System Release 7.17
ASTRO® 25
INTEGRATED VOICE AND DATA

Unix Supplemental Configuration

Setup Guide

SEPTEMBER 2020

MN003373A01-C

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.

Contact Us

The Solutions Support Center (SSC) is the primary contact for technical support included in your organization's service agreement with Motorola Solutions.

Service agreement customers should be sure to call the SSC in all situations listed under Customer Responsibilities in their agreement, such as:

- Before reloading software
- To confirm troubleshooting results and analysis before taking action

Your organization received support phone numbers and other contact information appropriate for your geographic region and service agreement. Use that contact information for the most efficient response. However, if needed, you can also find general support contact information on the Motorola Solutions website, by following these steps:

1. Enter motorolasolutions.com in your browser.
2. Ensure that your organization's country or region is displayed on the page. Clicking or tapping the name of the region provides a way to change it.
3. Select "Support" on the motorolasolutions.com page.

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 or title of the section with the error
- A description of the error

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to https://learning.motorolasolutions.com to view the current course offerings and technology paths.

Document History

Version	Description	Date
MN003373A01-A	Original release of the *Unix Supplemental Configuration* manual	November 2016
MN003373A01-B	The following section was added: • Configuring Password Complexity Settings on Linux-Based Devices on page 13	June 2018
MN003373A01-C	Updated section: • Changing Root Account Passwords for Linux-Based Devices on page 12	September 2020

Contents

List of Tables

List of Procedures

About Unix Supplemental Configuration

This booklet supplements the ASTRO® 25 system documentation set with additional procedures for Linux-based and Solaris-based devices in an ASTRO® 25 system.

The information and procedures provided in this document should only be performed by a qualified administrator of the Linux or Solaris operating system, to safeguard the integrity of your system.

What Is Covered In This Manual?

This manual contains the following chapters:

- Linux Supplemental Configuration on page 11 provides configuration procedures for Linux-based devices.
- Solaris Supplemental Configuration on page 23 provides configuration procedures for Solaris-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 to view the current course offerings and technology paths.

Related Information

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

Related Information	Purpose
Standards and Guidelines for Communication Sites	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. Also known as the *R56* manual. This manual may be purchased on CD **9880384V83**, 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 Hardware	Provides information for implementing, maintaining, and replacing common Hewlett-Packard hardware for servers in an ASTRO® 25 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.
Generic Application Server	Covers information required to implement, maintain, and replace Generic Application Server hardware which is based on the Sun Netra platform and is used to host the ISSI.1 Network Gateway virtual server application.
ASTRO® 25 system manuals about specific Li-	For information on Linux-based devices implemented as virtual machines, see the following manuals:

Related Information	Purpose
nux-based devices	• *Backup and Restore Services* • *Centralized Event Logging* • *Fortinet Firewall Manager* • *IP Packet Capture* • *License Manager* • *Packet Data Gateways* • *Private Network Management Servers* • *Zone Controller* • *ISSI 8000/CSSI 8000 Intersystem Gateway Feature Guide* • *Unified Event Manager* • *Unified Network Configurator*
ASTRO® 25 system manual about the specific Solaris-based device	For information on the Solaris-based server application residing on Generic Application Servers in ASTRO® 25 systems, see the *ISSI.1 Network Gateway Feature Guide* manual.

Chapter 1

Linux Supplemental Configuration

This chapter provides procedures for changing passwords for domain and root users, as well as for supplemental configuration of Linux-based devices, including procedures for configuring passwords, enabling/disabling password aging, and welcome banners.

Many of the ASTRO® 25 system server applications are established on a Virtual Management Server (VMS) host platform where the server applications run under the Linux/ESXi operating system in a Virtual Machine (VM) environment supported by VMware. For more information, see the *Virtual Management Server Software* manual.

1.1 ASTRO 25 Linux-Based Devices Logging

In an ASTRO® 25 system, you can log on to Linux-based devices using your domain account or the root account.

1.1.1 Linux-Based Devices with an ASTRO 25 Domain Account Logging

For procedures that need to be performed as a domain user on a Linux-based device in an ASTRO® 25 system, you can log on to the Linux-based device using your Active Directory account that is a member of a user group authorized to access the device. For example, **fms-login** is a user group authorized to access the Firewall Management Server.

For information on Active Directory user groups in ASTRO® 25 systems, see the *Authentication Services* manual.

