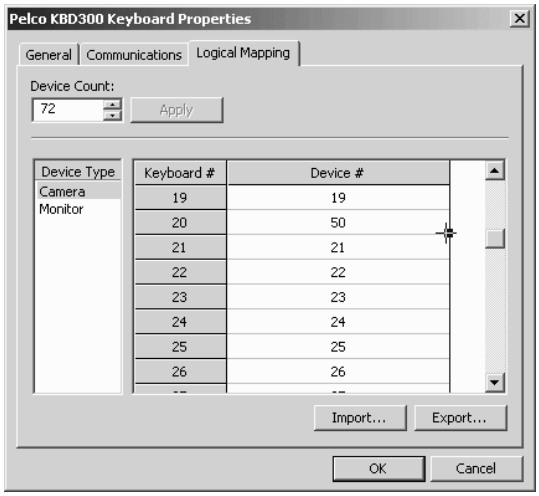


Figure 105. Mapping Consecutive Logical Numbers

3. Press the left mouse button and drag the square to the end of the consecutive range, in this example, Keyboard # 25. The range is enclosed in a rectangle.

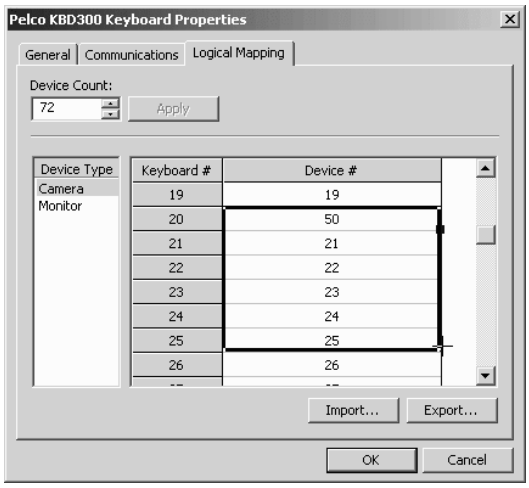


Figure 106. Logical Mapping Range

4. Release the mouse button. VMX300(-E) automatically numbers the selected devices consecutively, starting from the number of the first device in the range.

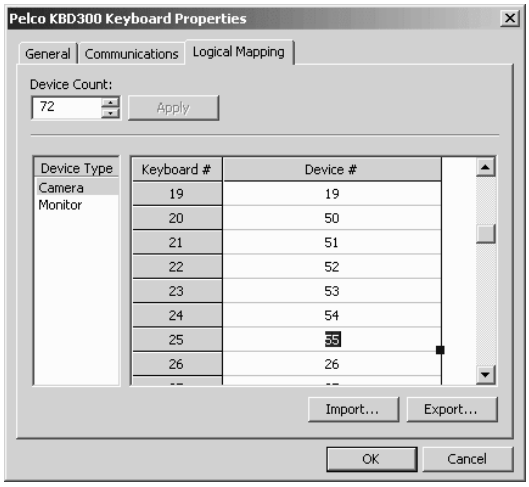


Figure 107. Consecutive Logical Numbers

ADD A CM9760-ALM ALARM INTERFACE UNIT

The Pelco ALM driver supports the CM9760-ALM alarm interface unit, which can be used to bring contact information into the VMX300(-E) system. Examples of contacts that can be connected are motion sensors, door switches, and pushbuttons. Refer to the CM9760-ALM Installation/Operation manual for information on connecting devices to the alarm unit.

Each alarm module supports 64 alarm points, and up to 4 modules can be daisy chained together for a maximum of 256 input points on one serial port.

Before you can add a alarm unit to the server configuration, you must first start the device driver—either on the server workstation or on the network—and then add the driver to the server configuration. Refer to the *Device Drivers* section for instructions.

1. Navigate the Object Browser tree to [project name] > Device Drivers > Pelco ALM Driver > Devices.
2. Double-click <Add New Device>. The Add New Device dialog box appears.

   You can also configure settings after you have added the device to the server configuration. Right-click the device, and then select Edit from the pop-up menu. The Edit Properties dialog box appears, which contains the same tabs and fields as the Add New Device dialog box.
3. Configure the device settings, as described in the following sections.
4. Click OK to close the Add New Device dialog box.

CONFIGURE THE GENERAL TAB

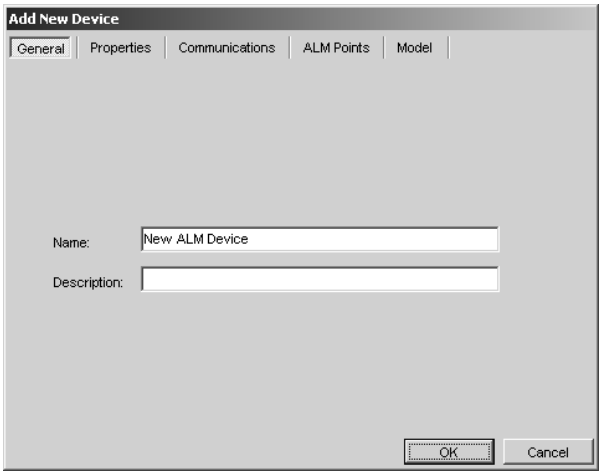


Figure 108. General Tab for CM9760-ALM

Use the General tab to name and describe the alarm unit. The device name can be a maximum of 50 characters. You cannot use single or double quotation marks in a name, but you can use any other letter, digit, or special character. Device names are not case sensitive. The optional description appears in the Object Browser beside the device name.

CONFIGURE THE PROPERTIES TAB

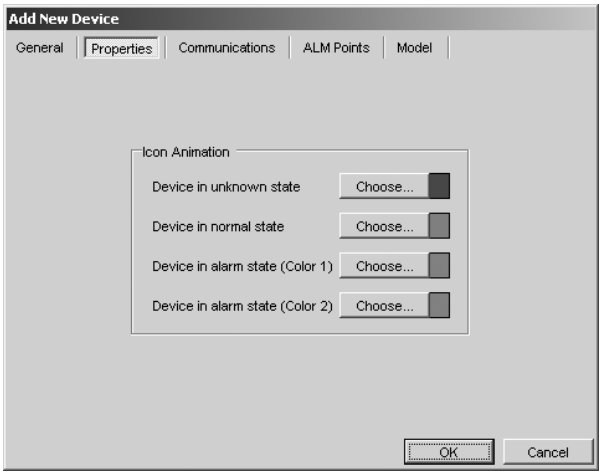


Figure 109. Properties Tab for CM9760-ALM

Use the Properties tab to configure the animation settings of the CM9760-ALM unit's icon viewed on maps in the VMX300(-E) client. Click Choose next to each condition to select the color settings for that condition. Note that you can configure a different color setting for each alarm unit.

Unknown state: When the alarm unit's Status property equals Unknown, the icon is the color specified here.

Normal state: When the alarm unit's Status property equals Normal, the icon is the color specified here.

Alarm state: When the alarm unit's Alarm write property equals True, the icon changes to the color specified here. If you change either Color 1 or Color 2, then the icon flashes alternately between the two colors when the alarm unit is in the alarm state. Note, however, that flashing icons can increase the CPU workload.

CONFIGURE THE COMMUNICATIONS TAB

1. **Connection Type:** Specify the type of connection between the device driver and the alarm unit.
   - DIRECT SERIAL: The alarm unit is connected using an RS-232 to RS-422 converter or using an RS-422 PC serial port.
   - INTERNET PROTOCOL: The alarm unit is connected to the serial port on a networked device.
   - MODEM: This feature is reserved for future development.
2. **Settings:** Complete the instructions provided below for the appropriate connection type specified in Step 1. The settings must match the settings specified within the alarm unit. Refer to the CM9760-ALM installation/operation manual for information on unit settings.

Direct Serial Settings

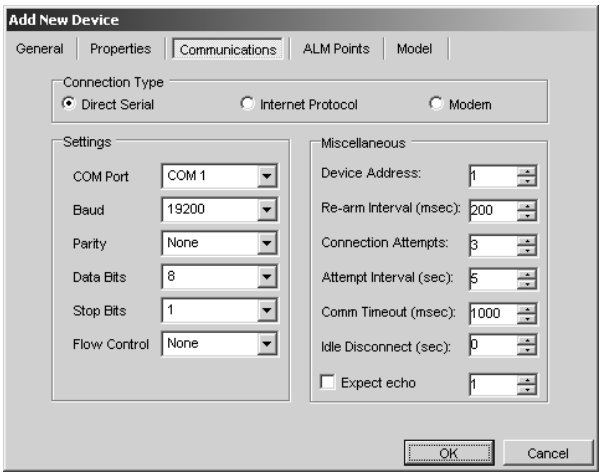


Figure 110. Communications Tab for CM9760-ALM Serial Settings

a. Select the COM port the alarm unit is connected to from the drop-down box.

b. Set the baud rate to match the Port 0 DIP switch settings on the alarm unit. 19200 is recommended. If the alarm unit is daisy-chained from another alarm unit, use the same baud rate for all the units in the chain.

c. The remaining settings should specify no parity, 8 data bits, 1 stop bit, and no flow control.

d. Refer to Step 3 for instructions on completing the fields in the Miscellaneous section.

Internet Protocol Settings

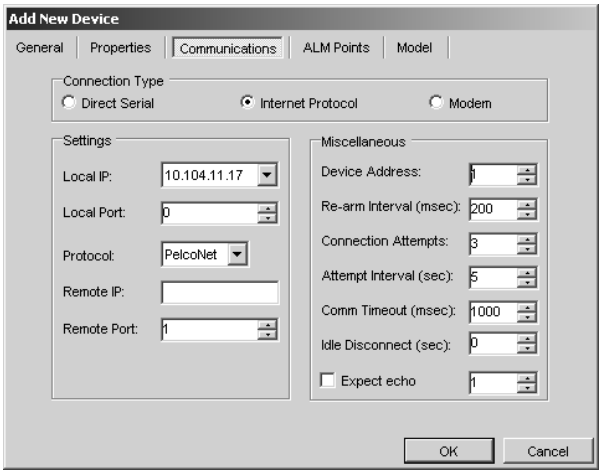


Figure 111. Communications Tab for CM9760-ALM IP Settings

a. Local IP: The local IP is the IP address of the computer that the Pelco ALM driver runs on. Select the local IP from the drop-down box.

b. Local Port: The local port is the port the Pelco ALM driver uses to transmit commands. Enter the local port.

c. Protocol, Remote IP, Remote Port: The remote device is the device the alarm unit is physically connected to. If the alarm unit is connected to a PelcoNet device, follow the instructions in step (1). If the alarm unit is connected to some other kind of device, follow the instructions in step (2).

   (1) PelcoNet: Select the PelcoNet protocol from the Protocol drop-down box. If the PelcoNet device has a user name and password defined in the device settings, you will be prompted to enter the user name and password before proceeding. Enter the IP address of the PelcoNet device in the Remote IP box. In the Remote Port box, select the port on the PelcoNet device that the alarm unit is connected to. Select 1 if the alarm unit is connected to COM 1 on the PelcoNet device. Select 2 if the alarm unit is connected to COM 2.

   (2) Other: Select the desired transport protocol from the Protocol drop-down box. The remote IP is the IP address of the computer the remote device's driver runs on. Enter the remote IP in the Remote IP box. In the Remote Port box, enter the port the remote device's driver uses to receive commands.

d. Refer to Step 3 for instructions on completing the fields in the Miscellaneous section.

3. **Miscellaneous:** Configure the following fields in the Miscellaneous section of the Communications tab:

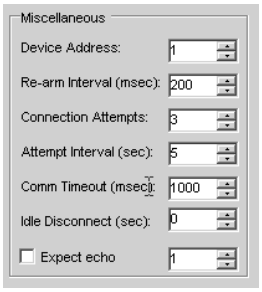


Figure 112. Miscellaneous Section of Communications Tab

Device Address: Enter the device address. The device address must match the Group Address configured through the alarm unit's DIP switches. Refer to the CM9760-ALM Installation/Operation manual for instructions.

Re-arm Interval: (Optional) Enter the re-arm interval. The re-arm interval determines how soon after an event a state change can be detected. Any change in state is ignored for the duration of the re-arm interval.

Idle Disconnect (sec): (Optional) Enter the number of seconds of inactivity you want to elapse before VMX300(-E) closes the COM port (direct serial connection) or the local port (IP connection). The port will open again automatically when a new connection is established with the alarm unit. Use the default value of 0 to indicate that the port should never be closed while the driver is running.

Note that the following fields should not be changed:

Connection Attempts: This field is used for troubleshooting and should specify the default value of 3.

Attempt Interval (sec): This field is used for troubleshooting and should specify the default value of 5.

Comm Timeout (msec): This field is used for troubleshooting and should specify the default value of 1000.

Expect echo: This field is reserved for future development.

CONFIGURE THE ALM POINTS TAB

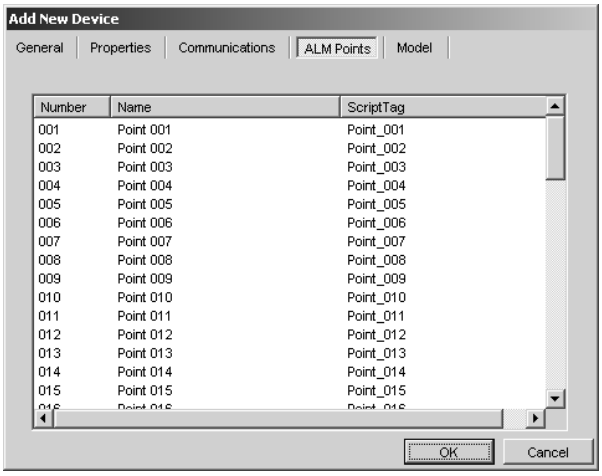


Figure 113. ALM Points Tab for CM9760-ALM

The ALM Points tab lists each alarm point in the device and the name and script tag used within VMX300(-E) to refer to the point. The device address entered on the Communications tab determines how the points are numbered. If the device address is set to 1, the points are numbered 1 - 64. If the address is set to 2, the points are numbered 65 - 128, and so on.

The ALM Points tab allows you to rename points to give them meaningful names.

Rename an Alarm Point

1. Double-click the point you want to rename. The Edit Point dialog box appears.

   Note that the alarm point number appears in the Number field, and the alarm point's script tag appears in the Script Tag field. These fields cannot be edited.

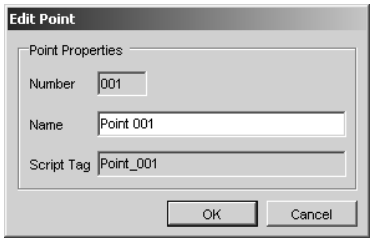


Figure 114. Edit Point Dialog Box

2. Type a new name for the point. The name can include any letter, digit, or special character, with the exception of single and double quotation marks.
3. Click OK. The dialog box closes and the new alarm point name appears on the ALM Points tab.

CONFIGURE THE MODEL TAB

Figure 115. Model Tab for CM9760-ALM

The Model tab displays the model of alarm unit supported by the Pelco ALM Driver. Only one model is currently supported.

ADD A CM9760-REL RELAY INTERFACE UNIT

The Pelco Relay driver supports the CM9760-REL relay interface unit, which can be used to control peripheral equipment through single-pole, single-throw (SPST) contact outputs. Each relay unit provides 64 contact outputs.

Before you can add a relay unit to the server configuration, you must first start the device driver—either on the server workstation or on the network—and then add the driver to the server configuration. Refer to the *Device Drivers* section for instructions.

1. Navigate the Object Browser tree to [project name] > Device Drivers > Pelco Relay Driver > Devices.
2. Double-click <Add New Device>. The Add New Device dialog box appears.

   You can also configure settings after you have added the device to the server configuration. Right-click the device, and then select Edit from the pop-up menu. The Edit Properties dialog box appears, which contains the same tabs and fields as the Add New Device dialog box.
3. Configure the device settings, as described in the following sections.
4. Click OK to close the Add New Device dialog box.

CONFIGURE THE GENERAL TAB

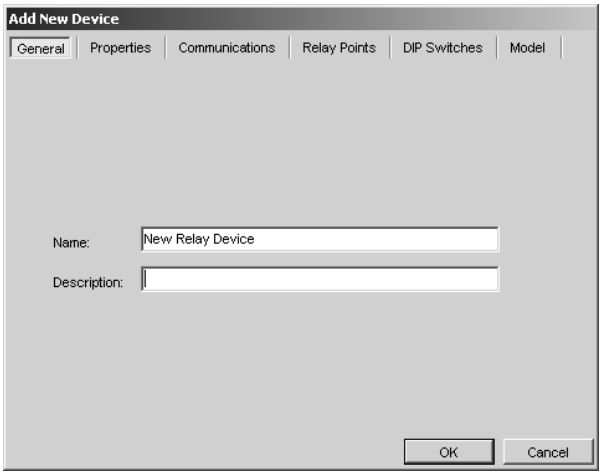


Figure 116. General Tab for CM9760-REL

Use the General tab to name and describe the relay unit. The device name can be a maximum of 50 characters. You cannot use single or double quotation marks in a name, but you can use any other letter, digit, or special character. Device names are not case sensitive. The optional description appears in the Object Browser beside the device name.

CONFIGURE THE PROPERTIES TAB

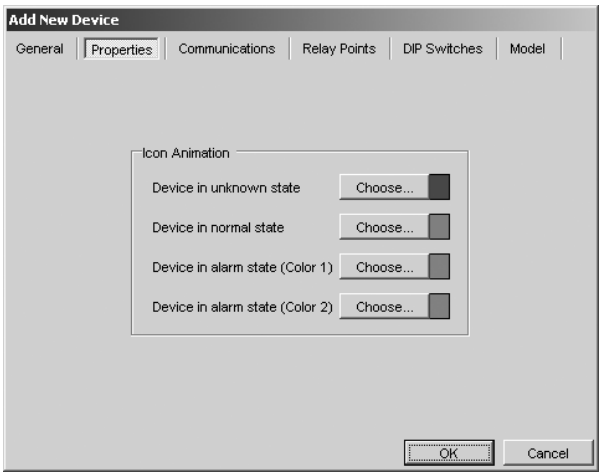


Figure 117. Properties Tab for CM9760-REL

Use the Properties tab to configure the animation settings of the CM9760-REL unit's icon viewed on maps in the VMX300(-E) client. Click Choose next to each condition to select the color settings for that condition. Note that you can configure a different color setting for each relay unit.

Unknown state: When the relay unit's Status property equals Unknown, the icon is the color specified here.

Normal state: When the relay unit's Status property equals Normal, the icon is the color specified here.

Alarm state: When the relay unit's Alarm write property equals True, the icon changes to the color specified here. If you change either Color 1 or Color 2, then the icon flashes alternately between the two colors when the relay unit is in the alarm state. Note, however, that flashing icons can increase the CPU workload.

CONFIGURE THE COMMUNICATIONS TAB

1. **Connection Type:** Specify the type of connection between the device driver and the relay unit.
   - DIRECT SERIAL: The relay unit is connected using an RS-232 to RS-422 converter or using an RS-422 PC serial port.
   - INTERNET PROTOCOL: The relay unit is connected to the serial port on a networked device.
   - MODEM: This feature is reserved for future development.
2. **Settings:** Complete the instructions provided below for the appropriate connection type specified in Step 1. The settings must match the settings specified within the relay unit. Refer to the CM9760-REL installation/operation manual for information on unit settings.

Direct Serial Settings

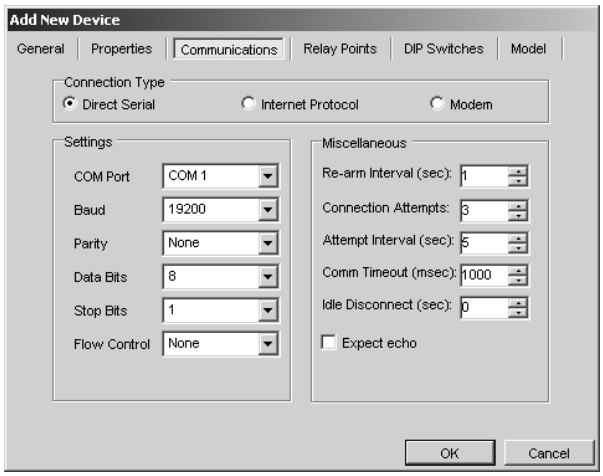


Figure 118. Communications Tab for CM9760-REL Serial Settings

a. Select the COM port the relay unit is connected to from the drop-down box.

b. Set the baud rate to match the DIP switch settings on the relay unit's IN port. 19200 is recommended. If the relay unit is daisy-chained from another relay unit, use the same baud rate for all the units in the chain.

c. The remaining settings should specify no parity, 8 data bits, 1 stop bit, and no flow control.

d. Refer to Step 3 for instructions on completing the fields in the Miscellaneous section.

Internet Protocol Settings

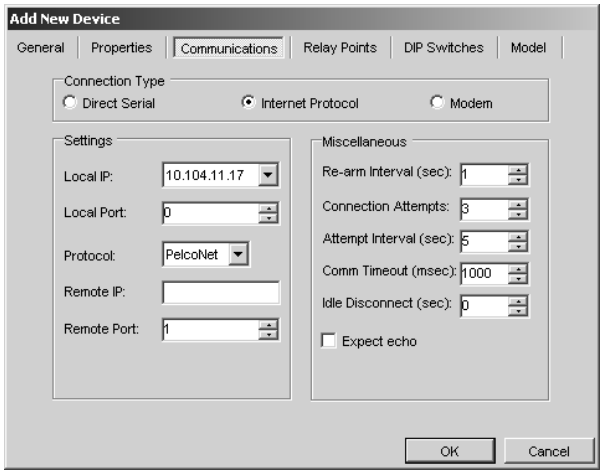


Figure 119. Communications Tab for CM9760-REL IP Settings

a. Local IP: The local IP is the IP address of the computer that the Pelco Relay driver runs on. Select the local IP from the drop-down box.

b. Local Port: The local port is the port the Pelco Relay driver uses to transmit commands. Enter the local port.

c. Remote IP, Remote Port, Protocol: The remote device is the device the relay unit is physically connected to. If the relay unit is connected to a PelcoNet device, follow the instructions in step (1). If the relay unit is connected to some other kind of device, follow the instructions in step (2).

   (1) PelcoNet: Select the PelcoNet protocol from the Protocol drop-down box. If the PelcoNet device has a user name and password defined in the device settings, you will be prompted to enter the user name and password before proceeding. Enter the IP address of the PelcoNet device in the Remote IP box. In the Remote Port box, select the port on the PelcoNet device that the relay unit is connected to. Select 1 if the relay unit is connected to COM 1 on the PelcoNet device. Select 2 if the relay unit is connected to COM 2.

   (2) Other: Select the desired transport protocol from the Protocol drop-down box. The remote IP is the IP address of the computer the remote device's driver runs on. Enter the remote IP in the Remote IP box. In the Remote Port box, enter the port the remote device's driver uses to receive commands.

d. Refer to Step 3 for instructions on completing the fields in the Miscellaneous section.

3. **Miscellaneous:** (Optional) Configure the following optional field in the Miscellaneous section of the Communications tab:

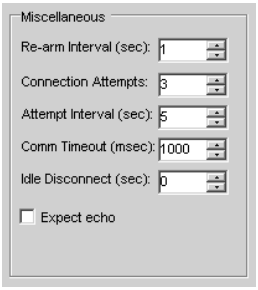


Figure 120. Miscellaneous Section of Communications Tab

Idle Disconnect (sec): Enter the number of seconds of inactivity you want to elapse before VMX300(-E) closes the COM port (direct serial connection) or the local port (IP connection). The port will open again automatically when a new connection is established with the relay unit. Use the default value of 0 to indicate that the port should never be closed while the driver is running.

Note that the following fields should not be changed:

Re-arm Interval (sec): This field is reserved for future development.

Connection Attempts: This field is used for troubleshooting and should specify the default value of 3.

Attempt Interval (sec): This field is used for troubleshooting and should specify the default value of 5.

Comm Timeout (msec): This field is used for troubleshooting and should specify the default value of 1000.

Expect echo: This field is reserved for future development.

CONFIGURE THE RELAY POINTS TAB

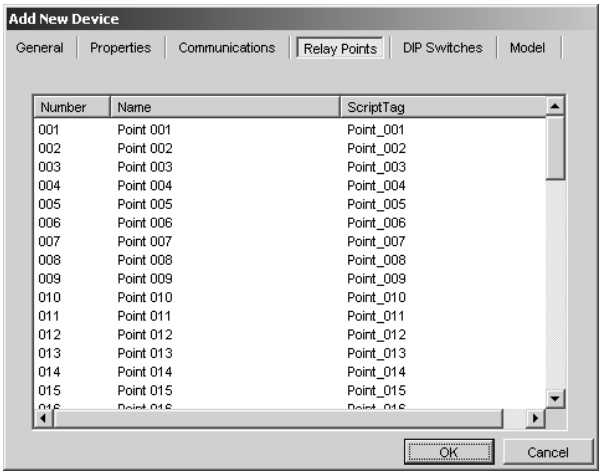


Figure 121. Relay Points Tab for CM9760-REL

The Relay Points tab lists each relay point in the device and the name and script tag used within VMX300(-E) to refer to the point. The list of relay points also appears in the Device Control dialog box in the VMX300(-E) client. The Relay Points tab allows you to rename points to give them meaningful names.

Rename a Relay Point

1. Double-click the point you want to rename. The Edit Point dialog box appears.

   Note that the relay point number appears in the Number field, and the relay point's script tag appears in the Script Tag field. These fields cannot be edited.

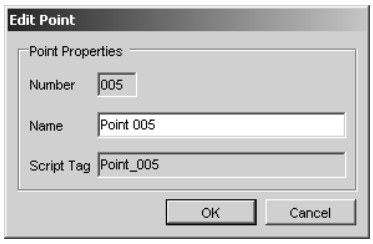


Figure 122. Edit Point Dialog Box

2. Type a new name for the point. The name can include any letter, digit, or special character, with the exception of single and double quotation marks.

3. Click OK. The dialog box closes and the new relay point name appears on the Relay Points tab and in the client Device Control dialog box.

CONFIGURE THE DIP SWITCHES TAB

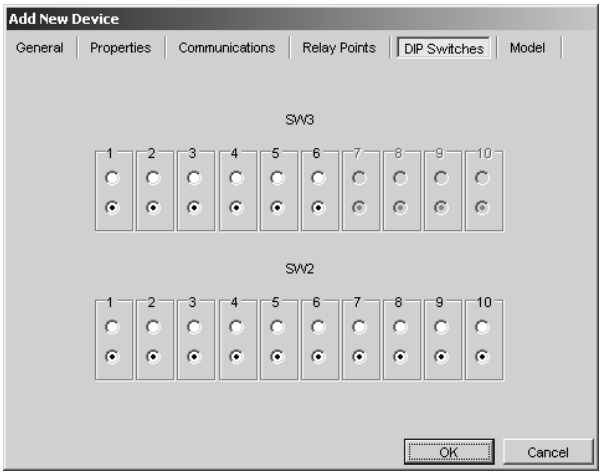


Figure 123. DIP Switches Tab for CM9760-REL

The DIP Switches tab provides a schematic of the DIP switches located under the front panel of the relay unit. Set the DIP switches in the schematic to match the DIP switch settings on the relay unit.

CONFIGURE THE MODEL TAB

Figure 124. Model Tab for CM9760-REL

The Model tab displays the model of relay unit supported by the Pelco Relay Driver. Only one model is currently supported.

ADD A SERIAL OUTPUT DEVICE

The serial output driver can be used to send ASCII commands to an external serial (RS-232) device. For example, you could send ASCII commands to report alarms to an access control system, start a VCR in play mode, or control a camera.

Note that the particular device-control commands that are available and the ASCII strings that represent them depend on what is available in the specific device. Refer to the device's product documentation for information on the protocol for that device.

VMX300(-E) provides the following ways for a system operator to send ASCII output to a serial output device:

- Custom button—you can define a custom button (through the server configuration) containing an ASCII string that will be sent to the serial output device when a system operator clicks the button. Custom buttons appear in the device's device control dialog box in the VMX300(-E) client.
- Script—you can define a script (through the server configuration) to send an ASCII string to the device when a system operator runs the script. A script can also be associated with a hotlink, label, alarm, or schedule.
- Text tab—the system operator can use the text tab on the device's device control dialog box (in the VMX300(-E) client) to send an ASCII string to the device. This method requires the operator to type each string and does not provide a way to save a string.

Before you can add a serial output device to the server configuration, you must first start the Serial Output driver—either on the workstation that the serial output device is connected to or on the network—and then add the driver to the server configuration. Refer to the *Device Drivers* section for instructions.

1. Navigate the Object Browser tree to [project name] > Device Drivers > Serial Output > Devices.
2. Double-click <Add New Device>. The Add New Serial Output Device dialog box appears.

   You can also configure settings after you have added the device to the server configuration. Right-click the device, and then select Edit from the pop-up menu. The Edit Properties dialog box appears, which contains the same tabs and fields as the Add New Serial Output Device dialog box.
3. Configure the device settings, as described in the following sections.
4. Click OK to close the Add New Device dialog box.

CONFIGURE THE GENERAL TAB

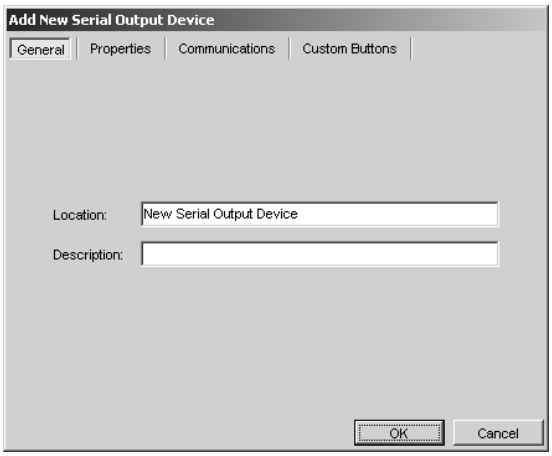


Figure 125. General Tab for a Serial Output Device

Use the General tab to name and describe the serial output device. The device name can be a maximum of 50 characters. You cannot use single or double quotation marks in a name, but you can use any other letter, digit, or special character. Device names are not case sensitive. The optional description appears in the Object Browser beside the device name.

CONFIGURE THE PROPERTIES TAB

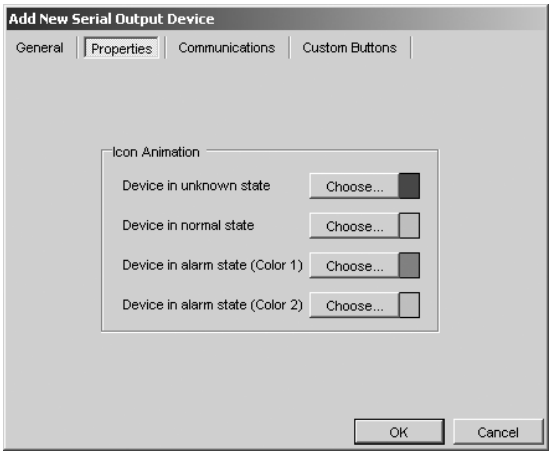


Figure 126. Properties Tab for a Serial Output Device

Use the Properties tab to configure the animation settings of the device icon viewed on maps in the VMX300(-E) client. Click Choose next to each condition to select the color settings for that condition. Note that you can configure a different color setting for each serial output device.

Unknown state: If the Serial Output Driver cannot open the port on the serial output device, the device icon is the color specified here.

Normal state: As long as the Serial Output Driver has not failed to open the port on the serial output device, the icon is the color specified here.

Alarm state: This function is reserved for future use.

CONFIGURE THE COMMUNICATIONS TAB

1. **Connection Type:** Specify the type of connection between the device driver and the serial output device.
   - DIRECT SERIAL: The device is connected using an RS-232 to RS-422 converter or using an RS-422 PC serial port.
   - INTERNET PROTOCOL: The device is connected to the serial port on a networked device.
2. **Settings:** Complete the instructions provided below for the appropriate connection type specified in Step 1. The settings must match the settings specified within the serial output device. Refer to the serial output device documentation for information on configuring the device's internal settings.

Direct Serial Settings

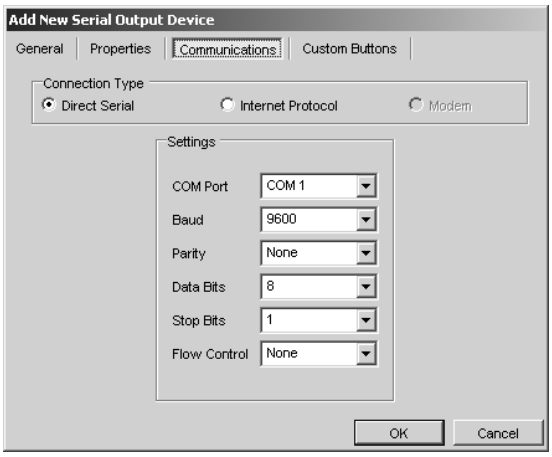


Figure 127. Communications Tab for Serial Output Device Serial Settings

a. Select the VMX300(-E) COM port the serial output device is connected to from the drop-down box. This is the COM port on the workstation that the Serial Output driver runs on.

b. The remaining settings should specify 9600 baud, no parity, 8 data bits, 1 stop bit, and no flow control.

Internet Protocol Settings

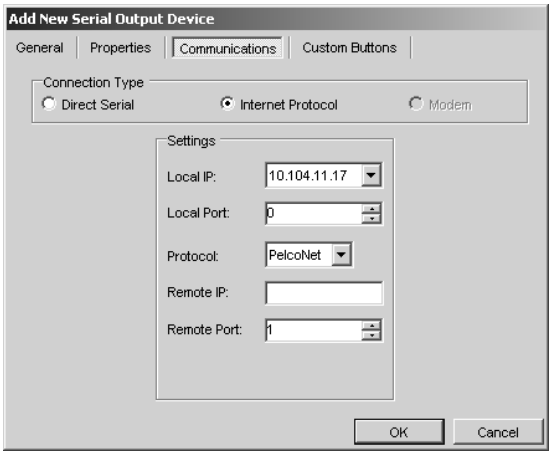


Figure 128. Communications Tab for Serial Output Device IP Settings

a. Local IP: The local IP is the IP address of the computer that the Serial Output Device driver runs on. Select the local IP from the drop-down box.

b. Local Port: The local port is the port the Serial Output Device driver uses to transmit commands. Enter the local port. If your system is secured behind a firewall, enter one of the ports made available by the firewall. Otherwise, enter 0 to have the driver randomly assign an available port.

When the local port is set to 0, the driver has many ports to choose from. If two or more users attempt to control the serial output device at the same time, the driver assigns a different port to each user.

When a specific (non-zero) port is selected, the driver is limited to using that one port. If two or more users attempt to control the serial output device at the same time, the port will only be available for the first user. Other users will be unable to control the device while the port is assigned to the first user.

TIP: To find out what port the driver assigned, switch or control the device in the VMX300(-E) client, and then use the netstat command at the DOS prompt to view assigned ports.

c. Protocol, Remote IP, Remote Port: The remote device is the device the serial output device is physically connected to. If the serial output device is connected to a PelcoNet device, follow the instructions in step (1). If the serial output device is connected to some other kind of device, follow the instructions in step (2).

(1) PelcoNet: Select the PelcoNet protocol from the Protocol drop-down box. If the PelcoNet device has a user name and password defined in the device settings, you will be prompted to enter the user name and password before proceeding. Enter the IP address of the PelcoNet device in the Remote IP box. In the Remote Port box, select the port on the PelcoNet device that the serial output device is connected to. Select 1 if the serial output unit is connected to COM 1 on the PelcoNet device. Select 2 if the serial output device is connected to COM 2.

(2) Other: Select the desired transport protocol from the Protocol drop-down box. Enter the IP address of the networked device in the Remote IP box. In the Remote Port box, enter the port on the networked device that serial output device is connected to.

CONFIGURE THE CUSTOM BUTTONS TAB

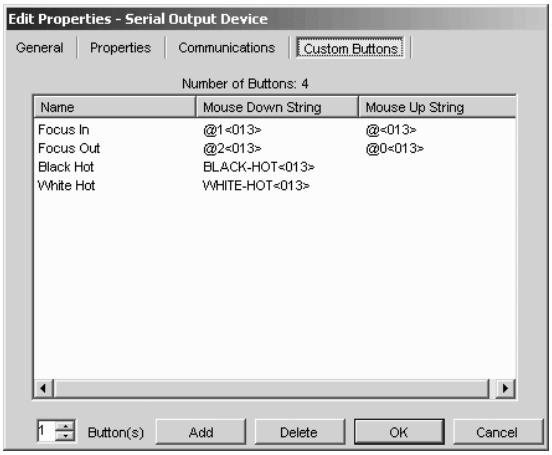


Figure 129. Custom Buttons Tab for Serial Output Device

Each custom button that you define for a serial output device appears in the device's Device Control dialog box in the VMX300(-E) client. The operator can then click the button to send the command(s) associated with the button to the serial output device.

Each custom button can have up to two strings associated with it. The mouse down string defines the command that is sent when the custom button is pressed. The mouse up string defines the command that is sent when the custom button is released.

Add a Custom Button

1. To add a new custom button click Add. The button appears in the list of custom buttons (in the Name column) with a generic name, and with no strings listed in the Mouse Down and Mouse Up columns.

   To add more than one custom button at once, enter the number of buttons you want to add in the Button(s) box, and then click Add. The specified number of new buttons will appear in the list of custom buttons.

2. To add a string to the custom button complete the instructions provided below, in Edit Custom Buttons.

Edit a Custom Button

1. Double-click the button in the Name column. The Edit Button dialog box appears.

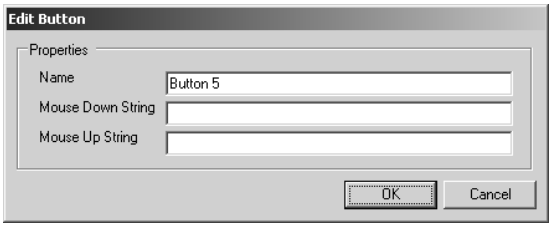


Figure 130. Edit Button Dialog Box

2. (Optional) Type a new name. The name appears on the custom button in the VMX300(-E) client. The name can include any letter, digit, or special character, with the exception of single and double quotation marks. Custom button names are not case sensitive.

3. Type a Mouse Down string. This is the command that is sent to the serial output device when an operator presses the custom button.

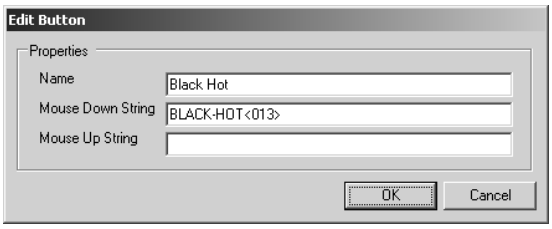


Figure 131. Sample Mouse Down String

4. (Optional) Type a Mouse Up string. This is the command that is sent to the serial output device when an operator releases the custom button. Leave this field blank if you do not want a command sent when the button is released.

5. Click OK. The Edit Button dialog box closes.

ASCII COMMAND SPECIAL CHARACTERS

If a command contains unprintable characters, replace each unprintable character with its three-digit ASCII code between angle brackets. For example, the command BLACK-HOT<Carriage Return> is represented in VMX300(-E) as BLACK-HOT<013>. Note that ASCII codes must be three digits in length. Add leading zeroes, if an ASCII code contains less that three digits.

If a command contains single or double quotation marks, replace the quotation marks with their ASCII codes: <039> for a single quotation mark and <034> for a double quotation mark.

Other useful ASCII codes for unprintable characters are <002> for the Start of Text (STX) character and <003> for the End of Text (ETX) character.

Delete a Custom Button

Click the custom button name in the list of buttons, and then click Delete. The button is removed from the list.

To delete more than one custom button at a time, select the buttons you want to delete and then click Delete. To select buttons that appear consecutively in the list, click the first button, and then press the Shift key and click the last button. To select buttons that are not consecutive, press the Ctrl key while clicking the buttons.

LIMITATIONS OF CONTROLLING A SERIAL OUTPUT DEVICE

Note that you cannot control a device under two different device drivers by configuring them with the same communications settings.

For example, suppose you have a camera that runs under a particular PTZ driver, and suppose the camera has certain features that are not supported by the PTZ driver. A tempting workaround might be to configure the camera under both the PTZ driver (so you can control the camera using the advanced controls made available by the PTZ driver) and the Serial Output Driver (so you can take advantage of custom buttons to access the additional features), but unfortunately, this will not work.

Only one device driver can have the communications port open. Whichever driver you launch first will open the port and be able to control the camera.

ADD AN IP DEVICE STATUS MONITOR

The IP device status monitor allows you to monitor the status of a networked device. Since almost every other VMX300(-E) device driver allows you to monitor the status of that device, you would only need to use the IP device status monitor to keep track of an IP device that is not in the VMX300(-E) system.

When you add an IP device status monitor to the VMX300(-E) system, it acts as a placeholder for the IP device. The IP device status monitor periodically pings the IP device, and if the device fails to respond to the ping, then the following actions occur:

- The IP device status monitor's Status read property is set to Alarm.
- The IP device status monitor icon flashes alternately between the two alarm colors.

If you define an alarm or event to be triggered when the IP device status monitor's Status property equals Alarm, then you can script a response and alert operators of the device status, so that they can take appropriate action.

Example: Configure a status monitor for an encoder/decoder that is not in the VMX300(-E) system. You can then define an alarm that prompts an operator to ask a technician to troubleshoot the encoder/decoder if it remains inaccessible for more than a minute.

Before you can add a IP device status monitor to the server configuration, you must first start the device driver—either on the server workstation or on the network—and then add the driver to the server configuration. Refer to the *Device Drivers* section for instructions.

1. Navigate the Object Browser tree to [project name] > Device Drivers > IP Monitor Driver > Devices.
2. Double-click <Add New Device>. The Add New Device dialog box appears.

   You can also configure settings after you have added the device to the server configuration. Right-click the device, and then select Edit from the pop-up menu. The Edit Properties dialog box appears, which contains the same tabs and fields as the Add New Device dialog box.
3. Configure the device settings, as described in the following sections.
4. Click OK to close the Add New Device dialog box.

CONFIGURE THE GENERAL TAB

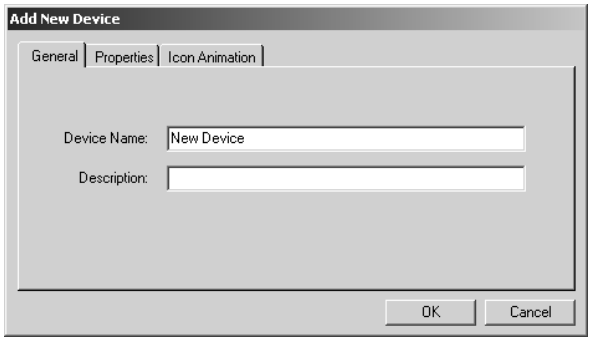


Figure 132. General Tab for an IP Device Status Monitor

Use the General tab to name and describe the IP device status monitor. The status monitor name can be a maximum of 31 characters. You cannot use single or double quotation marks in a name, but you can use any other letter, digit, or special character. Device names are not case sensitive. The optional description appears in the Object Browser beside the device name.

CONFIGURE THE PROPERTIES TAB

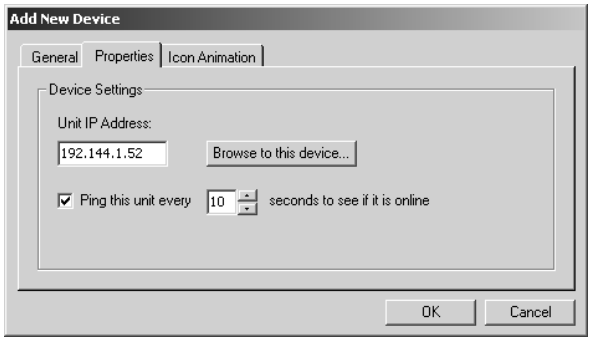


Figure 133. Properties Tab for an IP Device Status Monitor

1. Unit IP Address: Type the IP address of the device you want to monitor.
2. Browse: If the device you are monitoring has an embedded web server, click "Browse to this device" to open the embedded web server in a new window. This provides access to the device's internal configuration.
3. Ping this unit: To monitor the device, click "Ping this unit" and then enter the frequency, in seconds, with which you want the device monitored. To temporarily suspend monitoring, clear the check mark from the "Ping this unit" field.

CONFIGURE THE ICON ANIMATION TAB

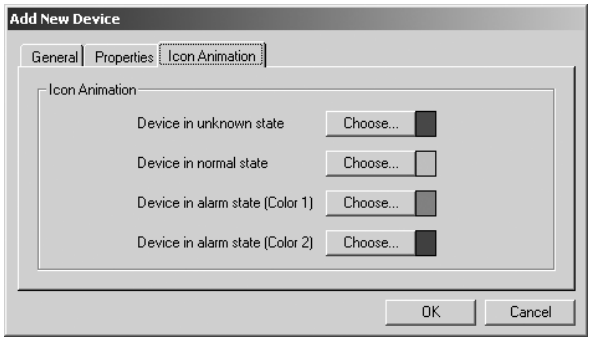


Figure 134. Icon Animation Tab for an IP Device Status Monitor

Use the Icon Animation tab to configure the animation settings of the status monitor icon viewed on maps in the VMX300(-E) client. Click Choose next to each condition to select the color settings for that condition. Note that you can configure a different color setting for each status monitor.

Unknown state: The unknown state occurs between the time the IP Monitor driver is launched and the device is first pinged. In this state, the status monitor's Status property has a value of Unknown and the icon is the color specified here.

Normal state: As long as the IP device responds when pinged, the status monitor's Status property has a value of Normal and the icon is the color specified here.

Alarm state: If the device fails to respond when pinged, the status monitor's icon flashes alternately between Color 1 and Color 2. Note, however, that flashing icons can increase the CPU workload. To reduce the overall workload, set Color 1 and Color 2 to the same color.

ADD AN ACCESS CONTROL DEVICE

The access control driver can be used to receive ASCII commands from an external serial (RS-232) device. For example, you could receive ASCII strings from a building access control system, an external alarm system, or an elevator control system. Any device controlled by the Access Control driver is referred to in this document as an access control device.

Use the access control driver to provide a video response from the VMX300(-E) system to a specified event in the external system.

Example: You have an elevator control system that indicates when each elevator moves to a different floor. You can program the elevator control system to send an ASCII string to the VMX whenever an elevator arrives on the first floor. The ASCII string can trigger the VMX system to switch a camera to track elevator activity on that floor.

HOW THE ACCESS CONTROL DRIVER WORKS

When an alarm is received by an access control device, the device transmits a serial string representing the alarm. VMX300(-E) attempts to match the alarm string to the access control information configured for that device. If a match is made, one of the device's read properties is set to True, which then triggers a VMX300(-E) alarm.

Two conditions must hold for VMX300(-E) to manage an alarm sent by an access control device:

- The point number in the alarm string must be the same as the number of a point specified on the Access Control Points tab. Refer to *Configure Access Control Points* for instructions.
- Some portion of the alarm string must match the Pattern To Match defined on the Pattern Matching tab. Refer to *Configure Pattern Matching for Incoming Alarm Strings* for instructions.

In addition to configuring the access control information, you must create the alarms and events that are triggered when a match is made. Refer to *Define Alarms Based on Access Control Points* for instructions.

After the VMX300(-E) alarm has been triggered, the point's property must be reset to False. Some access control devices send a reset string to indicate that the alarm condition no longer holds. In this case, you should define a Reset Pattern To Match. When VMX300(-E) matches an incoming string to the Reset Pattern To Match, VMX300(-E) resets the property to false. If the access control device does not send a reset string, you are responsible for resetting the property in one of the alarm's scripts.

Logic Used for the Access Control Driver

When the VMX300(-E) receives a string from an access control device one of the following situations occurs:

- If the string matches the Pattern To Match, and the point number in the string matches the number of a point defined on the Access Control Points tab, VMX300(-E) sets the point's read property to True.
- If a Reset Pattern To Match is defined, and the string matches the Reset Pattern To Match, and the point number in the string matches the number of a point defined on the Access Control Points tab, VMX300(-E) sets the point's read property to False.
- If the string doesn't match either of the patterns, or the point number in the string doesn't match the number of a point defined on the Access Control Points tab, VMX300(-E) discards the string.

ADD AN ACCESS CONTROL DEVICE TO THE SERVER CONFIGURATION

Before you can add an access control device to the server configuration, you must first start the device driver—either on the server workstation or on the network—and then add the driver to the server configuration. Refer to the *Device Drivers* section for instructions.

1. Navigate the Object Browser tree to [project name] > Device Drivers > Access Control Driver > Devices.
2. Double-click <Add New Device>. The Add New Device dialog box opens.

   You can also configure settings after you have added the device to the server configuration. Right-click the device, and then select Edit from the pop-up menu. The Edit Properties dialog box opens, which contains the same tabs and fields as the Add New Device dialog box.
3. Configure the device settings, as described in the following sections.
4. Click OK to close the Add New Device dialog box.
5. Configure alarms that use the access control points as the trigger. Refer to *Define Alarms Based on Access Control Points* for instructions.

CONFIGURE THE GENERAL TAB

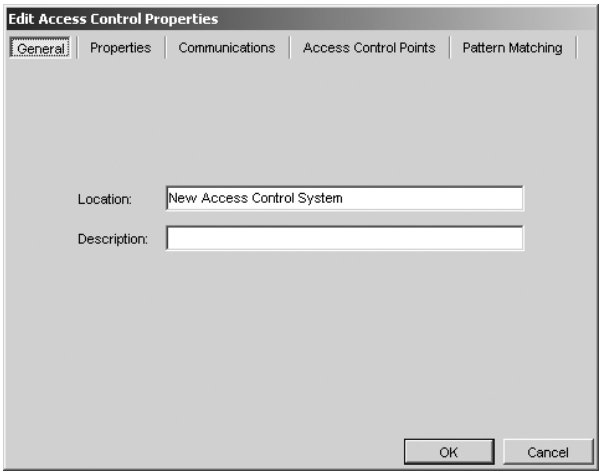


Figure 135. General Tab for an Access Control Device

Use the General tab to enter a location name and an optional description. The location name can be a maximum of 31 characters. You cannot use single or double quotation marks in a name, but you can use any other letter, digit, or special character. Location names are not case sensitive. The description appears in the Object Browser beside the device name.

CONFIGURE THE PROPERTIES TAB

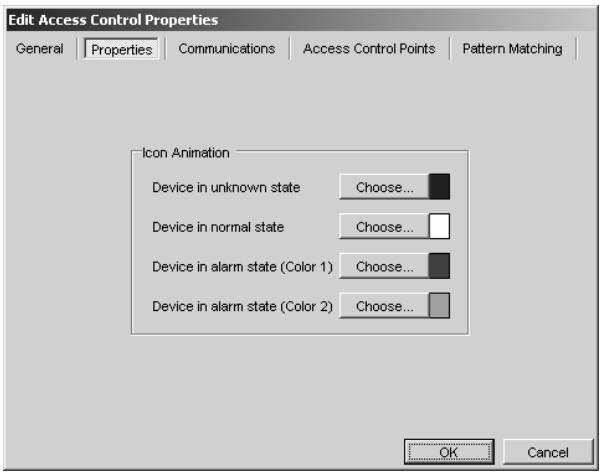


Figure 136. Properties Tab for an Access Control Device

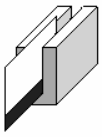


Figure 137. Access Control Device Icon

Use the Properties tab to configure the animation settings of the devices icon viewed on maps in the VMX300(-E) client. Click Choose next to each condition to select the color settings for that condition. Note that you can configure a different color setting for each access control device.

Unknown state: When the device driver cannot open the port, the icon is the color specified here.

Normal state: When the device driver is communicating normally with the device and the device's read properties all equal False, the icon is the color specified here.

Alarm state: When one or more of the device's read properties equal True, the icon flashes alternately between Color 1 and Color 2. Note, however, that flashing icons can increase the CPU workload. To reduce the overall workload, set Color 1 and Color 2 to the same color.

