System Release 7.17
ASTRO® 25
INTEGRATED VOICE AND DATA

Securing Protocols with SSH

APRIL 2020

MN003352A01-D

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
MN003352A01-A	Original release of the *Securing Protocols with SSH* manual	November 2016
MN003352A01-B	Second release of the *Securing Protocols with SSH* manual	December 2016
MN003352A01-C	Second release of the *Securing Protocols with SSH* manual	November 2017
MN003352A01-D	Updated sections: • Disabling Clear Protocols on page 76 • SSH Configuration for RF Site Devices and VPMs Using CSS – Overview on page 155 • Configuring Secure Services/Keys and Clear Services Using CSS on page 156	April 2020

Contents

List of Figures

List of Tables

List of Processes

List of Procedures

About Securing Protocols with SSH

This manual covers implementation and management of the Secure Shell (SSH) protocol for secure transmission of data between devices in an ASTRO® 25 communication system.

What Is Covered In This Manual?

This manual contains the following chapters:

- SSH Description on page 25 introduces the concept of secure and clear protocols in the context of an ASTRO® 25 system.
- SSH Theory of Operation on page 33 provides additional details about the concept of secure and clear protocols in the context of an ASTRO® 25 system.
- SSH Installation on page 40 is for installation procedures relating to the Securing Protocols with SSH feature.
- SSH Configuration on page 42 provides configuration processes and procedures for configuring the Securing Protocols with SSH feature on your system. Includes configuration sequences that minimize downtime when adding this feature to a system that is already in operation.
- SSH Optimization on page 207 is for optimization information relating to the Securing Protocols with SSH feature. (No optimization is required for this feature.)
- SSH Operation on page 208 provides information about tasks you can perform after the Securing Protocols with SSH feature is operational on your system.
- SSH Maintenance on page 211 is for information relating to periodic maintenance of the Securing Protocols with SSH feature. (All of the maintenance required for this feature is covered in other chapters.)
- SSH Troubleshooting on page 212 provides fault management and troubleshooting information relating to the Securing Protocols with SSH feature.
- SSH Connection Lists (Primary Cores and Sites) on page 217 lists SSH connections that are included in the Securing Protocols with SSH feature for primary cores and sites in ASTRO® 25 communication systems.
- SSH Connection Lists – DSR Only on page 226 lists SSH connections that are included in the Securing Protocols with SSH feature and are specific to ASTRO® 25 communication systems with the Dynamic System Resilience (DSR) feature.

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 (6881089E50)	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. Also known as R56 manual.

Related Information	Purpose
	This 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.

NOTICE: For more information about the manuals to be located before configuring a system for the Securing Protocols with SSH feature, see the process tables in SSH Configuration on page 42.

Chapter 1

SSH Description

This chapter introduces the concept of secure and clear protocols in the context of your ASTRO® 25 communication system.

1.1 SSH Overview

Secure Shell (SSH) is an industry-standard protocol that allows secure transmission of data between two devices on a network by using public-key encryption techniques. SSH authenticates both ends of a connection, encrypts bearer traffic, and ensures the integrity of data.

SSH uses a client-server model to secure traffic generated during remote login, remote file transfer, and remote command execution across a network.

SSH provides the following functions:

- Provides strong authentication and secure communications over channels that are not secure
- Encrypts authentication credentials and payload data before they are transmitted across the network
- Provides a secure channel using Advanced Encryption Standard (AES) encryption

The Securing Protocols with SSH feature provides a secure alternative to the clear protocols that are used in an ASTRO® 25 communication system, including ftp, tftp, telnet, rlogin, rsh, and rcp. Many elements in the ASTRO® 25 system utilize this capability for secure communications.

1.1.1 SSH Deployment Scope

Subsystems and products impacted by the ASTRO® 25 system Securing Protocols with SSH feature include:

Generic I/O Monitoring
SDM3000 RTU, SDM3000 Network Translator, GMC (MOSCAD NFM Server), GWS (MOSCAD NFM Client), SDM3000 Builder, MCC 7500 Aux I/O Server

Transport Network Subsystem
Core Routers, Exit Routers, Gateway Routers, GGSN Routers, Site Routers, Prime Site Routers, Access Routers, Conventional Channel Gateway Router, NM Dispatch Routers, Core/Gateway Routers, Core LAN Switches, Mediation LAN Switches, IDS LAN Switch, Fan-out LAN Switches, IVD Site LAN Switches, HPD Site LAN Switches, Simulcast Prime LAN Switches, Simulcast Remote LAN Switches, Conv Only Site LAN Switches, NM Dispatch LAN Switches, Core Terminal Server, Simulcast Prime Terminal Server

IP Services Subsystem
InfoVista, Domain Controller, Centralized Event Logging servers, Core Security Management Server, Backup and Recovery Server, Baseline Backup and Recovery Server, IP Packet Capture

Radio Network Management Subsystem
Unified Network Configurator, Unified Network Configurator Device Servers, Unified Event Manager, System Statistics Server application, Zone Statistics Server application, User Configuration Server application, Zone Database Server application, Generic Application Server, Network Management Client, MKM 7000 Console Alias Manager server (CAM), License Manager

System Traffic Monitoring Subsystem
Air Traffic Router, Generic Application Server

Fixed Radio Subsystem
G-Series based: Site Controller, Conventional Site Controller, Conventional Base Radio, Conventional Comparator, Trunked Comparator and Site Repeater, HPD RF Site Controller, HPD Base Radio, Reference Distribution Module, Configuration System Software, MLC 8000 Analog Comparator, MLC 8000 Subsite Link Converter, MLC 8000 Configuration Tool (CT)

Fixed Device Management Subsystem
Configuration/Service Software

Data Subsystem
Packet Data Router, Radio Network Gateway

Zone Controller Subsystem
Zone Controller

Legacy 3600 Gateway Subsystem
SmartX Site Converter

Console Subsystem
Voice Processor Module (VPM) component of MCC 7500 Console; also see MKM 7000 Console Alias Manager under Radio Network Management subsystem

Gateway Subsystem
ISSI.1 Network Gateway, Intersystem Gateway (ISGW)

Key Management Subsystem
Authentication Center Server

Time and Frequency Reference Subsystem
TRAK devices

Telephone Interconnect Subsystem
Telephone Media Gateway, Console Telephony Media Gateway

Server Virtualization Subsystem
vCenter Appliance, Virtual Management Server (ESXi/Hypervisor), Direct Attached Storage (DAS)

For more information, see SSH in an ASTRO 25 Communication System on page 27.

1.1.2
SSH Terminology

SSH (in upper case)
Generic reference to all Secure Shell (SSH) protocols (such as ssh, scp, or sftp).

ssh (in lower case)
Refers to the client program used to initiate secure terminal sessions and remote commands.

scp
Secure Copy, used for file transfer. Provides no file management capabilities.

sftp
Secure File Transfer protocol, uses SSH to provide a secure service, allowing the server to encrypt the data and handle the file transfer. SFTP includes many file management capabilities such as deletion, renaming, interrupted transfer resumption, and directory listings.

Secure operation
Refers to the use of ssh, scp, or sftp protocols to secure one or more connections in an ASTRO® 25 communication system.

SSH host
A device or component that supports SSH functionality (includes **both** SSH clients and SSH servers).

SSH client
The device or component that initiates the SSH connection request.

SSH server
The device or component that receives the SSH connection request.

1.1.3
SSH Protocols

There are two versions of Secure Shell available: SSH1 and SSH2. The ASTRO® 25 communication system uses SSH2. The following table lists the mapping of SSH utilities and the clear protocols they replace in an ASTRO® 25 communication system.

Table 1: Clear Protocols and Their SSH Equivalents

Clear Protocol	Secure Protocol	Description
ftp, tftp	sftp	Used for file transfers.
rcp (Remote Copy Protocol)	scp	Used to remotely copy files between devices on a network. Unlike rcp, scp prompts for passwords or passphrases, if required, for authentication.
rlogin (Remote Login)	ssh	Used to remotely log into a device to execute commands.
rsh (Remote Shell)	ssh	
rsync	rsync over SSH	Used for incremental file transfer. **NOTICE:** The rsync protocol is capable of both secure and non-secure operation, but the secure method of rsync inherently uses SSH. This is the only method permitted when secure operation is enabled on the system.
telnet	ssh	Used for remote logins.

1.2
SSH in an ASTRO 25 Communication System

Securing Protocols with SSH provides a secure point-to-point connection between two devices in an ASTRO® 25 communication system in which the connection is encrypted and both ends have been authenticated.

NOTICE: Implementing the Securing Protocols with SSH feature depends on your organization's policies.

Enabling secure operation involves configuring devices that support SSH functionality (servers and clients) to use SSH. Once enabled, secure operation can be disabled at any time by disabling individual components.

After the system components are appropriately set up for secure operation, system technicians can initiate secure login, command line, and file transfer sessions using one or more of the following methods depending on the device being accessed and/or ASTRO® 25 configuration management applications:

- Pre-installed SSH utilities
- ASTRO® 25 configuration management applications
  - Configuration/Service Software (CSS)
  - Unified Network Configurator (UNC)
- SSH configuration functionality in other ASTRO® 25 communication system software applications

For more information, see the “Configuration” chapter.

NOTICE: Secure operation requires more bandwidth than clear operation.

1.2.1
Secure-Capable System Devices and Applications

The following table lists the devices in an ASTRO® 25 communication system that support secure operation using SSH. For information on the configuration procedures for each device, see the “Configuration” chapter.

NOTICE: The devices in the following table may not all be present in the system you are configuring. The devices in your system depend on the features implemented.

For details on differences between configurations in an ASTRO® 25 system, see the *Master Site Infrastructure Reference Guide*.

SSH communications are supported in ASTRO® 25 systems for trunking and conventional devices, for Integrated Voice Data (IVD) devices and High Performance Data (HPD) devices, and for devices in K, L, and M master site configurations.

Supported types of SSH connections are summarized in the following table in the column on the right. For more details about the device that is the SSH client and the device that is the SSH server for these connections, see SSH Connection Lists (Primary Cores and Sites) on page 217 and SSH Connection Lists – DSR Only on page 226.

Table 2: Secure-Mode Support by ASTRO 25 Devices

Type of ASTRO 25 System Device That Supports SSH	Comments:
Network Transport: HP switch LX terminal server Fortinet firewall Router or gateway (in an ASTRO® 25 system, the S6000, S2500, and GGM 8000 models support SSH). Console Telephony Media Gateway Peripheral Network Router Border Router	SSH configuration on these devices supports centralized configuration and service, if available in your system. The InReach (IR) terminal server does **not** support SSH.

Type of ASTRO 25 System Device That Supports SSH	Comments:
IP Services: Domain Controller (DC) InfoVista server Centralized Event Logging server Core Security Management Server (CSMS) BAR server (baseline or full functionality) IP Packet Capture	SSH configuration on these devices (except for the FMS) supports centralized backup and restore operations, if available in your system. SSH should be disabled by default on the Fortinet FortiManager. See the *Fortinet Firewall Manager* manual.
Network Management: Private Network Management Client Private Network Management Servers applications implemented on a Virtual Management Server (VMS): • Unified Network Configurator (UNC) server • Unified Network Configurator Device Servers (UNCDS): - UNCDS01 - UNCDS02 - UNCDS03 • User Configuration Server (UCS) • System Statistics Server (SSS) • Unified Event Manager (UEM) Server • Zone Statistics Server (ZSS) • Zone Database Server (ZDS) • Air Traffic Router (ATR) • Zone Controller (ZC) • MOSCAD NFM Graphical Master Computer (GMC) • License Manager MKM 7000 Console Alias Manager server (CAM)	SSH configuration on NM Clients supports centralized backup and restore services, other non-interactive secure operations, and interactive sessions with other devices. The UNCDS is a network configuration tool that provides controlled and validated configuration management of system devices. It works with the UNC allowing increased capacity of managed devices. A zone includes three UNCDS servers (UNCDS01, UNCDS02, UNCDS03).
Inter RF Subsystem Interface (ISSI) Services: ISSI 8000/CSSI 8000	The ISGW is the server application used to support for the Inter-RF Subsystem Interface/Console Subsystem Interface 8000 (ISSI 8000/CSSI 8000) feature. For details of ASTRO® 25 system configurations for the ISSI/CSSI 8000 feature, see the *Dynamic System Resilience Feature Guide* and the *ISSI 8000/CSSI 8000 Intersystem Gateway Feature Guide*.
ISSI.1 Network Gateway Site: (server applications implemented on a GAS):	SSH configuration on these devices supports interactive sessions with NM Clients.

Type of ASTRO 25 System Device That Supports SSH	Comments:
ISSI.1 Gateway Module Site Link Relay Module	
RF site devices (trunking and conventional): GTR 8000 base radio GCP 8000 site controller GPB 8000 Reference Distribution Module (RDM) GCM 8000 comparator **VPM-based devices:** SmartX Site Converter Telephone Media Gateway (in the Enhanced Telephone Interconnect subsystem) MCC 7500 Voice Processor Module (VPM) **NOTICE:** The Voice Processing Module (VPM) is the only component of the MCC 7500 console that supports SSH. Console devices other than the VPM-based MCC 7500 do not require a VPM, but may connect to one through SSH for the purpose of VPM diagnostics.	SSH configuration on these devices supports interactive sessions with Configuration/Service Software (CSS), Software Download Manager (SWDL), and interactive sessions with NM Clients. The following RF site device models do **not** support SSH: QUANTAR® station STR 3000 base radio ASTRO-TAC 9600 comparator PSC 9600 site controller
MLC devices: MLC 8000 Analog Comparator MLC 8000 Subsite Link Converter	SSH configuration on these devices supports interactive session for remote MMI access and non-interactive sessions with CT clients.
MOSCAD Network Fault Management (NFM): SDM3000 RTU SDM3000 Network Translator (SNT) Graphical Master Computer (GMC) Graphical Workstation (GWS)	SSH configuration on these devices and the SDM3000 Builder (SDMB) application support MOSCAD NFM services.
Data services: Packet Data Gateway (PDG)	SSH configuration on PDGs supports non-interactive secure operations, and interactive sessions with NM Clients. The following data device does not require SSH configuration: CAI Data Encryption Module (CDEM)
Key Management Subsystem: Authentication Center (AuC) server	SSH configuration on the AuC server supports centralized backup and restore services.

Type of ASTRO 25 System Device That Supports SSH	Comments:
Time and Frequency Reference Subsystem: TRAK devices: • 9100 • 8835-2M • 8835-3M	SSH configuration on these devices supports interactive sessions with TRAK configuration application.
Server Virtualization Subsystem: vCenter Appliance Virtual Management Server (ESXi/Hypervisor) Direct Attached Storage (DAS)	SSH configuration on these devices supports interactive sessions with NM Clients and Hypervisor Statistics collection.

1.2.2
Clear Mode and Secure Mode in ASTRO 25 Systems

A secure-capable device must be set up to function in both secure mode and clear mode to interact with devices that do not support secure operation. If clear protocols are disabled, such device rejects the connection request.

Also, during SSH configuration, both secure mode and clear mode must remain enabled on devices (such as the UNC server) that communicate with devices where secure mode is not yet enabled. After SSH configuration for those devices is complete, clear mode can be disabled on the UNC server if it is not required to continue communicating with any devices that do not support secure mode.

In an ASTRO® 25 system, many devices that do not require clear mode are configured by Motorola Solutions only to support secure mode. This includes the Network Management servers other than the UNC server, and the Packet Data Gateway. Default SSH keys are included in the initial installation of these devices so that SSH configuration is not required before they can communicate. The default keys get replaced during the processes required for SSH key rotation, which are provided in this manual.

The following devices support **secure protocol operation only**:

- Network Management Servers (with the exception of the UNC for transport interface)
- Generic Application Server
- Zone Controller
- Packet Data Router
- Console Alias Manager
- MLC 8000 devices
- ISSI.1 Network Gateway
- Intersystem Gateway
- Authentication Center Server
- Console Telephony Media Gateway
- Direct Attached Storage
- Virtual Management Server (ESXi/Hypervisor)
- Fortinet Firewall
- Centralized Event Logging Server

- IP Packet Capture
- Backup Server (baseline and full functionality)
- Core Security Management Server
- InfoVista
- Domain Controller
- vCenter Appliance

Chapter 2

SSH Theory of Operation

This chapter provides additional detail on how secure and clear protocols work in the context of your system.

2.1 SSH Server Role

An SSH connection is established between two devices that function as a server and client. In some cases, a device may serve both roles. The device that receives a connection request is referred to as the SSH server.

Configuring a device as an SSH server requires the following:

- **SSH Server Host Key:** The SSH server's host key uniquely identifies a server to SSH clients. The host key is stored on the server and consists of a private key and a public key. This public key must be stored in the known hosts list on the SSH client so that the client can authenticate the SSH server.
- **SSH Client Public Keys in Authorized List of Keys:** The public key from the non-interactive user account key pair that was generated on the SSH client must be stored in the authorized list of keys on the SSH server.
- **SSH Client Information for Password Authentication:** A user ID and password is required for each account that uses Password Authentication for interactive sessions if not previously configured. This information may be stored on a centralized authentication server.

2.2 SSH Client Role

An SSH client initiates a connection request and establishes a connection to an SSH server. The SSH client stores a list of known hosts locally and uses this list to authenticate the SSH server each time an SSH connection is made.

Configuring a network element as an SSH client requires the following:

SSH Client Known Hosts List(s)

The client's known hosts list must be populated with the host name and/or IP address and public portion of the SSH server host key, so that the SSH client can use it to authenticate the SSH server. There may be more than one known hosts list on an SSH client device. For example, the Network Management (NM) Client has known hosts lists for:

- Configuration/Service Software (CSS) (to communicate with RF site devices)
- ATIA Log Viewer (to communicate with Air Traffic Routers)
- PuTTY (to communicate with any SSH-enabled device that is accessible in the system)

SSH Client User Keys

For non-interactive accounts, configuring a network element as an SSH client also requires the non-interactive user account on the SSH client to be configured with a key pair consisting of a private key and a public key. The SSH server needs to store the public key in its authorized list of keys in order to authenticate this user.

2.3 SSH Operational Modes

When securing protocols with SSH is implemented for the ASTRO® 25 communication system, the following configurable parameters are used to determine whether the communication between two devices occurs in secure mode (using SSH) or clear mode (without SSH):

- Clear protocol enable/disable
- Secure protocol enable/disable

These parameters are independently configurable on each device that supports secure and clear protocols. Enabling one variable and disabling the other allows only the class of protocols enabled and denies the disabled protocols. For example, if the clear protocol variable is set to enable and the secure protocol variable is set to disable on a client and server, then the communication between the two devices will be in the clear mode. Enabling both variables allows a host to use both the protocols. Disabling both variables results in the host denying all transfer and remote command operations.

The following table lists the various combinations of secure mode and clear mode settings and their impact on device operation.

Table 3: Secure and Clear Configurations

SSH Server		SSH Client		Protocol Used
Secure	**Clear**	**Secure**	**Clear**	
Disabled	Enabled	Disabled	Enabled	Clear
Enabled	Enabled	Disabled	Enabled	Clear
Enabled	Enabled	Enabled	Enabled	Secure or Clear (see below)
Enabled	Enabled	Enabled	Disabled	Secure
Enabled	Disabled	Enabled	Disabled	Secure
Enabled	Disabled	Enabled	Enabled	Secure

If configured for both clear and secure protocols, the SSH server establishes a connection based on the protocol that is initiated by the client. If configured for secure protocol operation only (that is, clear protocols are disabled), the SSH server rejects any clear protocol connection requests that it receives.

NOTICE: A combination of clear and secure protocols is required during implementation of the SSH feature in a system. Once SSH implementation is complete in the system, all clear protocols can be disabled if needed. However, if there are devices in the system that do not support SSH, the device accepting the connection (that is, the SSH server) must have both clear and secure settings enabled to ensure smooth system operation.

The following secure and clear configurations are not supported and result in a failure to establish a connection between the SSH server and client:

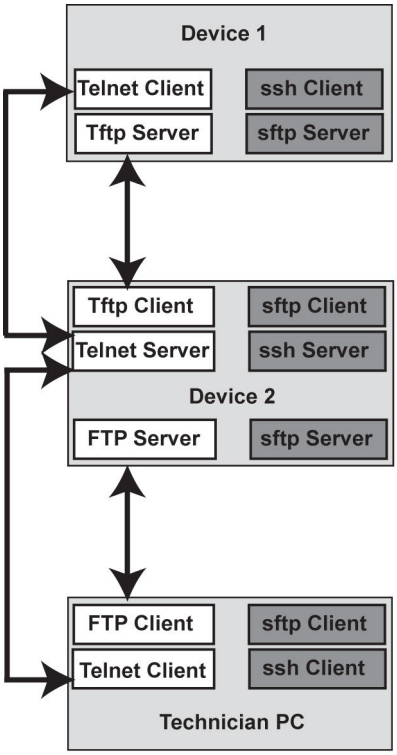
- Disabling *secure* and disabling *clear* on the same device (many devices in an ASTRO® 25 communication system are configured to prevent disabling of both secure and clear protocols)
- Enabling *secure* on the SSH server and enabling *clear* on the SSH client
- Enabling *clear* on the SSH server and enabling *secure* on the SSH client

2.4

Secure and Clear Communication Flow

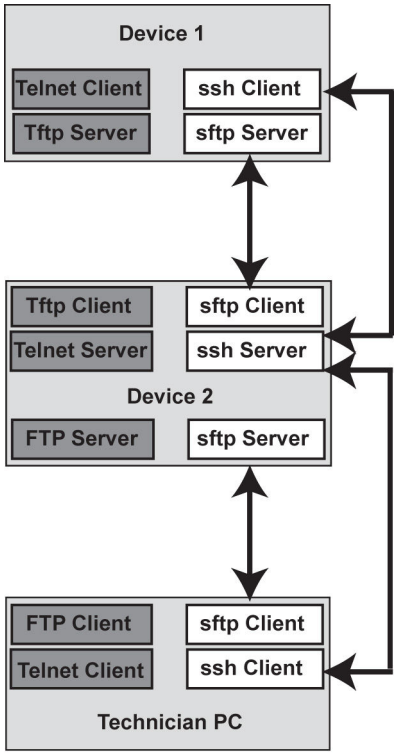
The diagrams in this section show secure and clear communication methods.

Figure 1: Clear Communication Methods



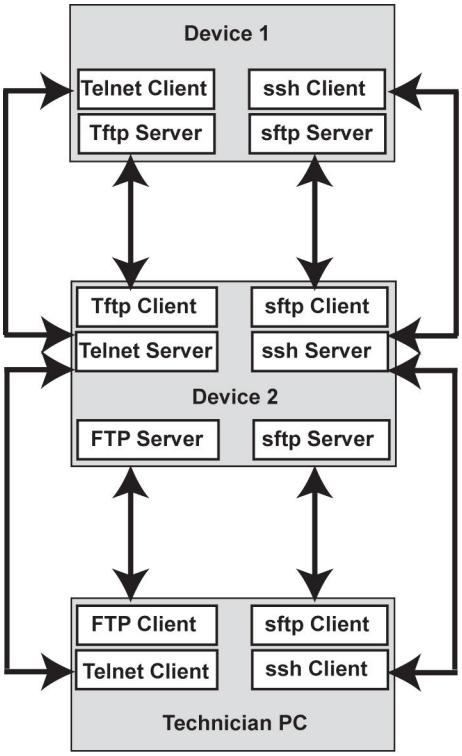
Secure_Protocol_Disabled_Clear_Enabled.

Figure 2: Secure Communication Methods



Secure_Protocol_Enabled_Clear_Disabled.

Figure 3: Clear and Secure Communication Methods



Secure_Protocol_Enabled_Clear_Enabled.

2.5 SSH Authentication Methods

The Securing Protocols with SSH feature in an ASTRO® 25 communication system supports the two types of authentication methods based on the type of session being initiated (interactive or non-interactive):

- “Public Key Authentication for Non-Interactive SSH Sessions”
- “Password Authentication for Interactive SSH Sessions”

2.5.1 Public Key Authentication for Non-Interactive SSH Sessions

Public key authentication is used for non-interactive sessions such as batch jobs and automated scripts. This ensures that the SSH client (user account) setting up the connection is allowed to establish such a connection. It also ensures that the SSH server is known to the SSH client.

- **SSH client user keys:** In order to use public key authentication to validate the client, the public key for the non-interactive user account (from the generated public/private key pair on the SSH client) must also be stored at the SSH server. The public key must be stored in a specific location (for example, file, directory, or database) containing the authorized keys for the specific user. This location is pre-configured during installation.
- **SSH server (host) keys:** A public/private key pair is generated at the SSH server (host) and the public host key is added to the SSH client’s known hosts list.

2.5.1.1

Key Management

Key management includes the following concepts:

Key generation

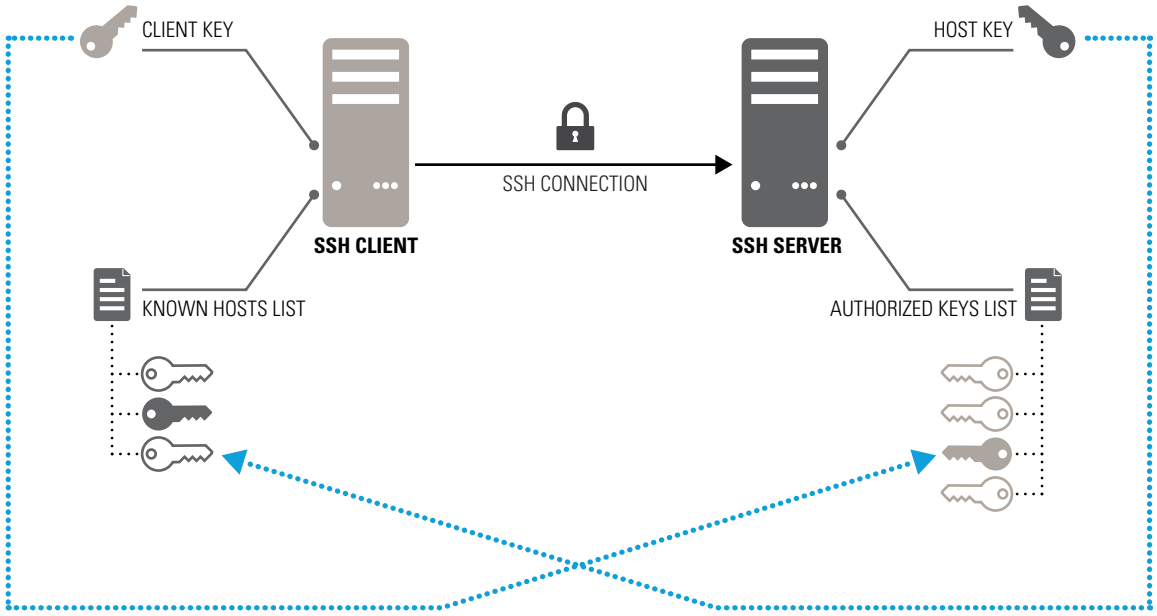
The process of generating the public/private key pairs. Keys can be generated locally or remotely or both depending on the device. The key pair can be generated on the server, or it can be generated externally and copied to the server over a secure connection.
For information on the key generation procedures, see the “Configuration” chapter.

Key rotation

The process of deleting existing keys and generating/propagating new keys. When SSH client (user) keys are generated, the SSH server’s list of authorized keys must be updated. When SSH server (host) keys are generated, the SSH clients known hosts list must be updated.

The following figure shows the basic SSH key rotation concept.

Figure 4: Basic Key Rotation Concept



For more information on key rotation, see SSH Key Rotation for Devices Using Default Keys Overview on page 61.

An administrator may delete established key pairs and reestablish them at any time if required by system policies (see the “Configuration” chapter for procedures). Once keys are changed, the new keys are used for new SSH connections. Existing SSH sessions continue undisturbed. Services which do not depend on SSH are not affected by the change.

2.5.1.1.1

SSH Key Specifications

The Secure Shell (SSH) feature in an ASTRO® 25 communication system uses keys based on the following algorithms:

Rivest Shamir Adleman (RSA)

RSA is the preferred algorithm. You can configure the RSA key size to provide flexibility in meeting security policies, requirements, and/or standards.

Digital Signature Algorithm (DSA)

Primarily used for fallback/failure scenarios.

Per FIPS and NIST standards, the minimum recommended key size is 2048. For details, see the applicable FIPS and NIST Standards at: http://csrc.nist.gov/publications/PubsFIPS.html and http://csrc.nist.gov/publications/PubsSPs.html. Applicable references include, but are not limited to, NIST SP800-131A and NIST SP800-57.

2.5.1.2
Known Hosts List – Located on SSH Clients

An SSH clients known hosts list contains the public keys for all hosts with which the client can communicate. This list can be populated as follows:

- Remotely over a secure connection and/or locally depending on the device.
- Through a script or utility prior to connecting to the server.
- Through a prompt upon connecting to the server if the servers host key does not reside in the known hosts list. The user may then choose to accept and automatically add the server (host name and public key) to the known hosts list or reject the connection attempt.

See the “Configuration” chapter for procedures on how to populate known hosts lists.

2.5.1.3
Authorized List of Keys – Located on SSH Servers

An authorized list of keys for SSH non-interactive user accounts is maintained on the SSH server.

See the “Configuration” chapter for procedures on how to populate the authorized list of keys when new SSH non-interactive user keys are generated.

2.5.2
Password Authentication for Interactive SSH Sessions

For interactive SSH sessions, public host keys are used by SSH clients to authenticate the SSH servers (hosts), and passwords are used to authenticate the SSH user. Password authentication uses existing user authentication methods. No additional configuration is required for SSH for this method of authentication.

See the following ASTRO® 25 communication system manuals for the authentication methods used in ASTRO® 25 communication systems:

- *Authentication Services* (regarding Active Directory and RADIUS authentication methods)
- Individual device manuals (regarding local authentication)

2.6
SSH Configuration Data Integrity

Devices and applications retain SSH key values during device initialization and reset. For many devices, SSH configuration data is stored in non-volatile memory.

The SSH configuration data and settings such as the key pairs, host files, and operational mode are backed up using any of the following methods, which may depend on the device:

- Using centralized backup, if the feature is implemented for that device (see the *Backup and Restore Services* manual)
- Using the Configuration/Service Software (CSS) application for devices it supports, to read the configuration from the device and create an archive file (see *Core CSS Online Help*), and to backup/restore known hosts lists
- Local backup and restore methods for the device

2.7 SSH Session Integrity

Modifications in SSH server/client configuration, secure enable/disable state changes, server keys, and client keys do not impact SSH sessions that were initiated prior to the change. The new configuration data and settings are used for new connections established after the changes are made.

2.8 SSH References

For information on the processes that occur on SSH clients and the SSH servers to accomplish secure communications, see the following documentation:

- *The Secure Shell (SSH) Protocol Architecture, RFC4251*
- *The Secure Shell (SSH) Authentication Protocol, RFC4252*
- *The Secure Shell (SSH) Transport Layer Protocol, RFC4253*
- *The Secure Shell (SSH) Connection Protocol, RFC4254*
- *Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol, RFC4419*

Chapter 3

SSH Installation

This chapter is for installation procedures relating to the Securing Protocols with SSH feature.

3.1 Devices with SSH Utilities Pre-Installed

For platforms other than Windows in an ASTRO® 25 communication system, SSH utilities, such as OpenSSH and SunSSH, are made available without requiring a separate installation procedure.

For Windows-based devices in an ASTRO® 25 communication system, PuTTY is the utility that is certified for initiating interactive sessions in Secure Shell (SSH) or other protocols. PuTTY can be installed on Windows-based devices as needed, using Installing Motorola Solutions PuTTY on Windows-Based Devices on page 40.

3.2 Installing Motorola Solutions PuTTY on Windows-Based Devices

PuTTY is, by default, automatically installed on an NM Client. However, if it is not installed, use this procedure to install it.

When and where to use:
For Windows-based devices that do not already have PuTTY installed, the application can be installed as needed.

NOTICE:
This procedure installs a version of PuTTY customized by Motorola Solutions.

The Motorola Solutions customization adds a version of PuTTYgen that is modified for the Microsoft Windows operating systems used in ASTRO® 25 systems. Command syntax and details are included in a “Motorola Changes” topic in the *PuTTY User Manual* included in the PuTTY installed files. `PuTTY.exe` and other PuTTY tools that are installed in this procedure have not been customized by Motorola Solutions. See the *PuTTY User Manual* for instructions on these other tools.

Procedure:

1. Insert the *Windows Supplemental* media into the drive of the Windows-based device.

   IMPORTANT: If you are installing 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 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 the Windows-based device with administrator privileges.
3. To uninstall a previous version of PuTTY on Windows 7 and Windows 10:
   a. From **Start**, open **Control Panel**.
   b. Click **Programs** → **Programs and Features** → **Uninstall a program**
   c. From the list of programs, select **Motorola PuTTY**. Click **Uninstall** above the list.
4. Open the command prompt window.

5 Navigate to the `\WIF` directory on the CD/DVD drive.

6 Enter: `WindowsInstallFramework.exe /e /i` ***<feature.xml>***

Where ***<feature.xml>*** is `"Motorola PuTTY.xml"`

To install other features at the same time, you can add more ***<feature.xml>*** parameters, depending on whether the following features are implemented in your ASTRO® 25 system:

- `"Motorola WinSCP.xml"` installs the WinSCP utility.

  For information, see http://www.winscp.net.

- `"Motorola Windows Bar Client.xml"` installs the Backup and Restore (BAR) client application.

  This applies only to domain controllers and Authentication Center servers, unless you have implemented the backup feature for all Windows-based BAR clients in your system.

  For details, see the *Backup and Restore Services* manual.

- `"Motorola Windows Logging Client.xml"` installs the Event Logging client application, if you have implemented the Centralized Event Logging feature in your system.

  For details, see the *Centralized Event Logging* manual.

7 Click **Finish**.

The **PuTTY** utility and the *PuTTY User Manual* are available by navigating to the list of programs on your computer, and selecting:

- For Windows 7: **Motorola** → **Motorola PuTTY**
- For Windows 10: **Motorola**

.

8 Remove the media from the drive.

9 Optional: Create a shortcut on the desktop to the PuTTY application, which is located at:

<systemdrive>`:\Program Files (x86)\Motorola\Motorola PuTTY\bin\PuTTY.exe`

This is recommended if you need to use the application to initiate multiple sessions because the PuTTY application window automatically closes each time it initiates a session.

Chapter 4

SSH Configuration

This chapter provides configuration processes and procedures for configuring the Securing Protocols with SSH feature on an ASTRO® 25 communication system. Do not perform tasks in this chapter that are designated for:

- Components that are not present in your system.
- Backup Clients not supported in your system (for example, if your system includes the *baseline* centralized backup and restore feature, do not perform the SSH tasks for the devices listed as Backup Clients that are not supported by the *baseline* feature).

NOTICE: It is recommended to create checklists for these tasks customized for your system configuration. You can use the processes in this chapter as a basis for your checklists.

4.1 ASTRO 25 System SSH Configuration Considerations

The following considerations must be taken into account when configuring SSH:

- Procedures for configuring SSH in an ASTRO® 25 communication system should be performed only by personnel with advanced expertise in operating system commands, in SSH, and in ASTRO® 25 communication system configuration. Performing a single step incorrectly can result in minimizing system availability.
- Only authorized users are permitted to change secure and clear operational modes, and SSH keys. See the configuration procedures for the account privileges needed by the users performing the procedures. Before performing the procedures, ensure that the passwords for each account are available. For passwords, contact your system administrator.
- If clear protocols are disabled on a device, subsequent configuration changes can only be made over a secure connection. The processes provided in this documentation ensure that clear protocols are disabled on a device only when they are no longer needed for configuration changes, so that the processes can be used for initial setup or full recovery of a system before it becomes operational. Review these processes to see if you can perform the procedures remotely. Your organizations policies may require that some procedures be performed locally if clear protocols are still enabled.
- If clear protocols are disabled on a device, that device cannot communicate with devices that do not support secure protocols. Before disabling clear protocols, see the “Description” chapter for a list of devices in an ASTRO® 25 communication system that do not support SSH. To determine what is connected to those devices in your system, see the appropriate ASTRO® 25 communication system manuals and talk to your system administrator.

  NOTICE: When devices configured with CSS do not match the secure/clear setting in the UNC, the devices will be marked as non-compliant. The UNC will move the device back to the state configured in the UNC pending approval by the user. It is recommended to use the UNC for SSH configuration steps.
- For additional considerations, see SSH Key Rotation Impact on ASTRO 25 System Non-Interactive Services on page 208 and other topics in the "Operation" chapter and "Troubleshooting" chapter.

4.2 Secure Operation in an ASTRO 25 System

Configuring a system for secure operation involves:

- Identifying the hosts which can use the secure protocols
- Creating new SSH keys for SSH servers and SSH clients
- Updating the known hosts list on SSH clients with the new SSH server keys
- Updating the authorized keys list on SSH servers with the new SSH client keys
- Ensuring that secure protocols are enabled on each device
- Ensuring that clear protocols are disabled on each device that communicates only with devices that support secure protocols (if it communicates with any devices that do not support secure protocols, then clear and secure must both be enabled)

For general information about these concepts, see SSH Theory of Operation on page 33.

Configuring a system for secure operation involves performing procedures on the following devices hosted on Virtual Management Servers (Linux-based):

- Air Traffic Router (ATR)
- Unified Event Manager (UEM) Server
- System Statistics Server (SSS)
- Zone Database Server (ZDS)
- Zone Statistics Server (ZSS)
- Unified Network Configurator (UNC) Server
- Unified Network Configurator Device Servers (UNCDS)
- Zone Controller (ZC)
- MOSCAD NFM Graphical Master Computer (GMC)
- Packet Data Gateway (PDG)
- License Manager

4.3 Configuring the ASTRO 25 System for Secure Operation

The following process lists the steps to be followed for configuring the devices in the ASTRO® 25 system for secure operation.
The sequence in the following process and in each step has been carefully planned to maximize system availability. This sequence ensures that SSH servers are configured before SSH clients, that secure mode is enabled at the correct point in the process, and that clear mode is disabled at the correct point in the process.

Prerequisites:

IMPORTANT: Ensure that the initial installation and configuration of the devices was completed up to the SSH configuration step in the configuration process for each device. For initial installation and configuration processes, refer to the ASTRO® 25 system manual for each device.

Obtain the following information from your system administrator:

- Password for the root account for each device configured in these procedures
- Username and passwords for the interactive account that is a member of the appropriate Active Directory user groups to log on to the devices in these procedures
- IP addresses, hostnames, and Fully Qualified Domain Name (FQDN) of each device in each zone as required in these procedures

If you are implementing the Dynamic System Resilience (DSR) feature:

- Obtain the hostnames, IP addresses, account names, and passwords for the backup core devices in your system before proceeding to the DSR sequences.

  For information about DSR backup core configurations, see your system plan and the ASTRO® 25 system *Dynamic System Resilience Feature Guide*.
- The zone core steps prior to step 11 in the following process apply to the primary core devices, not a DSR backup core.
- On an existing system that already had the SSH feature configured for the primary core and remote sites, skip to the DSR step (step 11) in the following process.

For additional configuration considerations regarding periodic key rotation, see SSH Operation on page 208.

Process:

1. Only if the centralized Backup and Restore service is implemented in your system, and only for the supported Backup Clients, configure SSH for centralized Backup and Restore.

   See Configuring SSH for Centralized Backup and Restore on page 45.
2. Configure SSH for devices at the Zone Core.

   See Configuring SSH for Devices at the Zone Core on page 47.
3. Perform the following SSH configuration processes:

   a. Configuring SSH for Devices at an RF Site on page 50

   b. Configuring SSH for Devices at an ISSI.1 Network Gateway Site on page 52
4. Configure SSH for devices at a Dispatch Site.

   See Configuring SSH for Devices at a Dispatch Site on page 53.
5. Configure SSH for MOSCAD NFM devices.

   See Configuring SSH for MOSCAD Network Fault Management (NFM) Devices on page 56.
6. Configure SSH for Transport Network Devices.

   See Configuring SSH for Transport Network Devices on page 58.
7. Configure SSH for Console Telephony Media Gateway.

   See Configuring SSH for Console Telephony Media Gateway on page 59.
8. Configure SSH for MCC7500 Aux I/O server.

   See Configuring SSH for MCC7500 Aux I/O Server on page 60.
9. **For a multizone system:** repeat the preceding processes for other zones.
10. Rotate SSH keys on devices using default keys.

    See SSH Rotation on Devices Using Default Keys on page 60.
11. **For DSR systems only:** perform additional SSH DSR configuration.

    See Performing Additional SSH Configuration Processes for DSR Systems on page 68.
12. **For DSR and non-DSR systems:** remove remaining SSH default keys.

    See Removing Remaining SSH Default Keys on page 75.

    NOTICE: This process includes as its final step an SSH connectivity verification for all servers involved.
13. Disable Clear protocols.

    See Disabling Clear Protocols on page 76.
14. Back up a baseline SSH configuration.

See Backing Up a Baseline SSH Configuration on page 78.

4.3.1
Configuring SSH for Centralized Backup and Restore

The ASTRO® 25 system centralized Backup and Restore (BAR) service supports secure mode only. The Windows-based and Linux-based BAR Clients only operate in secure mode, whether or not SSH is being enabled throughout your system. However, if required by your organizations policies, you must perform BAR SSH client key provisioning to all of the BAR Clients, to replace the default client keys.

NOTICE:
BAR Server host keys will be automatically provisioned to BAR Clients as part of the BAR registration mechanism.

ISSI.1 and PS LTE devices listed in Secure-Capable System Devices and Applications on page 28 are **not** supported by the Backup and Restore (BAR) service.

Prerequisites: Complete all installation and configuration for the BAR Server and BAR Clients. Instructions for prerequisite BAR server and BAR client tasks are located in the *Backup and Restore Services* manual, and in the manuals specific to individual BAR Client devices.

When and where to use:
This process:

- Lists the steps to be followed for configuring SSH for the centralized backup and restore feature for the ASTRO® 25 system.
- Includes all the tasks required if the full functionality BAR service is implemented in your system. If your system includes the “baseline” centralized BAR service that is limited to Linux-based BAR Clients, domain controllers, and Authentication Center (AuC) servers, do **not** perform the tasks that are designated for other BAR Clients. (Also, do **not** perform Backup Client tasks designated for other optional components that are not present in your system.)

  IMPORTANT: When performing the process for the backup core in systems with the Dynamic System Resilience (DSR) feature implemented, be sure that you are using the Backup Server and Backup Clients in the DSR backup core, not in the primary core.
- Configures SSH for non-interactive SSH sessions between the BAR Server and BAR Clients, but that does **not** provide the SSH functionality needed for interactive SSH sessions with other devices. To set up interactive sessions, see sections in the "Configuration" chapter for the types of devices which require interactive SSH sessions.
- With the exception of the Console Alias Manager (CAM) server located at the dispatch site, this process assumes that the Backup Server and all of its Backup Clients reside at the same geographic location and the Backup Server only supports one zone core. For the SSH configuration process for the Console Alias Manager (CAM) server, see Configuring SSH for Devices at a Dispatch Site on page 53.

Process:

1 Create a new host key (server key pair) for the Backup Server.

See Generating New SSH Host Keys on a Backup Server on page 79.

NOTICE:
This also automatically updates known host lists for BAR-related accounts on the Backup Server.

This BAR Server host key is automatically provisioned to the Backup Clients the next time they register with the BAR Server (which occurs in step 5), or as part of provisioning SSH client keys to Backup Clients in step 2.

2 If your organizations policies prohibit the use of the default Backup Client registration keys, perform the following:

   a Create new SSH client keys on the Backup Server.

   See Generating New SSH Client Keys on a Backup Server on page 80.

   This also automatically updates the authorized client key list on the Backup Server.

   b For the following Backup Client devices, replace the default registration key (the client's default SSH user key) with the new keys generated in the previous step:

   - Backup Server, see Updating SSH Client Keys for Accounts on the Backup Server on page 81

     NOTICE: This step is required because SSH is used for communication between the Backup Server and other Backup-related applications that reside on the same device.

   - The following servers:
     - NM servers (ATR, ZDS, ZSS, UCS, SSS, UEM, UNC, UNCDS)
     - ZC (including each Tsub, if present)
     - ISGW (ISSI 8000/CSSI 8000)
     - PDG
     - License Manager

     see Performing the Secure Transfer of the SSH Client Key to Linux-Based Backup Clients on page 82

   - Centralized Event Logging server (if present in the system), see Performing the Secure Transfer of the SSH Client Key to Linux-Based Backup Clients on page 82
   - IP Packet Capture (if present in the system), see Performing the Secure Transfer of the SSH Client Key to Linux-Based Backup Clients on page 82
   - NM Client, DC, AuC server, InfoVista, GMC, GWS (if present in the system), CSMS, see Performing the Secure Transfer of the SSH Client Key to Windows-Based Backup Clients on page 83

   c Disable default key usage at the Backup Server.

   See Disabling Default SSH Key Usage on page 86.

   The default user key being removed from the Backup Servers authorized list of keys

3 Optional: If the Console Alias Manager (CAM) at the Dispatch Sites is utilizing backup and recovery, it is not able to connect to the BAR Server once default key usage is disabled. If this is not acceptable, proceed with updating the CAM server with the new registration key prior to disabling default key usage or defer disabling default key usage until after the CAM update steps.

   See Configuring SSH for Devices at a Dispatch Site on page 53.

4 Verify that a connection using SSH can be interactively established to the Backup Server from installer/maintainer positions (such as NM Clients).

   See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

   When prompted to add the server to the known hosts list, accept the host.

5 Verify the non-interactive account configuration by establishing a secure connection between the Backup Server and the following Backup Clients:

- InfoVista, DCs, AuC server, GMC, GWS (any that are present in this zone core), CSMS, Backup Server accounts
- The following servers:
  - NM servers (ATR, ZDS, ZSS, UCS, SSS, UEM, UNC)
  - ZC
  - ISGW (ISSI 8000/CSSI 8000)
  - PDG
  - License Manager
- Centralized Event Logging server (if present in the system)
- IP Packet Capture (if present in the system, including each Tsub)
- NM Client

See SSH Configuration Verification for Backup Clients on page 84.

Related Links

Configuring the ASTRO 25 System for Secure Operation on page 43

4.3.2 Configuring SSH for Devices at the Zone Core

When and where to use:
When performing the procedures in this section for the backup core in systems with the Dynamic System Resilience (DSR) feature implemented, be sure that you are performing the procedures in this process on the devices in the DSR backup core, not in the primary core. Additional notes about DSR considerations are included in the appropriate steps.

ISGWs, ZCs, License Manager, and NM servers at the zone core are not configured as part of this process. These devices are configured later, in SSH Key Rotation for Devices Using Default Keys Overview on page 61.

MOSCAD Network Fault Management (NFM) devices at the zone core are not configured as part of this process. These devices are configured later, in Configuring SSH for MOSCAD Network Fault Management (NFM) Devices on page 56.

Process:

1. Generate a new host key (server key pair) for the Packet Data Gateway (PDG):
   a. Log into the Packet Data Router (PDR) module of the PDG.
   b. Execute the command to generate a new SSH host key.

      See Host Key Generation on SSH Servers on page 111.

      NOTICE: For optimal security, record the fingerprint when generating each key, to use later in the process.
2. Perform the following actions:
   a. Generate a new host key (server key pair) for the following Linux-based devices if they are present in the zone core:
      - Centralized Event Logging server (any that are present in this zone core or this zone cores ZCP mediation LAN)
      - IP Packet Capture

      See the commands to generate new server keys in Host Key Generation on SSH Servers on page 111.

NOTICE: For optimal security, record the fingerprint when generating each key, to use later in the process.

b Verify that an SSH connection can be made from the NM Client to the Linux-based devices listed above. See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

When prompted to add the server to the known hosts list, accept the host.

3 If a terminal server is present in the zone core, perform the following steps:

a Generate a new host key (server key pair) for the terminal server. See Terminal Server SSH Server (Host) Keys Management on page 191.

NOTICE: For optimal security, record the fingerprint when generating each key, to use later in the process.

b Enable secure protocol operation for the terminal server. See Commands for Enabling/ Disabling Secure Mode on the Terminal Server on page 190.

c Verify that an SSH connection can be made from the NM Client to the terminal server in the zone core. See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

When prompted to add the server to the known hosts list, accept the host.

NOTICE: When performing the DSR SSH configuration procedures, do not regenerate keys on a terminal server that is shared between a primary core and a backup core (these keys need to stay the same for SSH connections with primary core devices that were already configured).
In that case, proceed to the verification step for the terminal server.

4 Generate a new host key (SSH server key pair) and enable secure protocols operation for the following network transport devices:

- HP switches. See Generating Initial SSH Host Keys and Enabling Secure Mode for HP Switches Using VoyenceControl on page 165 or SSH Configuration on HP Switches Using Commands on page 183
- Motorola routers and gateways. See Generating Initial SSH Host Keys and Enabling Secure Mode for Routers and Gateways Using VoyenceControl on page 165 or SSH Configuration on Routers and Gateways Using Commands on page 185

NOTICE: When performing the additional SSH configuration procedures required for implementing DSR, do not regenerate SSH keys on transport devices that are shared between a primary core and a backup core (these keys need to stay the same for SSH connections with primary core devices that were already configured).
In that case, proceed to the SSH verification step for the transport device (step 5 or step 6).

The following transport devices are shared between a primary core and a backup core located at the same master site: Exit Routers, Gateway Routers, GGSN Routers, Core LAN Switches, Mediation LAN Switches, IDS LAN Switch, Fan-out LAN Switches

However, for an Exit Router that was added as part of a single-zone DSR implementation, you need to perform the key generation and secure mode procedure listed below.

NOTICE: If the Unified Network Configurator (UNC) is used to perform this step (assuming your organization's policy permits configuration using clear protocols), it is permissible to use UNC to configure switches, routers, and gateways at RF Sites and Dispatch Site at this time, in addition to the switches and routers at the zone core. This includes all of the procedures from here to the end of this zone core process.

5 Optional: For the following network transport devices, enable secure mode for management of the device by the Unified Network Configurator (UNC) and verify the SSH connection from the UNC to the devices:

- HP switches
- Motorola routers and gateways

This also adds the devices to the UNC servers known hosts list.

