MIP 5000 VoIP Radio Console Windows Supplemental Configuration

MOTOROLA

6871013P79-B
OCTOBER 2010

CONTENTS

INDEX

LIST OF FIGURES

LIST OF TABLES

LIST OF PROCEDURES & PROCESSES

WINDOWS SUPPLEMENTAL CONFIGURATION

This manual supplements the MIP 5000 system documentation set with additional procedures for Microsoft® Windows®-based devices in a MIP 5000 system.

WHAT IS COVERED IN THIS MANUAL

This manual describes how to configure a computer to run MIP 5000 VoIP Radio Console and other Windows applications in a secure environment.

Chapter 1, “Overview and Preparation” provides an overview on the procedures required in this document and essential information before you start.

Chapter 2, “Windows Supplemental CD System Configuration” contains the procedures for the Windows Supplemental CD.

Chapter 3, “Optional System Configuration” describes common procedures for customizing system capabilities.

HELPFUL BACKGROUND INFORMATION

The Motorola technical training team offers a variety of courses designed to assist you in learning about your system. For a complete list of available courses and schedules, go to http://www.motorola-wls.com.

RELATED INFORMATION

Refer to the following documents for associated information about the MIP 5000 system:

Related Manuals	Purpose
MIP 5000 VoIP Radio Console System Planner	Provides information necessary to plan a MIP 5000 VoIP Radio Console system
MIP 5000 VoIP Radio Console Operator Manual (6881013Y34)	Describes how to use a MIP 5000 VoIP Radio Console position
MIP 5000 VoIP Radio Console Supervisor Manual (6881013Y33)	Describes how to configure and customize MIP 5000 VoIP Radio Console positions
MIP 5000 VoIP Radio Console Installation and Configuration Manual (6881013Y35)	Describes how to install and configure a MIP 5000 system

ASSUMPTIONS AND CAVEATS

This document assumes the following:

- Windows Vista Business Edition with Service Pack 2 is running on computer on which the MIP 5000 VoIP Radio Console is installed.
- The operating system (OS) has been installed and correctly configured.
- MIP 5000 3.0 Radio Console computers are configured as members of a Windows workgroup, not a domain.
- The latest available OS patches have been applied. For more information, see Appendix A, “Product Exceptions,” on page A-1.
- All the product applications have been installed.

NOTE

If all these assumptions are not met, do not proceed with the procedures in this document.

- When you perform any administrative tasks on Microsoft® Windows Vista™ Business edition Operating System, the User Access Control (UAC) dialog box appears. Depending on the PC configuration, the system asks you either to click **Continue/Allow** to continue or provide local or domain administrator credentials.

IMPORTANT

In order to successfully complete the procedures, you must perform all the procedures when logged in as a valid local administrator (except where otherwise stated).

- After applying these procedures, the Windows **Autorun** (also known as Autoplay) feature is turned off which means its functionality is no longer accessible. For example, CDs do not automatically start when inserted in the drive, nor is the name of the CD automatically refreshed in Windows Explorer.
- After these procedures are applied, passwords for existing user accounts will continue to work. However, password complexity requirements will be enforced when the existing passwords are changed. The password will require eight or 14 characters in length (depending on the feature option), with at least one upper and lower case letter, and at least one number and special character (for example, emPadg2! or weRjkt&53dqa).

IMPORTANT

Applying these procedures to any PC/application other than what is explicitly mentioned in this manual is not recommended. Doing so may require a reinstallation of the operating system.

NOTE

This manual describes how to configure a computer to run Windows applications in a secure environment. It does not describe how to configure a secure network.

THIS PAGE INTENTIONALLY LEFT BLANK.