CONFIGURE THE COMMUNICATIONS TAB

1. **Connection Type:** Specify the type of connection between the device driver and the access control device.
   - Direct Serial: The device is connected using an RS-232 to RS-422 converter or using an RS-422 PC serial port.
   - Internet Protocol: The device is connected to the serial port on a networked device.
   - Modem: This feature is reserved for future development.
2. **Settings:** Complete the instructions provided below for the appropriate connection type specified in Step 1. The settings must match the settings specified within the access control device. Refer to the access control device documentation for information on configuring the device's internal settings.

Direct Serial Settings

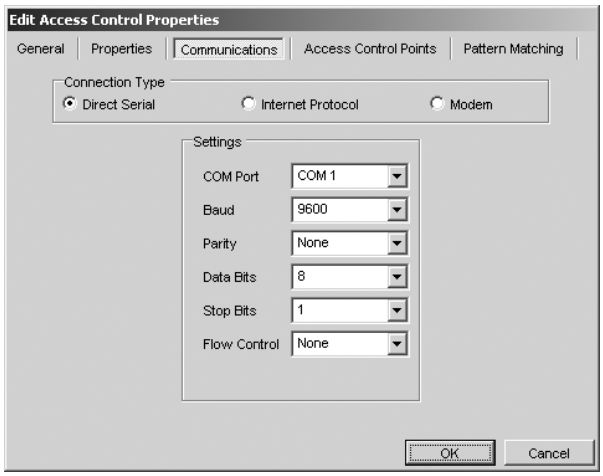


Figure 138. Communications Tab for Access Control Device Serial Settings

a. Select the VMX300(-E) COM port the access control device is connected to from the drop-down box. This is the COM port on the workstation that the Access Control driver runs on.

b. The remaining settings must match the values set in the access control device.

Internet Protocol Settings

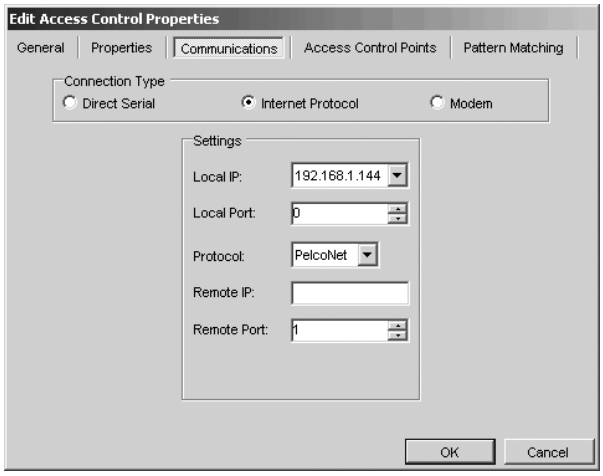


Figure 139. Communications Tab for Access Control Device IP Settings

a. Local IP: The local IP is the IP address of the computer that the Access Control Device driver runs on. Select the local IP from the drop-down box.

b. Local Port: The local port is the port the Access Control Device driver uses to transmit commands. Enter the local port.

c. Protocol, Remote IP, Remote Port: The remote device is the device the access control device is physically connected to. If the access control device is connected to a PelcoNet device, follow the instructions in step (1). If the access control device is connected to some other kind of device, follow the instructions in step (2).

(1) PelcoNet: Select the PelcoNet protocol from the Protocol drop-down box. If the PelcoNet device has a user name and password defined in the device settings, you will be prompted to enter the user name and password before proceeding. Enter the IP address of the PelcoNet device in the Remote IP box. In the Remote Port box, select the port on the PelcoNet device that the access control device is connected to. Select 1 if the access control device is connected to COM 1 on the PelcoNet device. Select 2 if the access control device is connected to COM 2.

(2) Other: Select the desired transport protocol from the Protocol drop-down box. Enter the IP address of the networked device in the Remote IP box. In the Remote Port box, enter the port the remote device's driver uses to receive ASCII strings. The remote port cannot be the same as the listening port used by any device driver.

CONFIGURE ACCESS CONTROL POINTS

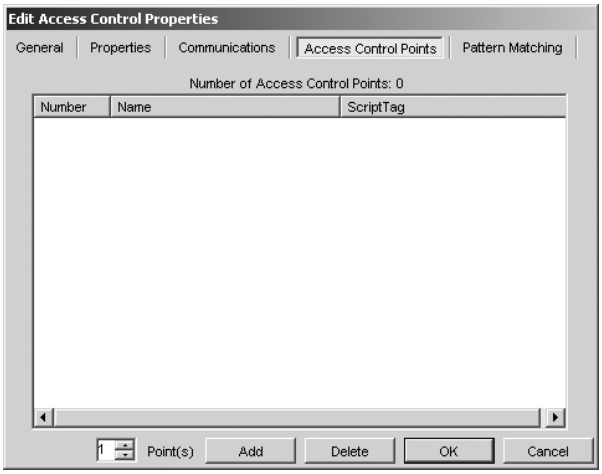


Figure 140. Access Control Points Tab

The Access Control Points tab is used to specify the access control alarms that you want VMX300(-E) to manage. For each alarm you want to be managed in VMX300(-E), add a point to the Access Control Points tab and assign it a number that identifies that alarm.

How VMX300(-E) Uses Access Control Points

Point number: VMX300(-E) uses the point number specified on the Access Control Points tab to identify which alarms to manage. If the point number in an incoming alarm string matches the number for a point defined on the Access Control Points tab, VMX300(-E) sets the read property for that point. If the point number does not match the number of a point defined on the Access Control Points tab, VMX300(-E) discards the alarm.

Choosing alarms: When VMX300(-E) is integrated with an existing access control installation, it is typical to configure VMX300(-E) to manage the same set of alarms as were being managed in the existing system. For a new installation, you will have to select the alarms you want VMX300(-E) to manage.

Determining point numbers: Some access control devices allow you to configure the number assigned to alarms. Other access control devices have preset numbers for alarms. If the access control device you are configuring uses preset numbers, refer to the device's product documentation to determine the numbers of the alarms you want VMX300(-E) to manage. If the access control device uses configurable numbers, determine the numbers from the device's internal configuration.

Points in the client: Each point you add to the server configuration appears in the Device Control dialog box in the VMX300(-E) client. When a particular alarm is triggered, the point for that alarm appears in bold print in the Device Control dialog box, allowing operators to monitor the status of the access control points.

Add Access Control Points

1. Type the number of access control points that you want to add in the Point(s) box, and then click Add.

   The specified number of new points appears in the list. New points are assigned sequential numbers, and generic names and script tags.

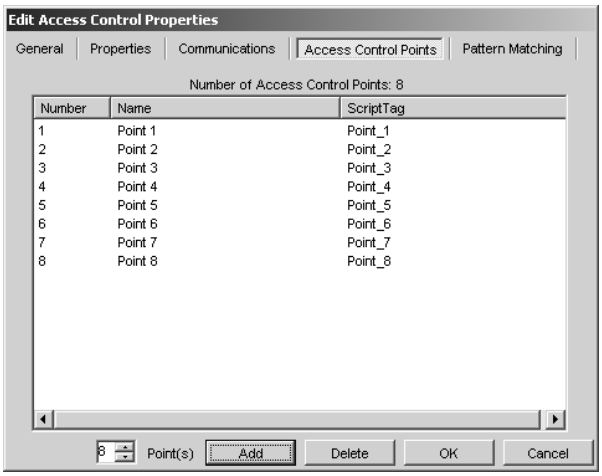


Figure 141. Adding Access Control Points

For each point that you add, one new read property and one new write property are added to the access control device when you exit the dialog box.

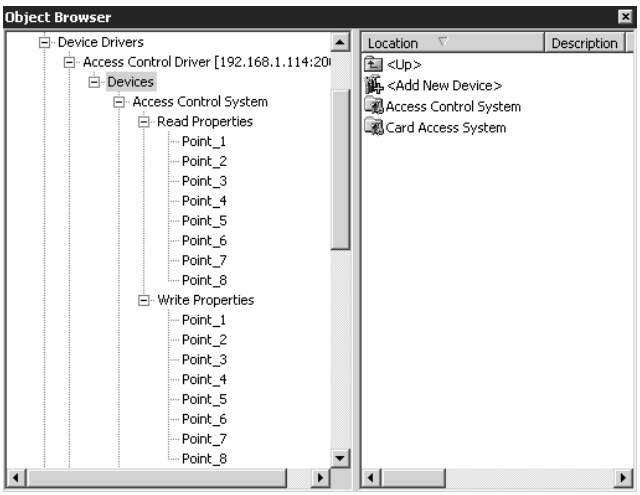


Figure 142. Access Control Device Read and Write Properties

2. To customize the number, name, or script tag of a specific point, double-click the point to open the Edit Point dialog box. Refer to *Edit an Access Control Point* for instructions.

Edit an Access Control Point

Edit each access control point so that the point's number is the same as the point number sent out in the string for that type of alarm. You can also change a point's name and script tag, or use the generic name and tag assigned by VMX300(-E).

1. Double-click the desired access control point. The Edit Point dialog box opens.

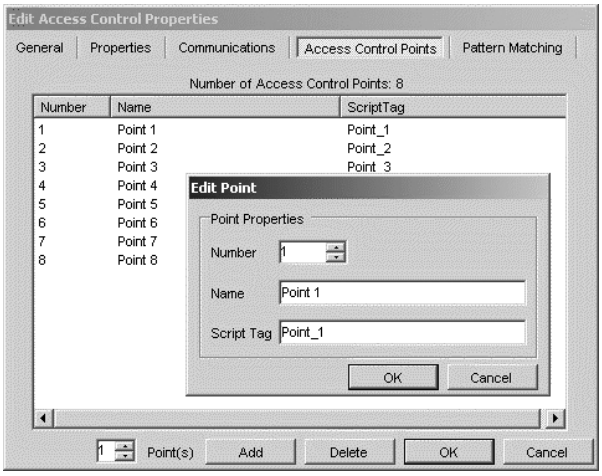


Figure 143. Edit Point Dialog Box

2. Type a new point number. Set this number to match the point number sent out by the access control device when that type of alarm occurs. VMX300(-E) manages an alarm only if the point number in the string matches a point number on the Access Control Points tab. VMX300(-E) discards any incoming alarm that does not match the number of a point defined on the Access Control Points tab.

3. (Optional) Type a new point name. The name appears in the Device Control dialog box in the VMX300(-E) client. The name must be unique and can include any letter, digit, or special character, with the exception of single and double quotation marks. The name is not case sensitive. For example, NW door card reader is equivalent to NW DOOR CARD READER.

4. (Optional) Type a new script tag for the point. Use the script tag to refer to the point in scripts and expressions. For more information, refer to *Access Control Device Properties Exposed for Scripts and Expressions*.

   Script tags are at most 50 characters long. They can include any letter, digit, or the underscore character, but cannot begin with a digit. They cannot contain spaces or special characters. Script tags are not case sensitive. For example, Door_1 is equivalent to DOOR_1. The script tag must be unique.

5. Click OK. The Edit Point dialog box closes. The new numbers, names, and script tags appear on the Access Control Points tab, and in the Device Control dialog box in the VMX300(-E) client. The device's read and write properties are renamed based on the new script tags.

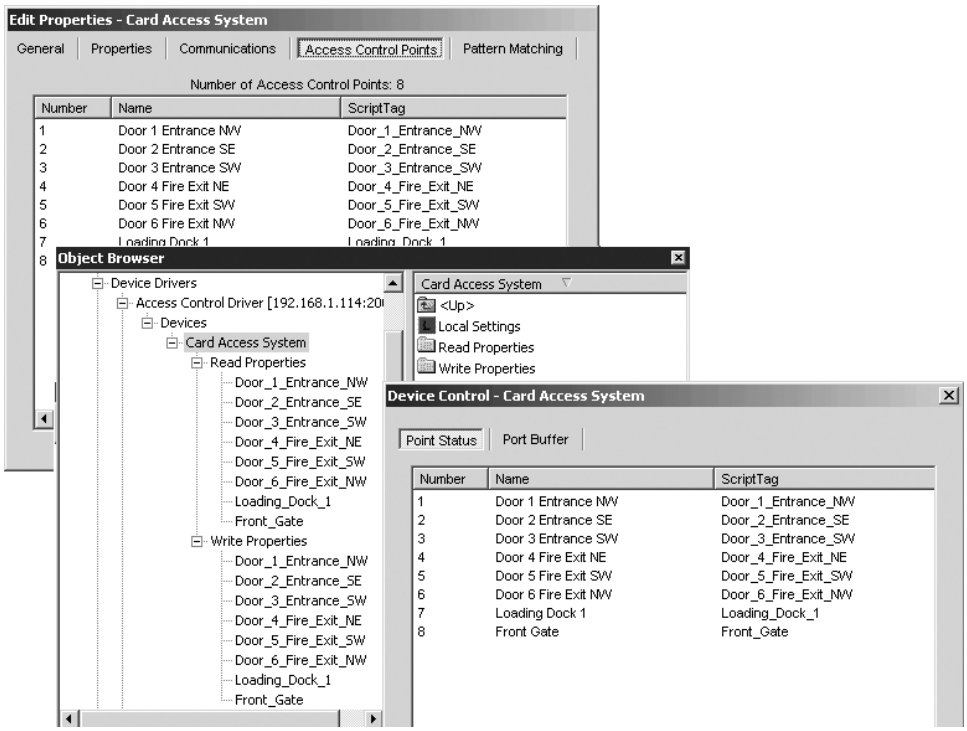


Figure 144. Edited Access Control Points

Delete an Access Control Point

Click the point that you want to delete, and then click Delete.

To select multiple points, hold the Ctrl key down while clicking each point that you want to delete.

CONFIGURE PATTERN MATCHING FOR INCOMING ALARM STRINGS

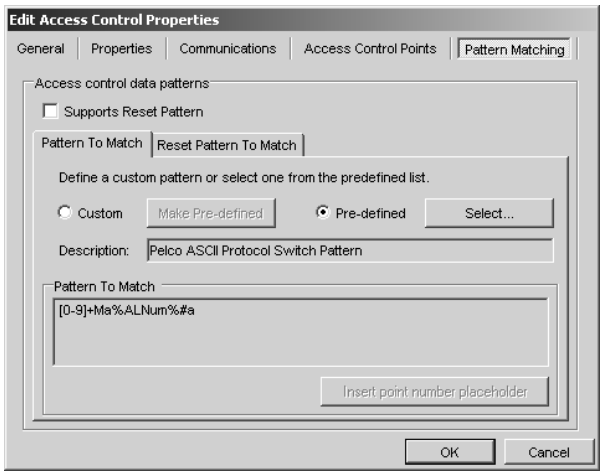


Figure 145. Pattern Matching Tab

The Pattern Matching tab is used to configure the pattern(s) that incoming alarm strings must match as the first step in identifying alarms to be handled by VMX300(-E). If an incoming string matches one of the patterns, VMX300(-E) attempts to match the point number in the string to the number of a point defined on the Access Control Points tab. If a match is found, VMX300(-E) sets the value of the point's read property. If no match is found, VMX300(-E) discards the string.

The Pattern Matching tab allows you to define the following patterns:

- **Pattern To Match:** Use this section to configure the pattern that matches the string that will be sent when an alarm has been tripped. Every access control device must have a Pattern To Match defined for it. When an incoming string matches the Pattern To Match and the point number in the string matches a point number on the Access Control Points tab, VMX300(-E) sets the read property for that point to True.
- **Reset Pattern To Match:** (Optional) Use this section to configure the pattern that matches the reset string, which is the string sent when an alarm condition is no longer in place. When an incoming string matches the Reset Pattern To Match and the point number in the string matches a point number on the Access Control Points tab, VMX300(-E) resets the read property for that point to False. If the access control device does not send a reset string, you do not need to define this pattern.

You can use either a predefined pattern or a custom pattern. You can also define a custom pattern and then save it to the list of predefined patterns for later use. Refer to *Create a Custom Pattern as the Pattern to Match* and *Create a Custom Pattern as the Reset Pattern to Match* for instruction on saving custom patterns.

Select a Predefined Pattern as the Pattern to Match

1. Click the Pattern To Match tab.
2. Click "Pre-defined," and then click Select. The Pre-defined Patterns list opens.

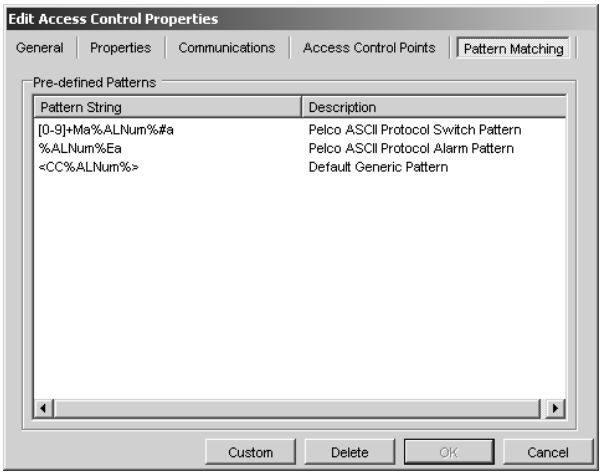


Figure 146. Predefined Patterns List

VMX300(-E) provides the following predefined patterns:

- **Pelco ASCII Protocol Switch Pattern:** Use this pattern for any access control device that employs the Pelco ASCII Protocol to switch cameras to monitors in response to alarms. In this case, the point number in the alarm string is a camera number. Refer to *How to Define Alarms Based on Access Control Points: Example* for instructions on configuring VMX300(-E) to switch cameras to monitors in response to alarms.
- **Pelco ASCII Protocol Alarm Pattern:** Use this pattern for any access control device that sends out an actual alarm number, rather than a camera number, as the Pelco ASCII Protocol Switch Pattern does. The VMX300(-E) response to an alarm that matches this pattern is determined by the scripts you associate with the VMX300(-E) alarm or event that is triggered when the point's read property is set to True.
- **Default Generic Pattern:** Use this pattern for access control devices that allow you to customize the strings that are sent out when alarm conditions are detected.

For a description of the syntax used in the predefined patterns, refer to *Pattern Syntax.*

3. Double-click the pattern that you want to use. The Pre-defined Patterns list closes, and the selected pattern appears in the Pattern To Match box.

Create a Custom Pattern as the Pattern to Match

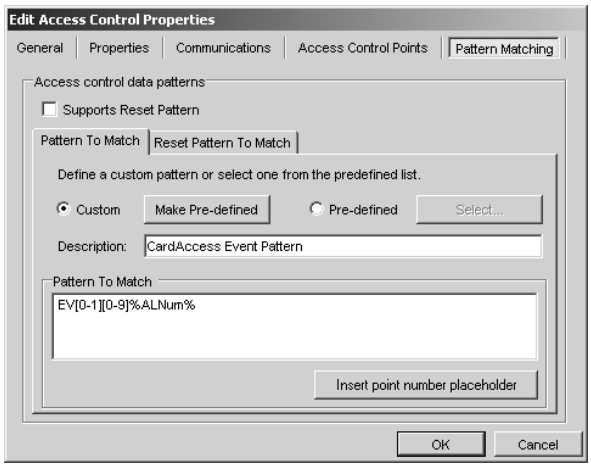


Figure 147. Create a Custom Pattern to Match

1. Click the Pattern To Match tab.
2. Click Custom.
3. Type a description of the pattern in the Description field. If you save the pattern to the Predefined Patterns list (step 5), the description will appear beside the pattern in the list.
4. Type the pattern. Refer to *Pattern Syntax* for information on creating patterns.
5. (Optional) Click Make Pre-defined to the pattern to the Predefined Patterns list. If you save the pattern, in the future you can select the pattern from the list.

Select a Predefined Pattern as the Reset Pattern to Match

Note that you only need to complete these steps if the access control device sends a reset string to indicate that the alarm condition is no longer in place.

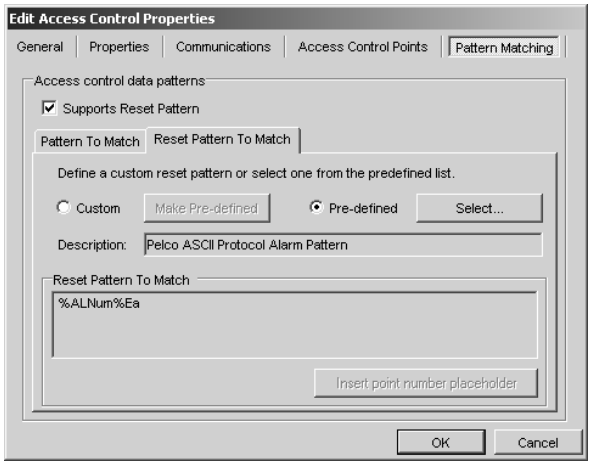


Figure 148. Assign a Reset Pattern to Match

1. Click the Supports Reset Pattern field.
2. Click the Reset Pattern To Match tab.
3. Click "Pre-defined," and then click Select. The Pre-defined Patterns list opens. Refer to *Select a Predefined Pattern as the Pattern to Match* for a description of the predefined patterns provided by VMX300(-E).
4. Double-click the pattern that you want to use. The Pre-defined Patterns list closes, and the selected pattern appears in the Reset Pattern To Match box.

Create a Custom Pattern as the Reset Pattern to Match

Note that you only need to complete these steps if the access control device sends a reset string to indicate that the alarm condition is no longer in place.

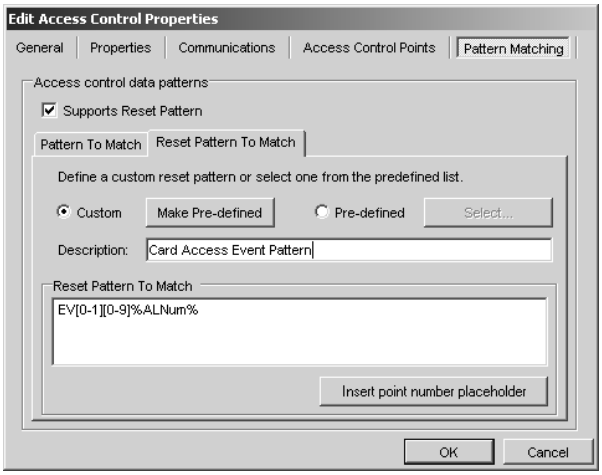


Figure 149. Create a Custom Reset Pattern to Match

1. Click the Supports Reset Pattern field.
2. Click the Reset Pattern To Match tab.
3. Click Custom.
4. Type a description of the pattern.
5. Type the pattern. Refer to *Pattern Syntax* for information on creating patterns.
6. (Optional) Click Make Pre-defined to the pattern to the Predefined Patterns list.

Pattern Syntax

A pattern is a regular expression that is used to match patterns of text in access control alarm strings. Patterns are written using special symbols, each of which describes one or more text strings.

Note that you can only define one Pattern To Match per access control device, so the pattern must be general enough to match every alarm string you want VMX300(-E) to manage.

Table C describes the symbols you can use to define patterns.

Point Number Placeholder: The point number placeholder is the symbol that matches the point number within the alarm string. The symbol for the point number placeholder is %ALNum%. Every Pattern To Match and Reset Pattern To Match must contain a single instance of the point number placeholder. To insert the point number placeholder into a pattern quickly and easily, click "Insert point number placeholder" in the Pattern matching Dialog box. You can also type in the point number placeholder.

Syntax in Predefined Patterns

- **Pelco ASCII Protocol Switch Pattern:** [0-9]+Ma%ALNum%#a

  This pattern matches a string that contains a number made up of one or more digits, followed by the literal Ma, followed by the point number, followed by the literal number sign (#), followed by the termination literal a.

- **Pelco ASCII Protocol Alarm Pattern:** ALNum%Ea

  This pattern matches a string that contains the point number, followed by the literal E, followed by the termination literal a.

- **Default Generic Pattern:** <CC%ALNum%>

  This pattern matches a string that contains the literal <CC, followed by the point number, followed by the literal >.

Table C. Symbols Used to Build Patterns

SYMBOL	MATCHES	EXAMPLE
\	Marks the following character as a special character or a literal.	Special character: **\w** is a special character that matches any letter, number, or the underscore (see below). Literal: **\$** means to ignore the special value of **$** and match the literal **$**. Similarly, **** matches **** and **\(** matches **(.**
\w	Matches any letter, number, or the underscore. Equivalent to **[a-zA-Z0-9_]**.	**ALARM\w** matches **ALARMx** and **ALARM9** and **ALARM_**, etc.
^	Matches the position at the beginning of an input string.	
$	Matches the position at the end of an input string.	
*	Matches the preceding subexpression zero or more times.	**zo*** matches **z** and **zo** and **zoo** and **zooo**, etc.
+	Matches the preceding subexpression one or more times. Equivalent to **{1,}**.	**zo+** matches **zo** and **zoo** and **zooo** and **zoooo**, etc.; does not match **z**.
?	Matches the preceding subexpression zero or one times. Equivalent to **{0,1}**.	**zo?** matches **z** and **zo**. Does not match **zoo**.
.	Matches any character except **\n** (newline).	To match any character including newline, use **[.\n]**.
{*n*}	Matches exactly *n* occurrences of the previous character or group of characters.	**o{2}** matches **root**. Does not match **rot** or **rooot**.
{*n,*}	Matches at least *n* occurrences of the previous character or group of characters.	**o{2}** matches **root** and **rooot** and **roooot**, etc. Does not match **rot**.
{*n/m*}	Matches between *n* and *m* occurrences of the previous character.	**o{2,3}** matches the first three **o**'s in **roooooot**.
xly	Either x or y	**g|food** matches **g** or **food**. **(g|f)ood** matches **good** and **food**.
[abcde]	A character set. Matches any one of the enclosed characters.	**[abcde]** matches the **a** in **plain**.
[^abcde]	The complement of a character set. Matches any single character not enclosed.	**[^abcde]** matches the **p** in **plain**.
[a-e]	A range of characters. Matches any character in the specified range.	**[a-e]** matches any lowercase alphabetic character in the range **a-e**, that is **a**, **b**, **c**, **d**, and **e**.
[^a-e]	The complement of a range of characters. Matches any character not in the specified range.	**[^a-e]** matches any character except **a**, **b**, **c**, **d**, or **e**.
(abc)	A grouping of characters.	**do(es)?** matches **do** and **does**. Does not match **doe** or **dos**.

Delete a Pattern From the Predefined Pattern List

1. On either the Pattern To Match tab or the Reset Pattern To Match tab, click Pre-defined, and then click Select. The Pre-defined Patterns list opens.
2. Click the pattern that you want to delete. You can only delete patterns that were created as custom patterns and then saved to the Pre-defined Patterns list with the Make Pre-defined feature. You cannot delete the predefined patterns that are provided with VMX300(-E).
3. Click Delete. The pattern is removed from the list.
4. Click Custom to return to the Pattern To Match tab or the Reset Pattern To Match tab.

DEFINE ALARMS BASED ON ACCESS CONTROL POINTS

The Access Control driver sets a read property to True when it identifies an alarm from an access control device. Any further action by VMX300(-E) depends on alarms and events created by you to detect the change in the read property's value. Depending on the nature of the alarm, you might want to simply archive a record of the alarm, or you might want to write scripts that perform complex tasks in response to the alarm.

Alarm Expression

To define a VMX300(-E) alarm or event that is triggered by an access control alarm, add a new alarm to the server configuration and base the alarm expression on the appropriate point. For example, to define a VMX300(-E) alarm that is triggered by a Point_3 alarm from the device AxCtrl, use the following expression:

AxCtrl.Point_3 = AxCtrl.True

Resetting Alarms

Once a VMX300(-E) alarm or event has been triggered by an access control alarm, you must reset the point's property to False. If you do not reset the property to False, the next time the access control device sends that alarm, the VMX300(-E) alarm will not be triggered, since VMX300(-E) detects the alarm based on the point's value changing from False to True.

Some access control devices send a reset string to indicate that the alarm condition no longer holds. In this case, you should define a Reset Pattern To Match. When VMX300(-E) matches an incoming string to the Reset Pattern To Match, VMX300(-E) resets the property to False. If the access control device does not send a reset string, you are responsible for resetting the property in one of the alarm's scripts.

TIP: Use the Suppress Subsequent Alarms feature to suppress alarms that are triggered in quick succession. Refer to the *Alarms and Events* section for more information.

How to Define Alarms Based on Access Control Points: Example

In this overview example, the access control device is named AxCtrl, and the access control point is named Point_1. The access control device in this example does not send a reset string.

Complete the following steps to configure VMX300(-E) to manage the Point_1 alarm.

1. (Optional) Create a recipient group. You can create a unique recipient group that is to be notified when a Point_1 alarm is received, or you can use an existing recipient group. Refer to the *Recipient Groups* section for instructions.
2. (Optional) Create an alarm/event category. You can create a unique alarm/event category for the access control alarm, or you can use one of the predefined categories. Refer to the *Alarm/Event Categories* section for instructions.
3. Create the alarm. Add an alarm with the following parameters:

   Expression: The expression must test whether Point_1 has the value of True.

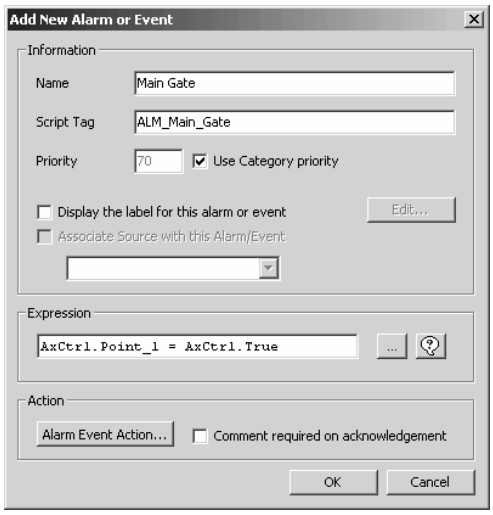


Figure 150. Add an Alarm for the Access Control Point

Action: Click Alarm Event Action to open the Alarm/Event Action dialog box. Create scripts to respond to the alarm. One of the scripts must set the point back to False, since the device does not send a reset string.

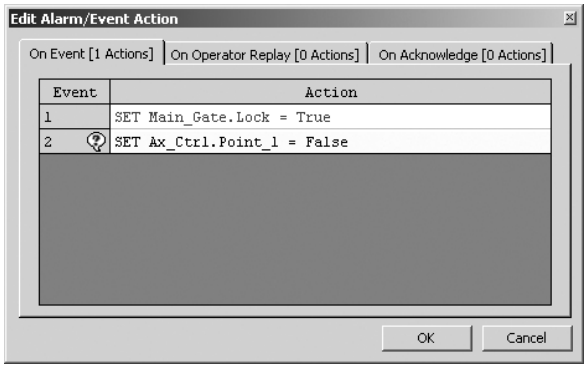


Figure 151. Associate Scripts with the Alarm

Refer to *Add a New Alarm or Event* in the *Alarms and Events* section for instructions on creating alarms.

Connections

Connections map out the analog connections between devices. You must define a connection for every analog connection in the system. This includes analog connections from IP devices.

MANAGING CONNECTIONS

Source devices and destination devices: Devices that transmit a signal are called source devices. For example, any device with video out, such as a camera, is a source device. Devices that receive signals are destination devices. For example, any device with video in, such as a monitor, is a destination device. Some devices, such as switchers, act as both sources and destinations.

1. Navigate the Object Browser to [project name] > Connections. In the right pane, double-click the type of connection you want to manage. The Connections dialog box opens. Source devices are listed in the left pane. Destination devices are listed in the right pane.

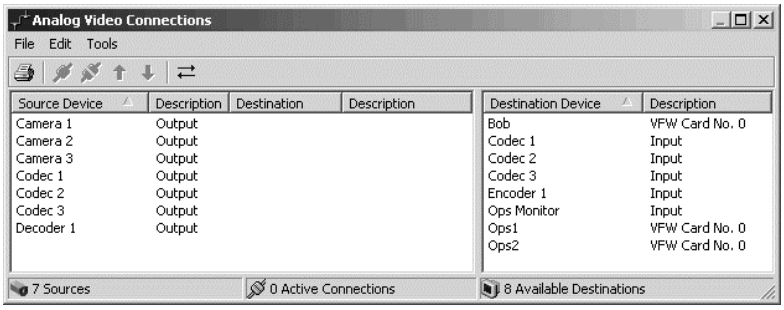


Figure 152. Connections Dialog Box

2. **Add a connection:**

   a. In the left pane, select the desired source device.

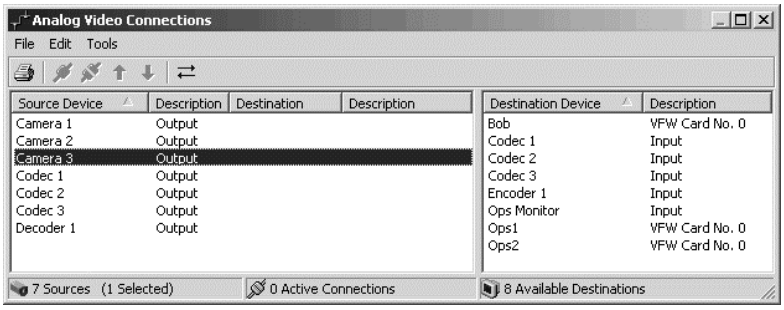


Figure 153. Selecting Source

   b. In the right pane, select the desired destination device and select Tools > Connect, or click the Connect button  , or double-click the destination device, or right-click one of the selected devices and select Connect from the pop-up menu.

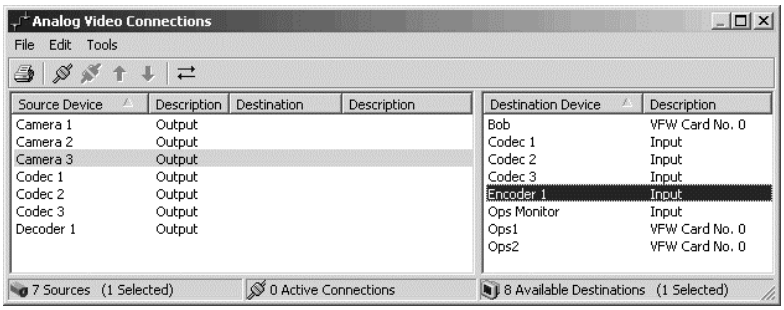


Figure 154. Selecting Destination

   The destination device moves beside the source device in the left pane.

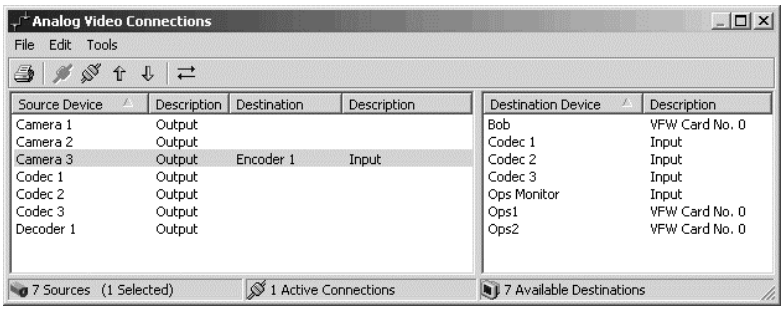


Figure 155. Making Connection

3. Add multiple connections:

   a. Select the source devices you want to connect. To select consecutive devices, select the first device, press and hold the Shift key down, then select the last device. To select nonconsecutive devices, hold the Ctrl key down while selecting. Now select the destination devices you want to connect to the sources.

   b. Click the Connect button , or select Tools > Connect, or right-click one of the selected devices and select Connect from the pop-up menu.

      The destination devices move beside the source devices in the left pane. The highest destination device in the list connects to the highest source device, the second highest destination connects to the second highest source, and so on.

      If you selected more destination devices than source devices, the extra destination devices at the bottom of the list remain unconnected. If you selected more source devices than destination devices, the extra source devices remain unconnected.

4. **Remove a connection:** In the left pane, select the connection you want to remove and select Tools > Disconnect or click the Disconnect button . Alternatively, double-click the connection, or right-click the connection and select Disconnect from the pop-up menu. The destination device moves to the right pane.

5. **Remove multiple connections:**

   a. In the left pane, select the connections you want to remove. To select consecutive connections, select the first connection, press and hold the Shift key down, then select the last connection. To select non-consecutive connections, hold the Ctrl key down while selecting.

   b. Select Tools > Disconnect, or click the Disconnect button , or right-click one of the selected connections and select Disconnect from the pop-up menu. The destination devices move to the right pane.

6. Remove all connections:

   a. Click the left pane to make it active. Select Edit > Select All, or press Ctrl-A, or right-click a connection and select Select All from the pop-up menu. All the connections are selected.

   b. Select Tools > Disconnect, or click the Disconnect button , or right-click one of the selected connections and select Disconnect from the pop-up menu. The destination devices move to the right pane.

7. **Modify a connection:** You can change which source device a destination device is connected to by moving the destination device up or down in the left pane.

   a. **Move up:** To move a destination device up in the list of connections, select the connection and select Tools > Move Up or click the Move Up button . Alternatively, right-click the connection and select Move Up from the pop-up menu.

      The destination device moves up to connect to the next available source device above it in the list, leaving the source device it was originally connected to unconnected. If all the source devices above the destination device are already connected, the destination device will not move.

b. **Move down:** To move a destination device down in the list, select the connection and select Tools > Move Down or click the Move Down button . Alternatively, right-click the connection and select Move Down from the pop-up menu.

The destination device moves down to connect to the next available source device below it in the list, leaving the source device it was originally connected to unconnected. If all the source devices below the destination device are already connected, the destination device will not move.

8. **Autosize column headers:** To adjust the width of the columns in the Connections dialog box, select Tools > Autosize Column Headers or click the Autosize Column Headers button . Columns that are not wide enough to accommodate the full device names are increased. Columns that are wider than they need to be are reduced.

9. **Print connections:**

   a. Select File > Print or click the Print button , or press Ctrl-P. The Print dialog box opens.

   b. Select the desired printer and click Print. The list of connections prints. The list includes additional information not provided in the Connections dialog box, specifically, the driver each device is configured under, and the driver's IP address and port.

10. When your connections are set up as you want them, click OK, or select File > Close, or click the Close button at the right end of the title bar. The Connections dialog box closes.

TIP: Double-click the Connections title bar to maximize the dialog box. Double-click again to restore it.

PELCONET CONNECTIONS

You must define connections that reflect how each PelcoNet is physically connected within the system.

Encode video directly from source device: The PelcoNet device encodes video directly from a source device, such as a camera. The PelcoNet device's input is connected to the source device's output:

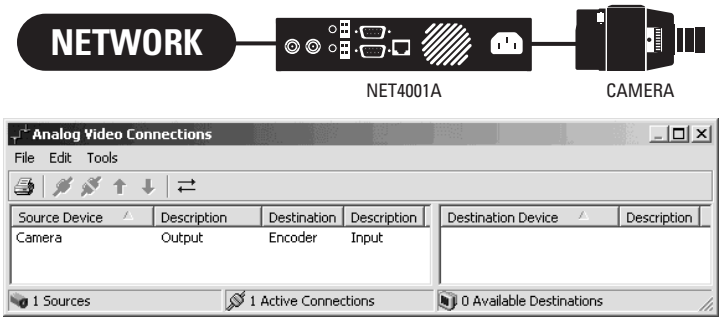


Figure 156. Encoding Video Directly

Encode video through switcher: The PelcoNet device encodes video that is switched from a source device, such as a camera. The PelcoNet device's input is connected to the switcher's output:

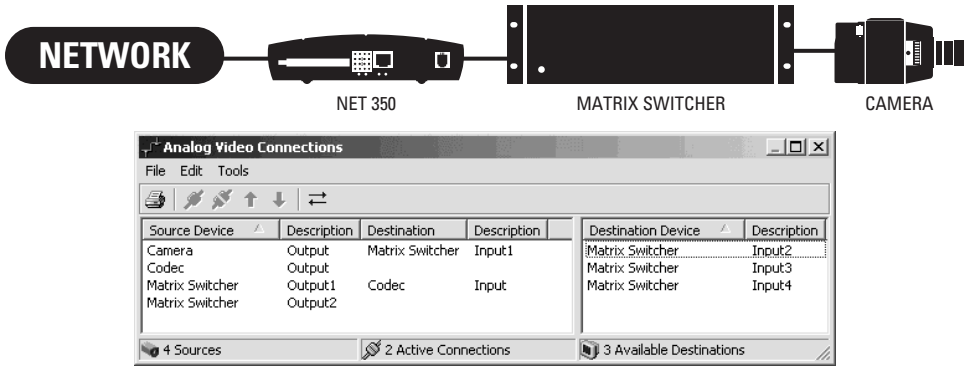


Figure 157. Encoding Video Through Switcher

Encode video from switcher's looping inputs: The PelcoNet device encodes video that is from a switcher's looping inputs. The PelcoNet device's input is connected to the appropriate looping input on the switcher:

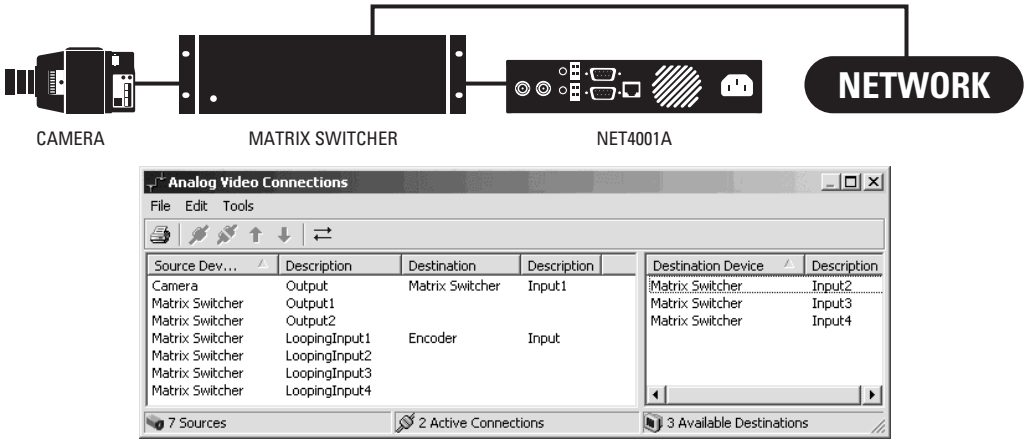


Figure 158. Encoding Looped Video

Decode video to output device: The PelcoNet device decodes video directly from an output device, such as an external monitor. The PelcoNet device's output is connected to the output device's input:

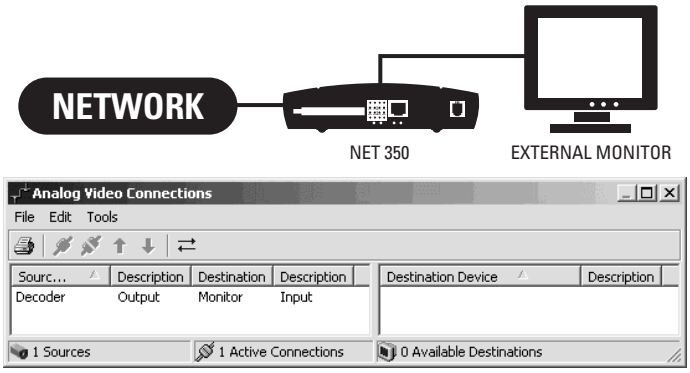


Figure 159. Decoding Video Directly

Decode video to switcher: The PelcoNet device decodes video that is switched to an output device, such as an external monitor. The PelcoNet device's output is connected to the switcher's input:

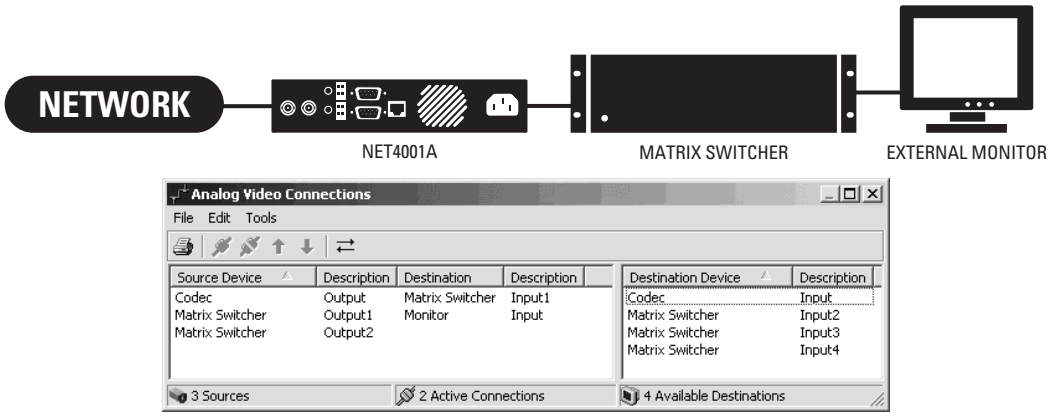


Figure 160. Decoding Video to Switcher

DVR CONNECTIONS

You must define connections that reflect how each DVR is physically connected within the system.

If a camera is connected directly to the recorder, define a connection from the camera's output to the appropriate input on the recorder. The following graphic illustrates a camera connected to Input 1 on a DX8000.

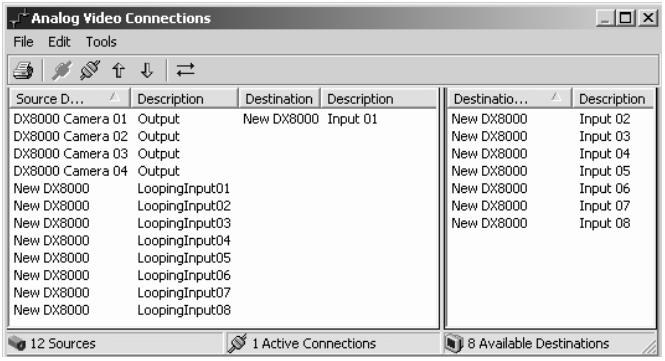


Figure 161. Connecting Video Directly to DVR

If a camera is connected to a recorder that loops video to a switcher, define the following connections:

- from the camera's output to the appropriate input on the recorder
- from the recorder's looping input to the appropriate input on the switcher

In the following example, Camera 1 is physically connected to Input 1 on the switcher, and the switcher's Looping Input 1 is physically connected to the DVR's Input 0:

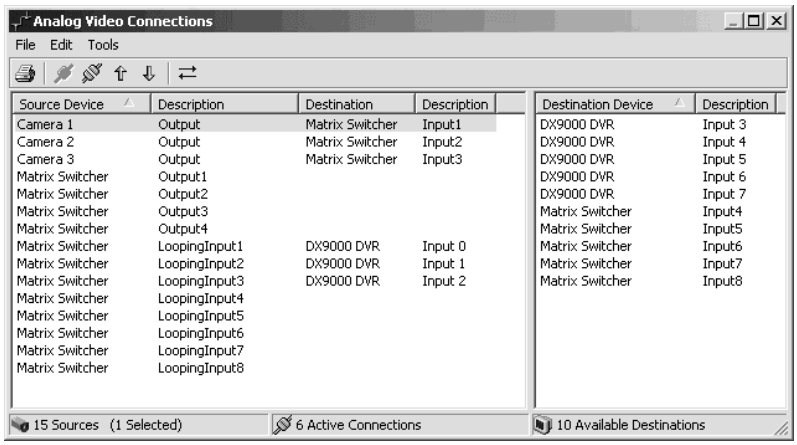


Figure 162. Connecting Video to DVR Through Switcher

ASCII CONNECTIONS

You must define connections that reflect how cameras and output devices are physically connected to the switcher. In addition, if a switcher has looping inputs, you must define connections for the looping inputs. Specifically, you must:

- Connect camera output to switcher input.
- Connect switcher output to output device input.
- Connect looping input to output device input.

The following example illustrates the connections for a switcher with four available outputs and eight available inputs that supports looping. In the example, logical numbering is not used. If logical numbering were used, the logical identifiers would appear in the dialog box.

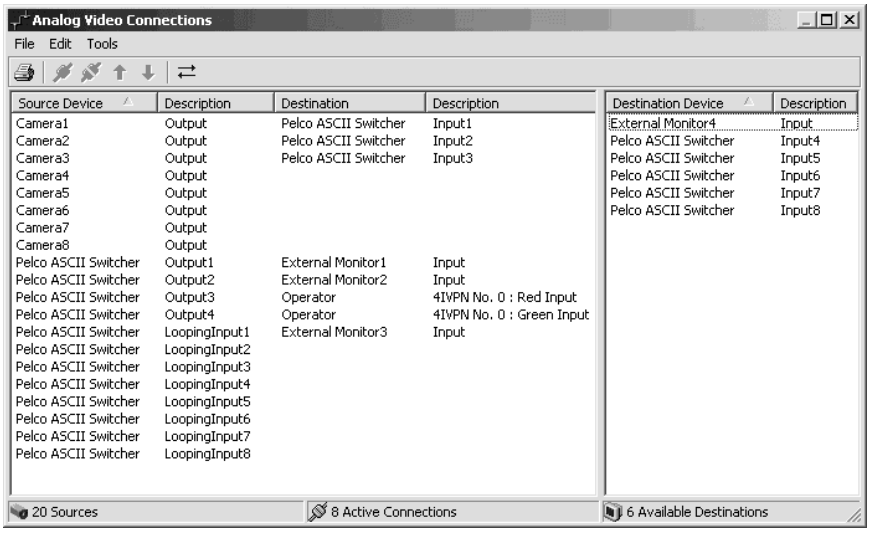


Figure 163. Connecting ASCII Devices

In the example, Camera1 is connected to Input1 on the switcher, Camera2 is connected to Input2, and Camera3 is connected to Input3. The switcher's other five available inputs do not have connections defined for them. Even if cameras are physically connected to those other inputs, VMX300(-E) will not be able to switch the cameras until connections are defined for them.

Two of the switcher's four outputs, Output1 and Output2, are connected to external monitors. The other two outputs are connected to a video display card's inputs on the client called Operator.

The switcher's LoopingInput1, which transmits the input from the switcher's Input1, is connected to External Monitor3. Since Input1 is connected to Camera1, External Monitor3 will always display the video from Camera1.

Archive Servers

Archive servers are used to permanently store information about alarms and events. When an alarm or event becomes complete, the following information about the alarm or event is recorded:

- Date and time the alarm or event was triggered
- Alarm/event name
- Server the alarm or event is defined on
- Alarm/event category
- Date and time the alarm or event was acknowledged
- User name of operator who acknowledged the alarm or event
- Operator comments entered when the alarm or event was acknowledged

Only alarms and events belonging to an alarm/event category that has archiving turned on are archived. Refer to *Alarms and Events - Alarm/Event Categories* for more information.

Alarms and events are archived in database files; a new file is created daily. The VMX300(-E) client provides tools to locate and view archived alarms and events. Refer to *Event Picker* and *Session Manager* in the VMX300(-E) Client Operation Manual for information on locating and viewing archived alarms and events.

Any workstation on the network can be used as an archive server, including a workstation that has the VMX300(-E) server or client application running on it.

START AN ARCHIVE SERVER

When you start an archive server, you have the choice of running it as an executable or as a service. If you ever have to restart an archive server that is run as an executable, you will have to follow the steps outlined here. To restart an archive server that is run as a service, restart the computer the driver is installed on, or start the server through the Windows Control Panel Administrative Tools.

For archives to be created or retrieved from an archive server, the archive server must be running.

To start an archive server:

1. Run the archive server application from the Windows Start menu, or double-click the archive server icon on the Windows desktop if there is one. The Configure Archive Server dialog box opens.

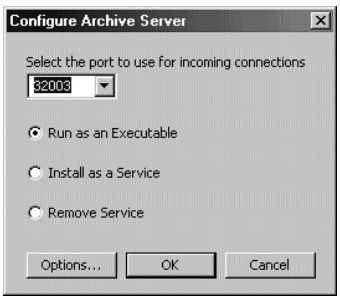


Figure 164. Configure Archive Server Dialog Box

2. If the archive server is currently installed to run as a service and you want to run it as an executable, click Remove Service, then click OK. Repeat step 1 to re-open the Configure Archive Server dialog box.
3. **Port:** Enter the port you want used by servers connecting to the archive server, or select the port from the drop-down list.
4. **Mode:**
    a. **Executable:** To run the archive server as an executable, click Run as an executable.
    b. **Service:** To run the archive server as a service, click Install as a service.
5. **Options:** Click Options to select the type of database you want to use for storing the archives.The Options dialog box appears.