NOTICE: In ASTRO® 25 systems, you can access Linux-based devices that are implemented as virtual machines by first logging in as `root` to the ESXi-based server where the virtual machine is hosted. For instructions on using the ESXi-based server and virtual machines, see the *Virtual Management Server Software* manual.

1.1.2 Accessing the Root Prompt on Linux-Based Devices

When and where to use: In ASTRO® 25 systems, you can access Linux-based devices that are implemented as virtual machines by first logging in as root to the ESXi-based server where the virtual machine is hosted. For instructions on using the ESXi-based server and virtual machines, see the *Virtual Management Server Software* manual.

Procedure:

1. For procedures that need to be performed from the root command prompt on a Linux-based device, establish a connection to the console of the device.

   The login prompt appears.

2. Perform the following steps:

   a. In the command prompt, enter: `root`

   b. Enter the password for the root account, when prompted.

1.1.3
Accessing the Root Prompt on Linux-Based Devices in ASTRO 25 Systems with Active Directory

When and where to use:
This procedure is an alternative way to log in using your Active Directory account.

NOTICE: When you type the command `logout` or `exit` from the root prompt, you return to the prompt for your domain user account. Type the command again to log out completely.

Procedure:

1. Log in using your Active Directory account that is a member of a user group authorized to access the device.
2. Do the following:
   a. Enter: `su - root`
   b. When prompted, enter the root password.

Postrequisites:
Accessing the Root Prompt on Linux-Based Devices on page 11.

1.2
Root Account Password for a Linux-Based Device

In an ASTRO® 25 system, the root account is the only local account on a Linux-based server. It is not managed by the Active Directory domain.

Root account passwords are specific to an individual Linux-based server. A password change on one server is not propagated to other servers. The root account password can only be changed while logged in as root.

To change domain account passwords when logged on to a Linux-based device, see Changing Your Domain Account Password from a Linux-Based Device on page 13.

1.2.1
Changing Root Account Passwords for Linux-Based Devices

IMPORTANT: Upon the initial system installation, all passwords for non-domain interactive administrative accounts must be changed.

All passwords must meet the following criteria:

- Must be at least fourteen characters long.
- Must contain at least two uppercase letters and at least two lowercase letters.
- Must contain at least two numbers and at least two non-alphanumeric characters (for example, any character that is not a letter or a number).
- Must contain at least twelve unique characters for a fourteen character password. Longer passwords require additional unique characters.
- An upper case letter that begins the password and a digit that ends it do not count towards the number of character classes used, unless the **disable_firstupper_lastdigit_check** option is enabled.

Procedure:

1. Log on to the Linux-based device as the root user.

   See Accessing the Root Prompt on Linux-Based Devices on page 11.

2 In the root prompt, enter: `passwd`

A message reports that the password is being changed. You are prompted to type a new Unix password.

3 Enter the new Unix password for the root account. When prompted, re-enter the password.

IMPORTANT: If the password entered does not meet password restrictions, an invalid message appears, followed by the prompt to enter new password.

4 In the command prompt, enter: `logout`

The login prompt appears.

1.3 Changing Your Domain Account Password from a Linux-Based Device

Procedure:

1 Log on to the Linux-based device using your Active Directory account that is a member of the user group with privileges to access this device.

NOTICE: This procedure is only for changing the password of the domain account you use in this logon step. Changing the password for other accounts is possible when you log on to a Linux-based device as the root user, or using **su**. However, in general, it is recommended that domain account passwords be managed using Active Directory on the Domain Controller.

2 In the command prompt, enter: `passwd`

A message reports that the password is being changed for the account you used to log in to this device. You are prompted to enter the current (“old”) password.

3 Enter the current password for the account.

NOTICE: There may be a slight delay while the server queries the domain controller for the credentials.

You are prompted to enter a new password.

4 Enter and re-enter the new password.

A message reports the password changed.

1.4 Configuring Password Complexity Settings on Linux-Based Devices

Procedure:

1 Access the root command prompt on the device. See Accessing the Root Prompt on Linux-Based Devices on page 11.

2 At the root prompt, enter: `/opt/Motorola/clc/sbin/configure_password_settings`

A list of parameters appears. The script parameters have the following meaning:

- ***<-m>*** is the minimum length of the new password.
- ***<-o>*** is the minimum number of special characters in the new password.