CHAPTER

1

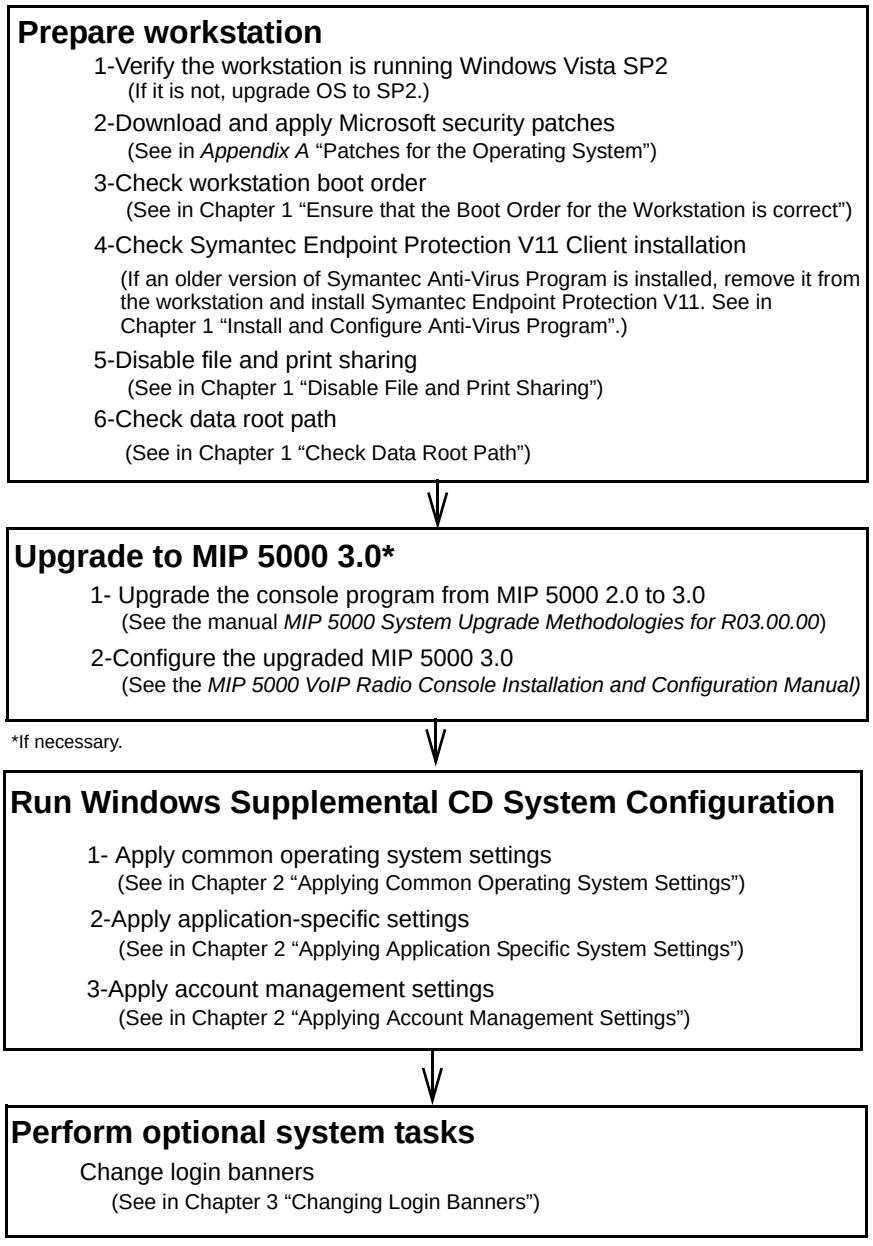
OVERVIEW AND PREPARATION

This chapter describes the procedures for creating a secure environment for the MIP 5000 VoIP Radio Console on a Windows Vista system and the order in which the procedures must be followed.

WORKFLOW

The flowchart below describes the chapters in this manual and the order of procedures described within each:

FIGURE 1-1 SYSTEM ENVIRONMENT SECURITY WORKFLOW



Compatibility Matrix

The compatibility matrix contains information regarding the compatibility between the procedures in this documents and Windows products found in a MIP 5000 system. The procedures should be applied in the order in which they appear in this document (from top to bottom in the Procedures row).

Table 1-1 Legend for the Compatibility Matrix

Symbol	Meaning
YES	This procedure can be performed if the customer wishes.
NO	This procedure must NEVER be performed as it will break functionality.
NA	This procedure is not applicable to the operating system for a given product.
REQ	This procedure is REQUIRED for proper operation.
(Blank)	Refer to product documentation for specific settings.

