

V2406A Windows Embedded Standard 7 Software Manual

Second Edition, May 2015

www.moxa.com/product

MOXA[®]

© 2015 Moxa Inc. All rights reserved.

V2406A Windows Embedded Standard 7 Software Manual

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

© 2015 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

Moxa Americas

Toll-free: 1-888-669-2872
Tel: +1-714-528-6777
Fax: +1-714-528-6778

Moxa Europe

Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99

Moxa India

Tel: +91-80-4172-9088
Fax: +91-80-4132-1045

Moxa China (Shanghai office)

Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505

Moxa Asia-Pacific

Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Table of Contents

1. Introduction	1-1
Software Components	1-2
2. System Initialization	2-1
Overview	2-2
Initializing User Settings	2-2
3. Configuring the Serial Interface	3-1
Overview	3-2
Configuring the 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	4-5
File-Based Write Filter	4-6
Configuring File-Based Write Filter	4-7
Excluding Files from FBWF Protection	4-9
Managing Temporary Files Cached in the Overlay	4-10
5. Moxa Diagnostic Package	5-1
Installing Moxa Diagnostic Utility	5-2
Using Moxa Diagnostic Utility	5-4
6. Moxa SynMap Package	6-1
Moxa SynMap Package	6-2
Overview	6-2
Moxa SynMap OID List	6-2
Installing CrystalDiskInfo	6-3
Installing the Moxa SynMap Package	6-6
Installing MXview	6-10
Configuring MXview	6-13
Loading the Moxa SynMap MIB File	6-22
Loading the Host Resource MIB File	6-26
Using Moxa SynMap OIDs	6-29
Using HOST RESOURCE OIDs	6-30
7. Examples	7-1
SerialInterface	7-2
Digital Input/Output	7-3
Watchdog	7-4
8. System Recovery	8-1
Overview	8-2
Setting Up the Recovery Environment	8-2
Setting Up a Factory Default Recovery Image	8-2
Step 1: Preparing the USB drive	8-2
Step 2: Setting the BIOS to Boot via USB	8-4
Step 3: Performing a System Recovery	8-6
Step 4: Resetting the BIOS	8-9
Creating a Custom System Image	8-11
A. Moxa SynMap OID Table	A-1
Moxa SynMap OID Table	A-2
HOST RESOURCE OID Table	A-4

Introduction

Thank you for purchasing a Moxa V2406A panel computer running the Windows 7 Embedded operating system. The Windows 7 Embedded OS provides a simple and familiar development environment for a variety of industrial applications.

□ **Software Components**

Software Components

The following software components of the Windows Embedded Standard 7 OS come pre-installed on the V2406A computer.

Windows Embedded Standard 7

Core OS:

- 32/64-bit support
- Remote Client
- Remote Procedure Call

Applications and Services Development:

- .Net Framework 4.5
- Remote Desktop Protocol 7.1
- COM OLE Application Support
- COM+ Application Support
- MSMQ

Internet Services:

- Internet Explorer 8.0
- IIS 7.0

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 Decoders
- Windows Media Video VC-1 (WMV) Codecs
- DirectX and Windows Device Experience
- Windows Media Player 12

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

File Systems and Data Store:

- Windows Data Access Components
- Windows Backup and Restore

Embedded Self-Health Diagnostic Software: SNMP-based remote scripting layer for monitoring, reporting, and control

Linux

OS: Linux Debian 7

File System: EXT 4

Internet Protocol Suite: TCP, UDP, IPv4, SNMPv1/v2c/v3, ICMP, ARP, HTTP, SSH 1.0/2.0, SSL, DHCP, NTP, NFS, Telnet, FTP, TFTP, PPP, PPPoE

Internet Security: OpenVPN, iptables firewall

Web Server (Apache): Allows you to create and manage web sites; supports PHP and XML

Secure Shell for Remote Access: SSH allows remote logins to a secure encrypted console from any connected network

Dial-up Networking: PPP Daemon for Linux that allows Unix machines to connect to the Internet through dialup lines, using the Point-to-Point Protocol (PPP). Works with 'chat', 'dip', and 'dialu dip', and 'diald', among (many) others. Supports IP, TCP, UDP, and (for Linux) IPX (Novell).

File Server: Enables remote clients to access files and other resources over the network

Watchdog: A watchdog timer that triggers a system reset upon software freezes, for both specific applications and system-wide failures.

Application Development Software:

- Moxa API Library
- GNU C/C++ cross-compiler
- GNU C library
- Perl

Software Package:

- SNMP
- SafeGaurd technology

Terminal Server (SSH): Provides secure encrypted communications between two un-trusted hosts over an insecure network

Tailored MIB File for SNMP Control: SNMP allows centralized network monitoring and control. With Moxa's proprietary MIB file, trap notifications keep network overhead low while providing monitoring and control of key BIOS settings; internal hardware sensors; interface connectivity for DI/DO, USB, and UART; and other peripheral devices.

System Initialization

In this chapter, we describe how to initialize the system settings on the V2406A embedded computer when booting up for the first time.

The following topic is covered in this chapter:

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

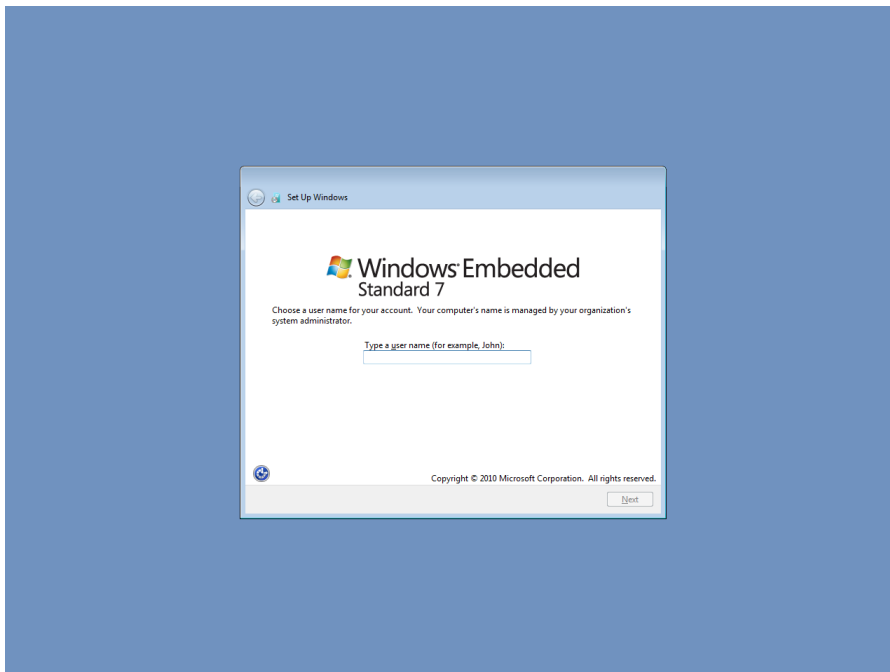
Overview

Similar to using a laptop computer for the first time, you need to specify a user name and create a user account to start using the V2406A embedded computer. Follow the procedure described in the next section.

NOTE If you perform a system recovery on the V2406A embedded computer, the system automatically resets to the factory defaults. You must initialize the user settings again.

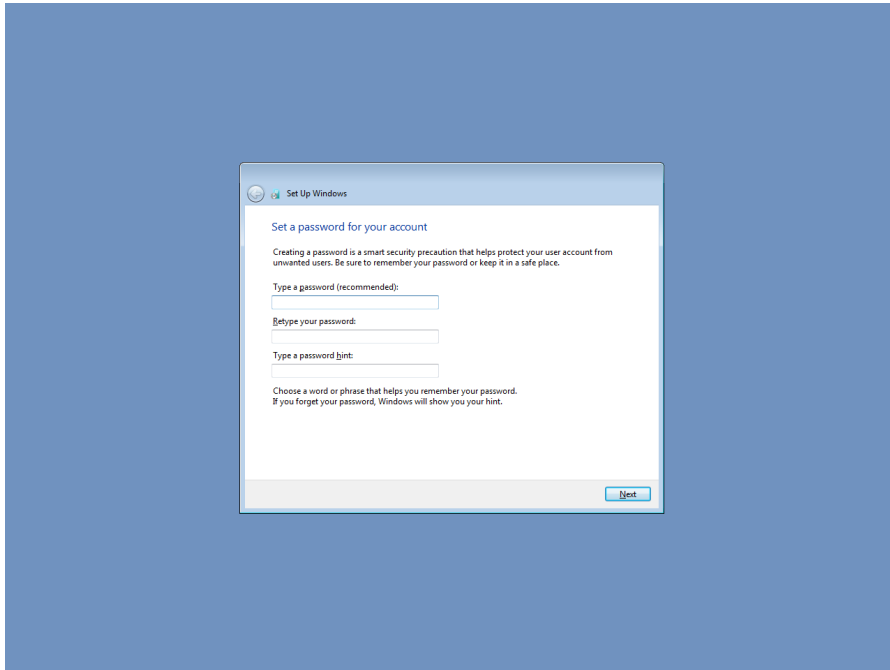
Initializing User Settings

1. When you turn on the embedded computer for the first time, enter a user name for the computer.

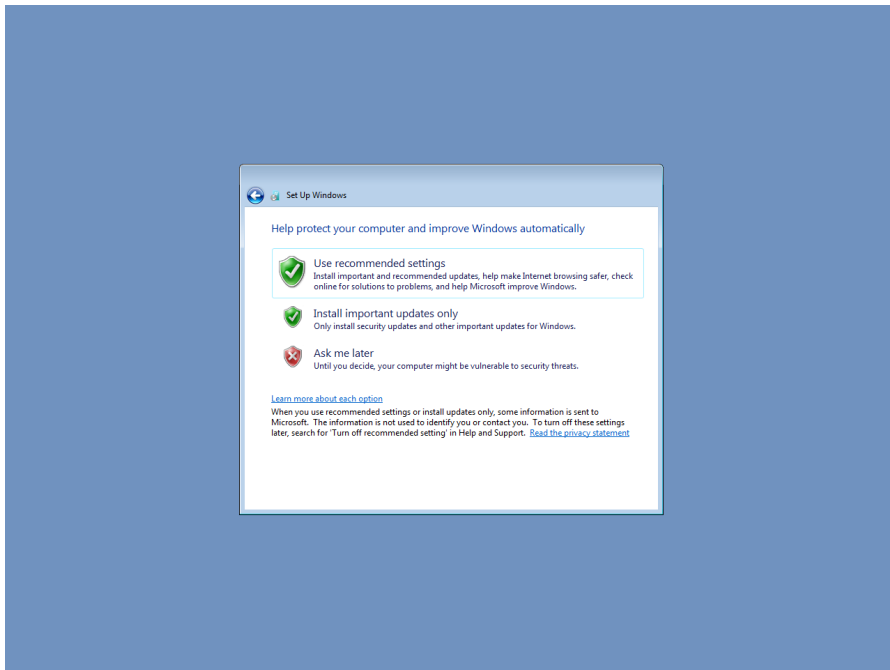


2. Type a password and retype the password to confirm.

You may also type a password hint that you can refer to if you forget your password. If you do not want to set a password, leave all three fields blank. Click **Next** to continue.

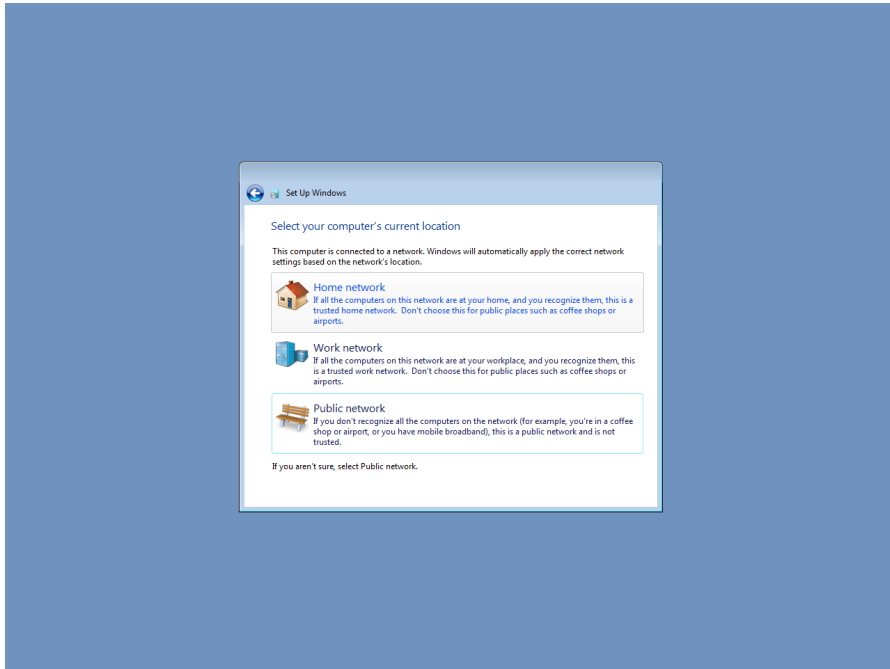


3. Select a Windows update option.

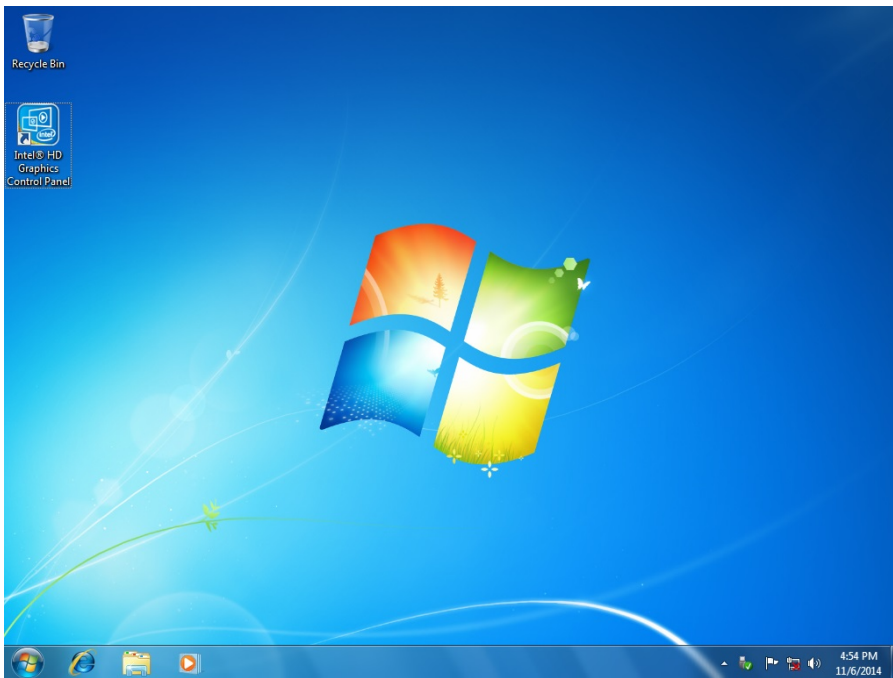


4. Select the computer's current location.

Windows automatically applies the appropriate network settings based on the type of network you select.



5. When the Windows desktop screen appears, you can start using your V2406A embedded computer.



Configuring the Serial Interface

This chapter describes how to configure the serial interface on the V2406A embedded computer.

The following topics are covered in this chapter:

- **Overview**
- **Configuring the Serial Interface Mode**

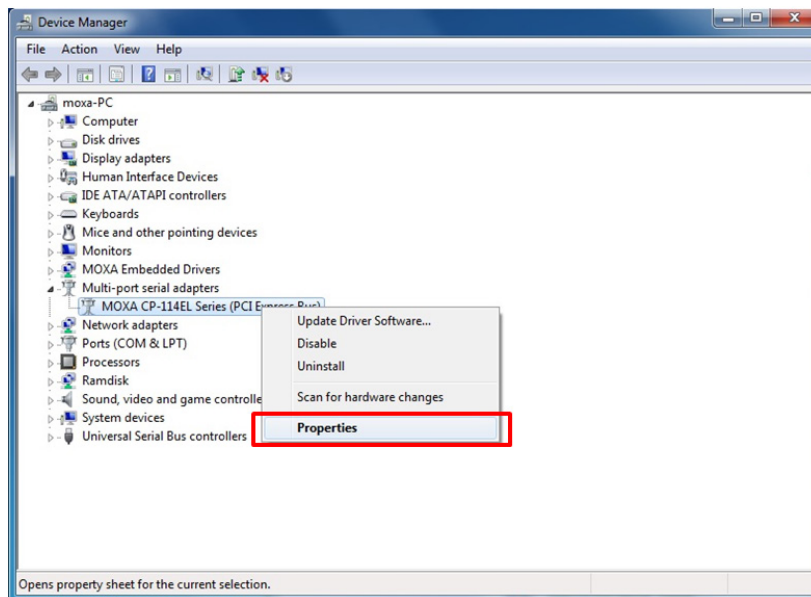
Overview

The V2406A supports the following serial modes: **RS-232**, **RS-485-2-wire** and **RS-422/485-4-wire**. These modes can be configured from COM1 to COM4.

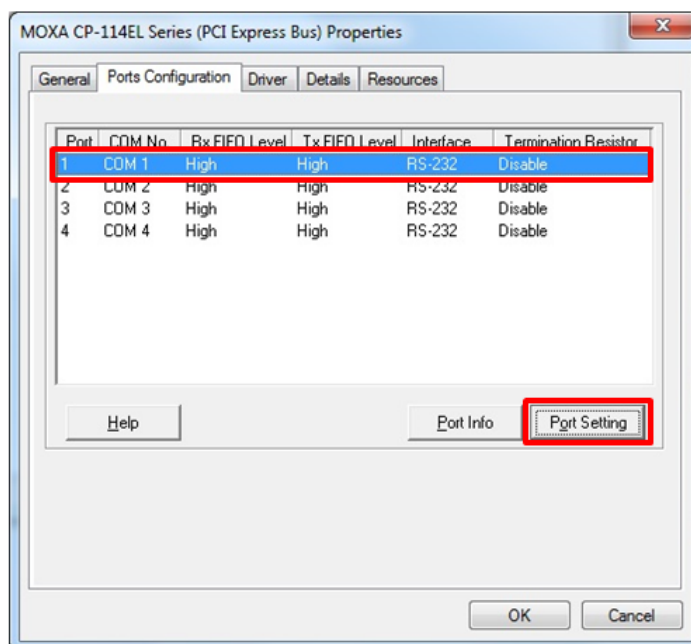
Configuring the Serial Interface Mode

Complete the following steps to configure the serial interface mode:

1. Open Device Manager.
2. Under **Multi-port serial adapters**, right-click **MOXA CP-114EL Series (PCI Express Bus)** and select **Properties**.

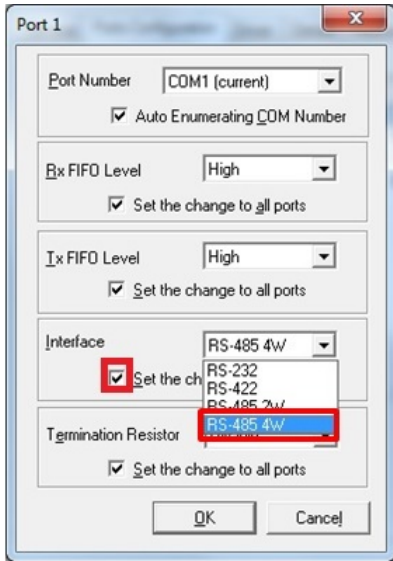


3. Click the **Ports Configuration** tab and select the COM port to configure (for example, COM1); then, click **Port Setting**.

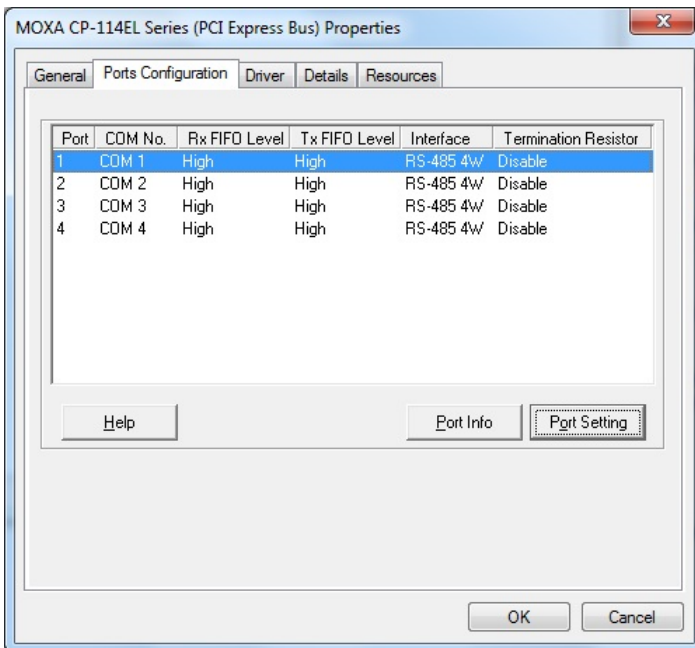


- 4. From the **Interface** drop-down list, select a serial mode and click **OK**.

NOTE By default, the serial mode setting applies to all ports on the V2406A computer. If you want to configure the serial mode for a port, clear the **Set the change to all port** check box.



- 5. Check that the serial interface is correct.



Enabling Embedded Filters

In this chapter, we describe how to enable the V2406A's embedded filters.

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**

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

Enhanced Write Filter

Overview

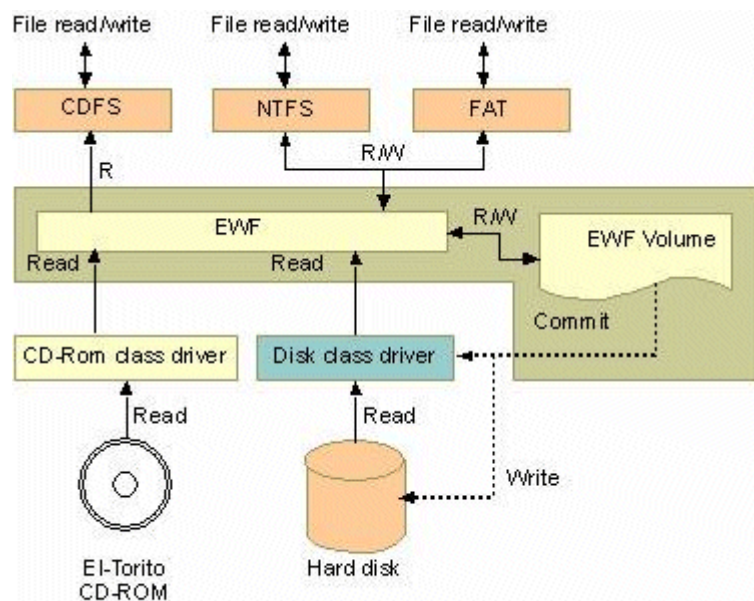
Enhanced Write Filter (EWF) enables you to protect a volume from unauthorized writes by making the main operating system (OS) drive a write-protected volume, effectively making the system a read-only system for most users. This provides much stronger protection against malicious computer attacks (such as trojans, worms, and viruses).

Enhanced Write Filter (EWF) allows Windows 7 users to protect data on their storage drive from permanent changes of any sort, at the lowest level of hardware protection available: the bit level. **EWF** allows the 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 the following figure) are only recorded on this virtual overlay (the **EWF Volume** in the following figure), which is stored independently in random access memory (RAM).

Because EWF does not write data directly to the hard disk but instead only records 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 required, data written to the overlay can be committed to the protected volume, but this requires additional setup and permissions that can only be granted by the administrator.

The following figure shows an overview of the EWF structure.



For more detailed information about EWF configuration and usage, refer to the following resources:

- Visit Microsoft's [EWF Volume Configuration](#) help pages.
- See Microsoft's [EWF overview](#) on the official Microsoft EWF help pages.
- See Microsoft's detailed description of [EWF modes](#) on the EWF help pages.
- See Microsoft's detailed description of the [EWF API](#).
- For EWF commands, refer to the MSDN web site:
<http://msdn.microsoft.com/en-us/library/ms940853%28v=winembedded.5%29.aspx>

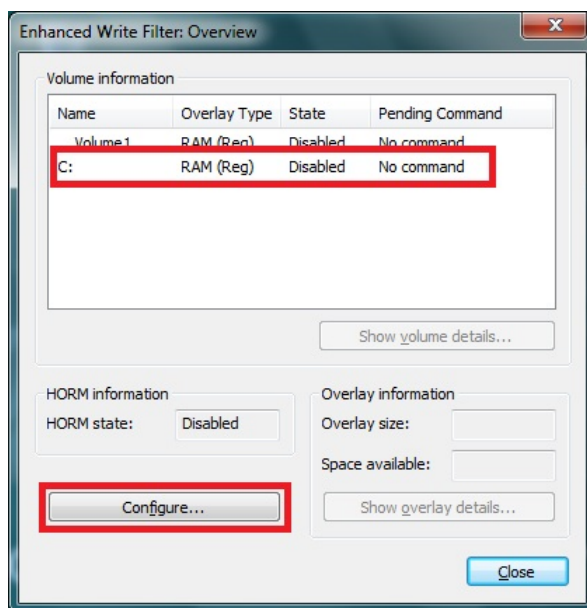
Enabling Enhanced Write Filter

Follow these steps to enable Enhanced Write Filter (EWF):

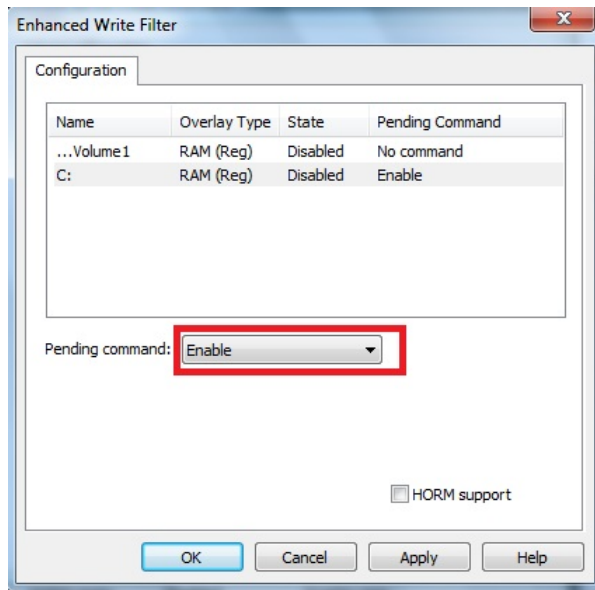
1. To open EWF, double-click the padlock icon in the system tray.
2. You may need to show hidden icons in the system tray.



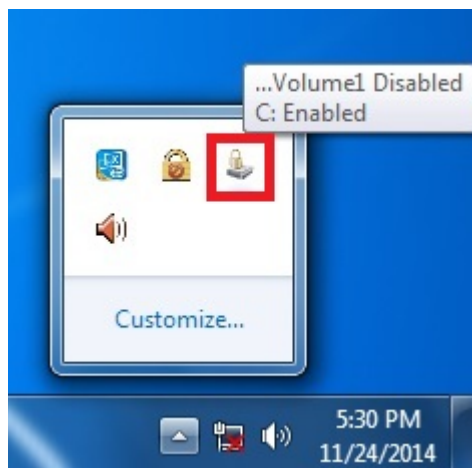
3. In the **Volume Information** area, select the partition you want to enable write-protection on and click **Configure...**



- The Configuration dialog box appears. Select **Enable** from the **Pending command** drop-down list and click **OK**.



- Reboot the system.
- Log into the system and verify that the padlock icon in the system tray indicates that the drive volume is locked with EWF.

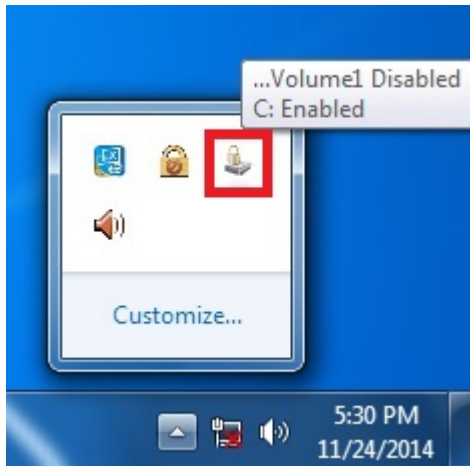


Committing Data and/or Disabling EWF

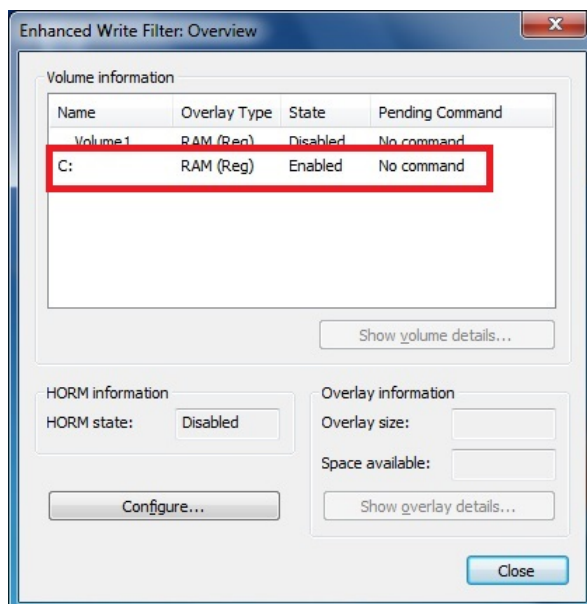
Perform the following steps to write (or commit) data to an EWF-enabled drive.

NOTE You must have administrator privileges to commit data to the drive.