- ***<-d>*** is the minimum number of digits in the new password.
- ***<-l>*** is the minimum number of lowercase letters in the new password.
- ***<-u>*** is the minimum number of uppercase letters in the new password.
- ***<-r>*** is the maximum number of allowed consecutive same characters in the new password.
- ***<-f>*** is the minimum number of characters in the new password that must not be present in the old password.
- ***<-c>*** is the minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others).
- ***<-x>*** is the maximum number of allowed consecutive characters of the same class in the new password.
- ***<-e>*** indicates that password complexity is checked even if the user changing the password is root (default setting).
- ***<-E>*** indicates that password complexity is not checked if the user changing the password is root.
- ***<-t>*** restores defaults.
- ***<-j>*** applies `pwquality` and `root` enforcing configuration from a `.json` file.

3 Adjust password complexity settings by entering:
`/opt/Motorola/clc/sbin/configure_password_settings`
<parameter><parameter value>

NOTICE:
You can mix options except that ***<-t>*** and ***<-j>*** must be used alone and ***<-E>***/***<-e>*** are mutually exclusive.

The value range is from 0 to 255.

1.5 Re-Activation of Domain User Accounts if Passwords Expire

Accounts managed on the Active Directory Domain Controller can be set to have their passwords expire after a specific amount of time. If users log in to a Linux-based server using an account with a password that expired, the authentication failure message appears.

An expired domain account password cannot be reset from the Linux-based device.

The preferred method to reset domain account passwords is to have the domain administrator perform this function in Active Directory on the Domain Controller. For instructions, see *Active Directory* online help or “Resetting User Passwords in Active Directory” in the *Authentication Services* manual.

IMPORTANT: When changing a password using Active Directory, make sure that the check box is unmarked for the option **User must change password at next logon**.

Alternately, users can reset an ASTRO® 25 system domain account password by pressing ALT + CTRL + DEL, and selecting the Change Password option, when logged on to another account on an ASTRO® 25 system Network Management Client. (The Windows-based Change Password function allows any username to be entered, with the domain name, and old and new passwords.)

1.6 Password Aging Configuration on a Linux-Based Device

This section provides password aging configuration procedures for Linux-based devices in an ASTRO® 25 system.

1.6.1
Enabling Password Aging for the Non-Root Local Users

Procedure:

1. Access the root command prompt on the device.

   See Accessing the Root Prompt on Linux-Based Devices on page 11.
2. At the root prompt, enter: `/opt/Motorola/clc/sbin/switch_pass_aging -e`

   Password aging duration is enabled.

Postrequisites:
After you complete this procedure, password aging becomes effective immediately (the days specified for aging begin to count down). After that, if the specified number of days is reached during a user session, the user is not notified that the password needs to be changed and the user can complete the current session without changing the password.

In that case, the next time you log on to this device using the root account, you will be prompted to enter the old password and create a new password.

1.6.2
Disabling Password Aging for the Non-Root Local Users

Procedure:

1. Access the root command prompt on the device.

   See Accessing the Root Prompt on Linux-Based Devices on page 11.
2. At the root prompt, enter: `/opt/Motorola/clc/sbin/switch_pass_aging -d`

   A message reports that the password aging has been disabled.

1.6.3
Enabling Password Aging for the Root Account

Procedure:

1. Access the root command prompt on the device.

   See Accessing the Root Prompt on Linux-Based Devices on page 11.

   The root prompt appears.
2. To enable password aging for Root, enter: `chage –I 35 –m 1 –M 60 root`

1.6.4
Disabling Password Aging for the Root Account

Procedure:

1. Access the root command prompt on the device.

   See Accessing the Root Prompt on Linux-Based Devices on page 11.

   The root prompt appears.
2. To disable password aging for Root, enter: `chage –I -1 –m 0 –M 99999 root`

1.6.5
Linux Password Parameters Configuration for Fortinet Firewall Manager

For password configuration procedures for Linux-based devices in an ASTRO® 25 system pertaining to the Fortinet Firewall Manager, see the *Fortinet Firewall Manager* manual.

1.7
Deleting Local User Files After Deleting a User from Active Directory

When and where to use:
When an interactive domain user logs on to a Linux-based device, several files are created on that device specific to that user.

When a user account is removed from Active Directory on the domain controller and is no longer needed, perform Deleting Local User Files After Deleting a User from Active Directory on page 16 to delete the user's local files from a Linux-based device.

Procedure:

1. Access the root command prompt on the device.

   See Accessing the Root Prompt on Linux-Based Devices on page 11.

2. At the root prompt, enter: `/opt/Motorola/aaa/bin/delete_user_files <username>`

   where `<username>` is the user account that was deleted from Active Directory.