Table 1-2 Compatibility Matrix

Procedures	Applications		
	MIP 5000 (Console, CSDM, and SSH in any combination)	PlantCML IRR	Anti-Virus Client
USB Boot Order See "Ensure that the Boot Order for the Workstation is correct" on page 1-5.	REQ	REQ	NA
Disable File & Print Sharing See "Disable File and Print Sharing" on page 1-7.	YES	YES	NA
Apply Operating System Settings See "Applying Common Operating System Settings" on page 2-2.	REQ	REQ	NA

TABLE 1-2 COMPATIBILITY MATRIX (CONTINUED)

Procedures	Applications		
	MIP 5000 (Console, CSDM, and SSH in any combination)	PlantCML IRR	Anti-Virus Client
Apply Application Specific Settings See "Applying Application-Specific System Settings" on page 2-4.	REQ	REQ	REQ
Apply Account Management "Applying Account Management Settings" on page 2-6.	REQ	REQ	NA

COHABITATION

In cohabitation situations, this matrix will tell you how to configure a computer so that its multiple applications can operate correctly under a given environment. When reading this chart for cohabitation purposes, you need to consider multiple rows for a given column. If any row for a given column is marked with NO, then that procedure should NOT be performed on the cohabitation computer that will host multiple applications. This is true even if another row for another product indicates YES. If one product indicates REQ and another product indicates NO for a given procedure, these products may not cohabitate.

Before You Begin

IMPORTANT

Before you begin, you must ensure that the following tasks have been completed:

- The operating system (OS) has been installed and correctly configured.
- The Windows Vista Business Edition operating system has been upgraded from Service Pack 1 to Service Pack 2.
- All appropriate Microsoft security patches have been applied.
- All the product applications have been installed and correctly configured.

CAUTION

Do not configure the workstation's OS firewall settings if an earlier version of the Windows Supplemental CD has been applied to the workstation.

Do not attempt to open the Windows Firewall after completing the Windows Supplemental Configuration CD procedures.

Doing either will compromise security and could interfere with the MIP 5000 product.

Ensure that the Boot Order for the Workstation is Correct

The PC boot order and configuration are found in the PC BIOS. Please refer to the documentation from the PC manufacture for instructions on how to set this correctly.

Perform one of the following tasks, preferably the first one:

- Ensure that USB devices do not appear anywhere in the PC boot order.
- Ensure that USB devices do not appear before the hard drives in the PC boot order.

IMPORTANT

Do not disable USB devices on MIP 5000 VoIP Radio Console computers. USB devices are required for MIP 5000 operation.

INSTALL AND CONFIGURE ANTI-VIRUS PROGRAM

Install the Symantec anti-virus program, Symantec Endpoint Protection, on each console computer.

TO INSTALL UNMANAGED SYMANTEC ENDPOINT PROTECTION CLIENT SOFTWARE

PROCEDURE 1-1 HOW TO INSTALL UNMANAGED SYMANTEC ENDPOINT PROTECTION CLIENT SOFTWARE

1	Log on as a valid administrator.
2	Insert the installation CD into the DVD/CD drive and start the installation program if it does not start automatically.
3	Click **Install Symantec Endpoint Protection Client**.
4	Click **Next** on the **Welcome** panel.
5	Click **I accept the terms in the license agreement** in the License Agreement Panel and click **Next**.
6	Ensure **Unmanaged client** is selected in the Client Type panel and click **Next**.
7	Click **Typical** in the Setup Type panel to install the client software with the most common options and click **Next**.
8	Click **Install** in the Ready to Install the Program panel.
9	After the installation completes, LiveUpdate launches. If the computer is connected to the Internet, LiveUpdate automatically downloads and installs the latest update from the Symantec update Website.  **NOTE** You might be prompted to restart the computer.
10	Click **Exit**.
11	Repeat for each console computer.

To Update Symantec Endpoint Protection Client Software

In a secure environment, Symantec Endpoint Protection may not be able to update its list of virus definitions automatically from the Internet, so the list must be updated manually. (When not connected to the Internet, the Automatic Live Update feature is disabled.) Download and install the latest copy of Symantec virus definitions from the Symantec FTP site using a computer connected to the Internet.