See Enabling SSH/SCP Management Mechanism in Device Properties in VoyenceControl on page 176 and Verifying Secure Mode/Updating Known Hosts List for UNC Management of a Device on page 177.

NOTICE: The SSH configuration for these devices can be verified using either the UNC (step 5), if present in the system, or the NM Client (step 6).

6 Optional: Verify that an SSH connection can be made to the following network transport devices from an NM Client or technicians laptop:

- HP switches
- Motorola routers and gateways

See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

NOTICE: Only authorized NM Clients can initiate an interactive SSH session with these devices, as specified in the configuration files and ACLs for these devices.
For Motorola routers or gateways, an SSH session can be initiated only from NM Client 1, NM Client 2 (if present), NM Client 3 (if present), NM Client 33 (if present in a DSR backup core), NM Client 34 (if present in a DSR backup core), or NM Client 35 (if present in a DSR backup core).

For HP switches in a system without the DSR feature, an SSH session can be initiated only from NM Client 1, or NM Client 2 (if present). In a system with DSR, an SSH connection with an HP switch can be initiated by all NM Clients in the same zone or paired zone.

7 Generate a new host key (server key pair), enable secure protocol operation, and add the host key to the CSS known hosts list, for the Telephone Media Gateway (TMG) if present in the system. See Configuring Secure Services/Keys and Clear Services Using CSS on page 156 and Adding a Device to the CSS Known Hosts List on page 159.

Be sure to enable Secure Shell Service, Secure FTP Service, and Secure Terminal Service. When prompted to add the server to the known hosts list, accept the host.

NOTICE: Enabling Secure Shell Service automatically generates new host keys on the device.
Adding the server to the known hosts list verifies the sftp connection between CSS and the device.

When devices configured with CSS do not match the secure/clear setting in the UNC, the devices will be marked as non-compliant. The UNC will move the device back to the state configured in the UNC pending approval by the user. It is recommended to use the UNC for SSH configuration steps.

8 Verify that an SSH connection can be made from a technician's laptop or NM Client to the TMG, if present in the system.

See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

When prompted to add the server to the known hosts list, accept the host.

9 Generate new host key for the vCenter Appliance.

See Generating SSH Keys on a vCenter Appliance on page 188.

10 Perform the following actions for the Virtual Management Server (ESXi/Hypervisor):

   a Generate new host key for the VMS.

   See Generating SSH Keys on a Virtual Management Server (ESXi/Hypervisor) on page 189.

   b Add the VMS host key to the IP Packet Capture known hosts list.

   See Updating Known Hosts List on an IP Packet Capture for Connections to a VMS on page 189

11 Verify successful SSH connection can be made from an NM Client to DAS.

   See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

   When prompted to add the server to the known hosts list, accept the host.

12 Verify successful SSH connection can be made from an NM Client to vCenter Appliance.

   See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

   When prompted to add the server to the known hosts list, accept the host.

13 Verify successful SSH connection from NM Client to the Virtual Management Server (ESXi/Hypervisor).

   See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

   When prompted to add the server to the known hosts list, accept the host.

14 Verify Hypervisor Statistics Service operation.

   Check the UEM for faults from IPCAP running on the VMS.

Related Links

Configuring the ASTRO 25 System for Secure Operation on page 43

4.3.3
Configuring SSH for Devices at an RF Site

These procedures do not necessitate a site visit if remote configuration using clear protocols is permitted by your organizations policies. Otherwise, a site visit may be required if the referenced procedure does not provide a secure alternative for remote configuration.

Process:

1 Generate a new host key (server key pair), enable secure protocol operation, and add the host key to the CSS known hosts list, for the following devices (in any order):

   - All GTR 8000 base radios
   - All GCP 8000 site controllers
   - All GPB 8000 Reference Distribution Modules
   - All GCM 8000 comparators

   See Configuring Secure Services/Keys and Clear Services Using CSS on page 156 and Adding a Device to the CSS Known Hosts List on page 159.

   Be sure to enable Secure Shell Service, Secure FTP Service, and Secure Terminal Service. When prompted to add the server to the known hosts list, accept the host.

NOTICE: Enabling Secure Shell Service automatically generates new host keys on the device.
Adding the device to the CSS known hosts list verifies the sftp connection between CSS and the device.

When devices configured with CSS do not match the secure/clear setting in the UNC, the devices will be marked as non-compliant. The UNC will move the device back to the state configured in the UNC pending approval by the user. It is recommended to use the UNC for SSH configuration steps.

2 Generate a new key (server key pair) for MLC 8000 devices.

See Changing Server SSH Public/Private Key Pair on an MLC 8000 Device on page 163.

3 Verify that an SSH connection can be made from a technicians laptop or NM Client to the following SSH server devices:

- All GTR 8000 base radios
- All GCP 8000 site controllers
- All GPB 8000 Reference Distribution Modules
- All GCM 8000 comparators

See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89. When prompted to add the server to the known hosts list, accept the host.

4 Perform the following actions:

a Verify successful SSH connection between technicians laptop with CT client and MLC 8000 devices.

For instructions regarding the connection between CT Client and MLC 8000 devices, see the *MLC 8000 Configuration Tool User Guide*.

b Verify successful SSH connection between technicians laptop and the remote MMI with PuTTY SSH Client. See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

When prompted to add the server to the known hosts list, accept the host.

5 Generate a new host key (server key pair), enable secure protocol operation, and add the host key to the CSS known hosts list, for the SmartX Site Converter (if implemented in the system, either at an RF site or at a master site).

See Configuring Secure Services/Keys and Clear Services Using CSS on page 156 and Adding a Device to the CSS Known Hosts List on page 159.

Be sure to enable Secure Shell Service, Secure FTP Service, and Secure Terminal Service. When prompted to add the server to the known hosts list, accept the host.

NOTICE:
Enabling Secure Shell Service automatically generates new host keys on the device.

Adding the device to the CSS known hosts list verifies the sftp connection between CSS and the device.

When devices configured with CSS do not match the secure/clear setting in the UNC, the devices will be marked as non-compliant. The UNC will move the device back to the state configured in the UNC pending approval by the user. It is recommended to use the UNC for SSH configuration steps.

6 Verify that an SSH connection can be made from a technicians laptop or NM Client to the SmartX Site Converter (if implemented in the system).

See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

When prompted to add the server to the known hosts list, accept the host.

7 Generate a new host key (server key pair), and enable secure protocol operation for the following devices (in any order), if present at the RF site:

- HP switches – see Generating Initial SSH Host Keys and Enabling Secure Mode for HP Switches Using VoyenceControl on page 165 or SSH Configuration on HP Switches Using Commands on page 183
- Motorola routers and gateways – see Generating Initial SSH Host Keys and Enabling Secure Mode for Routers and Gateways Using VoyenceControl on page 165 or SSH Configuration on Routers and Gateways Using Commands on page 185
- Terminal server – see Terminal Server SSH Server (Host) Keys Management on page 191 and Commands for Enabling/Disabling Secure Mode on the Terminal Server on page 190
- SDM3000 RTU – see Generating and Provisioning a New Host Key for an SDM3000 Hardware-Based Device on page 195

NOTICE: If your organizations policies restrict remote configuration, you must perform these procedures locally.
For these procedures, the SDM3000 Builder application can be loaded on a technicians laptop at the RF site. For installation instructions, see the *SDM3000 Builder User Guide* and the ASTRO® 25 system *MOSCAD Network Fault Management Feature Guide*.

The process sequences in this manual assume that you will perform these procedures locally, not from an SDM3000 Builder installation at the zone core.

8 Verify that an SSH connection can be made from a technicians laptop to the following SSH server devices at the RF site:

- HP switches
- Motorola routers and gateways
- Terminal server (if present at the RF site)
- SDM3000 RTU (if present at the RF site)

See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

When prompted to add the server to the known hosts list, accept the host.

NOTICE: For the network transport and MOSCAD NFM devices, additional SSH configuration is required, as indicated in SSH processes that follow.

9 Repeat this process for all RF Sites in the same zone.

Related Links

Configuring the ASTRO 25 System for Secure Operation on page 43

4.3.4
Configuring SSH for Devices at an ISSI.1 Network Gateway Site

This section lists the steps to be followed for configuring SSH on the ISSI.1 Network Gateway, if present in an ASTRO® 25 communication system.

Prerequisites: These procedures do not necessitate a site visit if remote configuration using clear protocols is permitted by your organizations policies. Otherwise, a site visit may be required if the referenced procedure does not provide a secure alternative for remote configuration.

Process:

1 Generate a new host key (server key pair) for the following ISSI.1 Network Gateway site modules (in any order):

- For ISSI.1 Gateway module, see Regenerating the SSH Host Keys on an ISSI.1 Gateway Module on page 153
- For Site Link Relay module, see Regenerating the SSH Host Keys on a Site Link Relay Module in an ISSI.1 Network Gateway Site on page 154

2 Verify that an SSH connection can be made from a technicians laptop or NM Client to the following ISSI.1 Network Gateway site modules (in any order):

- ISSI.1 Gateway module
- Site Link Relay module

See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

When prompted to add the server to the known hosts list, accept the host.

3 Generate a new host key (server key pair), and enable secure protocol operation for the following network transport devices (in any order):

- HP switch – see Generating Initial SSH Host Keys and Enabling Secure Mode for HP Switches Using VoyenceControl on page 165
- Motorola site router or gateway – see Generating Initial SSH Host Keys and Enabling Secure Mode for Routers and Gateways Using VoyenceControl on page 165 .

4 Verify that an SSH connection can be made from a technicians laptop to the following SSH server devices at the ISSI.1 Network Gateway site:

- HP switch
- Motorola routers and gateways

See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

When prompted to add the server to the known hosts list, accept the host.

NOTICE: For these network transport devices, additional SSH configuration is required, as indicated in SSH processes that follow.

Related Links

Configuring the ASTRO 25 System for Secure Operation on page 43

4.3.5
Configuring SSH for Devices at a Dispatch Site

This process lists the steps to be followed for configuring SSH for devices at a dispatch site in an ASTRO® 25 communication system.

Process:

1 Enable secure protocol operation for the following devices, if present at the site:

- Conventional Site Controller
- Conventional GTR 8000 Base Radio
- Conventional GCM 8000 Comparator

See Configuring Secure Services/Keys and Clear Services Using CSS on page 156 and Adding a Device to the CSS Known Hosts List on page 159.

Ensure to enable Secure Shell Service, Secure FTP Service, and Secure Terminal Service. When prompted to add the server to the known hosts list, accept the host.

NOTICE:
Enabling Secure Shell Service automatically generates new host keys on the device.

Adding the device to the CSS known hosts list verifies the sftp connection between CSS and the device.

When devices configured with CSS do not match the secure/clear setting in the UNC, the devices will be marked as non-compliant. The UNC will move the device back to the state configured in the UNC pending approval by the user. It is recommended to use the UNC for SSH configuration steps.

2 Verify that an SSH connection can be established from a technicians laptop or an NM Client to the following devices, if present at the site:

- Conventional Site Controller
- Conventional GTR 8000 Base Radio
- Conventional GCM 8000 Comparator

See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

When prompted to add the server to the known hosts list, accept the host.

3 Generate a new host key (server key pair), enable secure protocol operation and add the host key to the known hosts list, for the MCC 7500 Console Voice Processor Module (VPM). See Configuring Secure Services/Keys and Clear Services Using CSS on page 156 and Adding a Device to the CSS Known Hosts List on page 159.

Ensure to enable Secure Shell Service, Secure FTP Service, and Secure Terminal Service. When prompted to add the server to the known hosts list, accept the host.

NOTICE:
Enabling Secure Shell Service automatically generates new host keys on the device.

Adding the server to the known hosts list verifies the sftp connection between CSS and the device.

When devices configured with CSS do not match the secure/clear setting in the UNC, the devices will be marked as non-compliant. The UNC will move the device back to the state configured in the UNC pending approval by the user. It is recommended to use the UNC for SSH configuration steps.

4 Verify that an SSH connection can be made from a technicians laptop or NM Client to the MCC 7500 Console Voice Processor Module (VPM). See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89

When prompted to add the server to the known hosts list, accept the host.

5 Generate a new host key (server key pair) and enable secure protocol operation for the following devices (in any order):

- HP switches – see Generating Initial SSH Host Keys and Enabling Secure Mode for HP Switches Using VoyenceControl on page 165 or SSH Configuration on HP Switches Using Commands on page 183
- Motorola routers and gateways – see Generating Initial SSH Host Keys and Enabling Secure Mode for Routers and Gateways Using VoyenceControl on page 165 or SSH Configuration on Routers and Gateways Using Commands on page 185
- SDM3000 RTU, if present at the dispatch site – see Generating and Provisioning a New Host Key for an SDM3000 Hardware-Based Device on page 195

NOTICE:
If your organizations policies restrict remote configuration, you must perform these procedures locally.

For these procedures, the SDM3000 Builder application can be loaded on a local NM Client or technicians laptop at the dispatch site. For installation instructions, see the *SDM3000 Builder User Guide* and ASTRO® 25 system *MOSCAD Network Fault Management Feature Guide*.

The process sequences in this manual assume that you will perform these procedures locally, not from an SDM3000 Builder installation at the zone core.

6 Generate a new host key (server key pair) for Console telephony media gateway. See Using a Saved Command in VoyenceControl to Generate SSH Keys on Console Telephony Media Gateway on page 170 or Using Cisco IOS Command to Generate SSH Keys on Console Telephony Media Gateway on page 201

7 Verify that an SSH connection can be established from a technicians laptop or local NM Client at the dispatch site to the following devices at the dispatch site:

- Conventional Site Controller (if present at the dispatch site)
- SDM3000 RTU (if present at the dispatch site)
- HP switches
- Motorola routers and gateways
- Console telephony media gateway

See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

When prompted to add the server to the known hosts list, accept the prompt.

NOTICE: For the network transport devices, MOSCAD NFM devices, and Console telephony media gateway additional SSH configuration is required, as indicated in SSH processes that follow.

8 Update the “known host list” for the backup and recovery operation (to account for the latest host key generated on the Backup Server) for the Console Alias Manager (CAM). See Verifying SSH Configuration for Windows-Based Backup Clients on page 85.

9 Repeat all preceding steps for all dispatch sites in the same zone.

10 If you have a CAM Server and have purchased full backup and recovery functionality, and if your policy does not permit default client registration key usage for the backup and recovery operation, perform the following steps:

a Replace the default BAR client registration key on the CAM with a new (non-default) client registration key already present on the Backup Server. See Performing the Secure Transfer of the SSH Client Key to Windows-Based Backup Clients on page 83.

b Once the registration key has been replaced for CAM Servers at all Dispatch Sites in the zone, proceed with disabling default key usage at the Backup Server (at the primary core for this zone). See Disabling Default SSH Key Usage on page 86.

c Verify the non-interactive account configuration for all CAM Servers by establishing a secure connection between each CAM Server and the Backup Server. See Verifying SSH Configuration for Windows-Based Backup Clients on page 85.

d If not already performed with default key usage disabled at the Backup Server, verify the non-interactive account configuration for all other backup clients by establishing a secure connection between the backup client and the Backup Server. See SSH Configuration Verification for Backup Clients on page 84.

Related Links

Configuring the ASTRO 25 System for Secure Operation on page 43
Configuring SSH for Centralized Backup and Restore on page 45

4.3.6

Configuring SSH for MOSCAD Network Fault Management (NFM) Devices

This process lists the steps for SSH configuration for MOSCAD Network Fault Management (NFM) devices from the zone core.

When and where to use:
When performing the procedures for the backup core in systems with the Dynamic System Resilience (DSR) feature implemented, be sure that you are using the SDM3000 Builder, Graphical Master Computer (GMC), and Graphical Workstation (GWS) in the backup core, not in the primary core.

Appendix A and Appendix B tables list the SSH configuration that is needed for each SSH interface between MOSCAD NFM applications and devices. These checklists include configuration that occurs automatically and configuration that is performed interactively. For clarification of which configuration tasks are automatic and which are performed interactively, review the notes in the following steps.

SDM3000 RTUs can be supported by fault managers other than MOSCAD NFM.

Process:

1. In the SDM3000 Builder, set the SSH mode:
   a. From the Tools menu, select **Options**.
   b. In the **Options** window, click the **Security** tab.
   c. Clear the **Automatically Accept SDM3000's SSH Host Key** check box.
   d. To save the protocol settings, click **OK**.
2. Generate a new host key (server key pair).

   See Generating a New Host Key for the SDM3000 Builder on page 199.
3. Generate and provision a new host key (server key pair) for the following devices at the master site:
   - SDM3000 Network Translator (SNT)
   - SDM3000 RTU at the master site, if present

   See Generating and Provisioning a New Host Key for an SDM3000 Hardware-Based Device on page 195.

   IMPORTANT: When performing this process for a DSR backup core, you only need to perform this step for the SDM3000 RTU if there is an SDM3000 RTU in the backup core you are currently configuring.
   For example, in a two-core master site, there will not be an SDM3000 RTU in a ZoneY backup core if that backup core uses the SDM3000 RTU in the ZoneX primary core at the same physical master site. In that case, the SSH host key was already generated for the one SDM3000 RTU at the master site as part of SSH configuration for the ZoneX primary core, so you should *not* generate a new key for it again when configuring the ZoneY backup core located at the same master site.

   NOTICE: When you use the SDM3000 Builder to provision a new host key for the SDM3000 hardware-based device, the known hosts list in SDM3000 Builder is updated automatically with the device host key over a secure connection.

4 Use the zone core SDM3000 Builder to generate and provision a new SSH client (user) key for the following SDM3000 hardware-based devices:

- SDM3000 Network Translator (SNT) at the master site
- SDM3000 RTU at the master site, if present
- SDM3000 RTUs at RF sites
- SDM3000 RTUs at dispatch sites

See Generating and Provisioning a New SFTP Client Public Key Authentication Key Pair for an SDM3000 Hardware-Based Device on page 197.

IMPORTANT: When configuring SSH for a DSR backup core, do *not* perform this procedure for the primary core SNT, RF site SDM3000 RTUs, dispatch site SDM3000 RTUs, and any master site SDM3000 RTU that already had new SSH client keys generated during primary core SSH configuration.

NOTICE: SDM3000 Builder automatically updates its authorized list of keys when configuring a new user key at an SDM3000 hardware-based device.
In addition, the SDM3000 hardware-based device sends its public **host** key over the ssh connection for population of the known hosts list at the SDM3000 Builder. A fingerprint verification prompt will display if this is the first time you are connecting to the SDM3000 hardware-based device *from this SDM3000 Builder location* after generating SSH host keys on the device.

5 Verify the configuration update by establishing an SSH connection and initiating an sftp file transfer between the zone core SDM3000 Builder and the following devices:

- SDM3000 Network Translator (SNT)
- SDM3000 RTU at the master site, if present
- RF site SDM3000 RTU
- Dispatch site SDM3000 RTU

Use the Update Configuration Files function in SDM3000 Builder. For instructions, see:

- Secure Operation Verification Between SDM3000 Builder and an SDM3000 Hardware-Based Device on page 200
- *SDM3000 Builder Users Guide*

NOTICE: During this procedure, the SDM3000 hardware-based device sends its public host key over the ssh connection for population of the known hosts list at the SDM3000 Builder.
A fingerprint verification prompt will display if this is the first time you are connecting to the SDM3000 hardware-based device *from this SDM3000 Builder location* after generating SSH host keys on the device.

For example, a fingerprint verification prompt will occur if this is the first time you are connecting to an SDM3000 RTU at an RF site from SDM3000 Builder on a backup core GMC.

After the SDM3000 hardware-based device has been accepted in the SDM3000 Builder known hosts list, then the SDM3000 Builder authorized keys list is automatically updated with client keys from the device, over a secure connection.

6 Verify that an SSH connection can be established to the following devices from NM Client(s) where these devices were not already accepted as trusted hosts:

- SDM3000 Network Translator (SNT) at the master site
- SDM3000 RTU at the master site, if present
- SDM3000 RTUs at RF sites

- SDM3000 RTUs at dispatch sites

See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

When prompted to add the server to the known hosts list, accept the host.

7 If a QUANTAR® station or TeNSr devices are present at an RF Site and are managed by the GMC Application, connect to the RF Site SDM3000 RTU and Dispatch Site SDM3000 RTU from the zone core GMC, through the SSH connection provided by the GMC Application. See Adding SDM3000 RTU SSH Host Keys to the GMC and GWS Known Hosts Lists on page 201.

When prompted to add the server to the known hosts list (at the GMC), accept the prompt.

NOTICE: Repeat this step for any GWS present in the same core.

Postrequisites: See SSH Configuration for MOSCAD Network Fault Management (NFM) Devices on page 195.

Related Links

Configuring the ASTRO 25 System for Secure Operation on page 43

4.3.7

Configuring SSH for Transport Network Devices

This process lists the steps for SSH configuration for HP switches, Motorola routers and gateways, and TRAK devices at the zone core, RF sites, ISSI.1 sites, and dispatch sites in an ASTRO® 25 communication system. These procedures can be performed at the zone core.

When and where to use: These steps may be skipped if you opted to perform them earlier.

NOTICE: For multizone systems, after completing Configuring SSH for Transport Network Devices on page 58, repeat all the processes you have completed from Configuring the ASTRO 25 System for Secure Operation on page 43, for the next zone.

Process:

1 For the following network transport devices, enable SSH/SCP Management Mechanism in the properties for each device in VoyenceControl, and verify the SSH connection from the UNC to the devices (this also adds the devices to the UNC servers known hosts list):

- HP switches
- Motorola routers and gateways
- Terminal Servers
- TRAK devices

See Enabling SSH/SCP Management Mechanism in Device Properties in VoyenceControl on page 176 and Verifying Secure Mode/Updating Known Hosts List for UNC Management of a Device on page 177.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

2 Verify that an SSH connection can be made to the following network transport devices from an NM Client or technicians laptop:

- HP switches
- Motorola routers and gateways
- Terminal server (if present)
- TRAK devices

See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

When prompted to add the server to the known host list, accept the host.

NOTICE: Only authorized NM Clients can initiate an interactive SSH session with these devices.
For Motorola routers and gateways, an SSH session can be initiated only from NM Client 1, NM Client 2 (if present), NM Client 3 (if present), NM Client 33 (if present in a DSR backup core), NM Client 34 (if present in a DSR backup core), or NM Client 35 (if present in a DSR backup core).

For HP switches in a system without the DSR feature, an SSH session can be initiated only from NM Client 1, or NM Client 2 (if present). In a system with DSR, an SSH connection with an HP switch can be initiated by all NM Clients in the same zone or paired zone.

Related Links

Configuring the ASTRO 25 System for Secure Operation on page 43

4.3.8
Configuring SSH for Console Telephony Media Gateway

When and where to use:
This process lists the steps for SSH configuration for the Console telephony media gateway at the dispatch sites in an ASTRO® 25 communication system.

These steps may be skipped if you opted to perform them earlier.

NOTICE: For multizone systems, after completing Configuring SSH for Console Telephony Media Gateway on page 59, repeat all the processes you have completed from Configuring the ASTRO 25 System for Secure Operation on page 43, for the next zone.

Process:

1. Generate a new host key for the Console telephony media gateway. See Using a Saved Command in VoyenceControl to Generate SSH Keys on Console Telephony Media Gateway on page 170 or Using Cisco IOS Command to Generate SSH Keys on Console Telephony Media Gateway on page 201.
2. If the UNC contains an old host key in the known host list for the Console telephony media gateway, remove the host key from UNC. See Deleting SSH Keys from the UNC Server Known Hosts List Using the Administration Menu on page 179.
3. Verify the SSH connection from the UNC to the Console telephony media gateway (this also adds the devices to the UNC servers known hosts list). See Verifying Secure Mode/Updating Known Hosts List for UNC Management of a Device on page 177.

   NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.
4. Verify that an SSH connection can be made to the Console telephony media gateway from an NM Client or technician's laptop. See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

   When prompted to add the server to the known host list, accept the host.

   NOTICE: Only authorized NM Clients can initiate an interactive SSH session with these devices.

Related Links

Configuring the ASTRO 25 System for Secure Operation on page 43

4.3.9
Configuring SSH for MCC7500 Aux I/O Server

This process lists the steps for SSH configuration for MCC7500 Aux I/O Server at the dispatch sites in an ASTRO® 25 system.

Process:

1 Generate a new host key (server key pair) for the MCC7500 Aux I/O Server(s) from the UNC.

See Using a Saved Command in VoyenceControl to Generate SSH Keys on MCC7500 Aux I/O Server on page 171.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

Related Links

Configuring the ASTRO 25 System for Secure Operation on page 43

4.3.10
SSH Rotation on Devices Using Default Keys

This section applies to the following devices in an ASTRO® 25 system which can only operate with secure mode enabled and clear mode disabled (with the exception of the UNC server which can have both secure mode and clear mode enabled, so that it can configure devices which can only operate in clear mode).

The devices are listed in a sequence recommended for performing various SSH procedures from this manual.

1 **System level:**
   1 Unified Network Configurator (UNC)
   2 Unified Network Configurator Device Servers (UNCDS)
   3 User Configuration Server (UCS)
   4 System Statistics Server (SSS)
2 **Zone level:**
   a Zone Statistics Server (ZSS)
   b Zone Database Server (ZDS)
   c Unified Event Manager (UEM) Server
   d Air Traffic Router (ATR)
   e Zone Controller (ZC)
   f Packet Data Gateway (PDG)
   g Inter-RF Subsystem Interface/Console Subsystem Interface 8000 (ISSI 8000/CSSI 8000)
   h License Manager

NOTICE: License Manager does not use default keys, but it is part of this sequence.

3 **Network Management (NM) Clients**

This section also includes rotating keys between NM Clients and ATRs.

NOTICE: The processes and procedures in this section do **not** configure SSH for the Configuration/Service Software application on the NM Client.
Do **not** perform the processes in this section in an ASTRO® 25 system K master site configuration. The PDG is the only device listed above that may be present in a K master site, and in that configuration, it does not require the SSH key rotation procedures listed in this section.

For additional considerations, see SSH Key Rotation Impact on ASTRO 25 System Non-Interactive Services on page 208 and other topics in the “Operation” chapter and “Troubleshooting” chapter.

Related Links

Configuring the ASTRO 25 System for Secure Operation on page 43

4.3.10.1

SSH Key Rotation for Devices Using Default Keys Overview

For supported SSH interfaces between ASTRO® 25 communication system devices:

- Server devices discussed in this section (except for the ISSI.1 Network Gateway) are pre-populated with default SSH server (host) keys and default SSH client (user) keys, and default entries in known hosts lists and authorized keys lists.
- The PDG is pre-populated with SSH host keys and default SSH client keys, and the PDG known hosts list is pre-populated with default Unified Network Configurator (UNC) server host key entries.

As part of initial SSH configuration in an ASTRO® 25 communication system, the default SSH server (host) keys must be replaced on the SSH server devices. Then, the **known hosts list** on the SSH clients must be updated with the new keys.

In addition, the default SSH client keys must be replaced on the SSH clients. Then, the **authorized keys list** on the SSH server devices must be updated with the new client keys.

The process of replacing keys (initially and periodically) is referred to as **key rotation**. See Key Management on page 37.

As part of the initial key rotation after an installation that includes default keys, it is important that all default keys be removed, including default keys for devices that are not present in your system. This requirement is accommodated by the sequences in this section.

For maximum system availability (for systems already in operation), the sequences in this section assume that you remove and replace one SSH key at a time, instead of simultaneously removing all existing SSH keys from a device. The exceptions are: default SSH client key entries in an authorized keys list that are shared by more than one device, and default key entries for devices not present in your system – these entries are deleted all at once at the end of the overall key rotation process (see Removing Remaining SSH Default Keys on page 75.)

System availability is impacted as soon as an SSH key is regenerated on a device, until the entire rotation process for that key is completed. (For examples, see SSH Key Rotation Impact on ASTRO 25 System Non-Interactive Services on page 208.)

NOTICE: It is recommended that system migration should not be performed during an SSH key rotation.

This section provides the sequences for rotating SSH host keys and SSH client keys on server devices using default keys. The sequences provided in this section accommodate multizone systems. (In multizone systems, system-level Network Management servers need SSH connections to each zone-level server in each zone.)

Note that there is an additional key rotation process for devices if centralized backup and restore is implemented in the system. See Configuring SSH for Centralized Backup and Restore on page 45.

4.3.10.1.1
Rotating Keys Using Default Keys

Process:

1. Prepare for key rotation:
   a. Review the following: SSH Key Rotation Process – Preparation on page 108 and SSH Key Rotation Process – Recommendations on page 108.
   b. Before backing up the devices, verify that SSH non-interactive connections are working with the existing SSH keys. See: Verifying SSH Connectivity on page 109 – this section includes verification procedures for:
      - Connections between the servers
      - Connections between a PDG and a UNC
   c. Back up the devices before beginning a key rotation.
   - See Configuring SSH for Centralized Backup and Restore on page 45.
   - If the BAR service is operational, these BAR clients register periodically at the BAR server (about every two hours), without any need for intervention. BAR Clients can be registered manually using the **Manage BAR Client Configuration** menu option under **Services Administration**. See the *Backup and Restore Services* manual.
   - Ensure that SSH data is backed up to the centralized backup server for all backup clients. See Backing Up SSH Data to the Centralized Backup Server from All Backup Clients on page 152. For Network Management servers, be sure to review dependencies that impact the backup operation, listed in the table at the end of the *Private Network Management Servers* manual.
2. Follow the sequences for intrazone SSH connections:
   a. Rotating SSH Host Key – Intrazone Interfaces on page 62
   b. Rotating SSH Client Key – Intrazone Interfaces on page 64
3. After completing the first zone, repeat these intrazone SSH configuration sequences for each additional zone (if the system is multizone).
4. Complete SSH configuration required by ATIA Log Viewer on the Network Management (NM) Clients.

   See Continuing Key Rotation for ATIA Log Viewer on NM Clients on page 65.
5. Complete the sequences for system-level devices and interzone SSH connections:
   a. Rotating SSH Host Key – System-Level and Interzone Interfaces on page 66
   b. Rotating SSH Client Key – System-Level and Interzone Interfaces on page 67
6. Verify SSH connections.

   See Verifying SSH Connectivity on page 109.

4.3.10.2
Rotating SSH Host Key – Intrazone Interfaces

When and where to use:

See the following table while performing the steps below. For each row in the table, perform this process to configure the devices for the zone.

Table 4: Sequence for SSH Host Key Rotation – Intrazone Interfaces

Rotation Order	SSH Client	SSH Server
1	Only the server host key is rotated.	UEM
2	ZSS, SSS, NM Client(s)	ATR
3	Only the server key is rotated.	ZDS
4	Only the server key is rotated.	ZSS
5	Only the server key is rotated.	ZC01
6	Only the server key is rotated.	ZC02
7	Only the server key is rotated.	Tsub ZC
8	Only the server key is rotated.	PDG
9	Only the server key is rotated.	ISGW01
10	Only the server key is rotated.	ISGW02
11	Only the server key is rotated.	LM
12	Only the server key is rotated.	IP Packet Capture (also for each Tsub IP Packet Capture, if present)

Process:

1. For the listed SSH server device on that row, replace the existing SSH host key. See Host Key Generation on SSH Servers on page 111.
2. Verify that an SSH connection can be interactively established from a Network Management (NM) Client to the SSH server device. See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

   NOTICE: If you accept the host when prompted (after verifying the fingerprint), this updates the known hosts list on the NM Client with the SSH server host key that was generated in the previous step.
3. In the known hosts list on each of the associated SSH client devices in the row, replace the host key for this SSH server on that row.
   a. For Linux- or Solaris-based devices in the SSH Client column, see NM Servers, ZCs and ISGWs Update in Known Hosts Lists – Overview on page 114.
   b. For the NM Client(s) in the second row of the table, see Replacing ATIA Log Viewer ATR Entries in the NM Client Known Hosts List on page 96.
4. Proceed to the next row of Table 4: Sequence for SSH Host Key Rotation – Intrazone Interfaces on page 63 until all rows have been addressed. Then, proceed to the next sequence of procedures.

   NOTICE: After the ATR host key has been updated in this zone, secure access to that ATR from the ATIA Log Viewer application on an NM Client in another zone is not possible until the NM Client in that zone has been updated with the ATR's new public host key. If your system requires access to an ATR from NM Clients in other zones, you may choose to additionally update those NM Clients in other zones, immediately after generating an ATRs new host key. See the steps provided for that in the Continuing Key Rotation for ATIA Log Viewer on NM Clients on page 65.

4.3.10.3

Rotating SSH Client Key – Intrazone Interfaces

When and where to use:
See the following table while performing the steps below, to update the SSH client (user) keys for intrazone SSH connections between Network Management servers, Zone Controllers (ZCs), and ISGWs. Perform this process for each row in the table.

NOTICE: For Linux- and Solaris-based devices that can only operate in secure mode, when you remove or change an SSH client key on a device, communication with its SSH hosts is not possible until you update the authorized keys list on the SSH hosts.
For maximum system availability (for systems already in operation), the sequences in this section assume that you remove and replace one authorized key at a time, instead of simultaneously deleting all authorized keys from a device. The exception is for default keys in an authorized keys list that are for devices not present in your system – these can be deleted all at once (see Removing Remaining SSH Default Keys on page 75.)

Table 5: Sequence for Client Key Rotation – Intrazone Interfaces

Rotation Order	SSH Client	SSH Server
1	n/a	n/a
2	ZSS	ATR
3	ATR	UNC
4	ZSS	UNC
5	PDG	UNC
6	ZC01	UNC
7	ZC02	UNC
8	Tsub ZC	UNC
9	ISGW01	UNC
10	ISGW02	UNC

Process:

1. Replace the SSH client keys on the SSH client device. See the following (note that for the ATR on the second row, you must perform the first two procedures in this list):
   - Regenerating SSH Client Keys on a Network Management Server on page 128
   - Regenerating SSH Client Keys on an ATR for Connections to a UNC Server on page 131
   - Regenerating SSH Client Keys on a ZSS for Connections to a UNC Server on page 132
   - Regenerating SSH Client Keys on a PDG for Connections to a UNC Server on page 136
   - Generating SSH Client Keys on a Zone Controller on page 138
   - Generating SSH Client Keys on an ISGW on page 140
2. Transfer the new keys to each SSH server on the same row with that SSH client in Table 5: Sequence for Client Key Rotation – Intrazone Interfaces on page 64. See the following (note that for the ATR on the second row, you must perform the first two procedures in this list):
   - Transferring SSH Client Keys from an NM Server to an NM Server on page 128
   - Transferring SSH Client Keys from an ATR to a UNC Server on page 131
   - Transferring SSH Client Keys from a ZSS to a UNC Server on page 133

- Transferring PDG SSH Client Keys to a UNC Server on page 137
- Transferring SSH Client Keys from a Zone Controller to a UNC Server on page 139
- Transferring SSH Client Keys from an ISGW to a UNC Server on page 141

3 For each SSH server on the same row with that SSH client in Table 5: Sequence for Client Key Rotation – Intrazone Interfaces on page 64, update the SSH client key in the SSH servers authorized keys list. See the following (note that for the ATR on the second row, you must perform the first two procedures in the following list):

- Updating NM Server Entries in the Authorized Keys List on an NM Server on page 130
- Updating the ATR Entries in the Authorized Keys List on a UNC Server on page 132
- Updating ZSS Entries in the Authorized Keys List on a UNC Server on page 134
- Adding PDG Entries to the Authorized Keys List on a UNC Server on page 137
- Updating the ZC Entries in the Authorized Keys List on a UNC Server on page 139
- Updating the ISGW (ISSI 8000/CSSI 8000) Entries in the Authorized Keys List on a UNC Server on page 142

4 For the updated devices, re-verify all non-interactive SSH connections. See Verifying SSH Connectivity on page 109.

5 Repeat the steps above for the next row of Table 5: Sequence for Client Key Rotation – Intrazone Interfaces on page 64 until all rows have been addressed.

4.3.10.4
Repeating Previous Sequences for the Next Zone in Multizone Systems

When and where to use:
In multizone systems, repeat the following sequences for the next zone, until all zones have been addressed.

Process:

1 Rotating SSH Host Key – Intrazone Interfaces on page 62

2 Rotating SSH Client Key – Intrazone Interfaces on page 64

4.3.10.5
Continuing Key Rotation for ATIA Log Viewer on NM Clients

This section lists procedures for rotating SSH keys for the ATIA Log Viewer connection to Air Traffic Routers (ATRs) in each zone.

SSH must be configured to secure non-interactive processes between the ATIA Log Viewer application and ATRs. In multizone systems, the ATIA Log Viewer application on an NM Client may be set up to communicate with servers in one or more zones. In that case, SSH keys must be rotated between that NM Client and the ATR for each zone.

Process:

1 On each NM Client, for each ATR outside the zone where the NM Client is located, update Known Hosts Lists on NM Clients with Keys From ATRs in Other Zones.

Entries for the ATR in the same zone were already added to that NM Clients known hosts list as a result of the intrazone configuration procedures; also, you can skip these procedures entirely at this point if you opted to complete it at the same time as the intrazone configuration.
See Replacing ATIA Log Viewer ATR Entries in the NM Client Known Hosts List on page 96.

2 Generate and Propagate New NM Client ATIA Log Viewer User Keys.

The following configuration procedures are needed for all systems (single zone or multizone) so that a *new SSH user (SSH client) key replaces the existing user key on each NM Client* for the ATIA Log Viewer connection. The new user key for each NM Client is then propagated to each ATR in each zone.
Perform the following procedures to generate SSH user keys on each NM Client, transfer them to each ATR, and update the ATRs authorized list of keys with the new NM Client public keys:

a Generating SSH Client Keys for the NM Client ATIA Log Viewer on page 99

b Transferring Keys Securely from an NM Client to an ATR for ATIA Log Viewer on page 101

c Updating the ATR Authorized Keys List for ATIA Log Viewer on page 101

3 Verify the connection between each NM Client and each ATR.

See Verifying the SSH Configuration for ATIA Log Viewer on the NM Client on page 102.

4.3.10.6

Rotating SSH Host Key – System-Level and Interzone Interfaces

When and where to use: See the following table while performing the steps below. For each row in the table, configure each of the listed zone-level devices *for each zone,* and configure each of the listed system-level devices.

Table 6: Sequence for SSH Host Key Rotation – System-Level and Interzone Interfaces

Rotation Order	SSH Client	SSH Server
1	UNC	UCS
2	Only the server host key is rotated.	SSS
3	UCS, UNC, ATR, ZSS, PDG, ZC01, ZC02, ISGW01, ISGW02, SSS, UNCDS01, UNCDS02, UNCDS03	UNC

Process:

1 For the listed SSH server device on a row, regenerate the SSH host key.

See Host Key Generation on SSH Servers on page 111.

2 Verify that an SSH connection can be interactively established from each Network Management (NM Client) to the SSH server device on that row.

See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

NOTICE: If you accept the host when prompted (after verifying the fingerprint), this updates the known hosts list on the NM Client with the SSH server host key that was generated in the previous step.

3 For SSH client devices on that row, update their known hosts lists with the host keys from the SSH server on that row.

See NM Servers, ZCs and ISGWs Update in Known Hosts Lists – Overview on page 114.

4 Make sure that for each zone-level device, you completed these procedures for each zone. Also, make sure that each row of Table 6: Sequence for SSH Host Key Rotation – System-Level and Interzone Interfaces on page 66 was addressed.

4.3.10.7

Rotating SSH Client Key – System-Level and Interzone Interfaces

When and where to use:
See the following table while performing the steps below, to update the SSH client (user) keys for system-level NM servers and interzone SSH connections. For each row in the table, configure each of the listed zone-level devices *for each zone*, and configure each of the listed system-level devices.

Table 7: Sequence for SSH Client Key Rotation – System-Level and Interzone Interfaces

Rotation Order	SSH Client	SSH Server
1	SSS	ATR, UNC
2	UCS	UNC
3	UNC	UCS, UNC
4	UNCDS01, UNCDS02, UNCDS03	UNC

Process:

1. Perform the following actions:
   a. Replace the SSH client keys on the SSH client device.

      See Updating the SSS Entries in the Authorized Keys List on a UNC Server on page 135 (for SSS) and Regenerating SSH Client Keys on a Network Management Server on page 128 (for other NM servers).

   b. Transfer the new keys to each SSH server on the same row with that SSH client in Table 7: Sequence for SSH Client Key Rotation – System-Level and Interzone Interfaces on page 67.

      See Transferring SSH Client Keys from an NM Server to an NM Server on page 128.
2. For each SSH server on the same row with that SSH client in Table 7: Sequence for SSH Client Key Rotation – System-Level and Interzone Interfaces on page 67, replace the SSH client key in the servers authorized keys list.

   See Updating NM Server Entries in the Authorized Keys List on an NM Server on page 130.
3. For the updated devices, re-verify all non-interactive SSH connections.

   See Verifying SSH Connectivity on page 109 to verify:

   - Connections between servers (for NM Servers, ZCs and ISGWs)
   - Connections between a PDG and a UNC
4. Make sure that for each zone-level device, you completed these procedures for each zone. Also, make sure that each row of Table 7: Sequence for SSH Client Key Rotation – System-Level and Interzone Interfaces on page 67 was addressed.

4.3.11

Performing Additional SSH Configuration Processes for DSR Systems

This section provides the additional processes required for configuring SSH on ASTRO® 25 systems with the Dynamic System Resilience (DSR) feature implemented.

IMPORTANT: For Network Management (NM) client procedures listed in this process, do **not** perform any steps for configuring SSH client keys on NM Clients that were configured when implementing SSH for the primary core, but be sure to perform the steps that rotate SSH keys between these NM Clients and devices in the backup core.
NM Clients that were added to backup cores as part of the DSR expansion require **all** the steps to be performed in the NM Client procedures listed in the following process.

Prerequisites: Before you perform the processes on a backup core, ensure that the initial installation and configuration of the backup core devices were completed up to the SSH configuration step in the configuration process for that device. For initial installation and configuration processes for zone core devices, refer to the ASTRO® 25 system manual for each device.
Ensure that you perform the procedures in this process on backup core devices, not primary core devices, except when you are instructed to configure SSH between backup core and primary core devices.

Process:

1. For DSR systems, perform the following on the devices in each backup core:
   a. Configuring SSH for Centralized Backup and Restore on page 45

      Only if this feature is implemented, and only for supported Backup Clients that are present in the backup core.

   b. Configuring SSH for Devices at the Zone Core on page 47
   c. Configuring SSH for MOSCAD Network Fault Management (NFM) Devices on page 56
   d. Configuring SSH for Transport Network Devices on page 58

      Ensure to review the note at the NM Client step for which NM Clients can be used. Also, review the first Transport Network Equipment checklist in “Appendix B” for guidance on what transport network equipment needs SSH configuration from the backup core UNC and backup core NM clients at this point in the DSR SSH process, depending on your system configuration.

   e. Configuring SSH for Console Telephony Media Gateway on page 59

   Complete these procedures for all backup cores.
2. Follow the instructions in Secure Operation Verification Between SDM3000 Builder and an SDM3000 Hardware-Based Device on page 200 to verify that SSH connections can be established between SDM3000 Builder in the backup core and the following devices in the primary core:
   - SDM3000 Network Translator (SNT)
   - SDM3000 RTU, if present

   When a fingerprint verification prompt displays, validate the fingerprint, then click **OK** to trust the host.
3. Follow the instructions in Secure Operation Verification Between SDM3000 Builder and an SDM3000 Hardware-Based Device on page 200 to verify that SSH connections can be established between SDM3000 Builder in the primary core and the following devices in the backup core:
   - SDM3000 Network Translator (SNT)

- SDM3000 RTU, if present

When a fingerprint verification prompt displays, validate the fingerprint, then click **OK** to trust the host.

4 Return to the beginning of SSH Rotation on Devices Using Default Keys on page 60 and repeat all of the sequences from that process, for the backup core that is associated with the primary core you just configured. This time, perform the procedures for the devices in the backup core.

IMPORTANT:
When performing this process for the backup core, you can ignore verification failure messages for SSH connections between the primary core and backup core that have not yet been reconfigured, when you perform the procedures in Verifying SSH Connectivity on page 109. The scripts in these procedures test all SSH connections from a device. For DSR systems, this includes the supported connections between primary core and backup core.

Also, when the process refers to ZC01 perform the procedure on ZC03 instead. When the process refers to ZC02, perform the procedure on ZC04 instead.

Similarly, when the process refers to ISGW01 perform the procedure on ISGW03 instead. When the process refers to ISGW02, perform the procedure on ISGW04 instead, if present in the system.

When you have completed these instructions for one backup core, proceed to the next backup core and complete the instructions, until you have completed the instructions for all backup cores.

5 Complete Sequence for Key Rotation Between Primary Core SSH Clients and Backup Core SSH Servers on page 69.

6 Complete Sequence for Key Rotation Between Backup Core SSH Clients and Primary Core SSH Servers on page 72.

7 Complete Configuring SSH for Primary Core Interface to Backup Core Network Transport Devices on page 74.

8 Complete Configuring SSH for Backup Core Interface to Primary Core Network Transport Devices on page 75.

Related Links

Configuring the ASTRO 25 System for Secure Operation on page 43

4.3.11.1

Sequence for Key Rotation Between Primary Core SSH Clients and Backup Core SSH Servers

This section provides the sequence for configuring interfaces between SSH clients in the primary core and SSH servers in the backup core.

See the following table while performing Rotating Keys Between Primary Core SSH Clients and Backup Core SSH Servers on page 71.

Table 8: Sequence for Key Rotation Between Primary Core SSH Clients and Backup Core SSH Servers

	Primary Core SSH Client	Backup Core SSH Server
1		**ATR**
	SSS – See:	See:

	Updating Known Hosts List on the SSS for Connections to an ATR on page 116	Transferring SSH Client Keys from an NM Server to an NM Server on page 128 Updating NM Server Entries in the Authorized Keys List on an NM Server on page 130
	NM Client(s) – See: Replacing ATIA Log Viewer ATR Entries in the NM Client Known Hosts List on page 96	See: Transferring Keys Securely from an NM Client to an ATR for ATIA Log Viewer on page 101 Updating the ATR Authorized Keys List for ATIA Log Viewer on page 101
2		**UNC**
	UNC – See: Updating Known Hosts List on the UNC Server for Connections to the Same UNC Server on page 119	See: Transferring SSH Client Keys from an NM Server to an NM Server on page 128 Updating NM Server Entries in the Authorized Keys List on an NM Server on page 130
	ATR – See: Updating Known Hosts List on an ATR for Connections to a UNC Server on page 121	See: Transferring SSH Client Keys from an ATR to a UNC Server on page 131 Updating the ATR Entries in the Authorized Keys List on a UNC Server on page 132
	ZSS – See: Updating Known Hosts List on a ZSS for Connections to a UNC Server on page 122	See: Transferring SSH Client Keys from a ZSS to a UNC Server on page 133 Updating ZSS Entries in the Authorized Keys List on a UNC Server on page 134
	PDG – See: Updating Known Hosts List on a PDG for Connections to a UNC Server on page 122	See: Transferring PDG SSH Client Keys to a UNC Server on page 137 Adding PDG Entries to the Authorized Keys List on a UNC Server on page 137
	ZC01, ZC02 – See: Updating Known Hosts List on a Zone Controller for Connections to a UNC Server on page 123	See: Transferring SSH Client Keys from a Zone Controller to a UNC Server on page 139 Updating the ZC Entries in the Authorized Keys List on a UNC Server on page 139
	ISGW01, ISGW02 – See:	See:

	Updating Known Hosts List on an ISGW for Connections to a UNC Server on page 124	Transferring SSH Client Keys from an ISGW to a UNC Server on page 141 Updating the ISGW (ISSI 8000/CSSI 8000) Entries in the Authorized Keys List on a UNC Server on page 142
	SSS – See: Updating Known Hosts List on an SSS for Connections to a UNC Server on page 120	See: Transferring SSH Client Keys from an NM Server to an NM Server on page 128 Updating the SSS Entries in the Authorized Keys List on a UNC Server on page 135
3		**UCS**
	UCS – See: Updating Known Hosts List on the UCS for Connections to Another UCS (DSR Systems Only) on page 117	See: Transferring SSH Client Keys from an NM Server to an NM Server on page 128 Updating NM Server Entries in the Authorized Keys List on an NM Server on page 130

4.3.11.1.1
Rotating Keys Between Primary Core SSH Clients and Backup Core SSH Servers

When and where to use: For each row in Table 8: Sequence for Key Rotation Between Primary Core SSH Clients and Backup Core SSH Servers on page 69, configure each of the listed zone-level devices **for each zone**, and configure each of the listed system-level devices.

Process:

1. In the known hosts lists on SSH client devices on a row of the table, update the host keys for the SSH server on that row.

   See procedures listed in the appropriate rows of Table 8: Sequence for Key Rotation Between Primary Core SSH Clients and Backup Core SSH Servers on page 69 in the Primary Core SSH Client column.

2. For SSH server devices on a row of the table, in their authorized keys lists, update the SSH client keys for the SSH client on that row.

   See procedures listed in the appropriate rows of Table 8: Sequence for Key Rotation Between Primary Core SSH Clients and Backup Core SSH Servers on page 69 in the Backup Core SSH Server column.

3. For the updated devices, re-verify all non-interactive SSH connections.
   - For NM servers, zone controllers, ISGWs, and PDGs, see Verifying SSH Connectivity on page 109. (You can ignore verification failure messages for SSH connections between the primary core and backup core that have not yet been reconfigured.)
   - For NM Clients, see Verifying the SSH Configuration for ATIA Log Viewer on the NM Client on page 102.

4 Make sure that for each zone-level device, you completed these procedures for each zone. Also, make sure that each row of Table 8: Sequence for Key Rotation Between Primary Core SSH Clients and Backup Core SSH Servers on page 69 was addressed.

4.3.11.2

Sequence for Key Rotation Between Backup Core SSH Clients and Primary Core SSH Servers

This section provides the sequence for configuring interfaces between SSH clients in the backup core and SSH servers in the primary core.

See the following table while performing the steps listed in Rotating Keys Between Backup Core SSH Clients and Primary Core SSH Servers on page 73.

