The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

© 2014 Moxa Inc. All rights reserved.

Trademarks

The MOXA logo is a registered trademark of Moxa Inc.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

[www.moxa.com/support](http://www.moxa.com/support)

<table>
<thead>
<tr>
<th>Moxa Americas</th>
<th>Moxa China (Shanghai office)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toll-free: 1-888-669-2872</td>
<td>Toll-free: 800-820-5036</td>
</tr>
<tr>
<td>Tel: +1-714-528-6777</td>
<td>Tel: +86-21-5258-9955</td>
</tr>
<tr>
<td>Fax: +1-714-528-6778</td>
<td>Fax: +86-21-5258-5505</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Moxa Europe</th>
<th>Moxa Asia-Pacific</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tel: +49-89-3 70 03 99-0</td>
<td>Tel: +886-2-8919-1230</td>
</tr>
<tr>
<td>Fax: +49-89-3 70 03 99-99</td>
<td>Fax: +886-2-8919-1231</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Moxa India</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tel: +91-80-4172-9088</td>
</tr>
<tr>
<td>Fax: +91-80-4132-1045</td>
</tr>
</tbody>
</table>
Table of Contents

1. Introduction ........................................................................................................... 1-1
   Software Components ............................................................................................................. 1-2
2. System Initialization ............................................................................................... 2-1
   Overview: Initializing User Settings .................................................................................. 2-2
3. Configuring Serial Interfaces .................................................................................. 3-1
   Overview .............................................................................................................................. 3-2
   Setting a Serial Interface Mode .......................................................................................... 3-2
4. Enabling Embedded Filters ..................................................................................... 4-1
   Enhanced Write Filter .......................................................................................................... 4-2
   Overview .............................................................................................................................. 4-2
   Enabling Enhanced Write Filter .......................................................................................... 4-3
   Committing Data and/or Disabling EWF ........................................................................... 4-4
   File-Based Write Filter ........................................................................................................ 4-5
   Overview .............................................................................................................................. 4-5
   Configuring File-Based Write Filter ................................................................................... 4-5
   Excluding Files from FBWF Protection ................................................................................ 4-7
   Managing Temporary Files Cached in the Overlay ........................................................... 4-9
5. Moxa Diagnostic Package ....................................................................................... 5-1
   Installing the Moxa Diagnostic Utility .............................................................................. 5-2
   Using the Moxa Diagnostic Utility ..................................................................................... 5-3
   Installing CrystalDiskInfo .................................................................................................... 5-5
6. Moxa Hot Swap Package ....................................................................................... 6-1
   Installing the Hot-Swap Software Package ....................................................................... 6-2
   Configuring the Hot-Swap Utility ...................................................................................... 6-3
7. Moxa SynMap Package .......................................................................................... 7-1
   The Synmap™ Virtualization Layer: Full Interoperability with Any Moxa Device .......... 7-2
   Overview .............................................................................................................................. 7-2
   The Synmap Design Concept ............................................................................................... 7-2
   Moxa Synmap OIDs List ....................................................................................................... 7-3
   Installing the Synmap Virtualization Layer .......................................................................... 7-5
   Installing and Using an NMS ............................................................................................... 7-5
   Installing Moxa MxView ..................................................................................................... 7-6
   Basic Configuration of MxView ........................................................................................... 7-7
   Loading the Synmap MIB File .............................................................................................. 7-10
   Using Synmap OIDs to Control the TC-6110 ....................................................................... 7-13
8. Examples .................................................................................................................. 8-1
   Setting a Serial Interface .................................................................................................... 8-2
   Digital Input/Output .............................................................................................................. 8-3
   LED Indicators ..................................................................................................................... 8-4
   Button Scripts ...................................................................................................................... 8-5
   PCIe Reset ............................................................................................................................. 8-6
9. System Backup ....................................................................................................... 9-1
   Overview .............................................................................................................................. 9-2
   Setting Up the Recovery Environment ............................................................................... 9-2
   Setup of a Factory Default Recovery Image ........................................................................ 9-2
   Step 1: Prepare the USB drive ............................................................................................ 9-2
   Step 2: Setting the BIOS to Boot via USB .......................................................................... 9-4
   Step 3: How to Perform a System Recovery ....................................................................... 9-6
   Step 4: Reset the BIOS to its Original State ....................................................................... 9-8
   Creating a Custom System Image ....................................................................................... 9-10
A. Moxa SynMap OID Table ....................................................................................... A-1
   Moxa SynMap OID Table ..................................................................................................... A-2
   HOST RESOURCE OID Table ............................................................................................ A-4
Thank you for buying Moxa’s V2616A panel computer. It comes with the Windows 7 Embedded software platform, providing a simple and familiar development environment for various industrial applications.

- **Software Components**
Software Components

Refer to the following content for the software components of the Windows Embedded Standard 7 pre-installed on the V2616A computes.

Windows Embedded Standard 7
Core OS:
• 32-bit support
• Remote Client
• Remote Procedure Call
Applications and Services Development:
• .Net Framework 3.5
• Remote Desktop Protocol 7.1
• COM OLE Application Support
• COM+ Application Support
• MSMQ
Internet Services:
• Internet Explorer 8.0
• IIS 7.0
File Systems and Data Store:
• Windows Data Access Components
• Windows Backup and Restore
Diagnostics:
• Common Diagnostic Tools
• Problem Reports and Solutions
Fonts: Chinese (Trad. and Simp.), Japanese, Korean, Western, Middle Eastern, South East Asian, and South Asian Fonts
Graphics and Multimedia:
• MPEG DTV-DVD Audio Decoder (MPEG-2, AAC)
• MPEG Layer-3 Audio Codecs(MP3)
• MPEG4 Decoder
• Windows Media Video VC-1 (WMV) Codecs
• DirectX and Windows Device Experience
• Windows Media Player 12
International:
• IME Simplified Chinese Support
• IME Traditional Chinese Support
• IME Japanese Support
• IME Korean Support
Management:
• Group Policy Management
• Windows Management Instrument (WMI)
• Windows Update
Networking:
- Extensible Authentication Protocol (EAP)
- Internet Authentication Service
- Telnet Server
- Bluetooth
- Domain Services
- Network Access Protection
- Network and Sharing Center
- Quality of Service
- Remote Access Service (RAS)
- Telephony API Client
- Windows Firewall
- Wireless Networking

Security:
- Credential Roaming Service
- Credentials and Certificate Management
- Windows Authorization Manager (AZMAN)
- Windows Security Center
- Active Directory Rights Management
- Security Base
- Encrypted File System (EFS)

Embedded Features:
- Enhanced Write Filter (EWF)
- File-Based Write Filter (FBWF)
- Message Box Default Reply
- Registry Filter
- WSDAPI for .NET

Embedded Self-Health Diagnostic Software: SNMP-based remote scripting layer for monitoring, reporting, and control
This chapter describes how to initialize the system settings on V2616A computer when you boot up the computer at first time.

The following topics are covered in this chapter:

- **Overview: Initializing User Settings**
Overview: Initializing User Settings

Like most laptop computer, you need to type a user name to create your user account to enable the embedded computer to work, follow the steps below:

1. When you boot the embedded computer for the first time, you need to enter a user name for this computer.

2. Type the password, retype the password. In addition, you may also type a password hint in case you forget your password. If you do not want to set the password, leave it blank and click Next.
3. Select the windows update option.

4. Select computer’s current location. Windows will automatically apply the correct network settings based on the network’s location.
5. Now you can start to use V2616A embedded computer.
This chapter describes how to configure the serial interface on the V2616A computer.

The following topics are covered in this chapter:

- **Overview**
- **Setting a Serial Interface Mode**
Overview

The V2616A supports different serial modes: **RS232**, **RS485-2-wire** and **RS422/RS485-4-wire**. These modes can be configured as COM1 and COM2.

Setting a Serial Interface Mode

Follow these steps to change serial interface mode.

1. Open device manager and right-click the **MOXA CP-102E Series (PCI Express Bus)**.

2. Select **Properties**.
3. Change to **Ports Configuration** tab, and select the COM port which you want to change its serial interface (Ex. COM1) and then click **Port Setting**.

4. Select the **Interface** drop down box, and then select the serial interface you want to set.

5. Make sure the serial interface has been changed successfully.
Enabling Embedded Filters

This chapter describes how to operate the embedded enabling features on the V2616A embedded computer.

The following topics are covered in this chapter:

- **Enhanced Write Filter**
  - Overview
  - Enabling Enhanced Write Filter
  - Committing Data and/or Disabling EWF

- **File-Based Write Filter**
  - Overview
  - Configuring File-Based Write Filter
  - Excluding Files from FBWF Protection
  - Managing Temporary Files Cached in the Overlay
Enhanced Write Filter

Overview

Enhanced Write Filter (EWF) provides a means for protecting a volume from unauthorized writes by making the main OS drive a write-protected volume, effectively making the system a read-only system for most users. This gives much stronger protection against malicious computer code like trojans, worms, and viruses.