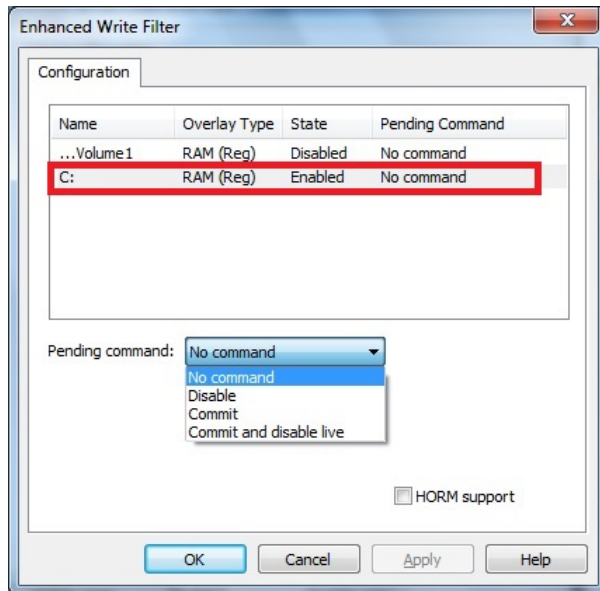
1. Double-click the padlocked drive in the system tray.
You may need to show hidden icons in the system tray.



2. In the **Enhanced Write Filter: Overview** dialog box, select the drive you want to configure and click **Configure**.



3. In the Enhanced Write Filter Configuration screen, select a drive volume; then, select an option from the **Pending Command** drop-down list:
- **No Command**
 - **Disable:** Disables EWF on the selected drive. The system automatically reboots if you select this option.
 - **Commit:** Writes all current system changes to the hard drive.
 - **Commit and Disable Live:** 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). The system does not automatically reboot if you select this option.



NOTE For detailed information, go to the Microsoft website at [http://msdn.microsoft.com/en-us/library/ff794092\(v=winembedded.60\).aspx](http://msdn.microsoft.com/en-us/library/ff794092(v=winembedded.60).aspx).

File-Based Write Filter

This section describes how to use the File-Based Writer Filter (FBWF). Note that when Enhanced Writer Filter is enabled, the File-Based Writer Filter function will not work.

According to 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.”

FBWF supports an advanced ESF feature, which allows users to specify which directory to write data to. The default directory is c:\temp. The advanced feature allows you can read/write data to disk without committing an action.

Configuring File-Based Write Filter

Complete the following steps to enable the File-Based Write Filter (FBWF) feature. Note that although FBWF and EWF may both be enabled on the same machine, FBWF does not protect a volume that is already protected by EWF. Similarly, EWF does not protect a volume that is already protected by FBWF.

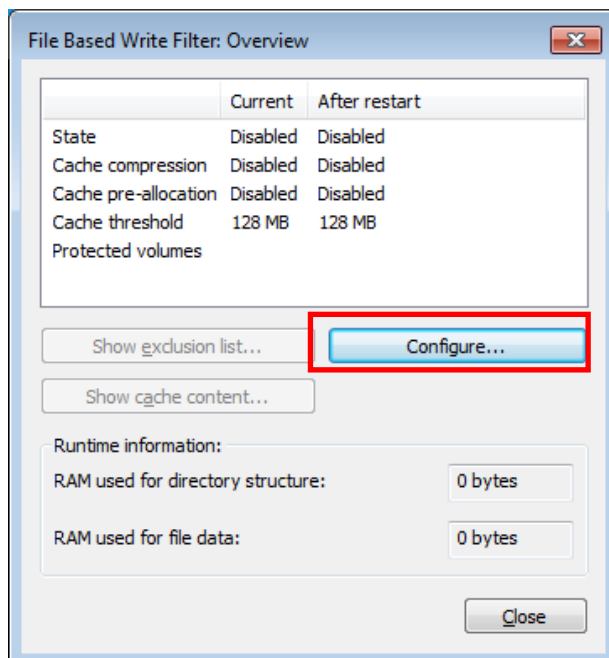
NOTE Before using FBWF, make sure that you disable EWF.

1. Double-click the padlock icon in the system tray.
You may need to show hidden icons in the system tray.

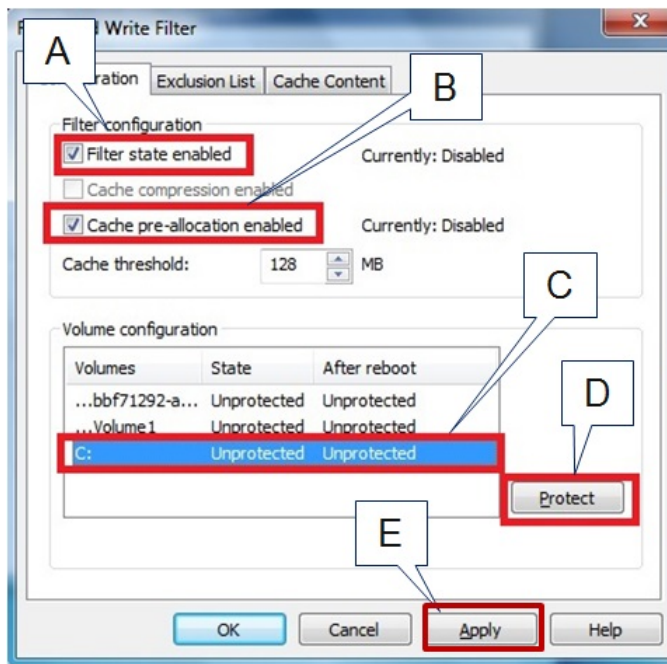
NOTE When disabled, the EWF and FBWF icons in the system tray look the same. To verify that you have opened the correct writer filter program, check the screen title.



2. In the **File Based Writer Filter: Overview** screen, click **Configure**.

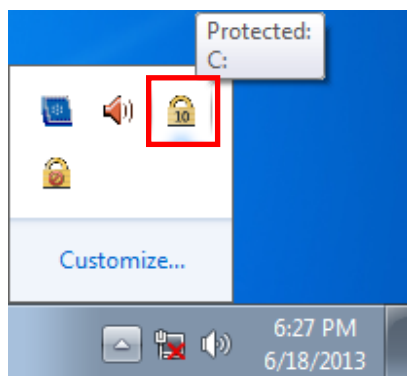


3. To enable FBWF protection on a storage drive, perform the following actions:
 - a. Select **Filter state enabled** and **Cache pre-allocation enabled**.
 - b. In the **Volume Configuration** area, select the storage drive you want to protect and click **Protect**.
 - c. Click **Apply** or **OK**.



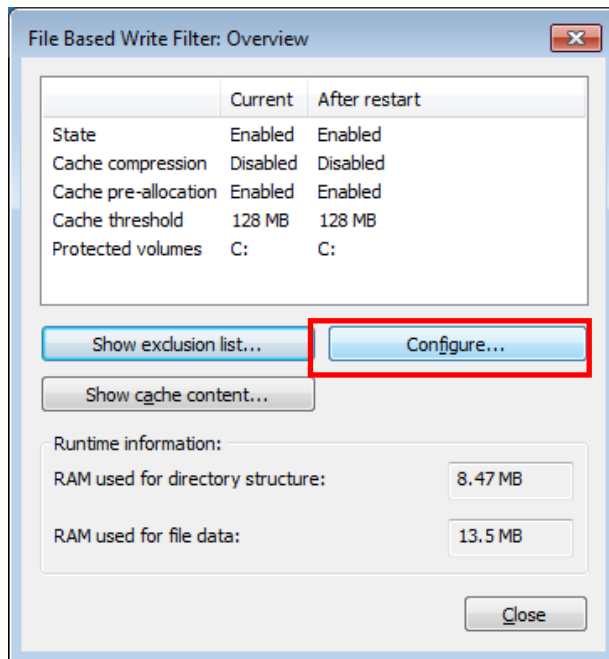
NOTE To minimize memory usage on the overlay cache, select **Cache compression enabled**. However, cache compression decreases performance when accessing protected volumes. Select **Cache pre-allocation enable** to set the memory space available for the overlay cache when the system starts up, instead of adjusting it as needed. You cannot enable cache pre-allocation and cache compression at the same time. The **cache threshold** field sets 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 depending on the operating system.

4. Reboot the system.
5. Log into the system and verify that the padlock icon in the system tray displays a number and indicates that FBWF is enabled on a drive. The following figure shows an example.

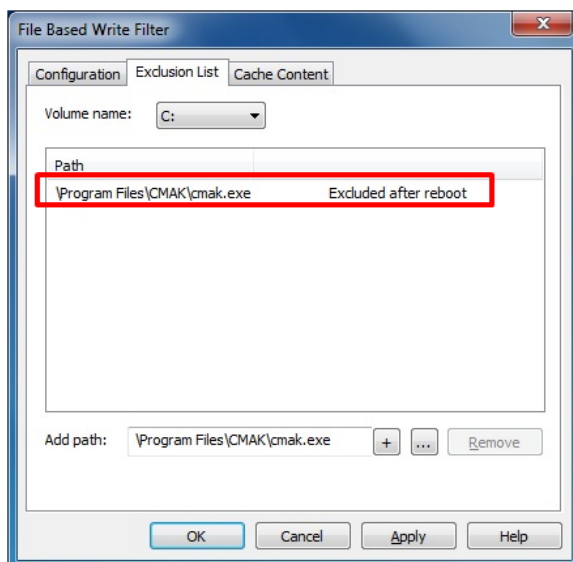


Excluding Files from FBWF Protection

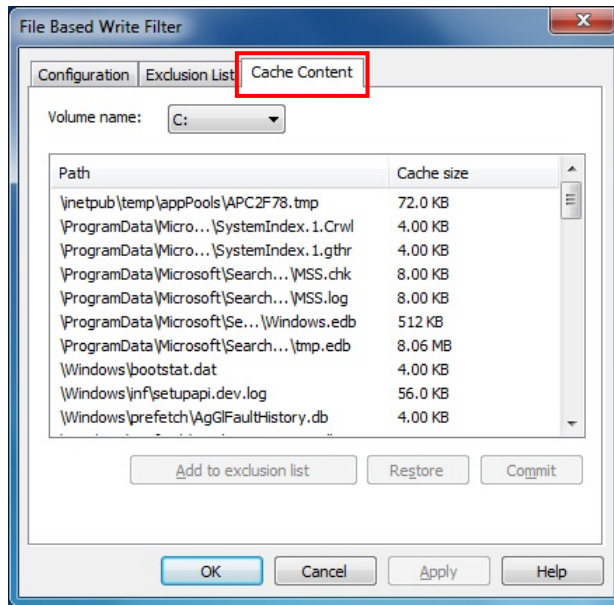
1. Double-click the FBWF icon in the system tray.
You may need to show hidden icons in the system tray.
2. In the **File Based Write Filter: Overview** window, click **Configure**.



3. Click the **Exclusion List** tab and configure the following fields:
 - **Volume name** – Select a drive volume from the drop-down list.
 - **Add path** – click the ellipsis (...) button to select a directory or file you want to exclude from FBWF protection; then click the + button. The system displays the selected directory or file in the **Path** table.



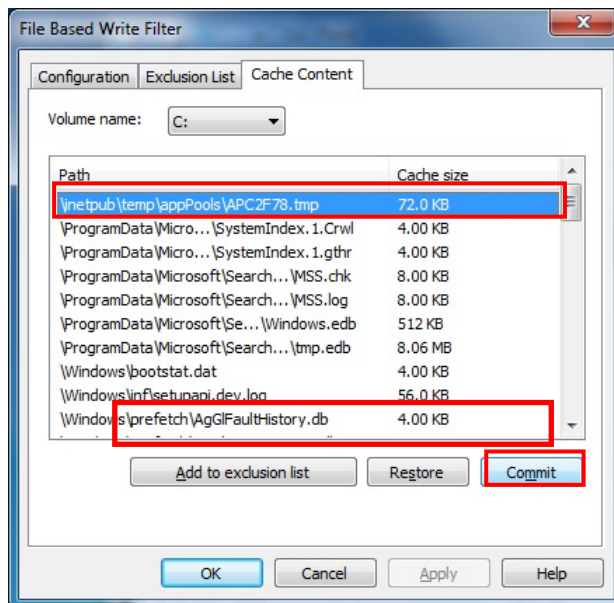
4. Click the **Cache Content** tab and click **Apply** and **OK**.



5. Reboot the system to make the changes take effect.

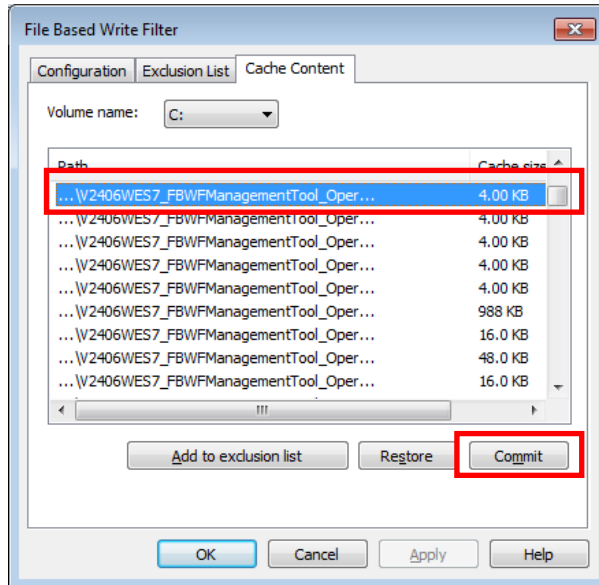
Managing Temporary Files Cached in the Overlay

1. On the **Cached Content** tab, you will see all the files currently cached in the RAM overlay. Three commands are available:
 - **Commit:** Save a file from the cache to permanent storage, delete the file from the overlay, and overwrite the original file.
 - **Restore:** Return the file to its original state, remove the file from the overlay cache and discard the changes that added the file to the cache.
 - **Add to exclusion list:** Adds the file to the exclusion list after the next restart. This will delete the file from the cached overlay and replace the current file in permanent storage with the modified cache file.



2. The most common usage of the Cache Content filter 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.

Keep in mind that committing a configuration or application file will permanently alter the setup and/or performance of the application or system.



For more details about FBWF configuration and usage, refer to the Microsoft help file that came with your computer, or go to the following websites:

- Microsoft's [FBWF Installation and Configuration](#) help pages.
- Microsoft's [FBWF overview](#) on the official Microsoft FBWF help pages.
- Microsoft's detailed description of [FBWF features](#) on the FBWF help pages.
- Microsoft's detailed description of the [FBWF API](#).

Moxa Diagnostic Package

In this chapter, we describe the software package that can be used to monitor the system status of the V2406A computer.

The following topics are covered in this chapter:

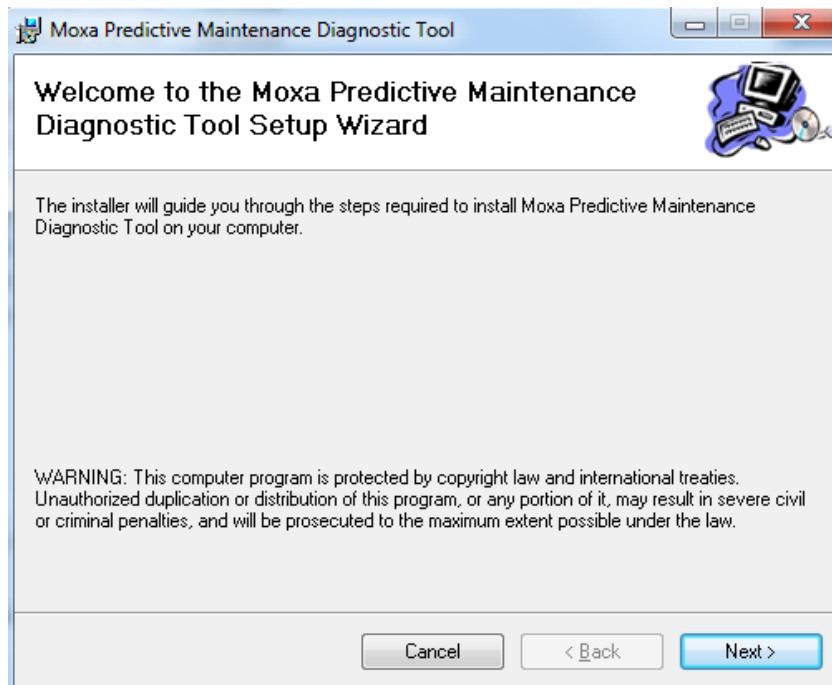
- ❑ **Installing Moxa Diagnostic Utility**
- ❑ **Using Moxa Diagnostic Utility**

Installing Moxa Diagnostic Utility

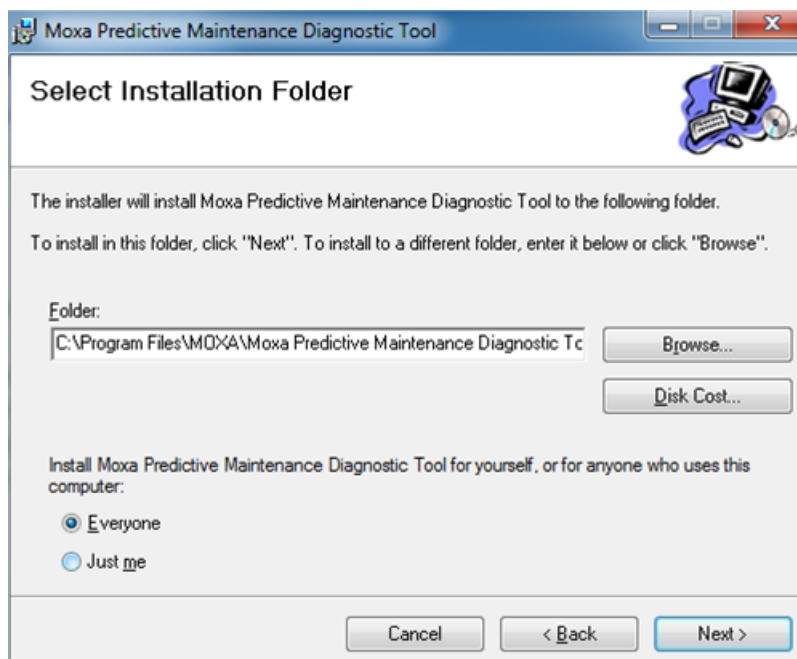
To use Moxa Diagnostic Utility on the V2406A computer, first install the Moxa Diagnostic package.

Complete the following steps to install the Moxa Diagnostic package.

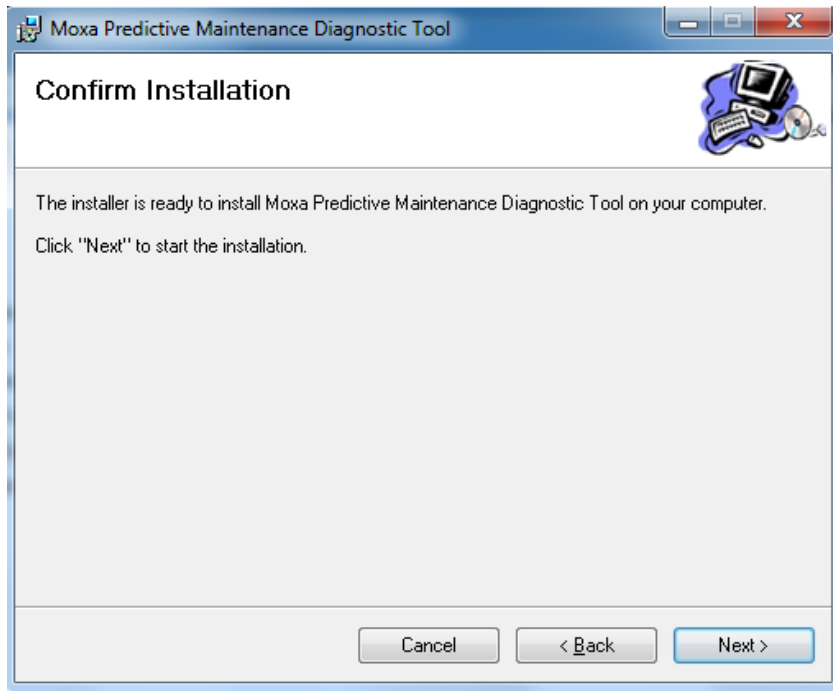
1. In the \utility\mxdiagnostic\ folder on the software DVD, double-click **mxDiagnosticTool.msi**.
2. A Welcome screen appears. Click **Next**.



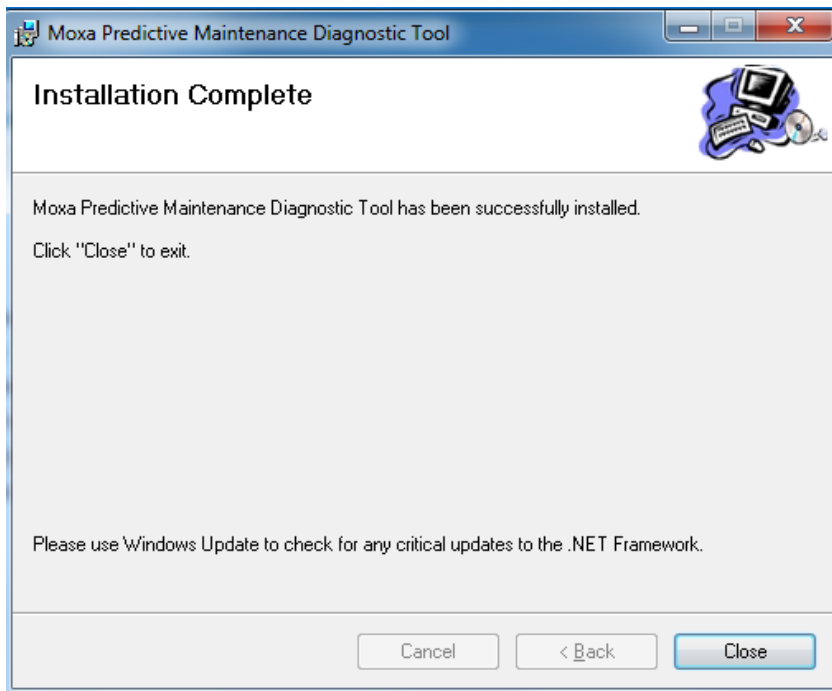
3. Accept the default folder location or click **Browse** to select an installation folder; then, click **Next**.



4. Click **Next** to continue.



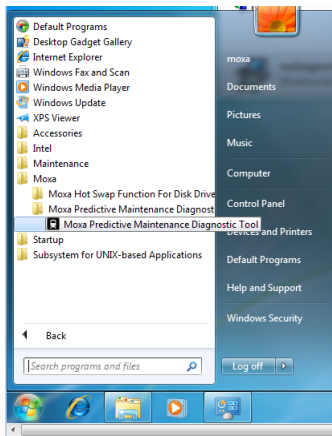
5. Click **Close** to complete the installation process.



Using Moxa Diagnostic Utility

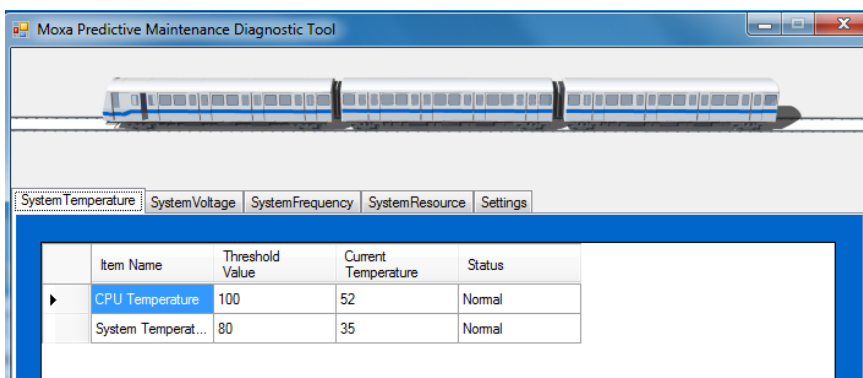
This section describes how to use the Moxa Diagnostic Utility on the V2406A.

1. From the Start menu, click **All Programs > Moxa > Moxa Predictive Maintenance Diagnostic Tool > Moxa Predictive Maintenance Diagnostic Tool**.

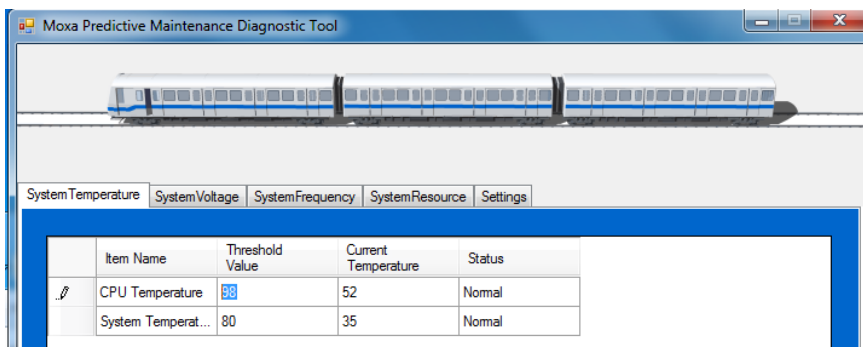


2. The **System Temperature** tab shows the current and threshold values of the CPU and system temperatures (in degrees Celsius).

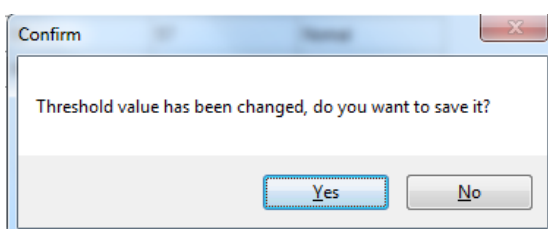
When the current temperature exceeds the threshold value, the screen displays “warning” in the **Status** field and logs the status change.



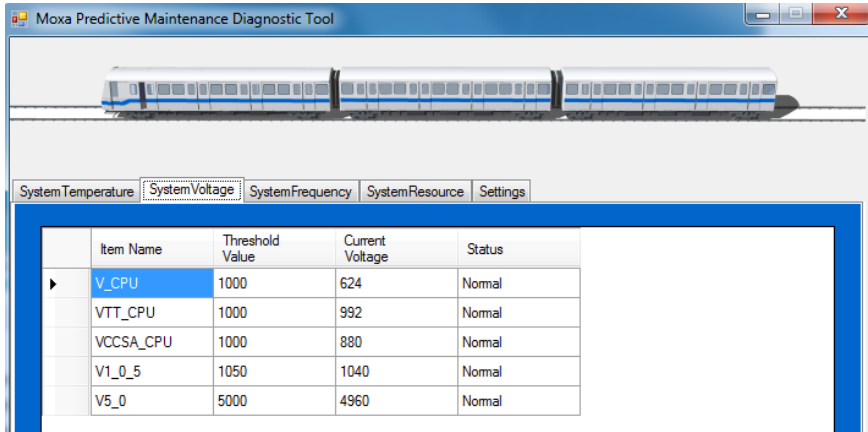
3. To change the threshold value, double-click the value in the **Threshold Value** field and enter a number.



4. Click **Yes** to save the changes.

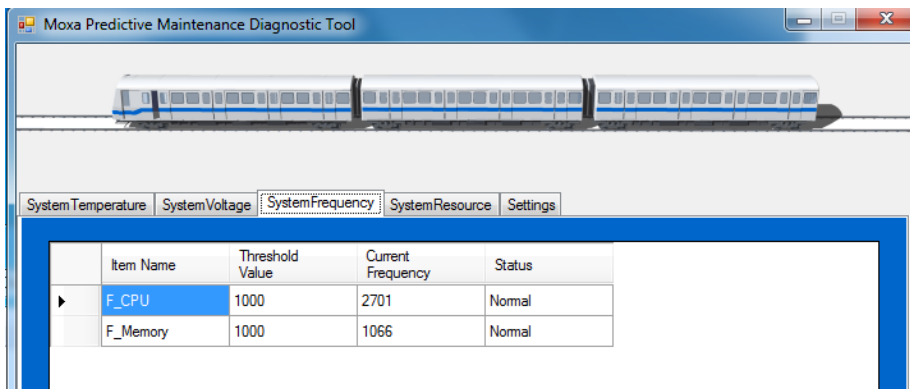


- Click the **System Voltage** tab to view the current system voltages (in V).

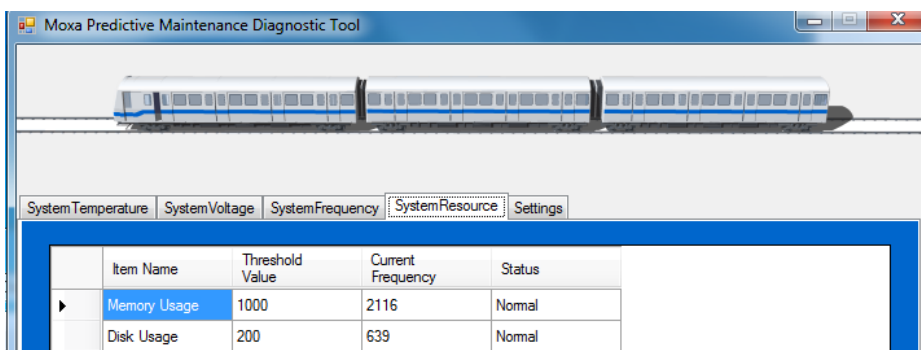


NOTE V_CPU = Voltage for processor core
 VTT_CPU = Voltage for L3 shared cache, memory controller, and processor I/O power rail (Uncore)
 VCCSA_CPU = Voltage for CPU System Agent
 V1_0_5 = (VCCIO) = Voltage for processor uncore
 V5_0 = Voltage for other chips

- Click the **System Frequency** tab to view the current system frequency.