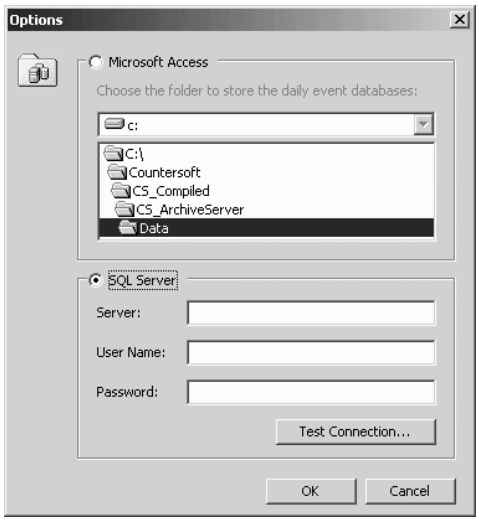


Figure 165. Archive Server Options Dialog Box

a. **MICROSOFT ACCESS:** To store archived alarms and events in Microsoft Access files, select **Microsoft Access.** Select the folder where the archive files will be stored from the drop-down list. You can change the folder at any time without shutting down the archive server. Refer to *View Archive Server Status* for instructions on selecting a folder once the archive server is running.

b. **SQL SERVER:** To store archived alarms and events on a SQL Server, select **SQL Server.**

(1) **SERVER:** Type the IP address or computer name of the SQL server that will store the archives.

(2) **USER NAME:** Type the SQL Server user name.

(3) **PASSWORD:** Type the SQL Server password.

(4) **TEST CONNECTION:** To make sure a connection can be made to the SQL server, click **Test Connection.**

A window opens that tells you whether the connection was successfully established or not. Click OK to close the window.

6. Click OK. The Configure Archive Server dialog box will close. If you are running the archive server as a service, start the server through the Windows Control Panel Administrative Tools, or restart the computer the archive server application is installed on. An icon representing the archive server will appear in the Windows system tray, indicating that the server is running.

VIEW ARCHIVE SERVER STATUS

1. Double-click the archive server icon in the Windows system tray, or right-click the icon and select Show from the pop-up menu. The Archive Server window opens.

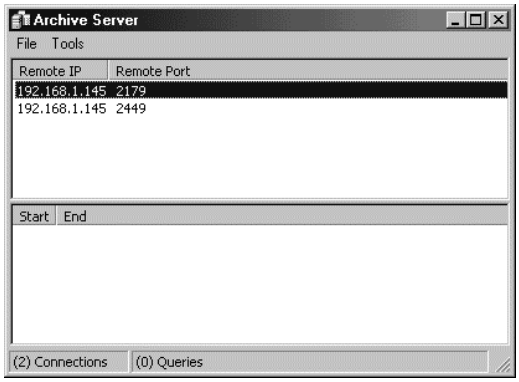


Figure 166. Archive Server Window

The top pane of the window lists the IP address and port number of the servers that are connected to the archive server, and any clients that are connected to those servers.

The bottom pane of the window lists the date range of any queries being made against the archives from the Session Manager. Queries include searches on a particular date or filters being applied. The information on queries is used for diagnostic purposes.

2. **Options:** To change the folder where the archive files are stored, click Tools > Options. The Options dialog box will open. Navigate to the desired folder and click OK.

3. **Close window:** To close the Archive Server window, right-click the archive server icon in the Windows system tray and select Hide from the pop-up menu, or click the Minimize button at the right end of the title bar.

4. **Shut down:** To shut down the archive server, click File > Exit, or click the Close button at the right end of the title bar. You will be asked to confirm. Click Yes.

SHUT DOWN AN ARCHIVE SERVER

1. Right-click the archive server icon in the Windows system tray and select Exit from the pop-up menu. Alternatively, select Show from the pop-up menu to open the Archive Server dialog box, then select File > Exit, or click the Close button at the right end of the title bar. You are prompted for confirmation.

2. If you are sure you want to shut down the archive server, click Yes. The archive server shuts down.

NOTE: If the archive server is running as a service, you can also shut it down through the Windows Control Panel Administrative Tools.

Project Properties

As part of the server configuration process, you must use the Project Properties dialog box to configure the following conditions:

- Which ports are used for clients, drivers, and FTP traffic
- How you want the server to select switch paths
- Whether archive servers and time servers will be configured
- Whether the server will be used as a primary server or as a backup server

Note that archive servers and backup servers are available only with VMX300-E systems.

To set the project properties, right-click the project name at the root of the Object Browser and select Edit from the pop-up menu. The Project Properties dialog box opens.

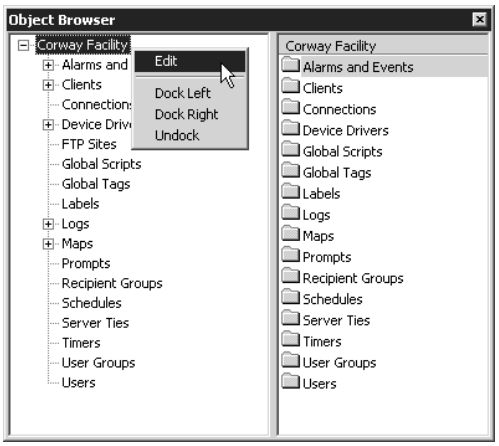


Figure 167. Opening Project Properties Dialog Box

NETWORK TAB

CONFIGURE A PRIMARY SERVER

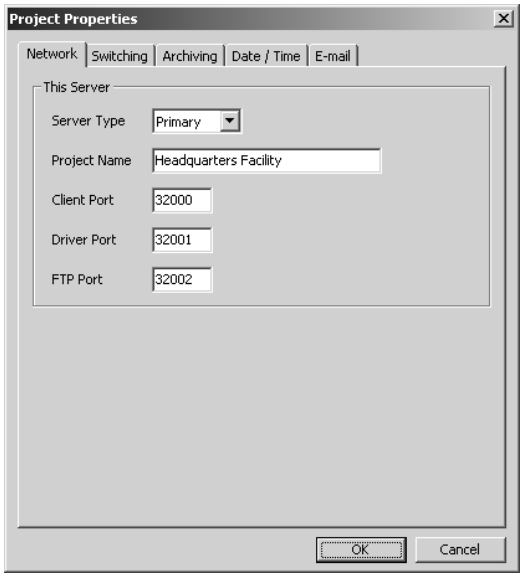


Figure 168. Configuring Primary Server

To configure a primary server:

1. **Server type:** The Server Type option is only available under software licenses that support backup servers. Select Primary from the drop-down list.
2. **Project name:** Type a descriptive name for the project. The project name is at least one character and at most 50 characters long and can include any letter, digit or special character, with the exception of single and double quotation marks. By default, the computer name is used as the project name.

   The project name appears at the top of the Object Browser. Wherever instructions for navigating the Object Browser are given in this manual, the top of the Object Browser is referred to as [project name].

   As well, the project name is used as the server name in server configuration mode and in the client. For example, if you browse servers when defining a server tie, the servers are listed by project name. Similarly, if you autodiscover servers when logging in to the client, the servers are listed by project name. The Session Manager also refers to servers using the project name.
3. **Client port:** Type the listening port the server will use to receive commands from clients. The default client port is 32000.
4. **Driver port:** Type the listening port the server will use to receive commands from drivers. The default driver port is 32001.
5. **FTP port:** Type the listening port the server will use to receive FTP commands. The default FTP port is 32002. All resource files, such as map files and server-supplied workspace files, are transferred from server to client using FTP.

CONFIGURE A BACKUP SERVER

NOTE: Backup servers are available only with VMX300-E systems.

Backup servers ensure that operations can continue in the event the primary server fails. If a backup server is running when the primary server fails, the backup server automatically steps in to take the place of the primary server. Operators logged in to the primary server experience a brief interruption as they are switched to the backup server. Operators have access to the same devices, maps, and workspaces as they did before the interruption, provided backups of the server and driver databases are up to date.

TIP: Connect serial-controlled devices in such a way that they can be controlled through both the primary server and the backup server. This ensures operators can control the devices in the event the primary server fails. If devices are connected to the primary server only, you will have to re-cable the serial-controlled devices to the backup server after a failure. IP devices require no special connection to be accessible by the backup server.

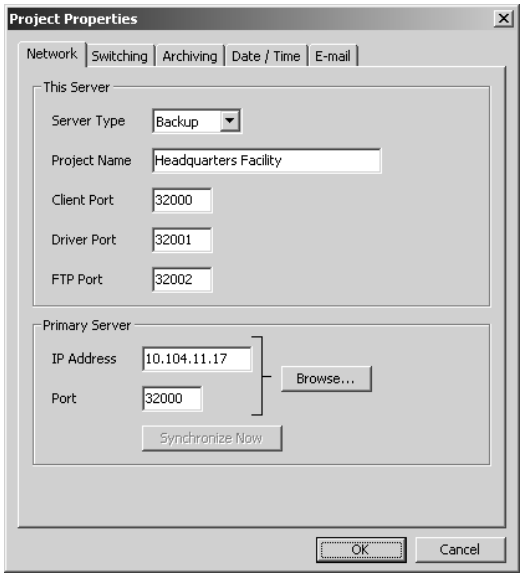


Figure 169. Configuring Backup Server

To configure a backup server:

1. **Server type:** The Server Type option is only available under software licenses that support backup servers. Select Backup from the drop-down list. Additional boxes appear at the bottom of the Network tab.

2. **Project name:** Type a descriptive name for the project. The project name is at least one character and at most 50 characters long and can include any letter, digit or special character, with the exception of single and double quotation marks. By default, the computer name is used as the project name. The project name for the backup server can be the same as the project name for the primary server.

   The project name appears at the top of the backup server's Object Browser. Wherever instructions for navigating the Object Browser are given in this manual, the top of the Object Browser is referred to as [project name].

   As well, the project name is used as the backup server name in server configuration mode and in the client.

TIP: Use a name that indicates that this is a backup. For example, if the primary server's project name is Corway Facility, name the backup server project Corway Facility Backup.

3. **Client port:** Type the listening port the backup server will use to receive commands from clients in the event the primary server fails. The default client port is 32000.
4. **Driver port:** Type the listening port the backup server will use to receive commands from drivers in the event the primary server fails. The default driver port is 32001.
5. **FTP port:** Type the listening port the backup server will use to receive FTP commands in the event the primary server fails. The default FTP port is 32002. All resource files, such as map files and server-supplied workspace files, are transferred from server to client using FTP.
6. **IP address:** Type the IP address of the primary server the backup server will be backing up, or click Browse to select a server from the drop-down list.
7. **Port:** Type the listening port configured as the Client Port on the primary server.
8. **Synchronize now:** For future development.

Once you have configured the backup server settings on the Network tab, it is recommended that you perform the following steps:

1. **Back up server database:** Copy the server database from the primary server to the corresponding directory on the backup server. This ensures that the backup server has the same configuration as the primary server.

   For example, assuming you installed VMX300(-E) in the default directory, copy c:\Program Files\ CS_Program Files\CS_Server.mdb from the primary server to the same location on the backup server.

   Whenever you change the primary server configuration, copy the updated server database to the backup server to ensure the backup is current.

2. **Back up device drivers and driver databases:** Backing up device drivers is recommended if the drivers are installed on the same computer as the primary server application, since access to the device drivers is lost if the computer fails.

   Install backup copies of all the device drivers used in your system, and copy each driver database to the backup location. This ensures that the backup server has access to all the device drivers it needs, in their current configuration.

   For example, assuming you installed VMX300(-E) in the default location, copy all the driver databases from c:\Program Files\CS_Program Files\ to the corresponding directory at the backup location. If the primary server is running on Windows 2000, also copy all driver databases from c:\WINNT\system32\CS_Components\COF\ to the backup location. If the primary server is running on Windows XP, copy the additional driver databases from c:\Windows\system32\CS_Components\COF\ to the backup location.

   Whenever you change how a device driver is configured in the primary server configuration, copy the updated driver database to the backup location to ensure the backup is current.

3. **Update driver information:** In server configuration mode on the backup server, edit each device driver in turn to change the IP address and listening port to the address and port of the computer the backup driver is installed on. This ensures that the backup server accesses the backup copies of the device drivers, rather than the primary copies.
4. **Run backup archive server:** Running a backup archive server is recommended if the primary archive server is installed on the same computer as the primary server application, since access to the archive server is lost if the computer fails.

   If you are archiving alarms and events, configure and run a backup archive server. This ensures the backup server can provide access to archived alarms and events.

   Launch the archive server at the backup location. On the Project Properties Archiving tab in the primary server configuration, add and select the archive server running at the backup location. You should have two archive servers configured on the primary server: the primary archive server and the backup. Alarms and events will be recorded on both archive servers.

NOTE: For automatic switchover to the backup server to occur, the backup server must be running when the primary server fails. The backup device drivers and archive server must also be running so the backup server can access them.

SWITCHING TAB

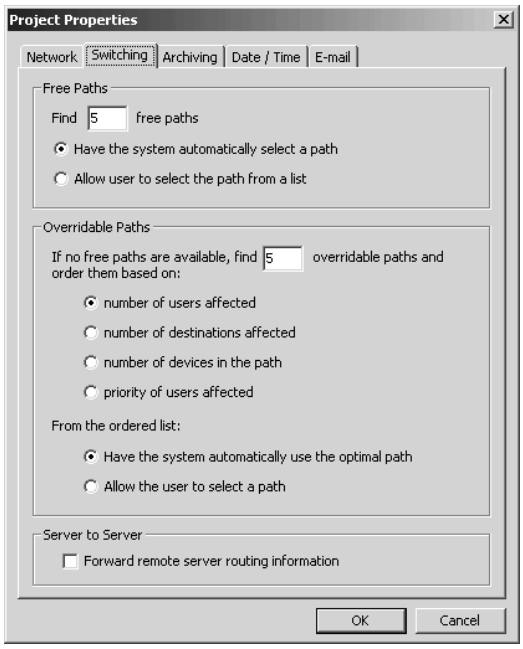


Figure 170. Switching Tab

The Switching tab allows you to specify how you want the server to select the switch path when a user or script accesses a video or audio device.

The server uses free paths (paths that are not in use) whenever possible. If there is only one free path, the server uses it automatically. When there are two or more free paths, the server finds as many free paths as you have specified, then either automatically uses the path through the least number of devices or presents the list to the user to select from.

A user or script with higher priority can override use of a path by a user or script with lower priority. In this case, the path is considered to be overridable. The server uses overridable paths only when there are no free paths. If there is only one overridable path available, the server uses it automatically. When there are two or more overridable paths available, the server finds as many overridable paths as you have specified, sorts them according to your specification, then either automatically uses the optimal path or presents the list to the user to select from.

NOTE: In most cases, automatic path selection is used.

1. **Free paths:** Type the number of free paths you want the server to find in the "Find free paths" box.

   If you want the server to automatically use the path it found that involves the fewest number of devices, select "Have the system automatically use the path through the least number of devices." If you want the server to present the list of free paths to the user to select from, select "Allow the user to select a path."

   Limiting the number of free paths speeds up switching. Limiting the number of free paths also keeps the list presented to the user a manageable length, when the user is allowed to select the path.

2. **Overridable paths:** Type the number of overridable paths you want the server to find in the "Find overridable paths" box.

   Select the criterion you want the server to use when finding overridable paths. You can choose to find paths that minimize the number of users affected, paths that minimize the number of destinations affected, paths that minimize the number of devices in the path, or paths that affect the lowest priority users.

   If you want the server to automatically use the optimal path from the list, click "Have the system automatically use the optimal path." If you want the server to present the list to the user to select from, click "Allow the user to select a path." When presented to the user, the list is sorted with the minimal path at the top of the list.

3. **Server to Server:** In a situation in which three (or more) servers have three-way server ties, it is possible for two of the servers to monopolize the other server's ties. Clearing Forward remote server routing information prevents other servers from monopolizing your server's available paths. To allow other servers to route signals through your server, select Forward remote server routing information.

   Refer to *Prevent Other Servers from Monopolizing Your Ties* in the *Server Ties* section for more information on the types of situation in which other servers might be able to monopolize your ties.

ARCHIVING TAB

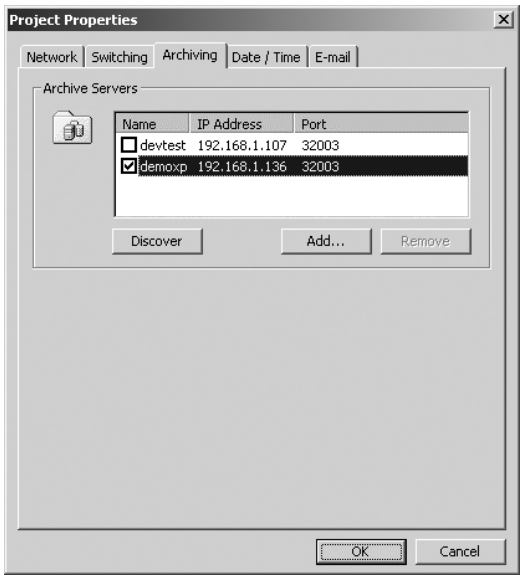


Figure 171. Archiving Tab

The Archiving tab allows you to define archive servers for recording alarms and events. Note that archive servers are available only with VMX300-E systems.

Only alarms and events that belong to an alarm/event category that has archiving turned on are recorded. Refer to *Alarms and Events - Alarm/Event Categories - Add a New Alarm/Event Category* for instructions on turning archiving on.

To record alarms and events, an archive server must be running when the alarm or event occurs. Refer to *Archive Servers - Start an Archive Server* for instructions on starting an archive server.

1. **Discover:** Click Discover to automatically locate all archive servers that are running.

2. **Add:** If you know the IP address and port number of a server that was not located automatically, click Add to add it manually. The Add Archive Server dialog box opens.

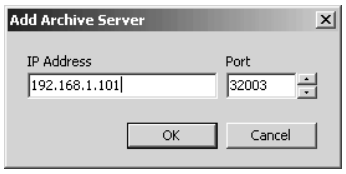


Figure 172. Add Archive Server Dialog Box

   Type the archive server's IP address and port number and then click OK.

3. **Select archive servers:** Alarms and events are recorded on every archive server that is selected on the Archiving tab when the alarm or event occurs, provided the archive server is running. Use the check box to the left of the archive server name to select the server. Clear the check box to the left of any archive server you do not want to archive data. To keep a duplicate copy of your archives, select two archive servers.

4. **Remove:** To remove an archive server from the list, select the server and click Remove.

DATE/TIME TAB

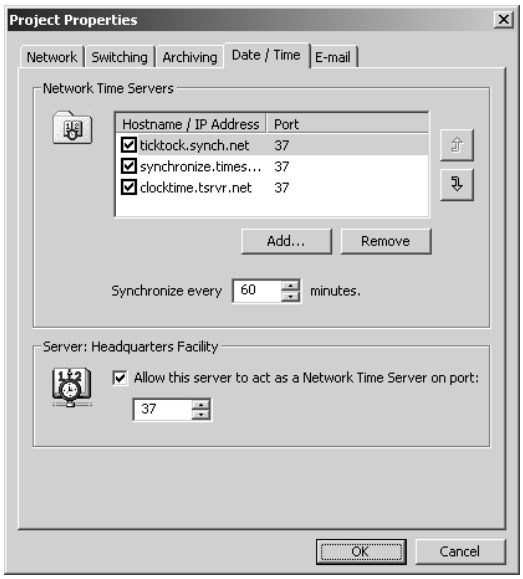


Figure 173. Date/Time Tab

The Date/Time tab allows you to configure a time server for the VMX300(-E) server to synchronize to.

1. **Add:** To add a time server, click Add. The Add Time Server dialog box opens.

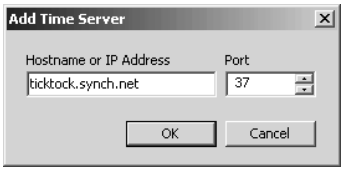


Figure 174. Add Time Server Dialog Box

   Type the time server's host name or IP address, and port number. Click OK.

2. **Select time servers:** The VMX300(-E) server will not attempt to synchronize to any time server whose check box is not checked. Select each time server you want the VMX300(-E) server to attempt to synchronize to. Clear the check box of any time server you do not want the VMX300(-E) server to attempt to synchronize to.

3. **Order list:** The VMX300(-E) server attempts to synchronize to the topmost selected server in the list, and, if that fails, the next selected server in the list, and so on, until there are no more selected servers in the list. To move a time server up in the list, select the server and click the up arrow to the right of the list. To move a server down in the list, select the server and click the down arrow.

4. **Remove:** To remove a time server from the list, select the server and click Remove.

5. **Frequency:** Use the "Synchronize every _ minutes" box to specify how often you want the VMX300(-E) server to synchronize its time to a time server.

6. **Network time server:** If you want to use the VMX300(-E) server as a time server for devices and other servers to synchronize to, select "Allow this server to act as a Network Time Server on port" and enter the port number.

TIP: In a multi-server system (VMX300-E only), you might want to synchronize one VMX300-E server with an Internet time server, then synchronize all the other VMX300-E servers on your network to the first, saving them from having to access the Internet to synchronize.

E-MAIL TAB

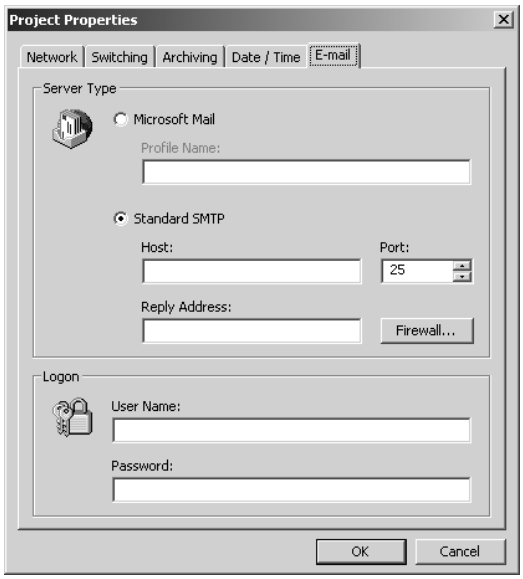


Figure 175. E-mail Tab

The E-mail tab allows you to specify an e-mail server so that alarm/event recipients can be notified of alarms and events by email. In order to notify recipients via e-mail the following criteria must be met:

- Recipients must have an e-mail address configured in their user settings. Refer to the *Users* section for information on configuring user accounts.
- The "Notify via E-mail" option must be selected for each alarm/event category for which e-mail notification will be used. Refer to the *Alarm/Event Categories* section for information on configuring alarm/event categories.

Complete the following steps to configure an e-mail server:

1. Select the appropriate server type. If you use a Microsoft mail server, follow the directions in step a. If you use an SMTP server, follow the directions in step b.

    a. Microsoft Mail: Click Microsoft Mail, and then type the Profile Name.

    b. Standard SMTP: Click Standard SMTP, and then complete the following fields:

    Host: This is the IP address or computer name of the SMTP server.

    Port: This is the listening port assigned to the SMTP server.

    Reply Address: This indicates where the e-mail is from, and appears in the "From" line of the e-mail header. This field is optional, however, some Internet providers reject e-mail that does not have a reply address.

    Firewall: Complete the steps listed in the Configure Firewall Settings section (following) if the SMTP server is behind one of the following types of firewalls:

    - Tunnel
    - Socks 4
    - Socks 5

CONFIGURE FIREWALL SETTINGS

(1) Click Firewall. The Firewall Settings dialog box appears.

(2) Select the type of firewall from the Type of Firewall drop-down box.

(3) Type the address of the firewall host; type either a web address, such as "www.fwallhost.com" or an IP address.

(4) Type the firewall host's listening port in the Port field.

(5) If the firewall host requires a user name and password, complete the Username and Password fields.

(6) Click OK. The Firewall Settings dialog box closes.

2. If the e-mail server requires a user name and password, complete the fields in the Logon section.

User Groups

User groups are a security feature. A user group embodies a set of privileges, called group permissions, that are granted to every member of the group. These permissions delineate which parts of the VMX300(-E) software group members can access. To limit a user's access to the software, restrict the user's permissions.

Setting up user groups requires forethought about what tasks you want different users to do. If you want a user to do a certain task, you must set up a user group with the permissions needed for that task, then make the user a member of that group. Conversely, if there are certain tasks that you want to preclude a user from carrying out, you must make sure the user does not belong to any group that grants the permissions needed for that task.

A user can belong to more than one user group. When a user who belongs to more than one group logs in to the VMX300(-E) server, the permissions are treated as cumulative in the sense that the user is granted all the permissions of each group he belongs to. For example, a user who belongs to two groups, Group A and Group B, has all the permissions of Group A in addition to all the permissions of Group B when logged in to the server.

Unlike the server, the VMX300(-E) client does not treat permissions cumulatively. When the user logs in, the client prompts the user to specify which group he wants to log in under. For the duration of that session, the user's permissions are limited to those granted by the group he logged in under. To exercise the permissions of another, different group he belongs to, the user must log out and log in again, this time logging in under the other group.

GROUP PERMISSIONS

Table D lists the group permissions available on an unconfigured server, and the privileges each permission grants. The core permissions fall into three categories: Administrative, Client Workspaces, and Window Content. Other categories are added to the list as needed. For example, when you first add a map to the server configuration, a Maps category is added to the Group Permissions.

Table D. Core Group Permissions

PERMISSION	ENABLES USER TO
Administrative	
Can configure software	Edit alarms and events, clients, connections, device drivers, labels, maps, global scripts, global tags, prompts, recipient groups, schedules, server ties, timers, user groups, users. View logs.
Can manage users	Edit users.
Can modify schedules	Edit schedules. View logs.
Client Workspaces	
Show 'All Devices' in device list	Include sublist that lists all devices in Device List.
Can load workspaces	Open workspaces. Set workspace preferences.
Can edit workspaces	Edit the current workspace.
Can save workspaces	Save the current workspace under its original name or under a new name.
Window Content	
Can view live video	View live video in an appropriately configured custom window.
Can view archived video	View archived video in an appropriately configured custom window.
Can view maps	View maps in a custom window.
Can view web pages	View an Internet browser in a custom window.
Can view remote PCs	View and control remote workstations in a custom window.

The following permissions are added to the group permissions as they become relevant:

- **Maps:** Selecting the permission for a particular map allows a user with that permission to view the map.
- **Global scripts:** Selecting the permission for a particular global script allows an operator with that permission to run the global script directly. This permission does not affect the execution of local scripts that call the global script.
- **Devices:** For a complete list of a device's permissions, refer to the following pages.

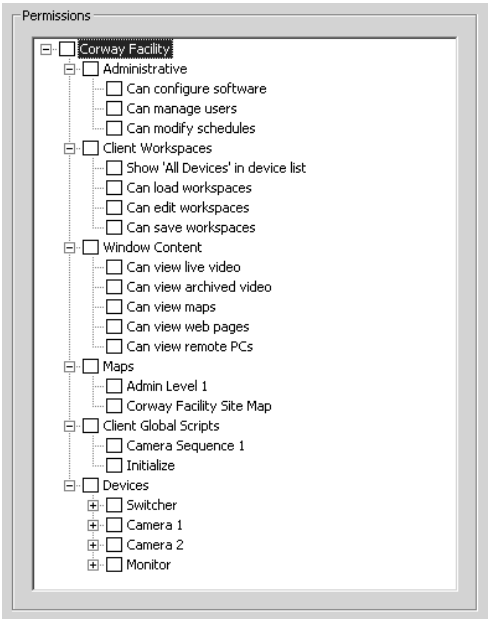


Figure 176. Group Permissions

FIXED CAMERA PERMISSION

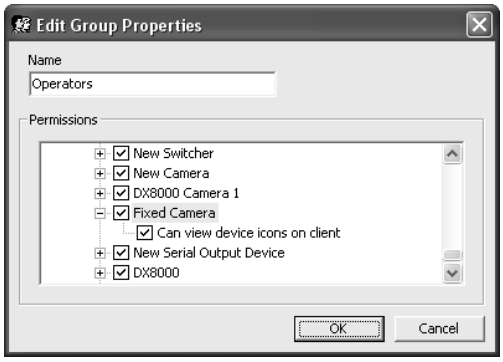


Figure 177. Fixed Camera Permission

Each Fixed Camera device that you configure appears in the Group Permissions list under Devices.

Table E. Fixed Camera Permission

PERMISSION	ENABLES USER TO
Can view device icons on client	Make Fixed Camera device icons visible in the client and list the device in the Device List.

PTZ PERMISSIONS

Each Pelco PTZ camera that you configure appears in the Group Permissions list under Devices.

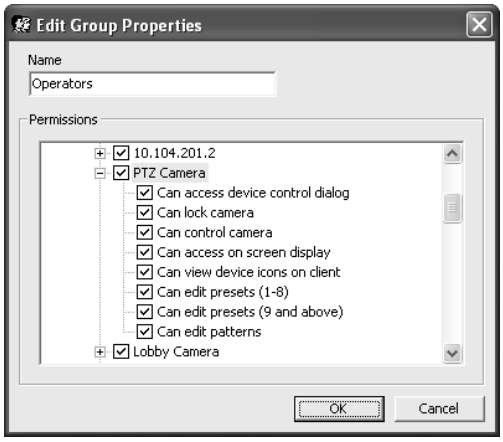


Figure 178. PTZ Permissions

Table F. PTZ Camera Permissions

PERMISSION	ENABLES USER TO
Can access device control dialog	Access the camera's Device Control dialog box in the VMX300(-E) client. This permission includes the ability to control the camera's auxiliaries.
Can lock device	Lock the camera in the client, preventing users and scripts with lower priority from controlling the camera.
Can control camera	In the VMX300(-E) client, pan, tilt, zoom, and focus the camera, adjust the iris, go to presets, and run patterns.
Can access on screen display	Access the On-Screen Display tab of the camera's Device Control dialog box in the client.
Can calibrate the camera	Do not use this permission; it is reserved for future use.
Can view device icons on client	Make Pelco PTZ camera icons visible in the client and list the camera in the Device List.
Can edit presets (1-8)	In the VMX300(-E) client, create, save, rename, and unassign presets numbered 1 to 8.
Can edit presets (9 and above)	In the VMX300(-E) client, create, save, rename, and unassign presets numbered 9 and higher, and set and clear the home preset.
Can edit patterns	In the VMX300(-E) client, create, save, rename, and unassign patterns, and set and clear the default pattern.

PELCONET DEVICE PERMISSIONS

Figure 179. PelcoNet Device Permissions

Each PelcoNet device you configure appears in the Group Permissions list under Devices.

Table G. PelcoNet Device Permissions

PERMISSION	ENABLES USER TO
Can access device manager dialog	Access device properties in the VMX300(-E) server.
Can access device control dialog	Access device controls in the VMX300(-E) client.
Can view device icons on client	Make PelcoNet device icons visible in the client and list the device in the Device List.
Can modify MPEG-4 or Stream 1 settings	For encoders, modify the MPEG-4 settings on the Encoding tab. For encoder/decoders, modify the MPEG-4 settings on the Encoding/Decoding tab. For decoders, do not use this permission; it is reserved for future use.
Can modify MPEG-2 or Stream 2 settings	For encoders, modify the MPEG-2 settings on the Encoding tab. For encoder/decoders, modify the MPEG-2 settings on the Encoding/Decoding tab. For decoders, do not use this permission; it is reserved for future use.

EXTERNAL MONITOR PERMISSION

Each external monitor device that you configure appears in the Group Permissions list under Devices.

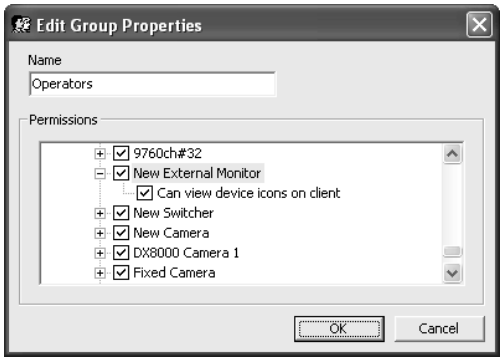


Figure 180. External Monitor Permission

Table H. External Monitor Permission

PERMISSION	ENABLES USER TO
Can view device icons on client	Make External Monitor device icons visible in the client and list the device in the Device List.

DX8000 PERMISSIONS

Each DX8000 device that you configure appears in the Group Permissions list under Devices.

DX8000 Recorder Permissions

Table I. DX8000 Recorder Permissions

PERMISSION	ENABLES USER TO
Can access device control dialog	Access the recorder's Device Control dialog box in the VMX300(-E) client.
Can lock device	Do not use this permission; it is reserved for future use.
Can control device	Do not use this permission; it is reserved for future use.
Can access on screen display	Do not use this permission; it is reserved for future use.
Can view device icons on client	Make DX8000 recorder icons visible in the client and list the recorder in the Device List.
Can edit presets (1-8)	Do not use this permission; it is reserved for future use.
Can edit presets (9 and above)	Do not use this permission; it is reserved for future use.
Can edit patterns	Do not use this permission; it is reserved for future use.

DX8000 Camera Permissions

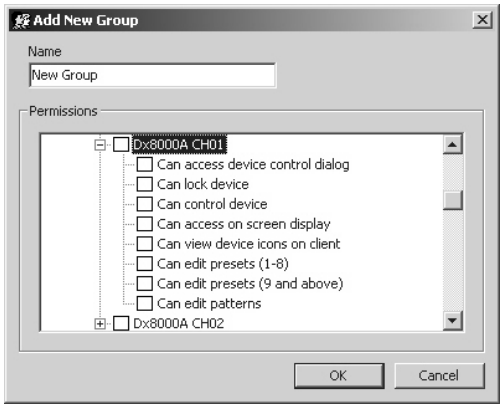


Figure 181. DX8000 Camera Permissions

Table J. DX8000 Camera Permissions

PERMISSION	ENABLES USER TO
Can access device control dialog	Access the camera's Device Control dialog box in the VMX300(-E) client.
Can lock device	Lock the camera in the client, preventing users and scripts with lower priority from controlling the camera.
Can control device	In the VMX300(-E) client, pan, tilt, zoom, and focus the camera, adjust the iris, go to presets, and run patterns.
Can access on screen display	Access the On-screen Display tab of the camera's Device Control dialog box in the client.
Can view device icons on client	Make DX8000 camera icons visible in the client and list the camera in the Device List.
Can edit presets (1-8)	In the VMX300(-E) client, create, save, rename, and unassign presets numbered 1 to 8.
Can edit presets (9 and above)	In the VMX300(-E) client, create, save, rename, and unassign presets numbered 9 and higher, and set and clear the home preset.
Can edit patterns	In the VMX300(-E) client, create, save, rename, and unassign patterns, and set and clear the default pattern.

DX9000 PERMISSION

Each DX9000 device that you configure appears in the Group Permissions list under Devices.

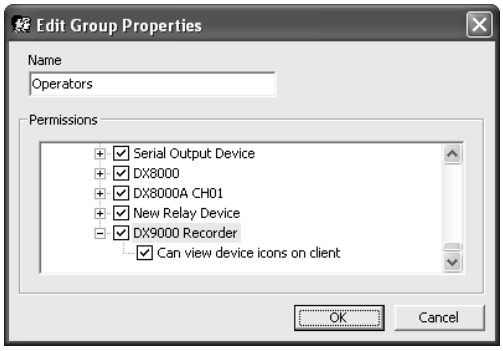


Figure 182. DX9000 Permission

Table K. DX9000 Permission

PERMISSION	ENABLES USER TO
Can view device icons on client	Make DX9000 icons visible in the client and list the DVR in the Device List.

ASCII DEVICE PERMISSIONS

Each ASCII device that you configure appears in the Group Permissions list under Devices.

ASCII Switcher Permissions

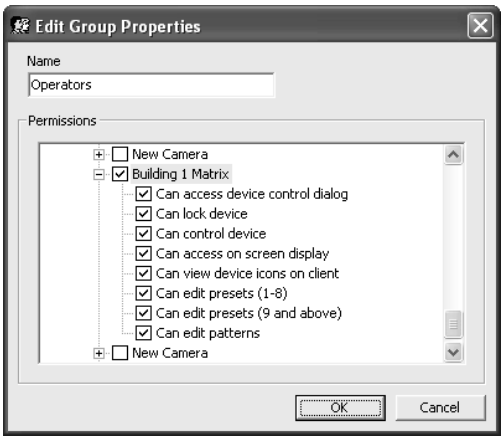


Figure 183. ASCII Switcher Permissions

Table L. ASCII Switcher Permissions

PERMISSION	ENABLES USER TO
Can access device control dialog	Access the switcher's Device Control dialog box in the VMX300(-E) client.
Can lock device	Do not use this permission; it is reserved for future use.
Can control device	In the VMX300(-E) client, set the switcher's date and time.
Can access on screen display	Access the On-Screen Display tab of the switcher's Device Control dialog box in the client.
Can view device icons on client	Make ASCII switcher icons visible in the client and list the switcher in the Device List.
Can edit presets (1-8)	Do not use this permission; it is reserved for future use.
Can edit presets (9 and above)	Do not use this permission; it is reserved for future use.
Can edit patterns	Do not use this permission; it is reserved for future use.

ASCII Camera Permissions

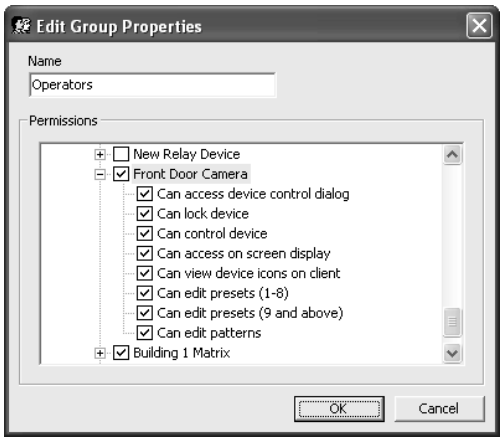


Figure 184. ASCII Camera Permissions

Table M. ASCII Camera Permissions

PERMISSION	ENABLES USER TO
Can access device control dialog	Access the camera's Device Control dialog box in the VMX300(-E) client. This permission includes the ability to control the camera's auxiliaries.
Can lock device	Lock the camera in the client, preventing users and scripts with lower priority from controlling the camera.
Can control camera	In the VMX300(-E) client, pan, tilt, zoom, and focus the camera, adjust the iris, go to presets, and run patterns.
Can access on screen display	Access the On-Screen Display tab of the camera's Device Control dialog box in the client.
Can view device icons on client	Make ASCII camera icons visible in the client and list the camera in the Device List.
Can edit presets (1-8)	In the VMX300(-E) client, create, save, rename, and unassign presets numbered 1 to 8.
Can edit presets (9 and above)	In the VMX300(-E) client, create, save, rename, and unassign presets numbered 9 and higher, and set and clear the home preset.
Can edit patterns	In the VMX300(-E) client, create, save, rename, and unassign patterns, and set and clear the default pattern.

KBD300A PERMISSION

Each KBD300A keyboard that you configure appears in the Group Permissions list under Devices.

Table N. KBD300A Permission

PERMISSION	ENABLES USER TO
Can view device icons on client	Make Pelco KBD300A icons visible in the client and list the device in the Device List.

CM9760-ALM PERMISSIONS

Each CM9760-ALM alarm interface unit that you configure appears in the Group Permissions list under Devices.

Table O. CM9760-ALM Permission

PERMISSION	ENABLES USER TO
Can access device control dialog	Do not use this permission; it is reserved for future use.
Can view device icons on client	Make alarm unit icons visible in the client and list the alarm unit in the Device List.

CM9760-REL PERMISSIONS

Each CM9760-REL relay interface unit that you configure appears in the Group Permissions list under Devices.

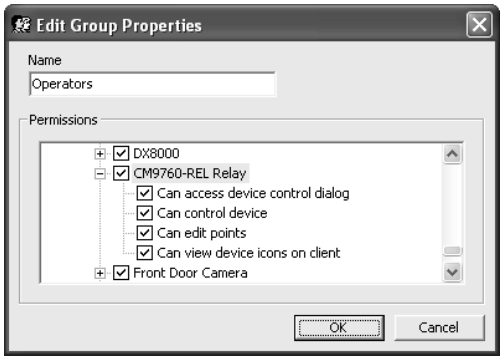


Figure 185. CM9760-REL Permissions

Table P. CM9760-REL Permissions

PERMISSION	ENABLES USER TO
Can access device control dialog	Access the relay unit's Device Control dialog box in the VMX300(-E) client. This permission alone allows the user to view, but not use, the controls available through the Device Control dialog box. In combination with the "Can control device" permission, this permission allows the user not only to view the controls, but also to use them.
Can control device	In combination with the "Can access device control dialog" permission, allows the user to set a relay unit's points to True, set the points to False, and use the Momentary feature.
Can view device icons on client	Make relay unit icons visible in the client and list the relay units in the Device List.
Can enable and disable points	In the VMX300(-E) client, disable points so they cannot change state, and re-enable disabled points. This permission does not affect enabling and disabling points in the server configuration.

SERIAL OUTPUT PERMISSIONS

Each serial output device that you configure appears in the Group Permissions list under Devices.

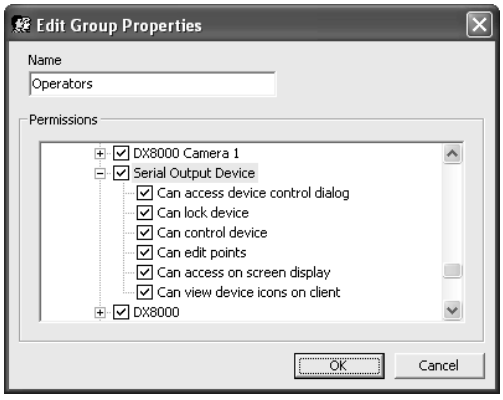


Figure 186. Serial Output Device Permissions

Table Q. Serial Output Device Permissions

PERMISSION	ENABLES USER TO
Can access device control dialog	Access the serial output device's Device Control dialog box in the VMX300(-E) client. This permission alone allows the user to view, but not use, the controls available through the Device Control dialog box. In combination with the "Can control device" permission, this permission allows the user not only to view the controls, but also to use them.
Can lock device	Do not use this permission; it is reserved for future use.
Can control device	Allows the user to run scripts that control the device. In combination with the "Can access device control dialog" permission, allows the user to send string commands using the Text tab or custom buttons in the client.
Can edit points	Do not use this permission; it is reserved for future use.
Can access on screen display	Do not use this permission; it is reserved for future use.
Can view device icons on client	Make serial output device icons visible in the client and list the device in the Device List.

IP DEVICE STATUS MONITOR PERMISSIONS

Each IP device status monitor that you configure appears in the Group Permissions list under Devices.

Table R. IP Device Status Monitor Permissions

PERMISSION	ENABLES USER TO
Can access device manager dialog	Do not use this permission; it is reserved for future use.
Can access device control dialog	If the device has an embedded web server, access the device's embedded web server from the VMX300(-E) client.
Can view device icons on client	Make IP device status monitor icons visible in the client and list the status monitor in the Device List.

ACCESS CONTROL DEVICE PERMISSIONS

Each Access Control device that you configure appears in the Group Permissions list under Devices.

Table S. Access Control Device Permissions

PERMISSION	ENABLES USER TO
Can access device control dialog	Access the device's Device Control dialog box in the VMX300(-E) client.
Can lock device	Do not use this permission; it is reserved for future use.
Can control device	Do not use this permission; it is reserved for future use.
Can edit points	Do not use this permission; it is reserved for future use.
Can access on-screen display	Do not use this permission; it is reserved for future use.
Can view device icons on client	Make device icons visible in the client and list the recorder in the Device List.

THE PREDEFINED USER GROUP

VMX300(-E) provides one predefined user group: Users. The Users group initially has all Window Content and Client Workspaces permissions, but no Administrative permissions. You can change the privileges granted by the Users group, rename the group, and delete the group. The predefined operator account belongs to the Users group. Refer to *Users - The Predefined Operator Account* for more information.

ADD A NEW USER GROUP

Once you have created a new user group, you can then make any new or existing user a member of the group. There is one exception: groups that grant the "Can configure software" permission are not available to users who can manage users but cannot configure software. This prevents users who can manage users but cannot configure software from giving themselves software configuration privileges.

You can create a new user group from scratch or you can base new groups on an existing group. To create a new user group based on an existing group, make a copy of the existing group and then edit the copy. Refer to *Pop-Up Menus* in the *Appendix* for information on using Copy and Paste or Paste Many to make copies of objects.

To create a new user group from scratch:

1. Navigate the Object Browser to [project name] > User Groups. Double-click <Add New User Group> in the right pane, or right-click User Groups in the left pane and select Add New from the pop-up menu. The Add New Group dialog box opens.

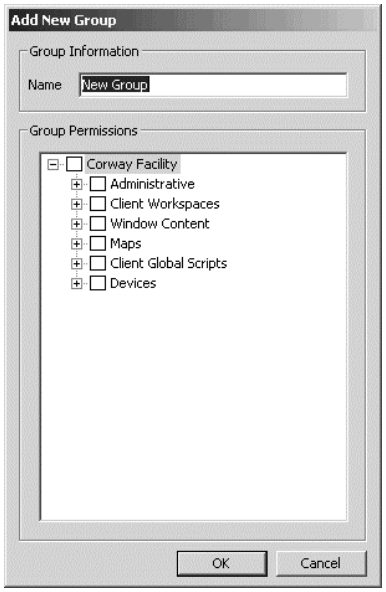


Figure 187. Add New Group Dialog Box

2. **Name:** Type in a unique, descriptive name for the group you want to add. User group names are at most 50 characters long. They can include any letter, digit or special character, with the exception of single and double quotation marks. User group names are not case sensitive.

3. **Permissions:** Select the permissions you want members of the new group to have. If necessary, click any plus signs to expand the list. To select all the permissions in a category, select the head category. Selecting [project name] at the top of the Group Permissions list selects all the permissions in the list.

4. Click OK. The Add New Group dialog box closes and the new group is created. The name of the new group appears in the right pane of the Object Browser.

TIPS:

- Selecting a category of permissions ensures that the user group has all permissions in that category, even if the category later acquires a new permission because a new object has been configured. For example, suppose you have a user group that includes personnel responsible for installing and maintaining devices. Select Devices to give group members access to all devices. If a new device is added to the server configuration, the group will automatically be given permission to access the new device.
- To select a permission for all similar devices at once, hold the Shift key down and select the permission for any one of the devices. The permission will be selected for every other device that has it. For example, to select the "Can lock camera" permission for all lockable cameras, regardless of make or model, hold down the Shift key when you select "Can lock camera" for any one camera. The permission will automatically be selected for every camera that has the permission.

EDIT A USER GROUP

To change the properties of an existing user group:

1. Navigate the Object Browser to [project name] > User Groups. In the right pane, double-click the user group you want to change, or right-click the group and select Edit from the pop-up menu. The Edit Group Properties dialog box opens.

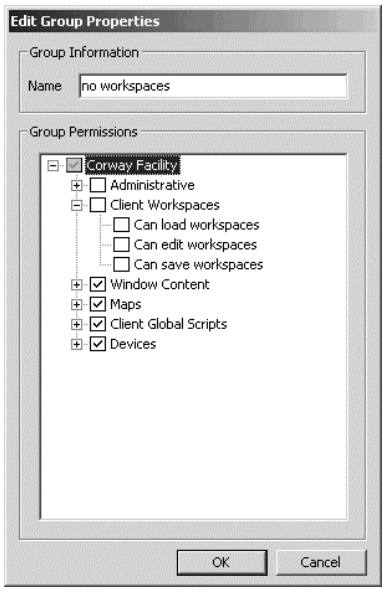


Figure 188. Edit Group Properties Dialog Box

2. Change the properties of the user group as desired. Refer to *Add a New User Group* for more information.
3. Click OK. The Edit Group Properties dialog box closes.

DELETE A USER GROUP

NOTE: Deleting a user group is irreversible. If you delete a user group and then change your mind, you must re-create it using the Add New User Group option and edit each user you want to make a member of the group.

You can delete a user group regardless of whether it has members. If you delete a user group that has members, they will lose the permissions the deleted group granted, unless they belong to another group that offers those same permissions.

To delete a user group:

1. Navigate the Object Browser to [project name] > User Groups. In the right pane, right-click the user group you want to delete and select Delete from the pop-up menu. The Confirm dialog box opens.
2. If you are sure you want to delete the user group, click Yes. The selected user group is deleted and the Confirm dialog box closes. The name of the deleted group disappears from the Object Browser.

NOTE: You cannot delete the group you are currently logged in under if it is the only group you belong to.

Users

The parts of the VMX300(-E) software a particular user has access to are determined by which user groups the user belongs to. Refer to *User Groups - Group Permissions* for more information.

PREDEFINED USER ACCOUNTS

THE PREDEFINED ADMINISTRATOR ACCOUNT

VMX300(-E) provides a predefined administrator account that allows you to configure the server. The user name and password for the predefined administrator account are the following:

- User name: administrator
- Password: 2899100

The predefined administrator account cannot be deleted, nor can it be fully edited. The only properties you can change for the administrator account are the password, the user's name, and the priority.

Unlike other user accounts, the administrator account does not acquire permissions through membership in user groups. The administrator account allows you to log in to server configuration mode and perform all configuration activities. You cannot log in to the client using the predefined administrator account. To log in to the client, use the predefined operator account, or add a new user that belongs to at least one user group.

THE PREDEFINED OPERATOR ACCOUNT

VMX300(-E) provides a predefined operator account that allows you to log in to the client without having to add a new user. The predefined operator account can be edited and deleted.

Initially, the predefined operator account has a user name, but no password:

- User name: user
- Password: <none>

Like all properties of the predefined operator account, the user name and password can be changed.

The predefined operator account initially belongs to the predefined Users group, which grants all Window Content and Client Workspaces permissions, but no Administrative permissions. Refer to *User Groups - The Predefined User Group* for more information.

ADD A NEW USER

You can create new users from scratch or you can base new users on an existing user. To create a new user based on an existing user, make a copy of the existing user and then edit the copy. Refer to *Pop-Up Menus* in the *Appendix* for information on using Copy and Paste or Paste Many to make copies of objects.

To create a new user from scratch:

1. Navigate the Object Browser to [project name] > Users. Double-click <Add New User> in the right pane, or right-click Users in the left pane and select Add New from the pop-up menu. The Add New User dialog box opens.

Figure 189. Add New User Dialog Box

2. **User name:** Type a unique user name for the user you want to add. The user name is the name the user types in when logging in to the client. User names are at most 50 characters long and can include any letter, digit or special character, with the exception of single and double quotation marks. User names are not case sensitive.

3. **Password:** A password is optional but recommended. Passwords can include any letter, digit or special character, with the exception of single and double quotation marks. A password does not have to be unique. Passwords are case sensitive. For example, *Operator1* and *OPERATOR1* are not equivalent to *operator1*.

4. **Confirm password:** Retype the password. If the passwords entered in the Password and Confirm Password boxes differ in any way, you will not be allowed to add the new user.

5. **E-mail Address:** If you want the user to receive e-mail notification of alarms and events, type the user's e-mail address.

   In order to be notified via e-mail, the user must belong to a recipient group for an alarm/event category that uses e-mail notification. In addition, the e-mail server must be configured. Refer to *Project Properties - E-mail Tab* for instructions on configuring the e-mail server. Refer to *Recipient Groups* for information on defining recipient groups. Refer to *Alarm/Event Categories* for information on configuring alarm/event categories to use e-mail notification.

6. **Full name:** Type the user's proper name. The full name appears beside the user name in the right pane of the Object Browser.

7. **Description:** Type any pertinent comments about the user or the account.

8. **Member of group(s):** The Member of Group(s) area lists all configured groups. Select each user group you want the user to belong to. The user will be granted the permissions associated with each group you select. For more information, refer to *User Groups - Group Permissions*.