Enhanced Write Filter (EWF) allows Windows 7 users to protect their all information on their storage drive from permanent changes of any sort, at the lowest level of hardware protection available: the bit level. EWF allows the operating system (OS) to boot from the hard disk, but protects the system by creating a virtual file system called an overlay. All writes to an EWF-protected volume (the hard disk, in Fig. 1) are only recorded on this virtual overlay (the EWF Volume, in Fig. 1), which is stored independently in random access memory (RAM). Because EWF does not write data directly to the hard disk—instead, only recording system writes to this virtual RAM overlay—any data that is “written” during system operation will disappear upon the next re-boot. This approach allows the system to operate as if it is writeable when in reality all OS and user-space file systems are stored in a permanent, read-only state. If desired, the data written to the overlay may be committed to the protected volume, but this requires additional setup and permissions that can only be granted by the administrator. Refer to the following figure (from Microsoft) for an overview of the EWF structure.

For more details about EWF configuration and usage, you may:

Visit Microsoft’s EWF Volume Configuration help pages.

Visit Microsoft’s EWF overview on the official Microsoft EWF help pages.

Visit Microsoft’s detailed description of EWF modes on the EWF help pages.

Visit Microsoft’s detailed description of the EWF API.

For the EWF commands, refer to the MSDN web site:

http://msdn.microsoft.com/en-us/library/ms940853%28v=winembedded.5%29.aspx
Enabling Enhanced Write Filter

Follow these steps to enable the Enhanced Write Filter.

1. To open the EWF control dialog, open the system tray (located in the lower right corner of the desktop) and right-click on the padlock icon.

2. Select the volume you wish to enable write-protection on by selecting the partition (A) in the Volume Information dialog, and then pressing the Configure button (B) in the lower left section of the dialog.

3. After opening the configuration dialog, choose to enable Enhanced Write Filter on your drive volume by selecting Enable from the Pending command dialog and then clicking OK to close the dialog.
4. Reboot the system.
5. After logging in to the desktop environment, open the system tray (located in the lower right corner of the desktop) and check to verify that the padlock icon now shows the drive volume is locked down with EWF.

**Committing Data and/or Disabling EWF**

When EWF is enabled on a drive users will need to go through a special process to write any data to the hard drive. Writing data to the drive in this situation is called a Commit, and users must be given administrator privileges to be able to do so.

1. Open the EWF control dialog by right-clicking on the padlocked drive in the system tray (located in the lower right corner of the desktop).

2. Once the EWF control dialog is open, select the drive you wish to operate and click on the Configure button in the lower left corner. This will open the EWF Configuration page.
3. Once the EWF control dialog is open, select the drive you wish to operate from the upper window of the dialog, and then click on the Pending Command drop-down menu just beneath. Here, you will see four choices:

No Command: Does nothing.
Disable: This disables EWF on the selected drive. Be aware that the system will automatically reboot if you select this command.
Commit: This writes all current changes to the system data to the hard drive; any changes that have been made to the system settings.
Commit and Disable Live: This writes all current data and changes to the system, and also turns off EWF on the selected drive (so that all future data and system changes will also be committed to the drive, as well). Selecting this option will NOT automatically reboot your system.

For more detailed descriptions of these commands, please refer to the Microsoft website shown below:

File-Based Write Filter

Overview

**File-Based Write Filter** (FBWF) is similar to EWF, but is enforced at the file level rather than at the hardware (bit) level. This means it is slightly less secure, but this allows it to provide more user features than is possible with EWF. From Microsoft:

*File-Based Write Filter (FBWF) allows the Windows Embedded platform to maintain the appearance of read and write access on write-sensitive or read-only storage. FBWF makes read and write access transparent to applications.*

*Writing to storage media may be undesirable or impossible in embedded devices. FBWF redirects all writes targeted for protected volumes to a RAM cache called an overlay. Used in this context, an overlay is similar to a transparency overlay on an overhead projector. Any change made to the overlay affects the picture as seen in the aggregate, but if the overlay is removed, the underlying picture remains unchanged.*

One of FBWF’s more advanced features allows the user to specify a directory where data may be more conveniently written to the data drive than is possible with EWF.

Configuring File-Based Write Filter

Follow these steps to enable the File-Based Write Filter. Keep in mind that, while FBWF and EWF may both be enabled on the same machine; FBWF can not protect a volume also protected by EWF. Similarly, EWF can not protect a volume also protected by FBWF.
1. To open the FBWF overview window, open the system tray (located in the lower right corner of the desktop) and right-click on the padlock icon.  

   **NOTE:** When disabled, the icons for EWF and FBWF are identical. After the dialog opens be sure to verify which write filter you are working with: FBWF, or EWF.

2. When the overview window opens, you will receive a quick report on the current FBWF configuration. The diagram at right shows what it will look like before it is enabled. To continue with the setup, click on the Configure button.

3. The FBWF configuration window is considerably more complicated than the EWF setup. To enable FBWF protection on your main storage drive, you will need to enable the filter by ticking Filter state enabled (A) and Cache pre-allocation enabled (B). Next, select the drive you want to protect from the Volume Configuration menu (C) and then click on the Protect button (D). Finally, click on Apply (E), or OK to set the FBWF configuration.

   Cache compression may be used on the overlay cache to minimize the amount of memory used. Cache compression decreases performance when accessing protected volumes, and cannot be used with pre-allocation.

   Cache pre-allocation sets the memory space available for the overlay cache at the system’s start, instead of adjusting it as needed. It cannot be used with cache compression.

   The cache threshold specifies the amount of memory that can be used by the write filter for the overlay cache. The default value and size limits for the overlay cache vary by operating system.

4. Reboot the system.
5. Once again, open the system tray (located in the lower right corner of the desktop) and check to verify that the padlock icon now shows you have enabled FBWF. The icon should have changed to become a padlock displaying the number 10, as shown in the figure at right.

Excluding Files from FBWF Protection

1. Click on the FBWF icon (in the desktop systray) to open the Overview dialog. Click on Configure to switch to the configuration interface.

2. Click on the Exclusion List tab. Make sure the correct drive volume is shown in the dropdown menu labeled Volume Name; if not, select the correct volume from the dropdown menu.

   Next, you must select the file path you wish to exclude from FBWF protection; this will allow the drive to write to the selected files and directories, so be careful. You may indicate an entire section of the file tree by selecting an entire file path, or you may select individual files.

   To select individual files, click on the Browse button (marked with ellipses, in the lower right corner, as shown at right). This will open a Windows Explorer interface.
3. Navigate to the file(s) you wish to exclude from FBWF protection, select the file, and then click **Open** to enter the path into the exclusion dialog; this will exit the Windows Explorer interface and return you to the **Exclusion List** interface shown in step 2.

4. You should now see the file or file path you selected for exclusion listed in the **Add Path** dialog, at the bottom of the **Exclusion List** tab. Click the add button (++) to add the path or file to the exclusion list.

5. After adding a file or path to the exclusion list, you should see it listed in the **Path** window. If the file does not appear, then it has not yet been added.

6. Reboot the system for the changes to take effect.
Managing Temporary Files Cached in the Overlay

1. In the Cache Content tab you will see all the files currently cached in the RAM overlay, with three commands you may execute:
   - **Commit** will save a file from the cache to permanent storage, deleting the file from the overlay and overwriting the original. Restore will return the file to its original state, removing it from the overlay cache and discarding the changes that caused it to be added to the cache.
   - Add to exclusion list adds the file to the exclusion list after the next restart. Because this makes the file read-only, if it is executed on the wrong file it may render your system or particular applications inoperable.

2. The most common usage of the Cache Content list will likely be to permanently write content to the hard drive. To do this, select the file you wish to write to permanent memory and click on the commit button. This will delete the file from the cached overlay and replace the current file in permanent storage with the modified cache file.
   - Users should understand that if they commit a configuration or application file, they will be permanently altering the setup and/or performance of the application or system. If a core system or configuration file is committed in a corrupt or intermediate state, then this will render your system inoperable.

To get more details about FBWF configuration and usage, you may consult the Microsoft help file that comes with your computer, or:

Go to Microsoft’s FBWF Installation and Configuration help pages.

Go to Microsoft’s FBWF overview on the official Microsoft FBWF help pages.

Go to Microsoft’s detailed description of FBWF features on the FBWF help pages.

Go to Microsoft’s detailed description of the FBWF API.
This chapter describes the software package for users to monitor the system status of V2616A computer.

The following topics are covered in this chapter:

- Installing the Moxa Diagnostic Utility
- Using the Moxa Diagnostic Utility
- Installing CrystalDiskInfo
Installing the Moxa Diagnostic Utility

To install the Moxa Diagnostic Utility, follow the steps below.

1. Double click **mxDiagnosticTool.msi** in the **Utility** folder located on your software DVD under `utility\mxdiagnostic\`.

2. Click **Next** to continue.

3. Select the folder you want to install the package, or simply click **Next** to continue if you want to use the default folder.