   The local files for the specified user are removed from the device.

1.8
Banners Management on a Linux-Based Device

This section provides procedures for managing the welcome banner on a Linux-based device.

NOTICE: The running session must be restarted before the new banner is displayed. This can be accomplished by terminating the remote connection to the Virtual Machine or rebooting the Virtual Machine.

NOTICE: It is recommended to perform a backup of the banner. See Backing Up the Current Welcome Banner on a Linux-Based Device on page 17.

1.8.1
Changing the Welcome Banner on a Linux-Based Device

Procedure:

1. Access the root command prompt on the device.

   See Accessing the Root Prompt on Linux-Based Devices on page 11.

   The root prompt appears.

2. Create the banner file using a text editor or command and save the banner as `/tmp/banner`

   NOTICE: Alternatively, to revert to a previous banner that you backed up using the procedure in Backing Up the Current Welcome Banner on a Linux-Based Device on page 17, you can skip this step. In the next step, enter: `cp /etc/issue.backup /etc/issue` instead.

3 Apply the banner text file. Enter: `cp /tmp/banner /etc/issue`

The new banner is used for all logins.

4 In the root prompt, enter: `exit`

1.8.2
Backing Up the Current Welcome Banner on a Linux-Based Device

Procedure:

1 Access the root command prompt on the device.

See Accessing the Root Prompt on Linux-Based Devices on page 11.

The root prompt appears.

2 Back up the banner text file. Enter: `cp /etc/issue /etc/issue.backup`

1.8.3
Configuring a Linux-Based Device to Use the Default Welcome Banner

Procedure:

1 Access the root command prompt on the device.

See Accessing the Root Prompt on Linux-Based Devices on page 11.

2 In the root prompt, enter: `cp -f /opt/Motorola/clc/config/base/issue /etc/issue`

The system prompts the user to overwrite the file.

3 Enter: `y`

The root prompt appears. The default banner is used for all logins.

1.8.4
Changing the Welcome Banner for the vCenter Application

Prerequisites: For more information on vCenter, see the *ASTRO 25 vCenter Application Setup and Operations Guide*.

Procedure:

1 Access the root command prompt on the device.

See Accessing the Root Prompt on Linux-Based Devices on page 11.

The root prompt appears.

2 Create the banner file using a text editor or command and save the banner as `/tmp/banner`.

NOTICE: Alternatively, to revert to a previous banner that you backed up using the procedure in Backing Up the Current Welcome Banner on a Linux-Based Device on page 17, you can skip this step. In the next step, enter `cp /etc/issue.backup /etc/issue` instead.

3 Apply the banner text file. Enter: `cp /tmp/banner /etc/issue`

The new banner is used for all logins.

4 In the root prompt, enter: `exit`

1.9 General Administration Menu Operations on a Linux-Based Device

Motorola provides server administration menus on Linux-based devices in ASTRO® 25 systems that include operations specific to ASTRO® 25 systems. For convenience, these menus also include the general Linux server administration operations listed in the following table.

Table 1: General Administration Menu Operations on Linux-Based Devices

Administration menu names	Related information
Software Administration:	
Display Software Package Versions	This displays release numbers and creation dates.
Eject CD	This unmounts the media (if not already unmounted by a reboot after patching the Linux OS) and opens the drive drawer. **NOTICE:** After removing the media, be sure to disconnect the Linux-based virtual machine from the DVD drive. See the instructions in the *Virtual Management Server Software* manual.
Reboot Server	After selecting this option, you are prompted to confirm that you want to reboot. After you confirm, the device reboots, and the login prompt appears. **NOTICE:** A successful Linux OS patch automatically reboots the device, so it is not necessary to use this menu option.
OS Administration:	
Manage Platform Configuration and Display Platform Configuration Information	Allows the user to set the identity of the application after initial installation of the application. Time Parameters Configuration on a Linux-Based Device on page 19 Displays hardware and OS configuration information.
Display Platform Resource Usage Information	Displays memory usage, disk usage, and CPU usage.
Reboot Server	After selecting this option, you are prompted to confirm that you want to reboot. After you confirm, the device reboots, and the login prompt appears.
Shutdown	After selecting this option, you are prompted to confirm that you want to shut down. After you confirm, the device shuts down. Its console in VMware vSphere Client is blank. (See the Note below regarding powering on the device.)
For information about the other operations available under the **OS Administration** menu, see the following ASTRO® 25 system manuals:	**NOTICE:** For instructions about using VMware vSphere Client to power on ASTRO® 25 system virtual machines, see the *Virtual Management Server Software* manual.