9. **Priority:** Enter the priority with which the user's activities are to be treated by VMX300(-E). VMX300(-E) uses priorities to resolve situations in which two or more objects attempt to control a particular device at the same time. The object with the higher priority number is given control of the device. The highest priority you can assign to an object is 99. The lowest is 1. System events have priority 100. Users, schedules, and alarms and events all have a priority. The scripts associated with these objects inherit the object's priority.

10. **Import:** The Import option is only available with VMX300-E Systems. The Import option allows you to import user accounts from other servers. If you have configured a server tie to share video with a remote server, import the accounts of remote users who will be viewing your video. Refer to *Server Ties* for more information.

    Only the user name, password, full name, and description are imported. Membership in user groups and priority are left for you to fill in.

TIP: You might want to define a new user group for imported users to belong to.

To import user accounts defined on other servers, click Import. The Browse Users dialog box opens.

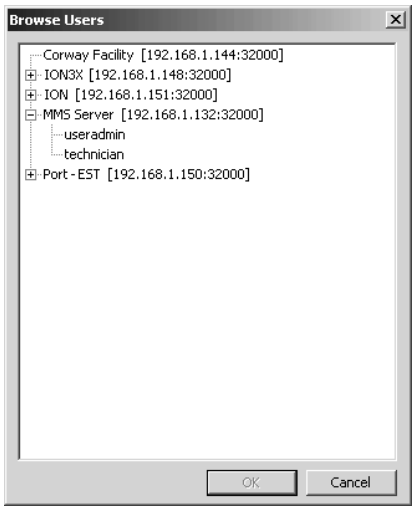


Figure 190. Browse Users Dialog Box

Locate the user you want to import under the server the user account is defined on. Select the user and click OK. The Browse Users dialog box will close and the user name, password, full name, and description will appear in their respective boxes.

11. Click OK. The Add New User dialog box closes and the new user is created. The user name and full name of the new user appear in the right pane of the Object Browser.

NOTES:

- If you want a particular user to be able to log in to more than one server at a time, you must add the user to each server with the same user name and password. Logging in to multiple servers gives the user access to all the maps and devices configured on each server, provided the user has the necessary permissions. The user's permissions do not need to be the same on the different servers. If you want the user to be able to view video from a server other than his home server, configure a server tie between the user's home server and the other server. Refer to *Server Ties* for more information.
- Logging in as a particular user from two different clients is not recommended. Define enough user accounts that this can be avoided.

EDIT A USER

To change the properties of an existing user:

1. Navigate the Object Browser to [project name] > Users. In the right pane, double-click the user you want to change, or right-click the user and select Edit from the pop-up menu. The Edit User Properties dialog box opens.

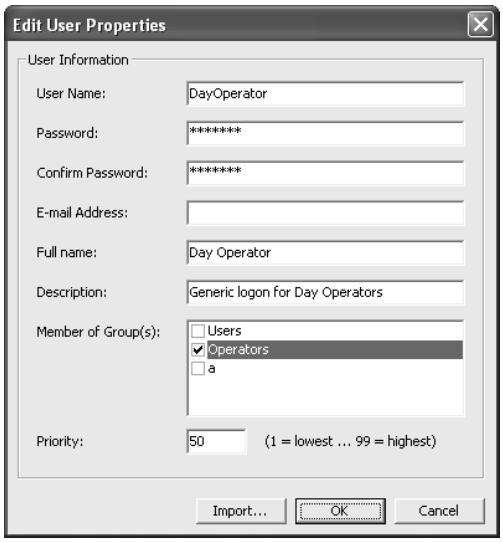


Figure 191. Edit User Properties Dialog Box

2. Change properties of the user as desired. Refer to *Add a New User* for information on specific properties.
3. Click OK. The Edit User Properties dialog box closes.

DELETE A USER

Deleting a user is irreversible. If you delete a user and then change your mind, you must re-create it using the Add New User option.

1. Navigate the Object Browser to [project name] > Users. In the right pane, right-click the user you want to delete and select Delete from the pop-up menu. The Confirm dialog box opens.
2. If you are sure you want to delete the user, click Yes. The selected user is deleted and the Confirm dialog box closes. The name of the deleted user disappears from the Object Browser.

NOTE: You cannot delete the user you are currently logged in as.

Maps

Maps provide VMX300(-E) operators with a graphical representation of the site they are monitoring, complete with installed devices such as cameras and video recorders. VMX300(-E) provides tools to create links between maps and to customize maps with icons that represent installed equipment and alarms.

The first time you start the server, no maps are listed in the Object Browser. You must individually add each map you want to make available to VMX300(-E) operators.

VMX300(-E) does not offer the capability to create maps. Use graphics or CAD software to create your maps, and then import them into VMX300(-E) as described in *Add a New Map*. Or you can use the Print Screen key on your workstation keyboard to create a map file, as described in *Use Print Screen to Create a Map File*.

Note that you cannot change a map file through VMX300(-E). Nothing you do in VMX300(-E) will affect the original file specified when the map is added.

File formats: VMX300(-E) accepts the following graphic file formats.

- JPEG (.jpg)
- Bitmap (.bmp)
- Windows metafile (.wmf)
- Extended metafile (.emf)

To reduce the CPU workload, map files should be as small as possible. Avoid using files with a file size over 1 MB.

TIP: If you have an AutoCAD drawing that you want to use as a VMX300(-E) map, create a .wmf version of the drawing by opening the drawing in AutoCAD and exporting the drawing as type Metafile (.wmf).

USE PRINT SCREEN TO CREATE A MAP FILE

1. Display the image you want to use as a map on your computer. Click the image to make it active.
2. Take a screen capture of the active window by holding the Alt key down and pressing Print Screen.
3. In any software package that allows you to save bitmaps, such as the Paint program available through Windows Accessories, open a new file and press Ctrl-V to paste the screen capture.
4. Save the file as one of the supported bitmap formats, .bmp or .jpg.
5. If desired, open the new file in a graphics package and crop the map.

ADD A NEW MAP

1. Navigate the Object Browser to [project name] > Maps. Double-click <Add New Map> in the right pane, or right-click Maps in the left pane and select Add New from the pop-up menu. The Add New Map dialog box opens.

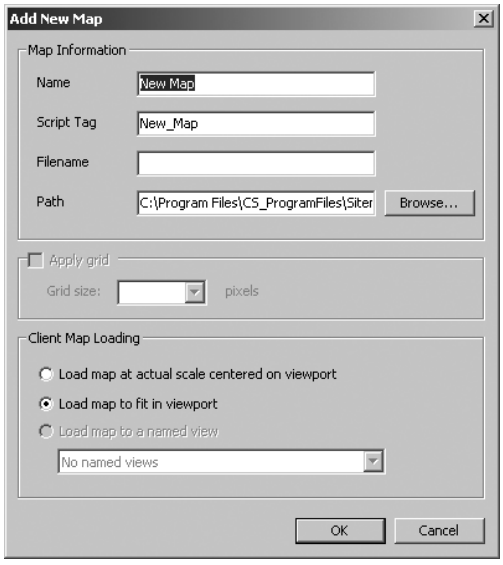


Figure 192. Add New Map Dialog Box

2. **Name:** Type a unique, descriptive name for the map you want to add. Map names are at most 50 characters long and can include any letter, digit or special character, with the exception of single and double quotation marks. Map names are not case sensitive.

   A tag resembling the map name appears in the Script Tag box. If the map name contains special characters, they are omitted from the tag. Leading digits are removed. Spaces are replaced with underscores.

3. **Script tag:** If you do not want to use the script tag provided by the server, type a unique, meaningful tag. Script tags are at most 50 characters long. They can include any letter, digit or the underscore character, but cannot begin with a digit. They cannot contain spaces or special characters. Tags are not case sensitive. Use the script tag to refer to the map in scripts.

4. **Filename:** Click Browse to locate the map file you want to add. Select the desired image file and click Open. If you select a file on a network drive, the server's access to the file could be interrupted by network problems. You can avoid this by having the map file reside on a fixed drive on the server. The file name appears in the Filename area.

5. **Grid:** If you want a grid of dots to display on the map, select Apply Grid. Any objects you place on the map, like devices, labels and hotlinks, will snap to the grid. Make sure the grid is fine-grained enough to allow you to place objects where you want them. If you want, change the grid size by selecting a number from the Grid Size drop-down list, or by typing a number directly into the Grid Size box. The grid displays on the VMX300(-E) server only. It does not display on the client.

6. **Client map loading:** Select the default view you want operators to see when they load the map in the VMX300(-E) client. This default is used only if the operator has not loaded a client workspace. The options for how the map loads by default are:

   a. **Load map at actual scale centered on viewport:** Display the map at its actual size, centered in the map viewport. If the map viewport is not large enough to display the entire map at its actual size, a portion of the map will display.

   b. **Load map to fit in viewport:** Display the map as large as possible to fit within the map viewport.

   c. **Load map to a named view:** Display the map as prescribed by the selected named view. This option is only available if you have defined at least one named view. For more information, refer to *Named Views*.

7. Click OK. The Add New Map dialog box closes and the new map is added. The name and script tag of the new map appear in the Object Browser.

NOTE: To have a named view as the client map loading default:

1. Add the map.
2. Create the named view.
3. Edit the map and change the Client Map Loading setting to "Load map to a named view."

TIP: If you want to use the name of the map file as the map name, browse for the map file before typing in the name. The server will automatically fill in the name box with the file name and generate a tag based on the name.

EDIT A MAP'S PROPERTIES

NOTE: If you change the script tag for a map, any script that refers to the map will contain an error. To correct the error, update the scripts so they use the map's new script tag. Refer to *Scripts and Expressions* for more information.

To change the properties of an existing map:

1. Navigate the Object Browser to [project name] > Maps. In either pane, right-click the map whose properties you want to change and select Edit from the pop-up menu. The Edit Map Properties dialog box opens.

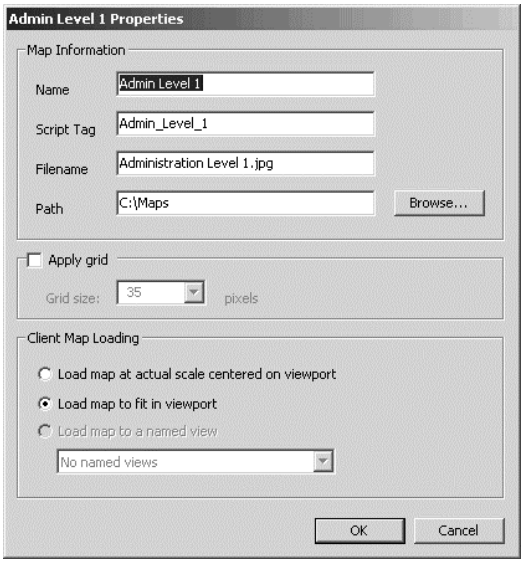


Figure 193. Edit Map Properties Dialog Box

2. Change properties of the map as desired. Refer to *Add a New Map* for information on specific properties.
3. Click OK. The Edit Map Properties dialog box closes.

LOAD A MAP

Before you can place objects like devices on a map, you must load the map, so it displays in the map viewport. Only one map can be loaded at a time.

To load a map:

1. Navigate the Object Browser to [project name] > Maps. In either pane, click the map you want to load and hold the mouse button down.

   If you move the pointer slightly, it changes to a representation of the Earth. 
2. Drag the pointer to the map viewport and release the mouse button. The selected map appears, complete with any objects that were previously placed on the map. The map is fitted to the viewport.

TIP: You can also load a map directly from a named view. Refer to *Named Views - Load a Named View* for instructions.

CUSTOMIZE YOUR MAPS

VMX300(-E) provides a number of tools that allow you to customize your maps:

- **Place device icons on maps:** Place icons representing installed devices on maps, allowing operators to control the devices by clicking the icons. Refer to *Device Icons* for more information.
- **Store different views of a map:** Create named views that allow operators to quickly focus on a particular view of a map. Refer to *Named Views* for more information.
- **Define links between maps:** Create hotlinks that allow an operator to load a related map or named view with a single mouse click. Refer to *Hotlinks* for more information.
- **Run scripts by clicking a map:** Create scripts to automate common actions that operators can run by clicking a label or hotlink on a map. Refer to *Labels* and *Hotlinks* for more information.
- **Place alarm/event icons on maps:** Place icons representing alarms and events on maps so operators can respond to an alarm by clicking the icon. Refer to *Alarms and Events - Alarm/Event Icons* for more information.

DELETE A MAP

NOTE: Deleting a map that is referred to in a script introduces an error into the script. Refer to *Scripts and Expressions* for more information.

Deleting a map does not affect the original map file. If you change your mind after deleting a map, you can reimport the map as described in *Add a New Map*.

1. Navigate the Object Browser to [project name] > Maps. In either pane, right-click the map you want to delete and select Delete from the pop-up menu. The Confirm dialog box opens.
2. If you are sure you want to delete the map, click Yes. The selected map is deleted and the Confirm dialog box closes. The deleted map disappears from the Object Browser. If the map was loaded when it was deleted, it disappears from the viewport.

Device Settings

EDIT A DEVICE'S PROPERTIES

A device has certain properties in virtue of being a device of a particular type. These properties are inherited from the device driver. When you add a device, you specify values for these inherited properties. You can also change them after the device has been added by editing the device.

In addition to the inherited properties, a device has properties that pertain to how the device is represented within VMX300(-E). This includes whether the device will be used in scripts and expressions and how the device's alarms will be mapped. These properties are set through the device's local settings. Refer to *Edit a Device's Local Settings* for more information.

NOTES:

- The settings accessed through the Edit Device Properties dialog box are driver-specific. For more information on the settings for the device you want to edit, refer to the *Devices* section for the appropriate device driver.
- To edit a device, the driver must be running on the network.
- Changes to a device's properties come into effect immediately. You cannot discard your changes by exiting configuration mode without saving.

To edit the properties of an existing device, navigate the Object Browser to [project name] > Device Drivers > [device driver name]. In either pane, right-click the device you want to edit and select Edit from the pop-up menu. Alternatively, load a map that has a device icon for the device you want to edit on it, and either double-click the icon, or right-click the icon and select Edit from the pop-up menu. Make sure you position the pointer over the icon, not the label, before clicking. The Edit Device Properties dialog box opens.

Figure 194. Edit Device Properties Dialog Box

EDIT A DEVICE'S LOCAL SETTINGS

A device has certain properties in virtue of being a device of a particular type. These properties are inherited from the device driver and configured when you add the device. You can also change them after the device has been added as described in *Edit a Device's Properties*.

In addition to the inherited properties, a device has properties that have to do with how the device is represented within VMX300(-E). This includes whether the device will be used in scripts and expressions and how the device's alarms will be mapped. These properties are set through the device's local settings.

To edit the local settings for a device:

1. Navigate the Object Browser to [project name] > Device Drivers > [device driver name] > Devices > [device name]. Double-click Local Settings in the right pane. Alternatively, right-click the device in either pane and select Local Settings from the pop-up menu. The Edit Local Settings dialog box opens.

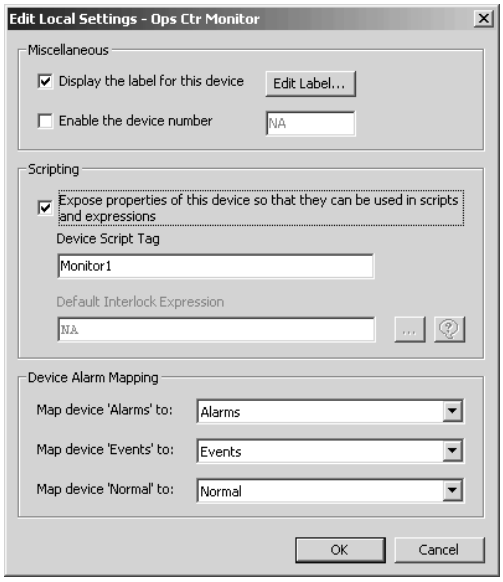


Figure 195. Edit Local Settings Dialog Box

2. **Display label:** If you want device icons labeled, select "Display the label for this device." To edit the text and formatting of the device label, click Edit Label. The Edit Device Label Properties dialog box opens.

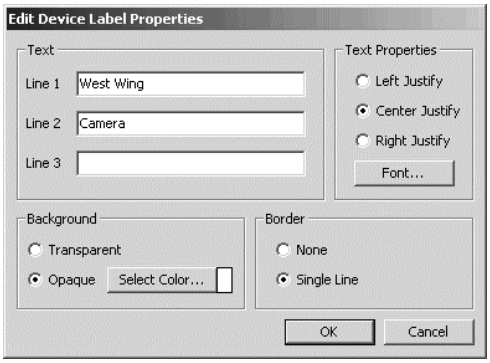


Figure 196. Edit Device Label Properties Dialog Box

a. **Text:** Type up to three lines of text as the label contents. When you place a device icon on a map, this text will display in the label. Each line of text can be at most 50 characters long and can include any letter, digit or special character, with the exception of single and double quotation marks.

b. **Text properties:** Select the justification you want for the device label's text. All the lines of text will be justified the same. Click Font to select the font for the label's text, as well as display attributes like bold face and italics.

c. **Background:** Select the background you want for the label you are creating. A transparent background allows the underlying map to show through. An opaque background makes the label appear as a colored rectangle. Click Select Color to choose the fill color for an opaque label.

d. **Border:** Specify whether you want the label to have a border around it by selecting None or Single Line.

e. Click OK. The Edit Device Label Properties dialog box closes.

3. **Device number:** If operators will be using a CCTV keyboard that employs numeric identifiers for devices, select "Enable the device number" and type in the device number. If operators will be using computer keyboards that allow the use of textual names for devices, do not select this option.

4. **Expose properties:** The "Expose properties of this device so that they can be used in scripts and expressions" field is enabled by default. This allows you to refer to the device in scripts and expressions. To prevent a device's properties from being used in scripts and expressions, click this field to clear the checkmark. Refer to *Scripts and Expressions* for information on scripts and expressions and the objects that use them.

5. **Device script tag:** If you do not want to use the script tag provided by the server, type in a unique, meaningful tag. Script tags are at most 50 characters long. They can include any letter, digit or the underscore character, but cannot begin with a digit. They cannot contain spaces or special characters. Tags are not case sensitive. Use the script tag to refer to the device in scripts and expressions. For a list of device properties that can be scripted, refer to the *Scripts and Expressions* section for the appropriate device driver.

NOTE: If you change the script tag for a device, any script that refers to the device will contain an error. To correct the error, update the scripts so they use the device's new script tag. Refer to *Scripts and Expressions* for more information.

6. **Default interlock expression:** This feature is reserved for future use.

7. **Device alarm mapping:** Specify how you want the VMX300(-E) server to handle signals sent out by the device.

   To specify how you want device alarms handled, select an alarm/event category from the drop-down list to the right of "Map device 'Alarms' to." When the device sends an alarm to the VMX300(-E) server, the server will treat the alarm like it would a custom alarm or event belonging to the category you have specified. The server will notify the recipients for the specified category according to the category's settings for color, sound, acknowledgement, and archiving.

   To specify how you want device events handled, select an alarm/event category from the drop-down list to the right of "Map device 'Events' to." To specify how you want device normal signals handled, select an alarm/event category from the drop-down list to the right of "Map device 'Normal' to."

   If you want the VMX300(-E) server to discard a category of signal, select <None> from the drop-down list for that category.

   Refer to *Alarms and Events* for detailed information on how the VMX300(-E) server handles alarms and events.

NOTE: Configuring device alarm mapping is a two-step process. In addition to the device alarm mapping defined through the local settings, you must configure the device alarm mapping through the Edit Device Properties dialog box. Refer to *Edit a Device's Properties* for instructions on opening the Edit Device Properties dialog box. Refer to the *Devices* section for information on configuring the different alarms and events sent out by devices of that type.

8. Click OK. The Edit Local Settings dialog box closes.

9. Click File > Save (changes to a device's local settings do not take effect until you save the server configuration).

VIEW A DEVICE'S READ AND WRITE PROPERTIES

Devices have read and write properties that can act as variables in VMX300(-E) scripts and expressions.

Read properties: Read properties indicate the state the device is in at a particular time. You can use the device's read properties in any context that reads the value of a property, but does not change it, such as an alarm/event expression or an IF-THEN command. You can view the value of a read property at any time using the Current Status option; refer to *Current Status: View Run-Time Values of Variables* in the *Scripts and Expressions* section.

Write properties: You can use the device's write properties in any context that changes the value of the property, such as the SET command. For example, a script that turns on the wiper for a camera with script tag Camera1 would include the following statement:

```
SET Camera1.Wiper = Camera1.On
```

Specific Device Read and Write Properties: The particular properties of a device and the values each property can take are device-dependent. To find out the properties for a particular device that is installed on your server, display the Read Properties and Write Properties for the device. Refer to the *Scripts and Expressions* section for a complete list of each device's properties.

Refer to *Scripts and Expressions* for information on the scripting language in VMX300(-E).

NOTE: A device's properties can only be used in scripts and expressions if they are exposed. All device properties are exposed by default. To prevent a device's properties from being used in scripts and expressions, edit the device's local settings and clear "Expose properties of this device so that they can be used in scripts and expressions." Refer to *Edit a Device's Local Settings* for more information.

To view a device's write properties:

1. Navigate the Object Browser to [project name] > Device Drivers > [device driver name] > Devices > [device name] > Write Properties. The list of write properties appears.
2. To view the values a specific property can take, click the desired property in the left pane, or double-click the property folder in the right pane. The list of values appears in the right pane of the Object Browser.

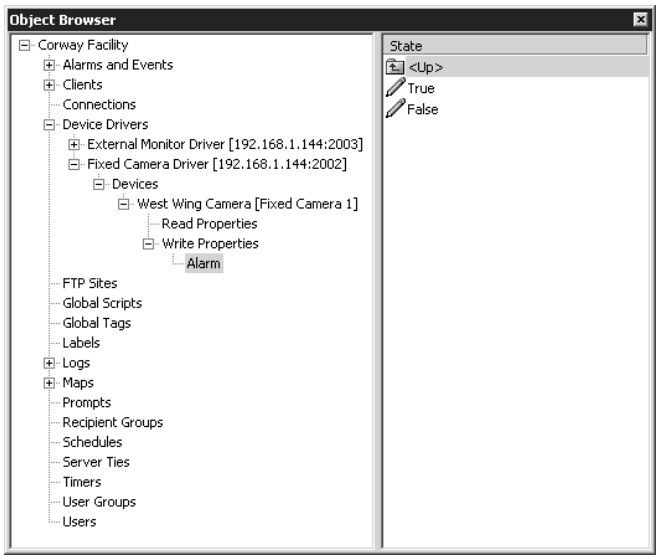


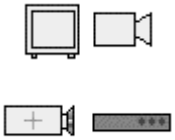
Figure 197. Viewing Properties Values

To view a device's read properties:

1. Navigate the Object Browser to [project name] > Device Drivers > [device driver name] > Devices > [device name] > Read Properties. The list of read properties appears.
2. To view the values a specific property can take, click the desired property in the left pane, or double-click the property folder in the right pane. The list of values appears in the right pane of the Object Browser.

Device Icons

VMX300(-E) allows you to customize maps by placing icons on them that represent physical devices installed in the field. Judicious placement of device icons provides operators with an easy-to-use visual representation of the installation they are monitoring. Operators can control devices by clicking the icons.



Before you can place a device icon for a particular device on a map, you must add the device itself as described in *Add a New Device*. Once you have added the device, you can place as many icons representing the device as you want.

NOTES:

- You do not need to have a device icon on a map in order for the device to function. The icon's role is to provide operators with an active visual representation of the device, its status, and controls. Operators can also access devices and their controls through the Device List.
- Device icons appear as a hollow outline in the VMX300(-E) client if the device driver is not running.

PLACE A DEVICE ICON ON A MAP

1. Load the map you want to place a device icon on. The map appears in the map viewport.
2. Navigate the Object Browser to [project name] > Device Drivers > [device driver name] > Devices. Click the device you want to place on the map and hold the mouse button down. If you move the pointer slightly, it changes to cross-hairs.
3. Drag the pointer to the map, position it where you want to place the device, and release the mouse button. An icon representing the selected device appears on the map and the pointer changes back to an arrow. If "Display the label for this device" is selected in the device's local settings, the device's label appears below the icon. Refer to *Edit a Device's Local Settings* for more information on displaying labels.
4. **Scale and rotate:** Move the pointer away from the icon to make the icon larger. Move the pointer towards the center of the icon to make the icon smaller. Scaling the device icon does not affect the size of the device's label. Refer to *Scale a Device Label* for instructions on scaling the device's label.

NOTE: To minimize the CPU workload, device icons should be as small as possible.

   Move the pointer in a circle around the icon to change the orientation of the icon. Note that you can only rotate icons that represent devices that are made to be oriented different ways, such as cameras. Icons representing devices that are not normally rotated, such as monitors, cannot be rotated.

5. When the icon is sized and oriented the way you want it, press the left mouse button. The icon's size and orientation freezes. If the device's label is displayed, it freezes in place below the icon.

TIP: Hold the Shift key down while scaling and rotating to constrain the scaling to 5 unit increments and the rotation to 15° increments.

MOVE A DEVICE ICON

Any device icon placed on a map can later be moved to another position on the same map. When you move an icon, only its position changes; its size and orientation remain fixed. For information on changing an icon's size and orientation, refer to *Scale and Rotate a Device Icon*.

To move a device icon to a different position on the map:

1. With the desired map loaded, right-click the device icon you want to move and select Move from the pop-up menu. Make sure you position the pointer over the icon, not the label, before right-clicking.
2. Move the pointer to the icon's new location. The icon follows the pointer as you move it. If the device's label is displayed, it moves with the icon.
3. When the icon is located where you want it, press the left mouse button. The icon freezes in place. If the map has a grid, the icon snaps to the grid.

SCALE AND ROTATE A DEVICE ICON

NOTE: To minimize the CPU workload, device icons should be as small as possible.

Changing the size and orientation of a device icon does not affect its position. For information on changing an icon's position, refer to *Move a Device Icon*.

To change the size or orientation of a device icon:

1. With the desired map loaded, right-click the device icon you want to resize or reorient and select Scale and Rotate from the pop-up menu. Make sure you position the pointer over the icon, not the label, before right-clicking.

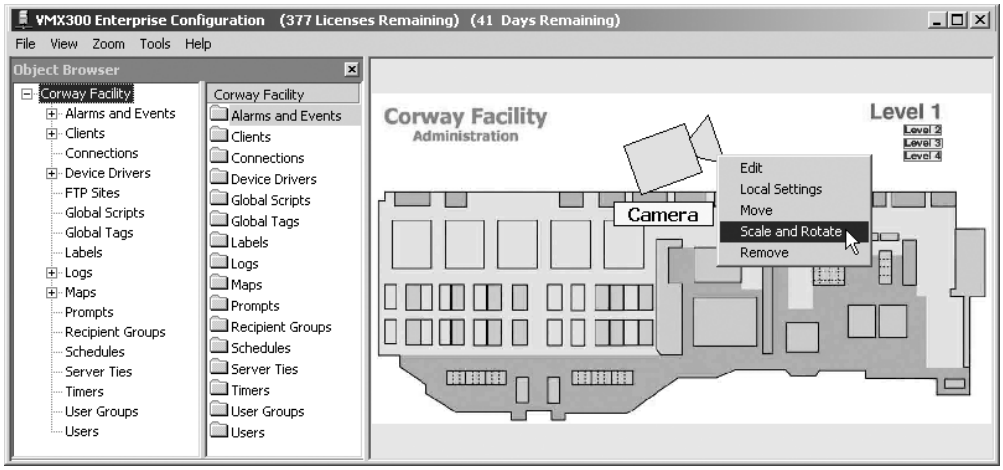


Figure 198. Scaling and Rotating an Icon

2. Move the pointer away from the icon to make the icon larger. Move the pointer towards the center of the icon to make the icon smaller. Move the pointer in a circle around the icon to change the orientation of the icon.
3. When the device icon is sized and oriented the way you want it, press the left mouse button. The icon's size and orientation freeze.

TIP: Hold the Shift key down while scaling and rotating to constrain the scaling to 5 unit increments and the rotation to 15° increments.

NOTE: Scaling a device icon does not affect the size of the device's label. Refer to *Scale a Device Label* for information on scaling the label.

REMOVE A DEVICE ICON FROM A MAP

Removing a device icon from a map does not affect any other icons for that device, whether they are on the same map or another map, nor does it affect the device in the Object Browser. If you change your mind after removing a device from a map, you can add it back as described in *Place a Device Icon on a Map*.

TIP: You do not need to have a device icon on a map in order for the device to function. The icon's role is to provide operators with an active visual representation of the device, its status, and controls.

With the desired map loaded, right-click the device icon you want to remove and select Remove from the pop-up menu. Make sure you position the pointer over the icon, not the label, before right-clicking. The device icon disappears from the map. If it is displayed, the device's label also is removed from the map.

MOVE A DEVICE LABEL

You can move a device label independently of the icon itself.

To adjust the position of a device label:

1. With the desired map loaded, right-click the device label you want to move and select Move from the pop-up menu. Make sure you position the pointer over the label, not the icon, before right-clicking.
2. Move the pointer to the label's new location. The label follows the pointer as you move it. The icon does not move.
3. When the label is located where you want it, press the left mouse button. The label freezes in place.

SCALE A DEVICE LABEL

Changing the size of a device label does not affect its position. For information on changing a label's position, refer to *Move a Device Label*.

To change the size of a device label:

1. With the desired map loaded, right-click the device label you want to resize and select Scale from the pop-up menu. Make sure you position the pointer over the label, not the icon, before right-clicking.

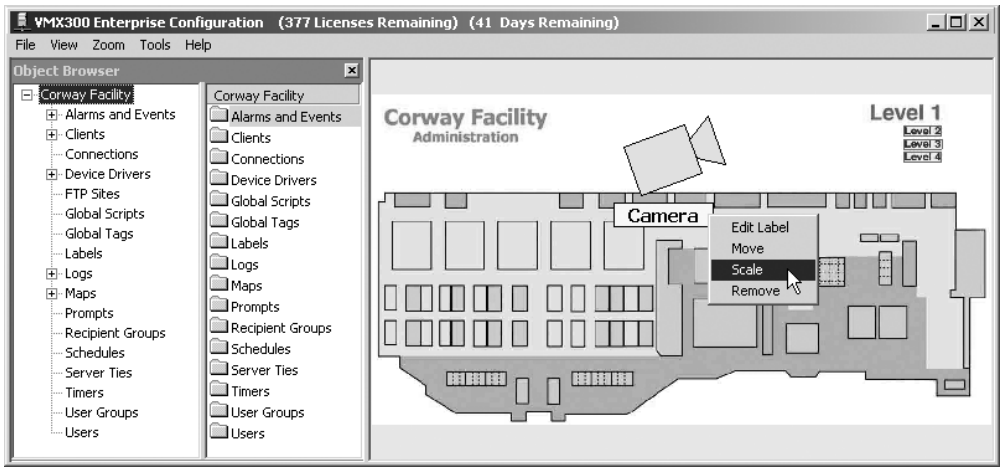


Figure 199. Changing Label Size

2. Move the pointer away from the label to make the label larger. Move the pointer towards the center of the label to make the label smaller.
3. When the device label is sized the way you want it, press the left mouse button. The label's size freezes.

NOTE: You cannot change the orientation of a device label. Labels are always oriented horizontally.

EDIT A DEVICE LABEL

To change the text and formatting of an existing device label:

1. Right-click the label and select Edit Label from the pop-up menu. Make sure you position the pointer over the label, not the icon, before right-clicking.

   Alternatively, navigate the Object Browser to [project name] > Device Drivers > [device driver name] > Devices. In the right pane, double-click Local Settings, then click Edit Label. The Edit Label Properties dialog box opens.

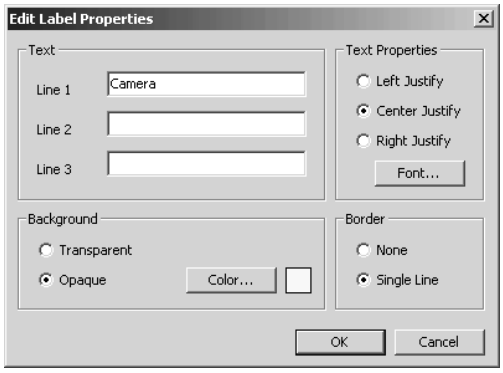


Figure 200. Edit Label Properties Dialog Box

2. Change properties of the label as desired. Refer to *Edit a Device's Local Settings* for information on specific properties.
3. Click OK. The Edit Label Properties dialog box closes.

REMOVE A DEVICE LABEL

Removing a device label from one icon removes the label from all icons representing that device, whether the icons are on the same map or different maps. If you change your mind after removing a device label, you can add it back as described in *Edit a Device's Local Settings*.

With the desired map loaded, right-click the device label you want to remove and select Remove from the pop-up menu. Make sure you position the pointer over the label, not the icon, before right-clicking. The device label disappears from the map and "Display the label for this device" is cleared in the device's local settings. The icon is unaffected.

TIP: If you want a label to appear on only one instance of a device icon, use a label rather than the device label. Device labels always appear on every device icon. Refer to *Labels* for more information.

Named Views

Named views allow you to save a particular view of a map so an operator can reload it at any time without having to zoom and scroll. You can create as many named views as you want for a map.

ADD A NEW NAMED VIEW

1. With the desired map loaded, isolate the view you want to name by zooming and scrolling.
2. Navigate the Object Browser to [project name] > Maps > [map] > Named Views. Double-click <Add New View> in the right pane, or right-click Named Views in the left pane and select Add New from the pop-up menu. The Add New Named View dialog box opens.

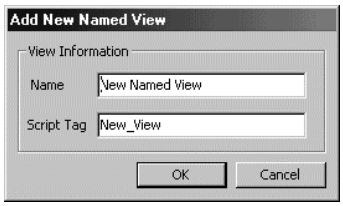


Figure 201. Add New Named View Dialog Box

3. **Name:** Type in a unique, descriptive name for the named view you want to add. View names are at most 50 characters long. They can include any letter, digit or special character, with the exception of single and double quotation marks. View names are not case sensitive. The view name is displayed in the right pane of the Object Browser. A tag resembling the view name will appear in the Script Tag box. If the view name contains special characters, they will be omitted from the tag. Leading digits will be removed. Spaces will be replaced with underscores.
4. **Script tag:** If you do not want to use the script tag supplied by the server, type in a unique, meaningful tag. Script tags are at most 50 characters long. They can include any letter, digit or the underscore character, but cannot begin with a digit. They cannot contain spaces or special characters. Tags are not case sensitive. Use the script tag to refer to the named view in scripts.
5. Click OK. The named view is created and the Add New Named View dialog box closes. The name and script tag of the new named view appear in the right pane of the Object Browser.

EDIT A NAMED VIEW

NOTE: If you change the script tag for a named view, any script that refers to the named view will contain an error. To correct the error, update the scripts so they use the named views's new script tag. Refer to *Scripts and Expressions* for more information.

To change the view that is called up by a named view, use the Update View option. Refer to *Update a Named View* for more information.
To change the name or script tag of a named view:

1. Navigate the Object Browser to [project name] > Maps > [map] > Named Views. In the right pane, double-click the named view you want to edit, or right-click the named view and select Edit from the pop-up menu. The Edit Named View Properties dialog box opens.

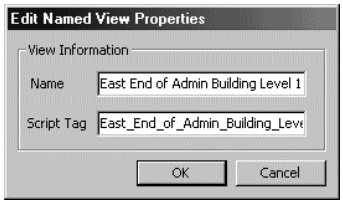


Figure 202. Edit Named View Properties Dialog Box

2. Change properties of the named view as desired. Refer to *Add a New Named View* for information on specific properties.
3. Click OK. The Edit Named View Properties dialog box closes.

LOAD A NAMED VIEW

1. Navigate the Object Browser to [project name] > Maps > [map] > Named Views. In the right pane, click the named view you want to load and hold the mouse button down. If you move the pointer slightly, it changes to a representation of the Earth. 
2. Drag the pointer to the map viewport and release the mouse button. The selected view appears in the viewport.

UPDATE A NAMED VIEW

You can change the view called up by a named view using the Update View option:

1. With the desired map loaded, isolate the new view you want to change to by zooming and scrolling.
2. Navigate the Object Browser to [project name] > Maps > [map] > Named Views. In the right pane, right-click the named view you want to update and select Update View from the pop-up menu. The named view is updated to the current view.

DELETE A NAMED VIEW

Deleting a named view is irreversible. If you delete a named view and then change your mind, you must add a new named view. Also note that if you delete a named view, any script that refers to the named view will contain an error.

1. Navigate the Object Browser to [project name] > Maps > [map] > Named Views. In the right pane, right-click the named view you want to delete and select Delete from the pop-up menu. The Confirm dialog box opens.
2. If you are sure you want to delete the named view, click Yes. The selected named view is deleted and the Confirm dialog box closes. The deleted view disappears from the Object Browser.

Hotlinks

A hotlink is an area of a map that, when clicked, runs a script. Hotlinks are generally used to run a script that loads another map, effectively linking the maps.

If you want, you can omit the script when creating a hotlink. In this case, the hotlink is for information only, to define an area on a map.

ADD A NEW HOTLINK

TIPS:

- To create a hotlink that is perfectly rectangular, apply a grid to the map. The corner points of the hotlink will snap to the closest grid point. If you want, turn the grid off after you've created the hotlink.
- Conventionally, a clickable hotlink changes color when you move the pointer over it.

To create a hotlink and place it on a map:

1. Load the map you want to create a hotlink for. The map appears in the map viewport.
2. Navigate the Object Browser to [project name] > Maps > [map] > Hotlinks. Double-click <Add New Hotlink> in the right pane, or right-click Hotlinks in the left pane and select Add New from the pop-up menu. If you move the pointer over the map in the viewport, it changes into cross-hairs with 'hot link' in the lower right corner.
3. **Define hotlink area:** With the pointer positioned at one corner of the area you want the hotlink, click the left mouse button. Position the pointer at an adjacent corner and click the left mouse button. Continue positioning the pointer and clicking until all the corners have been defined. A hotlink must have at least three corners. With the pointer positioned anywhere on the map, right-click. The outline freezes in place and the Add New Hotlink dialog box opens.

NOTE: To minimize the CPU workload, hotlinks should be as small as possible. For example, a hotlink that covers half of a map could cause CPU performance problems.

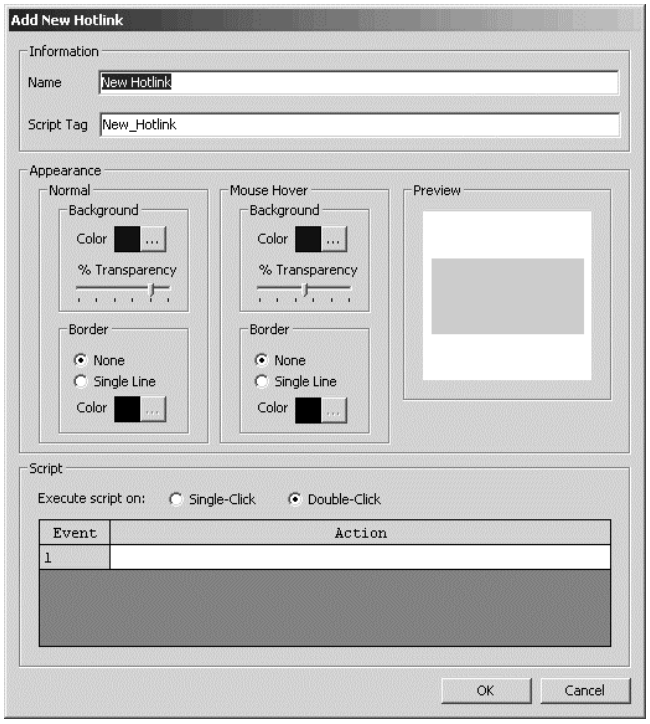


Figure 203. Add New Hotlink Dialog Box

4. **Name:** Type a unique, descriptive name for the hotlink you want to add. Hotlink names are at most 50 characters long. They can include any letter, digit or special character, with the exception of single and double quotation marks. Hotlink names are not case sensitive. A tag resembling the hotlink name appears in the Script Tag box. If the hotlink name contains special characters, they are omitted from the tag. Leading digits are removed. Spaces are replaced with underscores.

5. **Script tag:** If you do not want to use the script tag provided by the server, type a unique, meaningful tag. Script tags are at most 50 characters long. They can include any letter, digit or the underscore character, but cannot begin with a digit. They cannot contain spaces or special characters. Tags are not case sensitive. Use the script tag to refer to the hotlink in scripts. For a list of hotlink properties that can be scripted, refer to *Scripts and Expressions - Properties of Objects*.

6. **Normal appearance:** Adjust the appearance of the hotlink, referring to the Preview area of the dialog box to view your selections.

   To set the hotlink's fill color, click the button to the immediate right of the background color sample, select a color and click OK. To adjust the transparency of the hotlink's fill, drag the % Transparency slider, or click the slider bar to move in 5% increments. At 100% transparency, the hotlink will not be visible on the map. At 0%, it will be fully opaque, obscuring any items underneath it.

   Specify whether you want the hotlink to have a border around it by selecting None or Single Line. To set the border's color, click the button to the immediate right of the color sample, select a color and click OK.

7. **Mouse hover appearance:** You can configure a hotlink to change color when the pointer is positioned over it using the Mouse Hover settings. To preview the appearance, position the pointer over the hotlink in the Preview area of the dialog box.

   To set the fill color, click the button to the immediate right of the color sample, select a color and click OK. To adjust the transparency of the fill, drag the % Transparency slider, or click the slider bar to move in 5% increments. At 100% transparency, the hotlink will not be visible when the pointer is positioned over it. At 0%, it will be fully opaque.

   Specify whether you want the hotlink to have a border around it when the pointer is positioned over it by selecting None or Single Line. To set the border's color, click the button to the immediate right of the color sample, select a color and click OK.

8. **Run script:** If you want to associate a script with the hotlink, type the script in the Run Script area.

   If you want the script to run with a single click of the hotlink, select Single-Click. If you want the script to run when the hotlink is double-clicked, select Double-Click.

   Type the script actions directly into the Action column, or use the script wizard to help you write the script. For more information on writing scripts, refer to *Scripts and Expressions*.

   To test the script, save the server configuration, log in to the client, load the map the hotlink is on, and click the hotlink.

9. Click OK. The hotlink is created and the Add New Hotlink dialog box closes. The name and script tag of the new hotlink appear in the right pane of the Object Browser and the hotlink appears on the map.

EDIT A HOTLINK'S PROPERTIES

NOTE: If you change the script tag for a hotlink, any script that refers to the hotlink will contain an error. To correct the error, update the scripts so they use the hotlink's new script tag. Refer to *Scripts and Expressions* for more information.

To change the properties of an existing hotlink:

1. Navigate the Object Browser to [project name] > Maps > [map] > Hotlinks. In the right pane of the Object Browser, double-click the hotlink you want to edit, or right-click the hotlink and select Edit from the pop-up menu. Alternatively, load the map the hotlink is on and either double-click the hotlink, or right-click the hotlink and select Edit from the pop-up menu. The Edit Hotlink Properties dialog box opens.

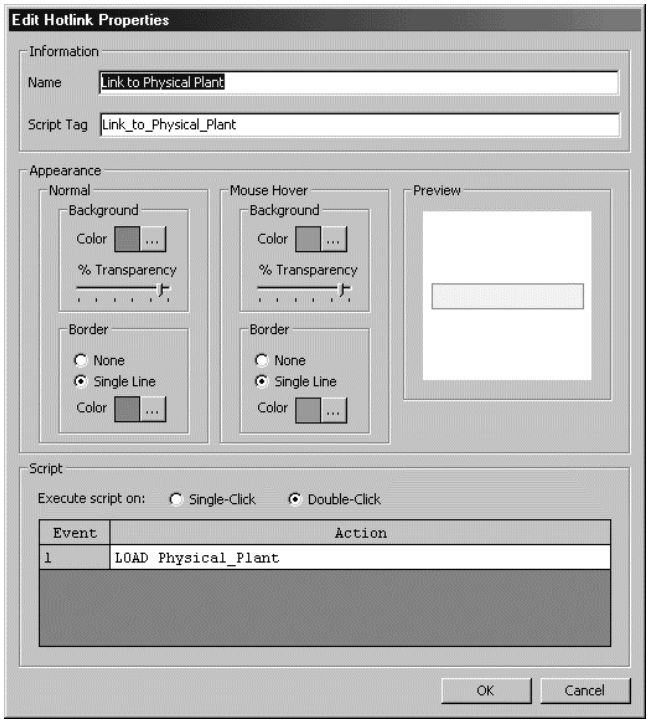


Figure 204. Edit Hotlink Properties Dialog Box

2. Change properties of the hotlink as desired. Refer to *Add a New Hotlink* for information on specific properties.
3. Click OK. The Edit Hotlink Properties dialog box closes.

NOTE: When you edit a hotlink's script, make it available in its updated form by saving the server configuration before attempting to run the script.

MODIFY A HOTLINK'S SHAPE AND SIZE

You can modify the area defined by an existing hotlink by changing the number and location of its vertices. Specifically, you can perform the following functions:

- Move a vertex
- Add a vertex
- Delete a vertex

TIP: Move the position of a hotlink on a map by moving each of its vertices in turn.

MOVE A VERTEX

TIP: To make a hotlink perfectly rectangular, apply a grid to the map, then move the vertices to grid points. A vertex will snap to the closest grid point. If you want, turn the grid off after you've finished.

To move a hotlink's vertex:

1. Load the map the hotlink is on and click the hotlink. A small circle appears at each of the hotlink's vertices.
2. Position the pointer over the vertex you want to move. A four-headed arrow appears beside the pointer.
3. Click and hold the mouse key down.
4. Drag the vertex to its new position.
5. Release the mouse button. The vertex freezes in place, giving the hotlink its new shape.

ADD A VERTEX

To add a vertex to an existing hotlink:

1. Load the map the hotlink is on and click the hotlink. A small circle appears at each of the hotlink's vertices.
2. Click the vertex next to where you want the new vertex created. A green square appears at the vertex you clicked, and a small blue square appears at the adjacent vertex. The new vertex is inserted between these two vertices.
3. Right-click the vertex with the green square and select Insert vertex from the pop-up menu. A new vertex is inserted midway between the two vertices marked by squares.

DELETE A VERTEX

To delete a vertex from an existing hotlink:

1. Load the map the hotlink is on and click the hotlink. A small circle appears at each of the hotlink's vertices.
2. Right-click the vertex you want to delete and select Delete vertex from the pop-up menu. The vertex is deleted from the hotlink, reshaping the hotlink.

NOTE: A hotlink must have at least three vertices. The Delete vertex option is not available for a hotlink that has only three vertices.

DELETE A HOTLINK

Deleting a hotlink is irreversible. If you delete a hotlink and then change your mind, you must add a new hotlink. Also note that if you delete a hotlink, any script that refers to the hotlink will contain an error.

To delete a hotlink:

1. Navigate the Object Browser to [project name] > Maps > [map] > Hotlinks. In the right pane, right-click the hotlink you want to delete and select Delete from the pop-up menu. Alternatively, load the map the hotlink is on, right-click the hotlink, and select Delete from the pop-up menu. A dialog box prompting for confirmation opens.
2. If you are sure you want to delete the hotlink, click Yes. The dialog box closes and the selected hotlink is deleted from the map and the Object Browser.

Labels

Labels are free-standing descriptive phrases that are placed on maps. You can associate a script with a label, so that when you click the label, the script runs. If you omit the script the label is for information only. For example, you might use a label to identify an item on a map.

TIP: Device icons and alarm/event icons have built-in labels associated with them. Built-in labels are for information only; you cannot associate a script with them. Refer to *Edit a Device's Local Settings* for information on displaying a device's label. Refer to *Alarms and Events - Alarms, Events, and Normal Occurrences* for information on displaying an alarm or event's label.

Before you can place a label on a map, you must create the label. Once created, you can place it as many times as you want on a single map or on different maps. Each instance of a particular label has the same appearance and runs exactly the same script. The only difference between one instance and another is its location.

Any label placed on a map can later be moved to a different location on the map using the Move option.

ADD A NEW LABEL

1. Navigate the Object Browser to [project name] > Labels. Double-click <Add New Label> in the right pane, or right-click Labels in the left pane and select Add New from the pop-up menu. The Add New Label dialog box opens.

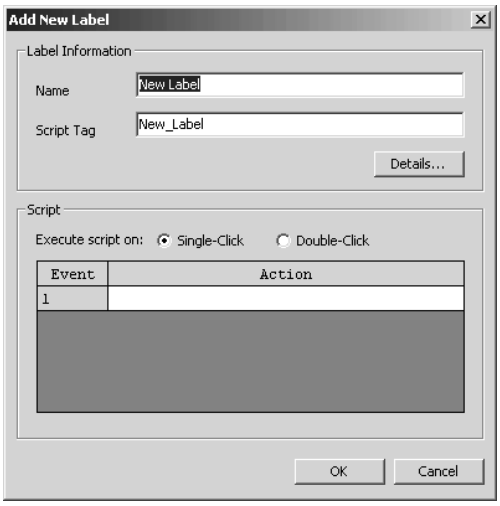


Figure 205. Add New Label Dialog Box

2. **Name:** Type a unique, descriptive name for the label you want to add. Label names are at most 50 characters long and can include any letter, digit or special character, with the exception of single and double quotation marks. Label names are not case sensitive. A tag resembling the name appears in the Script Tag box. If the name contains special characters, they are omitted from the tag. Spaces are replaced with underscores. Leading digits are removed.

3. **Script tag:** If you do not want to use the script tag provided by the server, type a unique, meaningful tag. Script tags are at most 50 characters long. They can include any letter, digit or the underscore character, but cannot begin with a digit. They cannot contain spaces or special characters. Tags are not case sensitive. Use the script tag to refer to the label in scripts. For a list of label properties that can be scripted, refer to *Scripts and Expressions - Properties of Objects*.

4. **Details:** To edit the text and formatting of the label, click Details. The Properties dialog box opens.

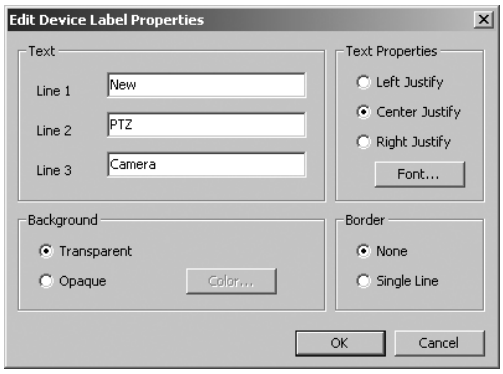


Figure 206. New Label Properties Dialog Box

5. **Text:** Type up to three lines of text as the label contents. When you place the label on a map, this text will display in the label. Each line of text can be at most 50 characters long and can include any letter, digit or special character, with the exception of single and double quotation marks.

6. **Text properties:** Select the justification you want for the label's text. All the lines of text will be justified the same. Click Font to select the font for the label's text, as well as display attributes like bold face and italics.

7. **Background:** Select the background you want for the label you are creating. A transparent background allows the underlying map to show through. An opaque background makes the label appear as a colored rectangle. Click Select Color to choose the fill color for an opaque label.

8. **Border:** Specify whether you want the label to have a border around it by selecting None or Single Line.

9. Click OK. The Properties dialog box closes.

10. **Run script:** If you want to associate a script with the label, type the script in the Run Script area.

    If you want the script to run with a single click of the label, select Single-Click. If you want the script to run when the label is double-clicked, select Double-Click.

    Type the script actions directly into the Action column, or use the script wizard to help you write the script. For more information on writing scripts, refer to *Scripts and Expressions*.

    To test the script, save the server configuration, log in to the client, load the map the label is on, and click the label.

11. Click OK. The new label is created and the Add New Label dialog box closes. The name and script tag of the new label appear in the right pane of the Object Browser.

NOTE: You cannot change the orientation of a label. Labels are always oriented horizontally.