4. Click **Next** to affirm the installation.

5. After the installation concludes, click **Close**.
Using the Moxa Diagnostic Utility

The steps below describe how to use the Moxa diagnostic utility. This diagnostic tool allows users to directly
view and monitor the performance stats of all low-level system processes, like CPU frequency, memory usage,
CPU and system temperatures, and so forth. Moxa’s diagnostic utility monitors these processes over the
Windows API, and its warnings and alarms are confined to the application window. However, users may add
remote or desktop notifications using SNMP and an NMS suite (of which free software versions are available).

The Moxa Diagnostic Utility has five tabs: System Temperature, which monitors CPU and the computer’s
average internal temperature; System Voltage, which monitors voltage levels for the CPU and motherboard
chipset; System Frequency, which monitors clock frequencies for the CPU and memory; System Resources,
which monitors usage stats for RAM and CPU; and Settings, which allows you to set the polling frequency and
file-tree path to the log. The steps below describe how open the utility, and the use of each tab.

1. Open the Windows Start Menu and click on the Moxa Predictive
   Maintenance Diagnostic Tool, found under <All Programs>\Moxa\Moxa
   Predictive Maintenance Diagnostic Tool\.

2. After opening the diagnostic tool, you will see the five subsystem tabs. The first tab, System
   Temperature, shows the average temperature within the chassis and the temperature of the CPU.
   You may also configure an alarm threshold for each. If either of these temperatures rises above the
   threshold, the diagnostic utility will display a warning. At the same time, all information will be logged
to the file, according to the frequency of the polling interval.

3. To change the threshold value, double-click anywhere in the Threshold Value field.

4. After you enter the new value, press Enter. A confirmation dialog will pop up; click Yes to confirm this
   is the value you wish to set.
5. The **System Voltage** tab displays the current system voltages. Consult your CPU and chipset manufacturer to determine what each value represents.

6. Change to **System Frequency** tab to get current clock speed for the CPU and RAM.

7. Change to **System Resource** tab to see how much memory is being used on your permanent storage drive and RAM.

8. In the **Settings** tab you can set the polling interval and path for the log file.

9. To save the settings, click **Apply**
Installing CrystalDiskInfo

To install Moxa's storage drive health diagnostic utility, follow these steps.

1. Locate to the software CD and click `CrystalDiskInfo6_1_9a-en.exe`.
2. Click **Next**.
3. Select **I accept the agreement** and click **Next**.
4. Click **Next**.
5. Click **Next**.

6. Click **Next**.

7. Click **Install**.
8. Click **Finish**.

Put the shortcut to **startup** to execute the program when system boot up
This chapter describes the software package that users may use to implement, control, and monitor hot-swappable drives.

The following topics are covered in this chapter:

- Installing the Hot-Swap Software Package
- Configuring the Hot-Swap Utility
Installing the Hot-Swap Software Package

To use the Moxa Disk Hot-Swap utility on the V2616A computer, you need to install the Moxa Disk Hot-Swap driver and user-space utility. Follow these steps to install hot-swap software package.

1. Double click mxDiskHotSwap.msi under Utility folder under <software DVD>\utility\mxhtsp\.
2. Click Next to continue.

3. Click Next

4. Click Next
5. Click **Close** to complete the package installation

Configuring the Hot-Swap Utility

In this section you will learn how to configure the hot-swap utility for custom actions and log features.

1. Double click on the **Moxa Hot Swap Function For Disk Drive** under the Windows Start button menu.

2. The tray icon will load in the system tray, and it will start to monitor the disk status when new disk is inserted or current disk is removed.

If the log option is enabled, all actions and notifications will be logged under

C:\Program Files\Moxa\Moxa Hot Swap Function For Disk Drive\program\
3. To reconfigure logging and other features, right-click the icon and select **Settings**.

4. You will see currently mounted drives listed along with their storage capacity and free space. To edit the settings for a specific drive, click on it to select it from the list and then click **Edit Setting**.

5. In the settings dialog there are four tabs that allow you to specify actions that will take place whenever a button on the module is pressed (**Button Pressed**), a module is plugged in (**Disk Plugged**) or unplugged (**Disk unplugged**), and a certain memory usage is reached (**Disk Usage**).

6. First, let’s look at the the **Button Pressed** tab: here, you can associate a program to be executed whenever the button on the face of the computer is pressed; otherwise, the default action will be to unmount both the drives (in slot A and B) and to blink the LED three times per second.
7. In the **Disk Plugged** tab, you can set a custom notification or use the default notification whenever a drive is first plugged in. To specify a custom notification, use **Browse** to select your script from the file tree.

8. In the **Disk Unplugged** tab, you may set a custom notification or use the default notification whenever a drive is unplugged. To specify a custom notification, use **Browse** to select your script from the file tree.

9. In the **Disk Usage** tab, you may set a custom notification or use the default notification whenever the memory drive is filled to a certain capacity. To specify a custom notification, use **Browse** to select your script from the file tree.

10. To save your changes, click **Apply** and then click **Yes** to permanently save the settings.
This chapter describes the software package for users to easily control and monitor the V2616A computers.

The following topics are covered in this chapter:

- **The Synmap™ Virtualization Layer: Full Interoperability with Any Moxa Device**
  - Overview
  - The Synmap Design Concept
  - Moxa Synmap OIDs List

- **Installing the Synmap Virtualization Layer**

- **Installing and Using an NMS**
  - Installing Moxa MxView
  - Basic Configuration of MxView
  - Loading the Synmap MIB File
  - Using Synmap OIDs to Control the TC-6110
The Synmap™ Virtualization Layer: Full Interoperability with Any Moxa Device

Overview

Synmap™ is Moxa’s revolutionary software virtualization, an evolutionary advance in network device control that adapts solid, reliable SNMP into a fully portable remote procedure interface. Synmap allows engineers to automate remote processes using SNMP object identifiers (OIDs) rather than device- or OS-specific API addressing, making a scripted Synmap procedure fully interoperable with any other Synmap device. This means that a script created for one Synmap device may be directly copied to another, immediately conferring the same functionality. This eliminates the need for rewriting and compiling code for newly configured devices, significantly reducing maintenance and deployment times.

SNMP is lightweight and easy-to-configure, and is already long-popular with IT professionals; it also enjoys comprehensive native support in high-level languages like .NET, Java, Python, or Ruby. For these reasons, the Synmap framework has re-imagined SNMP as a universal configuration and control interface for remote procedures, adapting it to not only monitor and control device internals like temperature, BIOS parameters, and local interfaces, but also to report on and automate tasks at the process layer, as well. Easily integrated into any existing Network Management System (NMS), Synmap devices are a flexible and cost-effective upgrade that returns obvious benefits to any IA network.

Synmap currently allows you to use SNMP for remote monitoring and control of a select set of computer processes, but its list of features is rapidly growing. Using Synmap’s fully portable scripts, engineers will soon be able to:

- Access, monitor, control, and report on digital I/O at both the process and hardware layers
- Use OIDs to monitor, configure, and give process control over serial ports and other interfaces
- Monitor and control system attributes and process events via any NMS
- Build automated remote procedures using Synmap OIDs called by simple shell scripts, or a preferred high-level language like Python, Perl, or VBScript—all without any need for low-level APIs, or platform-specific libraries
- Significantly simplify and reduce development times for custom utilities and automated executables
- Gain scripting and automation independence from OS-dependent libraries

All of this may be achieved using simple, reliable, and familiar SNMP, the easily accessible standard that IT engineers are already familiar with.

The Synmap Design Concept

Synmap is a software design concept that offers programmers a wholly unique and superior conception of infrastructure development for IA control. Instead of using low level APIs, Synmap adapts the higher level SNMP protocol to serve as a universal API across all machines. With Synmap, application developers gain several benefits, the two biggest being a significantly reduced learning curve for control APIs and remarkable code portability. For example, if a user wants to control GPIO in a Linux environment, an application developer needs to generate code that follows the pseudo code shown below:

1. Open() the device node
2. Read() the file descriptor
3. Read() the return value, and make a logical decision
4. Perform an ioctl function on the file descriptor
5. Close() the file descriptor

The above example shows how this is done in a *NIX environment. In a Windows environment, it looks a little different, but the process is essentially the same, and of equal complexity:
1. Open a required file handle using `mxgpio_open`
2. Get data using the file handle, an assigned port, and `mxgpio_get_data`
3. Evaluate the returned data, and make a logical/control decision
4. Use `mxgpio_set_data` with the file handle to set a value
5. Use `mxgpio_close` to close the file handle

These examples show, in concise form, the difficulties application developers face when dealing with low level APIs. Developers must understand each system’s API and track down various device node IDs from within the user manual, the sample code, or the general system. Synmap significantly simplifies this situation. In comparison to the example just shown, the pseudo code that replaces it will look something like this:

- GET an OID using SNMP and the localhost connection (127.0.0.1)
- Evaluate the returned data, make a logical decision
- SET an OID using SNMP and the localhost connection (127.0.0.1)

The benefits of using SNMP in this way should be clear.

