System Release 7.17
ASTRO® 25
INTEGRATED VOICE AND DATA

# Windows Supplemental Configuration Setup Guide

AUGUST 2017

MN003380A01-B

# Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.



No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Furthermore, the purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

## Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a particular system, or may be dependent upon the characteristics of a particular mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

## Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

## European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive

The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

This page intentionally left blank.

# Contact Us

## Motorola Solutions Support Center

The Solutions Support Center (SSC) is the primary Motorola Solutions support contact. Call:

- Before any software reload.
- To confirm troubleshooting results and analysis before removing and replacing a Field Replaceable Unit (FRU) and Field Replaceable Entity (FRE) to repair the system.

| For... | Phone |
|---|---|
| United States Calls | **800-221-7144** |
| International Calls | **302-444-9800** |

## North America Parts Organization

For assistance in ordering replacement parts or identifying a part number, contact the Motorola Solutions Parts organization. Your first response when troubleshooting your system is to call the Motorola Solutions SSC.

| For... | Phone |
|---|---|
| Phone Orders | **800-422-4210** (US and Canada Orders)<br>For help identifying an item or part number, select choice 3 from the menu. |
| | **302-444-9842** (International Orders)<br>Includes help for identifying an item or part number and for translation as needed. |
| Fax Orders | **800-622-6210** (US and Canada Orders) |

## Comments

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Provide the following information when reporting a documentation error:

- The document title and part number
- The page number with the error
- A description of the error

We welcome your feedback on this and other Motorola Solutions manuals. To take a short, confidential survey on Motorola Solutions Customer Documentation, go to docsurvey.motorolasolutions.com or scan the following QR code with your mobile device to access the survey.

This page intentionally left blank.

# Document History

| Version | Description | Date |
|---|---|---|
| MN003380A01-A | Original release of the *Windows Supplemental Configuration Setup Guide* manual | November 2016 |
| MN003380A01-B | Updated Joining and Rejoining a Windows-Based Device to an Active Directory Domain on page 33 with information on backward compatibility. | August 2017 |

This page intentionally left blank.

# Contents

# List of Figures

This page intentionally left blank.

# List of Tables

This page intentionally left blank.

# List of Processes

This page intentionally left blank.

# List of Procedures

This page intentionally left blank.

# About Windows Supplemental Configuration Setup Guide

This manual supplements the ASTRO® 25 system documentation set with additional procedures for Microsoft Windows-based devices in an ASTRO® 25 system.

This includes procedures that must be performed on all Windows-based devices in an ASTRO® 25 system, and additional procedures that are performed only for specific Windows-based devices in an ASTRO® 25 system.

## What Is Covered In This Manual?

This manual contains the following chapters:

- Windows Supplemental Configuration Overview on page 21 contains assumptions and caveats for supplemental Windows configuration procedures in this manual. It also lists the contents of the ASTRO® 25 system *Windows Supplemental* media and provides a procedure for installing specific *Windows Supplemental* media files using a Windows Install Framework application.
- Common Windows Procedures on page 33 contains common supplemental configuration procedures for Windows-based devices in ASTRO® 25 systems.
- Remote Desktop Installation and Configuration on page 47 provides remote desktop configuration information and procedures for Windows-based devices in ASTRO® 25 systems.
- Windows Supplemental Configuration Troubleshooting on page 51 provides a way to determine types of ASTRO® 25 system supplemental configuration settings applied to specific Windows-based devices.

## Helpful Background Information

Motorola Solutions offers various courses designed to assist in learning about the system.

For information, go to http://www.motorolasolutions.com/training.

## Related Information

See the following documents for associated information about the radio system:

| Related Information | Purpose |
|---|---|
| *Standards and Guidelines for Communication Sites* (6881089E50) | Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. Also known as R56 manual.<br>This document may be purchased by calling the North America Parts Organization at 800-422-4210 (or the international number 302-444-9842). |
| *System Overview and Documentation* | Provides an overview of the ASTRO® 25 new system features, documentation set, technical illustrations, and system-level disaster recovery that support the ASTRO® 25 radio communication system. |
| *Virtual Management Server Software* | Provides procedures for implementing and managing VMware ESXi-based virtual server hosts on the common Hewlett-Packard hardware platform in ASTRO® 25 systems. |

This page intentionally left blank.

Chapter 1

# Windows Supplemental Configuration Overview

This chapter contains assumptions and caveats for supplemental Windows configuration procedures in this manual. It also lists the contents of the *Windows Supplemental* media.

## 1.1 Windows Supplemental Configuration Assumptions and Caveats

This document assumes the following:

- The operating system has been installed and correctly configured.
- All the correct operating system patches have been applied and correctly configured.
- All necessary domains have been **Trusted** according to the installation requirements.
- All the product applications have been installed and correctly configured.

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

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

Removing a Windows-based device from a domain, when the Domain Controller is not available, may result in a permanently undesirable state that will require a reinstallation of the operating system. Always make sure that the Domain Controller is operating and authenticate the removal from the domain at the Domain Controller.

## 1.2 Windows Supplemental Configuration Post-Configuration Caveats

To successfully complete Windows supplemental configuration procedures, you must perform all the procedures when logged in as a valid domain or local Windows administrator (except where otherwise stated).

When you perform administrative tasks on Windows operating systems, a **User Account Control (UAC)** dialog box might prompt you to click **Continue**, **Allow**, or **Yes**, or it may prompt you to provide domain or local Windows administrator credentials.

After applying 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 procedures are applied, passwords for existing user accounts will continue to work. However, password complexity requirements are enforced when the existing passwords are changed. See Windows Password Length and Complexity Requirements on page 22.

### 1.2.1
## Windows Password Length and Complexity Requirements

Windows passwords must meet the following minimum requirements when they are changed or created:

**Password Length**

Depending on the policies of your organization, the minimum password length requirement for Windows-based devices is either 8 or 14 characters. For information on which requirement applies to your device, see Viewing Minimum Password Length on Windows-Based Devices on page 22.

**Password Complexity**

Passwords must not contain the entire samAccountName (Account Name) value of a user or the entire displayName (Full Name) value. Both checks are not case sensitive:

- The samAccountName is checked in its entirety only to determine whether it is part of the password. If the samAccountName is less than three characters long, this check is skipped.
- The displayName is parsed for delimiters: commas, periods, dashes or hyphens, underscores, spaces, pound signs, and tabs. If any of these delimiters are found, the displayName is split and all parsed sections (tokens) are confirmed not to be included in the password.

  Tokens that are less than three characters in length are ignored, and substrings of the tokens are not checked. For example, the name “Erin M. Hagens” is split into three tokens: “Erin,“ “M, “ and “Hagens.“ Because the second token is only one character long, it is ignored. Therefore, this user could not have a password that included either “erin“ or “hagens“ as a substring anywhere in the password.

Passwords must contain characters from three of the following five categories:

- Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
- Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
- Base 10 digits (0 through 9)
- Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

### 1.2.2
## Viewing Minimum Password Length on Windows-Based Devices

Perform this procedure to view minimum password length for the Windows-based device you are currently logged on to using the Resultant Set of Policy (RSoP) query.

**Procedure:**

1. From **Start**, in the search field, enter: `rsop.msc`
2. In the left pane of the **Resultant Set of Policy** window, expand **Computer Configuration** → **Windows Settings** → **Security Settings** → **Account Policies** → **Password Policy**.

   In the right pane, the computer setting for the **Minimum password length** displays the minimum length allowed for domain and local account passwords.

1.3

# Windows Supplemental Media Contents

The following table lists components located on the *Windows Supplemental* media provided by Motorola Solutions with the ASTRO® 25 system. Many of these files are part of initial installation on supported ASTRO® 25 system devices. For example, OpenSSL and Embedded Password Management are part of Private Network Management (PNM) Client initial installation.