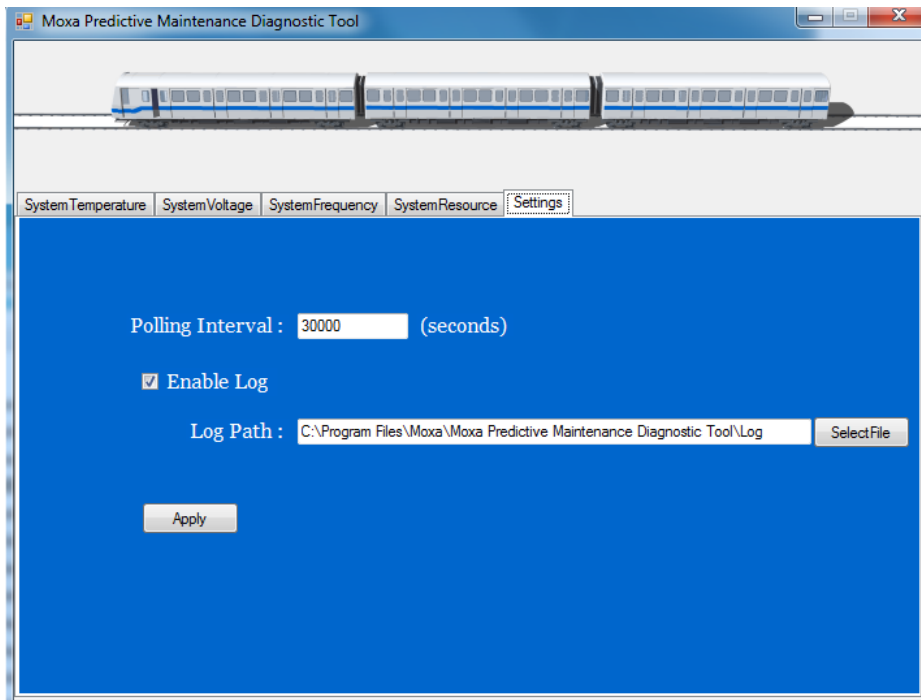


- Click the **System Resource** tab to view the current resource usage.

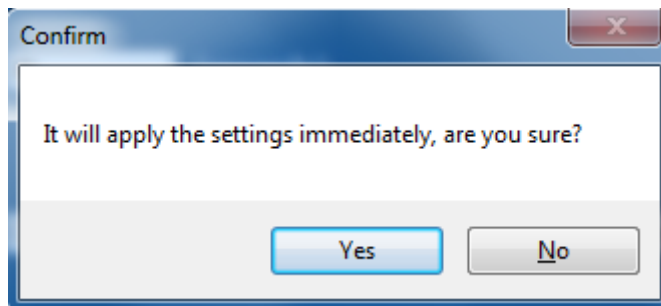


- Click the **Settings** tab to set the polling interval and log options.

NOTE If the folder you specify in the **Log Path** field does not exist, the system automatically creates the folder when new logs are recorded.



- To save the settings, click **Apply**.
- Click **Yes** to confirm.



Moxa SynMap Package

In this chapter, we describe the software package that can be used to easily control and monitor V2406A computers.

The following topics are covered in this chapter:

- ❑ **Moxa SynMap Package**
 - Overview
 - Moxa SynMap OID List
- ❑ **Installing CrystalDiskInfo**
- ❑ **Installing the Moxa SynMap Package**
- ❑ **Installing MXview**
- ❑ **Configuring MXview**
- ❑ **Loading the Moxa SynMap MIB File**
- ❑ **Loading the Host Resource MIB File**
- ❑ **Using Moxa SynMap OIDs**
- ❑ **Using HOST RESOURCE OIDs**

Moxa SynMap Package

Overview

SynMap is Moxa's revolutionary software virtualization tool, which adapts SNMP into a fully portable remote procedure interface. SynMap allows engineers to automate remote processes using SNMP object identifiers (OIDs) rather than device-specific addresses, 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 to rewrite and compile code for newly configured devices, significantly reducing maintenance and deployment times.

SNMP is lightweight and easy-to-configure, and has long been popular with IT professionals. SNMP also enjoys comprehensive native support in high-level languages, including .NET, Java, Python, and Ruby. For these reasons, the SynMap framework has re-purposed SNMP into 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 C 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 the simple, reliable, and familiar SNMP, the easily accessible standard every IT engineer knows. Discover how Moxa is expanding automation frontiers with the innovation we call SynMap.

Moxa SynMap OID List

For a complete listing of Moxa SynMap OIDs, refer to **Appendix A: Moxa SynMap OID Table**.

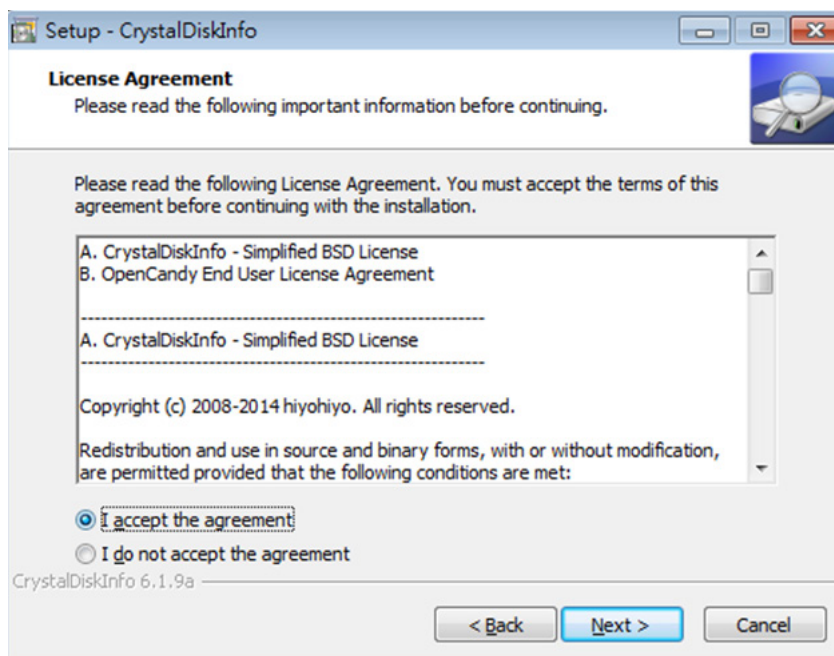
Installing CrystalDiskInfo

Complete the following steps to install CrystalDiskInfo, a disk health diagnostics tool that allows you to monitor the health of a disk.

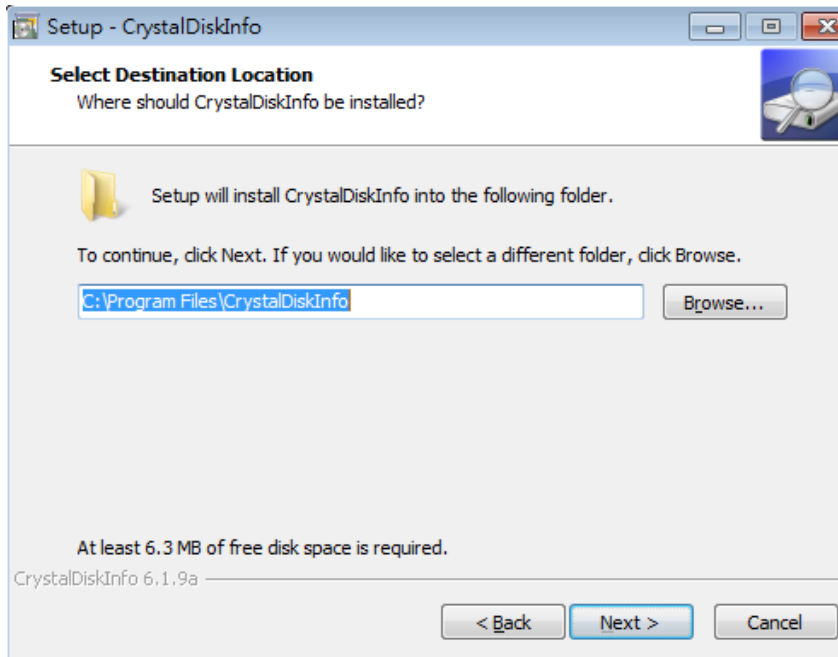
1. On the software DVD, click **CrystalDiskInfo6_1_9a-en.exe** in the `\utility\mxSynMap\` folder.
2. A Welcome screen appears. Click **Next**.



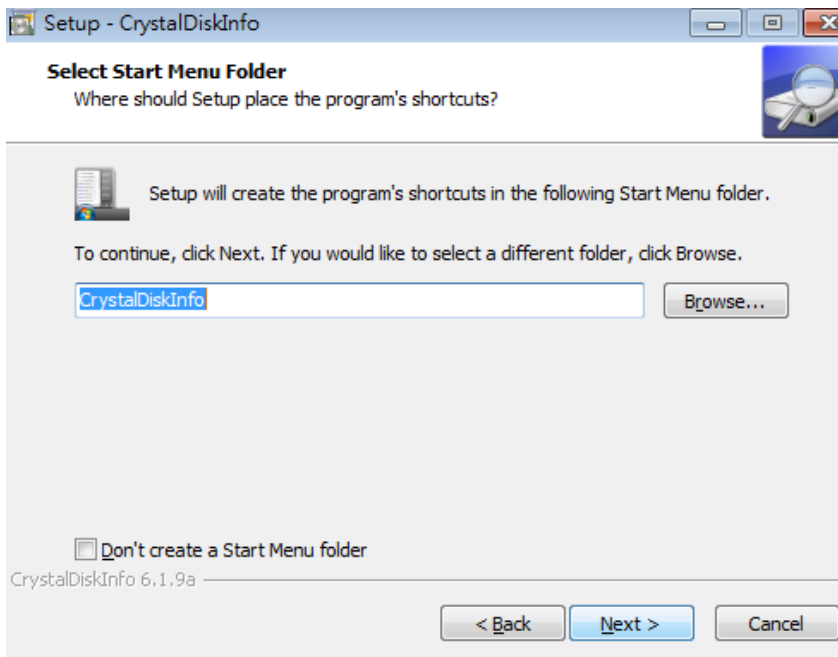
3. Select **I accept the agreement** and click **Next**.



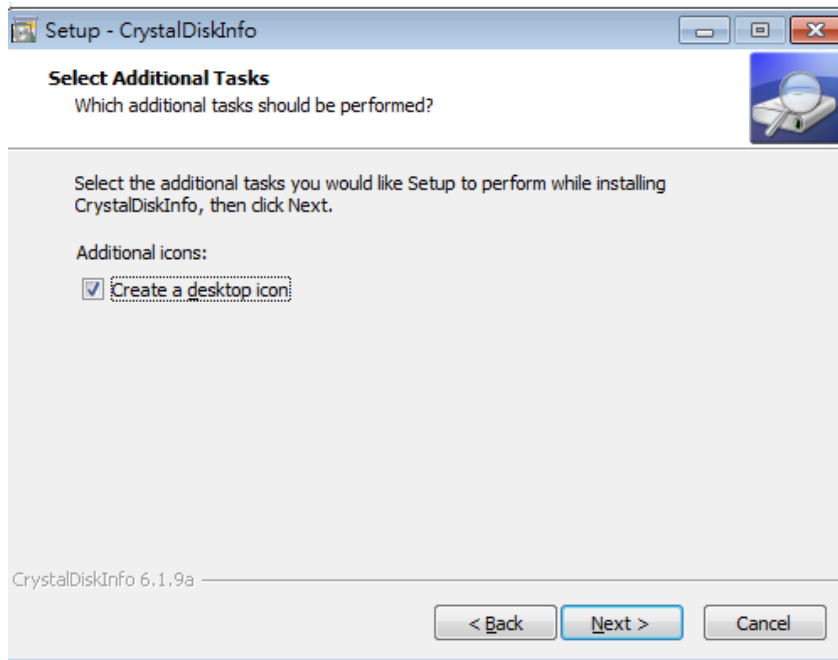
4. Accept the default destination folder or click **Browse** to select one; then, click **Next**.



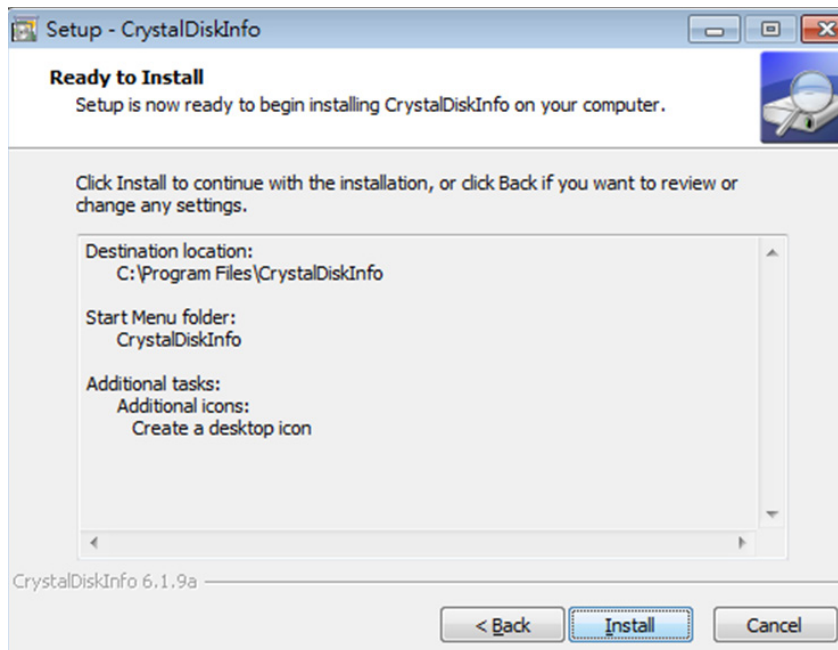
5. Accept the default Start menu folder or click **Browse** to select one; then, click **Next**.



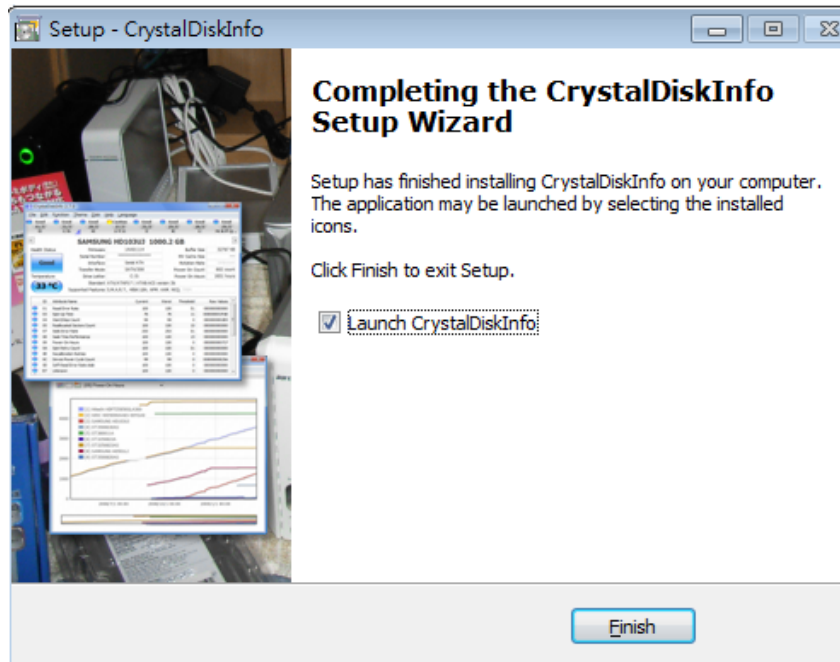
- 6. Click **Next**.



- 7. Click **Install**.



- Click **Finish**.

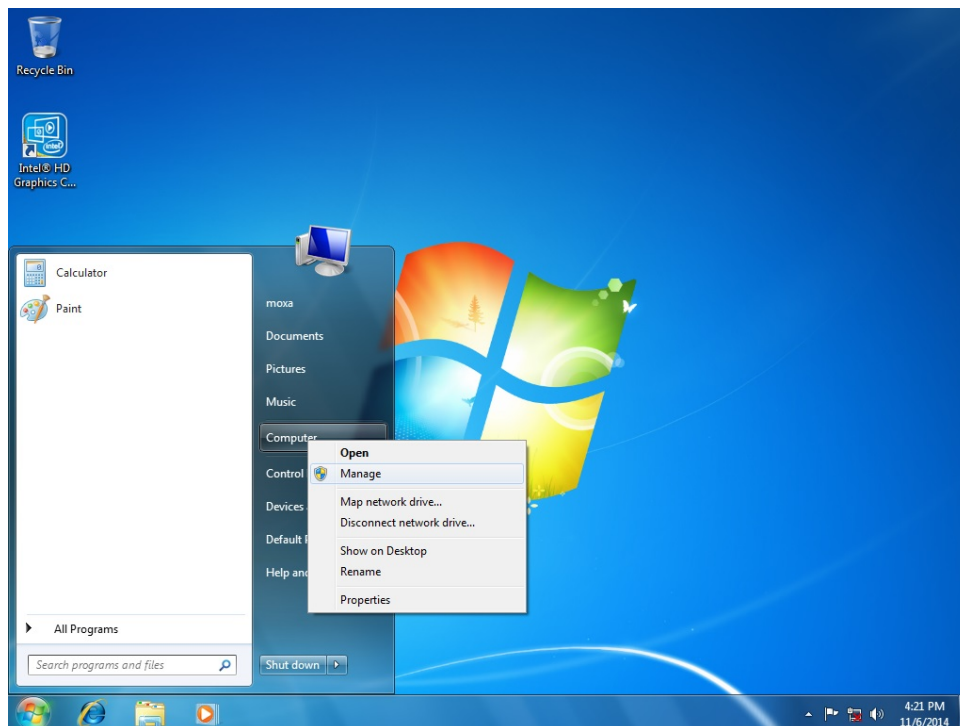


- Add a shortcut in the **startup** folder to execute the program when system boots up.

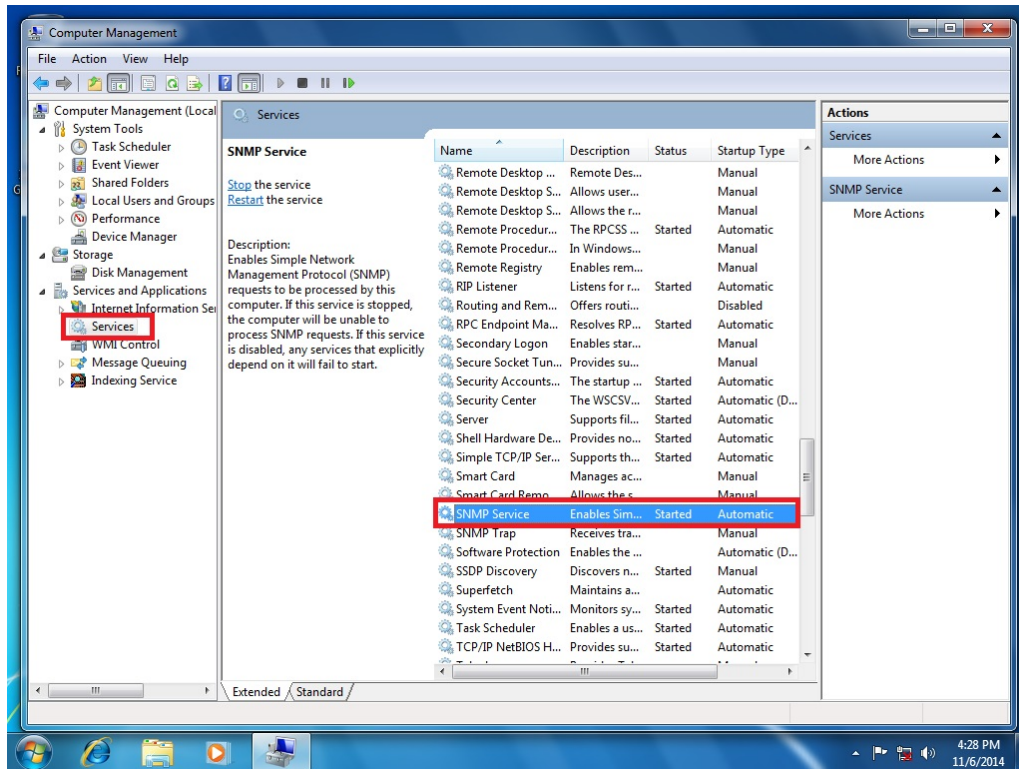
Installing the Moxa SynMap Package

Before you install the Moxa SynMap Package, disable the Windows SNMP server. Complete the following steps:

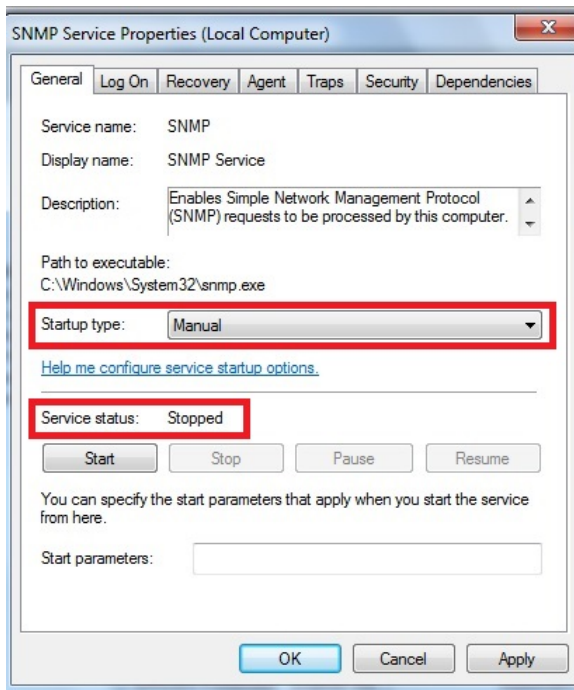
- From the Start menu, right-click **Computer** and select **Manage**.



- In the **Computer Management** screen, select **Services** under **Service and Applications**.



3. In the **Services** pane, double-click **SNMP Service**.
4. In the SNMP Service Properties window, select **Manual** from the **Startup type** drop-down list and set the **Service status** field to **Stopped**.



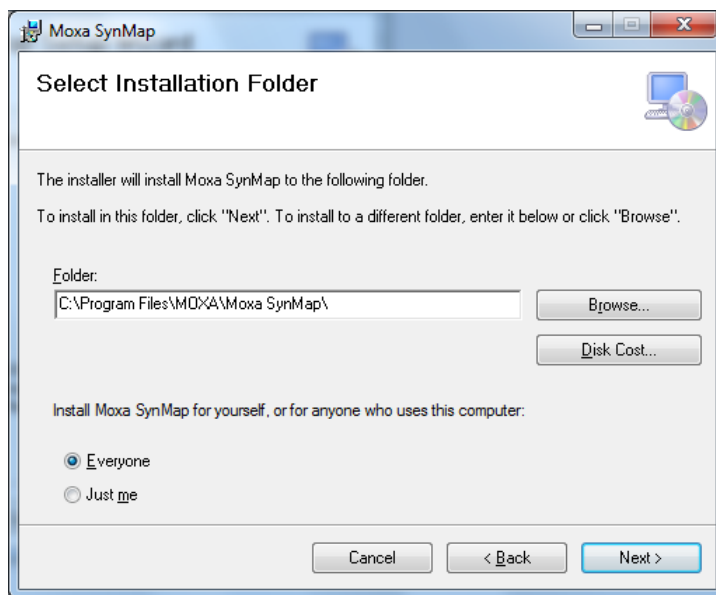
5. Click **Apply** and **OK** to disable the Windows SNMP service.

To install the Moxa SynMap package, complete the following steps:

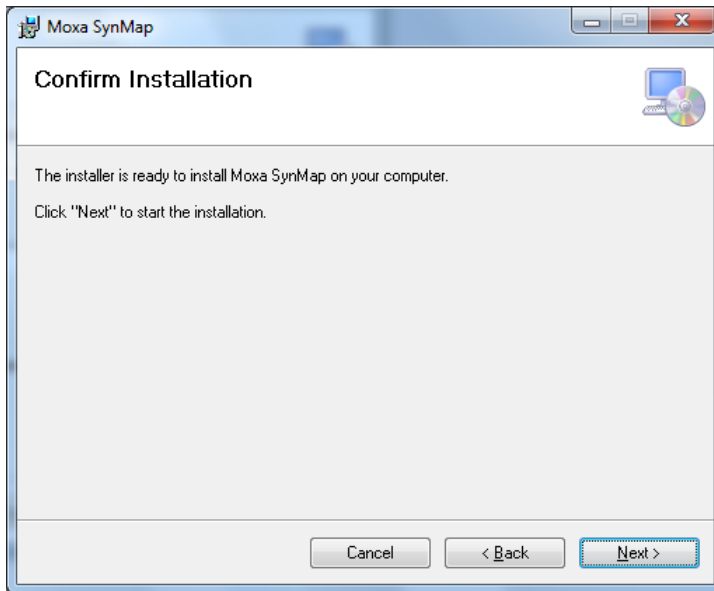
1. On the software DVD, double-click **mxSynMap_setup** in the **\utility\mxSynMap** folder.
2. A Welcome screen appears. Click **Next**.



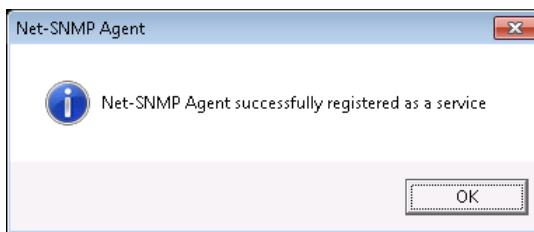
3. Accept the default installation folder or click **Browse** to select one; then, click **Next**.



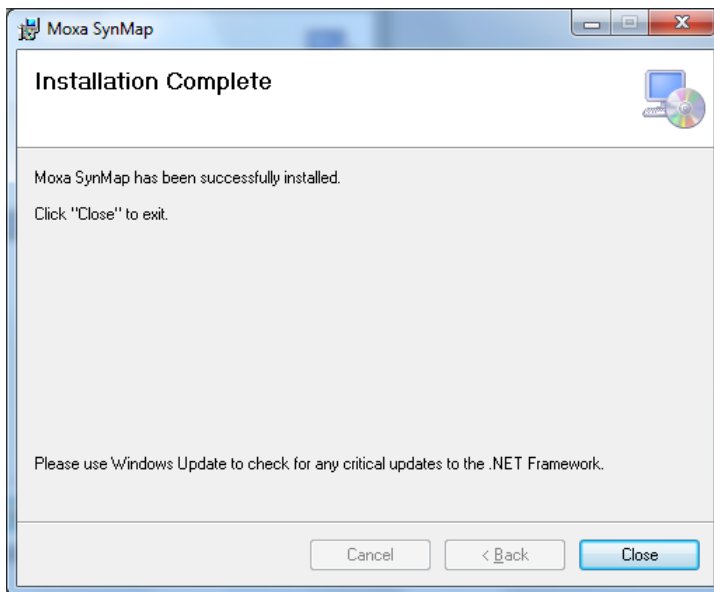
4. Click **Next** to continue.



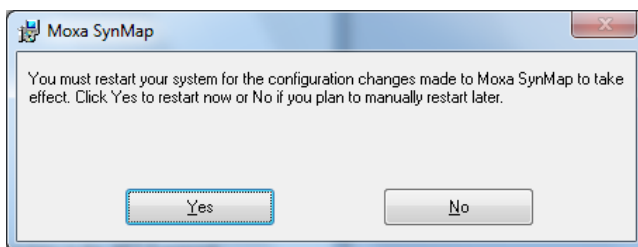
- 5. Click **OK** to continue.



- 6. When the installation process is complete, click **Close**.



- 7. When prompted, click **Yes** to restart the V2406A to use the SNMP functions.

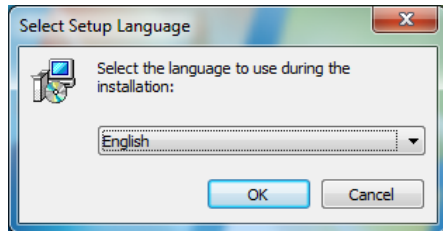


Installing MXview

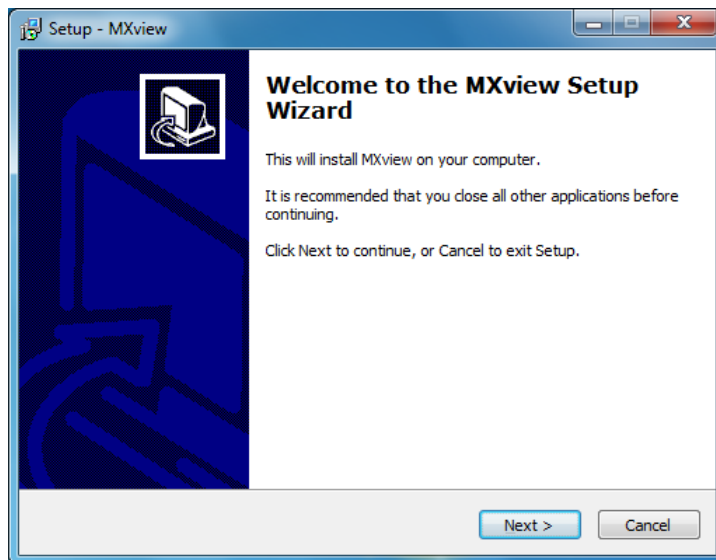
This section describes how to use the MIB browser (mxView) to monitor or control Moxa SynMap OIDs. If you already have your own MIB browser, skip this section.

Complete the following steps to install the MXview package:

1. On the software DVD, double-click **MXView_Trial_V2.4.exe** in the `\utility\mxViewTrial` folder.
2. In the **Select Setup Language** screen, select a language from the drop-down list and click **OK**.



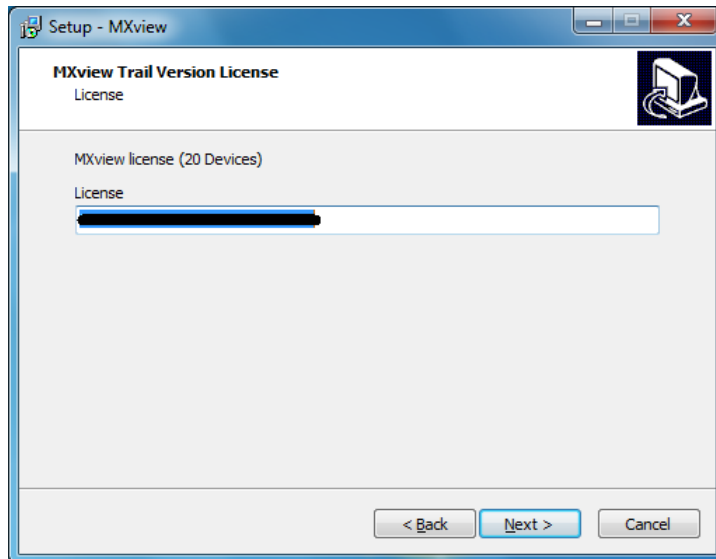
3. Click **Next**.