- First, the code is easily migrated across different computers and even different operating systems, because Moxa’s SNMP libraries are supported on both Windows XPE and Linux, as well as a host of other platforms.
- Second, the program can just as easily be ported to the network for remote operations simply by changing the localhost connection (127.0.0.1) to the target IP address and hostname.
- Third, the time needed to learn how to control a peripheral is drastically cut; all one needs to do is understand how to use an SNMP OID, and start scripting.
- Fourth, Developers are free to choose any kind of programming languages or utilities with which they might be familiar, so long as they are apropos to the platform(s) on which they will be used. For example, in place of the C API, Microsoft developers might want to use the SNMP libraries in .NET or Java to control remote Linux devices, or it can be flipped around so that Linux developers use Net-SNMP libraries to control remote Windows XPE machines.

All of these things mean that the Synmap virtualization makes the work of programming custom applications much faster and simpler, and dramatically increases code interoperability. Complex controls such as USB notify, mounting information, and BIOS settings have been integrated into the Synmap engine, so that creating a customized monitoring or control application now only requires the coordination of a few SNMP SET/GET calls, potentially allowing developers to save on hundreds of lines of code when authoring new applications.

### Moxa Synmap OIDs List

The following table shows the OIDs currently supported on the TC-6110. For a full review of all Moxa Synmap OIDs, check the Appendix section.

<table>
<thead>
<tr>
<th>Item Name</th>
<th>OID</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>productName</td>
<td>1.3.6.1.4.1.8691.17.1.1.1</td>
<td>read-only</td>
<td>Returns the product name</td>
</tr>
<tr>
<td>productDesc</td>
<td>1.3.6.1.4.1.8691.17.1.1.2</td>
<td>read-only</td>
<td>Returns a short device description</td>
</tr>
<tr>
<td>productVersion</td>
<td>1.3.6.1.4.1.8691.17.1.1.3</td>
<td>read-only</td>
<td>Returns product version</td>
</tr>
<tr>
<td>productBuildDate</td>
<td>1.3.6.1.4.1.8691.17.1.1.4</td>
<td>read-only</td>
<td>Returns the last software build date, YYMMDHH format</td>
</tr>
<tr>
<td>tempSensorsIndex</td>
<td>1.3.6.1.4.1.8691.17.1.5.1.1.1</td>
<td>read-only</td>
<td>Reference index showing all available temperature sensors; starts from 1</td>
</tr>
<tr>
<td>tempSensorsDevice</td>
<td>1.3.6.1.4.1.8691.17.1.5.1.1.2</td>
<td>read-only</td>
<td>Returns a list of the unique string values that the database associates with a temperature sensor index value. May be used with tempSensorIndex to identify temperature sensors by name/position, and to subsequently call them in scripts</td>
</tr>
</tbody>
</table>
tempSensorsValue 1.3.6.1.4.1.8691.17.1.5.1.1.1.3 read-only The reading returned by the thermometer, in degrees Celsius
Note: On the TC-6110, temp. is currently represented as the current reading truncated to its base integer, without rounding

accelometerIndex 1.3.6.1.4.1.8691.17.1.5.1.3.1.1 read-only Reference index showing all available accelerometers; starts from 1

accelometerAxis 1.3.6.1.4.1.8691.17.1.5.1.3.1.2 read-only Shows the format in which accelerometer’s axial values will be returned. This will always be in X_n Y_n Z form, with n the index number of the accelerometer with which the axis is associated

accelometerValue 1.3.6.1.4.1.8691.17.1.5.1.3.1.3 read-only Returns a block of the last hundred recorded values for all three axes of a particular accelerometer, taken from the log file; this will be g-force in micro gravities (µG).
Note: this OID requires the accelerometer’s log file to be activated and up-to-date. If the log file is unreadable for any reason, this OID will not return data.

accelometerTimestamp 1.3.6.1.4.1.8691.17.1.5.1.3.1.4 read-only Returns the accelerometer timestamp

usbDeviceProductID 1.3.6.1.4.1.8691.17.1.6.4.1.3.1.3 read-only Returns the USB’s hexadecimal product ID

usbDeviceActiveClass 1.3.6.1.4.1.8691.17.1.6.4.1.3.1.4 read-only Returns the USB device class for any connected device

watchdogPeriod 1.3.6.1.4.1.8691.17.1.6.6.2.1 read-write Sets the watchdog’s timeout interval, in seconds:
• Entering 0 disables the watchdog
• Entering an integer from 1 to 255 configures the timeout interval to that number of seconds

watchdogStatus 1.3.6.1.4.1.8691.17.1.6.6.2.2 read-write Returns the watchdog’s current status and timeout interval

powerPolicy 1.3.6.1.4.1.8691.17.1.7.2 read-write Returns the system’s current power policy, as configured by the Windows 7 Embedded OS
Installing the Synmap Virtualization Layer

The following steps will install Synmap.

1. Double click mxSynmap_setup.msi, found in the Utility folder located on the software DVD under \utility\3.mxSynmap. Then click Next to start the Synmap setup wizard.

2. In the middle of the dialog, the button Disk Cost will display how much space the Synmap software package will occupy on your storage drive, as well as the remaining storage space on the drive where the system is stored.

   At the bottom of the dialog, select whether Synmap will be installed for every user across the entire system, or just for the current user account. Above that (in the text dialog), you may click the Browse button to browse the file tree and select the folder where you want to install the package, or simply click Next to install Synmap to the default folder.

3. Click through the next few dialogs to complete the installation of the Net-SNMP agent. The SNMP agent will not begin working until you reboot the TC-6110 computer.

Installing and Using an NMS

For full implementation, Synmap requires (like any SNMP-based system) an NMS to become fully functional; an NMS with an MIB browser also makes using SNMP a far simpler task. If you already have your own MIB browser, you can skip this section. However, if your network is lacking an NMS then you may install a free version of
Moxa’s **MXview** to get Synmap up and running. MXview provides an MIB browser and an interface that will allow you to monitor and control any Synmap enabled device. This section will walk you through a basic MXview installation, and show you how to use the MXview MIB browser to start working with the TC-6110’s MIB.

**Installing Moxa MxView**

1. MXview is included on your TC-6110 software DVD. Double click `mxView_Trial_V2.3.msi` in the Utility folder, which you can find on the software DVD in `utility\4.mxViewTrial`. Select **OK** to choose the language, and when the next dialog appears click **Next** to continue.

2. Accept the licensing agreement and click **Next** to move to the licensing dialog.

3. On the next dialog you may change the folder and path where MXview will be installed. On the next, you may select where MXView shortcuts will be stored in the Windows Start Menu.

4. Next, you may register MXview as a Windows service and create a **desktop shortcut**.
5. After you have completed the pre-install configuration, click **Install** to transfer MXview to disk and wind up the installation.

![Image of Install process](image1.png)

6. After MXview has installed, you must enter the IP address of the machine on which it is located. This may be the **localhost** address, **127.0.0.1**, or if you are connecting to MXview over a LAN it will be a remote IP address. Additionally, you must configure the ports which MXview will use for HTTP and HTTPS communications. Once the installation is complete, you may choose to restart the computer to get MXview up and running.

![Image of port configuration](image2.png)

7. After rebooting, the MXview shortcut will appear on your desktop (shown at right). Click on the shortcut to continue on to the next section and begin the MxView setup.

### Basic Configuration of MxView

1. Open MXview (see step 7 of the last section, immediately above) and select **Start** to initialize the MXview NMS; wait for the **System Status** notification to change to **Running**, then click **Launch Client**.

![Image of MXview configuration](image3.png)
2. If opening Microsoft Internet Explorer for the first time, make sure to turn off the **suggested sites** feature (shown at right). If you wish to use another browser you may, and IE’s other settings may be configured to your own preferences.

3. The IP address for MXview will be 127.0.0.1 followed by a colon and the HTTP port you configured MXview to communicate over (in **step 6 of MXview**). If you have used the suggested settings above, then to login using HTTP would be 127.0.0.1:81, and using HTTPS you would use 127.0.0.1:443.

   **WARNING**  
   For security’s sake, Moxa strongly recommends resetting the password to a strongly secure password of at least 8 characters, mixing numbers and symbols in a non-word series.

   For the login, the default username is **admin**, with a blank password.

4. When opening your browser for the first time, a warning message will pop up telling you to install the Java runtime environment. Click **OK** to continue.

5. Click the title bar, and select **File Download Blocked-->Download File** to continue.

6. Select **Run** to download and install the Java Runtime Environment (JRE), and when Windows posts a security warning asking if you wish to run the installer, click **Run** again.
7. Click **Install** to continue.

8. Click **Close** to complete.

9. In Windows IE, a banner will appear at the top of the browser window. Click the message and select **Enable Intranet Settings**.
10. A security warning will appear, telling you that intranet settings are not secure enough for the open Internet. Click Yes to ignore this, and when another security warning appears telling you that the application’s digital signature is not recognized, click Run.