PLACE A LABEL ON A MAP

1. Load the map you want to place the label on. The map appears in the map viewport.

2. Navigate the Object Browser to [project name] > Labels. In the right pane, click the label you want to place on the map and hold the mouse button down. If you move the pointer slightly, it changes to cross-hairs.

3. **Place:** Drag the pointer to the map, position it where you want to place the label, and release the mouse button. The label appears on the map and the pointer changes back to a pointer.

EDIT A LABEL

NOTES:

- A label's properties apply to all instances of the label. When you edit one instance of a label, it changes all other instances of the label.
- If you change the script tag for a label, any script that refers to the label will contain an error. To correct the error, update the scripts so they use the label's new script tag. Refer to *Scripts and Expressions* for more information.

To change the properties of an existing label:

1. Navigate the Object Browser to [project name] > Labels. In the right pane, double-click the label you want to edit, or right-click the label and select Edit from the pop-up menu. Alternatively, load the map the label is on, right-click the label, and select Edit Label from the pop-up menu. The Edit Label Properties dialog box opens.

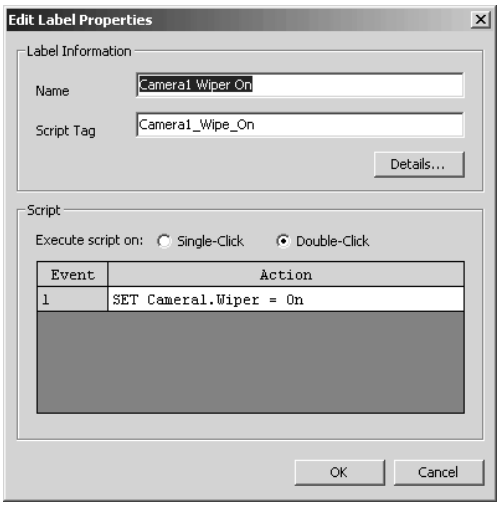


Figure 207. Edit Label Properties Dialog Box

2. Change properties of the label as desired. Refer to *Add a New Label* for information on specific properties.
3. Click OK. The Edit Label Properties dialog box closes.

NOTE: When you edit a label's script, make it available in its updated form by saving the server configuration before attempting to run the script.

MOVE A LABEL

NOTE: You cannot move a label directly from one map to another. You must remove the label from the first map and place it on the other map.

To move a label to a different location on a particular map:

1. With the desired map loaded, right-click the label you want to move and select Move from the pop-up menu.
2. **Move:** Drag the label to its new location.
3. When the label is located where you want it, press the left mouse button. If the map has a grid, the label will snap to the nearest grid point. The label freezes in place.

SCALE A LABEL

To change the size of a label:

1. With the desired map loaded, right-click the label you want to scale and select Scale from the pop-up menu.
2. **Scale:** Move the pointer closer to the label to make is smaller. Move the pointer away from the label to make it larger.
3. When the label is scaled the way you want it, press the left mouse button. The label's size freezes.

REMOVE A LABEL FROM A MAP

Removing a label from a map does not affect any other instances of the label that have been placed on that map or any other map. If you change your mind after removing a label from a map, you can add it back as described in *Place a Label on a Map*.

With the desired map loaded, right-click the label you want to remove from the map and select Remove from the pop-up menu. The label disappears from the map.

DELETE A LABEL

NOTES:

- Deleting a label is irreversible. If you delete a label and then change your mind, you must re-create it as described in *Add a New Label*. If you have placed instances of a particular label on one or more maps and you delete the label, every instance of the label will be removed from any map that has one, regardless of whether the map is loaded at the time. The label will disappear from your server configuration altogether.
- Deleting a label that is referred to in a script introduces an error into the script. Refer to *Scripts and Expressions* for more information.

1. Navigate the Object Browser to [project name] > Labels. In the right pane, right-click the label you want to delete and select Delete from the pop-up menu. The Confirm dialog box opens.
2. If you are sure you want to delete the label, click Yes. The selected label is deleted and the Confirm dialog box closes. All instances of the deleted label are removed from maps. The name of the deleted label disappears from the Object Browser.

Scripts and Expressions

Use scripts and expressions as tools to automate your system. Scripts and expressions are defined as follows:

- **Scripts:** A script is a custom program written within VMX300(-E). Scripts are used to automate common tasks and to ensure that the correct conditions exist before a particular action takes place.
- **Expressions:** Expressions are used to detect a condition that triggers an action. For example, when the expression associated with a timer becomes true, the timer starts. Similarly, when the expression associated with an alarm or event becomes true, recipients are notified and the alarm/event's script is executed. Expressions are also used in IF statements.

You can use the following types of scripts in a VMX300(-E) system:

- **Local Scripts:** Most scripts are local, that is, they cannot be run from other scripts. This includes scripts associated with the following:
  - Labels
  - Hotlinks
  - Timers
  - Prompts
  - Schedules
  - Alarms and events
- **Global scripts:** Global scripts can be run from other scripts. If there is an action you want performed by more than one script, define the action in a global script and then call it from the other scripts. Refer to *Global Scripts* for more information.

VMX300(-E) provides the following tools to help you develop error-free code:

- **Context-Sensitive Help:** These are pop-up menus that offer valid options for the current position within a statement. Refer to *Context-Sensitive Help for Scripts* and *Context-Sensitive Help for Expressions* for more information.
- Expression Wizard: This wizard steps you through the creation of an expression. Refer to *The Expression Wizard* for more information.
- Script Wizard: This wizard steps you through the creation of a statement. Refer to *The Script Wizard* for more information.
- Syntax Error-Checking: Hover help containing error messages and information on command syntax, is available as you enter each line of a script. When you save the server configuration, syntax errors are identified, and tools are provided to edit the objects containing errors. Refer to *Syntax Error-Checking* for more information.

When you edit a script, you must make it available in its updated form by saving the server configuration.

TIP: Use global tags to implement script return values. For example, if you have a prompt with three buttons, set global tags to reflect which button the operator clicked, to pass back to the script that called the prompt. Refer to *Global Tags* for more information.

VARIABLES AND VALUES

Scripts and expressions are made up of variables and values, which are defined as follows:

Variables: Object properties act as variables. They are written as follows:

[object tag name].[property name]

where [object tag name] is an object's script tag, and [property name] is a property of that particular type of object. For example, the following are all valid variables:

Door_Alarm.Value

DVR2.CommStatus

Alarm_Timer.NO

Values: Property values act as values that variables can be compared to. They are written as follows:

[object tag name].[property value name]

where [object tag name] is an object's script tag, and [property value name] is a value of that particular object property. For example, the following are all valid property values:

Door_Alarm.True

DVR2.Online

Alarm_Timer.True

Other possible values are the following:

- Numeric values
- Boolean values: False, True (or 0, 1)

Refer to *Properties of Objects* for a list of valid object properties and values.

PROPERTIES OF OBJECTS

Object properties perform the role of variables in VMX300(-E) scripts and expressions. Table T lists the properties different types of objects have and the values each property can take.

Since device properties are device-dependent, the specific properties of each device are listed in the tables following Table T.

Refer to *View a Device's Read and Write Properties* in the *Device Settings* section for more information on viewing read and write properties.

Table T. Properties and Values of Objects

OBJECT	PROPERTY	VALUES
Alarm or Event	Value	False, true (or 0, 1)
	Acknowledged	False, true (or 0, 1)
Client	Workspace	"path" e.g. "c:\Program Files\CS_ProgramFiles\alarmworksapce.wsp"
Custom Window	LiveSource	[device tag name]
	ArchivedSource	[device tag name]
	Map	[map tag name]
	RemotePC	[computer name] or [IP address]
	URL	"[URL]" e.g. "www.devicesrus.com"
Date	DayOfMonth	1, 2, 3, ... 31
	DayOfWeek	Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday
	Hour	0, 1, 2, ... 23, where 0 is midnight
	IsHoliday	False, true (or 0, 1)
	IsWeekday	False, true (or 0, 1)
	IsWeekend	False, true (or 0, 1)
	Minute	0, 1, 2, ... 59, where 0 is less than a minute past the hour
	Month	January, February, March, ... December
	Year	[YYYY] e.g. 2004
Global Tag	Value	False, true (or 0, 1)
Hotlink	NormalFillColor	Black, blue, cyan, default, green, magenta, orange, red, white, yellow
	NormalBorderColor	Black, blue, cyan, default, green, magenta, orange, red, white, yellow
	NormalBorderVisible	False, true (or 0, 1)
	NormalTransparency	0, 1, 2, . 100
	HoverFillColor	Black, blue, cyan, green, magenta, orange, red, white, yellow
	HoverBorderColor	Black, blue, cyan, green, magenta, orange, red, white, yellow
	HoverBorderVisible	False, true (or 0, 1)
	HoverTransparency	0, 1, 2, ... 100
Label	BackColor	Black, blue, cyan, default, green, magenta, orange, red, white, yellow
	Line1Text	"Place your text between double quotation marks"
	Line2Text	"Place your text between double quotation marks"
	Line3Text	"Place your text between double quotation marks"
	TextColor	Black, blue, cyan, default, green, magenta, orange, red, white, yellow
Local Variable	Value	False, true (or 0, 1)
RecipientObject	LiveVideoSource	[device tag name]
	ArchivedVideoSource	[device tag name]
	AudioMode	Off, Receive, Send, SendReceive
	Map	[map tag]
	RemotePC	[computer name] or [IP address]
	URL	"[URL]" e.g. "www.devicesrus.com"
Timer	Value	False, true (or 0, 1)

FIXED CAMERA PROPERTIES EXPOSED FOR SCRIPTS AND EXPRESSIONS

The following table lists Fixed Camera device properties that can be used in scripts and expressions.

Table U. Fixed Camera Properties and Values

TYPE OF PROPERTY	PROPERTY	VALUE	INDICATES
Write	Alarm	True (1)	Set Alarm to True to indicate the device is in an alarm state. Device icons flash in the alarm colors when Alarm is True.
		False (0)	Set Alarm to False to indicate the device is not in an alarm state.
Signal source	Output	n/a	Use in SET statements to assign the source for live video. **Example:** SET window1.LiveSource = fixed_camera1.output.

PTZ CAMERA PROPERTIES EXPOSED FOR SCRIPTS AND EXPRESSIONS

The following table lists Pelco PTZ camera properties that can be used in scripts and expressions.

For instructions on creating user-defined presets and patterns for PTZ cameras, refer to *Devices* in the Client Operation Manual. To see newly created presets and patterns in the PTZ camera's read and write properties in the Object Browser, you must force the server to update its read/write property lists for that device. To do this, open the Edit Driver Properties dialog box for that driver, and then click Synchronize.

Table V. PTZ Cameras Properties and Values

TYPE OF PROPERTY	PROPERTY	VALUE	INDICATES
Read	CommStatus	Online	The device driver is successfully communicating with the camera.
		Offline	The device driver cannot communicate with the camera. This could be a result of the serial cable being removed or the camera's power being turned off. In Spectra III cameras, offline status could indicate that feedback expected from the camera was not received.
	Preset	NoPreset	The camera's current view is not the result of a preset.
		<preset *i*>	The camera's current view results from going to this user-defined preset. This value is created when you create the preset. Note that "*i*" equals the preset number, which can range from 1 to the maximum number available in the camera.
	Pattern	NoPattern	The camera is not currently running a pattern.
		<pattern *i*>	The camera is currently running this user-defined pattern. This value is created when you create the pattern. Note that *"i"* equals the pattern number, which can range from 1 to the maximum number available in the camera.

(Continued on next page)

Table V. PTZ Cameras Properties and Values (Continued)

TYPE OF PROPERTY	PROPERTY	VALUE	INDICATES
Write	Preset	DontCare	When a SET statement with a FOR clause causes a camera to go to a preset, the camera is locked in the preset view for the duration specified in the FOR clause. The lock is automatically released once the specified duration has elapsed. Setting the Preset write property to DontCare releases the lock prior to the specified time, allowing the camera view to be changed immediately. For information on locking PTZ cameras, refer to *Devices* in the Client Operation Manual.
		<preset *i*>	Go to this user-defined preset. This value is created when you create the preset. Note that *"i"* equals the preset number, which can range from 1 to the maximum number available in the camera.
	Pattern	DontCare	When a SET statement with a FOR clause runs a pattern, the pattern runs for at least the duration specified in the FOR clause. Setting the Pattern property to DontCare releases the camera from having to run the pattern for the specified duration, allowing the pattern to be stopped. Setting Pattern to DontCare does not itself terminate the pattern; it simply enables the pattern to be stopped. For information on locking PTZ cameras, refer to *Devices* in the Client Operation Manual.
		<pattern *i*>	Run this user-defined pattern. This value is created when you create the pattern. Note that *"i"* equals the pattern number, which can range from 1 to the maximum number available in the camera.
	Alarm	True (1)	Set Alarm to True to indicate the device is in an alarm state. Device icons flash in the alarm colors when Alarm is True.
		False (0)	Set Alarm to False to indicate the device is not in an alarm state.
	Auxiliary*i*	On	Turn on the camera's Auxiliaryi feature. Note that *"i"* equals the auxiliary number, which can range from 1 to the maximum number available in the camera. Renaming the auxiliary renames this property. Refer to the *Add a Pelco PTZ Device* section for instructions on renaming auxiliaries.
		Off	Turn off the camera's Auxiliary*i* feature.

PELCONET DEVICE PROPERTIES EXPOSED FOR SCRIPTS AND EXPRESSIONS

The following table lists PelcoNet device properties that can be used in scripts and expressions.

Table W. PelcoNet Device Properties and Values

TYPE OF PROPERTY	PROPERTY	VALUE	INDICATES
Read	Status	Commloss	The device driver cannot communicate with the device.
		Unknown	The driver is initializing and has not yet attempted to communicate with the device.
		Normal	The device is in its normal state.
		Common-Alarm	At least one of the following is true: • The DigitalInput read property has value On. • The Motion read property has value True. • The Video read property has value Loss.
	AlarmInput	True (1)	There is digital input into the device.
		False (0)	There is no digital input into the device.
	RelayOutput	True (1)	The device's relay is closed.
		False (0)	The device's relay is open.
	Motion	True	The device's built-in motion detector detects motion.
		False	The device's built-in motion detector does not detect motion.
	Video	Present	There is video on the device's video input.
		Loss	There is no video on the device's video input.

(Continued on next page)

Table W. PelcoNet Device Properties and Values (Continued)

TYPE OF PROPERTY	PROPERTY	VALUE	INDICATES
Write	RelayOutput	True (1)	Close the device's relay.
		False (0)	Open the device's relay.
Signal source	PelcoNet_HDD	n/a	*Applies to PelcoNet 350 encoders only.* Use in SET statements to assign the source for archived video. **Example:** SET window1.ArchivedSource = encoder1.PelcoNet_HDD. Note that this property is available only when "This unit has integral recording capability" has been selected on the PelcoNet device's Properties tab. Refer to the *Add a PelcoNet MPEG Device* section for information on the Properties tab.
	NVR300_IP<ID>	n/a	*Applies to encoders and encoder/decoders only.* <ID> is the rightmost number in the NVR300's IP address. For example, if the NVR300's IP address is 192.168.1.53, the write property for that NVR is NVR_IP53. Use this property in SET statements to assign the source for archived video. **Example:** SET window2.ArchivedSource = encoder/decoder2.NVR300_IP53. Note that this property is available only when the NVR300 with the specified ID has been added to the PelcoNet device's NVR300 Recording tab. Refer to the *Add a PelcoNet MPEG Device* section for information on the NVR Recording tab.

EXTERNAL MONITOR PROPERTIES EXPOSED FOR SCRIPTS AND EXPRESSIONS

The following table lists External Monitor device properties that can be used in scripts and expressions.

Table X. External Monitor Properties and Values

TYPE OF PROPERTY	PROPERTY	VALUE	INDICATES
Write	Alarm	True (1)	Set Alarm to True to indicate the device is in an alarm state. Device icons flash in the alarm colors when Alarm is True.
		False (0)	Set Alarm to False to indicate the device is not in an alarm state. Device icons display in the Screen and Border colors when Alarm is False.
Signal destination	Input	n/a	Use in SET statements to assign the destination for live video. **Example:** SET external_monitor1.input = camera1.output.

DX9000 READ PROPERTY EXPOSED FOR SCRIPTS AND EXPRESSIONS

The following table lists the DX9000 DVR property that can be used in scripts and expressions.

NOTE: You can set up a DX9000 DVR to start or stop recording automatically in response to motion or time through the DX9000 unit itself. You cannot script a DX9000 DVR to start or stop recording automatically using the scripting language provided in VMX300(-E).

Table Y. DX9000 Read Property and Values

TYPE OF PROPERTY	PROPERTY	VALUE	INDICATES
Read	Status	Online	The device driver is successfully communicating with the DVR.
		Offline	The device driver cannot communicate with the DVR. This could be a result of the network cable being removed or the DVR's power being turned off.

DX8000 PROPERTIES EXPOSED FOR SCRIPTS AND EXPRESSIONS

The following tables list DX8000 properties that can be used in scripts and expressions.

For instructions on creating user-defined presets and patterns for DX8000 cameras, refer to *Scripts* in the Client Operation Manual. To see newly created presets and patterns in the DX8000 camera's read and write properties in the Object Browser, you must force the server to update its read/write property lists for that device. To do this, open the Edit Driver Properties dialog box for that driver, and then click Synchronize.

Table Z. DX8000 Recorder Properties and Values

TYPE OF PROPERTY	PROPERTY	VALUE	INDICATES
Read	CommStatus	Online	The device driver is successfully communicating with the recorder.
		Offline	The device driver cannot communicate with the DVR. This could be a result of the network cable being removed or the DVR's power being turned off.
	Alarm*ii*	True	The DVR alarm input numbered *ii* is True.*
		False	The DVR alarm input numbered *ii* False.*
		Unknown	The device driver has just started up and has not yet received an alarm input event; so it cannot determine the state of the DVR alarm input numbered *ii*.*
		*Note that *"ii"* equals the alarm input number, which can range from 01 to the maximum number available on the DVR (8 inputs on the DX8008; 16 inputs on the DX8016).	
	Relay*ii*	True	The DVR relay output numbered *ii* is True.*
		False	The DVR relay output numbered *ii* False.*
		Unknown	The device driver has just started up and has not yet received a relay output event; so it cannot determine the state of the DVR relay output numbered *ii*.*
		*Note that *"ii"* equals the relay output number, which can range from 01 to the maximum number available on the DVR (8 relays on the DX8008; 16 relays on the DX8016).	
Write	Alarm	True	Set Alarm to True to indicate the DVR is in an alarm state. DVR icons flash in the alarm colors when Alarm is set to True.
		False	Set Alarm to False to indicate the DVR is not in an alarm state.
Signal Source	Channel_*ii*		Specify the source of the archived video to display in a custom window.* **Example:** To display archived video from Channel_01 of the DX8000 with script tag DX8000_1 in the custom window with script tag Window_01 use the following script: SET Window_01.ArchivedSource = DX8000_1.Channel_01 *Note that "ii" equals the channel number, which can range from 01 to the maximum number available on the DVR (8 channels on the DX8008; 16 channels on the DX8016).

Table AA. DX8000 Camera Properties and Values

TYPE OF PROPERTY	PROPERTY	VALUE	INDICATES
Read	Preset	NoPreset	The camera's current view is not the result of a preset.
		<preset *i*>	The camera's current view results from going to this user-defined preset. This value is created when you create the preset. Note that *"i"* equals the preset number, which can range from 1 to the maximum number available in the camera.
	Pattern	NoPattern	The camera is not currently running a pattern.
		<pattern *i*>	The camera is currently running this user-defined pattern. This value is created when you create the pattern. Note that *"i"* equals the pattern number, which can range from 1 to the maximum number available in the camera.
Write	Preset	DontCare	When a SET statement with a FOR clause causes a camera to go to a preset, the camera is locked in the preset view for the duration specified in the FOR clause. The lock is automatically released once the specified duration has elapsed. Setting the Preset write property to DontCare releases the lock prior to the specified time, allowing the camera view to be changed immediately. For information on locking DX8000 cameras, refer to *Devices* in the Client Operation Manual.
		<preset *i*>	Go to this user-defined preset. This value is created when you create the preset. Note that *"i"* equals the preset number, which can range from 1 to the maximum number available in the camera.
	Pattern	DontCare	When a SET statement with a FOR clause runs a pattern, the pattern runs for at least the duration specified in the FOR clause. Setting the Pattern property to DontCare releases the camera from having to run the pattern for the specified duration, allowing the pattern to be stopped. Setting Pattern to DontCare does not itself terminate the pattern; it simply enables the pattern to be stopped. For information on locking DX8000 cameras, refer to *Devices* in the Client Operation Manual.
		<pattern *i*>	Run this user-defined pattern. This value is created when you create the pattern. Note that *"i"* equals the pattern number, which can range from 1 to the maximum number available in the camera.
	Alarm	True	Set Alarm to True to indicate the camera is in an alarm state. Camera icons flash in the alarm colors when Alarm is True.
		False	Set Alarm to False to indicate the camera is not in an alarm state.
	Auxiliary*i*	On	Turn on the camera's Auxiliaryi feature. Note that *"i"* equals the auxiliary number, which can range from 1 to the maximum number available in the camera. Renaming the auxiliary renames this property. Refer to the *Add a DX8000 Camera* section for instructions on renaming auxiliaries.
		Off	Turn off the camera's Auxiliary*i* feature.

ASCII DEVICE PROPERTIES EXPOSED FOR SCRIPTS AND EXPRESSIONS

The following tables list Pelco ASCII device properties that can be used in scripts and expressions.

For instructions on creating user-defined presets and patterns for ASCII cameras, refer to *Scripts* in the Client Operation Manual. To see newly created presets and patterns in the ASCII camera's read and write properties in the Object Browser, you must force the server to update its read/write property lists for that device. To do this, open the Edit Driver Properties dialog box for that driver, and then click Synchronize.

Table AB. ASCII Switcher Properties and Values

TYPE OF PROPERTY	PROPERTY	VALUE	INDICATES
Read	CommStatus	Online	The device driver is successfully communicating with the switcher.
		Offline	The device driver cannot communicate with the switcher. This could be a result of the serial cable being removed or the switcher's power being turned off.
Write	Alarm	True	Set Alarm to True to indicate the device is in an alarm state. Device icons flash in the alarm colors when Alarm is set to True.
		False	Set Alarm to False to indicate the device is not in an alarm state.

Table AC. ASCII Camera Properties and Values

TYPE OF PROPERTY	PROPERTY	VALUE	INDICATES
Read	Preset	NoPreset	The camera's current view is not the result of a preset.
		<preset *i*>	The camera's current view results from going to this user-defined preset. This value is created when you create the preset. Note that *"i "* equals the preset number, which can range from 1 to the maximum number available in the camera.
	Pattern	NoPattern	The camera is not currently running a pattern.
		<pattern *i*>	The camera is currently running this user-defined pattern. This value is created when you create the pattern. Note that *"i "* equals the pattern number, which can range from 1 to the maximum number available in the camera.
Write	Preset	DontCare	When a SET statement with a FOR clause causes a camera to go to a preset, the camera is locked in the preset view for the duration specified in the FOR clause. The lock is automatically released once the specified duration has elapsed. Setting the Preset write property to DontCare releases the lock prior to the specified time, allowing the camera view to be changed immediately. For information on locking ASCII cameras, refer to *Devices* in the Client Operation Manual.
		<preset *i*>	Go to this user-defined preset. This value is created when you create the preset. Note that *"i "* equals the preset number, which can range from 1 to the maximum number available in the camera.
	Pattern	DontCare	When a SET statement with a FOR clause runs a pattern, the pattern runs for at least the duration specified in the FOR clause. Setting the Pattern property to DontCare releases the camera from having to run the pattern for the specified duration, allowing the pattern to be stopped. Setting Pattern to DontCare does not itself terminate the pattern; it simply enables the pattern to be stopped. For information on locking ASCII cameras, refer to *Devices* in the Client Operation Manual.
		<pattern *i*>	Run this user-defined pattern. This value is created when you create the pattern. Note that *"i "* equals the pattern number, which can range from 1 to the maximum number available in the camera.
	Alarm	True (1)	Set Alarm to True to indicate the camera is in an alarm state. Camera icons flash in the alarm colors when Alarm is True.
		False (0)	Set Alarm to False to indicate the camera is not in an alarm state.
	Auxiliary*i*	On	Turn on the camera's Auxiliary*i* feature. Note that *"i"* equals the auxiliary number, which can range from 1 to the maximum number available in the camera. Renaming the auxiliary renames this property. Refer to the *Add an ASCII Camera* section for instructions on renaming auxiliaries.
		Off	Turn off the camera's Auxiliary*i* feature.

KBD300A PROPERTIES EXPOSED FOR SCRIPTS AND EXPRESSIONS

The following table lists Pelco KBD300A device properties that can be used in scripts and expressions.

Table AD. KBD300A Properties and Values

TYPE OF PROPERTY	PROPERTY	VALUE	INDICATES
Read	Username		Reserved for internal use by system.
	Password		Reserved for internal use by system.
	Camera		Reserved for internal use by system.
	Monitor		Reserved for internal use by system.
	Preset		Reserved for internal use by system.
	MomentaryKey	1	The MOM key is being pressed by the operator. Use this property to trigger an alarm or event. **Example:** You might define the alarm/event expression as follows: Keyboard1.MomentaryKey = 1 Then you can define an On Event script that runs when the expression becomes true.
		0	The MOM key has been released by the operator.
	AuxOnKey	1	The AUX ON key is being pressed by the operator. Use this property to trigger an alarm or event. **Example:** You might define the alarm/event expression as follows: Keyboard1.AuxOnKey = 1 Then you can define an On Event script that runs when the expression becomes true.
		0	The AUX ON key has been released by the operator.
	AuxOffkey	1	The AUX OFF key is being pressed by the operator. Use this property to trigger an alarm or event. **Example:** You might define the alarm/event expression as follows: Keyboard1.AuxOffKey = 1 Then you can define an On Event script that runs when the expression becomes true.
		0	The AUX OFF key has been released by the operator.
	HoldKey	1 or 0	The value of each of these keys (HOLD, PATTERN, and MACRO) toggles between 1 and 0 each time the key is pressed and released. The value is initially 0. The first time the key is pressed and released, the value becomes 1; the second time, it becomes 0; and so on. Use these properties to trigger an alarm or event. **Example:** You might define the alarm/event expression as follows: Keyboard1.HoldKey = 1 Then you can define an On Event script that runs when the expression becomes true.
	PatternKey	1 or 0	
	MacroKey	1 or 0	

CM9760-ALM PROPERTIES EXPOSED FOR SCRIPTS AND EXPRESSIONS

The following table lists CM9760-ALM alarm unit properties that can be used in scripts and expressions.

Table AE. CM9760-ALM Properties and Values

TYPE OF PROPERTY	PROPERTY	VALUE	INDICATES
Read	Status	CommLoss	The device driver cannot communicate with the device.
		Normal	The device is in its normal state.
		Unknown	The communications status between the device driver and the device cannot be determined.
	Alarm	True	The alarm unit is currently in an alarm state.
		False	The alarm unit is not in an alarm state.
	Point_*iii*	True	The relay output numbered *iii* is True.*
		False	The relay output numbered *iii* is False.*
		*Note that *"iii"* equals the alarm input number, which can range from 001 to the maximum number available on the alarm units (the maximum number for one relay unit is 64; with two daisy-chained alarm units the maximum number is 128, and so on to a maximum of 256).	
Write	Alarm	True	Set Alarm to True to indicate the CM9760-ALM is in an alarm state. CM9760-ALM icons flash in the alarm colors when Alarm is set to True.
		False	Set Alarm to False to indicate the CM9760-ALM is not in an alarm state.

Sample VMX300(-E) Alarm Expression

To take advantage of the alarm-handling capabilities provided by VMX300(-E), including operator notification and automated execution of scripts, you can define a VMX300(-E) alarm based on an CM9760-ALM alarm input. To define a VMX300(-E) alarm that is triggered by an alarm unit contact, add a new alarm to the server configuration and use the appropriate CM9760-ALM alarm input point in the alarm expression.

Example: Use the following syntax to define a VMX300(-E) alarm that is triggered by Point_001 on the alarm unit named CM9760-ALM_1

Alarm_Module_1.Point_001 = Alarm_Module_1.True

Refer to the *Alarms and Events* section for instructions on adding alarms to the server configuration.

Defining Normally Open and Normally Closed Alarm Inputs

Alarm inputs are commonly wired as normally open (N.O.), so that if the sensor contact closes, the alarm is triggered. When the alarm is triggered, the alarm state corresponds to "True" in VMX300(-E), whereas "False" corresponds to the normal (nonalarm; N.O.) state of the input.

When an alarm is wired as normally closed (N.C.), the alarm state still corresponds to "True" in VMX300(-E), and "False" still corresponds to the normal (non-alarm) state, which is N.C. in this case.

When you define an alarm expression in the server configuration, the expression tests whether the point is "True," regardless of whether the actual alarm input is wired as N.O. or N.C., as shown in the following table.

Table AF. Defining Normally Open and Normally Closed Alarm Inputs

State of Contact	N.O.	N.C.
Open	False	True
Closed	True	False

CM9760-REL PROPERTIES EXPOSED FOR SCRIPTS AND EXPRESSIONS

The following table lists CM9760-REL relay interface unit properties that can be used in scripts and expressions.

Table AG. CM9760-REL Properties and Values

TYPE OF PROPERTY	PROPERTY	VALUE	INDICATES
Read	Status	CommLoss	The device driver cannot communicate with the device.
		Normal	The device is in its normal state.
		Unknown	The communications status between the device driver and the device cannot be determined.
	Alarm	True	The relay unit is currently in an alarm state.
		False	The relay unit is not in an alarm state.
	Point_*iii*	True	The relay output numbered *iii* is True.*
		False	The relay output numbered *iii* is False.*
Write	Alarm	True	Set Alarm to True to indicate the CM9760-REL is in an alarm state. CM9760-REL icons flash in the alarm colors when Alarm is set to True.
		False	Set Alarm to False to indicate the CM9760-REL is not in an alarm state.
	Point_*iii*	True	Set Point_*iii* to True. **Example:** SET Relay_Unit_01.Point_001 = True
		False	Set Point_*iii* to False. **Example:** SET Relay_Unit_01.Point_001 = False
*Note that *"iii"* equals the relay output number, which can range from 001 to the maximum number available on the relay units (the maximum number for one relay unit is 64; with two daisy-chained relay units the maximum number is 128, and so on).			

Changing the State of a Relay Point

An operator can change the state of a relay point by working within the CM9760-REL relay unit's Device Control dialog box in the client (refer to the Client Operation Manual for instructions). However, you may want to allow an operator to change the state of a relay point without opening the Device Control dialog box. VMX300(-E) provides the following methods:

- **Global Script:** Write a global script that changes the state of the specific relay point. Give the operator permission to run the global script and permission to control the relay unit. This method is useful when you do not want to give the operator permission to access the relay unit's Device Control dialog box. Refer to the *Global Scripts* section for instructions on writing a global script. Refer to the *User Groups* section for instructions on assigning operator permissions.
- **Label or Hotlink:** Create a label or hotlink that sets the state of a specific relay point and give the operator permission to control the relay unit. This allows the operator to quickly change the state of a frequently accessed relay point, without having to open the Device Control dialog box. Refer to the *Hotlinks* and *Labels* sections for instructions on creating labels and hotlinks. Refer to the *User Groups* section for instructions on assigning operator permissions.

Defining Normally Open and Normally Closed Relay Outputs

Relay outputs are commonly wired as normally open (N.O.), so that if the contact wires close, the relay action is triggered. When the relay is triggered, the relay state corresponds to "True" in VMX300(-E), whereas "False" corresponds to the normal (N.O.) state of the output. For example, if the relay action is to turn on a VCR, "True" equals "On" and "False" equals "Off."

When a relay is wired as normally closed (N.C.), the relay state still corresponds to "True" in VMX300(-E), and "False" still corresponds to the normal state, which is N.C. in this case.

When you define an expression in the server configuration using the relay outputs, the expression tests whether the point is "True," regardless of whether the actual relay output is wired as N.O. or N.C., as shown in the following table.

Table AH. Defining Normally Open and Normally Closed Relay Outputs

State of Contact	N.O.	N.C.
Open	False	True
Closed	True	False

SERIAL OUTPUT DEVICE PROPERTY EXPOSED FOR SCRIPTS AND EXPRESSIONS

The following table lists the serial output device property that can be used in scripts and expressions.

NOTES ON USING SPECIAL ASCII CHARACTERS IN SCRIPTS AND EXPRESSIONS: If a command contains unprintable characters, replace each unprintable character with its three-digit ASCII code between angle brackets. For example, the command BLACK-HOT<Carriage Return> is represented in VMX300(-E) as BLACK-HOT<013>. Note that ASCII codes must be three digits in length. If an ASCII code contains less that three digits add leading zeroes.

When using ASCII characters in scripts and expressions, VMX300(-E) transforms lower case ASCII letters to upper case. If a lower case letter is required in the command, use its ASCII code. For example, the command 1Ra is represented as 1R<097>. If a command contains single or double quotation marks, replace the quotation marks with their ASCII codes: <039> for a single quotation mark and <034> for a double quotation mark.

Table AI. Serial Output Device Write Property

TYPE OF PROPERTY	PROPERTY	VALUE	INDICATES
Write	OutputString		Set OutputString to the device-control command you want to send to the serial output device. The string must be enclosed in double quotation marks. **Example:** If the command to put an infrared camera in black hot mode is "BLACK-HOT" and if the command is terminated by a carriage return ("<013>"), use the following script statement: SET SerialOutputCamera.OutputString = "BLACK-HOT<013>" Run the script to send the string to the camera.

IP DEVICE STATUS MONITOR PROPERTY EXPOSED FOR SCRIPTS AND EXPRESSIONS

The following table lists the IP device status monitor property that can be used in scripts and expressions.

Table AJ. IP Device Status Monitor Read Property and Values

TYPE OF PROPERTY	PROPERTY	VALUE	INDICATES
Read	Status	Alarm	The device failed to respond when pinged; the device is not accessible.
		Commloss	Do not use this value; it is reserved for future use.
		Normal	The device responded when pinged; the device is accessible.
		Unknown	The driver was just launched and the device has not yet been pinged; it is not known whether the device is accessible or not.

ACCESS CONTROL DEVICE PROPERTIES EXPOSED FOR SCRIPTS AND EXPRESSIONS

The following table lists access control device properties that can be used in scripts and expressions.

Table AK. Access Control Device Properties and Values

TYPE OF PROPERTY	PROPERTY	VALUE	INDICATES
Read	Point_*iii*	True	The access control point numbered *iii* is True, indicating that an alarm string has been received that matches Point_*iii*, and the point has not yet been reset.*
		False	The access control point numbered *iii* is False.*
Write	Point_*iii*	True	Do not use this property; it is reserved for future use.
		False	Set Point_*iii* to False to reset the alarm received for the point.

*Note that "*iii*" equals the access control point number, which can range from 001 to the maximum number of alarms available on the access control device.

CURRENT STATUS: VIEW RUN-TIME VALUES OF VARIABLES

When the server is running, you can check the value of read property variables using the Current Status option.

1. Right-click the VMX300(-E) icon in the Windows server tray and select Current Status from the pop-up menu. The Current Status window opens. Variable names are listed alphabetically. Scroll to find the variables whose value you want to find out.

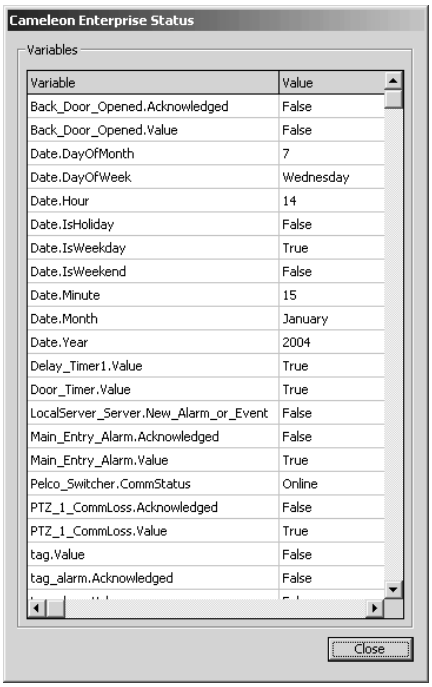


Figure 208. Current Status Window

2. Click Close. The Current Status window closes.

NOTE: The status given in the Current Status window is live. If a variable changes value while the window is open, the change will be reflected in the window.

EXPRESSIONS

Expressions are used to detect a condition that triggers an action. For example, when the expression associated with a timer becomes true, the timer starts. Similarly, when the expression associated with an alarm or event becomes true, recipients are notified and the alarm/event's script is executed. Expressions are also used in IF statements.

Syntax: A simple expression compares an object property to a value. Complex expressions are made up of one or more simple expressions connected by logical operators and optionally containing parentheses.

The operators listed in Table AL are used to compare an object property to a value.

Table AL. Comparison Operators

OPERATOR	MEANING	EXAMPLE
=	equals	Door_Alarm.Value = True
~	not equal to	DVR2.CommStatus ~ DVR2.Online
>	greater than	Date.DayOfMonth > 15
<	less than	Date.Hour < 12

The operators listed in Table AM are used to construct complex expressions.

Table AM. Logical Operators

OPERATOR	MEANING	EXAMPLE
~	unary not	~ (Date.DayOfWeek = Date.Friday)
& *or* AND	and	(Date.DayOfWeek = Date.Monday) & (Date.IsHoliday = False)
| *or* OR	or	(Camera1.CommStatus = Camera1.OffLine) OR (Camera2.CommStatus = Camera2.OffLine)

STATEMENTS

A script is made up of one or more statements. A statement is made up of a command and possibly some arguments. Each statement occupies one line in a script, with the exception of the IF statement, which spans two or more lines. the following table lists the commands used to build statements in VMX300(-E) scripts.

LOCAL VARIABLES: The VMX300(-E) scripting language has local Boolean variables that are declared in a script's DIM or VAR statement. They are local in the sense that they can be accessed only within the script that declares them, as well as from any global script the script calls using the CALL command. They cannot be accessed from a global script run using the RUN command. Any script, global or local, can declare local variables.

Local variables have one property, Value, which is accessed [variable identifier].Value. They can take values True or False, or, equivalently, 1 or 0.

Table AN. Script Commands

Optional arguments are in parentheses. Refer to *Properties of Objects* for valid properties and values of different types of objects.

COMMAND	ACTION
Abort	
ABORT [<global script tag>]	Abort the specified global script, or, if no script is specified, abort the current script.
Call	
CALL <global script tag>	Run the specified global script in the current thread.
DIM	
DIM <variable identifier>	Declare a local Boolean variable. The same as VAR.
Display	
DISPLAY <device tag name>.DeviceControl	Display the Device Control dialog box for the specified device on the client running the script.
FTP	
FTP <window tag>, <camera tag>, [<preset tag>], <preset delay>, <FTP site tag>, "<file name>.jpg"	Switch the camera to the window. Start timing the delay. If a preset is specified, go to the preset. When the delay time has elapsed, capture the video in the window and upload the image to the FTP server, saving it under the specified file name. For more information, refer to *FTP Sites - Write an FTP Script.*
GoTo	
GOTO <label identifier>	Continue running the script at the specified label. The same as JUMP.
If-Then	
IF <expression> [IN <duration>] THEN <statement(s)> [ELSE <statement(s)>] ENDIF	If the expression is true within the specified number of seconds, execute the statement[s) following THEN. Otherwise, execute the statement(s) following ELSE.
Jump	
JUMP <label identifier>	Continue running the script at the specified label. The same as GOTO.
Label	
LABEL <label identifier>	Define a position within the script to GOTO or JUMP to. The label identifier must begin with a letter.

(Continued on next page)

Table AN. Script Commands (Continued)

Optional arguments are in parentheses. Refer to *Properties of Objects* for valid properties and values of different types of objects.

COMMAND	ACTION
Load	
LOAD <map tag>[.<named view>]	Load the specified map or named view into the map viewport.
On Error	
ON ERROR GOTO <label identifier>	If an error occurs, continue running the script at the specified label.
ON ERROR GOTO 0	If an error occurs, continue running the script at the beginning of the script.
ON ERROR RESUME NEXT	If an error occurs, continue running the script at the next line.
Pause	
PAUSE <duration>	Pause the script for the specified number of seconds. The duration can be a decimal amount e.g. 3.5.
Prompt	
PROMPT <prompt tag>	Display the specified prompt in the client window.
Run	
RUN <global script tag>	Run the specified global script in a new thread.
Set	
SET <client tag>.Workspace="<path name>"	Set the client workspace to the workspace file specified in the path name, e.g. SET Client1.Workspace = "c:\Workspaces\Operator_Workspace.wsp".
SET <device tag name>.<write property>= <device tag name>.<state> (FOR <duration>)	Set the write property for the device to the specified state for the specified number of seconds.
SET <global tag>.<property name> = <value>	Set the global tag property to the specified value. Refer to *Properties of Objects* for valid properties and values.
SET <hotlink tag>.<property name>=<value>	Set the hotlink property to the specified value. Refer to *Properties of Objects* for valid properties and values.
SET <label tag>.<property name>=<value>	Set the label property to the specified value. Refer to *Properties of Objects* for valid properties and values.
SET <variable identifier>.<property name>=<value>	Set the local variable property to the specified value. Refer to *Properties of Objects* for valid properties and values.
SET RecipientObject=<window tag>	Set the recipient object to the specified custom window.
SET RecipientObject=<device tag name>	Set the recipient object to the specified video input device.
SET RecipientObject.<property name>=<value>	Set the recipient object to the specified value. Refer to *Properties of Objects* for valid properties and values.
SET <window tag>.<property name> = <value>	Set the custom window property to the specified value. Refer to *Properties of Objects* for valid properties and values.
VAR	
VAR <variable identifier>	Declare a local Boolean variable. The same as DIM.

TIP: Use RecipientObject to implement sequences. For example, if you have a custom window called 'window1' and analog video from cameras 'camera1', 'camera2', etc., implement a sequence as follows:

```
SET RecipientObject = window1
SET RecipientObject.LiveSource = camera1.analogvideo
PAUSE 5
SET RecipientObject.LiveSource = camera2.analogvideo
PAUSE 5
...
```

MECHANICS OF EDITING SCRIPTS AND EXPRESSIONS

You can create and edit scripts and expressions by directly typing the code or by using the script wizard and expression wizard. In either case, context-sensitive help is available to help you create error-free code.

KEYSTROKE EDITING

Use the keystrokes listed in Table AO to edit your scripts. These are also available from a pop-up menu by right-clicking the line of code you want to edit.

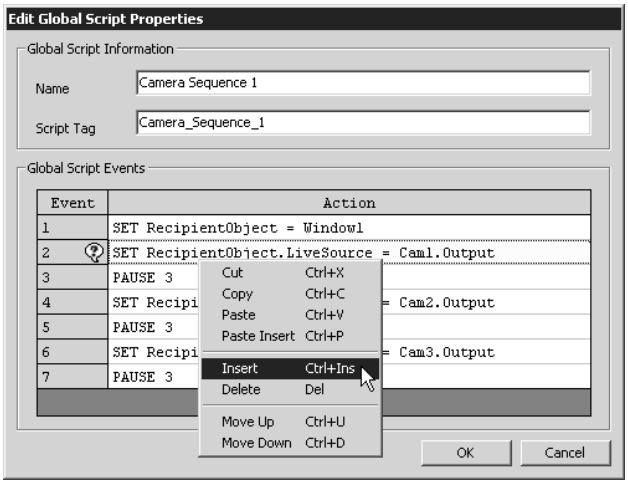


Figure 209. Keystroke Editing

Table AO. Keystrokes for Editing Scripts

KEYSTROKE	EFFECT
Ctrl-X	Cut selected text or lines to clipboard.
Ctrl-C	Copy selected lines to clipboard.
Ctrl-V	Paste contents of clipboard to selected lines or to position of cursor.
Ctrl-P	Insert new line above selected lines and paste contents of clipboard in new line.
Ctrl-Insert	Insert new line above selected lines.
Delete	Delete selected lines or text.
Ctrl-U	Move selected lines up one line.
Ctrl-D	Move selected lines down one line.

TIPS:

- You can apply the keystroke editing options to more than one line at a time. Select multiple consecutive lines by clicking and dragging the line numbers in the Event column.
- If you delete a line of code from a script, then change your mind, use the Undo option to undo the deletion. Right-click the line you deleted the code from and select Undo from the pop-up menu.

CONTEXT-SENSITIVE HELP FOR SCRIPTS

To help you write error-free scripts, VMX300(-E) provides context-sensitive help in the form of pop-up lists. Select an item in the pop-up list and press Enter to enter the item into the current line.

Use pop-up lists as follows:

- At the beginning of a new line, press Ctrl-Space Bar to open a pop-up list of commands.

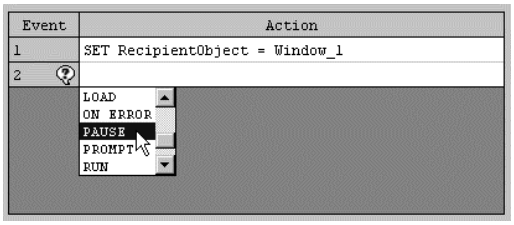


Figure 210. Opening a List of Commands

- After a command, press the space bar once to open a pop-up list of items that can occur as an argument.

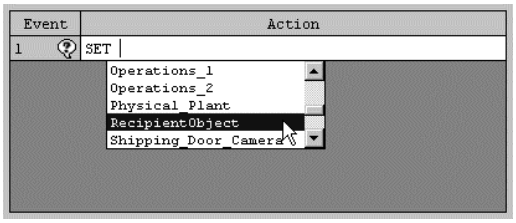


Figure 211. Opening a List of Arguments

- In a command argument that includes an object property, press "." after the object to open a pop-up list of valid properties for that object.

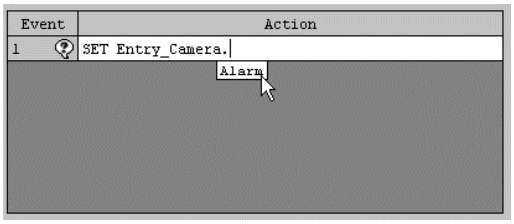


Figure 212. Opening a List of Properties

NOTE: In order for a device's properties to be presented in a context-sensitive pop-up list, the object's properties must be exposed. By default, device properties are exposed. Refer to *Edit a Device's Local Settings* for information on exposing properties.

CONTEXT-SENSITIVE HELP FOR EXPRESSIONS

To help you write error-free expressions, VMX300(-E) provides context-sensitive help in the form of pop-up lists.

To use pop-up lists, complete the following steps:

1. Click the expression editor button next to the Expression field (in either the Add New Timer dialog box or the Add New Alarm or Event dialog box).

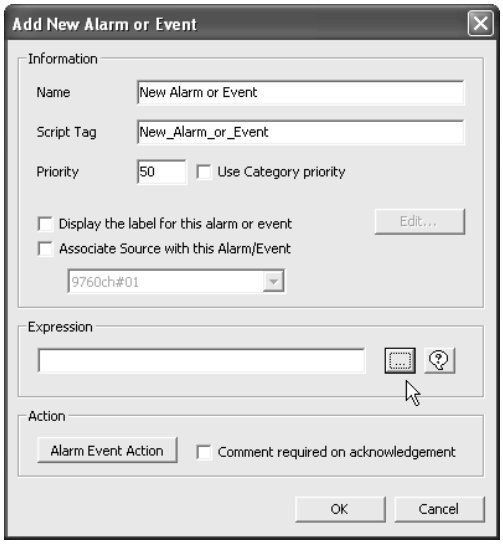


Figure 213. Clicking the Expression Editor Button

The Expression Editor dialog box appears, as shown in Figure 214.

2. From the Expression Editor dialog box you can access pop-up lists as follows:

   - At the beginning of a condition, press Ctrl-Space Bar to open a pop-up list of objects.

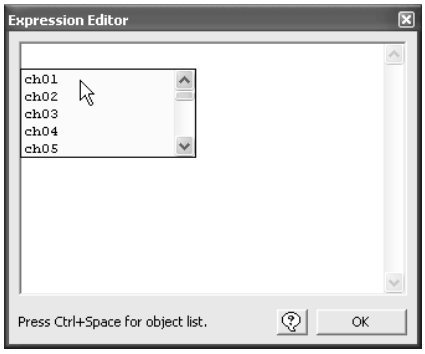


Figure 214. Context-Sensitive Help at the Beginning of an Expression

   - After an object, press "." to open a pop-up list of valid object properties.

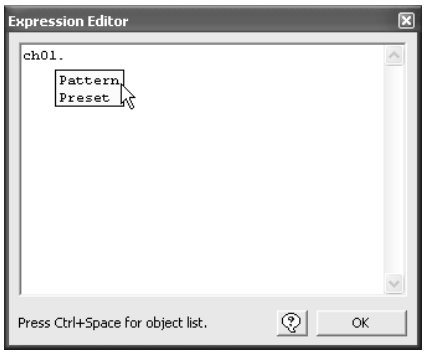


Figure 215. Context-Sensitive Help for Object Properties

- After a condition operator, press Space Bar to open a pop-up list of valid property values.

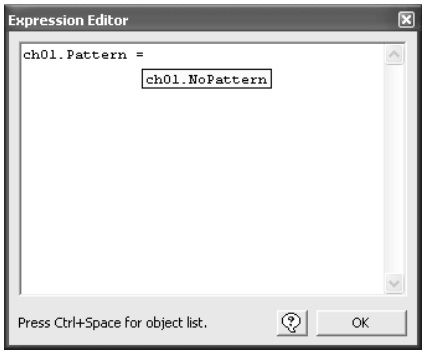


Figure 216. Context-Sensitive Help for Property Values

THE EXPRESSION WIZARD

The expression wizard helps you write an expression for a timer or alarm by stepping you through its creation, providing you with valid options for each part of the expression as needed.

To use the expression wizard, complete the following steps:

1. Click the wizard button. This button is located next to the Expression field in either the Add New Timer dialog box or the Add New Alarm or Event dialog box, and it is also available from the Expression Editor dialog box. 

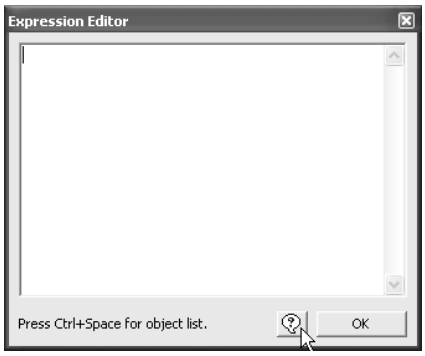


Figure 217. Opening the Expression Wizard from the Expression Editor Dialog Box

The Expression Wizard appears.

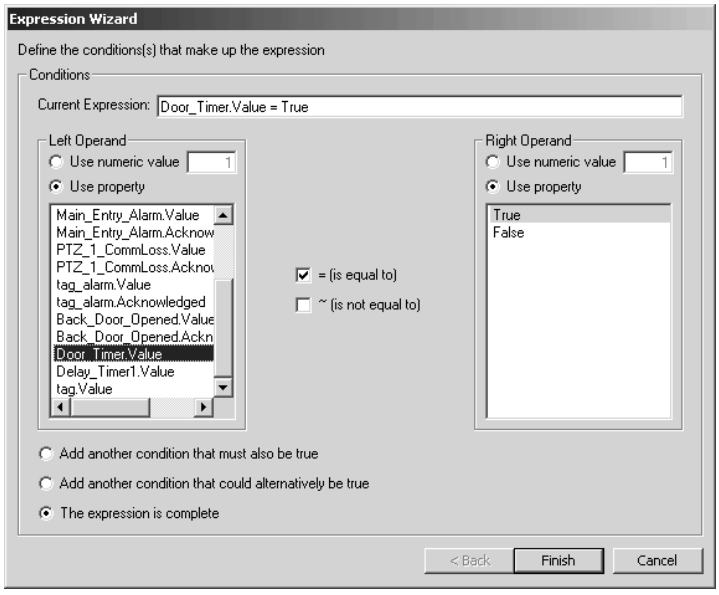


Figure 218. Expression Wizard

2. Select the left operand, operator, and right operand of the condition you are defining. The expression appears in the Current Expression box.
3. (Optional) If you want to add another condition connected by the AND operator, select "Add another condition that must also be true." If you want to add another condition connected by the OR operator, select "Add another condition that could alternatively be true." Then click Next, and repeat step 2.
4. When you have added all the conditions that make up the expression, click Finish. The Expression Wizard dialog box closes and the expression you created appears in the Expression box.