Procedure 1-2 How to Update Symantec AntiVirus Virus Definitions

1	Use Internet Explorer or another Internet browser to navigate to http://www.symantec.com/business/security_response/definitions/download/detail.jsp?gid=savce **Result:** The Webpage contains the installation files for virus definition updates of the Symantec Endpoint Protection V11 program.
2	Under **Client installations on Windows Platforms (32-bit)** in the sub-section **Symantec Endpoint Protection Client installations on Windows platforms (32-bit)**, select and download the virus definition update file: for example, **20100527-039-v5i32.exe** is the update file for 27 May 2010.
3	Copy the virus definition executable file to removable media so it can be installed easily on each console computer.
4	On each console computer, run the virus definition update file. To the question **Do you want to deploy all the updates from the Intelligent Updater?**, answer **Yes**.

Disable File and Print Sharing

Note

With File and Print Sharing disabled, it is not possible to use the PlantCML IRR Remote Access feature.

If you have already enabled remote access for PlantCML IRR, you must disable it. To disable remote access, use Windows Explorer to navigate to the PlantCMLIRR folder and run the MS-DOS batch file, **disableremote.bat**, then restart the PC. (Right-click the file name and select **Run as administrator**.)

PROCEDURE 1-3 HOW TO DISABLE FILE AND PRINT SHARING

1	Log on as a valid Local administrator.
2	Click **Start** > **Control Panel** > **Network and Sharing Center.**
3	Click **Manage Network Connections**.
4	Right-click **Local Area Connection** and select **Properties**.
5	Clear the check box (remove the check mark) next to **File and Printer Sharing for Microsoft Networks**.
6	Click **OK**.
7	Click the **Close** button.

CHECK DATA ROOT PATH

Users can choose to save their CSDM and the MIP 5000 VoIP Radio Console data files to locations other than the default ones. However, before you proceed further with any additional configuration procedures, you *must* set the data paths of the CSDM and console Windows applications to their defaults. After the system is hardened, *you only have access to the default paths*.

- CSDM Data Root Path—See Chapter 14 “Data Root Path” in the *MIP 5000 VoIP Radio Console Installation and Configuration Manual.*
- Console Data Root Path—See Procedure 4-11 in “Configuring MIP 5000 VoIP Radio Console” in the *MIP 5000 VoIP Radio Console Installation and Configuration Manual*.

CHAPTER 2

WINDOWS SUPPLEMENTAL CD SYSTEM CONFIGURATION

This chapter contains the procedures for configuring the system on which the MIP 5000 VoIP Radio Console is installed.

These procedures only need to be performed whenever the operating system is installed. In most cases, this means they only need to be applied once.

CONFIGURATION WITH THE WINDOWS SUPPLEMENTAL CD

This section should be applied whenever ***any*** software (operating system included) is installed or upgraded on any computer.

NOTE

When applying the Operating System Settings, Application, and Account Management Settings, a command prompt window will appear for a period of time. You may ignore all errors or warnings that are displayed in that window.

NOTE

All the security changes made in Procedure 2-1, Procedure 2-2, and Procedure 2-3 do not take effect until the computer has been rebooted. It important that you reboot the computer after all procedures have been completed.

WINDOWS SUPPLEMENTAL CD LOG FILE

Running the Windows Supplemental CD creates a log file that can be used by Motorola support personnel to answer questions such as which version of the CD was applied. By default, the log file is named “wscdlog.txt” and it is stored in the following location:

- C:\ProgramData\Motorola\IA

If you cannot access this log file or if you cannot write to it after starting the Windows Supplemental CD, the program prompts you to specify a different file.

FIGURE 2-1 WINDOWS SUPPLEMENTAL CD MAIN SCREEN

APPLYING COMMON OPERATING SYSTEM SETTINGS

PROCEDURE 2-1 HOW TO APPLY COMMON OS SETTINGS

1	Log on as a valid administrator.
2	Insert the Windows Supplemental CD into the DVD/CD drive.

Procedure 2-1 How to Apply Common OS Settings (continued)

3 Navigate to the \bin folder of the Windows Supplemental CD and double-click the application file **Windows_Supplemental_GUI.exe**.