Components installed optionally are listed in Optional Components Located on the Windows Supplemental Media on page 30.

For installation instructions, see Installing Components Located on the Windows Supplemental Media on page 28.

Table 1: Windows Supplemental Media Contents

| Component Name | Component Description | Component Filename |
|---|---|---|
| Motorola Windows **Backup and Restore (BAR) Client** for ASTRO® 25 system BAR services | See Optional Components Located on the Windows Supplemental Media on page 30. | `Motorola Windows Bar Client.xml` |
| Motorola Windows **Event Logging Client** for the ASTRO® 25 system Centralized Event Logging service | See Optional Components Located on the Windows Supplemental Media on page 30. | `Motorola Windows Logging Client.xml` |
| **PuTTY version customized by Motorola** | Utility certified for initiating interactive sessions in Secure SHell (SSH) or other protocols.<br>The utility and the *PuTTY User Manual* are available by navigating to the list of programs on your computer, and selecting **Motorola** → **Motorola PuTTY**. The `.msi` package is customized by Motorola Solutions.<br>For detailed information, see the *Securing Protocols with SSH* manual. | `Motorola PuTTY.xml` |
| **WinSCP** | Can be used to drag and drop files between a Windows-based device and an FTP server.<br>See "Transferring Files to or from the BAR Server" in the *Backup and Restore Services* manual.<br>For detailed information, see www.winscp.net. | `Motorola WinSCP.xml` |
| **OpenSSL** | A toolkit implementing the Secure Sockets Layer, Transport Layer Security, and general purpose cryptography library.<br>For detailed information, see www.openssl.org. | `Motorola OpenSSL.xml` |

*Table continued…*

| Component Name | Component Description | Component Filename |
|---|---|---|
| **OpenSSL x64** | A toolkit implementing the Secure Sockets Layer, Transport Layer Security, and general purpose cryptography library on a Windows 64-bit system.<br>For detailed information, see www.openssl.org. | `Motorola OpenSSL x64.xml` |
| **Motorola Certificate Generation and Deployment (CGD)** | A tool that creates and distributes Motorola Solutions default certificates for target windows devices to authenticate with the installed Trusted Root Certificate. | `Motorola Certificate Generation Deployment Tool.xml` |
| **Motorola CA Certs (MOT_CACerts)** | An `.msi` package installing public root certificates for SSC and ASTRO® 25 systems. These are public certificates required by client devices to authenticate with different web services which are using Motorola Solutions certificates. | `Motorola MOT_CACerts.xml` |
| **SNMP Common Agent** configuration file folder | Used for advanced fault state management. Only use the files in the `\Motorola Common Agent\` folder if instructed to do so in the ASTRO® 25 system manual for the Windows-based device or in the *SNMPv3* manual.<br>SNMP-related procedures for individual devices are located in the ASTRO® 25 system manual for that device.<br>For detailed information on how to install the Common Agent, refer to the *SNMPv3* manual. | `Motorola Common Agent.xml`<br>`Motorola Common Agent Configuration.xml` |
| **SNMPv3 passphrase configuration utility (SNMPv3 Credential GUI)** | Used by SNMP Common Agent to reset credentials. For detailed information, see the *SNMPv3* manual. | `Motorola SNMPv3-Credentials-WSUI.xml` |
| **Motorola Initial SNMPv3 Credentials Extractor Application** | Used for setting initial SNMPv3 credentials securely. | `Motorola Initial SNMPv3 Credential Extractor Application.xml` |
| **Motorola Initial SNMPv3 Credentials Extractor Default Configuration** | Default configuration for MISCE Application. Contains default passphrases for the MotoAdmin SNMPv3 user. | `Motorola Initial SNMPv3 Credential Extractor Default Configuration.xml` |
| **Common Licensing Layer** | Used for installing the Dynamic Link Library (DLL) of licenses for the License Manager. See the *License Manager* manual. | `Motorola Common Licensing Layer.xml` |

*Table continued…*

| Component Name | Component Description | Component Filename |
|---|---|---|
| **Common Licensing Layer x64** | Used for installing the Dynamic Link Library (DLL) of licenses for the License Manager on a Windows 64-bit system. See the *License Manager* manual. | `Motorola Common Licensing Layer x64.xml` |
| **Motorola VM Automation Tools** | See Optional Components Located on the Windows Supplemental Media on page 30. | `Motorola VM Automation Tools.xml` |
| **Motorola joinADomain** | Aplication for Windows devices to join the Active Directory (AD) domain. | `Motorola JoinADomain.xml` |
| **Group Policy Objects (GPOs)** | Contains Motorola Solutions-provided Group Policy Objects (GPOs), located under `\ActiveDirectory\`.<br>For detailed information, see the *Authentication Services* manual. | |
| **Motorola Windows Security Configurations** | One of the following directories, depending on your organization's policies:<br>• `\Motorola Windows Supplemental Fullconfig\bin`<br>• `\Motorola Windows Supplemental Transconfig\bin`<br>See Common Windows Procedures on page 33. | |
| **Adobe Reader** | Application used to view files in the `.pdf` format.<br>You can also load Adobe Reader from the ASTRO® 25 system documentation media.<br>If you install Adobe Reader, see the `Readme.txt` file on the latest *MOTOPATCH for Windows 3PP CD* and install the patch if required by your organization. | `Motorola ASTRO Adobe Reader.xml` |
| **JRE 8 (Java Runtime Environment version 8)** | Allows your system to run Java applications and websites. | `Motorola ASTRO Java Family.xml` |
| **JRE 8 (Java Runtime Environment version 8) x64** | Allows your system to run Java applications and websites in a Windows 64-bit system. | `Motorola ASTRO Java Family x64.xml` |

*Table continued…*

| Component Name | Component Description | Component Filename |
|---|---|---|
| **OpenJDK** | Installs an open-source implementation of Java. For details, see http://openjdk.java.net/. | `Motorola OpenJDK.xml` |
| **Motorola Embedded Password Management** | Embedded Password Management is used to change embedded account passwords only on supported devices. See the “Embedded Password Management” appendix in the *Authentication Services* manual. | `Motorola Password Vault.xml` |
| **Motorola Embedded Password Management x64** | Embedded Password Management is used to change embedded account passwords only on supported devices in a Windows 64-bit system. See the “Embedded Password Management” appendix in the *Authentication Services* manual. | `Motorola Password Vault x64.xml` |
| **Motorola AAA API Package** | The AAA API provides a consistent interface to authenticate and retrieve authorization information from Active Directory. It also provides a mechanism for authenticating a user if Kerberos is unavailable.<br>Applies to the following devices:<br>• MKM 7000 Console Alias Manager (CAM) server<br>• NM Client<br>• Console devices<br>• Software Download Manager<br>For detailed information, see the manual specific to that device. | `Motorola AAA API.xml` |
| **7-Zip** | Archiving software that can be used to compress and uncompress files. For details, see http://www.7-zip.org/. | `Motorola ASTRO 7-Zip.xml` |
| **Internet Explorer** | A Microsoft graphical web browser used to access information provided by web servers in ASTRO® 25 systems.<br>For details, see windows.microsoft.com/en-US/internet-explorer/internet-explorer-help. | `Internet Explorer.xml` |
| **Microsoft Windows Management Framework** | Makes updated management functionality available for installation on Windows. | `Microsoft Windows Management Framework.xml` |

*Table continued…*

| Component Name | Component Description | Component Filename |
|---|---|---|
| | For details, see http://www.microsoft.com. | |
| **Microsoft .NET** | A software framework for Windows. It provides language interoperability across several programming languages.<br>For details, see http://www.microsoft.com/net. | `Microsoft .NET Framework.xml` |

1.4
# Microsoft EMET

This section describes the Enhanced Mitigation Experience Toolkit (EMET) in the ASTRO® 25 system.