THE SCRIPT WIZARD

The script wizard helps you write a script statement by stepping you through its creation, providing you with valid options for each part of the statement as needed. Since the script wizard creates a single statement, you must re-invoke the wizard for every statement you want help with.

To write a statement using the script wizard:

1. Add or edit the object whose script you want to write.
2. Click the line where you want the new statement to be placed. If you do not want to overwrite existing code, make sure the line you select is blank. If necessary, insert a blank line by positioning the cursor on the line before the position you want the new line, and press Enter. The Script Wizard button appears in the Event column of the selected line.

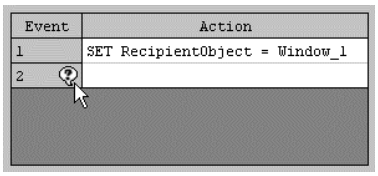


Figure 219. Opening the Script Wizard

3. Click the Script Wizard button. The Script Wizard dialog box opens.

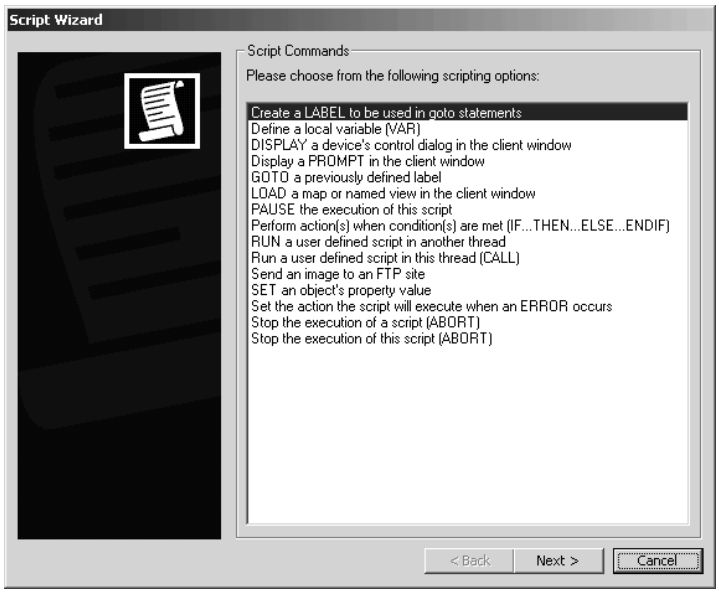


Figure 220. Opening the Script Wizard

4. Select the statement you want to write and press Next.
5. Continue to select options as the script wizard presents them to you until you have built the statement you want, then press Finish. The Script Wizard dialog box closes and the statement you created appears in the Action column of the selected line.

SYNTAX ERROR-CHECKING

VMX300(-E) checks the syntax of each line of a script as you enter it. If an error is detected in a line, the text for the line is displayed in red. For help in identifying the error, position the pointer over the line with the error. This opens hover help containing an error message and information on command syntax.

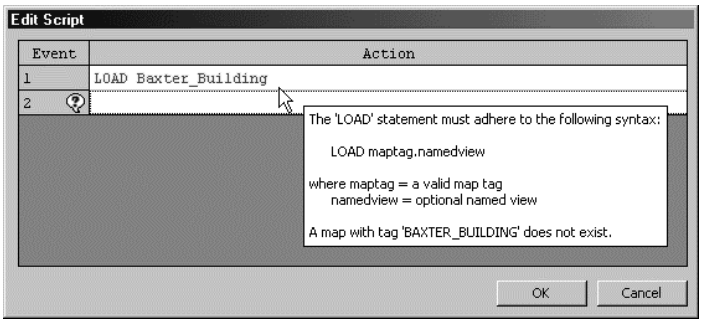


Figure 221. Script Syntax Hover Help

If there is an error in a script or expression when you save the server configuration, the Script and Expression Verification window appears and gives you the option of correcting the error before exiting.

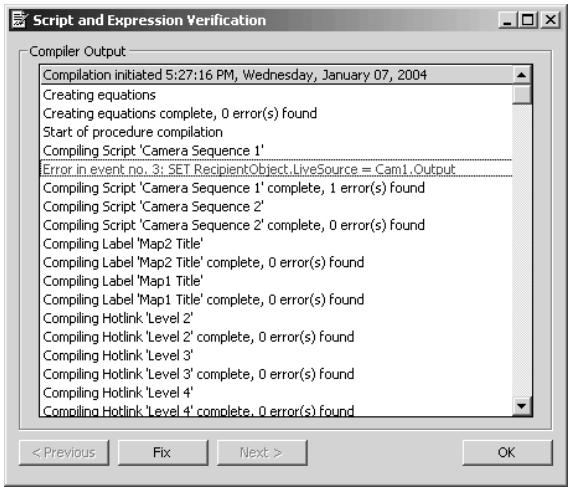


Figure 222. Script and Expression Verification Dialog Box

To correct errors caught when you save the server configuration:

1. In the Script and Expression Verification dialog box, double-click the error you want to fix, or select the error and click Fix. Errors appear in red. The Edit Properties dialog box for the object containing the error opens.
2. Correct the error. Use syntax error-checking hover help to help you identify the error. Click OK. The Edit Properties dialog box closes.
3. Continue correcting errors until there are no more. Click Previous to select the previous error in the list. Click Next to select the next error in the list.
4. Click OK. The Script and Expression Verification dialog box closes and the configuration is saved.

EXAMPLE SCRIPTS

EXAMPLE 1: INITIALIZATION SCRIPT

The following script loads a map into the map viewport and sets the video source for each of three custom windows.

Since this is a global script, any operator with permission to run the script can run it from the client. The script affects only the client it is run on.

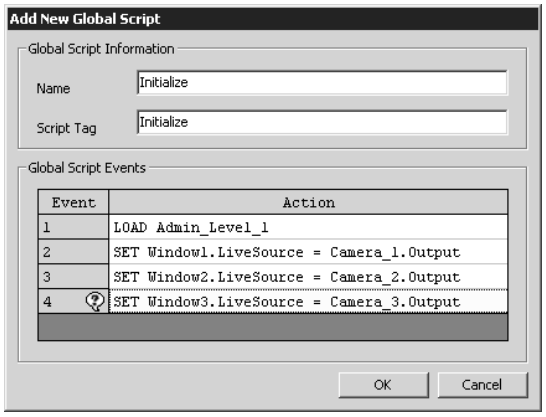


Figure 223. Initialization Script

EXAMPLE 2: CAMERA SEQUENCE

The following script implements a sequence that sends cameras to presets. The sequence repeats until the global tag ContinueSequence becomes false.

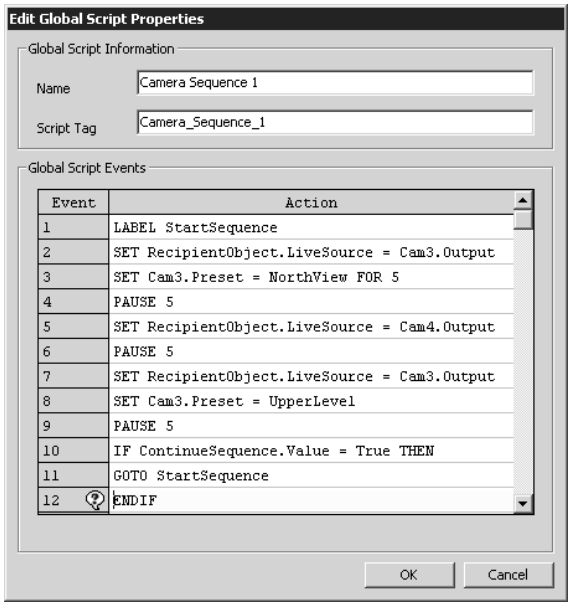


Figure 224. Camera Sequence Script

EXAMPLE 3: ALARM LOCATION SCRIPT

The following alarm scripts highlight an area on a map when the alarm is triggered, then return the area to its normal appearance once the alarm has been acknowledged. The scripts use a hotlink called Area51 to do this.

The On Event script changes the hotlink's normal and mouse hover colors to red and makes the hotlink background visible by giving it a transparency of 10%. The On Acknowledge script sets the hotlink's colors back to the default color and makes the hotlink background invisible. The effect is to make the hotlink appear red when the alarm is triggered.

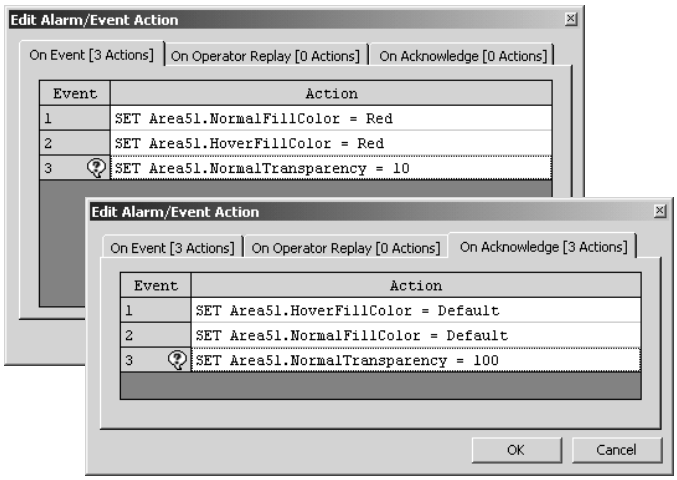


Figure 225. Alarm Scripts

Global Scripts

Global scripts are scripts that can be run from other scripts using the RUN or CALL command. This distinguishes them from the scripts associated with labels, hotlinks, timers, prompts, and alarms and events, which cannot be run from other scripts. If there is an action you want performed by more than one script, define the action in a global script and call it from the other scripts as needed.

Global scripts can also be run directly from a custom window in the client, provided the operator has permission. When you create a user group, if you check the permission for a particular global script, then operators who log in under that user group can run the global script. Refer to *User Groups - Group Permissions* for more information on permissions. For information on how an operator runs a global script from a custom window, refer to *Custom Windows* in the VMX300(-E) Client Operation Manual.

Local Variables: The VMX300(-E) scripting language has local Boolean variables that are declared in a script's DIM or VAR statement. They are local in the sense that they can be accessed only within the script that declares them, as well as from any global script the script calls using the CALL command. They cannot be accessed from a global script run using the RUN command. Any script, global or local, can declare local variables.

ADD A NEW GLOBAL SCRIPT

1. Navigate the Object Browser to [project name] > Global Scripts. Double-click <Add New Global Script> in the right pane, or right-click Global Scripts in the left pane and select Add New from the pop-up menu. The Add New Global Script dialog box opens.

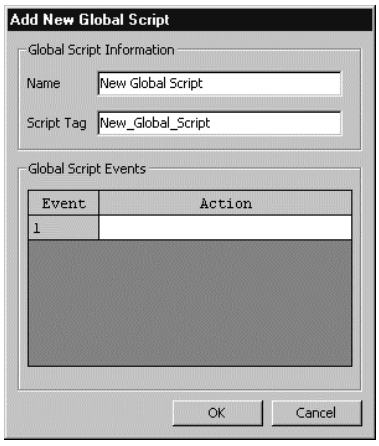


Figure 226. Add New Global Script Dialog Box

2. **Name:** Type in a unique, descriptive name for the global script you want to create. Script names are at most 50 characters long and can include any letter, digit or special character, with the exception of single and double quotation marks. Script names are not case sensitive. A tag resembling the name appears in the Script Tag box. If the name contains special characters, they are omitted from the tag. Spaces are replaced with underscores. Leading digits are removed.

3. **Script tag:** If you do not want to use the script tag provided by the server, type in a unique, meaningful tag. Script tags are at most 50 characters long. They can include any letter, digit or the underscore character, but cannot begin with a digit. They cannot contain spaces or special characters. Tags are not case sensitive. Use the script tag to refer to the global script in other scripts.

4. **Action:** Type the script action directly into the Action column, or use the script wizard to help you write the script. For more information on writing scripts, refer to *Scripts and Expressions*.

5. Click OK. The Add New Global Script dialog box closes and the new global script is created. The name and script tag of the new global script appear in the right pane of the Object Browser.

NOTE: When you edit a global script, make it available in its updated form by saving the server configuration before attempting to run the script.

TIP: A global script that is run from another script can access local variables declared in the calling script. The calling script must CALL, not RUN, the global script.

EDIT A GLOBAL SCRIPT

NOTE: If you change the script tag for a global script, all the scripts that run the global script will contain an error. To correct the error, update the scripts so they use the global script's new script tag.

1. Navigate the Object Browser to [project name] > Global Scripts. In the right pane, double-click the global script you want to change, or right-click the global script and select Edit from the pop-up menu. The Edit Global Script Properties dialog box opens.

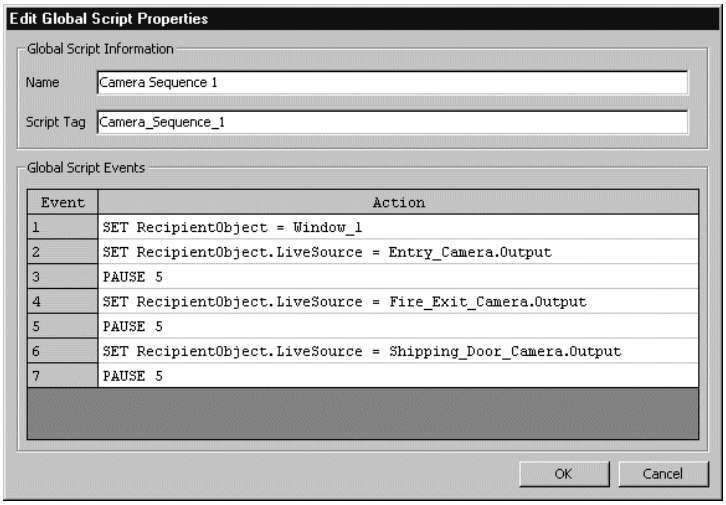


Figure 227. Edit Global Script Properties Dialog Box

2. Change properties of the global script as desired. Refer to *Add a New Global Script* for information on specific properties.
3. Click OK. The Edit Global Script Properties dialog box closes.

NOTE: If you edit a global script's actions, make the global script available in its updated form by saving the server configuration before attempting to run the script.

DELETE A GLOBAL SCRIPT

Deleting a global script is irreversible. If you delete a global script and then change your mind, you must add a new global script. Also note that if you delete a global script, any local script that runs the global script will contain an error.

1. Navigate the Object Browser to [project name] > Global Scripts. In the right pane, right-click the global script you want to delete and select Delete from the pop-up menu. The Confirm dialog box opens.
2. If you are sure you want to delete the global script, click Yes. The selected global script is deleted and the Confirm dialog box closes. The deleted global script disappears from the Object Browser.

Global Tags

A global tag is a Boolean variable that can be used in any script or expression, including both local scripts, such as those defined in hotlinks, labels, schedules, and alarms and events, as well as global scripts. Global tags are used in the same way other Boolean variables are. They can be assigned a value using the SET statement, and compared to a value in an IF statement. Refer to *Scripts and Expressions* for more information.

TIP: Use global tags to implement script return values. For example, if you have a prompt with three buttons, set global tags to reflect which button the operator clicked, to pass back to the script that called the prompt.

ADD A NEW GLOBAL TAG

1. Navigate the Object Browser to [project name] > Global Tags. Double-click <Add New Global Tag> in the right pane, or right-click Global Tags in the left pane and select Add New from the pop-up menu. The Add New Global Tag dialog box opens.

Figure 228. Add New Global Tag Dialog Box

2. **Script tag:** If you do not want to use the script tag provided by the server, type in a unique, meaningful tag. Script tags are at most 50 characters long. They can include any letter, digit or the underscore character, but cannot begin with a digit. They cannot contain spaces or special characters. Tags are not case sensitive. Use the script tag to refer to the global tag in scripts and expressions. For a list of global tag properties that can be scripted, refer to *Scripts and Expressions - Properties of Objects.*

3. **Initial value:** Select an initial value for the global tag by selecting Uninitialized, True, or False. A global tag that is set to True is equal to 1. A global tag that is set to False is equal to 0.

4. Click OK. The Add New Global Tag dialog box closes and the new global tag is created. The script tag and initial value of the new global tag appear in the right pane of the Object Browser.

EDIT A GLOBAL TAG

NOTE: If you change the script tag for a global tag, any scripts that refer to the global tag will contain an error. To correct the error, update the scripts so they use the global tag's new script tag. Refer to *Scripts and Expressions* for more information.

1. Navigate the Object Browser to [project name] > Global Tags. In the right pane, double-click the global tag you want to change, or right-click the global tag and select Edit from the pop-up menu. The Edit Global Tag Properties dialog box opens.

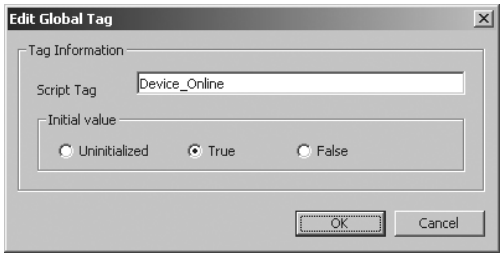


Figure 229. Edit Global Tag Dialog Box

2. Change properties of the global tag as desired. Refer to *Add a New Global Tag* for information on specific properties.

3. Click OK. The Edit Global Tag Properties dialog box closes.

DELETE A GLOBAL TAG

Deleting a global tag is irreversible. If you delete a global tag and then change your mind, you must add a new global tag. Also note that if you delete a global tag, any script that refers to the global tag will contain an error.

1. Navigate the Object Browser to [project name] > Global Tags. In the right pane, right-click the global tag you want to delete and select Delete from the pop-up menu. The Confirm dialog box opens.
2. If you are sure you want to delete the global tag, click Yes. The selected global tag is deleted and the Confirm dialog box closes. The deleted global tag disappears from the Object Browser.

Prompts

Prompts are custom dialog boxes used to elicit input from the operator or to inform the operator of something. When you create a prompt, you specify the text of the prompt and up to five buttons for the operator to click in response to the prompt text. If you want, you can define scripts for one or more of the buttons. You can also set a timer to automatically click one of the buttons if the operator does not respond within a certain amount of time.

You must configure at least one button. Only the buttons that are configured are displayed. They are displayed in order with the lowest numbered button at the left. The rightmost (highest-numbered) button has a dashed rectangle within it to indicate that the operator can select it by pressing Enter.

To use a prompt you have created, you must call it from a script using the PROMPT command. When the line of code containing the PROMPT command executes, the prompt displays in the window of the client running the script. For more information on the PROMPT command, refer to *Scripts and Expressions - Statements.*

ADD A NEW PROMPT

1. Navigate the Object Browser to [project name] > Prompts. Double-click <Add New Prompt> in the right pane, or right-click Prompts in the left pane and select Add New from the pop-up menu. The Add New Prompt dialog box opens.

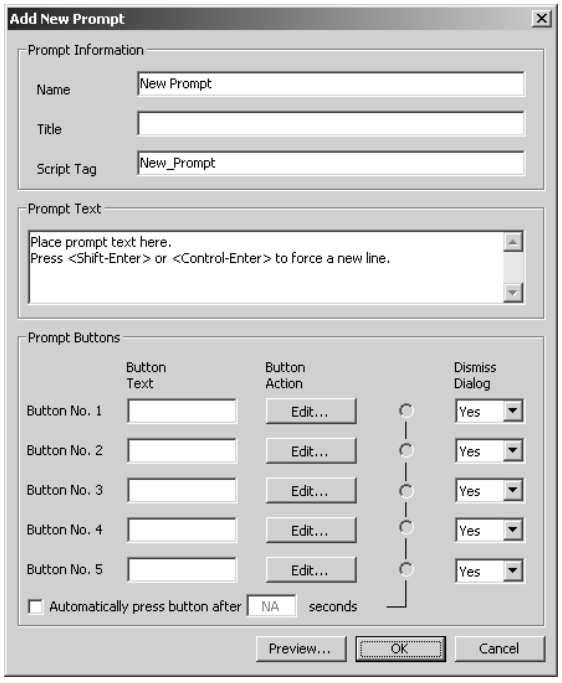


Figure 230. Add New Prompt Dialog Box

2. **Name:** Type a unique, descriptive name for the prompt you want to create. Prompt names are at most 50 characters long and can include any letter, digit or special character, with the exception of single and double quotation marks. Prompt names are not case sensitive. A tag resembling the name appears in the Script Tag box. If the name contains special characters, they are omitted from the tag. Spaces are replaced with underscores. Leading digits are removed.

3. **Title:** Type a title for the prompt dialog box. The title appears in the title bar at the top of the dialog box when the prompt is displayed on the VMX300(-E) client. Prompt titles are at most 50 characters long and can include any letter, digit or special character, with the exception of single and double quotation marks.

4. **Script tag:** If you do not want to use the script tag provided by the server, type in a unique, meaningful tag. Script tags are at most 50 characters long. They can include any letter, digit or the underscore character, but cannot begin with a digit. They cannot contain spaces or special characters. Tags are not case sensitive. Use the script tag to refer to the prompt in scripts. “Prompt” is not a valid script tag.

5. **Prompt text:** Type the text of the prompt. Prompt text can include any letter, digit or special character, with the exception of single and double quotation marks. Press Shift-Enter or Ctrl-Enter to go to a new line, or let the text wrap automatically. The text appears in the main part of the dialog box when the prompt is displayed on the VMX300(-E) client. It is often phrased as a question, with possible answers to the question appearing on the buttons the operator clicks in response. Make sure the prompt text is informative enough that the operator will know how to respond.

6. **Button text:** Type the text to display on the button. The text should reflect the action the button invokes when it is clicked. If you phrased the prompt text as a question, phrase the button text as an answer to the question. Button text is at most 10 characters and can include any letter, digit or special character, with the exception of single and double quotation marks. You must configure at least one button.

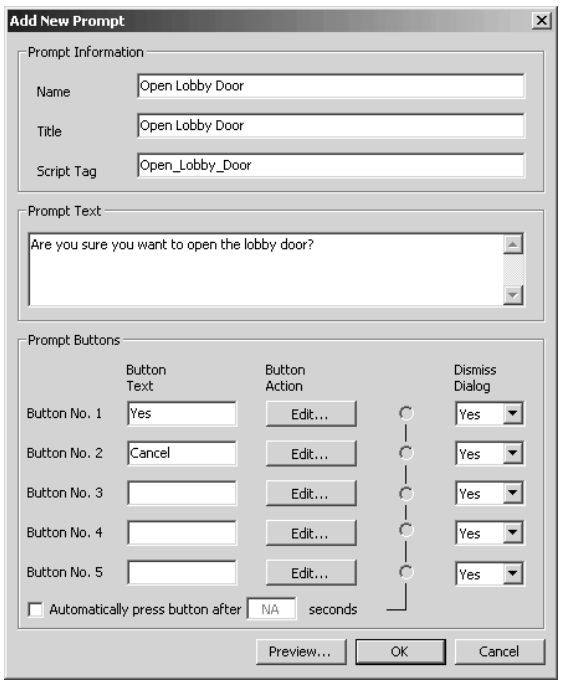


Figure 231. Example of a Prompt

7. **Button action:** Click Edit to open the Edit Script dialog box and define a script to run when the button is pressed. The script is required for any button that does not dismiss the dialog box. It is optional for buttons that dismiss the dialog box. Type the script actions directly into the Action column, or use the script wizard to help you write the script. For more information on writing scripts, refer to *Scripts and Expressions.*

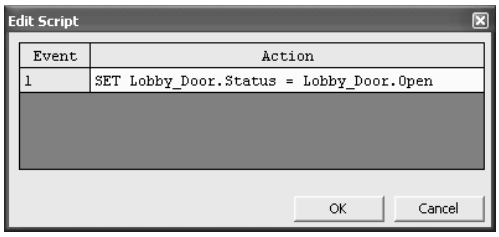


Figure 232. Edit Script Dialog Box

8. **Dismiss dialog:** Select Yes from the Dismiss Dialog drop-down list if you want the prompt dialog box to close after the operator has responded. If you want the dialog box to remain open after the operator has responded, select No. You must define a button action for any button that does not dismiss the dialog box.

9. Repeat steps 6 - 8 for each button you want to define.

10. **Prompt timeout:** In the event that the operator does not respond within a certain time, you can elect to have the prompt automatically click a button of your choice. To set the prompt to time out, select Automatically press button after. In the seconds box, type the number of seconds you want to elapse before timeout. Select the radio button for the button you want clicked when the prompt times out. The button you select as the timeout button must dismiss the dialog box or have an action associated with it, or both.

11. **Preview:** To see what the dialog box you have defined looks like, click Preview. The dialog box opens. To close the dialog box, click one of its buttons.

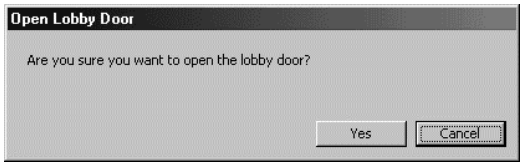


Figure 233. Preview of Dialog Box

12. Click OK. The Add New Prompt dialog box closes and the new prompt is created. The name and script tag of the new prompt appear in the right pane of the Object Browser.

NOTE: When you edit a prompt's script, make it available in its updated form by saving the server configuration before attempting to run the script.

EDIT A PROMPT

NOTE: If you change the script tag for a prompt, any script that refers to the prompt will contain an error. To correct the error, update the scripts so they use the prompt's new script tag. Refer to *Scripts and Expressions* for more information.

1. Navigate the Object Browser to [project name] > Prompts. In the right pane, double-click the prompt you want to change, or right-click the prompt and select Edit from the pop-up menu. The Edit Prompt Properties dialog box opens.

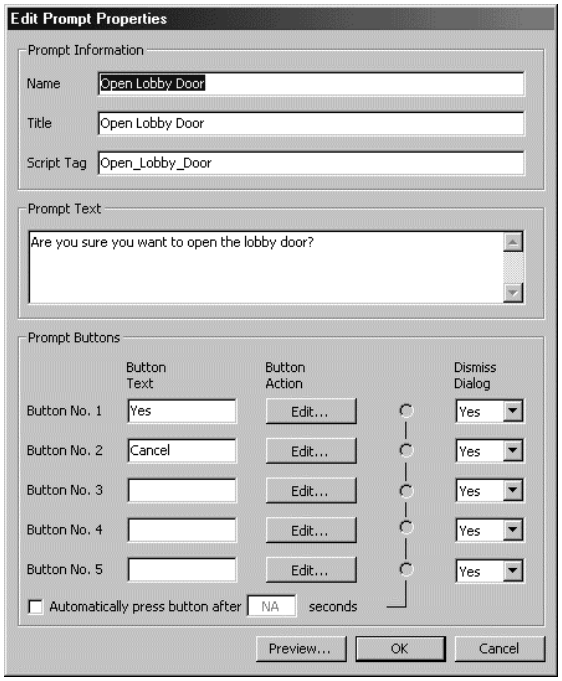


Figure 234. Edit Prompt Properties Dialog Box

2. Change properties of the prompt as desired. Refer to *Add a New Prompt* for information on specific properties.

3. Click OK. The Edit Prompt Properties dialog box closes.

NOTE: If you edit a script associated with a prompt button, make it available in its updated form by saving the server configuration before attempting to run the script.

DELETE A PROMPT

Deleting a prompt is irreversible. If you delete a prompt and then change your mind, you must add a new prompt. Also note that if you delete a prompt, any script that refers to it will contain an error.

1. Navigate the Object Browser to [project name] > Prompts. In the right pane, right-click the prompt you want to delete and select Delete from the pop-up menu. The Confirm dialog box opens.
2. If you are sure you want to delete the prompt, click Yes. The selected prompt is deleted and the Confirm dialog box closes. The deleted prompt disappears from the Object Browser.

Timers

Timers are used to delay an action by a predetermined length of time. Timers themselves cannot run scripts, but you can use a timer to trigger a script to run.

Expression: Every timer has an expression associated with it. Whenever something happens that could affect the value of the expression, the expression is evaluated. If the expression becomes true as a result of the event, the timer starts counting down. If the expression becomes false as a result of the event, the timer is reset to its delay value. If the value of the expression does not change as a result of the event, the timer is unaffected.

Property: Timers have one property, Value, that can be used in scripts and expressions. The Value property can be True or False (1 or 0). It becomes true when the timer reaches zero. It is reset to false when the timer is reset to its delay value.

States: Timers have three states:

1. **Reset:** The timer is set to its delay value.
2. **Countdown:** The timer is counting down from its delay value.
3. **Expired:** The timer has finished counting down to zero.

Reset: In the timer's reset state, the expression is false and the timer is set to its delay value. In this state, the Value property is false.

Countdown: When something happens that could affect the value of the timer's expression, the server evaluates the expression. If the expression becomes true as a result of the event, the timer is started. The Value property remains false. This is the countdown state. If an event occurs while the timer is counting down which makes the expression false, the timer is reset to its delay value.

Expired: If the timer counts all the way down to zero, the Value property becomes true. This is the expired state. The timer remains in the expired state until another event occurs which makes the expression false.

Table AP summarizes how the Value property is affected by the expression and timer values.

Table AP. Timer Property and Value

STATE	EXPRESSION	TIMER	VALUE PROPERTY
Reset	0	delay value	0
Countdown	1	0 < timer < delay value	0
Expired	1	0	1

Use the Value property to trigger other actions. For example, you might define an alarm that alerts an operator when communications with a camera have been lost for 10 seconds. The timer's expression is:

```
Camera1.CommLoss = True
```

The alarm's expression is:

```
CommLossDelayTimer.Value = True
```

When Camera1 loses communications, the timer's expression becomes true and the timer starts to count down from 10. When the timer reaches zero, the timer's Value property becomes true, which makes the alarm's expression true, triggering the alarm.

ADD A NEW TIMER

1. Navigate the Object Browser to [project name] > Timers. Double-click <Add New Timer> in the right pane, or right-click Timers in the left pane and select Add New from the pop-up menu. The Add New Timer dialog box opens.

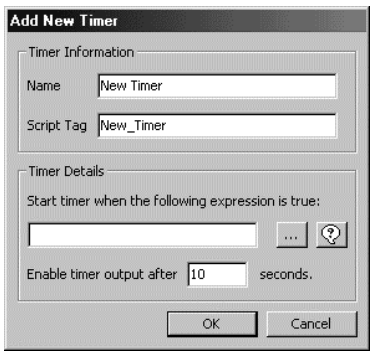


Figure 235. Add New Timer Dialog Box

2. **Name:** Type a unique name for the timer you want to add. Timer names are at most 50 characters long and can include any letter, digit or special character, with the exception of single and double quotation marks. Timer names are not case sensitive. A tag resembling the timer name appears in the Script Tag box. If the timer name contains special characters, they are omitted from the tag. Spaces are replaced with underscores. Leading digits are removed.

3. **Script tag:** If you do not want to use the script tag provided by the server, type a unique, meaningful tag. Script tags are, at most, 50 characters long. They can include any letter, digit or the underscore character, but cannot begin with a digit. They cannot contain spaces or special characters. Tags are not case sensitive. Use the script tag to refer to the timer in scripts and expressions. For a list of timer properties that can be scripted, refer to *Scripts and Expressions - Properties of Objects*.

4. **Expression:** Type the expression that will start the timer when it becomes true and reset the timer when it becomes false. If the expression is too long for the box, open the expression editor by clicking the expression editor button ... . This provides you with a larger window to work in.

   Or you can use the expression wizard to create the timer expression by clicking the Wizard button .

   Refer to *Scripts and Expressions* for information on the syntax of expressions.

5. **Delay value:** In the "Enable timer output after _ seconds box," type in the number of seconds for the timer to count down. The delay value must be between 0.1 of a second and 86,400 seconds (24 hours).

6. Click OK. The Add New Timer dialog box closes and the new timer is created. The name of the new timer appears in the Object Browser.

EDIT A TIMER

NOTE: If you change the script tag for a timer, any script that refers to the timer will contain an error. To correct the error, update the scripts so they use the timer's new script tag. Refer to *Scripts and Expressions* for more information.

1. Navigate the Object Browser to [project name] > Timers. In the right pane, double-click the timer you want to change, or right-click the timer and select Edit from the pop-up menu. The Edit Timer Properties dialog box opens.

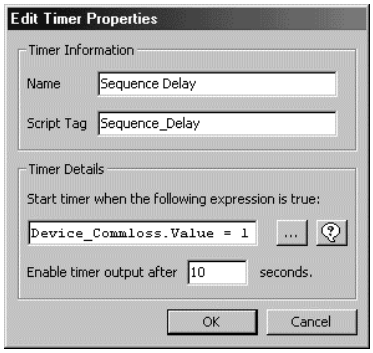


Figure 236. Edit Timer Properties Dialog Box

2. Change properties of the timer as desired. Refer to *Add a New Timer* for information on specific properties.
3. Click OK. The Edit Timer Properties dialog box closes.

DELETE A TIMER

Deleting a timer is irreversible. If you delete a timer and then change your mind, you must add a new timer. Also note that if you delete a timer, any script that refers to it will contain an error.

1. Navigate the Object Browser to [project name] > Timers. In the right pane, right-click the timer you want to delete and select Delete from the pop-up menu. The Confirm dialog box opens.
2. If you are sure you want to delete the timer, click Yes. The selected timer is deleted and the Confirm dialog box closes. The name of the deleted timer disappears from the Object Browser.

Schedules

Schedules allow you to define scripts that execute at a scheduled time. If you want, you can specify a recipient group to be notified when the scheduled action executes. Refer to *Recipient Groups* for instructions on creating a recipient group.

ADD A NEW SCHEDULE

1. Navigate the Object Browser to [project name] > Schedules. Double-click <Add New Schedule> in the right pane, or right-click Schedules in the left pane and select Add New from the pop-up menu. The Add New Schedule dialog box opens.

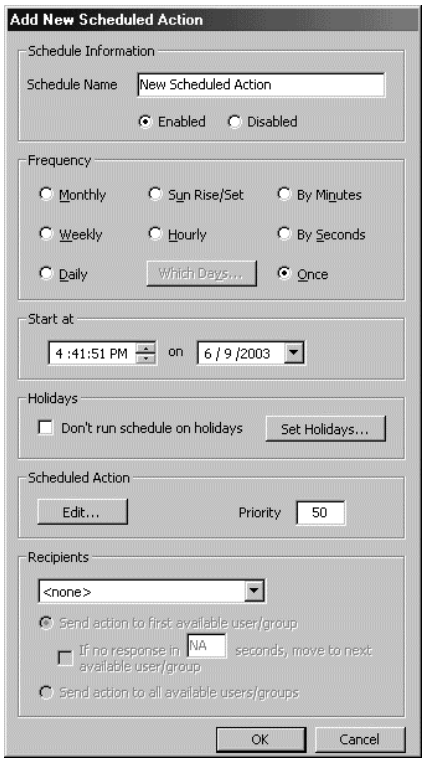


Figure 237. Add New Schedule Dialog Box

2. **Schedule name:** Type a unique, descriptive name for the schedule you want to create. Schedule names are, at most, 50 characters long and can include any letter, digit or special character, with the exception of single and double quotation marks. Schedule names are not case sensitive.

3. **Enabled/disabled:** If you want the action to execute as scheduled, click Enable. If you want to prevent the scheduled action from executing, click Disable. This gives you a quick way to suspend a schedule temporarily without having to delete the schedule and re-create it later.

4. **Frequency and start time:** To select the frequency with which you want the scheduled action to execute, click the appropriate radio button:

    a. **Monthly:** Click Monthly to have the scheduled action execute once a month. In the Start At area, specify the day of the month and time of day for the action to execute. To set the time, select the hour, minutes, or seconds and click the up and down arrows. To execute the action on the last day of every month, regardless of how many days there are in the month, select 31 as the day.

    b. **Weekly:** To have the scheduled action execute once a week, click Weekly. In the Start At area, specify the day of the week and time of day for the action to execute. To set the time, select the hour, minutes, or seconds and click the up and down arrows. Select a day of the week from the drop-down list.

c. **Daily:** To have the scheduled action execute certain days of the week, click Daily. Click Which Days to specify which days of the week you want the action to execute. The Daily Schedule dialog box opens.

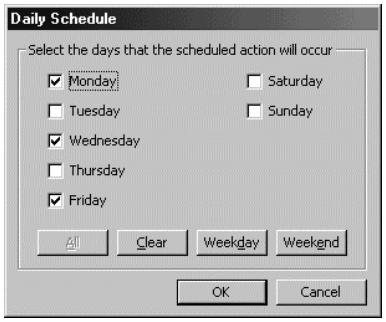


Figure 238. Daily Schedule Dialog Box

Select days individually or use the buttons to select and deselect multiple days at once. All selects all seven days of the week. Clear clears all seven days of the week. Weekday selects Monday through Friday only. Weekend selects Saturday and Sunday only. Once you have selected the days, click OK to close the Daily Schedule dialog box.

In the Start At area, specify the time of day for the action to execute. To set the time, select the hour, minutes, or seconds and click the up and down arrows.

d. **Sunrise or sunset:** To have the scheduled action execute once a day at sunrise or sunset, click Sun Rise/Set. Click Setup to specify geographic location and other information the server needs to calculate when to execute the action. The Sunrise/Sunset Setup dialog box opens.

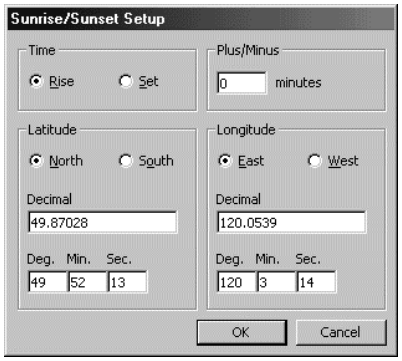


Figure 239. Sunrise/Sunset Dialog Box

In the Time area, click Rise if you want the action to execute at sunrise, or Set if you want it to execute at sunset. If you want to execute an action at both sunrise and sunset, you must create two different schedules.

In the Plus/Minus area, type in the number of minutes before or after sunrise/sunset that you want the action to execute. For example, if you want the action to execute a half hour before sunrise, select Rise in the Time area and type in -30 in the Plus/Minus area.

In the Latitude area, select North or South, and type in the latitude of the relevant location. For example, if the scheduled action is to control a camera every day at dusk, use the latitude of the camera, not of the server. You can either enter the latitude in decimal notation in the Decimal box, or in degrees, minutes and seconds in the Deg, Min and Sec boxes. As you type in the latitude, the server will automatically convert it to the other notation.

In the Longitude area, select East or West, and type in the longitude of the relevant location. Like the latitude, you can enter longitude either in decimal notation, or in degrees, seconds and minutes. Click OK to close the Sunrise/Sunset Setup dialog box.

e. **Hourly:** To have the scheduled action execute once an hour, click Hourly. In the Start At area, type in the number of minutes after the hour you want the action to execute. Fractional amounts will automatically be rounded.

f. **By minutes:** If you want the scheduled action to execute every few minutes, click By Minutes. In the Every area, type in the number of minutes you want to elapse before the action next executes, up to a maximum of 59 minutes. Fractional amounts will automatically be rounded.

g. **By seconds:** If you want the scheduled action to execute every few seconds, click By Seconds. In the Every area, type in the number of seconds you want to elapse before the action next executes, up to a maximum of 59 seconds. Fractional amounts will automatically be rounded.

h. **Once:** If you want the scheduled action to execute once only on a predetermined day at a predetermined time, click Once. Type the date in directly, or select it from the drop-down calendar. Use the left and right arrows to select the month in the drop-down calendar, then select a date by clicking it. Today's date is circled in red.

Specify the time of day for the action to execute. To set the time, select the hour, minutes, or seconds and click the up and down arrows.

A schedule that is set to execute once is automatically deleted from the server configuration once it has executed. To save a copy of the schedule, make a copy of it before it executes using Copy and Paste. Refer to *Pop-Up Menus* in the *Appendix* for information on making copies of objects.

5. **Holidays:** If you want prevent the scheduled action from executing on certain days of the year, click "Don't run schedule on holidays." Click Set holidays to specify the days you do not want the action to execute. The Edit Holidays dialog box opens.

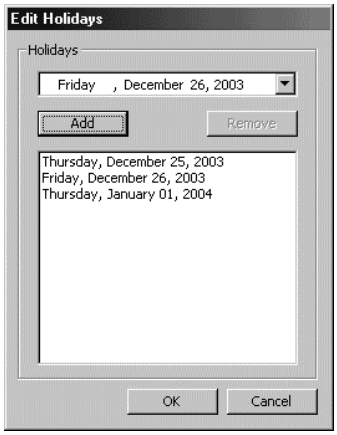


Figure 240. Edit Holidays Dialog Box

Click the down-arrow to the right of the date to open the drop-down calendar. Use the left and right arrows to select the month in the drop-down calendar, then select a date by clicking it. Today's date is circled in red. Click Add to add the date in the date box to the list of holidays. To remove a date from the list, select the date and click Remove. Click OK once you have specified all the days you want to prevent the action from executing.

6. **Scheduled action:** Click Edit to define the scheduled action. The Edit Script dialog box opens. Type the script actions directly into the Action column, or use the script wizard to help you write the script. For more information on writing scripts, refer to *Scripts and Expressions.*

A schedule's script runs on the client of any operator specified in the schedule's recipient group, provided the client is running and the operator is logged in when the script executes. If the client is not running or the operator is not logged in, or if no recipients are specified in the schedule, VMX300(-E) runs as much of the script as possible, namely, statements that do not require a recipient, such as a statement that sets the value of a device property.

7. **Priority:** Enter the priority with which the schedule's activities are to be treated by the server. VMX300(-E) uses priorities to resolve situations in which two or more objects attempt to control a particular device at the same time. The object with the higher priority number is given control of the device. The highest priority you can assign to an object is 99. The lowest is 1. System events have priority 100. Users, schedules, and alarms and events all have a priority. The scripts associated with these objects inherit the object's priority.

8. **Recipients:** Select the recipient group you want notified when the scheduled action executes. Recipients are only notified if they are logged in to the client when the scheduled action executes.

Specifying recipients also determines which clients the schedule's script runs on. A schedule's script runs on the client of any operator specified in the schedule's recipient group, provided the client is running and the operator is logged in when the script executes. If the client is not running or the operator is not logged in, or if no recipients are specified in the schedule, VMX300(-E) runs as much of the script as possible, namely, statements that do not require a recipient, such as a statement that sets the value of a device property.

a. **Recipient group:** Select the recipient group from the drop-down list. If you have not created the recipient group yet, finish adding the new schedule, create the recipient group, then edit the schedule to assign the recipient group. Refer to *Recipient Groups* for information on creating recipient groups.

   To send notification simultaneously to every operator configured on that server who is logged in, select the predefined recipient group All Users. Select <none> if you do not want anyone to be notified.

b. **Send action to first:** If you want notification sent to the member at the top of the recipient group's Members list, select "Send action to first available user/group." When the scheduled action executes, the server will scan down the list until it finds a member who is logged in, and send notification to that member. If the recipient is a user group, notification is sent to all members of the group who are logged in.

c. **If no response:** If you want the server to notify one recipient after another until someone responds to the scheduled action, select "If no response in _ seconds, move to next available user/group" and type in the number of seconds you want to elapse before notifying the next recipient.

   To use this option, the scheduled action must call a prompt using the PROMPT command. A recipient responds to the scheduled action by responding to the prompt. When the scheduled action executes, the prompt displays on the first recipient's workstation for the specified duration, then is removed from the first recipient's workstation and displayed on the second recipient's workstation for the specified duration, and so on, until either an operator has responded or the list of recipients has been exhausted. If the list has been exhausted, the prompt is then simultaneously redisplayed on every recipient's workstation, where it remains until someone has responded.

d. **Send action to all:** If you want to send notification simultaneously to every member of the recipient group who is logged in when the scheduled action executes, select "Send action to all available user/groups." In this case, the order of the members in the recipient group's Members list is irrelevant.

9. Click OK. The Add New Schedule dialog box closes and the new schedule is created. The name of the new schedule appears in the right pane of the Object Browser.

NOTE: When you edit a schedule's script, make it available in its updated form by saving the server configuration before attempting to run the script.

EDIT A SCHEDULE

1. Navigate the Object Browser to [project name] > Schedules. In the right pane, double-click the schedule you want to change, or right-click the schedule and select Edit from the pop-up menu. The Edit Scheduled Action Properties dialog box opens.

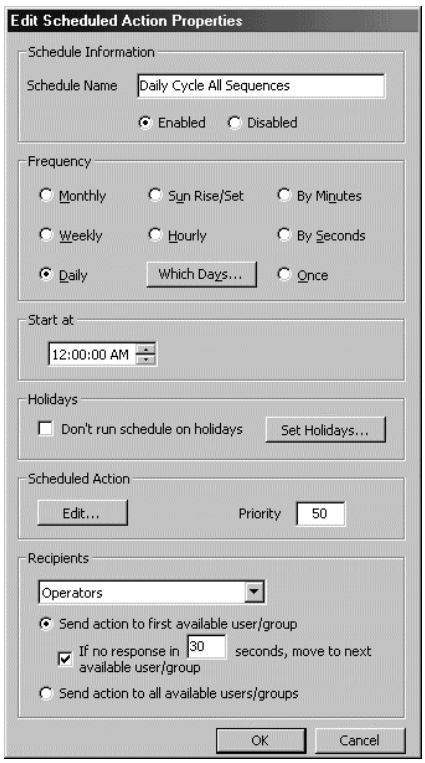


Figure 241. Edit Scheduled Action Dialog Box

2. Change properties of the schedule as desired. Refer to *Add a New Schedule* for information on specific properties.

3. Click OK. The Edit Scheduled Action Properties dialog box closes.

NOTE: If you edit the action associated with a schedule, make it available in its updated form by saving the server configuration.

DELETE A SCHEDULE

Deleting a schedule is irreversible. If you delete a schedule and then change your mind, you must add a new schedule.

1. Navigate the Object Browser to [project name] > Schedules. In the right pane, right-click the schedule you want to delete and select Delete from the pop-up menu. The Confirm dialog box opens.

2. If you are sure you want to delete the schedule, click Yes. The selected schedule is deleted and the Confirm dialog box closes. The deleted schedule disappears from the Object Browser.

Alarms and Events

TIP: Refer to *Alarms and Events* and *Session Manager* in the VMX300(-E) Client Operation Manual for additional information on how alarms and events behave in the client.

Alarms and events are actions that are executed when specific conditions occur within the system. As system administrator, you define the condition that triggers an alarm or event. You also define the scripts that run under the following conditions:

- When the alarm is triggered
- When an operator replays the alarm or event
- When the alarm or event is acknowledged

Categories: Alarms and events are organized into categories that have certain settings in common, including the following:

- The operators notified
- The sound they make
- Whether they require acknowledgement
- Whether they are archived

These settings apply to all the alarms or events in the category, without exception.

Predefined categories: For convenience, the VMX300(-E) server has three predefined categories:

- Alarms
- Events
- Normal

Alarms are intended for exceptional occurrences. By default, alarms require acknowledgement and appear in the Session Manager in red. The Events and Normal categories are intended for routine occurrences. By default, these categories appear in the Session Manager in blue and do not require acknowledgement.

You do not need to use the predefined categories. You can create your own categories as needed, or adapt the predefined ones by changing the settings. The name and type of predefined categories cannot be changed, but all other options can.

Property: Alarms and events have one Boolean property that you can use in scripts and expressions: Value. Value is false when the alarm/event's expression is false, and true when the expression is true.

HOW ALARMS AND EVENTS WORK

WHEN AN ALARM OR EVENT IS TRIGGERED

Whenever something happens that could affect the value of an alarm/event expression, the expression is evaluated. If the expression becomes true as a result of what happened, the first of the alarm/event's scripts runs and recipients are notified. Specifically, the following events occur:

- On the workstation of an alarm/event recipient, the alarm/event icon becomes animated (the bell hammer strikes the bell) and changes color to the alarm/event category's Color. The animation continues as long as the expression remains true; the color changes back to the default when the alarm or event is acknowledged or becomes complete.
- The alarm or event's On Event script runs.
- On the workstation of all alarm/event recipients, an entry recording the alarm or event appears in the Session Manager. The entry displays in the alarm/event category's Color.
- If there is no active entry highlighted in the Session Manager of a particular recipient when the alarm or event is triggered, the entry for the new alarm or event is automatically highlighted and the On Operator Replay script runs. If acknowledgement is required, Acknowledge or Acknowledge with Comment becomes available on the Session Manager tool bar and in the alarm icon pop-up menu. The entry for the new alarm or event will not be highlighted if the recipient already has a highlighted entry in the Session Manager when the alarm or event is triggered. This ensures that the operator's current activity is not interrupted.
- If Sound is selected in the alarm/event category, the sound plays on the workstations of alarm/event recipients. If the category has "Play sound continuously" selected, the sound continues to play until the operator turns it off by clicking the Silence Alarm button in the Session Manager.
- If the alarm/event category has "Archive events of this category" selected, the entry is committed to the archives.

When the expression that triggers an alarm or event becomes false, the icon animation stops (the bell hammer stops striking the bell).

If an alarm or event is triggered more than once in quick succession, a new entry appears in the recipient's Session Manager each time the alarm or event is triggered. If the alarm or event has a sound, the sound will play each time the alarm or event is triggered, unless you have selected "Silence subsequent events."

OPERATOR REPLAYS

The On Operator Replay script runs automatically on the workstation of any recipient who does not already have a Session Manager entry highlighted when the alarm or event is triggered. If a recipient already has a highlighted entry in the Session Manager when the alarm or event is triggered, the new alarm/event entry will not be highlighted. This ensures that the operator's current activity is not interrupted.

The On Operator Replay script can also be run on demand by a recipient. To run the On Operator Replay script, the recipient selects the entry in the Session Manager. An alarm or event can be replayed no matter what its status.

When an operator replays an alarm or event, the following occurs:

- The On Operator Replay script runs.
- On the workstation of the operator who replayed the alarm or event, an entry recording the replay appears in the Session Manager. The entry displays in the alarm/event category's Color.

Operator replays do not do the following:

- Change the icon color
- Change the icon animation
- Play the alarm sound
- Require acknowledgement
- Affect the workstation of any operator except the operator who replayed the script

ACKNOWLEDGEMENT

If "Requires acknowledgement" is selected for the alarm/event category, the entry will remain active until the alarm or event has been acknowledged, either by an operator or by automatic acknowledgement. If more than one operator is notified of an alarm or event, only one operator needs to acknowledge it.

To acknowledge an alarm or event, an operator must do one of the following:

- Highlight the alarm entry in the Session Manager and click the Acknowledge or Acknowledge with Comment button on the Session Manager tool bar.
- Right-click the alarm/event icon and select Acknowledge or Acknowledge with Comment from the pop-up menu. If the alarm or event has been triggered more than once in quick succession, creating multiple entries into the Session Manager, this acknowledges every instance.
- If the alarm or event does not require a comment, click the Acknowledge All button on the Session Manager tool bar, which acknowledges all alarms and events that do not require a comment.

When an alarm or event is acknowledged, the following occurs:

- The entry in the Session Manager and the alarm/event icon change back to the category's Default Color.
- If an On Acknowledge script is associated with the alarm or event, it runs.

Once an alarm or event has been acknowledged and its scripts have finished executing, the status of the entry in the Session Manger is set to Complete. Any entry that does not have status Complete is considered to be active. When an alarm or event becomes complete, the following occurs:

- If the alarm or event did not require acknowledgement, the entry in the Session Manager and the alarm/event icon change back to the category's Default Color.
- The entry for the complete alarm or event is moved from the Active list to the Complete list.
- The entry for the complete alarm or event is no longer highlighted.
- The highest active entry in the Session Manager becomes highlighted. Which entry this is depends on how the Session Manager is sorted.