Administration menu names	Related information
Security Provisioning: *SNMPv3* manual, *Securing Protocols with SSH* manual Get Log Files: Display Log Files: *Centralized Event Logging* manual, and the manual for the specific Linux-based device	
Services Administration:	
Manage NTP Configuration	Configuring NTP Client on a Linux-Based Device on page 20
For information about the other menu options of the **Manage client name** → **Configuration** under the Services Administration menu, see the following ASTRO® 25 system manuals: • **AAA Client:***Authentication Services* manual • **BAR Client:***Backup and Restore Services* manual • **Syslog Client:***Centralized Event Logging* manual	

1.9.1
Time Parameters Configuration on a Linux-Based Device

The section includes procedures for displaying the time zone and configuring the time zone on a Linux-based device in an ASTRO® 25 system.

1.9.1.1
Displaying the Time Zone on a Linux-Based Device

Perform this procedure on a Linux-based device to display the currently configured time of day, date, and time zone.

Procedure:

1. Access the root command prompt on the device.

   See Accessing the Root Prompt on Linux-Based Devices on page 11.

2. At the root prompt, enter: `date`

   The current day of the month, date, time, and time zone display.

1.9.1.2

Configuring the Time Zone on Linux Servers

As a part of the installation, ensure that the virtual machine is set to the correct time zone.

Procedure:

1. From a Windows-based device, launch the VMware vSphere Client.

   A desktop shortcut was created during installation.
2. Log on to the ESXi server hosting the virtual machine as root by entering the IP address of the server and the root credentials.
3. In the **vSphere Client Inventory** window, verify that the virtual machine is powered on. If the virtual machine is powered off, power it on by right-clicking the virtual machine in the navigation pane and selecting **Power** → **Power On**.
4. From the navigation pane on the left, select the virtual machine. Click the **Console** tab for this virtual machine.
5. Wait until a prompt to log on console appears.
6. Click in the **Console** window and log on to the virtual machine as root.
7. At the prompt, enter: `admin_menu`
8. In the main administration menu, enter the number for the **OS Administration** option.
9. In the **OS Administration** menu, enter the corresponding number for **Manage Platform Configuration**.
10. In the **Manage Platform Configuration** menu, enter the corresponding number for **Set Time Zone**.

    A menu displays numbered options to the change time zone.
11. The **Set Time Zone** option starts by prompting you for the region of the world.

    You can choose to specify the time zone using the **Posix TZ format**. Continue responding to the prompts until you see a message regarding `/usr/bin/tzselect`. Ignore the message.
12. Press `q` to quit the menu.

1.9.2

Configuring NTP Client on a Linux-Based Device

Procedure:

1. Log on to the Linux-based server using your Active Directory account.

   For information about setting up group membership of Active Directory users so that they can perform specific administration menu procedures, contact your Active Directory administrator.
2. At the command prompt, enter: `admin_menu`
3. In the server administration **Main Menu**, enter the number for the option **Services Administration**.
4. In the **Services Administration** menu, enter the number for the option **Manage NTP Client Configuration**.

   NOTICE: To see what NTP servers are currently configured, enter the number for the option **Display NTP Status**.
5. In the **Manage NTP Client Configuration** menu, enter the number for one of the following options:

- **Add External NTP Time Source** – After selecting this option, you are prompted to enter the IP address
- **Remove External NTP Time Source** – After selecting this option, you are prompted to enter the number for one of the NTP servers in a numbered list

NOTICE: To verify the changes, enter the number for the option **Display NTP Status**. To add another NTP server, enter the number for the option **Add External NTP Time Source**.

The **Manage NTP Configuration** menu appears.

1.10 vCenter Administrator Password Configuration

This section contains procedures for the VMware vCenter Server administrator password configuration in the ASTRO® 25 system.

1.10.1 Resetting the Administrator Password on the vCenter Server

Perform the following procedure to reset the administrator password on the Platform Services Controller or vCenter Server with the Embedded Platform Services Controller Appliance.