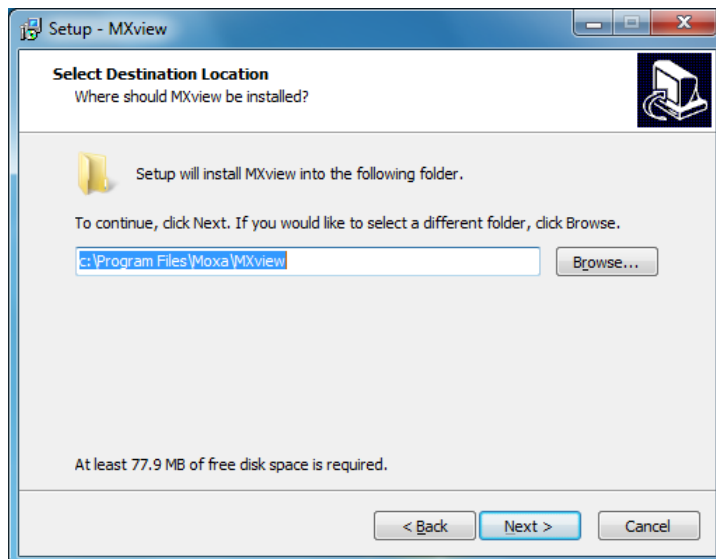
4. Select **I accept the agreement** and click **Next**.



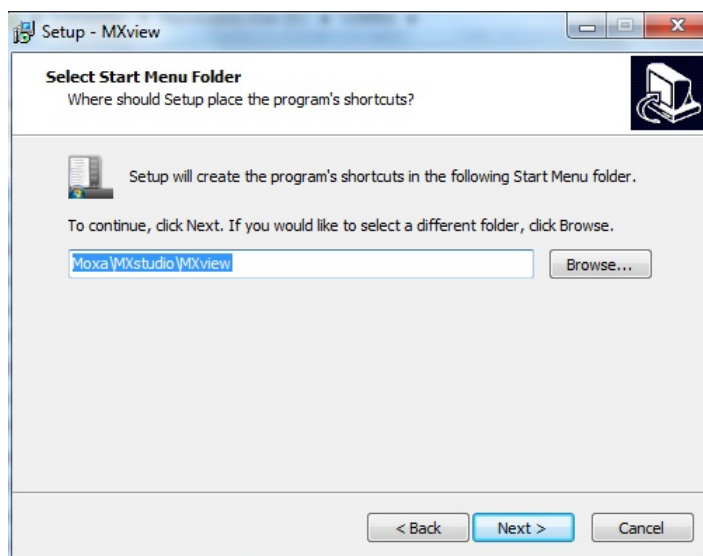
5. Click **Next**.



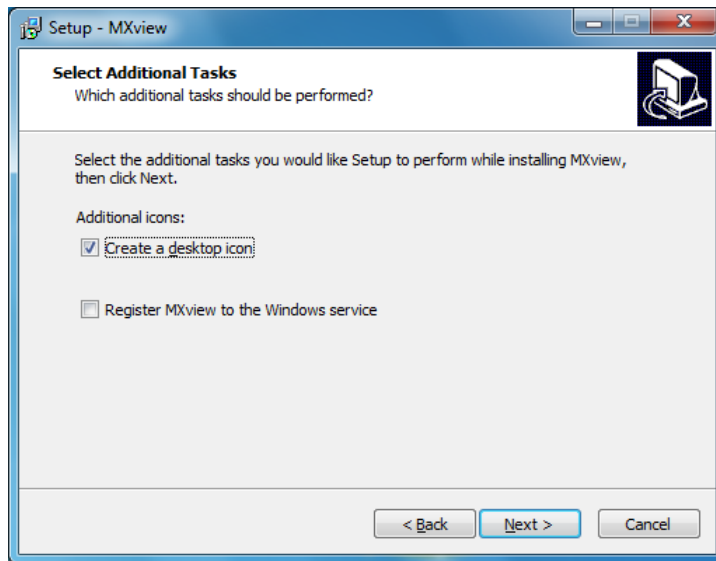
6. Accept the default destination folder or click **Browse** to select one; then, click **Next**.



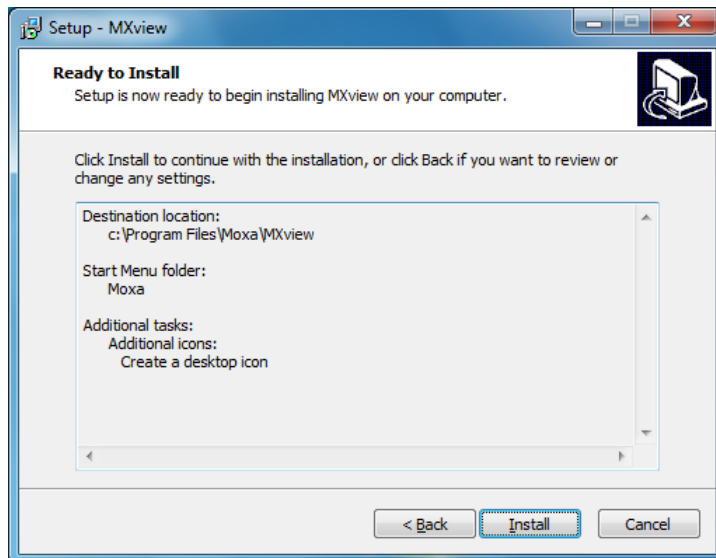
7. Click **Next** to continue.



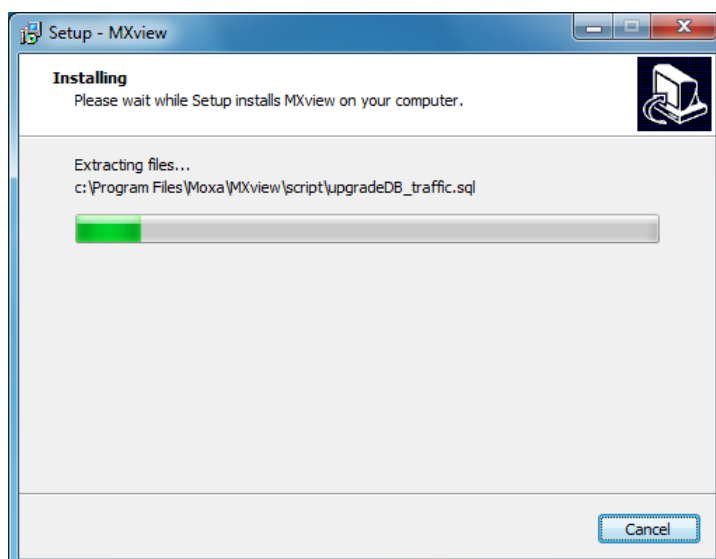
8. Click **Next** to continue.



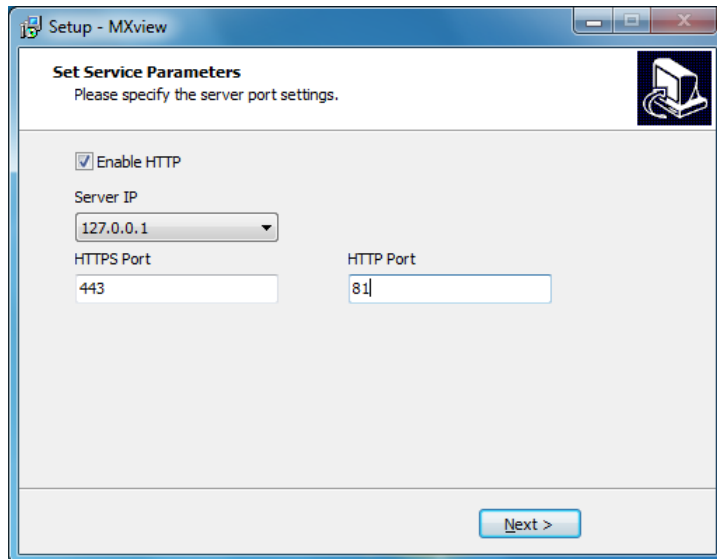
9. Click **Install**.



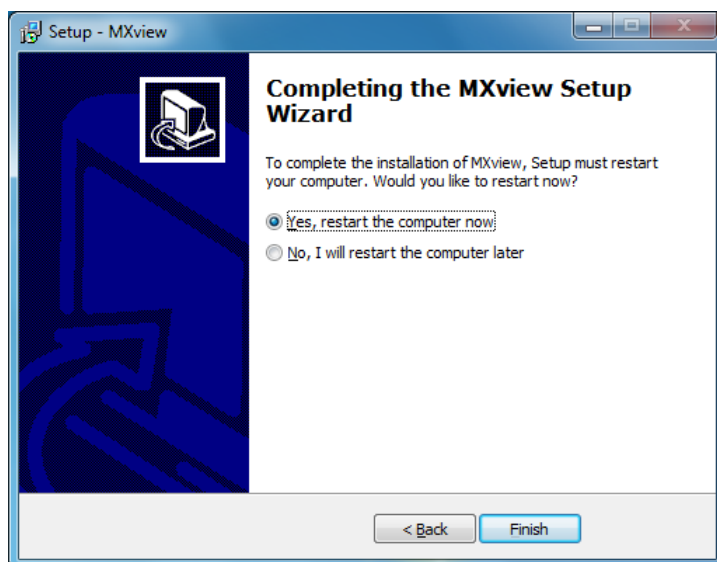
10. Wait until the installation process is complete.



- Set the HTTP port to 81 and click **Next**.



- Select **Yes, restart the computer now** and click **Finish** to reboot the system



- After the computer is restarted, the **MXview Service** shortcut appears on the computer desktop.



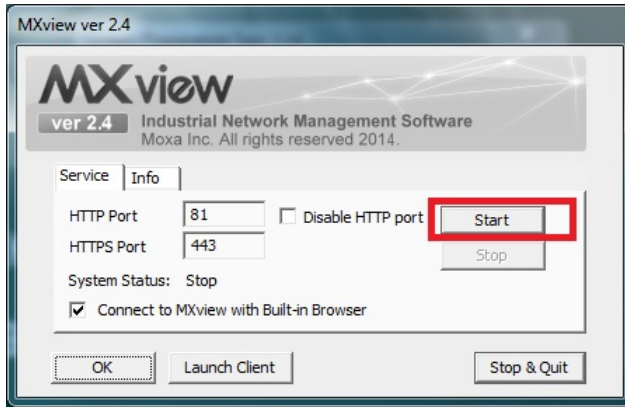
Configuring MXview

Complete the following steps to configure MXview:

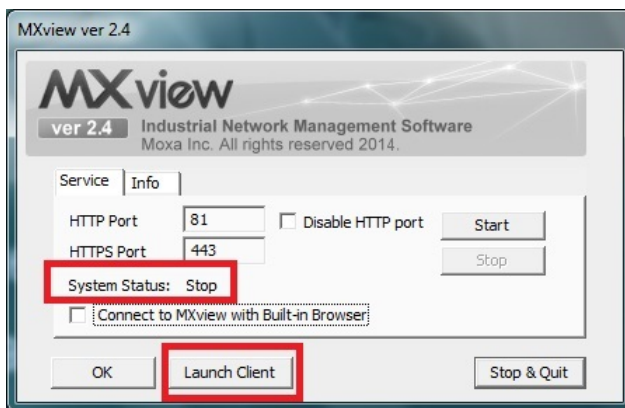
- Double-click the **MXview** shortcut on the desktop.



- 2. Click **Start** to continue.



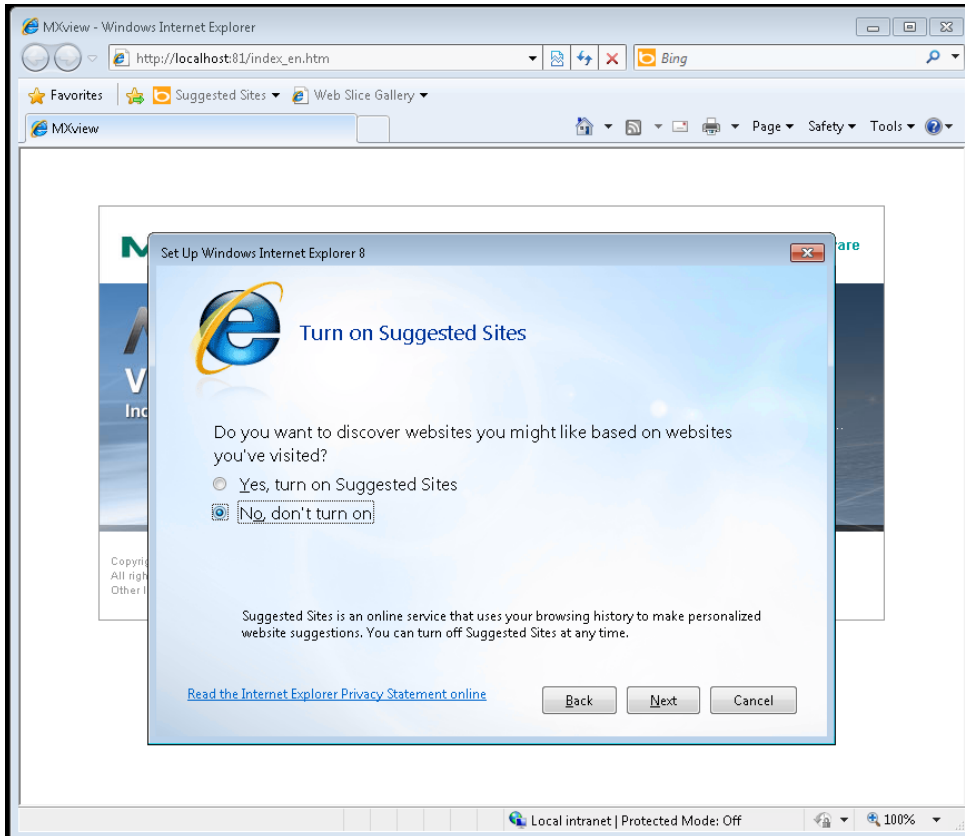
- 3. Wait until the **System Status** field displays **Running**; then, clear the **Connect to MXview with Built-in Browser** check box and click **Launch Client**.



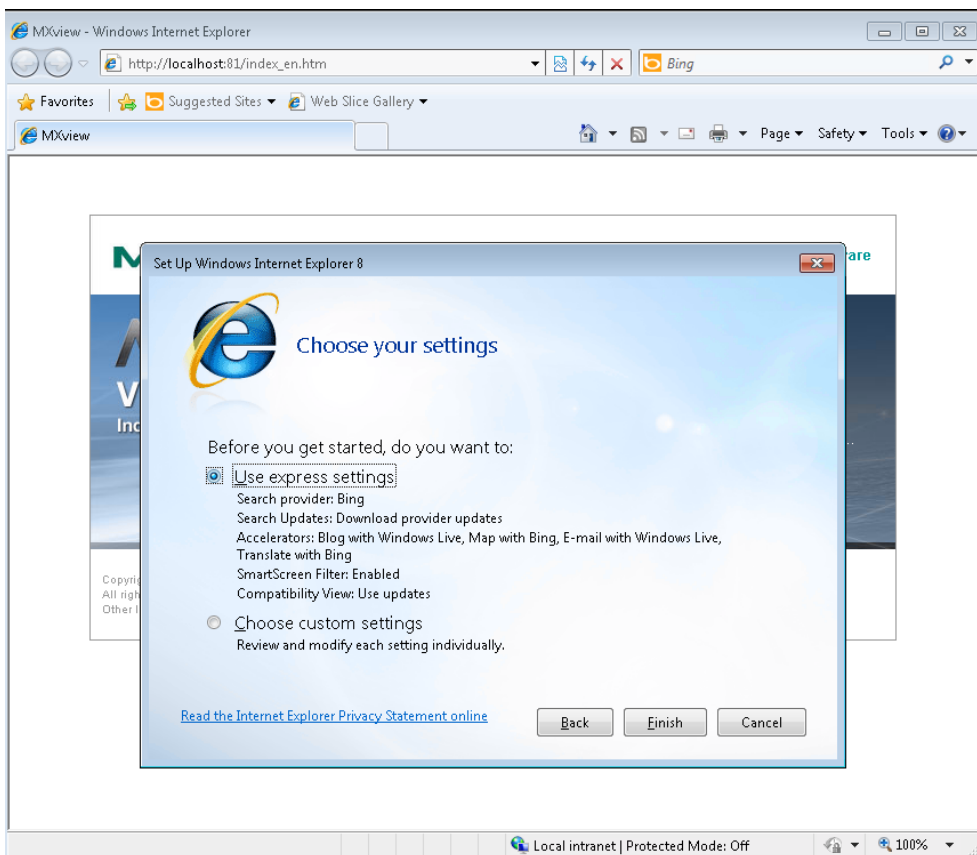
- 4. MXview opens Internet Explorer. Follow the on-screen instruction to configure Internet Explorer settings. Click **Next** to continue.



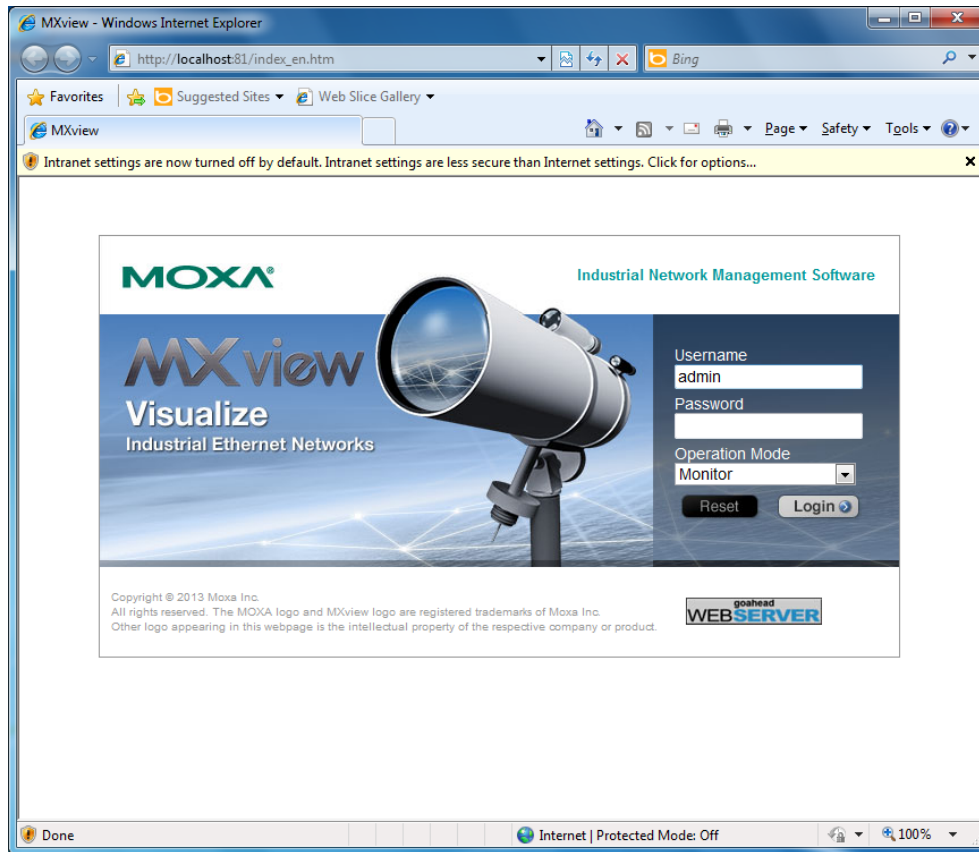
5. Select **No, don't turn on** and click **Next**.



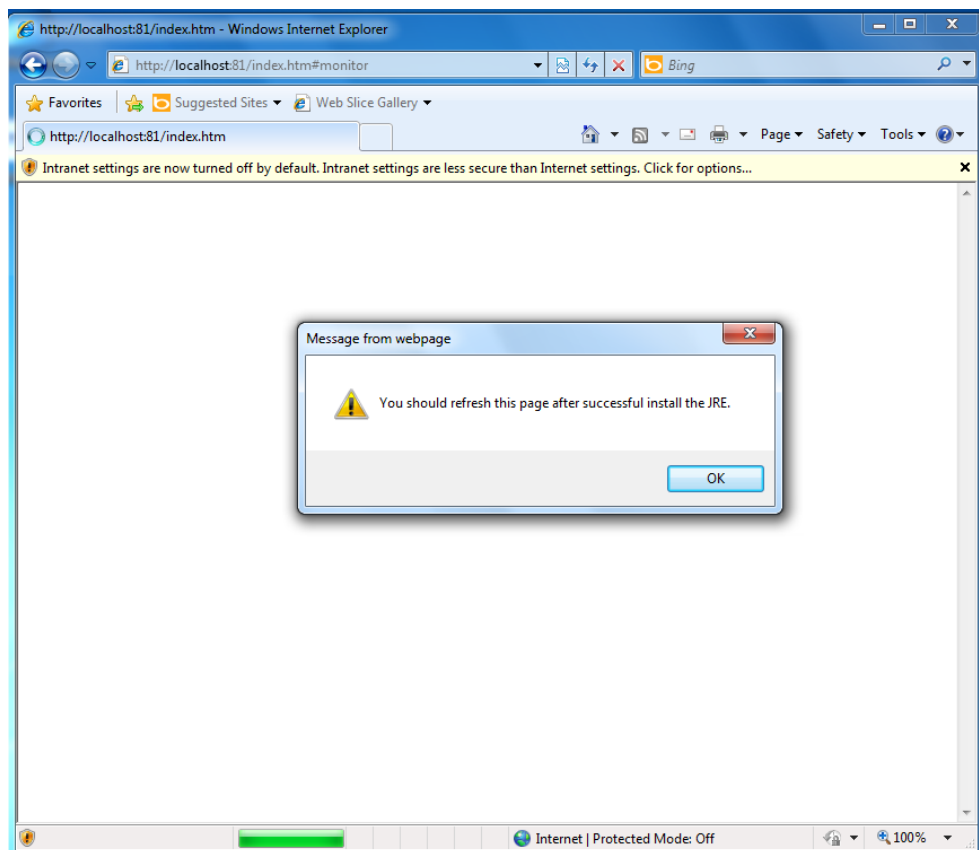
6. Select **Use express settings** and click **Finish** to complete the configuration.



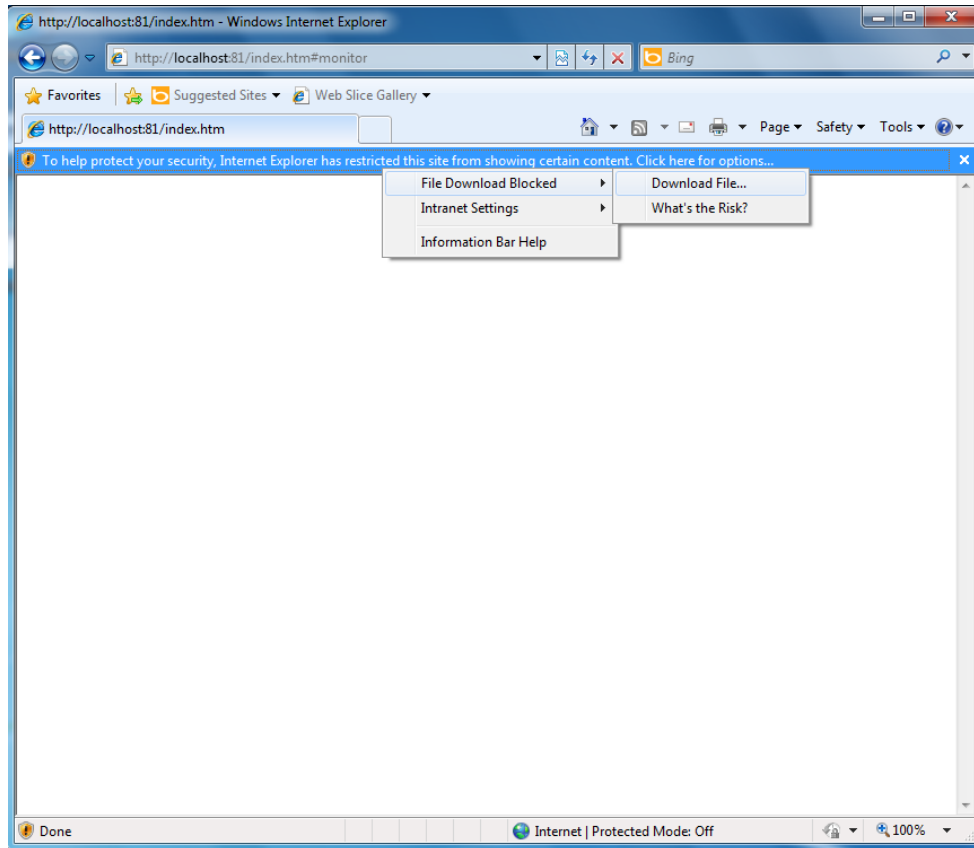
7. Log in using the default username (**admin**). Leave the **Password** field blank. Then, click **Login**.



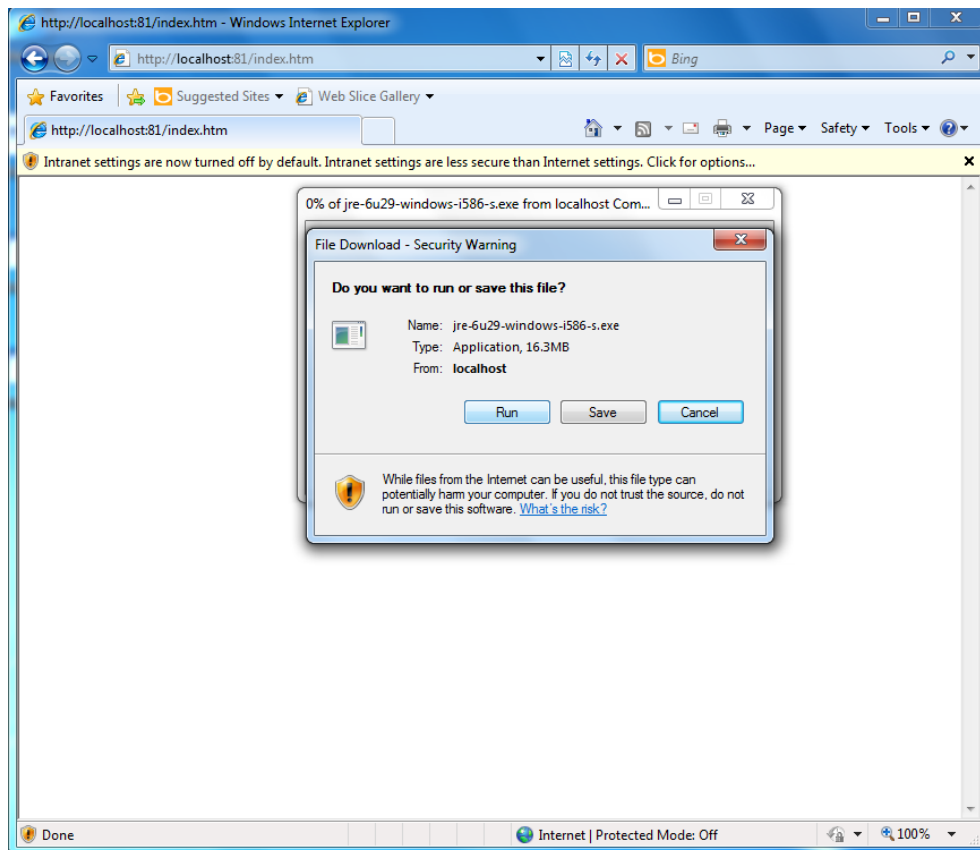
8. A popup message appears prompting you to install Java Runtime Environment (JRE). Click **OK**.



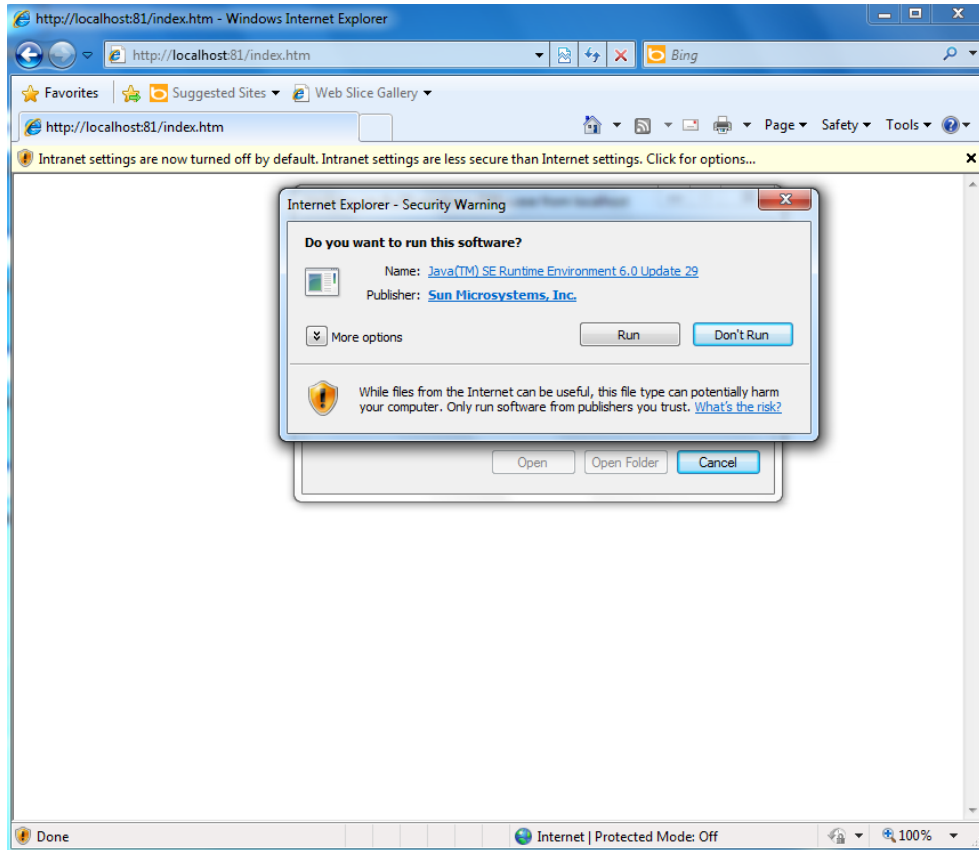
9. Click the title bar and select **File Download Blocked > Download File**.