11. The **Moxa MXview Setup Wizard** will now appear. You may click Next if you wish to enter the setup routine, or select Cancel to launch the program immediately. If you click Cancel, The program will be launched. It should look like the screenshot below.

**Loading the Synmap MIB File**

To load the Synmap MIB file you must first have a running NMS; if you do not have an NMS, you may install the free version of MXview included with your TC-6110 computer software. If you have already started MXview, go directly to step 5 of this section.

1. Click the **MxView Service** shortcut on the desktop

2. Click Start, wait for the **System Status** indicator to show Running, and then select Launch Client; the **System Status** value should switch to Running.
3. When the **MXview Setup Wizard** appears, click **Cancel** to skip the MXview setup process and directly open the MXview interface.

4. Once the MXview interface is open, click on the **MIB** tab and select **MIB Browser** from the dropdown.

5. After the MIB browser has opened, select **File** from the browser’s upper left corner, and then **Load MIB**.

(Instructions continue on next page)
6. Navigate to `c:\usr\share\snmp\mibs\` and select `MOXA-SYS-MIB.txt`.

7. After opening the Synmap MIB in the browser, check that it appears in the File window. If it is not, then it is likely because the MIB file is corrupted. To remedy this, re-copy the MIB file from the software DVD, and re-load the MIB file following the instructions above.
Using Synmap OIDs to Control the TC-6110

Follow these steps to use Moxa Synmap to read the MIB and set up controls for the TC-6110.

Retrieving Basic Device Information

1. In this first step, we will use Synmap to retrieve specific device information about the TC-6110. First, use the Get Next button to navigate the OID tree by clicking through these items: `MOXA-SYS-MIB\VALUES\Moxa\embeddedComputer\MoxaSystem\productInfoMgmt`

2. When you reach the final layer of OIDs, you will need to select GetSubTree to display the available information. When you use the MIB viewer to select the `productInfoMgmt` OID, you will see the following information displayed in the MIB viewer's information window: **Product Name** (TC-6110), **Product Description** (Moxa embedded computer), **Product Version** (1.0.0), and **Product Build Date** (13013018).
Using Synmap to Control the Programmable LEDs

The following figure shows the locations of the LED indicators on the TC-6110 computer. Using custom scripts, you can set these LEDs to be used as indicators for your own applications.

The following table shows the available OIDs for the TC-6110 LEDs.

<table>
<thead>
<tr>
<th>Item Name</th>
<th>OID</th>
<th>Access</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ledNumber</td>
<td>1.3.6.1.4.1.8691.17.1.6.2.1</td>
<td>read-only</td>
<td>N/A</td>
<td>Returns the total number of LEDs</td>
</tr>
<tr>
<td>ledIndex</td>
<td>1.3.6.1.4.1.8691.17.1.6.2.1.1</td>
<td>read-only</td>
<td>N/A</td>
<td>Returns a list of numbers that correspond with the LEDs, used by SNMP to identify the LEDs; begins with 1</td>
</tr>
<tr>
<td>ledPort</td>
<td>1.3.6.1.4.1.8691.17.1.6.2.1.2</td>
<td>read-only</td>
<td>N/A</td>
<td>Returns the names by which the index of LEDs may be called when used in scripts; begins with 0</td>
</tr>
<tr>
<td>ledValue</td>
<td>1.3.6.1.4.1.8691.17.1.6.2.1.3</td>
<td>read-write</td>
<td>0(off), 1(on)</td>
<td>Returns/sends a value indicating/changing the LED state</td>
</tr>
</tbody>
</table>

Follow these steps to configure the programmable LED indicators on the TC-6110 computer.

1. Start up MXview (or some other NMS) and open the MIB browser. For detailed instructions on loading MXview, you may refer to [Loading the Synmap MIB File](#), steps 1 to 3.
2. In the MIB browser, navigate the OID tree to `MOXA-SYS-MIB\VALUES\Moxa\embeddedComputer\MoxaSystem\peripheralMgmt\perLedMgmt\ledTable\ledEntry\ledValue`. Select the value by clicking on the entry, or pressing Enter. To change the state of an LED from on to off (or vice versa) click Set on the corresponding ledValue OID (shown in the figure at right). This will open a dialog called the Set Value dialog.
3. The Set Value dialog has four fields: one for the OID; another called Index, that identifies which section of the OID is being manipulated (here, it indicates the LED label); and a third called Value, to set the state of the OID (here, whether the LED is off or on). The fourth field (Syntax) informs you of the type of character to be used to set the value. In this case, we are using the integers 0 and 1: 0 turns the LED off, and 1 turns it on. After entering the correct information into the fields (as shown at right), click on the Set button and check if the LED indicator has lit up (LED 1 is shown in the figure at the top of this section, Using Synmap to Control the Programmable LEDs).

4. Next, set the value to 0 and click Set to turn off the LED, then verify that the LED has successfully turned off. If you experience problems at this point, please review the instructions above and if the problem persists, contact Moxa technical support.

Using Synmap to Set the OS Power Policy

The following table shows the OID power policy control, read/write option and available values.

<table>
<thead>
<tr>
<th>Item Name</th>
<th>OID</th>
<th>Access</th>
<th>Value to set</th>
</tr>
</thead>
<tbody>
<tr>
<td>powerPolicy</td>
<td>1.3.6.1.4.1.8691.17.1.7.2</td>
<td>read-write</td>
<td>1: Balanced</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2: Power Saver</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3: High Performance</td>
</tr>
</tbody>
</table>

The powerPolicy OID allows you to change the Windows 7 power policy. Balanced may be considered normal operations, and except in extreme circumstances of exceptionally high CPU use or where strict energy conservation must be maintained, this option will provide satisfactory performance. Power Saver will conserve power usage to the maximum extent possible, restricting the CPU to around 36% capacity. High Performance maximizes CPU cycles for all applications at all times; generally, High Performance is not recommended, and in many (perhaps most) circumstances where the TC-6110 is used, Power Saver mode may be adequate to the system’s needs. Sysadmins should carefully review the needs of the system and do some quick tests to make the most informed decision. These settings may be further fine-tuned with advanced choices in the Windows 7 OS.
To use Synmap to set the power policy:

1. Start up MXview (or some other NMS) and open the MIB browser. For detailed instructions on loading MXview, you may refer to Loading the Synmap MIB File, steps 1 to 3.

2. In the MIB browser, navigate to 
\( \text{MOXA-SYS-MIB\VALUES\Moxa\embeddedComputer\MoxaSystem\powerMgmt\powerPolicy} \).

To change the Windows 7 power policy settings, highlight the powerPolicy OID and click **Set**. This will open a dialog called the **Set Value** dialog.

3. The **Set Value** dialog for the **powerPolicy** OID has two variable fields: one showing the OID that is being called and a second called **Value**, to indicate which power management policy should be used. Use the integer 1 to indicate the **Balanced**, 2 for the **Power Saver**, and 3 for the **High Performance** policy. After entering the value, close the dialog by clicking **Set**.

4. To check if the policy has been changed, navigate to the Windows 7 Control Panel, and open the **Power Options** tab, located under **Control Panel ➔ System Security**.

---

**ATTENTION**

For more detailed information on the advanced settings of Windows 7 power management policies, you may refer to Microsoft’s online Windows support pages, which are currently (Jul. 2013) found at this link:


---

Using Synmap to Read the Temperature Sensor

The following table shows the temperature sensor OIDs.

<table>
<thead>
<tr>
<th>Item Name</th>
<th>OID</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tempSensorsIndex</td>
<td>1.3.6.1.4.1.8691.17.1.5.1.1.1.1</td>
<td>read-only</td>
<td>Returns a list of numbers (beginning with 1) that corresponds with the available T-sensors; these identifiers are used by SNMP and for system scripts.</td>
</tr>
<tr>
<td>tempSensorsDevice</td>
<td>1.3.6.1.4.1.8691.17.1.5.1.1.1.2</td>
<td>read-only</td>
<td>Returns a list of string values identifying the temperature sensors by name/location. Possible values are SATA1, SATA2, or CPU, for the CPU's internal thermometer.</td>
</tr>
<tr>
<td>tempSensorsValue</td>
<td>1.3.6.1.4.1.8691.17.1.5.1.1.1.3</td>
<td>read-only</td>
<td>The reading returned by the thermometer, in degrees</td>
</tr>
</tbody>
</table>
To use Synmap to check the temperature sensor (T-sensor) of the TC-6110 computer, follow the steps below.

1. Start up MXview (or some other NMS) and open the MIB browser. For detailed instructions on loading MXview, you may refer to [Loading the Synmap MIB File](#), steps 1 to 3.

2. Navigate to `MIB\VALUES\moxa\embeddedComputer\moxaSystem\sensorMgmt\sensorObject\tempSensorTable` in the MIB Browser, and then select Get Subtree to open the T-sensor’s OID tree.