The purpose of Microsoft EMET is to prevent exploitation of software vulnerabilities through security mitigation technologies including:

- Address Space Layout Randomization (ASLR)
- Data Execution Prevention (DEP)
- Structured Exception Handler Overwrite Protection (SEHOP)

EMET mitigations in the ASTRO® 25 system apply to Windows 10 only.

Motorola Solutions requires EMET version 5.5 or later to be installed:

- During applying local supplemental configuration. See Applying Device-Specific Settings Using the Windows Supplemental Media on page 37.
- During supplemental configuration involving joining an Active Directory (AD) domain, after the device is joined to the domain. See Joining and Rejoining a Windows-Based Device to an Active Directory Domain on page 33.

EMET mitigations work at the Kernel level in the OS.

## ASLR

Address Space Layout Randomization (ASLR) prevents malware from assembling its malicious activity from (multiple and specific) memory locations assigned in system memory.

ASLR randomizes the addresses where modules are loaded to help prevent an attacker from leveraging data at predictable locations. It prevents attackers from taking advantage of predictable mappings of dlls using Return Oriented Programming (ROP).

## DEP

Data Execution Prevention (DEP) denies the execution of malicious code at the processor level.

DEP prevents an attacker's attempt to exploit a vulnerability by jumping to shellcode at a memory location where controlled data resides, on the heap or the stack, by marking these regions non-executable.

## SEHOP

Structured Exception Handler Overwrite Protection (SEHOP) prevents malware from overwriting entries in the structured event handler and execution of malicious code referenced by that entry (prevents Windows stack overflows).

1.5

# Installing Components Located on the Windows Supplemental Media

This procedure describes the scenarios for using the Windows Install Framework application and can be used to automatically and simultaneously install all the required common software components from the *Windows Supplemental* media, for one of the devices listed in Device Name Parameters on page 30, as well as any necessary cohabitation devices and optional components listed in Optional Components Located on the Windows Supplemental Media on page 30.

**Prerequisites:** Obtain the *Windows Supplemental* media.

**When and where to use:**
For example, some of the required common components for the NM Client are:

7-Zip
PuTTY
JoinADomain
OpenSSL
CGD
MOT_CACerts
Embedded Password Management
Adobe Reader
Oracle Java
AAA API
Common Licensing Layer

Using the following procedure, you can install them all without the necessity to reinsert the *Windows Supplemental* media.

Similarly, AuC Client can be installed as a device cohabitating on the same operating system as the NM Client and Centralized Event Logging client and Backup and Restore Client as optional components of the NM Client.

**IMPORTANT:** Installation of components located on the *Windows Supplemental* media is supported only in the pre-defined location and cannot be changed by the user.

**Procedure:**

1. If you are installing to a Windows-based device that is a virtual machine, connect the virtual machine to the DVD drive where you will insert the *Windows Supplemental* media for this procedure.

   See the *Virtual Management Server Software* manual for information about connecting DVD drives to virtual machines in an ASTRO® 25 system.

2. Log on to a Windows-based device with a local Windows administrator account.

   The account name set up by Motorola Solutions for Windows 7 and Windows 10-based devices is “secmoto”.

   For Windows Server 2012-based devices the account is “administrator” until you perform one of the following procedures and the account becomes “motosec”: Applying Device-Specific Settings Using the Windows Supplemental Media on page 37 or Joining and Rejoining a Windows-Based Device to an Active Directory Domain on page 33.

3. Insert the *Windows Supplemental* media into the CD/DVD drive.
4. From **Start**, open the Command Prompt.
5. At the Command Prompt, navigate to the `\wif` directory on the CD/DVD drive.

6 Depending on the component you need, execute the following command (consisting of one, two, or three parameters, separated with a space):
`WindowsInstallFramework.exe /e /i <device name>.xml <cohab device name>.xml <optional component>.xml`

Where:

***<device name>*** is only one of the parameters listed in Device Name Parameters on page 30

***<cohab device name>*** is the name of a device cohabitating on the same operating system, for example, AuC Client can cohabitate with NM Client

***<optional component>*** is one or more of the components, separated with a space, listed in Optional Components Located on the Windows Supplemental Media on page 30.

**Step example:**
```
WindowsInstallFramework.exe /e /i NETWORK_MANAGEMENT_CLIENT.xml
AUTHENTICATION_CLIENT.xml "Motorola Windows Bar Client.xml" "Motorola
Windows Logging Client.xml"
```
For Windows, insert quotes around filenames that contain spaces.

7 When error `1638` appears for `Motorola ASTRO Adobe Reader\PreCheck.wsf`, click **Continue** to skip the installation of the component.

If further errors appear for other files in the same component, keep clicking **Continue** until the errors disappear.

Error `1638` means that the component's version installed is greater than the version provided on the *Windows Supplemental* media.

To verify what version of a component is installed on your computer, from **Start**, open **Control Panel**, and then **Uninstall a program** or **Programs and Features**, depending on your OS.

To verify what version of a component is installed on the *Windows Supplemental* media, see the `readme.txt` file on the DVD.

8 At the installation finished message, click **OK**.

9 If you installed these applications on a virtual machine and have no additional operations to perform for this virtual machine from the DVD drive, it is recommended that you disconnect the virtual machine from the DVD drive.

See the *Virtual Management Server Software* manual.

10 Before using any of the components that have been installed during this procedure, it is recommended that you reboot the device.

**Postrequisites:**

**IMPORTANT:**
If any of the components is missed during an installation, it can be additionally installed after performing this procedure. For example, to individually install one of the missing optional components, execute the following command:

`WindowsInstallFramework.exe /e /i <optional component>.xml`

### 1.5.1
## Device Name Parameters

The following table provides parameters only for devices that require installation of the common software through Installing Components Located on the Windows Supplemental Media on page 28.

Table 2: Device Name Parameters

| Device | *<device name>*.xml |
|---|---|
| Authentication Center (AuC) Client | AUTHENTICATION_CLIENT.xml |
| Authentication Center (AuC) Server | AUTHENTICATION_SERVER.xml |
| MKM 7000 Console Alias Manager (CAM) server | CAM_SERVER.xml |
| K core Client | K-CORE_PC_CLIENT.xml |
| Key Management Facility (KMF) Client | KMF_CLIENT.xml |
| Key Management Facility (KMF) Server | KMF_SERVER.xml |
| NM Client | NETWORK_MANAGEMENT_CLIENT.xml |
| Software Download Manager | SOFTWARE_DOWNLOAD_MANAGER.xml |
| Web-based Configuration Manager (CM) | WEBCM.xml |

### 1.5.2
## Optional Components Located on the Windows Supplemental Media

The following table lists all components located on the *Windows Supplemental* media which, if needed, can be installed as optional.

**NOTICE:** Installation of files located on the *Windows Supplemental* media is supported only in the pre-defined location and cannot be changed by the user.

Table 3: Optional Components Located on the Windows Supplemental Media

| Component Name | Component Description | Component Filename |
|---|---|---|
| **Backup and Restore (BAR) client application** | For Windows-based devices that use the full implementation of the ASTRO® 25 system BAR service (for feature details, see the *Backup and Restore Services* manual). | Motorola Windows Bar Client.xml |
| **Centralized Event Logging client application** | For Windows-based devices that use the ASTRO® 25 system Centralized Event Logging service (for feature details, see the *Centralized Event Logging* manual). | Motorola Windows Logging Client.xml |

*Table continued…*

| Component Name | Component Description | Component Filename |
|---|---|---|
| | **IMPORTANT:** You should install the BAR client and Logging client at the point indicated in the overall installation/configuration process in the manual for a Windows-based device in an ASTRO® 25 system. | |
| **Motorola VM Automation Tools** | Installation package used to configure virtual hardware specification of Common OS OVF and to set identity on it. | `Motorola VM Automation Tools.xml` |

This page intentionally left blank.