NOTE

The **User Account Control** dialog box might appear. Click **Allow** or log on with the administrator password, depending on the prompt command.

Result: The Windows Command Prompt window briefly opens and closes, then the Windows Supplemental CD screen appears as in Figure 2-1.

4 Click the **Operating System** button on the left side of the screen.

Result: The following message appears:

```
The operating system detected is:   <your OS>

Clicking OK will modify OS related security settings.
Do you wish to continue?
```

5 Click **OK**.

NOTE

Ignore any error or warning messages that appear in the Command Prompt window.

Result: A Command Prompt window appears and displays the message:

```
Applying Security Settings
```

After the security settings have been applied, the Command Prompt window closes. Then the following message appears:

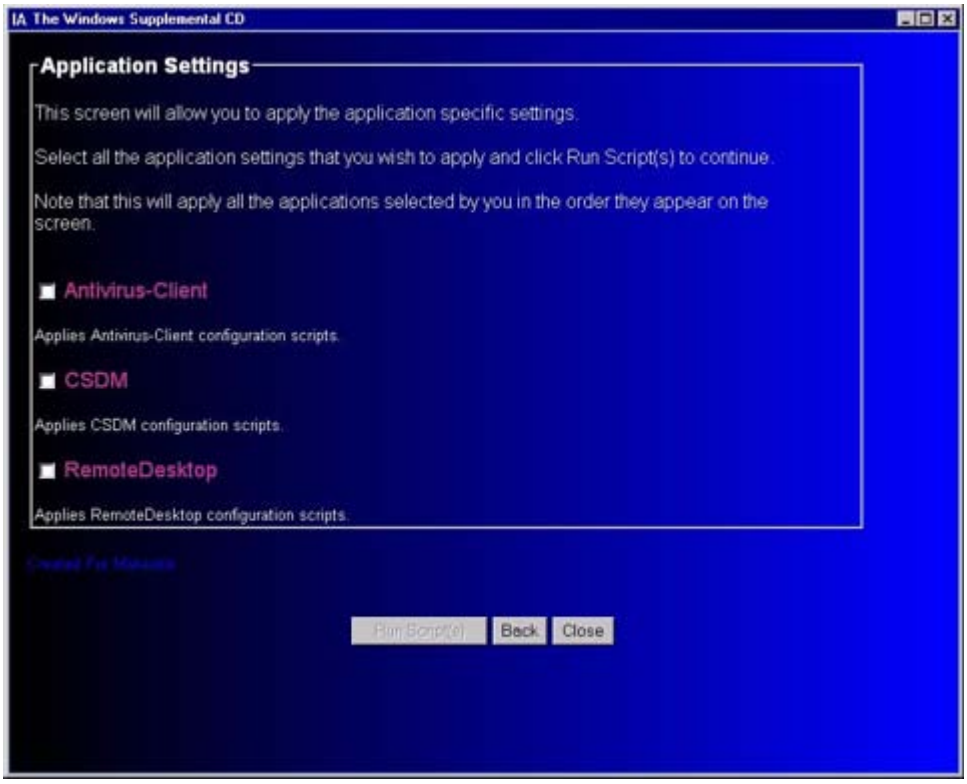
```
The OS security settings have completed successfully.
```

6 Click **Close** to close the Windows Supplemental CD program.

7 Reboot the computer now for the modified settings to take effect immediately or wait and reboot the computer after you have completed all procedures for all modified settings to take effect at the same time.

APPLYING APPLICATION-SPECIFIC SYSTEM SETTINGS

FIGURE 2-2 WINDOWS SUPPLEMENTAL CD APPLICATION SETTINGS SCREEN



PROCEDURE 2-2 HOW TO APPLY APPLICATION-SPECIFIC SETTINGS

1	Log on as a valid administrator.
2	Insert the Windows Supplemental CD into the DVD/CD drive.
3	Navigate to the \bin folder of the Windows Supplemental CD and double-click the application file **Windows_Supplemental_GUI.exe**.

NOTE

The **User Account Control** dialog box might appear. Click **Allow** or log on with the administrator password, depending on the prompt command.