Table 9: Sequence for Key Rotation Between Backup Core SSH Clients and Primary Core SSH Servers

	Backup Core SSH Client	Primary Core SSH Server
1		**ATR**
	SSS See:Updating Known Hosts List on the SSS for Connections to an ATR on page 116	See: Transferring SSH Client Keys from an NM Server to an NM Server on page 128 Updating NM Server Entries in the Authorized Keys List on an NM Server on page 130
	NM Client(s) See:Replacing ATIA Log Viewer ATR Entries in the NM Client Known Hosts List on page 96	See: Transferring Keys Securely from an NM Client to an ATR for ATIA Log Viewer on page 101 Updating the ATR Authorized Keys List for ATIA Log Viewer on page 101
2		**UNC**
	UNC See:Updating Known Hosts List on the UNC Server for Connections to the Same UNC Server on page 119	See: Transferring SSH Client Keys from an NM Server to an NM Server on page 128 Updating NM Server Entries in the Authorized Keys List on an NM Server on page 130
	ATR See:Updating Known Hosts List on an ATR for Connections to a UNC Server on page 121	See: Transferring SSH Client Keys from an ATR to a UNC Server on page 131 Updating Known Hosts List on an ATR for Connections to a UNC Server on page 121
	ZSS	See: Transferring SSH Client Keys from a ZSS to a UNC Server on page 133

	See: Updating Known Hosts List on a ZSS for Connections to a UNC Server on page 122	Updating ZSS Entries in the Authorized Keys List on a UNC Server on page 134
	PDG See:Updating Known Hosts List on a PDG for Connections to a UNC Server on page 122	See: Transferring PDG SSH Client Keys to a UNC Server on page 137 Adding PDG Entries to the Authorized Keys List on a UNC Server on page 137
	ZC03, ZC04 See:Updating Known Hosts List on a Zone Controller for Connections to a UNC Server on page 123	See: Transferring SSH Client Keys from a Zone Controller to a UNC Server on page 139 Updating the ZC Entries in the Authorized Keys List on a UNC Server on page 139
	ISGW03, ISGW04 See:Updating Known Hosts List on an ISGW for Connections to a UNC Server on page 124	See: Transferring SSH Client Keys from an ISGW to a UNC Server on page 141 Updating the ISGW (ISSI 8000/CSSI 8000) Entries in the Authorized Keys List on a UNC Server on page 142
	SSS See:Updating Known Hosts List on an SSS for Connections to a UNC Server on page 120	See: Transferring SSH Client Keys from an NM Server to an NM Server on page 128 Updating the SSS Entries in the Authorized Keys List on a UNC Server on page 135
3		**UCS**
	UCS See:Updating Known Hosts List on the UCS for Connections to Another UCS (DSR Systems Only) on page 117	See: Transferring SSH Client Keys from an NM Server to an NM Server on page 128 Updating NM Server Entries in the Authorized Keys List on an NM Server on page 130

4.3.11.2.1

Rotating Keys Between Backup Core SSH Clients and Primary Core SSH Servers

When and where to use: For each row in Table 9: Sequence for Key Rotation Between Backup Core SSH Clients and Primary Core SSH Servers on page 72, configure each of the listed zone-level devices **for each zone**, and configure each of the listed system-level devices.

Process:

1 In the known hosts lists on SSH client devices on a row of the table, replace the host keys for the SSH server on that row.

See procedures listed in the appropriate rows of Table 9: Sequence for Key Rotation Between Backup Core SSH Clients and Primary Core SSH Servers on page 72, in the Backup Core SSH Client column.

2 For SSH server devices on a row of the table, in their authorized keys lists, replace the SSH client keys for the SSH client on that row.

See procedures listed in the appropriate rows of Table 9: Sequence for Key Rotation Between Backup Core SSH Clients and Primary Core SSH Servers on page 72, in the Primary Core SSH Server column.

3 For the updated devices, re-verify all non-interactive SSH connections.

- For NM servers, zone controllers, PDGs, and ISGWs see Verifying SSH Connectivity on page 109.
- For NM Clients, see Verifying the SSH Configuration for ATIA Log Viewer on the NM Client on page 102.

4 Make sure that for each zone-level device, you completed these procedures for each zone. Also, make sure that each row of Table 9: Sequence for Key Rotation Between Backup Core SSH Clients and Primary Core SSH Servers on page 72 was addressed.

4.3.11.3

Configuring SSH for Primary Core Interface to Backup Core Network Transport Devices

This process lists the steps for completing SSH configuration for the HP switches, terminal servers, and Motorola routers and gateways in the backup core of an ASTRO® 25 communication system with the Dynamic System Resilience feature implemented.

Process:

1 For the following backup core network transport devices, enable the SSH/SCP management mechanism in the properties for each device in VoyenceControl, and verify the SSH connection from VoyenceControl to the devices (this also adds the devices to the UNC server known hosts list):

- HP switches
- Motorola routers and gateways

See Enabling SSH/SCP Management Mechanism in Device Properties in VoyenceControl on page 176 and Verifying Secure Mode/Updating Known Hosts List for UNC Management of a Device on page 177.

NOTICE: These procedures are performed in the VoyenceControl component of the Unified Network Configurator (UNC) solution, located on the UNC server in the *primary* core.
The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

2 Verify that an SSH connection can be made from all of the authorized primary core NM Clients to the following backup core network transport devices:

- HP switches
- Motorola routers and gateways
- Terminal server (if present)

See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

When prompted to add the server to the known host list, accept the host.

NOTICE:
In the primary core, only the following NM Clients are authorized to establish an SSH connection to a Motorola router or gateway: NM Client 1, NM Client 2 (if present), or NM Client 3 (if present).

In a system with DSR, SSH connections to an HP switch can be made by all NM Clients in the same zone or paired zone as the switch.

4.3.11.4
Configuring SSH for Backup Core Interface to Primary Core Network Transport Devices

This process lists the steps for completing SSH configuration for the backup core interface to HP switches, terminal servers, and Motorola routers and gateways, in the primary core of an ASTRO® 25 communication system with the Dynamic System Resilience feature implemented.

Process:

1. For the following primary core network transport devices, enable the SSH/SCP management mechanism in the properties for each device in VoyenceControl, and verify the SSH connection from VoyenceControl to the devices (this also adds the devices to the UNC server known hosts list):
   - HP switches
   - Motorola routers and gateways

   See Enabling SSH/SCP Management Mechanism in Device Properties in VoyenceControl on page 176 and Verifying Secure Mode/Updating Known Hosts List for UNC Management of a Device on page 177.

   NOTICE:
   These procedures are performed in the VoyenceControl component of the Unified Network Configurator (UNC) solution, located on the UNC server in the *backup* core.

   The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.
2. Verify that an SSH connection can be made from all of the authorized backup core NM Clients to the following primary core network transport devices:
   - HP switches
   - Motorola routers and gateways
   - Terminal server (if present)

   See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

   When prompted to add the server to the known host list, accept the host.

   NOTICE:
   In a DSR backup core, only the following NM Clients are authorized to establish an SSH connection to Motorola routers and gateways: NM Client 33, NM Client 34 (if present), or NM Client 35 (if present).

   In a system with DSR, SSH connections to an HP switch can be made by all NM Clients in the same zone or paired zone as the switch.

4.3.12
Removing Remaining SSH Default Keys

When and where to use:

Perform this procedure on the following devices to remove pre-populated default SSH keys that are not removed by other SSH configuration procedures:

- NM servers
- GAS servers
- Zone Controller
- PDG
- ISGW Server
- NM Clients

NOTICE: Removal of remaining default keys is only needed after the initial key rotation following an installation that includes default keys (such as a new system, an upgrade, or an expansion).
Default keys need to be removed for devices not present in your system, including all devices in zones not included in your system, and all devices specific to configurations not included in your system.

Process:

1. On each Network Management server, Zone Controller, and ISGW, perform Remaining Default SSH Keys Removal for Network Management Servers, ZCs and ISGWs on page 145.
2. In the previous step, the default entries for PDGs were removed from the Unified Network Configurator (UNC) server authorized keys lists. To ensure that default client keys on the PDG were replaced with new keys, and that default entries were removed from the PDG known hosts list, perform the following procedure on each Packet Data Gateway: Detecting Default Keys on a PDG on page 150.
3. Perform the appropriate procedures in Final Verification of Default Key Removal on page 148.
4. For each NM Client, perform the procedures in Verifying That SSH Keys Are No Longer Being Used by an NM Client on page 103.
5. Perform the appropriate procedures in Verifying SSH Connectivity on page 109.

Related Links

Configuring the ASTRO 25 System for Secure Operation on page 43

4.3.13
Disabling Clear Protocols

Prerequisites:
Review the following information:

- If clear protocols are disabled on a device, subsequent configuration changes can only be made over a secure connection. The processes provided in this documentation ensure that clear protocols are disabled on a device only when they are no longer needed for configuration changes, so that the processes can be used for initial setup or full recovery of a system before it becomes operational.
- If clear protocols are disabled on a device, that device cannot communicate with devices that do not support secure protocols. Before disabling clear protocols, see the “Description” chapter for a list of devices in an ASTRO® 25 communication system that do not support SSH. To determine what is connected to those devices in your system, see the appropriate ASTRO® 25 communication system manuals and talk to your system administrator.

When and where to use:

The following process lists the steps for disabling clear protocols for devices at the zone core, RF sites, and dispatch Sites. This can be performed from the Zone Core. Repeat this process for each zone.

Process:

1 Disable clear protocol operation for the zone core devices (in any order).

- For NM servers:
  - Disabling clear mode is required only for the Unified Network Configurator (UNC) server, because clear mode is disabled by default on all other Linux-based NM servers in an ASTRO® 25 system. The UNC administration menus provide an option for disabling clear mode.
  - After disabling clear mode on the UNC server, make sure that secure credentials are selected in the Communication properties for devices managed in the VoyenceControl component of the UNC. See: Verifying Secure Mode/Updating Known Hosts List for UNC Management of a Device on page 177.

  NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.
- For Routers, gateways and HP switches: Disabling Telnet on Routers, Gateways, and HP Switches Using VoyenceControl on page 181 or SSH Configuration on Routers and Gateways Using Commands on page 185 and SSH Configuration on HP Switches Using Commands on page 183.
- If a terminal server is present at the zone core, see: Commands for Enabling/Disabling Secure Mode on the Terminal Server on page 190.
- If a VPM-based device (SmartX Site Converter or Telephone Media Gateway) is present at the zone core, see: Configuring Secure Services/Keys and Clear Services Using CSS on page 156.

NOTICE: Other zone core devices default to secure-only mode, so they do not need clear protocol disabled.

2 From the zone core, disable clear protocol operation for RF site devices, ISSI.1 site devices and SmartX Site Converters (in any order). See:

- Configuring Secure Services/Keys and Clear Services Using CSS on page 156 and Disabling Telnet on Routers, Gateways, and HP Switches Using VoyenceControl on page 181
- SSH Configuration on Routers and Gateways Using Commands on page 185 and SSH Configuration on HP Switches Using Commands on page 183

If a Terminal Server is present at a Simulcast Prime Site, see Commands for Enabling/Disabling Secure Mode on the Terminal Server on page 190.

3 From the zone core, disable clear protocol operation for dispatch site devices (in any order, at all dispatch sites). See:

- Disabling Telnet on Routers, Gateways, and HP Switches Using VoyenceControl on page 181
- SSH Configuration on Routers and Gateways Using Commands on page 185 and SSH Configuration on HP Switches Using Commands on page 183

For information on disabling Telnet and FTP on the MCC 7500 Voice Processor Module (VPM), and if a Conventional Site Controller is present at the site, see Configuring Secure Services/ Keys and Clear Services Using CSS on page 156.

Related Links

Configuring the ASTRO 25 System for Secure Operation on page 43

4.3.14
Backing Up a Baseline SSH Configuration

When and where to use:
After a system has been configured for secure operation, you should create an SSH configuration baseline. Capturing a baseline SSH configuration involves backing up the keys, operational mode, and known host files for all the devices configured for secure operation. The following process provides procedures and reference information to back up SSH data on various devices. These process steps may be performed in any order.

Process:

1. Capture the System Baseline SSH Configuration on Windows-based devices.

   If the centralized Backup and Restore service is implemented, a backup will occur at the scheduled time. To force a centralized backup instead of waiting for the scheduled backup time, perform the procedure for a one-time backup of a selected backup client, in the ASTRO® 25 communication system *Backup and Restore Services* manual.

2. Capture the System Baseline SSH Configuration on Linux devices using default keys:

   See the backup preparation procedures in the ASTRO® 25 communication system *Private Network Management Servers* manual and *Zone Controller* manual.

   To force a centralized backup instead of waiting for the scheduled backup time, perform the procedure for a one-time backup of a selected backup client, in the ASTRO® 25 communication system *Backup and Restore Services* manual, or see: Backing Up SSH Data to the Centralized Backup Server from All Backup Clients on page 152.

3. Capture the System Baseline SSH Configuration on the following devices:
   - RF Site devices:
     - GTR 8000 Base Radios
     - GCP 8000 Site Controllers
     - GPB 8000 Reference Distribution Modules
     - GCM 8000 Comparators
   - VPM-based devices:
     - SmartX Site Converter
     - MCC 7500 Voice Processor Module (VPM)
     - Telephone Media Gateway

   See CSS Known Hosts List Management on page 159 and Backing Up the Secure Services Settings for a Device Using CSS on page 159.

   NOTICE: Note that key pairs are not backed up for these devices.

4. Capture the System Baseline SSH Configuration on the Terminal Server.

   For instructions for backing up keys and known hosts lists, see SSH Configuration on the LX Terminal Server on page 190.

5. Capture the System Baseline SSH Configuration on MOSCAD NFM devices.

   See Backing Up SSH Configuration for MOSCAD Network Fault Management (NFM) Devices on page 202.

Related Links

Configuring the ASTRO 25 System for Secure Operation on page 43

4.4 SSH Configuration for Centralized Backup and Restore

This section provides procedures for configuring SSH for the Backup and Recovery (BAR) Server and Backup Clients. The sequence for performing these procedures as part of initial SSH configuration is provided in Configuring SSH for Centralized Backup and Restore on page 45.

4.4.1 Generating New SSH Host Keys on a Backup Server

When and where to use:
Perform the following procedure to generate SSH host keys (public and private) for the Backup and Recovery (BAR) server. SSH host keys are required for non-interactive communications in secure mode between the BAR server and:

- Backup Service-related accounts on the BAR server
- All other Backup Clients for this BAR server

The host keys generated in this procedure will automatically be provisioned to Backup Clients the next time they register with the Backup Server. See Configuring SSH for Centralized Backup and Restore on page 45.

Procedure:

1. Log on to the Backup Server using your Active Directory account.

   IMPORTANT:
   The username and password used for this step must also be used in all procedures for provisioning this host key to Backup Clients.

   The command prompt displays. The username is included in the command prompt.

2. Enter the following command: `admin_menu`

   The Main Menu displays for the BAR server.

3. Enter the number for the option **Application Administration**.

   The Application Administration menu appears.

4. Enter the number for the option **Manage Application**.

   The Manage Application menu appears.

5. Enter the number for the option **Application Key Management**.

   The Application Key Management menu appears.

6. Enter the number for the option **Generate New BAR SSH Host Keys**.

   A message appears asking for confirmation.

7. Enter `y` to confirm you wish to create new host keys.

   The SSH host keys are generated on the BAR server. Also, the known hosts list is automatically updated for the Backup Client on the BAR server.

Related Links

Configuring SSH for Centralized Backup and Restore on page 45

4.4.2
Generating New SSH Client Keys on a Backup Server

When and where to use:
Perform the following procedure to generate new SSH client keys on the Backup and Recovery (BAR) server for use by:

- Backup Service-related accounts on the BAR server
- All other Backup Clients for this BAR server

Procedure:

1. Log on to the Backup Server using your Active Directory account.

   IMPORTANT:
   The username and password used for this step must also be used in all procedures for provisioning this host key to Backup Clients.

   The command prompt displays. The username is included in the command prompt.

2. Enter the following command: `admin_menu`

   The Main Menu displays for the BAR server.

3. Enter the number for the option **Application Administration**.

   The Application Administration menu appears.

4. Enter the number for the option **Manage Application**.

   The Manage Application menu appears.

5. Enter the number for the option **Application Key Management**.

   The Application Key Management menu appears.

6. Enter the number for the option **Generate New BAR SSH Client Keys**.

   A message appears asking for confirmation that you want to create new client keys.

7. Enter `y` to confirm that you want to generate new keys.

   SSH client keys are generated on the BAR server for use by all its Backup Clients. The BAR server automatically updates its authorized list of keys.

Postrequisites:
Additional procedures are required before the client keys generated in this procedure can be used by Backup Clients. See Configuring SSH for Centralized Backup and Restore on page 45.

Related Links

Configuring SSH for Centralized Backup and Restore on page 45

4.4.3
Provisioning SSH Client (User) Key for the Backup and Restore Feature

When and where to use:
If the default SSH Client keys (also known as SSH user keys or backup registration keys) are *not* going to be used for the centralized backup and restore feature, the following procedures must be performed in the specified order before registration, backup, and restore operations:

These key generation and provisioning procedures can also be used for key rotation as required by your organizations policies. To test the new keys, register the Backup Clients with the Backup Server, or for a more thorough test, perform a backup. For instructions, see the *Backup and Restore Services* manual.

Process:

1. Create New Client SSH Keys (see Generating New SSH Client Keys on a Backup Server on page 80).
2. Perform Client SSH Key Provisioning procedures in this section (these procedures update the SSH Client key for Backup Service-related accounts on the Backup Server and Backup Clients).
3. Disable Default Key Usage (see Disabling Default SSH Key Usage on page 86).

4.4.3.1
Updating SSH Client Keys for Accounts on the Backup Server

Prerequisites:
Perform this procedure according to the sequence specified in Configuring SSH for Centralized Backup and Restore on page 45.

When and where to use:
Perform the following procedure to update the SSH client key for Backup Service-related accounts on the Backup Server.

Procedure:

1. Log on to the Backup Server using your Active Directory account.

   IMPORTANT: You must perform this procedure using a domain account that is a member of the Active Directory user group with permissions to generate SSH keys on the BAR server, and the domain controllers must be available on the network. For information on Active Directory user groups for ASTRO® 25 systems, see the *Authentication Services* manual.

   The command prompt displays. The username is included in the command prompt.

2. Enter the following command: `admin_menu`

   The Main Menu displays for the BAR server.

3. Enter the number for the option **Services Administration**.

   The Services Administration menu appears.

4. Enter the number for the option **Manage BAR Client Configuration**.

   The Manage BAR Client Configuration menu appears.

5. Enter the number for the option **Get BAR Host and User Keys**.

   Messages confirm the operation was successful for each account on the BAR server that uses SSH keys. The Manage BAR Client Configuration menu re-appears.

Related Links

Configuring SSH for Centralized Backup and Restore on page 45

4.4.3.2

Performing the Secure Transfer of the SSH Client Key to Linux-Based Backup Clients

Prerequisites: Obtain the username and password for the account that belongs to the “bkupadm” group in Active Directory.

When and where to use:
The following procedure describes how to perform a secure transfer of the SSH Client key from the Backup and Recovery (BAR) server to a Backup Client.

Perform this procedure as part of Configuring SSH for Centralized Backup and Restore on page 45.

Procedure:

1. Log on to the Backup Client device using your Active Directory account.

   IMPORTANT:
   You must perform this procedure using a domain account that is a member of the Active Directory user group with privileges to get SSH keys for the Backup client on this device, and the domain controllers must be available on the network.

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

   The command prompt displays. The username is included in the command prompt.

2. Enter the following command: `admin_menu`

   The Main Menu displays for the BAR server.

3. Enter the number for the option **Services Administration**.

   The Services Administration menu appears.

4. Enter the number for the option **Manage BAR Client Configuration**.

   The Manage BAR Client Configuration menu appears.

5. Enter the number for the option **Get BAR Host and User Keys**.

   The process for provisioning the BAR server SSH *host* keys begins. A fingerprint message displays and a prompt asks if you want to continue.

6. Type `yes` after verifying that the displayed fingerprint matches the fingerprint of the BAR SSH host keys from the .pub files located in `etc/ssh` on the Backup Server.

   For additional information on verifying fingerprints, see: Fingerprint Verification in SSH Session Warning Banner on page 92.

   The same fingerprint message and prompt display again (the BAR keys must be provisioned to a second account on the Backup Client).

7. Type `yes` again.

   Entries for the new BAR server SSH host keys replace the previous BAR server entries in the Backup Client known hosts list on this device. The process for provisioning the BAR SSH *client* keys begins, starting with a prompt asking for the username that was used to generate keys on the BAR server.

8. Type the Active Directory username that belongs to the **bkupadm** group in Active Directory.

NOTICE: If needed, press the Ctrl+C keys to return to the menu.

A password prompt displays

9 Enter the password for the user from the previous step.

NOTICE:
The password will not be displayed while typing.

If needed, press the Ctrl+C keys to return to the menu.

A message confirms that the user keys were provisioned successfully. The Manage BAR Client Configuration menu appears.

Related Links

Configuring SSH for Centralized Backup and Restore on page 45

4.4.3.3

Performing the Secure Transfer of the SSH Client Key to Windows-Based Backup Clients

Prerequisites: Obtain the username and password for the account that belongs to the `bkupadm` group in Active Directory.

When and where to use: Perform the following procedure to transfer the SSH client key from the Backup and Recovery (BAR) server to the following Windows-based Backup Clients, according to the sequence specified in Configuring SSH for Centralized Backup and Restore on page 45:

- NM Client(s)
- CSMS
- DCs/Authentication Servers
- InfoVista (if present in the system)
- GMC (if present in the system)

  NOTICE: GMC runs on Windows Server 2008.

- GWS (if present in the system)
- Authentication Center server (if present in the system)
- MKM 7000 Console Alias Manager (CAM)

Procedure:

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

The Windows administrator account set up by Motorola Solutions for devices operating on Windows Server 2008 and Window Server 2012 is "motosec"; "secmoto" is the Windows administrator account set up by Motorola Solutions for Windows 7, and Windows 10-based devices.

2 Perform one of the following actions:

- **For Windows 7 and Windows Server 2008:** From **Start**, select **Programs** → **Motorola** → **Bar Client** → **Get Host & User Key**.
- **For Windows 10 and Windows Server 2012:** In the Windows search field, type in: `Get Host`. In the list of results, click **Get Host & User keys**.

3 In the **Get Host & User keys** command window, type the Active Directory username that belongs to the `bkupadm` group in Active Directory.

4 At the password prompt, enter the password for the user from the previous step.

The password will not be displayed while typing.

A message indicates that the user keys were provisioned successfully.

5 At the prompt, press any key.

The command window closes.

Related Links

Configuring SSH for Centralized Backup and Restore on page 45
Configuring SSH for Devices at a Dispatch Site on page 53

4.4.4
SSH Configuration Verification for Backup Clients

This section includes the procedures for verifying the SSH configuration for Linux-based and Windows-based backup clients.

Related Links

Configuring SSH for Centralized Backup and Restore on page 45
Verifying SSH Configuration for Linux-Based Backup Clients on page 84
Verifying SSH Configuration for Windows-Based Backup Clients on page 85
Configuring SSH for Devices at a Dispatch Site on page 53

4.4.4.1
Verifying SSH Configuration for Linux-Based Backup Clients

When and where to use: The following procedure describes how to verify the SSH configuration for Linux-based Backup Clients.

Procedure:

1 Log on to the Backup Client device using your Active Directory account.

IMPORTANT: You must perform this procedure using a domain account that is a member of the Active Directory user group with privileges to verify SSH keys for the Backup Client on this device, and the domain controllers must be available on the network.
For information on Active Directory user groups for ASTRO® 25 systems, see the *Authentication Services* manual.

The command prompt displays. The username is included in the command prompt.

2 Enter: `admin_menu`

The Main Menu displays for the BAR server.

3 Enter the number for the option **Services Administration**.

The Services Administration menu appears.

4 Enter the number for the option **Manage BAR Client Configuration**.

The Manage BAR Client Configuration menu appears.

5 Enter the number for the option **Verify BAR SSH Keys**. If any of the following occurs, then SSH was not configured properly:

A message confirms the operation was successful for each account on the Backup Client that uses BAR SSH keys. The Manage BAR Client Configuration menu re-appears.

IMPORTANT:

- If a fingerprint displays and a prompt asks `Are you sure you want to continue connecting (yes/no)?`, then the new BAR server host keys were not yet accepted into the known hosts list on this Backup Client. You can accept them now, after verifying that the displayed fingerprint matches the fingerprint of the BAR SSH host keys from the .pub files located in`etc/ssh` on the Backup Server. For additional information on verifying, see: Fingerprint Verification in SSH Session Warning Banner on page 92
- If a username prompt displays, then the Backup Client registration keys (SSH user keys) may be mismatched between the Backup Server and the Backup Client. See Provisioning SSH Client (User) Key for the Backup and Restore Feature on page 80 to configure SSH correctly.
- If the `key verification failed` message appears. See Provisioning SSH Client (User) Key for the Backup and Restore Feature on page 80 to configure SSH correctly.

Related Links

Verifying SSH Configuration for Windows-Based Backup Clients on page 85
SSH Configuration Verification for Backup Clients on page 84

4.4.4.2
Verifying SSH Configuration for Windows-Based Backup Clients

Procedure:

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

The Windows administrator account set up by Motorola Solutions for devices operating on Windows Server 2008 and Windows Server 2012 is "motosec"; "secmoto" is the Windows administrator account set up by Motorola Solutions for Windows 7 and Windows 10-based devices.

2 Perform one of the following actions:

- **For Windows 7 and Windows Server 2008:** From **Start**, select **Programs** → **Motorola** → **Bar Client** → **Verify Keys**.
- **For Windows 10 and Windows Server 2012:** In the Windows search field, type in: `verify`. In the list of results, click **Verify keys**.

3 In the **Verify keys** command prompt window:

- If SSH has been configured properly, the `key verification successful` message appears for the account associated with the Backup Client service.
- If any errors are encountered the `key verification failed` message appears. See Provisioning SSH Client (User) Key for the Backup and Restore Feature on page 80 to configure SSH correctly.

4 Press any key to close the command window.

Related Links

Verifying SSH Configuration for Linux-Based Backup Clients on page 84
SSH Configuration Verification for Backup Clients on page 84
Configuring SSH for Devices at a Dispatch Site on page 53

4.4.5
Disabling/Enabling Default Key Usage on the Backup Server

This section covers:

- Disabling Default Key Usage
- Enabling Default Key Usage

IMPORTANT: After selecting either of these menu options, you must re-provision SSH keys to all the Backup Clients for this Backup Server.

4.4.5.1
Disabling Default SSH Key Usage

When and where to use:
Perform the following procedure to disable default SSH key usage by a Backup and Recovery (BAR) server and by all its Backup Clients.

NOTICE: The sequence for performing this procedure as part of initial SSH configuration is provided in Configuring SSH for Centralized Backup and Restore on page 45.

Procedure:

1. Log on to the Backup Server using your Active Directory account.

   The command prompt displays. The username is included in the command prompt.

2. Enter the following command: `admin_menu`

   The Main Menu displays for the BAR server.

3. Enter the number for the option **Application Administration**.

   The Application Administration menu appears.

4. Enter the number for the option **Manage Application**.

   The Manage Application menu appears.

5. Enter the number for the option **Application Key Management**.

   The Application Key Management menu appears.

6. Enter the number for the option **Disable Default BAR SSH Key Usage**.

   A message appears asking you to confirm that you want to delete the default client keys.

7. Enter `y` to confirm that you want to delete default client keys.

   Default SSH key usage is disabled for the BAR server and all its Backup Clients.

Related Links

Configuring SSH for Centralized Backup and Restore on page 45
Configuring SSH for Devices at a Dispatch Site on page 53

4.4.5.2
Re-Enabling Default Key Usage

If files containing default keys are still in their original location on the Backup and Restore (BAR) clients, you can use the **Enable Default BAR SSH Key Usage** option on the Backup Server administration menu to re-enable default key usage on the Backup Server.

You must also perform the Backup Client procedures in this section to re-enable default key usage on the Backup Clients.

4.4.5.2.1
Re-Enabling Default SSH Key Usage on the Backup Server

Prerequisites:

NOTICE:
`bar_client_registration.orig` files containing the default Backup Client keys must exist in the locations specified in the procedure.

If you removed the `bar_client_registration.orig` files from the specified locations on the Backup Clients, you need to restore the `bar_client_registration.orig` files from your own archive.

When and where to use:
Perform this procedure to re-enable default SSH key usage on a Backup and Recovery (BAR) server.

Procedure:

1. Log on to the Backup Server using your Active Directory account.
   The command prompt displays. The username is included in the command prompt.
2. Enter the following command: `admin_menu`
   The Main Menu displays for the BAR server.
3. Enter the number for the option **Application Administration**.
   The Application Administration menu appears.
4. Enter the number for the option **Manage Application**.
   The Manage Application menu appears.
5. Enter the number for the option **Application Key Management**.
   The Application Key Management menu appears.
6. Enter the number for the option **Enable Default BAR SSH Key Usage**.
   A confirmation message appears asking if you want to enable default client keys.
7. Enter `y` to confirm that you want to enable default client keys.
   Default SSH key usage is re-enabled for the BAR servers.

4.4.5.2.2
Re-Enabling Default Key Usage on a Linux-Based Backup Client

Prerequisites:
Make sure that `bar_client_registration.orig` files containing the default Backup Client keys exist in the locations specified in the procedure.

If you removed the `bar_client_registration.orig` files from the specified locations on the Backup Clients, you need to restore the `bar_client_registration.orig` files from your own archive.

When and where to use:
Perform the following procedure to enable default key usage on a Linux-based Backup Client.

Procedure:

1 Access the root command prompt on the Linux-based Backup Client.

IMPORTANT: You must perform this procedure using a domain account that is a member of the Active Directory user group with privileges to log on to this device, and the domain controllers must be available on the network. For information on Active Directory user groups for ASTRO® 25 systems, see the *Authentication Services* manual.

2 Type the following to restore the copy of the pre-shared registration key:

```
cp /usr/local/home/bkupclnt/.ssh/bar_client_registration.orig/usr/
local/home/bkupclnt/.ssh/bar_client_registration
```

NOTICE: If a prompt asks if an overwrite is required, type `y`.

3 Type the following:

```
rm f /usr/local/home/bkupclnt/.ssh/bar_client_registration.orig
```

The `bar_client_registration.orig` file is deleted.

4.4.5.2.3 Re-Enabling Default Key Usage on a Windows-Based Backup Client

Prerequisites:

NOTICE:
`bar_client_registration.orig` files containing the default Backup Client keys must exist in the locations specified in the procedure.

If you removed the `bar_client_registration.orig` files from the specified locations on the Backup Clients, you need to restore the `bar_client_registration.orig` files from your own archive.

Procedure:

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

The Windows administrator account set up by Motorola Solutions for devices operating on Windows Server 2008 and Windows Server 2012 is "motosec"; "secmoto" is the Windows administrator account set up by Motorola Solutions for Windows 7, and Windows 10-based devices.

2 Navigate to one of the following locations:

- For 32-bit systems: `C:\Program Files\Motorola\bar\var\.ssh`
- For 64-bit systems: `C:\Program Files (x86)\Motorola\bar\var\.ssh`

3 Copy the `bar_client_registration.orig` file to `bar_client_registration`.

4 Delete the `bar_client_registration.orig` file in the `C:\Program Files\Motorola \bar\var\.ssh` folder.

4.5 Restoring SSH on the PDG

When and where to use:
Perform this procedure to restore SSH on the Packet Data Gateway (PDG).

NOTICE: For the proper sequence to rotate SSH keys for the non-interactive interface between the Linux-based Packet Data Router (PDR) component of the Packet Data Gateway (PDG) and the Unified Network Configurator (UNC) server, see SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1. Log on to the PDG using your Active Directory account.

   IMPORTANT: You must perform this procedure using a domain account that is a member of an Active Directory user group with privileges to perform this operation, and the domain controllers must be available on the network. For information on Active Directory user groups for ASTRO® 25 systems, see the *Authentication Services* manual.

   The command prompt displays. The username is included in the command prompt.

2. Enter the following command: `admin_menu`

   The Main Menu displays for the PDG.

3. Enter the number for the option **Backup and Restore Administration**.

   The OS Administration menu appears.

4. Enter the number for the option **Post Restore Operations**.

   The Manage Application menu appears.

5. Enter the number for the option **Restore SSH keys and Configuration**.

   The SSH keys are restored.

4.6 Using PuTTY to Access an SSH Server from a Windows-Based Device

Install PuTTY on the Windows-based device. (In ASTRO® 25 systems, generally the Windows-based device used for this procedure would be a Network Management (NM) Client, but in a K core configuration, other Windows-based service devices are provided instead of the NM Client.)

The devices you can access are limited by Router Access Control Lists (ACLs), configuration files, firewall rules, and user permissions. For details, contact your system administrator and see the configuration files for your network transport devices. For general information, see the *Information Assurance Features Overview* manual.

NOTICE: Consider creating a shortcut on the desktop to the PuTTY utility, because the PuTTY application window automatically closes after each session it initiates.

NOTICE:
A Motorola Solutions-customized version of PuTTY is available for installation from the ASTRO® 25 system *Windows Supplemental* media. See Installing Motorola Solutions PuTTY on Windows-Based Devices on page 40.

The Motorola Solutions customization is for PuTTY key generation. Command syntax and details are included in a “Motorola Changes” topic in the *PuTTY User Manual* included in the PuTTY installed files. Motorola Solutions does not customize `PuTTY.exe` and other PuTTY tools used for SSH, SCP (pscp), and SFTP (psftp) sessions (for instructions on these other tools, see their topics in the *PuTTY User Manual*).

Procedure:

1 Log on to the Windows-based device using the domain user account.

The desktop appears.

2 If the version of PuTTY on this Windows-based device was installed from the ASTRO® 25 system *Windows Supplemental* media, launch the PuTTY application:

- **For Windows 7 and Windows Server 2008:** From **Start**, select **Programs** → **Motorola** → **Motorola PuTTY** → **PuTTY**.
- **For Windows 10 and Windows Server 2012:** In the Windows search field, type in: `putty`. In the list of results, click **PuTTY**.

3 In the **PuTTY Configuration** window, perform the following actions:

a As the **Connection type**, select **SSH**.

b In the **Port** field, leave **22**.

For an SSH session with a Solaris-based server, make sure that the PuTTY application is configured as follows:

a From the **Category** pane on the left, select **Terminal** → **Keyboard**. Under **The Backspace key**, select **Control-H**.

b From the **Category** pane on the left, select **Window** → **Selection**. Under **Control use of mouse**, select **Compromise**.

It is important that the default settings are used for **Attempt “keyboard-interactive” auth [SSH-2]**. That check box should remain selected on the settings screen accessed from **Connection, SSH, Auth** in the **Category** pane. If this check box is not selected, the SSH session disconnects before you can log on to the SSH server device.

4 Specify a user name and an SSH server in the **Host Name (or IP address)** field, in the following format:

<User name>@<SSH server host name or IP address>

Other methods for specifying a user name for interactive sessions are available. For example, if you navigate to **Connection** then **Data** in PuTTY and select **Prompt**, then, when you do not provide a user name in the command above, you will be prompted for a user name after you click **Open** in the next step. For additional information, see PuTTY online help.

If you want to save these settings for future use, enter a name for the session in the **Saved Sessions** field on the main Session window in PuTTY and click **Save**. The session name that you entered appears in the list below the **Saved Sessions** field.

CAUTION: Do not save a session with the name “Default Settings”. Saving a host in a session called “Default Settings” may cause SSH connection failure for non-interactive and command-line functions.

5 Click **Open**.

The **PuTTY Configuration** window closes, and if you established the first connection to the SSH server or if the SSH servers key has changed, a window appears displaying the server's SSH fingerprint.

6 Perform one of the following actions:

a Click **Cancel** if the fingerprint does not match the fingerprint of the host key generated most recently on the SSH server device, so that the interactive session is not established, then skip the rest of this procedure so that you can investigate the reason for the mismatch.

b Click **Yes** after verifying the fingerprint, if you want to accept the SSH server device into the known hosts list on the SSH client device where PuTTY is installed.

If you click **Yes** when there are still default SSH server keys on the SSH server device, then entries for the default keys are added to a known hosts list on the SSH client device where PuTTY is installed. These entries are not automatically overwritten during the key rotation procedures for the supported non-interactive ASTRO® 25 system SSH interfaces. Perform additional procedure to remove them. See Removing Interactive Entries from the Known Hosts List on an NM Client on page 95.

The interactive session is established. Proceed to step 7.

c Click **No** to establish the interactive session, **without** accepting the SSH server device into the known hosts list on the SSH client device where PuTTY is installed. Then proceed to step 7.

It is recommended that you click **No** if your organizations policies require key rotation to replace default SSH keys, and the default SSH server keys from initial installation were not yet replaced by generating new SSH server keys on the device you are connecting to.

For verifying the fingerprint of an SSH server (host), it is recommended that you refer to the fingerprint recorded when generating the keys on the SSH server. For additional information on verifying fingerprints for Solaris-based and Linux-based SSH servers, see Fingerprint Verification in SSH Session Warning Banner on page 92.

7 Perform one of the following actions:

- If you launched the SSH session only for testing secure mode and adding the SSH server to the known hosts list on the Windows device, you can close the SSH window.
- If you launched the SSH sessions for additional reasons, proceed with the interactive session. Log in to the SSH server device, if prompted.

Related Links

Configuring SSH for Centralized Backup and Restore on page 45
Configuring SSH for Devices at the Zone Core on page 47
Configuring SSH for Devices at an RF Site on page 50
Configuring SSH for Devices at an ISSI.1 Network Gateway Site on page 52
Configuring SSH for Devices at a Dispatch Site on page 53
Configuring SSH for MOSCAD Network Fault Management (NFM) Devices on page 56
Configuring SSH for Transport Network Devices on page 58
Configuring SSH for Console Telephony Media Gateway on page 59

4.7 Fingerprint Verification in SSH Session Warning Banner

SSH session fingerprint verification (and accepting the host into the known hosts list) is performed for each device as part of the ASTRO® 25 system SSH configuration process, so that each device is ready for interactive sessions without requiring a service user to verify fingerprints.

If the warning banner displays for you when initiating an SSH session, fingerprint verification is recommended before accepting the host into the known hosts list.

It is recommended that you refer to the fingerprint recorded when generating the keys on the SSH server. Contact your system administrator for this information if needed.

For Solaris-based and Linux-based SSH servers, the root user can execute the following command to view the SSH key fingerprint on the device: `ssh-keygen -lf /etc/ssh/ssh_host_rsa_key`

IMPORTANT: This command should only be executed when you are connected to the console of the SSH server device. Performing this command when connected to a device over the network (for example, in a PuTTY session) is not a reliable method.
See the instructions for connecting to an SSH server in Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

4.8 Key Rotation for Devices Using Default Keys – Recommendations

The procedures in the following sections should be performed in the sequence specified in the SSH Rotation on Devices Using Default Keys on page 60.

Before you begin, it is recommended that you study the process carefully, and consider the recommendations that follow:

- Procedures in the following section rotate SSH keys for specific *non-interactive* SSH connections required for ASTRO® 25 communication system operation. For the initial rotation after an ASTRO® 25 system installation that included default keys, procedures are provided for replacing the defaults for devices in your system, then detecting and removing defaults for devices not in your system, but only for the specific non-interactive SSH connections required for ASTRO® 25 system operation. If a user initiates an *interactive* SSH session with an SSH server device before initial key rotation, it is possible to create a known hosts list entry for a default SSH host key that cannot be removed with procedures for non-interactive accounts in this manual.
  - Instructions for preventing these entries in an NM Client known hosts list is provided in Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.
  - Guidance for removing unexpected default entries in an NM server known hosts list is provided in Additional Default Key Removal Considerations – Unexpected Default Entries in Known Hosts Lists on page 150.
  - Instructions for removing defaults from a known hosts list for interactive users on an NM Client are located in Removing Interactive Entries from the Known Hosts List on an NM Client on page 95.
  - Instructions for removing defaults from a known hosts list for interactive users on a technicians laptop are beyond the scope of this manual.
- The procedures in the following sections may take several hours to complete. To track your progress and keep your place in case of interruptions, check off each step in each procedure as you complete it, and check off each procedure in the SSH Rotation on Devices Using Default Keys on page 60 as you complete it. (It is recommended that you create checklists customized for your systems configuration. Examples are provided in Appendix A and Appendix B.)

- If you copy and paste commands from this PDF file to the command line, then be sure to check them carefully before you execute them, and correct any character substitutions that may have occurred.
- If you have questions about the syntax of a command or the arguments provided for the command in a procedure, type the command using the same path as indicated in the procedure, except use `-h` as the only argument. This displays help for all the arguments supported by the command. For example, on a Network Management server, type `/opt/Motorola/ssh/bin/manage_authorized_keys -h` to display help for that command.
- You can log into multiple server devices in multiple terminal session windows. However, each session may automatically terminate after a period of inactivity.

For additional considerations, see SSH Key Rotation Impact on ASTRO 25 System Non-Interactive Services on page 208 and other topics in the “Operation” chapter and “Troubleshooting” chapter.

4.9 Use of a Domain Account to Log on to Devices Using Default Keys

For procedures that need to be performed as the domain user on a Linux-based device, establish an SSH session using your Active Directory account that is a member of a user group authorized to access the device.

NOTICE: The domain controller must be available on the network to log on as a domain user.

To perform the following SSH-related operations from the command line *or from administration menus* on ASTRO® 25 system server devices, log on using an Active Directory account that is member of the secadm or instadm user group (then, to access administration menus, type the `admin_menu` command).

NOTICE: For SSH key rotations, perform these operations according to the sequence specified in Configuring the ASTRO 25 System for Secure Operation on page 43.

Table 10: SSH Operations in Administration Menus and Corresponding Commands

admin_menu> OS Administration> Security Provisioning	Corresponding command
Detect Default SSH Key Usage	`esudo /opt/Motorola/ssh/bin/default_key_detector`
Verify SSH Connectivity	`esudo /opt/Motorola/ssh/bin/verify_ssh_connectivity`

Table 11: Backup and Restore (BAR) SSH Operations in Administration Menus and Corresponding Commands

admin_menu> Services Administration> Manage BAR Client Configuration	Corresponding command
Get BAR Host and User Keys	`esudo /opt/Motorola/bar//bin/get_host_user_keys`
Verify BAR SSH Keys	`esudo /opt/Motorola/bar//bin/verify_keys`

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

4.10 Accessing the Root Command Prompt on Devices Using Default Keys

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

Procedure:

For command-line procedures that need to be performed as the root user, access the root user prompt for the device by performing one of the following:

- Use an SSH session to connect to the device:
  1. Establish an SSH session using your Active Directory account that is a member of a user group authorized to access this device.

     For example, the user group ucs-login is authorized to log on to the UCS.
  2. Enter: `su -`
  3. Enter the root account password to access the root command prompt.
- Use a console connection to access the server and log on with the root account. For details, see the appropriate device manual:
  - *Virtual Management Server Software*
  - *Packet Data Gateways*
  - *ISSI.1 Network Gateway Feature Guide*
  - *ISSI 8000/CSSI 8000 Intersystem Gateway Feature Guide*

4.11 Logon to Network Management Clients SSH Configuration

For SSH configuration procedures performed on Network Management (NM) Clients, you need to log on either as the local Windows administrator, or using your Active Directory account that is a member of the “secadm” user group.

NOTICE: It is recommended that you log on with the Active Directory account.
To log on using an Active Directory account, the domain controller must be available on the network, and the NM Client must be joined to the domain.

When logging on to an NM Client, be sure to enter the Active Directory domain before your Active Directory username, in the following format: ***<domain>\<username>***.

For general use of PuTTY to initiate sessions with other devices from an NM Client, you can log on to the NM Client using any valid local account, or using your Active Directory account that is a member of a group with authority to log on to NM Clients (for example, the “nm_client-login” user group).

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

The following extra steps are required when configuring SSH:

When using the command prompt window to generate SSH keys on the NM Client, you need to access the command prompt window by right-clicking the Command Prompt option on the Accessories menu, and choosing to Run as administrator. If a **User Account Control** window displays, enter your password and click **Continue**, or click **Allow**.

For procedures that require logging on to the NM Client as the local Windows administrator, ask your system administrator for the username and password required. The local Windows administrator account set up by Motorola Solutions on NM Clients is "secmoto".

4.12 Removing Interactive Entries from the Known Hosts List on an NM Client

Perform the following procedure to detect and remove default SSH keys from the known hosts list for an interactive user on a Network Management (NM) Client.

IMPORTANT: Repeat this procedure, including the step for logging on to the NM Client, for each interactive user that may have added default SSH keys to the known hosts list on this NM Client.

When and where to use: If a user who is logged into a Network Management (NM) Client initiates an SSH session with an SSH server device before an SSH key rotation, and selects **Yes** at the fingerprint prompt, this creates entries in an NM Client known hosts list. These *interactive* account entries are not addressed in the key rotation procedures for the supported ASTRO® 25 system *non-interactive* SSH interfaces.

Procedure:

1. Log on to the NM Client using your Active Directory account that is a member of the “secadm” user group.

   See Logon to Network Management Clients SSH Configuration on page 94.

   The desktop appears.

2. From **Start**, select **All apps** → **Motorola** → **puttyDefaultKeyDetector**.

   NOTICE: If you are logging with an Administrator account, right-click **puttyDefaultKeyDetector** and select **Run As Administrator**.

   The following columns of information display in the **puttyDefaultKeyDetector** window:

   - **Key Type** will always display `Default PuTTY SSH Host Key`.
   - **Key Name** is a combination of Host IP and actual key type (dsa or rsa2).
   - **Windows Account** shows the user for which the keys are detected and can be removed (this is the account used to log on to the NM Client in step 1)

3. Based on the results in the **Key Name** column, select the rows for the keys you want to delete:
   - To select more than one consecutive entry, press the SHIFT key then click the entries you want to delete.
   - To select more than one non-consecutive entry, press the CTRL key then click the entries you want to delete.
   - To select one entry, click one row and proceed to the next step.
4. Click **Remove Selected**.

   You are prompted to confirm you want to remove the selected key(s).

5. On the confirmation window, click **OK**.

   A message reports that the deletion was successful.

6 On the success message window, click **OK**.

The list of keys automatically refreshes, and the key(s) you had selected for deletion no longer display in the list.

7 Click **Exit** to close the window.

The **puttyDefaultKeyDetector** window closes. The desktop appears.

4.13 Preparing to Generate SSH Client Keys on an NM Client

Procedure:

1 Log on to the NM Client using your Active Directory account that is a member of the “secadm” user group.

See Logon to Network Management Clients SSH Configuration on page 94.

The desktop appears.

2 Navigate to the following directory:

`C:\Program Files(x86)\Motorola\Motorola PuTTY\bin\`

3 Verify that `PuTTYcgn.exe` exists in this directory.

- If the directory listing includes the file `PuTTYcgn.exe`, proceed to the next step.
- If `PuTTYcgn.exe` does not display, install it using the procedure in the “Installation” chapter, before proceeding to the next step.

4 Obtain the Fully Qualified Domain Name of the NM Client:

a On the NM Client, right-click **Start**. Select **Control Panel**.

b In the **Control Panel** window, select **System and Security** → **System**.

c In the **Computer name, domain, and workgroup settings** area, the **Full computer name** field lists the Fully Qualified Domain Name of this NM Client.

d Record the **Full computer name** or leave this window open to access this information during the NM Client SSH key generation procedures.

4.14 SSH Key Rotation for ATIA Log Viewer on NM Clients

This section provides procedures for SSH key rotation between Network Management (NM) Clients and the Air Traffic Router (ATR), for the ATIA Log Viewer application on the NM Client.

The procedures in this section need to be repeated for each NM Client and, in multizone systems, for each Air Traffic Router (ATR). For the proper sequence to perform these procedures, see SSH Rotation on Devices Using Default Keys on page 60.

4.14.1 Replacing ATIA Log Viewer ATR Entries in the NM Client Known Hosts List

Prerequisites:
Ensure that a new SSH server key has been generated on the ATR. For the proper sequence to perform these procedures, see SSH Rotation on Devices Using Default Keys on page 60.

When and where to use:

To replace entries in a Network Management (NM) Client known hosts list for the ATIA Log Viewer applications interface to Air Traffic Routers (ATR), perform the following procedures.

Process:

1 Deleting ATIA Log Viewer ATR Entries in an NM Client Known Hosts List on page 97

2 Adding ATIA Log Viewer ATR Entries to an NM Client Known Hosts List on page 98

3 Repeat the above steps for each NM Client (and for each ATR, in multizone systems, and in single-zone systems with the Dynamic System Resilience feature implemented).

4.14.1.1
Deleting ATIA Log Viewer ATR Entries in an NM Client Known Hosts List

Perform the following procedure to delete existing entries for the ATIA Log Viewers interface to Air Traffic Routers (ATRs) in the known hosts list on a Network Management (NM) Client.

When and where to use:
The procedure needs to be repeated for each NM Client (and for each ATR, in multizone systems, and in single-zone systems with Dynamic System Resilience feature implemented).

NOTICE: For default key removal during an initial key rotation, this procedure requires you to enter IP addresses of devices not in your system that are included by default in the NM Client known hosts list. You can create a list of these devices by performing the procedure in Detecting Default Entries in an NM Client Known Hosts List on page 104.

Procedure:

1 Ensure that new SSH host keys have been generated on the ATR(s) you will add to the NM Client's known hosts list.

See SSH Rotation on Devices Using Default Keys on page 60.

2 Log on to the NM Client using your Active Directory account that is a member of the "secadm" user group.

See Logon to Network Management Clients SSH Configuration on page 94.

The desktop appears.

3 From **Start**, select **All apps** → **Motorola** → **manageKnownHosts**.

4 In the **KnownHostManager** window, click **Delete Key**.

An **Input** window prompts you to enter `username@hostname`.

5 Type the following and click **OK**:`atialv@`***<IP address>***

where: ***<IP address>*** is the IP address of the ATR you want to delete from the known hosts list.