Procedure:

1. Log on to vCenter Server Appliance through SSH:
   a. Establish an SSH session using your Active Directory account that is a member of a user group authorized to access this device.
   b. Enter: `su -`
   c. Enter the root account password.
2. At the root prompt, enter:
   `shell.set --enabled true`
3. Enter: `shell`
4. To open the `vdcadmintool`, enter: `/usr/lib/vmware-vmdir/bin/vdcadmintool`
5. At the menu prompt, select the number corresponding to the **Reset account password** option.
6. When prompted for the Account UPN, enter: `Administrator@<SSO.domain>`

   A new password is generated.
7. Log on to the domain account with the new password.

   The password is regenerated.
8. Log on to the **vSphere Web Client** and change the password.

   See Changing the vCenter Server Administrator Password in the vSphere Web Client on page 22.

1.10.2

Changing the vCenter Server Administrator Password in the vSphere Web Client

Perform the following procedure to change the vSphere Server administrator password using the VMware vSphere Web Client.

Procedure:

1. Log on to vCenter Server Appliance using the **vSphere Web Client**.

   See "Logging On and Off vSphere Web Client" in the *ASTRO 25 vCenter Application Setup and Operations Guide*.
2. In the **Navigator** pane on the left, click **Administration**.
3. Under **Single Sign-On**, click **Users and Groups**.
4. In the **Users and Groups** pane, click the **Users** tab.
5. From the **Domain** drop-down list, select the appropriate SSO domain of the administrator account.
6. Right-click the **Administrator** account and select **Edit User**.
7. In the **Administrator - Edit** window, the **Current Password** dialog box, enter the ***<current password>***.
8. In **Password** and **Confirm Password** fields, enter the ***<new password>***.

   where ***<new password>*** is the new password set up in Resetting the Administrator Password on the vCenter Server on page 21
9. Click **OK**.

Chapter 2

Solaris Supplemental Configuration

This chapter provides configuration procedures for Solaris-based devices in an ASTRO® 25 system.

NOTICE: The ISSI.1 feature may be supported on a Generic Application Server (GAS) server platform. For detailed information regarding the GAS server and ISSI.1, see the following manuals:

- *Generic Application Server*
- *ISSI.1 Network Gateway*

2.1 ASTRO 25 Solaris-Based Devices Logging

In an ASTRO® 25 system, you can log on to Solaris-based devices using your domain account or the root account.

2.1.1 Solaris-Based Devices with an ASTRO 25 Domain Account Logging

For procedures that need to be performed as a domain user, establish an SSH session using your Active Directory account that is a member of a user group authorized to access the device. For example, “gas-login” is a user group authorized to access the Generic Application Server.

For information on Active Directory user groups in ASTRO® 25 systems, see the *Authentication Services* manual.

2.1.2 Accessing the Root Command Prompt on Solaris-Based Devices

Prerequisites: For information on Active Directory user groups in ASTRO® 25 systems, see the *Authentication Services* manual.

When and where to use: For procedures that need to be performed from the root command prompt.

Procedure:

To access the root command prompt:

If…	Then…
If you are using an SSH session to connect to the device,	perform the following actions: **a** Establish an SSH session using your Active Directory account that is a member of a user group authorized to access this device. **b** Enter: `su -` **c** Enter the root account password to access the root command prompt.
If the device you connect to is hosted on a	perform the following actions:

If…	Then…
Generic Application Server,	**a** From a terminal server, log on to the Generic Application Server with an Active Directory user account that is a member of a user group with privileges to access the Generic Application Server. If a domain controller is not available on the network, log on to the Generic Application Server locally, using its root account. **b** Enter: `sudo zlogin -C` ***<server application hosted on the GAS>*** **c** From the command prompt for the server application, log on using its root account.

2.2
Change Passwords for Solaris-Based Devices

This section provides procedures for changing the passwords for the user accounts for a Solaris-based device, including root passwords, domain user passwords, and the EEPROM password.

It also provides a procedure for disabling password aging.

CAUTION: Failure to disable password aging may result in password expiration, which can cause failure of automated jobs and loss of functionality.

2.2.1
Changing the Root Account Password for a Solaris-Based Device

In an ASTRO® 25 system, the root account is the only local account on a Solaris-based server. It is not managed by the Active Directory domain.

Root account passwords are specific to an individual Solaris-based server. A password change on one server is not propagated to other servers. The root account password can only be changed while logged in as root.

To change domain account passwords when logged on to a Solaris-based device, see Changing Your Domain Account Password from a Solaris-Based Device on page 24.

Solaris passwords should avoid the use of the following symbols: # and @.

Procedure:

1. Log on to the Solaris-based device as the root user.
2. In the root prompt, enter: `epasswd`
3. Enter and re-enter the new password.