3. All of the T-sensor information should now be displayed in the MIB browser; if it is not, then there is a problem with your SNMP/Synmap configuration or a malfunction in the T-sensor. The temperatures are all displayed in Celsius. In the screenshot below, the temperature of disk 1 (SATA1) is 37 degrees. If the SATA module is not mounted, the temperature value will be shown as 178 degrees. Thus, in the screenshot at right, the disk 2 (SATA2) is showing 178 degrees because there is no disk mounted in slot 2 of the computer.
Using Synmap to Read the G-Sensor

The following table lists the accelerometer OIDs.

<table>
<thead>
<tr>
<th>Item Name</th>
<th>OID</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accelerometerIndex</td>
<td>1.3.6.1.4.1.8691.17.1.5.1.3.1.1</td>
<td>read-only</td>
<td>Returns a list of numbers (beginning with 1) that corresponds with the available G-sensors; these identifiers are used by SNMP and for scripting</td>
</tr>
<tr>
<td>accelerometerAxis</td>
<td>1.3.6.1.4.1.8691.17.1.5.1.3.1.2</td>
<td>read-only</td>
<td>Returns the format in which accelerometer axial values will be returned. This will always be Xn Yn Zn.</td>
</tr>
<tr>
<td>accelerometerValue</td>
<td>1.3.6.1.4.1.8691.17.1.5.1.3.1.3</td>
<td>read-only</td>
<td>Returns the accelerometer value associated with a particular axis; this will be g-force in micro gravities (µG).</td>
</tr>
<tr>
<td>accelerometerTimestamp</td>
<td>1.3.6.1.4.1.8691.17.1.5.1.3.1.4</td>
<td>read-only</td>
<td>Returns the G-sensor’s current timestamp.</td>
</tr>
</tbody>
</table>

To use Synmap to read the vibration sensor (accelerometer, or G-sensor), follow these steps:

1. Start up MXview (or some other NMS) and open the MIB browser. For detailed instructions on loading MXview, you may refer to [Loading the Synmap MIB File](#), steps 1 to 3.

2. Navigate to MOXA-SYS-MIB\VALUES\moxa\embeddedComputer\moxaSystem\sensorMgmt\sensorObject\accelerometerTable in the MIB Browser, and then select Get Subtree to open the accelerometer’s OID tree.
3. Check to verify if logs for both GSensor1 and GSensor2 exist.

4. Open the logs to verify they are logging correctly.

**Using Synmap to Enable and Configure the Watchdog Timer**

The TC-6110 comes with a default watchdog timer (a Computer Operating Properly/COP timer) that will initiate a soft reboot whenever the system or a specific program freezes for a specified time period. The watchdog timer has only two Synmap OIDs associated with it: `watchdogPeriod` and `watchdogStatus`. The value for `watchdogPeriod` sets the countdown interval during which the watchdog timer must receive a COP notification from the OS kernel; if it does not receive a COP notification during this interval, the watchdog will reboot the system.

The default value of `watchdogPeriod` is 0, which leaves the watchdog disabled. To enable the watchdog timer, you need to set the scanning interval to a non-zero integer between 1 and 255; this number will set the number of seconds that will pass following a system (or application) hang before the watchdog reboots the platform.

After setting a time interval for the watchdog, the OID `watchdogStatus` will automatically change to 1, to indicate that the watchdog timer is enabled. Once enabled, whenever the kernel fails to deliver a COP signal during the specified time period the watchdog will automatically initiate a soft reboot.

The following table shows the watchdog OIDs.

<table>
<thead>
<tr>
<th>Item Name</th>
<th>OID</th>
<th>Access</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>watchdogPeriod</td>
<td>1.3.6.1.4.1.8691.17.1.6.6.2.1</td>
<td>read-write</td>
<td>An integer between 1 and 255 representing the timeout period in seconds (E.g. 30 = 30 seconds)</td>
</tr>
<tr>
<td>watchdogStatus</td>
<td>1.3.6.1.4.1.8691.17.1.6.6.2.2</td>
<td>read</td>
<td>0 represents Off, 1 represents On</td>
</tr>
</tbody>
</table>
To enable the watchdog via Synmap, follow the instructions below.

1. **Navigate to** `MOXA-SYS-MIB\VALUES\Moxa\embeddedComputer\MoxaSystem\peripheralMgmt\systemWatchdog\watchdog period` **and select** *Set*.

2. In the *Set Value* dialog for *watchdogPeriod*, the refresh time can be entered as a number between 1 and 255 seconds in the *Value* field. Enter the desired value and click *Set*. Click *OK* when a dialog appears indicating that the watchdog has been successfully set.

3. **Right-click** `MOXA-SYS-MIB\VALUES\Moxa\embeddedComputer\MoxaSystem\peripheralMgmt\perSystemMgmt\watchdogStatus` **and select** *Get*. Note that in the screenshot below, the watchdog is currently disabled.
4. Since you have just changed the value of the **watchdogPeriod** OID, check to verify that the value of the **watchdogStatus** OID has changed to 1. This means that the watchdog is now activated and running.
This chapter describes how to use various examples on the V2616A computers for different functions.

The following topics are covered in this chapter:

- Setting a Serial Interface
- Digital Input/Output
- LED Indicators
- Button Scripts
- PCIe Reset
Selecting a Serial Interface Mode

This script allows a user to select and query the communications standard used on a particular serial interface.

1. Copy the following files from the product software DVD.
   - mxsp.dll: \DVDV2616A-W7E V1.0\examples\lib\mxsp\n   - sysinfo.dll: \DVDV2616A-W7E V1.0\examples\lib\mxsp\n   - sysinfo.sys: \DVDV2616A-W7E V1.0\examples\lib\mxsp\n   - mxGeneralIo.dll: \DVDV2616A-W7E V1.0\examples\lib\MxGeneralIo\n   - SerialInterface.exe: \DVDV2616A-W7E V1.0\examples\Release\n   - MxSer.reg: \DVDV2616A-W7E V1.0\examples\Release\n
2. Execute MxSer.reg to create registry for serial interface.

3. Execute SerialInterface.exe.

4. To set the communications standard for an interface, select 2, then select the interface.

5. Select 1 to check the current interface status.
Digital Input/Output

This script gives basic controls and monitoring of the DI/DO channels.

1. Copy the following files from the product software DVD.
   - `mxgpio.dll`: `\DVDV2616A-W7E V1.0\examples\lib\mxgpio\`
   - `mxGeneralIo.dll`: `\DVDV2616A-W7E V1.0\examples\lib\MxGeneralIo\`
   - `DIO.exe`: `\DVDV2616A-W7E V1.0\examples\Release\`

2. Execute `DIO.exe`.

3. Select 4 to return the current I/O values for all channels.

4. Choose 3 to set a value for a particular port. After choosing 3, next you must select the port number you wish to configure. Lastly, select the value you wish to set the channel to: 0 indicates low, 1 indicates high.
5. Finally, check to verify the port value is set correctly.

LED Indicators

This script reports on and controls the LED state, switching them on and off.

1. Copy the following files from the product software DVD.
   - mxgpio.dll: `\DVDV2616A-W7E V1.0\examples\lib\mxgpio\`
   - mxGeneralIo.dll: `\DVDV2616A-W7E V1.0\examples\lib\MxGeneralIo\`
   - LED.exe: `\DVDV2616A-W7E V1.0\examples\Release\`

2. Execute LED.exe.

3. Select 1 to get the current LED value.
4. To set LED value, select 2 and the value.

   ![Command Prompt window](image1.png)

**Button Scripts**

These scripts register button presses and releases.

1. Copy the following files from the product software DVD.
   - `mxgpio.dll`: DVDV2616A-W7E V1.0\examples\lib\mxgpio\
   - `mxGeneralIo.dll`: DVDV2616A-W7E V1.0\examples\lib\MxGeneralIo\
   - `Button.exe`: DVDV2616A-W7E V1.0\examples\Release\

2. Execute `Button.exe`, the program will start polling the button status.
   ![Command Prompt window](image2.png)

3. Now you can press the button and check if the button status has been changed.
   ![Command Prompt window](image3.png)
**PCIe Controls**

This script controls the PCIe card, allowing users to turn power to the slot (not the card) off or on, and to trigger the reset pin (pin 22) on the PCIe module. Triggering the reset pin should reload the module’s firmware.

1. Copy the following files from the product software DVD.

   - **mxgpio.dll**: `\DVDV2616A-W7E V1.0\examples\lib\mxgpio\`
   - **mxGeneralIo.dll**: `\DVDV2616A-W7E V1.0\examples\lib\MxGeneralIo\`
   - **PCIeReset.exe**: `\DVDV2616A-W7E V1.0\examples\Release\`

2. Select the option to trigger the slot power, or to trigger the module’s reset pin (pin 22).

3. Select the value to disable/enable the signal.
This chapter describes the system recovery process in the event of system instability.