Chapter 2

# Common Windows Procedures

This chapter provides common supplemental procedures for Windows-based devices in an ASTRO® 25 system.

## 2.1 Boot Order for Windows Devices (Not for Virtual Machines)

For all Windows-based devices in an ASTRO®25 system that are **not** implemented as virtual machines, ensure that the boot order is set as follows:

1. Internal hard drives
2. Internal optical drives
3. External hard drives
4. External USB devices

The boot order and configuration for a PC is found in the PC's BIOS. Refer to the PC manufacturer's documentation for instructions on how to set the boot order correctly.

**NOTICE:** The boot order needs to be set once and then verified each time the operating system is installed. In an ASTRO® 25 system, the ESXi-based host for virtual machines does not support the use of USB drives.

## 2.2 Joining and Rejoining a Windows-Based Device to an Active Directory Domain

**Join domain**
The join domain operation automatically unjoins the device from any domain it may have been previously joined to.

**Windows-based device**
A Windows-based device is a platform running on a Windows OS for remote deployment and configuration of a virtual machine.

**JoinADomain application**
The application for joining a Windows client to the domain which automatically configures NTP, DNS, and OU for that client.

For backward compatible devices, use the version of JoinADomain from the *Windows Supplemental* media appropriate for the version of the system core you are using.

**IMPORTANT:** While rejoining a Windows-based device to an Active Directory Domain, do **not** use this application to move the Windows-based device from an Organization Unit (OU) to another OU.

**Prerequisites:**
Obtain from your system administrator the Organizational Unit for this Windows-based device, as well as the user name and password for the account that is used to join this Windows-based device to the Active Directory domain.

For a list of Windows-based devices, see “Active Directory Client Devices and Applications” in the *Authentication Services* manual.

If the Windows-based device is a virtual machine, before performing this procedure, make sure that the virtual machine is connected to the DVD drive where you will insert the software media. For information about connecting DVD drives to virtual machines in ASTRO® 25 systems, see the *Virtual Management Server Software* manual.

**Procedure:**

1. If a Windows logon dialog box appears, enter the credentials for a Windows user account that is maintained locally on this Windows-based device.

   If you are logging on with a local account, and you need to perform operations requiring Windows administrator privileges, log on with a local Windows administrator account.

   Note that “motosec” is the local Windows administrator account set up by Motorola Solutions supplemental configuration for devices operating on Windows Server 2012; “secmoto” is the Windows administrator account set up by Motorola Solutions for Windows 7 and Windows 10-based devices.

   The administrator's desktop appears.

2. Insert the *Windows Supplemental* media in the drive.
3. Navigate to the `Motorola JoinADomain\OtherWindowsOS` folder on the *Windows Supplemental* media.
4. In the `Motorola JoinADomain\OtherWindowsOS` folder, double-click **JoinADomain.exe**.
5. Depending on the message displayed, perform the following actions:
   a. If a warning message appears stating that the application could not locate the AD domain, type in the ***<AD Domain Name>*** manually in the **AD Domain** field.

      See “User Input Requirements – Domain Controller Configuration” in the *Authentication Services* manual.

   b. If a command prompt opens along with the **Join Active Directory Domain** window, do not close the command prompt. It will close after the **Join Active Directory Domain** window is closed.

   c. If a **User Account Control** window appears, click **Allow**, **Yes**, or **Continue**, depending on the prompt, then fill in the required fields for the account displayed and click **Yes**.
6. When prompted, log on to the domain controller using your Active Directory account that is a member of the Domain Admins group.

   The default domain administrator account is “motosec”.

   **NOTICE:** If the **Organizational Unit** field does not update automatically, tab out of the password or **AD Domain Name** field or click the **Username** field.

   The **Organizational Unit** field is updated with the information entered.

7. Select the correct Organizational Unit (OU) for the Windows-based device from the drop-down list.

   The OU list reflects the information of the host type which could be either Client or Server. The corresponding prefixes identifying an OU name on the drop-down list are respectively **WinClient** or **WinServer** followed by the associated entity identifier and mentioned host types.

   **Step example:**

   - The OU for Network Management Clients is **WinClient Network Management Clients**
   - The OU for Core Security Management Server (CSMS) is **WinServ Security Management Servers**

8 **For cohabited applications:** select the OU of the primary device on which the cohabited application is placed.

**Step example:** When joining a Authentication Center (AuC) Client cohabited with Network Management Clients to the domain, from the drop-down list, select **WinClient Network Management Clients**.

9 Click **Join**.

If a message window appears stating that Windows Firewall has blocked some features of the program, click **Allow Access**.

A message states that the Windows-based device has been successfully joined to AD in the INFO text area.

**NOTICE:** If an error message appears, repeat the procedure. If the error persists, contact the Motorola Solutions Support Center (SSC).

10 In the reboot window, click **Yes**.

**Postrequisites:**
If the device has problems joining the domain:

- Ensure the time is synchronized between the client and the AD/DNS.
- Verify the DNS server in the TCP/IP properties of the Network Interface Card (NIC) is set to the correct DNS Server IP.
- Verify the Network Connectivity is up and domain controllers are reachable.

**NOTICE:** After a device joins the domain, its applications that have Role Based Access Control in Active Directory may not be usable by the local Windows administrator or the domain administrator if that user account is not a member of the group associated with the application for that device.
In some cases, the administrator can access the application by entering its executable path and filename at the elevated Windows command line. The path and filename can be seen in the properties for the application shortcut on the desktop or the **Start** menu. For information how to run the elevated Windows command line, see “Starting the Windows Command Line as Administrator” in the *Authentication Services* manual.

**NOTICE:** For Voice Card and Crypto Card-based consoles, after joining the device to the domain and rebooting the console, run `GPUpdate` or force it from a Windows command prompt.

## 2.3 Configuration Using the ASTRO 25 System Windows Supplemental Media User Interface

Applying Device-Specific Settings Using the Windows Supplemental Media on page 37 is **not** mandatory for Windows-based devices that are joined to the ASTRO® 25 domain, or in cases where your organization has requested that local security be applied to all devices.

Managing Local Windows Accounts Using the Windows Supplemental Media on page 39 is not required but can optionally be used to change passwords of specific local Windows accounts.

**IMPORTANT:** Perform these procedures on devices that have local security applied whenever any software (including the operating system) is installed or upgraded on any Windows-based device in an ASTRO® 25 system.
After you perform Applying Device-Specific Settings Using the Windows Supplemental Media on page 37, if your organization requires its own modifications to local Group Policy User Configuration settings on this Windows-based device, your organization's settings will need to be reconfigured (for example, modifying the secure Screen Saver settings). Refer to Microsoft documentation for details about how to modify local Group Policy User Configuration settings using `gpedit.msc`.

### 2.3.1
## Devices Supported by the ASTRO 25 System Windows Supplemental Media

Windows-based devices are supported by the ASTRO® 25 system *Windows Supplemental* media. Various combinations of these devices are also supported for cohabitation on the same physical device. When you perform Applying Device-Specific Settings Using the Windows Supplemental Media on page 37, the drop-down list on the **Device Specific Settings** window provides a way for you to select from a list that includes the devices below, and also the supported cohabitation combinations of devices.