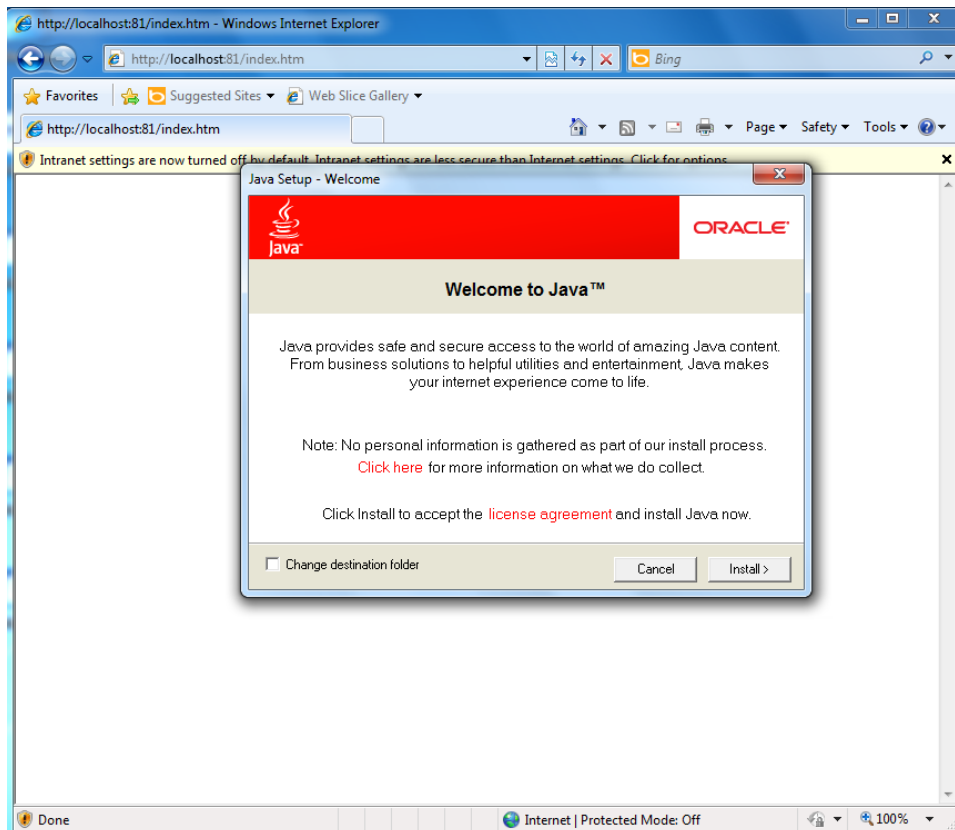
10. Select **Run** to download and install Java Runtime Environment.



11. Select **Run** to continue.



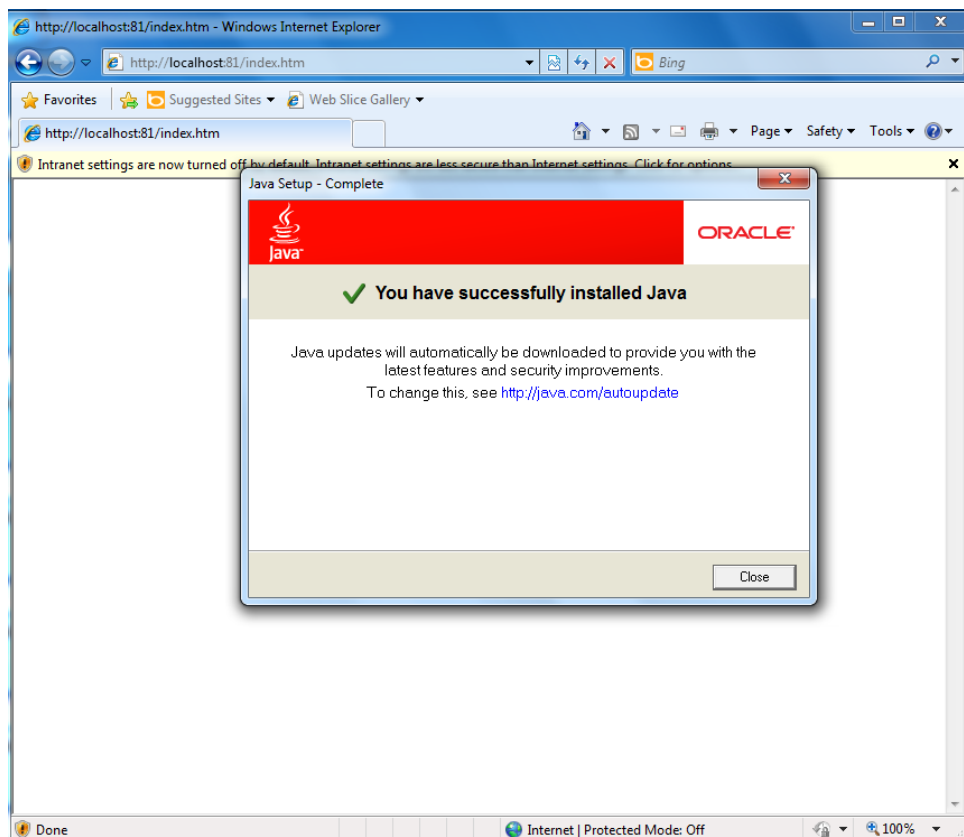
12. Click **Install**.



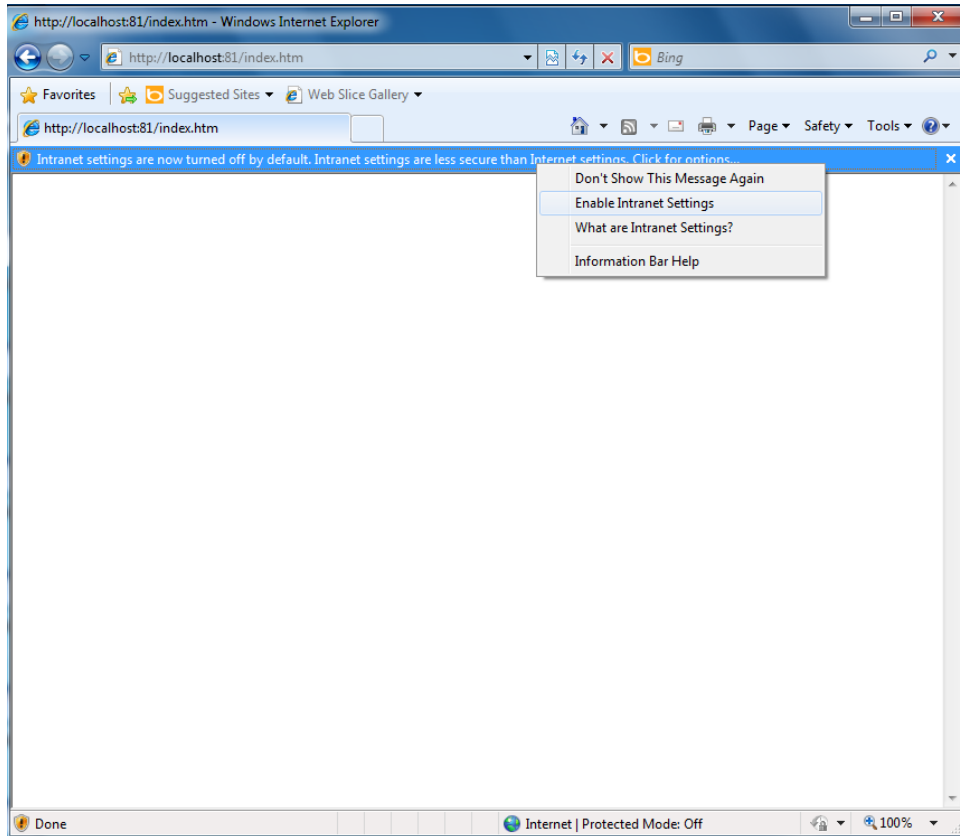
13. Wait until Java installation is complete.



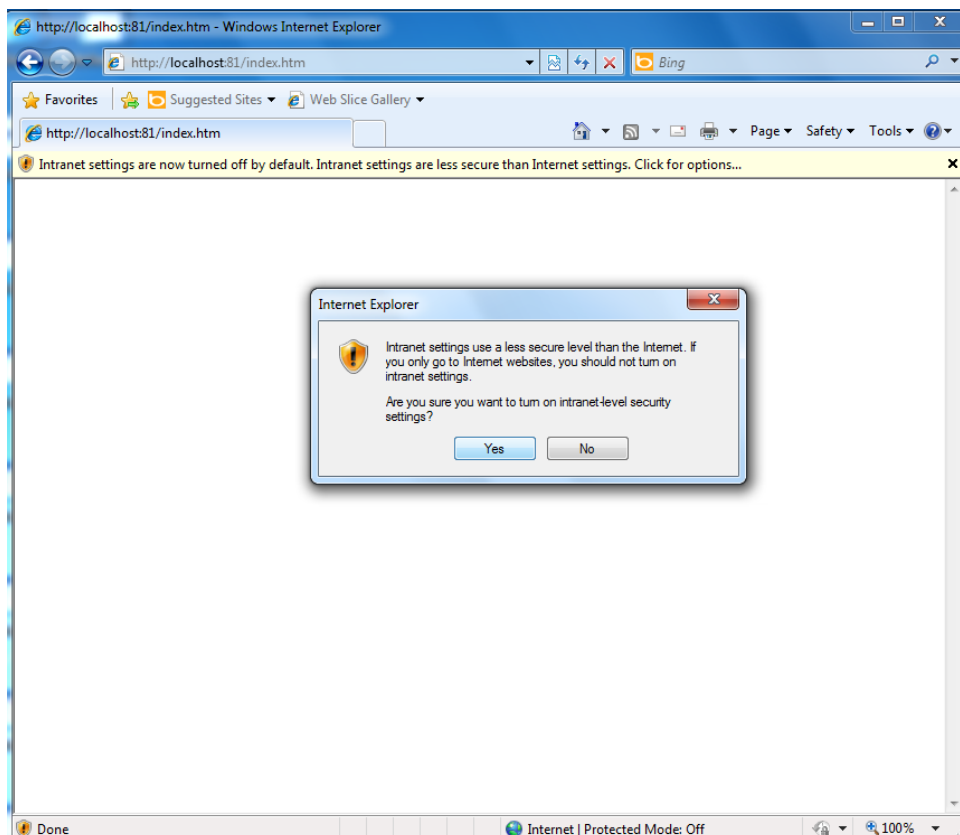
14. Click **Close** to complete the installation process.



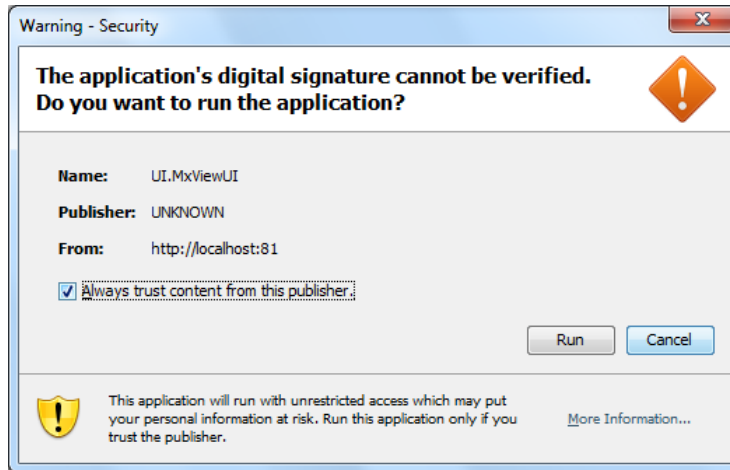
15. Click the message bar and select **Enable Intranet Settings**.



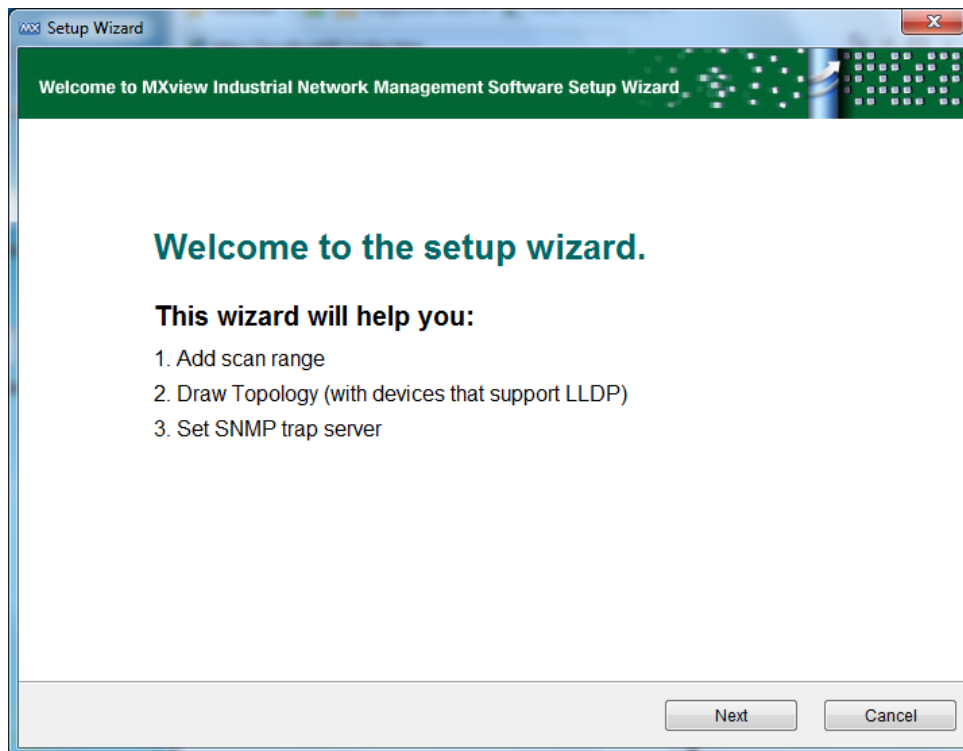
16. Click **Yes** to continue.



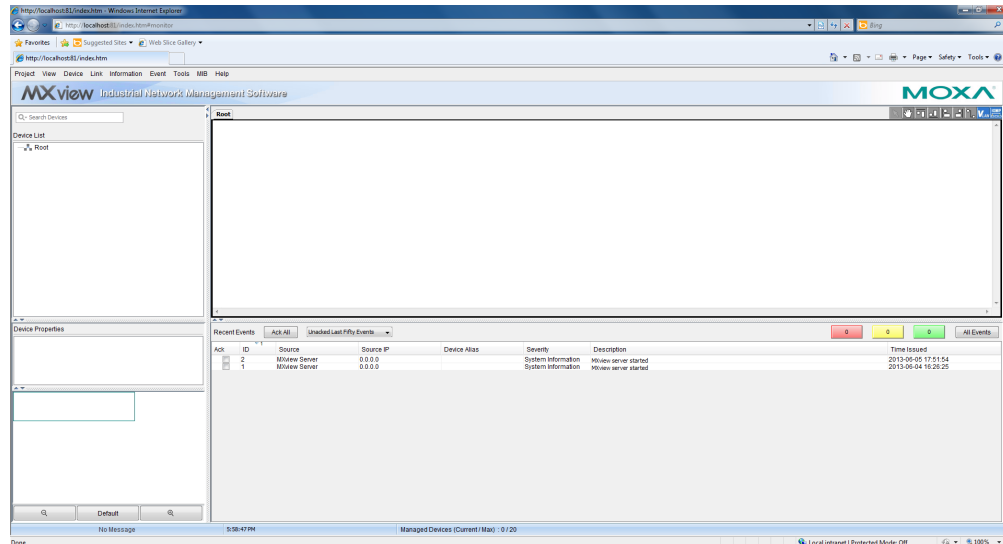
17. Click **Run**.



18. Click **Next** to launch the setup wizard to configure basic settings; otherwise, click **Cancel** to launch the program immediately.



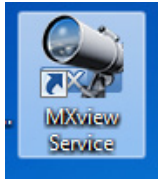
The MXview screen appears.



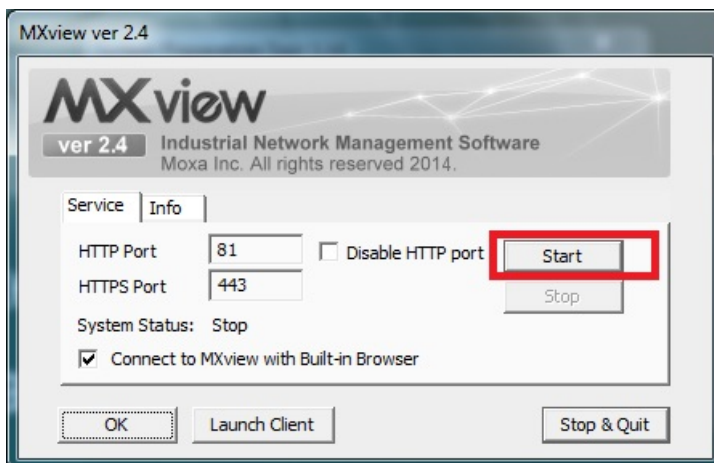
Loading the Moxa SynMap MIB File

Follow these steps to load the Moxa SynMap MIB file.

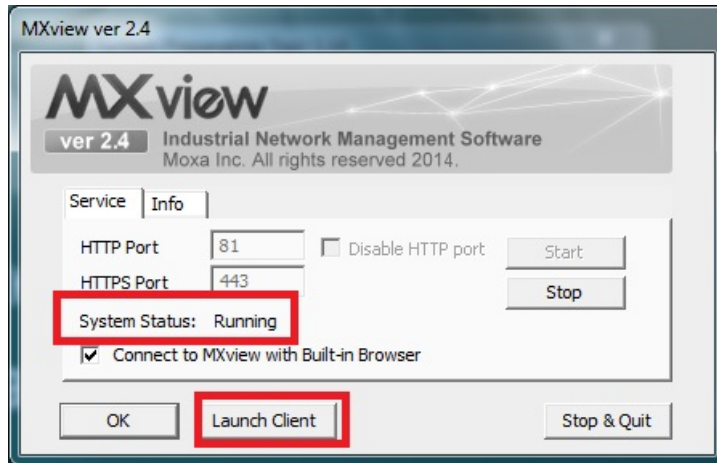
1. Double-click the **MxView Service** icon on the desktop.



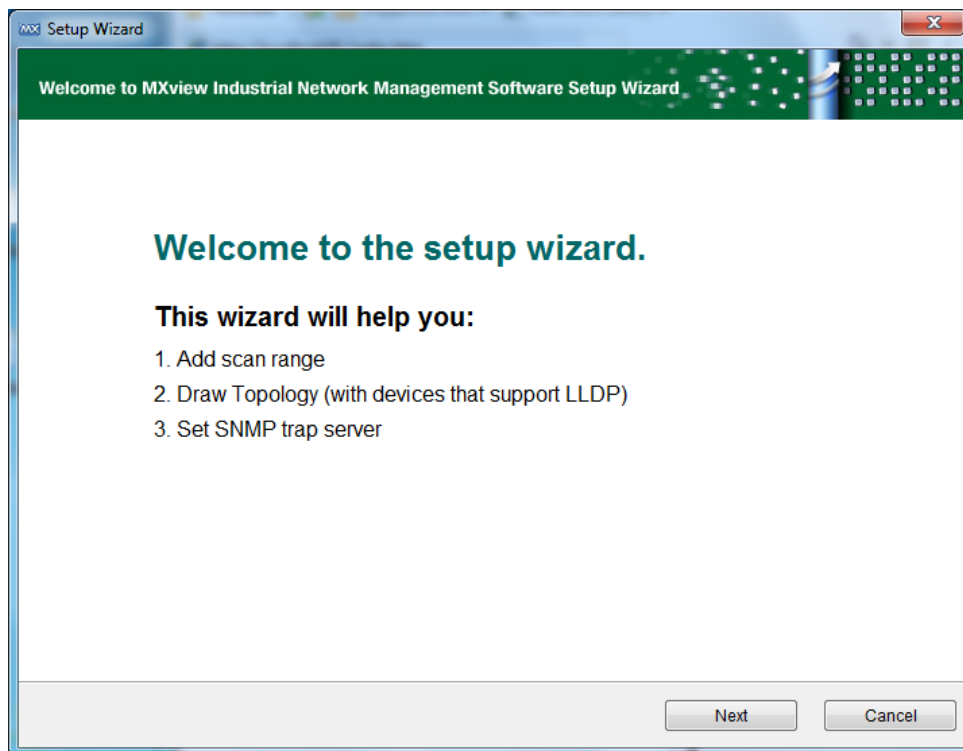
2. Click **Start**.



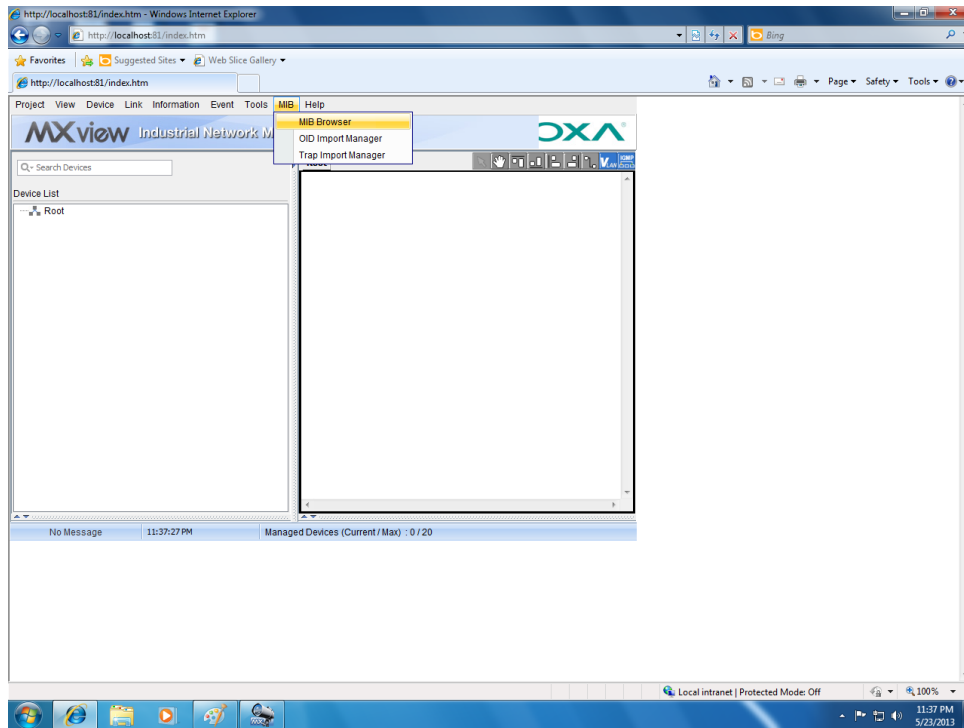
3. Wait until the **System Status** field changes to **Running**; then, click **Launch Client** to continue.



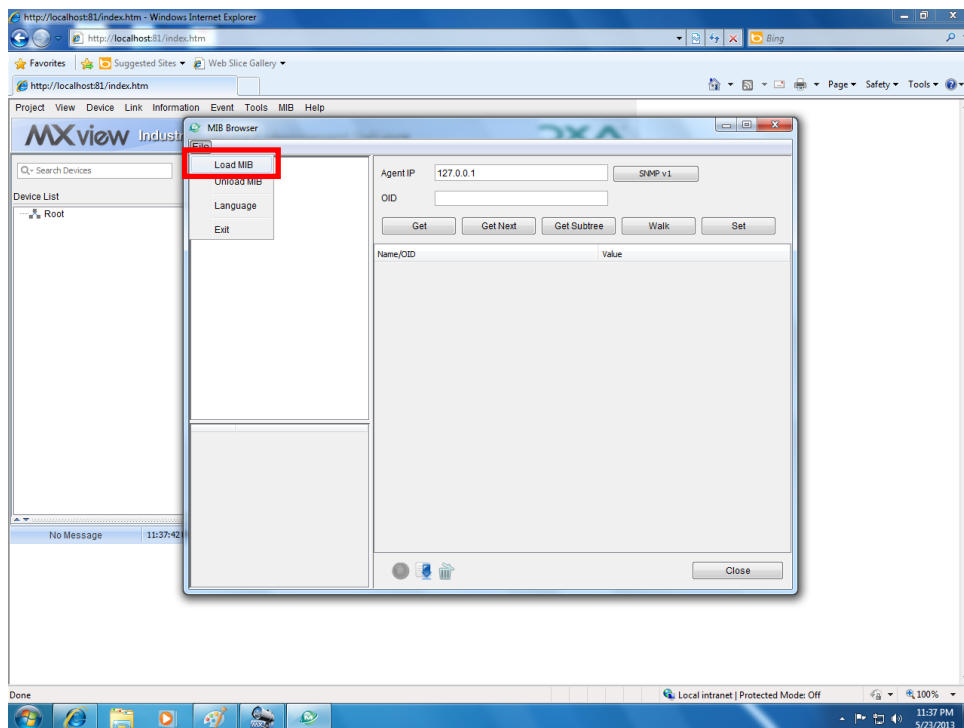
4. Click **Cancel**.



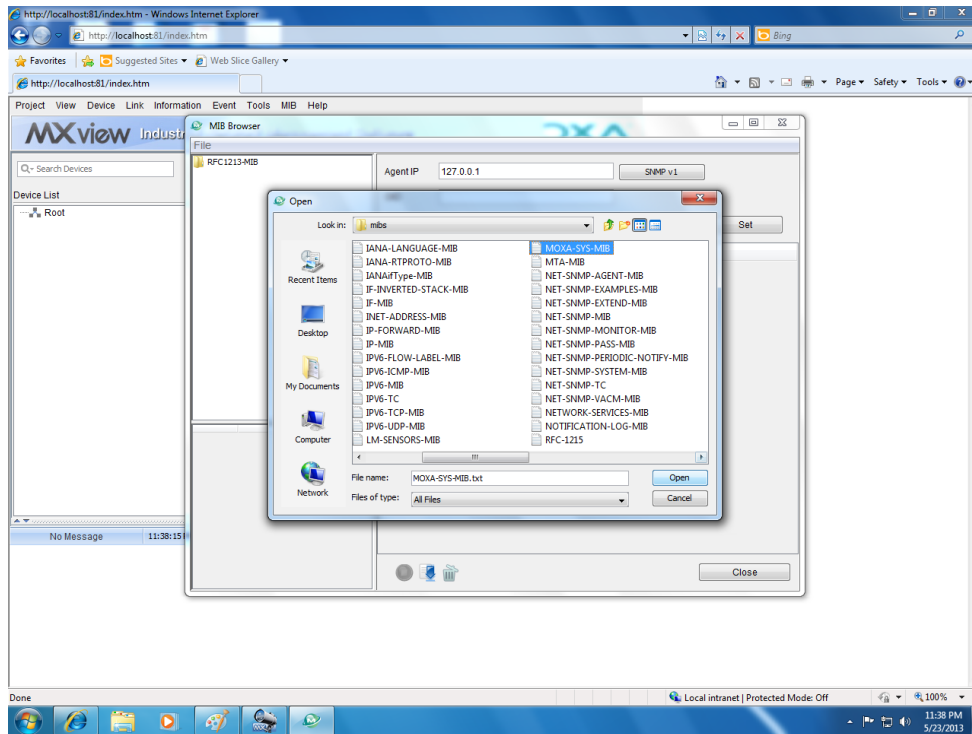
5. Select **MIB > MIB Browser**.



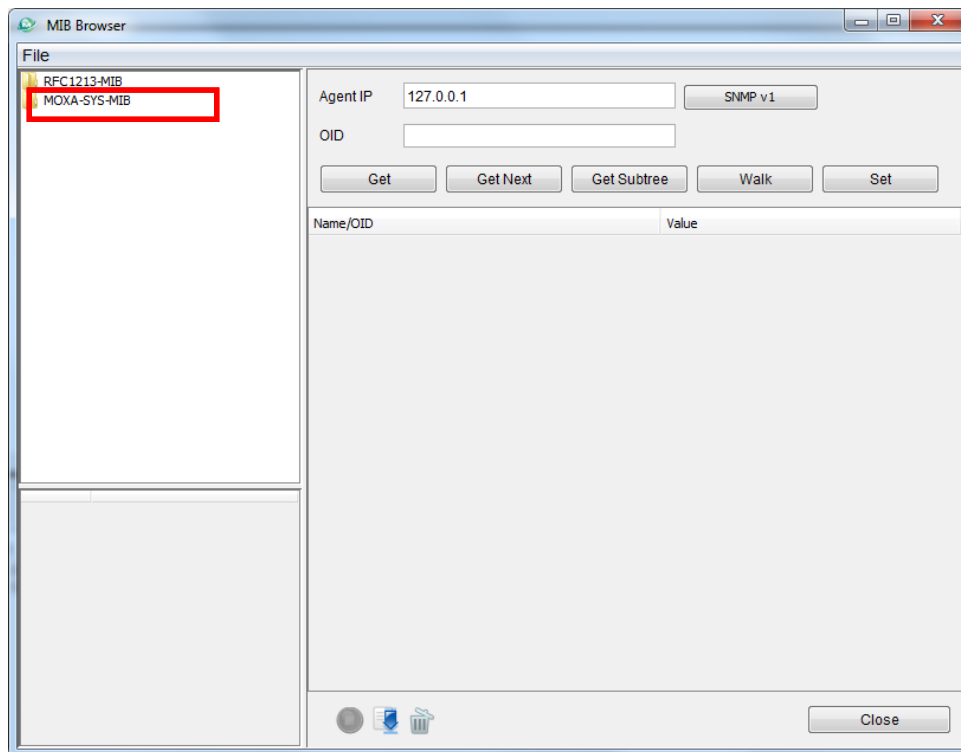
6. In the MIB Browser window, select **File > Load MIB**.