The following topics are covered in this chapter:

- Overview
- Setting Up the Recovery Environment
- Setup of a Factory Default Recovery Image
  - Step 1: Prepare the USB drive
  - Step 2: Setting the BIOS to Boot via USB
  - Step 3: How to Perform a System Recovery
  - Step 4: Reset the BIOS to its Original State
- Creating a Custom System Image
Overview

This section describes how to prepare your computer for a recovery procedure in the event of system instability. Users can perform two types of system recovery, from one of two system images: a clean factory default image, or a user-generated image taken of a fully configured, fully set up system.

Before you do any one of the system recoveries, you should prepare the system environment in advance.

Setting Up the Recovery Environment

To set up the recovery environment a V2616A computer, a 4 GB (min.) USB drive, and a copy of the recovery suite are all required.

For the recovery procedure itself, you will only need a V2616A computer and a prepared USB drive. The following procedure describes the basic process of setting up the system recovery environment.

1. First, the recovery programs and system image file will be copied over to the USB drive, and the drive will be set up as a live-drive system, with an ISO image of the boot environment.
2. The system will be re-booted, and BIOS will be manually configured to boot the recovery system from the USB port.
3. An image of the current software system will then be created on the USB drive, for the recovery environment to use when restoring the system.
4. The system will be re-booted again, and the BIOS returned to its original state.

Setup of a Factory Default Recovery Image

Step 1: Prepare the USB drive

1. Load the software DVD that came with your V2616A computer and execute tuxboot-windows-23.exe from the software DVD\recovery\V2616A-W7E_Recovery folder. Select Pre-Downloaded, and click the button marked with an ellipsis (…) to browse the file system and find the location of the boot environment’s ISO image.
2. Navigate to `recovery` on the software DVD and select the boot environment’s ISO image.

3. Set the device **Type** (lower left-hand corner) as **USB Drive**, then set the **Drive** dialog to the letter under which the USB is currently mounted.

4. Click **OK**, and the boot environment and bootloader will be copied to your USB drive.
5. When finished, click OK. Note that because of the file system naming conventions used, for any given computer only a single recovery image may be used on any given USB drive.

6. From within the desktop environment, the user should then manually copy the directory containing the base OS from the software DVD over to the USB drive. To do this, copy #:\<SoftwareDVD>\recovery\V2616A-W7E_Recovery\Clonezilla\os_image over to the partition image directory, F:\home\partimag\. However, if you want to recover to a fully configured, ready-to-deploy system image, you need to perform system image backup first. Refer to the section below, Creating a Custom System Image, for details. At this point, Step 1 has been completed, and you should proceed to the next section, Step 2: Setting the BIOS to Boot via USB.

![Image of file system]

**Step 2: Setting the BIOS to Boot via USB**

At this stage, users will reset the BIOS so that the system boots directly from the USB. This must be done before the rest of the system recovery environment may be configured.

1. Reboot the system, and, during the POST process, press **F2 until you hear a long beep. You should then** enter the BIOS setup menu. Select **SCU** to enter the BIOS setup menu.

![Image of BIOS setup menu]

2. Use the left/right arrow keys to navigate to the **Boot tab**, and then press **Enter**.
3. Use the up/down arrows to highlight **Legacy** in the boot tab’s menu, and press **Enter**.

4. Use the up/down arrow keys to navigate to the **Boot Type Order** link, and then press **Enter**.

5. Use the up/down arrows to highlight **USB** and then use the plus/minus signs (+ -) to move it to the first boot priority position.
Step 3: How to Perform a System Recovery

Below, we provide instructions on how to perform a system recovery. We include this as step 3 of the installation so administrators may first perform a test run, before deploying their system to the field.

To begin the system recovery, you will first need to have prepared the BIOS as described in the previous section Step 2: Setting the BIOS to Boot via USB, just above. After preparing the BIOS, you should connect the USB recovery drive to any of the V2616A’s USB ports and then reboot the computer. If you have successfully prepared the USB and BIOS, the computer will boot into the Clonezilla boot loader, from the USB.

1. Select ClonezillaLive Restore Disk to boot into the system restoration environment.

2. Wait for the boot process to finish.
3. At this point, the system will remind you that you are about to overwrite your entire operating system with a new drive image, and ask you if you want to continue. When prompted, enter **Y** (case insensitive) from the keyboard to start the system restoration process. Any other letter or **Ctrl-C** will cancel the recovery process and exit Clonezilla.

4. The system will give you another warning that you are about to overwrite your hard drive, and erase all data on the partition listed (**sda1**, in the example below). If you wish to continue, enter **Y** (case insensitive).

5. Wait for the process to finish.
6. At this point, complete the restoration by selecting (0), **Power off**. This will shut down the computer; however, if the **Power Switch** remains inserted in the front panel of the computer and is left in the **ON** position, then the system will fail to shut down and will immediately initiate a soft reboot. To avoid this, users may use the switch to cut power to the computer immediately following the shutdown, or may simply remove the power switch from the front panel and then use the console to shut down the computer by pressing **0**.

7. After the computer has powered down, remove the USB drive and store it in a secure place.

**Step 4: Reset the BIOS to its Original State**

Now you will need to return the boot priority to its original configuration so that the system will boot from the main system storage drive. This is done for two reasons; the first is security, so that the machine may not be rebooted from unauthorized USB drives.

The second reason, however, is functional: currently, **if the V2616A is set to boot from the USB drive, then the V2616A’s boot process will hang any time a non-bootable USB data drive is inserted into the machine**. The V2616A does not currently have the capacity to distinguish between simple USB data drives and boot-capable OS drives.

2. Reboot the system, and, during the POST process, press **F2 until you hear a long beep. You should then** enter the BIOS setup menu. Select **SCU** to enter the BIOS setup menu.
6. Use the left/right arrow keys to navigate to the **Boot tab**, and then press **Enter**.

7. Use the up/down arrows to highlight **Legacy** in the boot tab’s menu, and press **Enter**.

8. Use the up/down arrow keys to navigate to the **Boot Type Order** link, and then press **Enter**.

9. Use the up/down arrows to highlight **Hard Disk Drive** and then use the plus/minus signs (+ -) to move it to the first boot priority position.
10. Press **F10** and then press **Enter** to save and exit the BIOS configuration interface. This should initiate the next reboot, and your system should now boot from the USB drive.

## Creating a Custom System Image

This section describes how to create a custom system image so that all your applications can be kept and recovered. Using this procedure, you will save to the USB drive a copy of the entire system **as it is currently configured** to be used as a **full system recovery image** should the system crash. **All files under F:\home\partimag\ will be overwritten.**

You need to complete **Step 1: Prepare the USB Drive** and **Step 2: Setting the BIOS to Boot via USB**, and then continue the following steps for creating a custom system image.

1. Once the system has launched and the V2616A has booted the recovery environment from the USB drive, navigate to the entry ClonezillaLive Save Disk, and select it by pressing Enter. This will take you into the recovery image creation environment, allowing you to copy your full system setup to the USB drive.

2. The V2616A will now boot into the image creation environment. Wait for the boot process to finish.
3. Once the image creation environment has completed booting up, you will be given a warning and asked if you wish to continue. Please keep in mind that if you create the recovery image, then **any residual files currently copied to the "/home/partimag" directory will be deleted.** If there are any files remaining in the USB partition image directory and you wish to save them, you must exit the recovery environment and copy these files to another disk. If you wish to continue with the image creation, press Y (case insensitive) to continue.

4. At this point, the recovery environment will copy of the entire hard drive to your USB drive. This will likely take several minutes, and perhaps as long as half an hour. Do not remove the USB drive during this time; wait patiently for the process to finish. Depending on the speed of your USB drive, this may be a good time to get a cup of coffee, or take a nap.
5. At this point you may choose to power down the computer (press 0), reboot (press 1), enter a console terminal (access a console TTY -- press 2), or re-initiate the entire procedure (press 3). **Do not remove the USB drive until you have rebooted or powered down the system.**

6. Once you have powered down the system and removed the USB drive, you have finished configuring the recovery environment. Now you have your own OS image under **USB Folder\home\partimag\os_image**. The USB drive should be clearly labeled and stored in a safe place. You may now continue to the next section, where you will return the BIOS to its original state (**Step 4**).
This appendix describes the Moxa SynMap OID Table.

The following topics are covered in this appendix:

- Moxa SynMap OID Table
# Moxa SynMap OID Table

The following table shows the full list of the Moxa SynMap OID.