Result: The Windows Command Prompt window briefly opens and closes, then the Windows Supplemental CD screen appears as in Figure 2-1, “Windows Supplemental CD Main Screen,” on page 2-2.

Procedure 2-2 How to Apply Application-Specific Settings (continued)

4 Click the **Application Settings** button on the left side of the screen.

Result: The Application Settings screen appears, showing the list of applications required to apply the security settings, as in Figure 2-2, "Windows Supplemental CD Application Settings Screen," on page 2-4.

5 From the list of applications, select all the applications that will run on this computer, then click the **Run Script(s)** button at the bottom of the screen.

NOTE

The Remote Desktop application script turns off Windows Remote Desktop functionality, so that a user cannot remotely connect to the computer using Remote Desktop Protocol (RDP). The script is required to secure the Windows system.

Result: A Command Prompt window appears and displays the message:

```
Applying Security Settings
```

After the security settings have been applied, the Command Prompt window closes. Then the following message appears:

```
The settings have completed successfully.

You may exit or choose to run other settings.
```

6 Click **OK**.

Repeat this step for each application that was selected in step 5.

NOTE

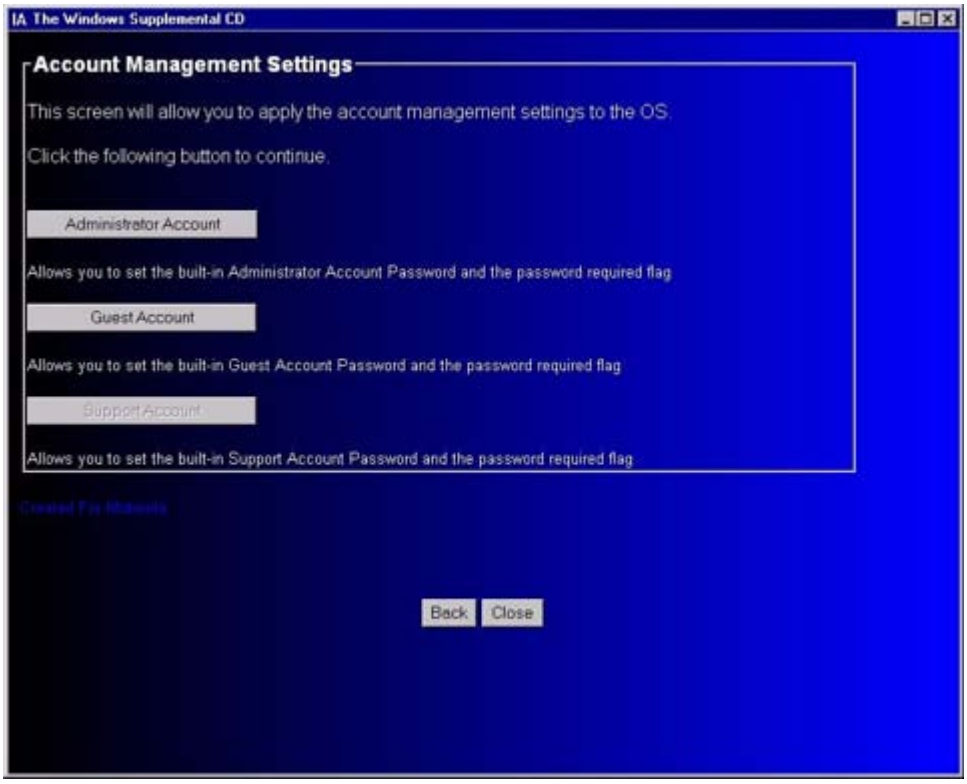
Ignore any error or warning messages that appear in the Command Prompt window.

7 Click **Close** to close the Windows Supplemental CD program

8 Reboot the computer now for the modified settings to take effect immediately or wait and reboot the computer after you have completed all procedures for all modified settings to take effect at the same time.