A window with one of the following messages appears:

- `Operation Failed` – displays if there are no rsa or dsa SSH host key entries for this username and server in the known hosts list.
- `Confirm Deletion` – displays with a key fingerprint, if there are SSH host key entries for this username and server in the known hosts list.

6 Perform one of the following actions:

- For the `Operation Failed` message, click **OK**.
- For the `Confirm Deletion` message, click **yes**.

7 In the **Choose** window, perform one of the following actions:

If…	Then…
If you need to delete another entry in the Known Hosts List,	perform the following actions: **a** Choose **yes**. The **Input** window appears. **b** Go to step 5.
If you are finished updating the Known Host List,	choose **no**. The **KnownHostManager** window appears.

8 Close the **KnownHostManager** window.

The desktop appears.

4.14.1.2
Adding ATIA Log Viewer ATR Entries to an NM Client Known Hosts List

Perform the following procedure to add new entries for the ATIA Log Viewers interface to that ATR in the known hosts list on a Network Management (NM) Client.

The procedure needs to be repeated for each NM Client (and for each ATR, in multizone systems, and in single-zone systems with Dynamic System Resilience feature implemented).

Prerequisites: This procedure assumes that a new SSH server key has been generated on the ATR. For the proper sequence to perform these procedures, see SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1 Ensure that new SSH host keys have been generated on the ATR(s) you will add to the NM Clients known hosts list.

See SSH Rotation on Devices Using Default Keys on page 60.

2 Log on to the NM Client using your Active Directory account that is a member of the “secadm” user group.

See Logon to Network Management Clients SSH Configuration on page 94.

The desktop appears.

3 From **Start**, select **All apps** → **Motorola** → **manageKnownHosts**.

4 In the **KnownHostManager** window, click **Update Key**.

5 In the **Input** window, type the following and click **OK**: `atialv@<IP address>`

where `<IP address>` is the IP address of the ATR you want to add to the known hosts list.

One of the following messages appears:

- If the SSH host key for this username and ATR is not in the known hosts list, the message displays a fingerprint and asks if you want to continue.
- If the SSH host key for this username and ATR is in the known hosts list but the fingerprint does not match, the message displays the new fingerprint and asks if you want to replace the old key with the new key.
- If the SSH host key for this username and ATR is in the known hosts list and the fingerprint does match, the message confirms the key is already in the known hosts list, and displays the fingerprint.

6 Perform one of the following actions:

If…	Then…
If the message displays a fingerprint and asks if you want to continue,	go to the next step.
If the message displays the new fingerprint and asks if you want to replace the old key with the new key,	go to the next step.
If the message confirms the key is already in the known hosts list, and displays the fingerprint,	perform the following actions: **a** Verify the fingerprint. **b** Click **OK**. **c** Go to the next step.

7 Verify the fingerprint by comparing it to the fingerprint from the most recent SSH host key generation on this ATR. Choose **Yes** to continue.

8 In the **SSH banner** window, click **OK** to close the banner window.

9 In the **Choose** window, perform one of the following actions:

If…	Then…
If you need to update the Known Host List for an ATR in another zone,	perform the following actions: **a** Choose **Yes**. The **Input** window appears. **b** Go to step 4.
If you are finished updating the Known Host List,	choose **No**. The **KnownHostManager** window appears.

10 Close the **KnownHostManager** window.

The desktop appears.

4.14.2
Generating SSH Client Keys for the NM Client ATIA Log Viewer

The following procedure describes how to generate SSH client keys (RSA and DSA) required by the ATIA Log Viewer application on a Network Management (NM) Client in an ASTRO® 25 communication system. The procedure replaces SSH keys used for a non-interactive process between the Air Traffic Routers (ATRs) and NM Clients.

Prerequisites: Preparing to Generate SSH Client Keys on an NM Client on page 96

When and where to use: This procedure uses a version of PuTTY that has been customized by Motorola Solutions.

NOTICE: Motorola Solutions version adds `PuTTYcgn.exe`, which is a version of PuTTY Unix PuTTYgen that has been modified for the Microsoft Windows operating systems used in ASTRO® 25 systems.

Repeat this procedure on each NM Client (for the proper sequence to follow, see SSH Rotation on Devices Using Default Keys on page 60).

Procedure:

1. Log on to the NM Client using your Active Directory account that is a member of the “secadm” user group.

   See Logon to Network Management Clients SSH Configuration on page 94.

   The desktop appears.

2. Verify that `PuTTYcgn.exe` was installed on this NM Client.
3. Verify that the NM Clients Fully Qualified Domain Name is available for use in the following key generation steps.
4. Open the command prompt window.
5. Navigate to the following directory in the command window: `C:\ProgramData\Motorola \Motorola PRNM Suite\security`.

   The directory is where the SSH client key files need to be located on an NM Client.

6. Enter the following command:

   `"%MOTOROLA%\Network Mgmt\security\generateSSHKeys.bat"`

   `atialv` ***<hostname>***

   where ***<hostname>*** is the Fully Qualified Domain Name (including the domain) of this NM Client.

   Both RSA and DSA (both private and public) keys are generated.

7. At the command prompt, enter: `dir`
8. In the comand prompt list of results, perform the following actions:
   a. Verify that all the file names you specified in the preceding steps appear in the `C:\ProgramData\Motorola\Motorola PRNM Suite\security` directory.
   b. Verify that the current date and time display on the following files:
      - `id_dsa_atialv_key`
      - `id_dsa_atialv_key.pub`
      - `id_rsa_atialv_key`
      - `id_rsa_atialv_key//pub`
9. Close the command prompt window.

4.14.3
Transferring Keys Securely from an NM Client to an ATR for ATIA Log Viewer

Perform the following procedure to transfer keys from a Network Management (NM) Client to an Air Traffic Router (ATR) for the non-interactive SSH connection between the NM Client and the ATR.

When and where to use: Repeat this procedure for each NM Client and, in multizone systems, for each Air Traffic Router (ATR). For the proper sequence to follow, see SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1. Log on to the NM Client using your Active Directory account that is a member of the “secadm” user group.

   See Logon to Network Management Clients SSH Configuration on page 94.

   The desktop appears.

2. Open the command prompt window.
3. At the command propmt, copy the RSA key to the ATR. Enter:

   ```
   pscp "C:\ProgramData\Motorola\Motorola PRNM Suite\security
   \id_rsa_atialv_key.pub"
   ```

   <username>`@atr`***<0Y>***`.zone`***<X>***`:/tmp/id_rsa_atialv_key.pub_nmclient`

   where:

   - ***<username>*** is your Active Directory account that is a member of the atr-login user group
   - ***<0Y>*** is the number of the ATR (01 in a primary core, 02 in a backup core)
   - ***<X>*** is the zone where the ATR resides

4. If a key fingerprint appears and you are asked whether to store the servers host key in cache, verify the fingerprint then enter `y` to accept storing the key in cache.

   You are prompted to enter a password.

5. Enter the password for your Active Directory account that is a member of the atr-login user group.

4.14.4
Updating the ATR Authorized Keys List for ATIA Log Viewer

Perform the following procedure to replace SSH user keys in the authorized keys list on an Air Traffic Router (ATR) for the non-interactive SSH connection between an NM Client and an ATR.

When and where to use:
Repeat this procedure for each NM Client and, in multizone systems, for each Air Traffic Router (ATR). For the proper sequence to follow, see SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1. Access the root command prompt for the ATR server.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. Update the authorized keys list with the RSA SSH public client keys for this NM Client, by executing the following commands:

   ```
   /opt/Motorola/ssh/bin/manage_authorized_keys
   ```

```
-a /tmp/id_rsa_atialv_key.pub_nmclient -u atialv
```

The authorized keys list now contains the new RSA SSH client public keys for the specified NM Client, for the non-interactive atialv account. Any keys with the same key comment are replaced.

3 Remove the temporary files by executing the following command: `rm /tmp/id_rsa_atialv_key.pub_nmclient`

The RSA SSH client keys are removed from the `/tmp/` directory.

4.14.5
Verifying the SSH Configuration for ATIA Log Viewer on the NM Client

Perform the following procedure on each Network Management (NM) Client, to verify that the non-interactive SSH connection between the NM Client and an Air Traffic Router (ATR) is working properly for the ATIA Log Viewer application on the NM Client.

Prerequisites:
For multizone systems:

- Start by testing the ATIA Log Viewer when it is set up to connect only to the ATR in the same zone as the NM Client.
- Repeat this procedure with the ATIA Log Viewer set up for connections to ATRs in other zones, and then for NM Clients in other zones.
- Repeat this for other NM Clients, including any NM Clients in other zones.

When and where to use: If errors occur while performing this procedure, see SSH Rotation on Devices Using Default Keys on page 60 to verify what SSH configuration steps for ATIA Log Viewer were missed.

Procedure:

1 If ATIA Call Logging has not yet been enabled on an ATR accessed by the ATIA Log Viewer on this NM Client, perform the following actions:

a Log on to the ATR server using your Active Directory account.

See Use of a Domain Account to Log on to Devices Using Default Keys on page 93.

The ATR command prompt displays.

b Enter: `admin_menu`

The ATR server administration menu displays.

c Enter the number for the menu option **Application Administration**.

The Application Administration menu displays.

d Enter the number for the menu option **ATIA Call Logging Parameter Setup**.

The ATIA Call Logging Parameter Setup menu displays.

e Enter the number for the menu option **Enable ATIA Call Logging**.

ATIA Call Logging is enabled and the ATIA Call Logging Parameter Setup menu displays.

f Enter the number for the menu option **ATIA Call Logging Status**.

ATIA Call Logging status is displayed as enabled and the ATIA Call Logging Parameter Setup menu displays.

2 Log on to the NM Client using any authorized account.

You can use an account that you used for the previous procedures in this section, as indicated in Logon to Network Management Clients SSH Configuration on page 94.

3 Launch ATIA Log Viewer on the NM Client.

Ensure that the list of available log files displays and that ATIA Log Viewer does not show any error messages.

4.15 Verifying That SSH Keys Are No Longer Being Used by an NM Client

The following process provides a way to verify that SSH keys are no longer being used by a Network Management (NM) Client, after performing the initial SSH key rotation for the ATIA Log Viewer application on the NM Client, according to the SSH Rotation on Devices Using Default Keys on page 60.

NOTICE: This process does **not** affect the known hosts list for the Configuration/Service Software (CSS) application on NM Clients.

Prerequisites: Ensure that:

1 You know the numbers of the zones in your system.

2 For the Air Traffic Router (ATR) server in each zone, Removing Default SSH Client Keys from an Authorized Keys List for Network Management Servers on page 147 has been completed.

Process:

1 Log on to the NM Client using your Active Directory account that is a member of the “secadm” user group.

See Logon to Network Management Clients SSH Configuration on page 94.

The desktop appears.

2 Back up SSH settings on each NM Client:

a From **Start**, select **All apps** → **Motorola**.

b Right-click **backupSshSettings** and select **Run as Administrator** from the context menu.

This backs up the known hosts list and keys for all non-interactive accounts on the NM Client where you are logged in.

NOTICE:
If the **User Account Control** window appears, click **Allow** or **Continue** option, depending on the prompt.

If the password prompt appears, enter administrator’s credentials and continue.

3 For each NM Client in each zone, perform Removing Remaining Default Entries from an NM Client Non-Interactive Known Hosts List on page 105.

4 For each NM Client in each zone, repeat the Verifying the SSH Configuration for ATIA Log Viewer on the NM Client on page 102 procedure.

5 For each NM Client, for each interactive user account that may have added keys for an SSH host device to an NM Client known host list before the keys were regenerated on that SSH host device, perform Removing Interactive Entries from the Known Hosts List on an NM Client on page 95.

4.15.1

Detecting Default Entries in an NM Client Known Hosts List

Perform this procedure to detect default entries in non-interactive account known hosts lists on a Network Management (NM) Client, as part of SSH key rotation to secure the non-interactive connection used by the ATIA Log Viewer application.

NOTICE: This procedure does **not** detect default key entries that a PuTTY user may have added to an NM Client known hosts list by selecting **Yes** at a fingerprint verification prompt, before the SSH server device keys were initially rotated.

When and where to use: Repeat this procedure for each NM Client. For the proper sequence to perform these procedures, see SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1 Log on to the NM Client using your Active Directory account that is a member of the “secadm” user group.

See Logon to Network Management Clients SSH Configuration on page 94.

The desktop appears.

2 From **Start**, select **All apps** → **Motorola** → **puttyDefaultKeyDetector**.

A command window displays a list of SSH hosts with default host key entries in the NM Client known hosts list.

3 Perform one of the following actions:

If…	Then…
If a message displays with the following format: `Default OpenSSH Host Key found ssh-<rsa or dsa>:atialv@<server IP address>` **informing that the known hosts list includes default SSH host key entries used by the ATIA Log Viewer application,**	perform the following actions: **a** Record the displayed IP addresses (and corresponding account name, if displayed) for use in default key removal procedures. **b** Perform the appropriate default key removal procedures. **c** Repeat this detection procedure.
If a message displays with one of the following formats: • `Default OpenSSH key found id_rsa_atialv_key` **informing about the detection of the default SSH RSA client keys used by the ATIA Log Viewer application on the NM Client,** • `Default OpenSSH key found id_dsa_atialv_key` **informing about the detection of the default SSH DSA client keys used by the ATIA Log Viewer application on the NM Client,**	perform the following actions: **a** Go to SSH Rotation on Devices Using Default Keys on page 60. **b** Perform the steps missed for rotating the SSH client keys on the NM Client that are used by the ATIA Log Viewer application. **c** Repeat this detection procedure.

4 Close the command window.

4.15.2

Removing Remaining Default Entries from an NM Client Non-Interactive Known Hosts List

When and where to use: This procedure deletes default entries from non-interactive known hosts lists on a Network Management (NM) Client, including entries that were included in the list by default for Air Traffic Routers (ATRs) not in your system.

NOTICE: This procedure does **not** apply to the known hosts list for the Configuration/Service Software (CSS) application on NM Clients.

For the proper sequence in which to perform key rotation procedures, see SSH Rotation on Devices Using Default Keys on page 60. (This indicates the proper point in the overall sequence to perform Verifying That SSH Keys Are No Longer Being Used by an NM Client on page 103.)

Procedure:

1. Create a list of the IP addresses of devices not in your system that still remain in the NM Client known hosts list.

   See Detecting Default Entries in an NM Client Known Hosts List on page 104.
   The list of IP addresses should be in the ***<username>***`@`***<IP address>*** format. You need to know the username associated with each IP address in order to delete it from the list.

2. Log on to the NM Client using your Active Directory account that is a member of the “secadm” user group.

   See Logon to Network Management Clients SSH Configuration on page 94.

   The desktop appears.

3. From **Start**, select **All apps** → **Motorola** → **manageKnownHosts**.
4. In the **KnownHostManager** window, click **Delete Key**.
5. Perform the following actions:
   a. In the **Input** window, if needed, change the username to match the username that is associated with an IP address you need to delete.
   b. Immediately after ***<username>***`@`, type the IP address for the entry you want to delete from the known hosts list.
   c. Click **OK**.

   A window with one of the following messages appears:

   - `Operation Failed` displays if there are no rsa or dsa SSH host key entries for this username and server in the known hosts list.
   - `Confirm Deletion` displays with a key fingerprint, if there are SSH host key entries for this username and server in the known hosts list.

6. Perform one of the following actions:
   - For the `Operation Failed` message, click **OK**.
   - For the `Confirm Deletion` message, click **yes**.
7. In the **Choose** window, perform one of the following actions:

If…	Then…
If you need to delete another entry in the known hosts list,	perform the following actions:

If…	Then…
	a Choose **yes**. The **Input** window appears. **b** Go to step 5.
If you are finished updating the Known Host List,	choose **no**. The **KnownHostManager** window appears.

8 Close the **KnownHostManager** window.

The desktop appears.

4.16
Backing Up SSH Data for NM Clients Manually

When and where to use:
If the centralized backup and restore feature is not implemented, you can use the following procedure for backing up SSH data for Network Management (NM) Clients.

NOTICE: This procedure does not apply to the SSH data for the Configuration/Service Software (CSS) application on NM Clients, which is covered in a separate section.

Procedure:

1 Log on to the NM Client using your Active Directory account that is a member of the “secadm” user group.

See Logon to Network Management Clients SSH Configuration on page 94.

The desktop appears.

2 Back up SSH settings on each NM Client:

a From **Start**, select **All apps** → **Motorola**.

b Right-click **backupSshSettings** and select **Run as Administrator** from the context menu.

This backs up the known hosts list and keys for all non-interactive accounts on the NM Client where you are logged in.

NOTICE:
If the **User Account Control** window appears, click **Allow** or **Continue** option, depending on the prompt.

If the password prompt appears, enter administrator’s credentials and continue.

The **ssh backup** window appears. The window contains no error messages. Only INFO messages appear.

3 Press ENTER to close the window.

The desktop appears.

4.17
Restoring SSH Data for NM Clients Manually

When and where to use:
If the centralized backup and restore feature is not implemented, you can use the following procedure for restoring SSH data for Network Management (NM) Clients.

NOTICE: This procedure does not apply to the SSH data for the Configuration/Service Software (CSS) application on NM Clients, which is covered in a separate section.

Procedure:

1 Log on to the NM Client using your Active Directory account that is a member of the “secadm” user group.

See Logon to Network Management Clients SSH Configuration on page 94.

2 Restore SSH settings on each NM Client:

a From **Start**, select **All apps** → **Motorola**.

b Right-click **restoreSshSettings** and select **Run as Administrator** from the context menu.

This restores the known hosts list and keys for all non-interactive accounts on the NM Client where you are logged in.

NOTICE:
If the **User Account Control** window appears, click **Allow** or **Continue** option, depending on the prompt.

If the password prompt appears, enter administrator’s credentials and continue.

3 Press ENTER to close the window.

The desktop appears.

4.18 SSH Key Rotation on NM Servers, ZCs, ISGWs and PDGs

This section provides the key rotation procedures for non-interactive SSH sessions between the following Linux-based devices:

System level:

- Unified Network Configurator (UNC)
- Unified Network Configurator Device Servers (UNCDS)
- User Configuration Server (UCS)
- System Statistics Server (SSS)

Zone level:

- Zone Statistics Server (ZSS)
- Zone Database Server (ZDS)
- Unified Event Manager (UEM) Server
- Air Traffic Router (ATR)
- Zone Controller (ZC)
- Packet Data Gateway (PDG)
- ISGW (ISSI 8000/CSSI 8000)
- License Manager

NOTICE: Do **not** perform the procedures in this section in an ASTRO® 25 system K master site configuration. The PDG is the only device listed above that may be present in a K master site, and in that configuration, it does not require the SSH key rotation procedures provided in this section.

For the proper sequence to perform SSH configuration for the devices listed here, see SSH Rotation on Devices Using Default Keys on page 60.

4.18.1
SSH Key Rotation Process – Preparation

Before performing the key rotation procedures in this section, obtain the following information from your system administrator:

- Usernames and passwords for the interactive accounts used in these key rotation procedures
- Number of zones installed
- IP addresses and Fully Qualified Domain Name (FQDN) of each device in each zone as required in these key rotation procedures. Also see the following table and Table 16: FQDN to Use in Commands for Rotating SSH Keys for Network Management Servers on page 127.

Table 12: Names to Use in SSH Key Rotation Commands for Generic Application Servers

Resident Server Applications	Generic Application Server Name to Use in Commands (FQDN)

Zone-level server applications	FQDN of the GAS for the RF GASes, where FQDN is in the ***<hostname.domainname>*** format.
	
	To determine the FQDN of the Generic Application Server where you are currently logged on, you can execute the following Solaris commands:
	
	`hostname`
	
	`domainname`

4.18.2
SSH Key Rotation Process – Recommendations

The procedures in this section should be performed in the sequence specified in the SSH Rotation on Devices Using Default Keys on page 60.

Before you begin, it is recommended that you study the process carefully, and consider the recommendations that follow:

- Procedures in the following section rotate SSH keys for specific *non-interactive* SSH connections required for ASTRO® 25 communication system operation. For the initial rotation after an ASTRO® 25 system installation that included default keys, procedures are provided for replacing the defaults for devices in your system, then detecting and removing defaults for devices not in your system, but only for the specific non-interactive SSH connections required for ASTRO® 25 system operation. It is possible for a user who initiates an *interactive* SSH session with an SSH server device to create a known hosts list entry for a default SSH host key that cannot be removed with procedures for non-interactive accounts in this manual.
  - Instructions for preventing these entries in an NM Client known hosts list are provided in Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.
  - Guidance for removing unexpected default entries in an NM server known hosts list are provided in Additional Default Key Removal Considerations – Unexpected Default Entries in Known Hosts Lists on page 150.
  - Instructions for removing these extra entries in an NM Client known hosts list are provided in Removing Interactive Entries from the Known Hosts List on an NM Client on page 95.
  - Instructions for removing extra entries in known hosts lists on service laptops are beyond the scope of this manual.

- The procedures in this section may take several hours to complete. To track your progress and keep your place in case of interruptions, check off each step in each procedure as you complete it, and check off each procedure in the SSH Rotation on Devices Using Default Keys on page 60 as you complete it. It is recommended that you customize a checklist for your system configuration. (Examples are provided in Appendix A and Appendix B.)
- If you copy and paste commands from this PDF file to the command line, then be sure to check them carefully before you execute them, and correct any character substitutions that may have occurred.
- If you have questions about the syntax of a command or the arguments provided for the command in a procedure, type the command using the same path as indicated in the procedure, except use `-h` as the only argument. This displays help for all the arguments supported by the command. For example, on a Network Management server, type `/opt/Motorola/ssh/bin/manage_authorized_keys -h` to display help for that command.
- You can log into multiple server devices in multiple terminal session windows. However, each session may automatically terminate after a period of inactivity.

For additional considerations, see SSH Key Rotation Impact on ASTRO 25 System Non-Interactive Services on page 208 and other topics in the "Operation" chapter and "Troubleshooting" chapter.

4.18.3
Enabling/Disabling Clear Mode and Secure Mode

Enabling and disabling *secure* mode is not supported in an ASTRO® 25 system.

The only NM servers that support enabling and disabling *clear* mode are the UNC server and the UNCDS. The UNC server and UNCDS administration menus provide options for enabling and disabling FTP and TFTP (these options are on the **FTP Services** menu under the **Application Administration** menu).

4.18.4
Verifying SSH Connectivity

When and where to use: Perform the following procedures before key rotation to test the existing SSH keys, or after a key rotation to test the new SSH keys.

Process:

1. Perform Verifying SSH Connectivity Between Network Management Servers, ZCs and ISGWs on page 110 on each of the following:
   - Unified Network Configurator (UNC) server
   - Unified Network Configurator Device Servers (UNCDS)
   - User Configuration Server (UCS)
   - System Statistics Server (SSS)
   - Zone Statistics Server (ZSS)
   - Zone Database Server (ZDS)
   - Unified Event Manager (UEM) Server
   - Air Traffic Router (ATR)
   - Zone Controller (ZC)
   - ISGW (ISSI 8000/CSSI 8000)
2. Perform Verifying SSH Connectivity Between a PDG and a UNC Server on page 110 on the Packet Data Router (PDR) module of each Packet Data Gateway (PDG).

4.18.4.1

Verifying SSH Connectivity Between Network Management Servers, ZCs and ISGWs

When and where to use:
Perform the following procedure to verify that the NM server, zone controller or ISGW that you log into can initiate SSH sessions with all supported devices using the following non-interactive SSH accounts:

- sshserv
- (For ATRs only): ATR-UNC SSH client account
- (For ZCs only): ZC-UNC SSH client account
- (For ISSI 8000/CSSI 8000 only): ISGW-UNC SSH client account
- (For SSS only): SSS-UNC SSH client account

Procedure:

1. Access the root command prompt on the NM Server, ZC or ISGW.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. Execute the following command:

   ```
   /opt/Motorola/ssh/bin/verify_ssh_connectivity
   ```

   The script tests all non-interactive secure connections that are supported for this device to initiate. Each connection displays under one of the following messages:

   ```
   SSH connection verification was not executed for the following
   servers.
   This could be due to the device not being physically present on the
   network
    or a general TCP/IP connection issue associated with a valid device
   on the network.
   ```

   ```
   SSH connection verification failed for the following servers.
   This is most likely due to the keys not being properly rotated.
   Refer to the verify_ssh_connectivity.log file for determining
   the cause of the failure
   ```

   ```
   SSH connection verification was completed successfully
   for the following servers.
   ```

   The log file is located in the root directory (where you executed the command).

3. Address any problems for devices in your system and repeat this verification procedure.

4.18.4.2

Verifying SSH Connectivity Between a PDG and a UNC Server

Perform the following procedure to verify that the Packet Data Gateway (PDG) that you log into can initiate SSH sessions with a UNC server:

Procedure:

1. Access the root command prompt for the PDG.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. Enter the following command:

   ```
   /opt/Motorola/ssh/bin/verify_ssh_connectivity
   ```

   A `Verified connection` or `ERROR: Failed verification` message displays for each connection tested. Validate the results as follows:

- If a backup core is present, a `Verified connection` message should display for the connection to ucs-unc01.ucs and the connection to ucs-unc02.ucs.
- If a backup core is not present, a `Verified connection` message should display for the connection to ucs-unc01.ucs, and an `ERROR: Failed verification` message will display for the backup core UNC server (ucs-unc02.ucs). If a backup core is not present, perform the procedure in Removing Backup Core UNC Server Defaults in a PDG Known Hosts List (Non-DSR Systems Only) on page 152, according to the sequence of procedures specified in the SSH Rotation on Devices Using Default Keys on page 60.

If any errors display, the error messages are saved in `verify_ssh_connectivity.log` in the directory where you logged in when you executed the verify_ssh_connectivity command. Address any problems for devices in your system and repeat this verification procedure.

3 Enter the following at the PDG console to log out of the PDG: `exit`

4.18.5
Host Key Generation on SSH Servers

This section lists the commands for generating SSH host (server) keys on Linux-based devices. For each of these commands entered, the specified types of SSH server keys (RSA or DSA) are generated for the specified SSH server. The public SSH host (server) keys are stored in a .pub file under `/etc/ssh/`.

This section does **not** apply to the following devices:

- ISSI.1 Network Gateway site modules on Generic Application Servers. For instructions on generating SSH host keys on ISSI.1 Network Gateways, see: Regenerating SSH Host Keys for an ISSI.1 Network Gateway Site on page 153.
- Devices that do not require host keys.

NOTICE: For optimal security, record the fingerprints of the SSH host keys that you generate, for comparison to fingerprints later in the process.
For maximizing system availability, perform SSH host key rotation in the sequence specified in the SSH Rotation on Devices Using Default Keys on page 60.

IMPORTANT:
It is recommended that system migration should **not** be performed during an SSH key rotation.

The commands in the following tables include Fully Qualified Domain Names (FQDNs) in the format hostname.domainname, for the server you are currently logged into. To determine the FQDN of the server where you are currently logged in, you can execute the following commands:

- `hostname`
- `domainname`

The commands in these tables are executed after accessing the servers root prompt. See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

For more information on the key length value, see Key Management on page 37.

Related Links

Configuring SSH for Devices at the Zone Core on page 47

4.18.5.1

SSH Host Key Generation on Generic Application Server – Commands To Use

The following table provides the commands for generating new SSH server keys on the Generic Application Server.

NOTICE: The ISSI.1 feature is supported on a Generic Application Server (GAS) server. For detailed information regarding GAS and ISSI.1, see the *Generic Application Server* manual and the *ISSI.1 Network Gateway Feature Guide*.

Table 13: SSH Host Key Generation on GAS – Commands To Use

SSH Servers	Command

Generic Application Server	`/opt/Motorola/ssh/bin/gen_server_keys -l 2048 -c <hostname.domainname>`
	where `<hostname.domainname>` is the FQDN for the RF GASes.
	To determine the FQDN of the Generic Application Server where you are currently logged on, you can execute the following Solaris commands:
	`hostname`
	`domainname`

4.18.5.2

SSH Host Key Generation on System-Level Servers – Commands To Use

The following table provides the commands for generating new SSH host keys on the system-level Linux-based servers.

NOTICE: The UEM, ZSS, SSS, and ZC SSH server host keys require key rotation only for interactive access. (These devices do not function as SSH servers for non-interactive operations.)

Table 14: SSH Host Key Generation on System-Level Servers – Commands To Use

SSH Servers	Command
Unified Network Configurator (UNC) Server	`/opt/Motorola/ssh/bin/gen_server_keys -l 2048 -c ucs-unc0<Y>.ucs` where `<Y>` is the number assigned to this server
Unified Network Configurator Device Servers (UNCDS)	`/opt/Motorola/ssh/bin/gen_server_keys -l 2048 -c ucs-uncds0<Y>.ucs` where `<Y>` is the number assigned to this server (1, 2, or 3)
User Configu-	`/opt/Motorola/ssh/bin/gen_server_keys -l 2048 -c ucs0<Y>.ucs`

SSH Servers	Command
ration Server (UCS)	where **<Y>** is the number assigned to this server
System Statistics Server (SSS)	`/opt/Motorola/ssh/bin/gen_server_keys -l 2048 -c sss0<Y>.ucs` where **<Y>** is the number assigned to this server

4.18.5.3

SSH Host Key Generation on Zone-Level Servers – Commands to Use

The following table provides the commands for generating SSH host keys on the zone-level Linux-based servers.

Table 15: SSH Host Key Generation on Zone-Level Servers – Commands to Use

SSH Servers	Command
Unified Event Manager (UEM) Server	`/opt/Motorola/ssh/bin/gen_server_keys -l 2048 -c z00<X>uem0<Y>.zone<X>` where: **<X>** is the number of the zone in which the UEM is installed **<Y>** is the number assigned to this server
Air Traffic Router (ATR)	`/opt/Motorola/ssh/bin/gen_server_keys -l 2048 -c atr0<Y>.zone<X>` where: **<X>** is the number of the zone in which the ATR is installed **<Y>** is the number assigned to this server
Zone Database Server (ZDS)	`/opt/Motorola/ssh/bin/gen_server_keys -l 2048 -c zds0<Y>.zone<X>` where: **<X>** is the number of the zone in which the ZDS is installed **<Y>** is the number assigned to this server
Zone Statistics Server (ZSS)	`/opt/Motorola/ssh/bin/gen_server_keys -l 2048 -c zss0<Y>.zone<X>` where: **<X>** is the number of the zone in which the ZSS is installed **<Y>** is the number assigned to this server
Zone Controller (ZC)	`/opt/Motorola/ssh/bin/gen_server_keys -l 2048 -c zc0<Y>.zone<X>` where: **<X>** is the number of the zone in which the zone controller is installed **<Y>** is the number assigned to this zone controller
Packet Data Gateway (PDG)	`/opt/Motorola/ssh/bin/gen_server_keys -l 2048 -c pdr0<Y>.zone<X>` where: **<X>** is the number of the zone in which the PDG is installed **<Y>** is the number assigned to this PDG

SSH Servers	Command
Intersystem Gateway (ISGW)	`/opt/Motorola/ssh/bin/gen_server_keys -l 2048 -c z00<X>isgw0<Y>.zone<X>` where: **<X>** is the number of the zone in which the ISGW is installed **<Y>** is the number assigned to this ISGW for the ISSI 8000/CSSI 8000 feature
Backup and Restore (BAR) Server	`/opt/Motorola/ssh/bin/gen_server_keys -l 2048 -c z00<X>bkup0<Y>.zone<X>` where: **<X>** is the number of the zone in which BAR is installed **<Y>** is the number assigned to this BAR
Centralized Event Logging Server	`/opt/Motorola/ssh/bin/gen_server_keys -l 2048 -c z00<X>log0<Y>.zone<X>` where: **<X>** is the number of the zone in which the Centralized Event Logging Server is installed **<Y>** is the number assigned to this server
IP Packet Capture	`/opt/Motorola/ssh/bin/gen_server_keys -l 2048 -c z00<X>ipcap0<Y>.zone<X>` where: **<X>** is the number of the zone in which the IP Packet Capture is installed **<Y>** is the number assigned to this server
License Manager	`/opt/Motorola/ssh/bin/gen_server_keys -l 2048 -c z00<X>lm0<Y>.zone<X>` where: **<X>** is the number of the zone in which License Manager is installed **<Y>** is the number assigned to this server

4.18.6
NM Servers, ZCs and ISGWs Update in Known Hosts Lists – Overview

The sections following this overview provide the procedures for updating known hosts lists on SSH clients for specific non-interactive accounts required for connecting with Linux-based SSH servers in ASTRO® 25 systems.

NOTICE: The procedures in the following sections do **not** apply to ISSI.1 Network Gateway site modules.

These procedures must be performed after new SSH server (host) keys are regenerated, in the sequence specified in SSH Rotation on Devices Using Default Keys on page 60. To locate the procedures you are ready to perform in that process, you can use the links below, for the Network Management server that has new SSH host keys ready to be propagated:

- Known Hosts Lists Update After Regenerating ATR Host Keys on page 115
- Known Hosts Lists Update After Regenerating UCS Host Keys on page 117
- Known Hosts Lists Update After Regenerating UNC Server Host Keys on page 118

The procedures in the following sections require accessing the root prompt on Network management servers, zone controllers and ISGWs.

For more information, see Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

The procedures in the following sections start by deleting specific existing entries in the known hosts list. (This is the recommended approach, instead of deleting the entire list, to minimize the amount of time that mismatched host keys on the SSH hosts and SSH clients prevent secure non-interactive communications.)

NOTICE: Deleting an entry in the known hosts list for a hostname automatically deletes entries with IP addresses associated with that hostname.

Also, for the default entries in known hosts lists that include all DNS names in one entry, separate commands for removing for each DNS name are not needed. However, they are included in these procedures for when you perform these procedures as part of a subsequent key rotations, when separate commands will be needed.

For the variables in procedures, replace ***<X>*** with the number of the zone where the device resides. You can determine the zone number by entering `domainname` at the command prompt.

Replace `0`***<Y>*** with the number of the device you are configuring (01 for devices in the primary core and 02 for devices in a DSR backup core, if present, with two exceptions:

- Redundant zone controllers are numbered 01 and 02 in the primary core, and 03 and 04 in a DSR backup core
- Redundant ISGWs are numbered 01 and 02 in the primary core; and 03 and 04 in a DSR backup core

For the steps in these procedures that require verifying the fingerprint of the SSH server (host), refer to the fingerprints you recorded when generating the keys on the SSH servers, or execute the following command on a Linux- or Solaris-based SSH server to view its fingerprint (before executing this command, connecting to the device using a terminal server is recommended, instead of connecting over the network):

```
ssh-keygen -lf /etc/ssh/ssh_host_rsa_key
```

After you accept the host, there are two possible results:

- The system name (output from the `hostname` command) will display at the command line.
- An “access denied” message means that SSH clients user keys do not match the keys in the SSH servers authorized list of keys. This is unexpected during these procedures because user key rotation will not be occurring at the same time as host key rotation, if you are following the SSH Rotation on Devices Using Default Keys on page 60.

In either case, the known hosts list has been successfully updated.

4.18.7
Known Hosts Lists Update After Regenerating ATR Host Keys

This section provides the procedures for updating known hosts lists on Linux- or Solaris-based devices after generating new SSH host keys on an Air Traffic Router (ATR).

4.18.7.1
Updating Known Hosts List on the ZSS for Connections to an ATR

When and where to use:

After generating new host keys on an ATR, perform the following procedure to update the known hosts list on the ZSS for non-interactive connections to the ATR.

Procedure:

1. Access the root command prompt on the ZSS.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. Execute the following commands to delete any existing entries for the ATR in the known hosts list on the ZSS for the sshserv account:

   ```
   /opt/Motorola/ssh/bin/manage_known_hosts -u sshserv -d atr0<Y>.zone<X>
   /opt/Motorola/ssh/bin/manage_known_hosts -u sshserv -d atr0<Y>
   ```

   where ***<X>*** is the zone number and ***<Y>*** is the number of the ATR with the new SSH host keys

3. To establish a connection to the ATR, enter:

   ```
   sudo -u sshserv ssh sshserv@atr0<Y>.zone<X> hostname
   ```

   where:

   <X> is the zone number

   <Y> is the number of the ATR with the new SSH host keys

4. After verifying the ATR fingerprint, at the command prompt, enter: `Yes`

   The key for this DNS name is added to the ZSS known hosts list for the sshserv account. The ATR system name displays, or a permission denied message displays.

5. To establish another connection to the same ATR, enter:

   ```
   sudo -u sshserv ssh sshserv@atr0<Y> hostname
   ```

   where ***<Y>*** is the number of the ATR with the new SSH host keys

6. After verifying the ATR fingerprint, at the command prompt, enter: `Yes`

   An entry for this hostname is added to the ZSS known hosts list for the sshserv account. The ATR system name displays, or a permission denied message displays.

7. Enter: `exit`

4.18.7.2

Updating Known Hosts List on the SSS for Connections to an ATR

When and where to use: After generating new host keys on an ATR, perform the following procedure to update the known hosts list on the SSS for non-interactive connections to the ATR.

Procedure:

1. Access the root command prompt on the SSS.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. To delete any existing entries for the ATR in the known hosts list on the SSS for the sshserv account, enter:

   ```
   /opt/Motorola/ssh/bin/manage_known_hosts -u sshserv -d
   atr0<Y>.zone<X>
   ```

   where:

   <X> is the zone number

   <Y> is the number of the ATR with the new SSH host keys

3. To establish a connection to the ATR, enter:

   ```
   sudo -u sshserv ssh sshserv@atr0<Y>.zone<X> hostname
   ```

where:

<X> is the zone number

<Y> is the number of the ATR with the new SSH host keys

4 After verifying the ATR fingerprint, at the prompt, enter: `Yes`

The key for this DNS name is added to the SSS known hosts list for the sshserv account. The ATR hostname displays, or a permission denied message displays.

5 Enter: `exit`

4.18.8 Known Hosts Lists Update After Regenerating UCS Host Keys

This section provides the procedures for updating known hosts lists on the UNC and UCS devices after generating new SSH host keys on the User Configuration Server (UCS).

The procedures in this section should not be performed until the new host keys for all zone-level Linux- or Solaris-based devices have been generated and updated in the appropriate known hosts lists for all zones.

4.18.8.1 Updating Known Hosts List on a UNC Server for Connections to a UCS

When and where to use:
After generating new host keys on a UCS, perform the following procedure to update the known hosts list on a UNC server for non-interactive connections to the UCS.

Procedure:

1 Access the root command prompt on the UNC server.

See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2 To delete any existing entries for the UCS in the UNC servers known hosts list for the sshserv account, enter:

`/opt/Motorola/ssh/bin/manage_known_hosts -u sshserv -d ucs0`***<Y>***`.ucs`

where ***<Y>*** is the number of the UCS with the new SSH host keys

3 To establish a connection to the UCS, enter:

`sudo -u sshserv ssh sshserv@ucs0`***<Y>***`.ucs hostname`
where ***<Y>*** is the number of the UCS with the new SSH host keys

4 After verifying the UCS server fingerprint, at the prompt, enter: `Yes`

An entry for this DNS name is added to the UNC servers known hosts list for the sshserv account. The UCS system name displays, or a `permission denied` message displays.

5 Enter: `exit`

4.18.8.2 Updating Known Hosts List on the UCS for Connections to Another UCS (DSR Systems Only)

When and where to use: Perform the following procedure to complete one of the following operations, depending on your point in the sequence specified in Performing Additional SSH Configuration Processes for DSR Systems on page 68:

- Update the known hosts list on the primary core UCS for non-interactive connections to the backup core UCS.
- Update the known hosts list on the backup core UCS for non-interactive connections to the primary core UCS.

Procedure:

1. Access the root command prompt on the UCS.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. To delete existing entries for the UCS in the known hosts list for the sshserv account on the UCS in the other core (**not** the UCS where you are logged in), enter:

   a `/opt/Motorola/ssh/bin/manage_known_hosts -u sshserv -d ucs0<Y>.ucs`

   b `/opt/Motorola/ssh/bin/manage_known_hosts -u sshserv -d ucs0<Y>`

   where `<Y>` is one of the following values:

   `1` if you are logged into ucs02

   `2` if you are logged into ucs01

3. To establish a connection to the UCS in the other core (**not** the UCS where you are logged in), enter:

   `sudo -u sshserv ssh sshserv@ucs0<Y>.ucs hostname`
   where `<Y>` is the number of the UCS you specified in the previous command

4. After verifying the UCS fingerprint, at the prompt, enter: `Yes`

   An entry for this DNS name is added to the UCS known hosts list for the sshserv account. UCS system name displays, or a `permission denied` message displays.

5. To establish another connection to the UCS, enter:

   `sudo -u sshserv ssh sshserv@ucs0<Y> hostname`
   where `<Y>` is the number of the UCS you specified in the previous command

6. After verifying the UCS fingerprint, at the prompt, enter: `Yes`

   An entry for this hostname is added to the UCS known hosts list for the sshserv account. The UCS system name displays, or a `permission denied` message displays.

7. Enter: `exit`

4.18.9
Known Hosts Lists Update After Regenerating UNC Server Host Keys

This section provides the procedures for updating known hosts lists on the following Linux- and Solaris-based devices: NM Servers, ZCs, PDGs and ISGWs after generating new SSH host keys on a Unified Network Configurator (UNC) server.

4.18.9.1
Updating Known Hosts List on a UCS for Connections to a UNC Server

When and where to use: After generating new host keys on a Unified Network Configurator (UNC) server, perform the following procedure to update the known hosts list on a User Configuration Server

(UCS) for non-interactive connections to the UNC server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1. Access the root command prompt on the UCS.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. To delete any existing entries for the UNC server in the known hosts list on the UCS for the sshserv account, enter:

   a. `/opt/Motorola/ssh/bin/manage_known_hosts -u sshserv -d ucs-unc0<Y>.ucs`

   b. `/opt/Motorola/ssh/bin/manage_known_hosts -u sshserv -d ucs-unc0<Y>`

   where ***<Y>*** is the number of the UNC server with the new SSH host keys

3. To establish a connection to the UNC server, enter:

   `sudo –u sshserv ssh sshserv@ucs-unc0<Y>.ucs hostname`
   where ***<Y>*** is the number of the UNC server with the new SSH host keys

4. Verify the fingerprint matches the fingerprint for the UNC server SSH host key that was generated most recently, then, at the prompt, enter: `Yes`

   An entry for this DNS name is added to the UCS known hosts list for the sshserv account. The UNC system name displays, or a `permission denied` message displays.

5. To establish another connection to the UNC server, enter:

   `sudo –u sshserv ssh sshserv@ucs-unc0<Y> hostname`

   where ***<Y>*** is the number of the UNC server with the new SSH host keys

6. Verify the fingerprint matches the fingerprint for UNC server SSH host key that was generated most recently, then, at the prompt, enter: `Yes`

   An entry for this hostname is added to the UCS known hosts list for the sshserv account. The UNC system name displays, or a `permission denied` message displays.

7. Enter: `exit`

4.18.9.2

Updating Known Hosts List on the UNC Server for Connections to the Same UNC Server

When and where to use: After generating new host keys on a UNC server, perform the following procedure to update the known hosts list on the UNC server for non-interactive connections to the same UNC server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

NOTICE: To configure SSH between a primary core UNC and backup core UNC, do **not** perform Updating Known Hosts List on the UNC Server for Connections to the Same UNC Server on page 119. Instead, perform the procedure specified for that in the DSR section of the SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1. Access the root command prompt on the UNC server.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. To delete any existing entries for the UNC server in the known hosts lists on the UNC server, enter:

a `/opt/Motorola/ssh/bin/manage_known_hosts -u sshserv -d ucs-unc0<Y>.ucs`

b `/opt/Motorola/ssh/bin/manage_known_hosts -u sshserv -d ucs-unc0<Y>`

where `<Y>` is the number of the UNC server you logged into in step 1.

3 To establish a connection to the UNC server, enter:

`sudo –u sshserv ssh sshserv@ucs-unc0<Y>.ucs hostname`
where `<Y>` is the number of the UNC server you logged into in step 1

4 Verify the fingerprint matches the fingerprint for UNC server SSH host key that was generated most recently, then, at the prompt, enter: `Yes`

An entry for this DNS name is added to the UNC servers known hosts list for the sshserv account. The UNC system name displays, or a `permission denied` message displays.

5 To establish another connection to the UNC server, enter:

`sudo –u sshserv ssh sshserv@ucs-unc0<Y> hostname`
where `<Y>` is the number of the UNC server you logged into in step 1

6 Verify the fingerprint matches the fingerprint for UNC server SSH host key that was generated most recently, then, at the prompt, enter: `Yes`

An entry for this DNS name is added to the UNC servers known hosts list for the sshserv account. The UNC system name displays, or a `permission denied` message displays.

7 To close the user shell, enter: `exit` twice.

8 Delete SSH Keys for 10.0.0.2 and 10.0.1.2 (for DSR).

See Deleting SSH Keys from the UNC Server Known Hosts List Using the Administration Menu on page 179.

4.18.9.3
Updating Known Hosts List on an SSS for Connections to a UNC Server

When and where to use: After generating new host keys on a UNC server, perform the following procedure to update the known hosts list on the UNC server for non-interactive connections to the same UNC server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

NOTICE: To configure SSH between a primary core UNC and backup core UNC, do **not** perform Updating Known Hosts List on an SSS for Connections to a UNC Server on page 120. Instead, perform the procedure specified for that in the DSR section of the SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1 Access the root command prompt for the SSS.

See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2 To delete an existing ucs-unc01.ucs key, enter:

`/opt/Motorola/ssh/bin/manage_known_hosts -u motagt -d ucs-unc0<Y>.ucs`

where `<Y>` is:

`1` for Primary Core
`2` for Backup Core

A message appears that the key was deleted. If no key is found, a message appears informing about it.

3 To delete an existing ucs-unc01 key, enter:

`/opt/Motorola/ssh/bin/manage_known_hosts -u motagt -d ucs-unc0<Y>`

where *<Y>* is:

1 for Primary Core
2 for Backup Core

A message appears that the key was deleted. If no key is found, a message appears informing about it.

4 To establish connection to the UNC server, enter:

`sudo -u motagt ssh sshserv@ucs-unc0<Y>.ucs hostname`

where *<Y>* is:

1 for Primary Core
2 for Backup Core

5 Verify the fingerprint matches the fingerprint for UNC server SSH host key that was generated most recently, then, at the prompt, enter: `Yes`

NOTICE: Ignore any messages, including error messages which may appear.

6 To establish connection to the UNC server, enter:

`sudo -u motagt ssh sshserv@ucs-unc0<Y> hostname`

where *<Y>* is:

1 for Primary Core
2 for Backup Core

7 Verify that key fingerprint is correct and press ENTER.

NOTICE: Ignore any other messages, including error messages which may appear.

8 To establish connection to the UNC server, enter:

`sudo -u motagt ssh sshserv@10.0.<y>.2 hostname`

where *<Y>* is:

1 for Primary Core
2 for Backup Core

9 Log out of the SSS server.

4.18.9.4

Updating Known Hosts List on an ATR for Connections to a UNC Server

When and where to use: After generating new host keys on a Unified Network Configurator (UNC) server, perform the following procedure to update the known hosts list on an Air Traffic Router (ATR) for non-interactive connections to a UNC server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1 Access the root command prompt on the ATR.

See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2 To delete any existing UNC server entries in the known hosts list on the ATR for the ATR-UNC SSH client account, enter:

`/opt/Motorola/ssh/bin/manage_known_hosts -u motagt -d ucs-unc0<Y>.ucs`
where *<Y>* is the number of the UNC server with the new SSH host keys

3 To establish a connection to the UNC server, enter:

`sudo -u motagt ssh sshserv@ucs-unc0<Y>.ucs hostname`
where *<Y>* is the number of the UNC server with the new SSH host keys

A confirmation message appears.

4 Verify that the fingerprint matches the fingerprint of the UNC server SSH host key that was generated most recently, then enter: `Yes`

An entry for this DNS name is added to the ATR known hosts list for the ATR-UNC SSH client account. The UNC system name displays, or a `permission denied` message displays.

5 Enter: `exit`

4.18.9.5
Updating Known Hosts List on a ZSS for Connections to a UNC Server

After generating new host keys on a Unified Network Configurator (UNC) server, perform the following procedure to update the known hosts list on a Zone Statistics Server (ZSS) for non-interactive connections to a UNC server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1 Access the root command prompt on the ZSS.

See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2 To delete any existing UNC server entries in the known hosts list on the ZSS for the ZSS-UNC SSH client account, enter:

`/opt/Motorola/ssh/bin/manage_known_hosts -u motagt -d ucs-unc0<Y>.ucs`
where *<Y>* is the number of the UNC server with the new SSH host keys

3 To establish a connection to the UNC server, enter:

`sudo -u motagt ssh sshserv@ucs-unc0<Y>.ucs hostname`
where *<Y>* is the number of the UNC server with the new SSH host keys

A confirmation message appears.

4 Verify that the fingerprint matches the fingerprint of the UNC server SSH host key that was generated most recently, then enter: `Yes`

An entry for this DNS name is added to the ZSS known hosts list for the ZSS-UNC SSH client account. The UNC system name displays, or a `permission denied` message displays.

5 Enter: `exit`

4.18.9.6
Updating Known Hosts List on a PDG for Connections to a UNC Server

After generating new host keys on a Unified Network Configurator (UNC) server, perform the following procedure to update the known hosts list on a Packet Data Gateway (PDR) module of a Linux-based Packet Data Gateway (PDG), for non-interactive connections to a UNC server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

NOTICE: Do **not** perform this procedure in an ASTRO® 25 system K master site configuration. The PDG does not function as an SSH client in that configuration.

Procedure:

1. Access the root command prompt for the PDG.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. To delete existing entries for the UNC server in the known hosts list on the PDG for the PDR-UNC SSH client account, enter:

   `/opt/Motorola/ssh/bin/manage_known_hosts -u pdr_app -d ucs-unc0<Y>.ucs`
   where `<Y>` is the number of the UNC server with the new SSH host keys

   A message confirms that the keys for the specified UNC server were deleted from known_hosts.

3. Enter: `sudo -u pdr_app ssh sshserv@ucs-unc0<Y>.ucs hostname`

   where `<Y>` is the number of the UNC server with the new SSH host keys

   A message displays a fingerprint and asks if you want to continue.