<table>
<thead>
<tr>
<th>Item Name</th>
<th>OID</th>
<th>MAX-Access</th>
<th>Description</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>productName</td>
<td>1.3.6.1.4.1.8691.17.1.1.1</td>
<td>read-only</td>
<td>Showing product name.</td>
<td></td>
</tr>
<tr>
<td>productDesc</td>
<td>1.3.6.1.4.1.8691.17.1.1.2</td>
<td>read-only</td>
<td>Showing product short description.</td>
<td></td>
</tr>
<tr>
<td>productVersion</td>
<td>1.3.6.1.4.1.8691.17.1.1.3</td>
<td>read-only</td>
<td>Showing product version.</td>
<td></td>
</tr>
<tr>
<td>productBuildDate</td>
<td>1.3.6.1.4.1.8691.17.1.1.4</td>
<td>read-only</td>
<td>Showing product last build date, the format is YYMMDDHH.</td>
<td></td>
</tr>
<tr>
<td>biosVersion</td>
<td>1.3.6.1.4.1.8691.17.1.1.4.1</td>
<td>read-only</td>
<td>Showing the BIOS version.</td>
<td></td>
</tr>
<tr>
<td>biosSaveSetting</td>
<td>1.3.6.1.4.1.8691.17.1.1.4.2</td>
<td>read-write</td>
<td>Write 1 to save bios setting, and read 0 mean setting had been applied.</td>
<td></td>
</tr>
<tr>
<td>biosSettingStatus</td>
<td>1.3.6.1.4.1.8691.17.1.1.4.3</td>
<td>read-only</td>
<td>Showing compare of bios CMOS setting and bios new setting.</td>
<td></td>
</tr>
<tr>
<td>bootDeviceStatus</td>
<td>1.3.6.1.4.1.8691.17.1.1.4.4.1</td>
<td>read-only</td>
<td>Showing the current support boot device.</td>
<td></td>
</tr>
<tr>
<td>firstBootDevice</td>
<td>1.3.6.1.4.1.8691.17.1.1.4.4.2</td>
<td>read-write</td>
<td>read show current first boot device, write set boot device.</td>
<td></td>
</tr>
<tr>
<td>pwrOnAfterPwrFail</td>
<td>1.3.6.1.4.1.8691.17.1.1.4.8.1</td>
<td>read-write</td>
<td>Select power on after power fail behavior.</td>
<td></td>
</tr>
<tr>
<td>pwrLanWakeUp</td>
<td>1.3.6.1.4.1.8691.17.1.1.4.8.3</td>
<td>read-write</td>
<td>Enable/Disable wake on LAN functionality.</td>
<td></td>
</tr>
<tr>
<td>tempSensorsIndex</td>
<td>1.3.6.1.4.1.8691.17.1.1.5.1.1.1.1</td>
<td>read-only</td>
<td>Reference index for each observed device.</td>
<td></td>
</tr>
<tr>
<td>tempSensorsDevice</td>
<td>1.3.6.1.4.1.8691.17.1.1.5.1.1.1.2</td>
<td>read-only</td>
<td>The name of the temperature sensor we are reading.</td>
<td></td>
</tr>
<tr>
<td>tempSensorsValue</td>
<td>1.3.6.1.4.1.8691.17.1.1.5.1.1.1.3</td>
<td>read-only</td>
<td>The temperature of this sensor in mC.</td>
<td></td>
</tr>
<tr>
<td>voltSensorsIndex</td>
<td>1.3.6.1.4.1.8691.17.1.1.5.1.2.1.1</td>
<td>read-only</td>
<td>Reference index for each observed device.</td>
<td></td>
</tr>
<tr>
<td>voltSensorsDevice</td>
<td>1.3.6.1.4.1.8691.17.1.1.5.1.2.1.2</td>
<td>read-only</td>
<td>The name of the device we are reading.</td>
<td></td>
</tr>
<tr>
<td>voltSensorsValue</td>
<td>1.3.6.1.4.1.8691.17.1.1.5.1.2.1.3</td>
<td>read-only</td>
<td>The voltage in mV.</td>
<td></td>
</tr>
<tr>
<td>ioDiNumber</td>
<td>1.3.6.1.4.1.8691.17.1.1.6.1.1.1</td>
<td>read-only</td>
<td>Number of digital input pin in current system.</td>
<td></td>
</tr>
<tr>
<td>diIndex</td>
<td>1.3.6.1.4.1.8691.17.1.1.6.1.1.1</td>
<td>read-only</td>
<td>Reference index for each</td>
<td></td>
</tr>
<tr>
<td>Object</td>
<td>OID</td>
<td>Access</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>diPort</td>
<td>1.3.6.1.4.1.8691.17.1.6.1.1.2</td>
<td>read-only</td>
<td>The port number of digital input pin.</td>
<td></td>
</tr>
<tr>
<td>diValue</td>
<td>1.3.6.1.4.1.8691.17.1.6.1.1.2</td>
<td>read-only</td>
<td>The digital input status, 0 is low, 1 is high.</td>
<td></td>
</tr>
<tr>
<td>diTrapEnable</td>
<td>1.3.6.1.4.1.8691.17.1.6.1.1.2</td>
<td>read-write</td>
<td>Agent will send trap message when digital input pin status changed and this object enabled.</td>
<td></td>
</tr>
<tr>
<td>ioDoNumber</td>
<td>1.3.6.1.4.1.8691.17.1.6.1.1.3</td>
<td>read-only</td>
<td>Number of digital output pin in current system.</td>
<td></td>
</tr>
<tr>
<td>doIndex</td>
<td>1.3.6.1.4.1.8691.17.1.6.1.1.4</td>
<td>read-only</td>
<td>Reference index for each digital output pin.</td>
<td></td>
</tr>
<tr>
<td>doPort</td>
<td>1.3.6.1.4.1.8691.17.1.6.1.1.4</td>
<td>read-only</td>
<td>The port number of digital output pin.</td>
<td></td>
</tr>
<tr>
<td>doValue</td>
<td>1.3.6.1.4.1.8691.17.1.6.1.1.4</td>
<td>read-write</td>
<td>The digital output status, 0 is low, 1 is high.</td>
<td></td>
</tr>
<tr>
<td>uartNumber</td>
<td>1.3.6.1.4.1.8691.17.1.6.1.3.1</td>
<td>read-only</td>
<td>Number of internal UART in current system.</td>
<td></td>
</tr>
<tr>
<td>uartIndex</td>
<td>1.3.6.1.4.1.8691.17.1.6.1.3.2</td>
<td>read-only</td>
<td>Reference index for each UART port.</td>
<td></td>
</tr>
<tr>
<td>uartType</td>
<td>1.3.6.1.4.1.8691.17.1.6.1.3.2</td>
<td>read-write</td>
<td>The UART mode, 0 is RS232, 1 is RS485 2 wires, 2 is RS422, 3 is RS485 4 wires.</td>
<td></td>
</tr>
<tr>
<td>usbNumber</td>
<td>1.3.6.1.4.1.8691.17.1.6.4.1.1</td>
<td>read-only</td>
<td>The number of ports regardless of their current state in the usb general port table.</td>
<td></td>
</tr>
<tr>
<td>usbDeviceIndex</td>
<td>1.3.6.1.4.1.8691.17.1.6.4.1.3</td>
<td>read-only</td>
<td>The index is identical to usbPortIndex for the correspondent USB port.</td>
<td></td>
</tr>
<tr>
<td>usbDeviceVendorID</td>
<td>1.3.6.1.4.1.8691.17.1.6.4.1.3</td>
<td>read-only</td>
<td>The USB device port vendor HEX-formatted string as it is provided to the USB host by the USB device.</td>
<td></td>
</tr>
<tr>
<td>usbDeviceProductID</td>
<td>1.3.6.1.4.1.8691.17.1.6.4.1.3</td>
<td>read-only</td>
<td>The product ID HEX-formatted string as it is provided to the USB host by the USB device.</td>
<td></td>
</tr>
<tr>
<td>usbDeviceActiveClass</td>
<td>1.3.6.1.4.1.8691.17.1.6.4.1.3</td>
<td>read-only</td>
<td>This object returns USB Device Class type of the active configuration</td>
<td></td>
</tr>
<tr>
<td>usbPlugTrapEnable</td>
<td>1.3.6.1.4.1.8691.17.1.6.4.1.3</td>
<td>read-write</td>
<td>Agent will send trap message when USB plug is removed from USB device.</td>
<td></td>
</tr>
</tbody>
</table>
V2616A W7E Series  Introduction

<table>
<thead>
<tr>
<th>4</th>
<th>device inserted or removed and this object enabled.</th>
</tr>
</thead>
</table>

moxaSystemTrapIP  
1.3.6.1.4.1.8691.17.1.9.1  read-write  Set Trap IP address.

moxaSystemTrapCommunity  
1.3.6.1.4.1.8691.17.1.9.2  read-write  Trap community.

HOST RESOURCE OID Table

The following table shows the list of the Host Resource OID.

<table>
<thead>
<tr>
<th>Item Name</th>
<th>OID</th>
<th>MAX-Access</th>
<th>Description</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>hrProcessorTable</td>
<td>1.3.6.1.2.1.25.3.3</td>
<td>read-only</td>
<td>Showing CPU usage</td>
<td></td>
</tr>
<tr>
<td>hrStorageTable</td>
<td>1.3.6.1.2.1.25.2.3</td>
<td>read-only</td>
<td>Showing disk and memory usage.</td>
<td></td>
</tr>
</tbody>
</table>