The following devices are supported by the ASTRO® 25 system *Windows Supplemental* media:

- Authentication Center (AuC) Client
- Authentication Center (AuC) Server
- Configuration Manager*
- Core Security Management Server (CSMS)
- Dynamic Transcoder
- InfoVista Server
- IP PBX Server (Telephony server)
- K core Client
- KMF Client
- KMF Server
- MCC 7100 IP Dispatch Console
- MCC 7500 Dispatch Console and AIS
- MCN (CTI) Server 8000 (Remote Comparator Display Software for Motorola IP Comparators)
- MCN (CTI) Client
- MKM 7000 Console Alias Manager (CAM) server
- Logging Recorder
- Replay Station
- NM Client
- PRX 7000 Console Proxy
- Software Download Manager

* For the Configuration Manager, depending on your organization’s policies:

- If the *Windows Supplemental* media provided with your ASTRO® 25 system contains `\Motorola Windows Supplemental Fullconfig\bin\`, do **not** perform Applying Device-Specific Settings Using the Windows Supplemental Media on page 37.

- If the *Windows Supplemental* media provided with your ASTRO® 25 system contains `\Motorola Windows Supplemental Transconfig\bin\`, perform Applying Device-Specific Settings Using the Windows Supplemental Media on page 37.

**NOTICE:** If a device or application is not listed in this section, refer to the product's documentation for supplemental configuration instructions.

### 2.3.2
## Using the ASTRO 25 System Windows Supplemental Media User Interface

In cases where your organization has requested that local security be applied to all devices, the following process is **not** mandatory for Windows-based devices that are joined to the ASTRO® 25 domain.

**Prerequisites:** Obtain the *Windows Supplemental* media provided by Motorola Solutions for your system.

**Process:**

1. If you are applying this process to a Windows-based device that is implemented as a virtual machine, you first need to connect the virtual machine to the DVD drive where you will insert the *Windows Supplemental* media.

   See the *Virtual Management Server Software* manual for information about connecting DVD drives to virtual machines in an ASTRO® 25 system.

2. Perform Applying Device-Specific Settings Using the Windows Supplemental Media on page 37.

   **IMPORTANT:** The Device-Specific Settings procedure changes password criteria for the Windows accounts. For Windows Server 2012, it changes the local Windows administrator account name to "motosec".

3. Optional: Set up new passwords for the applicable Windows accounts.

   See Managing Local Windows Accounts Using the Windows Supplemental Media on page 39.

4. Reboot the device.

5. If you applied settings to a Windows-based device that is a virtual machine and have no additional operations to perform for this virtual machine from the DVD drive, it is recommended that you disconnect the virtual machine from the DVD drive.

   See the *Virtual Management Server Software* manual.

### 2.3.3
## Applying Device-Specific Settings Using the Windows Supplemental Media

Perform this procedure to apply supplemental configuration settings for a specific Windows-based device in the ASTRO® 25 system, whenever any software (including the operating system) is installed or upgraded on any Windows-based device in the ASTRO® 25 system.

In cases where your organization has requested that local security is applied to all devices, the following procedure is **not** mandatory for Windows-based devices that are joined to the ASTRO® 25 domain.

**NOTICE:** Performing this procedure on Windows 10 automatically installs EMET. See Microsoft EMET on page 27.

**Prerequisites:** See Windows Supplemental Configuration Troubleshooting on page 51 for viewing summary information about the types of settings applied.

**Procedure:**

1. Log in to the Windows-based device using a valid domain account or local Windows "administrator" account.
2. Insert the *Windows Supplemental* media into the DVD drive.

   If you are applying this procedure to a Windows-based device that is implemented as a virtual machine, you must first connect the virtual machine to the DVD drive where you insert the *Windows Supplemental* media. See the *Virtual Management Server Software* manual for information about connecting DVD drives to virtual machines in an ASTRO® 25 system.
3. Navigate to one of the following folders:
   - `Motorola Windows Supplemental Fullconfig\bin\`
   - `Motorola Windows Supplemental Transconfig\bin\`

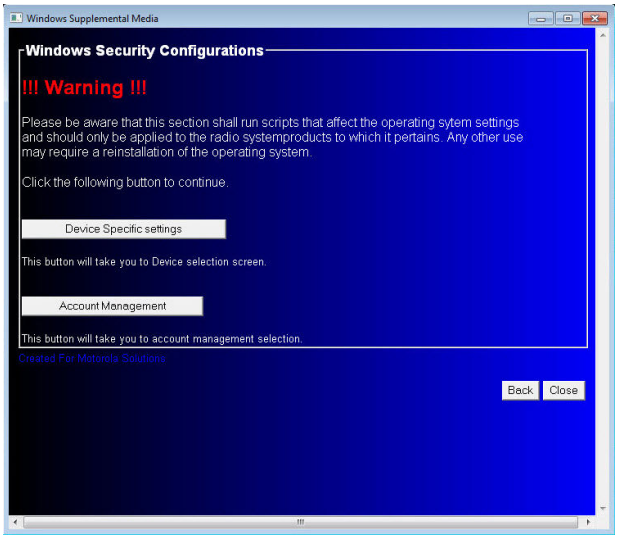
   Depending on the policies of your organization, your *Windows Supplemental* media contains either the `Fullconfig` or the `Transconfig` folder.
4. Double-click **Windows_Supplemental_GUI.exe**.

   If the **User Account Control** dialog box appears, click **Continue**, or type the administrator password for the account displayed then click **Yes**, depending on the prompt you see.

   **IMPORTANT:** Wait until the **Windows Supplemental Media** window appears. It may take up to 3 minutes for this window to appear.

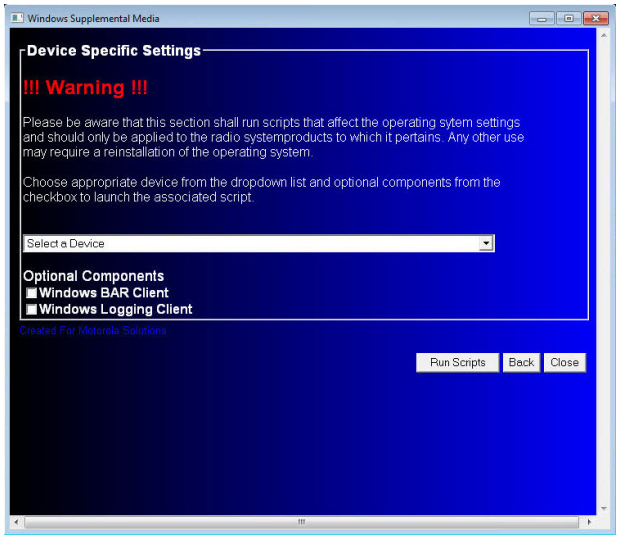
   The command prompt quickly opens and closes, then the **Windows Supplemental Media** window appears.
5. Click **Windows Security Configurations**.
6. On the **Windows Security Configurations** screen, click **Device Specific Settings**.

   **Figure 1: Windows Supplemental Media – Windows Security Configurations Screen**




7. On the **Device Specific Settings** screen, from the drop-down list, select the appropriate device supported by the operating system on the Windows-based device you are currently using.

**Figure 2: Windows Supplemental Media – Device Specific Settings Screen**




8 On the **Device Specific Settings** screen, select the check box for either one or both optional components that apply to this device:

- **Windows BAR Client**
- **Windows Logging Client**

If you are unsure which options apply to this device, contact your system administrator and see:
Windows-based Event Logging client procedures in the *Centralized Event Logging* manual.
Windows-based BAR client procedures in the *Backup and Restore Services* manual.

9 Click **Run Scripts**.

10 On the prompt, click **OK**.

The command prompt window displays messages as all the device-specific settings for this device type are applied. Then a list of all the settings applied displays on the screen.

11 Click **OK**.

12 Optional: If you want to proceed to Managing Local Windows Accounts Using the Windows Supplemental Media on page 39, leave the *Windows Supplemental* media in the drive of the Windows-based device and do not close the *Windows Supplemental* media user interface.

**Postrequisites:** Reboot the Windows device in order for the settings changed by the Windows Supplemental Configuration to become effective.