4. For optimal security, verify that the fingerprint matches the fingerprint of the UNC server SSH host key that was generated most recently. Then, enter: `yes`

   The UNC system name displays, or a `permission denied` message appears. An entry for the UNC server DNS name is added to the PDG known hosts list.

5. At the UNC server prompt, to end the SSH session with the UNC server, enter: `exit`
6. At the PDG command prompt, to log out of the PDG, enter: `exit`

4.18.9.7

Updating Known Hosts List on a Zone Controller for Connections to a UNC Server

When and where to use: After generating new host keys on a Unified Network Configurator (UNC) server, perform the following procedure to update the known hosts list on a zone controller (ZC) for non-interactive connections to a UNC server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1. Access the root command prompt on the zone controller.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. To delete any existing entries for the UNC server in the known hosts list on the zone controller for the ZC-UNC SSH client account, enter:

   `/opt/Motorola/ssh/bin/manage_known_hosts -u motoagt -d ucs-unc0<Y>.ucs`
   where `<Y>` is the number of the UNC server with the new SSH host keys

   Existing entries for the UNC server specified in the command are removed from the ZC known hosts list. (For the initial key rotation a message may report that no key was found.)

3. To establish a connection to the UNC server, enter:

   `sudo -u motoagt ssh sshserv@ucs-unc0<Y>.ucs hostname`
   where `<Y>` is the number of the UNC server with the new SSH host keys

   A confirmation message appears.

4 Verify that the fingerprint matches the fingerprint of the UNC server SSH host key that was generated most recently. Then enter: `yes`

An entry for this DNS name is added to the ZCs known hosts list for the ZC-UNC SSH client account. The UNC server system name displays, or a `permission denied` message displays.

5 Enter: `exit`

4.18.9.8

Updating Known Hosts List on an ISGW for Connections to a UNC Server

When and where to use: After generating new host keys on a Unified Network Configurator (UNC) server, perform the following procedure to update the known hosts list on an ISGW for non-interactive connections to a UNC server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1 Access the root command prompt on the ISGW server.

See: Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2 To delete any existing ucs-unc0***<Y>***.ucs key, enter:

`/opt/Motorola/ssh/bin/manage_known_hosts -u motoagt -d ucs-unc0`***<Y>***`.ucs`
where ***<Y>*** is the number of the UNC server with the new SSH host keys

One of the following messages appears (both are correct):

- `Keys for ucs-unc0`***<Y>***`.ucs in known_hosts successfully deleted.`
- `Failure: No key with a comment of ucs-unc0`***<Y>***`.ucs was found!`

3 To establish a connection to the UNC server, at the command prompt, enter:

`sudo -u motoagt ssh sshserv@ucs-unc0`***<Y>***`.ucs hostname`
where ***<Y>*** is the number of the UNC server with the new SSH host keys

The key fingerprint and the confirmation message appear.

4 Verify that the fingerprint matches the fingerprint of the UNC server SSH host key that was generated most recently. Enter: `yes`

A warning message appears.

NOTICE: Ignore any other messages (including error messages) that appear.

5 Enter: `Exit`

4.18.9.9

Updating Known Hosts List on the UNC Server for Connections to Another UNC Server (DSR Systems Only)

When and where to use:
After generating new host keys on a UNC server, perform the following procedure, depending on your point in the sequence specified in Performing Additional SSH Configuration Processes for DSR Systems on page 68 to:

- Update the known hosts list on the primary core UNC server for non-interactive connections to the backup core UNC server.

- Update the known hosts list on the backup core UNC server for non-interactive connections to the primary core UNC server.

Procedure:

1. Access the root command prompt on the UNC server that has new SSH host keys you need to rotate.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. To delete any existing entries for the UNC server in the known hosts lists on another UNC server (**not** the UNC server where you are logged in), enter:

   a. `/opt/Motorola/ssh/bin/manage_known_hosts -u sshserv -d ucs-unc0<Y>.ucs`

   b. `/opt/Motorola/ssh/bin/manage_known_hosts -u sshserv -d ucs-unc0<Y>`

   where `<Y>` is:

   `1` if you are logged into ucs-unc02

   `2` if you are logged into ucs-unc01

3. To establish a connection to the other UNC server, enter:

   `sudo –u sshserv ssh sshserv@ucs-unc0<Y>.ucs hostname`
   where `<Y>` is the number of the UNC server you specified in the previous command

   A confirmation message appears.

4. Verify the fingerprint matches the fingerprint for UNC server SSH host key that was generated most recently. Enter: `Yes`

   An entry for this DNS name is added to the UNC servers known hosts list for the sshserv account. The UNC system name displays, or a `permission denied` message displays.

5. To establish another connection to the UNC server, enter:

   `sudo –u sshserv ssh sshserv@ucs-unc0<Y> hostname`
   where `<Y>` is the number of the UNC server you specified in the previous command

   A confirmation message appears.

6. Verify the fingerprint matches the fingerprint for UNC server SSH host key that was generated most recently. Enter: `Yes`

   An entry for this DNS name is added to the UNC servers known hosts list for the sshserv account. The UNC system name displays, or a `permission denied` message displays.

7. Enter: `exit`

   This closes the sshserv user shell.

8. Enter: `exit`

   This closes the root user shell.

4.18.9.10
Updating Known Hosts List on UNCDS for Connections to UNC

Prerequisites: Ensure that you know that `<Y>` is the number of the UNC server with the new SSH host keys.

When and where to use: After generating new host keys on a Unified Network Configurator (UNC) server, perform this procedure for the three Unified Network Configurator Device Servers (UNCDS01,

UNCDS02, and UNCDS03) to update the known hosts list on the UNCDS for non-interactive connections to a UNC server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1. Access the root command prompt on the UNCDS.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. To delete any existing entries for the UNC server in the known hosts lists on the UNCDS, enter:

   a. `/opt/Motorola/ssh/bin/manage_known_hosts -u sshserv -d ucs-unc0<Y>.ucs`

   b. `/opt/Motorola/ssh/bin/manage_known_hosts -u sshserv -d ucs-unc0<Y>`

3. To establish a connection to the UNC server, enter: `sudo -u sshserv ssh sshserv@ucs-unc0<Y>.ucs ls /tmp`

   A confirmation message appears.

4. Verify that the fingerprint matches the fingerprint for the UNC server SSH host key that was generated most recently. Enter: `Yes`

   An entry for this DNS name is added to the UNC server known hosts list for the sshserv account. The UNC server `/tmp` directory displays, or a `permission denied` message displays.

5. To establish another connection to the UNC server, enter: `sudo -u sshserv ssh sshserv@ucs-unc0<Y>ls /tmp`

   A confirmation message appears.

6. Verify that the fingerprint matches the fingerprint for the UNC server SSH host key that was generated most recently. Enter: `Yes`

   An entry for this DNS name is added to the UNC server known hosts list for the sshserv account. The UNC server `/tmp` directory displays, or a `permission denied` message displays.

7. Enter: `exit`

   The sshserv user shell closes.

8. Enter: `exit`

   The root user shell closes.

4.18.10
SSH Client Key Rotation for Network Management Servers

Procedures in this section:

- Generate SSH client keys on a Network Management server that is an SSH client and propagate them to a Network Management server that is an SSH server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.
- Apply only to the Network Management servers listed in the following table.

- Use the Fully Qualified Domain Name (FQDN) for the Linux-based or Solaris-based devices, as indicated in the following table.

Table 16: FQDN to Use in Commands for Rotating SSH Keys for Network Management Servers

In the following table:

<X> is the number of the zone where the device resides

0***<Y>*** is the number of the server (01 for primary core devices)

0***<W>*** is the number of the device server (01 or 02 or 03)

Network Management Servers (SSH Clients / SSH Servers)	FQDN to Use in Commands (replace *<x>* with zone number)
Zone Database Server	zds0***<Y>***.zone***<Z>***
Zone Statistics Server	zss0***<Y>***.zone***<Z>***
Unified Event Manager server	z00***<Z>***uem***<X>***.zone***<Z>***
Air Traffic Router server	atr0***<Y>***.zone***<Z>***
User Configuration Server	ucs0***<Y>***.ucs
System Statistics Server*	sss0***<Y>***.ucs
Unified Network Configurator server	ucs-unc0***<Y>***.ucs
Unified Network Configurator Device Servers	ucs-uncds0***<W>***.ucs

* For rotating System Statistics Server (SSS) client keys, two separate processes are required. Perform Updating Known Hosts List on the SSS for Connections to an ATR on page 116 to rotate SSH client keys for the SSS connection to the ATR. To rotate SSH client keys for the SSS connection to the UNC server, see: SSH Client Key Rotation for SSS Connections to a UNC Server on page 134.

The procedures in this section apply to the following SSH relationships:

Table 17: SSH Client – NM Server Relationships

SSH Client	NM Server
ZSS01	ATR01
ZSS02	ATR02
SSS01	ATR01, ATR 02 (in all installed zones)
SSS02	ATR01, ATR 02 (in all installed zones)
UCS01	UNC01, UCS02
UCS02	UNC02, UCS01
UNC01	UCS01, UNC02, UNC01
UNC02	UCS02, UNC01, UNC02
UNCDS01	UNC01
UNCDS02	UNC01
UNCDS03	UNC01
ATR01	UNC01, UNC02
ATR02	UNC01, UNC02

SSH Client	NM Server
ZSS01	UNC01, UNC02
ZSS02	UNC01, UNC02
PDG01, PDG02	UNC01, UNC02
ZC01, ZC02, ZC03, ZC04	UNC01, UNC02
SSS01	UNC01, UNC02
SSS02	UNC01, UNC02
ISGW01, ISGW02, ISGW03, ISGW04	UNC01, UNC02

4.18.10.1
Regenerating SSH Client Keys on a Network Management Server

When and where to use:
Perform the following procedure on each Network Management server (SSH client) to generate SSH client keys for the non-interactive account “sshserv”, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

NOTICE: Do not perform this procedure on a Zone Controller, Packet Data Router, Generic Application Server or ISGW.

In the command entered to generate the client keys, you need to specify the DNS name of the Linux or Solaris SSH client. For the DNS names of the Linux or Solaris devices, see Table 16: FQDN to Use in Commands for Rotating SSH Keys for Network Management Servers on page 127.

NOTICE: For default SSH client key entries in an authorized keys list that are shared by more than one device, system availability is impacted as soon as a client key is regenerated on a device, until the entire rotation process for that key is completed.

Procedure:

1. Access the root command prompt on the Network Management server that is an SSH client.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. Enter the following command:

   `/opt/Motorola/ssh/bin/gen_client_keys -l 2048 -c sshserv@`***`<FQDN of SSH Client>`***`-noninteractive`

   (Use the Fully Qualified Domain Name of the Linux-based or Solaris-based SSH client device, from Table 16: FQDN to Use in Commands for Rotating SSH Keys for Network Management Servers on page 127.)

   Messages will appear reporting success when the SSH client keys (RSA and DSA) are generated for the SSH client specified in the command, for the non-interactive user account “sshserv”. The keys are stored in a .pub file under `/usr/local/home/sshserv/.ssh/`.

4.18.10.2
Transferring SSH Client Keys from an NM Server to an NM Server

Perform the following procedure to propagate the public portion of the SSH client RSA and DSA keys from a Network Management server that is an SSH client to a Network Management server that is an SSH server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

NOTICE: DSA SSH keys are not available on FIPS-enabled devices.

When and where to use:
Perform this procedure only on system-level devices, such as UCS, UNC, SSS, or UNCDS.

Do **not** perform this procedure on a Zone Controller, Packet Data Router, Generic Application Server, or ISGW.

Procedure:

1. Access the root command prompt on the Network Management server that is an SSH client.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. Enter:
   `sudo -u sshserv scp -F /etc/ssh/ssh_config /usr/local/home/sshserv/.ssh/id_rsa.pub <username>@<FQDN of SSH Server>:/tmp/id_rsa-sshserv.pub_<FQDN of SSH Client>`

   where ***<username>*** is your Active Directory account that is a member of the user group authorized to access the SSH *server* device

   Use the appropriate Fully Qualified Domain Names from Table 16: FQDN to Use in Commands for Rotating SSH Keys for Network Management Servers on page 127, depending on the devices you are configuring.

3. At the password prompt, enter the password for the account entered to replace ***<username>*** in the preceding step.

   The public portion of the RSA SSH client keys is copied securely to the `/tmp/` directory on the SSH server specified in the command.

4. **NOTICE:** DSA SSH keys are not available on FIPS-enabled devices.

   Enter:
   `sudo -u sshserv scp -F /etc/ssh/ssh_config /usr/local/home/sshserv/.ssh/id_dsa.pub <username>@<FQDN of SSH Server>:/tmp/id_dsa-sshserv.pub_<FQDN of SSH Client>`

   where ***<username>*** is your Active Directory account that is a member of the user group authorized to access the SSH *server* device

   Use the appropriate Fully Qualified Domain Names from Table 16: FQDN to Use in Commands for Rotating SSH Keys for Network Management Servers on page 127, depending on the devices you are configuring.

5. At the password prompt, enter the password for your Active Directory account that is a member of the user group authorized to access the SSH *server* device.

   The public portion of the DSA SSH client keys is copied securely to the `/tmp/` directory on the SSH server specified in the command.

4.18.10.3

Updating NM Server Entries in the Authorized Keys List on an NM Server

Perform this procedure after propagating SSH user keys on a Network Management server that is an SSH client to a Network Management server that is an SSH server to update the authorized keys list on each SSH server.

Prerequisites: In the commands, enter the Fully Qualified Domain Name of the Linux-based or Solaris-based SSH client device, as indicated in Table 16: FQDN to Use in Commands for Rotating SSH Keys for Network Management Servers on page 127.

When and where to use: This procedure needs to be repeated for each SSH client that needs to connect securely to this SSH server (according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

NOTICE: Do **not** perform this procedure on a Zone Controller, Packet Data Router, Generic Application Server or ISGW.

Procedure:

1. Access the root command prompt on the Network Management server that is an SSH server.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. Enter:
   `/opt/Motorola/ssh/bin/manage_authorized_keys -a /tmp/id_rsa-sshserv.pub_`***`<FQDN of SSH Client>`*** `-u sshserv`

   The authorized keys list now contains the new RSA SSH client public key for the specified SSH Client, for the non-interactive sshserv account. Any RSA keys with the same key comment are replaced.

3. Enter:
   `/opt/Motorola/ssh/bin/manage_authorized_keys -a /tmp/id_dsa-sshserv.pub_`***`<FQDN of SSH Client>`*** `-u sshserv`

   NOTICE: DSA SSH keys are not available on FIPS-enabled devices.

   The authorized keys list now contains the new DSA SSH client public key for the specified SSH Client, for the non-interactive sshserv account. Any DSA keys with the same key comment are replaced.

4. Enter: `rm /tmp/id_dsa-sshserv.pub_`***`<FQDN of SSH Client>`***

   The DSA SSH client keys are removed from the `/tmp/` directory.

5. Enter: `rm /tmp/id_rsa-sshserv.pub_`***`<FQDN of SSH Client>`***

   NOTICE: DSA SSH keys are not available on FIPS-enabled devices.

   The RSA SSH Client keys are removed from the `/tmp/` directory.

4.18.11

SSH Client Key Rotation for ATR Connections to a UNC Server

The procedures in this section generate SSH client keys on an Air Traffic Router (ATR) and propagate them to a Unified Network Configurator (UNC) server.

Perform these procedures in the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

4.18.11.1
Regenerating SSH Client Keys on an ATR for Connections to a UNC Server

When and where to use: Perform the following procedure on each ATR to regenerate SSH client keys for a non-interactive account used when the ATR initiates SSH sessions with the Unified Network Configurator (UNC) server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1. Access the root command prompt on the ATR.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. Enter:
   `/opt/Motorola/ssh/bin/gen_client_keys -l 2048 -c motagt@atr0<Y>.zone<X>-noninteractive`

   where:

   <X> is the number of the zone where the ATR resides

   `0`***<Y>*** one of the following values:

   For the ATR in the primary core, `0`***<Y>*** is `01`; in a DSR backup core, the number is `02`.

   For a UNC server in the primary core, `0`***<Y>*** is `01`; in a DSR backup core, the number is `02`.

   Use the `hostname` command and the `domainname` command to display the FQDN for the server you are logged into.

   Messages will appear reporting success when the SSH client keys (RSA and DSA) are generated for the ATR specified in the command. The keys are stored in a .pub file under `/usr/local/home/motagt/.ssh/`.

4.18.11.2
Transferring SSH Client Keys from an ATR to a UNC Server

Prerequisites: Ensure the following variables are replaced with appropriate values:

<username> is your Active Directory account that is a member of the unc-login user group

<X> is the number of the zone where the ATR resides

`0`***<Y>*** one of the following values:

For the ATR in the primary core, `0`***<Y>*** is `01`; in a DSR backup core, the number is `02`.

For a UNC server in the primary core, `0`***<Y>*** is `01`; in a DSR backup core, the number is `02`.

Use the `hostname` command and the `domainname` command to display the FQDN for the server you are logged into.

When and where to use: Perform the following procedure to transfer the public portion of the SSH client RSA and DSA keys from an ATR to a Unified Network Configurator (UNC) server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1. Access the root command prompt on the ATR.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. To copy the public portion of RSA key to the UNC, enter:
   `sudo -u motagt scp -F /etc/ssh/ssh_config /usr/local/home/motagt/.ssh/id_rsa.pub <username>@ucs-unc0<Y>.ucs:/tmp/id_rsa-motagt.pub_atr0<Y>.zone<X>`

3 At the password prompt, enter the password for your Active Directory account that is a member of the unc-login user group.

The public portion of the RSA SSH client keys is copied securely to the `/tmp/` directory on the UNC server.

4.18.11.3
Updating the ATR Entries in the Authorized Keys List on a UNC Server

Prerequisites: For each of the command lines in this procedure, replace the variables with the following values:

<X> is the number of the zone where the ATR resides

`0`***<Y>*** one of the following values:

For the ATR in the primary core, `0`***<Y>*** is `01`; in a DSR backup core, the number is `02`.

For a UNC server in the primary core, `0`***<Y>*** is `01`; in a DSR backup core, the number is `02`.

Use the `hostname` command and the `domainname` command to display the FQDN for the server you are logged into.

When and where to use: After transferring SSH user keys from an ATR to Unified Network Configurator (UNC) server, perform this procedure to update the authorized keys list on the UNC server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1 Access the root command prompt on the UNC server.

See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2 Enter:
`/opt/Motorola/ssh/bin/manage_authorized_keys -a /tmp/id_rsa-motagt.pub_atr0`***<Y>***`.zone`***<X>*** `-u sshserv`

The UNC servers authorized keys list now contains the new RSA SSH client public key for the non-interactive ATR-UNC SSH account on the ATR specified in the command. Any keys with the same key comment are replaced.

3 Enter: `rm /tmp/id_rsa-motagt.pub_atr0`***<Y>***`.zone`***<X>***

The RSA SSH client keys are removed from the `/tmp/` directory.

4.18.12
SSH Client Key Rotation for ZSS Connections to a UNC Server

The procedures in this section apply to Inbound RF Quality Metrics Collection.

The procedures in this section generate SSH client keys on a Zone Statistics Server (ZSS) and propagate them to a Unified Network Configurator (UNC) server.

Perform these procedures in the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

4.18.12.1
Regenerating SSH Client Keys on a ZSS for Connections to a UNC Server

When and where to use: Perform the following procedure on each ZSS to regenerate SSH client keys for a non-interactive account used when the ZSS initiates SSH sessions with the Unified Network

Configurator (UNC) server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1 Access the root command prompt on the ZSS.

See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2 Enter:
`/opt/Motorola/ssh/bin/gen_client_keys -l 2048 -c motagt@zss0<Y>.zone<X>-noninteractive`

where:

<X> is the number of the zone where the ZSS resides

`0`***<Y>*** one of the following values:

For the ZSS in the primary core, `0`***<Y>*** is `01`; in a DSR backup core, the number is `02`.

For a UNC server in the primary core, `0`***<Y>*** is `01`; in a DSR backup core, the number is `02`.

Use the `hostname` command and the `domainname` command to display the FQDN for the server you are logged into.

Messages will appear reporting success when the SSH client keys (RSA and DSA) are generated for the ZSS specified in the command. The keys are stored in a .pub file under `/usr/local/home/motagt/.ssh/`.

4.18.12.2
Transferring SSH Client Keys from a ZSS to a UNC Server

Perform the following procedure to transfer the public portion of the SSH client RSA and DSA keys from a Zone Statistics Server (ZSS) to a Unified Network Configurator (UNC) server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

Prerequisites: Ensure the following variables are replaced with appropriate values:

<username> is your Active Directory account that is a member of the **unc-login** user group

<X> is the number of the zone where the ZSS resides

`0`***<Y>*** is one of the following values:

For the ZSS in the primary core, `0`***<Y>*** is `01`; in a DSR backup core, the number is `02`.

For a UNC server in the primary core, `0`***<Y>*** is `01`; in a DSR backup core, the number is `02`.

Use the `hostname` command and the `domainname` command to display the FQDN for the server you are logged into.

Procedure:

1 Access the root command prompt on the ZSS.

See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2 To copy the public portion of RSA key to the UNC, enter:
`sudo -u motagt scp -F /etc/ssh/ssh_config /usr/local/home/motagt/.ssh/id_rsa.pub <username>@ucs-unc0<Y>.ucs:/tmp/id_rsa-motagt.pub_zss0<Y>.zone<X>`

3 At the password prompt, enter the password for your Active Directory account that is a member of the **unc-login** user group.

The public portion of the RSA SSH client keys is copied securely to the `/tmp/` directory on the UNC server.

4.18.12.3
Updating ZSS Entries in the Authorized Keys List on a UNC Server

After transferring SSH user keys from a Zone Statistics Server (ZSS) to Unified Network Configurator (UNC) server, perform this procedure to update the authorized keys list on the UNC server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

Prerequisites: For each of the command lines in this procedure, replace the variables with the following values:

<X> is the number of the zone where the ZSS resides

`0`***<Y>*** is one of the following values:

For the ZSS in the primary core, `0`***<Y>*** is `01`; in a DSR backup core, the number is `02`.

For a UNC server in the primary core, `0`***<Y>*** is `01`; in a DSR backup core, the number is `02`.

Use the `hostname` command and the `domainname` command to display the FQDN for the server you are logged into.

Procedure:

1. Access the root command prompt on the UNC server.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. Enter:
   `/opt/Motorola/ssh/bin/manage_authorized_keys -a /tmp/id_rsa-motagt.pub_zss0`***<Y>***`.zone`***<X>*** `-u sshserv`

   The UNC servers authorized keys list now contains the new RSA SSH client public key for the non-interactive ZSS-UNC SSH account on the ZSS specified in the command. Any keys with the same key comment are replaced.

3. Enter: `rm /tmp/id_rsa-motagt.pub_zss0`***<Y>***`.zone`***<X>***

   The RSA SSH client keys are removed from the `/tmp/` directory.

4.18.13
SSH Client Key Rotation for SSS Connections to a UNC Server

The procedures in this section generate SSH client keys on a System Statistics Server (SSS) and propagate them to a Unified Network Configurator (UNC) server.

Perform these procedures in the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

4.18.13.1
Regenerating SSH Client Keys on an SSS for Connections to a UNC Server

Prerequisites: Ensure that you know the values that replace the following variables in the procedure:

<user> is the login name for domain account

`0`***<Y>*** is the number of the device you are configuring, as follows:

For the SSS in the primary core, `0`***<Y>*** is 01; in a DSR backup core, the number is 02.

For a UNC server in the primary core, `0`***<Y>*** is 01; in a DSR backup core, the number is 02.

You can use the `hostname` command and the `domainname` command to display the FQDN for the server you are logged into.

When and where to use: Perform the following procedure on each SSS to regenerate SSH client keys for a non-interactive account used when the SSS initiates SSH sessions with the Unified Network

Configurator (UNC) server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1. Access the root command prompt on the SSS.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. Enter:
   `/opt/Motorola/ssh/bin/gen_client_keys -l 2048 -c motagt@sss0<Y>.ucs-noninteractive`

   A message appears, stating that new keys are generating. Once the generation is finished, the prompt appears.

3. Perform the following actions:

   a. To copy the public portion of the RSA key to the UNC, enter:
   `sudo -u motagt scp -F /etc/ssh/ssh_config /usr/local/home/motagt/.ssh/id_rsa.pub <user>@ucs-unc0<Y>.ucs:/tmp/id_rsa-motagt.pub_sss0<Y>.ucs`

   b. At the prompt, enter the domain user password.

   The copying progress bar appears. Once finished, the prompt appears.

4. Log out of the SSS server.

4.18.13.2
Updating the SSS Entries in the Authorized Keys List on a UNC Server

Prerequisites: Ensure that `0<Y>` is the number of the device you are configuring, as follows:

For the SSS in the primary core, `0<Y>` is 01; in a DSR backup core, the number is 02.

For a UNC server in the primary core, `0<Y>` is 01; in a DSR backup core, the number is 02.

You can use the `hostname` command and the `domainname` command to display the FQDN for the server you are logged into.

When and where to use: After transferring SSH user keys from an SSS to Unified Network Configurator (UNC) server, perform the following procedure to update the authorized keys list on the UNC server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1. Access the root command prompt on the UNC server.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. To remove an existing entry from the authorized keys repository, enter:
   `/opt/Motorola/ssh/bin/manage_authorized_keys -d motagt@sss0<Y>-general_key -u sshserv`

   NOTICE: Ignore the following message:
   `No key with a comment of motagt@sss0<Y>-general_key was found!`

   The message confirming successful key deletion appears.

3. To update the UNC authorized keys repository with the public portion of SSS RSA user key, enter:

`/opt/Motorola/ssh/bin/manage_authorized_keys -a /tmp/id_rsa-motagt.pub_sss0`***<Y>***`.ucs -u sshserv`

The keys are added message appears.

4 Log out of the UNC server.

4.18.14
SSH Client Key Rotation for PDG Connections to a UNC Server

SSH client keys on the Packet Data Router (PDR) module of a Linux-based Packet Data Gateway (PDG) device are generated and propagated to the Linux-based or Solaris-based Unified Network Configurator (UNC) server.

Perform procedures in this section in the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

NOTICE: Do **not** perform the procedures in this section in an ASTRO® 25 system K master site configuration. The PDG does not function as an SSH client in that configuration.

4.18.14.1
Regenerating SSH Client Keys on a PDG for Connections to a UNC Server

When and where to use: Perform the following procedure on each Packet Data Gateway (PDG) (SSH client) to regenerate SSH client keys for the non-interactive account required for SSH connections to the Unified Network Configurator (UNC) server, according to the sequence specified in the SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1 Access the root command prompt for the PDG.

See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2 Enter: `gen_client_keys –l 2048 –c pdr_app@`***<PDR hostname>***`.zone`***<X>***`–noninteractive`

where:

<PDR hostname> is one of the following values:

`pdr01` for a primary core Trunking IVD PDR

`hpdpdr01` for a primary core HPD PDR

`pdr02` for a backup core Trunking IVD PDR

`hpdpdr02` for a backup core HPD PDR

`convpdr01` for a Conventional IVD PDR

<X> is the number of the zone where the PDG resides

A message reports that the RSA key pair is being generated.

3 At the confirmation prompt, enter: `y`

The following location of the saved public keys displays: `/usr/local/home/pdr/.ssh/id_rsa.pub`

4 To log out of the PDG, enter: `exit`

4.18.14.2
Transferring PDG SSH Client Keys to a UNC Server

Perform the following procedure to transfer the public portion of the SSH client RSA and DSA keys from a Packet Data Gateway (PDG) to a Unified Network Configurator (UNC) server, according to the sequence specified in the SSH Rotation on Devices Using Default Keys on page 60.

Prerequisites: Ensure that you know the values that replace the following variables in the procedure:

<username> is your Active Directory account that is a member of the unc-login user group

`0`***<Y>*** is the number of the device you are configuring (in a primary core, `0`***<Y>*** is 01; in a DSR backup core, the number is 02).

<PDR hostname> is one of the following values:

`pdr01` for a primary core Trunking IVD PDR

`hpdpdr01` for a primary core HPD PDR

`pdr02` for a backup core Trunking IVD PDR

`hpdpdr02` for a backup core HPD PDR

`convpdr01` for a Conventional IVD PDR

<X> is the number of the zone where the PDG resides

Procedure:

1. Access the root command prompt for the PDG.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. Enter:
   `sudo -u pdr_app scp -F /etc/ssh/ssh_config /usr/local/home/pdr/.ssh/id_rsa.pub` ***<username>***`@ucs-unc0`***<Y>***`.ucs:/tmp/id_rsa.pub_`***<PDR hostname>***`.zone`***<X>***

3. If the `Are you sure you want to continue connecting?` prompt appears, enter `yes` after verifying UNC fingerprint.

4. At the prompt, enter the password for your Active Directory account that is a member of the unc-login user group.

   The public portion of the RSA SSH client keys is copied securely to the `/tmp/` directory on the UNC server.

5. To log out of the PDG, enter: `exit`

4.18.14.3
Adding PDG Entries to the Authorized Keys List on a UNC Server

After transferring SSH client keys from a Packet Data Gateway (PDG) to a Unified Network Configurator (UNC) server, perform the following procedure to update the authorized keys list on the UNC server, according to the sequence specified in the SSH Rotation on Devices Using Default Keys on page 60.

Prerequisites: Ensure that you know the values that replace the following variables in the procedure:

<PDR hostname> is one of the following values:

`pdr01` for a primary core Trunking IVD PDR

`hpdpdr01` for a primary core HPD PDR

`pdr02` for a backup core Trunking IVD PDR

`hpdpdr02` for a backup core HPD PDR

`convpdr01` for a Conventional IVD PDR

<X> is the number of the zone where the PDG resides

Procedure:

1. Access the root command prompt on the UNC server.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. Enter:
   `/opt/Motorola/ssh/bin/manage_authorized_keys -a /tmp/id_rsa.pub_<PDR hostname>.zone<X> -u sshserv`

   The UNC servers authorized keys list now contains the new RSA SSH client public key for the PDR-UNC SSH client account. Any keys with the same key comment are replaced.

3. Enter: `rm /tmp/id_rsa.pub_<PDR hostname>.zone<X>`

   The RSA SSH client keys are removed from the `/tmp/` directory.

4.18.15

SSH Client Key Rotation for ZC Connections to a UNC Server

Perform the procedures in this section to generate SSH client keys on a zone controller (ZC) and to propagate them to a Unified Network Configurator (UNC) server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

4.18.15.1

Generating SSH Client Keys on a Zone Controller

When and where to use: Perform the following procedure on each Zone Controller (ZC) (in the zone core and in the Trunking Subsystem) to generate SSH client keys for a non-interactive account that the ZC uses to initiate SSH sessions with a Unified Network Configurator (UNC) server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.
For more information on the Trunking Subsystem (Tsub) Zone Controller, see the *Edge Availability with Wireline Console Feature Guide for Trunking Subsystems* manual.

Procedure:

1. Access the root command prompt on the Zone Controller.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. **For the ZC in the zone core:** enter:
   `/opt/Motorola/ssh/bin/gen_client_keys -l 2048 -c motoagt@zc0<Y>.zone<X>-noninteractive`

   where:

   `0<Y>` is the number of the device you are configuring

   For Zone Controllers in the primary core, `0<Y>` is 01 or 02; in a DSR backup core, the number is 03 or 04.

   `<X>` is the number of the zone where the Zone Controller resides

   You can use the `hostname` command and the `domainname` command to display the FQDN for the server you are logged into.

   The keys are stored in a `.pub` file under `/usr/local/home/motoagt/.ssh/`.

   Messages appear reporting success when the SSH client keys (RSA and DSA) are generated for the Zone Controller specified in the command.

3. **For the Tsub ZC:** enter:
   `/opt/Motorola/ssh/bin/gen_client_keys -l 2048 -c motoagt@z00<X>s<PPP>tzc01-noninteractive`

where:

<X> is the number of the zone where the Zone Controller resides

<PPP> is the 3-digit, zero-padded site number where the Tsub ZC resides.

4.18.15.2

Transferring SSH Client Keys from a Zone Controller to a UNC Server

Perform the following procedure to transfer the public portion of the SSH client RSA keys from a Zone Controller (ZC) to a Unified Network Configurator (UNC) server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

Prerequisites: Ensure that you know the values that replace the following variables in the procedure:

<username> with your Active Directory account that is a member of the unc-login user group

<X> is the number of the zone where the ZC resides

`0`***<Y>*** is the number of the device you are configuring:

For ZCs in the primary core, `0`***<Y>*** is 01 or 02; in a DSR backup core, the number is 03 or 04.

For a UNC server in the primary core, `0`***<Y>*** is 01; in a DSR backup core, the number is 02.

<PPP> is the 3-digit, zero-padded site number where the Tsub ZC resides.

You can use the `hostname` command and the `domainname` command to display the FQDN for the server you are logged into.

Procedure:

1. Access the root command prompt on the Zone Controller.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. To copy the public portion of RSA key to the UNC, enter:

   - **For the ZC in the zone core:**
     `sudo -u motoagt scp -F /etc/ssh/ssh_config /usr/local/home/motoagt/.ssh/id_rsa.pub` ***<username>***`@ucs-unc0`***<Y>***`.ucs:/tmp/id_rsa-motoagt.pub_zc0`***<Y>***`.zone`***<X>***
   - **For the Tsub ZC:**
     `sudo -u motoagt scp -F /etc/ssh/ssh_config /usr/local/home/motoagt/.ssh/id_rsa.pub` ***<username>***`@ucs-unc0`***<Y>***`.ucs:/tmp/id_rsa-motoagt.pub_z00`***<X>***`s`***<PPP>***`tzc01`

3. At the prompt, enter the password for your Active Directory account that is a member of the unc-login user group.

   The public portion of the RSA SSH client keys is copied securely to the `/tmp/` directory on the UNC server.

4. Enter: `exit`

   You are returned to the root prompt.

4.18.15.3

Updating the ZC Entries in the Authorized Keys List on a UNC Server

After transferring SSH user keys from a Zone Controller to a Unified Network Configurator (UNC) server, perform the following procedure to update the authorized keys list on the UNC server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

Prerequisites: Ensure that you know the values that replace the following variables in the procedure:

<X> is the number of the zone where the Zone Controller resides

`0`***<Y>***with the number of the device you are configuring:

For Zone Controllers in the primary core, `0`***<Y>*** is 01 or 02; in a DSR backup core, the number is 03 or 04.

For a UNC server in the primary core, `0`***<Y>*** is 01; in a DSR backup core, the number is 02.

<PPP> is the 3-digit, zero-padded site number where the Tsub ZC resides.

You can use the `hostname` command and the `domainname` command to display the FQDN for the server you are logged into.

Procedure:

1. Access the root command prompt on the UNC server.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. Enter one of the following commands:

   - **For the ZC in the zone core:**
     `/opt/Motorola/ssh/bin/manage_authorized_keys -a /tmp/id_rsa-motoagt.pub_zc0`***<Y>***`.zone`***<X>*** `-u sshserv`
   - **For the Tsub ZC:**
     `/opt/Motorola/ssh/bin/manage_authorized_keys -a /tmp/id_rsa-motoagt.pub_z00`***<X>***`s`***<PPP>***`tzc01 -u sshserv`

   The authorized keys list now contains the new RSA SSH client public key for the non-interactive ZC-UNC SSH client account on the Zone Controller. Any keys with the same key comment are replaced.

3. Enter one of the following commands:

   - **For the ZC in the zone core:** `rm /tmp/id_rsa-motoagt.pub_zc0`***<Y>***`.zone`***<X>***
   - **For the Tsub ZC:**
     `rm /tmp/id_rsa-motoagt.pub_z00`***<X>***`s`***<PPP>***`tzc01`

   NOTICE: DSA keys are not supported on FIPS-enabled devices.

   The RSA SSH client keys are removed from the `/tmp/` directory. The command prompt appears.

4. Enter: `exit`

   You are returned to the root prompt.

4.18.16
SSH Client Key Rotation for ISGW Connections to a UNC Server

Perform procedures in this section to generate SSH client keys on an ISGW and to propagate them to a Unified Network Configurator (UNC) server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

4.18.16.1
Generating SSH Client Keys on an ISGW

When and where to use: Perform the following procedure on each ISGW to generate SSH client keys for a non-interactive account that the ISGW uses to initiate SSH sessions with a Unified Network Configurator (UNC) server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

The keys are stored in a .pub file under `/usr/local/home/motoagt/.ssh/`.

Procedure:

1 Access the root command prompt on the ISGW.

See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2 Enter:
`/opt/Motorola/ssh/bin/gen_client_keys -l 2048 -c motoagt@z00<x>isgw0<y>.zone<x>-noninteractive`

Where:

<X> is the number of the zone where the ISGW resides

`0`***<Y>*** is the number of the device you are configuring:

For ISGW in the primary core, `0`***<Y>*** is 01 or 02 (optional); in a DSR backup core, the number is 03 or 04 (optional).

For a UNC server in the primary core, `0`***<Y>*** is 01; in a DSR backup core, the number is 02.

You can use the `hostname` command and the `domainname` command to display the FQDN for the server you are logged into.

Messages will appear reporting success when the SSH client keys (RSA and DSA) are generated for the ISGW specified in the command.

4.18.16.2
Transferring SSH Client Keys from an ISGW to a UNC Server

Perform the following procedure to transfer the public portion of the SSH client RSA keys from an ISGW to a Unified Network Configurator (UNC) server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

Prerequisites: Ensure that you know the values that replace the following variables in the procedure:

<username> is your Active Directory account that is a member of the unc-login user group

<X> is the number of the zone where the ISGW resides

`0`***<Y>*** is the number of the device you are configuring:

For ISGW in the primary core, `0`***<Y>*** is 01 or 02 (optional); in a DSR backup core, the number is 03 or 04 (optional).

For a UNC server in the primary core, `0`***<Y>*** is 01; in a DSR backup core, the number is 02.

You can use the `hostname` command and the `domainname` command to display the FQDN for the server you are logged into.

Procedure:

1 Access the root command prompt on the ISGW.

See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2 To copy the public portion of RSA key to the UNC, enter:
`sudo -u motoagt scp -F /etc/ssh/ssh_config /usr/local/home/motoagt/.ssh/id_rsa.pub <username>@ucs-unc0<Y>.ucs:/tmp/id_rsa-motoagt.pub_z00<x>isgw0<y>.zone<x>`

3 At the prompt, enter the password for your Active Directory account that is a member of the unc-login user group.

The public portion of the RSA SSH client keys is copied securely to the `/tmp/` directory on the UNC server.

4 To copy the public portion of DSA key to the UNC, enter:

```
sudo -u motoagt scp -F /etc/ssh/ssh_config /usr/local/home/
motoagt/.ssh/id_dsa.pub <username>@ucs-unc0<Y>.ucs:/tmp/id_dsamotoagt.
pub_z00<x>isgw0<y>.zone<x>
```

5 At the prompt, enter the password for your Active Directory account that is a member of the unc-login user group.

The public portion of the DSA SSH client keys is copied securely to the `/tmp/` directory on the UNC server.

6 Enter: `exit`

You are returned to the root prompt.

4.18.16.3

Updating the ISGW (ISSI 8000/CSSI 8000) Entries in the Authorized Keys List on a UNC Server

After transferring SSH user keys from a zone controller to a Unified Network Configurator (UNC) server, perform the following procedure to update the authorized keys list on the UNC server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

Prerequisites: Ensure that you know the values that replace the following variables in the procedure:

<X> is the number of the zone where the ISGW resides

`0`***<Y>*** is the number of the device you are configuring:

For ISGW in the primary core, `0`***<Y>*** is 01 or 02 (optional); in a DSR backup core, the number is 03 or 04 (optional).

For a UNC server in the primary core, `0`***<Y>*** is 01; in a DSR backup core, the number is 02.

You can use the `hostname` command and the `domainname` command to display the FQDN for the server you are logged into.

Procedure:

1 Access the root command prompt on the UNC server.

See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2 To remove an existing entry from the authorized keys repository, enter:
`/opt/Motorola/ssh/bin/manage_authorized_keys -d sshserv@isgw-general_key -u sshserv`

A message confirming successful key deletion appears.

NOTICE: Ignore the following message: `Failure: No key with a comment of sshserv@isgw-general_key was found!`

3 Enter:
`/opt/Motorola/ssh/bin/manage_authorized_keys -a /tmp/id_rsa-motoagt.pub_z00`***<x>***`isgw0`***<y>***`.zone`***<x>*** `-u sshserv`

The authorized keys list now contains the new RSA SSH client public key for the non-interactive ISGW-UNC SSH client account on the zone controller. Any keys with the same key comment are replaced.

4 Enter:
`/opt/Motorola/ssh/bin/manage_authorized_keys -a /tmp/id_dsamotoagt.pub_z00`***<x>***`isgw0`***<y>***`.zone`***<x>*** `-u sshserv`

The authorized keys list now contains the new DSA SSH client public key for the non-interactive ISGW-UNC SSH client account on the zone controller. Any keys with the same key comment are replaced.

5 Enter:

a `rm /tmp/id_rsa-motoagt.pub_z00<x>isgw0<y>.zone<x>`

b `rm /tmp/id_dsa-motoagt.pub_z00<x>isgw0<y>.zone<x>`

The RSA and DSA SSH client keys are removed from the `/tmp/` directory.

6 At the prompt, enter: `exit`

You are returned to the root prompt.

4.18.17
SSH Client Key Rotation for UNCDS Connections to a UNC Server

Perform procedures in this section to generate SSH client keys on a UNCDS and to propagate them to a Unified Network Configurator (UNC) server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

4.18.17.1
Generating SSH Client Keys on a UNCDS

Perform the following procedure on each of the Unified Network Configurator Device Servers (UNCDS) to generate SSH client keys for a non-interactive account that the UNCDS uses to initiate SSH sessions with a Unified Network Configurator (UNC) server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.
The keys are stored in a .pub file under `/usr/local/home/motoagt/.ssh/`.

Procedure:

1 Access the root command prompt on the UNCDS.

See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2 Enter:
`/opt/Motorola/ssh/bin/gen_client_keys -l 2048 -c sshserv@ucs-uncds0<w>.ucs-noninteractive`

where:

`0<w>` is the number of Unified Network Configurator Device Server (01 or 02 or 03)

You can use the `hostname` command and the `domainname` command to display the FQDN for the server you are logged into.

Messages will appear reporting success when the SSH client keys (RSA and DSA) are generated for the UNCDS specified in the command.

4.18.17.2
Transferring SSH Client Keys from a UNCDS to a UNC Server

Perform the following procedure to transfer the public portion of the SSH client RSA and DSA keys from Unified Network Configurator Device Servers (UNCDS) to a Unified Network Configurator (UNC) server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

Prerequisites: Ensure that you know the values that replace the following variables in the procedure:

`<username>` is your Active Directory account that is a member of the unc-login user group

`0<w>` is the number of Unified Network Configurator Device Server (01 or 02 or 03)

`0<Y>` is the number of the device you are configuring:

For UNCDS in the primary core, `0<Y>` is 01. There is no UNCDS in a DSR backup core.

For a UNC server in the primary core, `0<Y>` is 01; in a DSR backup core, the number is 02.

You can use the `hostname` command and the `domainname` command to display the FQDN for the server you are logged into.

Procedure:

1. Access the root command prompt on the UNCDS.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. To copy the public portion of RSA key to the UNC, enter:
   `sudo -u sshserv scp -F /etc/ssh/ssh_config /usr/local/home/sshserv/.ssh/id_rsa.pub <username>@ucs-unc0<Y>.ucs:/tmp/id_rsa-sshserv.pub_ucs-uncds0<w>.ucs`

3. At the prompt, enter the password for your Active Directory account that is a member of the unc-login user group.

   The public portion of the RSA SSH client keys is copied securely to the `/tmp/` directory on the UNC server.

4. To copy the public portion of DSA key to the UNC, enter:
   `sudo -u sshserv scp -F /etc/ssh/ssh_config /usr/local/home/sshserv/.ssh/id_dsa.pub <username>@ucs-unc0<Y>.ucs:/tmp/id_dsa-sshserv.pub_ucs-uncds0<w>.ucs`

5. At the prompt, enter the password for your Active Directory account that is a member of the unc-login user group.

   The public portion of the DSA SSH client keys is copied securely to the `/tmp/` directory on the UNC server.

6. Enter: `exit`

   You are returned to the root prompt.

4.18.17.3
Updating UNCDS Entries in the Authorized Keys List on a UNC Server

After transferring SSH user keys from a zone controller to a Unified Network Configurator (UNC) server, perform the following procedure to update the authorized keys list on the UNC server, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

Prerequisites: Ensure that you know the values that replace the following variables in the procedure:

`0<w>` is the number of Unified Network Configurator Device Server (01 or 02 or 03)

You can use the `hostname` command and the `domainname` command to display the FQDN for the server you are logged into.

Procedure:

1. Access the root command prompt on the UNC server.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. To remove an existing entry from the authorized keys repository, enter:

```
/opt/Motorola/ssh/bin/manage_authorized_keys -d sshserv@uncds-
general_key -u sshserv
```

A message confirming successful key deletion appears.

NOTICE: Ignore the following message: `Failure: No key with a comment of sshserv@uncds-general_key was found!`

3 Enter:
`/opt/Motorola/ssh/bin/manage_authorized_keys -a /tmp/id_rsa-sshserv.pub_ucs-uncds0<w>.ucs -u sshserv`

The authorized keys list now contains the new RSA SSH client public key for the non-interactive UNCDS-UNC SSH client account on the zone controller. Any keys with the same key comment are replaced.

4 Enter:
`/opt/Motorola/ssh/bin/manage_authorized_keys -a /tmp/id_dsa-sshserv.pub_ucs-uncds0<w>.ucs -u sshserv`

The authorized keys list now contains the new DSA SSH client public key for the non-interactive UNCDS-UNC SSH client account on the zone controller. Any keys with the same key comment are replaced.

5 Enter:

a `rm /tmp/id_rsa-sshserv.pub_ucs-uncds0<w>.ucs`

b `rm /tmp/id_dsa-sshserv.pub_ucs-uncds0<w>.ucs`

The RSA and DSA SSH client keys are removed from the `/tmp/` directory.

6 At the prompt, enter: `exit`

You are returned to the root prompt.

4.18.18
Remaining Default SSH Keys Removal for Network Management Servers, ZCs and ISGWs

When specified in the sequence indicated by SSH Rotation on Devices Using Default Keys on page 60, perform the procedures in the following sections to remove remaining default SSH keys on Network Management servers, ZCs and ISGWs.

NOTICE: These procedures apply only to the Network Management servers listed in Table 16: FQDN to Use in Commands for Rotating SSH Keys for Network Management Servers on page 127:

1 Removing Remaining Default SSH Host Keys from Known Hosts Lists for Network Management Servers, ZCs, and ISGWs on page 146.

2 Removing Default SSH Client Keys from an Authorized Keys List for Network Management Servers on page 147

4.18.18.1

Removing Remaining Default SSH Host Keys from Known Hosts Lists for Network Management Servers, ZCs, and ISGWs

For each NM server, zone controller and ISGW, perform the following procedure to remove default SSH host (server) keys that were not removed by the other SSH key rotation procedures, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

NOTICE: Perform this procedure only once on each Network Management Server, ZC, and ISGW following the initial SSH key rotation after an installation that included default keys.

Procedure:

1. Access the root command prompt on the server.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. Enter: `/opt/Motorola/ssh/bin/default_key_detector | grep known_hosts`

   If default SSH host keys are found, a message displays the file name containing the key, in the following format:

   `/usr/local/home/<SSH client account name>/.ssh/ contains a default key found in /etc/opt/Motorola/ssh/ssh_host_keys/<file name>`

   The *<file name>* indicates there is a corresponding default entry in the specified "known_hosts" list. The *<file name>* starts with a name that matches an ASTRO® 25 system device.

   The first time you perform this procedure after initial key rotation, default keys may be detected for zone numbers not present in your system, and for NM servers not present in your system.

3. Review the output:

   - If the output of the `default_key_detector` command does **not** include any names of devices, as part of a *<file name>* at the end of the listing, skip the rest of this procedure.
   - If a *<file name>* displays for a device that does exist in your ASTRO® 25 system, for a non-interactive SSH client accounts known hosts list, then you did not properly provision SSH host keys to the known hosts list on the NM server where you are logged in. Return to SSH Rotation on Devices Using Default Keys on page 60 to perform procedures that you missed. (After completing missed procedures, execute the `default_key_detector` command again.)
   - If a *<file name>* displays for a device that does exist in your ASTRO® 25 system, for an interactive accounts known hosts list, see the note in step 4.
   - If the only *<file name>* that displays at the end of a listing is for a device that is **not** present in your ASTRO® 25 system, then you can proceed to the next step of this procedure.

4. Execute the following command for every device that is **not** present in your ASTRO® 25 system, but was part of a *<file name>* at the end of a `known_hosts_`*<SSH client account name>* listing in step 2:
   `/opt/Motorola/ssh/bin/manage_known_hosts -u <SSH client account name>-d <device name>`

   where *<device name>* is the Fully Qualified Domain Name (hostname.domainname) corresponding to a device that is **not** present in your system and is part of a *<file name>* displayed at the end of the listing in step 2.

NOTICE:
The command will fail for accounts and devices that should **not** be included in the known hosts list of this Network Management server, based on the SSH Rotation on Devices Using Default Keys on page 60.

For example, if a root-level user on a Network Management server accepted an ATR into the known hosts list on the Network Management server, which is not a supported ASTRO® 25 system non-interactive SSH interface, and the ATR default host key had not yet been replaced, the following command would be required to remove that default key information from the Network Management servers known hosts list:

`/opt/Motorola/ssh/bin/manage_known_hosts -u root -d <device name>`

where ***<device name>*** corresponds to the device in the file name at the end of a default_key_detector message (in this case, the ATR name, such as zone00_atr01 for a system-level ATR or zone01_atr01 for the first zone-level ATR)

5 If any other `known_hosts_<SSH client account name>` listing in step 2 displayed a device that is NOT present your ASTRO® 25 system, execute the following command:

`/opt/Motorola/ssh/bin/manage_known_hosts -u <SSH client account name> -d <device name>`

where ***<device name>*** is the Fully Qualified Domain Name (hostname.domainname) corresponding to a device that is NOT present in your system and is part of a ***<file name>*** displayed at the end of a known_hosts listing in step 2.