- Go to `c:\usr\share\snmp\mibs\` and select **MOXA-SYS-MIB.txt**; then, click **Open**.



- In the **MIB Browser** screen, verify that the **MOXA-SYS-MIB** folder displays in the **File** list.



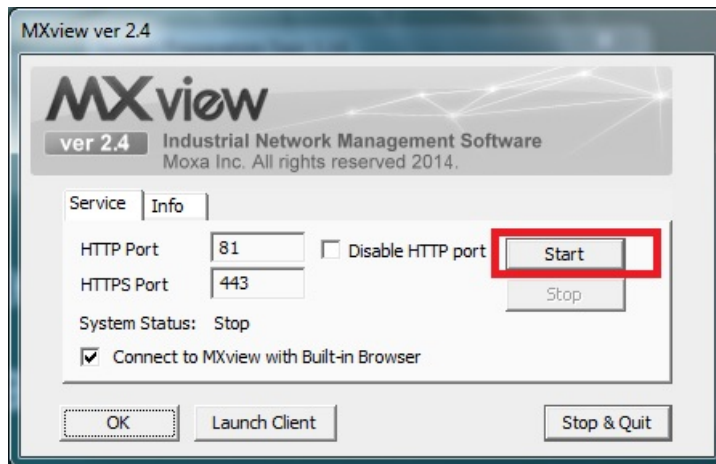
Loading the Host Resource MIB File

Complete the following steps to load the Host Resource MIB file.

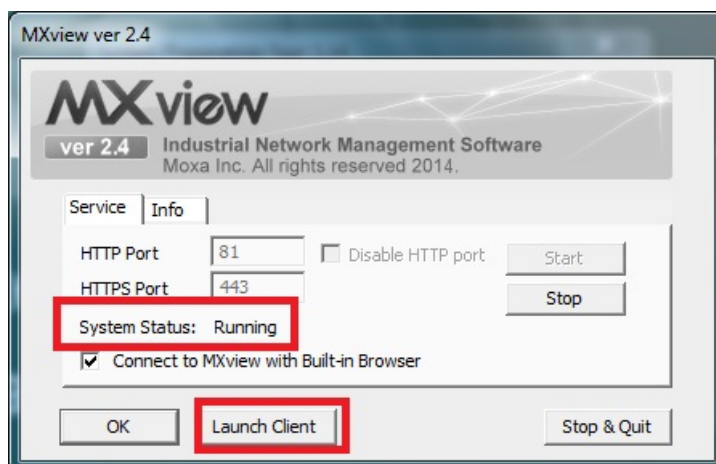
1. Double-click the **MxView Service** shortcut on the desktop.



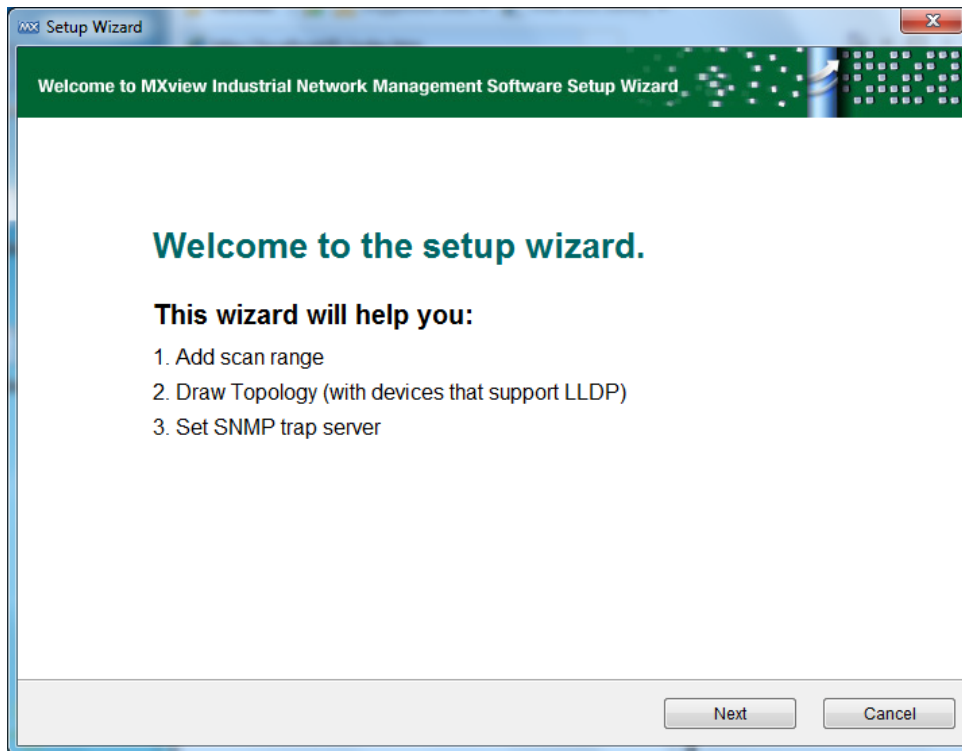
2. Click **Start**.



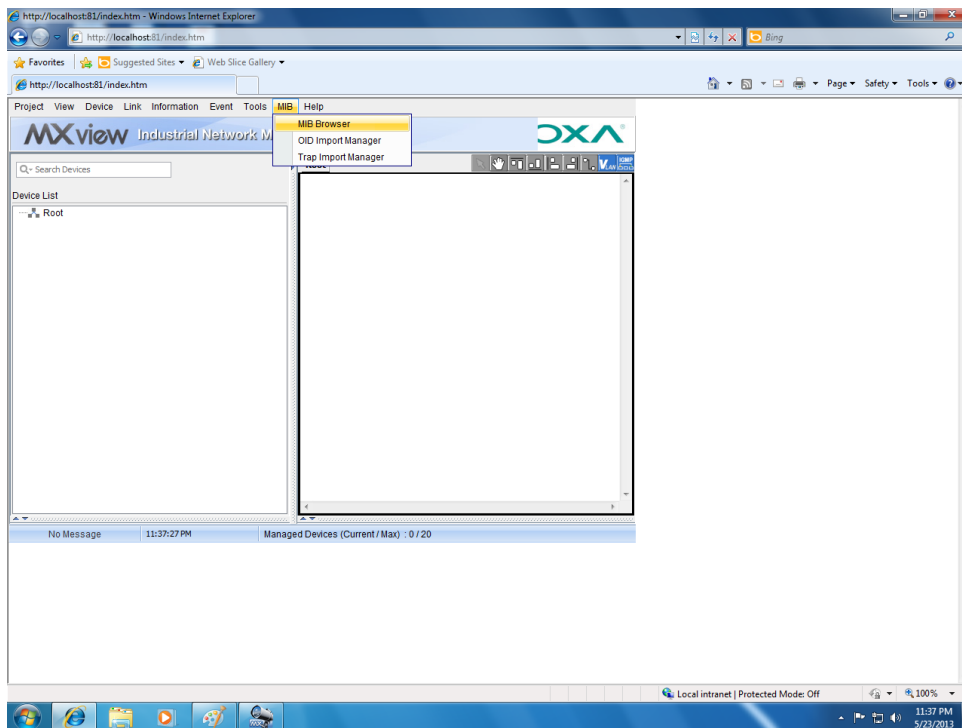
3. Wait until the **System Status** field becomes **Running**; then, click **Launch Client**.



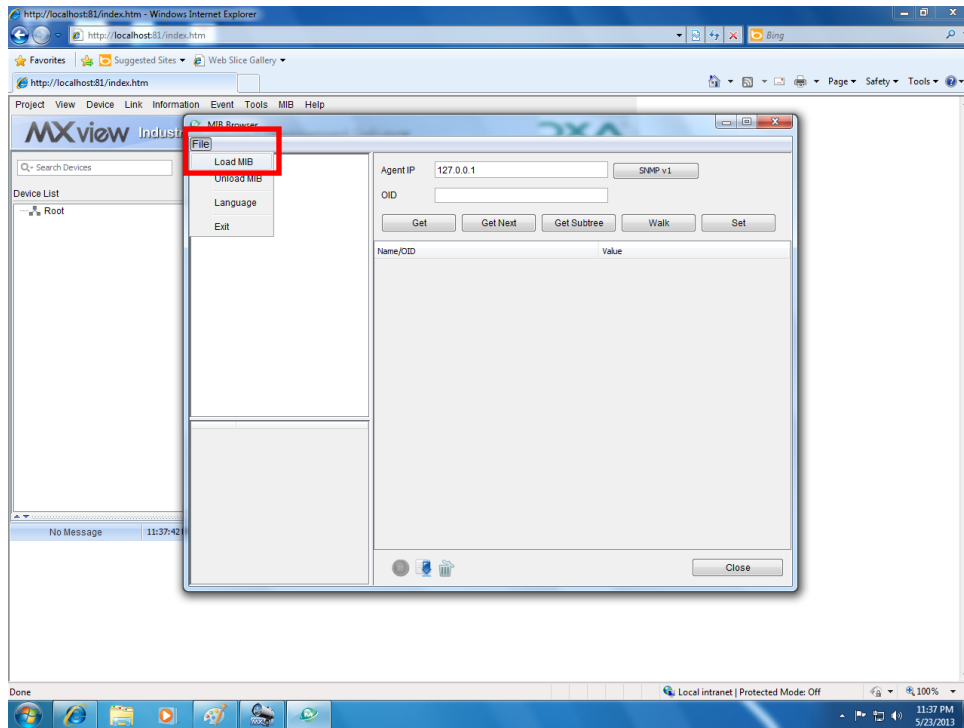
4. Click **Cancel**.



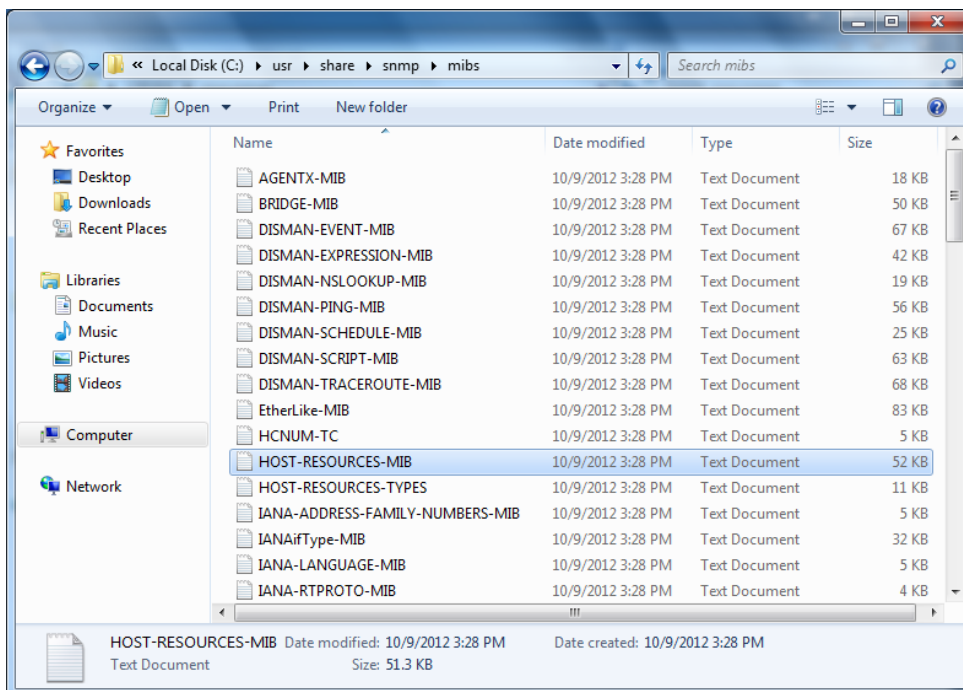
5. Select **MIB > MIB Browser**.



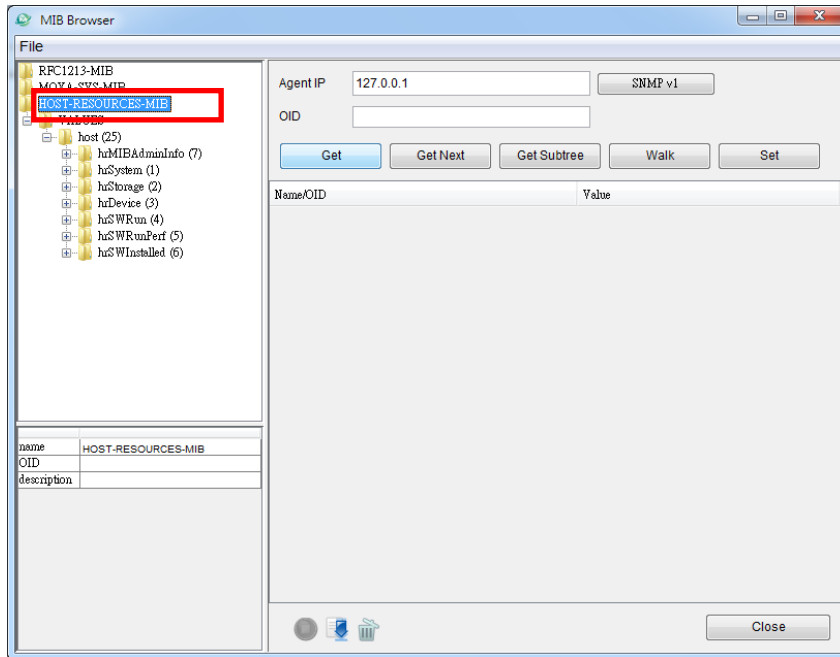
6. In the MIB Browser window, select **File > Load MIB**.



7. In the **c:\usr\share\snmp\libs** folder, select **HOST-RESOURCES-MIB.txt**.



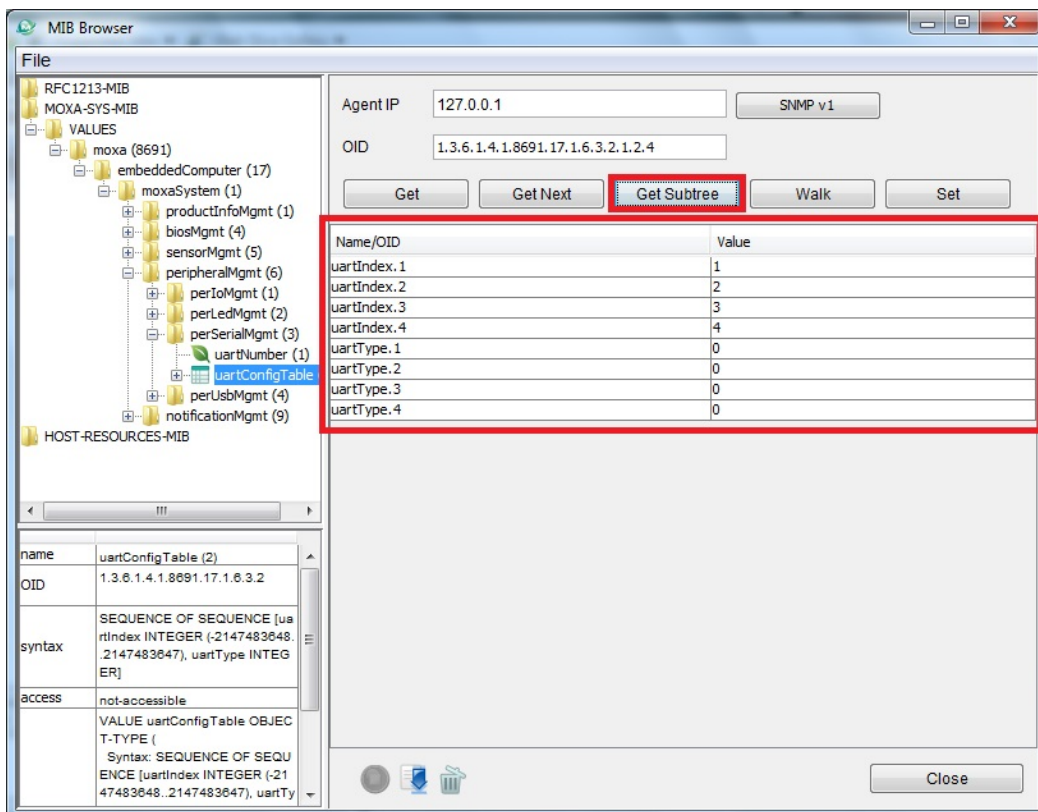
- In the **MIB Browser** screen, verify that the **HOST-RESOURCES-MIB** folder appears in the **File** list.



Using Moxa SynMap OIDs

Complete the following steps to use Moxa SynMap OIDs:

- Check the UART type. Navigate to **MOXA-SYS-MIB\VALUES\moxa\embeddedComputer\moxaSystem\peripheralMgmt** and double-click **uartConfigTable**.
- Click **Get Subtree** and verify that your MxView settings are correct.



Using HOST RESOURCE OIDs

Complete the following steps to use HOST RESOURCE OIDs.

1. Check disk usage. Navigate to **HOST-RESOURCES-MIB\VALUES\host\hrStorage\hrStorageTable** and double-click **hrStorageEntry**.
2. Click **Get Subtree** and verify that your MxView settings are correct.

The screenshot shows the MIB Browser interface. The left pane displays a tree view of MIB objects, with the path **HOST-RESOURCES-MIB\VALUES\host\hrStorage\hrStorageTable\hrStorageEntry (1)** selected. The right pane shows the configuration for the selected object, including the Agent IP (127.0.0.1) and the OID (1.3.6.1.2.1.25.2.3.1.7.3). The **Get Subtree** button is highlighted with a red box. Below the configuration, a table displays the retrieved values for the subtree.

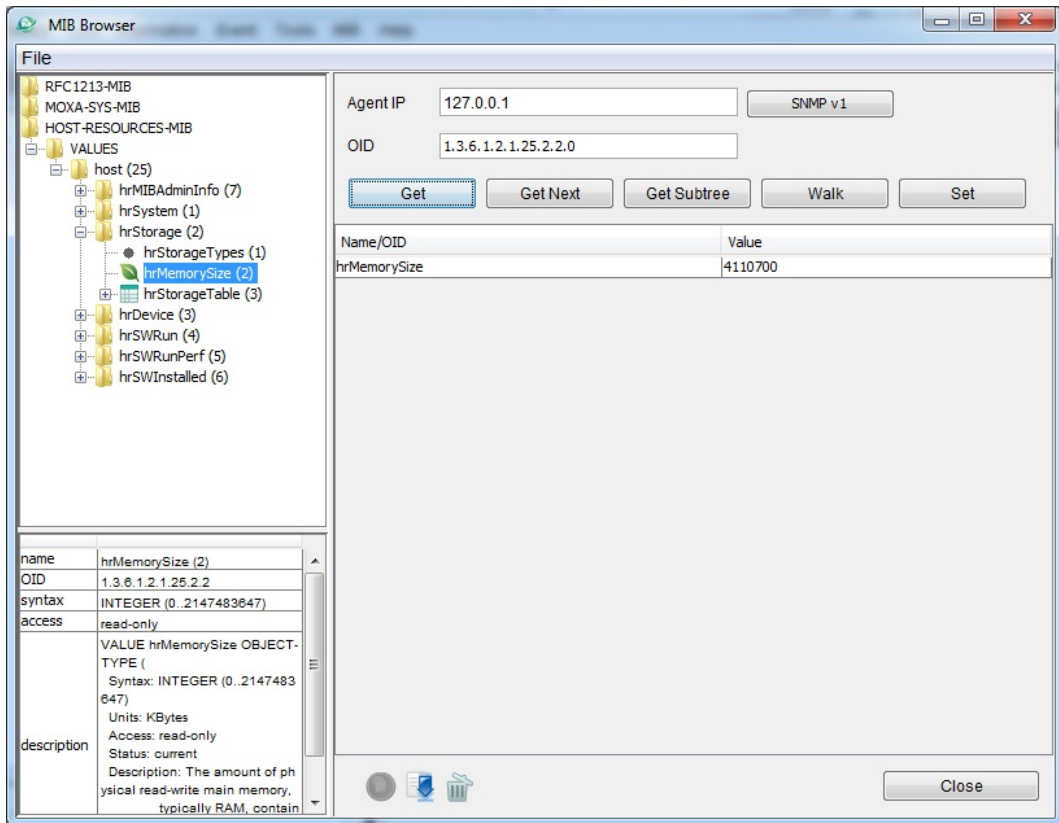
Name/OID	Value
hrStorageIndex.1	1
hrStorageIndex.2	2
hrStorageIndex.3	3
hrStorageType.1	1.3.6.1.2.1.25.2.1.4
hrStorageType.2	1.3.6.1.2.1.25.2.1.3
hrStorageType.3	1.3.6.1.2.1.25.2.1.2
hrStorageDescr.1	C:\Label: Serial Number 6607fe31
hrStorageDescr.2	Virtual Memory
hrStorageDescr.3	Physical Memory
hrStorageAllocationUnits.1	4096
hrStorageAllocationUnits.2	65536
hrStorageAllocationUnits.3	65536
hrStorageSize.1	3883519
hrStorageSize.2	64200
hrStorageSize.3	64229
hrStorageUsed.1	3502447
hrStorageUsed.2	24224
hrStorageUsed.3	22116
hrStorageAllocationFailures.1	0
hrStorageAllocationFailures.2	0
hrStorageAllocationFailures.3	0

The bottom pane shows the details for the selected object, including its name (**hrStorageEntry (1)**), OID (**1.3.6.1.2.1.25.2.3.1**), and syntax information.

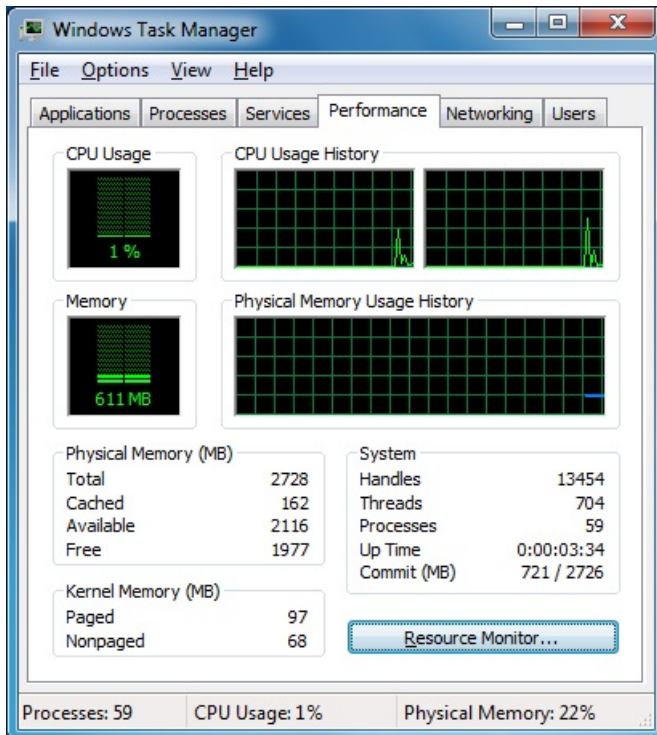
3. Retrieve the value of **hrStorageAllocationUnits.1** (for example, 4096).
4. Retrieve the value of **hrStorageSize.1** (for example, 14384127).
5. Calculate the total disk size using the following formula:

$$\text{total disk size} = \text{hrStorageAllocationUnits} \times \text{hrStorageSize}$$
 In this example, the total disk size is $4096 \times 14384127 = 58917384192 = 54.9 \text{ GB}$
6. Check memory usage. Go to the **HOST-RESOURCES-MIB\VALUES\host\hrStorage** folder and double-click **hrMemorySize**.

7. Click **Get**.

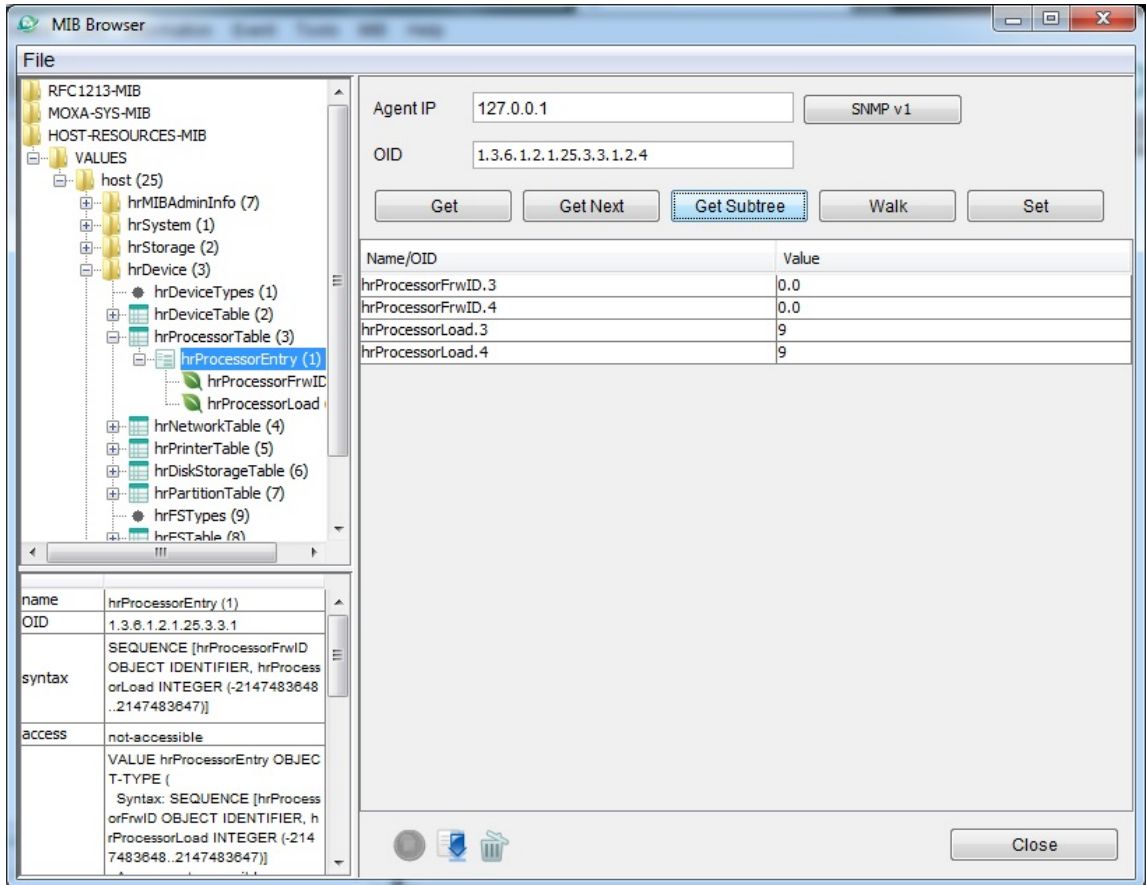


8. You can also check the physical memory size using Windows Task Manager.

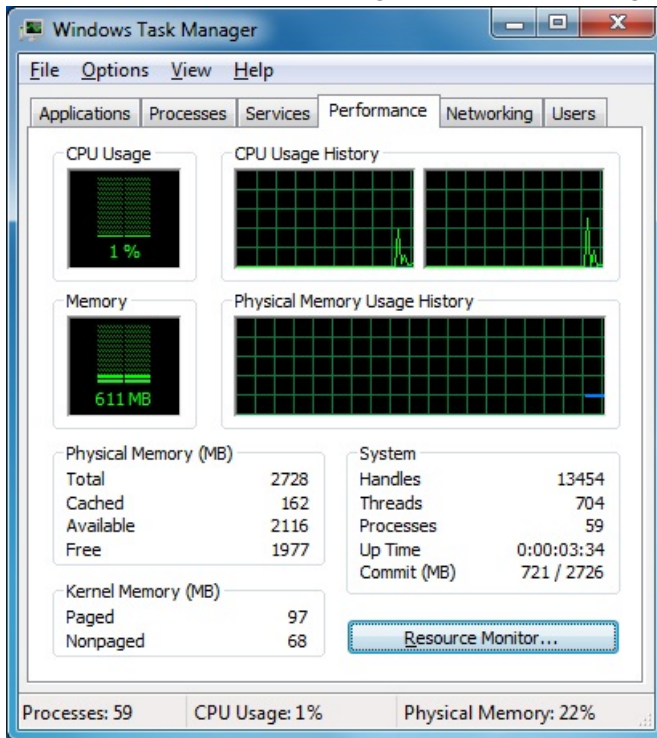


9. Check disk usage. Go to the **HOST-RESOURCES-MIB\VALUES\host\hrDevice\hrProcessorTable** folder and double-click **hrProcessorEntry**.