### 2.3.4
## Managing Local Windows Accounts Using the Windows Supplemental Media

**This procedure is optional.** Perform this procedure to change passwords of specific local Windows accounts whenever any software (including the operating system) is installed or upgraded on an ASTRO® 25 system Windows-based device.

**Prerequisites:** See Applying Device-Specific Settings Using the Windows Supplemental Media on page 37.

**Procedure:**

1 In the **Windows Supplemental Media** window, on the **Windows Security Configurations** screen, click **Account Management**.

2 In the **Account Management Settings** window, click **Administrator Account**.

3 At the prompt, enter the password for the administrator account.

4 At the prompt, re-enter the password.

5 **NOTICE:** Ensure that the preceding steps were successful by reviewing the command prompt message.

Press any key.

The command prompt window closes and the completed message appears.

6 Click **OK**.

7 In the **Account Management Settings** window, click **Guest Account**. Repeat step 3 through step 6.

8 Reboot the device.

Security settings take effect.

## 2.4 Deploying McAfee Anti-Malware From the CSMS

Deployment of McAfee Anti-Malware from the CSMS is required in order to configure each anti-malware client with the unique hostname for the CSMS, which hosts the McAfee Anti-Malware server.

For more information, see the *Core Security Management Server* manual.

### 2.4.1 Deploying the McAfee Client Software to Anti-Malware Clients in RNI

Deploy the McAfee ePO Client Software from the Core Security Management Server (CSMS) to one or more ASTRO® 25 system radio network infrastructure (RNI) Windows, Linux RHEL6 or RHEL7 devices in an ASTRO® 25 system using the Deployment Automation tool developed by Motorola Solutions. This tool provides the option of pushing agent and its component to a single IP or to a list of IP addresses that are passed as text file.

If this procedure fails on a Multi-Homed client, perform Deploying VSE to a Multi-Homed Client Device on page 42.

**Prerequisites:**

**IMPORTANT:** Before you deploy the McAfee VirusScan Enterprise (VSE) product on the device, see the product manual to confirm that McAfee VSE is supported by the given device or application. Deploying McAfee to a non-supported product may have unintended consequences.

Join:

- The Active Directory domain for any RNI Windows device to which the McAfee client software will be deployed.
- CSMS to the Active Directory domain.

Ensure that CSMS has access to the RNI Windows device on the network.

McAfee Client Software can be pushed only to a single operating system at a time. For example, when you provide a list of IP addresses, you can only provide IP addresses for Windows devices, RHEL 6 or RHEL7 devices. You cannot have a mix of Windows and RHEL IPs passed as an input to the deployment tool. Therefore:

- Obtain from your system administrator the IP address of each Windows and Linux devices to which the McAfee ePO client software will be deployed.

- Create separate `.txt` files for each operating system.

  Each `.txt` file contains only a single IP address on each line and in the standard ***<AAA.BBB.CCC.DDD>*** format.

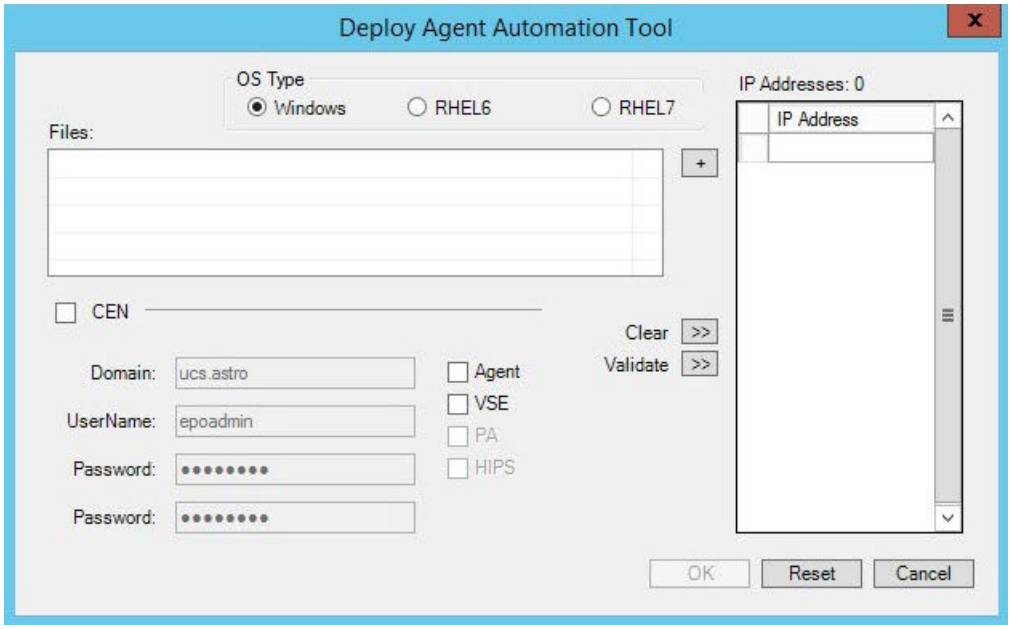
**NOTICE:** Push McAfee Client Software to devices which are multihomed (Multiple NICs\IP addresses) using the primary IP address assigned to the device.

**Procedure:**

1. Log on to the CSMS using a domain account belonging to the secadm or domain admin group.
2. In the desktop that appears, double-click the **Deploy_McAfee_Agent** icon.

   If the **User Access Control** dialog window appears, click **Continue** or type the administrator password for the account that appears and click **Yes**, depending on the prompt that appears.
3. In the **OS Type** section of the **Deploy Agent Automation Tool** window, select the appropriate OS type to indicate the client OS that you want to push the software to.

   **Figure 3: The Deploy Agent Automation Tool Window**




4. Select the **Agent** and **VSE** check boxes.

   **NOTICE:** If you want to install VirusScan Enterprise (VSE) when the VSE deployment fails, select only the **VSE** check box.
5. Perform one of the following actions:

| If… | Then… |
|---|---|
| **You want to deploy the software to a single device (Windows, RHEL 6, RHEL7),** | Enter a single IP address in the **IP Address** text box. |
| **You want to deploy the software to a list of devices (Windows, RHEL6, RHEL7)** | Perform the following actions:<br>**a** Click the plus (+) icon next to the **IP Addresses** text box.<br>**b** Browse to the appropriate text file with IP addresses of the devices. |

| If… | Then… |
|---|---|
| | **c** Click **OK**. |

IP addresses from the text file appear in the **IP Addresses** text box.

6 Click **OK**.

The **PowerShell** window displays the deployment status.

7 If the system fails, verify the reasons for failure, resolve the issues, and repeat the steps.

The **Agent Report** window appears when all systems and tasks complete.

### 2.4.2
## Deploying VSE to a Multi-Homed Client Device

Perform this procedure to deploy the McAfee VirusScan Enterprise (VSE) if Deploying the McAfee Client Software to Anti-Malware Clients in RNI on page 40 fails.

**Procedure:**

1 Log on to the CSMS as an administrator.

2 On the desktop, double-click **Launch McAfee ePolicy Orchestrator *<x.x.x>* Console**

where ***<x.x.x>*** is the version number

3 Log on to the McAfee ePolicy Orchestrator Console with the global administrator account.

See “McAfee ePolicy Orchestrator – Admin Accounts” in the *Core Security Management Server* manual.

4 On the toolbar, click **Menu**.

5 From the **Systems Section** area, select **System Tree**.

6 Select the **Systems** tab.

7 From the drop-down list in the **Preset** field, select **This Group and All Subgroups**.

8 Scroll down to navigate to the appropriate managed system. Select the check box with the appropriate system.

9 Select **Actions** → **Tags** → **Apply Tag**.

10 From the drop-down list, select one of the following options. Click **OK**.

- If the client OS is RHEL: **MSI_deploy_VSE_to_RHEL7**
- If the client OS is Windows: **MSI_deploy_VSE_to_Windows**

11 Scroll down to navigate to the appropriate managed system. Select the check box with the system selected in step 8.

12 Select **Actions** → **Agent** → **Wake Up Agents**.

13 In the **Force policy update** section, from the **Wake Up McAfee Agent** window, select **Force complete policy and task update**. Click **OK**.