6 Repeat this procedure starting at step 2 until no more default keys are detected.

4.18.18.2

Removing Default SSH Client Keys from an Authorized Keys List for Network Management Servers

When and where to use: For each Network Management (NM) server, perform the following procedure to remove default SSH client keys from an authorized keys list, according to the sequence specified in SSH Rotation on Devices Using Default Keys on page 60.

NOTICE: Perform this procedure only once on each Network Management server, after the initial SSH key rotation that follows an installation which included default keys.
This procedure does **not** apply to Packet Data Routers, ISGWs, and ISSI.1 Network Gateway site modules.

Procedure:

1 Access the root command prompt on the Network Management server that is an SSH Server.

See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2 To check for default keys, enter: `/opt/Motorola/ssh/bin/default_key_detector`

If default SSH keys are found, a list is displayed in the following format:

<key file>

where ***<key file>*** contains a default key found in `/etc/opt/Motorola/ssh/ssh_host_keys/<file name>`

3 If no file names are displayed, you can skip the rest of this procedure.

4 If default keys are found in the `atialv/.ssh/authorized_keys` file on an ATR, enter:

```
/opt/Motorola/ssh/bin/manage_authorized_keys -d atialv@nmclient-
general_key -u atialv
```

The default keys specified in the command are removed.

5 If default keys are found in an `ssherv/.ssh/authorized_keys` file, enter to display the key comments for the remaining default SSH client keys:
`/bin/awk '{print $3}' /usr/local/home/sshserv/.ssh/authorized_keys | grep general`

6 In the displayed lists, record the name of the SSH client (including zone number) that displays before `-general_key`.

For default keys, `general_key` will be the purpose you see in the key comment. For rotated keys, `noninteractive` will be the purpose you see in the key comment.

If an SSH client displays for a device that *does* exist in your ASTRO ® 25 system, for a non-interactive SSH client accounts known hosts list, then you did not properly provision SSH host keys to the known hosts list on the NM server where you are logged in. Return to SSH Rotation on Devices Using Default Keys on page 60 to perform procedures that you missed. (After completing missed procedures, repeat the command at the beginning of step 5.)

7 Perform the following actions:

a To remove default entries in authorized_keys-sshserv for a ***<user>*** and ***<device name>*** that was displayed in a key comment in the result of step 5, enter:
`/opt/Motorola/ssh/bin/manage_authorized_keys -d <user>@<device name>-general_key -u sshserv`

where ***<device name>*** should include the zone number, if provided in the key comment

b Repeat the preceding command for device names in any other sshserv key comments you recorded.

8 Repeat this procedure starting at step 2, until no more default keys exist in the authorized keys lists on this server.

4.18.19
Final Verification of Default Key Removal

Perform the procedures in the following sections for NM Servers, ZCs, and ISGWs.

Perform Detecting Remaining Default SSH Keys on an NM Server, ZC, or ISGW For Final Verification on page 148 on each NM server, zone controller and ISGW. Detecting Remaining Default SSH Keys on an NM Server, ZC, or ISGW For Final Verification on page 148 detects default SSH host and client keys on the NM server, zone controller and ISGW where you are logged in.

This includes default Packet Data Gateway (PDG) entries in the authorized keys list on a Unified Network Configurator (UNC) server, but does *not* include:

- Default keys or default entries in the known hosts list on the PDG
- Default Network Management (NM) Client entries in authorized keys lists

4.18.19.1
Detecting Remaining Default SSH Keys on an NM Server, ZC, or ISGW For Final Verification

When and where to use:

Perform this procedure according to the sequence of procedures specified in SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1. Access the root command prompt on the NM server, ZC, or ISGW.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. Execute the following command to check for default SSH host keys on the NM server, ZC or ISGW where you are logged in:

   `/opt/Motorola/ssh/bin/default_key_detector`

3. Use the output of the default_key_detector command, as described below, to determine if you need to return to SSH Rotation on Devices Using Default Keys on page 60 to perform procedures that you missed. (After completing missed procedures, execute the default_key_detector command again.)

   - If there are no default_key_detector messages with a ***<file name>*** at end that includes a device name, then you have completed this procedure. Continue to Additional Default Key Removal Considerations – Linux Backup Service Client Keys on page 149.
   - If one or both of the following display, then you did not properly replace the SSH host keys on the device where you are logged in:
     - `/etc/ssh/ssh_host_rsa_key.pub contains a default key...`
     - `/etc/ssh/ssh_host_dsa_key.pub contains a default key...`
   - If one or both of the following display, then you did not properly replace the SSH client keys on the device where you are logged in:
     - ***<SSH client account home directory>***`/.ssh/id_rsa.pub contains a default key...`
     - ***<SSH client account home directory>***`/.ssh/id_dsa.pub contains a default key...`
   - If a device name is part of the ***<file name>*** at the end of any other output from the default_key_detector command, then you did not properly update the known hosts list or the authorized key list on the device where you are logged in.

4.18.19.2
Additional Default Key Removal Considerations – Linux Backup Service Client Keys

If a default_key_detector message displays `/usr/local/home/bkupclnt/.ssh/bar_client_registration`, then return to and perform procedures you missed for updating the Backup and Restore (BAR) client registration keys on the Linux-based server where you are logged in.

After completing missed procedures, execute the default_key_detector command again. If `/usr/local/home/bkupclnt/.ssh/bar_client_registration` does not display, the default BAR client keys are no longer being used on the server where you are logged in.

Then, if required by your organizations policies, remove from this server the default BAR client registration key file which is stored at: `cp /usr/local/home/bkupclnt/.ssh/bar_client_registration.orig`. (If you first back it up to a secure location, then, if needed, you can restore it to its original location on this BAR client, so that you can still use the BAR server administration menu option to re-enable BAR service default keys.)

4.18.19.3

Additional Default Key Removal Considerations – Unexpected Default Entries in Known Hosts Lists

If a user accepts a device into the known hosts list on a Linux-based server before the default SSH host key has been replaced on that device, and that device should *not* be included in the known hosts list based on SSH Rotation on Devices Using Default Keys on page 60, then the default_key_detector will display a message about that default key.

In this case, the commands provided in previous procedures for removing default key information may fail. You will need to modify the commands for the account name and the device associated with the default key.

For example, if a root-level user on a Network Management server accepted an ATR into the known hosts list on the Network Management server, which is not a supported ASTRO® 25 system SSH relationship, and the ATR default host key had not yet been replaced, the following commands would be required to remove that default key information from the Network Management server:

```
/opt/Motorola/ssh/bin/manage_known_hosts -u root -d <device name>
```

where ***<device name>*** corresponds to the device in the file name at the end of a default_key_detector message (in this case, the ATR name, such as zone00_atr01 for a system-level ATR or zone01_atr01 for a zone-level ATR).

4.18.20

Detecting Default Keys on a PDG

Perform the following procedure to detect default SSH client keys on the Packet Data Gateway (PDG) and default entries in the PDG known hosts list.

Perform this procedure according to the sequence of procedures specified in the SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1. Access the root command prompt for the PDG.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2. Enter the following command:

   ```
   default_key_detector
   ```

   The script checks for default keys and known host list entries associated with the non-interactive SSH client account used for SSH communications between the PDG and UNC server and displays appropriate messages.

3. Perform one of the following actions:

   NOTICE: The same hostname message may appear twice, because it is generated exactly the same for RSA keys and for DSA keys in the known hosts list.

If…	Then…
If the following message displays: `no default key found` **informing that no default keys were detected on the PDG,**	go to the next step.
If the following message displays:	perform the following actions:

If…	Then…
`/usr/local/home/pdr/.ssh/id_rsa.pub contains a default key` **informing that the SSH client key file on the PDR is still the default file (it has not been re-generated),**	**a** Go to SSH Rotation on Devices Using Default Keys on page 60. **b** Complete the steps missed for regenerating the SSH client key files on this PDR. **c** Repeat this detection procedure.

If either of the following messages displays:
`/usr/local/home/pdr/.ssh/known_hosts contains a default key; hostname: ucs-unc01.ucs,ucs-unc01,<IP address of primary core UNC>`
or
`/usr/local/home/pdr/.ssh/known_hosts contains a default key; hostname: ucs-unc02.ucs,ucs-unc02,<IP address of backup core UNC>`
informing that UNC SSH host key entries in the PDR known hosts list are still the defaults (they have not been replaced), for devices that are present in your system, and your system includes the Dynamic System Resilience feature,
	perform the following actions:
	a Go to SSH Rotation on Devices Using Default Keys on page 60.
	b Complete the steps missed for replacing the UNC server entries in the known hosts list on this PDR.
	c Repeat this detection procedure.

If the following message displays: `/usr/local/home/pdr/.ssh/known_hosts contains a default key; hostname: ucs-unc01.ucs,ucs-unc01,<IP address of primary core UNC>` **informing that UNC SSH host key entries in the PDR known hosts list are still the defaults (they have not been replaced), for the primary core UNC, and your system does not include the Dynamic System Resilience feature,**	perform the following actions: **a** Go to SSH Rotation on Devices Using Default Keys on page 60. **b** Complete the steps missed for replacing the UNC server entries in the known hosts list on this PDR. **c** Repeat this detection procedure.
If the following message displays: `/usr/local/home/pdr/.ssh/known_hosts contains a default key; hostname: ucs-unc02.ucs,ucs-unc02,<IP address of backup core UNC>` **informing that UNC SSH host key entries in the PDR known hosts list are still the defaults for the backup core UNC, and your system does not include the Dynamic System Resilience feature,**	perform the following actions: **a** Go to Removing Backup Core UNC Server Defaults in a PDG Known Hosts List (Non-DSR Systems Only) on page 152. **b** Repeat this detection procedure.
If only the following message displays: `/tmp/secman_keys_hosts_backup.tar contains a default key`	execute the following command to overwrite this backup file:

If…	Then…
indicating that defaults were found,	`/usr/local/sbin/secman --backup`

4 Enter the following to log out of the PDG: `exit`

4.18.21

Removing Backup Core UNC Server Defaults in a PDG Known Hosts List (Non-DSR Systems Only)

If your system does not include the Dynamic System Resilience (DSR) feature, perform the following procedure to remove default entries in the Packet Data Gateway (PDG) known hosts list for the DSR backup core Unified Network Configurator (UNC) server.

Perform this procedure according to the sequence of procedures specified in the SSH Rotation on Devices Using Default Keys on page 60.

Procedure:

1 Access the root command prompt for the PDG.

See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.

2 Execute the following command to delete any default entries for the backup core UNC server in the known hosts list on the PDG for the PDR-UNC SSH client account:

`manage_known_hosts -u pdr_app -d ucs-unc0<Y>.ucs`

where `<Y>` is the number of the UNC server with the new SSH host keys

A message confirms that the keys for the specified UNC server were deleted from known_hosts.

3 Enter the following to log out of the PDG: `exit`

4.18.22

Backing Up SSH Data to the Centralized Backup Server from All Backup Clients

The following information applies to Network Management servers, ISGWs, and zone controllers.

The information does **not** apply to ISSI.1 Network Gateway site modules on Generic Application Servers, or to Packet Data Router modules on Packet Data Gateways, because they do not support the centralized Backup and Restore feature.

If the centralized backup and restore feature is implemented, you can use one of the following methods to back up SSH data from the Backup Clients to a centralized backup server:

- Wait for scheduled backups to occur. Confirm backups have occurred using the reporting tools on the centralized backup server(s).
- Schedule a one-time backup for one selected Backup Client at a time, using the administration menus on the centralized backup server(s).

IMPORTANT: Do not schedule backups of Backup Clients until indicated in SSH Rotation on Devices Using Default Keys on page 60, so that backups of SSH data occur in secure mode. If your system includes the Dynamic System Resilience feature, make sure that backups occurred on each primary core centralized backup server, and on each backup core centralized backup server.

For additional information, see the following ASTRO® 25 communication system manuals:

- *Backup and Restore Services*

- The manual for the specific server you are backing up

4.18.23
Restoring SSH Data To NM Servers, ZCs, and ISGWs Using Centralized Backups

When and where to use:
The following information applies to Network Management servers, zone controllers, and ISGWs.

The information does **not** apply to ISSI.1 Network Gateway site modules on Generic Application Servers, or to Packet Data Router modules on Packet Data Gateways, because they do not support the centralized Backup and Restore feature.

If the centralized backup and restore feature is implemented, restoring data is a two-step process:

Process:

1. Restore the consolidated backup file to the device from the centralized backup.
2. Use the administration menu options on the devices to restore SSH data to its proper location on the device from the consolidated data file that the centralized backup service restores to the device.

4.19
Regenerating SSH Host Keys for an ISSI.1 Network Gateway Site

Prerequisites:
Obtain the following information:

- ISSI administrator account name and password

  NOTICE: 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.
- ISSI.1 Gateway Module IP address
- Site Link Relay Module IP address

When and where to use:
An ASTRO® 25 system ISSI.1 Network Gateway site includes two modules that each require their own SSH host key in order to communicate with SSH clients such as the NM Client. This section provides the two procedures for generating these host keys:

Process:

1. Regenerating the SSH Host Keys on an ISSI.1 Gateway Module on page 153
2. Regenerating the SSH Host Keys on a Site Link Relay Module in an ISSI.1 Network Gateway Site on page 154

Related Links

Configuring SSH for Devices at an ISSI.1 Network Gateway Site on page 52

4.19.1
Regenerating the SSH Host Keys on an ISSI.1 Gateway Module

When and where to use:

Perform the following procedure to re-generate SSH host keys on an ISSI.1 Gateway Module. This procedure must be repeated for each ISSI.1 Gateway Module on each Generic Application Server in an ISSI.1 Network Gateway site.

Procedure:

1. Access the ISSI.1 Gateway Module using its IP address and your Active Directory account that is a member of the instadm or secadm user group.

   The command prompt displays.

2. Enter the following command: `admin_menu`

   The ISSI.1 Gateway Module server administration main menu displays.

3. Enter the number for the option **OS Administration**.

   The OS Administration menu displays.

4. Enter the number for the option **Security Provisioning**.

   The Security Provisioning menu displays.

5. Enter the number for the option **Manage SSH Keys**.

   The Manage SSH Keys menu displays.

6. Enter the number for the option **Regenerate SSH Keys**.

   You are prompted to confirm you want to re-generate the SSH keys.

7. Type `y` and press ENTER.

   A message displays the fingerprint for the new SSH host keys and prompts you to press `c` to continue.

8. For optimal security, record the fingerprint so that you can reference it when initiating an SSH session with this ISSI.1 Gateway Module from an SSH client.

9. Type `c` to continue.

   The Manage SSH Keys menu appears.

10. Type `q` and press ENTER.

    The shell prompt appears.

11. Type `exit` and press ENTER.

    The SSH session ends.

12. Verify that a secure connection can be established with this ISSI.1 Gateway Module, as follows:

    a Initiate another SSH session with this ISSI.1 Gateway Module (see step 1).

    b When the fingerprint displays, verify it and then accept the host.

4.19.2
Regenerating the SSH Host Keys on a Site Link Relay Module in an ISSI.1 Network Gateway Site

When and where to use:

Perform the following procedure to re-generate SSH host keys on a Site Link Relay Module. This procedure must be repeated for each Site Link Relay Module on each Generic Application Server in an ISSI.1 Network Gateway site.

Procedure:

1. Access the Site Link Relay Module using its IP address and your Active Directory account that is a member of the instadm or secadm user group.

   The command prompt displays.

2. Enter the following command: `admin_menu`

   The Site Link Relay Module server administration main menu displays.

3. Enter the number for the option **OS Administration**.

   The OS Administration menu displays.

4. Enter the number for the option **Security Provisioning**.

   The Security Provisioning menu displays.

5. Enter the number for the option **Manage SSH Keys**.

   The Manage SSH Keys menu displays.

6. Enter the number for the option **Regenerate SSH Keys**.

   You are prompted to confirm you want to re-generate the SSH keys.

7. Type `y` and press ENTER.

   A message displays the fingerprint for the new SSH host keys and prompts you to press `c` to continue.

8. For optimal security, record the fingerprint so that you can reference it when initiating an SSH session with this Site Link Relay Module from an SSH client.

9. Type `c` to continue.

   The Manage SSH Keys menu appears.

10. Type `q` and press ENTER.

    The shell prompt appears.

11. Type `exit` and press ENTER.

    The SSH session ends.

12. Verify that a secure connection can be established with this Site Link Relay Module, as follows:

    a Initiate another SSH session with this Site Link Relay Module (see step 1).

    b When the fingerprint displays, verify it, and then accept the host.

4.20 SSH Configuration for RF Site Devices and VPMs Using CSS – Overview

SSH can be configured for the following devices using Motorola Solutions Configuration/Service Software (CSS) application:

- GTR 8000 base radios

- GCP 8000 site controllers
- GPB 8000 Reference Distribution Modules (RDMs)
- GCM 8000 comparators
- VPM-based devices:
  - SmartX Site Converters
  - MCC 7500 console VPMs
  - Telephone Media Gateways

When SSH is implemented, CSS functions will automatically use the secure mode instead of the clear mode.

NOTICE: This information does not apply to VPM-based devices for which the SSH protocol is disabled by default and needs to be enabled manually.

In secure mode, CSS is the SSH client and the devices it manages are the SSH servers. CSS authenticates with an RF Site device (SSH server) based on the FQDN or IP address of the device, and the Public Key. If the Known Hosts List stored in CSS contains the correct Host - Public Key pair, then CSS will successfully connect to the device.

The following SSH configuration functionality is available in CSS:

- Configuring Secure Services/Keys and Clear Services Using CSS on page 156
- Adding a Device to the CSS Known Hosts List on page 159
- CSS Known Hosts List Management on page 159
- Backing Up the Secure Services Settings for a Device Using CSS on page 159
- Restoring the Secure Services Settings for a Device Using CSS on page 160
- Regenerating SSH Server Keys on a Device Using CSS on page 162

After you use CSS to regenerate SSH server keys for a device, or configure Secure/Clear settings for a device, you will be prompted to re-add that device (SSH server) to your CSS Known Hosts List the first time you connect to that device.

CSS can be used remotely from the Network Management (NM) Client, or locally from a technicians laptop connected to the service port of a device.

4.21 SSH Configuration Using CSS – Procedures

This section provides procedures for configuring SSH on devices using Motorola Solutions Configuration/Service Software (CSS) application.

4.21.1 Configuring Secure Services/Keys and Clear Services Using CSS

Prerequisites: To perform this procedure securely, enable SNMPv3 (with both authentication and encryption) first. For information about enabling SNMPv3 using CSS, see *Core CSS Online Help* and the *SNMPv3* manual.

When and where to use: Perform the following procedure to use Configuration/Service Software (CSS) to configure secure services settings and clear services settings on a device. When you enable Secure Shell Services using this procedure, keys are automatically generated on that device.

IMPORTANT: It is recommended to use secure protocols unless clear protocols are required for your system.

IMPORTANT: For VPM-based devices the clear protocols (i.e. FTP and Telnet) are enabled by default, while the secure protocols (i.e. SSH and SFTP) are disabled. Use the CSS to enable the secure protocols and disable the clear ones for the following devices: SmartX, MCC 7500 console VPMs and Telephone Media Gateways.

Procedure:

1 Launch the CSS application.

2 From the **File** menu, select **Read Configuration From Device**.

A message window states that an Ethernet connection must be established.

3 Click **OK**.

The **Connection** Screen appears.

4 Enter the ***<IP address>*** of the device you want to access and click **Connect**.

NOTICE: If an authentication window appears, enter your credentials and click **OK**.

A message window appears displaying the `CSS Successfully Connected to this Device` message and a `CSS has successfully read the configuration data` message.

5 Continue to click **OK** when prompted.

The device configuration displays in CSS.

6 From the **Security** menu, select **Device Security Configuration**, and then select **Remote Access/Login Banner (Ethernet)**.

The **Remote Access Configuration** tab of the **Remote Access/Login Banner** window displays.

7 Select the desired service to be either enabled or disabled:

- The **Enable** setting for **Secure Shell Services** must be selected in order for the other options to be available. When Secure Shell Services are disabled, the other secure protocols are disabled on the device even if the Requested field shows `Enabled` for these protocols on the configuration window. (For the current state of a protocol on the device, see the Actual field after clicking **Apply** or **OK**).
- To disable the FTP protocol for VPM-based devices, from the **Secure Software Download** section, select the SFTP option and then, in the **Clear Services** section, disable the FTP option.

If…	Then…
If you want to enable secure services on this device,	perform the following actions: **a** Click the **Enable** option for the following **(Requested)** fields: • **Secure Terminal** • **Secure FTP** • **Secure Shell Service** **NOTICE:** The Secure Terminal setting you select will depend on your organizations policies about the mechanism used for managing equipment. This setting does not impact any functions in CSS.

If…	Then…
	b Click the **Sftp** option for **Secure Download Transfer Mode** in order to enable secure software downloads.
If you want to disable secure services on this device,	perform the following actions: **a** Click the **Disable** option for the following **(Requested)** fields: • **Secure Terminal** • **Secure FTP** • **Secure Shell Service** **b** Click the **Ftp** option for **Secure Download Transfer Mode** in order to disable secure software downloads.
If you want to enable clear services on this device,	click the **Enable** option for the following **(Requested)** fields: • **TELNET** • **FTP** **NOTICE:** The **TELNET** setting you select will depend on your organizations policies about the mechanism used for managing equipment. This setting does not impact any functions in CSS.
If you want to disable telnet services on this device,	click the **Disable** option for the **TELNET** field.
If you want to disable FTP services on this device,	perform the following actions: **a** Select **Enable** for the **Secure Shell Service** option. **b** Select **Enable** for the **Secure FTP** option. **c** Click the **Disable** option for the **FTP** field. **NOTICE:** Software Download Manager will still use Clear FTP, even if the FTP setting selected here is **Disable**.

8 Perform one of the following actions:

- To apply the settings and close the window, click **OK**.
- To apply the settings and leave the window open, click **Apply**.

On the **Remote Access/Login Banner** window, the fields labeled **(Actual)** reflect the same settings as the fields labeled **(Requested)**. This verifies that the settings have been applied.

NOTICE: It is not necessary to perform any additional steps to write this configuration to the device, assuming that step 2 of this procedure was performed successfully.
It is not necessary to click the **Regenerate Keys** button when you enable secure services. The keys are automatically generated when **Enable** is applied for **Secure Shell Service**.

Related Links

Configuring SSH for Devices at the Zone Core on page 47
Configuring SSH for Devices at an RF Site on page 50
Configuring SSH for Devices at a Dispatch Site on page 53

4.21.2
Adding a Device to the CSS Known Hosts List

After applying the **Enable** setting for **Secure Shell Service** and **Secure FTP** on a device, you are prompted to accept that device into the CSS Known Hosts List the first time an SFTP session is initiated with that device. This prompt displays:

- When you select **Status Report Screen** from the **Service** menu for that device.
- When you select **Status Panel Screen** from the **Service** menu, if the device is a GTR 8000 base radio.
- When you select **Read Configuration from Device**, and CSS does not already have current data on that device.

After you accept the prompt, completion of the CSS function (including logging into the device) indicates that Secure FTP is working correctly.

You can verify that the device was accepted into the CSS Known Hosts List by selecting **Known Hosts List Management** from the **Security** menu in CSS. This list also displays the key fingerprint for each host.

For additional information, see *Core CSS Online Help*.

Related Links

Configuring SSH for Devices at the Zone Core on page 47
Configuring SSH for Devices at an RF Site on page 50
Configuring SSH for Devices at a Dispatch Site on page 53

4.21.3
CSS Known Hosts List Management

The CSS Known Hosts List includes keys for all of the devices that have established a secure session with CSS. It displays the fingerprint for each device.

The following tasks can be performed using the **Known Hosts List Management** screen in CSS:

- Backing up the Known Hosts List
- Restoring the Known Hosts List
- Clearing the Known Hosts List

To access these functions, select **Known Hosts List Management** from the **Security** menu in CSS.

The **Backup** button on the **Known Hosts List Management** screen provides a way to save a CSS Known Hosts List file with any file name and in any location accessible from the computer hosting CSS.

The **Restore** button on the **Known Hosts List Management** screen provides a way to load your backup file of the CSS Known Hosts List into other instances of CSS on other computers, in addition to using it to restore the Known Hosts List to CSS on the computer where the backup file was created.

For more information on how to use the **Known Hosts List Management** screen, see *Core CSS Online Help*.

4.21.4
Backing Up the Secure Services Settings for a Device Using CSS

Prerequisites:

NOTICE: To perform this procedure securely, enable SNMPv3 (with both authentication and encryption) first. For information about enabling SNMPv3 using CSS, see *Core CSS Online Help* and the ASTRO® 25 communication system *SNMPv3* manual.

When and where to use:
The following procedure describes how to use Configuration/Service Software (CSS) to back up the secure services settings for a device.

Procedure:

1. Launch the **CSS** application.
2. From the **File** menu, select **Read Configuration From Device**.

   A message window states that an Ethernet connection must be established.
3. Click **OK**.

   The **Connection** Screen appears.
4. Enter the ***<IP address>*** of the device you want to access and click **Connect**.

   NOTICE: If an authentication window appears, enter your credentials.

   A message window reports that CSS successfully connected to this device, and that CSS successfully read the configuration data.
5. Click **OK** when prompted.

   The device configuration displays in CSS.
6. From the **File** menu, select **Save As** to create a backup of the configuration file.

   The **Properties** dialog box appears.
7. Enter the required information, and a description for this file if desired. Click **OK**.

   The **Save** dialog box appears.
8. Enter a name for the file.
9. In the **Look in** field, navigate to the directory in which you want to store the backup file.
10. Click **Save**.

    The file is saved as a .CPL file.

4.21.5
Restoring the Secure Services Settings for a Device Using CSS

Prerequisites:

NOTICE: To perform this procedure securely, enable SNMPv3 (with both authentication and encryption) first. For information about enabling SNMPv3 using CSS, see *Core CSS Online Help* and the ASTRO® 25 communication system *SNMPv3* manual.

When and where to use:
Perform the following procedure to use Configuration/Service Software (CSS) to restore the secure services settings for a device. Before performing the procedure, review the following information for an explanation of impacts on the **CSS Remote Access/Login Banner (Ethernet)** screen at different points during the procedure.

The **Remote Access** tab of the **CSS Remote Access/Login Banner (Ethernet)** screen displays the secure settings for a device. The **Remote Access** tab operates in the following two modes:

- **Offline mode**: In offline mode, all the parameters on the **Remote Access/Login Banner** screen are read from the local backup and the actual status of the services is set to N/A. Offline mode occurs when you do not read the configuration from the device, even if CSS is connected to the device. The security parameters are not stored in the device or backup until you write the configuration to the device and back up the configuration.
- **Online mode**: In online mode, all parameters on the **Remote Access/Login Banner** screen are read from the connected device and the actual status of services is set to either On or Off. Online mode occurs when the configuration is read from the device and CSS remains connected to the same device. The security parameters are stored directly on the device after you click the **OK** or **Apply** button.

Procedure:

1. Launch the **CSS** application.
2. From the **Tools** menu, select **Connection Configuration** or click the **Connect to Device** icon on the toolbar.
3. Enter the ***<IP address>*** of the device you want to access and click **Connect**.

   NOTICE: If an authentication window appears, enter your credentials.

   A message window reports that CSS successfully connected to this device, and that CSS successfully read the configuration data.
4. From the **File** menu, select **Open**.

   The **Open** dialog box appears.
5. Navigate to the directory which contains the backup file (.cpl), select it, and then click **Open**.
6. From the **File** menu, select **Write Configuration to Device**.

   A success message appears after CSS writes the configuration data to the device.
7. From the **File** menu, select **Read Configuration From Device**.

   A success message appears after CSS reads the configuration data from the device.
8. From the **Security** menu, select **Device Security Configuration**, and then select **Remote Access/Login Banner (Ethernet)**.

   The **Remote Access/Login Banner** screen appears displaying the **Remote Access Configuration** tab.
9. Perform the following actions:
   a. Verify the states of the following secure options:
      - Secure Shell Service (Actual)
      - Secure Terminal (Actual)
      - Secure FTP (Actual)

   b. Verify the states of the following clear options:
      - TELNET (Actual)
      - FTP (Actual)

   The secure services settings display the values that are restored from the backup file.

4.21.6
Regenerating SSH Server Keys on a Device Using CSS

Prerequisites:

NOTICE: To perform this procedure securely, enable SNMPv3 (with both authentication and encryption) first. For information about enabling SNMPv3 using CSS, see *Core CSS Online Help* and the ASTRO® 25 communication system *SNMPv3* manual.

When and where to use:
Perform the following procedure to use Configuration/Service Software (CSS) to regenerate SSH server keys for a device).

Procedure:

1. Launch the CSS application.
2. From the **File** menu, select **Read Configuration From Device**.

   A message window states that an Ethernet connection must be established.
3. Click **OK**.

   The **Connection** Screen appears.
4. Enter the ***<IP address>*** of the device you want to access and click **Connect**.

   NOTICE: If an authentication window appears, enter your credentials.

   A message window reports that CSS successfully connected to this device, and that CSS successfully read the configuration data.
5. Click **OK** when prompted.

   The device configuration displays in CSS.
6. From the**Security** menu, select **Device Security Configuration**, and then select **Remote Access/Login Banner (Ethernet)**.
7. Click the **Regenerate Keys** button.

   NOTICE: This button is only available when Secure Shell Service **(Actual)** state is **On** and Secure Shell Service **(Requested)** state is **Enabled** and has not changed since the last successful Write Configuration to Device operation. See Configuring Secure Services/Keys and Clear Services Using CSS on page 156.

   The following message displays:

   ```
   Secure Shell keys were regenerated successfully
   ```

4.22
SSH Configuration on MLC 8000 Devices

This section covers configuring SSH on MLC 8000 Devices.

4.22.1
Changing Server SSH Public/Private Key Pair on an MLC 8000 Device

Follow this procedure to generate a new SSH public/private key pair for the MLC 8000 device.

Prerequisites: Verify that:

- The PC used to change the MLC 8000's SSH public/private key pair is connected to the MLC 8000 Analog Comparator or the MLC 8000 Subsite Link Converter through the local O&M connection or remotely.
- The PC used to create or change the MLC 8000's SSH public/private key pair has a terminal emulator or PuTTY installed on it.

NOTICE: A version of PuTTY is provided on the ASTRO® 25 System *Windows Supplemental* media.

Procedure:

1. Establish communication with the MLC 8000 device:
   - If the PC is connected to the MLC 8000 OM port, use a terminal emulation program, such as ProComm+ or HyperTerminal, or the serial connection option in PuTTY.
   - If the PC is connected to the external LAN port, use the SSH option in PuTTY.
2. When prompted, press the appropriate key to continue.
3. When prompted to log into the device, enter the username and password of the MLC 8000 device.

   The **MMI** window is opened.
4. Enter `1` for the option **Change Password or Keys**.
5. Enter `2` for the option **Update SSH Keys**.

   The MMI displays a message indicating that the update of SSH keys is in progress. Upon completion of new key generation, the MMI displays information regarding the success or failure of SSH keys generation.
6. Exit the command window.

Related Links

Configuring SSH for Devices at an RF Site on page 50

4.23
SSH Configuration on Routers, Gateways, and HP Switches Using VoyenceControl

This section covers configuring SSH on HP switches, Motorola routers and gateways, using the VoyenceControl component of Motorola Solutions Unified Network Configurator (UNC) tool.

In VoyenceControl, Motorola Solutions provides pre-tested templates and saved commands for configuring SSH on these devices.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

In an ASTRO® 25 communication system, these devices are only configured as SSH hosts for the purpose of interactive SSH sessions. The UNC is configured as the SSH client.

After performing the procedures in this section to generate host keys on routers and switches, you can use other SSH clients to initiate SSH sessions with routers and switches. For example, see Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

For VoyenceControl procedures in this section that can be performed on more than one device of the same type at the same time, where the procedure has a step to right-click a device, you can also select multiple devices, then right-click. You select multiple devices by holding down the SHIFT key and dragging the cursor over the devices, or holding down the CTRL key and clicking the device.

For additional information on the UNC tool, see the *Unified Network Configurator* manual.

4.23.1

Templates and Commands for Configuring SSH on Routers, Gateways and HP Switches Using VoyenceControl

The following table lists the Motorola Solutions templates and saved commands available in VoyenceControl that are used in the following processes for HP switches, Motorola routers and gateways:

- Generating Initial SSH Host Keys and Enabling Secure Mode for Routers and Gateways Using VoyenceControl on page 165
- Enabling Clear Mode for Routers, Gateways, and HP Switches Using VoyenceControl on page 179
- Rotating SSH Host Keys on Routers, Gateways, and HP Switches Using VoyenceControl on page 166
- Enabling Clear Mode for Routers, Gateways, and HP Switches Using VoyenceControl on page 179
- Disabling Telnet on Routers, Gateways, and HP Switches Using VoyenceControl on page 181
- Disabling Secure Mode on Routers, Gateways, and HP Switches Using VoyenceControl on page 182

Table 18: Templates and Saved Commands for Configuring Secure Mode and Clear Mode on Routers, Gateways and HP Switches Using VoyenceControl

Device	Task You Are Performing	Template or Saved Command	Subfolder Where Template is Located (Under System → Motorola)	Name of the Template
Motorola router or gateway	Generating SSH server keys	Saved Command	MNR	Generate Keys for MNR
	Enabling Secure and Clear modes	Template	MNR	Enable SSH and Telnet in MNR
	Disabling Clear mode	Template	MNR	Disable Telnet in MNR
	Disabling Secure mode	Template	MNR	Disable SSH in MNR
HP switch	Generating SSH server keys	Saved Command	HP	Generate Key Pair in HP Switch
	Enabling Secure mode	Template	HP	Enable SSH in HP Switch

Device	Task You Are Performing	Template or Saved Command	Subfolder Where Template is Located (Under System → Motorola)	Name of the Template
	Enabling Clear mode	Template	HP	Enable Telnet in HP Switch
	Disabling Clear mode	Template	HP	Disable Telnet in HP Switch
	Disabling Secure mode	Template	HP	Disable SSH in HP Switch

4.23.2

Generating Initial SSH Host Keys and Enabling Secure Mode for Routers and Gateways Using VoyenceControl

When and where to use:
Perform the following process to enable secure mode for Motorola routers and gateways in an ASTRO® 25 communication system using the VoyenceControl component of the Unified Network Configurator (UNC) tool. Use the saved command and template indicated in the steps of the process.

Process:

1. Perform Logging into VoyenceControl on page 167.
2. Perform Using a Saved Command to Generate Keys on Routers and Gateways on page 167.
3. Enable secure mode on the routers and gateways, using the template**Enable SSH and Telnet in MNR** located in the MNR template folder. See:
   a. Accessing the Configlet Editor on page 172.
   b. Using a Pre-Tested Template to Populate a Configlet on page 173.
   c. Scheduling the Job on page 174.
   d. Viewing Job Status in the Schedule Manager on page 176.
4. Perform Enabling SSH/SCP Management Mechanism in Device Properties in VoyenceControl on page 176.
5. For each router or gateway, right-click the device in the main **VoyenceControl** window, and select **Pull**, then **Pull Config** from the popup menus.

   This updates the VoyenceControl with the device configuration changes and adds the new SSH keys to the known hosts list on the UNC server.

Related Links

Configuring SSH for Devices at the Zone Core on page 47
Configuring SSH for Devices at an RF Site on page 50
Configuring SSH for Devices at an ISSI.1 Network Gateway Site on page 52
Configuring SSH for Devices at a Dispatch Site on page 53

4.23.3

Generating Initial SSH Host Keys and Enabling Secure Mode for HP Switches Using VoyenceControl

When and where to use:

Perform the following process to enable secure mode for HP switches in an ASTRO® 25 communication system using the VoyenceControl component of the Unified Network Configurator (UNC) tool. Use the Motorola Solutions templates indicated in the steps of the process.

NOTICE: When secure mode is enabled on an HP switch, file transfer is only supported through scp regardless of the clear protocol setting.

Process:

1. Perform Logging into VoyenceControl on page 167.
2. Generate keys on one or more HP switches at a time.

   See Using a Saved Command in VoyenceControl to Generate SSH Keys on HP Switches on page 168.
3. Enable secure mode on the switches, using the template **Enable SSH in HP Switch** located in the `HP` template folder under the `Motorola` folder.

   See:

   - Accessing the Configlet Editor on page 172.
   - Using a Pre-Tested Template to Populate a Configlet on page 173
   - Scheduling the Job on page 174
   - Viewing Job Status in the Schedule Manager on page 176
4. Perform Enabling SSH/SCP Management Mechanism in Device Properties in VoyenceControl on page 176.
5. For each switch, right-click the switch in the main VoyenceControl window, and select **Pull**, then **Pull Config** from the popup menus.

   This updates the VoyenceControl with the switch configuration changes and adds the new SSH keys to the known hosts list on the UNC server.

Related Links

Configuring SSH for Devices at the Zone Core on page 47
Configuring SSH for Devices at an RF Site on page 50
Configuring SSH for Devices at an ISSI.1 Network Gateway Site on page 52
Configuring SSH for Devices at a Dispatch Site on page 53

4.23.4

Rotating SSH Host Keys on Routers, Gateways, and HP Switches Using VoyenceControl

For periodic SSH key rotation (not for initial SSH configuration), perform the following procedures, so that a new key for the device will be added to the UNC servers known hosts list.

NOTICE: This process assumes that the device (router, gateway, or switch) is operating in secure mode, and that VoyenceControl is set up to communicate with the device in secure mode.

Process:

1. Perform one of the following actions:

   - To generate keys on a Motorola router or gateway, perform Using a Saved Command to Generate Keys on Routers and Gateways on page 167.
   - To generate keys on an HP switch, perform Using a Saved Command in VoyenceControl to Generate SSH Keys on HP Switches on page 168.

2 Perform Deleting SSH Keys from the UNC Server Known Hosts List Using the Administration Menu on page 179.

3 Perform Verifying Secure Mode/Updating Known Hosts List for UNC Management of a Device on page 177.

4.23.5
Logging into VoyenceControl

When and where to use:
Access to VoyenceControl is established through the Network Configuration Manager splash screen and sign-on screen.

The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

Procedure:

1 On the Network Management client where you set up VoyenceControl, double-click the UNC shortcut on the desktop.

You can also paste the following address into the IE web browser:

`https://ucs-unc0<Y>.ucs`

where `<Y>` is the number of the UNC server (1 for the primary core UNC server, and 2 for the backup core UNC server)

Internet Explorer opens to the URL of the application server, and a VoyenceControl client session launches with the welcome page.

2 Click the **VoyenceControl** link.

A VoyenceControl client session launches, and the login dialog box appears.

3 Enter the User ID and Password, and click **OK**.

The **VoyenceControl** main window appears.

4.23.6
Using a Saved Command to Generate Keys on Routers and Gateways

When and where to use:
The following procedure describes how to use a Saved Command in the VoyenceControl component of the Unified Network Configurator (UNC) tool to generate keys on a Motorola router or gateway.

NOTICE: For additional ways to use Saved Commands in VoyenceControl, see the *Unified Network Configurator* manual.

Procedure:

1 Log into VoyenceControl.

The **VoyenceControl** main window appears.

2 In the navigation pane on the left side of the window, double-click **Astro 25 Radio Network**.

The selected network tree expands to display the **Devices** node.

3 In the navigation pane on the left side of the window, double-click **Views**, and then double-click **MNR View**.

NOTICE: Alternatively, if you are configuring a single site at a time, you can select the Zone name and then the Site name in the navigation pane on the left side of the window. You can sort the Site view on the right side of the window by Device Class. This arranges the list so that all of the devices of the same type at the site are listed together.

The **Devices View** appears. A list of routers and gateways displays in the pane on the right side of the screen, with the associated device properties.

4 Right-click the desired device(s) in the Devices View pane on the right side of the screen.

The context menu appears.

5 From the context menu, select **Saved Command**.

The **Select Item** dialog box appears.

6 Click the folder icon at the top of the dialog box, to the right of the **Look in** field. Continue to click this icon until the `System` folder displays in the list of folders on the Select Item dialog box.

7 In the list of folders on the **Select Item** dialog box, double-click the **System folder**, then double-click the **Motorola** folder, and then double-click the **MNR** folder.

A list of saved commands displays in the Select Item dialog box.

8 Double-click the saved command named **Generate Keys for MNR**.

A progress bar window appears. When the operation completes, a results (**Device Command Parameters**) window appears. If the operation was successful on a device, the device displays in the Success list box. If the operation was not successful on a device, the device displays in the Failure list box.

9 Click each device in the **Device list** on the **Device Command Parameters** window.

The results for the selected device display in the **Results** text box. The operation was a success if `SSH key pair is SUCCESSFULLY generated` displays.

10 Verify that all the commands have been completed successfully for all the devices in the **Device list**.

11 Close the **Device Command Parameters** window.

Postrequisites:

NOTICE:
For additional verification, you can display the SSH public host key and fingerprint for a router or gateway, using the `ShowSshKey` command.

The command line for a router or gateway is available from the Cut-Through feature in VoyenceControl (right-click the router or gateway, then select **Cut-Through**, and then **In-band**).

4.23.7
Using a Saved Command in VoyenceControl to Generate SSH Keys on HP Switches

When and where to use:
The following procedure describes how to use a Saved Command in the VoyenceControl component of the Unified Network Configurator (UNC) tool to generate SSH keys on one or more HP switches in an ASTRO® 25 communication system.

NOTICE: For additional ways to use Saved Commands in VoyenceControl, see the *Unified Network Configurator* manual.

Procedure:

1. Log into VoyenceControl.

   The **VoyenceControl** main window appears.

2. In the navigation pane on the left side of the window, double-click **Astro 25 Radio Network**.

   The selected network tree expands to display the **Devices** node.

3. In the navigation pane on the left side of the window, double-click **Devices** for the Devices View, or double-click **Views** for other views.

   NOTICE: The **Devices View** displays a list of all the supported network devices and their associated properties.
   If you select **Views**, you can open a view with one category of device, such as Motorola Network Resources (MNR), which includes Motorola routers and gateways.

   Alternatively, if you are configuring a single site at a time, you can select the Zone name and then the Site name in the navigation pane on the left side of the window. You can sort the Site view on the right side of the window by Device Class. This arranges the list so that all of the devices of the same type at the site are listed together.

4. Right-click the desired device(s) in the pane on the right side of the screen.

   The context menu appears.

5. From the context menu, select **Saved Command**.

   The **Select Item** dialog box appears.

6. Click the folder icon at the top of the dialog box, to the right of the **Look in** field. Continue to click this icon until the **System** folder displays in the list of folders on the Select Item dialog box.
7. In the list of folders on the Select Item dialog box, double-click the **System** folder, then double-click the **Motorola** folder, and then double-click the **HP** folder.

   A list of saved commands displays in the **Select Item** dialog box.

8. Double-click the saved command named **Generate Key Pair in HP Switch**.

   A progress bar window appears. When the operation completes, a results (**Device Command Parameters**) window appears. If the operation was successful on a device, the device displays in the Success list box. If the operation was not successful on a device, the device displays in the Failure list box.

9. Click each switch in the **Device list** on the **Device Command Parameters** window.

   The results for a selected switch display in the **Results** text box. The operation was a success if `SSH key pair is SUCCESSFULLY generated` displays.

10. Verify that all the commands have been completed successfully for all the switches in the **Device list**.
11. Close the **Device Command Parameters** window.

4.23.8

Using a Saved Command in VoyenceControl to Generate SSH Keys on Console Telephony Media Gateway

When and where to use:
The following procedure describes how to use a Saved Command in the VoyenceControl component of the Unified Network Configurator (UNC) tool to generate SSH keys on one or more Console telephony media gateways in an ASTRO® 25 communication system.

NOTICE: For additional ways to use Saved Commands in VoyenceControl, see the *Unified Network Configurator* manual.
Perform Deleting SSH Keys from the UNC Server Known Hosts List Using the Administration Menu on page 179 to delete the existing SSH host key for a device from the Unified Network Configurator (UNC) known hosts list.

Procedure:

1. Log into VoyenceControl.

   The **VoyenceControl** main window appears.

2. In the navigation pane on the left side of the window, double-click **Astro 25 Radio Network**.

   The selected network tree expands to display the **Devices** node.

3. In the navigation pane on the left side of the window, double-click **Devices** for the Devices View, or double-click **Views** for other views.

   NOTICE:
   The Devices View displays a list of all the supported network devices and their associated properties.

   If you select **Views**, you can open a view with one category of device, such as Motorola Network Resources (MNR), which includes Motorola routers and gateways.

   Alternatively, if you are configuring a single site at a time, you can select the Zone name and then the Site name in the navigation pane on the left side of the window. You can sort the Site view on the right side of the window by Device Class. This arranges the list so that all of the devices of the same type at the site are listed together.

4. Right-click the desired device(s) in the pane on the right side of the screen.

   The context menu appears.

5. From the context menu, select **Saved Command**.

   The **Select Item** dialog box appears.

6. Click the folder icon at the top of the dialog box, to the right of the **Look in** field. Continue to click this icon until the **System** folder displays in the list of folders on the Select Item dialog box.
7. In the list of folders on the Select Item dialog box, double-click the **System** folder, then double-click the **Motorola** folder, and then double-click the **Cisco** folder.

   A list of saved commands displays in the **Select Item** dialog box.

8. Double-click the saved command named **Generate Cisco SSH Key**.

   A progress bar window appears. When the operation completes, a results (**Device Command Parameters**) window appears. If the operation was successful on a device, the device displays in the Success list box. If the operation was not successful on a device, the device displays in the Failure list box.

9 Click each Console telephony media gateway in the **Device list** on the **Device Command Parameters** window.

The results for a selected device display in the **Results** text box. The `SSH key pair is SUCCESSFULLY generated` message displays.

10 Verify that all the commands have been completed successfully for all the Console telephony media gateways in the **Device list**.

11 Close the **Device Command Parameters** window.

12 For each Console telephony media gateway, right-click the gateway in the main **VoyenceControl** window, and select **Pull**, then **Pull Config** from the pop-up menu.

The VoyenceControl is updated with the Console telephony media gateway configuration changes. The new SSH keys are added to the known hosts list on the UNC server.

Related Links

Configuring SSH for Devices at a Dispatch Site on page 53
Configuring SSH for Console Telephony Media Gateway on page 59

4.23.9

Using a Saved Command in VoyenceControl to Generate SSH Keys on MCC7500 Aux I/O Server

When and where to use:
The following procedure describes how to use a Saved Command in the VoyenceControl component of the Unified Network Configurator (UNC) tool to generate SSH keys on one or more MCC7500 Aux I/O Servers in an ASTRO® 25 communication system.

NOTICE:
For additional ways to use Saved Commands in VoyenceControl, see the *Unified Network Configurator* manual.

Perform Deleting SSH Keys from the UNC Server Known Hosts List Using the Administration Menu on page 179 to delete the existing SSH host key for a device from the Unified Network Configurator (UNC) known hosts list.

Procedure:

1 Log into VoyenceControl.

The **VoyenceControl** main window appears.

2 In the navigation pane on the left side of the window, double-click **Astro 25 Radio Network**.

The selected network tree expands to display the **Devices** node.

3 In the navigation pane on the left side of the window, double-click **Devices** for the Devices View, or double-click **Views** for other views.

NOTICE: The Devices View displays a list of all the supported network devices and their associated properties.
If you select **Views**, you can open a view with one category of device, such as Motorola Network Resources (MNR), which includes Motorola routers and gateways.

Alternatively, if you are configuring a single site at a time, you can select the Zone name and then the Site name in the navigation pane on the left side of the window. You can sort the Site view on the right side of the window by Device Class. This arranges the list so that all of the devices of the same type at the site are listed together.

4 Right-click the desired device(s) in the pane on the right side of the screen.

The context menu appears.

5 From the context menu, select **Saved Command**.

The **Select Item** dialog box appears.

6 Click the folder icon at the top of the dialog box, to the right of the **Look in** field. Continue to click this icon until the **System** folder displays in the list of folders on the Select Item dialog box.

7 In the list of folders on the Select Item dialog box, double-click the **System** → **Motorola** → **AuxIO** folders.

A list of saved commands displays in the **Select Item** dialog box.

8 Double-click the saved command named **Generate_SSH_Key_Pair**.

A progress bar window appears. When the operation completes, a results (**Device Command Parameters**) window appears. If the operation was successful on a device, the device displays in the Success list box. If the operation was not successful on a device, the device displays in the Failure list box.

9 Click each MCC7500 Aux I/O Server in the **Device list** on the **Device Command Parameters** window.

The results for a selected device display in the **Results** text box. The `SSH key pair is SUCCESSFULLY generated` message displays.

10 Verify that all the commands have been completed successfully for all the MCC7500 Aux I/O Servers in the **Device list**.

11 Close the **Device Command Parameters** window.

12 Right-click each MCC7500 Aux I/O Server in the main **VoyenceControl** window, and select **Pull**, then **Pull Config** from the pop-up menu.

The VoyenceControl is updated with the MCC7500 Aux I/O Server configuration changes. The new SSH keys are added to the known hosts list on the UNC server.

Postrequisites: Perform Deleting SSH Keys from the UNC Server Known Hosts List Using the Administration Menu on page 179.

Related Links

Configuring SSH for MCC7500 Aux I/O Server on page 60

4.23.10
Accessing the Configlet Editor

When and where to use:
The following procedure describes how to access the Configlet Editor in the VoyenceControl component of the Unified Network Configurator (UNC) tool.

NOTICE: For additional ways to use the Configlet Editor, see the *Unified Network Configurator* manual.

Procedure:

1. Log into VoyenceControl.

   The **VoyenceControl** main window appears.

2. In the navigation pane on the left side of the window, double-click **Astro 25 Radio Network**.

   The selected network tree expands to display the Devices node.

3. In the navigation pane on the left side of the window, double-click **Devices**.

   The **Devices View** appears. The list of devices and associated properties are displayed in the pane on the right side of the screen.