APPLYING ACCOUNT MANAGEMENT SETTINGS

FIGURE 2-3 WINDOWS SUPPLEMENTAL CD ACCOUNT MANAGEMENT SETTINGS SCREEN



MANAGING BUILT-IN ACCOUNTS

PROCEDURE 2-3 HOW TO APPLY BUILT-IN ACCOUNT MANAGEMENT SETTINGS

1	Log on as a valid administrator.
2	Insert the Windows Supplemental CD into the DVD/CD drive.
3	Navigate to the \bin folder of the Windows Supplemental CD and double-click the application file **Windows_Supplemental_GUI.exe**.

NOTE

The **User Account Control** dialog box might appear. Click **Allow** or log on with the administrator password, depending on the prompt command.

Result: The Windows Command Prompt window briefly opens and closes, then the Windows Supplemental CD screen appears, as in Figure 2-1, “Windows Supplemental CD Main Screen,” on page 2-2.

Procedure 2-3 How to Apply Built-in Account Management Settings (continued)

4	Click the **Account Management** button on the left side of the screen. **Result:** The Account Management screen appears as in Figure 2-3.

5	Click the **Administrator Account** button.
	Result: A Windows Command Prompt window opens displaying the following message:
	`Please provide a password for the built-in Administrator Account:`
	`Type a password for the user.`

6	Type a password for the built-in administrator account and press ENTER. **Result:** The following message appears in the Command Prompt window: `Retype the password to confirm.`

7	Retype the password and press ENTER.
	Result: If the new password is accepted, the following message appears in the Command Prompt window:
	`The command completed successfully.`
	`If you were not successful, please re-run this script Press any key to continue.`

8	Press any key. (If the command did not complete successfully, exit and restart this procedure at step .3.) **Result:** The Command Prompt window closes and the following message appears: `Account management script has completed, follow instructions from command line.`
9	Click **OK**.

10	Click the **Guest Account** button.
	Result: A Windows Command Prompt window opens displaying the following message:
	`Please provide a password for the built-in Guest Account:`
	`Type a password for the user.`

11	Type a password for the built-in guest account and press ENTER. **Result:** The following message appears in the Command Prompt window: `Retype the password to confirm.`

PROCEDURE 2-3 HOW TO APPLY BUILT-IN ACCOUNT MANAGEMENT SETTINGS (CONTINUED)

12	Retype the password and press ENTER.
	Result: If the new password is accepted, the following message appears in the Command Prompt window:
	`The command completed successfully.`
	`If you were not successful, please re-run this script Press any key to continue.`

13	Press any key. (If the command did not complete successfully, exit and restart this procedure at step .3, then skip from step 4 to step 10.) **Result:** The Command Prompt window closes and the following message appears: `Account management script has completed, follow instructions from command line.`
14	Click **OK**.
15	Click **Close** to close the Windows Supplemental CD program
16	Reboot the computer now for the modified settings to take effect immediately. If this is the last procedure, reboot the computer now.

CHAPTER 3

OPTIONAL SYSTEM CONFIGURATION

This section contains common procedures for customizing system capabilities to the customers specifications

CHANGING LOGIN BANNERS

All Motorola systems ship with default login banners. Follow Procedure 3-1 to change login banners.

Refer to Microsoft documentation for further detailed instructions.

CHANGE LOGIN BANNERS LOCALLY

Repeat Procedure 3-1 for each computer in your MIP 5000 system.

PROCEDURE 3-1 HOW TO CHANGE LOGIN BANNERS LOCALLY

1	Log on as a valid administrator.
2	Select **Start > Settings > Control Panel** or **Start > Control Panel**.
3	Double-click **Administrative Tools**. **Result:** The Administrative Tools window opens.
4	Double-click **Local Security Policy**. Click **Continue**. **Result:** The Local Security Policy window opens.
5	Expand **Local Polices** and select **Security Options**. **Result:** The right pane displays security options for local policies.
6	In the right pane, select **Interactive logon: Message title for users attempting to log on**.