The Agent wakes up in the next several seconds and deploys VSE on the tagged client.

14 Select **Actions** → **Tags** → **Clear Tag**.

15 From the drop-down list, select the option from step 10. Click **OK**.

## 2.5 Changing Logon Banners

The procedures in this section can be used to change a default logon banner to one specifically suited for your organization.

Perform Changing Logon Banners Locally on page 43 for any devices that are not joined to the domain.

Perform Changing Logon Banners Through a Domain Controller on page 44, then Changing Logon Banners Locally on page 43 for any devices that are joined to the domain.

### 2.5.1 Changing Logon Banners Locally

**When and where to use:** Perform this procedure to change the logon banner for a Windows-based device from the Local Security Settings window on that device.

**Procedure:**

1 Log on to the Windows-based device using the local Windows administrator account.

The Windows administrator account set up by Motorola Solutions is “motosec” for Windows Server 2012 and “secmoto” for Windows 7 and Windows 10 devices.

2 **NOTICE:** If you are performing this procedure on a Windows-based device that is implemented as a virtual machine, you first need to connect the virtual machine to the DVD drive where you will insert the *Windows Supplemental* media. See the *Virtual Management Server Software* manual for information about connecting DVD drives to virtual machines in an ASTRO® 25 system.

Insert the *Windows Supplemental* media into the DVD drive.

3 Navigate to one of the following folders:

- `\Motorola Windows Supplemental Fullconfig\Scripts\WindowsLogonBanner`
- `\Motorola Windows Supplemental Transconfig\Scripts\WindowsLogonBanner`

Depending on the policies of your organization, your *Windows Supplemental* media contains either the `Fullconfig` or the `Transconfig` folder.

4 Copy the following files to the `C:\windows\temp` location:

- `setLogonBanner-source.exe`
- `setWindowsLogonBanner.vbs`
- `LogonBanner.txt`

5 Depending on the policies of your organization, perform one of the following:

| If… | Then… |
|---|---|
| **If your organization does not require a logon banner,** | go to step 8. |
| **If your organization requires a logon banner,** | Perform the following actions:<br>**a** In the `C:\windows\temp` folder, right-click `LogonBanner.txt`<br>**b** Click **Edit**. |

| If… | Then… |
|---|---|
| | The `LogonBanner.txt` file opens in the editor window. |

6 In the editor, perform the following actions:

**a** On the first line, enter: `Title:`

**b** Make sure the second line contains the banner title.

**c** On the third line, enter: `Text:`

**d** Type the Message text for the logon banner.

**Step example:** `LogonBanner.txt` file format:

```
Title:
Warning: This is a monitored computer system.
Text: Illegal and unauthorized use of this device
and any related service is strictly prohibited…
```

7 Save the `LogonBanner.txt` file and close the editor.

8 Open the **Command Prompt** and navigate to the `C:\windows\temp` folder.

9 Depending on the policies of your organization, perform one of the following actions:

| If… | Then… |
|---|---|
| **If your organization does not require a logon banner,** | Enter: `setLogonBanner-source.exe –U`<br>The login banner value is set to undefined in the local policy. |
| **If your organization requires a logon banner,** | Enter: `setLogonBanner-source.exe`<br>The login banner value is the text entered in the `LogonBanner.txt` file.<br>**NOTICE:** If the **User Account Control** dialog box appears, click **Continue**, or type the administrator password for the account displayed then click **Yes**, depending on the prompt you see. |

10 Close the **Command Prompt** window.

11 Restart the device.

**Postrequisites:** To verify if this procedure has been performed successfully, log out and log in to the client using the valid username and password. As a result, a warning banner with the text you entered is displayed.

### 2.5.2
## Changing Logon Banners Through a Domain Controller

Perform this procedure to change logon banners by editing a Group Policy Object (GPO) on the ASTRO® 25 system Domain Controller.

**Procedure:**

1 Log on to the system-level domain controller using your Active Directory account that is a member of the Domain Admins group.

The account name set up by Motorola Solutions is "motosec".

2 Depending the policies of your organization, perform one of the following:

- If your organization requires a logon banner, navigate to the `C:\Program Files\Motorola\AstroDC\AD\data` folder.
- If your organization does not require a logon banner, go to step 6.

3 Right-click `LogonBanner.txt` and click **Edit**.

The `LogonBanner.txt` file opens in the editor.

4 In the editor, perform the following actions:

**a** On the first line, enter: `Title:`

**b** Make sure the second line contains the banner title.

**c** On the third line, enter: `Text:`

**d** Type the Message text for the logon banner.

**Step example:** `LogonBanner.txt` file format:

```
Title:
Warning: This is a monitored computer system.
Text:
Illegal and unauthorized use of this device and
any related service is strictly prohibited…
```

5 Save the `LogonBanner.txt` file and close the editor.

6 Open PowerShell:

**a** From **Start**, click **Search**.

**b** In the search field, type in: `powershell`

**c** Click **Windows PowerShell**.

7 In the **PowerShell** window, navigate to `C:\Program Files\Motorola\AstroDC\AD\scripts`.

8 Perform one of the following actions:

| If… | Then… |
|---|---|
| **If your organization follows the DISA/FDCC standard,** | Enter: `.\setWindowsLogonBanner.ps1 -U`<br>The login banner value in the BHT_ADM GPO is set to “Not Defined”. |
| **If your organization’s policy is for GPOs to define that no logon banner will display,** | Enter: `.\setWindowsLogonBanner.ps1 -Define`<br>The login banner value is set to “Defined” and blank in the BHT_ADM GPO. |
| **If your organization’s policy is for GPOs to define that a logon banner will display, using text from LogonBanner.txt file,** | Enter: `.\setWindowsLogonBanner.ps1`<br>The login banner value is set to “Defined” and value is set to the text entered in the LogonBanner.txt file in the following location:<br>`C:\Program Files\Motorola\AstroDC\AD\data` |

9 Close the **PowerShell** window.

2.6

# Removing BAR Client and Event Logging Client Software

If the ASTRO® 25 system Backup and Restore (BAR) client software or the Centralized Event Logging client software is installed as part of a Windows-based virtual machine deployment, such as the Network Management (NM) Client, they appear in the list of programs under **Motorola**.

If your organization does not use these services, perform the following procedure to remove the BAR client and Centralized Event Logging client software (use the standard function for removing programs from a Windows environment).

For more information, see the *Backup and Restore Services* and the *Centralized Event Logging* manuals.

**Procedure:**

1 Verify if BAR or Centralized Event Logging client software was installed:

- **If your OS version is Windows 7,** from **Start**, select **All Programs** → **Motorola**.
- **If your OS version is Windows 10,** from **Start**, select **All apps** → **Motorola**.

2 If BAR or Centralized Event Logging client software is present:

| If… | Then… |
|---|---|
| **If your OS version is Windows 7,** | from **Start**, select **Control Panel** → **Uninstall a program**. |
| **If your OS version is Windows 10,** | perform the following actions:<br>**a** From **Start**, in the search field, type in: `uninstall`<br>**b** Click **Change or remove a program**. |

3 Uninstall the BAR client:

**a** In the list of programs, select **Motorola Windows Bar Client**.

**b** Click the **Uninstall** button above the list.

**c** Select **Motorola Common Cygwin**.

**d** Click the **Uninstall** button above the list.

**e** Reboot the Windows-based device.

4 Uninstall the Centralized Event Logging client:

**a** In the list of programs, select **Motorola Windows Logging Client**

**b** Click the **Uninstall** button above the list.

Chapter 3

# Remote Desktop Installation and Configuration

This section provides procedures for Windows-based devices that may need remote access.