4. Right-click the desired device in the Devices View pane on the right side of the screen or in the navigation pane.

   The context menu appears.

5. Select **Properties**, then select the **Communications** tab.
6. If needed use the **Update Credentials** button to perform the following actions:
   a. Make sure that the Management Mechanism (protocol) is not SSH.
   b. Make sure that the Management Account field is appropriately configured.

      For example, if RADIUS authentication is currently enabled on the device, make sure that the VoyenceControl Management Account credential for this device matches the username and password for this device on the RADIUS server. For information on adding and modifying VoyenceControl credentials, see "EMC Smarts Network Configuration Manager Credential Modification" in the *Unified Network Configurator* manual.
7. Return to the Devices view and right-click the device again.

   A context menu appears.

8. From the context menu, select **Editor**, and then **Configlet**.

   The **Configlet Editor** window appears.

4.23.11
Using a Pre-Tested Template to Populate a Configlet

When and where to use:
The following procedure describes how to use a template to populate a Configlet in the VoyenceControl component of the Unified Network Configurator (UNC) tool.

For additional ways to use templates, see the *Unified Network Configurator* manual.

Procedure:

1. Access the **Configlet Editor** window in VoyenceControl.
2. Click inside the text box at the top of the **Configlet Editor** window.

   The Insert Template icon becomes active in the tool bar of the **Configlet Editor** window.

3. In the tool bar of the **Configlet Editor** window, click the **Insert Template** icon.

   The **Select Item** dialog box appears.

4 Click the folder icon at the top of the dialog box, to the right of the **Look in** field. Continue to click this icon until the **System** folder displays in the list of folders on the **Select Item** dialog box.

5 In the list of folders on the Select Item dialog box, double-click the **System** folder, then double-click the **Motorola** folder.

6 Double-click the subfolder that contains the template you need.

A list of templates displays on the **Select Item** dialog box.

7 Double-click the template you need from the list.

One of the following events occurs:

- If you are not required to input values, you are returned to the **Configlet Editor** window and the configuration lines generated by the template are displayed.
- If the template requires you to input values for variable(s), the **Template Variable Substitution** window displays a field for entering each value.

8 Perform one of the following:

If…	Then…
If you are returned to the Configlet Editor window,	go to the next step.
If the Template Variable Substitution window displays a field for entering each value,	perform the following actions: **a** Enter a value in each field on this window. **b** Click **OK**. You are returned to the **Configlet Editor** window and the configuration lines generated by the template are displayed.

9 To use an additional template, perform the following actions:

a Click at the end of the configuration lines generated by the first template.

b Press ENTER.

A line is added to the Configlet Editor for the next template.

c Repeat step 3 to step 8.

10 Go to Scheduling the Job on page 174.

4.23.12

Scheduling the Job

When and where to use:
After using the Configlet Editor window for a selected device in the VoyenceControl component of the Unified Network Configurator (UNC) tool, perform to push the contents of the **Editor** window to the device.

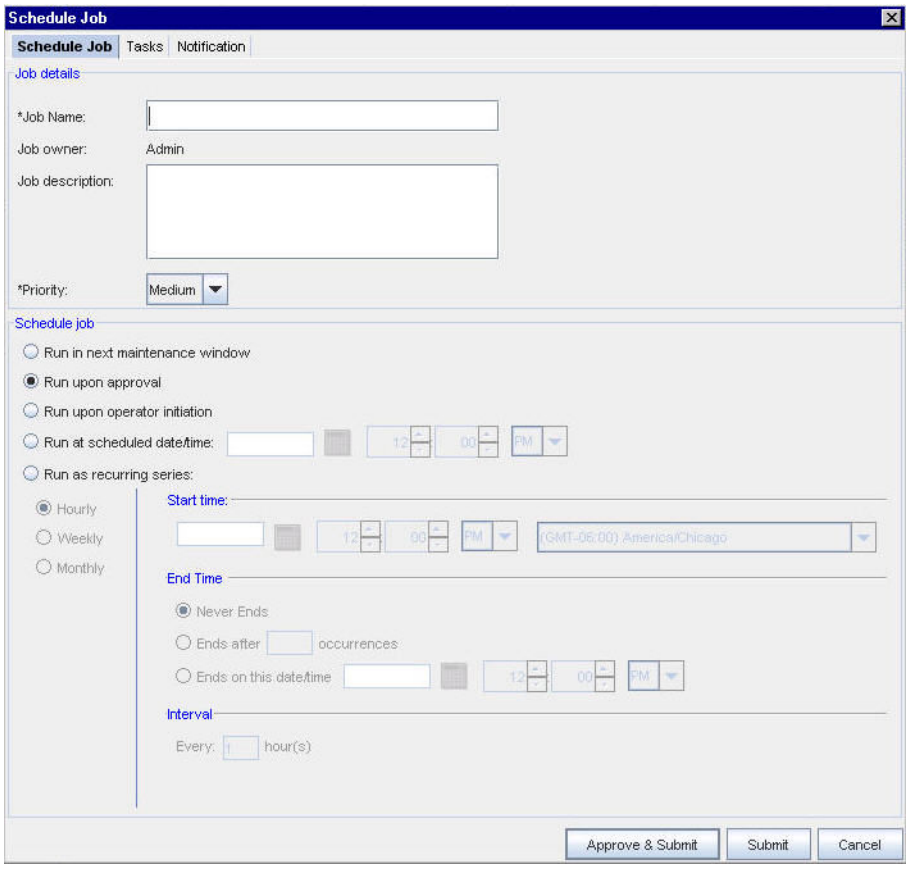
NOTICE: For additional ways to use the **Schedule Job** window, see the *Unified Network Configurator* manual.

Procedure:

1 Click the **Schedule** button at the bottom of the **Editor** window.

The **Schedule Job** window appears.

Figure 5: VoyenceControl Schedule Job Window



2 On the **Schedule Job** tab, enter a **Job Name**.

3 On the **Tasks** tab:

a In order for a Motorola router or gateway configuration change to persist after a reboot, select the **running-config** for **Destination** and **Copy To Start** for **Post Operation** on the **Tasks** tab of the **Schedule Job** window.

b For other devices, use the defaults for **Destination** and **Post Operation** on the **Tasks** tab.

c When scheduling a job that enables/disables secure mode or enables/disables clear mode, select **Do not Pull** for the **Pull After Push** parameter (perform the Pull later, after VoyenceControl is set up to communicate with the device in the mode that matches the new configuration on the device).

4 Click **Approve Submit**.

NOTICE: If you selected the **Run upon approval** option and then clicked the **Approve Submit** button on the **Schedule Job** window, the job begins immediately. The operation may take a few minutes, before successful completion is reported on the **Schedule Manager** window.

The **Schedule Job** window closes. The job status can be viewed using Schedule Manager.

5 Close the **Editor** window.

4.23.13

Viewing Job Status in the Schedule Manager

When and where to use:
After scheduling a job, perform the following procedure to use the VoyenceControl component of the Unified Network Configurator (UNC) tool to view the status of a scheduled job.

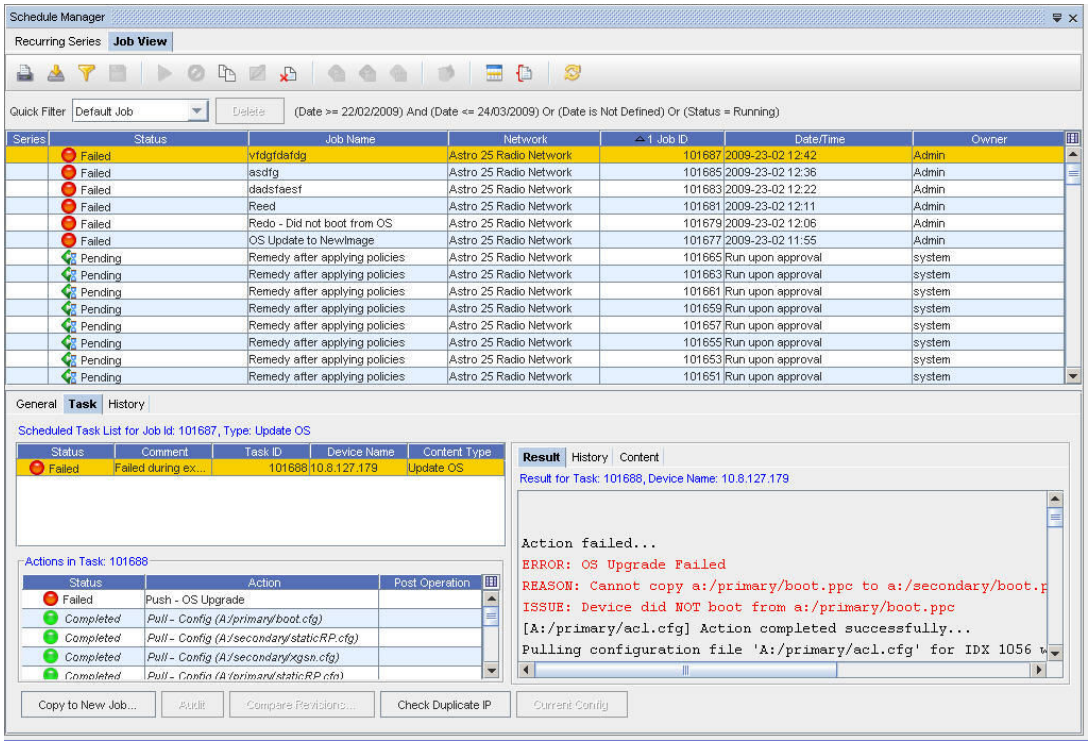
NOTICE: For additional ways to use Schedule Manager, see the *Unified Network Configurator* manual.

Procedure:

1. Go to the **Tools** menu.
2. Select **Schedule Manager**.

   The **Schedule Manager** window appears.

   Figure 6: Schedule Manager Window – Example



4.23.14

Enabling SSH/SCP Management Mechanism in Device Properties in VoyenceControl

When and where to use:

The following procedure describes how to use the VoyenceControl component of the Unified Network Configurator (UNC) tool to enable secure mode management mechanisms for devices in an ASTRO® 25 communication system.

Procedure:

1 Right-click the devices in the **Devices View** pane on the right side of the screen or in the navigation pane.

The context menu appears.

2 Select **Edit Device** then select **Update Credentials** from the context menu.

A window displays an In-Band tab and an Out-of-Band tab.

3 In the **In-Band** tab, select the following parameters:

a **SSH/SCP** as the Management Mechanism

b **SSH** as the Cut-Through Mechanism

4 Click **Save Only**.

The **Update Credential Setting** window closes.

5 Verify that the device is set up for **SSH/SCP** for the management account mechanism:

a Select the device and click the **Properties** button on the tool bar.

b Click the **Communication** tab and verify that the management mechanism is set to **SSH/SCP**.

Related Links

Configuring SSH for Devices at the Zone Core on page 47
Configuring SSH for Transport Network Devices on page 58

4.23.15

Verifying Secure Mode/Updating Known Hosts List for UNC Management of a Device

Prerequisites:

IMPORTANT: If a key for this device already exists in the known hosts list for the UNC, because initial key rotation has already been completed, then on a subsequent key rotation for this device, perform Deleting SSH Keys from the UNC Server Known Hosts List Using the Administration Menu on page 179.

When and where to use:
The following procedure describes how to use the VoyenceControl component of the Unified Network Configurator (UNC) tool to verify that the management mechanism is in secure mode for a device or devices in an ASTRO® 25 communication system.

This procedure also adds the SSH server (host) key for the device to the known hosts list for the UNC and UNCDS, if no key exists in the list for that device.

Procedure:

1 Right-click the device or devices in the **Devices View** pane on the right side of the screen or in the navigation pane.

The context menu appears.

2 Select **Quick Command** then select **Test Credentials** from the context menu.

A progress bar window appears. When the operation completes, a **Device Command Parameters** window displays results. If the operation was successful on a device, the device displays in the Success list box. If the operation was not successful on a device, the device displays in the Failure list box.

3 Click each device in the **Device list** on the **Device Command Parameters** window.

The results for a selected device will display in the **Results** text box.

4 Verify that the details indicate *SSH* and *SCP* were successfully tested.

5 Close the **Device Command Parameters** window.

Related Links

Configuring SSH for Devices at the Zone Core on page 47
Configuring SSH for Transport Network Devices on page 58
Configuring SSH for Console Telephony Media Gateway on page 59

4.23.16

Using Cut-Through to Generate an SSH Host Key on an HP Switch

When and where to use:
For key rotation purposes, perform the following procedure to generate a new SSH host key pair on an HP switch, using the Cut-Through feature in the VoyenceControl component of the Unified Network Configurator (UNC) tool.

This procedure differs from using the Motorola Solutions template (scheduled job) for generating a key pair on an HP switch, because it does not perform a configuration pull. For a system operating in secure mode, if a configuration pull occurs and a new SSH host key on the device does not match the existing host key for that device in the UNC server and UNCDS known hosts list, a pull failure occurs. The known hosts list cannot be cleared before pushing a scheduled job for key regeneration, because that would prevent a secure connection to the switch for the push.

This procedure can be used to prevent a pull failure. However, only one switch can be configured at a time using this procedure.

Procedure:

1 Right-click the device.

A context menu displays.

2 Select **Cut-Through**, then select **In-band** from the context menu.

A command-line session window appears.

3 Click inside the command-line session window. Press ENTER.

The switch command-line prompt appears and you are logged in.

4 Enter: `config`

5 Enter: `CRYPTO key generate ssh`

6 Enter: `exit` until the command window closes.

Postrequisites: Continue to Deleting SSH Keys from the UNC Server Known Hosts List Using the Administration Menu on page 179.

4.23.17

Deleting SSH Keys from the UNC Server Known Hosts List Using the Administration Menu

Perform this procedure only for devices such as switches and routers that are managed in the VoyenceControl component of the Unified Network Configurator (UNC) tool. You do not need to perform this procedure during initial SSH configuration for these devices, because there are no default host keys for these devices in the UNC servers and Unified Network Configurator Device Servers (UNCDS) known hosts list.

When and where to use:
For key rotation purposes, perform the following procedure to delete the existing SSH host key for a device from the Unified Network Configurator (UNC) known hosts list. This procedure must be performed before a new host key can be accepted into the list for that device.

Procedure:

1. Log on to the UNC server at its IP address, using your Active Directory account.

   See Use of a Domain Account to Log on to Devices Using Default Keys on page 93.
2. At the UNC server command prompt, enter: `admin_menu`
3. At the **UNC server administration** menu, enter the number for the option **OS Administration**.
4. At the **OS Administration** menu, enter the number for the option **Security Provisioning**.
5. At the **Security Provisioning** menu, enter the number for the option **Delete Devices Public SSH Key**.
6. At the prompt, enter the IP address of the device to delete from the UNC servers known hosts list.

   The public SSH key for the device you entered is deleted from the UNC servers known hosts list.
7. Right-click the device in the VoyenceControl component of the UNC, select **Quick Commands** and then **Test Credentials** to establish an SSH connection that automatically adds the devices SSH host key to the UNC servers known hosts list.

   Before using Test Credentials, ensure that SSH/SCP are selected as the protocols UNC will use for communication with that device. See Enabling SSH/SCP Management Mechanism in Device Properties in VoyenceControl on page 176.

Related Links

Configuring SSH for Console Telephony Media Gateway on page 59

4.23.18

Enabling Clear Mode for Routers, Gateways, and HP Switches Using VoyenceControl

When and where to use:
Perform the following process to use the VoyenceControl component of the Unified Network Configurator (UNC) tool to enable clear mode for HP switches, and Motorola routers and gateways, in an ASTRO® 25 communication system. Use the Motorola Solutions templates indicated in the steps of the process table.

Process:

1. Perform Logging into VoyenceControl on page 167.

2 Enable clear mode on routers and gateways, using the template **Enable SSH and Telnet in MNR** located in the `MNR` template folder. See:

   a Accessing the Configlet Editor on page 172.

   b Using a Pre-Tested Template to Populate a Configlet on page 173.

   c Scheduling the Job on page 174.

   d Viewing Job Status in the Schedule Manager on page 176.

3 Enable clear mode on switches, using the template **Enable Telnet in HP Switch** located in the `HP` template folder. See:

   a Accessing the Configlet Editor on page 172.

   b Using a Pre-Tested Template to Populate a Configlet on page 173.

   c Scheduling the Job on page 174.

   d Viewing Job Status in the Schedule Manager on page 176.

4 To perform clear mode communications between the UNC and the device, perform the following actions:

   a Enable clear mode in the UNC management mechanisms for that device.

   See: Enabling Clear Mode for UNC Management of a Device on page 180.

   b Enable clear mode on the UNC server, using the UNC server administration menu options. Use the **FTP Services** menu under the **Application Administration** menu.

   For more information on administration menus, see the *Private Network Management Servers* manual.

5 Right-click the device in the main **VoyenceControl** window, and select **Pull**, then **Pull Config** from the popup menus.

   This updates VoyenceControl with the configuration changes.

4.23.19
Enabling Clear Mode for UNC Management of a Device

Prerequisites:

IMPORTANT: To perform clear mode communications between the UNC and a device, the User Configuration Server (UCS) must also be in clear mode. To enable clear mode on the UNC server, use the UNC server administration menu options: the **FTP Services** menu under the **Application Administration** menu.
For more information on administration menus, see the *Private Network Management Servers* manual.

When and where to use:
The following procedure describes how to use the VoyenceControl component of the Unified Network Configurator (UNC) tool to enable clear mode management mechanisms for devices in an ASTRO® 25 communication system.

Procedure:

1 Right-click the device in the Devices View pane on the right side of the screen.

   The context menu appears.

2 Select **Edit Device** then select **Update Credentials** from the context menu.

   The **Update Credentials Device Selection** window appears.

3 Click **Next**.

The **Update Credential Setting** window appears.

4 Select the following parameters:

a **Telnet/TFTP** as the Management Mechanism

b **Telnet** as the Cut-Through Mechanism

5 Click **Save Only**.

The **Update Credential Setting** window closes.

6 Verify that the device is set up for **Telnet/TFTP** for the management account mechanism:

a Select the device and click the **Properties** button on the tool bar.

b Click the **Communication** tab and verify that the management mechanism is set to **Telnet/TFTP**.

7 Right-click on the device again (the same device that you selected in step 1).

NOTICE: If you are performing this procedure for more than one device, you can perform the remaining steps of this procedure on multiple devices at once, by selecting them all before right-clicking.

A context menu appears.

8 Select **Quick Command→Test Credentials** from the context menu.

A progress bar window appears. When the operation completes, a results (**Device Command Parameters**) window appears. If the operation was successful on a device, the device displays in the Success list box. If the operation was not successful on a device, the device displays in the Failure list box.

9 Verify that the details indicate *Telnet* and *TFTP* were being tested.

10 Close the **Device Command Parameters** window.

4.23.20

Disabling Telnet on Routers, Gateways, and HP Switches Using VoyenceControl

When and where to use:
Perform the following process to use the VoyenceControl component of the Unified Network Configurator (UNC) tool to disable telnet on HP switches, and Motorola routers and gateways.

Process:

1 Disable Clear mode on the routers and gateways, using the template **Disable Telnet in MNR** located in the `MNR` template folder. See:

a Accessing the Configlet Editor on page 172

b Using a Pre-Tested Template to Populate a Configlet on page 173

c Scheduling the Job on page 174

d Viewing Job Status in the Schedule Manager on page 176

2 Disable Clear mode on the switches, using the template **Disable Telnet in HP Switch** located in the `HP` template folder. See:

a Accessing the Configlet Editor on page 172

b Using a Pre-Tested Template to Populate a Configlet on page 173

c Scheduling the Job on page 174

d Viewing Job Status in the Schedule Manager on page 176

3 Right-click the device in the main **VoyenceControl** window, and select **Pull**, then **Pull Config** from the popup menus.

NOTICE: Before performing the pull, make sure that SSH/SCP is selected as the Management Mechanism (protocol) for this device, in its Communication Properties in VoyenceControl,

This pull updates VoyenceControl with the configuration changes.

4.23.21

Disabling Secure Mode on Routers, Gateways, and HP Switches Using VoyenceControl

When and where to use:
Perform the following process to use the VoyenceControl component of the Unified Network Configurator (UNC) tool to disable secure mode on HP switches , and Motorola routers and gateways.

Process:

1 Disable Secure mode on the routers and gateways, using the template **Disable SSH in MNR** in the `MNR` template folder.

See:

- Accessing the Configlet Editor on page 172
- Using a Pre-Tested Template to Populate a Configlet on page 173
- Scheduling the Job on page 174
- Viewing Job Status in the Schedule Manager on page 176

2 Disable Secure mode on the switches, using the template **Disable SSH in HP Switch** located in the `HP` folder.

See:

- Accessing the Configlet Editor on page 172
- Using a Pre-Tested Template to Populate a Configlet on page 173
- Scheduling the Job on page 174
- Viewing Job Status in the Schedule Manager on page 176

3 In order to perform clear mode communications between the UNC and the device, perform the following actions:

a Enable clear mode in the UNC management mechanisms for that device.

See Enabling Clear Mode for UNC Management of a Device on page 180.

b Enable clear mode on the UNC server, using the UNC server administration menu options. Use the **FTP Services** menu under the **Application Administration** menu.

For more information on administration menus, see the *Private Network Management Servers* manual.

4 Right-click the device in the main **VoyenceControl** window, and select **Pull**, then **Pull Config** from the popup menus.

NOTICE: Before performing the pull, make sure that Telnet is selected as the Management Mechanism (protocol) for this device, in its Communication Properties in VoyenceControl,

This pull updates VoyenceControl with the configuration changes.

4.24 SSH Configuration on HP Switches Using Commands

This section covers configuring SSH on HP switches using operating system commands.

NOTICE: In an ASTRO® 25 communication system, HP switches are only configured as SSH hosts for the purpose of interactive SSH sessions.
When you use an SSH client application, such as PuTTY, to initiate an SSH session with a switch, it will prompt you to verify the SSH host if the latest SSH key for that host is not included in the SSH clients known hosts list. See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89 (and the commands in Table 19: HP Switch Commands for Configuring SSH on page 183 for displaying SSH key fingerprints).

You can install PuTTY from the ASTRO® 25 system *Windows Supplemental* media. For instructions, see Installing Motorola Solutions PuTTY on Windows-Based Devices on page 40.

Table 19: HP Switch Commands for Configuring SSH

Task You Are Performing	Commands to Enter
Generating SSH server keys	`crypto key generate ssh`

Enabling secure mode	`ip ssh`
	`ip ssh timeout 60`
	`ip ssh filetransfer`
	NOTICE: When secure mode is enabled on an HP switch , file transfer is only supported through scp regardless of the clear protocol setting.

Enabling clear mode	`telnet-server` **NOTICE:** This command does not change whether ssh is enabled or disabled on the switch.
Disabling clear mode	`no telnet-server` **NOTICE:** This command does not change whether ssh is enabled or disabled on the switch.

Enabling clear mode and disabling secure mode	`telnet-server`
	`no ip ssh filetransfer`
	`no ip ssh`
	`tftp server`
	`tftp client`
	`ip ssh timeout 60`

Task You Are Performing	Commands to Enter
	NOTICE: The tftp commands included in this row automatically disable sftp. However, for enabling telnet and disabling ssh, separate commands are required.
Displaying SSH public host key and fingerprint for this device	`sh crypto host-public-key fingerprint`

Related Links

Configuring SSH for Devices at the Zone Core on page 47
Configuring SSH for Devices at an RF Site on page 50
Configuring SSH for Devices at a Dispatch Site on page 53

4.24.1
Entering SSH Configuration Commands on an HP Switch

When and where to use:
Perform the following procedure to enter the commands from Table 19: HP Switch Commands for Configuring SSH on page 183 on an HP switch.

Procedure:

1. Connect the PC or terminal to the switch console port using the console cable that came with the switch.

   NOTICE: If the PC or the terminal has a 25-pin serial connector, first attach a 9-pin to 25-pin straight-through adapter to the PC end of the console cable.

2. Turn on the PC or terminals power. If using a PC, start the PC terminal emulator program.
3. Press ENTER two or three times until you see the copyright page and the message:

   ```
   Press any key to continue
   ```

4. Press any key.

   The switch console command-line interface (CLI) appears.

5. If you are prompted for a password, type the Manager password and press ENTER.

   NOTICE: Entering the Manager password provides you with manager-level access to the switch. Entering the Operator password provides you with operator-level access to the switch. If you are not prompted for a password, it means that it has not been configured.

   The command-line interface prompt appears.

6. At the command line, type `config` and press ENTER.

   The switch enters the configuration mode.

7. Enter a configuration command or commands.
8. Enter the following command to save the configuration change so that it will persist through a reboot: `write memory`

9 At the command line, type `exit` to exit the switch configuration mode.

4.25 SSH Configuration on Routers and Gateways Using Commands

This section covers configuring SSH on Motorola routers and gateways using Enterprise Operating System (EOS) commands.

NOTICE: In an ASTRO® 25 communication system, Motorola routers and gateways are configured as SSH servers (hosts) only for the purpose of interactive SSH sessions.

When you use an SSH client application, such as PuTTY, to initiate an SSH session with a Motorola router or gateway, it will prompt you to verify the SSH host if the latest SSH key for that host is not included in the SSH clients known hosts list. See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89 and the command in Table 20: EOS Commands for Configuring SSH on Routers and Gateways on page 185 for displaying SSH key fingerprints.

You can install PuTTY from the ASTRO® 25 system *Windows Supplemental* media. For instructions, see Installing Motorola Solutions PuTTY on Windows-Based Devices on page 40.

Table 20: EOS Commands for Configuring SSH on Routers and Gateways

Task You Are Performing	Commands to Enter
Generating SSH server keys	For GGM 8000 gateways, MNR S2500 routers, and MNR S6000 routers: • `GenSshKey RSA 2048` • `GenSshKey DSA 1024`
Displaying SSH host public key and fingerprint for this device	`ShowSshKey`
Enabling clear mode and secure mode	`SETDefault -SYS NetAccess = (Telnet, NoWebLink, Ssh)`
Disabling clear mode and enabling secure mode	`SETDefault -SYS NetAccess = (NoTelnet, NoWebLink, Ssh)`
Enabling clear mode and disabling secure mode	`SETDefault -SYS NetAccess = (Telnet, NoWebLink, NoSsh)`
Allow SSH or Telnet access by	`DEL -SYS SSHManager *.*.*.*` `ADD -SYS SSHManager <IP address>`

Task You Are Performing	Commands to Enter
only one IP address	**NOTICE:** Network Manager privileges are required to enter SSHManager commands. You can configure a maximum of 64 addresses using either the SSHManager or TelnetManager commands.

It is recommended that you use the following command on a router or gateway before sending it for repair: `ZEROize`

The `ZEROize` command zeroizes all critical security parameters (CSPs) on the router or gateway, including the PSK and IPSec and SSH CSPs, which are not zeroized by the KEKZeroize command. CSPs include keys, secrets, and passwords.

IMPORTANT: Exercise extreme caution when using the `ZEROize` command as it destroys all keys and secrets on the router or gateway, causing all links that depend on those keys to go down. The `ZEROize` command is intended for use in maintenance situations or when a security breach has occurred, not during normal operation.

Related Links

Configuring SSH for Devices at the Zone Core on page 47
Configuring SSH for Devices at an RF Site on page 50
Configuring SSH for Devices at a Dispatch Site on page 53

4.25.1

Entering SSH Configuration Commands on a Router or Gateway

When and where to use:
Perform the following procedure to enter the commands from Table 19: HP Switch Commands for Configuring SSH on page 183 on a Motorola router or gateway.

Procedure:

1. Assign the following IP address and subnet mask to the LAN card on the PC used to perform the configuration:
   a. IP Address: `20.0.0.1`
   b. Subnet Mask: `255.255.255.0 2`
2. Connect a null modem cable between the serial port on the workstation PC and the console port on the router or gateway.
3. Power up the router or gateway, and connect to it using a terminal emulation program, such as ProComm+ or HyperTerminal. In the terminal emulation program, enter the following settings:
   a. 9600 baud rate
   b. 8 bit
   c. No parity
   d. 1 stop bit
4. Press ENTER several times until you see the `NetLogin:` prompt.
5. At the NetLogin prompt, enter: `root`
6. If you are prompted for a password, type it in. Press ENTER.

```
Enterprise OS#
```

The command-line interface prompt appears:

7 Enter a configuration command or commands.

8 Enter the following command: `exit`

4.26 Configuring SSH on TRAK Devices Using EOS Commands

Perform this procedure to configure Secure Shell (SSH) on the following TRAK devices using Enterprise Operating System (EOS) commands:

- 9100
- 8835-2M
- 8835-3M

When and where to use:

NOTICE:
In an ASTRO® 25 communication system, TRAK devices are configured as SSH servers (hosts) only for the purpose of interactive SSH sessions.

When you use an SSH client application, such as PuTTY, to initiate an SSH session with a TRAK device, it will prompt you to verify the SSH host if the latest SSH key for that host is not included in the SSH clients known hosts list. See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89 and the following table for SSH key fingerprints.

You can install PuTTY from the ASTRO® 25 system *Windows Supplemental* media. For instructions, see Installing Motorola Solutions PuTTY on Windows-Based Devices on page 40.

Procedure:

1 Connect a laptop to the TRAK device using a serial connection and Ethernet connection.

2 Power up the TRAK device and connect to it using a terminal emulation program, such as ProComm+ or HyperTerminal.

3 In the terminal emulation program, enter the baud rate: `8,1,N`

`9100>` or `8835>` prompt appears, depending on the device the PC connects to.

NOTICE: When logged into TRAK 9100, the `9100>` prompt appears. When logged into TRAK 8835-2M or 8835-3M, the `8835>` prompt appears.

4 Configure SSH by performing the following actions:

a Enable SSH on TRAK 9100. Enter:`9100>SSH on`

b Enable SSH on TRAK 8835. Enter: `8835>SSH on`

c Generate SSH keys on TRAK 9100. Enter: `9100>SSHKEY GEN RSA 2048`

d Generate SSH keys on TRAK 8835. Enter: `8835>SSHKEY GEN RSA 2048`

NOTICE: SSH key generation takes some time to complete, depending on the key length. The `success` response displays from few minutes to up to 45 minutes. For details, see SSH Key Specifications on page 37.

e Verify if the SSH key is generated for RSA. Enter:

```
9100>SSHKEY

rsa private: 1675
```

```
rsa public: 394
dsa private: 0
dsa public: 0
2069/5700
```

4.27 SSH Configuration on VMware Appliances

This section covers generating SSH keys on the vCenter Appliance and Virtual Management Server.

4.27.1 Generating SSH Keys on a vCenter Appliance

Procedure:

1. Log into the vCenter Appliance VM via the ESXi console from the vSphere client as the root user.

   For instructions, see the "Operation" chapter of the ASTRO® 25 system *Virtual Management Server Software* manual.

   The user is prompted to enter the password for the root user.

2. Enter the root users password.

   The command-line prompt is displayed.

3. Enter:

   `ssh-keygen -N "" -C <FQDN> -b 2048 -t rsa -f /etc/ssh/ssh_host_rsa_key`

   where ***<FQDN>*** is the combined hostname.domainname (for example, z001vcs01.zone1) of the Virtual Center Appliance

   The user is prompted to overwrite the current key.

4. Enter: `y`

   The new RSA SSH host key is generated.

5. Enter: `ssh-keygen -N "" -C <FQDN> -b 1024 -t dsa -f /etc/ssh/ssh_host_dsa_key`

   where ***<FQDN>*** is the combined hostname.domainname (for example, `z001vcs01.zone1`) of the Virtual Center Appliance

6. Enter: `y`

7. Enter: `exit`

   The user is prompted to overwrite the current key. The new DSA SSH host key is generated. The PuTTY session is closed.

Related Links

Configuring SSH for Devices at the Zone Core on page 47

4.27.2
Generating SSH Keys on a Virtual Management Server (ESXi/ Hypervisor)

Procedure:

1. From an NM Client, use PuTTY to open an ssh connection to the Virtual Management Server (ESXi/Hypervisor) IP address as the root user.
2. At the prompt, enter the ***<root user password>***.
3. At the command prompt, enter:
   `/usr/lib/vmware/openssh/bin/ssh-keygen -N "" -C <FQDN> -b 2048 -t rsa -f /etc/ssh/ssh_host_rsa_key`

   where ***<FQDN>*** is the combined hostname.domainname (for example, z001vms01.zone1) of the Virtual Management Server

   The user is prompted to overwrite the current key.
4. Enter: `y`

   The new RSA SSH host key is generated.
5. Enter:
   `/usr/lib/vmware/openssh/bin/ssh-keygen -N "" -C <FQDN> -b 1024 -t dsa -f /etc/ssh/ssh_host_dsa_key`

   where ***<FQDN>*** is the combined hostname.domainname (for example, z001vms01.zone1) of the Virtual Management Server

   The user is prompted to overwrite the current key.
6. Enter: `y`

   The new DSA SSH host key is generated.
7. Enter: `exit`

   The PuTTY session is closed.

Related Links

Configuring SSH for Devices at the Zone Core on page 47

4.27.3
Updating Known Hosts List on an IP Packet Capture for Connections to a VMS

Perform this procedure to update known hosts list on an IP Packet Capture after regenerating Virtual Management Server (VMS) host keys.

Procedure:

1. Access the root command prompt on the IP Packet Capture located on the VMS where keys were regenerated.

   See Accessing the Root Command Prompt on Devices Using Default Keys on page 94.
2. To delete any existing entries for the VMS in the known hosts list for the root account, enter:
   - **On the IP Packet Capture:** `/opt/Motorola/ssh/bin/manage_known_hosts -u root -d z00<Z>vms0<Y>`

where:
<Z> is the zone number
<Y> is the number of the VMS with the new SSH host keys

- **On the IP Packet Capture in the Trunking Subsystem (Tsub):** `/opt/Motorola/ssh/bin/manage_known_hosts -u root -d z<ZZZ>tsub<PP>vms01`
  where:
  <ZZZ> is the 3-digit, zero-padded zone number. The possible values are 1-7
  <PP> is the 2-digit, zero-padded number of the prime site in which the IP Packet Capture virtual machine is located. The possible values are: 1-64

3 To establish a connection to the VMS, enter:

- **On the IP Packet Capture:** `ssh sshserv@z00<Z>vms0<Y>`
  <Z> is the zone number
  <Y> is the number of the VMS with the new SSH host keys
- **On the IP Packet Capture in the Trunking Subsystem (Tsub):** `ssh sshserv@z<ZZZ>tsub<PP>vms01`
  where:
  <ZZZ> is the 3-digit, zero-padded zone number. The possible values are 1-7
  <PP> is the 2-digit, zero-padded number of the prime site in which the IP Packet Capture virtual machine is located. The possible values are: 1-64

4 After verifying the VMS fingerprint, at the prompt, enter: `Yes`

The key for this DNS name is added to the IP Packet Capture known hosts list for the sshserv account. The VMS hostname displays, or a permission denied message displays.

5 Enter: `exit`

Related Links

Configuring SSH for Devices at the Zone Core on page 47

4.28
SSH Configuration on the LX Terminal Server

This section provides information about configuring SSH on an LX Terminal Server in an ASTRO® 25 communication system.

This information assumes that you are configuring SSH locally at the Terminal Server. The Unified Network Configurator (UNC) tool cannot be used to configure SSH keys on the Terminal Server in secure mode (UNC can communicate with the Terminal Server only in clear mode).

4.28.1
Commands for Enabling/Disabling Secure Mode on the Terminal Server

The following table lists the commands for enabling/disabling secure mode on the Terminal Server.

NOTICE: Disabling SSH on the Terminal Server disables both Maintenance Access to the Terminal Server, which requires SSH, and access to Terminal Server menus.

Table 21: Commands for Enabling/Disabling Secure Mode on the Terminal Server

To perform the following functions...	Type the following at the InReach>>" prompt...
Enable Secure Protocol	`config ssh v2`
Disable Secure Protocol	`config no ssh`
Disable Clear Protocol	`config no telnet client` `config no telnet server`
Re-enable Clear Protocol	`config telnet client enable` `config telnet server enable`

Related Links

Configuring SSH for Devices at the Zone Core on page 47
Configuring SSH for Devices at an RF Site on page 50

4.28.2
Terminal Server SSH Server (Host) Keys Management

You can manage the Terminal Servers SSH server keys by performing the following functions (for instructions, see the procedures in this section):

- Regenerating SSH Keys
- Backing Up SSH Keys
- Restoring SSH Keys
- Viewing SSH Key Fingerprint

Related Links

Configuring SSH for Devices at the Zone Core on page 47
Configuring SSH for Devices at an RF Site on page 50

4.28.2.1
Regenerating SSH Server Keys on the Terminal Server

When and where to use: The following procedure describes how to regenerate SSH keys on the Terminal Server.

Procedure:

1. Log in as user `InReach`.
2. Enter `enable` and, when a password prompt displays, enter the privileged mode password.

   Contact your system administrator for passwords.
3. Type the following at the `InReach>>` prompt to regenerate SSH Keys:
   a. To save a backup of the *ssh_known_hosts* file:

      `shell comm mv /config/ssh_known_hosts /config/ssh_known_hosts.orig`

   b. To regenerate the RSA key:

```
shell comm ssh-keygen -t rsa -f /config/ssh_host_rsa_key -N ""
```

c To regenerate the DSA key:

```
shell comm ssh-keygen -t dsa -f /config/ssh_host_dsa_key -N ""
```

where:

`-t` indicates the encryption attribute (rsa or dsa)

`-N` indicates the passphrase attribute (not required when the Terminal Server is the SSH server, so only the quotation marks are required)

NOTICE: The path should not be changed and should be entered exactly as specified. After entering the command, the message `Generating public/private key pair` may display for an extended period of time. In addition, a prompt may appear to overwrite the existing key. Select **yes** when prompted. Messages will be displayed once the keys have been successfully saved.

When the key fingerprint displays, be sure to record it for comparison when an SSH client needs to accept the Terminal Server into its known hosts list.

You can use the `-b` parameter if you want to specify key size. For example:

```
shell comm ssh-keygen -t dsa -b <keysize> -f /config/
ssh_host_dsa_key -N ""
```

4 To save the configuration on the Terminal Server, type the following command and press ENTER:
`save configuration flash`

The configuration is saved.

4.28.2.2
Backing Up SSH Server Keys on the Terminal Server

When and where to use:
The following procedure describes how to back up SSH keys on the Terminal Server. The Terminal Server does not support a secure means for backing up the SSH server keys. If your organizations policies prohibit backup in clear mode, then in the event that the server keys are lost, they must be regenerated.

Procedure:

1 Log in as user `InReach`.

2 Enter `enable` and, when a password prompt displays, enter the privileged mode password.

(Contact your system administrator for passwords.)

3 Type `shell` at the `InReach>>` prompt.

4 Change the directory to `config` by typing: `cd config`

5 Type `ls` to view the files.

The rsa1, rsa2, and dsa keys are stored in the following files:

- **ssh_host_rsa_key**: RSA version 2 key
- **ssh_host_rsa_key.pub**: RSA version 2 public key
- **ssh_host_dsa_key**: DSA version 2 key
- **ssh_host_dsa_key.pub**: DSA version 2 public key

6 Issue the following command to tftp the file to the technician PC from the Terminal Server:

```
tftp -p -r<key file name> -l /config/<key file name><tftp IP>
```

where ***<key file name>*** is the name of the key file to be saved and ***<tftp IP>*** is the IP of the technician PC

4.28.2.3
Restoring SSH Server Keys on the Terminal Server

When and where to use:
The following procedure describes how to restore SSH keys on the Terminal Server.

Procedure:

1. Log in as user `InReach`.
2. Enter `enable` and, when a password prompt displays, enter the privileged mode password.

   (Contact your system administrator for passwords.)
3. Type `shell` at the `InReach>>` prompt.
4. Change the directory to `config` by typing: `cd config`
5. Issue the following command to tftp the file from the technician PC to the Terminal Server:

   `tftp -g -r`***<key file name>*** `-l /config/`***<key file name><tftp IP>***

   where ***<key file name>*** is the name of the key file to be restored and ***<tftp IP>*** is the IP of the technician PC
6. To save the configuration on the Terminal Server, type the following command and press ENTER:

   `save configuration flash`

   The configuration is saved.

4.28.2.4
Viewing the SSH Server Key Fingerprint on the Terminal Server

When and where to use:

Perform the following procedure to view the SSH fingerprint on the Terminal Server.

NOTICE: This procedure provides an alternative way to view the key fingerprint for the Terminal Server, if it is needed for comparison when an SSH client needs to accept the Terminal Server into its known hosts list.

Procedure:

1. Open the **ssh_known_hosts** file and delete the entry for the Terminal Server IP. The entry is listed in the format Terminal Server IP, followed by the key.
2. Initiate an SSH connection to the Terminal Server from the Terminal Server by executing the following command:

   `ssh` ***<terminal server IP>*** `InReach`

   A message displays the SSH fingerprint for the Terminal Server and asks whether you want to accept this host.
3. Type: `Yes`

   The new key is saved in the**ssh_known_hosts** file.
4. Enter the InReach maintenance access password to log in.
5. Type `exit` to log out of the session.

4.28.3
Known Hosts List on the Terminal Server Management

If the Terminal Server is required to initiate an SSH session with a device in the ASTRO® 25 communication system that is configured as an SSH server, then use the following information to manage the Terminal Server as an SSH client.

When you initiate the first SSH session with an SSH server device, you add the device to the known hosts list on the Terminal Server by accepting it as a known host when the key fingerprint message displays.

The following procedures provide instructions for backing up and restoring the known hosts list in clear mode. The Terminal Server does not support a secure means for backing up the known hosts list. If your organizations policies prohibit backup in clear mode, then in the event that the known hosts list is lost, it must be regenerated by initiating sessions with the SSH servers that were in the list.

4.28.3.1
Backing Up the Known Hosts List on the Terminal Server

Procedure:

1. Type `shell` at the `InReach>>` prompt.
2. Type: `cd config`
3. Log in as user **InReach** in privileged mode.
4. Issue the following command to tftp the file to the technician PC from the Terminal Server:

   `tftp -p -r ssh_known_hosts -l /config/ssh_known_hosts` ***<tftp IP>***

   where ***<tftp IP>*** is the IP of the technician PC

   The file is saved with the name **ssh_known_hosts**.

4.28.3.2
Restoring the Known Hosts List on the Terminal Server

Procedure:

1. Type `shell` at the `InReach>>` prompt.
2. Type: `cd config`
3. Log in as user **InReach** in privileged mode.
4. Issue the following command to tftp the file from the Laptop to the Terminal Server:

   `tftp -g -r` ***<remote file name>***`-l /config/ssh_known_hosts`***<tftp IP>***

   where ***<tftp IP>*** is the IP of the technician PC and ***<remote file name>*** is the name of the file that is stored on the technician PC

   If the file name was not changed after backup, it will be **ssh_known_hosts**.

   NOTICE: To save the configuration on the Terminal Server, issue the following command: `save configuration flash`

4.29
SSH Configuration for MOSCAD Network Fault Management (NFM) Devices

The procedures for configuring SSH for Network Fault Management (NFM) devices are mainly performed in the SDM3000 Builder application which can reside on:

- The Graphical Master Computer (GMC) or other Windows Server-based device in an ASTRO® 25 system.
- A service technician's laptop.
- Network Management (NM) Client
- K core Client

The SDM3000 Builder and the SDM3000 hardware-based devices exchange keys to support interactive and non-interactive SSH sessions.

An SDM3000 hardware-based device (SDM3000 RTU or SDM3000 Network Translator) can function as an SSH server or SSH client as follows:

- **SDM3000 hardware-based device as a server:** An SDM3000 hardware-based device functions as an SSH server to any device or application (including SDM3000 Builder, GMC, and GWS, if present)
- **SDM3000 hardware-based device as a client:** Any device or application (including SDM3000 Builder) can function as a client to the SDM3000 hardware-based device

For details on SDM3000 Builder, see the *SDM3000 Builder Users Guide*.

For details on the SDM3000, see the *SDM3000 Owner's Manual*.

For details on the GMC and GWS, see the *GMC/GWS Operations Manual*.

4.29.1
SSH Configuration on SDM3000 Hardware-Based Devices

The procedures in this section describe how to configure SSH on SDM3000 hardware-based devices.

4.29.1.1
Generating and Provisioning a New Host Key for an SDM3000 Hardware-Based Device

SDM3000 Network Translator (SNT) devices are only supported in the GMC Mode of operation. If you are using a system with the Centralized UEM Mode implemented, you can only configure SDM3000 RTU devices through the SDM3000 Builder as SNT devices are not supported.

Prerequisites: Ensure you have the SDM3000 Builder Administrator account name and password. If required, log on using your Active Directory account that is a member of the group with authority to perform the operations in this procedure as indicated in the Roles and Operations tool on the domain controller (instructions for the tool are located in the *Authentication Services* manual).

IMPORTANT: For optimal security, the initial configuration of operational settings such as keys, should be performed using a connection to the SDM3000 at the Console Port. See the *SDM3000 Builder User Guide* for information about connecting to the SDM3000 at the Console Port.

When and where to use:
After a device joins the domain, its applications that have Roles Based Access Control in Active Directory will not be usable by the local Windows administrator for that device unless the administrator accesses the application by entering its executable path and filename at the Windows command line. The path and filename can be seen in the properties for the application desktop shortcut.

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

Procedure:

1 Open a project in the SDM3000 Builder application.

You can open any project. However, if you open the project that contains the site with an SDM3000 RTU you want to configure, and then open that site, the IP address for this site will automatically display on the **Select Target** window (see step 6 of this procedure).

2 From the **Tools** menu, select **Operational Settings**. Perform one of the following actions:

- For the GMC Mode of operation, select one of the following devices:
  - **SDM3000 RTU**
  - **SNT** (SDM3000 Network Translator)
- For the Centralized UEM Mode, select **SDM3000 RTU**.

3 Select **Generate Keys**.

4 Select the **SSH Server Host Key** option.

5 Click **Next**.

The **Select Target** window appears.

6 Select the SDM3000 hardware-based device(s) you want to configure in this operation:

- For an SDM3000 Network Translator (SNT), only if in the GMC Mode of operation, you can configure one of the following options:
  - **Current SNT**
  - **All SNTs**
  - **Select SNTs**
- For SDM3000 RTUs, you can configure one of the following options:
  - **Current Site**
  - **All Sites**
  - **Select Sites**

IMPORTANT: Do not use the **All SNTs** or **All Sites** options if you are configuring the backup core of a system with the Dynamic System Resilience feature. Select only the SNT or the SDM3000 RTU in the backup core you are configuring.
If you already configured the SDM3000 RTU for this backup core, as part of another zones primary core SSH configuration, or no SDM3000 RTU is present at this master site, then click the **Cancel** button and skip the rest of this procedure, or click the **Back** button to return to the **Select Operation** window where you can choose to configure a different device.

If you chose the **Select SNTs** or **Select Sites** option, then an additional window displays devices to select.

7 If prompted, select the check box for each device you want to configure. Click **Next**.

8 Click **Next**.

9 In the **Host Key Generation** window, select the following key generation parameters:

a Key Type

b Key Size

10 For the RSA key type, select **2048** from the **Size** drop-down list.

RSA is the default key type used to connect in secure mode.

11 Click **Next**.

12 In the **Install Summary** window, click **Install**.

If a login window appears, enter your credentials.

The **Installation Process** window appears. The SDM3000 hardware-based device generates an authentication key pair. The public key and its fingerprint are returned to the SDM3000 Builder for future authentication. The IP address of the SDM3000 hardware-based device and the public key fingerprint are recorded in the SDM3000 Builder as a known host.

13 Click **Next**.

14 In the **Installation Complete** window, click **Finish**.

Related Links

Configuring SSH for Devices at an RF Site on page 50
Configuring SSH for Devices at a Dispatch Site on page 53
Configuring SSH for MOSCAD Network Fault Management (NFM) Devices on page 56

4.29.1.2

Generating and Provisioning a New SFTP Client Public Key Authentication Key Pair for an SDM3000 Hardware-Based Device

SDM3000 Network Translator (SNT) devices are only supported in the GMC Mode of operation. If you are using a system with the Centralized UEM Mode implemented, you can only configure SDM3000 RTU devices through the SDM3000 Builder as SNT devices are not supported.

Prerequisites: Ensure you have the SDM3000 Builder Administrator account name and password. If required, log on using your Active Directory account that is a member of the group with authority to perform the operations in this procedure as indicated in the Roles and Operations tool on the domain controller (instructions for the tool are located in the *Authentication Services* manual).

IMPORTANT: For optimal security, the initial configuration of operational settings such as keys should be performed using a connection to the SDM3000 hardware-based device at the Console Port. See the *SDM3000 Builder User Guide* for information about connecting to the SDM3000 hardware-based device at the Console Port.

When and where to use:
After a device joins the domain, its applications that have Roles Based Access Control in Active Directory will not be usable by the local Windows administrator for that device unless the administrator accesses the application by entering its executable path and filename at the Windows command line. The path and filename can be seen in the properties for the application desktop shortcut.

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

Procedure:

1 Open a project in the SDM3000 Builder application.

You can open any project. However, if you open the project that contains the site with an SDM3000 RTU you want to configure, and then open that site, the IP address for this site will automatically display on the **Select Target** window (see step 6 of this procedure).

2 From the **Tools** menu, select **Operational Settings**. Perform one of the following actions:

- For the GMC Mode of operation, select one of the following devices:

- **SDM3000 RTU**
- **SNT** (SDM3000 Network Translator)

- For the Centralized UEM Mode, select **SDM3000 RTU**.

3 Select **Generate Keys**.

4 Select the **SFTP Client Public Key Authentication** option.

5 Click **Next**.

The **Select Target** window appears.

6 Select the SDM3000 hardware-based device(s) you want to configure in this operation:

- For an SDM3000 Network Translator (SNT), only if in the GMC Mode of operation, you can configure one of the following options:
  - **Current SNT**
  - **All SNTs**
  - **Select SNTs**
- For SDM3000 RTUs, you can configure one of the following options:
  - **Current Site**
  - **All Sites**
  - **Select Sites**

IMPORTANT: Do not use the **All SNTs** or **All Sites** options if you are configuring the backup core of a system with the Dynamic System Resilience feature. Select only the SNT or the SDM3000 RTU in the backup core you are configuring.
If you already configured the SDM3000 RTU for this backup core, as part of another zones primary core SSH configuration, or no SDM3000 RTU is present at this master site, then click the **Cancel** button and skip the rest of this procedure, or click the **Back** button to return to the **Select Operation** window where you can choose to configure a different device.