10. Click **Get Subtree**.



11. You can also check the CPU loading of each CPU core using Windows Task Manager.



7

Examples

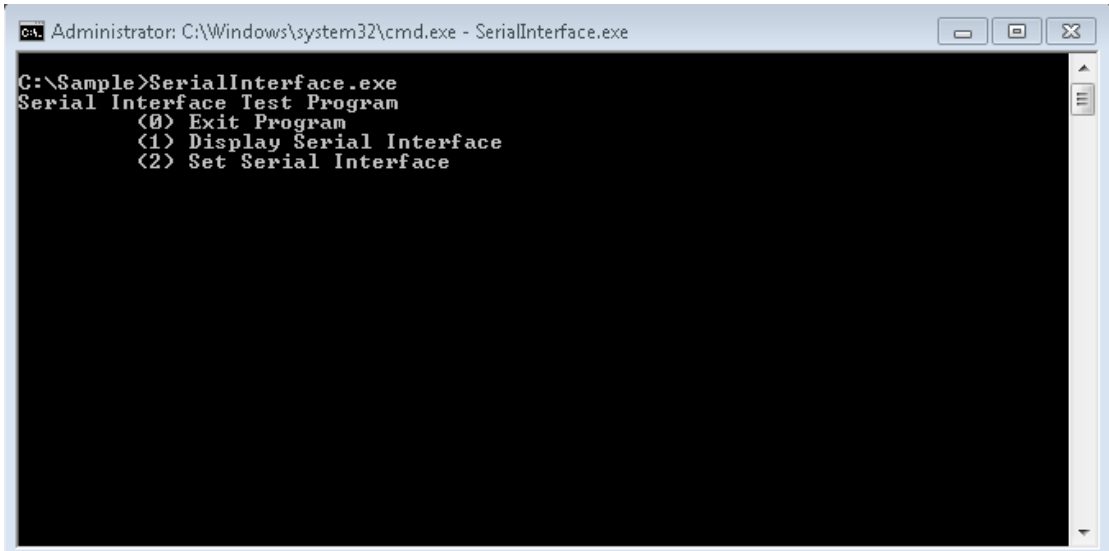
This chapter provides examples to illustrate how to use the V2406A computer for a variety of applications.

The following topics are covered in this chapter:

- ❑ **SerialInterface**
- ❑ **Digital Input/Output**
- ❑ **Watchdog**

SerialInterface

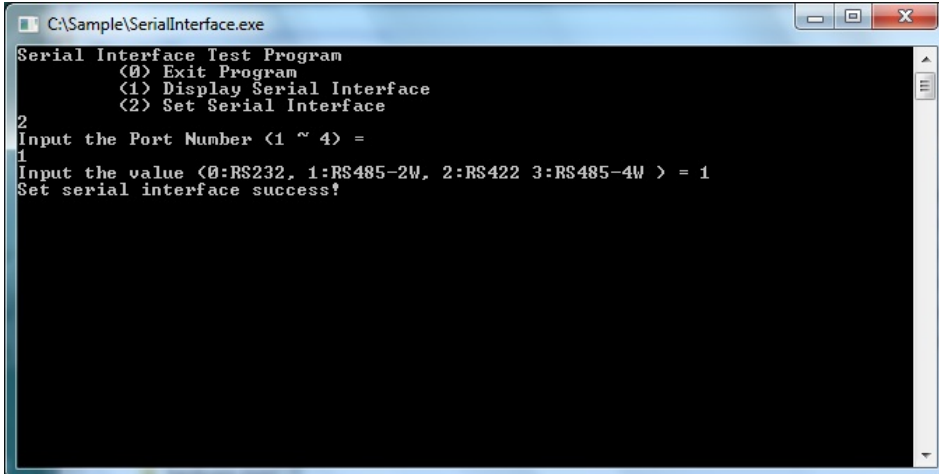
1. Copy the following files from the product software DVD.
mxsp.dll: \examples\V2406A_W7E_V1.0_example\lib\mxsp\x86\
sysinfo.dll: \examples\V2406A_W7E_V1.0_example\lib\mxsp\x86\
sysinfo.sys: \examples\V2406A_W7E_V1.0_example\lib\mxsp\x86\
mxGeneralIo.dll: \examples\V2406A_W7E_V1.0_example\lib\MxGeneralIo\x86\
SerialInterface.exe: \examples\V2406A_W7E_V1.0_example\Release\
2. Execute **SerialInterface.exe**.



```
Administrator: C:\Windows\system32\cmd.exe - SerialInterface.exe

C:\Sample>SerialInterface.exe
Serial Interface Test Program
  <0> Exit Program
  <1> Display Serial Interface
  <2> Set Serial Interface
```

3. Type **2** to set the serial interface. Follow the on-screen instructions.



```
C:\Sample\SerialInterface.exe

Serial Interface Test Program
  <0> Exit Program
  <1> Display Serial Interface
  <2> Set Serial Interface
2
Input the Port Number (1 ~ 4) =
1
Set serial interface success!
```


4. Type **1** to display the current serial interface settings.

```

C:\Sample\SerialInterface.exe
Serial Interface Test Program
  (0) Exit Program
  (1) Display Serial Interface
  (2) Set Serial Interface
1
COM1 = RS485-2W
COM2 = RS232
COM3 = RS232
COM4 = RS232
-

```

Digital Input/Output

1. Copy the following files from the product software DVD.
 mxdgio.dll: \examples\V2406A_W7E_V1.0_example\lib\mxdgio\x86\
 mxGeneralIo.dll: \examples\V2406A_W7E_V1.0_example\lib\MxGeneralIo\x86\
 DIO.exe: \examples\V2406A_W7E_V1.0_example\Release\
2. Execute **DIO.exe**.

```

Administrator: Command Prompt - dio
C:\Sample>dio
DIO Mode Test Program
  (0) Exit Program
  (1) Display DIN
  (2) Display DOUT
  (3) Set DOUT value
  (4) Display both DIN and DOUT
-

```

3. Type **4** to display the current DI and DO values.

```

Administrator: Command Prompt - dio
C:\Sample>dio
DIO Mode Test Program
  (0) Exit Program
  (1) Display DIN
  (2) Display DOUT
  (3) Set DOUT value
  (4) Display both DIN and DOUT
4
Din0 = 1 , Dout0 = 1
Din1 = 1 , Dout1 = 1
Din2 = 1
Din3 = 1
Din4 = 1
Din5 = 1
-

```

4. Type **3** to set the DOUT port number. Follow the on-screen instructions.

```
Administrator: Command Prompt - dio
C:\Sample>dio
UART Mode Test Program
(0) Exit Program
(1) Display DIN
(2) Display DOUT
(3) Set DOUT value
(4) Display both DIN and DOUT
3
Input the Port Number <0 ~ 1> =
0
Input the value <0 or 1> = 0
Set digital output success!
-
```

5. Type **4** to check if the port value was set correctly.

```
Administrator: Command Prompt - dio
C:\Sample>dio
UART Mode Test Program
(0) Exit Program
(1) Display DIN
(2) Display DOUT
(3) Set DOUT value
(4) Display both DIN and DOUT
4
Din0 = 1 , Dout0 = 0
Din1 = 1 , Dout1 = 1
Din2 = 1
Din3 = 1
Din4 = 1
Din5 = 1
-
```

Watchdog

1. From the product software DVD, copy the following files:
 - mxdev.dll: \examples\V2406A_W7E_V1.0_example\lib\mxwdg\x86\
 - mxGeneralIo.dll: \examples\V2406A_W7E_V1.0_example\lib\MxGeneralIo\x86\
 - Watchdog.exe: \examples\V2406A_W7E_V1.0_example\Release\
2. To prevent the system from rebooting, press [Enter] at least once every 10 seconds; otherwise, the system will reboot automatically.
3. To stop the watchdog, press **q** to exit the program

```
Administrator: C:\Windows\system32\cmd.exe
D:\>watchdog
Press "ENTER" in 10 seconds
^ 'q' to exit
Press "ENTER" in 10 seconds
^ 'q' to exit
Press "ENTER" in 10 seconds
^ 'q' to exit
Press "ENTER" in 10 seconds
^ 'q' to exit
Press "ENTER" in 10 seconds
^ 'q' to exit
Press "ENTER" in 10 seconds
^ 'q' to exit
Press "ENTER" in 10 seconds
^ 'q' to exit
Press "ENTER" in 10 seconds
^ 'q' to exit
Press "ENTER" in 10 seconds
^ 'q' to exitq
D:\>_
```

System Recovery

This chapter describes the system recovery process that you can perform if the system is not functioning properly.

The following topics are covered in this chapter:

- **Overview**
- **Setting Up the Recovery Environment**
- **Setting Up 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 recovery in the event the system becomes unstable. You can perform a system recovery using one of the following system images:

- A clean factory default image.
- A user-generated image created from a fully configured, fully set up system.

Before you perform a system recovery, set up the system environment.

Setting Up the Recovery Environment

To set up the recovery environment on a V2406A computer, prepare a USB drive that has at least 4 GB of memory and a copy of the recovery suite.

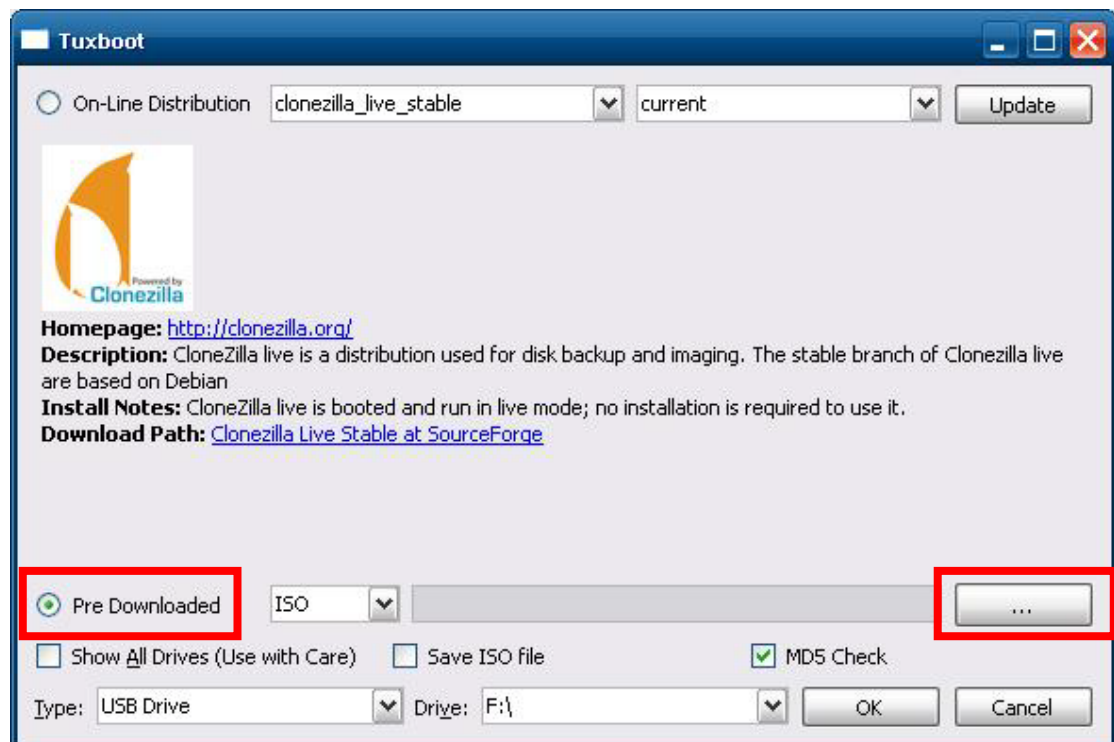
The following lists the major steps in the recovery procedure:

1. Copy the recovery programs and system image file on to the USB drive. Set up the drive as a live-drive system with an ISO image of the boot environment.
2. Reboot the system and configure the BIOS to boot the recovery system from the USB port.
3. An image of the current software system will be created on the USB drive. The recovery environment will use this image when restoring the system.
4. Reboot the system again and the BIOS is returned to its original state.

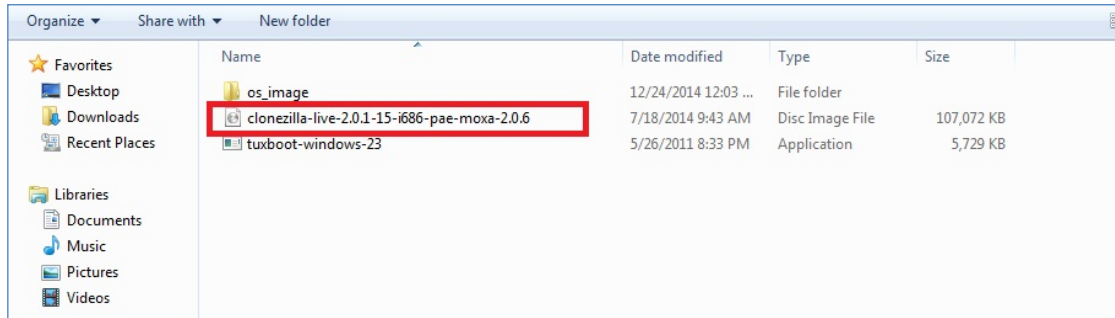
Setting Up a Factory Default Recovery Image

Step 1: Preparing the USB drive

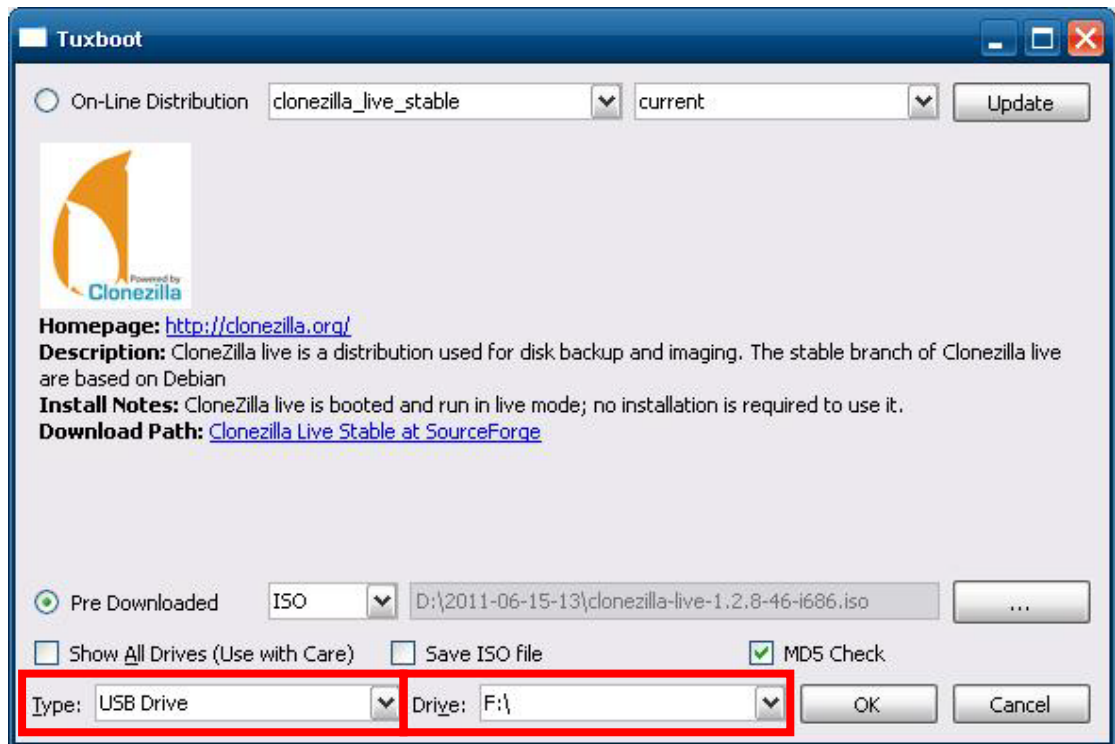
1. Load the software DVD that came with your V2406A computer and execute **tuxboot-windows-23.exe** in the **\recovery** folder.
2. Select **Pre Downloaded** and click the ellipsis (...) button to browse the file system and locate the boot environment's ISO image.



- Navigate to the `\recovery\` folder on the software DVD and select the boot environment's ISO image.



- Select **USB Drive** from the **Type** drop-down list and select the drive letter that corresponds to the USB drive from the **Drive** drop-down list. Click **OK** to copy the boot environment and bootloader to your USB drive.

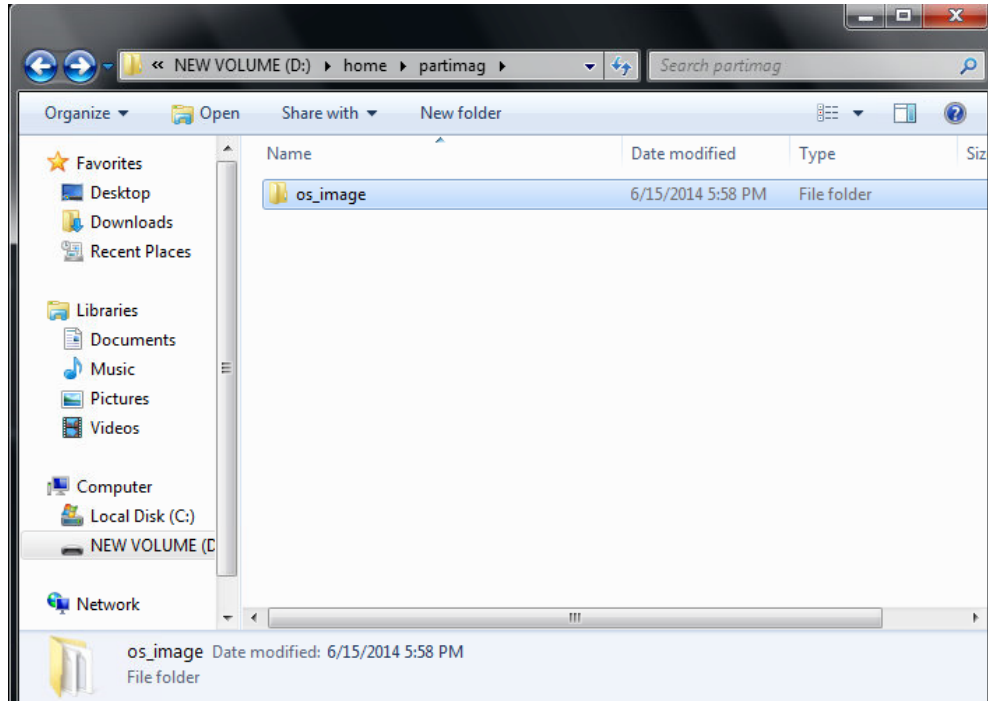


- Click **Exit**.



- From the desktop, copy the directory containing the base OS from the software DVD on to the USB drive. That is, copy **#:\<SoftwareDVD>\recovery\os_image** to the partition image directory, **F:\home\partimag**, on the USB drive. However, if you want to recover from your own system image, back up a system image first. For more information, refer to the **Creating a Custom System Image** section.

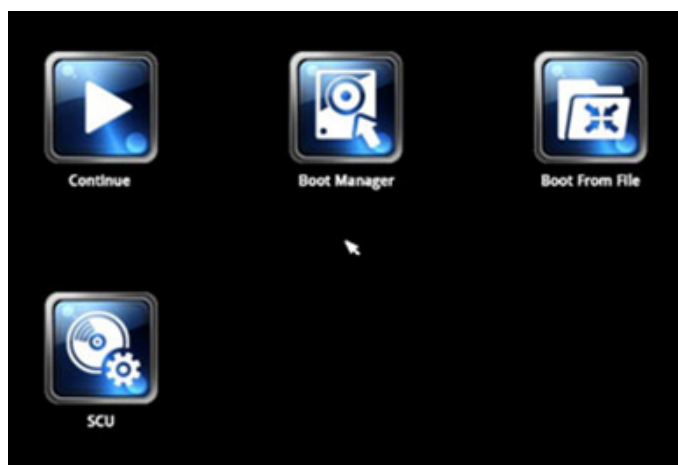
After **Step 1** procedure is complete, proceed to the next section, **Step 2: Setting the BIOS to Boot via USB**.



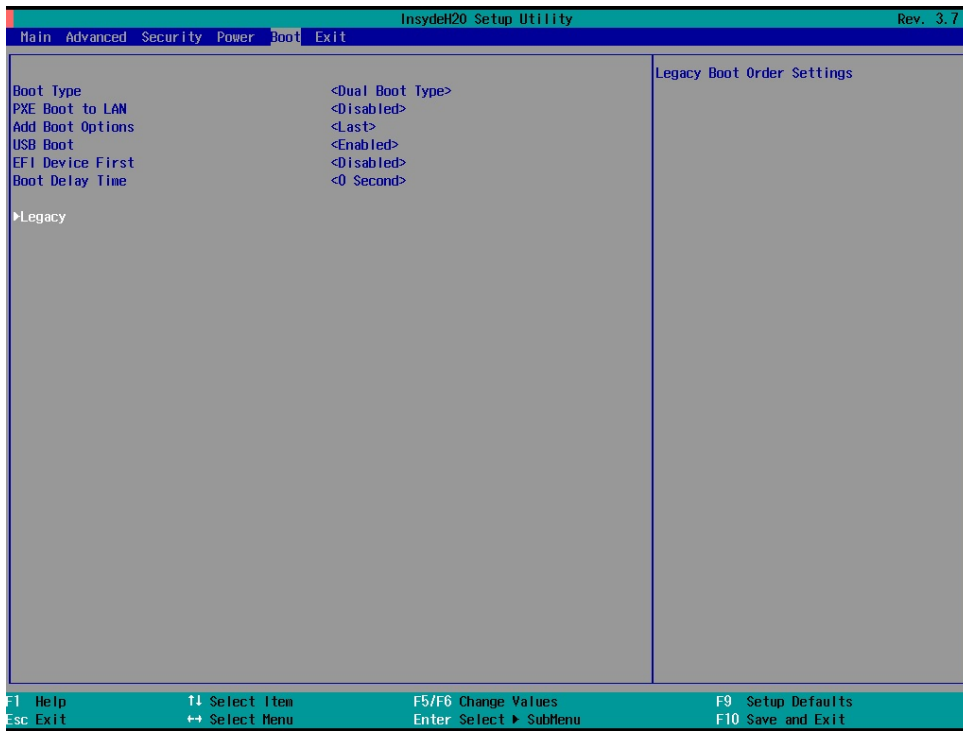
Step 2: Setting the BIOS to Boot via USB

This step shows you how to reset the BIOS so the system can boot directly from the USB port. You must perform this action before you can continue to configure the system recovery environment.

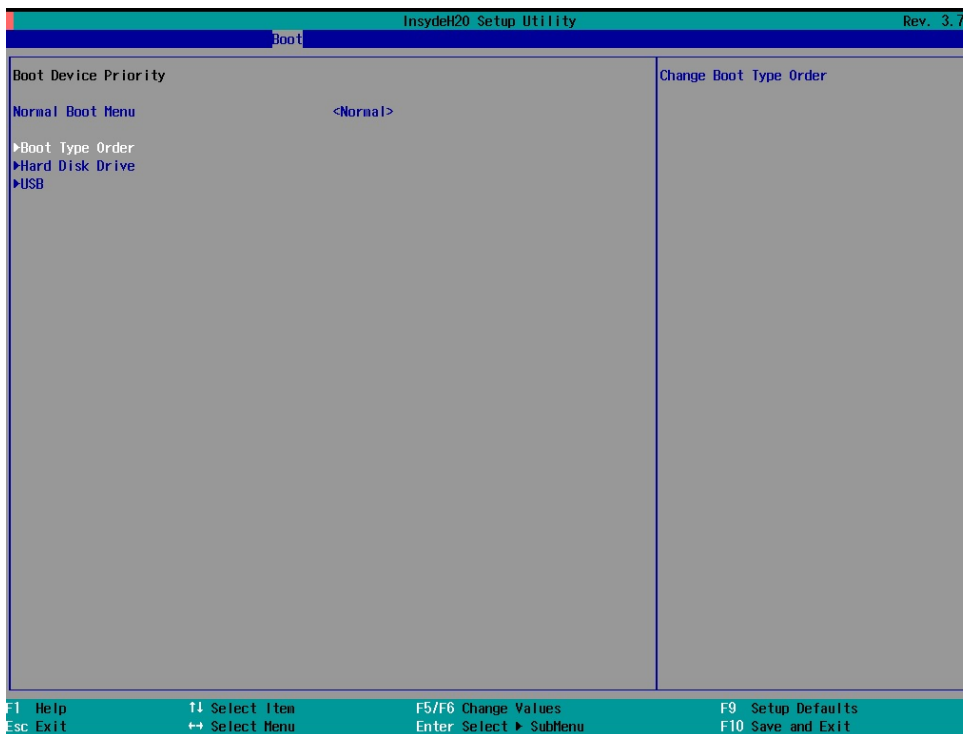
- Reboot the system, and, during the POST process, press **F2** until you hear a long beep. Click **SCU** to enter the BIOS setup menu.



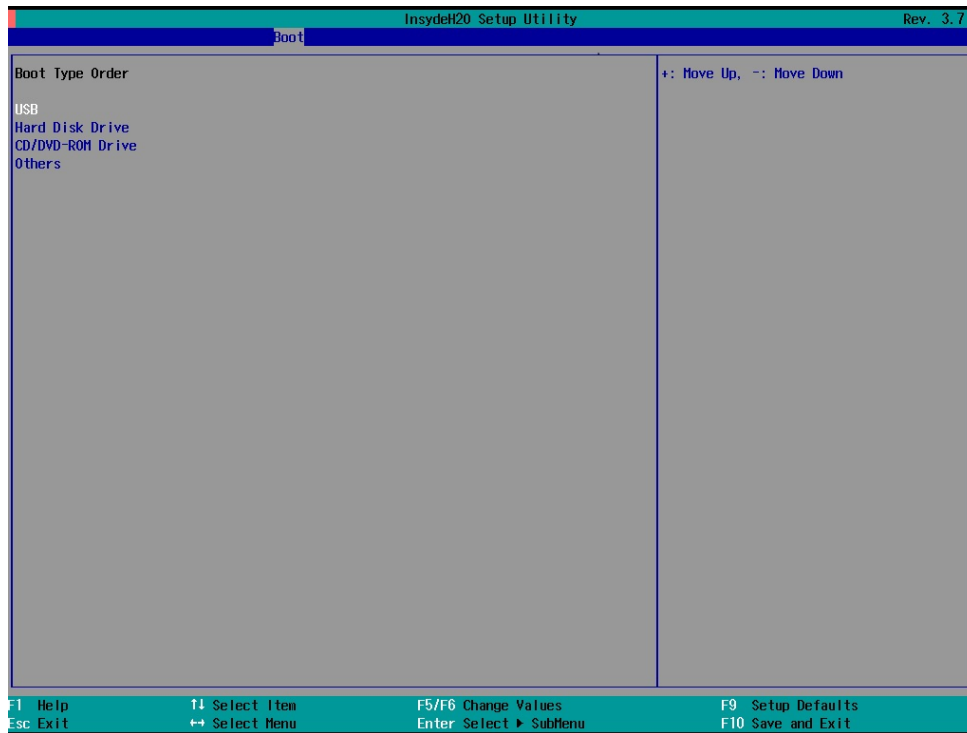
- Use the left and right arrow keys to navigate to the **Boot** menu.
- Use the up and down arrow keys to navigate to the **Legacy** field; then, press [Enter].



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



- 5. Use the up and down arrow keys to navigate to the **USB** link; then, use the plus or minus (+/-) key to move **USB** to the top of boot priority list.



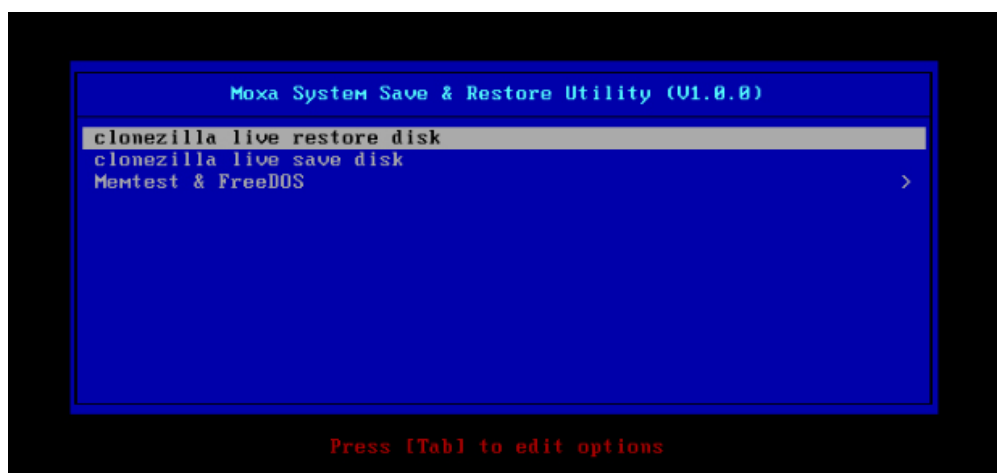
6. Press **F10** and [Enter] to save and exit the BIOS configuration interface. This sets the system to reboot from the hard drive.

Step 3: Performing a System Recovery

This step describes how to perform a system recovery. We include this as step 3 of the installation so administrators can first perform a test run before deploying the system to the field.

To begin the system recovery process, configure the BIOS settings as described in the previous section **Step 2: Setting the BIOS to Boot via USB**. Then, connect the USB recovery drive to any USB ports on the V2406A 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 port.

1. Select **clonezilla live restore disk** to boot into the system recovery environment.



2. Wait until the boot process is finished.


```

[ 5.153522] sd 0:0:0:0: [sda] Attached SCSI disk
[ 5.163726] sd 0:0:1:0: [sdb] Attached SCSI disk
[ 5.287941] sd 0:0:0:0: Attached scsi generic sg0 type 0
[ 5.310750] sd 0:0:1:0: Attached scsi generic sg1 type 0
[ 5.334915] sr 1:0:0:0: Attached scsi generic sg2 type 5
Begin: Loading essential drivers ... [ 5.690577] Atheros(R) L2 Ethernet Driver - version 2.2.3
[ 5.692430] Copyright (c) 2007 Atheros Corporation.
[ 5.776770] Broadcom NetXtreme II 5771x 10Gigabit Ethernet Driver bnx2x 1.62.00-6 (2011/01/30)
[ 5.914014] Btrfs loaded
[ 5.955475] device-mapper: uevent: version 1.0.3
[ 5.961407] device-mapper: ioctl: 4.19.1-ioctl (2011-01-07) initialised: dm-devel@redhat.com
done.
Begin: Running /scripts/init-premount ... done.
Begin: Mounting root file system ... [ 6.178946] Uniform Multi-Platform E-IDE driver
[ 6.186189] ide_generic: please use "probe_mask=0x3f" module parameter for probing all legacy ISA
IDE ports
[ 6.913744] FAT: utf8 is not a recommended IO charset for FAT filesystems, filesystem will be case
sensitive!
[ 7.047997] aufs: module is from the staging directory, the quality is unknown, you have been warn
ed.
[ 7.072516] aufs 2.1-standalone.tree-38-rcN-20110228
Begin: Running /scripts/live-premount ... done.
[ 7.213433] loop: module loaded
[ 7.509770] squashfs: version 4.0 (2009/01/31) Phillip Lougher
Begin: Running /scripts/live-realpremount ... done.
Begin: Mounting "/live/image/live/filesystem.squashfs" on "/filesystem.squashfs" via "/dev/loop0" .
.. done.
done.
Begin: Running /scripts/live-bottom
... Begin: Configuring fstab ... done.
Begin: Preconfiguring networking ... done.
Begin: Loading preseed file ... done.
Begin: Running /scripts/init-bottom ... done.
INIT: version 2.88 booting
Using makefile-style concurrent boot in runlevel S.
live-config: hostname user-setup sudo locales tzdata keyboard-configuration sysvinit sysv-rc initram
fs-tools util-linux login openssh-server_

```

3. The screen displays warning messages to 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) to start the system recovery process.