2.2.2
Changing Your Domain Account Password from a Solaris-Based Device

When and where to use:

NOTICE: A user can only change their own domain account password on a Solaris-based server.
It is recommended that domain account passwords be managed using Active Directory on the Domain Controller.

Procedure:

1. Log on to the Solaris-based device using your Active Directory account that is a member of the user group with privileges to access this device.
2. In the command prompt, enter: `epasswd`

   A message reports that the password is being changed for the account you used to log in to this device. You are prompted to enter the current ("old") password.
3. Enter the current password for the account.

   NOTICE: There may be a slight delay while the server queries the domain controller for the credentials.

   You are prompted to enter a new password.
4. Enter and re-enter the new password.

   A message reports the Kerberos password was changed.

2.2.3
Changing the EEPROM Password for a Solaris-Based Device

Procedure:

1. Log on to the Solaris-based device using your Active Directory account that is a member of the user group with privileges to access this device.
2. In the command prompt, enter: `sudo eeprom security-password=`

   NOTICE: The password cannot be set unless the security-mode setting is configured as `command`. Setting the `security-mode=command` only prompts for the password when the security-mode was previously `none`.

   You are prompted to enter a new PROM password.
3. Type and re-type the PROM password.
4. Press ENTER to finish.

2.2.4
Changing the EEPROM Security Mode

When and where to use:
Solaris-based servers when installed has the security-mode set to **none**. For heightened security, this mode can be changed to **command**. The **command** security mode prevents EEPROM changes and hardware command execution while at the OpenBoot PROM.

CAUTION: Do not set the security mode to full as this mode requires the OpenBoot PROM password to boot. This prevents the server from recovering automatically in case of software reset or power failure.

IMPORTANT: The EEPROM `security-mode=command` and `boot-command="boot -r"` settings conflict with each other and cause the Generic Application Server to fail to boot to Solaris automatically after non-standard shutdown, for example: power outage. The system instead boots to a login prompt for the EEPROM where the user is either prompted to log in to the EEPROM and is sent to the ok prompt, or is allowed to boot. Manual intervention is required to continue the boot process if both of the listed settings are configured.
Changing the boot-command from `boot -r` to `boot` causes the system to not automatically detect any new hardware devices during system boots.

Procedure:

1. Log on to the Solaris-based device using your Active Directory account that is a member of the user group with privileges to access this device.
2. In the command prompt, enter: `sudo eeprom security-mode=command`

   NOTICE: EEPROM security mode can be returned to its original setting by substituting `command` with `none`.

   NOTICE: Enabling EEPROM passwords requires changing the boot-mode setting to `boot`.

   You are prompted to enter a new PROM password.
3. Type and re-type the PROM password.
4. In the command prompt, enter: `sudo eeprom boot-command=boot`

   The EEPROM boot command is configured to not perform an auto-detection of hardware devices on every reboot.
5. Press ENTER to finish.

2.3 Re-Activation of Domain User Accounts if Passwords Expire

Accounts managed on the Active Directory Domain Controller can be set to have their passwords expire after a specific amount of time. If users log in to a Solaris-based server using an account with a password that expired, the following message appears:

```
Warning: Your password has expired, please change it now.
Please login through the Solaris console to unexpire your password.
```

When this message appears, you can close the session by pressing CTRL + C or by closing the PuTTY window. To change the password:

- The preferred method to reset domain account passwords is to have the domain administrator perform this function in Active Directory on the Domain Controller. For instructions, see the *Authentication Services* manual.
- Alternatively, users can reset an expired ASTRO® 25 system domain account password by pressing CTRL+ALT+DEL and selecting the **Change Password** option on the Windows Security dialog box, when logged on to another account on an ASTRO® 25 system Network Management Client. (The Change Password function allows any username to be entered, with the domain name, and old and new passwords.)

CAUTION: These methods cannot be used for a root account with an expired password. If the root account password expires, contact the Motorola Solutions Support Center (SSC).
If enabling password aging on a root account results in password expiration, this can cause failure of automated jobs and loss of functionality.

2.4 Enabling Eight-Week Password Aging for the Root Account on a Solaris-Based Device

If supported by your organization's policies, you can use this procedure to enable password aging, with password expiration after eight weeks, for the root account on a Solaris-based device in an ASTRO® 25 system. The password aging becomes effective for the root account the first time the root password is changed after password aging is enabled.