If you chose the **Select SNTs** or **Select Sites** option, then an additional window displays devices to select.

7 If prompted, select the check box for each device you want to configure. Click **Next**.

8 Click **Next**.

The **SFTP Client Key Authentication Generation** window appears. The user name for the SDM3000 Builder user account displays. This is the account that will be used for SFTP Client public key authentication.

9 Select the following key generation parameters. Click **Next**.

a Key Type

b Key Size

10 For the RSA key type, select **2048** from the **Size** drop-down list.

RSA is the default key type used to connect in secure mode.

11 Click **Next**.

12 In the **Install Summary** window, click **Install**.

If a login window appears, enter your credentials.

NOTICE:
Also, a fingerprint verification prompt will display if this is the first time you are connecting to the SDM3000 hardware-based device from this SDM3000 Builder after generating SSH host keys on the device. In that case, verify the fingerprint and click **OK**, to add the SSH host keys for the SDM3000 hardware-based device to this SDM3000 Builders known hosts list.

NOTICE: During an SFTP session (any type of file download including Complete Install, Update Configuration Files, or Software and System Upgrade), the keys are used by the SDM3000 Builder for authentication of the SDM3000 hardware-based device as an SFTP client.

The **Installation Process** window appears. The SDM3000 hardware-based device generates an authentication key pair for the SDM3000 Builder user. The public key is returned to the SDM3000 Builder for future authentication. The SDM3000 Builder user name and the public key are recorded in the SDM3000 Builder as an authorized user.

13 Click **Next**.

14 In the **Installation Complete** window, click **Finish**.

Related Links

Configuring SSH for MOSCAD Network Fault Management (NFM) Devices on page 56

4.29.2
SSH Configuration for the SDM3000 Builder Application

Perform the procedure in this section to configure Secure Shell (SSH) on the SDM3000 Builder.

4.29.2.1
Generating a New Host Key for the SDM3000 Builder

Prerequisites: Ensure you have the SDM3000 Builder Administrator account name and password. If required, log on using your Active Directory account that is a member of the group with authority to perform the operations in this procedure as indicated in the Roles and Operations tool on the domain controller (instructions for the tool are located in the *Authentication Services* manual).

When and where to use:
After a device joins the domain, its applications that have Roles Based Access Control in Active Directory will not be usable by the local Windows administrator for that device unless the administrator accesses the application by entering its executable path and filename at the Windows command line. The path and filename can be seen in the properties for the application desktop shortcut.

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

Procedure:

1 Open a project in the SDM3000 Builder application.

2 From the **Tools** menu, select **Options**.

If **Options** is grayed out on the **Tools** menu, switch to the Advanced Mode view. (For instructions on how to switch to the Advanced Mode view, see the *SDM3000 Builder Users Guide*.)

3 In the **Options** window, perform one of the following actions:

- For the GMC Mode of operation, select the **Protocols** tab.
- For the Centralized UEM Mode, select the **Security** tab.

4 Depending on your mode of operation, perform one of the following actions:

If…	Then…
If you are in the GMC Mode,	on the **Protocols** tab, select one of the following options for **Connect to SDM3000 units through**: • **Secure Protocol** • **Both**
If you are in the Centralized UEM Mode,	on the **Security** tab, select the **Automatically Accept SDM3000's SSH Host Key** check box.

5 Select the key generation parameters:

a Key Type

RSA is the default key type used to connect in secure mode.

b Key Size

For the RSA key type, select **2048** from the **Size** drop-down list.

6 Click **Generate Keys**.

After key generation is complete, the key fingerprint appears and you can click **Copy Fingerprint** to save it for future reference.

7 Click **OK**.

The SDM3000 Builder SSH server host key is generated.

Related Links

Configuring SSH for MOSCAD Network Fault Management (NFM) Devices on page 56

4.29.3
Secure Operation Verification Between SDM3000 Builder and an SDM3000 Hardware-Based Device

When you initiate an SFTP session between the SDM3000 Builder and an SDM3000 hardware-based device, first the SSH host key fingerprint from the device is compared to the entries in the SDM3000 Builder known hosts list. If it does not match, you are prompted to verify the fingerprint. If you click **OK**, RSA keys for the device are added to the SDM3000 Builder known hosts list, then the SSH client keys on the device are automatically synchronized with the SDM3000 Builder authorized keys list.

SFTP sessions include any of the following install options in SDM3000 Builder:

- **Update Configuration Files** (this function is recommended if the purpose is just to verify SSH)
- **Complete Install**
- **Software and System Upgrade**
- **Firmware installation**

For these functions, the SDM3000 Builder is the SFTP server and the SDM3000 hardware-based device is the SFTP client.

For details on SDM3000 Builder, see the *SDM3000 Builder Users Guide*.

For details on the SDM3000, see the *SDM3000 Owners Manual*.

Related Links

Configuring SSH for MOSCAD Network Fault Management (NFM) Devices on page 56

4.29.4
SSH Configuration for the GMC and GWS

For the Network Fault Management (NFM) feature available for ASTRO® 25 communication systems, the Graphical Master Computer (GMC) and Graphical Workstation (GWS) host an application that collects fault management information from RF Site devices. For a system to operate in secure mode, the connection between the NFM SDM3000 Builder application and the GMC/GWS must be secure.

There may be other network fault managers supported that can use SDM3000 Builder for SDM3000 RTU configuration.

Perform the procedures in this section only if there are QUANTAR® stations or TeNSr channel banks being managed by the application on the GMC and GWS.

4.29.4.1
Adding SDM3000 RTU SSH Host Keys to the GMC and GWS Known Hosts Lists

NOTICE: Perform this procedure only if there are QUANTAR® stations or TeNSr channel banks being managed by the application on the GMC and GWS.

When and where to use:
For the Network Fault Management (NFM) feature, the Graphical Master Computer (GMC) and Graphical Work Station (GWS) host an application that collects fault management information from RF site equipment. Perform the following procedure to add RF site SDM3000 RTU SSH keys to the known hosts lists on a GMC and a GWS.

For details on the GMC Application on the GMC and GWS, see the *GMC/GWS Operations Manual*.

Procedure:

1 Log on to the GMC or GWS using the local Windows administrator account.

Note that “secmoto” is the Windows administrator account set up by Motorola Solutions on the GWS; on the GMC, the local Windows administrator account is “motosec” after Motorola Solutions supplemental configuration is applied

The desktop appears.

2 Launch the GMC application (for example, double-click the **GMC Application X.YY** icon on the desktop).

3 Access the picture of the TeNSr channel bank and click the **Configure** button.

NOTICE: If there are no TeNSr channel banks being managed by the application, then access the picture of a QUANTAR® station and click the **RSS** button.

4 When prompted to confirm that you trust the host, accept the host into the known hosts list.

5 Repeat the procedure on the GWS (if present).

Related Links

Configuring SSH for MOSCAD Network Fault Management (NFM) Devices on page 56

4.30
Using Cisco IOS Command to Generate SSH Keys on Console Telephony Media Gateway

When and where to use:

Perform the following procedure to generate the SSH keys on a console telephony media gateway using Cisco IOS command.

Procedure:

1. Connect the PC or terminal to the console port of the Console telephony media gateway using the console cable that came with the Console telephony media gateway.

   NOTICE: If the PC or the terminal has a 25-pin serial connector, first attach a 9-pin to 25-pin straight-through adapter to the PC end of the console cable.

2. Turn on the PC or terminals power. If using a PC, start the PC terminal emulator program.
3. Keep pressing ENTER until you are asked to enter your username.

   The Console telephony media gateway command-line interface (CLI) appears.

4. Type your username and press ENTER. Then type password and press ENTER.

   The command-line interface prompt appears.

5. Type `enable` and press ENTER. Type the privilege mode password and press ENTER.

   The Console telephony media gateway enters privilege mode.

6. At the command line, type `config terminal` and press ENTER.

   The Console telephony media gateway enters the configuration mode.

7. Enter the following command and press ENTER:

   ```
   crypto key generate rsa general-keys label sshkey modulus 2048
   ```

   The SSH keys are generated.

8. Type `end` and press ENTER.

   The Console telephony media gateway returns to the privilege mode.

9. Type the following command to check if the SSH keys are successfully generated:

   ```
   show crypto key mypubkey rsa
   ```

10. Enter the following command to save the SSH Keys so that it will persist through a reboot:

    ```
    write memory
    ```

Related Links

Configuring SSH for Devices at a Dispatch Site on page 53
Configuring SSH for Console Telephony Media Gateway on page 59

4.31 Backing Up SSH Configuration for MOSCAD Network Fault Management (NFM) Devices

When and where to use:
Perform the following process to back up the SSH configuration for MOSCAD NFM devices.

Process:

1. Save the SSH mode of SDM3000 Builder on the GMC or other device where SDM3000 Builder was used to configure SSH.

   See Saving the SSH Mode of SDM3000 Builder on page 203.

NOTICE: Ensure to perform this procedure before uninstalling SDM3000 Builder, if your organizations policies require uninstalling SDM3000 Builder when it is not being used.

2 On any GMC or other device where SDM3000 Builder was used to configure SSH, back up the SDM3000 Builder SSH known hosts list and SSH keys by copying the following folders to a secure location:

- `C:\Motorola\SDM3000\Common\SFTP`
- `C:\Motorola\SDM3000\Common\SSH`

NOTICE:
Log on to the GMC or GWS using the local Windows administrator account (“secmoto” is the Windows administrator account set up by Motorola Solutions on the GWS; on the GMC, the local Windows administrator account is “motosec” after Motorola Solutions supplemental configuration is applied).

Ensure to back up these folders before uninstalling SDM3000 Builder, if your organizations policies require uninstalling SDM3000 Builder when it is not being used.

3 Back up the SSH mode of each SDM3000 hardware-based device.

See Backing Up the SSH Mode of an SDM3000 Hardware-Based Device on page 204.

4.31.1
Saving the SSH Mode of SDM3000 Builder

Perform the following procedure on any GMC or other device where SDM3000 Builder was used to configure SSH.

Procedure:

1 Log on to the GMC or GWS using the local Windows administrator account.

After Motorola Solutions supplemental configuration is applied, “secmoto” is the Windows administrator account set up by Motorola Solutions on the GWS; on the GMC, the local Windows administrator account is “motosec”.

The desktop appears.

2 Launch the SDM3000 Builder application.

Step example: Click the **SDM3000 Builder** ***<x.yy>*** icon on the desktop.

3 In the SDM3000 Builder application, select **View** → **Mode** → **Advanced**.

The Advanced mode is enabled.

4 In the SDM3000 Builder application, select **Tools** → **Options**.

5 In the **Options** dialog box, select the **Security** tab.

6 For recovery purposes, save the current configuration settings in the **Options** dialog box, **Security** tab:

a Press ALT + PRINTSCREEN.

b Paste the screen shot into a Wordpad or a Paint file.

c Save the file.

7 Click **Cancel**.

The **SDM3000 Builder Options** dialog box closes.

8 From the **File** menu, select **Exit**.

The SDM3000 Builder application closes.

4.31.2
Backing Up the SSH Mode of an SDM3000 Hardware-Based Device

When and where to use:
Perform the following procedure for SDM3000 RTUs and SDM3000 Network Translators:

Procedure:

1 Enter the IP address of the SDM3000 hardware-based device in the Address field of Internet Explorer to open the default web page for the SDM3000 hardware-based device.

NOTICE: If any security warnings display, click **Yes** or **OK**.

2 Click **Go to Home page**.

A prompt for username and password appears.

3 Enter the web administrator's username and password and click **OK**.

The SDM3000 device home page appears.

4 Click **Admin** on the SDM3000 device home page to open the **Administrator Tools** page.

The **Administrator Tools** page appears.

5 Click **Configuration** on the **Administrator Tools** page.

The **Configuration** page appears.

6 Click **Backup** on the **Configuration** page.

The **Backup** page appears.

7 Click **Upload SSH backup copy** on the **Backup** page.

NOTICE:
If an Information Bar message box appears, click **OK**.

If an Information Bar appears, click it and select **Download File**.

8 In the File Download dialog box, click **Save**, and save the file in a secure location on the network.

9 Close the **Internet Explorer** window.

4.32
Restoring SSH Configuration for MOSCAD Network Fault Management (NFM) Devices

When and where to use:
Perform the following process to restore the SSH configuration for MOSCAD NFM devices.

Process:

1 Perform the following actions immediately after re-installing SDM3000 Builder (if re-installation is required as part of the recovery process), on any GMC (or other device) where SDM3000 Builder was used to configure SSH:

a Log on to the GMC using the local Windows administrator account (after Motorola Solutions supplemental configuration of a GMC, the local Windows administrator account is “motosec”):

b Restore the SDM3000 Builder SSH known hosts list and SSH keys, by copying the `\SFTP` and `\SSH` folders from their backup location to:

- `C:\Motorola\SDM3000\Common\SFTP`
- `C:\Motorola\SDM3000\Common\SSH`

c Restore the SSH mode of SDM3000 Builder.

See Restoring the SSH Mode of SDM3000 Builder on page 205.

2 Restore the SSH mode of each SDM3000 hardware-based device.

See Restoring the SSH Mode of an SDM3000 Hardware-Based Device on page 205.

4.32.1
Restoring the SSH Mode of SDM3000 Builder

Perform this procedure on any GMC or other device where SDM3000 Builder will be used to configure SSH.

Procedure:

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

After the Motorola Solutions supplemental configuration of a GMC, the local Windows administrator account is “motosec”.

The desktop appears.

2 Launch the SDM3000 Builder application.

Step example: Click the `SDM3000 Builder x.yy` icon on the desktop.

3 In the SDM3000 Builder application, select **View** → **Mode** → **Advanced**.

The Advanced mode is enabled.

4 In the SDM3000 Builder application, select **Tools** → **Options**.

5 In the **Options** dialog box, select the **Security** tab.

6 Set the **Security** tab parameters, according to the settings saved in Saving the SSH Mode of SDM3000 Builder on page 203.

7 Click **OK**.

The **SDM3000 Builder Options** dialog box closes.

8 From the **File** menu, select **Exit**.

The SDM3000 Builder application closes.

4.32.2
Restoring the SSH Mode of an SDM3000 Hardware-Based Device

When and where to use:

Perform the following procedure for SDM3000 RTUs and SDM3000 Network Translators.

Procedure:

1. Enter the IP address of the SDM3000 hardware-based device in the **Address** field of Internet Explorer to open the default web page for the SDM3000 hardware-based device.

   NOTICE: If any security warnings display, click **Yes** or **OK**.

2. Click **Go to Home page**.

   A prompt for username and password appears.

3. Enter the web administrator's username and password and click **OK**.

   The SDM3000 device home page appears.

4. Click **Admin** on the SDM3000 device home page to open the **Administrator Tools** page.

   The **Administrator Tools** page appears.

5. Click **Configuration** on the **Administrator Tools** page.

   The **Configuration** page appears.

6. Click **Backup** on the **Configuration** page.

   The **Backup** page appears.

7. Click **Browse** on the **Backup** page, then navigate to and open the SSH configuration backup file previously created for this device.
8. Click **Restore SSH backup copy** on the **Backup** page.

   A confirmation window appears.

9. Click **OK**.

   The confirmation window closes.

10. Close the **Internet Explorer** window.

Chapter 5

SSH Optimization

This chapter is for optimization procedures related to Securing Protocols with SSH.

5.1 SSH Optimization

There are no optimization procedures applicable to the Securing Protocols with SSH feature.

Chapter 6

SSH Operation

This chapter provides information about tasks that you can perform after SSH is installed and operational on your system.

6.1 Periodic SSH Key Rotation – Considerations

SSH key rotation is the process of generating new keys on each device and propagating them to the other devices that need them.

The “Configuration” chapter documents a process for maximizing system availability while rotating all SSH keys for SSH servers (hosts) and SSH client user accounts as part of initial configuration of this feature.

The scope and frequency of periodic SSH key rotations depends on your organizations policies. For example, the scope may include:

- **Updating all of the SSH host and user keys for all interactive and non-interactive SSH accounts:**

  This requires a complete rotation of all host keys and user keys (all procedures in the “Configuration” chapter).

- **Updating only the SSH host keys:**

  If your organizations policies require key rotation only for interactive SSH accounts, then your organization performs only the procedures from the “Configuration” chapter that generate new host keys on the SSH servers and that replace those hosts in the known hosts lists on the associated SSH clients. (For interactive SSH sessions, user keys are not involved, because user authentication is accomplished with passwords.)

An important concept to understand is that there is a known hosts list for every account that connects to an SSH server. So, after new host keys are generated, known hosts lists need to be generated for:

- **Interactive accounts:** This can be any interactive account name you specify when connecting to an SSH server device for service or administrative purposes, using software such as PuTTY or Configuration/Service Software (CSS).
- **Non-interactive users:** The non-interactive users that must be configured for SSH in an ASTRO® 25 communication system are covered in the “Configuration” chapter. For example, see the processes for configuring SSH for centralized Backup Clients, for devices using default keys, and for Network Fault Management (NFM) devices.

6.1.1 SSH Key Rotation Impact on ASTRO 25 System Non-Interactive Services

The following table lists examples of ASTRO® 25 communication system services which require numerous ssh/scp/sftp sessions to be set up non-interactively after the service is launched by the user. Rather than prompt the user for a password for each instance, SSH public key authentication is used when establishing these connections.

An SSH key rotation has the following impacts on these services:

- After the SSH server host key is regenerated on the host device, the listed services for the associated SSH client devices will fail until the SSH client's known host list has been updated with the SSH server's new public key.
- After the SSH client key is regenerated on the SSH client device, the services for the client device will fail until the SSH server's authorized list of keys has been updated with the client's new public key.

Avoid launching these services when an SSH key rotation is being performed. (Also, be aware that Statistics Data Collection is performed without user intervention, and will be impacted during a key rotation.)

NOTICE: Service downtime will be minimized during a key rotation if you follow the sequences provided in the "Configuration" chapter of this manual.
For systems with the Dynamic System Resilience (DSR) feature, the corresponding interfaces between primary and backup cores will have services impacted during a key rotation in the same way if the device in the backup core is currently active (with the exception of Backup/Restore services). For redundant system level services (UNC and UCS), the impacts will only occur between devices and the UNC or UCS that is currently active.

Services unique to DSR are labeled "DSR Only" in the following table.

Table 22: SSH Key Rotation Impact on ASTRO 25 System Non-Interactive Services – Examples

SSH Client	SSH Server	Non-Interactive Service
ZSS, SSS, NM Client(s)	ATR	Statistics Data Collection (ZSS-ATR, SSS-ATR) ATIA Log Data Exchange (NM Client-ATR)
UCS, UNC server, UNCDS server, NM Client(s)	UCS	Database Sync (UNC-UCS) **DSR Only:** Data Synchronization between redundant cores (UCS-UCS)
UCS, UNC server, UNCDS server, ATR, ZSS, PDG, ZC01, ZC02, ZC03, ZC04, ISGW01, ISGW02, ISGW03, ISGW04, SSS	UNC	Configuration Management Services (ATR-UNC, ZSS-UNC, PDG-UNC, ZC01-UNC, ZC02-UNC, ZC03-UNC, ZC04-UNC, SSS-UNC, ISGW01-UNC, ISGW02-UNC, ISGW03-UNC, ISGW04-UNC) **DSR only:** Data Synchronization between redundant cores (UNC-UNC) Voyence (UNC-UNC) Data Distribution
Backup Client	Backup Server	Centralized backup service Centralized restore service

6.2 Secure Performance of the ASTRO 25 Communication System Operations

The scope of this manual does not include documentation of every operational procedure that can be performed securely in an ASTRO® 25 communication system.

The "Configuration" chapter indicates which SSH servers (hosts) and SSH client user accounts are part of initial configuration of this feature. This process configures all SSH communication required for normal operation of the system. You may perform additional configuration as needed such as saving additional sessions in PuTTY for the accounts you use most often to access devices in an ASTRO® 25

communication system that are SSH servers. See Using PuTTY to Access an SSH Server from a Windows-Based Device on page 89.

The “Configuration” chapter also provides other examples of procedures that are performed using secure protocols on the various device platforms in an ASTRO® 25 communication system.

Chapter 7

SSH Maintenance

This chapter is for periodic maintenance procedures relating to the Securing Protocols with SSH feature.

7.1 SSH Maintenance

There are no routine maintenance procedures for the Securing Protocols with SSH feature other than periodic key rotation, if the system policy requires it, backing up the SSH keys, and auditing these keys as needed. Key rotation and backup procedures vary by device. See the “Configuration” chapter for details.

Chapter 8

SSH Troubleshooting

This chapter provides fault management and troubleshooting information relating to the Securing Protocols with SSH feature.

8.1 Failure Scenarios

The following are the various failure scenarios that can impact secure sessions between devices:

- Device failures
- Connectivity failures
- SSH configuration failures (such as failures that occur due to inappropriate combinations of the secure and clear protocols)
- Public key authentication failures
- Password authentication failures

NOTICE: For information on troubleshooting password authentication failures, see the *Authentication Services* manual.

8.2 Troubleshooting PSCP and PSFTP

If pscp or psftp commands fail, one possible cause is that a host might be saved in the default settings of PuTTY. Open any instance of PuTTY on the computer, select **Default Settings**, and, if a host automatically displays in the **Host Name (or IP address)** field, delete it, and save the Default Settings.

8.3 Secure Mode and Clear Mode Settings Required for SFTP and SCP Sessions

For successful secure file transfer sessions to occur, one of the combinations of security modes listed in the following table should be configured.

NOTICE: To perform operations in secure mode, ensure that Key Provisioning has been performed on the SSH server and the SSH client.

Table 23: Secure Mode and Clear Mode Settings Required for SFTP and SCP Sessions

SSH Server	SSH Client
Secure	Secure
Both	Both
Both	Secure
Secure	Both

Any other combinations will prevent SSH communications from taking place.

8.4

Secure Mode and Clear Mode Settings Required for FTP and TFTP Sessions

For successful FTP and TFTP sessions to occur, one of the combinations of security modes listed in the following table should be present.

NOTICE: To perform operations in the Secure mode, ensure that Key Provisioning has been performed on the SSH server and the SSH client.

Table 24: Secure Mode and Clear Mode Settings Required for FTP and TFTP Sessions

SSH Server	SSH Client
Clear Only	Clear Only
Both	Both
Both	Clear Only

Any other combinations prevent FTP and TFTP communications from taking place. For example:

- Clear Only should not be configured on the SSH server when both protocols are enabled on the SSH client.
- An SSH client should not have secure protocols enabled unless the associated SSH server has secure protocols enabled.

8.5

Secure Operation Testing

The following is a summary of testing that can be performed to verify secure operation on a device:

- Querying the device for the secure mode and clear mode settings, if this functionality is available.
- Testing interactive (login) sessions using a secure terminal utility and testing non-interactive sessions (batch jobs and automated scripts) by using associated functions (such as scheduling a backup or requesting status from a device).

  NOTICE: You can test one protocol for each connection.

- Checking the event messages logged locally on the device and/or at the Centralized Event Logging server (if the Centralized Event Logging feature is implemented in the system).

The methods used for testing secure operation vary based on the device. See the “Configuration” chapter for examples of how to test specific devices once they have been configured for secure operation.

8.6

SSH Troubleshooting – Examples

Table 25: Troubleshooting Scenarios for SSH

Problem	Action to take
Failure to establish a secure connection	• Check to see if secure protocol operation has been disabled on the server.

Problem	Action to take
	• Verify the TCP/IP settings. • If clear protocols are enabled, verify that a connection can be established through a supported clear protocol. • Check the messages returned to the Centralized Event Logging server (if the Centralized Event Logging feature is implemented in the system) to determine how far the connection proceeded before the failure.
Secure connection failure due to an algorithm negotiation failure	• Check to see if any changes have been made to the preset configuration information. **NOTICE:** The preset configuration information should not be modified.
A warning message appears when you connect to the server	• Check to see if the server host key has changed or if this is the first connection to the server. **NOTICE:** For some devices, enabling a secure protocol automatically generates new host keys. For an example, see SSH Configuration for RF Site Devices and VPMs Using CSS – Overview on page 155. • Check to see if the client's known hosts list needs to be updated with the host name(s) and public key of the server. • Verify the fingerprint of the host.
Public key authentication failure	• Verify that a public/private key pair has been generated and stored at the correct location on the client. • Verify that the authorized list of keys at the server contains the client's public key.
Unable to update the authorized list of keys at the server	• Check the user account for which you are updating the authorized list of keys. (Public key authentication will only be supported for non-interactive accounts.)
Password authentication failure	• Verify that SSH Pluggable Authentication Module (PAM) support is enabled if PAM is being used. • Verify the settings of the PAM.
Logging into a device remotely to establish a remote secure terminal session results in a connection failure.	• Check to see if the device has been configured to support a remote secure terminal session. For example, it is possible to configure RF Site devices with SFTP enabled and Secure Terminal disabled.

Problem	Action to take
However, access to the device is possible using sftp.	

8.7

Syslog Information About Secure Sessions and Clear Sessions

Syslog messages can be viewed to verify protocol changes and the success of secure or clear sessions with a device. As an example, the following table lists the type of information contained in syslog messages about secure sessions and clear sessions on RF site devices.

For additional information about syslog messages and the Centralized Event Logging feature available for ASTRO® 25 communication systems, see the *Centralized Event Logging* manual.

Table 26: RF Site Devices – Syslog Information About Secure Sessions and Clear Sessions

System Event	Syslog Message Includes:
Service configuration changes made through Configuration/Service Software (CSS)	• Type of configuration change (such as service enable, disable, or restart) • Success or failure
Telnet and FTP service initialization	• Service Transition to ON or to OFF • Success or failure
Telnet login and logout	• Authentication information • Username • Telnet session opened or closed
Secure Shell terminal login and logout	• Authentication information • Username • SSH session opened or closed • Secure Terminal Sub-Service session opened or closed
FTP login and logout	• Authentication information • Username • FTP session opened or closed
Secure FTP login, file operation, and logout	• Authentication information • Username • SSH session opened or closed • Secure FTP Sub-Service session opened or closed • Success or failure of file operation

MNR routers and GGM 8000 gateways send an SSH `Login Failed` log message for each failed login attempt. In addition, a client that attempts to log in via an authentication method that is supported by the OpenSSH Library but not by the Enterprise Operating System (EOS) also triggers a `Login Failed` message:

- If a session consists of one or two failed password login attempts followed by a successful login, the EOS software sends a `Login Failed` log message for each failed password login attempt, following by a `Login Successful` message for the successful login.
- If a session consists of three failed password login attempts, the EOS software returns a `Login Failed` message for each failed attempt and disconnects the SSH session.
- If a session consists of a single successful password login attempt, the router or gateway may generate up to two `Login Failed` messages before the `Login Successful` message. This is because most clients try to log in with other authentication methods before attempting password authentication. The login attempts that use authentication methods not supported by EOS generate `Login Failed` messages prior to the `Login Successful` message that is sent upon the successful password authentication login.

8.8 Troubleshooting SSH Configuration for the Backup Server and Backup Clients

The following process describes the steps for troubleshooting the SSH configuration for the centralized Backup Server and Backup Clients. For details about the centralized backup solution, see the *Backup and Restore Services* manual.

Process:

1. Initiate an SSH operation from the Backup Client to the Backup Server.
2. Validate that a connection is established:

If…	Then…
If a password prompt appears,	the connection is established and all keys are provisioned properly for secure mode.
If a prompt to validate the RSA fingerprint appears,	compare the fingerprint in the prompt to the fingerprint you recorded after the most recent host key generation on the Backup Server. If the fingerprints do not match, immediately begin a new key rotation process for the Backup Server and all Backup Clients.

Appendix A

SSH Connection Lists (Primary Cores and Sites)

For reference purposes, this Appendix lists SSH connections that are included in the Securing Protocols with SSH feature in ASTRO® 25 systems. The detailed configuration processes and procedures for configuring these SSH connections are located in the “Configuration” chapter of this manual.

These lists include devices that may or may not be included in your system, depending on your system configuration and the optional features in your system. Also *Site N* in these lists represents one site, and your system may have more than one site with the listed SSH connections. Additionally, your system may include more than one zone with the SSH connections in these lists.

For consideration when reviewing these SSH connection lists, the following are a few of the differences that depend on system configuration:

ASTRO® 25 M3 system configurations with DSR
Primary core is used in these SSH connection lists to differentiate from the *backup core* that is implemented if the Dynamic System Resilience (DSR) feature will be implemented (see SSH Connection Lists – DSR Only on page 226 for SSH connections specific to DSR). For other ASTRO® 25 system configurations, *primary core* refers to any zone core in the system.

ASTRO® 25 L core configuration
The core router and gateway router are combined into a single device called the core gateway.

ASTRO® 25 K core configuration
A site gateway is present instead of a core router and gateway router. The equipment that is not present in a K core also includes Network Management servers and Network Management clients.

ASTRO® 25 Express Trunking Systems
The only SSH connections that require setup are between the Configuration/Service Software (CSS) and the equipment it configures (site controllers and site repeaters). See Table 32: RF and VPM-Based Devices SSH Connections (Primary Cores and Sites) on page 222.

A.1 Backup and Restore Services Non-Interactive SSH Connections (DSR Backup Cores)

Table 27: Backup and Restore Services Non-Interactive SSH Connections (L and M1–M3 Primary Cores)

SSH Client	SSH Server
MediaMgr - `bkup_mmr`	Backup Server
Backup Server - `bkup_svc` - `bkup_adm`	Backup Server
Backup Server	Backup Server

SSH Client	SSH Server
- bkupclnt - root	
ATR - bkupclnt - root	Backup Server
PDG - bkupclnt - root	Backup Server
ZDS - bkupclnt - root	Backup Server
ZSS - bkupclnt - **root**	Backup Server
UCS - bkupclnt - root	Backup Server
SSS - bkupclnt - root	Backup Server
ZC01 - bkupclnt - root	Backup Server
ZC02 - bkupclnt - root	Backup Server
ISGW01 - bkupclnt - root	Backup Server
ISGW02 - bkupclnt - root	Backup Server
UEM - bkupclnt - root	Backup Server

SSH Client	SSH Server
UNC - bkupclnt - root	Backup Server
UNCDS[1] - bkupclnt - root	Backup Server
Centralized Event Logging Server - bkupclnt - root	Backup Server
IP Packet Capture - bkupclnt - root	Backup Server
License Manager - bkupclnt - root	Backup Server
NM Clients	Backup Server
CSMS	Backup Server
System DC	Backup Server
Zone DC	Backup Server
InfoVista	Backup Server
GMC	Backup Server
GWS	Backup Server
AuC Server	Backup Server
CAM Server[2]	Backup Server

A.2 Network Management Non-Interactive SSH Connections (L and M1–M3 Primary Cores)

Table 28: Network Management Non-Interactive SSH Connections (L and M1–M3 Primary Cores)

SSH Client	SSH Server
ZSS	ATR
SSS	ATR
UNC	UCS

[1] There are three instances of the UNCDS on the server, if UNCDS is present.
[2] The CAM Server resides at the dispatch site.

SSH Client	SSH Server
UNCDS01, UNCDS02, UNCDS03	UNC
UCS	UNC
UNC	UNC
ATR	UNC
ZSS	UNC
PDG	UNC
ZC01	UNC
ZC02	UNC
ISGW01	UNC
ISGW02	UNC
SSS	UNC
NM Clients - ATIA Log Viewer	ATR (in each zone)

A.3 Network Management Interactive SSH Connections (L and M1–M3 Primary Cores)

Table 29: Network Management Interactive SSH Connections (L and M1–M3 Primary Cores)

SSH Client	SSH Server
Service laptop or, if present, NM Client	ATR
Service laptop or, if present, NM Client	SSS
Service laptop or, if present, NM Client	UCS
Service laptop or, if present, NM Client	UEM
Service laptop or, if present, NM Client	ZC01
Service laptop or, if present, NM Client	ZC02
Service laptop or, if present, NM Client	ISGW01
Service laptop or, if present, NM Client	ISGW02
Service laptop or, if present, NM Client	ZDS
Service laptop or, if present, NM Client	ZSS
Service laptop or, if present, NM Client	PDG

A.4

Network Transport SSH Connections (L and M1–M3 Primary Cores and Sites)

The Intrusion Detection System Sensor (IDSS) configuration in the following checklist is for a Motorola Solutions-provided scenario. Your organization may implement its own scenarios, in which case the SSH configuration for IDSS in the checklist does not apply.

Table 30: Network Transport SSH Connections (L and M1–M3 Primary Cores and Sites)

SSH Client	SSH Server
Primary Cores	
CSMS	IDSS (if Motorola Solutions-provided)
UNC	M1-M3 cores: Core Routers and Gateway Routers L core: Core Gateways
UNC	Exit Routers
UNC	GGSNs
UNC	Core LAN Switches
UNC	Mediation LAN Switches
UNC	IDS LAN Switch
UNC	Fan-out LAN Switches
Site N	
UNC	Site N Network Transport Devices
ISSI.1 NGW Site	
UNC	Site Network Transport Devices
Service laptop or, if present, NM Client	Generic Application Server (GAS)

A.5

Network Transport Interactive SSH Connections (K, L, M1–M3 Primary Cores and Sites)

Table 31: Network Transport Interactive SSH Connections (K, L, M1–M3 Primary Cores and Sites)

SSH Client	SSH Server
Primary Cores	
Service laptop or, if present, NM Client	M1-M3 cores: Core Routers and Gateway Routers L core: Core Gateways K core: Site Gateways

SSH Client	SSH Server
Service laptop or, if present, NM Client	Exit Routers
Service laptop or, if present, NM Client	GGSNs
Service laptop or, if present, NM Client	Core LAN Switches
Service laptop or, if present, NM Client	Mediation LAN Switches
Service laptop or, if present, NM Client	IDS LAN Switch
Service laptop or, if present, NM Client	Fan-out LAN Switches
Service laptop or, if present, NM Client	Core Terminal Server
Site N	
Service laptop or, if present, NM Client	Site N Network Transport Devices
ISSI.1 NGW Site	
Service laptop or, if present, NM Client	Site Network Transport Devices
Service laptop or, if present, NM Client	ISSI.1 Gateway Module
Service laptop or, if present, NM Client	Site Link Relay Module

A.6 RF and VPM-Based Devices SSH Connections (Primary Cores and Sites)

Table 32: RF and VPM-Based Devices SSH Connections (Primary Cores and Sites)

SSH Client	SSH Server
CSS	SmartX Site Converter
CSS	Telephone Media Gateways
MLC 8000 Configuration Tool (CT)	MLC 8000 Analog Comparator
MLC 8000 Configuration Tool (CT)	MLC 8000 Subsite Link Converter
Service laptop or, if present, NM Client	SmartX Site Converter

SSH Client	SSH Server
Service laptop or, if present, NM Client	Telephone Media Gateways
Site N	
CSS	GCP 8000 Site Controllers, GBP 8000 RDMs at Site N
CSS	GTR 8000 Base Radios, Repeaters, Receivers at Site N
CSS	GCM 8000 Comparators at Site N
CSS	MCC 7500 Voice Processor Modules (VPMs) at Site N
Service laptop or, if present, NM Client	GCP 8000 Site Controllers, GBP 8000 RDMs at Site N
Service laptop or, if present, NM Client	GTR 8000 Base Radios, Repeaters, Receivers at Site N
Service laptop or, if present, NM Client	GCM 8000 Comparators at Site N
Service laptop or, if present, NM Client	MCC 7500 Voice Processor Modules (VPMs) at Site N

A.7 MOSCAD NFM SSH Connections (Primary Cores and Sites)

Table 33: MOSCAD NFM SSH Connections (Primary Cores and Sites)

SSH Client	SSH Server
Primary Cores	
Service laptop or, if present, NM Client	SDM3000 Network Translator
SDM3000 Builder	SDM3000 Network Translator
SDM3000 Network Translator	SDM3000 Builder
Service laptop or, if present, NM Client	SDM3000 RTU
SDM3000 Builder	SDM3000 RTU
SDM3000 RTU	SDM3000 Builder
Site N	
Service laptop or, if present, NM Client	Site N SDM3000 RTU
Site N SDM3000 Builder	Site N SDM3000 RTU
Site N SDM3000 RTU	Site N SDM3000 Builder
Site N GMC	Site N SDM3000 RTU
Site N GWS	Site N SDM3000 RTU

A.8 Secure SWDL SSH Connections

Table 34: Secure SWDL SSH Connections

SSH Client	SSH Server
GCP 8000 Site Controllers	SWDL Manager
GTR 8000 Stations	SWDL Manager
GCM 8000 Comparators	SWDL Manager
GPB8000 RDM (Summit Based) Time Servers	SWDL Manager
GPW 8000 Stations (Rx only)	SWDL Manager
SmartX Controller	UNC
TMG	UNC
VPM	UNC

A.9 Edge Availability with Wireline Console (Tsub) SSH Connections

The following tables list SSH connections that are utilized for services between the Trunking Subsystem (Tsub) server devices and other ASTRO® 25 system devices.

Table 35: Tsub SSH Connections 1

Zone Core (SSH Client)	Tsub (SSH Server)
NM Client	Tsub Zone Controller (ZC)
NM Client	Tsub IP Packet Capture
NM Client	Tsub VMS
Service Laptop	Tsub Zone Controller (ZC)
Service Laptop	Tsub IP Packet Capture
Service Laptop	Tsub VMS

Table 36: Tsub SSH Connections 2

Tsub (SSH Client)	Zone Core (SSH Server)
Tsub Zone Controller (ZC)	Unified Network Configurator (UNC)
Tsub Zone Controller (ZC)	Backup and Restore (BAR) Server
Tsub IP Packet Capture	Backup and Restore (BAR) Server

Table 37: Tsub SSH Connections 3

Tsub (SSH Client)	Tsub (SSH Server)
Tsub IP Packet Capture	Tsub VMS

Tsub (SSH Client)	Tsub (SSH Server)
Service laptop or, if present, NM Client	Terminal Server
Terminal Server	SSH-capable devices

A.10
Other Interactive SSH Connections

Table 38: Other Interactive SSH Connections

SSH Client	SSH Server
M1-M3 Primary Cores	
Service laptop or, if present, NM Client	HPD Packet Data Gateway
L Core and M1–M3 Primary Cores	
Service laptop or, if present, NM Client	IVD Packet Data Gateway
Service laptop or, if present, NM Client	Backup and Restore (BAR) server
Service laptop or, if present, NM Client	Centralized Event Logging servers
Service laptop or, if present, NM Client	IP Packet Capture
Service laptop or, if present, NM Client	License Manager
K Primary Core	
Service laptop	Conventional Packet Data Gateway
Service laptop	IP Packet Capture

Appendix B

SSH Connection Lists – DSR Only

For reference purposes, this Appendix lists SSH connections that are specific to the Securing Protocols with SSH and Dynamic System Resilience (DSR) features in ASTRO® 25 systems. The detailed configuration processes and procedures for configuring these SSH connections are located in the "Configuration" chapter of this manual. (See Performing Additional SSH Configuration Processes for DSR Systems on page 68.)

If your ASTRO® 25 system does not have the DSR feature, this Appendix does not apply. If your system does include DSR, be aware that the lists in the Appendix include devices that may or may not be included in your system, depending on your system configuration and the optional features in your system.

B.1 Backup and Restore Services Non-Interactive SSH Connections (DSR Backup Cores)

Table 39: Backup and Restore Services Non-Interactive SSH Connections (DSR Backup Cores)

Backup Core SSH Client	Backup Core SSH Server
MediaMgr - bkup_mmr	Backup Server
Backup Server - bkup_svc - bkup_adm	Backup Server
Backup Server - bkupclnt - root	Backup Server
ATR - bkupclnt - root	Backup Server
PDG - bkupclnt - root	Backup Server
ZDS - bkupclnt - root	Backup Server
ZSS - bkupclnt - root	Backup Server
UCS	Backup Server

Backup Core SSH Client	Backup Core SSH Server
- bkupclnt - root	
SSS - bkupclnt - root	Backup Server
ZC03 - bkupclnt - root	Backup Server
ZC04 - bkupclnt - root	Backup Server
ISGW03, ISGW04 - bkupclnt- root	Backup Server
UEM - bkupclnt - root	Backup Server
UNC - bkupclnt - root	Backup Server
Centralized Event Logging Server - bkupclnt - root	Backup Server
IP Packet Capture - bkupclnt - root	Backup Server
License Manager - bkupclnt - root	Backup Server
NM Clients	Backup Server
CSMS	Backup Server
System DC	Backup Server
Zone DC	Backup Server
InfoVista	Backup Server
GMC	Backup Server
GWS	Backup Server
AuC Server	Backup Server

Backup Core SSH Client	Backup Core SSH Server
CAM Server	Backup Server

B.2
Network Management Interactive SSH Connections (DSR Backup Cores)

Table 40: Network Management Interactive SSH Connections (DSR Backup Cores)

Backup Core SSH Client	Backup Core SSH Server
NM Clients	UEM
NM Clients	ZDS
NM Clients	ZSS
NM Clients	UCS
NM Clients	SSS
NM Clients	ZC03
NM Clients	ZC04
NM Clients	ISGW03
NM Clients	ISGW04
NM Clients	ATR
NM Clients - ATIA Log Viewer	ATR (in each zone)
ZSS	ATR
SSS	ATR
UNC	UCS
UCS	UNC
UNC	UNC
ATR	UNC
ZSS	UNC
PDG	UNC
ZC03	UNC
ZC04	UNC
ISGW03, ISGW04	UNC
SSS	UNC

B.3
Other Interactive SSH Connections (DSR Backup Cores)

Table 41: Other Interactive SSH Connections (DSR Backup Cores)

Backup Core SSH Client	Backup Core SSH Server
NM Clients	PDG

Backup Core SSH Client	Backup Core SSH Server
NM Clients	BAR
NM Clients	Centralized Event Logging servers
NM Clients	IP Packet Capture
NM Clients	License Manager

B.4

Network Transport SSH Connections (List 1 of 3 for DSR)

The Intrusion Detection System Sensor (IDSS) configuration in the following list is for a Motorola-Solutions provided scenario. Your organization may implement its own scenarios, in which case the SSH configuration for IDSS in the checklist does not apply.

Table 42: Network Transport SSH Connections (List 1 of 3 for DSR)

Backup Core SSH Client	SSH Server
Master Sites Where Primary and Backup Core Share Transport Devices	
CSMS	Backup core IDSS (if Motorola Solutions-provided)
UNC	Core Routers
UNC	Gateway Routers
UNC	Exit Routers*that were added for DSR*
UNC	Exit Routers *(other)*
UNC	GGSNs
UNC	Core LAN Switches
UNC	Mediation LAN Switches
UNC	IDS LAN Switch
UNC	Fan-out LAN Switches
NM Clients	Core Routers
NM Clients	Gateway Routers
NM Clients	Exit Routers *that were added for DSR*
NM Clients	Exit Routers *(other)*
NM Clients	GGSNs
NM Clients	Core LAN Switches
NM Clients	Mediation LAN Switches
NM Clients	IDS LAN Switch
NM Clients	Fan-out LAN Switches
NM Clients	Core Terminal Server
Master Sites With Standalone Backup Core (No Shared Transport)	
CSMS	IDSS (if Motorola Solutions-provided)
UNC	Core Routers
UNC	Gateway Routers

Backup Core SSH Client	SSH Server
UNC	Exit Routers
UNC	GGSNs
UNC	Core LAN Switches
UNC	Mediation LAN Switches
UNC	IDS LAN Switch
UNC	Fan-out LAN Switches
NM Clients	Core Routers
NM Clients	Gateway Routers
NM Clients	Exit Routers
NM Clients	GGSNs
NM Clients	Core LAN Switches
NM Clients	Mediation LAN Switches
NM Clients	IDS LAN Switch
NM Clients	Fan-out LAN Switches
NM Clients	Core Terminal Server

B.5 MOSCAD NFM SSH Connections (DSR Backup Cores)

Table 43: MOSCAD NFM SSH Connections (DSR Backup Cores)

SSH Client	SSH Server
Master Sites – Backup Core Only	
NM Clients in backup core	SDM3000 Network Translator in backup core
SDM3000 Builder in backup core	SDM3000 Network Translator in backup core
SDM3000 Network Translator in backup core	SDM3000 Builder in backup core
NM Clients in backup core	SDM3000 RTU in backup core
SDM3000 Builder in backup core	SDM3000 RTU in backup core
SDM3000 RTU in backup core	SDM3000 Builder in backup core
Site N	
GMC in backup core	SDM3000 RTU at Site N
GWS in backup core	SDM3000 RTU at Site N
NM Clients in backup core	SDM3000 RTU at Site N
SDM3000 Builder in backup core	SDM3000 RTU at Site N

B.6
MOSCAD NFM SSH Connections (DSR – Primary Core to Backup Core)

Table 44: MOSCAD NFM SSH Connections (DSR – Primary Core to Backup Core)

Primary Core SSH Client	Backup Core SSH Server
Master Sites	
NM Clients	SDM3000 Network Translator
SDM3000 Builder	SDM3000 Network Translator
SDM3000 Network Translator	SDM3000 Builder
NM Clients	SDM3000 RTU
SDM3000 Builder	SDM3000 RTU
SDM3000 RTU	SDM3000 Builder

B.7
MOSCAD NFM SSH Connections (DSR – Backup Core to Primary Core)

Table 45: MOSCAD NFM SSH Connections (DSR – Backup Core to Primary Core)

Backup Core SSH Client	Primary Core SSH Server
Master Sites	
NM Clients	SDM3000 Network Translator
SDM3000 Builder	SDM3000 Network Translator
SDM3000 Network Translator	SDM3000 Builder
NM Clients	SDM3000 RTU
SDM3000 Builder	SDM3000 RTU
SDM3000 RTU	SDM3000 Builder

B.8
Network Management SSH Connections (DSR – Primary Core to Backup Core)

Table 46: Network Management SSH Connections (DSR – Primary Core to Backup Core)

Primary Core SSH Client	Backup Core SSH Server
NM Clients – ATIA Log Viewer	ATR
SSS	ATR
UCS	UCS
UNC	UNC
ATR	UNC

Primary Core SSH Client	Backup Core SSH Server
ZSS	UNC
PDG	UNC
ZC01	UNC
ZC02	UNC
ISGW01	UNC
ISGW02	UNC
SSS	UNC

B.9

Network Management Non-Interactive SSH Connections (DSR – Backup Core to Primary Core)

Table 47: Network Management Non-Interactive SSH Connections (DSR - Backup Core to Primary Core)

Backup Core SSH Client	Primary Core SSH Server
NM Clients – ATIA Log Viewer	ATR
SSS	ATR
UCS	UCS
UNC	UNC
ATR	UNC
ZSS	UNC
PDG	UNC
ZC03	UNC
ZC04	UNC
ISGW03	UNC
ISGW04	UNC
SSS	UNC

B.10

Network Transport SSH Connections (List 2 of 3 for DSR – Primary Core to Backup Core)

Table 48: Network Transport SSH Connections (List 2 of 3 for DSR – Primary Core to Backup Core)

Primary Core SSH Client	Backup Core SSH Server (in all zones; does not include shared transport previously listed)
UNC	Core Routers
UNC	Exit Routers
UNC	Gateway Routers

Primary Core SSH Client	Backup Core SSH Server (in all zones; does not include shared transport previously listed)
UNC	GGSNs
UNC	Core LAN Switches
UNC	Mediation LAN Switches
UNC	IDS LAN Switch
UNC	Fan-out LAN Switches
NM Clients	Core Routers
NM Clients	Exit Routers
NM Clients	Gateway Routers
NM Clients	GGSNs
NM Clients	Core LAN Switches
NM Clients	Mediation LAN Switches
NM Clients	IDS LAN Switch
NM Clients	Fan-out LAN Switches
NM Clients	Core Terminal Server

B.11

Network Transport SSH Connections (List 3 of 3 for DSR – Backup Core to Primary Core)

Table 49: Network Transport SSH Connections (List 3 of 3 for DSR – Backup Core to Primary Core)

Backup Core SSH Client	Primary Core SSH Server (in all zones, does not include shared transport previously listed)
UNC	Core Routers
UNC	Gateway Routers
UNC	Exit Routers
UNC	GGSNs
UNC	Core LAN Switches
UNC	Mediation LAN Switches
UNC	IDS LAN Switch
UNC	Fan-out LAN Switches
NM Clients	Core Routers
NM Clients	Gateway Routers
NM Clients	Exit Routers
NM Clients	GGSNs
NM Clients	Core LAN Switches
NM Clients	Mediation LAN Switches
NM Clients	IDS LAN Switch

Backup Core SSH Client	Primary Core SSH Server (in all zones, does not include shared transport previously listed)
NM Clients	Fan-out LAN Switches
NM Clients	Core Terminal Server

B.12

Edge Availability with Wireline Console (Tsub) SSH Connections (DSR)

The following tables list SSH connections that are utilized for services between the Trunking Subsystem (Tsub) server devices and other devices in the ASTRO® 25 Dynamic System Resilience (DSR) system.

Table 50: Tsub SSH DSR Connections 1

Primary Core (SSH Client)	Backup Core (SSH Client)	Tsub (SSH Server)
NM Client	N/A	Tsub Zone Controller (ZC)
NM Client	N/A	Tsub IP Packet Capture
NM Client	N/A	Tsub VMS
N/A	NM Client	Tsub Zone Controller (ZC)
N/A	NM Client	Tsub IP Packet Capture
N/A	NM Client	Tsub VMS

Table 51: Tsub SSH DSR Connections 2

Tsub (SSH Client)	Primary Core (SSH Server)	Backup Core (SSH Server)
Tsub Zone Controller (ZC)	Unified Network Configurator (UNC)	N/A
Tsub Zone Controller (ZC)	N/A	Unified Network Configurator (UNC)
Tsub Zone Controller (ZC)	Backup and Restore (BAR) Server	N/A
Tsub IP Packet Capture	Backup and Restore (BAR) Server	N/A