PROCEDURE 3-1 HOW TO CHANGE LOGIN BANNERS LOCALLY (CONTINUED)

7	Right-click and select **Properties**. **Result:** A **Properties** dialog box for this property appears.
8	In the tab **Local Security Setting** change the title of the current banner.
9	Click **OK**. **Result:** The **Properties** dialog box for this property closes and the title of the current banner is changed. If the security setting for this policy was previous undefined, it is now defined.
10	In the right pane, select **Interactive logon: Message text for users attempting to log on**.
11	Right-click and select **Properties**. **Result:** A **Properties** dialog box for this property appears.
12	In the Tab **Local Policy Setting** change the existing text banner.
13	Click **OK**. **Result:** The **Properties** dialog box for this property closes and the text of the current banner is changed. If the security setting for this policy was previous undefined, it is now defined.
14	Close all open windows.
15	Log off.

APPENDIX
A

PRODUCT EXCEPTIONS

This appendix identifies known security deficiencies the MIP 5000 VoIP Radio Console product.

PATCHES FOR THE OPERATING SYSTEM

It could compromise security to connect a secure production computer directly to the Internet. Instead, Motorola recommends acquiring a non-production computer for use in downloading Windows operating system updates. We will refer to this as the *OS Patch computer*.

The OS Patch computer should meet the following requirements:

- If your system uses more than one operating system, a separate OS Patch computer is required for each version of Windows.
- Each OS Patch computer should have had the same OS updates applied as the secure production computers.
- Each OS Patch computer must have Automatic Updates turned off. This prevents updates from being downloaded until you explicitly ask for them.
- Each OS Patch computer should be the same make and model as the secure production computers.
- Each OS Patch computer should have all the same application software installed as the secure production computers. You can install both the PC Console and the CSDM application software on a single computer for this purpose.
- Each OS Patch computer must be connected to the Internet.
- The Windows Supplemental Configuration CD should ***not*** be applied to the OS Patch computer(s).

It is recommended that you review the monthly Microsoft Security Update bulletins (http://www.microsoft.com/security/updates/bulletins/default.aspx) to see which updates apply to the computers in your MIP 5000 system. You should then use the OS Patch computer(s) to select and download the appropriate updates.

The following procedure is intended as a high-level guide for finding, downloading, and installing operating system updates in a secure MIP 5000 installation. It should be used only by experienced, qualified system administrators.

PROCEDURE A-1 HOW TO FIND AND APPLY OS UPDATES SECURELY

1	Use **Windows Update** on the OS Patch computer to find and select the appropriate updates.
2	Select updates identified as *Critical* and *Important*, except those for Internet Explorer 8 (IE8).
3	Download the selected updates onto the OS Patch computer from the Microsoft Update Catalog site (http://catalog.update.microsoft.com/v7/site/Home.aspx).
4	Copy the selected updates to removable media.
5	Apply the selected updates to the secure production computers from the removable media.

BACK UP AND RESTORE MIP 5000

Procedures for backing up MIP 5000 data and configuration files and for restoring them and the MIP 5000 application program files are described in Appendix C, "Upgrade and Recovery Procedures" of the *MIP 5000 VoIP Radio Console Installation and Configuration Manual* (6881013Y35).

Also, you can find information about backing up IRR recordings in the installation and operator manual of IRR.

ENFORCE SECURE PASSWORD USAGE

The MIP 5000 system uses internal passwords in two places:

- Within the MIP 5000 VoIP Radio Console program to gain access to supervisory features. The password is specified using the CSDM program

- Within the MIP 5000 gateway to gain access via secure shell (SSH) — using a default password that should be changed before connection to the network and that can then be maintained during SSH sessions using the Gateway Maintenance Menu

These passwords are not secure. Additional password security must be enforced manually by following these requirements:

- Password must not contain the user's first name, last name, or user name
- Password must not begin with a numeric character (the digits 0 through 9)
- Password must not match any of the previous four passwords used for this account
- Password must be at least eight characters long
- Password must have three of the following four characteristics:
  - At least one upper case letter (A-Z)
  - At least one lower case letter (a-z)
  - At least one numeric character (0-9)
  - At least one of the following symbols:
    - Hyphen (-)
    - Underscore (_)
    - Dollar sign ($)
    - Number sign (#) (also known as pound or hash sign)

The following sample passwords meet these requirements:

- G00d$ense
- F_NnYPa$$w0rd

THIS PAGE INTENTIONALLY LEFT BLANK.

INDEX

R

S

W

2215234G-02