NOTES:

- There is a limit of 500 unacknowledged alarms and events per server. When the limit is exceeded, the server automatically acknowledges the oldest alarm or event, making it complete. If archiving is turned on, the archive will show that the alarm or event was automatically acknowledged by the server.
- There is a limit of 500 completed events in Session View of the Session Manager. When the limit is exceeded, the 500 oldest events are deleted from Session View.

ACCESS ALARMS AND EVENTS DEFINED ON ANOTHER SERVER

You can access alarms and events defined on another server using the remote server driver feature. Remote server drivers appear as device drivers in the Object Browser, and are added, edited, and deleted the same way device drivers are. There is a remote server driver for every server that is running. Refer to *Device Drivers* for instructions on adding a remote server driver.

Script tags for remote servers are made up of the remote server name that appears in the Object Browser appended with "_Server". Script tags for remote devices are made up of the device name that appears in the Object Browser under Sources appended with "_RS", for "Remote Server". Script tags for remote alarms and events appear in the Object Browser as read properties.

The remote server driver for a particular server provides a list of alarms and events defined on that server. Each alarm or event is presented as a read property of the remote server. The read property has value True when the remote alarm/event's expression is true. The read property has value False when the remote alarm/event's expression is false. The remote server driver does not provide you with access to the alarm/event definition. You cannot edit the alarm or event, nor can you delete it from the server it is defined on.

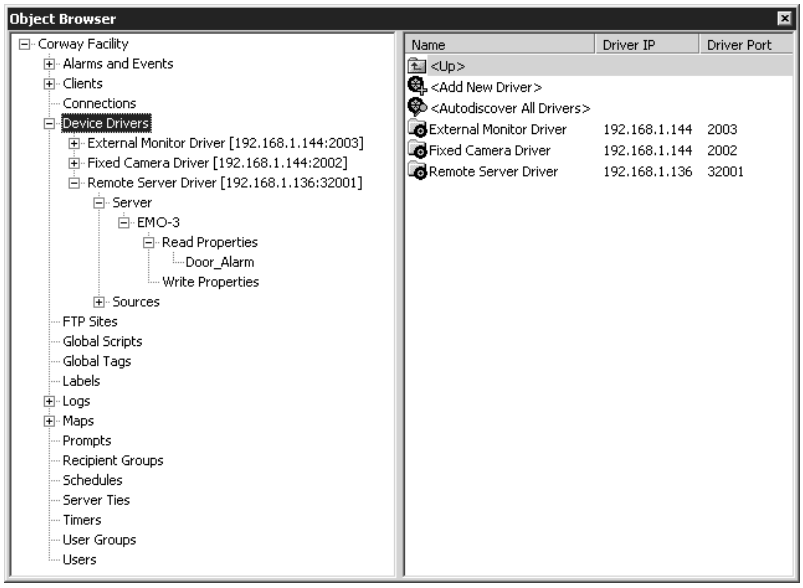


Figure 242. Accessing Alarms and Events on Another Server

To work with a remotely defined alarm or event, create an alarm or event on your server whose expression tests the remote server's read property.

For example, suppose you have added the remote server driver for a server called EMO-3. Suppose EMO-3 has an external door alarm that triggers an alarm, Door Alarm, that directs Camera1 at the door. On your server, create an alarm that loads live video from Camera1 into a custom window configured on your server, Window1, when the Door_Alarm read property becomes true. The expression for the alarm is:

EMO-3_Server.Door_Alarm = EMO-3_Server.True.

The alarm's On Event action is:

SET Window1.LiveSource = Camera1_RS.Output.

TIP: Use context-sensitive help or the script wizard to write scripts involving remote servers. VMX300(-E) will provide you with a pop-up list of script tags referring to remote servers and their alarms and events, in context. Refer to *Scripts and Expressions - Mechanics of Editing Scripts and Expressions* for more information.

ALARM/EVENT CATEGORIES

ADD A NEW ALARM/EVENT CATEGORY

1. Navigate the Object Browser to [project name] > Alarms and Events. Double-click <Add New Category> in the right pane, or right-click Alarms and Events in the left pane and select Add New from the pop-up menu. The Add New Category dialog box opens.

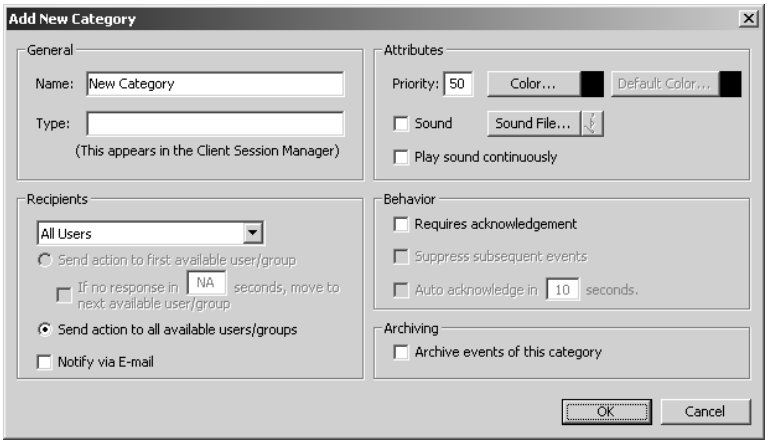


Figure 243. Add New Category Dialog Box

2. **Name:** Type a unique, descriptive name for the alarm/event category you want to create. Category names are at most 50 characters long and can include any letter, digit or special character, with the exception of single and double quotation marks. Category names are not case sensitive.

3. **Type:** Type a description of the type of category. The description appears in the right pane of the Object Browser beside the category name, and in the Session Manager entries for alarms and events in this category. The type is required.

4. **Recipients:** Select the recipient group you want notified when alarms and events in this category occur. Recipients are only notified if they are logged in to the client before the alarm/event status becomes Complete.

   Specifying recipients also determines which clients the alarm's scripts run on. An alarm's scripts run on the client of any operator specified in the category's recipient group, provided the client is running and the operator is logged in when the script executes. If the client is not running or the operator is not logged in, or if no recipients are specified in the category, VMX300(-E) runs as much of the scripts as possible, namely, statements that do not require a recipient, such as a statement that sets the value of a device property.

   a. **Recipient group:** Select the recipient group from the drop-down list. If you have not created the recipient group yet, finish adding the new category, create the recipient group, then edit the category to assign the recipient group. Refer to *Recipient Groups* for information on creating recipient groups.

      To send notification simultaneously to every operator configured on that server who is logged in, select the predefined recipient group All Users. Select <none> if you do not want anyone to be notified.

   b. **Send action to first:** If you want notification sent to the member at the top of the recipient group's Members list, select Send action to first available user/group. When an alarm or event in this category is triggered, the server will scan down the list until it finds a member who is logged in, and send notification to that member. If the recipient is a user group, notification is sent to all members of the group who are logged in.

   c. **If no response:** If you want the server to notify one recipient after another until someone responds to the alarm or event, select "If no response in _ seconds, move to next available user/group" and type the number of seconds you want to elapse before notifying the next recipient.

      A recipient responds to the alarm or event either by acknowledging it, if it requires acknowledgment, or by responding to a prompt that the script displays using the PROMPT command. If you define a prompt for the response, the prompt displays on the first recipient's workstation for the specified duration, then is removed from the first recipient's workstation and displayed on the second recipient's workstation for the specified duration, and so on, until either an operator has responded or the list of recipients has been exhausted. If the list has been exhausted, the prompt is then simultaneously redisplayed on every recipient's workstation, where it remains until someone has responded.

d. **Send action to all:** If you want to send notification simultaneously to every member of the recipient group who is logged in when an alarm or event in this category is triggered, select "Send action to all available user/groups." In this case, the order of the members in the recipient group's Members list is irrelevant.

e. **Notify via E-mail:** If you want recipients to be sent an e-mail message notifying them when an alarm or event in this category is triggered, click this field. E-mail notification is done in addition to the other methods of notification.

E-mail notification is sent to every member of the recipient group who has an e-mail address configured, regardless of whether the member is logged in when the alarm or event occurs. The e-mail message is broadcast simultaneously to all recipients, regardless of whether you have selected "Send action to first available user/group" or "Send action to all available user/groups." An alarm/event e-mail message includes the following information:

- The name of the server the alarm or event is defined on
- The alarm/event category
- The alarm/event type
- The date and time the alarm or event occurred

In addition to selecting "Notify via e-mail" for the alarm/event category, you must complete the following additional steps:

- Configure the e-mail server on the E-mail tab of the Project Properties dialog box. Refer to *Project Properties - E-mail Tab* for instructions.
- Configure an e-mail address for each recipient. If a user belongs to a recipient group for an alarm/event category that uses e-mail notification, but the user does not have an e-mail address configured, the user will not receive email notification. Refer to *Users* for instructions on configuring user accounts.

5. **Attributes:**

a. **Priority:** Assign a priority to the category if you want some or all of the alarms and events in the category to inherit their priority from the category. The category priority overrides the priority for a particular alarm or event only if "Use category priority" is selected for that alarm or event.

VMX300(-E) uses priorities to resolve situations in which two or more objects attempt to control a particular device at the same time. The object with the higher priority number is given control of the device. The highest priority you can assign to an object is 99. The lowest is 1. System events have priority 100. Users, schedules, and alarms and events all have a priority. The scripts associated with these objects inherit the object's priority.

b. **Color:** Select a color to signify that the alarm or event has been triggered. Alarm/event icons and Session Manager entries for alarms and events in this category display in the alarm color.

c. **Default color:** Select a color to signify that the alarm is not in an alarm state. Alarm/event icons and Session Manager entries for alarms and events in this category display in the default color once the alarm or event has been acknowledged, or, if it does not require acknowledgement, once it becomes complete. The icon for an alarm or event that has never been triggered displays in the default color.

d. **Sound:** If you want a sound to play on recipients' workstations when the alarm or event is triggered, select Sound.

e. **Sound file:** Click Sound File to select the file for the sound you want to play on a recipient's workstation when the alarm or event is triggered. VMX300(-E) supports one file format for sound files: .wav. Test the selected sound file by clicking the speaker button.

f. **Play sound continuously:** If you want the selected sound to play repeatedly, select "Play sound continuously." The sound plays until the operator stops it by clicking the Silence Alarm button on the Session Manager tool bar.

6. **Behavior:**

a. **Requires acknowledgement:** To require that a recipient acknowledge an alarm or event in this category, select "Requires acknowledgement." An alarm or event that requires acknowledgement will remain active in the Session Manager until it has been acknowledged, after which it has status Complete. If more than one user is notified of an alarm or event, only one user needs to acknowledge it for it to be considered complete.

b. **Suppress subsequent alarms:** Under some circumstances, an alarm or event can be triggered more than once in quick succession. For example, a door alarm could be set off several times in quick succession if someone opens and closes the door repeatedly. In this case, it is only meaningful to deal with a single instance of the alarm, since there is a single cause to the multiple occurrences of the alarm.

To limit the system's treatment of an alarm or event that is triggered multiple times in quick succession, select "Suppress subsequent alarms." The first time the alarm or event is triggered, an entry will appear in the Session Manager and the sound will play. No additional entries will appear nor sounds play until the alarm or event has been acknowledged. The next time the alarm or event is triggered, a new entry will appear and the sound will play.

You can only suppress subsequent alarms for alarms and events that require acknowledgement.

c. **Auto-acknowledge:** If you want the server to automatically acknowledge alarms and events in this category, select "Auto-acknowledge in _ seconds" and type in the number of seconds you want to elapse before acknowledgement. When an alarm or event is auto acknowledged, the On Acknowledge script runs. Having "auto acknowledge" selected does not preclude a recipient from manually acknowledging an alarm or event.

7. **Archiving:** If you want to keep a permanent record of alarms and events in this category, click "Archive events of this category." Alarms and events are archived in database files. For an alarm or event to be archived, an archive server must be configured and running. Refer to *Archive Servers* for more information.

8. Click OK. The new category is created and the Add New Category dialog box closes. The new category appears in the Object Browser.

EDIT AN ALARM/EVENT CATEGORY

To change the properties of an existing alarm/event category:

1. Navigate the Object Browser to [project name] > Alarms and Events. In either pane, right-click the alarm/event category you want to edit and select Edit from the pop-up menu. The Edit Category dialog box opens.

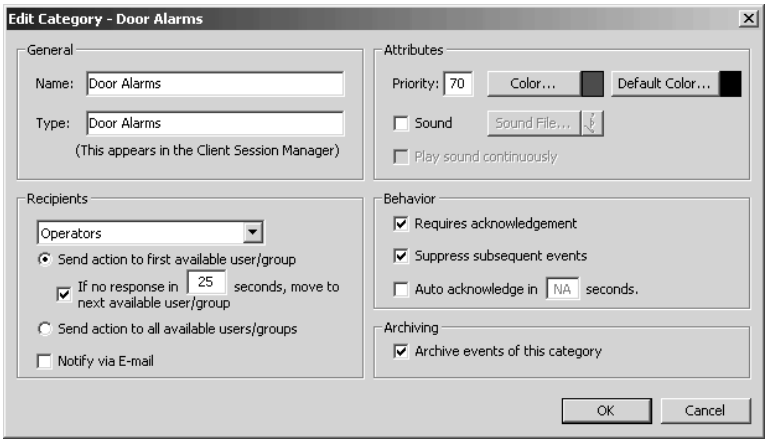


Figure 244. Edit Category Dialog Box

2. Change properties of the category as desired. Refer to *Add a New Alarm/Event Category* for information on specific properties.

3. Click OK. The Edit Category dialog box closes.

DELETE AN ALARM/EVENT CATEGORY

NOTES:

- Deleting an alarm/event category deletes all the alarms and events that belong to the category and removes their icons from maps. This introduces an error into scripts that refer to one of the deleted alarms or events.
- Deleting an alarm/event category is irreversible. If you delete an alarm/event category and then change your mind, you must re-create it as described in *Add a New Alarm/Event Category*, and re-create the alarms and events as described in *Alarms, Events, and Normal Occurrences - Add a New Alarm or Event*.

1. Navigate the Object Browser to [project name] > Alarms and Events. In either pane, right-click the category you want to delete and select Delete from the pop-up menu. The Confirm dialog box opens.

2. If you are sure you want to delete the alarm/event category, click Yes.The selected category is deleted and the Confirm dialog box closes.

NOTE: You cannot delete the predefined alarm/event categories.

ALARMS, EVENTS, AND NORMAL OCCURRENCES

ADD A NEW ALARM OR EVENT

1. Navigate the Object Browser to [project name] > Alarms and Events > [alarm/event category]. Double-click <Add New Alarm or Event> in the right pane, or right-click the desired alarm/event category in the left pane and select Add New from the pop-up menu. The Add New Alarm or Event dialog box opens.

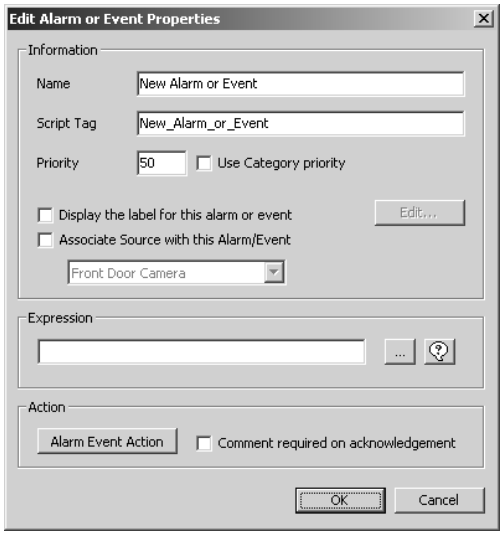


Figure 245. Add New Alarm or Event Dialog Box

2. **Name:** Type a unique, descriptive name for the alarm or event you want to create. Alarm/event names are at most 50 characters long and can include any letter, digit or special character, with the exception of single and double quotation marks. Alarm/event names are not case sensitive. The name is used as the description in the Session Manager. A tag resembling the name appears in the Script Tag box. If the name contains special characters, they are omitted from the tag. Spaces are replaced with underscores. Leading digits are removed.

3. **Script tag:** If you do not want to use the script tag provided by the server, type in a unique, meaningful tag. Script tags are at most 50 characters long. They can include any letter, digit or the underscore character, but cannot begin with a digit. They cannot contain spaces or special characters. Tags are not case sensitive. Use the script tag to refer to the alarm or event in scripts and expressions. For a list of alarm/event properties that can be scripted, refer to *Scripts and Expressions - Properties of Objects*.

4. **Priority:** Enter the priority with which the alarm or event's activities are to be treated by the server in the Priority box, or select Use category priority to inherit the category's priority. Refer to *Alarm/Event Categories - Add a New Alarm/Event Category* for instructions on setting the category's priority.

   VMX300(-E) uses priorities to resolve situations in which two or more objects attempt to control a particular device at the same time. The object with the higher priority number is given control of the device. The highest priority you can assign to an object is 99. The lowest is 1. System events have priority 100. Users, schedules, and alarms and events all have a priority. The scripts associated with these objects inherit the object's priority.

5. **Alarm/event label:** If you are going to place alarm/event icons on maps and you want the icons labeled, select "Display the label for this alarm or event." To edit the text and formatting of the label, click Edit. The Edit Label Properties dialog box opens.

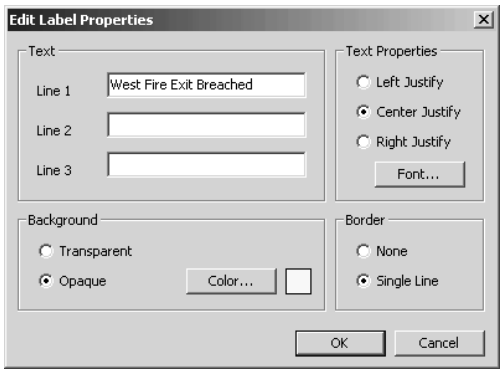


Figure 246. Edit Label Properties Dialog Box

a. **Text:** Type up to three lines of text as the label contents. When you place the alarm/event icon on a map, this text will display in the label. Each line of text can be at most 50 characters long and can include any letter, digit or special character, with the exception of single and double quotation marks.

b. **Text properties:** Select the justification you want for the label's text. All the lines of text will be justified the same. Click Font to select the font for the label's text, as well as display attributes like point size, bold face, and italics.

c. **Background:** Select the background you want for the label you are creating. A transparent background allows the underlying map to show through. An opaque background makes the label appear as a colored rectangle. Click Select Color to choose the background color for an opaque label.

d. **Border:** Specify whether you want the label to have a border around it by selecting None or Single Line.

e. Click OK. The Edit Label Properties dialog box closes.

6. **Source association:** The source association feature of the DX9000 DVR allows an operator to automatically retrieve archived video associated with an alarm or event, without having to know which camera to load and without having to cue the video.

   For example, suppose Front Door Camera is connected to a DX9000 DVR. You might associate Front Door Camera with an alarm that is triggered when the front door is breached. Suppose the door alarm was triggered some time during the night and an operator wants to review the video associated with the alarm. To do this, the operator locates the alarm in the Session Manager and drags it to a custom window that has an appropriate DVR canvas. This loads the archived video from Front Door Camera into the window. The video automatically starts playing, cued to the time of the alarm.

   For more information on how an operator retrieves archived video using source association, refer to the VMX300(-E) Client Operation Manual.

   Associating a source device with an alarm or event is a simple matter of editing the alarm or event and selecting the source device from a drop-down box. In addition to defining the association itself, you must complete the following steps:

   a. Synchronize the DX9000 DVR and VMX300(-E) server clocks using a time server. This ensures the time stamp on the archived video is identical to the time stamp on the archived alarm or event.

      Either synchronize the DVR to the VMX300(-E) server, or synchronize the VMX300(-E) server to the DVR. To synchronize the DVR to the VMX300(-E) server, configure the VMX300(-E) server by selecting Allow this server to act as a Network Time Server on the Date/Time tab of the Project Properties dialog box. Refer to *Project Properties* for more information. Configure the DX9000 DVR using the software provided with the DVR by setting the DVR to synchronize to the VMX300(-E) server. Refer to the appropriate DVR installation/operation manual for information on DVR-internal settings.

      To synchronize the VMX300(-E) server to the DVR, configure the VMX300(-E) server by entering the IP address or hostname of the DX9000 DVR in the Network Time Servers list on the Date/Time tab of the Project Properties dialog box. Refer to *Project Properties* for more information.

      If you have more than one DX9000 DVR, synchronize each one to a particular DVR, then synchronize that DVR with the VMX300(-E) server.

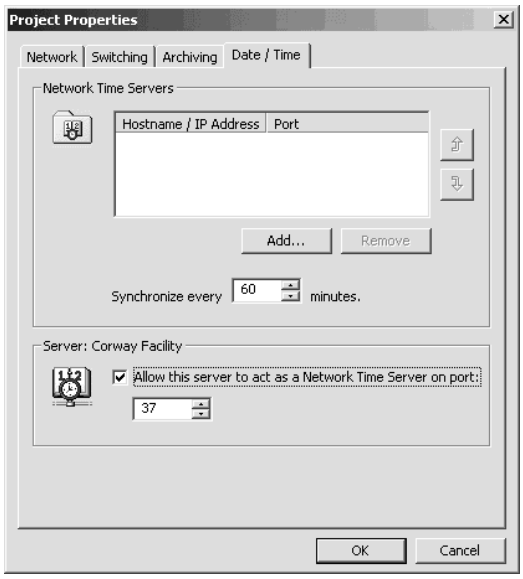


Figure 247. Synchronizing DVR with Server

b. Run an archive server: This ensures that alarms and events can be recorded. First launch the archive server. Refer to *Archive Servers* for instructions. Then add the archive server to the server configuration using the Archiving tab of the Project Properties dialog box. Select the archive server. Refer to *Project Properties* for instructions on adding and selecting archive servers.

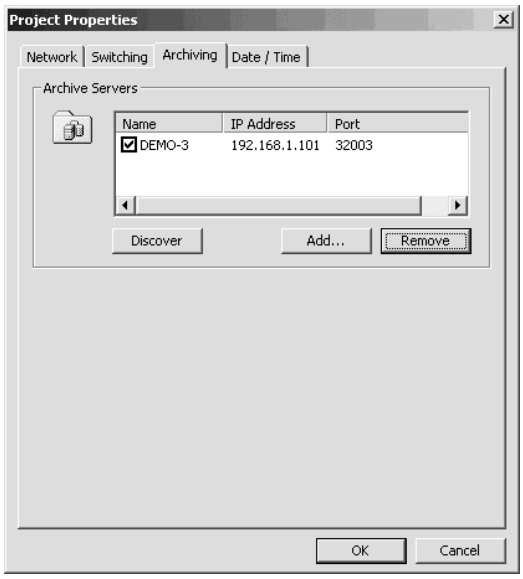


Figure 248. Running an Archive Server

c. Turn on alarm/event archiving: Turn on archiving for the alarm/event category the associated alarm or event belongs to. This ensures that alarms and events belonging to that category are recorded on the archive server. To turn archiving on, add or edit the desired alarm/event category and select Archive events of this category. Refer to *Alarm/Event Categories* for more information.

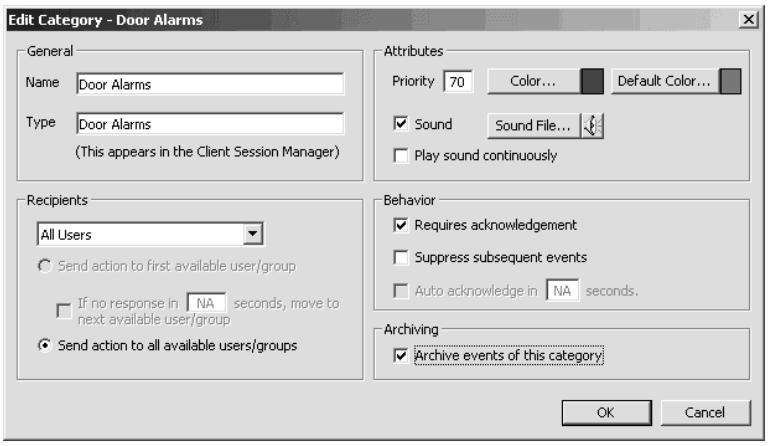


Figure 249. Activating Archiving

To associate a source device with an alarm or event complete the following steps:

a. Edit the alarm or event: Add or edit the alarm or event you want to associate with a source device. Refer to *Alarms, Events, and Normal Occurrences* for instructions.

b. Associate the source device: Select Associate source with this alarm/event. Select the desired source device from the drop-down box.

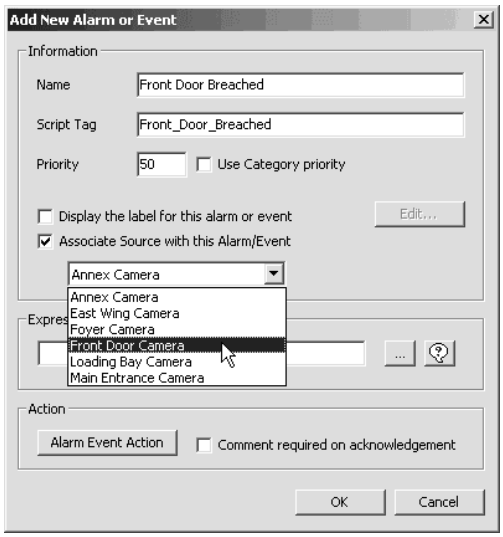


Figure 250. Associating a Source Device

7. **Expression:** Type the expression that will trigger the alarm or event when it becomes true. If the expression is too long for the box, open the expression editor by clicking the expression editor button ... . This provides you with a larger window to work in.

   Or you can use the expression wizard to create the alarm/event expression by clicking the Wizard button  .

   Refer to *Scripts and Expressions* for information on the syntax of expressions.

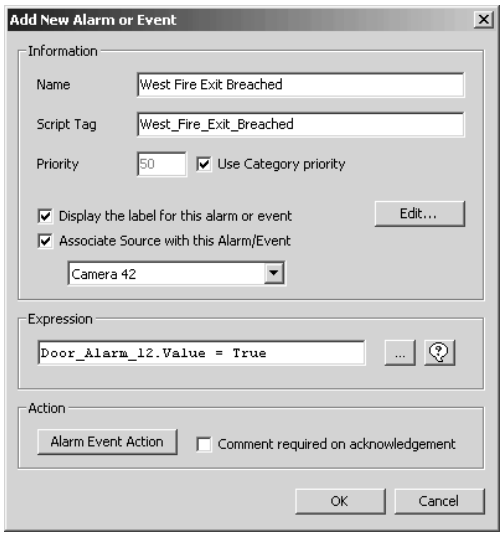


Figure 251. Entering Expression

8. **Action:** If you want to associate one or more scripts with the alarm or event, click Alarm Event Action. The Edit Alarm/Event Action dialog box opens.

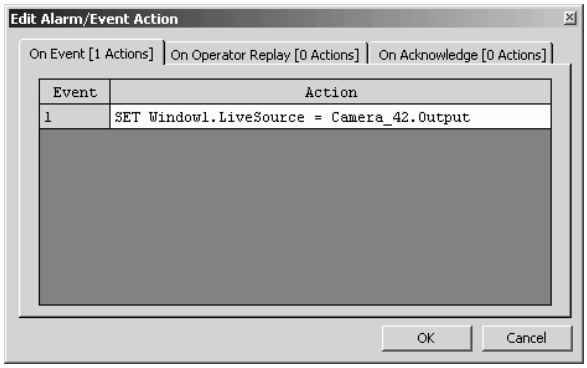


Figure 252. Edit Alarm/Event Action Dialog Box

You can define an On Event script that runs when the alarm or event is triggered, an On Operator Replay script that runs when a recipient replays the alarm or event, and/or an On Acknowledge script that runs when a recipient acknowledges the alarm or event. Type the script actions directly into the Action column, or use the script wizard to help you write the script. For more information on writing scripts, refer to *Scripts and Expressions*.

An alarm's scripts run on the client of any operator specified in the alarm/event category's recipient group, provided the client is running and the operator is logged in when the script executes. If the client is not running or the operator is not logged in, or if no recipients are specified in the category, VMX300(-E) runs as much of the script as possible, namely, statements that do not require a recipient, such as a statement that sets the value of a device property.

9. **Comment required:** If you want a recipient to type in a comment when acknowledging an alarm/event, click "Comment required on acknowledgement." The comment will be archived. If you are going to require comments for a particular type of alarm or event, make sure "Requires acknowledgement" and "Archive events of this category" are selected for the alarm/event category.

   The "Comment required on acknowledgement" option is not available when "Auto acknowledge in _ seconds" is selected for that alarm/event category.

10. Click OK. The Add New Alarm or Event dialog box closes and the new alarm or event is created. The name, script tag, and expression of the new alarm or event appear in the Object Browser.

NOTE: When you edit the script associated with an alarm or event, make it available in its updated form by saving the server configuration before attempting to run the script.

EDIT AN ALARM OR EVENT

NOTE: If you change the script tag for an alarm or event, any script that refers to the alarm or event will contain an error. To correct the error, update the scripts so they use the alarm or event's new script tag. Refer to *Scripts and Expressions* for more information.

1. Navigate the Object Browser to [project name] > Alarms and Events > [alarm/event category name]. In either pane, right-click the alarm or event you want to edit and select Edit from the pop-up menu. Alternatively, load a map that has an icon for the alarm or event you want to edit on it, and either double-click the icon, or right-click the icon and select Edit from the pop-up menu. Make sure you position the pointer over the icon, not the label, before clicking. The Edit Alarm or Event Properties dialog box opens.

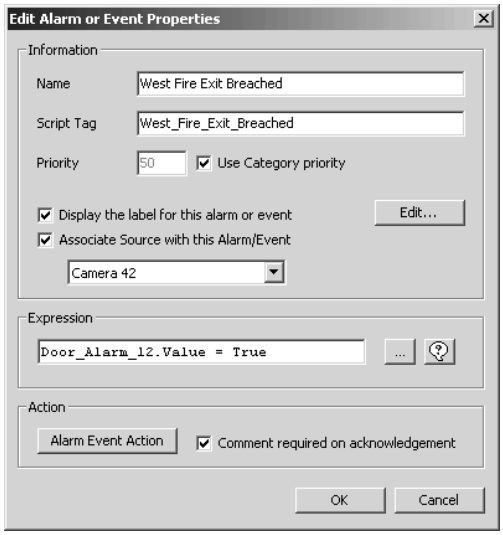


Figure 253. Edit Alarm or Event Properties Dialog Box

2. Change properties of the alarm or event as desired. Refer to *Add a New Alarm or Event* for information on specific properties.

3. Click OK. The Edit Alarm or Event Properties dialog box closes.

NOTE: If you edit a script associated with an alarm or event, make it available in its updated form by saving the server configuration before attempting to run the script.

DELETE AN ALARM OR EVENT

Deleting an alarm or event is irreversible. If you delete an alarm or event and then change your mind, you must add a new an alarm or event. Also note that if you delete an alarm or event, any script that refers to the alarm or event will contain an error.

1. Navigate the Object Browser to [project name] > Alarms and Events > [alarm/event category name]. In the right pane, right-click the alarm or event you want to delete and select Delete from the pop-up menu. The Confirm dialog box opens.

2. If you are sure you want to delete the alarm or event, click Yes. The selected alarm or event is deleted and the Confirm dialog box closes. The deleted alarm or event disappears from the Object Browser.

ALARM/EVENT ICONS

VMX300(-E) allows you to customize your maps by placing icons on them that represent the alarms and events configured on your server. Icons are an effective way to alert a recipient visually that an alarm or event has been triggered, and then acknowledged.

- When the alarm or event is triggered, the icon changes to the alarm color.
- When the alarm or event is acknowledged, the icon changes back to the default color.
- While the alarm/event expression is true, the bell hammer strikes the bell.

You do not need to place an alarm/event icon on a map for the alarm or event to function. Notification, sounds, scripts, and archiving all function independently of the icon. The icon's role is to provide operators with a visual alert.

Before you can place an alarm/event icon on a map, you must add the alarm or event itself as described in *Add a New Alarm or Event*. Once you have added the alarm or event, you can place as many icons representing the alarm or event as you want.

PLACE AN ALARM/EVENT ICON ON A MAP

NOTE: You do not need to place an alarm/event icon on a map for the alarm or event to function. Notification, sounds, scripts, and archiving all function independently of the icon.

1. Load the map you want to place an alarm/event icon on. The map appears in the map viewport.
2. Navigate the Object Browser to [project name] > Alarms and Events > [alarm/event category name]. In the right pane, click the alarm or event you want to place on the map and hold the mouse button down. If you move the pointer slightly, it changes to cross-hairs.
3. Drag the pointer to the map, position it where you want to place the alarm/event icon, and release the mouse button. An icon representing an alarm appears on the map and the pointer changes back to an arrow. If you selected "Display the label for this alarm or event" when you added the alarm or event, the label appears below the icon.
4. **Scale:** Move the pointer away from the icon to make the icon larger. Move the pointer towards the center of the icon to make the icon smaller. Scaling the alarm/event icon does not affect the size of the alarm/event label. Refer to *Scale an Alarm/Event Icon* for instructions on scaling the icon.

NOTE: To minimize the CPU workload, icons should be as small as possible.

5. When the icon is sized the way you want it, press the left mouse button. The icon freezes in place. If the alarm/event label is displayed, it freezes in place below the icon.

TIP: Hold the Shift key down while scaling to constrain the scaling to 5 unit increments.

MOVE AN ALARM/EVENT ICON

Any alarm/event icon placed on a map can later be moved to another position on the same map. When you move an alarm/event icon, only its position changes; its size remains fixed. For information on changing an icon's size, refer to *Scale an Alarm/Event Icon.*

1. With the desired map loaded, right-click the alarm/event icon you want to move and select Move from the pop-up menu. Make sure you position the pointer over the icon, not the label, before right-clicking.
2. Move the pointer to the icon's new location. The icon follows the pointer as you move it. If the icon's label is displayed, it moves with the icon.
3. When the icon is located where you want it, press the left mouse button. The icon freezes in place. If the map has a grid, the icon snaps to the grid.

SCALE AN ALARM/EVENT ICON

NOTE: To minimize the CPU workload, icons should be as small as possible.

Changing the size of an alarm/event icon does not affect its position. For information on changing an icon's position, refer to *Move an Alarm/Event Icon*.

1. With the desired map loaded, right-click the alarm/event icon you want to resize and select Scale from the pop-up menu. Make sure you position the pointer over the icon, not the label.

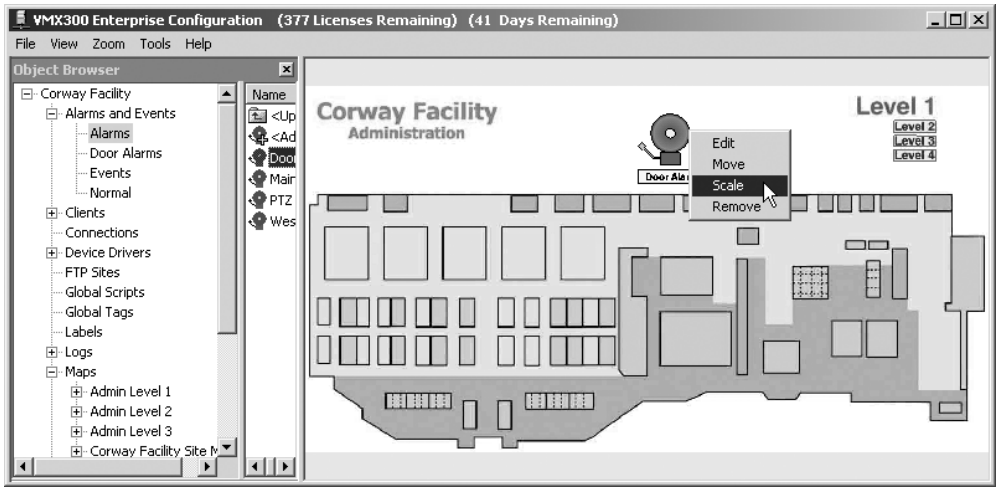


Figure 254. Changing Icon Size

2. Move the pointer away from the alarm/event icon to make the icon larger. Move the pointer towards the center of the icon to make it smaller.

3. When the icon is sized the way you want it, press the left mouse button. The icon's size freezes.

TIP: Hold the Shift key down while scaling to constrain the scaling to 5 unit increments.

NOTE: Scaling an alarm/event icon does not affect the size of the label. Refer to *Scale an Alarm/Event Label* for information on scaling the label.

REMOVE AN ALARM/EVENT ICON FROM A MAP

Removing an alarm/event icon from a map does not affect any other icons for that alarm or event, whether they are on the same map or another map, nor does it affect the alarm or event in the Object Browser. If you change your mind after removing an alarm/event icon from a map, you can add it back as described in *Place an Alarm/Event Icon on a Map*.

TIP: You do not need to have an alarm/event icon on a map in order for the alarm or event to function. Notification, sounds, scripts, and archiving all function independently of the icon. The icon's role is to provide operators with a visual alert.

With the desired map loaded, right-click the alarm/event icon you want to remove and select Remove from the pop-up menu. Make sure you position the pointer over the icon, not the label, before right-clicking. The icon disappears from the map. If it is displayed, the alarm/event label also is removed from the map.

MOVE AN ALARM/EVENT LABEL

You can move an alarm/event label independently of the icon itself.

1. With the desired map loaded, right-click the label you want to move and select Move from the pop-up menu. Make sure you position the pointer over the label, not the icon, before right-clicking.
2. Move the pointer to the label's new location. The label follows the pointer as you move it. The icon does not move.
3. When the label is located where you want it, press the left mouse button. The label freezes in place.

SCALE AN ALARM/EVENT LABEL

Changing the size of an alarm/event label does not affect its position. For information on changing a label's position, refer to *Move an Alarm/ Event Label.*

1. With the desired map loaded, right-click the alarm/event label you want to resize and select Scale from the pop-up menu. Make sure you position the pointer over the label, not the icon, before right-clicking.

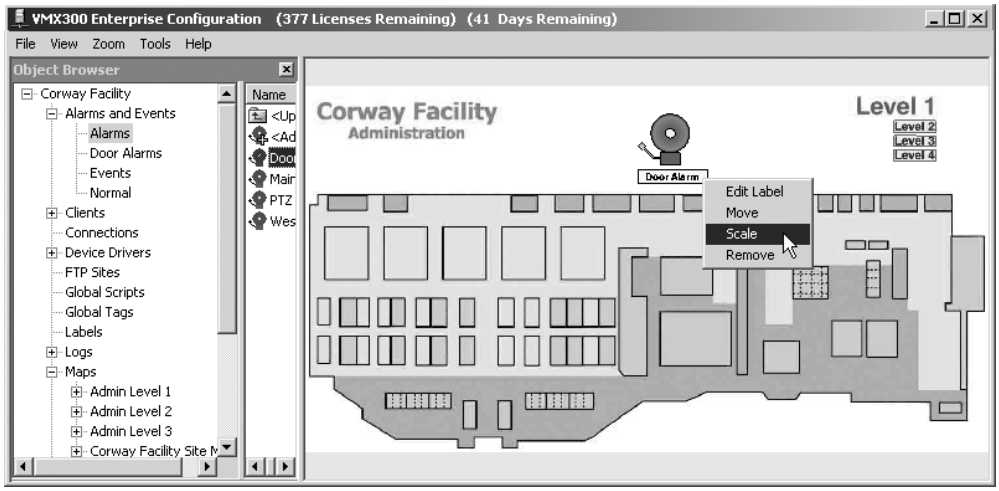


Figure 255. Changing Label Size

2. Move the pointer away from the label to make the label larger. Move the pointer towards the center of the label to make the label smaller.
3. When the alarm/event label is sized the way you want it, press the left mouse button. The label's size freezes.

NOTE: You cannot change the orientation of an alarm/event label. Labels are always oriented horizontally.

EDIT AN ALARM/EVENT LABEL

1. Right-click the alarm/event label, and select Edit Label from the pop-up menu. Make sure you position the pointer over the label, not the icon, before right-clicking.

   Alternatively, navigate the Object Browser to [project name] > Alarms and Events > [alarm/event category name]. In the right pane, double-click the desired alarm or event, or right-click the alarm or event and select Edit from the pop-up menu, then click Edit Label. The Edit Label Properties dialog box opens.

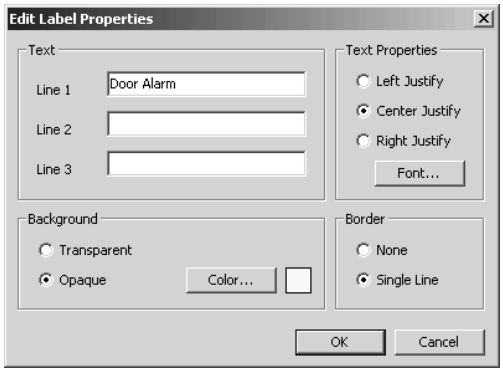


Figure 256. Edit Label Properties Dialog Box

2. Change properties of the label as desired. Refer to *Add a New Alarm or Event* for information on specific properties.

3. Click OK. The Edit Label Properties dialog box closes.

REMOVE AN ALARM/EVENT LABEL

Removing an alarm/event label from one icon removes the label from all icons representing that alarm or event, whether the icons are on the same map or different maps. If you change your mind after removing an alarm/event label, you can add it back as described in *Add a New Alarm or Event.*

With the desired map loaded, right-click the alarm/event label you want to remove and select Remove from the pop-up menu. Make sure you position the pointer over the label, not the icon, before right-clicking. The alarm/event label disappears from the map and "Display the label for this alarm or event" is cleared in the alarm/event properties. The icon is unaffected.

Recipient Groups

Recipient groups define which operators are notified of scheduled actions and alarms and events. Recipients are notified through the Session Manager. In addition, if you have associated scripts with the scheduled action or alarm or event, the scripts will be run on the recipient's workstation. To receive notification, an operator who is listed as a recipient must be logged in when the scheduled action or alarm or event occurs. For information on the Session Manager, refer to the VMX300(-E) Client Operation Manual.

Refer to *Alarms and Events - Alarm/Event Categories - Add a New Alarm/Event Category* for instructions on selecting a recipient group for a category of alarms or events. Refer to *Schedules - Add a New Schedule* for instructions on selecting a recipient group for a schedule.

For example, if you create an alarm that is triggered when an exit door is opened, you might define a script that loads video from a camera covering the area around the door. When the alarm is triggered, a recipient's workstation will automatically display video of the exit door, saving the recipient from having to locate the source of the alarm and load the video manually.

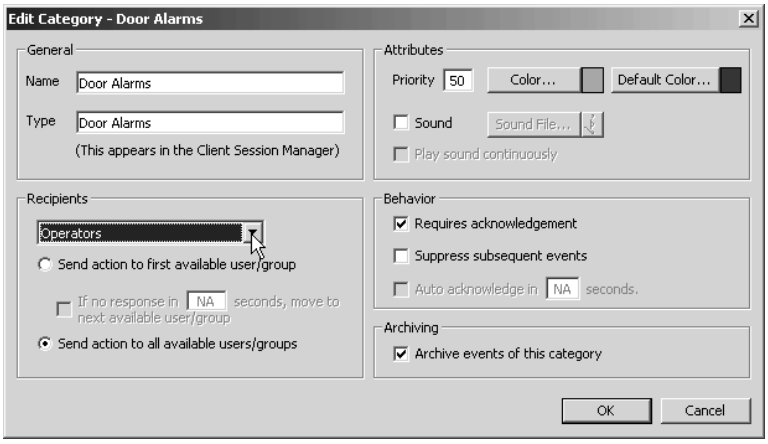


Figure 257. Recipients

THE PREDEFINED RECIPIENT GROUP

VMX300(-E) provides one predefined recipient group: All Users. If you select All Users as the recipient group for a schedule or alarm or event, notification will be sent simultaneously to every user configured on the server who is logged in when the schedule or alarm or event occurs.

The All Users recipient group does not appear as in the Object Browser. It cannot be edited or deleted. It only appears in the Recipients drop-down list for schedules and alarm/event categories.

ADD A NEW RECIPIENT GROUP

When you create a new recipient group, the group automatically appears in the Recipients list of every alarm/event category and schedule. You can then select that recipient group for any new or existing schedule or alarm or event.

You can create a new recipient group from scratch or you can base new groups on an existing group. To create a new recipient group based on an existing group, make a copy of the existing group and then edit the copy. Refer to *Pop-Up Menus* in the *Appendix* for information on using Copy and Paste or Paste Many to make copies of objects.

To create a new recipient group from scratch:

1. Navigate the Object Browser to [project name] > Recipient Groups. Double-click <Add New Recipient Group> in the right pane, or right-click Recipient Groups in the left pane and select Add New from the pop-up menu. The Add New Recipient Group dialog box opens.

Figure 258. Add New Recipient Group Dialog Box

2. **Name:** Type a unique, descriptive name for the group you want to add. Recipient group names are, at most, 50 characters long. They can include any letter, digit or special character, with the exception of single and double quotation marks. Recipient group names are not case sensitive. You cannot use the name All Users, as it is reserved for the predefined recipient group.

3. **List recipients:** Move each user and user group you want to be included in the recipient group from the Available Users/<Groups> list to the Members list. The names of user groups appear between angle brackets.

   To move a single user or group, select the user or group you want to move in the Available Users/<Groups> list and click the right arrow button >. To move all the users and groups, click the double right arrow button >>. Use the left arrow button < and double left arrow button << to move users and groups back to the Available Users/<Groups> list from the Members list.

   To select multiple users and groups, hold the Control key down while selecting with the mouse.

4. **Order list:** Sort the users and groups in the Members list in the order you want them to be notified of a scheduled action or alarm or event. The order is only relevant if you select "Send action to first available user/group" in the alarm/event category or schedule. The member at the top of the list is notified first.

   To move a member higher in the list, select the member and click Move Up. To move a member lower in the list, select the member and click Move Down.

5. Click OK. The Add New Recipient Group dialog box closes and the new group is created. The name of the new group appears in the Object Browser.

EDIT A RECIPIENT GROUP

To change the properties of an existing recipient group:

1. Navigate the Object Browser to [project name] > Recipient Groups. In the right pane, double-click the recipient group you want to change, or right-click the group and select Edit from the pop-up menu. The Edit Recipient Group Properties dialog box opens.

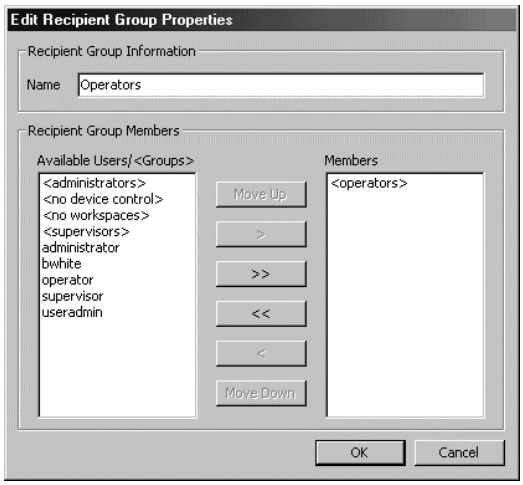


Figure 259. Edit Recipient Group Properties Dialog Box

2. Change the properties of the recipient group as desired. Refer to *Add a New Recipient Group* for information on specific properties.
3. Click OK. The Edit Recipient Group Properties dialog box closes.

DELETE A RECIPIENT GROUP

NOTE: Deleting a recipient group is irreversible. If you delete a recipient group and then change your mind, you must re-create it as described in *Add a New Recipient Group* and individually edit each alarm/event category and schedule that used to go to that recipient group to re-assign the recipient group.

1. Navigate the Object Browser to [project name] > Recipient Groups. In the right pane, right-click the recipient group you want to delete and select Delete from the pop-up menu. The Confirm dialog box opens.
2. If you are sure you want to delete the recipient group, click Yes. The selected recipient group is deleted and the Confirm dialog box closes. The name of the deleted group disappears from the Object Browser.

Server Ties

NOTE: Server ties are available only with VMX300-E systems.

Share signals: Server ties enable one server to share signals, such as video or audio, with another server. For example, if you have a camera configured on one server, and you want to view the camera's video on a destination (for example, external monitor or custom window) configured on a different server, you must define a server tie. In Figure 260, Server A has a server tie to Server B so the camera's video can be viewed on the monitor or client.

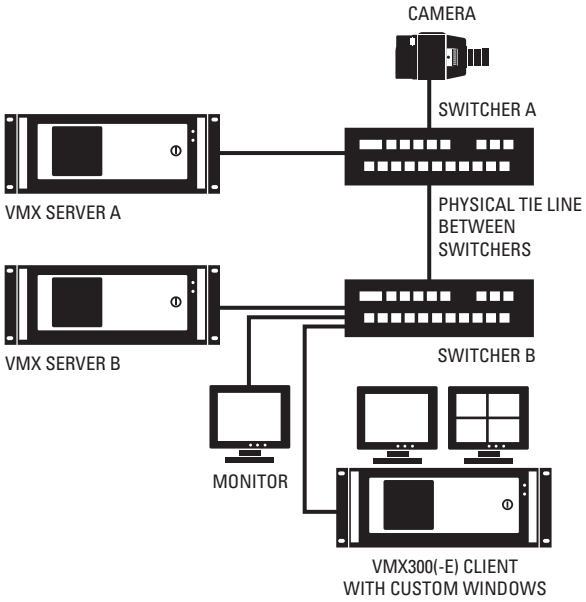


Figure 260. Server Tie

To access signals over the server tie illustrated in Figure 260, operators must be logged in to both servers, typically with Server B as their home server. Logging in to Server A gives the remote operator access to Server A's maps and devices, provided the operator's Server A user account grants the necessary privileges. To limit a remote user's access to maps and devices, restrict the user's permissions in the Server A configuration exactly as you would any other user.

Operators load video from a remote server the same way they load video from their home server: by dragging the camera from the Device List or from a map to the destination.

Signal types: You must define a server tie for each type of signal you want to share. Signals fall into two broad categories: analog and IP. The specific types of IP and analog signals depend on the equipment configured on your server. Analog signal types can include Analog Video, VGA Video, and Audio. IP signal types are specific to the models of IP encoders configured on your server. For each analog server tie you configure, you must add a connection on both servers to map out the physical connections between devices.

Number of simultaneous destinations: A server tie allows a signal to be transmitted to one destination at a time. If you want to transmit signals to more than one destination at one time, you must define a server tie for each destination. For example, if you want to be able to display video from a remote server in all four video windows provided by a quad card, you must configure four server ties, one for each window.

TIP: IP server ties enable you to limit bandwidth between servers across wide area networks. Several operators viewing remote video at the same time across a WAN use a significant portion of the available bandwidth. Server ties limit the bandwidth used for remote video by limiting the number of operators who can view remote video at one time to the number of server ties configured.

Define scripts: Configuring a server tie provides Server B with limited access to Server A's devices for scripting. Specifically, Server B can use the SET command to load the signal from a device configured on Server A. For example, to automatically load video from Server A's Cam1 into Server B's Window1, use the following statement:

```
SET Window1.LiveSource = Cam1_RS.Output
```

Server B has no access to the read and write properties of devices configured on Server A.

The ability to script signal loading results from adding Server A's remote server driver to the Server B configuration. Server A's devices appear as Sources in the Object Browser. Refer to *Configure a Server Tie* for instructions on adding a remote server driver.