## 3.1 Using Windows Remote Desktop Connection

**When and where to use:** Using the Windows Remote Desktop Connection (RDC), you can connect to a terminal server or to another computer running Windows, with the proper network access and permissions. The Remote Desktop Connection software communicates over a TCP/IP network connection using Microsoft Remote Desktop Protocol (RDP). Perform this procedure to log on or log off a remote computer or server using Windows Remote Desktop Connection.

**NOTICE:** The Windows Remote Desktop is automatically installed as part of the operating system installation.

**Procedure:**

1. From **Start**, open **Remote Desktop Connection**.
2. In the **Remote Desktop Connection** dialog box, **Computer** field, type in the hostname or IP Address.
3. Click **Connect**.

   The desktop of the remote computer appears.
4. Log on to the remote computer using the user name and password provided by your system administrator.

   The Windows Remote Desktop session begins.
5. To log off completely from a Windows Remote Desktop session, select **Start** → **Log off**.

   **NOTICE:**
   - The CTRL+ALT+DEL option cannot be used to log off from the remote session.
   - Clicking **X** in the Remote Desktop Connection dialog box closes this dialog box and not the remote session.

## 3.2 Allowing Multiple User Sessions on a Device

If your organization's policies allow multiple interactive user sessions on a device, you can perform the following procedures so that you can use Remote Desktop Connection to access a Windows-based device when a user is already logged on to that device.

**IMPORTANT:** Leaving the maximum number of sessions at one per device improves performance because it reduces the demand that can be placed on system resources. If each user is sure to log off a device when finished with it, the setting of one session per device can be sufficient.

### 3.2.1
## Changing Maximum Connections for Each Device in a Domain

**When and where to use:** If your organization's policies allow multiple user sessions on each device in a domain, you can perform this procedure to change the maximum number of Terminal Services (Remote Desktop Services) connections on each Windows-based device in a domain.

**Procedure:**

1. Log on to the system-level domain controller using your Active Directory account that is a member of the Domain Admins group.

   The account name set up by Motorola Solutions is "motosec".

2. Navigate to the **Server Manager**.

   **Step example:** Type `gpmc.msc` in the command field.

3. In the left pane of the **Server Manager** window, navigate to **Features** → **Group Policy Management**.

4. Expand the tree under **Group Policy Management**, as needed, to navigate to **Group Policy Objects** under the ASTRO® 25 system domain.

5. Depending on the Windows operating system of the device where you want to limit Remote Desktop connections, click one of the following **Group Policy Objects**:

   - For Windows Server 2012:
     - Domain Controllers: **DHT_2012_DC**
     - Other devices: **DHT_2012_ADM**
   - For Windows 7: **DHT_7_ADM**
   - For Windows 10: **DHT_10_ADM**

   Information about the selected Group Policy Object appears in the right pane. The devices that use this policy are listed on the **Scope** tab.

6. After confirming the Group Policy Object you want to edit, based on the devices listed on its Scope tab, right-click **Group Policy Object** and select **Edit**.

7. Under **Computer Configuration**, expand each of the following:

   a. **Policies**

   b. **Administrative Templates**

   c. **Windows Components**

   d. **Remote Desktop Services**

   e. **Remote Desktop Session Host**

8. Click **Connections**.

   Policy settings display.

9. In the right pane, double-click **Limit number of connections**.

10. Change the value in the field next to **RD Maximum connections allowed**.

    **Step example:**

    - If you want to allow multiple user sessions on each device in this domain, type: **999999**
    - If you want a maximum of one user session on each device, type: **1**

11. Click **OK**.

### 3.2.2
## Changing Maximum Connections for One Device

**When and where to use:** If your organization's policies allow multiple user sessions on a device, you can perform this procedure to change the maximum number of Terminal Services (Remote Desktop Services) connections on one Windows-based device.

**Procedure:**

1. Log in to the Windows-based device using the local Windows administrator account.

   The local Windows administrator account set up by Motorola Solutions is “motosec” for Windows Server devices, and “secmoto” for Windows 7 and Windows 10 devices.
2. Navigate to the **Microsoft Management Console** window.

   **Step example:** Type `mmc` in the command field.
3. Select **File** → **Add/Remove Snap-in**.
4. In the **Add/Remove Snap-in** window, click **Add**.
5. In the **Add Standalone Snap-in** window, click **Group Policy Object Editor**.
6. Click **Add**.
7. In the **Select Group Policy Object** window, click **Finish**.
8. In the **Add Standalone Snap-in** window, click **Close**.
9. In the **Add/Remove Snap-in** window, click **OK**.
10. In the left pane of the **Microsoft Management Console** window, expand each of the following:
    a. **Local Computer Policy**
    b. **Computer Configuration**
    c. **Administrative Templates**
    d. **Windows Components**
11. Perform the following actions:
    a. Select **Remote Desktop Services**.
    b. Expand **Remote Desktop Session Host**.
    c. Select **Connections**.
12. In the details pane, double-click **Limit number of connections**.

    A dialog box opens for editing the number of connections.
13. Select **Enabled**.
14. Change the value of maximum connections allowed.

    **Step example:**

    - If you want to allow multiple user sessions on this device, type in: `999999`
    - If you want a maximum of one user session on this device, type in: `1`
15. Click **OK**.

    The dialog box closes.
16. Close the **Microsoft Management Console** window.

This page intentionally left blank.

Chapter 4

# Windows Supplemental Configuration Troubleshooting

This chapter provides information about the configuration settings applied by the procedure Applying Device-Specific Settings Using the Windows Supplemental Media on page 37.

## 4.1 Types of Windows Supplemental Configuration Settings Applied

If you are troubleshooting problems with a Windows-based device in an ASTRO® 25 system, you can view types of supplemental configuration settings that were applied to that device.

The following are examples of settings applied by the Applying Device-Specific Settings Using the Windows Supplemental Media on page 37 procedure. The actual settings applied depend on the device selected during the procedure:

- Applies OS-specific settings (if a device supports more than one operating system, the Device Specific Settings function on the *Windows Supplemental* media automatically detects the operating system and applies the appropriate settings)
- Applies application-specific settings

The supplemental configuration settings of Microsoft-installed applications are summarized for each Windows-based device in a `.txt` file (**not** the `key.txt` file) in one of the following directories on the *Windows Supplemental* media, depending on your organization's policies:

- `\Motorola Windows Supplemental Fullconfig\bin`
- `\Motorola Windows Supplemental Transconfig\bin`

Each row of the `.txt` file includes types of information from the following table.

Table 4: Windows Supplemental Configuration – Format of Motorola Solutions' List of Settings Automatically Applied

| Identifier | If configuration of Microsoft-installed applications is needed (.NET, Media Player, Games, MSN, ASPNET, Messenger) | If OS-specific settings are needed: | If device- specific settings are needed: |
|---|---|---|---|
| ***<device name or names>***; | ***<common setting name>***;***<common setting name>***;etc. | ***<OS name>***; | ***<device name>***; |

If the **Windows Logging Client** check box or the **Windows BAR Client** check box were selected during Applying Device-Specific Settings Using the Windows Supplemental Media on page 37, this configuration is displayed in the last two rows of the `.txt` file.

If more than one device name appears at the beginning of a row in the `.txt` file, this indicates applications that reside on the same Windows-based device, as specified by the user during Applying Device-Specific Settings Using the Windows Supplemental Media on page 37.

**IMPORTANT:** The combinations available for selection are the only combinations of applications that have been designed and tested by Motorola Solutions for cohabitation on the same Windows-based device in ASTRO® 25 systems.