You can press any key or [Ctrl + C] to cancel the recovery process and exit Clonezilla.

```

The jobs in /etc/ocs/ocs-live.d/ are finished. Start "ocs-live-restore" now.
Setting the TERM as linux
*****
Clonezilla image dir: /home/partimag
*****
Shutting down the Logical Volume Manager
  No volume groups found
  No volume groups found
Finished Shutting down the Logical Volume Manager
*****
Activating the partition info in /proc... done!
*****
The following step is to restore an image to the hard disk/partition(s) on this machine: "/home/part
imag/xpe_savedisk" -> "sda sda1"
WARNING!!! WARNING!!! WARNING!!!
WARNING! THE EXISTING DATA IN THIS HARDDISK/PARTITION(S) WILL BE OVERWRITTEN! ALL EXISTING DATA WILL
BE LOST:
*****
Machine: VirtualBox
sda (2.1GB_VBOX_HARDDISK__ata-VBOX_HARDDISK_VB1c64a0a3-c9f7523d)
*****
Are you sure you want to continue? ?
[y/n] y

```

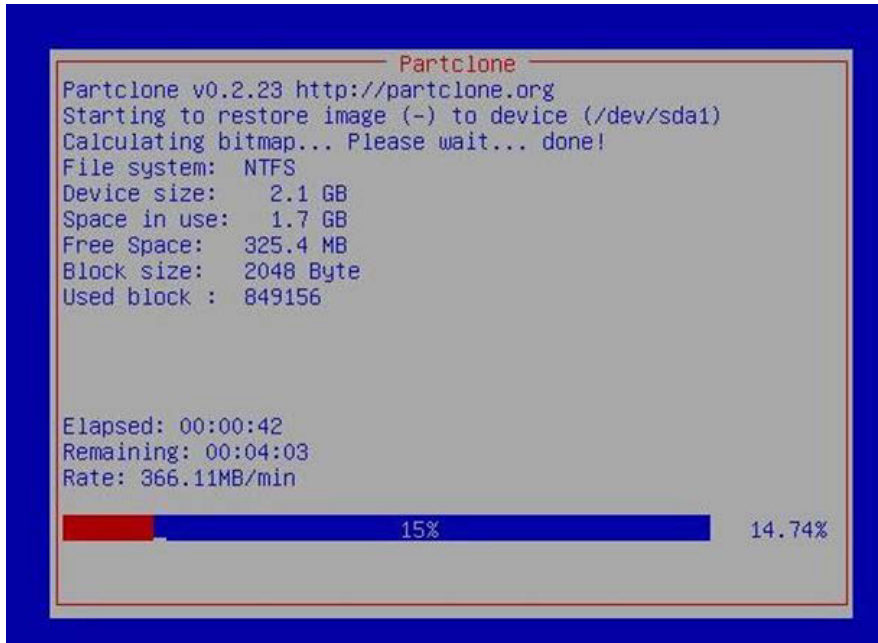
4. The screen displays another warning message to remind you that you are about to overwrite your hard drive and erase all data on the partition listed (**sda1**, in the following figure). If you want to continue, enter **Y** (case insensitive).

```

*****
Machine: VirtualBox
sda (2.1GB_VBOX_HARDDISK__ata-VBOX_HARDDISK_VB1c64a0a3-c9f7523d)
*****
Are you sure you want to continue? ?
[y/n] y
OK, let's do it!!
This program is not started by clonezilla server.
The following step is to restore an image to the hard disk/partition(s) on this machine: "/home/part
imag/xpe_savedisk" -> "sda (sda1)"
WARNING!!! WARNING!!! WARNING!!!
WARNING! THE EXISTING DATA IN THIS HARDDISK/PARTITION(S) WILL BE OVERWRITTEN! ALL EXISTING DATA WILL
BE LOST:
*****
Machine: VirtualBox
sda (2.1GB_VBOX_HARDDISK__ata-VBOX_HARDDISK_VB1c64a0a3-c9f7523d)
*****
Let me ask you again, Are you sure you want to continue? ?
[y/n] _

```

5. Wait until the process is finished.



The screenshot shows the Partclone utility in a terminal window. The title bar reads "Partclone". The text displayed is as follows:

```

Partclone v0.2.23 http://partclone.org
Starting to restore image (-) to device (/dev/sda1)
Calculating bitmap... Please wait... done!
File system: NTFS
Device size: 2.1 GB
Space in use: 1.7 GB
Free Space: 325.4 MB
Block size: 2048 Byte
Used block : 849156

Elapsed: 00:00:42
Remaining: 00:04:03
Rate: 366.11MB/min

```

At the bottom, there is a progress bar with a red segment on the left. The text "15%" is centered above the bar, and "14.74%" is shown to the right of the bar.

6. To complete the recovery process, select **(0) Power off** to 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, the system will not shut down and will immediately initiate a soft reboot. To avoid this, use the switch to cut off power to the computer immediately following the shutdown command, or simply the power switch from the front panel and use the console to shut down the computer by pressing **0**.

```

Restoring the first 446 bytes of MBR data, i.e. executable code area, for sda... done!
*****
Now resize the partition for sda1
ntfsresize -f /dev/sda1
ntfsresize v2.0.0 (libntfs 10:0:0)
Device name      : /dev/sda1
NTFS volume version: 3.1
Cluster size     : 2048 bytes
Current volume size: 2064511488 bytes (2065 MB)
Current device size: 2064513024 bytes (2065 MB)
New volume size   : 2064511488 bytes (2065 MB)
Nothing to do: NTFS volume size is already OK.
*****
The grub directory is NOT found. Maybe it does not exist (so other boot manager exists) or the file
system is not supported in the kernel. Skip running grub-install.
*****
Found NTFS boot partition among the restored partition(s): /dev/sda1
Head and sector no. of /dev/sda from EDD: 64, 63.
The start sector of NTFS partition /dev/sda1: 63
Adjust filesystem geometry for the NTFS partition: /dev/sda1
Running: partclone.ntfsfixboot -w -h 64 -t 63 -s 63 /dev/sda1
ntfsfixboot version 0.9
done!
*****
*****
This program is not started by Clonezilla server, so skip notifying it the job is done.
Finished!
Now syncing - flush filesystem buffers...

"ocs-live-restore" is finished.
Now you can choose to:
(0) Poweroff
(1) Reboot
(2) Enter command line prompt
(3) Start over
[2]

```

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

Step 4: Resetting the BIOS

Reset the boot priority to the factory default settings to allow the system to boot from the main system storage drive. This is done for two reasons:

- The first reason is for security, since the computer will not be able to be rebooted from unauthorized USB drives.
- The second reason is because the computer is able to boot up from a non-bootable USB drive. Currently, if the V2406A is set to boot from a USB drive, the V2406A's boot process stops anytime you insert a non-bootable USB data drive into the machine. The V2406A cannot detect USB data drives and boot-capable OS drives.

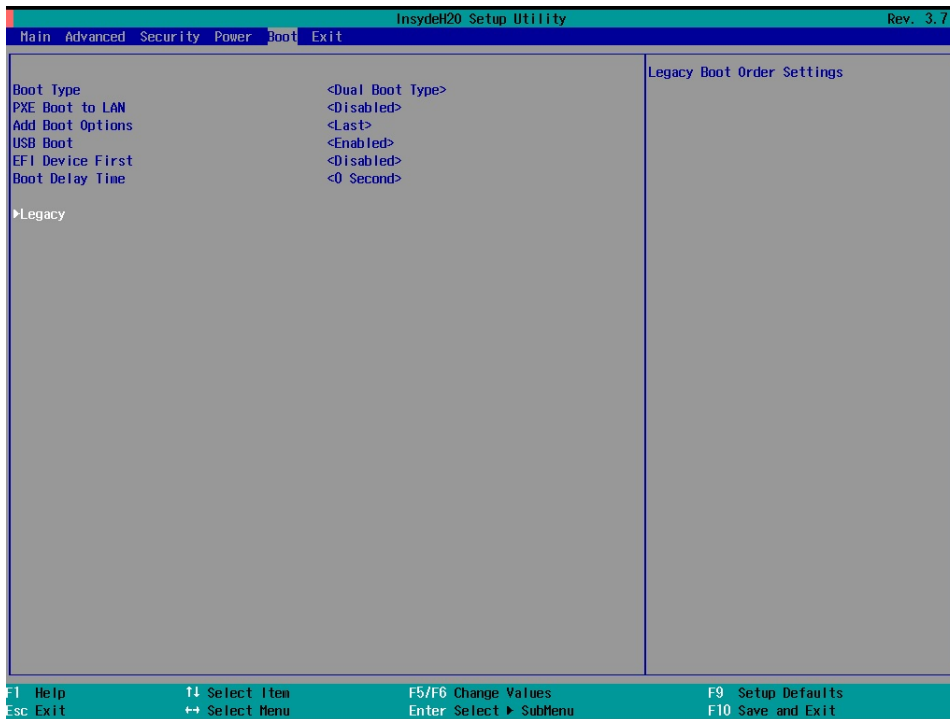
Complete the following steps to reset the boot priority setting:

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

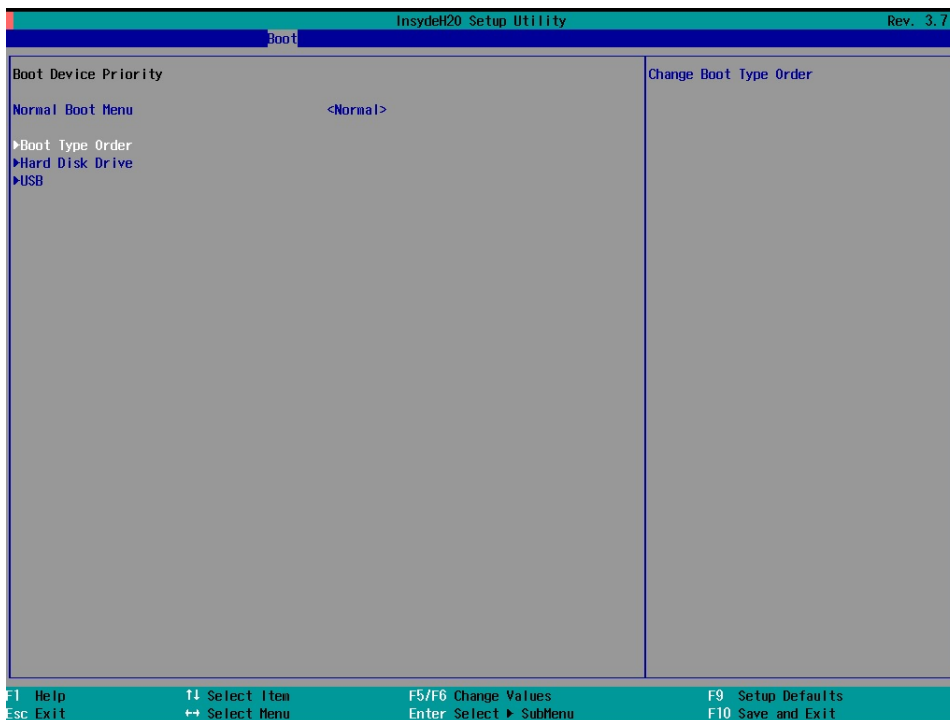


2. Use the left and right arrow keys to navigate to the **Boot** menu.

- Use the up and down arrows to navigate to the **Legacy** link; then, press [Enter].



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



- Use the up and down arrows to highlight **Hard Disk Drive** and use the plus or minus (+/-) key to move **Hard Disk Drive** to the top of the boot priority list.



6. Press **F10** and [Enter] to save and exit the BIOS configuration interface. This sets the system to reboot, and the system should now boot from the hard drive.

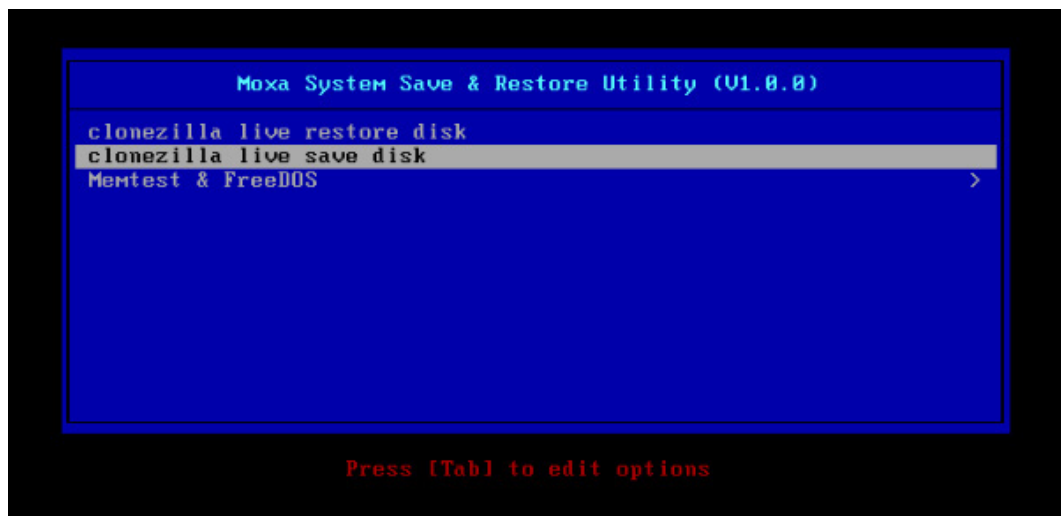
For more information about initializing user settings, refer to the **System Initialization** chapter.

Creating a Custom System Image

In this section, we describe how to create a custom system image so that all of 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**, and to be used as a **full system recovery image** if the system crashes. **All files under F:\home\partimag\ will be overwritten.**

Before proceeding, make sure you have already completed **Step 1: Prepare the USB drive** and **Step 2: Setting the BIOS to Boot via USB**, and then continue with the following steps to create a custom system image.

1. Once the system has launched and the V2406A has booted the recovery environment from the USB drive, navigate to **clonezilla live save disk**, and then 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 V2406A boots into the image creation environment. Wait until the boot process is complete.

```

[ 5.141941] sd 0:0:1:0: [sdb] Attached SCSI disk
[ 5.257277] sd 0:0:0:0: Attached scsi generic sg0 type 0
[ 5.269691] sd 0:0:1:0: Attached scsi generic sg1 type 0
[ 5.280668] sr 1:0:0:0: Attached scsi generic sg2 type 5
Begin: Loading essential drivers ... [ 5.772551] Atheros(R) L2 Ethernet Driver - version 2.2.3
[ 5.774561] Copyright (c) 2007 Atheros Corporation.
[ 5.863196] Broadcom NetXtreme II 5771x 10Gigabit Ethernet Driver bnx2x 1.62.00-6 (2011/01/30)
[ 6.005932] Btrfs loaded
[ 6.054095] device-mapper: uevent: version 1.0.3
[ 6.059737] device-mapper: ioctl: 4.19.1-ioctl (2011-01-07) initialised: dm-devel@redhat.com
done.
Begin: Running /scripts/init-premount ... done.
Begin: Mounting root file system ... [ 6.289382] Uniform Multi-Platform E-IDE driver
[ 6.301889] ide_generic: please use "probe_mask=0x3f" module parameter for probing all legacy ISA
IDE ports
[ 6.801141] NTFS driver 2.1.30 [Flags: R/W MODULE].
[ 6.914295] NTFS volume version 3.1.
Begin: Running /scripts/live-premount ... done.
[ 7.331989] FAT: utf8 is not a recommended IO charset for FAT filesystems, filesystem will be cas
e sensitive!
[ 7.453369] aufs: module is from the staging directory, the quality is unknown, you have been war
ned.
[ 7.479098] aufs 2.1-standalone.tree-38-rcN-20110228
[ 7.610228] loop: module loaded
[ 7.905144] squashfs: version 4.0 (2009/01/31) Phillip Lougher
Begin: Running /scripts/live-realpremount ... done.
Begin: Mounting "/live/image/live/filesystem.squashfs" on "/"filesystem.squashfs" via "/dev/loop0" .
.. done.
done.
Begin: Running /scripts/live-bottom
... Begin: Configuring fstab ... done.
Begin: Preconfiguring networking ... done.
Begin: Loading preseed file ... done.
Begin: Running /scripts/init-bottom ... done.
INIT: version 2.88 booting
Using makefile-style concurrent boot in runlevel S.

```

- Once the image creation environment is booted up, a warning message displays asking whether you want to continue. Note that if you create the recovery image, then **any files copied in the /home/partimag directory will be deleted**. If you want to save the files in the USB **partition image** directory, you must exit the recovery environment and copy the files to another disk. Press **Y** (case insensitive) to continue with the image creation.

```

Setting the TERM as linux
*****
Clonezilla image dir: /home/partimag
*****
Shutting down the Logical Volume Manager
  No volume groups found
  No volume groups found
Finished Shutting down the Logical Volume Manager
Selected device [sda] found!
The selected devices: sda
*****
Activating the partition info in /proc... done!
Selected device [sda] found!
The selected devices: sda
Searching for data partition(s)...
Excluding busy partition or disk...
Unmounted partitions (including extended or swap): sda1
Collecting info.. done!
Searching for swap partition(s)...
Excluding busy partition or disk...
Unmounted partitions (including extended or swap): sda1
Collecting info.. done!
The data partition to be saved:  sda1
The swap partition to be saved:
Activating the partition info in /proc... done!
Selected device [sda1] found!
The selected devices: sda1
Getting /dev/sda1 info...
*****
The following step is to save the hard disk/partition(s) on this machine as an image:
*****
Machine: VirtualBox
sda (2103MB_VBOX_HARDDISK__ata-VBOX_HARDDISK_VB1c64a0a3-c9f7523d)
sda1 (2065MB_ntfs(In_VBOX_HARDDISK_)_ata-VBOX_HARDDISK_VB1c64a0a3-c9f7523d)
*****
-> "/home/partimag/xpe_savedisk".
Are you sure you want to continue? ? (y/n) y

```

- The recovery environment starts to copy the entire hard drive to your USB drive. This may take several minutes. Wait until the process is complete.

**WARNING**

Do NOT remove the USB drive from the computer during the data copy process.

```

/dev/sdb1: read failed after 0 of 2048 at 0: Input/output error
No volume groups found
No volume groups found
Finished Shutting down the Logical Volume Manager
Checking the integrity of partition table in the disk /dev/sda...
Reading the partition table for /dev/sda..RETV=0
*****
done!
Saving the MBR data for sda...
1+0 records in
1+0 records out
512 bytes (512 B) copied, 0.00347646 s, 147 kB/s
*****
Starting saving /dev/sda1 as /home/partimag/xpe_savedisk/sda1.XXX...
/dev/sda1 filesystem: ntfs.
*****
Checking NTFS integrity in /dev/sda1... done!
Checking the disk space...
Use ntfsclone with gzip to save the image.
Image file will be split with size limit 1000000 MB.
*****
If this action fails or hangs, check:
* Is the disk full ?
*****
ntfsclone v2.0.0 (libntfs 10:0:0)
NTFS volume version: 3.1
Cluster size      : 2048 bytes
Current volume size: 2064510976 bytes (2065 MB)
Current device size: 2064513024 bytes (2065 MB)
Scanning volume ...
100.00 percent completed
Accounting clusters ...
Space in use      : 1770 MB (85.7%)
Saving NTFS to image ...
_ 0.64 percent completed

```

- Choose whether to power down the computer (press **0**), reboot (press **1**), access the console terminal (to access a console TTY, press **2**), or re-initiate the entire procedure (press **3**).

**WARNING**

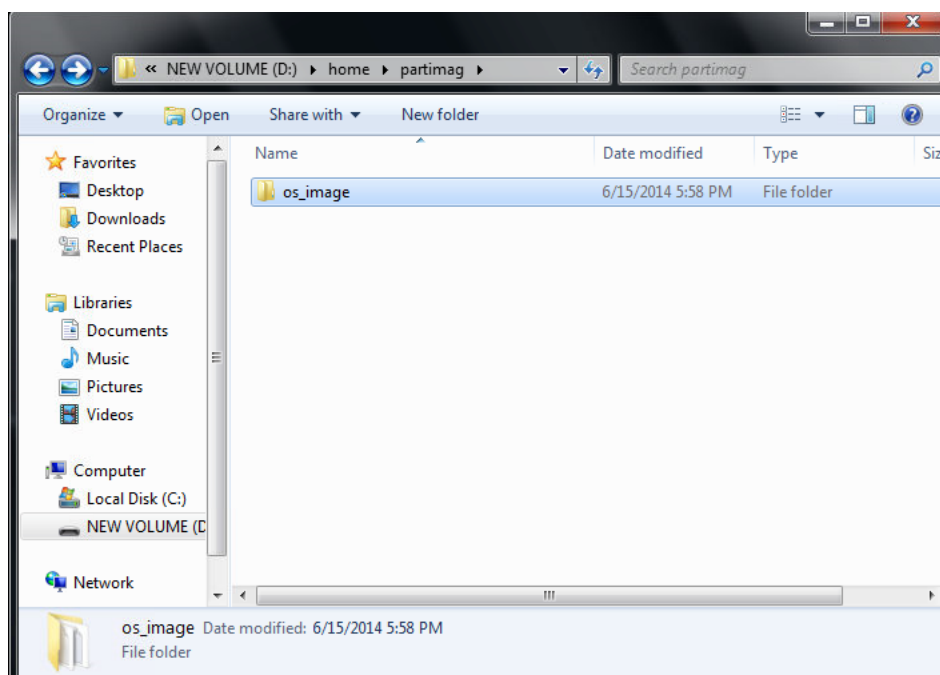
Do NOT remove the USB drive from the computer until you have rebooted or powered down the system.

```
Restoring the first 446 bytes of MBR data, i.e. executable code area, for sda... done!
*****
Now resize the partition for sda1
ntfsresize -f /dev/sda1
ntfsresize v2.0.0 (libntfs 10:0:0)
Device name      : /dev/sda1
NTFS volume version: 3.1
Cluster size    : 2048 bytes
Current volume size: 2064511488 bytes (2065 MB)
Current device size: 2064513024 bytes (2065 MB)
New volume size  : 2064511488 bytes (2065 MB)
Nothing to do: NTFS volume size is already OK.
*****
The grub directory is NOT found. Maybe it does not exist (so other boot manager exists) or the file
system is not supported in the kernel. Skip running grub-install.
*****
Found NTFS boot partition among the restored partition(s): /dev/sda1
Head and sector no. of /dev/sda from EDD: 64, 63.
The start sector of NTFS partition /dev/sda1: 63
Adjust filesystem geometry for the NTFS partition: /dev/sda1
Running: partclone.ntfsfixboot -w -h 64 -t 63 -s 63 /dev/sda1
ntfsfixboot version 0.9
done!
*****
*****
This program is not started by Clonezilla server, so skip notifying it the job is done.
Finished!
Now syncing - flush filesystem buffers...

"ocs-live-restore" is finished.
Now you can choose to:
(0) Poweroff
(1) Reboot
(2) Enter command line prompt
(3) Start over
[2]
```

- Power down the system and remove the USB drive.

The recovery environment setup is complete and you have created an OS image in the **USB Folder\home\partimag\os_image** folder. Label the USB drive and store it in a safe place.



A

Moxa SynMap OID Table

This appendix provides information on the Moxa SynMap OID table.

The following topics are covered in this appendix:

- **Moxa SynMap OID Table**
- **HOST RESOURCE OID Table**

Moxa SynMap OID Table

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

Item Name	OID	MAX-Access	Description	Support
productName	1.3.6.1.4.1.8691.17.1.1.1.0	read-only	Show the product name	✓
productDesc	1.3.6.1.4.1.8691.17.1.1.2.0	read-only	Show the product short description	
productVersion	1.3.6.1.4.1.8691.17.1.1.3.0	read-only	Show the product version	✓
productBuildDate	1.3.6.1.4.1.8691.17.1.1.4.0	read-only	Show the product's last build date; the format is YYMMDDHH	✓
biosVersion	1.3.6.1.4.1.8691.17.1.4.1	read-only	Show the BIOS version	
biosSaveSetting	1.3.6.1.4.1.8691.17.1.4.2	read-write	Write: 1 saves the bios setting Read: 0 means the setting has been applied	
biosSettingStatus	1.3.6.1.4.1.8691.17.1.4.3	read-only	Show a comparison of "bios CMOS setting" and "bios new setting"	
bootDeviceStatus	1.3.6.1.4.1.8691.17.1.4.4.1	read-only	Show the currently active boot devices	
firstBootDevice	1.3.6.1.4.1.8691.17.1.4.4.2	read-write	Read: Show the current first boot device Write: Set the boot device	
pwrOnAfterPwrFail	1.3.6.1.4.1.8691.17.1.4.8.1	read-write	Set the computer to power on after a power failure	
pwrLanWakeUp	1.3.6.1.4.1.8691.17.1.4.8.3	read-write	Enable/Disable wake on LAN functionality	
tempSensorsIndex	1.3.6.1.4.1.8691.17.1.5.1.1.1	read-only	Reference index for each observed device	✓
tempSensorsDevice	1.3.6.1.4.1.8691.17.1.5.1.1.2	read-only	The name of the temperature sensor being read	✓
tempSensorsValue	1.3.6.1.4.1.8691.17.1.5.1.1.3	read-only	The temperature of this sensor in mC	✓
voltSensorsIndex	1.3.6.1.4.1.8691.17.1.5.1.2.1.1	read-only	Reference index for each observed device	✓
voltSensorsDevice	1.3.6.1.4.1.8691.17.1.5.1.2.1.2	read-only	The name of the device we are reading.	✓
voltSensorsValue	1.3.6.1.4.1.8691.17.1.5.1.2.1.3	read-only	The voltage in mV	✓
ioDiNumber	1.3.6.1.4.1.8691.17.1.6.1.2.1.0	read-only	Number of digital input pins in the current system	✓
diIndex	1.3.6.1.4.1.8691.17.1.6.1.2.2.1.1	read-only	Reference index of each digital input pin	✓
diPort	1.3.6.1.4.1.8691.17.1.6.1.2.2.1.2	read-only	Port number of the digital input pin	✓
diValue	1.3.6.1.4.1.8691.17.1.6.1.2.2.1.3	read-only	Digital input status: 0 is low, 1 is high	✓

Item Name	OID	MAX-Access	Description	Support
diTrapEnable	1.3.6.1.4.1.8691.17.1.6.1.1.2.1.4	read-write	Agent will send a trap message when the digital input pin status has changed and this object is enabled	
ioDoNumber	1.3.6.1.4.1.8691.17.1.6.1.2.3.0	read-only	Number of digital output pins in the current system	✓
doIndex	1.3.6.1.4.1.8691.17.1.6.1.1.4.1.1	read-only	Reference index of each digital output pin	✓
doPort	1.3.6.1.4.1.8691.17.1.6.1.2.4.1.2	read-only	Port number of the digital output pin	✓
doValue	1.3.6.1.4.1.8691.17.1.6.1.2.4.1.3	read-write	Digital output status: 0 is low, 1 is high	✓
uartNumber	1.3.6.1.4.1.8691.17.1.6.3.1	read-only	Number of internal UARTs in the current system	✓
uartIndex	1.3.6.1.4.1.8691.17.1.6.3.2.1.1	read-only	Reference index of each UART port	✓
uartType	1.3.6.1.4.1.8691.17.1.6.3.2.1.2	read-write	UART mode: 0 is RS232, 1 is RS485 2-wire, 2 is RS422, 3 is RS485 4-wire	✓
usbNumber	1.3.6.1.4.1.8691.17.1.6.3.1.0	read-only	Number of ports, regardless of their current state, in the usb general port table	
usbDeviceIndex	1.3.6.1.4.1.8691.17.1.6.4.1.3.1.1	read-only	The index is identical to usbPortIndex for the corresponding USB port	
usbDeviceVendorID	1.3.6.1.4.1.8691.17.1.6.4.1.3.1.2	read-only	The USB device port vendor HEX-formatted string, as it is provided to the USB host by the USB device	
usbDeviceProductID	1.3.6.1.4.1.8691.17.1.6.4.1.3.1.3	read-only	The product ID HEX-formatted string as it is provided to the USB host by the USB device	
usbDeviceActiveClasses	1.3.6.1.4.1.8691.17.1.6.4.1.3.1.4	read-only	Returns the USB Device Class type of the active configuration	
usbPlugTrapEnable	1.3.6.1.4.1.8691.17.1.6.4.1.4	read-write	Agent will send a trap message when a USB device is inserted or removed, and this object is enabled	
moxaSystemTrapIP	1.3.6.1.4.1.8691.17.1.9.1.0	read-write	Set Trap IP address	✓
moxaSystemTrapCommunity	1.3.6.1.4.1.8691.17.1.9.2.0	read-write	Trap community	✓

HOST RESOURCE OID Table

The following table shows Host Resource OIDs.

Item Name	OID	MAX-Access	Description	Support
hrProcessorTable	1.3.6.1.2.1.25.3.3	read-only	Show CPU usage	✓
hrStorageTable	1.3.6.1.2.1.25.2.3	read-only	Show disk and memory usage	✓