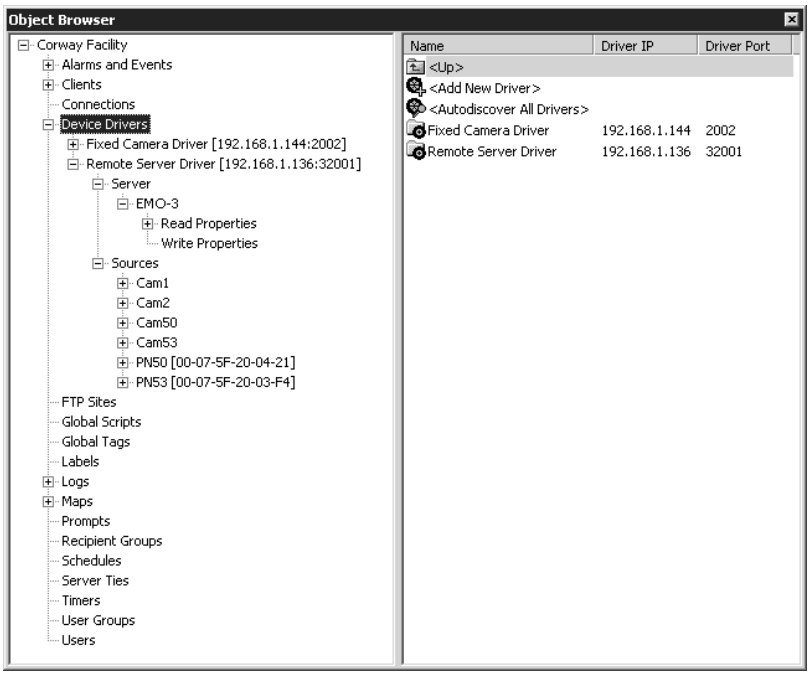


Figure 261. Server A's Devices

By default, a remote device's script tag ends with "_RS", to indicate "Remote Server". To edit the device's script tag, edit the device's local settings. Refer to *Devices - Edit a Device's Local Settings* for instructions.

TIP: Use context-sensitive help or the script wizard to write scripts involving remote servers. VMX300(-E) will provide you with a pop-up list of script tags referring to remote servers and their devices and alarms, in context. Refer to *Scripts and Expressions - Mechanics of Editing Scripts and Expressions* for more information.

Share alarms and events: Configuring a server tie enables Server B to refer to alarms and events defined on Server A in scripts and expressions. Alarm-sharing results from adding Server A's remote server driver to the Server B configuration. Server A's alarms and events appear as Server Read Properties in the Object Browser. Refer to *Configure a Server Tie* for instructions on adding a remote server driver.

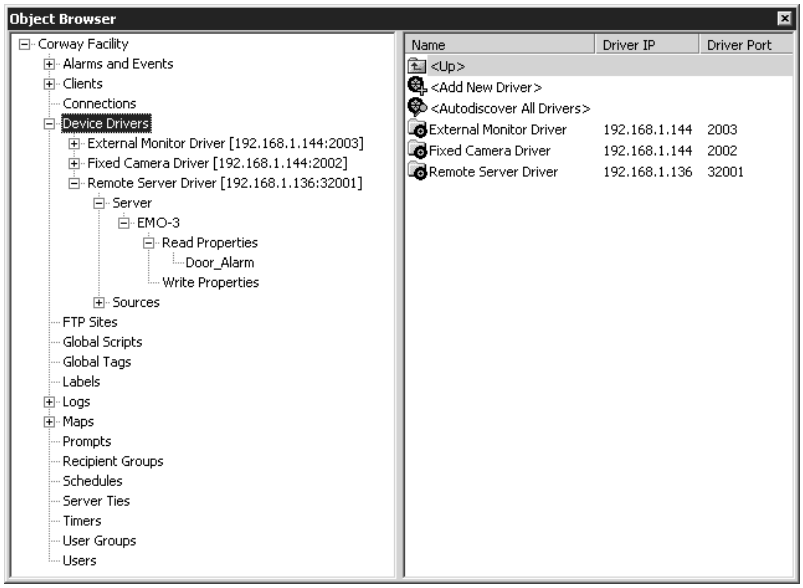


Figure 262. Server A's Alarms and Events

By default, a remote server's script tag ends with "_Server". For example, if the remote server is called EMO-3, its script tag is EMO-3_Server. To edit the server's script tag, edit the server's local settings. Refer to *Devices - Edit a Device's Local Settings* for instructions.

Script tags for remote alarms and events appear in the Object Browser.

Suppose Server A (EMO-3) has an external door alarm that triggers an alarm, Door Alarm, that directs the camera at the door. On Server B, create an alarm that loads live video from Server A's camera when the Door_Alarm read property becomes true. The expression for the Server B alarm is as follows:

EMO-3_Server.Door_Alarm = EMO-3_Server.True

The alarm's On Event action is:

SET Window1.LiveSource = Cam1_RS.Output

TIP: Use context-sensitive help or the script wizard to write scripts involving remote servers. VMX300(-E) will provide you with a pop-up list of script tags referring to remote servers and their devices and alarms, in context. Refer to *Scripts and Expressions - Mechanics of Editing Scripts and Expressions* for more information.

PREVENT OTHER SERVERS FROM MONOPOLIZING YOUR TIES

In a situation in which three (or more) servers have three-way server ties, it is possible for two of the servers to monopolize the other server's ties. For example, consider the scenario depicted in the following illustration:

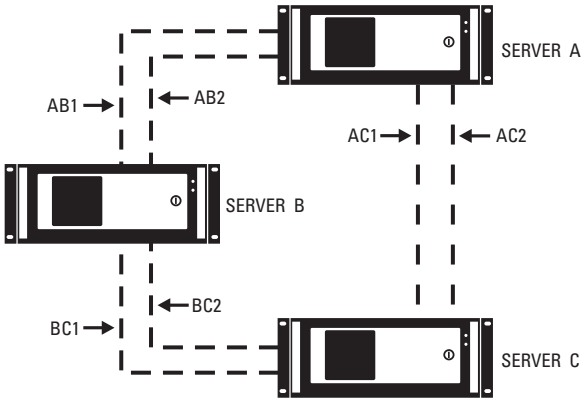


Figure 263. Sample Three-way Server Tie Scenario

Suppose demand for shared video between servers A and C is very heavy. The first two operators who access shared video between servers A and C will be allocated server ties AC1 and AC2. When a third operator accesses shared video, no more direct paths between the two servers are available, so a path through server B would be used, such as AB1 - BC1, effectively tying up two of server B's server ties. Now if a fourth operator accesses shared video between servers A and C, the remaining path through server B (AB2 - BC2) would be used, leaving no free paths for server B's operators to use to access shared video.

You can prevent other servers from using your ties to share signals with each other by instructing Cameleon not to forward the remote server's routing information. For example, server B can prevent servers A and C from sharing video over paths AB1 - BC1 and AB2 - BC2. This reserves the paths between servers B and A for video sharing between servers B and A, and reserves the paths between servers B and C for video sharing between servers B and C.

To prevent other servers from using your ties to share signals with each other, click the "Forward remote server routing information" field on the Project Properties Switching tab. Refer to *Project Properties* for instructions.

CONFIGURE A SERVER TIE

Assuming the set-up shown in Figure 260, in which you want to share signals from Server A with Server B, configure the servers as follows:

1. **Server A:**
   a. **Log in:** Log in to configuration mode on Server A.
   b. **Add server tie:** Create a server tie to Server B. Refer to *Add a New Server Tie* for instructions.

c. **Create connection:** If you are sharing analog signals, create a connection from the signal source's output to the server tie. Refer to *Connections* for instructions.

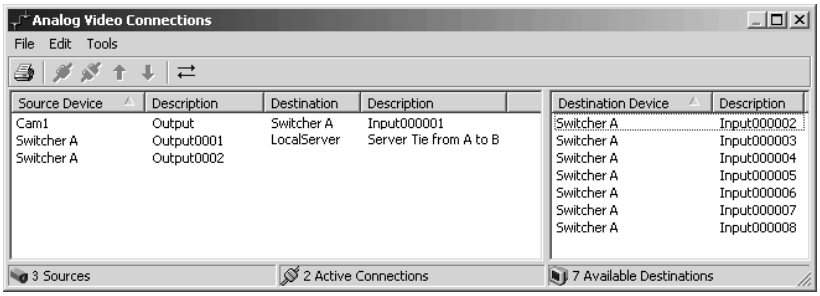


Figure 264. Creating Connection for Server A

d. **Add clients:** Add each client that will access Server A's video from Server B. Refer to *Clients, Custom Windows, and Canvases - Clients - Add a New Client* for instructions. Do not add custom windows to the clients.

e. **Create user group:** If desired, create a user group for the remote users to belong to. Make sure the user group provides permission to the desired source devices. Refer to *User Groups - Add a New User Group* for instructions.

f. **Add user accounts:** Create a user account for each operator who will be viewing Server A's video from Server B. To enable an operator to log in to both servers simultaneously, make the user name and password the same as on Server B.

VMX300(-E) provides an Import function that allows you to import a user account from another server. As well as guarding the security of the user account, this saves you from having to enter the user information manually. Refer to *Users - Add a New User* for instructions.

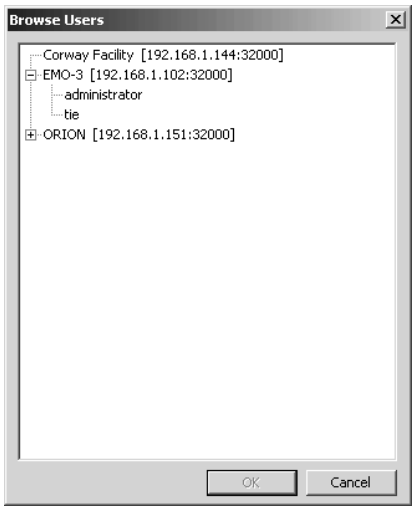


Figure 265. Creating User Account

g. **Save configuration:** Exit configuration mode and save Server A's configuration. Refer to *Starting and Stopping the Server* for instructions.

h. **Run Server A:** If it is not already running, put Server A in run mode. Refer to *Starting and Stopping the Server* for instructions.

2. **Server B:**

a. **Log in:** Log in to configuration mode on Server B.

b. **Add remote server driver:** Add the remote server driver for Server A. Remote server drivers provide a list of source devices on the remote server and a list of alarms and events on the remote server. Alarms and events are presented as read properties of the remote server. Refer to *Server Ties* for information on using remote server devices and alarms and events in scripts.

Remote server drivers appear as device drivers in the Object Browser, and are added, edited, and deleted the same way device drivers are. There is a remote server driver for each server that is running.

VMX300(-E) provides a Browse All function that allows you to select a remote server driver from a list of running drivers. Refer to *Device Drivers - Add a New Device Driver* for instructions on browsing drivers. Select the desired remote server driver and click OK.

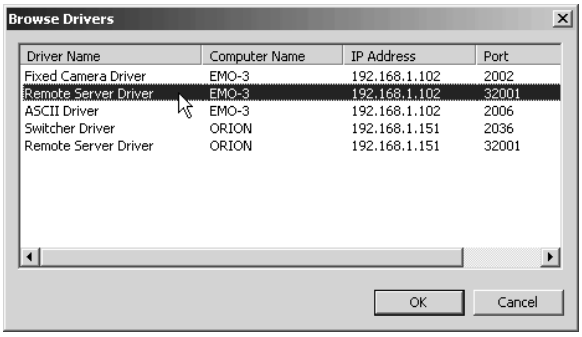


Figure 266. Selecting a Remote Server Driver

The remote server driver appears in the Object Browser. Expand the list to view the remote server's devices and alarms and events.

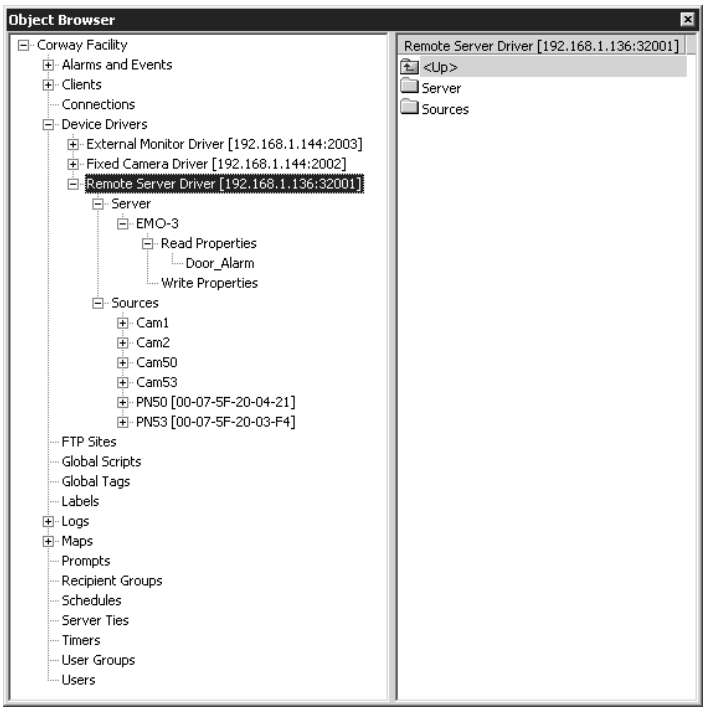


Figure 267. Viewing Devices, Alarms, and Events

c. **Create connection:** If you are sharing analog signals, create a connection from the server tie to the destination device's input. Refer to *Connections* for instructions.

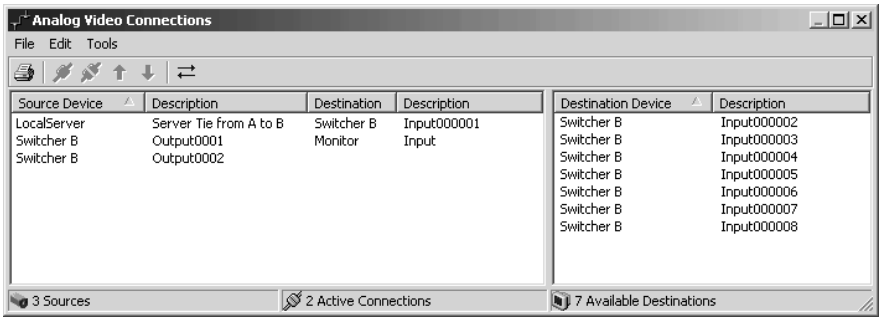


Figure 268. Creating a Connection For Server B

d. **Add clients, custom windows, and canvases:** If you have not already done so, add each client that will access Server A's video. If signals from Server A are going to be viewed in a custom window, add the window and configure the appropriate type of canvas for the window. Refer to *Clients, Custom Windows, and Canvases* for instructions.

e. **Save configuration:** Exit configuration mode and save Server B's configuration. Refer to *Starting and Stopping the Server* for instructions.

f. **Run Server B:** If it is not already running, put Server B in run mode. Refer to *Starting and Stopping the Server* for instructions.

NOTE: If you add a new camera to Server A, you can use an existing server tie to access video from the camera, provided the server tie is for the correct signal type. To make the new camera available to Server B, you must synchronize Server B's configuration. Synchronization is performed automatically when you log in to configuration mode on Server B, or you can synchronize explicitly by editing the remote server driver and clicking Synchronize.

TEST A SERVER TIE

1. Log in to the VMX300(-E) client, connecting to both Server A and Server B, with Server B as your home server. Refer to *Configuring Servers* in the VMX300(-E) Client Operation Manual for instructions on selecting the servers to connect to.
2. Drag the Server A source device to the destination configured on Server B. Make sure you drag the source to the correct destination. For example, if you are testing an analog server tie, you must drag the source device connected to the server tie in Server A's connections (Cam1 in *Configure a Server Tie* step 1.c) to the destination device connected to the server tie in Server B's connections (Monitor in *Configure a Server Tie,* step 2.c). The signal from the source device loads and appears in the destination device.

ADD A NEW SERVER TIE

1. Navigate the Object Browser to [project name] > Server Ties. Double-click <Add New Server Tie> in the right pane, or right-click Server Ties in the left pane and select Add New from the pop-up menu. The Add New Server Tie dialog box opens.

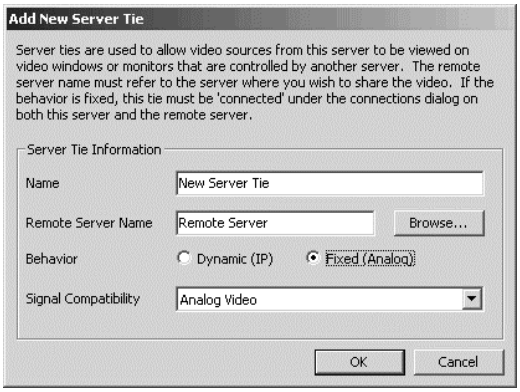


Figure 269. Add New Server Tie Dialog Box

2. **Name:** Type in a unique, descriptive name for the server tie you want to create. Server tie names are at most 50 characters long and can include any letter, digit or special character, with the exception of single and double quotation marks. Server tie names are not case sensitive.
3. **Remote server name:** Type in the name of the server you want to share signals with, or click Browse to open a list of servers to select from.
4. **Behavior:**
   a. To share IP signals, select Dynamic (IP). A list of available types of IP signals appears in the Signal Compatibility box.
   b. To share analog signals, select Fixed (Analog). A list of available types of analog signals appears in the Signal Compatibility box.
5. **Signal compatibility:** Select the type of signal you want this server tie to share from the drop-down list.
6. Click OK. The server tie is created and the Add New Server Tie dialog box closes. The new server tie appears in the Object Browser.

EDIT A SERVER TIE

1. Navigate the Object Browser to [project name] > Server Ties. In the right pane, double-click the server tie you want to change, or right-click the server tie and select Edit from the pop-up menu. The Edit Server Tie Properties dialog box opens.

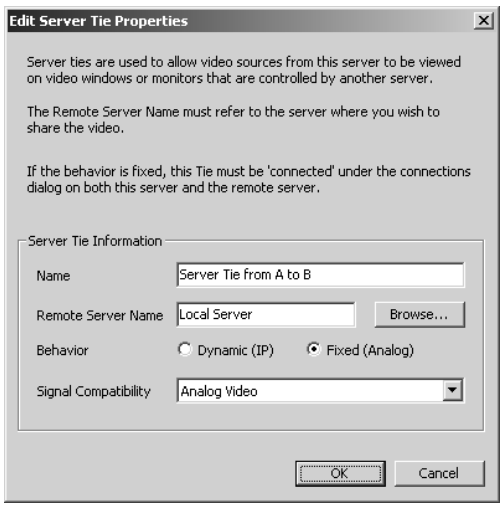


Figure 270. Edit Server Tie Properties Dialog Box

2. Change the properties of the server tie as desired. Refer to *Add a New Server Tie* for information on specific properties.

3. Click OK. The Edit Server Tie Properties dialog box closes.

DELETE A SERVER TIE

Deleting a server tie is irreversible. If you delete a server tie and then change your mind, you must add a new server tie.

1. Navigate the Object Browser to [project name] > Server Ties. In the right pane, right-click the server tie you want to delete and select Delete from the pop-up menu. The Confirm dialog box opens.

2. If you are sure you want to delete the server tie, click Yes. The selected server tie is deleted and the Confirm dialog box closes. The deleted server tie disappears from the Object Browser.

FTP Sites

FTP (File Transfer Protocol) is a set of communication rules that allow two computers to exchange files over a network. The FTP image capture feature allows you to capture live video in a custom window and upload the image file to an FTP server, such as a Web host. The action of capturing and uploading an image is controlled through the FTP script command.

To use the FTP image capture feature, you must do the following procedures:

- **Configure FTP site:** Add the FTP site to the server configuration. Refer to *Add a New FTP Site* for instructions.
- **Write script:** Write a script that initiates an FTP image capture. Refer to *Write an FTP Script* for more information.

You might also want to do this:

- **Adjust image attributes:** Adjust the dimensions and quality of captured images. Refer to *Clients, Custom Windows, and Canvases - Canvases - Add a New Canvas (General)* for more information.

ADD A NEW FTP SITE

To add a new FTP site:

1. Navigate the Object Browser to [project name] > FTP Sites. Double-click <Add New FTP Site> in the right pane, or right-click FTP Sites in the left pane and select Add New from the pop-up menu. The New FTP Site Properties dialog box opens with the General tab showing.
2. **General tab:**

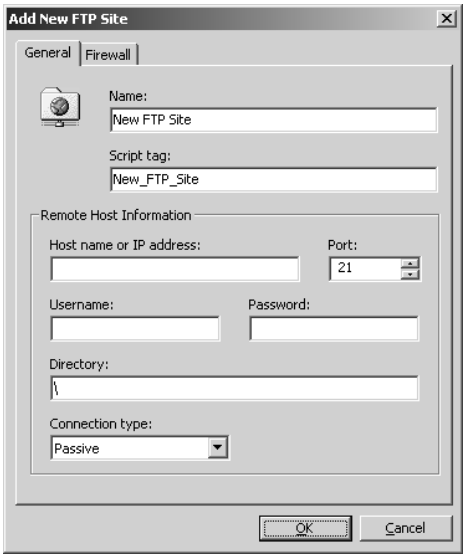


Figure 271. New FTP Site Properties General Tab

a. **Name:** Type a unique, descriptive name for the FTP site you want to add. FTP site names are, at most, 50 characters long and can include any letter, digit or special character, with the exception of single and double quotation marks. FTP site names are not case sensitive.

b. **Script tag:** If you do not want to use the script tag provided by the server, type a unique, meaningful tag. Script tags are, at most, 50 characters long. They can include any letter, digit or the underscore character, but cannot begin with a digit. They cannot contain spaces or special characters. Tags are not case sensitive. Use the script tag to initiate FTP image captures in scripts. For information on using the FTP script statement, refer to *Write an FTP Script*.

c. **Remote host information:** The Remote Host Information area is used to enter information about the FTP server where image files will be sent and stored. If you are missing any of the information in the Remote Host Information area, contact the system administrator of the FTP server.

(1) **Address:** In the Host name or IP address box, type in the address of the remote host you will be uploading images to. You can type in the remote host's Web address, such as www.webhost.com, or IP address, or, if the host is on your local network, the computer name.

(2) **Port:** Type the port the remote host opens to FTP traffic. Port 21 is the standard FTP port.

(3) **User name:** Type the user name you enter to upload files to the remote host. If no user name is defined on the remote host, then type anonymous in the User Name box.

(4) **Password:** Type the password you enter to upload files to the remote host. If no password is defined on the remote host, leave the Password box empty.

(5) **Directory:** Type the name of the directory on the remote host where the captured images will be stored. For example, if you will be storing the captured image files in a directory called 'captures', then enter \captures in the Directory box.

(6) **Connection type:** Select the FTP connection type from the drop-down list. Typically, FTP connections are passive.

3. **Firewall tab:** Configure the settings on the Firewall tab if the FTP server is behind one of the following types of firewall:

- Socks 4
- Socks 5
- Proxy USER command
- Proxy SITE command
- Proxy OPEN command
- Simple Pipe

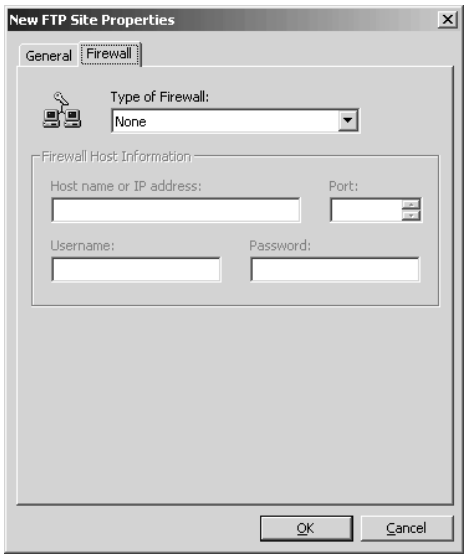


Figure 272. New FTP Site Properties Firewall Tab

a. **Type of firewall:** Select the type of firewall from the drop-down list.

b. **Firewall host information:** The Firewall Host Information area is used to enter information about the firewall the FTP server is behind. If you are missing any of the information in the Firewall Host Information area, contact the system administrator of the FTP server.

(1) **Address:** In the "Host name or IP address" box, type the address of the firewall host. You can type the firewall host's Web address, such as www.fwallhost.com, or IP address.

(2) **Port:** Type the firewall host's listening port.

(3) **User name:** If the firewall host requires a user name, type the user name in the User Name box. If no user name is defined on the firewall host, then leave the User Name box empty.

(4) **Password:** If the firewall host requires a password, type the password in the Password box. If no password is defined on the firewall host, leave the Password box empty.

4. Click OK. The server tie is created and the Add New Server Tie dialog box closes. The new server tie appears in the Object Browser.

EDIT AN FTP SITE

1. Navigate the Object Browser to [project name] > FTP Sites. In the right pane, double-click the FTP site you want to change, or right-click the FTP site and select Edit from the pop-up menu. The Properties dialog box opens.

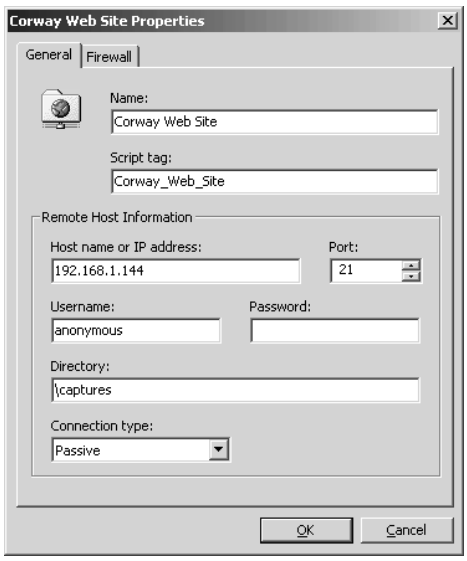


Figure 273. Edit FTP Site Properties Dialog Box

2. Change the properties of the FTP site as desired. Refer to *Add a New FTP Site* for information on specific properties.
3. Click OK. The Properties dialog box closes.

WRITE AN FTP SCRIPT

THE FTP COMMAND

The action of capturing and uploading an image to an FTP site is controlled through the FTP script command. The syntax of the FTP statement is:

FTP [window tag], [camera tag], [preset tag], [delay], [FTP site tag], "[file name]"

Briefly, VMX300(-E) interprets the FTP statement as follows: Switch the camera to the custom window and move the camera to the preset. When the delay time has elapsed, capture the window's video. Upload the captured image to the FTP server, saving it under the specified file name.

TIP: Use context-sensitive help or the script wizard to help you write FTP statements. Refer to *Scripts and Expressions - Mechanics of Editing Scripts and Expressions* for more information.

Window: The window must have the correct canvas defined for it. Refer to *Clients, Custom Windows, and Canvases - Canvases* for more information. If the client that the window is defined on is running but the window is closed, VMX300(-E) automatically opens the window when the FTP statement executes.

TIP: It is recommended that you define only one canvas for any window you are using for FTP image capture. If you need to capture more than one type of video, create a window for each type.

Preset: Sending the camera to a preset is optional. If you want to omit the preset, either enter NoPreset, or omit the preset. For example, the following FTP statements are equivalent and valid:

FTP Window1, ReceptionCamera, NoPreset, 1, Corway_Web_Site, "reception.jpg"

FTP Window1, ReceptionCamera, , 1, Corway_Web_Site, "reception.jpg"

Note that, if you omit NoPreset, you still need to include the comma, so the camera tag is followed by two commas.

Delay: The intent of the delay is to give the camera time to move to the preset before taking the capture. Make sure the delay is long enough to allow the camera to reach the preset. The delay is in seconds. A delay of zero seconds is valid. Use a zero second delay when no preset is specified.

The camera is locked during the delay. An operator who is viewing the camera's gadget or Device Control dialog box when the FTP delay occurs will see the Lock button change to yellow, indicating that the camera is locked by a script. For information on the Lock button, refer to the appropriate camera Driver Notes in the VMX300(-E) Client Operation Manual.

File name: FTP image files are JPG files. The file name should end with ".jpg". If a file of that name already exists on the FTP server, the old file is overwritten when the new one is uploaded.

In detail, VMX300(-E) executes an FTP statement as follows:

1. If the specified custom window is closed, open the window. Set the window content type to LiveVideo.
2. Switch the specified camera to the window. If the switch was unsuccessful, the FTP command fails.
3. If the switch was successful, lock the camera and start timing the delay. A delay of zero seconds causes the capture to be taken immediately.
4. If a preset is specified, send the camera to the preset.
5. When the delay has elapsed, unlock the camera. If the camera was sent to a preset, check that it is still positioned at the preset. The camera might have been moved from the preset by a user or script with higher priority than the FTP script. If the camera is not at the preset, the FTP command fails.
6. Capture the video displayed in the custom window and create the image file.
7. When the image file has been created, log in to the FTP server and upload the file. If a file with the specified name already exists, overwrite it.

Failure: If any step in the FTP process fails, the FTP command fails. If you want the script to continue executing, include an ON ERROR RESUME NEXT command at the beginning of the script.

Below are some possible causes of failure:

- No switch path found.
- The camera is locked by a higher priority user or script, and the camera is not at the desired preset.
- A higher priority user or script took the lock from the FTP script and moved the camera.
- An operator or script switched a different camera to the window after the FTP switch.
- An operator or script changed the content type of the FTP window before the capture was taken.
- The capture failed, possibly because the window has the wrong type of canvas defined for it.
- The specified preset does not exist, because it has been renamed.

FTP SCRIPTS

Like any script command, the FTP command can be used in any type of script. Often, FTP commands are put in a global script that is run from a schedule's script using the RUN command. Putting the FTP commands in a global script allows you to have more than one schedule that calls the script. For example, you might want to have two schedules: one for weekdays and another for weekends, so the sequence can be run more frequently on weekdays.

Using a global script also allows an operator to run the script on demand from the client, provided the operator has the necessary permissions. Make sure you limit permissions to just those users you want to be able to run the global script.

A schedule runs on the client of any operator specified in the schedule's recipient group, provided the operator is logged in when the script executes. If no recipients are specified in the schedule, VMX300(-E) runs the script on any running client that has the necessary window.

In some cases, VMX300(-E) will execute different lines of the script on different clients. For example, suppose a particular schedule has no recipients. The schedule's script has two FTP commands:

```
FTP Window1, Cam1, NoPreset, 0, Corway_Web_Site, "image.jpg"

FTP Window2, Cam1, NoPreset, 0, Corway_Web_Site, "image.jpg"
```

The only difference between the two commands is the window specified. When the first FTP command executes, VMX300(-E) looks for a running client that has Window1 defined on it. Suppose Client1 is running and has Window1 defined on it. The first FTP command executes on Client1. When the second FTP command executes, VMX300(-E) looks for a running client that has Window2 defined on it. Suppose Client2 is running and has Window2 defined on it. The second FTP command executes on Client2.

Example: The following example illustrates an FTP sequence defined in a global script that is run from a schedule. The sequence starts with an ON ERROR RESUME NEXT command, to ensure that, in the event that an FTP command fails, the next statement will execute. Every time the global script is run by the schedule, VMX300(-E) executes every statement, including any statement that failed the last time it was run.

Image captures in this sequence are taken between 5 AM and 7 AM only. The schedule that runs the global script controls how frequently the sequence is run. The schedule's script is

```
RUN FTP_Sequence
```

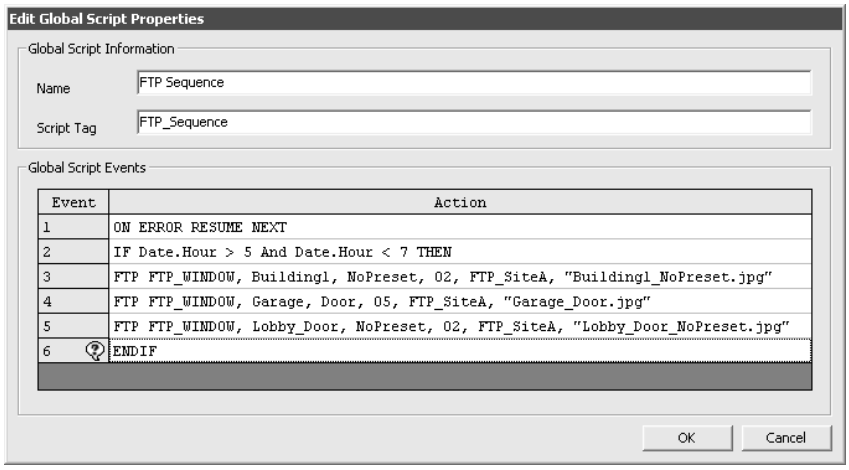


Figure 274. FTP sequence

TIPS:

- If you are going to take regular, scheduled FTP image captures, it is recommended that you employ a dedicated FTP computer that is isolated from routine daily operations. This ensures that an operator will not shut down the client by mistake, which would cause FTP captures to fail.
- To control FTP captures, define objects that are dedicated to FTP. Create a dedicated user account that is always logged in. If the FTP commands are in a schedule, make the dedicated user the recipient of the schedule. Add a window to the dedicated client that is only used for FTP image capture. These steps ensure that you know exactly where the image capture is taking place, as well as preventing operators from being interrupted in their routine duties.

DELETE AN FTP SITE

Deleting an FTP site is irreversible. If you delete an FTP site and then change your mind, you must add it as a new FTP site.

1. Navigate the Object Browser to [project name] > FTP Sites. In the right pane, right-click the FTP site you want to delete and select Delete from the pop-up menu. The Confirm dialog box opens.
2. If you are sure you want to delete the FTP site, click Yes. The selected FTP site is deleted and the Confirm dialog box closes. The deleted FTP site disappears from the Object Browser.

Database Utilities

VMX300(-E) provides the following database utilities:

- Backup, which creates a backup of the server database.
- Restore, which restores a backup of the server database.

BACKUP A DATABASE

Use the Backup utility to create a backup of the server database and to save backup databases to alternative media (such as a CD).

NOTE: The Backup utility backs up the server database only. The Backup utility does not back up maps, workspace files, driver databases, archive server databases, or the client database.

1. Click Tools > Database Utilities > Backup. The Backup Database dialog box opens.

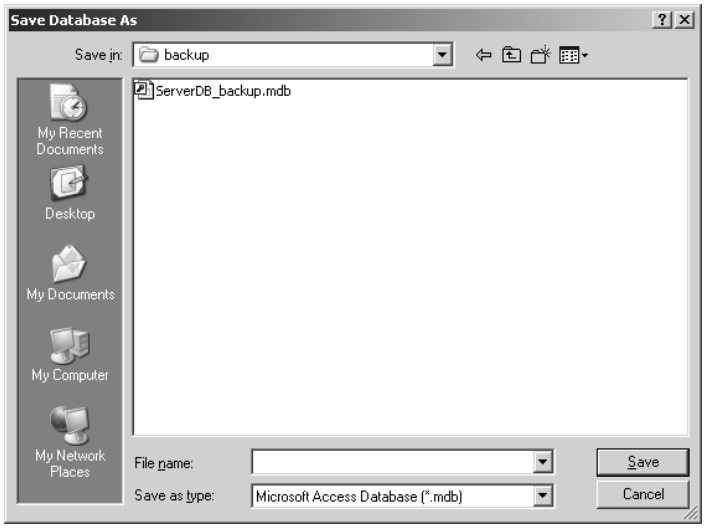


Figure 275. Backup Database Dialog Box

2. Type an appropriate filename, and then navigate to a new folder location. Name the file with a recognizable filename, and save the file in a unique folder location that is separate from the backup files that are automatically generated by VMX300(-E). If you have to restore a database it will be very important to select the correct backup file.

3. Click Save.

RESTORE A DATABASE

NOTE: If you have to restore a database, it is very important to select the correct backup file. VMX300(-E) creates an automatic database backup file every time you launch the server in run mode, but you should be using the Backup utility to make backup files on a regular basis, rather than relying on these backup files.

To restore a database from a backup:

1. Click Tools > Database Utilities > Restore. The Restore Database dialog box opens.

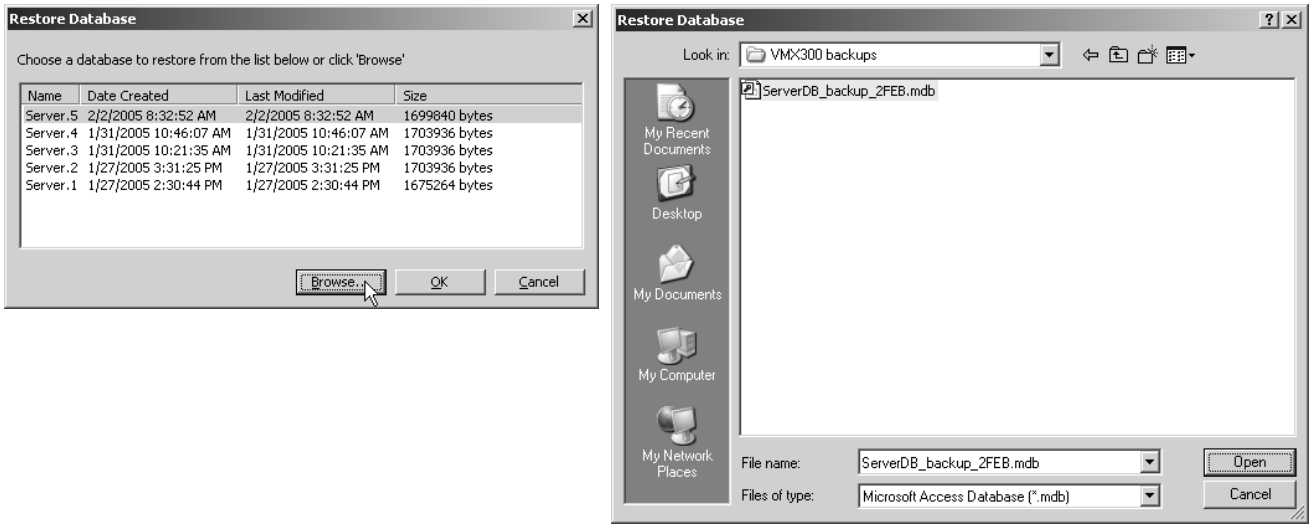


Figure 276. Restore Database Dialog Box

2. Click Browse to navigate to the folder containing the backup file that you have created. Click the backup you want to restore, and then click Open. Click OK in the Restore Database dialog box. A confirmation message box appears.
3. Click Yes. The database is restored and you are reminded to restart the server. Click OK to close the reminder dialog box.
4. To access the restored version of the database, shut down the server and relaunch it.

System Logs

VMX300(-E) maintains a log of system activities for diagnostic purposes. Activities fall into three categories:

- **System:** Background activities that are not seen by users, such as opening sockets and compiling scripts.
- **Administrative:** Server configuration mode activities.
- **Operational:** Activities initiated in the client, such as operator-initiated changes to a device's controls or acknowledgement of an alarm or event.

You can filter out categories of activity that you do not want displayed.

Logs are stored in text (.txt) files, a new one for each day the server is run. The VMX300(-E) server provides a log viewer to locate and view log files. The log viewer displays one day of logged activities at a time. You can step forward and backward through logs without exiting and reopening the viewer.

Each log entry has the following information:

- **Time:** The time of day the activity took place
- **Category:** System, Administrative, or Operational
- **Owner:** The initiator of the activity
- **Message:** Details of the activity

VIEW SYSTEM LOGS

1. Navigate the Object Browser to [project name] > Logs > [year] > [month]. In the right pane, double-click the day whose log you want to view, or right-click the day and select View from the pop-up menu. The Log Viewer window opens. The date of the log appears at the center, top of the window.

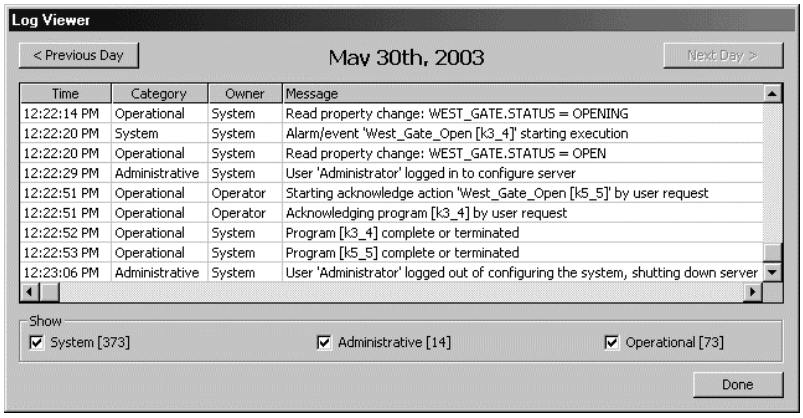


Figure 277. Log Viewer Window

2. **Filter:** Categories are listed at the bottom of the window, with the number of entries in each category to the right of the category. To filter out entries of a particular category, clear the check box to its left.
3. **Previous/next:** To view the next log, click Next. To view the previous log, click Previous.
4. When you have finished viewing the logs, click Done. The Log Viewer window closes.

TIP: Double-click the Log Viewer title bar to maximize the dialog box. Double-click again to restore the window.

Appendix

ADJUSTING THE DISPLAY

ADJUST THE OBJECT BROWSER DISPLAY

When the Object Browser is docked, you can adjust its width. Position the pointer over the border that abuts the map viewport. When the pointer changes to a double-headed resizing pointer, drag the border to the right or left. As you change the width of the Object Browser, the map viewport automatically adjusts to fill the available space.

You can also drag the vertical bar in the center of the Object Browser to adjust the relative size of the two panes.

Undock the Object Browser

You can undock the Object Browser as follows:

1. Click the Object Browser title bar and hold the mouse key down.
2. Drag the pointer away from the title bar. A gray rectangle surrounding the pointer appears.
3. Release the mouse button. The Object Browser moves to the space defined by the gray rectangle.

Alternatively, right-click anywhere in the Object Browser window and select Undock from the pop-up menu.

TIP: When the Object Browser is undocked and the Configuration window is restored down, you can move the Object Browser outside the Configuration window, to the desktop.

Dock the Object Browser to the Left

You can re-dock the Object Browser in its default position to the left of the map viewport as follows:

1. Click the Object Browser title bar and hold the mouse key down.
2. Drag the pointer to the extreme left of the Configuration window. A gray rectangle the full height of the map viewport snaps to the left edge of the Configuration window.
3. Release the mouse button. The Object Browser moves to the space defined by the gray rectangle.

Alternatively, right-click anywhere in the Object Browser window and select Dock Left from the pop-up menu.

Dock the Object Browser to the Right

You can dock the Object Browser to the right of the map viewport as follows:

1. Click the Object Browser title bar and hold the mouse key down.
2. Drag the pointer to the extreme right of the Configuration window. A gray rectangle the full height of the map viewport snaps to the right edge of the Configuration window.
3. Release the mouse button. The Object Browser moves to the space defined by the gray rectangle.

Alternatively, right-click anywhere in the Object Browser window and select Dock Right from the pop-up menu.

RESIZE WINDOWS

Many windows can be resized, including the Configuration window, the Object Browser window, and some dialog boxes.

You cannot resize a window when it is maximized, that is, when it fills the entire screen. If you want to resize a window that is maximized, first reduce it by clicking the Restore Down button in the right corner of the title bar, or double-click the title bar. In order to resize the Object Browser, you must undock it first.

Resize windows as follows:

- Change the width: Point to the left or right window border. When the pointer changes into a horizontal double-headed arrow, drag the border to the right or left.
- Change the height: Point to the top or bottom window border. When the pointer changes into a vertical double-headed arrow, drag the border up or down.
- Change the width and height simultaneously: Point to a corner of the window border. When the pointer changes into a diagonal double-headed arrow, drag the border in any direction.

NOTE: If the pointer does not change when it's positioned over a window border, then that window cannot be resized.

REPOSITION WINDOWS

You can reposition the Configuration window when it is restored down, the Object Browser when it is undocked, or any dialog box as follows:

1. Position the pointer over the window's title bar.
2. Click the left mouse button and hold it down.
3. Drag the window to the desired location.
4. Release the mouse button.

POP-UP MENUS

In many contexts, right-clicking an item opens a pop-up menu of actions you can apply to the item. Table AQ lists the contexts in which pop-up menus are available and the commands they contain.

Table AQ. Pop-up Menu Commands

ITEM	LOCATION OF ITEM	COMMANDS
Object Browser	n/a	Object Browser docking commands
Project	Root of Object Browser	Edit; Object Browser docking commands
Object type	Object Browser left pane	Add New; Object Browser docking commands
Object	Object Browser either pane	Edit, Cut, Copy, Paste, Paste Many, Delete; Object Browser docking commands
Canvas	Object Browser right pane	All Object commands, plus Move Up, Move Down
Named view	Object Browser right pane	All Object commands, plus Update
Device	Object Browser either pane	All Object commands, plus Local Settings
Device write property	Object Browser right pane	Edit Interlock; Object Browser docking commands
Log	Object Browser right pane	View; Object Browser docking commands
Device icon	Map viewport	Edit, Local Settings, Move, Scale and Rotate, Remove
Device label	Map viewport	Edit Label, Move, Scale, Remove
Alarm icon	Map viewport	Edit, Move, Scale, Remove
Alarm label	Map viewport	Edit Label, Move, Scale, Remove
Hotlink	Map viewport	Edit, Delete
Hotlink vertex	Map viewport	Delete Vertex, Insert Vertex
Label	Map viewport	Edit Label, Move, Scale, Remove

USE COPY AND PASTE TO CREATE A NEW OBJECT

The Copy and Paste options are useful for creating an object that has similar attributes to an existing object. For example, if you want to create a prompt that has the same button set-up as an existing prompt, you can save yourself from having to re-create the buttons by using Copy and Paste to copy the prompt, then editing the prompt information and text.

NOTE: Copy and Paste cannot be used for maps, hotlinks, named views, device drivers, and certain devices.

1. Navigate the Object Browser to display the object you want to copy in the right pane of the Object Browser.
2. Right-click the object and select Copy from the pop-up menu.
3. Right-click anywhere in the right pane of the Object Browser and select Paste from the pop-up menu. A copy of the selected object is created and its name appears in the Object Browser. The new object is named "Copy of [name of original object]".
4. Edit the new object as desired.

USE COPY AND PASTE MANY TO CREATE MULTIPLE NEW OBJECTS

To create more than one new object based on an existing object, use the Copy and Paste Many options. Paste Many simultaneously creates as many copies of an object as you want. The new objects are sequentially named "[base name]*i*", where [base name] is a name you specify, and *i* is a positive integer. The objects differ in name only; all their other attributes are identical.

Copy and Paste Many are particularly useful when configuring a new server, because they allow you to create many similar objects very quickly. For example, if you are setting up many similarly configured clients, you can save time by creating one client with the desired custom windows, then use Copy and Paste Many to make multiple copies of the client, each configured with the same windows.

Paste Many is also useful for creating users when you are first configuring a new server.

NOTE: Copy and Paste Many cannot be used for canvases, maps, hotlinks, named views, device drivers, and certain devices.

1. Navigate the Object Browser to display the object you want to copy in the right pane of the Object Browser.
2. Right-click the object and select Copy from the pop-up menu.
3. Right-click anywhere in the right pane of the Object Browser and select Paste Many from the pop-up menu. The Paste Many dialog box opens.

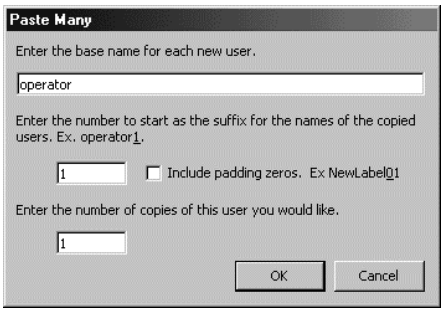


Figure 278. Paste Many Dialog Box

4. **Base name:** Type the base name you want to use.
5. **Start number:** Type the start integer for numbering the new objects.
6. **Padding zeroes:** If you want the numbering to always have the same number of digits in it, select Include padding zeroes. For example, if you create twelve copies of something, the first nine will be numbered 01, 02, 03, . 09, instead of 1, 2, 3, . 9. This keeps the objects ordered.
7. **Number of copies:** Type the number of new objects you want to create.
8. Press OK. The Paste Many dialog box closes and the new objects are created. The names of the new objects appear in the Object Browser.
9. Edit the new objects as desired.

TIP: You can also create multiple objects based on a particular object by using Paste multiple times. In this case, the new objects will be sequentially named "Copy (i) of [name of copied object]", where *i* is an integer.

PRODUCT WARRANTY AND RETURN INFORMATION

WARRANTY

Pelco will repair or replace, without charge, any merchandise proved defective in material or workmanship **for a period of one year** after the date of shipment.

Exceptions to this warranty are as noted below:

- Five years on FT/FR8000 Series fiber optic products.
- Three years on Genex® Series products (multiplexers, server, and keyboard).
- Three years on Camclosure® and fixed camera models, except the CC3701H-2, CC3701H-2X, CC3751H-2, CC3651H-2X, MC3651H-2, and MC3651H-2X camera models, which have a five-year warranty.
- Two years on standard motorized or fixed focal length lenses.
- Two years on Legacy®, CM6700/CM6800/CM9700 Series matrix, and DF5/DF8 Series fixed dome products.
- Two years on Spectra®, Esprit®, ExSite™, and PS20 scanners, including when used in continuous motion applications.
- Two years on Esprit® and WW5700 Series window wiper (excluding wiper blades).
- Eighteen months on DX Series digital video recorders, NVR300 Series network video recorders, and Endura™ Series distributed network-based video products.
- One year (except video heads) on video cassette recorders (VCRs). Video heads will be covered for a period of six months.
- Six months on all pan and tilts, scanners or preset lenses used in continuous motion applications (that is, preset scan, tour and auto scan modes).

Pelco will warrant all replacement parts and repairs for 90 days from the date of Pelco shipment. All goods requiring warranty repair shall be sent freight prepaid to Pelco, Clovis, California. Repairs made necessary by reason of misuse, alteration, normal wear, or accident are not covered under this warranty.

Pelco assumes no risk and shall be subject to no liability for damages or loss resulting from the specific use or application made of the Products. Pelco's liability for any claim, whether based on breach of contract, negligence, infringement of any rights of any party or product liability, relating to the Products shall not exceed the price paid by the Dealer to Pelco for such Products. In no event will Pelco be liable for any special, incidental or consequential damages (including loss of use, loss of profit and claims of third parties) however caused, whether by the negligence of Pelco or otherwise.

The above warranty provides the Dealer with specific legal rights. The Dealer may also have additional rights, which are subject to variation from state to state.

If a warranty repair is required, the Dealer must contact Pelco at (800) 289-9100 or (559) 292-1981 to obtain a Repair Authorization number (RA), and provide the following information:

1. Model and serial number
2. Date of shipment, P.O. number, Sales Order number, or Pelco invoice number
3. Details of the defect or problem

If there is a dispute regarding the warranty of a product which does not fall under the warranty conditions stated above, please include a written explanation with the product when returned.

Method of return shipment shall be the same or equal to the method by which the item was received by Pelco.

RETURNS

In order to expedite parts returned to the factory for repair or credit, please call the factory at (800) 289-9100 or (559) 292-1981 to obtain an authorization number (CA number if returned for credit, and RA number if returned for repair).

All merchandise returned for credit may be subject to a 20% restocking and refurbishing charge.

Goods returned for repair or credit should be clearly identified with the assigned CA or RA number and freight should be prepaid. Ship to the appropriate address below.

If you are located within the continental U.S., Alaska, Hawaii or Puerto Rico, send goods to:

Service Department
Pelco
3500 Pelco Way
Clovis, CA 93612-5699

If you are located outside the continental U.S., Alaska, Hawaii or Puerto Rico and are instructed to return goods to the USA, you may do one of the following:

If the goods are to be sent by a COURIER SERVICE, send the goods to:

Pelco
3500 Pelco Way
Clovis, CA 93612-5699 USA

If the goods are to be sent by a FREIGHT FORWARDER, send the goods to:

Pelco c/o Expeditors
473 Eccles Avenue
South San Francisco, CA 94080 USA
Phone: 650-737-1700
Fax: 650-737-0933

REVISION HISTORY

Manual #	Date	Comments
C1553M	8/04	Original version.
C1553M-A	3/05	Revised to reflect software changes (as a result of ECO 04-10212).
C1553M-B	4/05	Revised Table B (Digital Video Stream Settings) and revised the notes on using special ASCII characters in scripts and expressions (Table AI Serial Output Device Write Property).

Worldwide Headquarters
3500 Pelco Way
Clovis, California 93612 USA

USA & Canada
Tel: 800/289-9100
Fax: 800/289-9150

International
Tel: 1-559/292-1981
Fax: 1-559/348-1120

www.pelco.com

ISO**9001**