CAUTION:
Enabling password aging requires passwords to be changed at periodic intervals because the passwords expire.

If enabling password aging on a root account results in password expiration, this can cause failure of automated jobs and loss of functionality.

If the root account password has expired, contact Motorola Solutions Support Center (SSC) to refresh the password.

Procedure:

1. Log on to the Solaris-based device as the root user.
2. In the root prompt, enter: `cp -p /etc/default/passwd /tmp/passwd`
3. In the root prompt, enter:
   `/usr/bin/perl -pe 's/^MAXWEEKS=.*/MAXWEEKS=8/;s/^MINWEEKS=.*/MINWEEKS=1/' -i /tmp/passwd`
4. In the root prompt, enter: `grep WEEKS /tmp/passwd`

   The following message is displayed:

   ```
   MAXWEEKS=8
   MINWEEKS=1
   ```

5. In the root prompt, enter: `cp -p /tmp/passwd /etc/default/passwd`

2.5 Deleting Domain User Files and Home Directory from a Solaris-Based Device

When and where to use:
When a user account is removed from the Active Directory domain, perform Deleting Domain User Files and Home Directory from a Solaris-Based Device on page 27 to remove the user files and the user home directory from each Solaris-based server where the user logged on.

Procedure:

1. Log on to the Solaris-based device using your Active Directory account that is a member of the user group with privileges to access this device.

   NOTICE: Do not perform this procedure while the user to be deleted is logged in.

2. In the command prompt, enter: `su -`
3. In the password prompt, enter the root account password.

   The root command prompt displays.

4. Perform one of the following actions:

- If you logged in directly to a server application on a Generic Application Server, enter: `delete_user_files` ***<user account>***
- If you logged in to the Generic Application Server, not a server application that it hosts, enter:

  `/opt/MOTghssvcs/bin/delete_user_files` ***<user account>***

  where ***<user account>*** is the account that needs its files and home directory to be deleted.

A warning message states the following and asks if you want to continue with the script:

```
This script performs various operations which can damage the system. It
changes owner of files with no user to root (for session history
files), removes given user filesystem and removes files owned by the
user. This script will attempt to remove a users home directory.
Running this within the users directory structure can prevent removal
of the users home directory.
```

5 Enter: `y`

A list of proposed changes concerning the users files, home directory, and running process display followed by a confirmation message.

6 Enter: `y`

A list of the changes performed is displayed and a message stating the users files were successfully removed and the root prompt appears.

2.6 Banners Management on a Solaris-Based Device

This section provides procedures for managing banners on Solaris-based devices.

2.6.1 Setting or Changing the Electrically Erasable Programmable Read-Only Memory (EEPROM) Banner on a Generic Application Server

Procedure:

1 Log on to the Generic Application Server using your Active Directory account that is a member of the user group with privileges to access this device (gas-login is the user group set up by Motorola Solutions).

NOTICE: Do not perform this procedure while the user to be deleted is logged in.

2 In the command prompt, enter: `su -`

3 In the password prompt, enter the root account password.

The root command prompt displays.

4 To start the banner, enter: `eeprom oem-banner?=true`

5 To change the banner text, enter: `eeprom oem-banner="`***<your banner text>***`"`

2.6.2
Backing Up Banner Files for Solaris-Based Devices

Procedure:

1. Log on to the Solaris-based device using your Active Directory account that is a member of the user group with privileges to access this device.

   NOTICE: Do not perform this procedure while the user to be deleted is logged in.

2. In the command prompt, enter: `su -`
3. In the password prompt, type the root account password.

   The root command prompt displays.

4. Back up the banner text files by executing the following commands:
   - For Generic Application Servers enter: `cp /etc/issue /etc/issue.backup`
   - For all devices, enter: `cp /etc/banners/sshd /etc/banners/sshd.backup`

2.6.3
Changing Banner Text for Solaris-Based Devices

Procedure:

1. Log on to the Solaris-based device using your Active Directory account that is a member of the user group with privileges to access this device.

   NOTICE: Do not perform this procedure while the user to be deleted is logged in.

2. In the command prompt, enter: `su -`
3. In the password prompt, enter the root account password.

   The root command prompt displays.

4. Create the banner file using a text editor or command and save the banner as `/tmp/banner`
5. Create and apply the individual banner text files by executing the following commands:
   - For Generic Application Servers, enter: `cp /tmp/banner /etc/issue`
   - For all devices, enter: `cp /tmp/banner /etc/banners/sshd`